FortiTester Handbook

VERSION 3.9.0

May 18, 2020
FortiTester 3.9.0 Handbook

TABLE OF CONTENTS

Change Log

Date	Change Description
May 18, 2020	FortiTester 3.9.0 initial release.

Introduction

Welcome, and thank you for selecting Fortinet products for your testing environment.

FortiTester™ appliances and VMs offer an enterprise-grade solution for performance testing and validating their network security infrastructure and services, providing a comprehensive range of application test cases to evaluate equipment and right-size infrastructure. All test functionality is included in one simple device-based license. FortiTester is also ideal for testing performance and security of next-gen firewalls and applications on public cloud infrastructures. It is available in most major public cloud marketplaces.

FortiTester provides powerful yet easy-to-use test cases that simulate many applications and a case history browser for simple analysis. It enables you to establish performance standards and run audits to validate they continue to be met. A single 40 GE appliance allows 20 million concurrent connections and new TCP connection rates greater than 1 million/second, hardware-based acceleration supports new HTTPS connection rates above 20,000/second. Up to 4 appliances can be grouped in Test Center mode to massively scale performance. 40 GE device interfaces can be split to 4x 10 GE SPF+ for additional testing flexibility. Furthermore, the virtual appliance version provides an ideal tester for NFV and SDN environments.

Meanwhile, the 100 GE device has a single QSFP28 interface and is designed to run in test center mode. Two devices in test center mode have 93 Gbps HTTP throughput and 76,000,000 HTTP concurrent connections.

FortiTester implements DPDK, which provides libraries and user-space NIC drivers for accelerated packet processing performance. The implementation allows FortiTester to offer comprehensive line-rate testing on server-class hardware.

This document describes how to set up your FortiTester appliance. It also describes how to use the web user interface (web UI) and command-line interface (CLI).

Features and benefits

FortiTester is a network traffic test tool that is based on Fortinet's specialized hardware and software platform. It provides performance tests, security tests, and ATT&CK tests.

Performance tests

HTTP CPS test

FortiTester tests HTTP new connections per second (CPS) performance by simulating multiple clients that generate HTTP traffic.

HTTP RPS test

FortiTester tests requests per second (RPS) performance by simulating multiple clients that generate HTTP traffic.

HTTP CC test

FortiTester tests HTTP concurrent connection (CC) performance by simulating multiple clients that generate HTTP traffic. All connections include a TCP three-way handshake, a loop of HTTP requests and responses (complete HTTP transaction), and close the connection with TCP FIN.

HTTP throughput test

FortiTester tests HTTP throughput performance by simulating multiple clients that generate HTTP traffic.

HTTPS CPS test

The HTTPS CPS test is almost the same as the HTTP CPS test, except that it uses HTTPS traffic, and does not have the Limit by option; also, the MTU is editable.

HTTPS RPS test

The HTTPS RPS test is the same as the HTTP RPS test, except that it uses HTTPS traffic, and does not have the Limit by option; also, the MTU is editable.

HTTPS CC test

The HTTPS CC test is the same as the HTTP CC test, except that it uses HTTPS traffic and the MTU is editable.

HTTPS throughput test

The HTTPS Throughput test is the same as the HTTP Throughput test, except that it uses HTTPS traffic and the MTU is editable.

IPsec remote access test

FortiTester tests IPSec remote access by establishing a remote access IPSec tunnel, completes a full set of HTTP transactions (TCP connection, HTTP request, HTTP response, TCP connection close) through the tunnel, and terminates the tunnel.

IPsec remote access CC test

FortiTester tests IPSec remote access tunnel concurrent connections (CC) by establishing a remote access IPSec tunnel, completes a full set of HTTP transaction (TCP connection, HTTP request, HTTP response, and TCP connection close) through the tunnel, and terminates the tunnel.

SSL VPN tunnel CC test

FortiTester tests the DUT's ability to support concurrent SSL VPN tunnel connections by establishing a large number of concurrent SSL VPN tunnel connections and completing a full round of HTTP transactions through each tunnel.

UDP PPS test

FortiTester tests UDP throughput by sending a specified size of UDP frames at a maximum or limited speed from simulated clients to simulated servers.

UDP Payload test

FortiTester tests UDP payload by sending UDP frames with the specified payload from the client ports to the server ports.

TCP throughput test

FortiTester tests TCP throughput by generating a specified volume of two-way TCP traffic flow via specified ports.

TurboTCP test

FortiTester tests TurboTCP connections per second (CPS) performance by generating a specified volume of two-way TCP traffic flow via specified ports.

TCP connection test

FortiTester tests TCP concurrent connection performance by generating a specified volume of two-way TCP traffic flow via specified ports.

RFC 2544 throughput test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 throughput. According to RFC2544, throughput is the fastest rate for the number of test frames transmitted by the DUT, which is equal to the number of test frames sent to it by the test equipment.

RFC 2544 latency test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 latency. According to RFC1242, for store and forward devices, latency is the time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port.

RFC 2544 loss rate test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 loss rate. According to RFC2544, to determine the frame loss rate, as defined in RFC1242 of a DUT throughout the entire range of input data rates and frame sizes.

RFC 2544 back to back test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 back to back. According to RFC 2544, to characterize the ability of a DUT to process back-to-back frames as defined in RFC 1242.

RFC 3511 IP throughput test

FortiTester tests the ability of the DUT to handle network-layer data throughput. RFC 3511 is specifically focused on firewall performance.

RFC 3511 Concurrent Capacity throughput test

FortiTester tests the ability of the DUT to determine the maximum number of entries it can store in its connection table.

Amazon S3 test

The Amazon S3 test simulates Amazon S3 (Simple Storage Service) traffic, such as file uploading and downloading, and folder creating.

AOL Chat test

The AOL Chat (AIM) establishes a TCP connection (three-way handshake), simulates a AIM session, and closes the TCP connection.

BitTorrent test

The TCP BitTorrent test simulates a download process between peers.

DB2 test

The DB2 test establishes a TCP connection (three-way handshake), sends SQL command by DB2, and then closes the TCP connection.

Facebook test

The Facebook test simulates Facebook traffic, such as login, search and watch video.

Gtalk test

The Gtalk test establishes a TCP connection (three-way handshake), simulates a Gtalk chat by XMPP, and closes the TCP connection.

Gmail test

The Gmail test establishes a TCP connection (three-way handshake), sends one email by Gmail and closes the TCP connection.

MSSQL test

The test traffic establishes a TCP connection (three-way handshake), sends MSSQL command by MSSQL client, and then closes the TCP connection.

MySQL test

The MySQL test establishes a TCP connection (three-way handshake), sends SQL command by MySQL, and then closes the TCP connection.

Netflix test

The Netflix test establishes a TCP connection (three-way handshake), and simulates Netflix traffic, such as login, watching movie and logout.

Oracle TNS test

The Oracle TNS test establishes a TCP connection (three-way handshake), connects and authenticates to databases, and then closes the TCP connection.

PSQL test

This FortiTester test establishes a TCP connection (three-way handshake), send psql command by PSQL, and then closes the TCP connection.

Twitter test

The Twitter test simulates Twitter traffic, such as post article and watch video.

WebEx test

The WebEx test establishes a TCP connection (three-way handshake), and simulates WebEx traffic, such as login and WebEx.

WhatsApp test

The WhatsApp case establishes a TCP connection(three-way handshake), controls media sessions between end points and closes the TCP connection.

Yahoo Mail test

The Yahoo Mail test establishes a TCP connection (three-way handshake), sends one email by Yahoo and closes the TCP connection.

YouTube test

The TCP YouTube test simulates YouTube client to connect to a YouTube server and access audio or video streams.

TCP Protocol CIFS/SMB test

The TCP CIFS/SMB test establishes a TCP connection (three-way handshake), simulates a SMBv2 session, and closes the TCP connection.

TCP Protocol FIX test

The TCP FIX test establishes a TCP connection (three-way handshake), simulates a FIXv3 session, and closes the TCP connection.

TCP Protocol FTP test

This FortiTester test establishes a TCP connection (three-way handshake), transfers one file by FTP, and then closes the TCP.

TCP Protocol IMAP test

FortiTester tests the ability of the DUT to handle different types of IMAP. This test establishes a TCP connection (three-way handshake), receives one email by IMAP and closes the TCP connection.

TCP Protocol LDAP test

This FortiTester test establishes a TCP connection (three-way handshake), searches entries by LDAP, and then closes the TCP connection.

TCP Protocol NFS test

The TCP NFS test establishes a TCP connection (three-way handshake), simulates a NFSv3 session, and closes the TCP connection.

TCP Protocol POP3 test

FortiTester tests the ability of the DUT to handle different types of POP3. This test traffic establishes a TCP connection (three-way handshake), receives one mail by POP3 and closes the TCP connection.

TCP Protocol RDP test

The test traffic establishes a TCP connection (three-way handshake), constructs a RDP connection, sends fastpath format events and then closes the TCP connection.

TCP Protocol SMTP test

FortiTester tests performance of a target device under SMTP traffic by simulating a volume of clients to generate SMTP traffic.

TCP Protocol SSH test

This test establishes a TCP connection (three-way handshake), simulates a SSH interactive session and closes the TCP connection.

UDP Protocol DNS latency test

FortiTester tests the latency of the DUT while handling DNS query requests. The DUT could be a gateway device or a DNS server. This test traffic sends DNS requests to a DNS server and measures latency.

UDP Protocol NTP test

The NTP test sends NTP query traffic to an NTP server under test. FortiTester receives real time information from the DUT and measures latency.

UDP Protocol RADIUS test

The RADIUS test sends RADIUS requests to a RADIUS server to measure the number of response types per second.

UDP Protocol SIP test

FortiTester tests UDP SIP by sending UDP frames with the specified SIP from the client ports to the server ports.

UDP Protocol TFTP test

The TFTP test sends TFTP requests to a TFTP server to measure the number of requests sent and performed per second.

DHCP test

The IPv4 DHCP test sends DHCP requests to the DHCP server and measures latency. The IPv6 DHCP test sends NS and RA messages to request an IPv6 address through DHCPv6 stateless mode.

IGMP test

The IGMP test sends join messages to the device under test (DUT), such as a router or firewall, and the DUT forwards the data stream from the server.

RTSP/RTP test

The RTSP/RTP test establishes a TCP connection with a three-way handshake, controls media sessions between end points, and closes the TCP connection. This test also tests the firewall's ability to open and close pinholes.

Traffic Replay test

FortiTester tests user-defined scenarios by replaying pcap files. Typically, pcap files are generated by programs like tcpdump or Wireshark.

GTP Replay test

FortiTester tests GTP connections by replaying existing GTPv1 and GTPv2 files. FortiTester uses these files to send test packets to the device under test (DUT).

Packet capture test

The packet capture test captures packets received from the network adapter.

Mixed traffic test

FortiTester tests mixed traffic performance by simulating multiple clients that burst all types of traffic simultaneously.

Security tests

DDoS single packet flood test

FortiTester tests the DUT's ability to handle different types of DDoS attacks. This test attempts to deplete the DUT's resources by flooding the DUT with non-session based attacks.

DDoS TCP session flood test

FortiTester tests the DUT's ability to handle different types of DDoS attacks. This test attempts to deplete the DUT's resources by flooding the DUT with TCP attacks.

DDoS HTTP session flood test

FortiTester tests the DUT's ability to handle attempts to deplete the DUT's resources by flooding the DUT with HTTP attacks.

DDoS concurrent session flood test

FortiTester tests the DUT's ability to handle attempts to deplete the DUT's resources. FortiTester floods the DUT with HTTP attacks and then puts the session on hold for an extended period of time.

DDoS UDP packet flood test

FortiTester tests the DUT's ability to handle attempts to deplete DUT's resources. FortiTester floods the DUT with UDP packets with random source IP and port on client-traffic side.

IPS Attack Replay test

FortiTester can test security systems by replaying a predefined or customized set of attack traffic. The predefined set covers 100 types of attacks. The test result shows the CVE-ID for every type of attack. You can also see the attack list in the Cases > Security Testing > IPS > Attack page.

IPS HTTP Evasion test

The HTTP Evasion Replay test replays packet tampered through HTTP evasion engine. FortiTester corrupts custom HTTP pcap file according to the selected Evasion Types, then replay such corrupted pcap files to target servers to see if servers have the ability to resist such attack.

AntiVirus test

This test sends files with HTTP/FTP/SMTP/IMAP/POP3 protocol and detect viruses in files.

Web crawler test

The web crawler test runs a web crawler simulation to query URLs through the DUT. This is done to test the DUT's web access security policies.

Web Protection test

The Web Protection test simulates sending web application attacks expected to be detected by the security DUT..

ATT&CK tests

ATT&CK Testing

FortiTester simulates the actions that a real adversary would do on the clients' systems. It features a Remote Access Tool (RAT) that performs adversary actions on infected hosts and copies itself over the whole network to increase its foothold.

What's new

FortiTester 3.9.0 offers the following new features and enhancements:

New features

New Application cases

According to the latest 2019 NSS tests for NGFW, FortiTester adds these cases to simulate sessions of these applications. This allows you to choose popular applications when configuring traffic mix tailored to your environment.

- DB2
- MySQL
- Netflix
- WebEx

ECN (Explicit Congestion Notification) support

FortiTester now supports ECN option to control the TCP-base applications which is defined in RFC 3168. This option allows end-to-end notification of network congestion without dropping packets.

RESTful API Browser

FortiTester supports comprehensive REST API for automation such as case/object creation, and test running, etc. A new API Browser item will appear on **Homepage**.

For more information, see Using the REST API.

Pre/post scripts added in Script Object

Scripts in **Performance Testing > Objects > Scripts > Scripts Management > Script Settings** are separated into Pre Test script and Post Test script which will be executed before and after the case runs respectively. FortiTester also allows to add multiple API calls in the script object. You can also click **Test Script** to check whether the script is executable.

For more information, see Using script object templates.

Running case page optimized for ease of viewing

Widget view is optimized for ease of viewing, you can customize view-port to show the statistics.

- Floating windows are supported for each result column.
- You can choose to minimize or adjust the size of each window.
- You can click hide buttons to minimize the running status and navigation areas.

Client Certification Authentication supported in HTTPS Application mode

FortiTester now supports simulating the mutual certificate based authentication cases in Application Mode.

For more information, see HTTPS Cases.

Radius support for administrator login

RADIUS server can be added in FortiTester to authenticate the administrator accounts when they log in.

For more information, see Configuring a RADIUS server.

Custom TLS certificate support

It is now supported to add custom TLS certificates for the HTTPS access to FortiTester's GUI.

For more information, see Uploading TLS certificates

Idle timeout for FortiTester GUI session

You can define **Idle Timeout** to expire a FortiTester GUI session if it idles for a certain period of time.

For more information, see Configuring specific settings.

Enhancements

GUI changes

In this release, the following GUI changes are made:

- A new Application category is added in **Performance Testing.**
- Move Amazon S3, AOL Chat, BitTorrent, Facebook, Gtalk, Gmail, MSSQL, Oracle TNS, PSQL, Twitter, WhatsApp, Yahoo Mail, and YouTube cases from **Performance Testing > Protocol** to **Performance Testing > Application.**
- A new API Browser column is added to the welcome page.

Virtual Router support in server side in HTTP/HTTPS proxy

FortiTester now supports Virtual Router in both client and server profile for HTTP/HTTPS proxy mode. It is helpful to reduce the environment IP address list especially in the cloud environment.

Virtual Router support in Attack Replay case

When creating an attack replay case and the DUT Working Mode is NAT in Case Options configuration, Virtual Router is supported on both the Client side and Server side.

Loops and Delay support in AntiVirus/Web Protection/IPS Replay/IPS HTTP Evasion Profiles

FortiTester allows you to control the loops count and the delay time in AntiVirus/web protection/IPS replay/IPS HTTP evasion cases.

Script Config change support in all cases

For all existing cases, you can now update the Script Config in **Basic Information** when editing the case.

SNMP Monitor change support in all cases

For all existing cases, you can now update the DUT Monitor in **Basic Information** when editing the case.

Automatic deletion of system events older than 7 days

In this release, the system events older than 7 days will be automatically deleted at 0 o'clock every day to release the storage space. This is a system setting and it is not configurable.

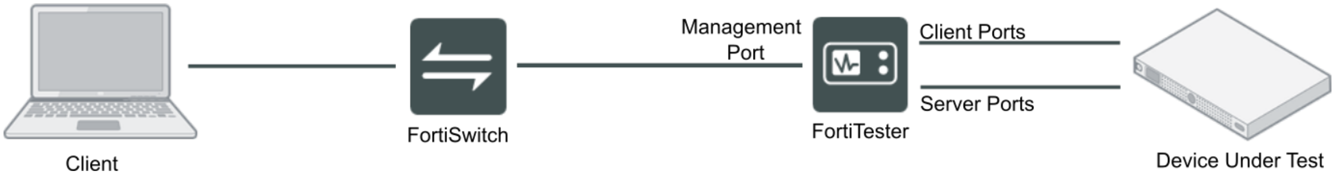
Getting Started

This chapter provides the procedures for getting started with FortiTester.

Connecting to FortiTester

A basic network connection topology for FortiTester is shown in A basic network connection topology on page 20.

A basic network connection topology

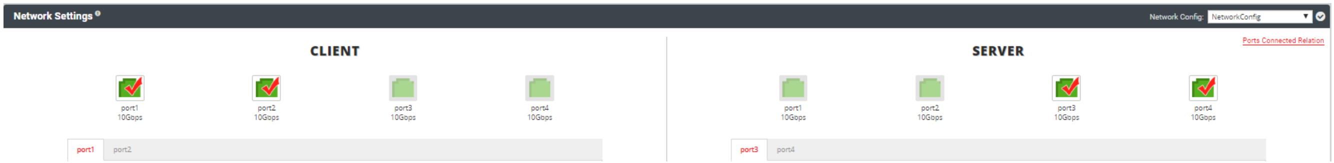


A FortiTester appliance has multiple network ports. In most cases, one port is for management and the others are for testing. The management port (usually mgmt or port1) connects to a local network to enable the user to access the FortiTester appliance via the web UI.

The test ports are divided into client ports and server ports that connect to the device under test (DUT). Client ports simulate multiple client devices that access the simulated server devices via server ports. Use the provided cables to connect the FortiTester to the DUT.

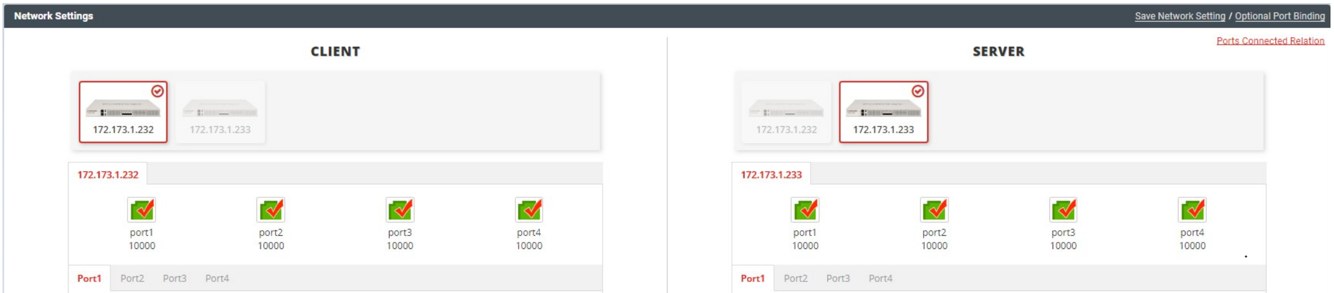
When you use one FortiTester appliance in standalone work mode, the test ports on the standalone appliance are divided between client and server. Test ports in standalone work mode on page 20 shows the distribution of ports in a standalone environment. Port 1, a client port, is paired with port 3, a server port; port 2, a client port, is paired with port 4, a server port.

Test ports in standalone work mode



If your tests require more ports, you can join up to 4 pairs of FortiTester appliances in a Test Center. Test ports in Test Center / Slave work mode on page 20 shows the distribution of ports in a Test Center environment with two FortiTester appliances. Ports 1-4 of the first appliance are client ports; ports 1-4 of the second appliance are server ports. Port 1 on the first appliance is paired with port 1 on the second appliance.

Test ports in Test Center / Slave work mode



For information on configuring a Test Center, see Test Center.

Configuring the management port

The management port must be connected to the same switch as the administrator client computer. Use the ethernet cord provided with the FortiTester.

The following procedure assumes that the default management port IP address (192.168.1.99) is not on the same subnet as your client computer.

To configure the management port:

1. Configure your computer to match the FortiTester default management port subnet.
   For example, from the Control Panel (Windows 7), go to **Network and Internet > Network and Sharing Center**. Click the **Local Area Connection** link, and then click the **Properties** button. Select **Internet Protocol Version 4 (TCP/IPv4)** and then click its **Properties** button. Select **Use the following IP address**, and then enter the following settings:
   - IP address: 192.168.1.2
   - Subnet mask: 255.255.255.0
2. To connect to the web UI, start a web browser and go to http://192.168.1.99, or https://192.168.1.99.
3. Type **admin** in the Username field, enter the password, and then click **Login**.
4. In the top right banner, click **System > Network > Interfaces** to display the **Interfaces Setting** page.
5. Configure the following settings.

Addressing Mode	Specify whether FortiTester acquires an IPv4/IPv6 address for this network interface manually or using DHCP.
IPv4/IPv6	Type the IP address.
Netmask/IPv6 Netmask	Type the netmask.
Gateway/IPv6 Gateway	Type the gateway address.

6.
7. Click **Apply** to complete the management port configuration.

Configuring DNS settings

Like many other types of network devices, FortiTester appliances require connectivity to DNS servers for DNS lookups.

Your Internet service provider (ISP) may supply IP addresses of DNS servers, or you may want to use the IP addresses of your own DNS servers. You must provide unicast, non-local addresses for your DNS servers. Local host and broadcast addresses will not be accepted.

Incorrect DNS settings or unreliable DNS connectivity can cause issues with other features, including FortiGuard services and NTP system time.

To configure DNS settings via the web UI:

1. Go to **System > Network > DNS**.
2. In **Primary DNS Server**, type the IP address of the primary DNS server.
3. In **Secondary DNS Server**, type the IP address of the secondary DNS server.
4. Click **Apply**.
   The appliance will query the DNS servers whenever it needs to resolve a domain name into an IP address, such as for NTP system time, FortiGuard services, or web servers defined by their domain names (“domain servers").

Configuring system time

Go to **System > Dashboard > Status** to change the system time. You can manually modify the time or synchronize the system time with an NTP server.

To configure system time:

1. Click **Change** at the end of **System Time**.
2. From the **Time configuration** dialogue box, select **Time Zone** from the drop down list, and click **Apply**.
3. Check **Set Time**, set the time, and click **Apply**.
4. Or check **Synchronize with NTP server**, enter the IP address or domain name of an NTP server; for **Sync Interval**, set the internal to calibrate more accurate time. Click **Apply**.
5. Click **Close** to finish the time setting.

System Time

Settings	Guidelines
Time Zone	Select the time zone where the FortiTester appliance is installed.
Set Time	The text boxes are populated with the current settings for the system date and time. You can change these manually.
Synchronize with	Enter the IP address or domain name of an NTP server. To find an NTP server that

Settings	Guidelines
NTP Server	you can use, see http://www.ntp.org. The time is not synched at a regular interval, only when you click the Save button.

Changing the admin password

FortiTester has a default user **admin**.

To change the password for the admin account:

1. In the top right banner, hover over **admin**.
2. Select **Modify Password** from the drop down menu.
3. Enter the old password, the new password twice, and click **Save**.

Configuring the device under test

The DUT must be configured to connect with FortiTester before tests can be run.

If the DUT is a FortiGate appliance, you generally need to configure interfaces, routes, and a firewall policy. Gateways for the test case are typically set as the IP address of the FortiGate's interfaces. If the client and server subnets are not on the same network as the gateway addresses, routes must be added.

Running Tests

This chapter provides procedures for running tests and viewing test results.

Test case configuration overview

The test case configuration workflow includes the following standard elements:

- Test type—The test template to use. It determines the mandatory and optional settings for specific cases.
- Case options—IP version, DUT role, DUT mode, network configuration, optional port binding, VLAN and Client Virtual Router.
- Interface ports—Client and server interface port configuration.
- Optional elements—Enable or disable packet capture and MAC masquerade.
- Test case specifics—Variables that determine the test parameters, such as load, rates/limits, and client/server profiles and actions.

The first four items set up the basic test environment. Once you become familiar with them, you can assume they can be configured in the same manner for each test. The Client Virtual Router will simulate a router between FortiTester's client subnets and the connected DUT.

The test case specifics are key to testing the performance of the device under test (DUT). We recommend you become familiar with guidelines for test case specifics whenever you get started with a new test case type.

Using network configuration templates

Many test cases you may want to run will have the same basic network setup. To simplify configuration, you can create a network configuration template and then import it when you initially configure test case settings. The template settings are used to populate the network settings for the new test case configuration.

The network configuration template specifies the IP address type, DUT working mode, client/server port settings, subnet settings, port binding, and VLAN settings, etc.

You can only import template settings if the IP address type and DUT working mode you select in the new test case popup dialog box match the settings in the network configuration template.

After the settings have been imported, you can modify client/server port settings, subnet settings, port binding and VLAN settings if necessary.

Creating a network configuration template

To create a network configuration template:

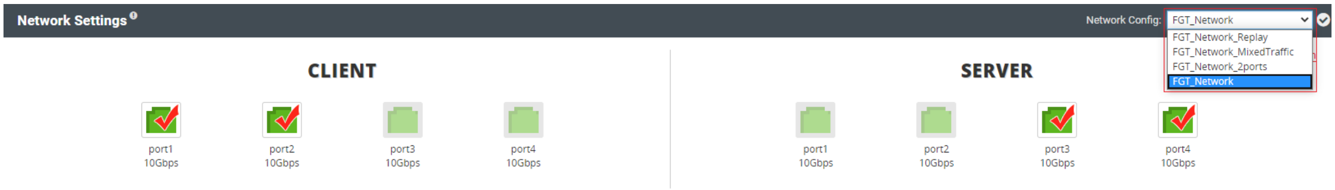
1. Go to **Objects > Networks** under either **Performance Testing** or **Security Testing**.
2. Click **Add** to display the configuration page.
3. In the popup dialog, configure the following settings:

Settings	Guidelines
IP Version	Select IPv4, IPv6 or mixed version.
DUT Role	Select Network Gateway or Application Server. If you want to test an application server, the FortiTester appliance will work as a pure client; if you want to test a network gateway, it will work as both client and server.
DUT Working Mode	• Transparent mode: the DUT does not change the IP address of the packet. In NAT mode, the device is considered to be a router hop and the IP addresses can be translated. • NAT mode: the DUT does not change the IP address of the packet. • Web Proxy mode: the proxy address is used. If the DUT is configured in Web Note: This setting will be shown only when DUT role is **Network Gateway**.
Tester and Application Server	Specify that the FortiTester appliance and the application server are in the same subnet or route by a gateway to send/receive traffic. Note: This setting will be shown only when DUT role is Application Server.
Port Binding	Optional. Port binding aggregates two or more physical ports into one logical port.
Support NAT Policy	Optional. Select SNAT/DNAT to allow DUT to do source and destination NAT on the same session, or select NAT64/NAT46 to allow IPv6 addressed hosts to communicate with IPv4 addressed hosts and vice-versa. **Note:** If the DUT performs SNAT/DNAT on the data traffic, use the **Translated To** field to change the IP address before starting the run. Note: This setting will be shown only when DUT Working Mode is Network Address Translation (NAT).
Support	The network for the three cases are different from the general network, so configure the network specially for them. When the DUT Role is Application Server, only Web Crawler is supported.
Virtual Router	Optional. This option allows the clients and/or servers to be on subnets different from the DUTs interfaces and all traffic to/from the DUTs uses the virtual router's MAC address.

4. Click **OK** to continue.
5. Complete the configuration as described in Network configuration object settings on page 26.
6. Save the configuration.

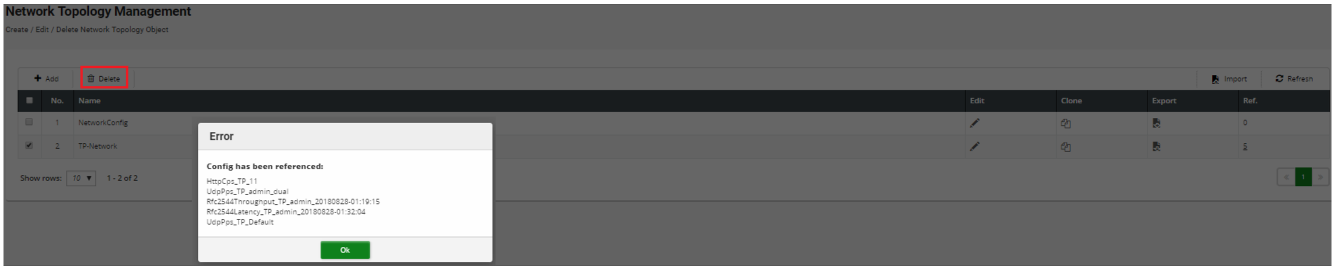
After you have created a network configuration template, you can clone it, or export it as a zip file and import the zip file later.

If you select self-created template instead of the default template, you can now select the created **Network Config** templates from the option list on a test case page as below. Select the template and click ✓ to apply this network configuration.



Tip: If you select the default template when creating a test case, here it does not support template switch.

Also, for old test cases that refer to this network configuration template, the template can not be deleted.



Network Topology Management

Create / Edit / Delete Network Topology Object

■	No.	Name	Edit	Clone	Export	Ref.
□	1	NetworkConfig				0
☑	2	TP-Network				5

Show rows: 10 ▼ 1 - 2 of 2

Error

Config has been referenced:

HttpCps_TP_11
UdpPps_TP_admin_dual
Rfc2544Throughput_TP_admin_20180828-01:19:15
Rfc2544Latency_TP_admin_20180828-01:32:04
UdpPps_TP_Default

Configuring network configuration object settings

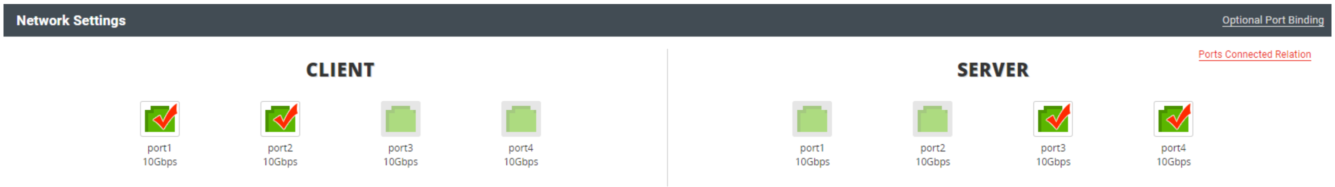
Network configuration object settings

Settings	Guidelines
Basic Information	
Name	Specify a configuration name. The name appears in the Network Config drop-down list when you configure test cases.
Network Settings	
Client Ports, Server Ports	The page lists all the test ports for client-side and server-side connections. The client ports simulate the behavior of clients; the server ports simulate the behavior of servers. FortiTester builds the TCP connections between client ports and server ports (and through the DUT, of course). You must select at least one client port and one server port. After you select a port for client, a ✓ (check mark) is displayed on the port icon. The same port on the server side is no longer available.

Settings	Guidelines
	Note: You don’t need to select the server port if you've selected the DUT role as Application Server.
MAC Masquerade	
MAC Masquerade	Specify the first two bytes of a MAC address for the traffic.
QinQ	
Outer VLAN ID	Specify a Service VLAN tag for FortiTester to use during the test.
Subnet	
IP Address or Range	Specify a single IP address with standard format (for example, 10.1.2.1) or an address range like 10.1.2.1-10.1.2.99.
Translated To	NAT mode only. If the DUT uses SNAT/DNAT, specify the new, translated, IP address.
Netmask	Specify a netmask between 1 and 31.
NAT46 Prefix	Available only when NAT46 is selected as the Support NAT Policy.
NAT64 Prefix	Available only when NAT64 is selected as the Support NAT Policy.
External Address or Range	Available only when NAT46/NAT64 is selected as the Support NAT Policy.
External Address Netmask	Available only when NAT46/NAT64 is selected as the Support NAT Policy.
VLAN ID	Specify a VLAN ID between 1 and 4094.
Server IP	When the DUT role is an application server, specify a single IP address in the standard format.
Gateway	Specify the gateway IP address when the DUT role is an application server or the DUT working mode is in NAT mode.
Peer Network	NAT mode only. Specify the peer network subnet address. If the DUT uses SNAT/DNAT, use the translated IP address.
Proxy IP/Mask	Web Proxy mode only. Specify the proxy IP address/netmask.
Add Subnet	If necessary, click + Add Subnet to display additional subnet configuration controls. An interface port can have multiple subnets. FortiTester uses IP addresses in the specified subnets to create TCP connections and transfer data.
Remove Subnet	Click 🗑 Remove to remove the mapping subnet.

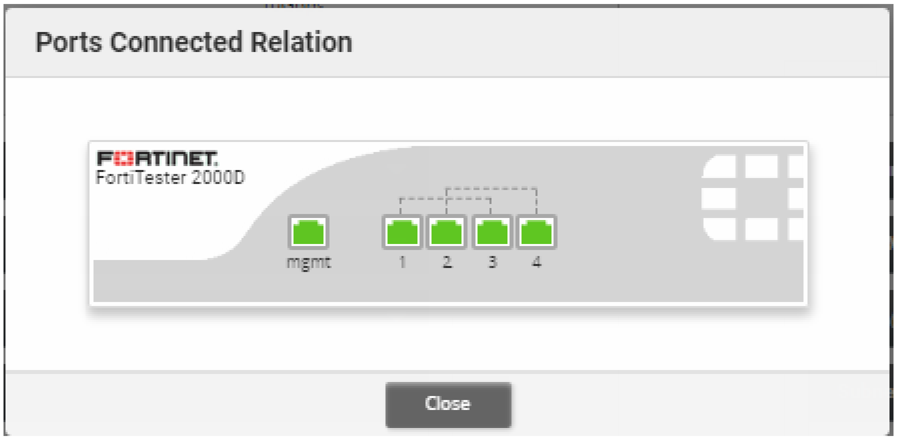
Using Ports Connected Relation

Ports Connected Relation link allows you to know the port connection status.

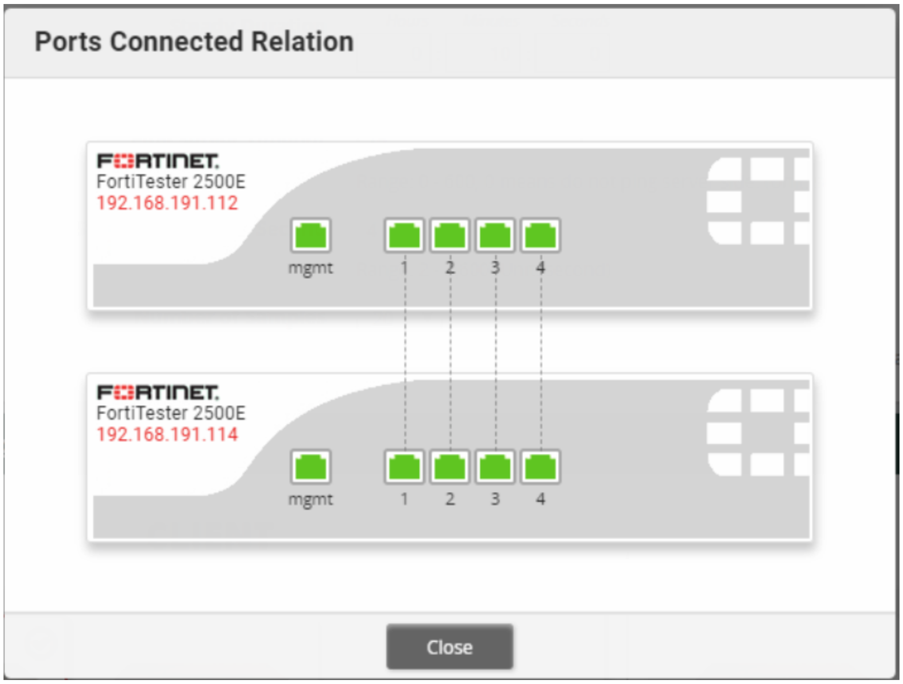


Click the link, and you can see figures below:

Standalone Mode



TestCenter Mode



Using port binding and link aggregation

FortiTester system can bind multiple physical ports as one logical port. We call this feature *port binding*. The physical ports in one logical port share one network configuration, such as IP address, netmask, and gateway.

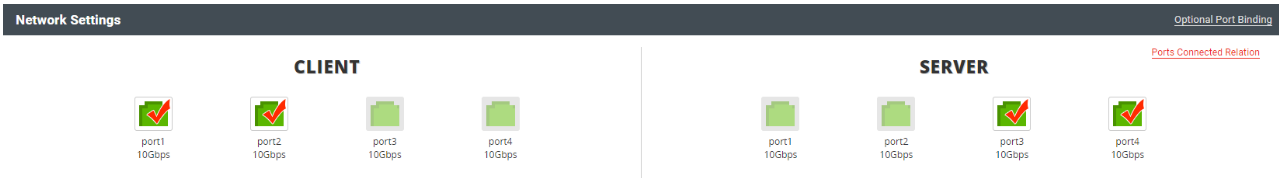
This feature is useful in the following scenarios:

- To test the link aggregation feature of a DUT. A DUT might also support port binding (also called link aggregation or TRUNK). In that case, FortiTester can test this feature and its performance.
- To test 40G/100G ports of DUT. A DUT might have some ports that have bandwidth greater than a single FortiTester port. To test such port performance, we can bind multiple FortiTester ports as one logical port and connect to a switch to transfer traffic with a DUT. For example, a FortiTester appliance can bind 4 10G ports as one to test a 40G port in DUT via a 10G/40G switch.

FortiTester averages traffic on physical ports that belong to one logical port.

