Administration Guide

FortiTester 7.4.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

January 27, 2026
FortiTester 7.4.4 Administration Guide
86-744-934662-20260127

TABLE OF CONTENTS

Change log 9
Introduction 10
Features and benefits 11
Performance tests 11
Security tests 16
ATT&CK tests 17
Getting started 18
Connecting to FortiTester 18
Configuring the management port 19
Configuring DNS settings 20
Configuring system time 20
Changing the admin password 21
Configuring the device under test 21
Using the REST API 21
Introduction 21
Example API commands 22
Running tests 25
Test case configuration overview 25
Using network configuration templates 25
Creating a network configuration template 26
Configuring network configuration object settings 27
Using Ports Connected Relation 28
Using port binding and link aggregation 30
Using 40G to 4 × 10G fan out 31
Using success criteria 31
Displaying test status 32
Using widget view 36
Modifying traffic load mid-run 38
Viewing test results 39
Results for a throughput test 40
Attack replay test 41
Subnet statistics 41
Exporting and importing a test case 42
Scheduling cases 42
Stopping tests 42
Performance testing 43
HTTP cases 43
Starting an HTTP CPS test 43
Starting an HTTP RPS test 45
Starting an HTTP CC test 47
Starting an HTTP Throughput test 47
Starting an HTTP Real Life test 48
HTTP Test Case common options 49

HTTPS cases 53
- Starting an HTTPS CPS test 53
- Starting an HTTPS RPS test 54
- Starting an HTTPS CC test 55
- Starting an HTTPS Throughput test 56
- Starting an HTTPS Real Life test 57
- HTTPS test case common options 58

HTTP/2 cases 63
- Starting an HTTP/2 CPS test 64
- Starting an HTTP/2 RPS test 65
- Starting an HTTP/2 CC test 66
- Starting an HTTP/2 Throughput test 68
- HTTP/2 test case common options 69

VPN cases 75
- Starting an IPsec Remote Access test 75
- Starting an IPsec Remote Access CC test 77
- Starting an IPsec Throughput test 79
- Starting an SSL-VPN CPS test 80
- Starting an SSL-VPN RPS test 84
- Starting an SSL-VPN CC test 89
- Starting an SSL-VPN Real Life test 91
- VPN test case common options 96

UDP cases 98
- Starting a UDP PPS test 98
- Starting a UDP payload test 101

TCP cases 103
- Starting a TCP throughput test 103
- Starting a TCP TurboTCP test 104
- Starting a TCP connection test 105
- TCP Test Case common options 106

DNS cases 110
- What is DoT? 110
- Where to find the DoT Case in the GUI? 110
- How does DoT case work? 110
- Key configurations 111

RFC benchmark cases 116
- Starting an RFC 2544 throughput test 116
- Starting an RFC 2544 latency test 117
- Starting an RFC 2544 loss rate test 118
- Starting an RFC 2544 back to back test 119
- Starting an RFC 3511 IP throughput test 120
- Starting an RFC 3511 concurrent capacity test 121
- RFC Test Case common options 124

Protocol cases 126
- Starting a TCP Protocol CIFS/SMB test 126
- Starting a TCP Protocol DNS-AXFR test 127
- Starting a TCP Protocol FIX test 128
- Starting a TCP Protocol FTP test 129

Starting a TCP Protocol IMAP test 130
Starting a TCP LDAP test 131
Starting a TCP NFS test 132
Starting a TCP Protocol POP3 test 132
Starting a TCP Protocol RDP test 133
Starting a TCP Protocol SMTP test 134
Starting a TCP Protocol SSH test 135
Starting a UDP Protocol DNS latency test 136
Starting a UDP Protocol NTP test 138
Starting a UDP Protocol RADIUS test 138
Starting a UDP Protocol SIP test 139
Starting a UDP Protocol TFTP test 140
Starting a Protocol DHCP test 141
Starting a Protocol ICMP test 142
Starting a Protocol IGMP test 143
Starting a Protocol RTSP/RTP test 144
Protocol Test Case common options 145
Application cases 149
Starting an Amazon S3 test 149
Starting an AOL chat test 150
Starting a BitTorrent test 151
Starting a DB2 test 152
Starting a Facebook test 153
Starting a Gmail test 154
Starting a Gtalk test 155
Starting a MSSQL test 156
Starting a MySQL test 157
Starting a Netflix test 158
Starting an Oracle TNS test 159
Starting a PSQL test 160
Starting a Twitter test 161
Starting a WebEx test 161
Starting a WhatsApp test 162
Starting a Yahoo Mail test 163
Starting a YouTube test 165
Application test case common options 166
Replay cases 170
Starting a Traffic Replay test 170
Starting a GTP Replay test 172
Starting a packet capture test 174
packet capture test case options 175
Starting a mixed traffic test 176
mixed traffic test case options 178
Managing performance testing objects 182
Networks 183
Port Settings 183
Port Mapping 183
Files 184
Hosts 184

Host groups 184
URL groups 185
User groups 185
iMIX 186
Certificates and Certificate Groups 186
SNI 187
Payloads 187
Scripts 187
SNMP Monitors 188
Creating a custom traffic template 189
Performance testing examples 190
Using virtual router with AWS public cloud to run a HTTPS CPS test 190
Security testing 196
DDoS cases 196
Starting a DDoS single packet flood test 196
Starting a DDoS TCP session flood test 199
Starting a DDoS HTTP session flood test 202
Starting a DDoS concurrent session flood test 206
Starting a DDoS UDP packet flood test 209
Starting a fuzzing test 211
Starting a malware test 212
malware test case options 212
IPS cases 215
Starting an IPS attack replay test 215
Starting an IPS HTTP evasion test 218
Web protection cases 220
Starting a web protection test 220
Starting a Web protection web crawler test 224
Managing security testing objects 225
Networks 226
Certificates and certificate groups 226
Payloads 226
Scripts 227
SNMP Monitors 227
Single Packets 229
Single Packet Group 230
User Intrusion group 230
FGD Intrusion group 230
User Malware group 231
FGD Malware Group 231
Web protection group 231
URLs 232
Creating a custom traffic template 232
Maintaining FortiGuard intrusion and webprotections services 233
Security testing cookbook 233
Using an IPS Attack Replay case 233

MITRE ATT&CK® 237
System requirments 237
Installing FortiAgent 237
Running an ATT&CK case 238
Adding domains 238
Adding a host group 238
Creating an ability group 239
Creating an adversary 239
Creating an ATT&CK Case 239
Viewing ATT&CK cases 241
MITRE ATT&CK Breach simulation examples 241
Using attack cases 244
System administration 248
Viewing system status 248
System Information Overview 248
Security fabric 248
Setting password 251
CLI command for maintainer account 251
Configuring a RADIUS server 252
Updating firmware 253
Shutting down the system 254
Rebooting the system 254
Configuring specific settings 255
Creating test users 255
Updating FortiGuard 256
Reset, back up, restore, or downgrade the system 259
Reset 260
Backup 260
Restore 260
Downgrade 260
Uploading TLS certificates 261
Log & Report 262
Report Settings 262
Report fields 262
Log Settings 262
Viewing system events 263
Searching logs 263
Downloading logs 263
Test Center 264
Requirements and restrictions 264
Configuring work mode settings 264
Default and maximum values 267
Setting up a VM 268
Introduction 268
Deployment 268

Deployment package 268
Deploying the appliance 269
Uploading the license file 269
Deployment examples 269
Creating the virtual machine 269
Getting started with the virtual machine 273
Glossary 274
FAQ 280

Change log

Date	Change description
2025-04-24	Initial release
2025-05-27	Updated Deployment on page 268.
2025-08-18	Updated Installing FortiAgent on page 237.
2026-01-27	Removed video links.

Introduction

FortiTester™ appliances and VMs offer an enterprise-grade solution for performance and security testing.

FortiTester appliances provide 10/40/100G options for simulating network traffic, including RFC2544/3511, HTTP/HTTPS/HTTP 2 simulation, UDP (PPS / Payload), SSL/IPSEC VPN testing (for FortiGates), Q-in-Q traffic generation and PCAP/GTP replay. As well as different traffic generation, FortiTester allows customer to customise traffic mix templates with different protocol and application mix. Both FortiTester appliance and VM02-32 offers standalone and test center mode, where FortiTester can be combined as either clients or servers mode to test DUT (Device Under Test) for high performance gain. Available in most popular public cloud platforms, FortiTester can also be used as validating public cloud architecture and performance.

From a security standpoint, FortiTester can be used for Breach Attack Simulation (MITRE ATT&CK simulation), CVE based IPS, DDoS, Malware Strike pack, Fuzzing attacks, web attacks. With comprehensive API to automate, run and retrieve result, FortiTester allows users to natively integrate into Fortinet Security Fabric with FortiSIEM support, SYSLOG, SNMP traps, LDAP and RADIUS support. PCAP replay also provides an excellent tool for troubleshooting difficult network issues.

Features and benefits

FortiTester is a network performance and security attack simulation tool, available both in appliances (10/40/100G), in VM form factor and in public cloud. It provides performance and security tests (Intrusions, malware strike pack, web based/IOT attacks, and MITRE ATT&CK simulation).

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.

HTTPS RPS test

The HTTPS RPS test is the same as the HTTP RPS test, except that it uses HTTPS traffic.

HTTPS CC test

The HTTPS CC test is the same as the HTTP CC test.

HTTPS throughput test

The HTTPS Throughput test is the same as the HTTP Throughput test.

HTTP/2 CPS test

This test establishes a TCP connection (three-way handshake), optional SSL connection (handshake), and completes an HTTP/2 transaction (HTTP/2 request and response), and closes the TCP connection (Reset). It creates one HTTP/2 GET per TCP connection.

HTTP/2 RPS case

This test establishes a TCP connection (three-way handshake), optional SSL connection (handshake), completes multiple HTTP/2 transactions (HTTP/2 request and response), and closes the TCP connection (Reset). It creates multiple HTTPS/2 GET per TCP connection.

HTTP/2 CC Test

This test establishes a large number of TCP connections (three-way handshake), loops complete HTTP/2 transactions (HTTP/2 request and response), and closes the TCP connection.

HTTP/2 Throughput test

As opposed to the HTTP Throughput test, which keeps all requests and responses in plain text format, HTTP/2 Throughput uses the binary framing layer to encapsulate all messages in binary format, while still maintaining HTTP semantics, such as verbs, methods, and headers.

IPsec remote access test

This test establishes a HTTP/2 connection (three-way handshake), loops completed HTTP/2 transactions (HTTP/2 request and response), and closes the HTTP/2 connection (Reset), which determines the maximum throughput (total bits per second "on the wire").

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 CPS test

FortiTester establishes a SSL-VPN tunnel connection and completes a full HTTP transaction through it. It creates one HTTP(FTP) transaction per tunnel.

SSL-VPN tunnel RPS test

FortiTester establishes a SSL-VPN tunnel connection and completes multiple full HTTP transactions through it. It creates multiple HTTP transactions per 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.

SSL-VPN tunnel Throughput test

FortiTester establishes a SSL-VPN tunnel connection, loops a completed HTTP/TCP/UDP transaction and closes the 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 to the server.

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 CP connection (three-way handshake) and resets the TCP connection.

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, 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 the 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 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 to the server.

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.

Fuzzing

FortiTester measure the device's ability to handle invalid IP, TCP, UDP, and ICMP packets, which send invalid fuzzed packets to DUT devices and validate whether the device continues to operate.

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.

Malware 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.

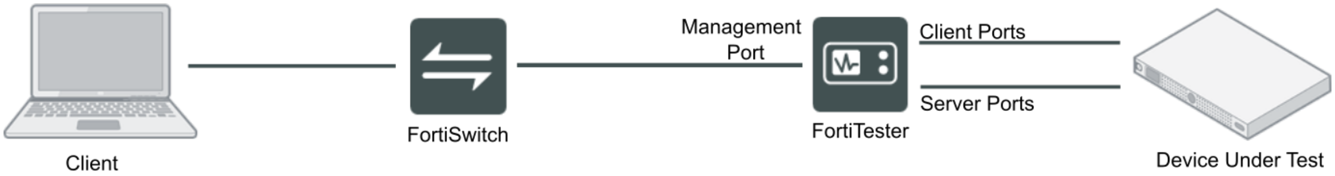
Getting started

This chapter provides the procedures for getting started with FortiTester.

Connecting to FortiTester

A basic network connection topology for FortiTester is shown in Figure 1.

Figure 1

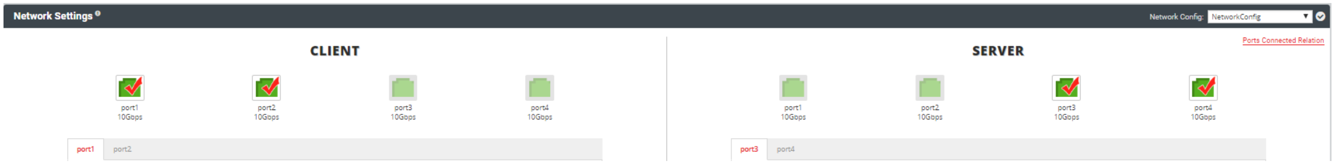


A FortiTester appliance has multiple network ports. In most cases, one port is for management and the others are for testing. The management port (usually `mgmt` or `port1`) connects to a local network to enable the user to access the FortiTester appliance via the web UI.

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.

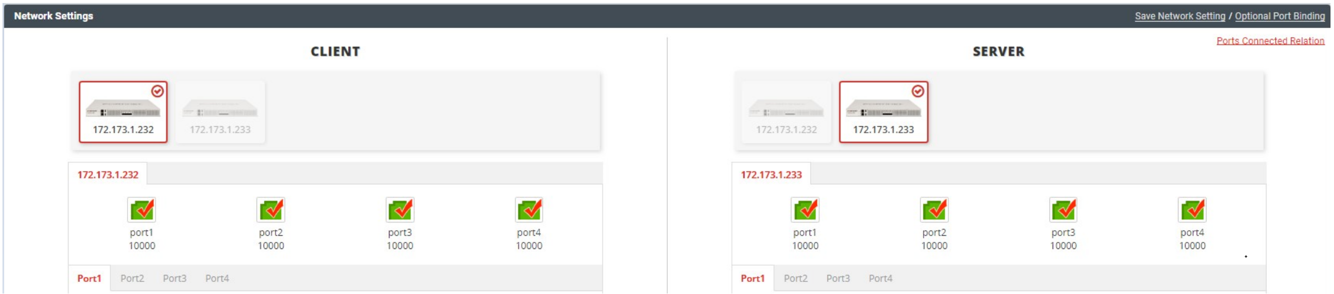
When you use one FortiTester appliance in standalone work mode, the test ports on the standalone appliance are divided between client and server. Figure 2 shows the distribution of ports in a standalone environment. Port 1, a client port, is paired with port 3, a server port; port 2, a client port, is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

Figure 2



If your tests require more ports, you can join up to 4 pairs of FortiTester appliances in a Test Center. Figure 3 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.

Figure 3



For information on configuring a Test Center, see Chapter 4 - Joining multiple appliances into a 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. Enter `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	Enter the IP address.
Netmask/IPv6 Netmask	Enter the netmask.
Gateway/IPv6 Gateway	Enter the gateway address.

6. 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. Localhost 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*, Enter the IP address of the primary DNS server.
3. In *Secondary DNS Server*, enter the IP address of the secondary DNS server.
4. Click *Apply*.

   FortiTester queries 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. In the *Time Zone*, select the appropriate time zone from the dropdown and click *Apply*.
3. *In Set Time*, click *Manual Settings*, enter the date and time, then click *Apply*.

   Alternatively, click *NTP* , enter the IP address or domain name of an NTP server, set the *Sync Interval*, then click *Apply*.
4. Click *Close*.

System Time

Settings	Guidelines
Time Zone	Select the time zone where the FortiTester appliance is installed. The system will be updated according to the timezone, accounting for daylight savings time.
Set Time	Enter the current settings for the system date and time. You can change these

Settings	Guidelines
	manually. Use the calendar button to select the date and time from a calendar.
NTP Server	Enter the IP address or domain name of an NTP server. To find an NTP server that you can use, see http://www.ntp.org.
Sync Interval	Enter the interval, in minutes, at which the system time is synchronized with the NTP server. Default: 60 minutes.

Changing the admin password

FortiTester has a default user `admin`.

To change the password for the admin account:

1. In the top right banner, click *admin*.
2. Click *Change Password*.
3. Enter the old password, the new password twice, and click *Save*.

Configuring the device under test

The device under test (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.

Using the REST API

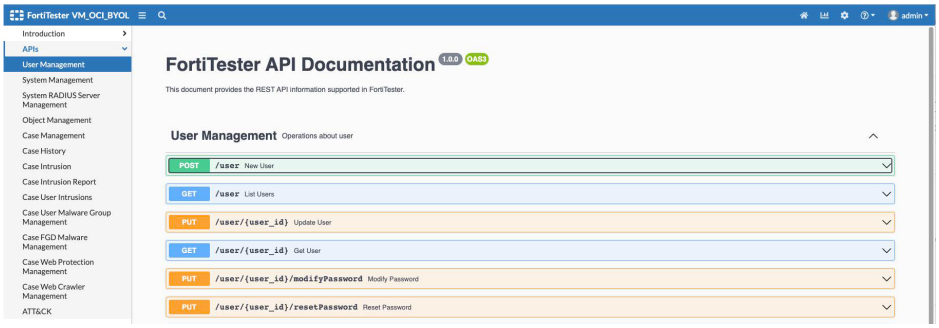
Introduction

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.

FortiTester API are also available on Fortinet Developer Network, at https://fndn.fortinet.net/index.php?/fortiapi/1003-fortitesterbeta/

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.

The API browser in GUI allows users to try out the API in GUI. Users can also find FortiTester API documentation on FNDN (Fortinet Developer Network).



FortiTester API Documentation 1.0.0 OAS3

This document provides the REST API information supported in FortiTester.

User Management Operations about user

POST `/user` New User

GET `/user` List Users

PUT `/user/{user_id}` Update User

GET `/user/{user_id}` Get User

PUT `/user/{user_id}/modifyPassword` Modify Password

PUT `/user/{user_id}/resetPassword` Reset Password

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:

- A valid admin username and password (so that an authenticated session can be established)
- 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":""
}
```

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. Determines the mandatory and optional settings for specific cases.
- **Case options**: IP version, device under test (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 the FortiTester client and the connected DUT.

The test case specifics are key to testing the performance of the DUT. We recommend that 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 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 dialog match the settings in the network configuration template.

After the settings have been imported, you cannot 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:

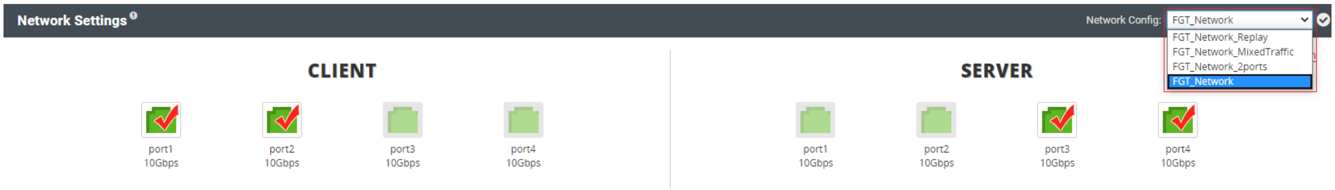
1. Go to *Objects > Networks* under either *Performance Testing* or *Security Testing*.
2. Click *+ Create New* to display the configuration page.
3. In the popup dialog, configure the following settings:

Settings	Guidelines
IP Version	Select *v4*, *v6*, or *Mixed*.
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	Select from the following options: • *Transparent (TP)*: 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. • *Network Address Translation (NAT)*: The DUT does not change the IP address of the packet. • *Web Proxy*: 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 Gateway* to send and 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. Enable *SNAT/DNAT* to allow DUT to do source and destination NAT on the same session, or enable *NAT64* or *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. Allow the clients or servers to be on subnets different from the DUT interfaces, with all traffic to and from the DUT using the virtual router MAC address.

4. Click *OK* to continue.
5. Complete the configuration as described below in To configure network configuration object settings on page 27.
6. Save the configuration.

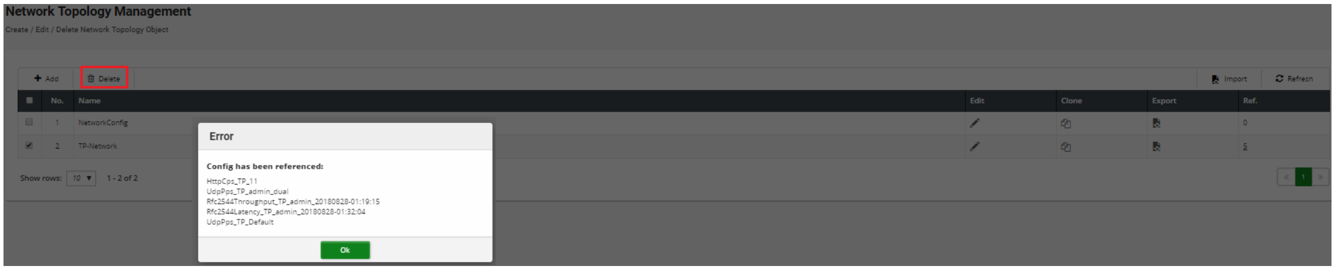
After you have created a network configuration template, you can clone it or export it as a ZIP file which can be imported later.

You can select the created *Network Config* templates from the option list on a test case page. Select the template and click ✓ to apply the template network configuration.



Network Config: FGT_Network

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


Network Topology Management
Create / Edit / Delete Network Topology Object
Add
Delete
Import
Refresh
Edit
Clone
Export
Ref.
Show rows: 10
1 - 2 of 2
Ok

No.	Name
1	NetworkConfig
2	TP-Network

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

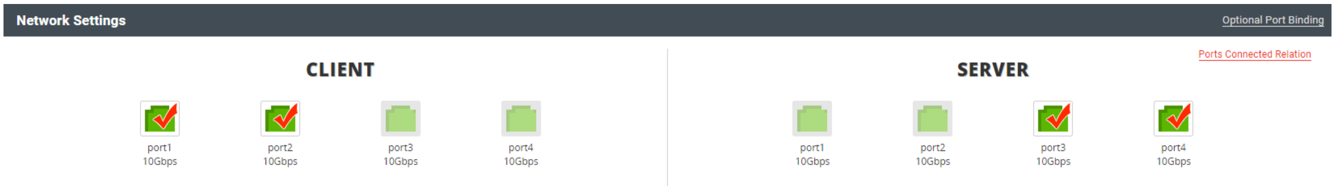
To configure network configuration object settings

Settings	Guidelines
Basic Information	
Name	Specify a configuration name. The name appears in the *Network Config* dropdown 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). 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. **NOTE:** The server port does not need to be set if you have set the *DUT Role* to *Application Server*.

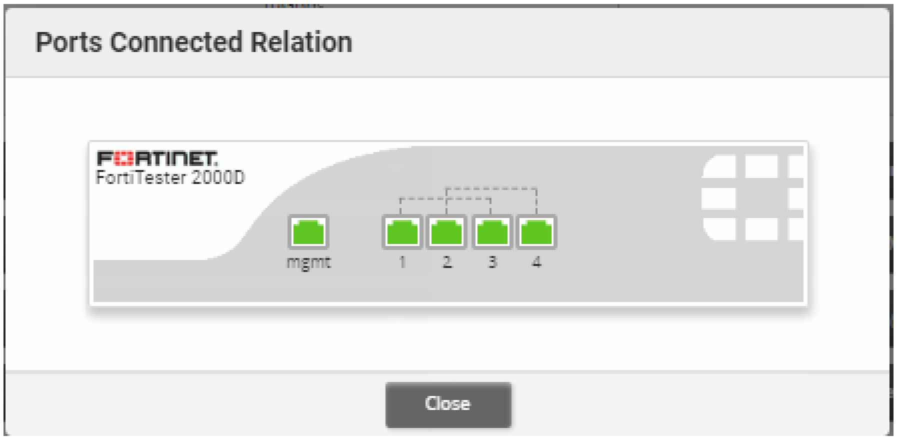
Settings	Guidelines
MAC Masquerade	
MAC Masquerade	Specify the first two bytes of a MAC address for the traffic.
QinQ	
Outer VLAN ID	Specify a Service VLAN tag for FortiTester to use during the test.
Tag Protocol Identifier	Specify the QinQ format.
Subnet	
IP Address or Range	Specify a single IP address 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 *DUT Role* is *Application Server*, specify a single IP address in the standard format.
Gateway	Specify the gateway IP address when *DUT Role* is *Application Server* or *DUT Working Mode* is *NAT*.
Peer Network	Available in NAT mode only. Specify the peer network subnet address. If the DUT uses SNAT/DNAT, use the translated IP address.
Proxy IP/Mask	Available in web proxy mode only. Specify the proxy IP address and netmask.
Add Subnet (+)	If necessary, click the *Add Subnet* button (*+*) 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 (X)	Click the *Remove* button (*X*) to remove the subnet.

Using Ports Connected Relation

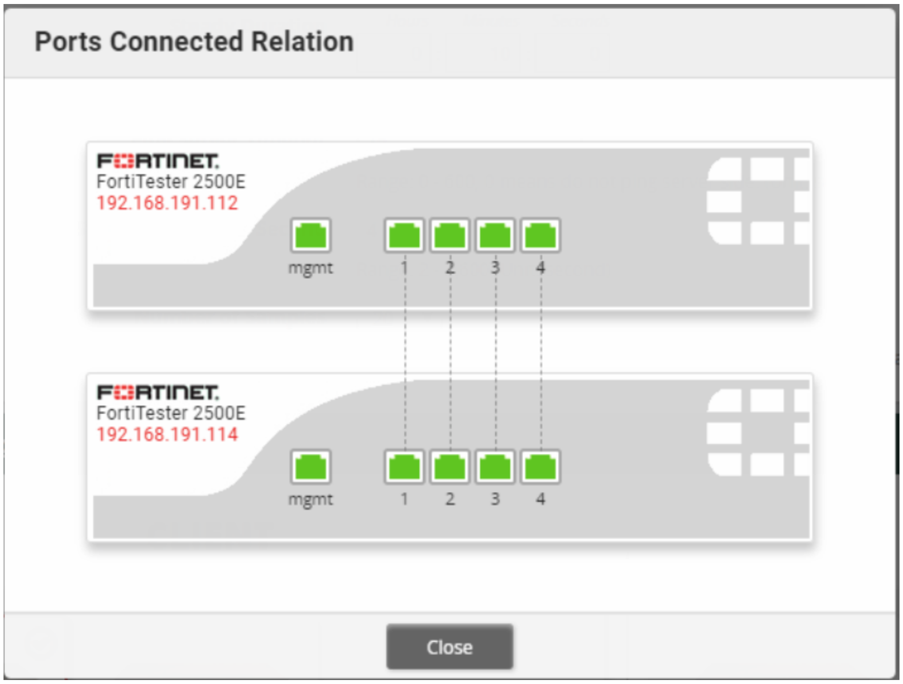
Click *Ports Connected Relation* to view the port connection status.



Standalone Mode



TestCenter Mode



Using port binding and link aggregation

FortiTester *port binding* can be used to bind multiple physical ports as one logical port. The physical ports in one logical port share one network configuration, including IP address, netmask, and gateway.

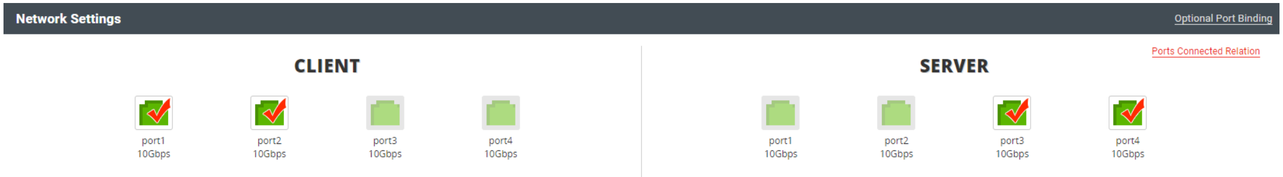
This feature is useful in the following scenarios:

- To test the link aggregation feature of the 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 the DUT. A DUT might have some ports that have bandwidth greater than a single FortiTester port. To test such port performance, you 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 four 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.

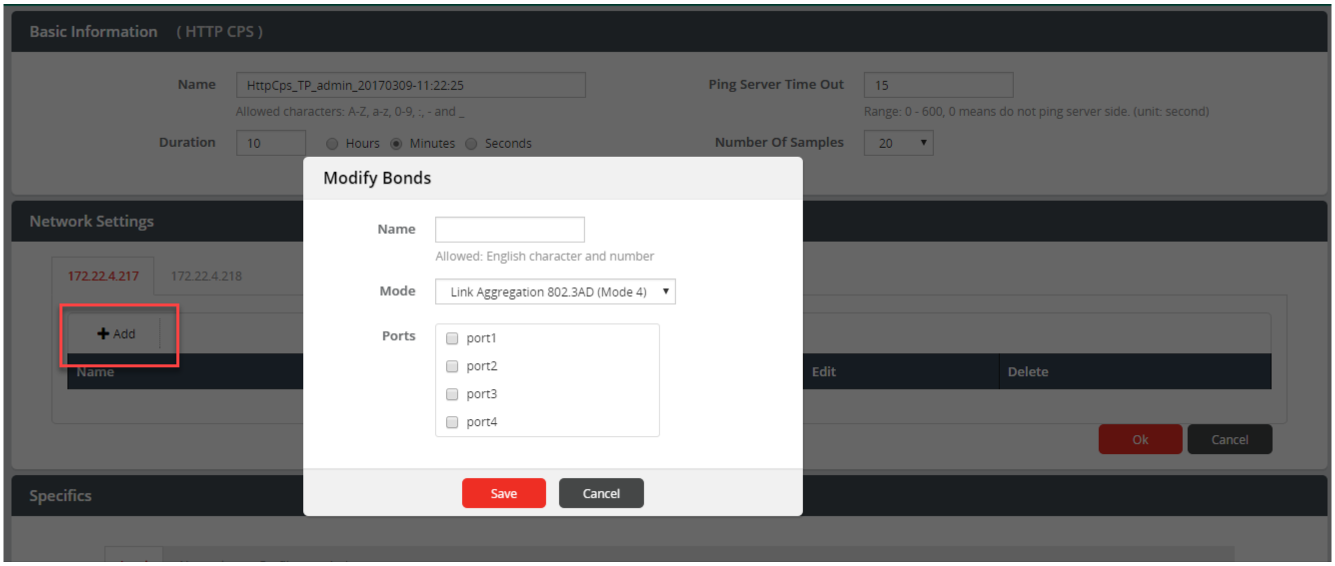
To change the port binding:

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 as 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

Network Settings

Modify Bonds

Name:

Allowed: English character and number

Mode: Link Aggregation 802.3AD (Mode 4)

Ports:
- □ port1
- □ port2
- □ port3
- □ port4

Using 40G to 4 × 10G fan out

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

This is available only on FortiTester 3000E.

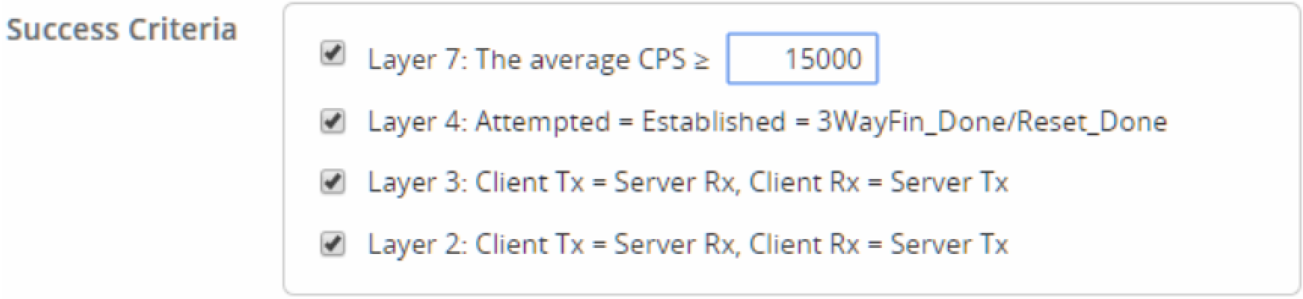
To enable fan-out:

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

After you have rebooted the system, the fan out is enabled. You can check it in *System > Settings*.

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

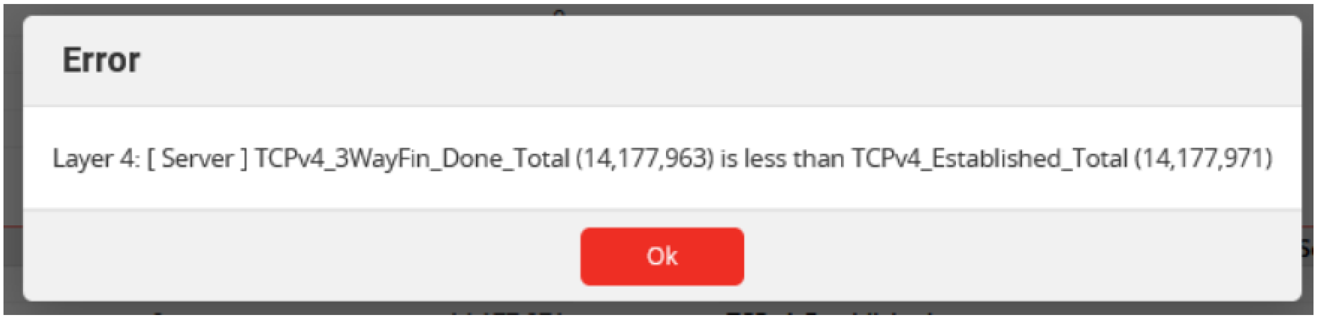
If Layer 7 criteria is set, the test will only be considered successful if the average CPS is equal to or greater than the set number.

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 Fin.

If Layer 2 or Layer 3 criteria is set, the test will be considered successful if the server receives the same number of bytes or packets 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

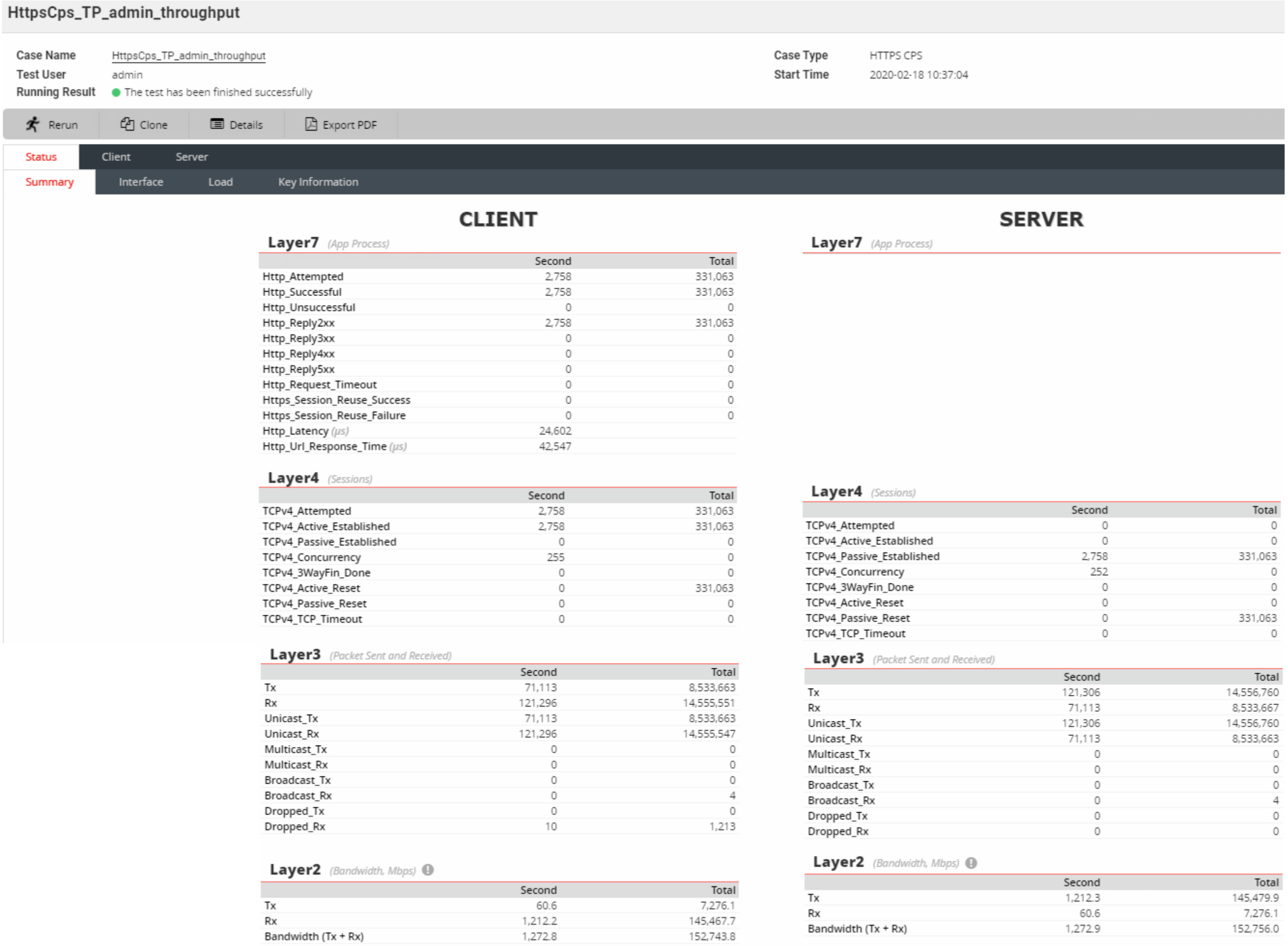
Refer to chapter Performance Testing, Security Testing, and ATT&CK Testing on how to start a test case.

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 displayed on the *Status* > *Summary* tab of an HTTPS CPS test.



HttpsCps_TP_admin_throughput

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

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)*

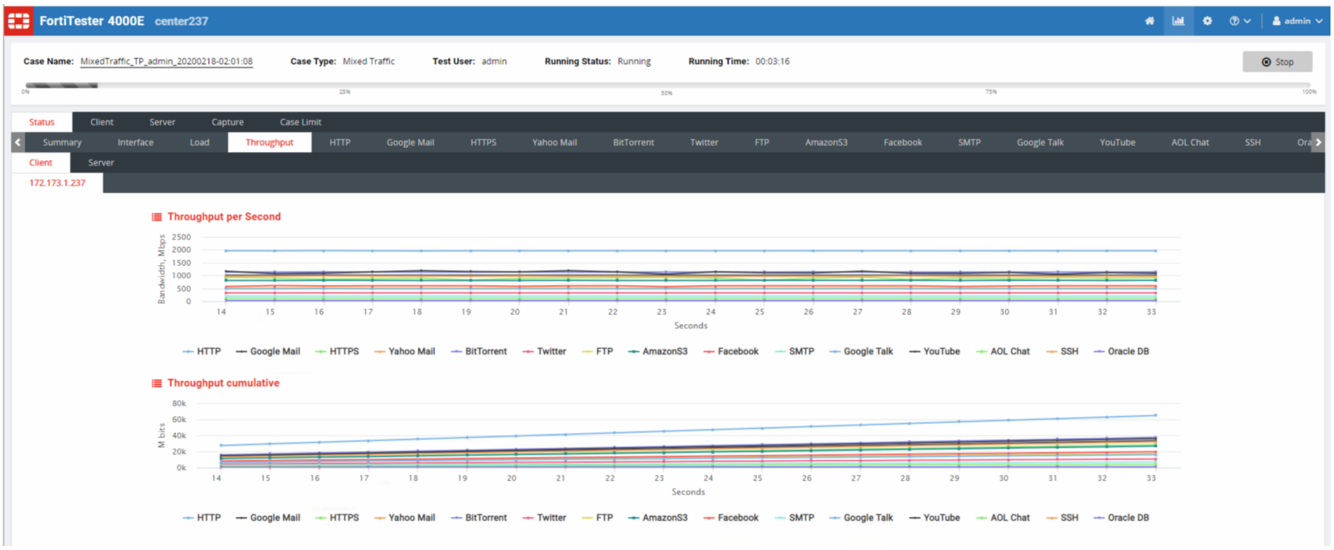
	Second	Total
Tx	121,306	14,556,760
Rx	71,113	8,533,667
Unicast_Tx	121,306	14,556,760
Unicast_Rx	71,113	8,533,663
Multicast_Tx	0	0
Multicast_Rx	0	0
Broadcast_Tx	0	0
Broadcast_Rx	0	4
Dropped_Tx	0	0
Dropped_Rx	0	0

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.

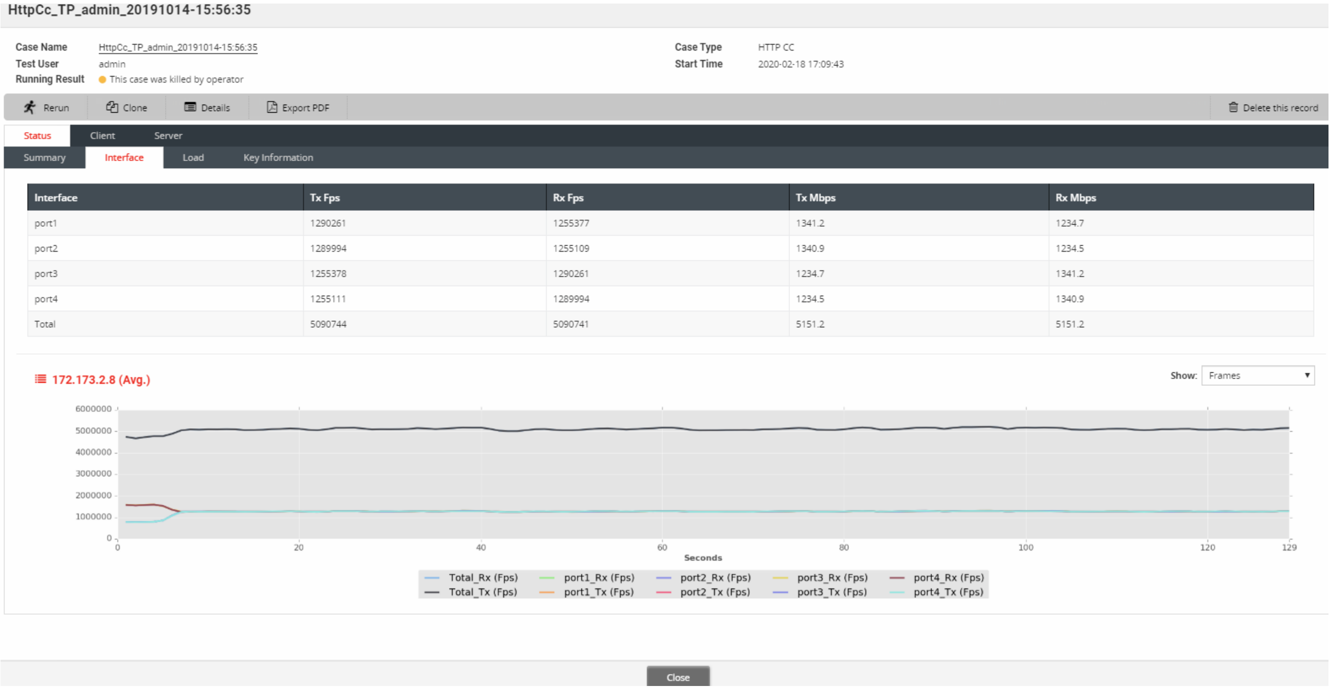
The following figure shows the information on *Status > Throughput* of a mixed traffic case.



FortiTester 4000E center237

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

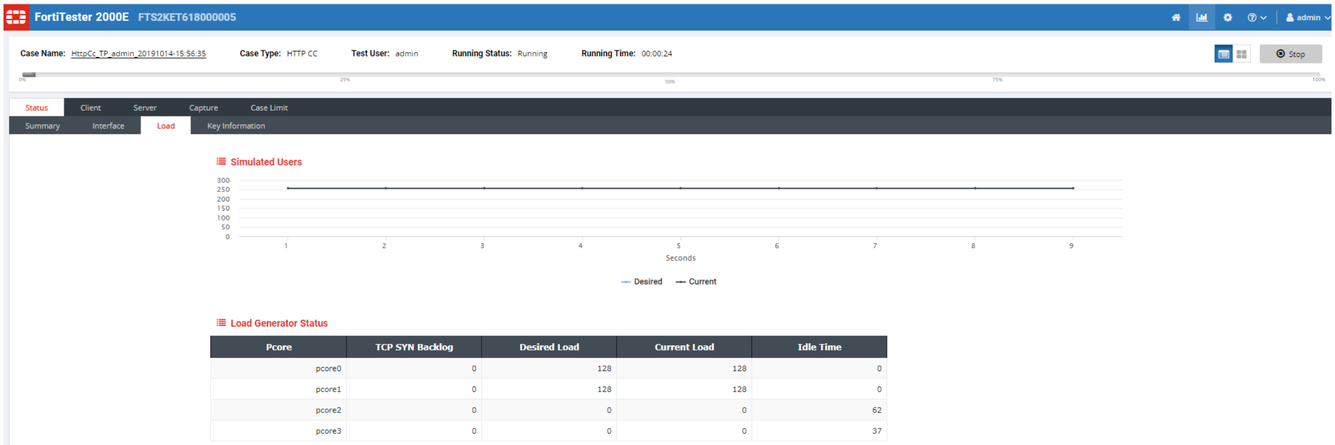
Case Name: HttpCc_TP_admin_20191014-15:56:35
Test User: admin
Running Result: ● This case was killed by operator
Case Type: HTTP CC
Start Time: 2020-02-18 17:09:43

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

172.173.2.8 (Avg.)

Show: Frames

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

Simulated Users

Load Generator Status

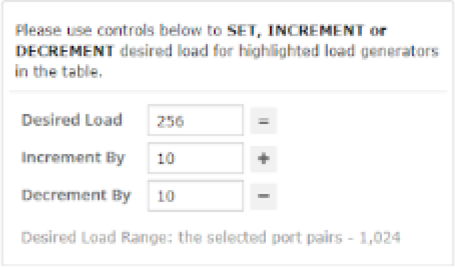
Pcore	TCP SYN Backlog	Desired Load	Current Load	Idle Time
pcore0	0	128	128	0
pcore1	0	128	128	0
pcore2	0	0	0	62
pcore3	0	0	0	37

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.

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 =

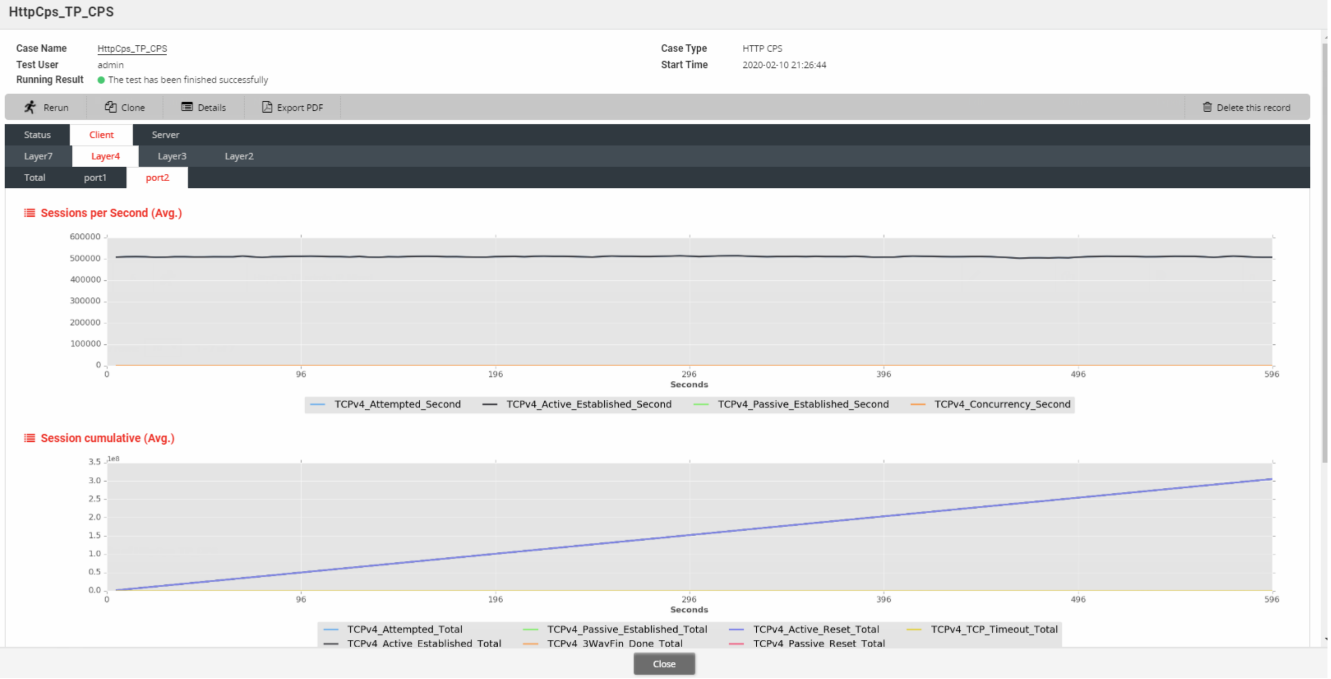
Increment By 10 +

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	Case Type	HTTP CPS
Test User	admin	Start Time	2020-02-10 21:26:44
Running Result	● The test has been finished successfully		

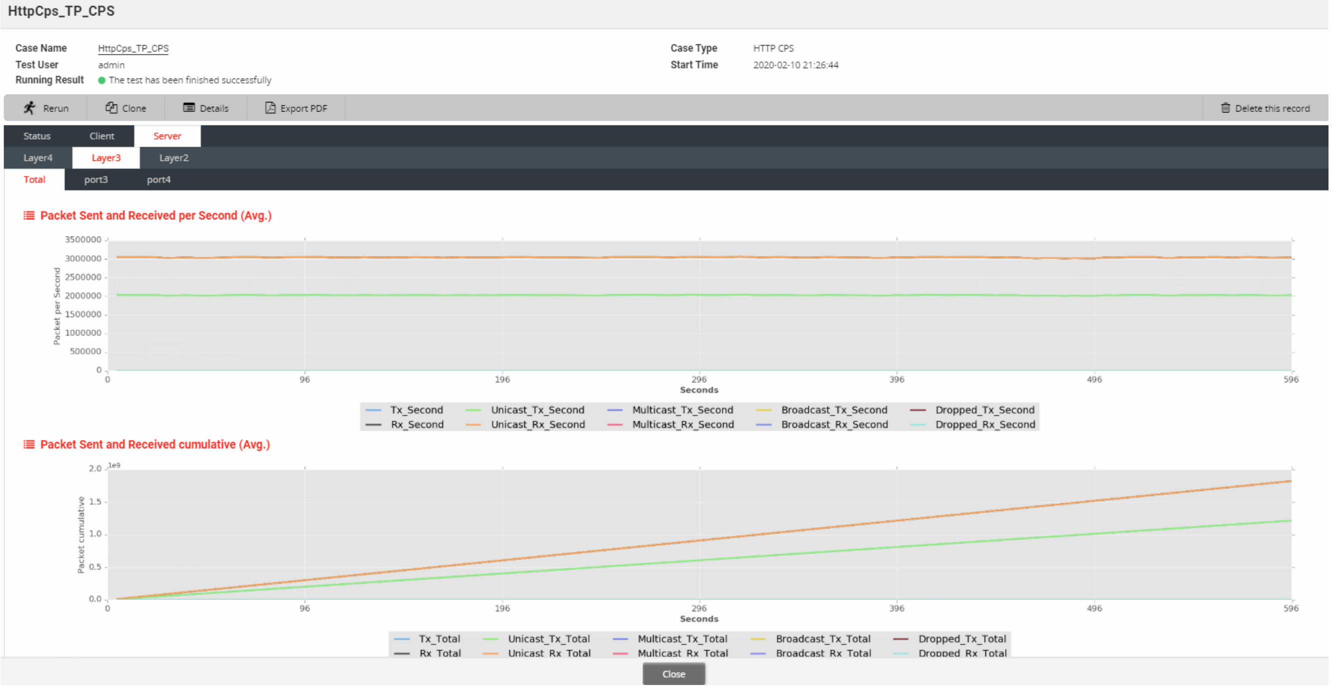
For TCP Response Time, the following information is shown:

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

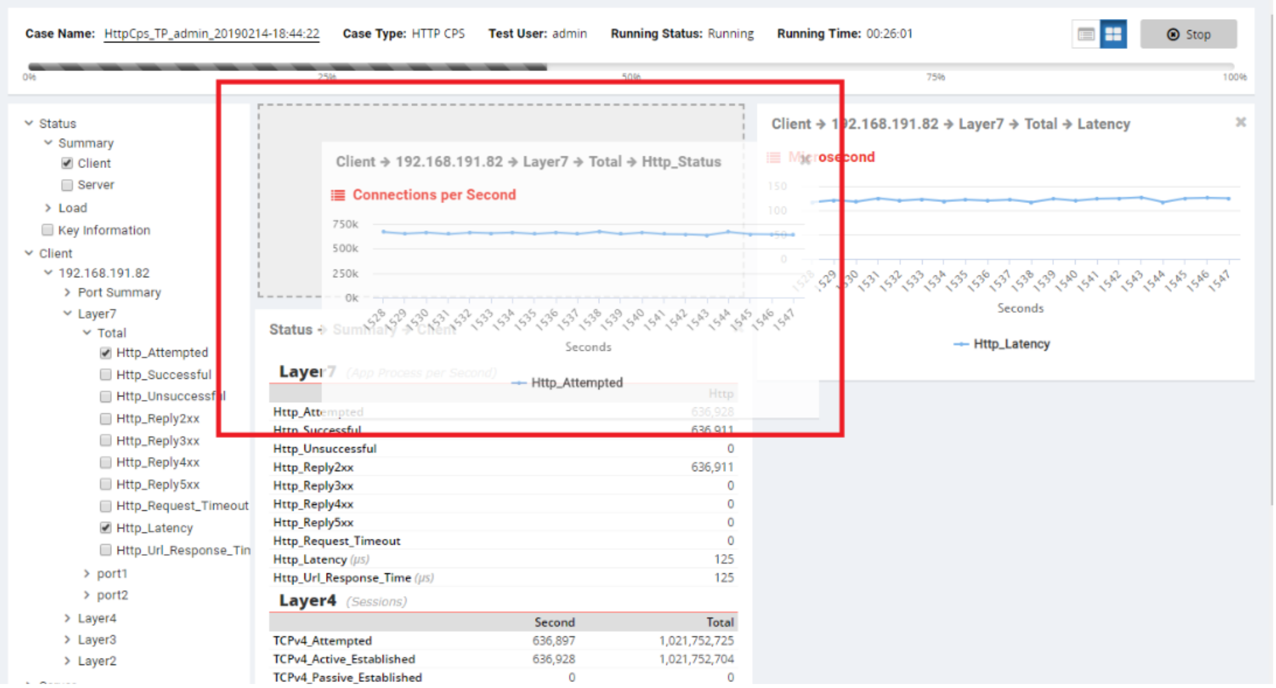
You can use the widget view to monitor the test status.

To enable the widget view:

1. Go to *System > Log & Report > Report > 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 to display as widgets.
2. Dr ag 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

Layer7 (App Process per Second)

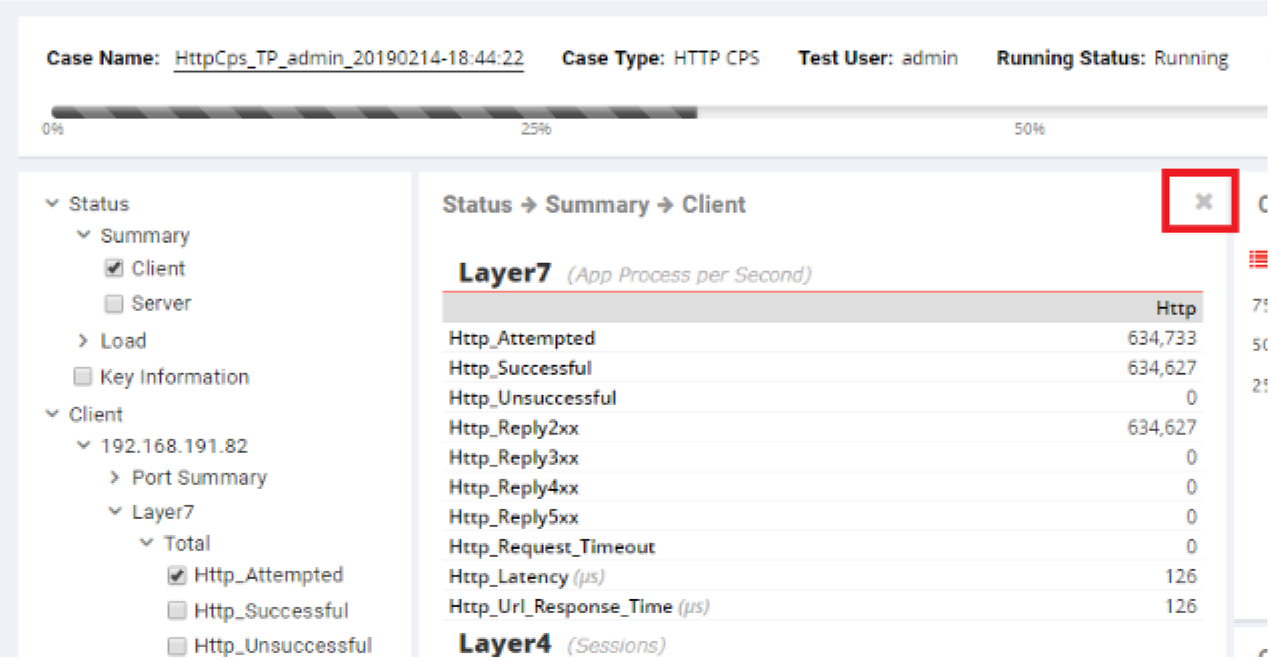
	Http
Http_Attempted	636,928
Http_Successful	636,911
Http_Unsuccessful	0
Http_Reply2xx	636,911
Http_Reply3xx	0
Http_Reply4xx	0
Http_Reply5xx	0
Http_Request_Timeout	0
Http_Latency (μs)	125
Http_Url_Response_Time (μs)	125

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 to exclude from the widget view.
2. Alternatively, 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

Layer7 *(App Process per Second)*

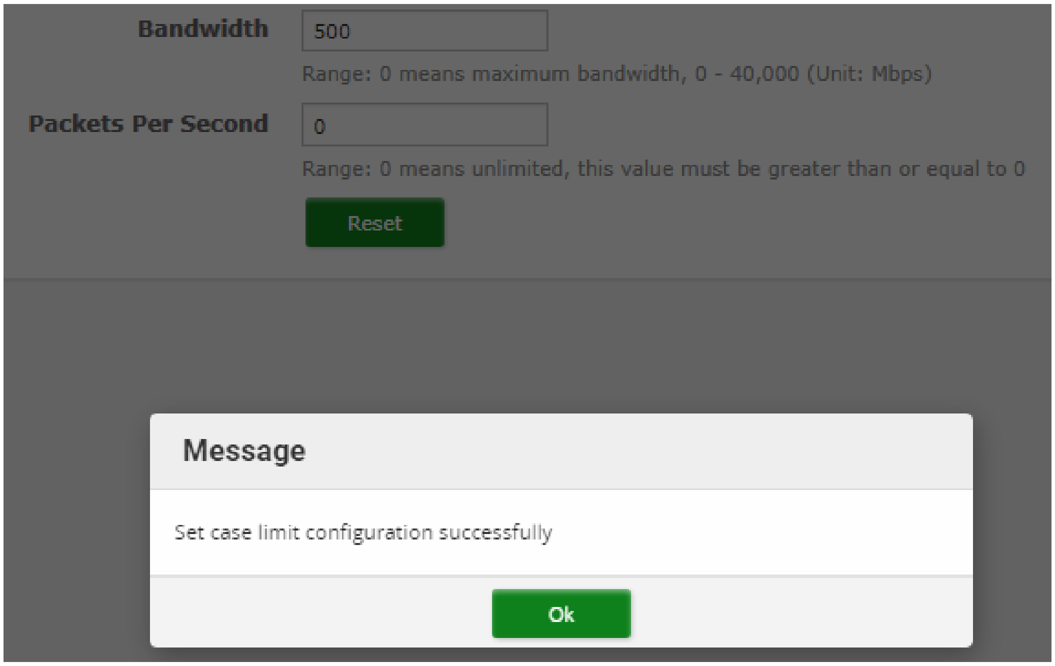
	Http
Http_Attempted	634,733
Http_Successful	634,627
Http_Unsuccessful	0
Http_Reply2xx	634,627
Http_Reply3xx	0
Http_Reply4xx	0
Http_Reply5xx	0
Http_Request_Timeout	0
Http_Latency *(µs)*	126
Http_Url_Response_Time *(µs)*	126

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, set *Packets per Second* to `500`.
3. Click *Reset*.
   The "Set case limit configuration successfully" message displays.



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

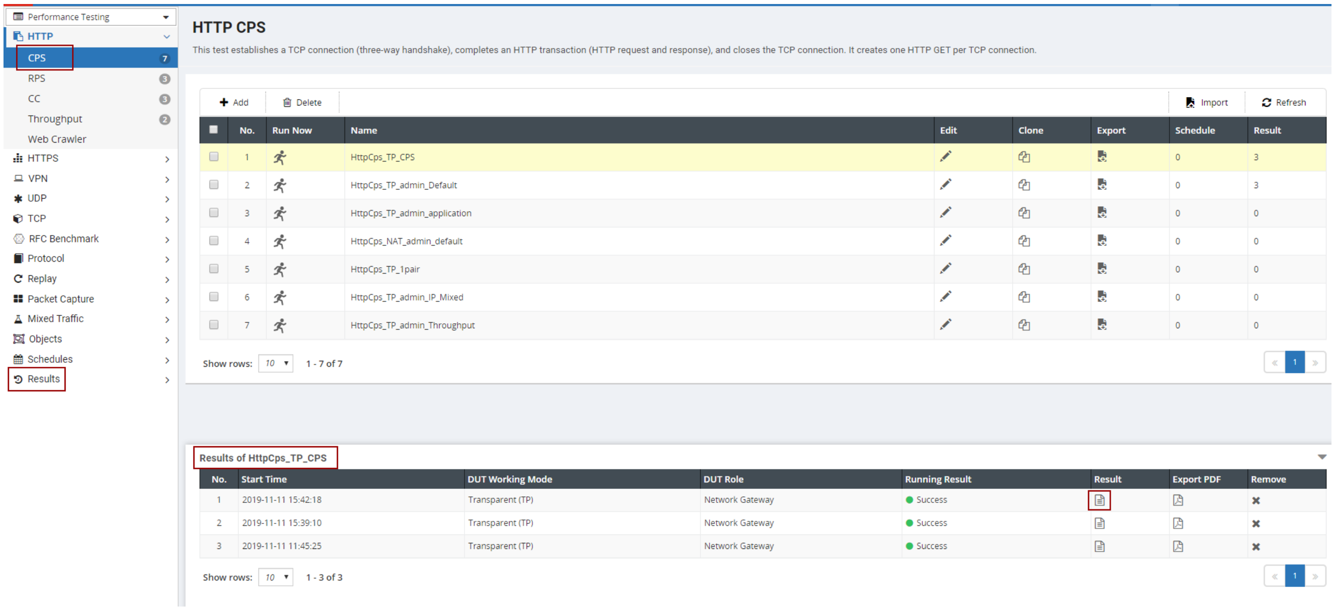
Message

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

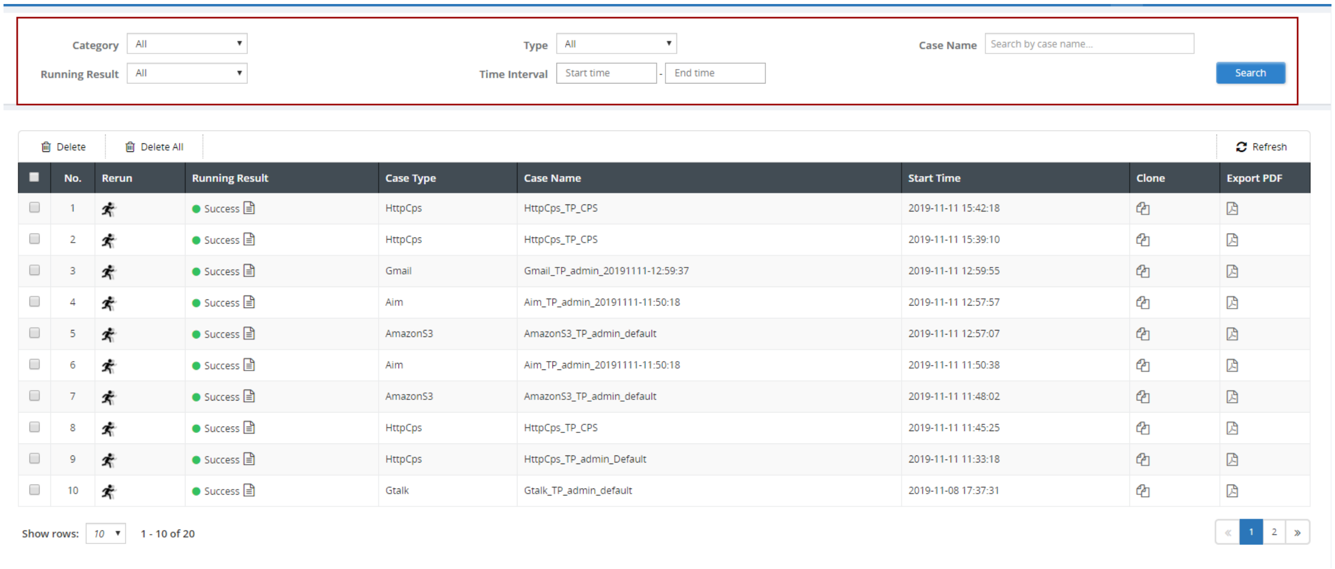
Show rows: 10 1 - 7 of 7

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.



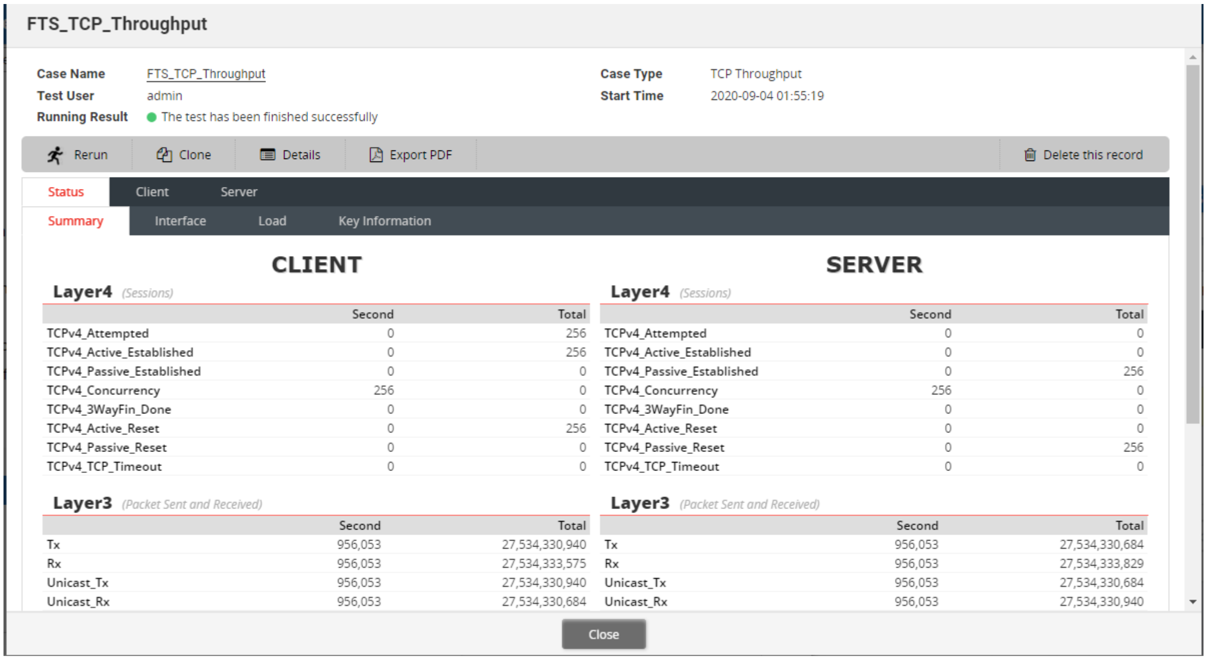
Category: All
Type: All
Case Name: Search by case name...
Running Result: All
Time Interval: Start time - End time

☐	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 a throughput test



FTS_TCP_Throughput

Case Name: FTS_TCP_Throughput
Test User: admin
Running Result: ● The test has been finished successfully
Case Type: TCP Throughput
Start Time: 2020-09-04 01:55:19

CLIENT

Layer4 (Sessions)

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

Layer3 (Packet Sent and Received)

	Second	Total
Tx	956,053	27,534,330,940
Rx	956,053	27,534,333,575
Unicast_Tx	956,053	27,534,330,940
Unicast_Rx	956,053	27,534,330,684

SERVER

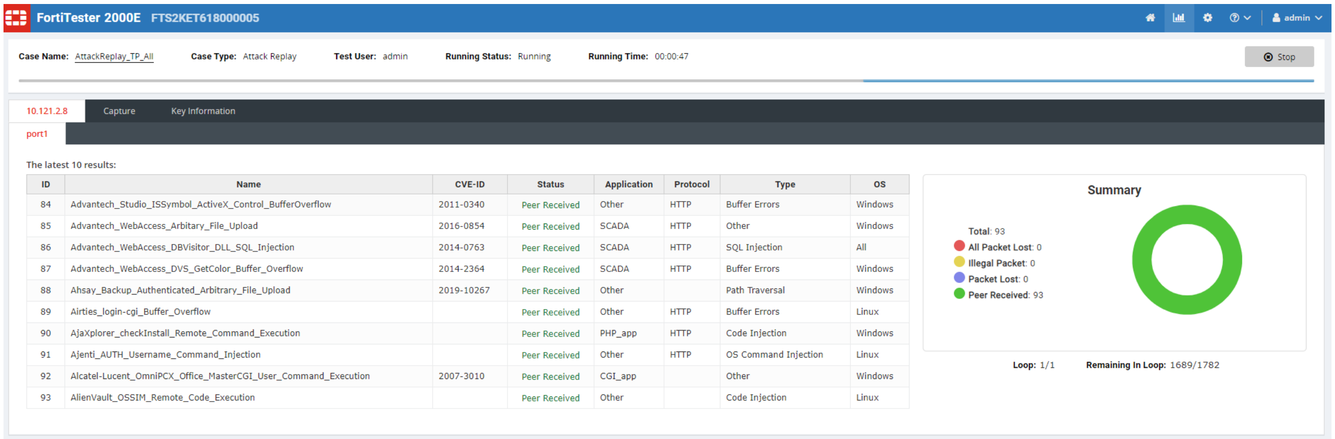
Layer4 (Sessions)

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

Layer3 (Packet Sent and Received)

	Second	Total
Tx	956,053	27,534,330,684
Rx	956,053	27,534,333,829
Unicast_Tx	956,053	27,534,330,684
Unicast_Rx	956,053	27,534,330,940

Attack replay test



Case Name: AttackReplay_TP_All **Case Type:** Attack Replay **Test User:** admin **Running Status:** Running **Running Time:** 00:00:47

The latest 10 results:

ID	Name	CVE-ID	Status	Application	Protocol	Type	OS
84	Advantech_Studio_ISSymbol_ActiveX_Control_BufferOverflow	2011-0340	Peer Received	Other	HTTP	Buffer Errors	Windows
85	Advantech_WebAccess_Arbitary_File_Upload	2016-0854	Peer Received	SCADA	HTTP	Other	Windows
86	Advantech_WebAccess_DBVisitor_DLL_SQL_Injection	2014-0763	Peer Received	SCADA	HTTP	SQL Injection	All
87	Advantech_WebAccess_DVS_GetColor_Buffer_Overflow	2014-2364	Peer Received	SCADA	HTTP	Buffer Errors	Windows
88	Ahsay_Backup_Authenticated_Arbitrary_File_Upload	2019-10267	Peer Received	Other		Path Traversal	Windows
89	Airties_login-cgi_Buffer_Overflow		Peer Received	Other	HTTP	Buffer Errors	Linux
90	AjaXplorer_checkInstall_Remote_Command_Execution		Peer Received	PHP_app	HTTP	Code Injection	Windows
91	Ajenti_AUTH_Username_Command_Injection		Peer Received	Other	HTTP	OS Command Injection	Linux
92	Alcatel-Lucent_OmniPCX_Office_MasterCGI_User_Command_Execution	2007-3010	Peer Received	CGI_app		Other	Windows
93	AlienVault_OSSIM_Remote_Code_Execution		Peer Received	Other		Code Injection	Linux

Summary

Total: 93
🔴 All Packet Lost: 0
🟡 Illegal Packet: 0
🔵 Packet Lost: 0
🟢 Peer Received: 93

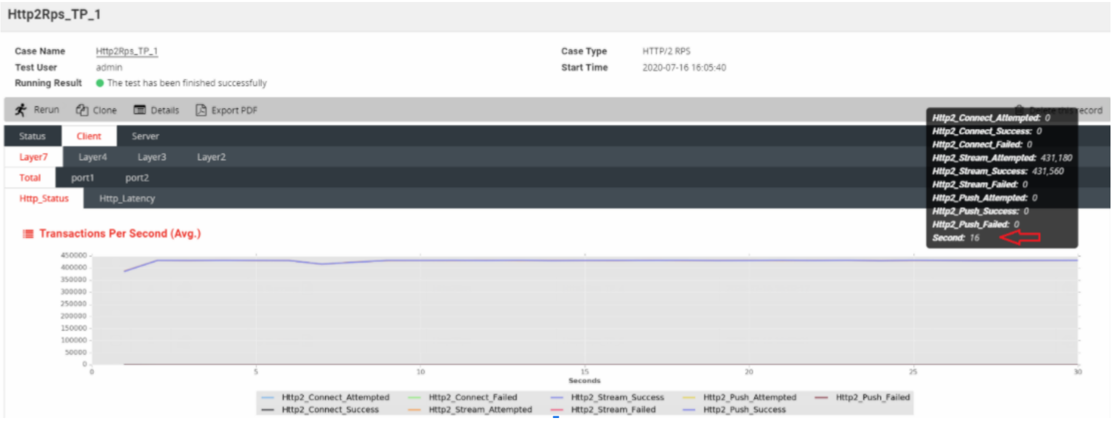
Loop: 1/1 **Remaining In Loop:** 1689/1782

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.

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

Display the second text by hovering the mouse over the picture in the *Client* tab.



Http2Rps_TP_1

Case Name	Http2Rps_TP_1	Case Type	HTTP/2 RPS
Test User	admin	Start Time	2020-07-16 16:05:40
Running Result	● The test has been finished successfully		

Http2_Connect_Attempted: 0
Http2_Connect_Success: 0
Http2_Connect_Failed: 0
Http2_Stream_Attempted: 431,180
Http2_Stream_Success: 431,560
Http2_Stream_Failed: 0
Http2_Push_Attempted: 0
Http2_Push_Success: 0
Http2_Push_Failed: 0
Second: 16

Subnet statistics

FortiTester can calculate and display statistics based on subnets.

1. In *System > Log & Report > Report > Report Settings*, enable *Subnet statistics*.
2. Run a case and view subnet statistics in the *Client* or *ServerPort Summary* tab.

3. Use the dropdown for each port to display statistics for different subnets.

Exporting and 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.

Use the *Export* and *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 specified time. 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 *+ Create New* 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 in progress.

Performance testing

In *Performance Testing*, configure and run the following cases to test device performance:

- HTTP
- HTTPS
- HTTP/2
- VPN
- UDP
- TCP
- DNS
- RFC Benchmark
- Protocol
- Application
- Replay
- Packet Capture
- Mixed Traffic

The description of each test case includes the configuration options specific to that case. For configuration options common to all test cases, see Test case configuration overview on page 25.

HTTP cases

The following types of HTTP cases are available:

- CPS
- RPS
- CC
- Throughput

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. In *Performance Testing*, expand *HTTP* and click *CPS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Click *OK*.
5. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP CPS test case options

For details about the common options for HTTP cases, see HTTP Test Case common options on page 49.

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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
Client Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, *HTTP 1.1* will have backward compatibility with *HTTP 1.0*.
Keep Alive	Enable to add `keepalive` header. Only available when *Protocol Level* is *HTTP 1.0*.

Settings	Guidelines
Piggyback Get Requests	If enabled, an acknowledgment is sent on the data frame, instead of in an individual frame. Otherwise, the client sends an ACK frame individually. This feature only works with GET and POST requests.
Server Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, *HTTP 1.1* will have backward compatibility with *HTTP 1.0*.
Keep Alive	Enable to add `keepalive` header. Only available when *Protocol Level* is *HTTP 1.0*.
Client Limit	
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 in *Client > Limit* tab.
Action	
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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