To change the port binding:

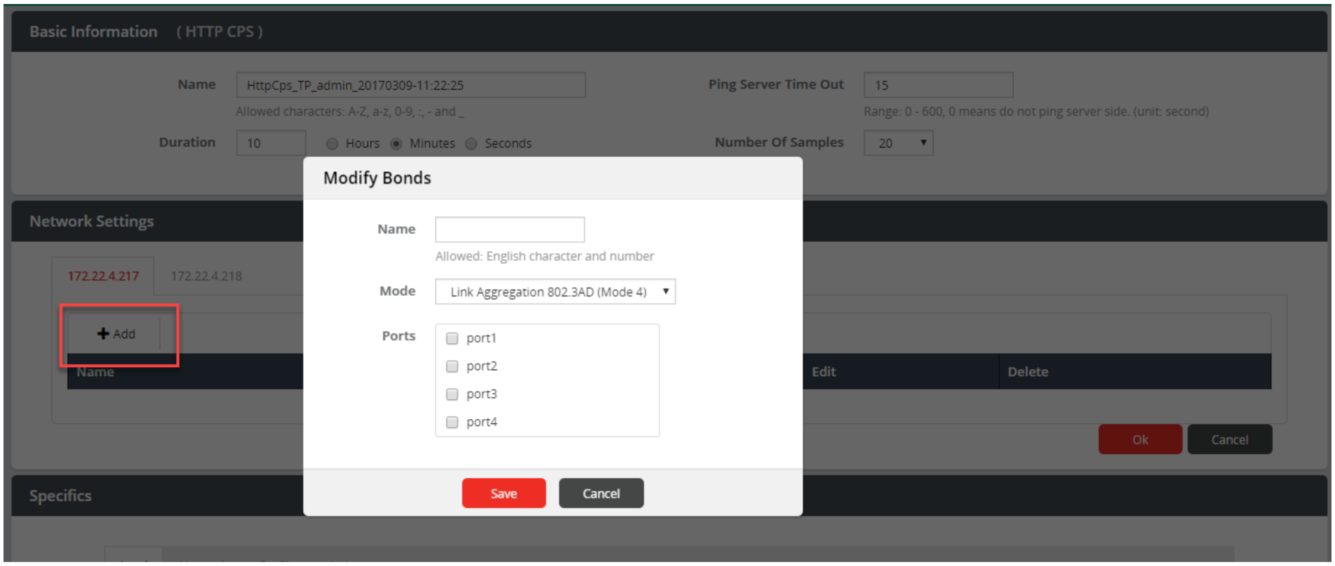
1. When you create a test case, in its **Network Settings** pane, click on the **Optional Port Binding** link.



2. Click **Add**, under Network Settings.

3. Configure the settings. You can configure the number of bond interfaces and member ports, as well a the bond type.
4. Click **Save**.

Optional Port Binding Configuration



Basic Information (HTTP CPS)

Name: HttpCps_TP_admin_20170309-11:22:25
Allowed characters: A-Z, a-z, 0-9, :, - and _

Ping Server Time Out: 15
Range: 0 - 600, 0 means do not ping server side. (unit: second)

Duration: 10 ○ Hours ● Minutes ○ Seconds

Number Of Samples: 20

Modify Bonds

Name:
Allowed: English character and number

Mode: Link Aggregation 802.3AD (Mode 4)

Ports:
□ port1
□ port2
□ port3
□ port4

Using 40 G to 4 × 10 G fan out

FortiTester now supports 4 × 10 G fan out. This feature splits the 40 G port into four separate 10 G ports. Use the corresponding cable to link the 10 G ports to the DUT.

This is available only on FortiTester 3000E.

To enable fan-out:

1. Go to **System > Settings**.
2. Switch 40 G fan-out 4 × 10 G to Enabled.
3. Click **OK** .
4. Wait for the system to reboot.

After you have rebooted the system, the fan out should be enabled. You can check it from **System > Settings**.

Creating file objects

Some of the test cases require you to upload a file. To simplify the configuration, you can create a file object and then import it when you configure test case settings.

To create a file object:

1. Go to **Cases > Performance Testing > Objects > Files**.
2. Click **Add** to display the configuration page.
3. In the popup dialog, choose the file template.
4. Click **OK**.
5. Under **File Management**, click **Choose File** to select the file from your local directory.
6. Click to upload the file.
   Repeat this step if you want to upload multiple files.
   Also, you can compress multiple files into a ZIP file and then upload it. After you upload the ZIP file, you can check Unzip file to uncompress it.
7. Click **Close**.

After you have created a file object, you can clone or export it as a zip file. This object can now be referenced when you create a test.

Creating DNS host group

Some of the cases require DNS hosts to look up the IP address of a domain name. You can create a DNS host group and add DNS hosts in it, then reference the host group when creating test cases.

To add DNS servers:

1. Go to **Cases > Performance Testing > Objects > hosts**.
2. Click **Add**.
3. Enter a name for the DNS host.
4. Click **OK**.
5. Click **Add** under **Host Management**.
6. Enter the hostname and its IP address.
7. Click **OK**.
8. Repeat step 5 to 7 if you want to add more hosts.

To add DNS host groups:

1. Go to **Cases > Performance Testing > Objects > Host Groups**.
2. Click **Add**.
3. Enter a name for the host group.
4. Click **OK**.
5. Click **Add** under **Host Group Management**.
6. Select the port and the host you have created in **Cases > Performance Testing > Objects > hosts**.
7. Click **OK**.

You can later reference the host group when you create test cases.

Using certificate groups

Some of the test cases you may want to run will require you to provide SSL certificates. To simplify configuration, you can create a certification group and then reference it when you configure test case settings.

You can first upload the certificates on **Certificates** page, then bind them together in a group on the **Certificate Groups** page. When you create test cases, you can reference the certificate group.

To upload a certificate:

1. Go to **Cases > Performance Testing > Objects > Certificates**.
2. Click **Add** to display the configuration page.
3. Click Choose file to select the certificate file and key file from your local directory.
4. Click **Import**.
5. Enter the passphrase.
6. Click **Close**.

To upload a certificate group:

1. Go to **Cases > Performance Testing > Objects > Certificate Groups**.
2. Click **Add**.
3. Enter a name for the certificate group.
4. Select the local certificate and the remote certificate you have upload in **Objects > Certificates**.
5. Click **Save**.

You can later reference the certificate group in the Server tab of the HTTPS and VPN cases .

Creating SNI objects

The SNI object specifies a list of host names that the server will use to match the host name in the SNI extension of client hello messages, and return the corresponding certificate to the client. It can be used in HTTPS profiles.

To create SNI objects:

1. Go to **Cases > Performance Testing > Objects > SNI**.
2. Click **Add**.
3. Enter a name for the SNI group.
4. Click **Add**.
5. Enter the hostname.
6. Select the certificate you have uploaded in **Objects > Certificates**. The server will return the corresponding certificate to the clients.
7. Click **OK**.
8. Repeat step 4 to 7 to add more hostnames.
9. Click **Close**.

Using payload templates

Some of the test cases require you to provide a payload. To simplify the configuration, you can create a payload template and then import it when you configure test case settings.

To create a payload template:

1. Go to **Cases > Performance Testing > Objects > Payloads**.
2. Click **Add** to display the configuration page.
3. In the popup dialog, choose the payload type.
4. Click **OK**.
5. Configure the following settings:
   - Name—The name of your payload template
   - Payload—The payload you want to use
6. Click **Save**.

After you have created a payload template, you can clone or export it as a zip file. This template can now be selected from the payload Group option on the popup dialogue when running a test.

Using URL list templates

Some test cases you want to run require you to provide a list of URLs. To simplify the configuration, you can create a URL list template and then import it when you configure test case settings.

To create a URL list template:

1. Go to **Cases > Security Testing > Objects > URLs**.
2. Click **Add** to display the configuration page.
3. Enter a name for your URL template (a name similar to UrlObject_20180822-21:41:07 is shown by default, and you can rename it).
4. Click **URLs Management**.
5. In the popup dialogue box, add URL by using the Add URL box or the Upload file option.
6. Click **OK**.
7. Click **Save** to save the configuration (at least one URL shall be selected).

After you have created a URL list template, you can clone or export it as a zip file. This template can now be selected from the URL Group option on the popup dialogue when running a test.

Using script object templates

FortiTester allows you to give shell commands to the device under test (DUT) before running a test. To simplify the configuration, you can create a script object template and then import it when you configure test case settings.

To create a script object template:

1. Go to **Cases > Performance Testing > Objects > Scripts**.
2. Click **Add** to display the configuration page.
3. Configure the following settings:
   - Name—The name of your script object template
   - Username—The account of FortiGate
   - Password—The login password of FortiGate
   - DUT IP—The IP of FortiGate
   - Pre Test RESTful API URL & Content—The RESTful API command that runs before the test.
   - Post Test RESTful API URL & Content—The RESTful API command that runs after the test.
4. Click **Test Script** to avoid using a failed script object.
5. Click **Save** to save the configuration.

After you have created a script object template, you can clone or export it as a zip file. This template can now be selected from the Script Config option on the popup dialogue when running a test.

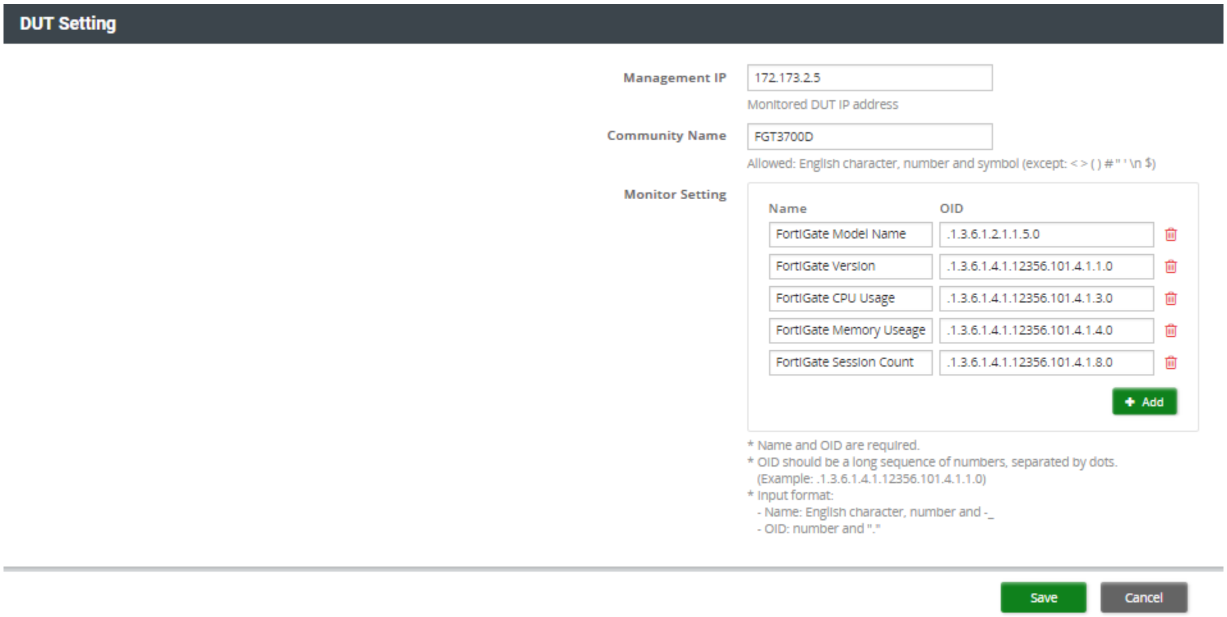
Using DUT monitoring

FortiTester allows you to monitor a FortiGate device under test (DUT) from the management interface. To do so, you must create a DUT monitor object template and then import it when you configure test settings.

To create a DUT monitor object template:

1. Go to **Cases > Objects & Schedule > SNMP Monitors**.
2. Click **Add** to display the configuration page.
3. Configure the following settings:
   - Name—The name of your DUT monitor object template
   - Management IP—The monitored DUT IP address
   - Community Name—The community name you choose for the DUT
   - Monitor Setting—The name and OID for the DUT.

     You can customize the OIDs by clicking ✚ Add or click 🗑 to delete the OID.



DUT Setting

Management IP: 172.173.2.5

Monitored DUT IP address

Community Name: FGT3700D

Allowed: English character, number and symbol (except: < > ( ) # " ' \n $)

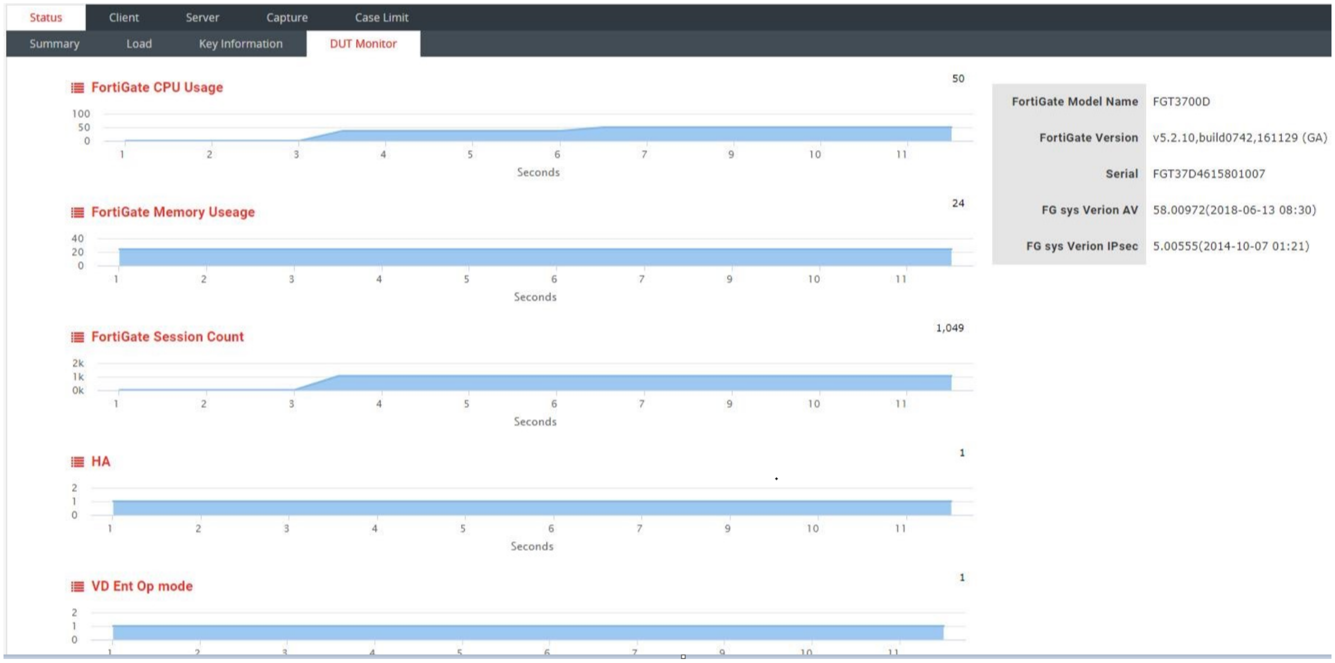
Monitor Setting

Name	OID
FortiGate Model Name	.1.3.6.1.2.1.1.5.0
FortiGate Version	.1.3.6.1.4.1.12356.101.4.1.1.0
FortiGate CPU Usage	.1.3.6.1.4.1.12356.101.4.1.3.0
FortiGate Memory Useage	.1.3.6.1.4.1.12356.101.4.1.4.0
FortiGate Session Count	.1.3.6.1.4.1.12356.101.4.1.8.0

* Name and OID are required.
* OID should be a long sequence of numbers, separated by dots.
(Example: .1.3.6.1.4.1.12356.101.4.1.1.0)
* Input format:
- Name: English character, number and -_
- OID: number and "."

4. Click **Save** to save the configuration.

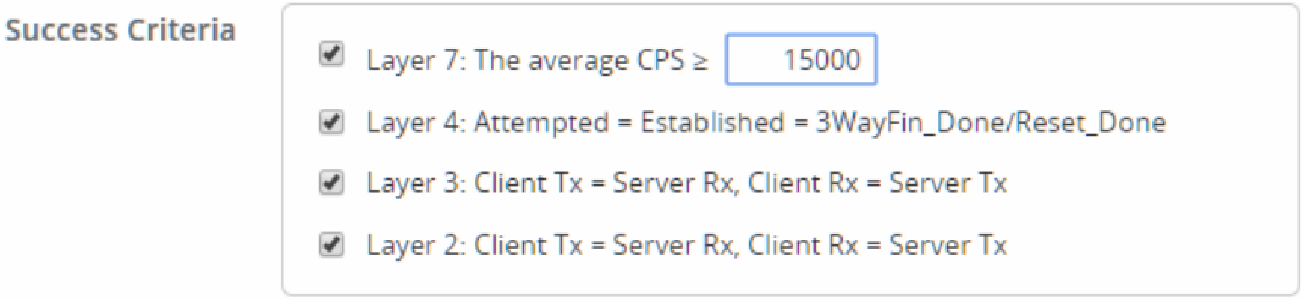
After you have created a DUT monitor template, you can clone or export it as a zip file. This template can be selected from the DUT Monitor option when creating a test. If it is selected, you can monitor the DUT from the **DUT Monitor** tab on the management interface.



FortiGate Model Name	FGT3700D
FortiGate Version	v5.2.10,build0742,161129 (GA)
Serial	FGT37D4615801007
FG sys Verion AV	58.00972(2018-06-13 08:30)
FG sys Verion IPsec	5.00555(2014-10-07 01:21)

Using success criteria

FortiTester allows you to set specific success criteria for HTTP and HTTPS tests.



Success Criteria

☑ Layer 7: The average CPS ≥ 15000

☑ Layer 4: Attempted = Established = 3WayFin_Done/Reset_Done

☑ Layer 3: Client Tx = Server Rx, Client Rx = Server Tx

☑ Layer 2: Client Tx = Server Rx, Client Rx = Server Tx

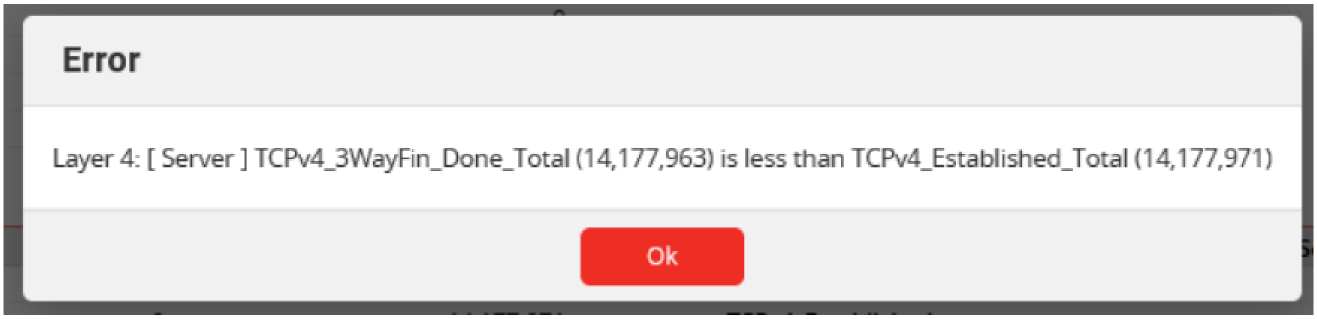
If Layer 7 criteria is set, the test will only be considered successful if the average CPS is equal to or greater than the set number.

If Layer 4 criteria is set, the test will only be considered successful if the number of attempted connections equals to both the number of established connections and the number of connections terminated through a

successful 3-way handshake.

If Layer 2 or Layer 3 criteria is set, the test will be considered successful if the server receives the same number of bytes as the client has sent out, and vice-versa.

If any test fails because of a success criteria, an error message similar to the following will be displayed:



Error

Layer 4: [Server] TCPv4_3WayFin_Done_Total (14,177,963) is less than TCPv4_Established_Total (14,177,971)

The test will have a result of "Failed".

Displaying test status

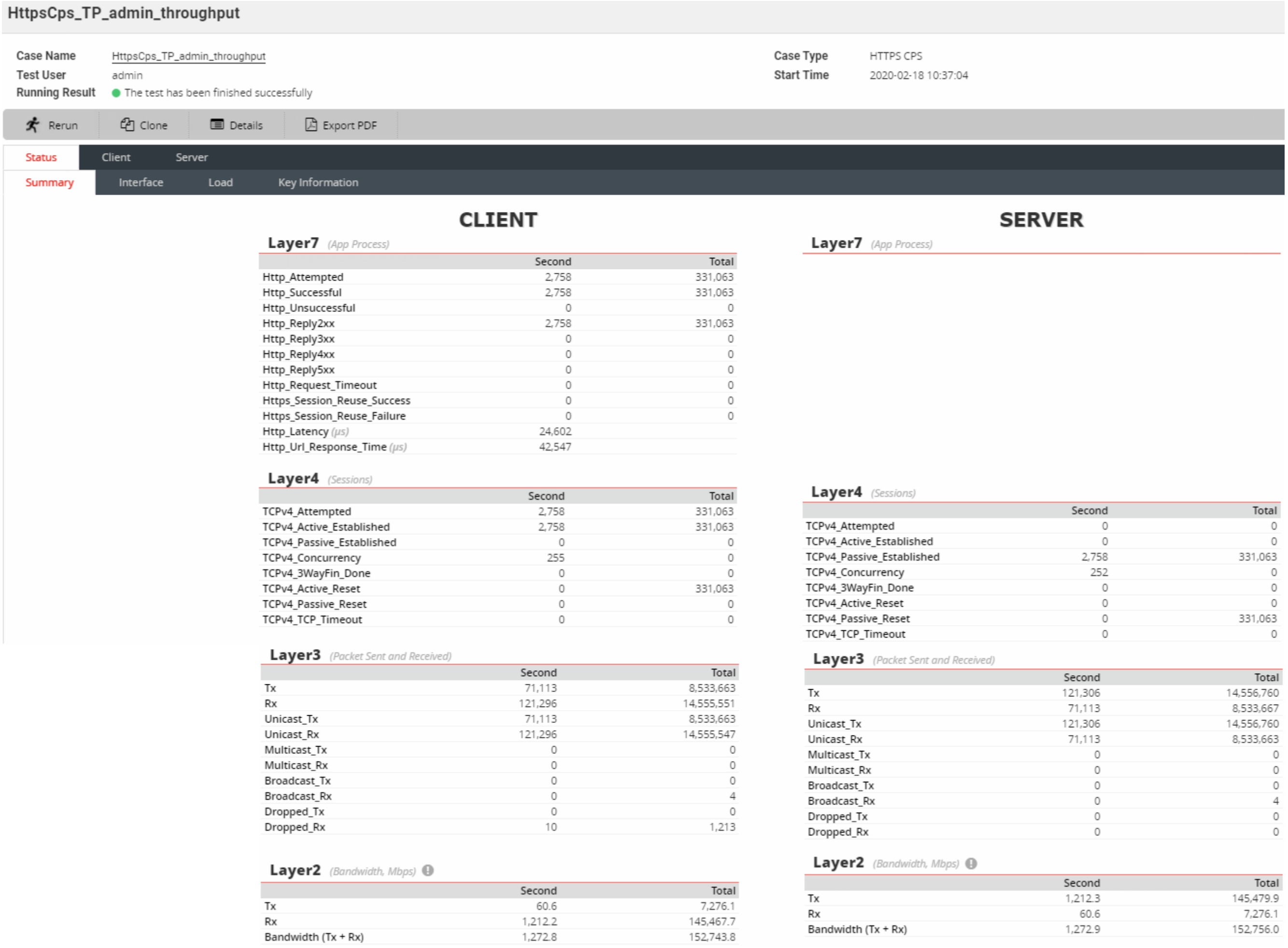
Refer to chapter Performance Testing on page 48, Security Testing on page 260, and MITRE ATT&CK® on page 292 on how to start a test case.

A few seconds after you start a test, the page automatically switches to a test status page.

You can also navigate to the status page by clicking the Running icon in the top navigation menu.

Status tab

The following figure shows the information on **Status > Summary** tab of an HTTPS CPS test.



HttpsCps_TP_admin_throughput

Case Name	HttpsCps_TP_admin_throughput	Case Type	HTTPS CPS
Test User	admin	Start Time	2020-02-18 10:37:04
Running Result	● The test has been finished successfully		

CLIENT

Layer7 *(App Process)*

	Second	Total
Http_Attempted	2,758	331,063
Http_Successful	2,758	331,063
Http_Unsuccessful	0	0
Http_Reply2xx	2,758	331,063
Http_Reply3xx	0	0
Http_Reply4xx	0	0
Http_Reply5xx	0	0
Http_Request_Timeout	0	0
Https_Session_Reuse_Success	0	0
Https_Session_Reuse_Failure	0	0
Http_Latency *(μs)*	24,602	
Http_Url_Response_Time *(μs)*	42,547	

Layer4 *(Sessions)*

	Second	Total
TCPv4_Attempted	2,758	331,063
TCPv4_Active_Established	2,758	331,063
TCPv4_Passive_Established	0	0
TCPv4_Concurrency	255	0
TCPv4_3WayFin_Done	0	0
TCPv4_Active_Reset	0	331,063
TCPv4_Passive_Reset	0	0
TCPv4_TCP_Timeout	0	0

Layer3 *(Packet Sent and Received)*

	Second	Total
Tx	71,113	8,533,663
Rx	121,296	14,555,551
Unicast_Tx	71,113	8,533,663
Unicast_Rx	121,296	14,555,547
Multicast_Tx	0	0
Multicast_Rx	0	0
Broadcast_Tx	0	0
Broadcast_Rx	0	4
Dropped_Tx	0	0
Dropped_Rx	10	1,213

Layer2 *(Bandwidth, Mbps)*

	Second	Total
Tx	60.6	7,276.1
Rx	1,212.2	145,467.7
Bandwidth (Tx + Rx)	1,272.8	152,743.8

SERVER

Layer7 *(App Process)*

Layer4 *(Sessions)*

	Second	Total
TCPv4_Attempted	0	0
TCPv4_Active_Established	0	0
TCPv4_Passive_Established	2,758	331,063
TCPv4_Concurrency	252	0
TCPv4_3WayFin_Done	0	0
TCPv4_Active_Reset	0	0
TCPv4_Passive_Reset	0	331,063
TCPv4_TCP_Timeout	0	0

Layer3 *(Packet Sent and Received)*

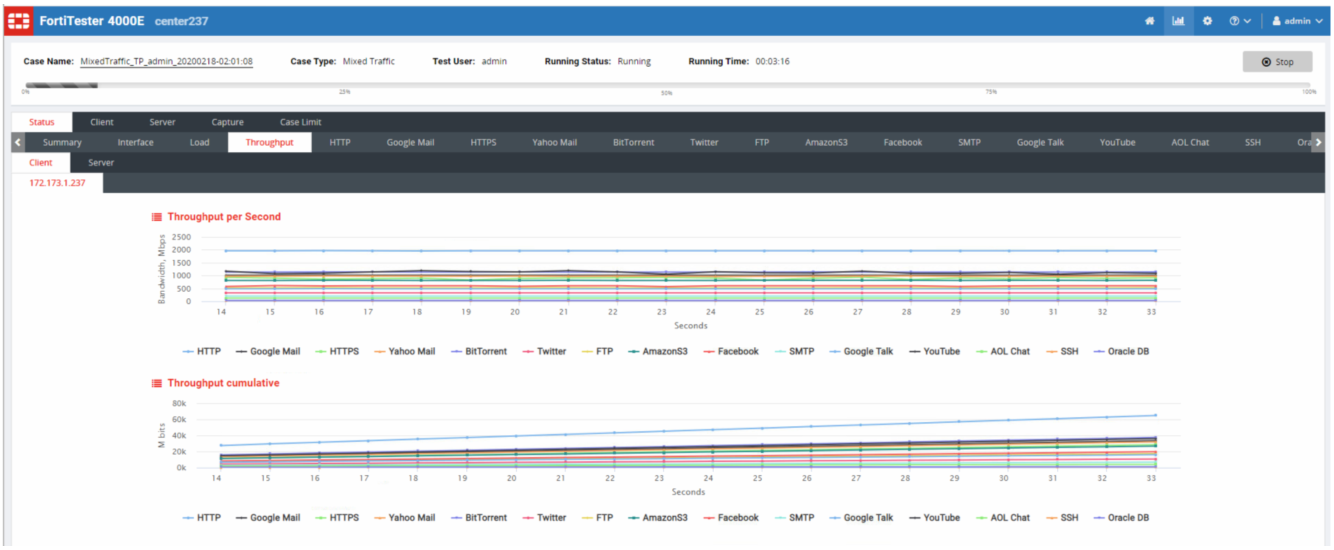
	Second	Total
Tx	121,306	14,556,760
Rx	71,113	8,533,667
Unicast_Tx	121,306	14,556,760
Unicast_Rx	71,113	8,533,663
Multicast_Tx	0	0
Multicast_Rx	0	0
Broadcast_Tx	0	0
Broadcast_Rx	0	4
Dropped_Tx	0	0
Dropped_Rx	0	0

Layer2 *(Bandwidth, Mbps)*

	Second	Total
Tx	1,212.3	145,479.9
Rx	60.6	7,276.1
Bandwidth (Tx + Rx)	1,272.9	152,756.0

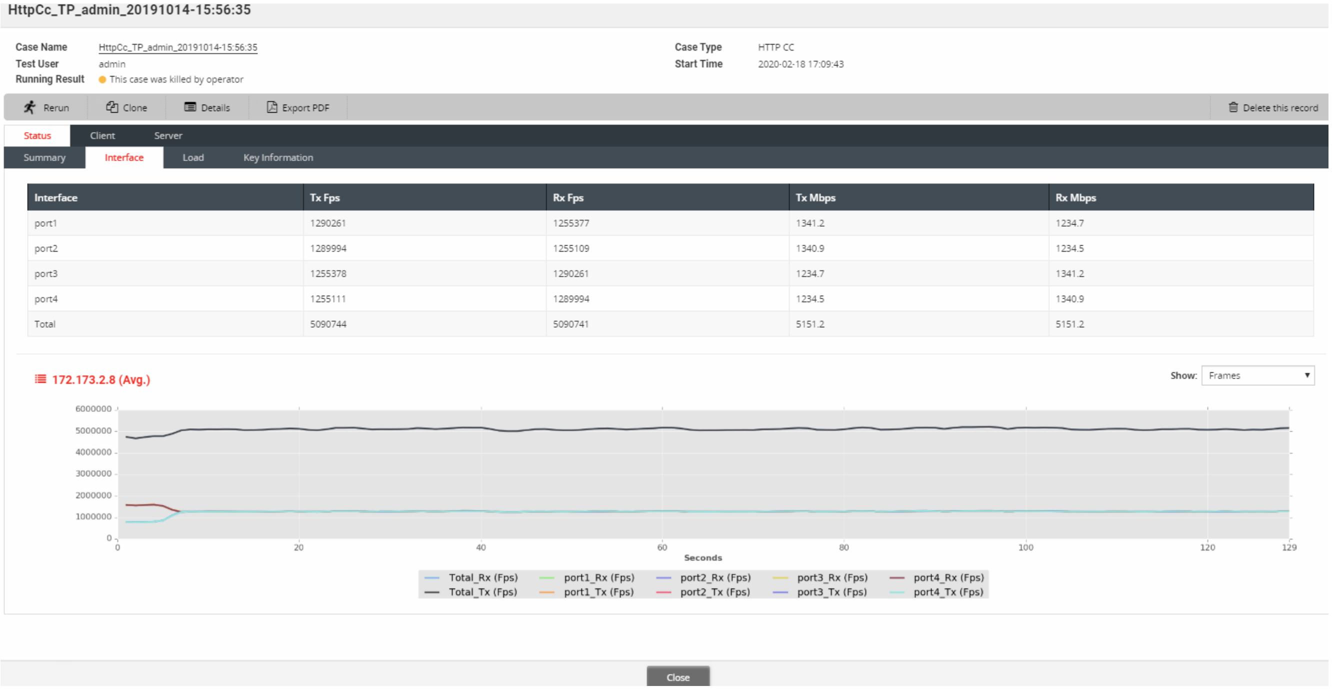
The data is updated every second. It includes Layer 2, Layer 3, Layer 4, and Layer 7 data.

The following figure shows the information on **Status > Throughput** of a mixed traffic case.



Case Name: MixedTraffic_TP_admin_20200218-02:01:08 **Case Type:** Mixed Traffic **Test User:** admin **Running Status:** Running **Running Time:** 00:03:16

The following figure shows the information on **Status > Interface** tab of an HTTP CC test.

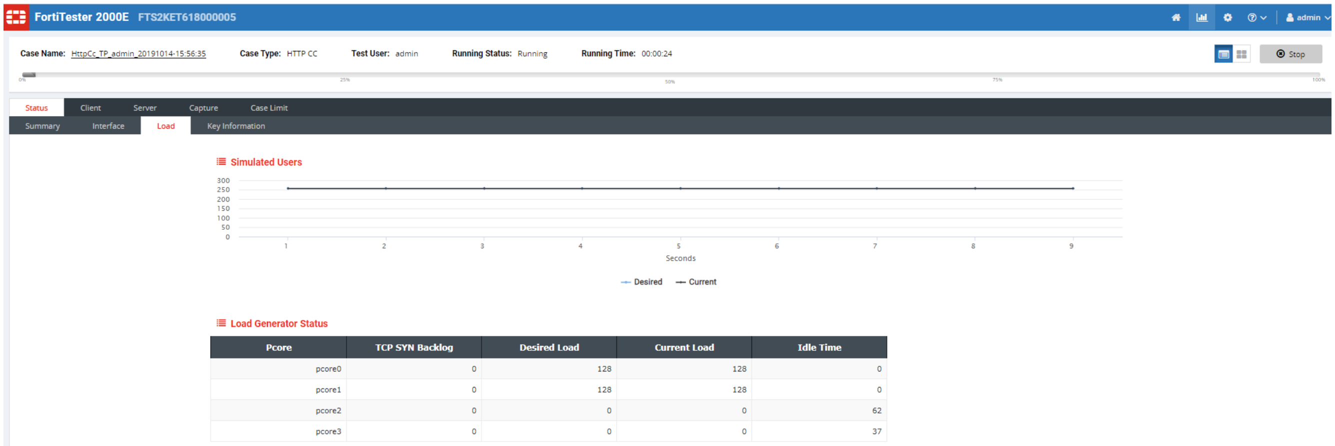


HttpCc_TP_admin_20191014-15:56:35

Case Name HttpCc_TP_admin_20191014-15:56:35
Test User admin
Running Result ● This case was killed by operator
Case Type HTTP CC
Start Time 2020-02-18 17:09:43

Interface	Tx Fps	Rx Fps	Tx Mbps	Rx Mbps
port1	1290261	1255377	1341.2	1234.7
port2	1289994	1255109	1340.9	1234.5
port3	1255378	1290261	1234.7	1341.2
port4	1255111	1289994	1234.5	1340.9
Total	5090744	5090741	5151.2	5151.2

The following figure shows the information on **Status > Load** tab of an HTTP CC test (Simuser mode).



Case Name: HttpCc_TP_admin_20191014-15:56:35 **Case Type:** HTTP CC **Test User:** admin **Running Status:** Running **Running Time:** 00:00:24

Load Generator Status

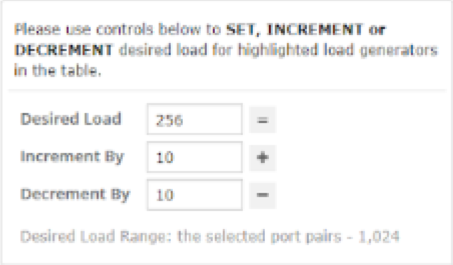
Pcore	TCP SYN Backlog	Desired Load	Current Load	Idle Time
pcore0	0	128	128	0
pcore1	0	128	128	0
pcore2	0	0	0	62
pcore3	0	0	0	37

The Load Generator Status chart includes the following information:

Pcore	The physical CPU core number.
TCP SYN Backlog	The length of TCP-SYN queue on server side.
Desired Load	The desired load that you specify in the load profile, or manually request in the Load Control pane.
Current Load	The currently achieved load.
Idle Time	The idle time for this CPU, an indicator of CPU utilization. Less value means the CPU is more busy. The max value is 9999.

If you have selected the **Simusers/second** or **Connections/second** mode when creating a case, the following window will appear beside the Load Generator Status table. You can set, increment, or decrement the desired simulated users or connections per second when the case is running.

- If you click =, the **Desired Load** will come into force immediately.
- If you click + or −, the simusers or connections will increase or decrease by the specified number until it reaches the **Desired Load**.



Please use controls below to **SET, INCREMENT or DECREMENT** desired load for highlighted load generators in the table.