Starting an HTTP RPS test

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

To start an HTTP RPS test:

1. In *Performance Testing*, expand *HTTP* and click *RPS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Click *OK*.
5. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP RPS test case options

For details about the common options for HTTP cases, see HTTP Test Case common options on page 49.

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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
Client > Limit	
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 *Client > Limit* tab.
Action	
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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

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. In *Performance Testing*, expand *HTTP* and click *CC*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Click *OK*.
5. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP CC test case options

For details about the common options for HTTP cases, see HTTP Test Case common options on page 49.

Settings	Guidelines
Load	
Maximum Concurrent Connections	Determines the maximum number of concurrent TCP connections supported through or with the DUT/SUT. This test is intended to find the maximum number of entries the DUT/SUT can store in its connection table.
Think Time	The delay between client HTTP requests, in seconds.
Reconnect Connections	Restart or renew sessions that fail due to DUT. Failed sessions will be restarted or renewed automatically when the case is running.

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. In *Performance Testing*, expand *HTTP* and click *Throughput*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Click *OK*.
5. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP Throughput test case options

For details about the common options for HTTP cases, see HTTP Test Case common options on page 49.

Starting an HTTP Real Life test

FortiTestersupports the scenario of maintaining fixed number of TCP sessions while simultaneously setting up and tearing down additional TCP sessions. HTTP traffic is sent in each TCP session.

To start an HTTP Real Life test:

1. In *Performance Testing*, expand *HTTP* and click *Real Life*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Click *OK*.
5. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP Real Life test case options

For details about the common options for HTTP cases, see HTTP Test Case common options on page 49.

HTTP Test Case common options

Use this page as a generic for information that is common to all HTTP case configurations. Anything specific to the case itself will be found within the case's page, i.e. HTTP RPS test specifics will be found under the HTTP RPS document page.

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.
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.

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.
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 for the description of network settings.	
Load	
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 per Second	Rate of new connections per second. The value must be greater than 0. Available only when Connections/second is selected for Mode.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
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**.
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

Settings	Guidelines
	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.
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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
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 URL Group to configure/reuse a URL host group object of up to 1000 URLs. To configure a URL Group object, go to **Performance Testing > Objects > URL Groups**. **NOTE:** You can add URL Group hosts using existing Host Groups. **NOTE:** After being created, this imported Host Group has no relationship with the URL Group anymore.
POST Content	Select the POST content to use in requests. The file objects used here must first be created under *Performance Testing > Objects > Files*.
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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

HTTPS cases

The following types of HTTPS cases are available:

- CPS
- RPS
- CC
- Throughput

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. Additionaly, the MTU is editable.

To start an HTTPS CPS test:

1. In *Performance Testing*, expand *HTTPS* and click *CPS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTPS CPS test case options

For details about the common options for HTTPS cases, see HTTPS test case common options on page 58.

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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
Client Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, *HTTP 1.1* will have backward compatibility with *HTTP 1.0*.
Keep Alive	Enable to add `keepalive` header. Only available when *Protocol Level* is *HTTP 1.0*.
Server Profile	
Protocol Level	Select HTTP version. If you select different HTTP versions for client and server, *HTTP 1.1* will have backward compatibility with *HTTP 1.0*.
Keep Alive	Enable to add `keepalive` header. Only available when *Protocol Level* is *HTTP 1.0*.

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. In *Performance Testing*, expand *HTTPS* and click *RPS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTPS RPS test case options

For details about the common options for HTTPS cases, see HTTPS test case common options on page 58.

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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
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.

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. In *Performance Testing*, expand *HTTPS* and click *CC*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTPS CC test case options

For details about the common options for HTTPS cases, see HTTPS test case common options on page 58.

Settings	Guidelines
Load	
Maximum Concurrent Connections	Determines the maximum number of concurrent TCP connections supported through or with the DUT/SUT. This test is intended to find the maximum number of entries the DUT/SUT can store in its connection table.
Think Time	The delay between client HTTP requests (unit: second).
Reconnect Connections	Restart or renew sessions that fail due to DUT. Failed sessions will be restarted or renewed automatically when the case is running.

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. In *Performance Testing*, expand *HTTPS* and click *Throughput*.
2. Click *Create New*.

3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTPS Throughput test case options

For details about the common options for HTTPS cases, see HTTPS test case common options on page 58.

Starting an HTTPS Real Life test

The HTTPS Real Life supports the scenario of maintaining fixed number of TCP sessions while simultaneously setting up and tearing down additional TCP sessions. HTTPS traffic is sent in each TCP session.

To start an HTTPS Real Life test:

1. In *Performance Testing*, expand *HTTPS* and click *Real Life*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTPS Real Life test case options

For details about the common options for HTTPS cases, see HTTPS test case common options on page 58.

HTTPS test case common options

Use this page as a generic for information that is common to all HTTPS case configurations. Anything specific to the case itself will be found within the case's page, i.e. HTTPS RPS test specifics will be found under the HTTPS RPS document page.

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.
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.
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.
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 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.

Settings	Guidelines
Connections per Second	Rate of new connections per second. The value must be greater than 0. If the user wants FortiTester to create connections as fast as possible, the user should set the Mode to Simulated Users. Available only when Connections/second is selected for Mode.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
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**.
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.

Settings	Guidelines
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 acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
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 >**

Settings	Guidelines
	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.
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.

Settings	Guidelines
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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
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.

Settings	Guidelines
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 URL Group to configure/reuse a URL host group object of up to 1000 URLs. To configure a URL Group object, go to **Performance Testing > Objects > URL Groups**. **NOTE:** You can add URL Group hosts using existing Host Groups. **NOTE:** After being created, this imported Host Group has no relationship with the URL Group anymore.
POST Content	Select the POST content to use in requests. The file objects used here must first be created under *Performance Testing > Objects > Files*.
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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

HTTP/2 cases

The following types of HTTP/2 cases are available:

- CPS
- RPS
- CC

- Throughput

Starting an HTTP/2 CPS test

This test establishes a TCP connection (three-way handshake), optional SSL connection (handshake), completes an HTTP/2 transaction (HTTP/2 request and response), and closes the TCP connection (Reset). It creates one HTTP/2 GET per TCP connection.

To start an HTTP/2 CPS test:

1. In *Performance Testing*, expand *HTTP/2* and click *CPS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP/2 CPS test case options

For details about the common options for HTTP/2 cases, see HTTP/2 test case common options on page 69.

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. **NOTE:** Available only for CPS and RPS. **NOTE:** If the user wants FortiTester to create connections as fast as possible, the user should set the Mode to Simulated Users.

Settings	Guidelines
	What is the difference between Simuser and Connections/second?
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.

Starting an HTTP/2 RPS test

This test establishes a TCP connection (three-way handshake), optional SSL connection (handshake), completes multiple HTTP/2 transactions (HTTP/2 request and response), and closes the TCP connection (Reset). It creates multiple HTTPS/2 GET per TCP connection.

To start an HTTP/2 RPS test:

1. In *Performance Testing*, expand *HTTP/2* and click *RPS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP/2 RPS test case options

For details about the common options for HTTP/2 cases, see HTTP/2 test case common options on page 69.

Settings	Guidelines
Load	

Settings	Guidelines
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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
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.

Starting an HTTP/2 CC test

This test establishes a large number of TCP connections (three-way handshake), loops complete HTTP/2 transactions (HTTP/2 request and response), and closes the TCP connection.

To start an HTTP/2 CC test:

1. In *Performance Testing*, expand *HTTP/2* and click *CC*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP/2 CC test case options

For details about the common options for HTTP/2 cases, see HTTP/2 test case common options on page 69.

Settings	Guidelines
Client Profile	
Send Goaway	The GOAWAY frame (type=0x7) is used to initiate shutdown of a connection or to signal serious error conditions.
Max Data Frame Size	The maximum DATA frame payload size that the client can send in bytes.
Max Concurrent Streams per Connection	The maximum concurrent streams per connection that the client allows the DUT to create.
Override Flow Control	Select to enable the HTTP2 flow control fields, Connection Window Size, Stream Window Size, and Send WINDOW_UPDATE.
Connection Window Size	The HTTP2 connection window size that the client can accept in bytes.
Stream Window Size	The HTTP2 stream window size that the client can accept in bytes.
Send WINDOW_UPDATE when remaining window size below	Sends a WINDOW_UPDATE frame when the remaining window size that the server can accept is below the specified number of bytes. This value should be smaller than Connection Window Size and Stream Window Size.
Allow Server Push	Select to allow the server to send additional resources to the client, before the client requests them. If deselected, the server sends resources only upon client request. *Allow Server Push* only exist in *Specifics->Client*.
Server Profile	
Protocol Level	In proxy mode, we can choose HTTP1.1 or HTTP/2 for server side. • HTTP1.1: This means DUT will convert HTTP/2 traffic to HTTP1.1 and forward it to the server. • HTTP/2: This means the backend server supports HTTP/2.
Max Data Frame Size	The maximum DATA frame payload size that the server can send in bytes.

Settings	Guidelines
Max Concurrent Streams per Connection	The maximum concurrent streams per connection that the server allows the DUT (device under test) to create.
Override Flow Control	Select to enable the HTTP2 flow control fields, Connection Window Size, Stream Window Size, and Send WINDOW_UPDATE.
Connection Window Size	The HTTP2 connection window size that the server can accept in bytes.
Stream Window Size	The HTTP2 stream window size that the server can accept in bytes.
Send WINDOW_UPDATE when remaining window size below	Sends a WINDOW_UPDATE frame when the remaining window size that the client can accept is below the specified number of bytes. This value should be smaller than *Connection Window Size* and *Stream Window Size*.

Starting an HTTP/2 Throughput test

This test establishes a HTTP/2 connection (three-way handshake), loops completed HTTP/2 transactions (HTTP/2 request and response), and closes the HTTP/2 connection (Reset), which determines the maximum throughput (total bits per second "on the wire").

To start an HTTP/2 Throughput test:

1. In *Performance Testing*, expand *HTTP/2* and click *Throughput*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

HTTP/2 Throughput test case options

For details about the common options for HTTP/2 cases, see HTTP/2 test case common options on page 69.

HTTP/2 test case common options

Use this page as a generic for information that is common to all HTTP/2 case configurations. Anything specific to the case itself will be found within the case's page, i.e. HTTP/2 RPS test specifics will be found under the HTTP/2 RPS document page.

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.
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.
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.
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 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.

Settings	Guidelines
	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.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
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.
Concurrent Requests per Connection	Determines the maximum TCP connection establishment rate through or with the DUT/SUT. This test is intended to find the maximum rate the DUT/SUT can update its connection table.
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**.
Send Goaway	The GOAWAY frame (type=0x7) is used to initiate shutdown of a connection or to signal serious error conditions.
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.
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).

Settings	Guidelines
	• 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.
Piggyback Get Requests	If enabled, this means an acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
Max Data Frame Size	The maximum DATA frame payload size that the client can send in bytes.
Max Concurrent Streams per Connection	The maximum concurrent streams per connection that the client allows the DUT to create.
Override Flow Control	Select to enable the HTTP2 flow control fields, Connection Window Size, Stream Window Size, and Send WINDOW_UPDATE.
Connection Window Size	The HTTP2 connection window size that the client can accept in bytes.
Stream Window Size	The HTTP2 stream window size that the client can accept in bytes.
Send WINDOW_UPDATE when remaining window size below	Sends a WINDOW_UPDATE frame when the remaining window size that the server can accept is below the specified number of bytes. **NOTE:** This value should be smaller than Connection Window Size and Stream Window Size.
Allow Server Push	Select to allow the server to send additional resources to the client, before the client requests them. If deselected, the server sends resources only upon client request. **NOTE: Allow Server Push** only exists in **Specifics->Client**.
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.
Protocol Level	In proxy mode, we can choose HTTP1.1 or HTTP/2 for server side. • HTTP1.1: This means DUT will convert HTTP/2 traffic to HTTP1.1

Settings	Guidelines
	and forward it to the server. - HTTP/2: This means the backend server supports HTTP/2.
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
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.
Max Data Frame Size	The maximum DATA frame payload size that the server can send in bytes.
Max Concurrent Streams per Connection	The maximum concurrent streams per connection that the server allows the DUT (device under test) to create.
Override Flow Control	Select to enable the HTTP2 flow control fields, Connection Window Size, Stream Window Size, and Send WINDOW_UPDATE.
Connection Window Size	The HTTP2 connection window size that the server can accept in bytes.
Stream Window Size	The HTTP2 stream window size that the server can accept in bytes.
Send WINDOW_UPDATE when remaining window size below	Sends a WINDOW_UPDATE frame when the remaining window size that the client can accept is below the specified number of bytes. **NOTE:** This value should be smaller than Connection Window Size and Stream Window Size.
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.
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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
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.
Action	
Method	Three methods are available here: GET, POST, and Custom. If you select Custom, you can URL Group to configure/reuse a URL host group object of up to 1000 URLs. To configure a URL Group object, go to **Performance Testing > Objects > URL Groups**. **NOTE:** You can add URL Group hosts using existing Host Groups. **NOTE:** After being created, this imported Host Group has no relationship with the URL Group anymore.
POST Content	Select the POST content to use in requests. The file objects used here must first be created under *Performance Testing > Objects > Files*.
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**.

Settings	Guidelines
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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

VPN cases

The following types of VPN cases are available:

- IPsec Remote Access
- IPsec CC
- IPsec Throughput
- SSL-VPN CPS
- SSL-VPN RPS
- SSL-VPN CC
- SSL-VPN Throughput

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 an IPsec Remote Access test:

1. In *Performance Testing*, expand *IPsec* and click *Remote Access*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

IPsec Remote Access test case options

For details about the common options for IPsec cases, see VPN test case common options on page 96.

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 an IPsec Remote Access CC test:

1. In *Performance Testing*, expand *IPsec* and click *Remote Access CC*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

IPsec Remote Access CC test case options

For details about the common options for IPsec cases, see VPN test case common options on page 96.

Settings	Guidelines
Load	

Settings	Guidelines
Tunnel Concurrent Connection	Specify the number of concurrent connections.
Think Time	The delay between client HTTP requests (unit: second).

Starting an IPsec Throughput test

This test establishes remote access IPsec tunnels, creates a TCP connection for each tunnel, loops HTTP transactions, and finally closes the TCP connections and terminates the tunnels.

To start an IPsec Throughput test:

1. In *Performance Testing*, expand *IPsec* and click *Throughput*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

IPsec Throughput test case options

For details about the common options for IPsec cases, see VPN test case common options on page 96.

Starting an SSL-VPN CPS test

This test establishes a SSL-VPN tunnel connection and completes a full of HTTP transaction through it. It creates one HTTP(FTP) transaction per tunnel.

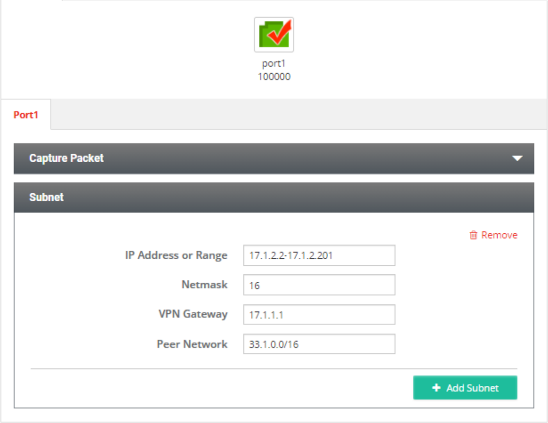
The tunnel is only established if configured in empty tunnel mode.

To start an SSL VPN CPS tunnel test:

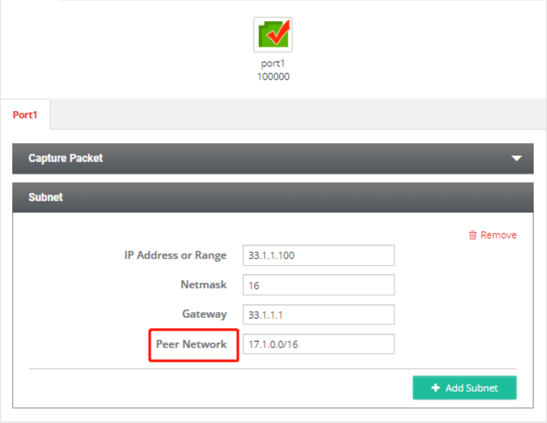
1. Go to *Cases > Performance Testing> VPN > SSLVPN > CPS* to display the test case summary page.
2. Click *+ Create New* to display the *Select case options* dialog box.
3. Configure the Inner Traffic and click *OK* to continue.

HTTP CPS
FTP

4. Set the server network to *Peer Network*.



IP Address or Range: 17.1.2.2-17.1.2.201
Netmask: 16
VPN Gateway: 17.1.1.1
Peer Network: 33.1.0.0/16



IP Address or Range: 33.1.1.100
Netmask: 16
Gateway: 33.1.1.1
Peer Network: 17.1.0.0/16

If FortiGate SSLVPN policy has disabled NAT mode, you need set the Internal IP assigned by FortiGate.

If FortiGate SSLVPN policy has enabled NAT mode, you need to set a peer IP.

5. Set *Specifics* for *Load* and *Client*. See the table below.
6. Set Inner protocol case *Specifics >HTTPCPS*.

Simulated Users	Number of simusers in a Tunnel.

SSL-VPN CPS test case options

For details about the common options for SSL-VPN cases, see VPN test case common options on page 96.

Settings	Guidelines
Basic Information	
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 for the description of network settings.	
Load	

Settings	Guidelines
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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
Tunnel Concurrent Connection	The total number of tunnels created in the Throughput case.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
VPN Gateway Port	Specify the VPN gateway port number.
Enable User Group	Enable to simulate multiple user names. This allows FortiView to populate with more rich user name information, for example. 1. Go to *Objects > User Groups > Create New* to create a user group object. 2. Click *Create New* to create multiple users/password pairs to the current *User Group Object*. 3. In SSL-VPN (CPS/RPS/CC/Throughput) cases, click on the "*Enable User Group*" switch option button and select the User Group created in step 1.
VPN Username	Enter the VPN username.
VPN Password	Enter the VPN password.
Tunnel mode	Select TCP or UDP.
Client Profile	
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.
Available SSL Versions	Select SSL versions.

Settings	Guidelines
	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.
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.
Piggyback Get Requests	If enabled, this means an acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
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

Settings	Guidelines
	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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
Client Network	
Tunnel Mode	Select TCP or UDP.
Server Network	
Network MTU	The maximum transmission unit size.

Starting an SSL-VPN RPS test

This test establishes a SSL-VPN tunnel connection and completes multiple full of HTTP transaction through it. It creates multiple HTTP transaction per tunnel.

To start an SSL-VPN tunnel RPS test:

1. Go to *Cases > Performance Testing> VPN> SSL-VPN > RPS* to display the test case summary page.
2. Click *+ Create New* to display the *Select case options* dialog box.
3. Configure the Inner Traffic and click *OK* to continue.
4. Set the server network to *Peer Network*.

> If FortiGate SSLVPN policy has disabled NAT mode, you need set the Internal IP assigned by FortiGate.
>
> If FortiGate SSLVPN policy has enabled NAT mode, you need to set a peer IP.

5. Set **Specifics** for **Load** and **Client.** See the table below.
6. Set Inner protocol case **Specifics >HTTPCPS**.

Simulated Users	Number of simusers in a Tunnel.

SSL-VPN RPS test case options

For details about the common options for SSL-VPN cases, see VPN test case common options on page 96.

Settings	Guidelines
Basic Information	
VPN Host Group	Specify VPN hosts defined under *Objects > Host Group*. A Host Group is comprised of Hosts e.g. abc.com = 1.1.1.1 . FortiTester will inject the hosts configured into SNI field (server name indication) within the TLS handshake.
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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
Tunnel Concurrent Connection	The total number of tunnels created in the Throughput case.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
Transactions per Tunnel	Number of transactions in a Tunnel
VPN Gateway Port	Specify the VPN gateway port number.
Enable User Group	Enable to simulate multiple user names. This allows FortiView to populate with more rich user name information, for example. 1. Go to *Objects > User Groups > Create New* to create a user group object. 2. Click *Create New* to create multiple users/password pairs to the current *User Group Object*.

Settings	Guidelines
	3. In SSL-VPN (CPS/RPS/CC/Throughput) cases, click *Enable User Group*and select the User Group created in step 1.
VPN Username	Enter the VPN username.
VPN Password	Enter the VPN password.
Tunnel mode	Select TCP or UDP.
Client Profile	
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.
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.
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.
Piggyback Get Requests	If enabled, this means an acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
Client/Server Network	
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
Inner Network MSS	The inner TCP MSS.
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
Tunnels per Second	The rate at which DUT establishes tunnels per second.
HttpCps server profiles	
HttpCps Load	
Simulated Users	Number of users to simulate.
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.
HttpCps Client	
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.
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 acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
HttpCps 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.
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.
HttpCps 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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
HttpCps Server Network	
IP Option DCSP	Provide quality of service (QoS).
HttpCps 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.
HttpCps Action	

Settings	Guidelines
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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

Starting an SSL-VPN 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 CC test:

1. In *Performance Testing*, expand *SSL-VPN* and click *CC*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

SSL-VPN CC test case options

For details about the common options for SSL-VPN cases, see VPN test case common options on page 96.

Settings	Guidelines
Basic Information	
VPN Host Group	Specify VPN hosts defined under *Objects > Host Group*. A Host Group is comprised of Hosts e.g. abc.com = 1.1.1.1 . FortiTester will inject the hosts configured into SNI field (server name indication) within the TLS handshake.
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. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simuser*. For more information, see What is the difference between Connections per Second and Simulated Users? on page 285
Tunnel Concurrent Connection	The total number of tunnels created in the Throughput case.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
Tunnel Concurrent Connection	Specify the number of concurrent connections.
VPN Gateway Port	Specify the VPN gateway port number.

Settings	Guidelines
Enable User Group	Enable to simulate multiple user names. This allows FortiView to populate with more rich user name information, for example. 1. Go to *Objects > User Groups > Create New* to create a user group object. 2. Click *Create New* to create multiple users/password pairs to the current *User Group Object*. 3. In SSL-VPN (CPS/RPS/CC/Throughput) cases, click on the *Enable User Group* switch option button and select the User Group created in step 1.
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 here.
Think Time	The delay between client HTTP requests (unit: second).
Client Network	
Tunnel Mode	Select TCP or UDP.

Starting an SSL-VPN Real Life test

This test establishes a SSL-VPN tunnel connection, loops completed HTTP/TCP/UDP transaction and closes the tunnel.

To start an SSL-VPN Real Life test:

1. Go to *Cases > Performance Testing> VPN > SSL-VPN > Throughput* to display the test case summary page.
2. Click *Create New*.
3. Set *Inner Traffic* and click *OK* to continue.
4. Set the server network to *Peer Network*.

> If the FortiGate SSL-VPN policy has disabled NAT mode, you need to set the Internal IP assigned by FortiGate.
>
> If the FortiGate SSL-VPN policy has enabled NAT mode, you need to set a peer IP.

5. Set *Specifics*. See the table below.
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.

SSL-VPN Real Life test case options

For details about the common options for SSL-VPN cases, see VPN test case common options on page 96.

Settings	Guidelines
Basic Information	
VPN Host Group	Specify VPN hosts defined under *Objects > Host Group*. A Host Group is comprised of Hosts e.g. abc.com = 1.1.1.1 . FortiTester will inject the hosts configured into SNI field (server name indication) within the TLS handshake.