Desired Load 256 =

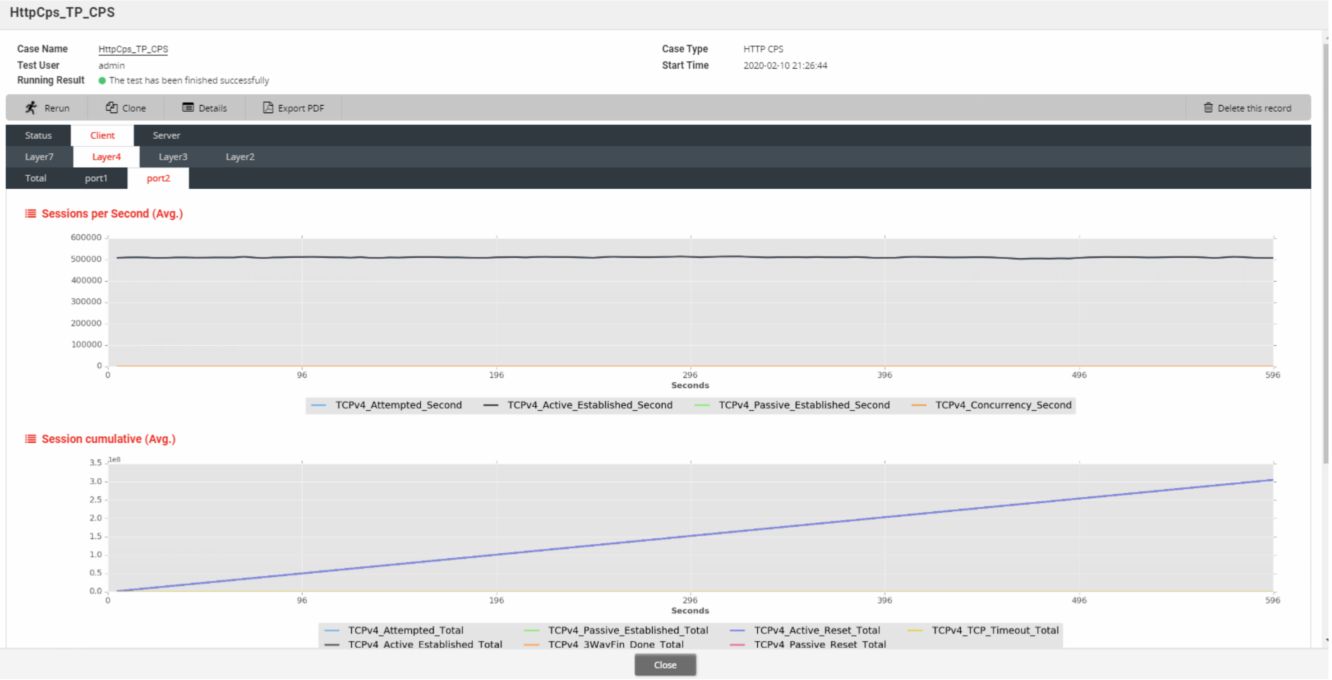
Increment By 10 +

Decrement By 10 −

Desired Load Range: the selected port pairs - 1,024

Client tab

The following figure shows the information on **Client > Layer 4 > Port 2** tab of an HTTP CPS test.



HttpCps_TP_CPS

Case Name HttpCps_TP_CPS

Test User admin

Running Result ● The test has been finished successfully

Case Type HTTP CPS

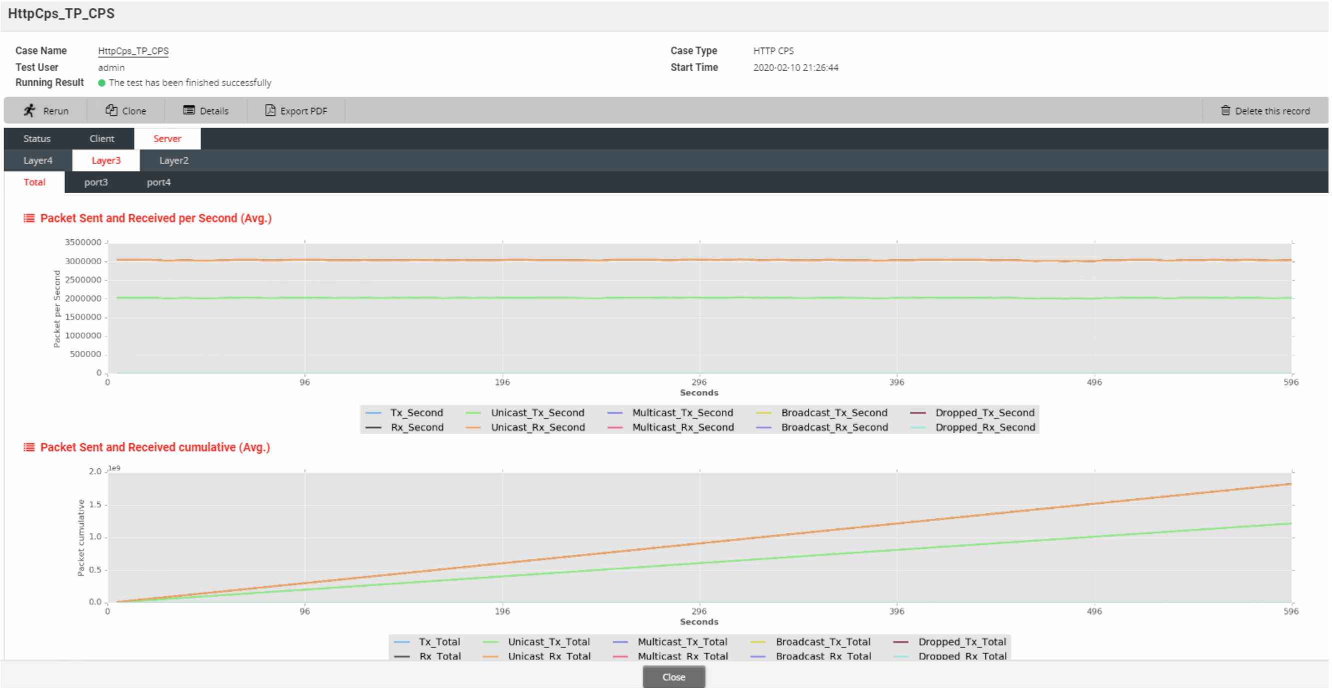
Start Time 2020-02-10 21:26:44

For TCP Response Time, the following information is shown:

TCPv4_Time_to_TCP_Syn_Ack/TCPV6_Time_to_TCP_Syn_Ack	The elapsed time (unit: milliseconds) between sending the SYN packet from the client and receiving the SYN/ACK packet from DUT.
TCPV4_Time_to_TCP_First_Byte/TCPV4_Time_to_TCP_First_Byte	The elapsed time (unit: milliseconds) between sending the SYN packet from the client and receiving the first Layer 7 packet from DUT.
TCPV4_Estimated_Server/TCPV4_Estimated_Server	An estimate of the time taken for the server to respond to a request (unit: milliseconds), derived from the formula, Time to TCP first byte - 2 X Time to TCP Syn/Ack.

Server tab

The following figure shows the information on **Server > Layer 2** tab of an HTTP CPS test.



HttpCps_TP_CPS

Case Name HttpCps_TP_CPS
Test User admin
Running Result ● The test has been finished successfully

Case Type HTTP CPS
Start Time 2020-02-10 21:26:44

For TCP Response Time, the following information is shown:

TCPv4_To_First_ RX_ Data/TCPv6_To_First_ RX_Data	The elapsed time (unit: milliseconds) between sending the SYN packet from the client and receiving the SYN/ACK packet from DUT.
TCPv4_To_First_TX_Data_ ACK/TCPv6_To_First_ RX_Data	The elapsed time (unit: milliseconds) between sending the SYN packet from the client and receiving the first Layer 7 packet from DUT.
TCPv4_To_Connection_ Close/TCPv6_To_First_ RX_ Data	An estimate of the time taken for the server to respond to a request (unit: milliseconds), derived from the formula, Time to TCP first byte - 2 X Time to TCP Syn/Ack.

Using widget view

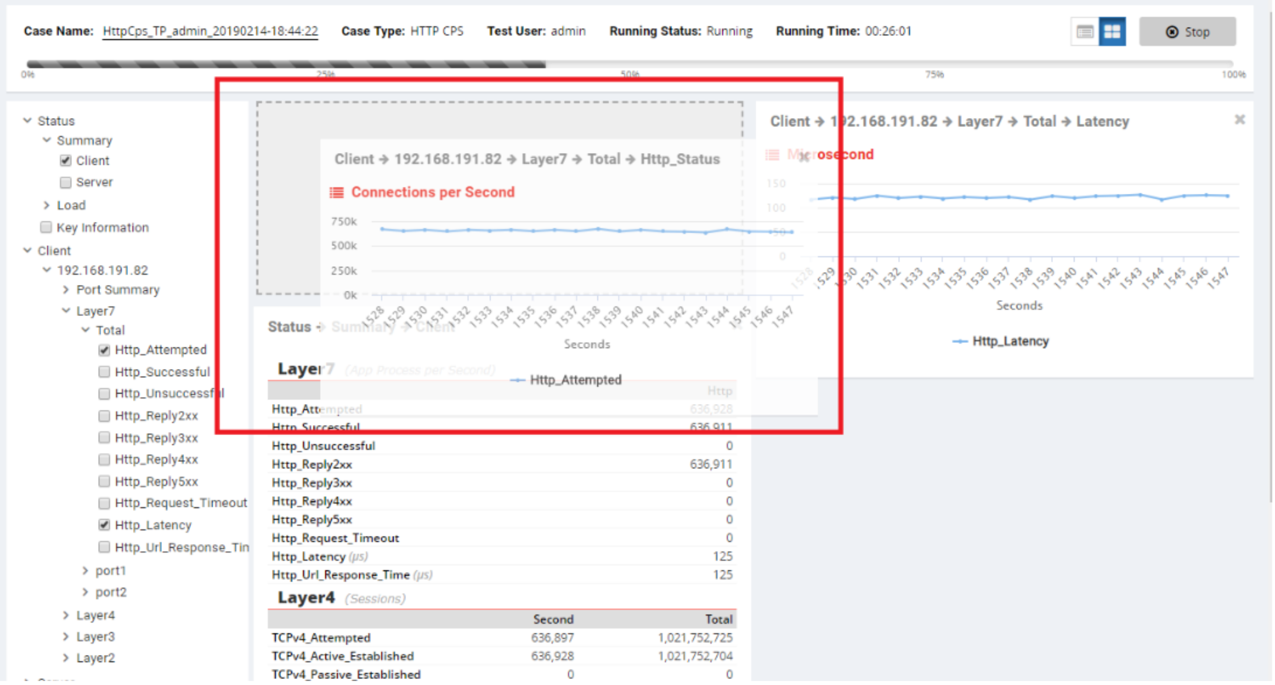
You can use the widget view to monitor the test status.

To enable the widget view:

1. Go to **System > Log & Report > Report Settings**.
2. Enable **Use Widget view as default**. The widget view will be displayed as default on the test status page.
3. You can also click the ⊞ button on the test status page to switch to the widget view.

To add widgets on the test status page:

1. On the left side of the widget view page, select the items that you'd like to display as widgets.
2. You drag the widget to move its position.



Case Name: HttpCps_TP_admin_20190214-18:44:22 **Case Type:** HTTP CPS **Test User:** admin **Running Status:** Running **Running Time:** 00:26:01

- Status
  - Summary
    - ☑ Client
    - ☐ Server
  - Load
  - ☐ Key Information
- Client
  - 192.168.191.82
    - Port Summary
    - Layer7
      - Total
        - ☑ Http_Attempted
        - ☐ Http_Successful
        - ☐ Http_Unsuccessful
        - ☐ Http_Reply2xx
        - ☐ Http_Reply3xx
        - ☐ Http_Reply4xx
        - ☐ Http_Reply5xx
        - ☐ Http_Request_Timeout
        - ☑ Http_Latency
        - ☐ Http_Url_Response_Tin
      - port1
      - port2
    - Layer4
    - Layer3
    - Layer2

Status → Summary → Client

Layer7 (App Process per Second)

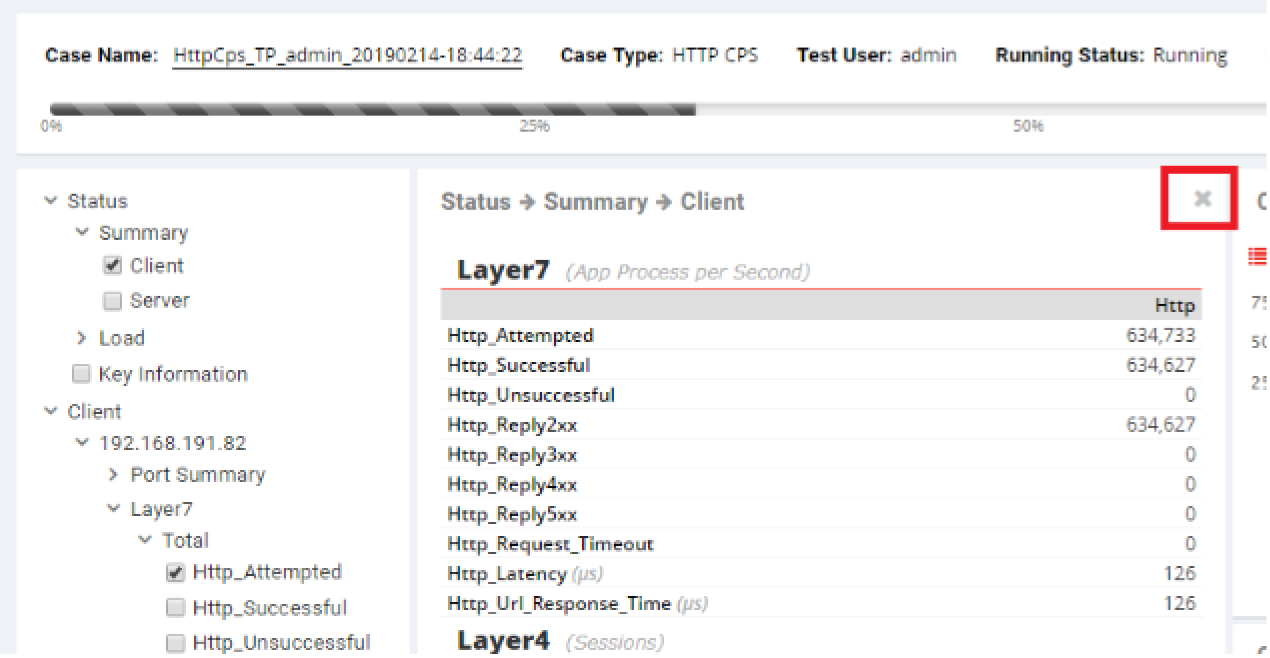
	Http
Http_Attempted	636,928
Http_Successful	636,911
Http_Unsuccessful	0
Http_Reply2xx	636,911
Http_Reply3xx	0
Http_Reply4xx	0
Http_Reply5xx	0
Http_Request_Timeout	0
Http_Latency (μs)	125
Http_Url_Response_Time (μs)	125

Layer4 (Sessions)

	Second	Total
TCPv4_Attempted	636,897	1,021,752,725
TCPv4_Active_Established	636,928	1,021,752,704
TCPv4_Passive_Established	0	0

To close widgets on the test status page:

1. On the left side of the widget view page, uncheck the items that you'd like to exclude from the widget view.
2. Or, you can click the close button of each widget.



Case Name: HttpCps_TP_admin_20190214-18:44:22 **Case Type:** HTTP CPS **Test User:** admin **Running Status:** Running

- Status
  - Summary
    - ☑ Client
    - ☐ Server
  - Load
  - ☐ Key Information
- Client
  - 192.168.191.82
    - Port Summary
    - Layer7
      - Total
        - ☑ Http_Attempted
        - ☐ Http_Successful
        - ☐ Http_Unsuccessful

Status → Summary → Client

Layer7 (App Process per Second)

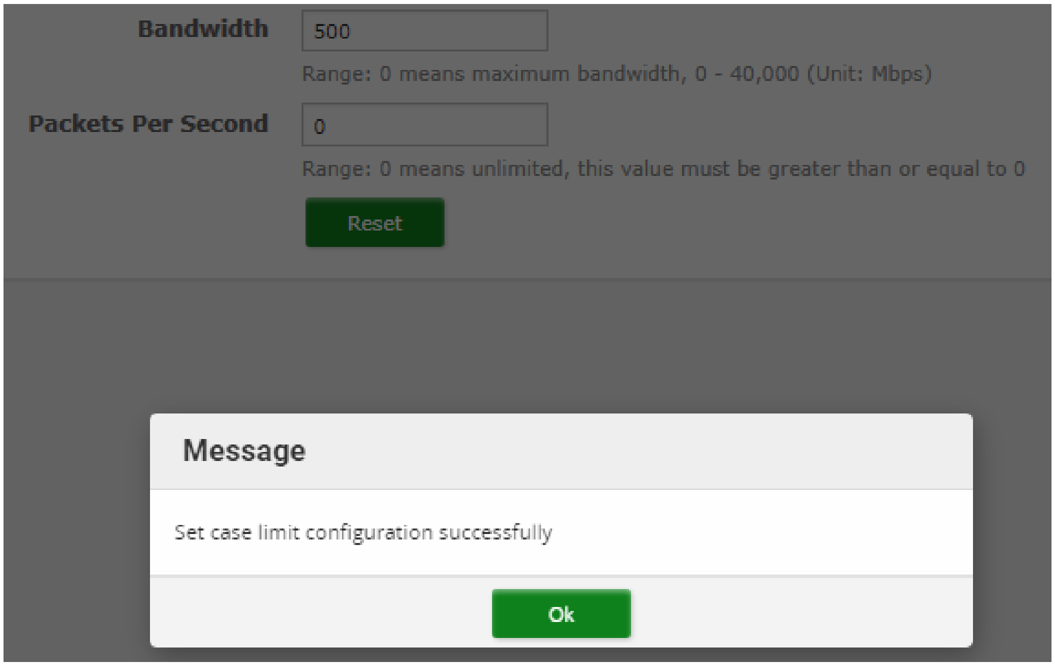
	Http
Http_Attempted	634,733
Http_Successful	634,627
Http_Unsuccessful	0
Http_Reply2xx	634,627
Http_Reply3xx	0
Http_Reply4xx	0
Http_Reply5xx	0
Http_Request_Timeout	0
Http_Latency (μs)	126
Http_Url_Response_Time (μs)	126

Layer4 (Sessions)

Modifying traffic load mid-run

You can modify a test's traffic load while the test is running.

1. Click **Case Limit** tab.
2. Modify settings for Bandwidth and Packets per Second accordingly.
   For example, to limit an HTTP CPS test to 500 packets per second, enter 500 for the Packets per Second field.
3. Click **Reset**.
   A message "Set case limit configuration successfully" appears.



Bandwidth: 500
Range: 0 means maximum bandwidth, 0 - 40,000 (Unit: Mbps)

Packets Per Second: 0
Range: 0 means unlimited, this value must be greater than or equal to 0

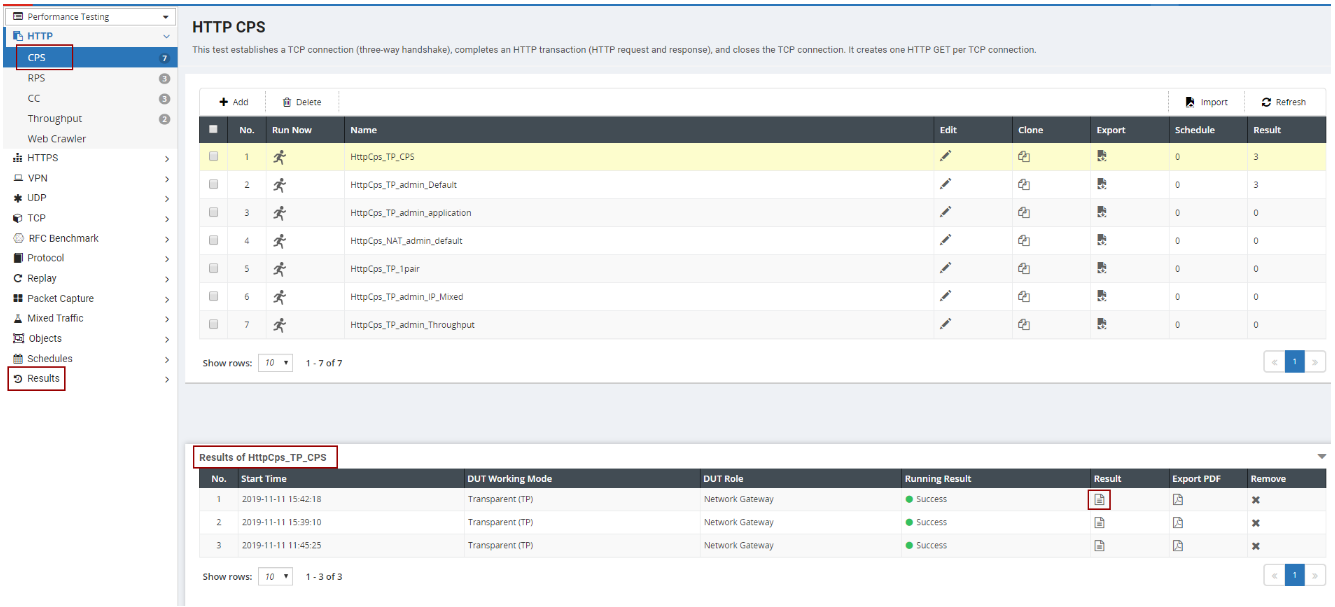
Message

Set case limit configuration successfully

Viewing test results

When you start a test, a status page is displayed showing results.

When the test finishes running, they will be listed in the **Results** list on the specific test case page, or on the **Performance Testing/Security Testing/ATT&CK Testing > Results** pages.



HTTP CPS

This test establishes a TCP connection (three-way handshake), completes an HTTP transaction (HTTP request and response), and closes the TCP connection. It creates one HTTP GET per TCP connection.

☐	No.	Run Now	Name	Edit	Clone	Export	Schedule	Result
☐	1		HttpCps_TP_CPS				0	3
☐	2		HttpCps_TP_admin_Default				0	3
☐	3		HttpCps_TP_admin_application				0	0
☐	4		HttpCps_NAT_admin_default				0	0
☐	5		HttpCps_TP_1pair				0	0
☐	6		HttpCps_TP_admin_IP_Mixed				0	0
☐	7		HttpCps_TP_admin_Throughput				0	0

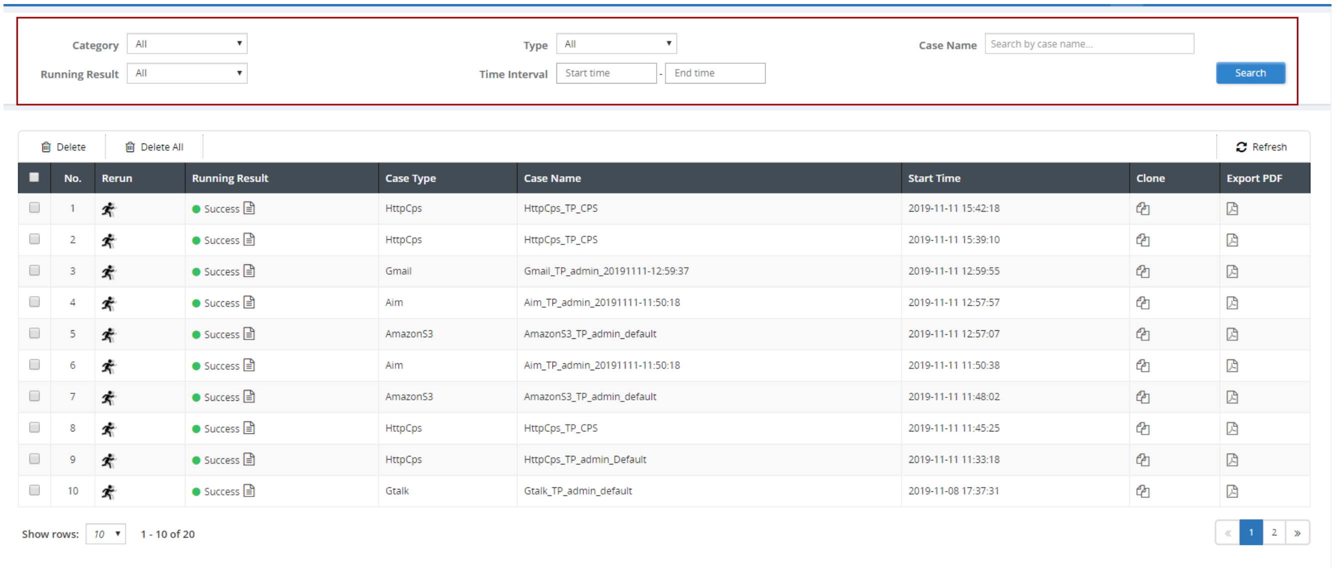
Show rows: 10 1 - 7 of 7

Results of HttpCps_TP_CPS

No.	Start Time	DUT Working Mode	DUT Role	Running Result	Result	Export PDF	Remove
1	2019-11-11 15:42:18	Transparent (TP)	Network Gateway	● Success			✖
2	2019-11-11 15:39:10	Transparent (TP)	Network Gateway	● Success			✖
3	2019-11-11 11:45:25	Transparent (TP)	Network Gateway	● Success			✖

Show rows: 10 1 - 3 of 3

On the **Results** page, the list includes cases with status of Success, User Killed, and Failed. The cases are ordered by test start time. You can use the search function, at the top, to search for test cases. You can click **Delete** to delete the selected results, or click **Delete All** to delete all results.



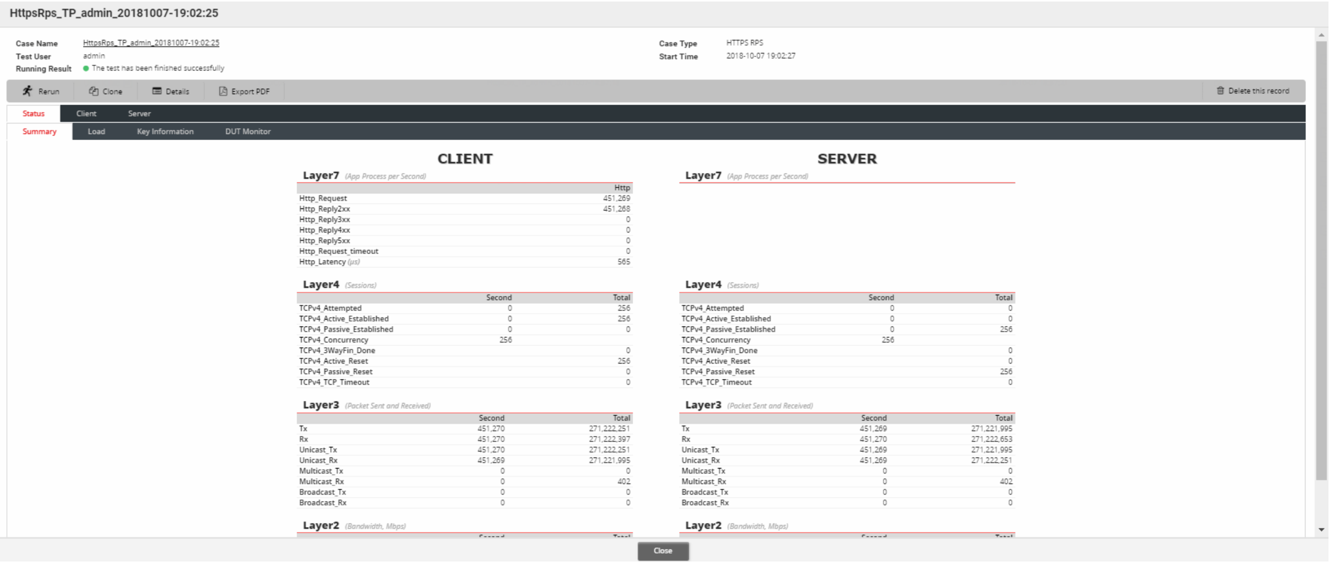
Category: All
Running Result: All
Type: All
Time Interval: Start time - End time
Case Name: Search by case name...

☐	No.	Rerun	Running Result	Case Type	Case Name	Start Time	Clone	Export PDF
☐	1		● Success	HttpCps	HttpCps_TP_CPS	2019-11-11 15:42:18		
☐	2		● Success	HttpCps	HttpCps_TP_CPS	2019-11-11 15:39:10		
☐	3		● Success	Gmail	Gmail_TP_admin_20191111-12:59:37	2019-11-11 12:59:55		
☐	4		● Success	Aim	Aim_TP_admin_20191111-11:50:18	2019-11-11 12:57:57		
☐	5		● Success	AmazonS3	AmazonS3_TP_admin_default	2019-11-11 12:57:07		
☐	6		● Success	Aim	Aim_TP_admin_20191111-11:50:18	2019-11-11 11:50:38		
☐	7		● Success	AmazonS3	AmazonS3_TP_admin_default	2019-11-11 11:48:02		
☐	8		● Success	HttpCps	HttpCps_TP_CPS	2019-11-11 11:45:25		
☐	9		● Success	HttpCps	HttpCps_TP_admin_Default	2019-11-11 11:33:18		
☐	10		● Success	Gtalk	Gtalk_TP_admin_default	2019-11-08 17:37:31		

Show rows: 10 1 - 10 of 20

Double click a test case to view its results. The following example shows results for an HTTPS RPS test.

Results for an HTTPS RPS Test



HttpsRps_TP_admin_20181007-19:02:25

Case Name HttpsRps_TP_admin_20181007-19:02:25
Test User admin
Running Result ● The test has been finished successfully

Case Type HTTPS RPS
Start Time 2018-10-07 19:02:27

CLIENT

Layer7 (App Process per Second)

	Http
Http_Request	451,269
Http_Reply2xx	451,268
Http_Reply3xx	0
Http_Reply4xx	0
Http_Reply5xx	0
Http_Request_timeout	0
Http_Latency (μs)	565

Layer4 (Sessions)

	Second	Total
TCPv4_Attempted	0	256
TCPv4_Active_Established	0	256
TCPv4_Passive_Established	0	0
TCPv4_Concurrency	256	
TCPv4_3WayFin_Done		0
TCPv4_Active_Reset		256
TCPv4_Passive_Reset		0
TCPv4_TCP_Timeout		0

Layer3 (Packet Sent and Received)

	Second	Total
Tx	451,270	271,222,251
Rx	451,270	271,222,397
Unicast_Tx	451,270	271,222,251
Unicast_Rx	451,269	271,221,995
Multicast_Tx	0	0
Multicast_Rx	0	402
Broadcast_Tx	0	0
Broadcast_Rx	0	0

Layer2 (Bandwidth, Mbps)

SERVER

Layer7 (App Process per Second)

Layer4 (Sessions)

	Second	Total
TCPv4_Attempted	0	0
TCPv4_Active_Established	0	0
TCPv4_Passive_Established	0	256
TCPv4_Concurrency	256	
TCPv4_3WayFin_Done		0
TCPv4_Active_Reset		0
TCPv4_Passive_Reset		256
TCPv4_TCP_Timeout		0

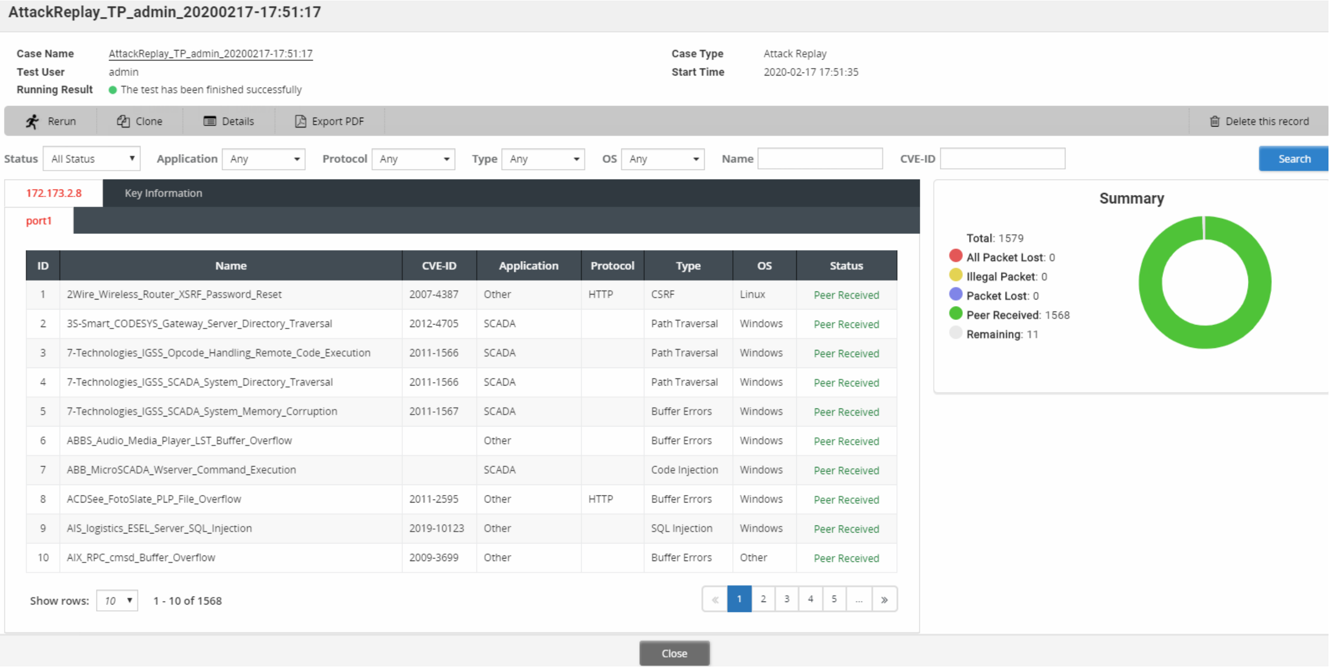
Layer3 (Packet Sent and Received)

	Second	Total
Tx	451,269	271,221,995
Rx	451,270	271,222,653
Unicast_Tx	451,269	271,221,995
Unicast_Rx	451,269	271,222,251
Multicast_Tx	0	0
Multicast_Rx	0	402
Broadcast_Tx	0	0
Broadcast_Rx	0	0

Layer2 (Bandwidth, Mbps)

The following figure shows results for an Attack Replay test.

Attack Replay results



AttackReplay_TP_admin_20200217-17:51:17

Case Name AttackReplay_TP_admin_20200217-17:51:17
Test User admin
Running Result ● The test has been finished successfully

Case Type Attack Replay
Start Time 2020-02-17 17:51:35

Status All Status
Application Any
Protocol Any
Type Any
OS Any
Name
CVE-ID

ID	Name	CVE-ID	Application	Protocol	Type	OS	Status
1	2Wire_Wireless_Router_XSRF_Password_Reset	2007-4387	Other	HTTP	CSRF	Linux	Peer Received
2	3S-Smart_CODESYS_Gateway_Server_Directory_Traversal	2012-4705	SCADA		Path Traversal	Windows	Peer Received
3	7-Technologies_IGSS_Opcode_Handling_Remote_Code_Execution	2011-1566	SCADA		Path Traversal	Windows	Peer Received
4	7-Technologies_IGSS_SCADA_System_Directory_Traversal	2011-1566	SCADA		Path Traversal	Windows	Peer Received
5	7-Technologies_IGSS_SCADA_System_Memory_Corruption	2011-1567	SCADA		Buffer Errors	Windows	Peer Received
6	ABBS_Audio_Media_Player_LST_Buffer_Overflow		Other		Buffer Errors	Windows	Peer Received
7	ABB_MicroSCADA_Wserver_Command_Execution		SCADA		Code Injection	Windows	Peer Received
8	ACDSee_FotoSlate_PLP_File_Overflow	2011-2595	Other	HTTP	Buffer Errors	Windows	Peer Received
9	AIS_logistics_ESEL_Server_SQL_Injection	2019-10123	Other		SQL Injection	Windows	Peer Received
10	AIX_RPC_cmsd_Buffer_Overflow	2009-3699	Other		Buffer Errors	Other	Peer Received

Show rows: 10 1 - 10 of 1568

Summary

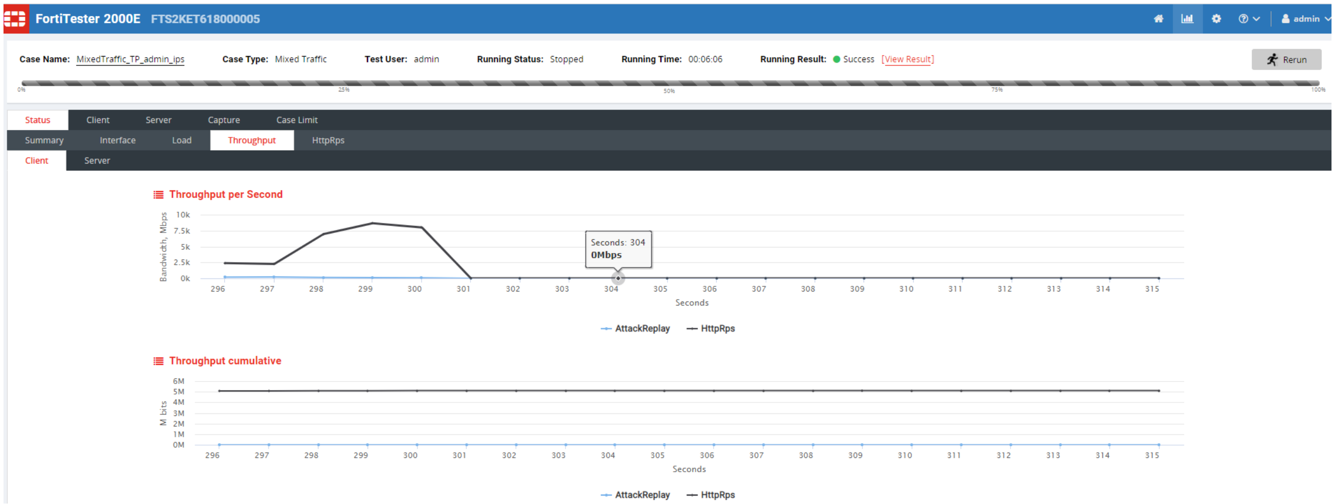
Total: 1579
● All Packet Lost: 0
● Illegal Packet: 0
● Packet Lost: 0
● Peer Received: 1568
● Remaining: 11

For Attack Replay tests, the results show status for every attack traffic file and a summary count for packets with the following statuses: Peer Received, All Packet Lost, Packet Lost or Illegal Packet. Peer Received means the server has received all the packets sent out by the client. All Packet Lost means the server has not received all the packets sent out by the client. Packet Lost means one or more packets were lost after the traffic passed through the DUT. Illegal Packet means the FortiTester system encountered a packet larger than the MTU (the default is 1500) and has stopped the replay of that pcap file.

You can filter attack files with multple fields such as status, application, protocol, type, OS, name, and CVE-ID.