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. **NOTE:** Available only for CPS and RPS. **NOTE:** If you want FortiTester to create connections as fast as possible, set *Mode* to *Simulated Users*. What is the difference between Simuser and Connections/second?
Tunnel Concurrent Connection	The total number of tunnels created in the throughput case.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the *Connections per Second* configured during the specified *Ramp Up Time*, it will keep the highest CPS it reached during the *Ramp Up Time*.
Ramp Down Time	The duration in seconds during which the device ramps down the number of connections it is making. 0 will cause FortiTester to cease generating sessions. (Range: 0 - 300).
Transactions per Tunnel	Number of transactions in a Tunnel
VPN Gateway Port	Specify the VPN gateway port number.
Enable User Group	Enable to simulate multiple user names. This allows FortiView to populate with more rich user name information, for example. 1. Go to *Objects > User Groups > Create New* to create

Settings	Guidelines
	a user group object. 2. Click *Create New* to create multiple user/password pairs in the current *User Group Object*. 3. In SSL-VPN (CPS/RPS/CC/Throughput) cases, enable *Enable User Group* and select the *User Group* created in step 1.
VPN Username	Enter the VPN username.
VPN Password	Enter the VPN password.
Tunnel mode	Select TCP or UDP.
Client Profile	
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.
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.
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.
Piggyback Get Requests	If enabled, this means an acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
Client 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.

Settings	Guidelines
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
Client Network	
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
Inner Network MSS	The inner TCP MSS.
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.
Tunnels per Second	The rate at which DUT establishes tunnels per second.
HttpThroughput profiles	
HttpThroughput Load	
Simulated Users	Number of users to simulate.
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.
HttpThroughput Client	
HttpThroughput 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*.
HttpThroughput Server Profile	
Case Server Port	The server port where the test case traffic arrives.
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.

Settings	Guidelines
HttpThroughput Server Network	
IP Option DCSP	Provide quality of service (QoS).
HttpThroughput 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.
HttpThroughput 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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

VPN test case common options

Use this page as a generic for information that is common to all VPN case configurations. Anything specific to the case itself will be found within the case's page, i.e. VPN RPS test specifics will be found under the VPN RPS document page.

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 Scripts on page 187.
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.
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.
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.
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 25 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

Settings	Guidelines
	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.
Enable EMS-SN	Enable or disable EMS-SN then enter the FortiClient EMS serial number.
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.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

UDP cases

The following types of UDP cases are available:

- UDP PPS
- UDP Payload

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. In *Performance Testing*, expand *UDP* and click *PPS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

UDP PPS test case options

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.
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.
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.
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 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 or iMIX 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.

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 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. In *Performance Testing*, expand *UDP* and click *Payload*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

UDP payload test case options

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.
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.
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.
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 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	

Settings	Guidelines
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.

TCP cases

The following types of TCP cases are available:

- TCP Throughput
- TCP Turbo
- TCP Connection

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. In *Performance Testing*, expand *TCP* and click *Throughput*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.

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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP throughput test case options

For details about the common options for TCP cases, see TCP Test Case common options on page 106.

Starting a TCP 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 TCP TurboTCP test:

1. In *Performance Testing*, expand *TCP* and click *TurboTCP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP TurboTCP test case options

For details about the common options for TCP cases, see TCP Test Case common options on page 106.

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.
TurboTcp Buffer Size	The size of the buffer sent to server when the TCP connection is established.
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.

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. In *Performance Testing*, expand *TCP* and click *Connection*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP connection test case options

For details about the common options for TCP cases, see TCP Test Case common options on page 106.

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 for the description of network settings.	
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 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.

TCP Test Case common options

Use this page as a generic for information that is common to all TCP case configurations. Anything specific to the case itself will be found within the case's page. For example, TCP RPS test specifics will be found under the TCP RPS page.

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.
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.
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.
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 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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
Out of Order Reset	If enabled, FortiTester will send Reset packet to close the TCP session which has occurred in the out of order sequence. Enabling this option sets the "Out of Order Reset" flag in both client and server sides for TCP Options.
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.

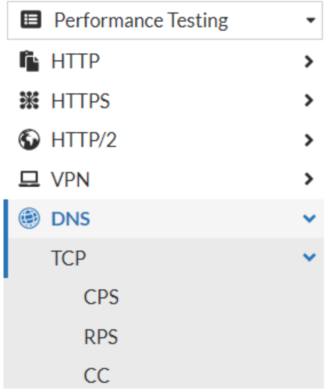
DNS cases

What is DoT?

DNS over TLS (DoT) is a network security protocol for encrypting and wrapping Domain Name System (DNS) queries and answers using the Transport Layer Security (TLS) protocol. The goal of this method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data through man-in-the-middle attacks. The well-known port number for DoT is 853.

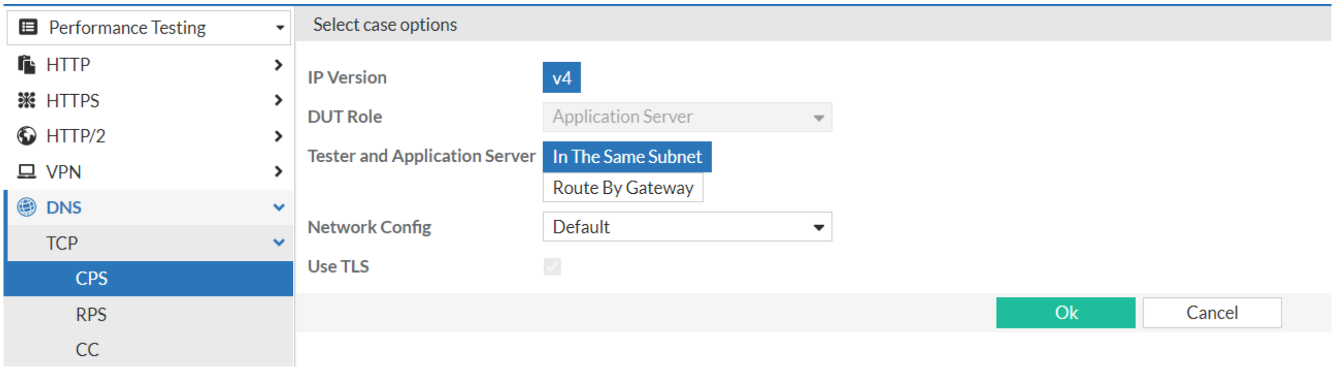
Where to find the DoT Case in the GUI?

Go to *Performance Testing>Protocol>DNS>TCP*.



How does DoT case work?

Currently, the application server is only supported in the DUT role. The DoT case only simulates the DNS client that sends the DNS queries.



Select case options

IP Version: v4

DUT Role: Application Server

Tester and Application Server: In The Same Subnet / Route By Gateway

Network Config: Default

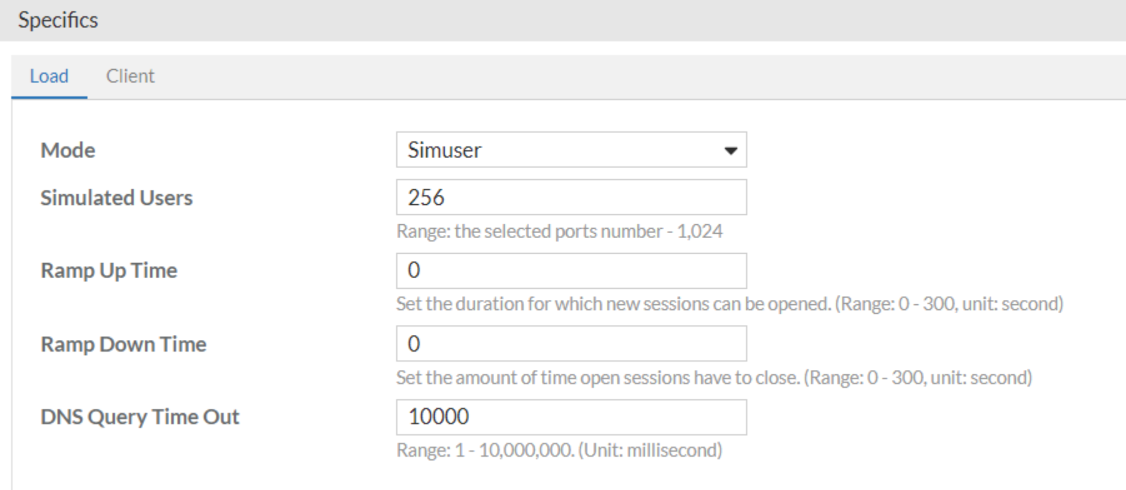
Use TLS: ☑

The Bind9 SDNS server and FDN SDNS server can be used as the DNS server side for the DoT case.

Key configurations

Mode (DoT CPS/RPS)

If you select *Simuser* (CPS/RPS/CC), FortiTester simulates users 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.



Specifics

Mode: Simuser

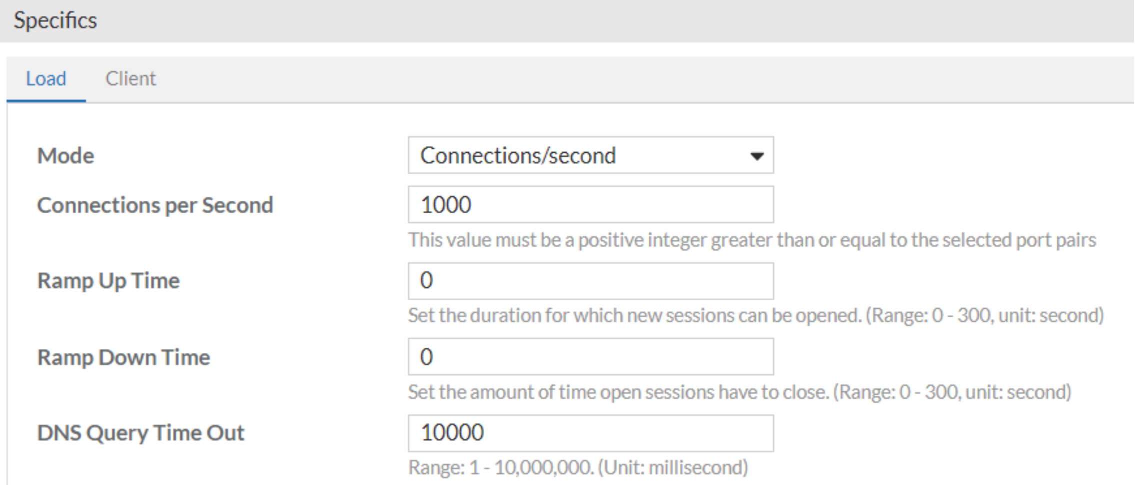
Simulated Users: 256
Range: the selected ports number - 1,024

Ramp Up Time: 0
Set the duration for which new sessions can be opened. (Range: 0 - 300, unit: second)

Ramp Down Time: 0
Set the amount of time open sessions have to close. (Range: 0 - 300, unit: second)

DNS Query Time Out: 10000
Range: 1 - 10,000,000. (Unit: millisecond)

If you select *Connections/second* (CPS/RPS), FortiTester simulates TCP connections, each of them containing up to hundreds of transactions. It is useful to test how many concurrent connections can be handled by your device.



Specifics

Mode: Connections/second

Connections per Second: 1000
This value must be a positive integer greater than or equal to the selected port pairs

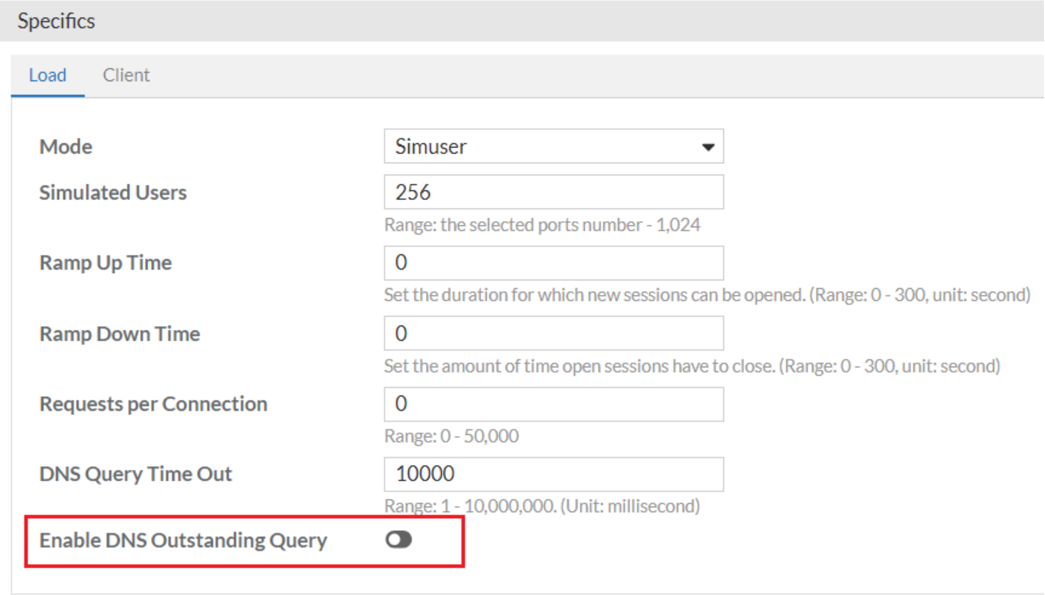
Ramp Up Time: 0
Set the duration for which new sessions can be opened. (Range: 0 - 300, unit: second)

Ramp Down Time: 0
Set the amount of time open sessions have to close. (Range: 0 - 300, unit: second)

DNS Query Time Out: 10000
Range: 1 - 10,000,000. (Unit: millisecond)

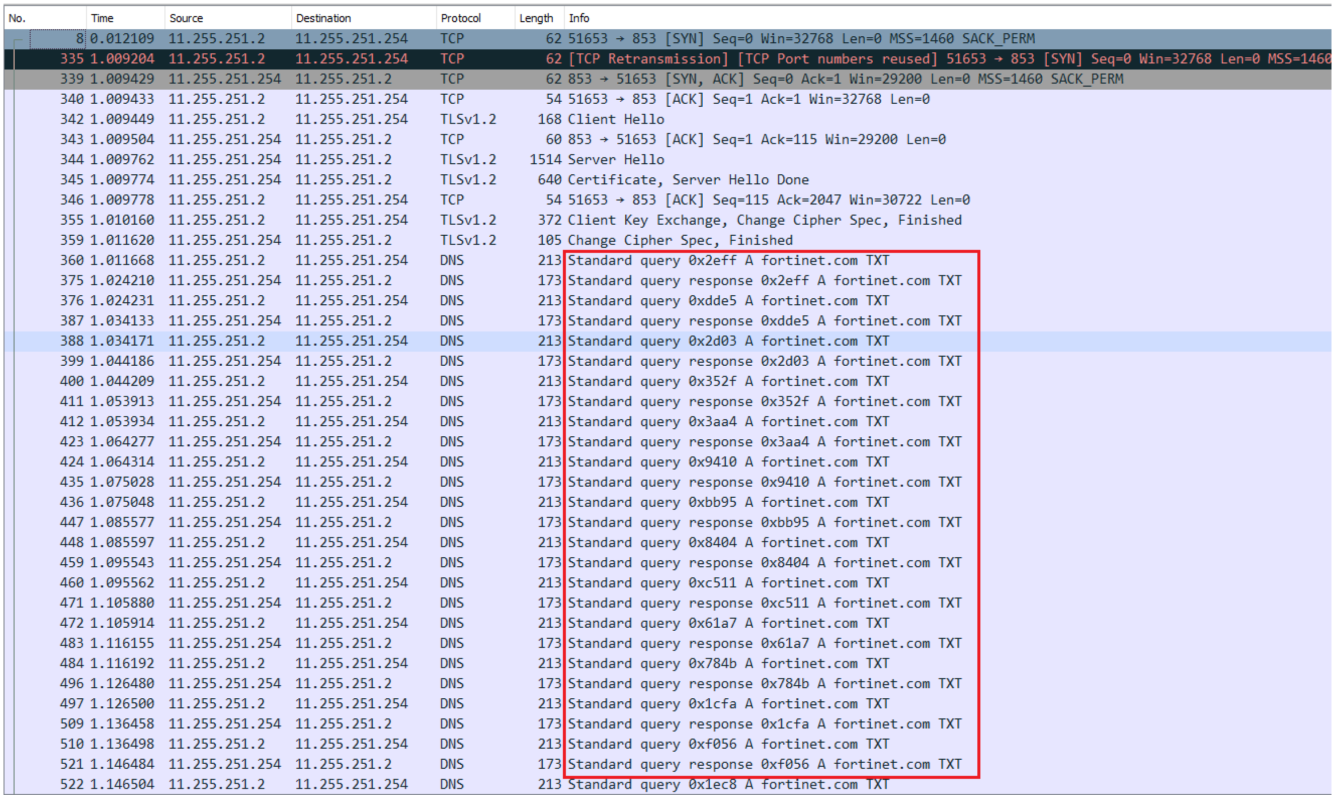
Enable DNS Outstanding Query (DoT RPS)

The *Enable DNS Outstanding Query* toggle button allows multiple DNS queries to be sent in parallel. By default, this option is disabled, and one DNS query is sent at a time; FortiTester waits for the DNS answer before sending the next DNS query.



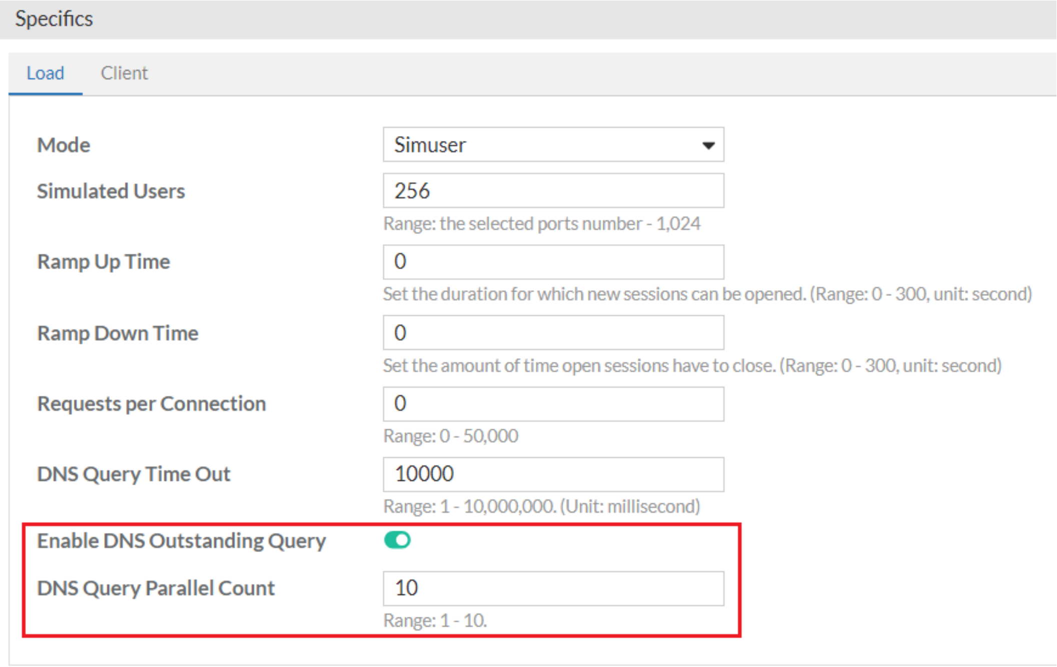
Specifics

Mode	Simuser
Simulated Users	256 Range: the selected ports number - 1,024
Ramp Up Time	0 Set the duration for which new sessions can be opened. (Range: 0 - 300, unit: second)
Ramp Down Time	0 Set the amount of time open sessions have to close. (Range: 0 - 300, unit: second)
Requests per Connection	0 Range: 0 - 50,000
DNS Query Time Out	10000 Range: 1 - 10,000,000. (Unit: millisecond)
Enable DNS Outstanding Query	○



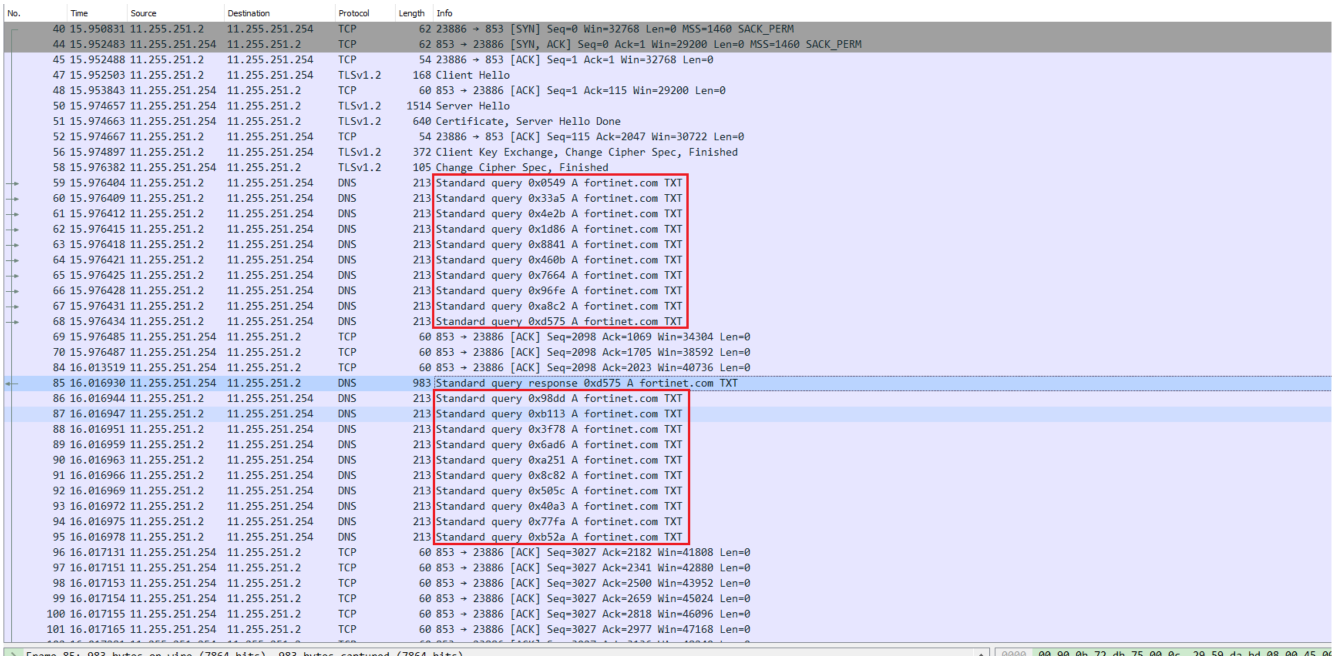
```
No.     Time     Source          Destination     Protocol  Length Info
      8 0.012109 11.255.251.2    11.255.251.254  TCP         62 51653 → 853 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PERM
    335 1.009204 11.255.251.2    11.255.251.254  TCP         62 [TCP Retransmission] [TCP Port numbers reused] 51653 → 853 [SYN] Seq=0 Win=32768 Len=0 MSS=1460
    339 1.009429 11.255.251.254  11.255.251.2    TCP         62 853 → 51653 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
    340 1.009433 11.255.251.2    11.255.251.254  TCP         54 51653 → 853 [ACK] Seq=1 Ack=1 Win=32768 Len=0
    342 1.009449 11.255.251.2    11.255.251.254  TLSv1.2    168 Client Hello
    343 1.009504 11.255.251.254  11.255.251.2    TCP         60 853 → 51653 [ACK] Seq=1 Ack=115 Win=29200 Len=0
    344 1.009762 11.255.251.254  11.255.251.2    TLSv1.2   1514 Server Hello
    345 1.009774 11.255.251.254  11.255.251.2    TLSv1.2    640 Certificate, Server Hello Done
    346 1.009778 11.255.251.2    11.255.251.254  TCP         54 51653 → 853 [ACK] Seq=115 Ack=2047 Win=30722 Len=0
    355 1.010160 11.255.251.2    11.255.251.254  TLSv1.2    372 Client Key Exchange, Change Cipher Spec, Finished
    359 1.011620 11.255.251.254  11.255.251.2    TLSv1.2    105 Change Cipher Spec, Finished
    360 1.011668 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x2eff A fortinet.com TXT
    375 1.024210 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x2eff A fortinet.com TXT
    376 1.024231 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xdde5 A fortinet.com TXT
    387 1.034133 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0xdde5 A fortinet.com TXT
    388 1.034171 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x2d03 A fortinet.com TXT
    399 1.044186 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x2d03 A fortinet.com TXT
    400 1.044209 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x352f A fortinet.com TXT
    411 1.053913 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x352f A fortinet.com TXT
    412 1.053934 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x3aa4 A fortinet.com TXT
    423 1.064277 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x3aa4 A fortinet.com TXT
    424 1.064314 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x9410 A fortinet.com TXT
    435 1.075028 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x9410 A fortinet.com TXT
    436 1.075048 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xbb95 A fortinet.com TXT
    447 1.085577 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0xbb95 A fortinet.com TXT
    448 1.085597 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x8404 A fortinet.com TXT
    459 1.095543 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x8404 A fortinet.com TXT
    460 1.095562 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xc511 A fortinet.com TXT
    471 1.105880 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0xc511 A fortinet.com TXT
    472 1.105914 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x61a7 A fortinet.com TXT
    483 1.116155 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x61a7 A fortinet.com TXT
    484 1.116192 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x784b A fortinet.com TXT
    496 1.126480 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x784b A fortinet.com TXT
    497 1.126500 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x1cfa A fortinet.com TXT
    509 1.136458 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0x1cfa A fortinet.com TXT
    510 1.136498 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xf056 A fortinet.com TXT
    521 1.146484 11.255.251.254  11.255.251.2    DNS        173 Standard query response 0xf056 A fortinet.com TXT
    522 1.146504 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x1ec8 A fortinet.com TXT
```

If you enable *Enable DNS Outstanding Query*, you need to enter the *DNS Query Parallel Count* value so that this number of DNS queries can be sent in parallel.



Mode	Simuser
Simulated Users	256 Range: the selected ports number - 1,024
Ramp Up Time	0 Set the duration for which new sessions can be opened. (Range: 0 - 300, unit: second)
Ramp Down Time	0 Set the amount of time open sessions have to close. (Range: 0 - 300, unit: second)
Requests per Connection	0 Range: 0 - 50,000
DNS Query Time Out	10000 Range: 1 - 10,000,000. (Unit: millisecond)
Enable DNS Outstanding Query	●
DNS Query Parallel Count	10 Range: 1 - 10.

Pcap shows that 10 DNS queries are sent together in parallel, FortiTester waits for the response, then the next group of 10 DNS queries are sent to the server.

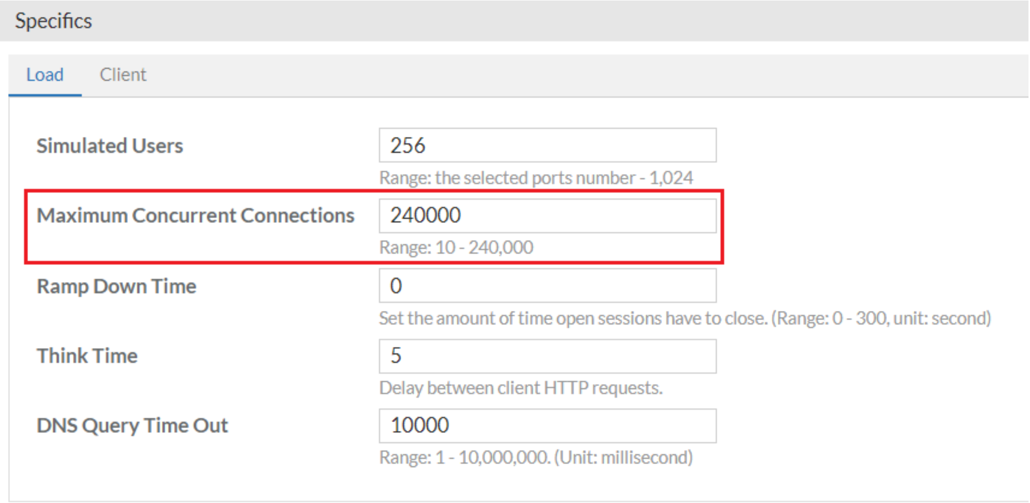