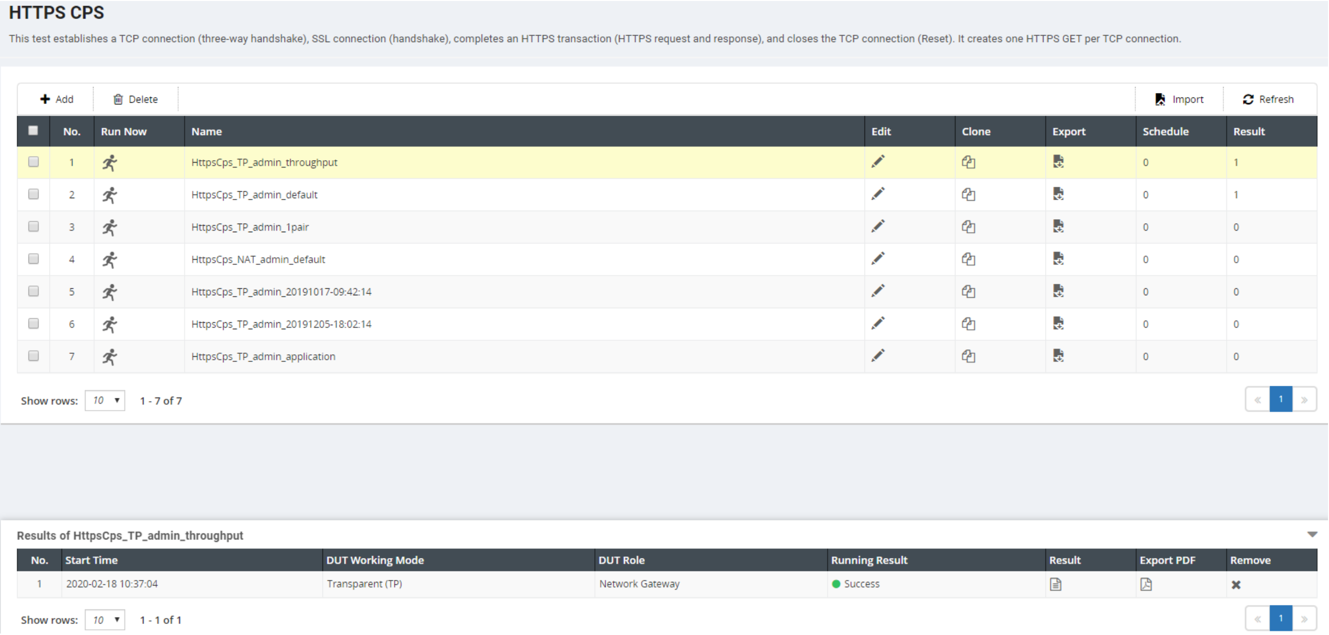
The following figure shows results for a Mixed Traffic test.

Mixed Traffic results



Case Name: MixedTraffic_TP_admin_ips **Case Type:** Mixed Traffic **Test User:** admin **Running Status:** Stopped **Running Time:** 00:06:06 **Running Result:** ● Success [View Result]

FortiTester also supports displaying test results on case page. You can double click one test result or click 🗎 to see the test result.



HTTPS CPS

This test establishes a TCP connection (three-way handshake), SSL connection (handshake), completes an HTTPS transaction (HTTPS request and response), and closes the TCP connection (Reset). It creates one HTTPS GET per TCP connection.

☐	No.	Run Now	Name	Edit	Clone	Export	Schedule	Result
☐	1	🏃	HttpsCps_TP_admin_throughput	✎	⧉	⇩	0	1
☐	2	🏃	HttpsCps_TP_admin_default	✎	⧉	⇩	0	1
☐	3	🏃	HttpsCps_TP_admin_1pair	✎	⧉	⇩	0	0
☐	4	🏃	HttpsCps_NAT_admin_default	✎	⧉	⇩	0	0
☐	5	🏃	HttpsCps_TP_admin_20191017-09:42:14	✎	⧉	⇩	0	0
☐	6	🏃	HttpsCps_TP_admin_20191205-18:02:14	✎	⧉	⇩	0	0
☐	7	🏃	HttpsCps_TP_admin_application	✎	⧉	⇩	0	0

Show rows: 10 ▾ 1 - 7 of 7 « 1 »

Results of HttpsCps_TP_admin_throughput

No.	Start Time	DUT Working Mode	DUT Role	Running Result	Result	Export PDF	Remove
1	2020-02-18 10:37:04	Transparent (TP)	Network Gateway	● Success	🗎	🗎	✖

Show rows: 10 ▾ 1 - 1 of 1 « 1 »

Exporting/importing a test case

After you click **Start** or **Save**, FortiTester automatically saves the test configuration. You can edit or make a copy of a test configuration before you run it.

You can use the **Export/Import** utilities to export a test case configuration (as a .zip file) and then import it into another FortiTester appliance.

In the top banner, click the Cases icon to display the list of saved test cases. Cases are categorized by test type.

Scheduling cases

You can schedule a test case to run automatically at a time you specify. You can also specify a repeat interval (once, hourly, daily, weekly, monthly).

To configure a schedule:

1. Go to **Schedules** under either **Cases > Performance Testing** or **Cases > Security Testing**.
2. Click **Add** to display the configuration page.
3. Enter a name for the schedule.
4. Select **Enable** to enable this schedule.
5. Enter a delay between test cases.
6. In **Settings**, select the start date and time, and the repeat option.
7. In Case Setting, select one or more cases, then click ⌄ to confirm the selection.
8. Click **Save** to save the schedule configuration.

Tip: To set up a schedule from the case list, click the 📅 icon to display the schedule configuration page.

Stopping tests

There are two ways to stop a running test:

- In the test configuration, specify an automatic stop after a specified duration.
- Click the **Stop** button on the running page of a test that is in progress.

Performance Testing

Go to **Cases > Performance Testing** to start the following cases to test the server performance.

- HTTP
- HTTPS
- VPN
- UDP
- TCP
- RFC Benchmark
- Protocol
- Application
- Replay
- Packet Capture
- Mixed Traffic

HTTP Cases

Starting an HTTP CPS test

FortiTester tests HTTP new connections per second (CPS) performance by simulating multiple clients that generate HTTP traffic.

The traffic generated for each connection includes the TCP three-way handshake, HTTP request and HTTP response (complete HTTP transaction), and the TCP connection close (FIN, ACK, FIN, ACK). Each TCP packet has one HTTP GET request. The traffic is HTTP 1.0 without HTTP persistent connections (HTTP keep-alive).

To start an HTTP CPS test:

1. Go to **Cases > Performance Testing > HTTP > CPS** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in HTTP CPS Test Case configuration on page 49.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTP CPS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing

Settings	Guidelines
	through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, HTTP 1.1 will backward compatibility with HTTP 1.0.
Keep Alive	Enable to add keepalive header. Only available when HTTP 1.0 is selected in Protocol Level.
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and

Settings	Guidelines
	server, HTTP 1.1 will backward compatibility with HTTP 1.0.
Keep Alive	Enable to add keepalive header. Only available when HTTP 1.0 is selected in Protocol Level.
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is

Settings	Guidelines
	logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Response pages	The size of the response. Available only when **Method** is **Custom**.
HTTP Pipelining	Available only when **Method** is **Custom**.
Generate Random Content	Enable to generate random content in response package. Available only when **Method** is **Custom**.
Random Method	Select to use which method to generate random content.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does

Settings	Guidelines
	not meet the criteria set, the test fails. See Using success criteria on page 36.

Starting an HTTP RPS test

FortiTester tests requests per second (RPS) performance by simulating multiple clients that generate HTTP traffic.

All requests include a TCP three-way handshake, one HTTP request and response, and a TCP connection close (FIN, ACK, FIN, ACK). There are 10 HTTP GET requests per TCP connection and 100 HTTP GET requests per TCP connection for Layer4/HTTPS testing.

To start an HTTP RPS test:

1. Go to **Cases > Performance Testing > HTTP > RPS** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in HTTP RPS Test Case configuration on page 53.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTP RPS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.

Settings	Guidelines
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Requests per Connection	Number of HTTP requests per connection. The default is 0, which means as many as possible. The valid range is 0 to 50,000.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing

Settings	Guidelines
	servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).

Settings	Guidelines
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.

Settings	Guidelines
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Response pages	The size of the response. Available only when **Method** is **Custom**.
HTTP Pipelining	Available only when **Method** is **Custom**.
Generate Random Content	Enable to generate random content in response package. Available only when **Method** is **Custom**.
Random Method	Select to use which method to generate random content.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does not meet the criteria set, the test fails. See Using success criteria on page 36.

Starting an HTTP CC test

FortiTester tests HTTP concurrent connection (CC) performance by simulating multiple clients that generate HTTP traffic. All connections include a TCP three-way handshake, a loop of HTTP requests and responses (complete HTTP transaction), and close the connection with TCP FIN.

To start an HTTP CC test:

1. Go to **Cases > Performance Testing > HTTP > CC** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in HTTP CC Test Case configuration on page 58.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTP CC Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Maximum Concurrent Connections	The number of concurrent connections.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Think Time	The delay between client HTTP requests (unit: second).
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or

Settings	Guidelines
	reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).

Settings	Guidelines
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.

Settings	Guidelines
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does not meet the criteria set, the test fails. See Using success criteria on page 36.

Starting an HTTP throughput test

FortiTester tests HTTP throughput performance by simulating multiple clients that generate HTTP traffic.

Note the following limitations:

- You cannot modify the HTTP request or HTTP response headers.

To start an HTTP throughput test:

1. Go to **Cases > Performance Testing > HTTP > Throughput** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in HTTP Throughput Test Case configuration on page 61.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically, so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTP Throughput Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600.

Settings	Guidelines
	Note: You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.

Settings	Guidelines
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.

Settings	Guidelines
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does not meet the criteria set, the test fails. See Using success criteria on page 36.

HTTPS Cases

Starting an HTTPS CPS test

The HTTPS CPS test is almost the same as the HTTP CPS test, except that it uses HTTPS traffic, and does not have the Limit by option; also, the MTU is editable.

To start an HTTPS CPS test:

1. Go to **Cases > Performance Testing > HTTPS > CPS** to display the test case summary page.
2. Click **Add**to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in HTTPS CPS Test Case configuration on page 65.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTPS CPS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case

Settings	Guidelines
	running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	

Settings	Guidelines
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, HTTP 1.1 will backward compatibility with HTTP 1.0.
Keep Alive	Enable to add keepalive header. Only available when HTTP 1.0 is selected in Protocol Level.
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Quiet Shutdown	Enable to apply safe shutdown procedure to SSL connections by sending SSL alert to the peer.
PSK/SRP	Enable to support PSK and SRP ciphers.
PSK/SRP Username	Username for PSK and SRP ciphers.
PSK/SRP Password	PSK/SRP for PSK and SRP ciphers.
Available SSL Versions	Select SSL versions. TLSv1.3 and other SSL versions are mutually exclusive. This means you can’t select TLSv1.3 at the same time with other SSL versions.
SSL Ciphers	Select one or more SSL ciphers from the list.
Elliptic Curve	Select the Elliptic Curve that the client support for key exchanges. Only available when you select TLSv1.3.
Send TLS Extension SNI	Enable to send a TLS SNI extension in the client's hello message to the server to indicate the name of the server to be connected.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server. This option applies only to TLS v1 and TLS v1.2. It does not apply to TLS v1.3.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.
Enable Client Certificate	Enable the client authentication for HTTPS cases.
Certificate	Select the certificate created in **Performance Testing > Objects > Certificates**. Available only when Enable Client Certificate is enabled.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.

Settings	Guidelines
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, HTTP 1.1 will backward compatibility with HTTP 1.0.
Keep Alive	Enable to add keepalive header. Only available when HTTP 1.0 is selected in Protocol Level.
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Certificate	Select the certificates you have created in **Performance Testing > Objects > Certificate Groups**. If you have selected a certificate group in the **Select case options** window, then you are not allowed to select certificate here. If you have selected ECDHE-ECDSA ciphers for the client, then you must reference an ECC certificate for the server, otherwise the SSL handshake will fail.
Enable SNI	Enable to select the SNI certificate group that specifies a list of host names that the server will use to match the host name in the SNI extension of client hello message.
SNI Certificate	Select the SNI Certificate created in **Performance Testing > Objects > SNI**.
Strict SNI Check	When enabled, the transactions will be disconnected if the server can't find a certificate matched with the requested SNI host name. When disabled, the default certificate will be used for the SSL encryption.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated

Settings	Guidelines
	with the server.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU,

Settings	Guidelines
	IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Response pages	The size of the response. Available only when **Method** is **Custom**.
HTTP Pipelining	Available only when **Method** is **Custom**.
Generate Random Content	Enable to generate random content in response package. Available only when **Method** is **Custom**.
Random Method	Select to use which method to generate random content.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does not meet the criteria set, the test fails. See Using success criteria on page 36.

Starting an HTTPS RPS test

The HTTPS RPS test is the same as the HTTP RPS test, except that it uses HTTPS traffic, and does not have the Limit by option; also, the MTU is editable.

To start an HTTPS RPS test:

1. Go to **Cases > Performance Testing > HTTPS > RPS** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in HTTPS RPS Test Case configuration on page 71.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTPS RPS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Requests per Connection	Number of HTTP requests per connection. The default is 0, which means as many as possible. The valid range is 0 to 50,000.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.

Settings	Guidelines
Quiet Shutdown	Enable to apply safe shutdown procedure to SSL connections by sending SSL alert to the peer.
PSK/SRP	Enable to support PSK and SRP ciphers.
PSK/SRP Username	Username for PSK and SRP ciphers.
PSK/SRP Password	PSK/SRP for PSK and SRP ciphers.
Available SSL Versions	Select SSL versions. TLSv1.3 and other SSL versions are mutually exclusive. This means you can't select TLSv1.3 at the same time with other SSL versions.
SSL Ciphers	Select one or more SSL ciphers from the list.
Elliptic Curve	Select the Elliptic Curve that the client support for key exchanges. Only available when you select TLSv1.3.
Send TLS Extension SNI	Enable to send a TLS SNI extension in the client's hello message to the server to indicate the name of the server to be connected.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server. This option applies only to TLS v1 and TLS v1.2. It does not apply to TLS v1.3.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.
Enable Client Certificate	Enable the client authentication for HTTPS cases.
Certificate	Select the certificate created in **Performance Testing > Objects > Certificates**. Available only when Enable Client Certificate is enabled.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -

Settings	Guidelines
	> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Certificate	Select the certificates you have created in **Performance Testing > Objects > Certificate Groups**. If you have selected a certificate group in the **Select case options** window, then you are not allowed to select certificate here. If you have selected ECDHE-ECDSA ciphers for the client, then you must reference an ECC certificate for the server, otherwise the SSL handshake will fail.
Enable SNI	Enable to select the SNI certificate group that specifies a list of host names that the server will use to match the host name in the SNI extension of client hello message.
SNI Certificate	Select the SNI Certificate created in **Performance Testing > Objects > SNI**.
Strict SNI Check	When enabled, the transactions will be disconnected if the server can't find a certificate matched with the requested SNI host name. When disabled, the default certificate will be used for the SSL encryption.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.

Settings	Guidelines
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	

Settings	Guidelines
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Response pages	The size of the response. Available only when **Method** is **Custom**.
HTTP Pipelining	Available only when **Method** is **Custom**.
Generate Random Content	Enable to generate random content in response package. Available only when **Method** is **Custom**.
Random Method	Select to use which method to generate random content.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does not meet the criteria set, the test fails. See Using success criteria on page 36.

Starting an HTTPS CC test

The HTTPS CC test is the same as the HTTP CC test, except that it uses HTTPS traffic and the MTU is editable.

To start an HTTPS CC test:

1. Go to **Cases > Performance Testing > HTTPS > CC** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See "Using network configuration templates" on page 1 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in Table 1.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTPS CC Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.

Settings	Guidelines
Maximum Concurrent Connections	The number of concurrent connections.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Think Time	The delay between client HTTP requests (unit: second).
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Quiet Shutdown	Enable to apply safe shutdown procedure to SSL connections by sending SSL alert to the peer.
PSK/SRP	Enable to support PSK and SRP ciphers.
PSK/SRP Username	Username for PSK and SRP ciphers.
PSK/SRP Password	PSK/SRP for PSK and SRP ciphers.
Available SSL Versions	Select SSL versions. TLSv1.3 and other SSL versions are mutually exclusive. This means you can’t select TLSv1.3 at the same time with other SSL versions.
SSL Ciphers	Select one or more SSL ciphers from the list.
Elliptic Curve	Select the Elliptic Curve that the client support for key exchanges. Only available when you select TLSv1.3.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server. This option applies only to TLS v1 and TLS v1.2. It does not apply to TLS v1.3.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.
Enable Client Certificate	Enable the client authentication for HTTPS cases.

Settings	Guidelines
Certificate	Select the certificate created in **Performance Testing > Objects > Certificates**. Available only when Enable Client Certificate is enabled.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Certificate	Select the certificates you have created in **Performance Testing > Objects > Certificate Groups**. If you have selected a certificate group in the **Select case options** window, then you are not allowed to select certificate here. If you have selected ECDHE-ECDSA ciphers for the client, then you must reference an ECC certificate for the server, otherwise the SSL handshake will fail.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.

Settings	Guidelines
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.

Settings	Guidelines
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does not meet the criteria set, the test fails. See Using success criteria on page 36.

Starting an HTTPS throughput test

The HTTPS Throughput test is the same as the HTTP Throughput test, except that it uses HTTPS traffic and the MTU is editable.

To start an HTTPS Throughput test:

1. Go to **Cases > Performance Testing > HTTPS > Throughput** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in HTTPS Throughput Test Case configuration on page 81.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTPS Throughput Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause

Settings	Guidelines
	a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.

Settings	Guidelines
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Quiet Shutdown	Enable to apply safe shutdown procedure to SSL connections by sending SSL alert to the peer.
PSK/SRP	Enable to support PSK and SRP ciphers.
PSK/SRP Username	Username for PSK and SRP ciphers.
PSK/SRP Password	PSK/SRP for PSK and SRP ciphers.
Available SSL Versions	Select SSL versions. TLSv1.3 and other SSL versions are mutually exclusive. This means you can't select TLSv1.3 at the same time with other SSL versions.
SSL Ciphers	Select one or more SSL ciphers from the list.
Elliptic Curve	Select the Elliptic Curve that the client support for key exchanges. Only available when you select TLSv1.3.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server. This option applies only to TLS v1 and TLS v1.2. It does not apply to TLS v1.3.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.
Enable Client Certificate	Enable the client authentication for HTTPS cases.
Certificate	Select the certificate created in **Performance Testing > Objects > Certificates**. Available only when Enable Client Certificate is enabled.
Transactions Before Renegotiation	The maximum number of TLS transactions that will use the same session.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP

Settings	Guidelines
	address or port in the range randomly.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Certificate	Select the certificates you have created in **Performance Testing > Objects > Certificate Groups**. If you have selected a certificate group in the **Select case options** window, then you are not allowed to select certificate here. If you have selected ECDHE-ECDSA ciphers for the client, then you must reference an ECC certificate for the server, otherwise the SSL handshake will fail.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.

Settings	Guidelines
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can

Settings	Guidelines
	select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.
Success criteria	Select criteria to determine if the test succeeds or fails. If the test does not meet the criteria set, the test fails. See Using success criteria on page 36.

VPN Cases

Starting an IPsec remote access test

FortiTester tests IPSec remote access by establishing a remote access IPSec tunnel, completes a full set of HTTP transactions (TCP connection, HTTP request, HTTP response, TCP connection close) through the tunnel, and terminates the tunnel.

To start a remote access test:

1. Go to **Cases > Performance Testing > IPSec > Remote Access** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in IPSec Remote Access Test Case configuration on page 88.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Below is a sample FortiGate IPsec configuration for the VPN gateway. FortiTester uses Fortitester as its ID. However, in this configuration the VPN gateway uses IKE version 1 Aggressive mode, and it is configured to accept any peer ID. The VPN gateway IP is configured as a secondary IP address, and this is used as the local gateway in the phase 1 config.

```
config system interface

edit "port33"

set ip 1.0.0.254 255.255.0.0

set allowaccess ping

set secondary-IP enable
```

```
config secondaryip
edit 1
set ip 1.0.0.253 255.255.0.0
set allowaccess ping
next
end
next
end
config system interface
edit "port35"
set ip 2.0.0.254 255.255.0.0
set allowaccess ping
next
end
config vpn ipsec phase1-interface
edit "tester"
set type dynamic
set interface "port33"
set ike-version 2
set local-gw 1.0.0.253
set peertype any
set psksecret fortinet
next
end
config vpn ipsec phase2-interface
edit "tester"
set phase1name "tester"
next
end
config firewall policy
edit 1
set srcintf "any"
set dstintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set logtraffic disable
next
end
```

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

IPSec Remote Access Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.

Settings	Guidelines
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
IKE Version	Select either version 1 or 2. For 1, configure IKE Mode and XAUTH.
Authentication Method	Select either PSK (Pre-shared Key) or Signature. If using a Signature you will need to import a client and server certificate.
Pre-shared Key	The parameter of IPsec.
Local Certificate	Select either of the certificates. If you have selected a certificate group in the Select case options window, then you are not allowed to select local certificate here.
Remote Certificate	Select either of the certificates. If you have selected a certificate group in the Select case options window, then you are not allowed select remote certificate here.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Action	
Request Page	Select System Pages with Fixed or Random File Name and Content.

Starting an IPsec remote access CC test

FortiTester tests IPSec remote access tunnel concurrent connections (CC) by establishing a remote access IPSec tunnel, completes a full set of HTTP transaction (TCP connection, HTTP request, HTTP response, and TCP connection close) through the tunnel, and terminates the tunnel.

To start a remote access CC test:

1. Go to **Cases > Performance Testing > IPSec > Remote Access CC** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described inIPSec Remote Access CC Test Case configuration on page 91 .
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Below is a sample FortiGate IPsec configuration for the VPN gateway. FortiTester uses FortiTester as its ID, however in this configuration the VPN gateway uses IKE version 1 Aggressive mode, and is configured to accept any peer ID. The VPN gateway IP is configured as a secondary IP address and this is used as the local gateway in the phase 1 config.

```
config system interface
edit "port33"
set ip 1.0.0.254 255.255.0.0
set allowaccess ping
set secondary-IP enable
config secondaryip
edit 1
set ip 1.0.0.253 255.255.0.0
set allowaccess ping
next
end
next
end
config system interface
edit "port35"
set ip 2.0.0.254 255.255.0.0
set allowaccess ping
next
end
config vpn ipsec phase1-interface
edit "tester"
set type dynamic
set interface "port33"
set ike-version 2
set local-gw 1.0.0.253
set peertype any
set psksecret fortinet
next
end
config vpn ipsec phase2-interface
edit "tester"
set phase1name "tester"
next
end
config firewall policy
edit 1
set srcintf "any"
set dstintf "any"
set srcaddr "all"
set dstaddr "all"
set action accept
set schedule "always"
set service "ALL"
set logtraffic disable
next
end
```

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

IPSec Remote Access CC Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.

Settings	Guidelines
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Tunnel Concurrent Connection	Specify the number of concurrent connections.
Think Time	The delay between client HTTP requests (unit: second).
IKE Version	Select either version 1 or 2. For 1, configure IKE Mode and XAUTH.
Authentication Method	Select either PSK (Pre-shared Key) or Signature. If using a Signature you will need to import a client and server certificate.
Pre-shared Key	The parameter of IPsec.
Local Certificate	Select either of the certificates. If you have selected a certificate group in the Select case options window, then you are not allowed to select local certificate here.
Remote Certificate	Select either of the certificates. If you have selected a certificate group

Settings	Guidelines
	in the Select case options window, then you are not allowed select remote certificate here.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Action	
Request Page	Select System Pages with Fixed or Random File Name and Content.

Starting an SSL VPN tunnel CC test

FortiTester tests the DUT's ability to support concurrent SSL VPN tunnel connections by establishing a large number of concurrent SSL VPN tunnel connections and completing a full round of HTTP transactions through each tunnel.

To start an SSL VPN tunnel CC test:

1. Go to **Cases > Performance Testing > SSL > SSL VPN CC** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in SSL VPN tunnel CC Test Case configuration on page 94.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

SSL VPN tunnel CC Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Tunnel Concurrent Connection	Specify the number of concurrent connections.
VPN Gateway Port	Specify the VPN gateway port number.
VPN Username	Enter the VPN username.
VPN Password	Enter the VPN password.
Certificate	The server certificate. If you have selected a certificate group in the Select case options window, then you are not allowed select certificate

Settings	Guidelines
	here.
Think Time	The delay between client HTTP requests (unit: second).
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client Network	
Network MTU	The maximum transmission unit size.
Tunnel Mode	Select TCP or UDP.
Server Network	
Network MTU	The maximum transmission unit size.
Action	
Request Page	Select System Pages with Fixed or Random File Name and Content.

UDP Cases

Starting a UDP PPS test

FortiTester tests UDP throughput by sending a specified size of UDP frames at a maximum or limited speed from simulated clients to simulated servers.

To start a UDP PPS test:

1. Go to **Cases > Performance Testing > UDP > PPS** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.

4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in UDP PPS Test Case configuration on page 96.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

UDP PPS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the	

Settings	Guidelines
configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Flows	Enter the port pair.
Frame Size	The range of frame size is 64 to 8192. When the (frame size-18) is larger than MTU, the UDP packet will be fragmented.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a UDP Payload test

FortiTester tests UDP payload by sending UDP frames with the specified payload from the client ports to the server ports.

To start a UDP payload test:

1. Go to **Cases > Performance Testing > UDP > Payload** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in UDP Payload Test Case configuration on page 98.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

UDP Payload Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Flows	Enter the port pair.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the

Settings	Guidelines
	device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

TCP Cases

Starting a TCP throughput test

FortiTester tests TCP throughput by generating a specified volume of two-way TCP traffic flow via specified ports.

To start a TCP throughput test:

1. Go to **Cases > Performance Testing > TCP > Throughput** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in TCP Throughput Test Case configuration on page 100.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TCP Throughput Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in

Settings	Guidelines
	the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Throughput Buffer Size	Set the throughput buffer size. The valid range is from 64-10M.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.

Settings	Guidelines
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.

Settings	Guidelines
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TurboTCP test

FortiTester tests TurboTCP connections per second (CPS) performance by generating a specified volume of two-way TCP traffic flow via specified ports.

The traffic generated for each connection includes the TCP three-way handshake and the TCP connection close (Reset).

To start a TurboTCP test:

1. Go to **Cases > Performance Testing > TCP > TurboTCP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.

6. Configure the test case options described in TurboTCP Test Case configuration on page 104.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TurboTCP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	

Settings	Guidelines
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
TurboTcp Buffer Size	The size of the buffer sent to server when the TCP connection is established.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Server Close Mode	Set to 3 Way Fin by default. Not configurable.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these

Settings	Guidelines
	acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the

Settings	Guidelines
	device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TCP connection test

FortiTester tests TCP concurrent connection performance by generating a specified volume of two-way TCP traffic flow via specified ports.

To start a TCP connection test:

1. Go to **Cases > Performance Testing > TCP > Connection** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in TCP Connection Test Case configuration on page 107.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TCP Connection Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600.

Settings	Guidelines
	Note: You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Maximum Concurrent Connections	The number of concurrent connections.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Bidirectional Traffic Flow	Select **Enable** to enable bidirectional traffic flow.
Client Profile	
Send Size	Specify the buffer size to send out from the client side. The default is 800 bytes. The valid range is from 1 to 100,000.
Receive Size	Specify the buffer size to receive from the server side. The default is 1,000 bytes. The valid range is from 1 to 100,000.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port	Select a change algorithm: **Increment** or **Random**. This setting

Settings	Guidelines
Change Algorithm	determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.

Settings	Guidelines
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

RFC Benchmark Cases

Starting an RFC 2544 throughput test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 throughput. According to RFC2544, throughput is the fastest rate for the number of test frames transmitted by the DUT, which is equal to the number of test frames sent to it by the test equipment.

To start a throughput test:

1. Go to **Cases > Performance Testing > RFC Benchmark > RFC 2544 > Throughput** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.

3. In the pop-up dialog, configure DUT Working Mode as TP or NAT.
4. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
5. Select a **Certificate Group** if applicable.
6. Click **OK** to continue.
7. Configure the test case options described in RFC 2544 Throughput Test Case configuration on page 111.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RFC 2544 Throughput Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.

Settings	Guidelines
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Flows	Enter the port pair.
Traffic Direction	Specify the direction of traffic flow.
Frame Size	The range of frame size is 64 to 8192. When the (frame size-18) is larger than MTU, the UDP packet will be fragmented.
Traffic Cycle Time	Traffic burst duration in seconds for each frame size. (minimum of 10)
Aging Time	Wait time for packet transmitting after traffic stop, in seconds. (range: 2 - 300)
Maximum Iterative Cycle	Maximum traffic cycle for each frame size. (minimum 1)
Acceptable Packet Loss Rate	Percentage of packets that can be lost.
Iteration Mode	Select either Binary Search to search using binary search mode or Custom Load to search using a custom load.
Initial Send Speed	Binary Search only. Specify a speed in Mbps. A setting of 0 means the speed will be set through automatic detection.
Maximum Send Speed	Speed in Mbps. A setting of 0 means throughput speed is copied from the BaseValue case.
Send Resolution Speed	Binary Search only. Specify a minimum send speed of the traffic cycle for each frame size.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.

Settings	Guidelines
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).

Starting an RFC 2544 latency test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 latency. According to RFC1242, for store and forward devices, latency is the time interval starting when the last bit of the input frame reaches the input port and ending when the first bit of the output frame is seen on the output port.

To start a latency test:

1. Go to **Cases > Performance Testing > RFC Benchmark > RFC 2544 > Latency** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.
3. In the pop-up dialog, configure DUT Working Mode as TP or NAT.
4. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
5. Select a **Certificate Group** if applicable.
6. Click **OK** to continue.
7. Configure the test case options described in RFC 2544 Latency Test Case configuration on page 113.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RFC 2544 Latency Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in

Settings	Guidelines
	the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Flows	Enter the port pair.
Traffic Direction	Specify the direction of traffic flow.
Frame Size	The range of frame size is 64 to 8192. When the (frame size-18) is larger than MTU, the UDP packet will be fragmented.
Traffic Cycle Time	Traffic burst duration in seconds for each frame size. (minimum of 10)
Aging Time	Wait time for packet transmitting after traffic stop, in seconds. (range: 2 - 300)
Maximum Iterative Cycle	Maximum traffic cycle for each frame size. (minimum 1)
Iteration Mode	Select either Binary Search to search using binary search mode or Custom Load to search using a custom load.

Settings	Guidelines
Maximum Send Speed	Speed in Mbps. A setting of 0 means throughput speed is copied from the BaseValue case.
Up/Down Granularity	Custom Load only. Traffic speed per cycle. 0 means sending speed in the next traffic cycle is equal to "Receive Mbps" in the previous cycle. 1 - 20 is the sending speed float percentage of maximum speed in the next cycle.
Correct Loss Rate Cycle	Custom Load only. Set to 1. Not configurable.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).

Starting an RFC 2544 loss rate test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 loss rate. According to RFC2544, to determine the frame loss rate, as defined in RFC1242 of a DUT throughout the entire range of input data rates and frame sizes.

To start a loss rate test:

1. Go to **Cases > Performance Testing > RFC Benchmark > RFC 2544 > Loss Rate** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.
3. In the pop-up dialog, configure DUT Working Mode as TP or NAT.

4. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
5. Select a **Certificate Group** if applicable.
6. Click **OK** to continue.
7. Configure the test case options described in RFC 2544 Loss Rate Test Case configuration on page 116.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RFC 2544 Loss Rate Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.

Settings	Guidelines
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Flows	Enter the port pair.
Traffic Direction	Specify the direction of traffic flow.
Frame Size	The range of frame size is 64 to 8192. When the (frame size-18) is larger than MTU, the UDP packet will be fragmented.
Traffic Cycle Time	Traffic burst duration in seconds for each frame size. (minimum of 10)
Aging Time	Wait time for packet transmitting after traffic stop, in seconds. (range: 2 - 300)
Maximum Iterative Cycle	Maximum traffic cycle for each frame size. (minimum 1)
Acceptable Packet Loss Rate	Percentage of packets that can be lost.
Iteration Mode	Select either Binary Search to search using binary search mode or Custom Load to search using a custom load.
Maximum Send Speed	Speed in Mbps. A setting of 0 means throughput speed is copied from the BaseValue case.
Up/Down Granularity	Custom Load only. Traffic speed per cycle. 0 means sending speed in the next traffic cycle is equal to "Receive Mbps" in the previous cycle. 1 - 20 is the sending speed float percentage of maximum speed in the next cycle.
Correct Loss Rate Cycle	Custom Load only. Set to 1. Not configurable.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4

Settings	Guidelines
	packets sent by this device.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).

Starting an RFC 2544 back to back test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 back to back. According to RFC 2544, to characterize the ability of a DUT to process back-to-back frames as defined in RFC 1242.

To start an RFC 2544 back to back test:

1. Go to **Cases > Performance Testing > RFC Benchmark > RFC 2544 > Back to Back** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.
3. In the pop-up dialog, configure DUT Working Mode as TP or NAT.
4. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
5. Select a **Certificate Group** if applicable.
6. Click **OK** to continue.
7. Configure the test case options described in RFC 2544 back to back Test Case configuration on page 118.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RFC 2544 back to back Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in

Settings	Guidelines
	the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Flows	Enter the port pair.
Traffic Direction	Specify the direction of traffic flow.
Frame Size	The range of frame size is 64 to 8192. When the (frame size-18) is larger than MTU, the UDP packet will be fragmented.
Aging Time	Wait time for packet transmitting after traffic stop, in seconds. (range: 2 - 300)
Acceptable Packet Loss Rate	Percentage of packets that can be lost.
Send Speed	Speed in Mbps. A setting of 0 means throughput speed is copied from the BaseValue case.
Iteration Mode	Select either Binary Search to search using binary search mode or

Settings	Guidelines
	Custom Load to search using a custom load.
Initial Traffic Cycle Time	Traffic burst duration in seconds for each frame size. (minimum of 2)
Maximum Traffic Cycle Time	Maximum traffic cycle, in seconds.
Duration Resolution Time	If the time difference between two iterations is lower than the specified value here, no iteration will be done.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).

Starting a RFC 3511 IP throughput test

FortiTester tests the ability of the DUT to handle network-layer data throughput. RFC 3511 is specifically focused on firewall performance.

To start a throughput test:

1. Go to **Cases > Performance Testing > RFC Benchmark > RFC 3511 > IP Throughput** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.
3. In the pop-up dialog, configure DUT Working Mode as TP or NAT.
4. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
5. Select a **Certificate Group** if applicable.

6. Click **OK** to continue.
7. Configure the test case options described in RFC 3511 IP Throughput Test Case configuration on page 121.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RFC 3511 IP Throughput Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	

Settings	Guidelines
Load	
Flows	Enter the port pair.
Traffic Direction	Specify the direction of traffic flow.
Packet Size	Specify the desired packet sizes, in bytes.
Traffic Cycle Time	Traffic burst duration in seconds for each frame size. (minimum of 10)
Aging Time	Wait time for packet transmitting after traffic stop, in seconds. (range: 2 - 300)
Maximum Iterative Cycle	Maximum traffic cycle for each frame size. (minimum 1)
Acceptable Packet Loss Rate	Percentage of packets that can be lost.
Iteration Mode	Select either Binary Search to search using binary search mode or Custom Load to search using a custom load.
Initial Send Speed	Binary Search only. Specify a speed in Mbps. A setting of 0 means the speed will be set through automatic detection.
Maximum Send Speed	Speed in Mbps. A setting of 0 means throughput speed is copied from the BaseValue case.
Send Resolution Speed	Binary Search only. Specify a minimum send speed of the traffic cycle for each frame size.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
IPv4 UDP Checksum	Select to enable the checksum calculation in the UDP header of IPv4 packets sent by this device.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).

Starting a RFC 3511 Concurrent Capacity throughput test

FortiTester tests the ability of the DUT to determine the maximum number of entries it can store in its connection table.

To start a concurrent capacity test:

1. Go to **Cases > Performance Testing > RFC Benchmark > RFC 3511 > Concurrent Capacity** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the pop-up dialog, configure DUT Working Mode as TP or NAT.
4. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
5. Select a **Certificate Group** if applicable.
6. Click **OK** to continue.
7. Configure the test case options described in RFC 3511 Concurrent Capacity Test Case configuration on page 123.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RFC 3511 Concurrent Capacity Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops

Settings	Guidelines
	automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Traffic Direction	Specify the direction of traffic flow.
Aging Time	Wait time for packet transmitting after traffic stop, in seconds. (range: 2 - 300)
Maximum Iterative Cycle	Maximum traffic cycle for each frame size. (minimum 1)
Iteration Mode	Select either Binary Search to search using binary search mode or Custom Load to search using a custom load.
Initial Concurrent TCP Connections	The number of concurrent TCP connections FortiTester creates at the beginning of the test.
Maximum Concurrent TCP Connections	The maximum number of concurrent TCP connections FortiTester will create during the test.
Concurrent Resolution Connections	FortiTester stops the binary search if the number of concurrent connections is less than the value set here.
Acceptable Failure Rate	Specify an acceptable failure rate.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.

Settings	Guidelines
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout	Select to override the TCP stack calculation of the retransmission

Settings	Guidelines
Calculation	timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can click **+Add** to add at most 32 requests.
Request Page	Select System Pages with Fixed or Random File Name and Content.
Get page	Select the file that the simulated clients access. Optionally, you can select **Custom** to choose the file template you have created in **Cases > Performance Testing > Objects > Files**.
Post page	Select the file that simulated servers response. You can edit the post parameters. The file size limit is 10MB.

Protocol Cases

Starting a TCP Protocol CIFS/SMB test

The TCP CIFS/SMB test establishes a TCP connection (three-way handshake), simulates a SMBv2 session, and closes the TCP connection.

To start a CIFS/SMB test:

1. Go to **Cases > Performance Testing > Application > CIFS/SMB** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.

3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a TCP Protocol CIFS/SMB test on page 126.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

CIFS/SMB Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.

Settings	Guidelines
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Domain Name	The domain of the hosting server.
User Name	The username used to log in to the host server and access the shared files.
Host Name	The name of the hosting server.
Share Directory	The directory of the shared files.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.

Settings	Guidelines
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.

Settings	Guidelines
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Request File	The file requested by the client. Select **Fixed File Name and Content** or select **Custom** to use files uploaded in **Objects > Files**.

Starting a TCP Protocol FIX test

The TCP FIX test establishes a TCP connection (three-way handshake), simulates a FIXv3 session, and closes the TCP connection.

To start a FIX test:

1. Go to **Cases > Performance Testing > Application > FIX** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a TCP Protocol FIX test on page 130.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TCP FIX Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing

Settings	Guidelines
	through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Username	The username of the simulated users. All the users use the same username and password.
Password	The password of the simulated users.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this

Settings	Guidelines
	timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the

Settings	Guidelines
	device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TCP Protocol FTP test

This FortiTester test establishes a TCP connection (three-way handshake), transfers one file by FTP, and then closes the TCP.

To start an FTP test:

1. Go to **Cases > Performance Testing > Protocol > TCP > FTP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in FTP Test Case configuration on page 134.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

FTP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to

Settings	Guidelines
	600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	

Settings	Guidelines
FTP Mode	Choose either active mode FTP or passive mode FTP.
FTP User	Create a username.
FTP Password	Create a password.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Server Close Mode	Set to 3 Way Fin by default. Not configurable.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).

Settings	Guidelines
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Request File	The file requested by the client. Select **Fixed File Name and Content** or select **Custom** to use files uploaded in **Objects > Files**.

Starting a TCP Protocol IMAP test

FortiTester tests the ability of the DUT to handle different types of IMAP. This test establishes a TCP connection (three-way handshake), receives one email by IMAP and closes the TCP connection.

To start an IMAP test:

1. Go to **Cases > Performance Testing > Protocol > TCP > IMAP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Mail IMAP Test Case configuration on page 138.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Mail IMAP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Email Address	The email sender address. The default is “tester@mailserver.com”.
Email Password	The password of email sender. The default is “tester@fts”.
Enable Attachment	Enable to add attachment in the email.
Attachment File Object	Select the file template you have created in **Cases > Performance Testing > Objects > Files**, then enter how many files you want to include in the attachment. For example, if you enter 3, the first three files in the file template will be included. Only available when the Enable Attachment is selected.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port	Select a change algorithm: **Increment** or **Random**. This setting

Settings	Guidelines
Change Algorithm	determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.

Settings	Guidelines
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TCP Protocol LDAP test

This FortiTester test establishes a TCP connection (three-way handshake), searches entries by LDAP, and then closes the TCP connection.

To start an LDAP test:

1. Go to **Cases > Performance Testing > Protocol > TCP > LDAP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.

5. Click **OK** to continue.
6. Configure the test case options described in Starting a TCP Protocol LDAP test on page 141.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

LDAP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	

Settings	Guidelines
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Search Type	Choose either Single level or Base object. A single level search will search one level below the base object, while a Base object search will only search the base object.
Login Type	Choose either Anonymous bind or Simple authentication.
Base DN	Enter the base distinguished name (DN) of the LDAP forest.
User DN	Enter the user DN subtree that is used when searching for user entries on the LDAP server. Only when the Login Type is Simple authentication.
Password	Enter the password of the bind account on the LDAP server. Only when the Login Type is Simple authentication.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of

Settings	Guidelines
	data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.

Settings	Guidelines
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TCP Protocol NFS test

The TCP NFS test establishes a TCP connection (three-way handshake), simulates a NFSv3 session, and closes the TCP connection.

To start a NFS test:

1. Go to **Cases > Performance Testing > Application > NFS** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a TCP Protocol NFS test on page 145.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

NFS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible.

Settings	Guidelines
	Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).

Settings	Guidelines
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Write Size	The buffer size of the write data sent from the client to the server.

Starting a TCP Protocol POP3 test

FortiTester tests the ability of the DUT to handle different types of POP3. This test traffic establishes a TCP connection (three-way handshake), receives one mail by POP3 and closes the TCP connection.

To start a POP3 test:

1. Go to **Cases > Performance Testing > Protocol > TCP > POP3** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Mail POP3 Test Case configuration on page 149.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Mail POP3 Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Email Address	The email sender address. The default is “tester@mailserver.com”.
Email Password	The password of email sender. The default is “tester@fts”.
Enable Attachment	Enable to add attachment in the email.
Attachment File Object	Select the file template you have created in **Cases > Performance Testing > Objects > Files**, then enter how many files you want to include in the attachment. For example, if you enter 3, the first three files in the file template will be included. Only available when the Enable Attachment is selected.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port	Select a change algorithm: **Increment** or **Random**. This setting

Settings	Guidelines
Change Algorithm	determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.

Settings	Guidelines
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TCP Protocol RDP test

The test traffic establishes a TCP connection (three-way handshake), constructs a RDP connection, sends fastpath format events and then closes the TCP connection.

To start a RDP test:

1. Go to **Cases > Performance Testing > Application > RDP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.

5. Click **OK** to continue.
6. Configure the test case options described in Starting a TCP Protocol RDP test on page 152.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TCP RDP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	

Settings	Guidelines
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Domain	The domain name of the remote server to access.
Username	The username of the simulated users. All the users use the same username and password.
Password	The password of the simulated users.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these

Settings	Guidelines
	acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send

Settings	Guidelines
	traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TCP Protocol SMTP test

FortiTester tests performance of a target device under SMTP traffic by simulating a volume of clients to generate SMTP traffic.

To start an SMTP test:

1. Go to **Cases > Performance Testing > Protocol > TCP > SMTP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Mail SMTP Test Case configuration on page 156.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Mail SMTP Test Case configuration

Settings	Guidelines
Basic Information	

Settings	Guidelines
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.

Settings	Guidelines
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
SMTP Email Address	The email sender address. The default is “tester@mailserver.com”.
SMTP Email To	The email receiver address. The default is “receiver@mailserver.com”.
Enable Authentication	Enable to use password when sending SMTP email.
SMTP Email Password	The password of email sender. The default is “tester@fts”.
Enable Attachment	Enable to add attachment in the email.
Attachment File Object	Select the file template you have created in **Cases > Performance Testing > Objects > Files**, then enter how many files you want to include in the attachment. For example, if you enter 3, the first three files in the file template will be included. Only available when the Enable Attachment is selected.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.

Settings	Guidelines
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible.

Settings	Guidelines
	Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a TCP Protocol SSH test

This test establishes a TCP connection (three-way handshake), simulates a SSH interactive session and closes the TCP connection.

To start a SSH test:

1. Go to **Cases > Performance Testing > Application > SSH** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a TCP Protocol SSH test on page 160.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TCP SSH Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600.

Settings	Guidelines
	Note: You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Username	The username of the simulated users. All the users use the same username and password.

Settings	Guidelines
Password	The password of the simulated users.
Crypto Enable	Enable to send packets in ciphertext.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the

Settings	Guidelines
	maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a UDP Protocol DNS latency test

FortiTester tests the latency of the DUT while handling DNS query requests. The DUT could be a gateway device or a DNS server. This test traffic sends DNS requests to a DNS server and measures latency.

To start a DNS test:

1. Go to **Cases > Performance Testing > Protocol > UDP > DNS Latency** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in DNS Latency Test Case configuration on page 164.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DNS Latency Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.

Settings	Guidelines
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Time Out	The default is 1000 microseconds.
Renew Socket	Specify Yes or No. If Yes, the client side renews a socket to send out the next query (note if the client profile "Domain Policy" is set as List, all queries for the names in the domain list will use the same socket; after that a new socket will be created for next batch of queries). If No, use the old socket.
Client Profile	
Domain Policy	Random or List. If Random is selected, FortiTester generates random domain names for queries. If List is select, FortiTester uses queries in the specified list.
Random Length	Specify the random length of the domain policy.
Domain	If Domain Policy is List, specify a list of domain name records. For example: `fortinet.com:A,www.fortinet.com:A, fortitester.com:MX` A name followed with a ":A" means it's an address record, while a ":MX" means a mail exchange record.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.

Settings	Guidelines
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a UDP Protocol NTP test

The NTP test sends NTP query traffic to an NTP server under test. FortiTester receives real time information from the DUT and measures latency.

To start an NTP test:

1. Go to **Cases > Performance Testing >Protocol > UDP > NTP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Configure the test case options as described in NTP Test Case configuration on page 167.
6. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

NTP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops

Settings	Guidelines
	automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Time Out	The default is 1000 microseconds.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Settings	Guidelines
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a UDP Protocol RADIUS test

The RADIUS test sends RADIUS requests to a RADIUS server to measure the number of response types per second.

To start a RADIUS test:

1. Go to **Cases > Performance Testing >Protocol > UDP > RADIUS** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in RADIUS Test Case configuration on page 169.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RADIUS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.

Settings	Guidelines
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
RADIUS Request Time Out	Time in microseconds before a RADIUS request times out.
Client Profile	
RADIUS Secret Key	Specify a shared secret key for the transaction.
Username	The username of the simulated users. All the users use the same username and password.
Password	The password of the simulated users.
Authentication Method	Select either the PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol).
Radius Accounting Time	Specify an accounting time. A time of 0 means accounting features will be disabled.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses

Settings	Guidelines
	and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a UDP Protocol SIP test

FortiTester tests UDP SIP by sending UDP frames with the specified SIP from the client ports to the server ports.

To start a UDP SIP test:

1. Go to **Cases > Performance Testing > Protocol > UDP > SIP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a UDP Protocol SIP test on page 171.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

UDP SIP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.

Settings	Guidelines
Client Profile	
From	This field indicates the initiator of the request.
To	This field specifies the logical recipient of the request.
Re-Transfer Time	Select a time limit after which FortiTester will resend the data packet.
Retry Limit	Select the number of times FortiTester will attempt a transfer.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a UDP Protocol TFTP test

The TFTP test sends TFTP requests to a TFTP server to measure the number of requests sent and performed per second.

To start a TFTP test:

1. Go to **Cases > Performance Testing > Protocol > UDP > TFTP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in TFTP Test Case configuration on page 174.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TFTP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.

Settings	Guidelines
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Renew Socket	Specify Yes or No. If Yes, the client side renews a socket to send out the next query (note if the client profile “Domain Policy” is set as List, all queries for the names in the domain list will use the same socket; after that a new socket will be created for next batch of queries). If No, use the old socket.
Client Profile	
TFTP Mode	Select to download or upload a file to the server.
Re-Transfer Time	Select a time limit after which FortiTester will resend the data packet.
Retry Limit	Select the number of times FortiTester will attempt a transfer.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
TFTP Block Size	Specify a Block Size. The default is 512 bytes.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	

Settings	Guidelines
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Request File	The file requested by the client. Select **Fixed File Name and Content** or select **Custom** to use files uploaded in **Objects > Files**.

Starting a DHCP test

The IPv4 DHCP test sends DHCP requests to the DHCP server and measures latency. The IPv6 DHCP test sends NS and RA messages to request an IPv6 address through DHCPv6 stateless mode.

To start a DHCP test:

1. Go to **Cases > Performance Testing > Protocol > DHCP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in DHCP Test Case configuration on page 177.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DHCP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.

Settings	Guidelines
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Time Out	The default is 1000 microseconds.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the

Settings	Guidelines
	device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting an IGMP test

The IGMP test sends join messages to the device under test (DUT), such as a router or firewall, and the DUT forwards the data stream from the server.

Before starting an IGMP test:

Configure a multicast firewall with multicast-routing protocols. The following shows an example configuration using FortiGate.

```
FG1K5D3I14801425 # get system settings | grep multicast
multicast-forward : enable
multicast-ttl-notchange: disable
gui-multicast-policy: enable

FG1K5D3I14801425 # get router multicast | grep routing
multicast-routing : disable

FG1K5D3I14801425 # show firewall multicast-policy
config firewall multicast-policy
edit 1
set srcintf "port35"
set dstintf "port33"
set srcaddr "host-19-1-1-100"
set dstaddr "m-226-1-2-3"
next
end
```

To start an IGMP test:

1. Go to **Cases > Performance Testing > Protocol > IGMP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in IGMP Test Case configuration on page 180.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

While the test case is running, use the following command on your FortiGate firewall to see the multicast session:

FG1K5D3I14801425 # diagnose sys mcast-session list

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

IGMP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all

Settings	Guidelines
	TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client Network	
Network MTU	The maximum transmission unit size.
Multicast IP	Specify a multicast IP. For the example FortiGate configuration shown above, the Muticast IP would be 226.1.2.3.
Server Network	
Network MTU	The maximum transmission unit size.
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting an RTSP/RTP test

The RTSP/RTP test establishes a TCP connection with a three-way handshake, controls media sessions between end points, and closes the TCP connection. This test also tests the firewall's ability to open and close pinholes.

To start an RTSP test:

1. Go to **Cases > Performance Testing > Protocol > RTSP/RTP** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in RTSP Test Case configuration on page 182.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

RTSP Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.

Settings	Guidelines
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.

Settings	Guidelines
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the

Settings	Guidelines
	device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Application Cases

Starting an Amazon S3 test

The Amazon S3 test simulates Amazon S3 (Simple Storage Service) traffic, such as file uploading and downloading, and folder creating.

To start an Amazon S3 test:

1. Go to **Cases > Performance Testing > Application > Amazon S3** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Select **Protocol** type of the simulated traffic.
6. Click **OK** to continue.
7. Configure the test case options described in Starting an Amazon S3 test on page 185.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Amazon S3 Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible.

Settings	Guidelines
	Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Amazon S3 Command List	Select the commands that will be sent in one TCP stream.
Amazon S3 Fixed Format	If it is enabled, FortiTester will generate traffic data before sending data to the target device, and the data will not be changed during the testing phase. It can improve the performance of FortiTester. If it is disabled, FortiTester will generate traffic data dynamically in the testing phase.
Amazon S3 Bucket Name (Folder Name)	User can set the bucket name, the bucket name is similar to a folder name
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked

Settings	Guidelines
	on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	

Settings	Guidelines
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Request File	The file requested by the client, and it has **Fixed File Name and Content** automatically generated by FortiTester. You need to specify the size of the file.

Starting an AOL Chat test

The AOL Chat (AIM) establishes a TCP connection (three-way handshake), simulates a AIM session, and closes the TCP connection.

To start an AOL Chat test:

1. Go to **Cases > Performance Testing > Application > AOL Chat** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting an AOL Chat test on page 189.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

AOL Chat Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible.

Settings	Guidelines
	Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Username	The username of the simulated users. All the users use the same username and password.
Password	The password of the simulated users.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag

Settings	Guidelines
	causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a BitTorrent test

The TCP BitTorrent test simulates a download process between peers.

To start a BitTorrent test:

1. Go to **Cases > Performance Testing > Application > BitTorrent** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a BitTorrent test on page 193.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

TCP BitTorrent Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
BitTorrent Piece Size	The size of pieces in downloading file.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.

Settings	Guidelines
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.

Settings	Guidelines
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Request File	The file requested by the client. Select **Fixed File Name and Content** or select **Custom** to use files uploaded in **Objects > Files**.

Starting a DB2 test

DB2 test traffic establishes a TCP connection (three-way handshake), sends SQL command by DB2, and then closes the TCP connection.

To start a DB2 test:

1. Go to **Cases > Performance Testing > Application > DB2** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Click **OK** to continue.
5. Configure the test case options described in Test Case configuration Table.
6. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DB2 Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.

Settings	Guidelines
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.

Settings	Guidelines
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a Facebook test

The Facebook test simulates Facebook traffic, such as login, search and watch video.

To start a Facebook test:

1. Go to **Cases > Performance Testing > Application > Facebook** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Select **Protocol** type of the simulated traffic.
6. Click **OK** to continue.
7. Configure the test case options described in Starting a Facebook test on page 200.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Facebook Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Supported Behaviors	Select the behaviors that will be simulated and sent in one TCP stream. **Other** means the traffic data will be recognized as “facebook” traffic without being sub-classified by FortiGate.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is

Settings	Guidelines
	also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.

Settings	Guidelines
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a Gmail test

The Gmail test establishes a TCP connection (three-way handshake), sends one email by Gmail and closes the TCP connection.

To start a Gmail test:

1. Go to **Cases > Performance Testing > Application > Gmail** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.

4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a Gmail test on page 203.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Gmail Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the	

Settings	Guidelines
configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Address	The sender's email address.
Password	The sender's email password.
To	The receiver's email address.
Subject	The subject of the mail. The maximum length is 256 bytes.
Body	The body of the mail. The maximum length is 512 bytes.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Quiet Shutdown	Enable to apply safe shutdown procedure to SSL connections by sending SSL alert to the peer.
PSK/SRP	Enable to support PSK and SRP ciphers.
PSK/SRP Username	Username for PSK and SRP ciphers.
PSK/SRP Password	PSK/SRP for PSK and SRP ciphers.
Available SSL Versions	Select SSL versions. TLSv1.3 and other SSL versions are mutually exclusive. This means you can't select TLSv1.3 at the same time with other SSL versions.

Settings	Guidelines
Elliptic Curve	Select the Elliptic Curve that the client support for key exchanges. Only available when you select TLSv1.3.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server. This option applies only to TLS v1 and TLS v1.2. It does not apply to TLS v1.3.
Enable Client Certificate	Enable the client authentication for HTTPS cases.
Certificate	Select the certificate created in **Performance Testing > Objects > Certificates**. Available only when Enable Client Certificate is enabled.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Certificate	Select the certificates you have created in **Performance Testing > Objects > Certificate Groups**. If you have selected a certificate group in the **Select case options** window, then you are not allowed to select certificate here. If you have selected ECDHE-ECDSA ciphers for the client, then you must reference an ECC certificate for the server, otherwise the SSL handshake will fail.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server.
Client/Server TCP Options	

Settings	Guidelines
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	

Settings	Guidelines
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a Gtalk test

The Gtalk test establishes a TCP connection (three-way handshake), simulates a Gtalk chat by XMPP, and closes the TCP connection.

To start a Gtalk test:

1. Go to **Cases > Performance Testing > Application > Gtalk** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a Gtalk test on page 208.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Gtalk Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the

Settings	Guidelines
	device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Gtalk From	This field indicates the initiator of the Gtalk request.
Gtalk To	This field specifies the logical recipient of the Gtalk request.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag

Settings	Guidelines
	causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a MSSQL test

MSSQL test traffic establishes a TCP connection (three-way handshake), sends SQL command by MSSQL client, and then closes the TCP connection.

To start a MSSQL test:

1. Go to **Cases > Performance Testing > Application > MSSQL** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a MSSQL test on page 212.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

MSSQL Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of

Settings	Guidelines
	data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.

Settings	Guidelines
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a MySQL test

MySQL test traffic establishes a TCP connection (three-way handshake), sends SQL command by MySQL, and then closes the TCP connection.

To start a MySQL test:

1. Go to **Cases > Performance Testing > Application > MySQL** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Test Case configuration Table.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

MySQL Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.

Settings	Guidelines
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).

Settings	Guidelines
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a Netflix test

Netflix test establishes a TCP connection (three-way handshake), and simulates Netflix traffic, such as login, watching movie and logout.

To start a Netflix test:

1. Go to **Cases > Performance Testing > Application > Netflix** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select **Protocol** type of the simulated traffic.
5. Click **OK** to continue.
6. Configure the test case options described in Test Case configuration Table.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Netflix Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.

Settings	Guidelines
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Supported Behaviors	Select the behaviors that will be simulated and sent in one TCP stream. **Other** means the traffic data will be recognized as "Netflix" traffic without being sub-classified by FortiGate.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.

Settings	Guidelines
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response

Settings	Guidelines
	after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting an Oracle TNS test

The Oracle TNS test establishes a TCP connection (three-way handshake), connects and authenticates to databases, and then closes the TCP connection.

To start an Oracle TNS test:

1. Go to **Cases > Performance Testing > Application > Oracle TNS** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting an Oracle TNS test on page 222.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Oracle TNS Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing

Settings	Guidelines
	through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the

Settings	Guidelines
	maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Settings	Guidelines
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a PSQL test

This FortiTester test establishes a TCP connection (three-way handshake), send psql command by PSQL, and then closes the TCP connection.

To start a PSQL test:

1. Go to **Cases > Performance Testing > Protocol > TCP > PSQL** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in PSQL Test Case configuration on page 226.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

PSQL Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs,

Settings	Guidelines
	increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	

Settings	Guidelines
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.

Settings	Guidelines
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a Twitter test

The Twitter test simulates Twitter traffic, such as post article and watch video.

To start a Twitter test:

1. Go to **Cases > Performance Testing > Application > Twitter** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Select **Protocol** type of the simulated traffic.
6. Click **OK** to continue.
7. Configure the test case options described in Starting a Twitter test on page 229.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Twitter Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.

Settings	Guidelines
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Supported Behaviors	Select the behaviors that will be simulated and sent in one TCP stream. **Other** means the traffic data will be recognized as "Twitter" traffic without being sub-classified by FortiGate.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.

Settings	Guidelines
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.

Settings	Guidelines
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a WebEx test

WebEx test establishes a TCP connection (three-way handshake), and simulates WebEx traffic, such as login and WebEx.

To start a WebEx test:

1. Go to **Cases > Performance Testing > Application > WebEx** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select **Protocol** type of the simulated traffic.

5. Click **OK** to continue.
6. Configure the test case options described in Test Case configuration Table.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

WebEx Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	

Settings	Guidelines
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Supported Behaviors	Select the behaviors that will be simulated and sent in one TCP stream.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK

Settings	Guidelines
	packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).

Settings	Guidelines
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a WhatsApp test

The WhatsApp case establishes a TCP connection(three-way handshake), controls media sessions between end points and closes the TCP connection.

To start a WhatsApp test:

1. Go to **Cases > Performance Testing > Protocol > WhatsApp** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a WhatsApp test on page 237.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

WhatsApp Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
Client Profile	
WhatsApp Type	Select the WhatsApp data type to simulate.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.

Settings	Guidelines
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response

Settings	Guidelines
	after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a Yahoo Mail test

The Yahoo Mail test establishes a TCP connection (three-way handshake), sends one email by Yahoo and closes the TCP connection.

To start a Yahoo Mail test:

1. Go to **Cases > Performance Testing > Application > Yahoo Mail** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Yahoo Mail Test Case configuration on page 241.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Yahoo Mail Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle.

Settings	Guidelines
	Connections/second: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible. Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Address	The sender’s email address.
Password	The sender’s email password.
To	The receiver’s email address.
Subject	The subject of the mail. The maximum length is 256 bytes.
Body	The body of the mail. The maximum length is 512 bytes.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Quiet Shutdown	Enable to apply safe shutdown procedure to SSL connections by sending SSL alert to the peer.
PSK/SRP	Enable to support PSK and SRP ciphers.
PSK/SRP Username	Username for PSK and SRP ciphers.
PSK/SRP Password	PSK/SRP for PSK and SRP ciphers.
Available SSL Versions	Select SSL versions. TLSv1.3 and other SSL versions are mutually exclusive. This means you can’t select TLSv1.3 at the same time with other SSL versions.
Elliptic Curve	Select the Elliptic Curve that the client support for key exchanges. Only available when you select TLSv1.3.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user

Settings	Guidelines
	attempting to use the same SSL Session ID, initially negotiated with the server. This option applies only to TLS v1 and TLS v1.2. It does not apply to TLS v1.3.
Enable Client Certificate	Enable the client authentication for HTTPS cases.
Certificate	Select the certificate created in **Performance Testing > Objects > Certificates**. Available only when Enable Client Certificate is enabled.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Certificate	Select the certificates you have created in **Performance Testing > Objects > Certificate Groups**. If you have selected a certificate group in the **Select case options** window, then you are not allowed to select certificate here. If you have selected ECDHE-ECDSA ciphers for the client, then you must reference an ECC certificate for the server, otherwise the SSL handshake will fail.
Session Resumption	• Disabled (turns off session resumption). • Resume Session by Ticket: Select this option to simulate a client presenting a ticket to a TLS server, having originated from that server, for the purpose of resuming a TLS session. • Resume Session by Session: Select this option to simulate a user attempting to use the same SSL Session ID, initially negotiated with the server.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked

Settings	Guidelines
	on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	

Settings	Guidelines
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Starting a YouTube test

The TCP YouTube test simulates YouTube client to connect to a YouTube server and access audio or video streams.

To start a YouTube test:

1. Go to **Cases > Performance Testing > Application > YouTube** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Select **Protocol** type of the simulated traffic.
6. Click **OK** to continue.
7. Configure the test case options described in Starting a YouTube test on page 245.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

YouTube Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Mode	**Simuser:** Simulated users. Simuser simulates a user processing through an Actions list one at a time. It allows you to determine the maximum number of concurrent users your device, infrastructure, or system can handle. **Connections/second**: This mode simulates TCP connections, each of them containing up to hundreds of transactions. It's useful to test how many concurrent connections can be handled by your device.
Simulated Users	Number of users to simulate.
Connections per Second	Rate of new connections per second. The default is 0, which means the device will Second create connections as fast as possible.

Settings	Guidelines
	Available only when Connections/second is selected for Mode.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the

Settings	Guidelines
	maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Explicit Congestion Notification	Select the Expilcit Congestion Notification(ECN) support level: **Disabled**: Disables all support for ECN. **Support ECN**: ECN will be supported if the remote host initiates it first. **Use ECN**: ECN will be initiated for new connections.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

Settings	Guidelines
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.
Action	
Request Stream	Select the stream file to request, or upload a new one in **Objects >Files**.

Replay Cases

Starting a Traffic Replay test

FortiTester tests user-defined scenarios by replaying pcap files. Typically, pcap files are generated by programs like tcpdump or Wireshark.

Note: The Traffic Replay test is available only in Standalone work mode.

Before you begin:

- You must create pcap files that can be replayed. Only IPv4 traffic is supported. Maximum file size is 200MB.

To start a Traffic Replay test:

1. Go to **Cases > Performance Testing > Replay > Traffic** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Traffic Replay Test Case configuration on page 250.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Traffic Replay Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Loops	Number of times to play the pcap file. 0 means as many as possible.
Input Pcap	Select a pcap file to send. Note the uploaded files can be used for future cases.

Settings	Guidelines
Client/Server Network	
Network MTU	The maximum transmission unit size.
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.

Starting a GTP Replay test

FortiTester tests GTP connections by replaying existing GTPv1 and GTPv2 files. FortiTester uses these files to send test packets to the device under test (DUT).

Note: The GTP Replay test is available only in Standalone work mode.

Before you begin:

- You must create pcap files that can be replayed. Only IPv4 traffic is supported. Maximum file size is 200MB.

To start a GTP Replay test:

1. Go to **Cases > Performance Testing > Replay > GTP** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting a GTP Replay test on page 251.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

GTP Replay Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Replay Time Out	This timeout specifies how long the client waits for a response from the server. If the client does not receive a response within the timeout, it considers the packet lost. The default value is 2 milliseconds.
Break Once Packet Lost	Select Yes or No. The Yes option means when the system identifies packet loss (the server side has not received the packet that client sent out), it stops the current GTP replay (pcap file), and continues the test with the next GTP file. The No option (the default) means a break is not set; the current replay continues.
Client/Server Network	

Settings	Guidelines
Network MTU	The maximum transmission unit size.
Action	
GTP Packet List	Select pcap files to test.

Packet Capture Cases

Starting a packet capture test

The packet capture test captures packets received from the network adapter.

To start a packet capture test:

1. Go to **Cases > Performance Testing > Packet Capture > Packet Capture** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options as described in Packet Capture Test Case configuration on page 254.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

To start /stop a packet capture test while another test is running:

From the run page of the other test, follow the steps below.

1. Go to **Capture > Client**.
2. Click **Restart**, under status.
3. Configure the desired settings.
4. Click **Start** to run the packet capture test.

Packet Capture Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.

Settings	Guidelines
Network Settings	
Client Ports	The graphic depicts the test ports for client-side connections. The client ports simulate the behavior of clients. You must select at least one client port. After you select a port for client, a ✓ (check mark) is displayed on the port icon, and a tab for the port is added below the graphic. Use the tabs to toggle the Capture Packets controls for each port.
Capture Packets	
Capture Packets	Set packet capture options if you want to capture the traffic of this port. You can capture all packets or specify a number. You can set packet capture filters for host IP/port and protocol. **Note**: The system allocates temporary disk space for packet captures. The limit is 6,000,000 packets. The packets are saved to a temporary file that you can download from the running test case page. The filename indicates whether it is client or server communication and the interface port number. For example, client_port1.pcap. When a subsequent test case with packet capture enabled uses the same interface port as a previous one, the previous file is overwritten.
Load	
Packet Analysis	Select **Yes** to analyze bandwidth percentage for each protocol.
Network	
Network MTU	Maximum Transmission Unit for a data packet. FortiTester does not send out data packets larger than this value. Most DUTs have a limit for packet size. The default is 1500. Not configurable.

Mixed Traffic Cases

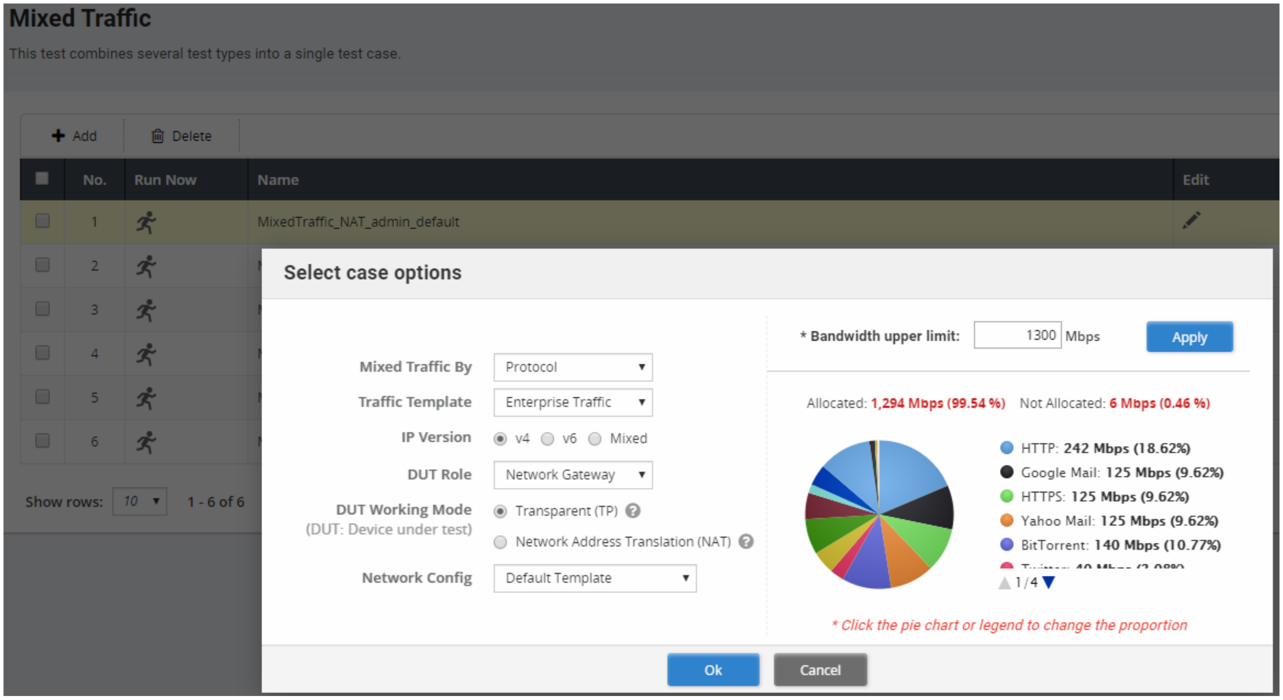
Starting a mixed traffic test

FortiTester tests mixed traffic performance by simulating multiple clients that burst all types of traffic simultaneously.

To start a Mixed Traffic test:

1. Go to **Cases > Performance Testing > Mixed Traffic** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.

3. In the popup dialog, select the kind of mixed traffic test you wish to create. You can create a test based on Protocol, Action, Case Type, or Existing Test Cases.
4. Select the traffic template when you create a test by protocol. When the template is Enterprise Traffic, Bandwidth Traffic, or Default, you can click any part of the pie chart to set the proportions.



Mixed Traffic

This test combines several test types into a single test case.

□	No.	Run Now	Name	Edit
□	1		MixedTraffic_NAT_admin_default	
□	2			
□	3			
□	4			
□	5			
□	6			

Show rows: 10 1 - 6 of 6

Select case options

Mixed Traffic By: Protocol

Traffic Template: Enterprise Traffic

IP Version: ● v4 ○ v6 ○ Mixed

DUT Role: Network Gateway

DUT Working Mode (DUT: Device under test): ● Transparent (TP) ○ Network Address Translation (NAT)

Network Config: Default Template

* Bandwidth upper limit: 1300 Mbps

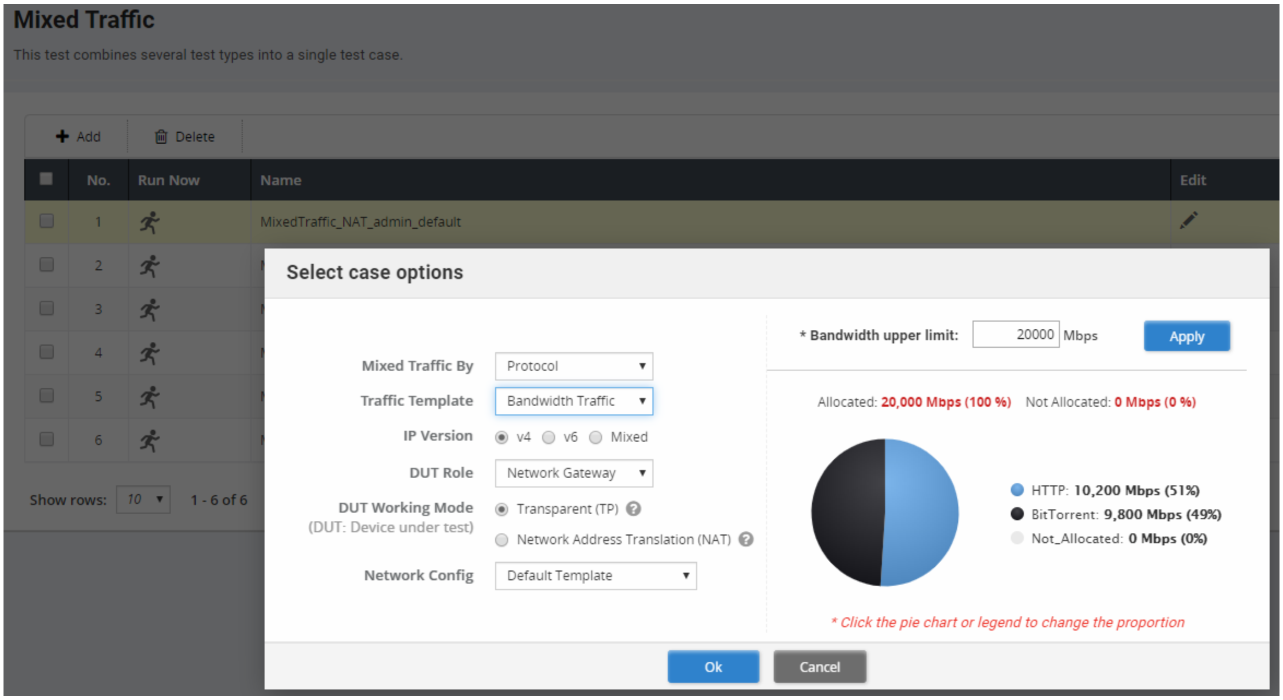
Allocated: 1,294 Mbps (99.54 %) Not Allocated: 6 Mbps (0.46 %)

- HTTP: 242 Mbps (18.62%)
- Google Mail: 125 Mbps (9.62%)
- HTTPS: 125 Mbps (9.62%)
- Yahoo Mail: 125 Mbps (9.62%)
- BitTorrent: 140 Mbps (10.77%)
- Twitter: 40 Mbps (3.08%)

1 / 4

* Click the pie chart or legend to change the proportion

For Enterprise traffic mix, FortiTester requires VM16 or above, with minimum 32GB of RAM assigned; as more processing power is required if more protocols are initiated.



Mixed Traffic

This test combines several test types into a single test case.

☐	No.	Run Now	Name	Edit
☐	1	🏃	MixedTraffic_NAT_admin_default	✎
☐	2	🏃		
☐	3	🏃		
☐	4	🏃		
☐	5	🏃		
☐	6	🏃		

Show rows: 10 1 - 6 of 6

Select case options

Mixed Traffic By: Protocol

Traffic Template: Bandwidth Traffic

IP Version: ● v4 ○ v6 ○ Mixed

DUT Role: Network Gateway

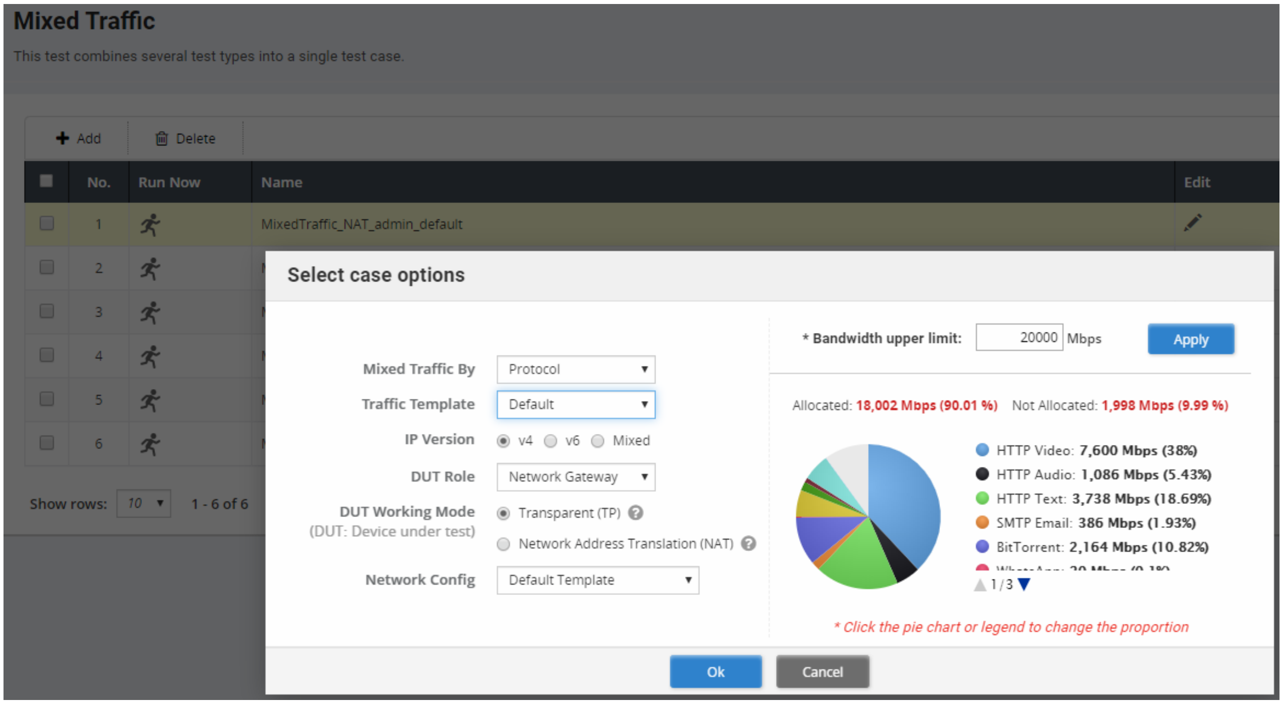
DUT Working Mode (DUT: Device under test): ● Transparent (TP) ○ Network Address Translation (NAT)

Network Config: Default Template

* Bandwidth upper limit: 20000 Mbps Apply

Allocated: 20,000 Mbps (100 %) Not Allocated: 0 Mbps (0 %)

* Click the pie chart or legend to change the proportion



Mixed Traffic

This test combines several test types into a single test case.