```
No.   Time      Source          Destination     Protocol  Length Info
   40 15.950831 11.255.251.2    11.255.251.254  TCP         62 23886 → 853 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PERM
   44 15.952483 11.255.251.254  11.255.251.2    TCP         62 853 → 23886 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
   45 15.952488 11.255.251.2    11.255.251.254  TCP         54 23886 → 853 [ACK] Seq=1 Ack=1 Win=32768 Len=0
   47 15.952503 11.255.251.2    11.255.251.254  TLSv1.2    168 Client Hello
   48 15.953843 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=1 Ack=115 Win=29200 Len=0
   50 15.974657 11.255.251.254  11.255.251.2    TLSv1.2   1514 Server Hello
   51 15.974663 11.255.251.254  11.255.251.2    TLSv1.2    640 Certificate, Server Hello Done
   52 15.974667 11.255.251.2    11.255.251.254  TCP         54 23886 → 853 [ACK] Seq=115 Ack=2047 Win=30722 Len=0
   56 15.974897 11.255.251.2    11.255.251.254  TLSv1.2    372 Client Key Exchange, Change Cipher Spec, Finished
   58 15.976382 11.255.251.254  11.255.251.2    TLSv1.2    105 Change Cipher Spec, Finished
   59 15.976404 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x0549 A fortinet.com TXT
   60 15.976409 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x33a5 A fortinet.com TXT
   61 15.976412 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x4e2b A fortinet.com TXT
   62 15.976415 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x1d86 A fortinet.com TXT
   63 15.976418 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x8841 A fortinet.com TXT
   64 15.976421 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x460b A fortinet.com TXT
   65 15.976425 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x7664 A fortinet.com TXT
   66 15.976428 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x96fe A fortinet.com TXT
   67 15.976431 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xa8c2 A fortinet.com TXT
   68 15.976434 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xd575 A fortinet.com TXT
   69 15.976485 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=2098 Ack=1069 Win=34304 Len=0
   70 15.976487 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=2098 Ack=1705 Win=38592 Len=0
   84 16.013519 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=2098 Ack=2023 Win=40736 Len=0
   85 16.016930 11.255.251.254  11.255.251.2    DNS        983 Standard query response 0xd575 A fortinet.com TXT
   86 16.016944 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x98dd A fortinet.com TXT
   87 16.016947 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xb113 A fortinet.com TXT
   88 16.016951 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x3f78 A fortinet.com TXT
   89 16.016959 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x6ad6 A fortinet.com TXT
   90 16.016963 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xa251 A fortinet.com TXT
   91 16.016966 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x8c82 A fortinet.com TXT
   92 16.016969 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x505c A fortinet.com TXT
   93 16.016972 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x40a3 A fortinet.com TXT
   94 16.016975 11.255.251.2    11.255.251.254  DNS        213 Standard query 0x77fa A fortinet.com TXT
   95 16.016978 11.255.251.2    11.255.251.254  DNS        213 Standard query 0xb52a A fortinet.com TXT
   96 16.017131 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=3027 Ack=2182 Win=41808 Len=0
   97 16.017151 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=3027 Ack=2341 Win=42880 Len=0
   98 16.017153 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=3027 Ack=2500 Win=43952 Len=0
   99 16.017154 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=3027 Ack=2659 Win=45024 Len=0
  100 16.017155 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=3027 Ack=2818 Win=46096 Len=0
  101 16.017165 11.255.251.254  11.255.251.2    TCP         60 853 → 23886 [ACK] Seq=3027 Ack=2977 Win=47168 Len=0