☐	No.	Run Now	Name	Edit
☐	1	🏃	MixedTraffic_NAT_admin_default	✎
☐	2	🏃		
☐	3	🏃		
☐	4	🏃		
☐	5	🏃		
☐	6	🏃		

Show rows: 10 1 - 6 of 6

Select case options

Mixed Traffic By: Protocol

Traffic Template: Default

IP Version: ● v4 ○ v6 ○ Mixed

DUT Role: Network Gateway

DUT Working Mode (DUT: Device under test): ● Transparent (TP) ○ Network Address Translation (NAT)

Network Config: Default Template

* Bandwidth upper limit: 20000 Mbps Apply

Allocated: 18,002 Mbps (90.01 %) Not Allocated: 1,998 Mbps (9.99 %)

HTTP Video: 7,600 Mbps (38%)
HTTP Audio: 1,086 Mbps (5.43%)
HTTP Text: 3,738 Mbps (18.69%)
SMTP Email: 386 Mbps (1.93%)
BitTorrent: 2,164 Mbps (10.82%)
1 / 3

* Click the pie chart or legend to change the proportion

5. Select the types of traffic to mix in the test.
6. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
7. Select a **Certificate Group** if applicable.
8. Click **OK** to continue.

9. Configure the proportions of the mixed traffic.
10. Configure the test case options as described in Mixed Traffic Test Case configuration on page 258. The specific settings will depend on what types of traffic were included in the mix. Refer to the section for that specific test for more information.
11. Click **Start** to run the test case.

FortiTester saves the configuration automatically, so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Mixed Traffic Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600.**Note:**You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Client/Server Network	
Network MTU	Maximum Transmission Unit for a data packet. FortiTester does not send out data packets larger than this value. Most DUTs have a limitation for packet size. The default is 1500. Not configurable.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.

Settings	Guidelines
Protocol Settings Configure settings for the cases you have selected When creating a case.	

Security Testing

Go to **Cases > Security Testing** to start the following security tests.

- DDoS
- IPS
- AntiVirus
- Web Protection
- Mixed Traffic

Also, you can manage the following:

- User intrusion group
- FGD intrusion group
- AntiVirus file group
- Web protection group
- FGD intrusion service
- Web protection service

DDoS Cases

Starting a DDoS single packet flood test

FortiTester tests the DUT's ability to handle different types of DDoS attacks. This test attempts to deplete the DUT's resources by flooding the DUT with non-session based attacks.

To start a single packet flood test:

1. Go to **Cases > Security Testing > DDoS > Single Packet Flood** to display the test case summary page.
2. Click **Add** to display the **Select case options**dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in DDoS Single Packet Flood Test Case configuration on page 261.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DDoS Single Packet Flood Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
DDoS Type	DDoS attack traffic: Single Packet Flood. After you select a type, selection boxes for subtypes are displayed below. To change the percentage mix of subtypes, double-click the pie chart and adjust the percentages.

Settings	Guidelines
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.

Starting a DDoS TCP session flood test

FortiTester tests the DUT's ability to handle different types of DDoS attacks. This test attempts to deplete the DUT's resources by flooding the DUT with TCP attacks.

To start a TCP session flood test:

1. Go to **Cases > Security Testing > DDoS > TCP Session Flood** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in DDoS TCP Session Flood Test Case configuration on page 263.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DDoS TCP Session Flood Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.

Settings	Guidelines
DDoS Type	DDoS attack traffic: Single Packet Flood. After you select a type, selection boxes for subtypes are displayed below. To change the percentage mix of subtypes, double-click the pie chart and adjust the percentages.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.

Settings	Guidelines
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.

Starting a DDoS HTTP session flood test

FortiTester tests the DUT's ability to handle attempts to deplete the DUT's resources by flooding the DUT with HTTP attacks.

To start a HTTP session flood test:

1. Go to **Cases > Security Testing > DDoS > HTTP Session Flood** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in DDoS HTTP Session Flood Test Case configuration on page 266.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DDoS HTTP Session Flood Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.

Settings	Guidelines
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.
DDoS Type	DDoS attack traffic: Single Packet Flood. After you select a type, selection boxes for subtypes are displayed below. To change the percentage mix of subtypes, double-click the pie chart and adjust the percentages.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the

Settings	Guidelines
	maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Transactions per Second	Rate of new transactions per second. The default is 0, which means the device will send traffic as fast as possible. Available only under Client tab.
Server Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.

Starting a DDoS concurrent session flood test

FortiTester tests the DUT's ability to handle attempts to deplete the DUT's resources. FortiTester floods the DUT with HTTP attacks and then puts the session on hold for an extended period of time.

To start a concurrent session flood test:

1. Go to **Cases > Security Testing > DDoS > Concurrent Session Flood** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.

5. Click **OK** to continue.
6. Configure the test case options described in DDoS Concurrent Session FloodTest Case configuration on page 269.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DDoS Concurrent Session FloodTest Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	

Settings	Guidelines
Load	
Simulated Users	Number of users to simulate.
Maximum Concurrent Connections	The number of concurrent connections.
DDoS Type	DDoS attack traffic: Single Packet Flood. After you select a type, selection boxes for subtypes are displayed below. To change the percentage mix of subtypes, double-click the pie chart and adjust the percentages.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).

Settings	Guidelines
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).

Starting a DDoS UDP packet flood test

FortiTester tests the DUT's ability to handle attempts to deplete DUT's resources. FortiTester floods the DUT with UDP packets with random source IP and port on client-traffic side.

To start a UDP packet flood test:

1. Go to **Cases > Security Testing > DDoS > UDP Packet Flood** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in DDos UDP Packet Flood Test Case configuration on page 272.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

DDos UDP Packet Flood Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	Time in seconds for traffic to ramp up when you start the test.
Ramp Down Time	Time in seconds for traffic to ramp down when you stop the test.

Settings	Guidelines
Frame Size	The range of frame size is 64 to 8192. When the (frame size-18) is larger than MTU, the UDP packet will be fragmented.
Client Profile	
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Case Server Port	The server port where the test case traffic arrives.
Client Network	
Network MTU	The maximum transmission unit size.
IP Option DSCP	Provide quality of service (QoS).
Client Limit	
Bandwidth	Bandwidth in Mbps. The default is 0, which means the device will send traffic as fast as possible.
Packets per Second	Rate of the packets per second. The default is 0, which means the device will create transactions as fast as possible.

IPS Cases

Starting an IPS Attack Replay test

FortiTester can test security systems by replaying a predefined or customized set of attack traffic. The predefined set covers 100 types of attacks. The test result shows the CVE-ID for every type of attack. You can also see the attack list in the **Cases > Security Testing > IPS > Attack** page.

Note: The Attack Replay test is available only in Standalone work mode.

Before you begin:

- Optional. If you want to test custom attack traffic, you must create a package of pcap files that can be replayed. Only IPv4 traffic is supported. Follow the file naming convention: ***Description*[_CVE-$CVEID].pcap**. Here [] means optional. The file type can be .pcap, .tgz, .tar.gz, or .zip. A .tgz, .tar.gz, or .zip file includes a group of .pcap files. Maximum file size is 200MB. You can upload it, put it into a default or customized group, and the select the group of attack files you want to replay later.

To start an Attack Replay test:

1. Go to **Cases > Security Testing > IPS > Attack** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Attack Replay Test Case configuration on page 274.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Attack Replay Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.

Settings	Guidelines
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Loops	Number of times to send the attacks. 0 means as many as possible.
Delay	The period that FortiTester will wait until it sends the next attack.
Replay Time Out	This timeout specifies how long the client waits for a response from the server. If the client does not receive a response within the timeout, it considers the packet lost. The default value is 2 milliseconds.
Break Once Packet Lost	Select Yes or No. The Yes option means when the system identifies packet loss (the server side has not received the packet that client sent out), it stops the current GTP replay (pcap file), and continues the test with the next GTP file. The No option (the default) means a break is not set; the current replay continues.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Action	
FGD Intrusion Group	Select the FortiGuard intrusion group you have created in **Security Testing > Objects > FGD Intrusion group**. See Managing the FGD Intrusion group on page 290.
FGD Free Package	Enable using FortiGuard free package.
User Intrusion Group	Select attacks from the user-defined attack list. Before you can select them, you must upload pcap files that contain your customized attack traffic. See Managing the User Instruction group on page 289.

Starting an IPS HTTP Evasion test

The HTTP Evasion Replay test replays packet tampered through HTTP evasion engine. FortiTester corrupts custom HTTP pcap file according to the selected Evasion Types, then replay such corrupted pcap files to target servers to see if servers have the ability to resist such attack.

It is only available for premium users. You should upgrade this device to FortiGuard Premium Subscription Services to enable this feature.

Before you begin:

- Optional. If you want to test custom attack traffic, you must create a package of pcap files that can be replayed. Only IPv4 traffic is supported. Follow the file naming convention: ***Description*****[_CVE-$CVEID].pcap**. Here [] means optional. The file type can be .pcap, .tgz, .tar.gz, or .zip. A .tgz, .tar.gz, or .zip file includes a group of .pcap files. Maximum file size is 200MB. You can upload it, put it into a default or customized group, and the select the group of attack files you want to replay later.

To start an HTTP Evasion test:

1. Go to **Cases > Security Testing > IPS > HTTP Evasion** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in HTTP Evasion Test Case configuration on page 276.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTP Evasion Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Loops	Number of times to send the attacks. 0 means as many as possible.
Delay	The period that FortiTester will wait until it sends the next attack.
Replay Time Out	This timeout specifies how long the client waits for a response from the server. If the client does not receive a response within the timeout, it considers the packet lost. The default value is 2 milliseconds.
Break Once Packet Lost	Select Yes or No. The Yes option means when the system identifies packet loss (the server side has not received the packet that client sent out), it stops the current GTP replay (pcap file), and continues the test with the next GTP file. The No option (the default) means a break is not set; the current replay continues.
Input Pcap	Select a pcap file to send. Note the uploaded files can be used for future cases.
Evasion Types	Select the evasion types. FortiTester will corrupt custom HTTP pcap file according to the selected Evasion Types.
Random Evasion	Enable this option so that FortiTester can randomly call one of the available HTTP evasions.
Client/Server Network	
Network MTU	The maximum transmission unit size.

AntiVirus Cases

Starting an AntiVirus test

This test sends files with HTTP/FTP/SMTP/IMAP/POP3 protocol and detect viruses in files.

To start an AntiVirus test:

1. Go to **Cases > Security Testing > AntiVirus > AntiVirus** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Click **OK** to continue.
6. Configure the test case options described in Starting an AntiVirus test on page 278.
7. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

AntiVirus Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.

Settings	Guidelines
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Loops	Number of times to send the attacks. 0 means as many as possible.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Delay	The period that FortiTester will wait until it sends the next attack.
Client Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, HTTP 1.1 will backward compatibility with HTTP 1.0.
Keep Alive	Enable to add keepalive header. Only available when HTTP 1.0 is selected in Protocol Level.
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.

Settings	Guidelines
Server Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, HTTP 1.1 will backward compatibility with HTTP 1.0.
Keep Alive	Enable to add keepalive header. Only available when HTTP 1.0 is selected in Protocol Level.
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.

Settings	Guidelines
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Action	
AntiVirus File Group	Select an existing antivirus file from the list or click **Manage Group** to upload new files.

Web Protection Cases

Starting a Web Protection test

The Web Protection test simulates sending web application attacks expected to be detected by the security DUT.

To start a Web Protection test:

1. Go to **Cases > Security Testing > Web Protection > Web Protection** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Select **Protocol** type of the simulated traffic.
6. Click **OK** to continue.
7. Configure the test case options described in Web Protection Test Case configuration on page 282.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Web Protection Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600. **Note:** You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates on page 33.
Steady Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
DNS Host Group	Select the DNS host group to look up the IP address of a domain name. To create a DNS host group, see Creating DNS host group on page 31.
DUT Monitor	Select to monitor a FortiGate device under test (DUT). If selected, you can monitor the DUT from the DUT Monitor tab on the management interface. To create a DUT monitoring, see Using DUT monitoring on page 34.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Load	
Loops	Number of times to send the attacks. 0 means as many as possible.
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but no data is responded back from the server within a certain time (in

Settings	Guidelines
	seconds). The timeout usually indicates an overwhelmed server or reverse proxy, or an outage of the back-end transactions processing servers. FortiTester will reset the connection upon timeout.
Delay	The period that FortiTester will wait until it sends the next web application attack.
Client Profile	
Client Close Mode	Select the connection close method: **3Way_Fin** or **Reset**.
Piggyback Get Requests	If enabled, this means an acknowledgement is sent on the data frame, not in an individual frame.
Source Port Range	Specify a client port range. The valid range is 10,000 to 65,535, which is also the default.
IP Change Algorithm/Port Change Algorithm	Select a change algorithm: **Increment** or **Random**. This setting determines how the system changes source/destination IP addresses and ports to simulate multiple client requests. The Increment option uses the next IP address or port in the range, for example: 10.11.12.1 -> 10.11.12.2; port 10000 -> 10001. The Random option selects an IP address or port in the range randomly.
Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Client/Server TCP Options	
TCP Receive Window	The receive window in which you want the TCP stack to send TCP segments. The receive window informs the peer how many bytes of data the stack is currently able to receive. The supplied value is used in all segments sent by the stack. The valid range is 0 to 65535.
Delayed Acks	Select to cause the TCP stack to implement the Delayed ACK strategy, which attempts to minimize the transmission of zero-payload ACK packets. Acknowledgments will be deferred and should be piggybacked on top of valid data packets. If successfully deferred, these acknowledgments are free, in the sense that they consume no additional bandwidth.
Delayed Ack Timeout	If you select Delayed ACKs, use this timeout value to specify the maximum time the TCP stack waits to defer ACK transmission. If this timer expires, the stack transmits a zero-payload acknowledgment.
Timestamps Option	Select to add a TCP time stamp to each TCP segment.
Enable Push Flag	Select to set the TCP PSH (push) flag in all TCP packets. This flag causes buffered data to be pushed to the receiving application. If deselected, the PSH flag is not set in any TCP packet.
SACK Option	Select to enable TCP Selective Acknowledgment Options(SACK).

Settings	Guidelines
Enable TCP Keepalive	Select to enable TCP Keep-alive Timer.
Keepalive Timeout	If you enable TCP Keepalive, use this timeout value to specify the maximum time to send your peer a keep-alive probe packet
Keepalive Probes	If you enable TCP Keepalive, use this value to specify the maximum probes to detect the broken connection.
Override Internal Timeout Calculation	Select to override the TCP stack calculation of the retransmission timeout value.
Retransmission Timeout	If you select **Override Internal Timeout Calculation**, use this value for the first transmission of a particular data or control packet; it is doubled for each subsequent retransmission.
Retries	The number of times a timed-out packet is retransmitted before aborting further retransmission. If the client does not receive a response after the configured number of retries have been attempted, the error is logged in the results. CSV file as a TCP timeout when a SYN or FIN is sent, and no SYN/ACK or FIN/ACK from the server is received.
Client/Server Network	
Network MTU	The maximum transmission unit size.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
IP Option DSCP	Provide quality of service (QoS).
Action	
Web Protection Group	Select the web protection group created in **Objects > Web Protection Group**. For how to create web protection group, see Managing the web protection group on page 290

Starting a web crawler test

The web crawler test runs a web crawler simulation to query URLs through the DUT. This is done to test the DUT's web access security policies. FortiTester only stores the URL responses.

To start a web crawler test:

1. Go to **Cases > Security Testing > Web Protection > Web Crawler** to display the test case summary page.
2. Click **Add** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
4. Select a **Certificate Group** if applicable.
5. Select **Protocol** type of the simulated traffic.
6. Click **OK** to continue.
7. Configure the test case options described in HTTP Web Crawler Test Case configuration on page 285.
8. Click **Start** to run the test case.

FortiTester saves the configuration automatically so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

HTTP Web Crawler Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Network Settings	
Client Ports	The graphic depicts the test ports for client-side connections. The client ports simulate the behavior of clients. You must select at least one client port . After you select a port for client, a ✓ (check mark) is displayed on the port icon, and a tab for the port is added below the graphic. Use the tabs to toggle the Capture Packets and Subnet settings controls for each port.
Capture Packet	
Capture Packet	Optional. Set packet capture options if you want to capture the traffic of this port.

Settings	Guidelines
	You can capture all packets or specify a number. You can set packet capture filters for host IP/port and protocol. **Note**: The system allocates temporary disk space for packet captures. The limit is 6,000,000 packets. The packets are saved to a temporary file that you can download from the running test case page. The filename indicates whether it is client or server communication and the interface port number. For example, client_port1.pcap. When a subsequent test case with packet capture enabled uses the same interface port as a previous one, the previous file is overwritten.
Subnet	
Subnet IP Address or Range	Specify a single IP address with standard format (for example, 10.1.2.1) or an address range like 10.1.2.1-10.1.2.99.
Netmask	Specify a netmask between 1 and 31.
Gateway	NAT mode only. Specify the gateway IP address.
Client (Profile)	
URL Group	Select the URL group. Click on Manager Group to add or delete URLs.

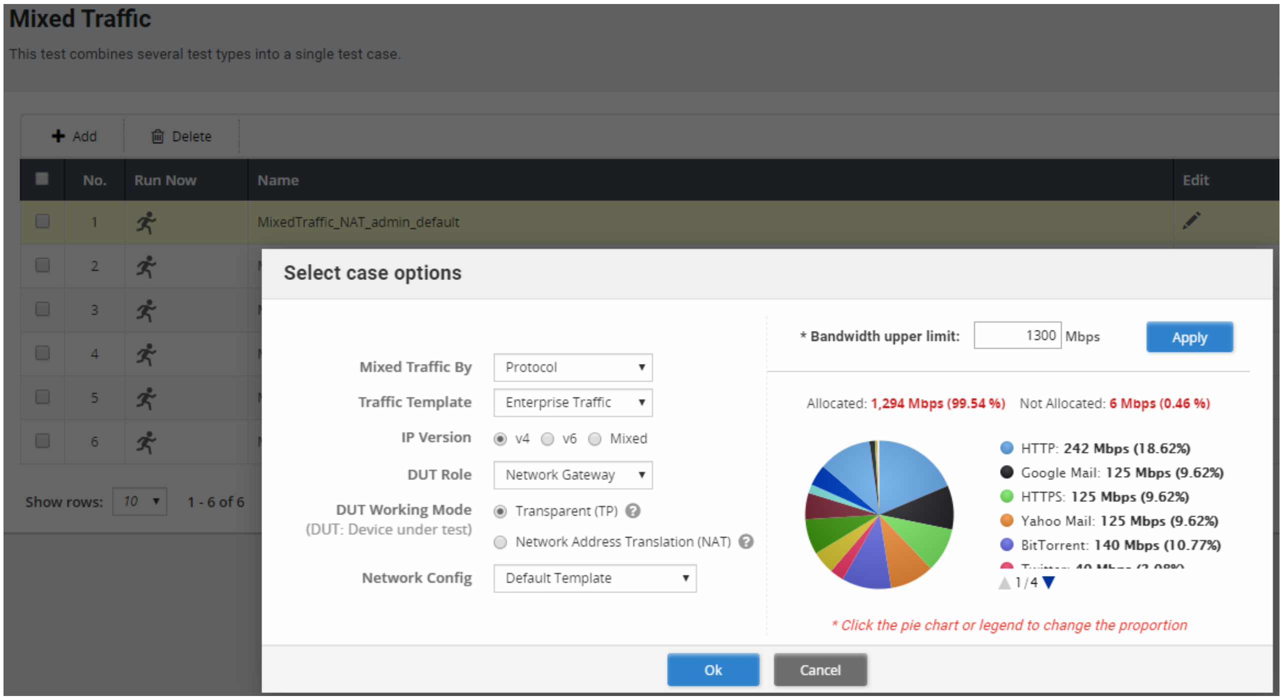
Mixed Traffic Cases

Starting a mixed traffic test

FortiTester tests mixed traffic performance by simulating multiple clients that burst all types of traffic simultaneously.

To start a Mixed Traffic test:

1. Go to **Cases > Performance Testing > Mixed Traffic** to display the test case summary page.
2. Click **Add** to display the Case Options dialog box.
3. In the popup dialog, select the kind of mixed traffic test you wish to create. You can create a test based on Protocol, Action, Case Type, or Existing Test Cases.
4. Select the traffic template when you create a test by protocol. When the template is Enterprise Traffic, Bandwidth Traffic, or Default, you can click any part of the pie chart to set the proportions.



Mixed Traffic

This test combines several test types into a single test case.

☐	No.	Run Now	Name	Edit
☐	1		MixedTraffic_NAT_admin_default	
☐	2			
☐	3			
☐	4			
☐	5			
☐	6			

Show rows: 10 1 - 6 of 6

Select case options

Mixed Traffic By: Protocol

Traffic Template: Enterprise Traffic

IP Version: ● v4 ○ v6 ○ Mixed

DUT Role: Network Gateway

DUT Working Mode (DUT: Device under test): ● Transparent (TP) ○ Network Address Translation (NAT)

Network Config: Default Template

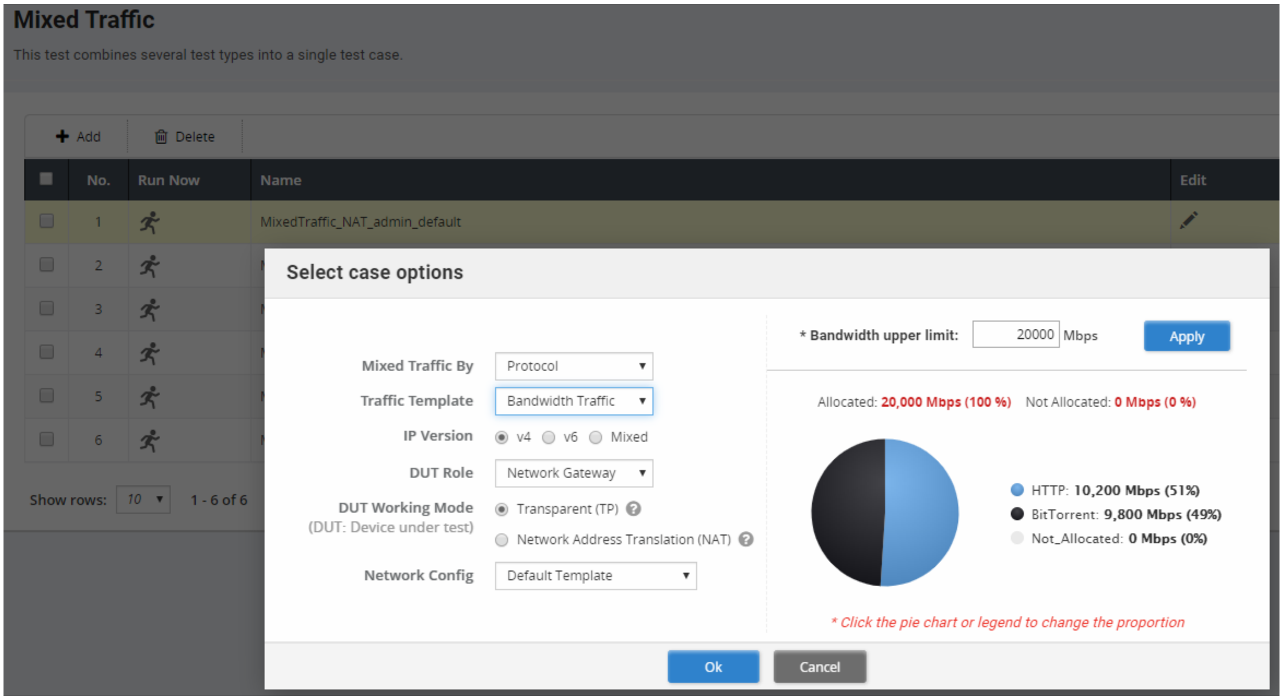
* Bandwidth upper limit: 1300 Mbps

Allocated: 1,294 Mbps (99.54 %) Not Allocated: 6 Mbps (0.46 %)

- HTTP: 242 Mbps (18.62%)
- Google Mail: 125 Mbps (9.62%)
- HTTPS: 125 Mbps (9.62%)
- Yahoo Mail: 125 Mbps (9.62%)
- BitTorrent: 140 Mbps (10.77%)
- Twitter: 40 Mbps (3.08%)

* Click the pie chart or legend to change the proportion

For Enterprise traffic mix, FortiTester requires VM16 or above, with minimum 32GB of RAM assigned; as more processing power is required if more protocols are initiated.



Mixed Traffic

This test combines several test types into a single test case.

☐	No.	Run Now	Name	Edit
☐	1		MixedTraffic_NAT_admin_default	
☐	2			
☐	3			
☐	4			
☐	5			
☐	6			

Show rows: 10 1 - 6 of 6

Select case options

Mixed Traffic By: Protocol

Traffic Template: Bandwidth Traffic

IP Version: ● v4 ○ v6 ○ Mixed

DUT Role: Network Gateway

DUT Working Mode (DUT: Device under test): ● Transparent (TP) ○ Network Address Translation (NAT)

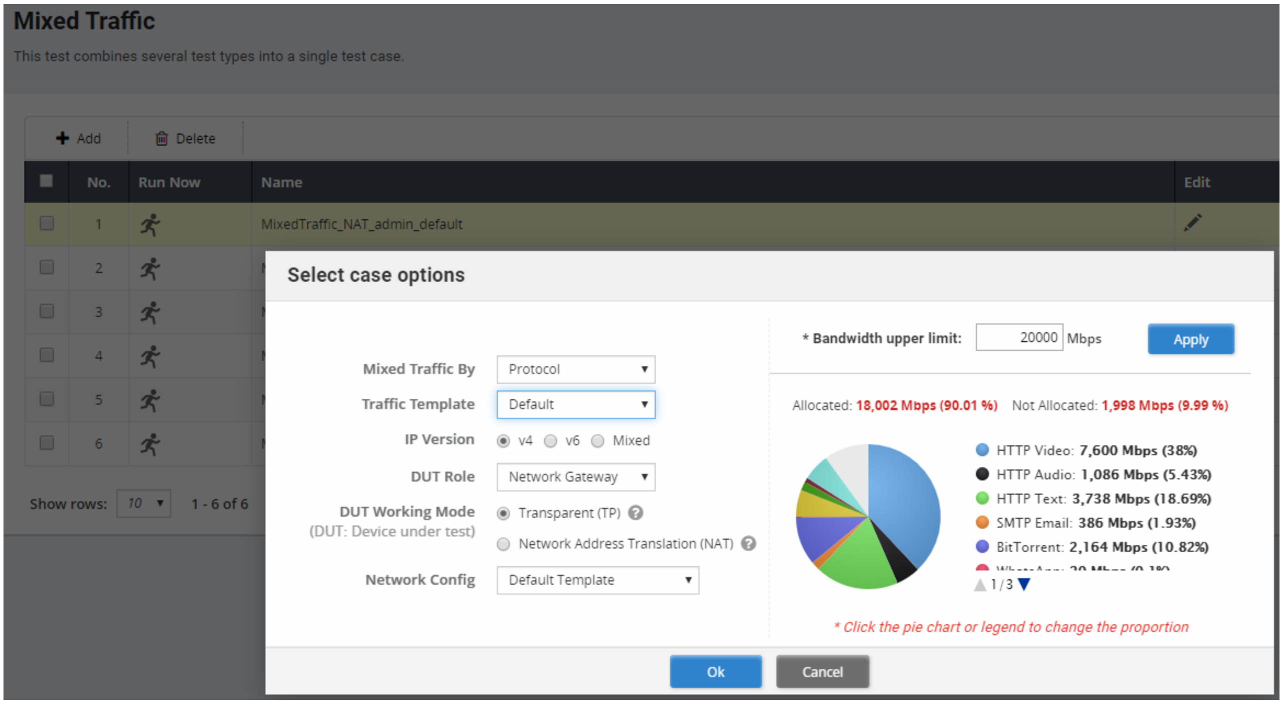
Network Config: Default Template

* Bandwidth upper limit: 20000 Mbps

Allocated: 20,000 Mbps (100 %) Not Allocated: 0 Mbps (0 %)

- HTTP: 10,200 Mbps (51%)
- BitTorrent: 9,800 Mbps (49%)
- Not_Allocated: 0 Mbps (0%)

* Click the pie chart or legend to change the proportion



Mixed Traffic

This test combines several test types into a single test case.

□	No.	Run Now	Name	Edit
□	1	🏃	MixedTraffic_NAT_admin_default	✎
□	2	🏃		
□	3	🏃		
□	4	🏃		
□	5	🏃		
□	6	🏃		

Show rows: 10 ▾ 1 - 6 of 6

Select case options

Mixed Traffic By: Protocol ▾

Traffic Template: Default ▾

IP Version: ● v4 ○ v6 ○ Mixed

DUT Role: Network Gateway ▾

DUT Working Mode (DUT: Device under test): ● Transparent (TP) ? ○ Network Address Translation (NAT) ?

Network Config: Default Template ▾

* Bandwidth upper limit: 20000 Mbps

Allocated: 18,002 Mbps (90.01 %) Not Allocated: 1,998 Mbps (9.99 %)

- HTTP Video: 7,600 Mbps (38%)
- HTTP Audio: 1,086 Mbps (5.43%)
- HTTP Text: 3,738 Mbps (18.69%)
- SMTP Email: 386 Mbps (1.93%)
- BitTorrent: 2,164 Mbps (10.82%)
- WhatsApp: 20 Mbps (0.1%)

* Click the pie chart or legend to change the proportion

5. Select the types of traffic to mix in the test.
6. For the **Network Config** option, select the network template you have created in **Cases > Security Testing > Objects > Networks**. Then the network related options will automatically be filled. See Using network configuration templates on page 24 for how to create a network template.
7. Select a **Certificate Group** if applicable.
8. Click **OK** to continue.
9. Configure the proportions of the mixed traffic.
10. Configure the test case options as described in Mixed Traffic Test Case configuration on page 288. The specific settings will depend on what types of traffic were included in the mix. Refer to the section for that specific test for more information.
11. Click **Start** to run the test case.

FortiTester saves the configuration automatically, so you can run the test again later. You can also click **Save** to save the test case without running it.

Tip: You can also copy an existing case, and change its settings to create a new case. In the case list, click **Clone** to clone the configuration. Only the case name is different from the original case.

Mixed Traffic Test Case configuration

Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test

Settings	Guidelines
	cases.
Ping Server Timeout	If a FortiTester connects to a DUT via a switch, the switch might cause a ping timeout, resulting in the test case failing to run. If this occurs, increase the timeout. The default is 15 seconds. The valid range is 0 to 600.**Note:**You can disable this end-to-end connectivity test by entering a setting of 0. If the DUT is unable to return packets, it is recommended you do so.
Number of Samples	Select the number of samples. The default is 20, which means the web UI will show the last 20 sample data (about 20 seconds) in the test case running page. You can select 20, 60, or 120.
Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Stopping Status in Second	The maximum time out in seconds allotted for FortiTester to close all TCP connections after the test finishes.
Network Settings If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates on page 24 for the description of network settings.	
Client/Server Network	
Network MTU	Maximum Transmission Unit for a data packet. FortiTester does not send out data packets larger than this value. Most DUTs have a limitation for packet size. The default is 1500. Not configurable.
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
Protocol Settings Configure settings for the cases you have selected When creating a case.	

Managing Objects

Managing the User Instruction group

You can use this service to manage the custom attack traffic and group. Upload pcap files that contain your customized attack traffic.

To add a user instruction group:

1. Go to **Cases > Security Testing > Objects > User Intrusion Group**.
2. Click **+ Add** to create a group where the uploaded files will be assigned.
3. Enter a name for the group. Click **Add**.

4. Find the group you have created in the table. Click the **Edit** button.
5. Click **Choose File** to upload the pcap files. Repeat this step to upload more files.

Managing the FGD Intrusion group

FortiGuard Intrusion Group allows you to create customized group from FortiGuard intrusion services. It can be referenced by Attack Replay Profile.

To add a FGD Intrusion group:

1. Go to **Cases > Security Testing > Objects > FGD Intrusion Group**.
2. Click **+ Add** to create a group to include the desired FDG instrusions. See Updating FortiGuard on page 301 on how to update the services.
3. Enter a name for the group. Click **Add**.
4. Find the group you have crated in the table. Click the **Edit** button
5. Click **Add**.
6. Select the FGD intrusions you want to include in this group.
7. Click **Save**.
8. Click **Close**.

Managing the AntiVirus file group

Manage the AntiVirus file and group. You can reference them in the AntiVirus cases.

To add an antivirus file group:

1. Go to **Cases > Security Testing > Objects > AntiVirus File Group**.
2. Click **+ Add** to create a group where the uploaded files will be assigned.
3. Enter a name for the group. Click **Add**.
4. Click **Choose File** to upload the AntiVirus files. Repeat this step to upload more files.

Managing the web protection group

Manage web protection group being referenced in the Web Protection cases.

To add an Web Protection group:

1. Go to **Cases > Security Testing > Objects > Web Protection Group**.
2. Click **+ Add** to create a group where the uploaded files will be assigned.
3. Enter a name for the group. Click **Add**.
4. Click **Add**.
5. Select the web protection signatures you want to include in this group.
6. Click **Save**.
7. Click **Close**.

Maintaining FortiGuard Intrusion and Web Protections services

You can view and search the security signatures and web protection signatures in **Cases > Security Testing > Maintenance**.

It's important to keep the service packages updated so that you can use the latest signatures in the security cases. Click **Update** in **Cases > Security Testing > Maintenance > FGD Intrusion Service** or **Cases > Security Testing > Maintenance > Web Protection Service** to update the corresponding services. See Updating FortiGuard for more information.

Please note that the Web Protection signature file is only available if you have purchased the Premium package.

MITRE ATT&CK®

You can use ATT&CK to simulate the post compromise behavior of a cyber adversary on an enterprise network.

FortiTester simulates the actions that a real adversary would do on the clients' systems. It features a Remote Access Tool (RAT) that performs adversary actions on infected hosts and copies itself over the whole network to increase its foothold. In order to emulate the adversary as realistic as possible, FortiTester uses Windows domain elements including users, shares and credentials, which are most commonly seen on the clients' system. It provides a library of executable techniques curated from ATT&CK, including favorites such as running Mimikatz to dump credentials and remote execution with WMI.

As a fully automated tool, defenders can use this feature to verify whether their defenses are working appropriately and as a resource to test defensive tools and analytics.

System Requirments

To use the ATT&CK feature, it requires to install the following operation system on the client devices.

- Windows 7, 8, 8.1 or 10, 64 bit

Installing FortiAgent

FortiAgent is a Windows service that facilitates communication between the FortiTester and the RATs. The FortiAgent program should be installed on every target host that is taking part in the adversary emulation operation. Once installed, they will communicate with FortiTester and interact with the RATs to participate in the adversary operation.

It requires admin permission of the Windows system to install FortiAgent.

To install FortiAgent on target hosts:

1. Install Visual C++ Redistributable for Visual Studio 2015.
   Visual C++ Redistributable may fail to install if Windows is not fully updated. If you encounter problems, try fully updating Windows.
2. Download the latest release of FortiAgent from FortiTester.
   a. Go to **ATT&CK > ATT&CK Cases > Resources**.
   b. In the **Available Clients** table, click the Download icon to download **FortiAgent** and **confg.yml**.
3. Place **fortiagent.exe** and **confg.yml** in the desired installation location. The recommended location is c:\Program Files\FortiAgent\fortiagent.exe.
4. In an Administrator command prompt, run the following command to install FortiAgent:
   ```
   fortiagent.exe --startup auto install
   ```
5. Run the following command to start FortiAgent:
   ```
   fortiagent.exe start
   ```
6. After FortiAgent is successfully started on the target hosts, it is listed on Agent Monitor page on FortiTester

(**ATT&CK > ATT&CK Cases > Monitor**).

7. Repeat step 3 to 5 to install FortiAgent on every target host.

Running an ATT&CK case

Adding domains

You need to first set up domains on the client devices, then add these domains on FortiTester.

1. Go to **Cases > ATT&CK Testing**.
2. Click **ATT&CK Cases > Domains**.
3. Click **Add**.
4. Enter the name for the domain. It should be exactly the same with the domains you have set up on the client devices.
   You can go to **Monitor > Agent Monitor**, and check the **Domain** column for the name of the domain.
5. Repeat step 3 and 4 to add more domains.

Adding a host group

A host group containing a collection of hosts. You can later reference this group in the ATT&CK case settings so that FortiTester will perform adversary actions on the hosts in this group.

1. Go to **Cases > ATT&CK Testing**.
2. Click **ATT&CK Cases > Hosts**.
3. Click **Add**.
4. Enter a name for the host group.
5. Select domain. The hosts to be added in this group should all belong to this domain. If you select **Any**, the hosts in this group can be in any domain.
6. Click **OK**.
7. Click **Add**.
8. Select a host.
9. Click **OK**.
10. Repeat step 7 to 9 to add more hosts.

To save a local copy of the configuration, you can click the **Export** icon to export the configuration of the host group. In case the host group is accidentally deleted, you can click **Import** to quickly recover the configuration.

Creating an ability group

An ability group contains a collection of operations that can be used by an adversary.

1. **Cases > ATT&CK Testing**.
2. Select **ATT&CK Cases > Abilities**.
3. Click **Add**.

4. Enter a name for the ability group.
5. Click **OK**.
6. Click **Add**.
7. On the **Add abilities** page, select the abilities you want to add. You can use the **Platform**, **ATT&CK Tactic**, and **ATT&CK Technique** options to filter out the desired abilities.
8. Click **Save**.

On **ATT&CK > ATT&CK Matrix Coverage**, the supported abilities on you FortiTester appliance are displayed in green background. You can upgrade your FortiGuard service through **System > FortiGuard** to support a higher version of ATT&CK, so that more abilities will be included.

Creating an adversary

The adversary represents a real adversary’s tactics and techniques. You can later reference the adversary in ATT&CK Cases.

1. Go to **Cases > ATT&CK Testing**.
2. Click **ATT&CK Cases > Adversaries**.
3. Click **Add**.
4. Enter a name for the Adversary.
5. Select the **Ability Group** to be used by this adversary. By referencing the ability group in adversary, you can flexibly switch the ability group when the case is running.
6. If exfiltrate_files is included in the ability group, you need to select the **Exfil Method** that will be used to exfiltrates target files on the target hosts.
7. Click **Save**.

Creating an ATT&CK Case

1. Go to **Cases > ATT&CK Testing**.
2. Select **ATT&CK Cases > ATT&CK Cases**.
3. Click **Add**.

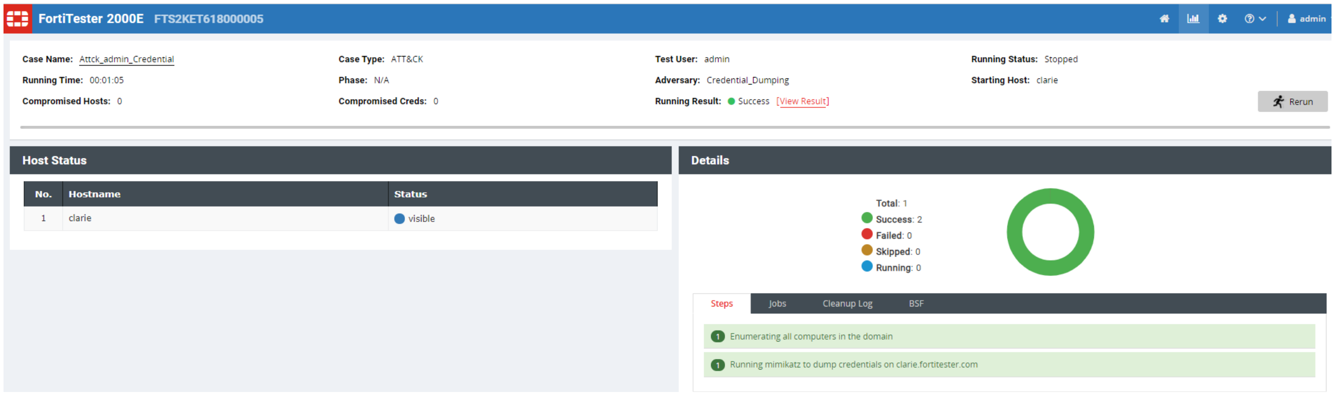
4. Configure the following settings.

Name	Enter a name for this case.
Adversary	Select the adversary which will perform a collection of operations on the target hosts.
Hosts	Select the host group which includes a collection of target hosts.
Starting Host	Select on which host the adversary actions begins.
Start Method	• Existing RAT: The adversary uses the existing Remote Access Tool (RAT) to start malicious actions. • Wait For New RAT: The actions do not start until a new RAT is installed on target hosts. • Bootstrap RAT: The RAT will be automatically installed on target hosts when you start the case, thus the adversary actions will also start. To manually download RAT, go to **ATT&CK Cases > Maintenance > Resources > RATs table**.
Start Path	The location of the RAT's executable file that is stored or to be stored on the client devices.
Starting User	• System: Start RAT by system user. • Active user: Start RAT by the active user. • Logon User: Start RAT by the specified user. You need to provide the user name and password.
Parent Process	Run the RAT process as a child process of the specified parent process, in order to disguise itself.
Starting User Name	If you select **Logon User** in **Starting User**, enter the name of this user.
Starting User Password	If you select **Logon User** in **Starting User**, enter the password of this user account.
Auto Cleanup	Enable to automatically perform cleanup when the case is finished.
Command Delay	The time interval that the adversary will wait to perform the next action (ability).
Command Jitter	The jitter that will compromise the Command Delay considering the network latency. For example, if the **Command Delay** is 3 seconds, and the **Command Jitter** is 1 second, then the actual Command Delay will be between 2 to 4 seconds.
Current Limit on Failed Actions	If an adversary action fails for the specified times, FortiTester will perform the next action.
Job Timeout	If FortiTester doesn't get response from FortiAgent for the specified time, the adversary action is considered failed.
Enable Windows Defender	Configure to enable or disable windows defender software in ATT&CK hosts.
Enable Windows Firewall	Configure to enable or disable windows firewall software in ATT&CK hosts.

5. Click **Save** to save the configuration, or click **Start** to start the case immediately.

Viewing ATT&CK cases

When the case is running, you can view its status on the **Running** page.



FortiTester 2000E FTS2KET618000005

Case Name: Attck_admin_Credential
Case Type: ATT&CK
Test User: admin
Running Status: Stopped
Running Time: 00:01:05
Phase: N/A
Adversary: Credential_Dumping
Starting Host: clarie
Compromised Hosts: 0
Compromised Creds: 0
Running Result: ● Success [View Result]

Host Status

No.	Hostname	Status
1	clarie	● visible

Details

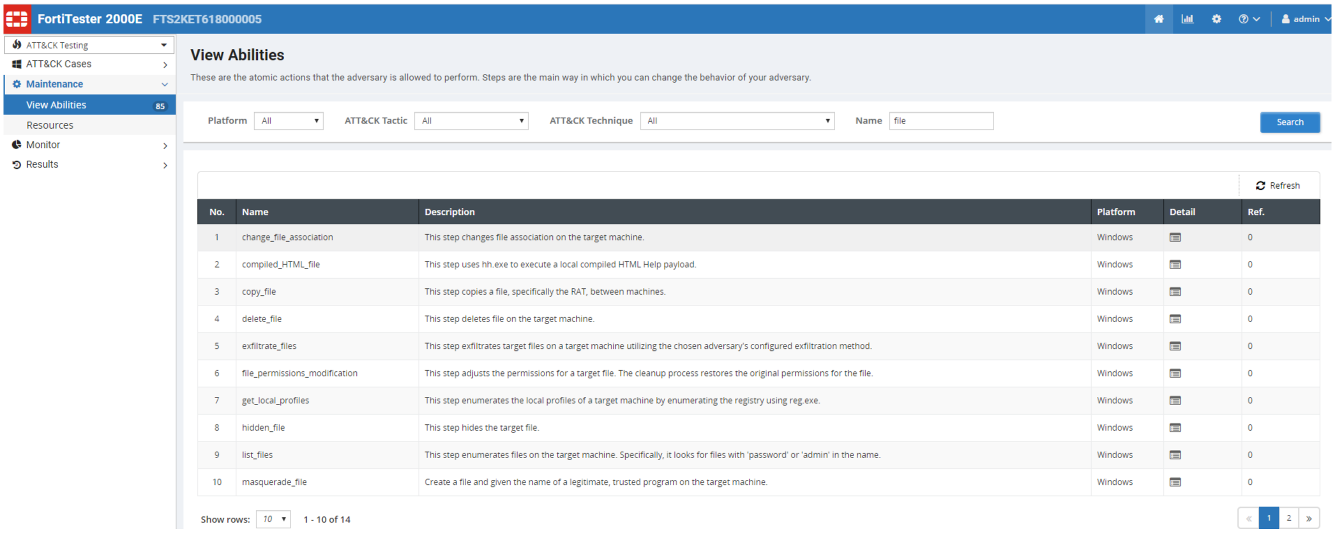
Total: 1
Success: 2
Failed: 0
Skipped: 0
Running: 0

1 Enumerating all computers in the domain
1 Running mimikatz to dump credentials on clarie.fortitester.com

Viewing Abilities

The Viewing Abilities page shows the atomic actions that the adversary is allowed to perform. Steps are the main way in which you can change the behavior of your adversary.

Go to **ATT&CK Testing > Maintenance > View Abilities**, you can use the **Name** filter to search for abilities.



FortiTester 2000E FTS2KET618000005

View Abilities

These are the atomic actions that the adversary is allowed to perform. Steps are the main way in which you can change the behavior of your adversary.

Platform: All
ATT&CK Tactic: All
ATT&CK Technique: All
Name: file

No.	Name	Description	Platform	Detail	Ref.
1	change_file_association	This step changes file association on the target machine.	Windows	▤	0
2	compiled_HTML_file	This step uses hh.exe to execute a local compiled HTML Help payload.	Windows	▤	0
3	copy_file	This step copies a file, specifically the RAT, between machines.	Windows	▤	0
4	delete_file	This step deletes file on the target machine.	Windows	▤	0
5	exfiltrate_files	This step exfiltrates target files on a target machine utilizing the chosen adversary's configured exfiltration method.	Windows	▤	0
6	file_permissions_modification	This step adjusts the permissions for a target file. The cleanup process restores the original permissions for the file.	Windows	▤	0
7	get_local_profiles	This step enumerates the local profiles of a target machine by enumerating the registry using reg.exe.	Windows	▤	0
8	hidden_file	This step hides the target file.	Windows	▤	0
9	list_files	This step enumerates files on the target machine. Specifically, it looks for files with 'password' or 'admin' in the name.	Windows	▤	0
10	masquerade_file	Create a file and given the name of a legitimate, trusted program on the target machine.	Windows	▤	0

Show rows: 10
1 - 10 of 14

Double click any ability, you can see ability details such as the summary, preconditions, and post-conditions, etc.

Also, on **Ability Detail** page, click **Related Abilities** beside the ability name, a window is opened showing the step dependency if any.

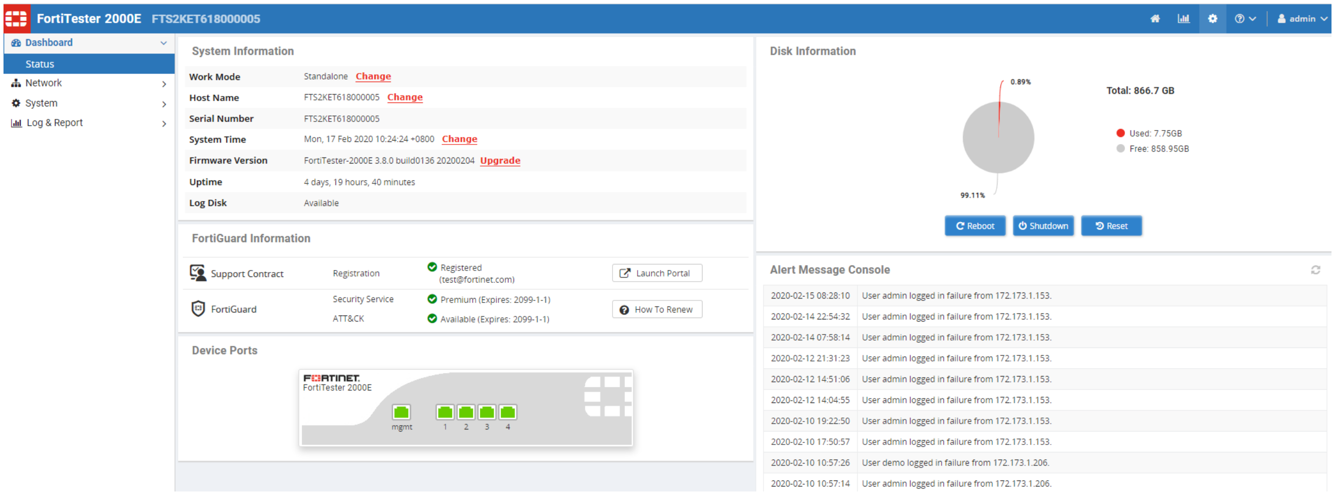
Administering the system

Go to **System** pane to view system related information, and manage system settings.

Viewing system status

Click **System > Dashboard > Status**, you can see information of the system, disk, FortiGuard, system resources, device ports, and alert message console.

System Information Overview



System Information

Work Mode	Standalone Change
Host Name	FTS2KET618000005 Change
Serial Number	FTS2KET618000005
System Time	Mon, 17 Feb 2020 10:24:24 +0800 Change
Firmware Version	FortiTester-2000E 3.8.0 build0136 20200204 Upgrade
Uptime	4 days, 19 hours, 40 minutes
Log Disk	Available

Disk Information

Total: 866.7 GB

● Used: 7.75GB
● Free: 858.95GB

FortiGuard Information

Support Contract	Registration	✓ Registered (test@fortinet.com)	Launch Portal
FortiGuard	Security Service ATT&CK	✓ Premium (Expires: 2099-1-1) ✓ Available (Expires: 2099-1-1)	How To Renew

Device Ports

Alert Message Console

```
2020-02-15 08:28:10  User admin logged in failure from 172.173.1.153.
2020-02-14 22:54:32  User admin logged in failure from 172.173.1.153.
2020-02-14 07:58:14  User admin logged in failure from 172.173.1.153.
2020-02-12 21:31:23  User admin logged in failure from 172.173.1.153.
2020-02-12 14:51:06  User admin logged in failure from 172.173.1.153.
2020-02-12 14:04:55  User admin logged in failure from 172.173.1.153.
2020-02-10 19:22:50  User admin logged in failure from 172.173.1.153.
2020-02-10 17:50:57  User admin logged in failure from 172.173.1.153.
2020-02-10 10:57:26  User demo logged in failure from 172.173.1.206.
2020-02-10 10:57:14  User admin logged in failure from 172.173.1.206.
```

Configuring a RADIUS server

Remote Authentication and Dial-in User Service (RADIUS) servers provide authentication, authorization, and accounting functions.

FortiTester can use RADIUS queries to authenticate access to the web GUI by administrators and end users.

To authenticate a user or administrator, the FortiTester appliance sends the user’s credentials to RADIUS for authentication. If the RADIUS server replies to the query with a signal of successful authentication, the client is successfully authenticated with the FortiTester appliance. If RADIUS authentication fails or the query returns a negative result, the appliance refuses the connection.

To configure a RADIUS server

1. Go to **System > RADIUS Servers**.
2. Click **+Add** to display the configuration page.

3. Configure these settings:

Name	Enter a name for the RADIUS server that can be referenced in other parts of the configuration.
Server IP/Domain	Enter the IP address or domain of the RADIUS server.
Server Port	Enter the port number where the RADIUS server listens to. The default port number is 1812.
Server Secret	Enter the RADIUS server secret key for the RADIUS server. The server secret key should be a maximum of 16 characters in length.
Authentication Scheme	Select either: • *Default* to authenticate with the default method. The default authentication scheme uses PAP, MS-CHAP, and CHAP, in that order. • CHAP, MS-CHAP, or PAP, depending on what your RADIUS server requires.
NAS IP	Enter the NAS IP address and Called Station ID (for more information about RADIUS Attribute 31, see RFC 2548 (http://www.ietf.org/rfc/rfc2548.txt) Microsoft Vendor-specific RADIUS Attributes). If you do not enter an IP address, the IP address that the FortiTester appliance uses to communicate with the RADIUS server will be applied.

4. Click **OK**.
   You can also click **Test RADIUS** to verify whether FortiTester can connect to the server, and the query is correctly configured.

To add a user with RADIUS authentication

1. Go to **System > Administrators**.
2. Click +Add to display the configuration page.
3. Configure these settings:

Name	Enter a name for the administrator user.
Role	Select the admin or tester role.
Type	• Match a user on a remote server For this option, the user name must be the same as the account name of the selected RADIUS. • Match all users in a remote server For this option, the user name is an alias name, and users can be authenticated by any account of the selected RADIUS.
RADIUS Server	Select the RADIUS Server created in **System > RADIUS Servers**.

4. Click **Save**.

Updating firmware

Go to **System > Dashboard > Status** to update the firmware image.

Before you begin:

- Download the firmware file from the Fortinet support website.
- Read the **FortiTester Release Notes** for the version you plan to install.
- You must be logged in as the user **admin** to upgrade the firmware.

To upgrade the firmware:

1. Click **Upgrade** at the end of **Firmware Version**.
2. Click **Choose File** from the **Upgrade Image** dialogue box, click **Close**.

The system replaces the firmware on the active partition and reboots.

Shutting down the system

Always properly shut down the FortiTester appliance operating system before turning off the power switch or unplugging the appliance. This causes it to finish writing buffered data, and to slow and park the hard disks.

Do not unplug or switch off the FortiTester appliance before halting the operating system. Failure to shut down correctly could cause data loss and hardware problems.

To power off the appliance via the web UI:

1. Go to **System > Dashboard > Status**.
2. Click **Shutdown**.
   The appliance becomes quieter when it stops its hardware and operating system, indicating that it is ready for power to be disconnected.
3. Disconnect the power cable from the power supply.

To power off the appliance via the CLI:

1. Connect to the CLI using a terminal emulator.
2. Enter the following command:

   ```
   execute shutdown
   ```

   The appliance becomes quieter when it stops its hardware and operating system, indicating that it is ready for power to be disconnected.
3. Disconnect the power cable from the power supply.

Rebooting the system

Rebooting the appliance is similar to shutting down.

To reboot the system:

1. Go to **System > Dashboard > Status** page.
2. Click **Reboot**.
3. Or enter the execute reboot command via the CLI.

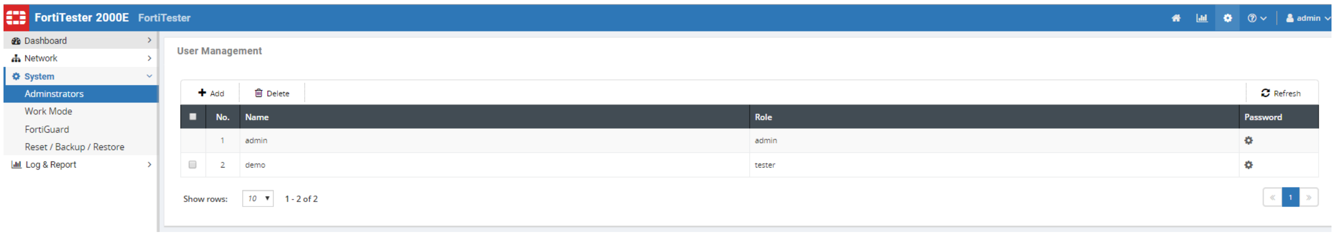
Configuring specific settings

In this section, you can configure the following:

HTTPS Server Certificate	Select the TLS certificates uploaded in **System > Certificates**.
Idle Timeout	Define the idle timeout period to expire a FortiTester GUI session.
Enable SSL Accelerator	When the FortiTester appliance works as the server side, you can enable it. This is available only for 2500E, 3000E, and 4000E appliances.
Enable Multi-Queue Support for NICs	Enable it so that the network performance can scale with the number of vCPUs and parallel packets can be processed by creating multiple TX and RX queues.
Enable Global Address Space	Disable it to limit the address space usage and you can only configure private IP.
40G fan out 4x10G	Enable to split the 40 G port into four separate 10 G ports. Use the corresponding cable to link the 10 G ports to the DUT. This is available only for 3000E platform.

Creating test users

The FortiTester system has one default administrative account named "admin". It also allows you to create other administrative or tester user accounts.



■	No.	Name	Role	Password
	1	admin	admin	⚙
□	2	demo	tester	⚙

Show rows: 10 ▾ 1 - 2 of 2

The default “admin” account is the super administrator, which can create and delete all other accounts, whereas the other administrative accounts can only create administrative/tester accounts and delete tester accounts.

The administrative user can perform a test, create and delete a tester, and set the system configuration.

A tester user can only perform tests and view test results. If a user logs in with a tester role, the User Management menu is not shown, and the contents in the System page is read-only.

To create a test user:

1. Go to **System > System > Administrators**.
2. On **User Management** page, click **Add** to display the **Create a new tester** dialogue box.
3. Select a role, admin or tester.
4. Complete the username and password settings.
5. Click **Save**.

Updating FortiGuard

One of the most important things you can do is to ensure that your FortiTester is receiving regular updates from the FortiGuard Web Security service.

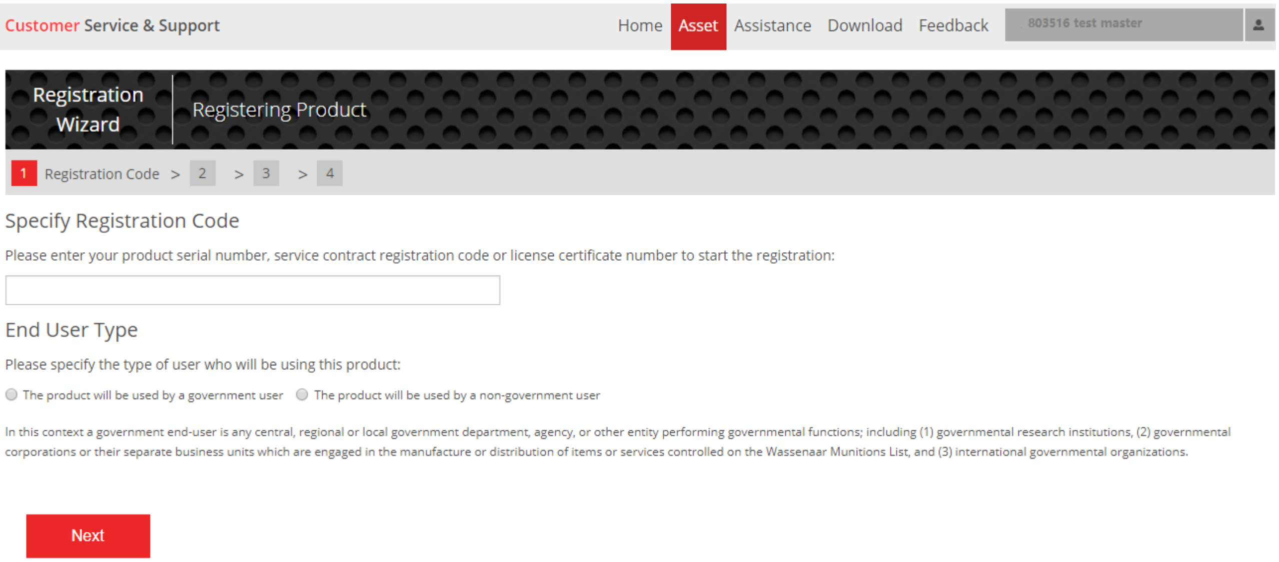
FortiTester provides three update packages.

- Basic package
  Monthly update containing the latest attack traffic files (about 300+).
- Premium package
  - Bi-monthly update containing all attack traffic files (including IoT/OT attacks, about 2400+).
  - Attack mutation engine (10 evasion techniques out of the box).
  - Web Protection signatures.
- ATT&CK abilities package

Renewing the service

Upon purchasing services from your reseller, you will receive the service registration document by email, which includes the service title and summary, such as the contractor registration code. Then follow steps below:

1. Log into FortiNet Support at *support.fortinet.com*.
2. Click **Register/Renew**.
   If you have not registered your FortiTester account, enter the serial number to register it.



Specify Registration Code

Please enter your product serial number, service contract registration code or license certificate number to start the registration:

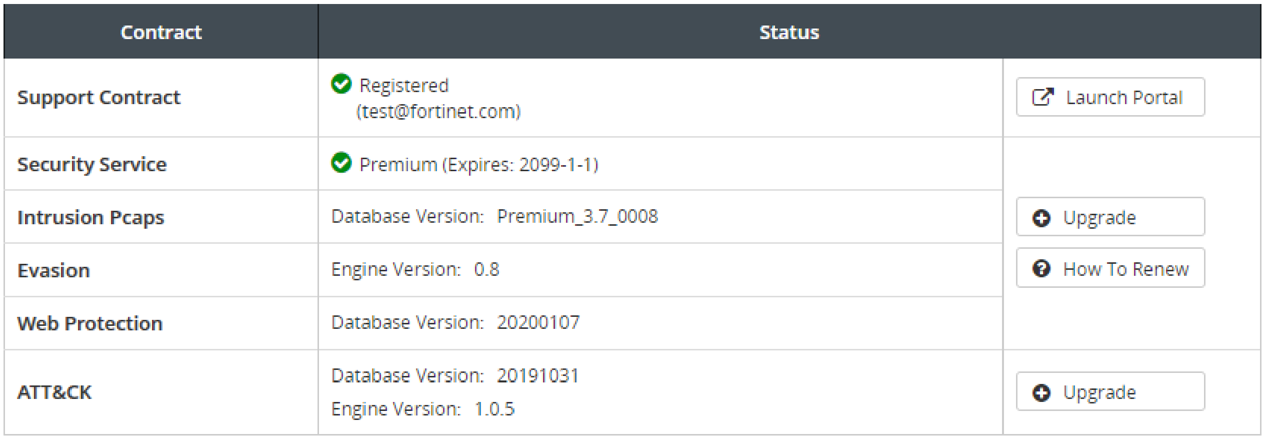
End User Type

Please specify the type of user who will be using this product:

○ The product will be used by a government user ○ The product will be used by a non-government user

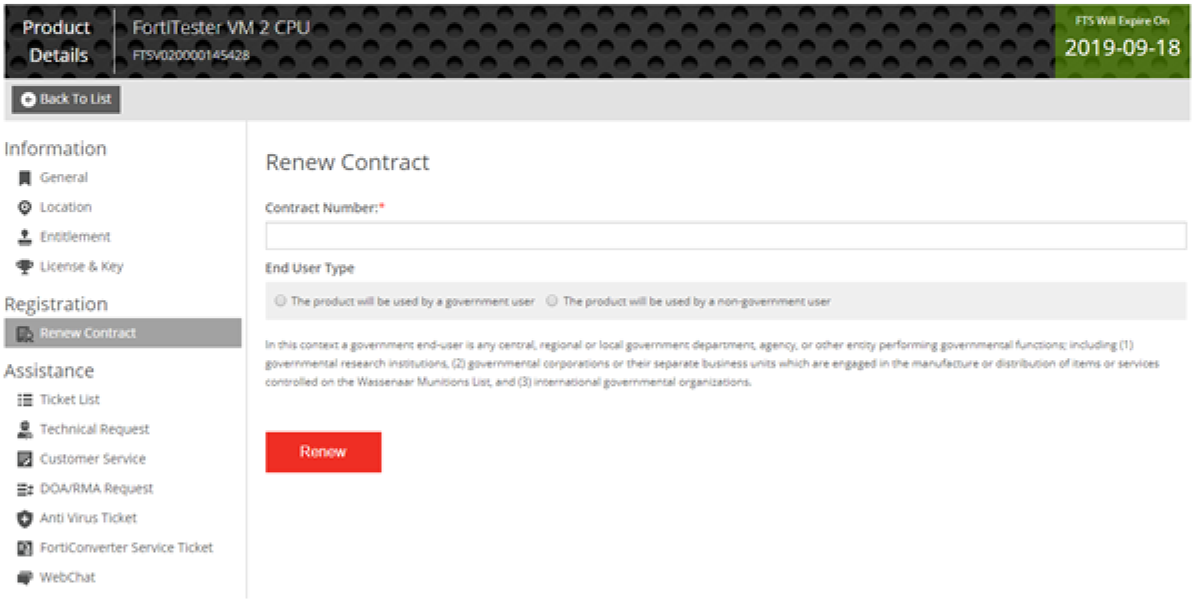
In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

If you have registered your FortiTester account, you can see the information from **System > Status > FortiGuard Information**.



Contract	Status	
Support Contract	✓ Registered (test@fortinet.com)	Launch Portal
Security Service	✓ Premium (Expires: 2099-1-1)	
Intrusion Pcaps	Database Version: Premium_3.7_0008	Upgrade
Evasion	Engine Version: 0.8	How To Renew
Web Protection	Database Version: 20200107	
ATT&CK	Database Version: 20191031 Engine Version: 1.0.5	Upgrade

3. Enter your Contract Registration Code (find the code from the Service Entitlement Summary).



Renew Contract

Contract Number:*

End User Type

○ The product will be used by a government user ○ The product will be used by a non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and (3) international governmental organizations.

Getting update package

Follow steps below to get the update package:

1. Log into FortiNet Support at *support.fortinet.com*.
2. Click **Download > FortiGuard Service Updates**.
3. Select **FortiTester** on the left menu to download the basic package.
4. Or select **Premium FortiTester** to download the premium package.
5. Or select **FortiTester ATT&CK** to download the ATT&CK package.

Upgrading the package

Follow steps below to upgrade the package:

1. Click **Update** on the following pages to update corresponding packages:
   a. **Cases > Security Testing > Maintenance > FGD Intrusion Service.**
   b. **Cases > Security Testing > Maintenance > Web Protection Service.**
   c. **Cases > ATT&CK > Maintenance > Resources.**
2. Or click **System > System > FortiGuard**.
3. Click **Upgrade** to select the package file.
4. Click **OK**.

Tip: The function is only available to users who have corresponding licenses to update.

Configuring web proxy server

If you cannot connect to the FortiGuard Distribution Network (FDN), you can configure FortiTester to connect through an explicit (non-transparent) web proxy server to the FortiGuard Distribution Network (FDN) for license validation. The FortiTester appliance will connect to the proxy using the HTTP CONNECT method, as described in RFC 2616 (http://tools.ietf.org/rfc/rfc2616.txt).

1. Go to **System > Fortiguard**.
2. Enable **Use Explicit Proxy for FortiGuard Server**.
3. Configure these settings.

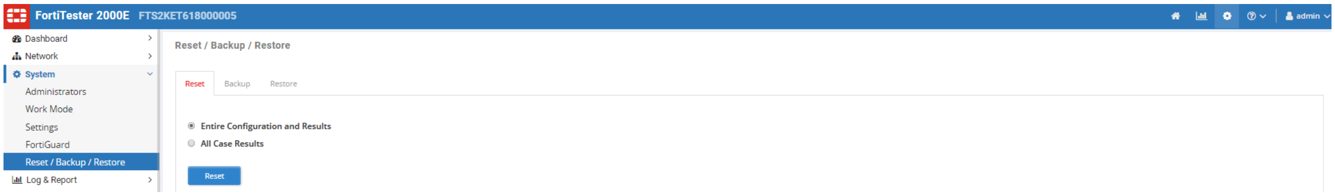
Proxy Address	Enter either the IP address or fully qualified domain name (FQDN) of the web proxy.
Proxy Port	Enter the port number on which the web proxy listens for connections.
Username	If the proxy requires authentication, enter the FortiTester appliance’s login name on the web proxy.
Password	If the proxy requires authentication, enter the password for the FortiTester appliance’s login name on the web proxy.

4.
5. Click **Apply**.

Resetting/Backuping/Restoring the system

Use the Reset/Backup/Restore tab to reset, backup, or restore the FortiTester configurations.

Go to **System > System > Reset/Backup/Restore**.



● Entire Configuration and Results
○ All Case Results

Reset

Click **Reset**, select **Entire Configuration and Results**, and click **Reset** to reset the configurations and results;

or select **All Case Results**, and click **Reset** to remove all case results.

Backup

Click **Backup**, select **All Case Configuration**, **All Case Results**, or/and **All System Configuration**, and click **Backup** to backup the case configurations (including the schedule, objects, and other configurations which are related with cases), case results, or/and system configuration.

Restore

Click **Restore > Choose File** to upload .zip file, and click **Restore**.

This operation clears all the data and cannot be canceled. Before you reset the system, you can export system configuration data so that you can import it later. The configuration data includes all the test case settings and test results, user accounts, and test HTML pages for HTTP/HTTPS test cases.

Uploading TLS certificates

FortiTester now supports uploading customized TLS certificates for HTTPS access to FortiTester's GUI.

To upload a certificate

1. Go to **System > Certificates**.
2. Click **+Add** to display the configuration page.
3. Click **Choose file** and **Key file** to select the certificate file and key file respectively from your local directory.
4. Click **Import**.
5. Enter the passphrase.
6. Click **Close**.

To apply a certificate

1. Go to **System > Settings**.
2. From **HTTPS Server Certificate**, select the uploaded TLS certificate.

3. Click **Apply**.

Note: You must reboot the appliance after changing the HTTPS server certificate.

Log & Report

Report Settings

Select whether to include the following items in the case reports.

Include None IPv4/IPv6 Packets	If enabled, the report will contain non ipv4/ipv6 packet records.
Include ICMP Packets	If enabled, the report will contain ICMP packet records.
Include ICMP6 Packets	If enabled, the report will contain ICMP6 packet records.
Include Ethernet Overhead in Bandwidth	If enabled, the Data Rate will include the Inter Frame Gap, MAC Preamble, and start frame delimiter (SFD).
Enable Testing Report	If enabled, the testing report after the case finished running will be generated.
Generate Report Immediate	If enabled, the report will generate immediately.
Generate Report Detail	If enabled, the detailed history results in PDF file will be generated.
Use Widget view as default	If enabled, the widget view will be displayed as default on the **Running** page.

Report fields

Select the fields that will be included in the case reports. By default, all the fields are selected. You can use the button beside **Layer** to include or exclude all the fields of a specific layer. Click **Apply** to apply your settings.

Log Settings

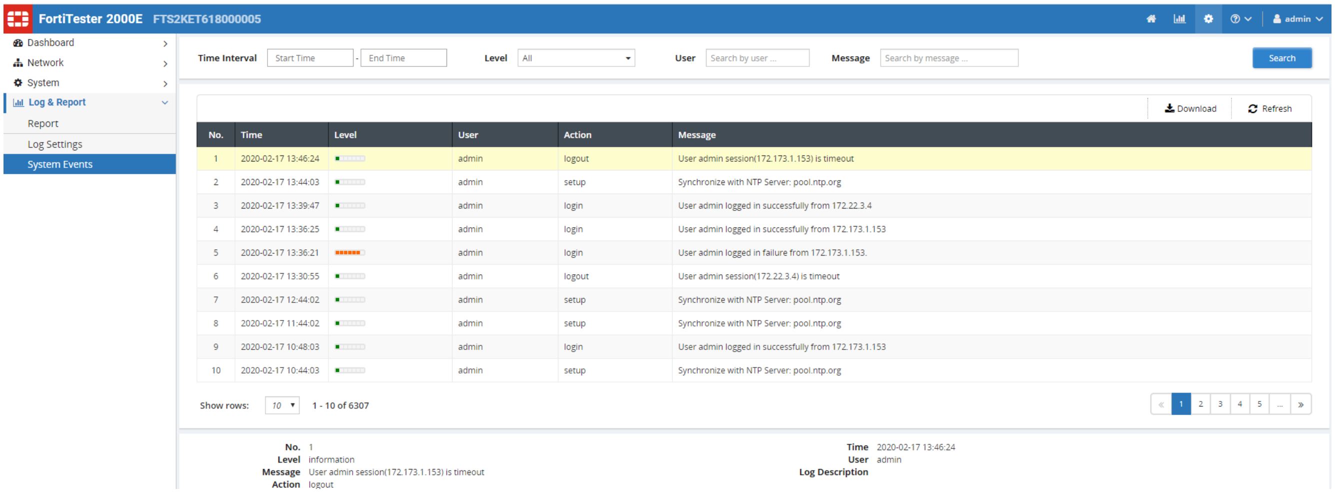
Select the events that will be reported in **System Events**.

System Activity Event	If enabled, system events such as reset/backup/restore will be reported in **System Events**.
User Activity Event	If enabled, user activities such as user login/log out will be reported in **System Events**.
Case Activity Event	If enabled, case related operations will be reported in **System Events**, for example, the case has started, or the case has finished running.
Object Activity Event	If enabled, the object-level operations will be reported in **System Events**, for example, the test is deleted.

Send logs to FortiSIEM	Enable to export the logs and view them in FortiSIEM.
IP Address	Enter the IP address of FortiSIEM.

Viewing system events

Click **System > Log & Report > System Events**, you can see the system log data. You can search the logs by different conditions and download them. System events older than 7 days will be automatically deleted at 0 o'clock every day.



Time Interval Start Time - End Time Level All User Search by user ... Message Search by message ...

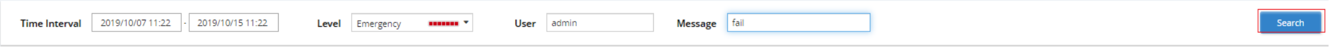
No.	Time	Level	User	Action	Message
1	2020-02-17 13:46:24	🟩	admin	logout	User admin session(172.173.1.153) is timeout
2	2020-02-17 13:44:03	🟩	admin	setup	Synchronize with NTP Server: pool.ntp.org
3	2020-02-17 13:39:47	🟩	admin	login	User admin logged in successfully from 172.22.3.4
4	2020-02-17 13:36:25	🟩	admin	login	User admin logged in successfully from 172.173.1.153
5	2020-02-17 13:36:21	🟧	admin	login	User admin logged in failure from 172.173.1.153.
6	2020-02-17 13:30:55	🟩	admin	logout	User admin session(172.22.3.4) is timeout
7	2020-02-17 12:44:02	🟩	admin	setup	Synchronize with NTP Server: pool.ntp.org
8	2020-02-17 11:44:02	🟩	admin	setup	Synchronize with NTP Server: pool.ntp.org
9	2020-02-17 10:48:03	🟩	admin	login	User admin logged in successfully from 172.173.1.153
10	2020-02-17 10:44:03	🟩	admin	setup	Synchronize with NTP Server: pool.ntp.org

Show rows: 10 1 - 10 of 6307 « 1 2 3 4 5 ... »

No. 1
Level information
Message User admin session(172.173.1.153) is timeout
Action logout
Time 2020-02-17 13:46:24
User admin
Log Description

Searching logs

Set conditions in the figure below, and click **Search** to search for the system event logs.



Time Interval 2019/10/07 11:22 - 2019/10/15 11:22 Level Emergency User admin Message fail

Downloading logs

Select one event log and click **Download** in the top right corner to download the system event log.

Test Center

You can join multiple appliances into a Test Center when throughput requirements are too high for a single FortiTester appliance to handle. In Test Center mode, some FortiTester appliances can act as clients and others act as servers, to provide more powerful capacity for performance testing.

Requirements and Restrictions

Tester Center supports at most 4 appliances or VMs:

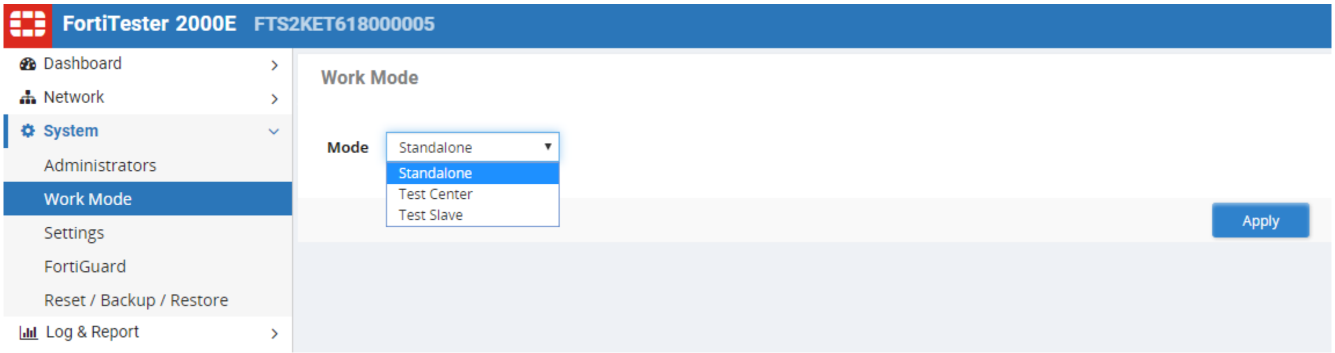
- In NAT or TP mode, you can configure at most 2 servers and 2 clients.
- In Application mode, you can configure at most 4 clients.

The appliances or VMs can be different models, but based on the following conditions:

- For all FortiTester-VMs they have to be properly licensed.
- For all FortiTester-VMs, Center/Slave must have the same vCPU number, VM type, port number.
- Software - Center/Slave must have the same major version number (e.g. 3.8.0 can run with 3.8.1 but NOT 3.7)
- For 3000E, Center/Slave must have the same fanout mode (e.g. 3000E can break out 2 x 40G into 8 x 10G)
- Center/Slave must be in the same group i.e.:
  - "2K": ["FTS_2000D", "FTS_2000E", "FTS_2500E"],
  - "3K": ["FTS_3000E"],
  - "4K": ["FTS_4000E"],
  - "VM": ["FTS_VM_KVM"],
  - "VM_ESXI": ["FTS_VM"],
  - "AWS": ["FTS_VM_AWS"],
  - "AWS_BYOL": ["FTS_VM_AWS_BYOL"],
  - "AZR_BYOL": ["FTS_VM_AZURE_BYOL"],
  - "OCI_BYOL": ["FTS_VM_OCI_BYOL"],
  - "GCP_BYOL": ["FTS_VM_GCP_BYOL"]

Configuring work mode settings

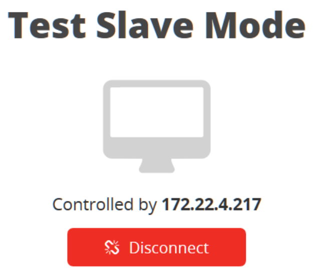
The work mode settings determine whether the FortiTester operates as a standalone appliance or is joined with other FortiTester appliances to form a Test Center.



By default, FortiTester appliances operate in Standalone work mode.

If your test plans require more interfaces than provided by a single FortiTester, you can join the appliances into what is called a Test Center. One appliance is the Test Center master appliance; the others are Test Center slaves. You manage test cases from the Test Center appliance management interface; the web UI is not available for an appliance in Test Slave work mode. When you enter the web UI address for the Test Slave appliance, it displays the following page instead.

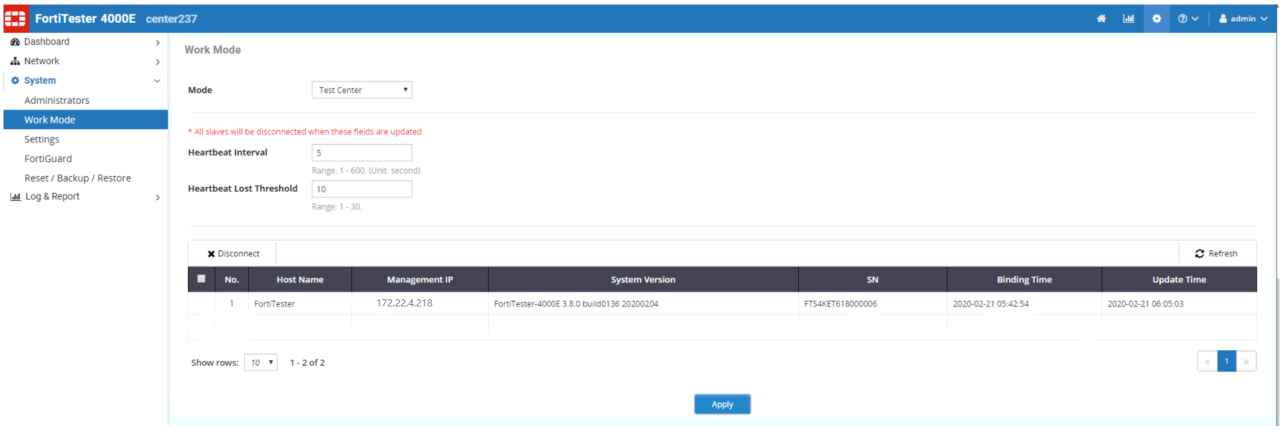
Test Slave Mode



To set up a Test Center:

1. Log into the web UI of one FortiTester (e.g. 172.22.4.217).
2. Go to **System > Work Mode**.
3. The appliance is in Standalone work mode by default.
4. Select **Test Center** to make it the Test Center master. The **Work Mode** page shows current work mode of this appliance is TestCenter, and a table lists the appliances that are under control of this one.
5. Log into another FortiTester (e.g. 172.22.4.218).
6. Go to **System > Work Mode**.
7. Select **Test Slave**.
8. Enter the IP address of the Test Center master and click **Connect**.
9. Return to the **Work Mode** page on the master and click **Refresh**. You will see 172.22.4.218 is in the table.

Test Center



Work Mode

Mode: Test Center

* All slaves will be disconnected when these fields are updated

Heartbeat Interval: 5
Range: 1 - 600. (Unit: second)

Heartbeat Lost Threshold: 10
Range: 1 - 30.

□	No.	Host Name	Management IP	System Version	SN	Binding Time	Update Time
	1	FortiTester	172.22.4.218	FortiTester-4000E 3.8.0 build0136 20200204	FTS4KET618000006	2020-02-21 05:42:54	2020-02-21 06:05:03

Show rows: 10 1 - 2 of 2

You can click the **Disconnect** button in the slave Web GUI to return to Standalone mode.

When the appliances have been added to the Test Center, you can select one or more FortiTester appliances to work as clients and others to work as servers when you create test cases. In this example, 172.22.4.217 has the client ports; 172.22.4.218 has the server ports. You can add up to four pairs of appliances to a Test Center.

10. Configure **Heartbeat Interval** and **Heartbeat Lost Threshold** to manage the heartbeat traffic between center and slaves in Test Center mode.

Using the CLI

You can configure some settings through a connection to the command-line interface (CLI).

Requires: Terminal emulator such as PuTTY, TeraTerm, or a terminal server.

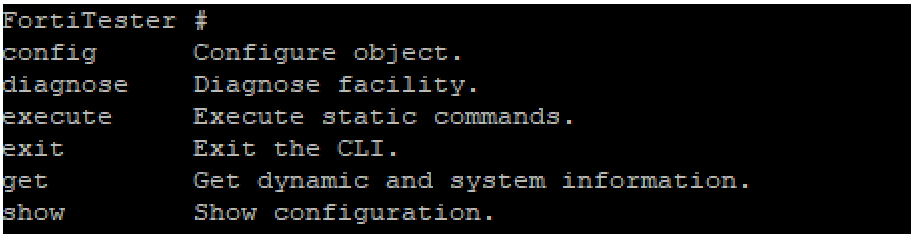
To connect to the CLI via serial console:

1. Use the console cable, connect the appliance console port to your terminal server or computer.
2. On your computer or terminal server, start the terminal emulator. Use these settings:
   - Baud rate: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
3. Press **Enter** on your keyboard to connect to the CLI.

Note: After you configure the management port, you can connect to the management port and use the CLI remotely by SSH or Telnet.

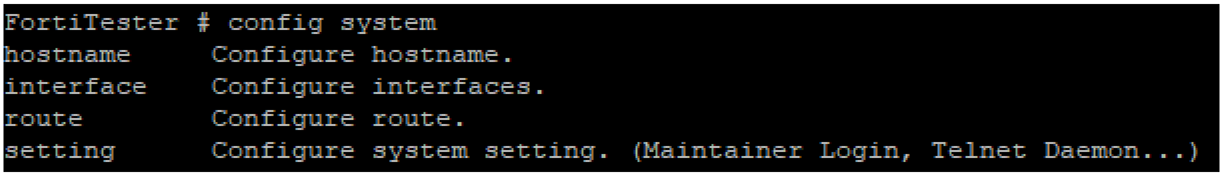
Getting CLI help

You can enter the question mark (?) at the command prompt to display a list of CLI commands and their description.



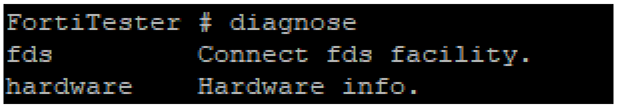
```
FortiTester #
config       Configure object.
diagnose     Diagnose facility.
execute      Execute static commands.
exit         Exit the CLI.
get          Get dynamic and system information.
show         Show configuration.
```

Enter `config system ?`, all config system related commands and their descriptions are displayed.



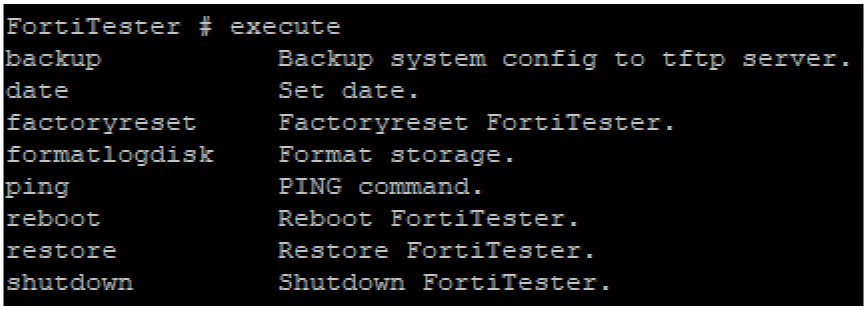
```
FortiTester # config system
hostname      Configure hostname.
interface     Configure interfaces.
route         Configure route.
setting       Configure system setting. (Maintainer Login, Telnet Daemon...)
```

Enter `diagnose ?`, all diagnose related commands and their descriptions are displayed.



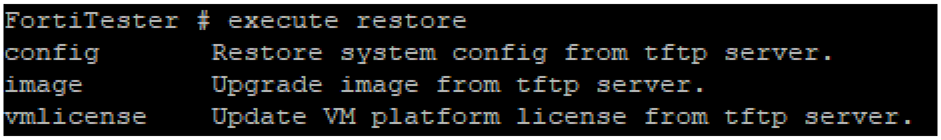
```
FortiTester # diagnose
fds          Connect fds facility.
hardware     Hardware info.
```

Enter `execute ?`, all execute related commands and their descriptions are displayed.



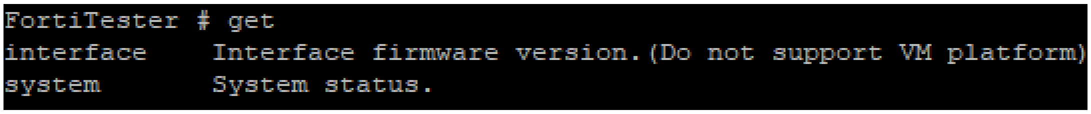
```
FortiTester # execute
backup           Backup system config to tftp server.
date             Set date.
factoryreset     Factoryreset FortiTester.
formatlogdisk    Format storage.
ping             PING command.
reboot           Reboot FortiTester.
restore          Restore FortiTester.
shutdown         Shutdown FortiTester.
```

Enter `execute restore ?`, all execute restore related commands and their descriptions are displayed.



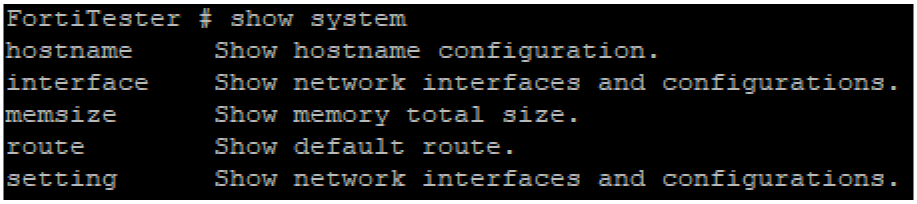
```
FortiTester # execute restore
config       Restore system config from tftp server.
image        Upgrade image from tftp server.
vmlicense    Update VM platform license from tftp server.
```

Enter `get ?`, all get related commands and their descriptions are displayed.



```
FortiTester # get
interface    Interface firmware version.(Do not support VM platform)
system       System status.
```

Enter `show system ?`, all show system related commands and their descriptions are displayed.

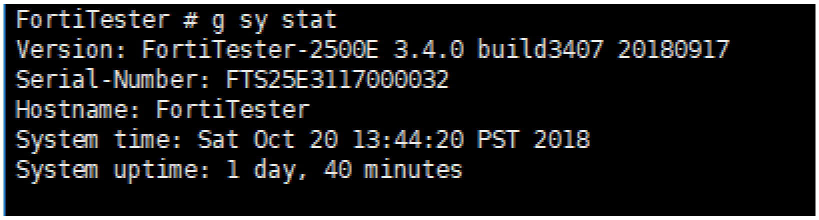


```
FortiTester # show system
hostname     Show hostname configuration.
interface    Show network interfaces and configurations.
memsize      Show memory total size.
route        Show default route.
setting      Show network interfaces and configurations.
```

Abbreviating commands

You can abbreviate words in the command line to their smallest number of non-ambiguous characters.

For example, the command `get system status` can be abbreviated to `g sy stat`.

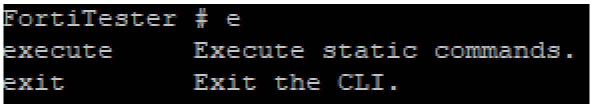


```
FortiTester # g sy stat
Version: FortiTester-2500E 3.4.0 build3407 20180917
Serial-Number: FTS25E3117000032
Hostname: FortiTester
System time: Sat Oct 20 13:44:20 PST 2018
System uptime: 1 day, 40 minutes
```

Completing commands automatically

Enter a word or part of a word, and then press ?. No space is required before ?.

For example, enter e and then ?. You can see the following information.



```
FortiTester # e
execute      Execute static commands.
exit         Exit the CLI.
```

The table below lists the shortcuts and descriptions:

?	List CLI commands and their descriptions.
Tab	Display the key command word. Press Tab multiple times to switch among different words, such as get, show, and config, etc.
Up arrow/Ctrl + P	Recall the previous command. Command memory is limited to the current session.
Down arrow/Ctrl + N	Recall the next command.
Left or Right arrow	Move the cursor within the command line.
Ctrl + A	Move the cursor to the beginning of the command line.
Ctrl + E	Move the cursor to the end of the command line.
Ctrl + B	Move the cursor after one word.
Ctrl + F	Move the cursor before one word.
Ctrl + D	Delete the current character.
Ctrl + C	Abort current interactive commands, such as when entering multiple lines. If you are not currently within an interactive command such as config or edit, this closes the CLI connection.
\ then Enter	Continue typing a command on the next line for a multi-line command. For each line that you want to continue, terminate it with a backslash (\ ). To complete the command line, terminate it by pressing the spacebar and then the Enter key, without an immediately preceding backslash.

CLI commands

The following table describes the commonly used CLI commands.

Command	Description
`?`	Show help information.
`get system`	Get system status.
`get interface`	Get interface firmware version.
`show system hostname`	Show hostname configuration.
`show system interface`	Show network interfaces and configurations.

Command	Description
show system memsize	Show total memory size.
show system route	Show the default route.
show system setting	Show network interfaces and configurations.
config system hostname	Set the host name for this appliance.
config system interface	Configure network interfaces.

config system route	Configure the gateway address for the management port.
	config system route
	    set gateway 172.173.1.248
	end

config system setting	Configure system setting.
execute date	Set the system date and system time. The format is MM/DD/YYYY hh:mm:ss.
execute ping	Execute a PING command.
execute reboot	Reboot the system.
execute shutdown	Shut down the system.
execute factoryreset	Reset the system into an initial state. Note this operation will clear all existing data/configuration.
execute formatlogdisk	Execute a format disk command for log storage.
execute restore image tftp	Upgrade image from tftp server. The format is "execute restore image tftp xxx.xxx x.x.x.x".
execute restore vmlicense tftp	Update VM platform license from tftp server. The format is "execute restore vmlicense tftp xxx.xxx x.x.x.x".
execute restore config tftp	Execute restore config tftp. The format is "execute restore config tftp xxx.xxx x.x.x.x".
execute backup config tftp	Execute backup config tftp. The format is "execute backup config tftp xxx.xxx x.x.x.x".
exit	Exit the current session.

Using the REST API

Introduction

FortiTester supports Representational state transfer application programming interface (REST API) access. These APIs can be used to retrieve, create, update and delete configuration settings, to retrieve system logs and statistics, and to perform basic administrative actions such as reboot and shut down.

A few examples of FortiTester API commands are given in this section. For the full list of available commands, see **API Browser** on the FortiTester landing page.

Enabling REST API Support

The API is enabled by default. No additional configuration is required.

Authentication

When making requests to FortiTester using the REST API, you will need:

1. A valid admin username and password (so that an authenticated session can be established)
2. Appropriate access permissions for the requested resource (controlled by admin profile)

Using curl, you may save the authentication information as a cookie to allow subsequent requests to be accepted automatically.

```
curl -k -d'{"name":"<username>","password":"<user password>"}' -c cookies.txt -H
"Content-Type: application/json" https://10.220.64.6/api/user/login
```

```
curl -k -b cookies.txt https://10.220.64.6/api/case/test2/rerun
```

Format

FortiTester REST API uses the JSON format.

Error Codes

An error code 0 means the operation was a success. Any error code that is a non-zero integer means an error occurred.

Example API commands

For the full list of available commands, see **API Browser** on the FortiTester landing page.

User login

HTTP Request: /api/user/login

Method: POST

Parameter Name	Type	Description
name	String	User name
Password	String	Password

Example:

```
{
"name":"test",
"password":"test123"
}
```

Response:

```
{
"ErrorCode":0,
"Data":{
"name": "test",
"_id": "55a5cc185b7e7bf073a98af0",
"role": "tester"
 }
}
```

- Data: Gives returned data if "ErrorCode" is 0 or an error message if "ErrorCode" is a non-zero integer.

Create user

HTTP Request: /api/user

Method: POST

Parameter Name	Type	Description
name	String	User name
Password	String	Password
cfmPsw	String	Confirmed password
role	String	Role of the user

Example:

```
{
"name":"test",
"password":"test"
"cfmPsw":"test",
"role":"tester"
}
```

Response:

```
{
"ErrorCode":0,
"Data":"55c8458e1d41c82b3b3a2604"
}
```

- Data:Gives the User ID.

Reboot system

HTTP Request: /api/system/reboot

Method:POST

Parameter Name	Type	Description
reboot	true/false	Reboot the system or not.

Response:

```
{
"ErrorCode":0
"Data":""
}
```

Setting up a VM

Introduction

This section describes how to deploy a FortiTester virtual appliance in a virtualization server environment. This includes how to configure the virtual hardware settings of the virtual appliance.

This document assumes:

- you have already successfully installed the virtualization server on the physical machine.
- you have installed appropriate VM management software on either the physical server or a computer to be used for VM management.

Supported Systems:

- VMware Workstation (Windows/Linux),
- VMware ESXi
- KVM
- OpenStack Cloud platforms
- AWS BYOL
- Azure BYOL
- OCI BYOL
- GCP BYOL

For more details about FortiTester-VM deployment, see FortiTester-VM deployment docs.

Licensing and deployment

Licensing

Fortinet offers the FortiTester VM through a licensing format. Please contact your usual Fortinet provider for more information on how to purchase a license.

License	vCPU	RAM	Storage
VM02	2	4	60GB
VM04	4	8	60GB
VM08	8	16	60GB
VM16	16	32	60GB
VM32	32	64	60GB

Note: The Enterprise mix feature under **Performance Testing > Mix Traffic** is only available on FortiTester-VMs with VM16 or VM32 license.

Deployment package

FortiTester VM deployment packages are included with firmware images on the Customer Service & Support site. The following table list the available VM deployment packages.

VM Platform	Deployment File
VMware ESXi 6.0 and 6.5	ESX/ESXi server: fts-vm-64-hw7.ovf.zip
Linux KVM	fts-vm-64-hw7.kvm.zip

To download the firmware package:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select **Download > Firmware Images**. The Firmware Images page opens.
2. Select **FortiTester** from the Select Product drop-down list, then select **Download**.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on your management computer.

Deploying the appliance

Prior to deploying the FortiTester VM, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiTester VM presume that you are familiar with the management software and terminology of your VM platform.

For assistance in deploying FortiTester VM, refer to Deployment examples on page 318. You may also need to refer to the documentation provided with your VM server.

Before you start your FortiTester VM appliance for the first time, you might need to adjust virtual disk sizes and network settings. The first time you start FortiTester VM, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiTester GUI.

Uploading the license file

1. Select the **System** tab.
2. Click **Upload**, under License Status.
3. Choose your license file, then click on the upload icon.
4. Click **Close**.

Deployment examples

The FortiTester VM can be deployed and configured using the VMware vSphere Hypervisor™ (ESX/ESXi) and VMware vSphere Client™ or the Linux KVM virtualization solution.

Creating the virtual machine

VMware vSphere

Once you have downloaded the zip file and extracted the package contents to a folder on your management computer, you can deploy the OVF package to your VMware environment.

Prior to deploying the FortiTester VM, ensure that the following are configured and functioning properly:

- VMware vSphere Hypervisor™ (ESX/ESXi) software must be installed on a server and updated to the latest patch release prior to installing FortiTester VM. Go to http://www.vmware.com/products/vspherehypervisor/index.html for installation details.
- VMware vSphere Client™ must be installed on the computer that you will be using for managing the FortiTester VM.

Deploy the OVF file

To deploy the OVF file template:

1. Launch the VMware vSphere client, enter the IP address or host name of your server, enter your user name and password, then click **Login**. The vSphere client home page opens.
2. Select **File > Deploy OVF Template** to launch the OVF Template wizard. The OVF Template Source page opens.
3. Click **Browse**, locate the OVF file on your computer (fts-vm-64-hw7.ovf), then click **Next** to continue. The OVF Template Details page opens.
4. Verify the OVF template details. This page details the product name, download size, size on disk, and description. Click **Next** to continue. The OVF Template End User License Agreement page opens.
5. Read the end user license agreement, then click **Accept** then **Next** to continue. The OVF Template Name and Location page opens.
6. Enter a name for this OVF template. The name can contain up to 80 characters and it must be unique within the inventory folder. Click **Next** to continue. The OVF Template Disk Format page opens.
7. Select one of the following:
   - Thick Provision Lazy Zeroed: Allocates the disk space statically (no other volumes can take the space), but does not write zeros to the blocks until the first write takes place to that block during runtime (which includes a full disk format).
   - Thick Provision Eager Zeroed: Allocates the disk space statically (no other volumes can take the space), and writes zeros to all the blocks.
   - Thin Provision: Allocates the disk space only when a write occurs to a block, but the total volume size is reported by the Virtual Machine File System (VMFS) to the OS. Other volumes can take the remaining space. This allows you to float space between your servers, and expand your storage when your size monitoring indicates there is a problem. Note that once a Thin Provisioned block is allocated, it remains in the volume regardless of if you have deleted data, etc.
8. Click **Next** to continue. The OVF Template Network Mapping page opens.
9. Map the networks used in this OVF template to networks in your inventory. You must set the destination network for this entry to access the device console. Click **Next** to continue. The OVF Template Ready to Complete page opens.
10. Review the template configuration. Ensure that Power on after deployment is not enabled. You might need to configure the FortiTester VM hardware settings prior to powering on the VM.

11. Click **Finish** to deploy the OVF template. You will receive a Deployment Completed Successfully dialog box once the FortiTester VM OVF template wizard has finished.

Configure hardware settings

Before powering on your FortiTester VM you must configure the virtual memory, virtual CPU, and virtual disk.

To configure the VM:

1. In the vSphere Client, right-click on the FortiTester VM in the left pane and select **Edit Settings** to open the Virtual Machine Properties window.
2. Select **Memory** from the Hardware list, then adjust the Memory Size to 8G.
3. Select **CPUs** from the Hardware list, then adjust the number of CPUs to 1.
4. Adjust the number of cores to 4.
5. FortiTester has 5 NICs.Assign the E1000 NIC for MGMT and the VMXNET3 NICs for DPDK. Make sure the four DPDK ports are assigned to the same switch or vSWITCH.
6. Select **Hard disk 2**, the log disk, from the Hardware list, and configure it as required. Hard disk 1 should not be edited.
7. Click **OK** to apply your changes.

The DPDK interface can also support 82599 with PCI-PASSTHROUGH.

Power on the virtual machine

You can now proceed to power on your FortiTester VM.

- Select the FortiTesterVM in the left pane and click **Power** on the virtual machine in the Getting Started tab.
- Select the VM in the left pane, then click **Power On** in the toolbar.
- Right-click the VM in the left pane, then select **Power > Power On** from the right-click menu.

Linux KVM

Once you have downloaded the zip file and extracted the package contents to a folder on your management computer, you can deploy the kvm package to your KVM environment.

Prior to deploying the FortiTester VM, ensure that the KVM platform is configured and functioning properly. The installation instructions presume that you are familiar with the management software of the platform.

To create the virtual machine:

1. Launch Virtual Machine Manager (virt-manager) on your KVM host server.
2. Click **Create a new virtual machine**.
3. Enter a name for the virtual machine.
4. Select Import existing disk image.

5. Click **Forward**.
6. Click **Browse**, then locate and select `boot.qcow2` in your local disk.
7. Click **Forward**.
8. Change the "Memory (RAM)" setting to 8192 MB and the "CPUs" setting to 4.
9. Click **Forward**.
10. Make sure the "Customize configuration before install" box is checked.
11. Click **Finish**.

To customize configurations:

1. From the customization screen, select Processor, located on the left. If Processor is not available from the menu, select CPUs.
2. Select or click **Copy host CPU configuration**.
3. Open the Topology menu and manually set CPU topology to include 1 Socket and 4 Cores.
4. Click **Apply**.
5. Select IDE Disk 1from the menu on the left.
6. Open the Advanced options menu.
7. Change the "Storage format" to qcow2, change the "Cache mode" to writeback, and change "Disk bus" to VIRTIO/SCSI.
8. Click **Apply**.
9. Click **Add Hardware**, located on the bottom left.
10. Select Storage from the menu on the left.
11. Choose "Select managed or other existing storage", then find and select `data.qcow2`.
12. Change the "Storage format" to qcow2, change the "Cache mode" to writeback, and change the "Device type" to SCSI/VIRTIO.
13. Click **Finish**.
14. Select your NIC, or your virtual network interface from the menu on the left.
15. Change the "Device model" to e1000.
16. Configure the source mode and source device according to your environment specifications.
17. Click **Add Hardware** and select Network.
18. Change the "Device model" to virtio.
19. Click **Finish**, then click **Apply**.
20. Click **Begin Installation**.

To customize advanced settings:

This section is not needed for most users.

- To support Multi Queue virtio:
  a. From the host terminal, enter the command: `virsh edit <instance-name>`.
  b. Find the block for your NIC, and add the following inside the <interface>
  ```
  <driver name='vhost' queues='8'/>
  <driver name='vhost' queues='4'/>
  ```
- To enable PCI passthrough:
  a. Add the command `intel_iommu=on` to the boot command of the host, then reboot.
  b. In the host terminal, use the command `modprobe pci_stub` to import the PCI stub driver.

c. Use the command `lspci -n` to find out the vendor and device ID of the NIC.
d. Detach the PCI device from the host
   i. Use `virsh nodedev-list | grep pci`, to get the PCI device info.
   It will appear in a format similar to: pci_8086_****, where * is the code for each device.
   ii. Detach the device with the command `virsh nodedev-detach pci_8086_****`.
   iii. Use the command `echo "<vendor id>:<device id> " > /sys/bus/pci/drivers/pci-stub/new_id`.
   iv. Use the command `echo "<PCI ID>" > /sys/bus/pci/devices/<PCI ID>/driver/unbind`.
   v. Use the command `echo "<PCI ID>" > /sys/bus/pci/drivers/pci-stub/bind`.
e. Using virt-manager, click **Add Hardware**, select PCI Host Device, find your NIC, then click **Finish**.

- To enable SR-IOV:

a. Add the command `intel_iommu=on` to the boot command of the host, then reboot.
b. Use the command `modprobe -r ixgbe`.
c. Use the command `modprobe ixgbe max_vfs=4`, where 4 can be replaced by a number appropriate for your network card.
d. Use the command `lspci` to check the SR-IOV function.
e. Using the virt-manager, click **Add Hardware**, select PCI Host Device, find your NIC, then click **Finish**.

To power on the virtual machine:

You can now proceed to power on your FortiTester VM.

- Select the FortiTester VM and click ▶ **Power on the virtual machine**.

Getting started with the virtual machine

1. Enter **admin** when asked for a FortiTester login. The default password is blank.

The interface will display `Welcome !` if you have successfully logged in.

2. See Connecting to FortiTester on page 20 for instructions on how to access the GUI, as well as other procedures for getting started with FortiTester.

Upload the license file

1. Select the **System** tab from the GUI.
2. Click **Upload**, under License Status.
3. Choose your license file, then click on the upload icon.
4. Click **Close**.

FAQ

Does FortiTester VM supports SR-IOV?

Yes. This was supported long time ago. FortiTester can utilize the NIC to perform faster input and output.

How do I replay large PCAPs in FortiTester?

You can consider using Attack Replay under Security Testing. See Starting an IPS Attack Replay test on page 273.

Please note the size of all the uploaded pcap files should not exceed 200 MB. You can upload more files by creating multiple Attack Replay cases and schedule to run them one after another.

As loading multiple 200MB files into memory, your FortiTester device might not have enough memory, e.g. FortiTester 2000E has 32 GB memory, FortiTester 3000E has 64 GB memory.

Can FortiTester run more than one case at a time?

No, FTS does not support more than one case at a time. However, you can schedule the test cases to run automatically one after another. See Scheduling cases on page 47.

Does FortiTester support API?

Yes, FortiTester has a very comprehensive REST API. Test cases can be created, launched and monitored using the API. See Using the REST API on page 314.

What are the supported hardware & port density?

- FortiTester 2000D - 1x GE RJ45, 4x 10 GE SFP+, 120 GB SSD storage [EOL already]
- FortiTester 2000E - 1x GE RJ45, 4x 10 GE SFP+, 1TB HDD Storage [Replacement of 2000D]
- FortiTester 2500E - 1x GE RJ45, 4x 10 GE SFP+, 1TB HDD Storage
- FortiTester 3000E - 1x GE RJ45, 2x 40 GE QSFP, 2 TB HDD storage
- FortiTester 4000E - 1x GE RJ45, 1x 100 GE QSFP28, 2 TB HDD storage

What are the limitations on CPU, RAM and Storage for different VM licenses?

- FortiTester VM02 - 2 vCPU, 4GB RAM, 60GB Storage
- FortiTester VM04 - 4 vCPU, 8GB RAM, 60GB Storage
- FortiTester VM08 - 8 vCPU, 16GB RAM, 60GB Storage
- FortiTester VM16 - 16 vCPU, 32GB RAM, 60GB Storage
- FortiTester VM32 - 32 vCPU, 64GB RAM, 60GB Storage

Note: The Enterprise mix feature under **Performance Testing > Mix Traffic** is only available on FortiTester-VMs with VM16 or VM32 license.

Where are the different attack packages and how often are they updated?

Different attack packages are provided based on the FortiGuard services you purchased:

- Basic package
  Monthly update containing the latest attack traffic files (about 300+).
- Premium package
  - Bi-monthly update containing all attack traffic files (including IoT/OT attacks, about 2400+).
  - Attack mutation engine (10 evasion techniques out of the box).
  - Web Protection signatures.
- ATT&CK abilities package

See Updating FortiGuard for how to update and upgrade the service package.

Where can I download the attack package?

You can download it from Fortinet Support site. See Updating FortiGuard for more information.

What are Test Centre model running conditions? Can they be different models?

Yes, they can be different models, but based on the following conditions:

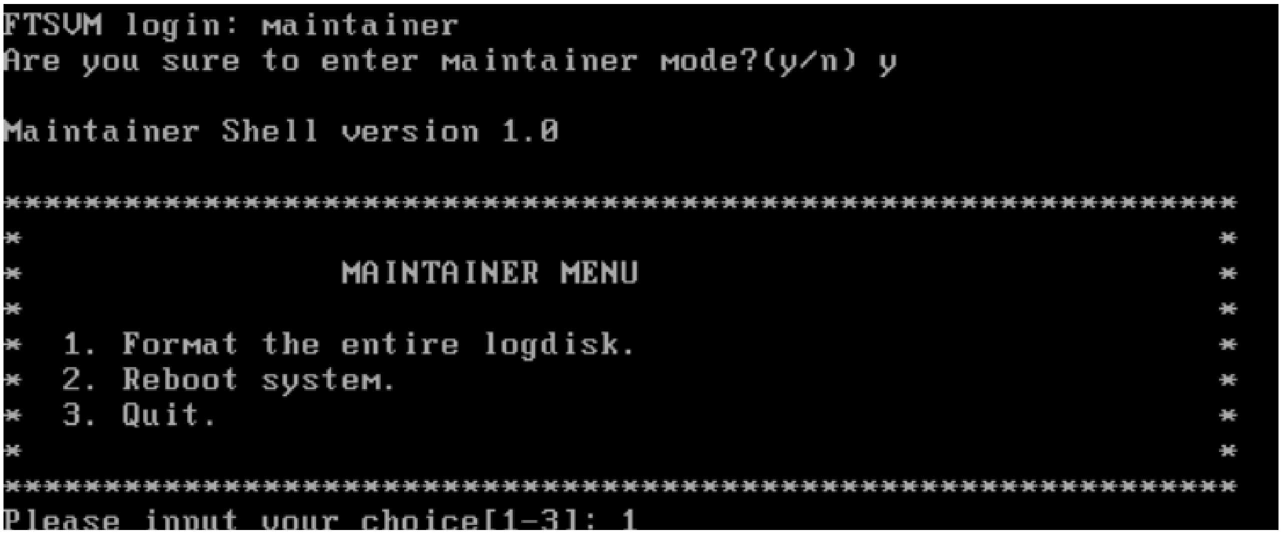
- For all FortiTester-VMs they have to be properly licensed.
- For all FortiTester-VMs, Center/Slave must have the same vCPU number, VM type, port number.
- Software - Center/Slave must have the same major version number (e.g. 3.8.0 can run with 3.8.1 but NOT 3.7)
- For 3000E, Center/Slave must have the same fanout mode (e.g. 3000E can break out 2 x 40G into 8 x 10G)
- Center/Slave must be in the same group i.e.:
  - "2K": ["FTS_2000D", "FTS_2000E", "FTS_2500E"],
  - "3K": ["FTS_3000E"],
  - "4K": ["FTS_4000E"],
  - "VM": ["FTS_VM_KVM"],
  - "VM_ESXI": ["FTS_VM"],
  - "AWS": ["FTS_VM_AWS"],
  - "AWS_BYOL": ["FTS_VM_AWS_BYOL"],
  - "AZR_BYOL": ["FTS_VM_AZURE_BYOL"],
  - "OCI_BYOL": ["FTS_VM_OCI_BYOL"],
  - "GCP_BYOL": ["FTS_VM_GCP_BYOL"]

How can we reset FortiTester admin password? Is there a maintainer account like FortiGate?

FortiTester does have a maintainer account, and it can be used to reset password, but all configurations and results on your FortiTester device will be removed once the password is reset.

Perform the following steps to reset password:

1. Log in to FortiTester's CLI with the maintainer user's credential.
2. Enter `1`.



```
FTSVM login: maintainer
Are you sure to enter maintainer mode?(y/n) y

Maintainer Shell version 1.0

*****************************************************************
*                                                               *
*                  MAINTAINER MENU                              *
*                                                               *
*  1. Format the entire logdisk.                                *
*  2. Reboot system.                                            *
*  3. Quit.                                                     *
*                                                               *
*****************************************************************
Please input your choice[1-3]: 1
```