> Frame 85: 983 bytes on wire (7864 bits), 983 bytes captured (7864 bits)
0000  00 90 0b 72 db 75 00 0c  29 59 da bd 08 00 45 00
```

Maximum Concurrent Connections (DoT CC)

This field determines the maximum number of concurrent TCP connections supported through or with the DUT/SUT. This test is intended to find the maximum number of entries the DUT/SUT can store in its connection table.



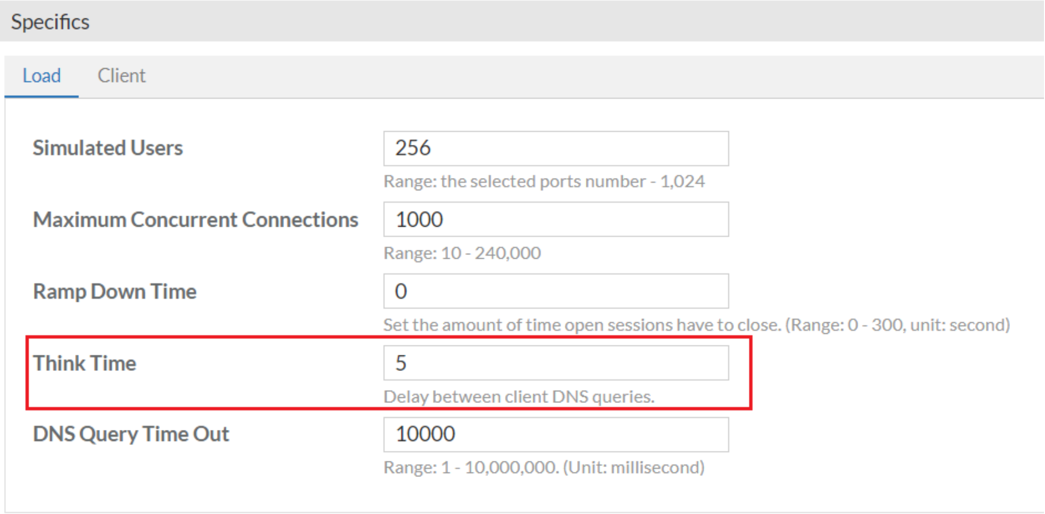
Specifics

Load | Client

Simulated Users	256 Range: the selected ports number - 1,024
Maximum Concurrent Connections	240000 Range: 10 - 240,000
Ramp Down Time	0 Set the amount of time open sessions have to close. (Range: 0 - 300, unit: second)
Think Time	5 Delay between client HTTP requests.
DNS Query Time Out	10000 Range: 1 - 10,000,000. (Unit: millisecond)

Think Time (DoT CC)

Think Time is the delay between client DNS queries (the unit is seconds).

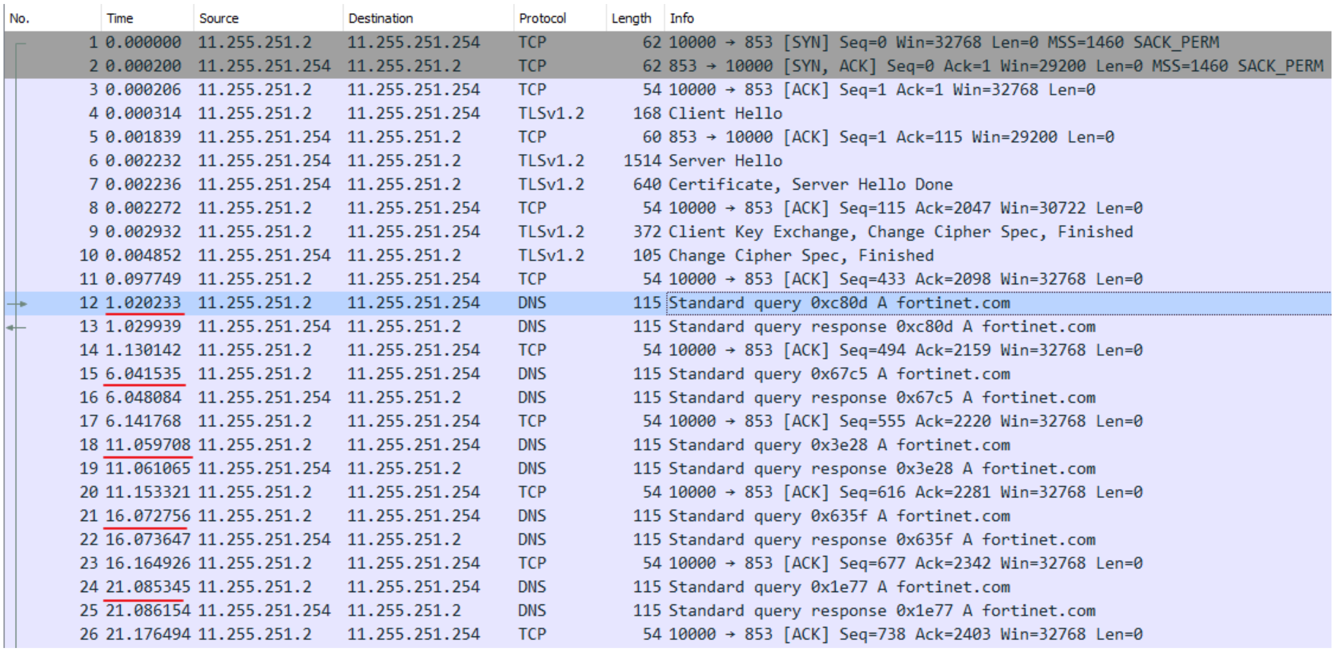


Specifics

Load | Client

Simulated Users	256 Range: the selected ports number - 1,024
Maximum Concurrent Connections	1000 Range: 10 - 240,000
Ramp Down Time	0 Set the amount of time open sessions have to close. (Range: 0 - 300, unit: second)
Think Time	5 Delay between client DNS queries.
DNS Query Time Out	10000 Range: 1 - 10,000,000. (Unit: millisecond)

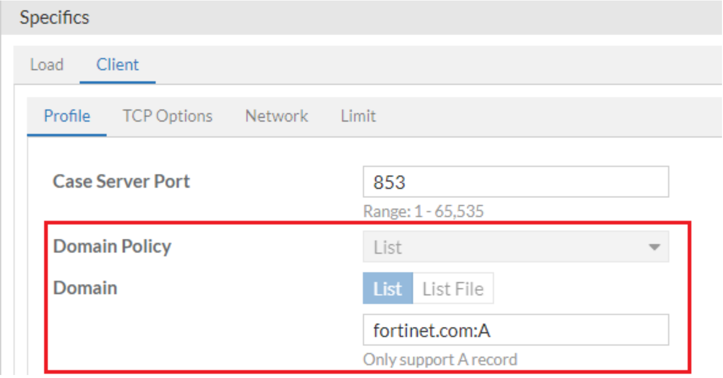
Pcap shows that the time between two DNS queries is about 5 seconds, as configured in a transaction.



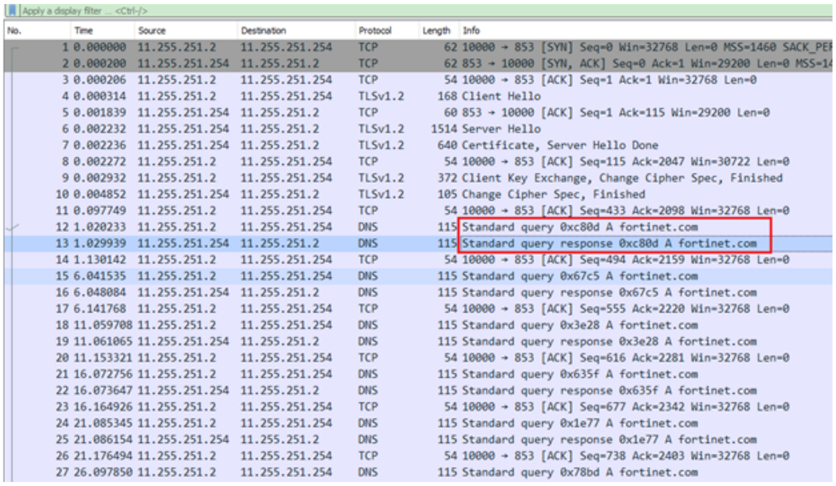
```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  11.255.251.2    11.255.251.254  TCP        62 10000 → 853 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PERM
    2 0.000200  11.255.251.254  11.255.251.2    TCP        62 853 → 10000 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM
    3 0.000206  11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=1 Ack=1 Win=32768 Len=0
    4 0.000314  11.255.251.2    11.255.251.254  TLSv1.2   168 Client Hello
    5 0.001839  11.255.251.254  11.255.251.2    TCP        60 853 → 10000 [ACK] Seq=1 Ack=115 Win=29200 Len=0
    6 0.002232  11.255.251.254  11.255.251.2    TLSv1.2  1514 Server Hello
    7 0.002236  11.255.251.254  11.255.251.2    TLSv1.2   640 Certificate, Server Hello Done
    8 0.002272  11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=115 Ack=2047 Win=30722 Len=0
    9 0.002932  11.255.251.2    11.255.251.254  TLSv1.2   372 Client Key Exchange, Change Cipher Spec, Finished
   10 0.004852  11.255.251.254  11.255.251.2    TLSv1.2   105 Change Cipher Spec, Finished
   11 0.097749  11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=433 Ack=2098 Win=32768 Len=0
   12 1.020233  11.255.251.2    11.255.251.254  DNS       115 Standard query 0xc80d A fortinet.com
   13 1.029939  11.255.251.254  11.255.251.2    DNS       115 Standard query response 0xc80d A fortinet.com
   14 1.130142  11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=494 Ack=2159 Win=32768 Len=0
   15 6.041535  11.255.251.2    11.255.251.254  DNS       115 Standard query 0x67c5 A fortinet.com
   16 6.048084  11.255.251.254  11.255.251.2    DNS       115 Standard query response 0x67c5 A fortinet.com
   17 6.141768  11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=555 Ack=2220 Win=32768 Len=0
   18 11.059708 11.255.251.2    11.255.251.254  DNS       115 Standard query 0x3e28 A fortinet.com
   19 11.061065 11.255.251.254  11.255.251.2    DNS       115 Standard query response 0x3e28 A fortinet.com
   20 11.153321 11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=616 Ack=2281 Win=32768 Len=0
   21 16.072756 11.255.251.2    11.255.251.254  DNS       115 Standard query 0x635f A fortinet.com
   22 16.073647 11.255.251.254  11.255.251.2    DNS       115 Standard query response 0x635f A fortinet.com
   23 16.164926 11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=677 Ack=2342 Win=32768 Len=0
   24 21.085345 11.255.251.2    11.255.251.254  DNS       115 Standard query 0x1e77 A fortinet.com
   25 21.086154 11.255.251.254  11.255.251.2    DNS       115 Standard query response 0x1e77 A fortinet.com
   26 21.176494 11.255.251.2    11.255.251.254  TCP        54 10000 → 853 [ACK] Seq=738 Ack=2403 Win=32768 Len=0
```

Domain Policy and Domain (DoT CPS/RPS/CC)

FortiTester queries the domains in the specified list. Only the “List” type and the “A” record are supported currently. You can configure the expected domain name.



Case Server Port	853 Range: 1 - 65,535
Domain Policy	List
Domain	List / List File fortinet.com:A Only support A record



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	11.255.251.2	11.255.251.254	TCP	62	10000 → 853 [SYN] Seq=0 Win=32768 Len=0 MSS=1460 SACK_PER
2	0.000200	11.255.251.254	11.255.251.2	TCP	62	853 → 10000 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=14
3	0.000206	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=1 Ack=1 Win=32768 Len=0
4	0.000314	11.255.251.2	11.255.251.254	TLSv1.2	168	Client Hello
5	0.001839	11.255.251.254	11.255.251.2	TCP	60	853 → 10000 [ACK] Seq=1 Ack=115 Win=29200 Len=0
6	0.002232	11.255.251.254	11.255.251.2	TLSv1.2	1514	Server Hello
7	0.002236	11.255.251.254	11.255.251.2	TLSv1.2	640	Certificate, Server Hello Done
8	0.002272	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=115 Ack=2047 Win=30722 Len=0
9	0.002932	11.255.251.2	11.255.251.254	TLSv1.2	372	Client Key Exchange, Change Cipher Spec, Finished
10	0.004852	11.255.251.254	11.255.251.2	TLSv1.2	105	Change Cipher Spec, Finished
11	0.097749	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=433 Ack=2098 Win=32768 Len=0
12	1.020233	11.255.251.2	11.255.251.254	DNS	115	Standard query 0xc80d A fortinet.com
13	1.029939	11.255.251.254	11.255.251.2	DNS	115	Standard query response 0xc80d A fortinet.com
14	1.130142	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=494 Ack=2159 Win=32768 Len=0
15	6.041535	11.255.251.2	11.255.251.254	DNS	115	Standard query 0x67c5 A fortinet.com
16	6.048084	11.255.251.254	11.255.251.2	DNS	115	Standard query response 0x67c5 A fortinet.com
17	6.141768	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=555 Ack=2220 Win=32768 Len=0
18	11.059708	11.255.251.2	11.255.251.254	DNS	115	Standard query 0x3e28 A fortinet.com
19	11.061065	11.255.251.254	11.255.251.2	DNS	115	Standard query response 0x3e28 A fortinet.com
20	11.153321	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=616 Ack=2281 Win=32768 Len=0
21	16.072756	11.255.251.2	11.255.251.254	DNS	115	Standard query 0x635f A fortinet.com
22	16.073647	11.255.251.254	11.255.251.2	DNS	115	Standard query response 0x635f A fortinet.com
23	16.164926	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=677 Ack=2342 Win=32768 Len=0
24	21.085345	11.255.251.2	11.255.251.254	DNS	115	Standard query 0x1e77 A fortinet.com
25	21.086154	11.255.251.254	11.255.251.2	DNS	115	Standard query response 0x1e77 A fortinet.com
26	21.176494	11.255.251.2	11.255.251.254	TCP	54	10000 → 853 [ACK] Seq=738 Ack=2403 Win=32768 Len=0
27	26.097850	11.255.251.2	11.255.251.254	DNS	115	Standard query 0x78bd A fortinet.com

RFC benchmark cases

The following types of RFC benchmark cases are available:

- RFC2544 Throughput
- RFC2544 Latency
- RFC2544 Lossrate
- RFC2544 Back to Back
- RFC3511 IP Throughput
- RFC3511 CC

Starting an RFC 2544 throughput test

FortiTester tests the ability of the DUT to handle different types of RFC 2544 throughput. According to RFC 2544, 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 an RFC 2544 throughput test:

1. In *Performance Testing*, expand *RFC Benchmark > RFC 2544* and click *Throughput*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

RFC 2544 throughput test case options

For details about the common options for RFC 2544 cases, see RFC Test Case common options on page 124.

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 an RFC 2544 latency test:

1. In *Performance Testing*, expand *RFC Benchmark > RFC 2544* and click *Latency*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

RFC 2544 latency test case options

For details about the common options for RFC 2544 cases, see RFC Test Case common options on page 124.

Settings	Guidelines
Load	
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.

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 an RFC 2544 loss rate test:

1. In *Performance Testing*, expand *RFC 2544* and click *Loss Rate*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

RFC 2544 loss rate test case options

For details about the common options for RFC 2544 cases, see RFC Test Case common options on page 124.

Settings	Guidelines
Load	
Up/Down Granularity	Custom Load only. Traffic speed per cycle. 0 means sending speed in

Settings	Guidelines
	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.

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. In *Performance Testing*, expand *RFC Benchmark > RFC 2544* and click *Back To Back*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

RFC 2544 back to back test case options

For details about the common options for RFC 2544 cases, see RFC Test Case common options on page 124.

Settings	Guidelines
Load	
Send Speed	Speed in Mbps. A setting of 0 means throughput speed is copied from the BaseValue case.
Initial Traffic Cycle Time	Traffic burst duration in seconds for each frame size. (minimum of 2)

Settings	Guidelines
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.

Starting an 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 an RFC 3511 IP throughput test:

1. In *Performance Testing*, expand *RFC Benchmark > RFC 3511* and click *IP Throughput*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

RFC 3511 IP throughput test case options

For details about the common options for RFC 3511 cases, see RFC Test Case common options on page 124.

Settings	Guidelines
Load	
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)

Starting an RFC 3511 concurrent capacity test

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

To start an RFC 3511 concurrent capacity test:

1. In *Performance Testing*, expand *RFC Benchmark > RFC 3511* and click *Concurrent Capacity*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

RFC 3511 concurrent capacity test case options

For details about the common options for RFC 3511 cases, see RFC Test Case common options on page 124.

Settings	Guidelines
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)

Settings	Guidelines
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.
Client Close Mode	Select the connection close method: *3Way_Fin* or *Reset*.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
Client/Server Network	
Network MSS	The maximum segment size. If MSS is bigger than the MTU, IP fragmentation will be triggered conditionally.
Network MTU	The Maximum Transmission Unit ranging from 1280 to 9000.
IP Option DSCP	IP Option DSCP value for QoS, ranging from 0 - 63.
IP Flags DF	Do not fragment packets. • 0 = disable (fragment) • 1 = enable (do not fragment)
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.

RFC Test Case common options

This page shows information that is common to all RFC case configurations. Anything specific to a particular case will be found within the case page. For example, RFC RPS test specifics will be found under the RFC RPS page.

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.
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.
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.
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 for the description of network settings.	
Load	
Flows	Enter the port pair.
Traffic Direction	Specify the direction of traffic flow.
Frame Size	**RFC fixed frame size**–64, 128, 256, 512, 1024, 1280 or 1518 **User Defined**–Useful if devices in path add/remove to packet size, so you can adjust the frame size FortiTester sends out.

Settings	Guidelines
	iMIX–Internet Mix or iMIX refers to typical Internet traffic passing some network equipment such as routers, switches or firewalls. **NOTE:** Before referencing iMIX, the iMIX object needs to be configured. Go to **Performance Testing > Objects > iMIX**. Configure the Frame Size, Packet Size and Weight. (Frame Size cannot be repeated, and in v7.1.0 supports up to 10 records).
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.
Iteration Level	Select the iteration level, either *Device* or *Port*, used to increase or decrease speed and connections between port pairs.
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	

Settings	Guidelines
Network MTU	The Maximum Transmission Unit ranging from 1280 to 9000.
IP Option DSCP	IP Option DSCP value for QoS, ranging from 0 - 63.
IP Flags DF	Do not fragment packets. • 0 = disable (fragment) • 1 = enable (do not fragment)

Protocol cases

The following types of protocol cases are available:

- TCP CIFS/SMB
- TCP DNS-AXFR
- TCP FIX
- TCP FTP
- TCP IMAP
- TCP LDAP
- TCP NFS
- TCP POP3
- TCP RDP
- TCP SMTP
- TCP SSH
- UDP DNS latency
- UDP NTP
- UDP RADIUS
- UDP SIP
- UDP TFTP
- UDP DHCP
- UDP ICMP
- IGMP
- RTSP/RTP

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 TCP CIFS/SMB test:

1. In *Performance Testing*, expand *Protocol > TCP* and click *CIFS/SMB*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP CIFS/SMB test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Starting a TCP Protocol DNS-AXFR test

This test established a TCP connection (three-way handshake), simulates a DNS zone transfer (AXFR), and closes the TCP connection.

To start a TCP DNS-AXFR test:

1. In *Performance Testing*, expand *Protocol > TCP* and click *DNS-AXFR*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP DNS-AXFR test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

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 TCP FIX test:

1. In *Performance Testing*, expand *Protocol* > *TCP* and click *FIX*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP FIX test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Client Profile	

Settings	Guidelines
Username	The username of the simulated users. All the users use the same username and password.
Password	The password of the simulated users.

Starting a TCP Protocol FTP test

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

To start a TCP FTP test:

1. In *Performance Testing*, expand *Protocol > TCP* and click *FTP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP FTP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Client Profile	
FTP Mode	Choose either active mode FTP or passive mode FTP.
FTP User	Create a username.
FTP Password	Create a password.
Server Profile	
Server Close Mode	Set to 3 Way Fin by default. Not configurable.

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 a TCP IMAP test:

1. In *Performance Testing*, expand *TCP* and click *IMAP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP IMAP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
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.

Starting a TCP LDAP test

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

To start a TCP LDAP test:

1. In *Performance Testing*, expand *Protocol > TCP* and click *LDAP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP LDAP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
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.

Starting a TCP 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 TCP NFS test:

1. In *Performance Testing*, expand *Protocol* > *TCP* and click *NFS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP NFS test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
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 establishes a TCP connection (three-way handshake), receives one mail by POP3 and closes the TCP connection.

To start a TCP POP3 test:

1. In *Performance Testing*, expand *Protocol* > *TCP* and click *POP3*.
2. Click *Create New*.

3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP POP3 test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
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.

Starting a TCP Protocol RDP test

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

To start a TCP RDP test:

1. In *Performance Testing*, expand *Protocol > TCP* and click *RDP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.

5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP RDP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
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.

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 a TCP SMTP test:

1. In *Performance Testing*, expand *Protocol* > *TCP* and click *SMTP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP SMTP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
SMTP Email Address	The email sender address. The default is “tester@mailserver.com”. The wildcard character (#) is used to generate a random address. For example: `FortiTester<###>@mailserver.com`.
SMTP Email To	The email receiver address. The default is “receiver@mailserver.com”. The wildcard character (#) is used to generate a random address. For example: `FortiTester<###>@mailserver.com`. This option supports up to 32 recipients.
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.
Random	Send a random attachment name and content.
Randomize File Name and Content	Enable or disable the sending of a random file name and response body based on the user-uploaded file.

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 TCP SSH test:

1. In *Performance Testing*, expand *Protocol > TCP* and click *SSH*.
2. Click *Create New*.

3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

TCP SSH test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
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.
Crypto Enable	Enable to send packets in ciphertext.

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 UDP DNS latency test:

1. In *Performance Testing*, expand *Protocol > UDP* and click *DNS Latency*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

UDP DNS latency test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
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.
Recursion Desired	Enable or disable *Recursion Desired* and *Recursion Available* to control the RD/RA flag when the client side sends DNS queries. When the client side of a DNS Latency case sends DNS queries, the RD/RA bits in the DNS flags will use the configuration of these two fields. The RD/RA bits configuration only affect the DNS query packets sent by client side.
Recursion Available	

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 a UDP NTP test:

1. In *Performance Testing*, expand *Protocol > UDP* and click *NTP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

UDP NTP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
Time Out	The default is 1000 microseconds.

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 UDP RADIUS test:

1. In *Performance Testing*, expand *Protocol > UDP* and click *RADIUS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.

4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

UDP RADIUS test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
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.

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. In *Performance Testing*, expand *Protocol* > *UDP* and click *SIP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.

4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

UDP SIP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

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.

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 UDP TFTP test:

1. In *Performance Testing*, expand *Protocol > UDP* and click *TFTP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

UDP TFTP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
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.
Client/Server Network	
TFTP Block Size	Specify a Block Size. The default is 512 bytes.

Starting a Protocol 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 Protocol DHCP test:

1. In *Performance Testing*, expand *Protocol* and click *DHCP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Protocol DHCP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Load	
Time Out	The default is 1000 microseconds.

Starting a Protocol ICMP test

The ICMP test sends ICMP messages of the specified types.

To start a Protocol ICMP test:

1. In *Performance Testing*, expand *Protocol* and click *ICMP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Protocol ICMP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Client Network	
ICMP Message Type	ICMPv4_Echo, ICMPv6_Echo, ICMPv6_Neighbor_Solicitation
Message Count	Number of echo/ Neighbor Solicitation requests to send
Timeout	Timeout in milliseconds to wait for each reply
Payload Size	Use payload size as number of data bytes to be sent
IP list	A list of destination IPs
Loop	Number of times to send requests to destination IPs in IP list
Delay	Delay between loops
Flood	Flood ping
Interval	Seconds between sending each packet
Increment ID	ICMP ID field value increment or random

Starting a Protocol 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.

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

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

# 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 a Protocol IGMP test:

1. In *Performance Testing*, expand *Protocol* and click *IGMP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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:

```
diagnose sys mcast-session list
```

Tip 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Protocol IGMP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Settings	Guidelines
Client Network	
Multicast IP	Specify a multicast IP. For the example FortiGate configuration shown above, *Multicast IP* would be 226.1.2.3.

Starting a Protocol 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 a Protocol RTSP/RTP test:

1. In *Performance Testing*, expand *Protocol* and click *RTSP/RTP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Protocol RTSP/RTP test case options

For details about the common options for protocol cases, see Protocol Test Case common options on page 145.

Protocol Test Case common options

Use this page as a generic for information that is common to all Protocol case configurations. Anything specific to the case itself will be found within the case's page, i.e. Protocol FTP test specifics will be found under the Protocol FTP document page.

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.
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.
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.
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 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 value must be greater than 0. If the user wants FortiTester to create connections as fast as possible, the user should set the Mode to Simulated Users. Available only when Connections/second is selected for Mode.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
Client Profile	

Settings	Guidelines
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.
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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
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.

Settings	Guidelines
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*.

Application cases

The following types of application cases are available:

- AmazonS3
- AOL
- BitTorrent
- DB2
- Facebook
- Gmail
- Gtalk
- MSSQL
- MySQL
- Netflix
- Oracle TNS
- PSQL
- Twitter
- Webex
- WhatsApp
- Yahoo Mail
- YouTube

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. In Performance Testing, expand *Application* and click *Amazon S3*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.

6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Amazon S3 test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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

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. In Performance Testing, expand *Application* and click *AOL Chat*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

AOL Chat test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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.

Starting a BitTorrent test

The BitTorrent test simulates a download process between peers.

To start a BitTorrent test:

1. In Performance Testing, expand *Application* and click *BitTorrent*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

BitTorrent test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
BitTorrent Piece Size	The size of pieces in downloading file.
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. In Performance Testing, expand *Application* and click *DB2*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

DB2 test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.

Starting a Facebook test

The Facebook test simulates Facebook traffic, such as logging in, searching, and watching videos.

To start a Facebook test:

1. In Performance Testing, expand *Application* and click *Facebook*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Facebook test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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.
User Agent	Set the value of the user agent in the HTTP header.

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. In Performance Testing, expand *Application* and click *Gmail*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Gmail test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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.
User Agent	Set the value of the user agent in the HTTP header.
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.

Settings	Guidelines
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 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 autheRntication for HTTPS cases.
Certificate	Select the certificate created in *Performance Testing > Objects > Certificates*. Available only when Enable Client Certificate is enabled.
Server Profile	
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.

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. In Performance Testing, expand *Application* and click *Gtalk*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Gtalk test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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.

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. In Performance Testing, expand *Application* and click *MSSQL*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.

6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

MSSQL test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.

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. In Performance Testing, expand *Application* and click *MySQL*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

MySQL test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.

Starting a Netflix test

The 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. In Performance Testing, expand *Application* and click *Netflix*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Netflix test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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.
User Agent	Set the value of the user agent in the HTTP header.

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. In Performance Testing, expand *Application* and click *Oracle TNS*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Oracle TNS test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.

Starting a PSQL test

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

To start a PSQL test:

1. In Performance Testing, expand *Application* and click *PSQL*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

PSQL test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
Database	The name of the database.
Database User	The database user name.
Database Password	The password of the database user.

Starting a Twitter test

The Twitter test simulates Twitter traffic, such as posting articles and watching videos.

To start a Twitter test:

1. In Performance Testing, expand *Application* and click *Twitter*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Twitter test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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.
User Agent	Set the value of the user agent in the HTTP header.

Starting a WebEx test

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

To start a WebEx test:

1. In Performance Testing, expand *Application* and click *WebEx*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

WebEx test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
Supported Behaviors	Select the behaviors that will be simulated and sent in one TCP stream.
User Agent	Set the value of the user agent in the HTTP header.

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. In Performance Testing, expand *Application* and click *WhatsApp*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.

6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

WhatsApp test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
WhatsApp Type	Select the WhatsApp data type to simulate.

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. In Performance Testing, expand *Application* and click *Yahoo Mail*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Yahoo Mail test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
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.
User Agent	Set the value of the user agent in the HTTP header.
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 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.

Settings	Guidelines
Enable Client Certificate	Enable the client autheRntication for HTTPS cases.
Certificate	Select the certificate created in **Performance Testing > Objects > Certificates**. Available only when Enable Client Certificate is enabled.
Server Profile	
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.

Starting a YouTube test

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

To start a YouTube test:

1. In Performance Testing, expand *Application* and click *YouTube*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

YouTube test case options

For details about the common options for application cases, see Application test case common options on page 166.

Settings	Guidelines
Client Profile	
Request Header	The HTTP header of the request packet. Click the Add button to specify more headers. Wild card is supported.
Server Profile	
Response Header	The HTTP header of the response packet. Click the Add button to specify more headers.
Action	
Request Stream	Select the stream file to request, or upload a new one in **Objects >Files**.

Application test case common options

Use this page as a generic for information that is common to all Application case configurations. Anything specific to the case itself will be found within the case's page, i.e. Application Twitter test specifics will be found under the Application Twitter document page.

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 Scripts on page 187.
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.
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.
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 25 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 value must be greater than 0. If the user wants FortiTester to create connections as fast as possible, the user should set the Mode to Simulated Users. Available only when Connections/second is selected for Mode.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
HTTP Request Time Out	An HTTP request timeout occurs when an HTTP request is issued, but

Settings	Guidelines
	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	
Client Close Mode	Select the connection close method: *3Way_Fin* or *Reset*.
Piggyback Get Requests	If enabled, this means an acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
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	• Write: Upload a file to the Samba server • Read: Download a file from the Samba server
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.
Request File Option	Choose the size or object of the file to upload/download.

Replay cases

The following types of replay cases are available:

- Traffic replay
- GTP Replay

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. In *Performance Testing*, expand *Replay* and click *Traffic*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Traffic Replay test case options

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.
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.
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.
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 for the description of network settings.	

Settings	Guidelines
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.
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. In *Performance Testing*, expand *Replay* and click *GTP*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

GTP Replay test case options

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.
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.
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.
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 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.

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

Starting a packet capture test

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

To start a packet capture test:

1. In Performance Testing, expand *Packet Capture* and click *Packet Capture*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

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 options

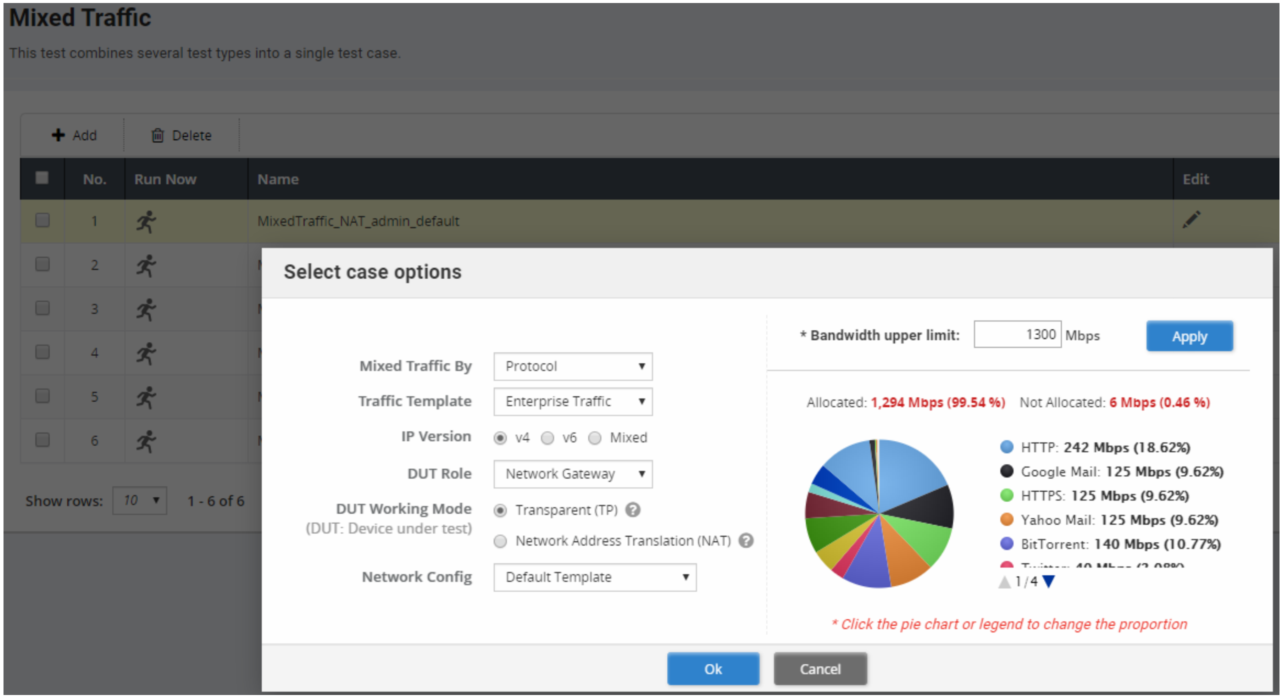
Settings	Guidelines
Basic Information	
Name	Specify the case name, or just use the default. The name appears in the list of test cases.
Duration	Specify the test duration. The default is 10 minutes. The test stops automatically after the duration you specify.
Number of Samples	Select the number of samples. 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.
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.

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 *+ Create New* 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

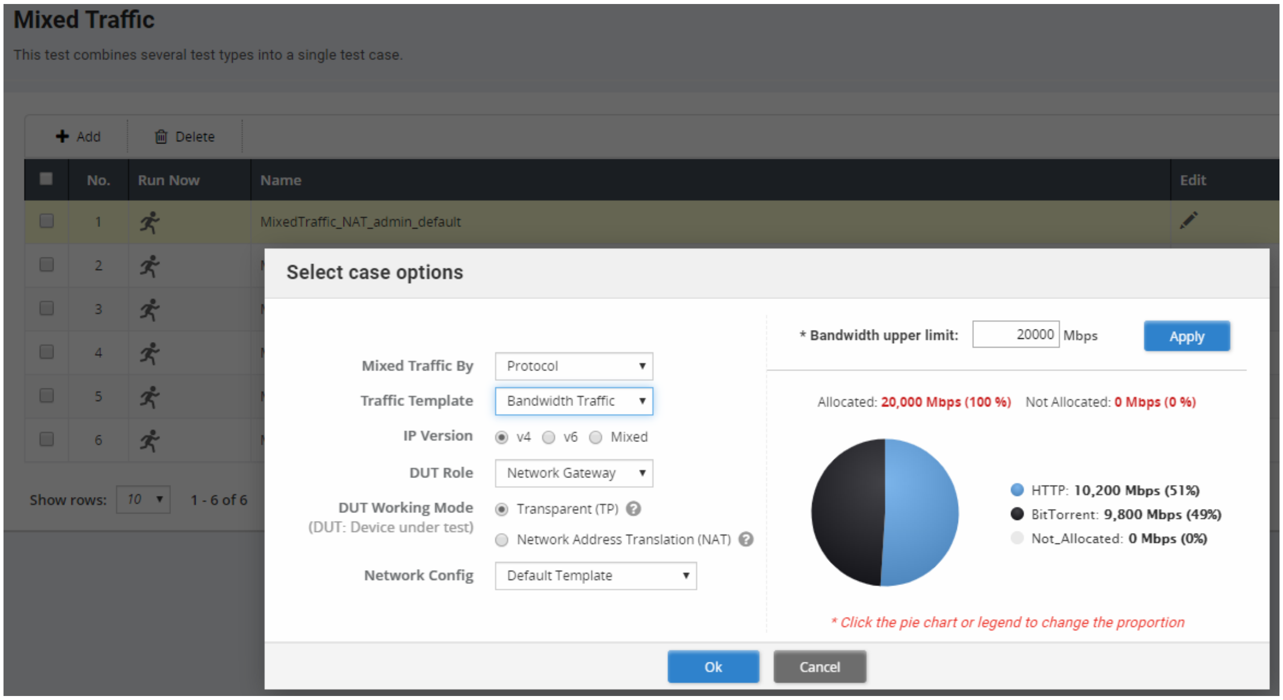
* Bandwidth upper limit: 1300 Mbps

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)

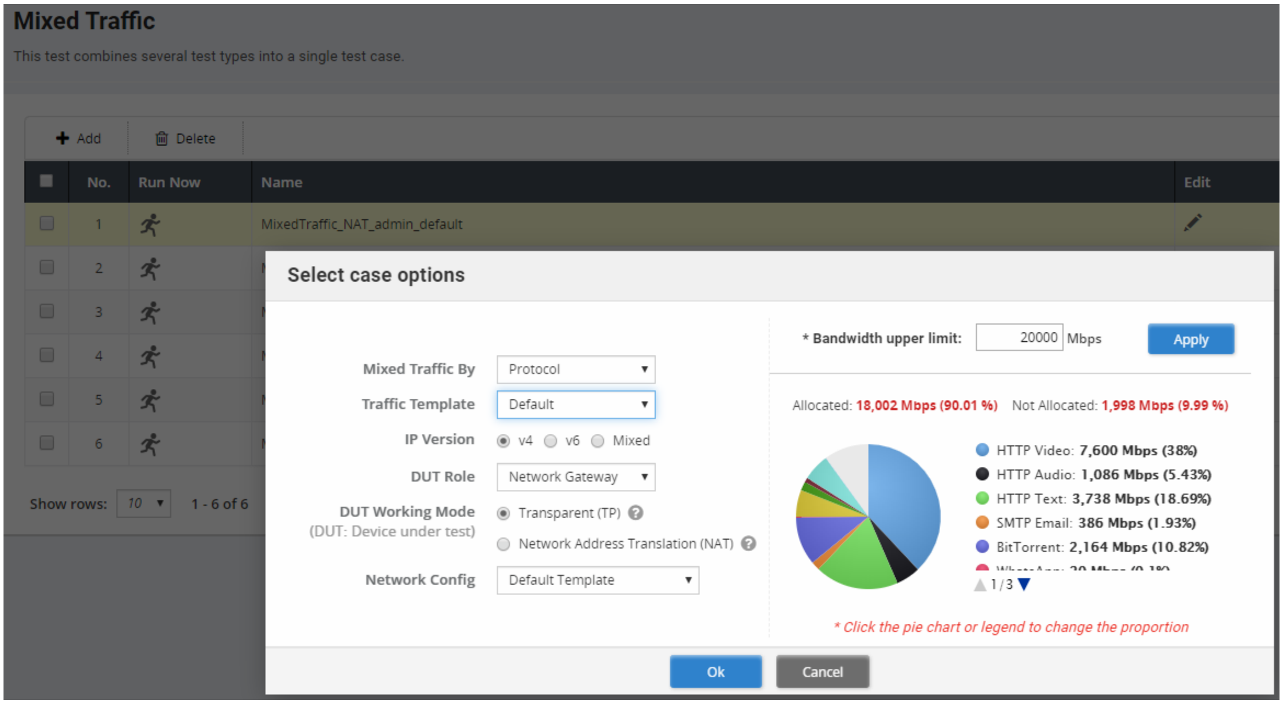
Network Config: Default Template ▾

* Bandwidth upper limit: 20000 Mbps Apply

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 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 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 below. 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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Mixed Traffic test case options

For information about creating a traffic template, see Creating a custom traffic template on page 189.

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 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

Settings	Guidelines
	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.	
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.
Maximum Concurrent Connections	Determines the maximum number of concurrent TCP connections supported through or with the DUT/SUT. This test is intended to find the maximum number of entries the DUT/SUT can store in its connection table.
Loops	Number of times to send the attacks. 0 means as many as possible.
Connections per Second	Rate of new connections per second. The value must be greater than 0. If the user wants FortiTester to create connections as fast as possible, the user should set the Mode to Simulated Users. Available only when Connections/second is selected for Mode.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
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.
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.

Settings	Guidelines
SMTP Email Password	The password of email sender. The default is “tester@fts”.
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.
Certificate	The server certificate. If you have selected a certificate group in the Select case options window, then you are not allowed select certificate here.
Think Time	The delay between client HTTP requests (unit: second).
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.
Delay	The period that FortiTester will wait until it sends the next web application attack.
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.
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.
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 Custom Load to search using a custom load.

Settings	Guidelines
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.
RADIUS Request Time Out	Time in microseconds before a RADIUS request times out.
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.
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.
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.
Throughput Buffer Size	Set the throughput buffer size. The valid range is from 64-10M.
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.
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.

Settings	Guidelines
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.
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.
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.

Managing performance testing objects

The following types of testing objects are available:

- Networks
- User groups
- Port Settings
- Port Mapping
- Files
- Hosts
- Host groups
- URL groups
- iMIX
- Certificates and Certificate Groups
- SNI
- Payloads
- Scripts
- SNMP Monitors

- Creating a custom traffic template

Networks

Networks defines the network connection topology of the FortiTester and DUT devices. Test case can reference a defined Network Topology object.

To create a network object:

1. Go to **Cases > Performance Testing > Objects > Networks**.
2. Click **+Create New** to create a network object.
3. Configure the options with the Network Configuration Templates. Click **OK**.
4. Name the Network object, set the Network Settings (see the Network Configuration Templates), click **Save**.
5. Repeat these steps to create more objects.

Port Settings

The Port Setting defines the port configuration of the FortiTester device. Test case can reference a defined Port Setting object.

To create a Port Settings object:

1. Go to **Cases > Performance Testing > Objects > Port Settings**.
2. Click **+Create New** to create a Port Mapping object.
3. Configure the options with the Network Configuration Templates. Click **OK**.
4. Click **Save**.
5. Repeat these steps to create more objects.

Port Mapping

The Port Mapping defines the mapping between test case ports and physical ports. Test case can reference a defined Port Mapping object.

Notes

- All ports are displayed for all cases
- The physical port icon on Ports Mapping page will be greyed-out if this physical port is not enabled.
- If the case port is not mapping to the physical port, all settings will be disabled.
- For optional port binding:
  - Port-binding can't be edited if it contains non-physical ports
  - All the port-bindings can be deleted
  - In the case of deleted port bindings that contain physical ports, physical ports will be displayed after deletion

To create a Port Mapping object:

1. Go to **Cases > Performance Testing > Objects > Port Mapping**.
2. Click **+Create New** to create a Port Mapping object.
3. Set the Name and the ports.

4. Click **Save**.
5. Repeat these steps to create more objects.

Files

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 **+ Create New** 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 **Open** 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.

Hosts

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 **Create New**.
3. Enter a name for the DNS host.
4. Click **OK**.
5. Click **Create New** 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.

Host groups

The host group defines the mapping between ports and hosts. It can be used in HTTP/S profiles.

To add DNS host groups:

1. Go to **Cases > Performance Testing > Objects > Host Groups**.
2. Click **Create New**.
3. Enter a name for the host group.
4. Click **OK**.
5. Click **Create New** under **Host Group Management**.
6. Select the device, 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.

URL groups

The URL group object is used to manage the URLs from the user. It can be usd in most of cases that support custom pages.

To add URL groups:

1. Go to **Cases > Performance Testing > Objects > URL Groups**.
2. Click **Create New**.
3. Enter a name for the URL group.
4. Click **OK**.
5. Click **Create New** under **URL Management**.
6. Select the **Hostname**, the **Host Group** (created in **Performance Testing > Objects > Host Groups**), **Method**, **URI**, then click **OK**.

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

User groups

The user group defines the users that can be used in VPN case for login in VPN gateway.

To add User groups:

1. Go to **Cases > Performance Testing > Objects > User Groups**.
2. Click **Create New**.
3. Enter a name for the User group.
4. Click **OK**.
5. Click **Create New** under **User Management**.
6. Set the **Username** and **Password**.

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

iMIX

Internet Mix or iMIX refers to typical Internet traffic passing some network equipment such as routers, switches or firewalls. When measuring equipment performance using an iMIX of packets the performance is assumed to resemble what can be seen in "real-world" conditions.

iMix is used in RFC Benchmark performance test cases.

To add an iMIX object:

1. Go to *Cases > Performance Testing > Objects > iMIX*.
2. Click *Create New*.
3. Enter a name for the iMIX object.
4. Click *OK*.
5. Click *Create New* under *Settings Management*.
6. Set the Frame Size, Packet Size, and Weight.

Frame size cannot be repeated, and currently supports up to 10 records.

You can later reference the iMIX object when you create test cases.

Certificates and 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 **+ Create New** 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 **+ Create New**.
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.

SNI

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**.

Payloads

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 **+ Create New** 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.

Scripts

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** or **Security Testing > Objects > Scripts**.
2. Click **+ Create New** 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.

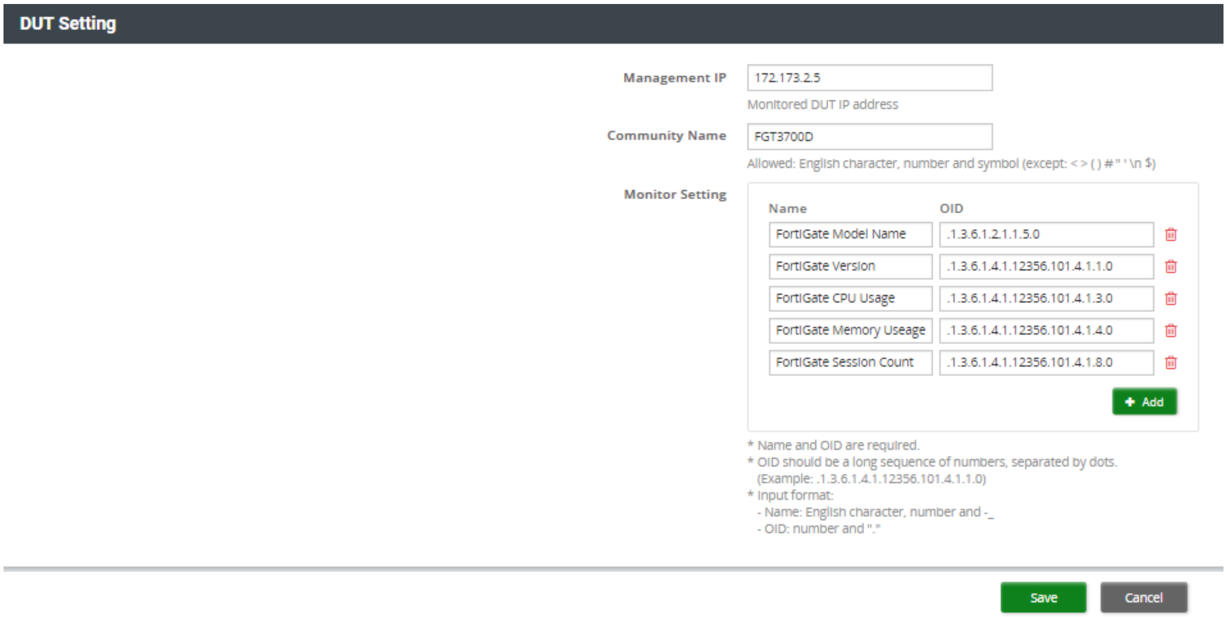
SNMP Monitors

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 **Performance Testing** or **Security Testing > Objects > SNMP Monitors**.
2. Click **+ Create New** 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 $)

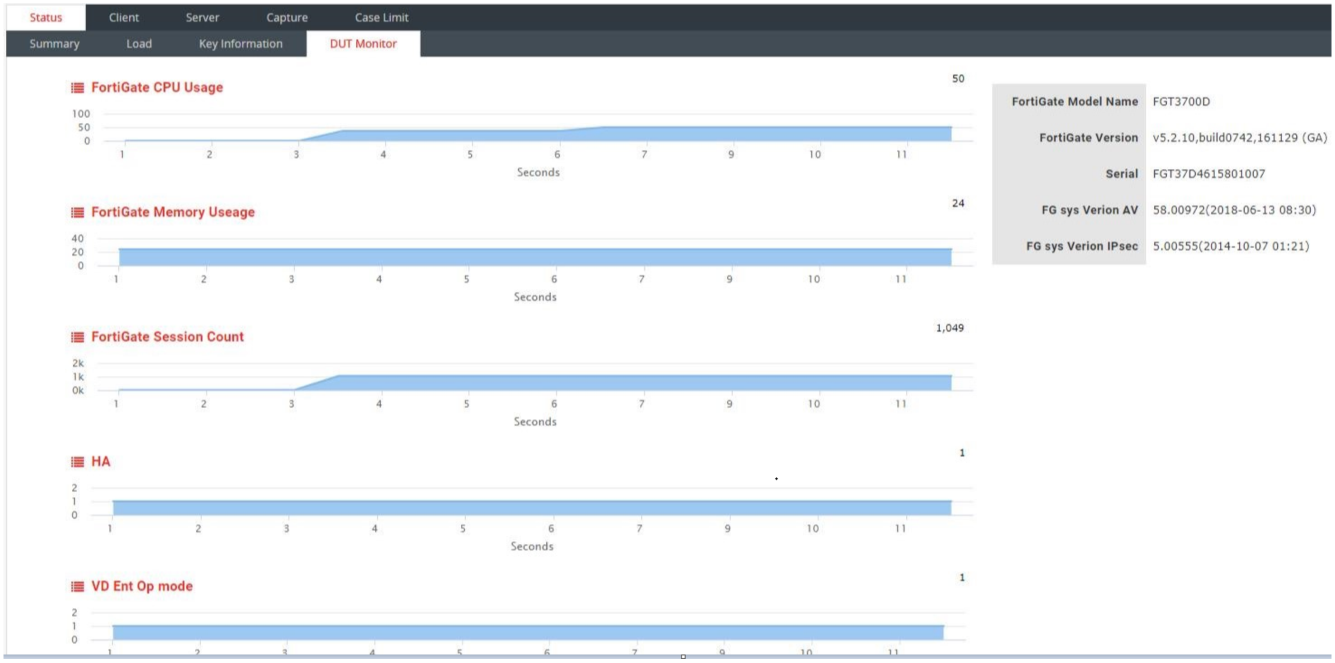
Monitor Setting

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.



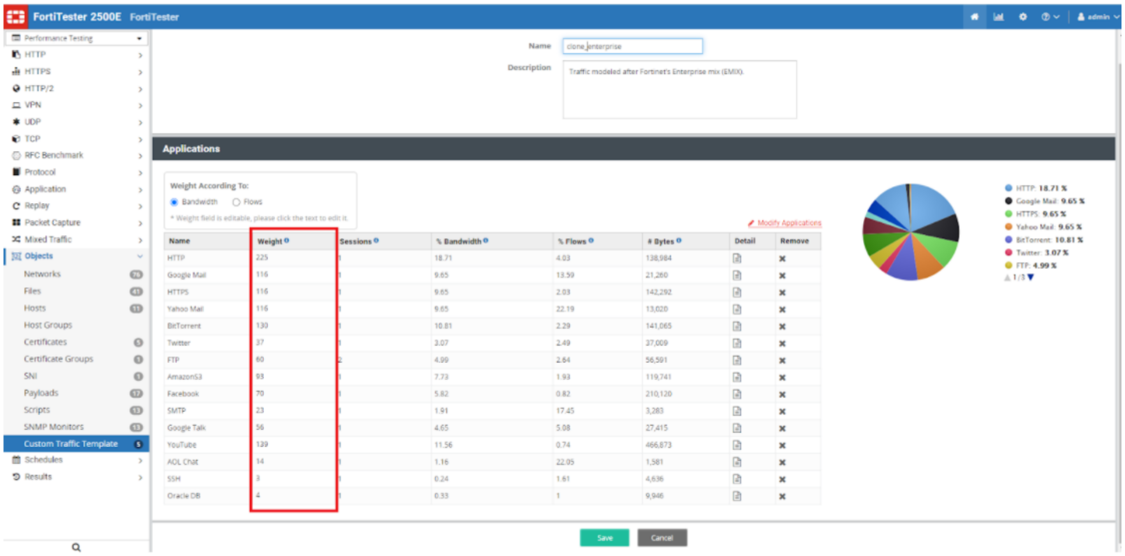
FortiGate Model Name	FGT3700D
FortiGate Version	v5.2.10,build0742,161129 (GA)
Serial	FGT37D4615801007
FG sys Verion AV	58.00972(2018-06-13 08:30)
FG sys Verion IPsec	5.00555(2014-10-07 01:21)

Creating a custom traffic template

This service is used to manage the custom traffic template. It can be used in mixed traffic cases.

To create a custom traffic template

1. Go to **Performance Testing** or **Security Testing > Objects > Custom Traffic Template** to create custom template.
2. Click **+ Create New** and select the applications for the template.
3. Double click **Weight** to edit weights. Click the Detail icon to edit specifics. Don't forget to save.



Name: clone_enterprise

Description: Traffic modeled after Fortinet's Enterprise mix (EMIX).

Weight According To:

● Bandwidth ○ Flows

* Weight field is editable, please click the text to edit it.

Name	Weight	Sessions	% Bandwidth	% Flows	# Bytes	Detail	Remove
HTTP	225	1	18.71	4.03	138,984	🗎	✖
Google Mail	116	1	9.65	13.59	21,260	🗎	✖
HTTPS	116	1	9.65	2.03	142,292	🗎	✖
Yahoo Mail	116	1	9.65	22.19	13,020	🗎	✖
BitTorrent	130	1	10.81	2.29	141,065	🗎	✖
Twitter	37	1	3.07	2.49	37,009	🗎	✖
FTP	60	2	4.99	2.64	56,591	🗎	✖
AmazonS3	93	1	7.73	1.93	119,741	🗎	✖
Facebook	70	1	5.82	0.82	210,120	🗎	✖
SMTP	23	1	1.91	17.45	3,283	🗎	✖
Google Talk	56	1	4.65	5.08	27,415	🗎	✖
YouTube	139	1	11.56	0.74	466,873	🗎	✖
AOL Chat	14	1	1.16	22.05	1,581	🗎	✖
SSH	3	1	0.24	1.61	4,636	🗎	✖
Oracle DB	4	1	0.33	1	9,946	🗎	✖

4. Go to **Performance Testing** or **Security Testing > Mixed Traffic**, create a new case, select **Protocol** at **Mixed Traffic By**, and choose any Custom Traffic Template. Click Ok.
5. Go to **Specifics > Action**, and edit Bandwidth Upper Limit to determine maximum bandwidth.

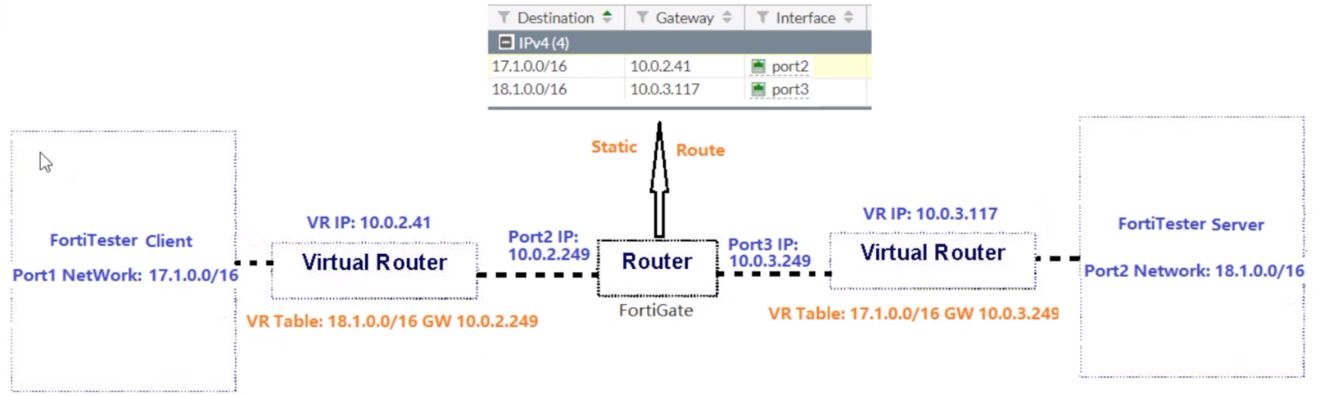
Performance testing examples

This section provides examples for running performance test cases.

Using virtual router with AWS public cloud to run a HTTPS CPS test

Virtual routers are useful when the FortiTester and the Device Under Test (DUT) are not in the same subnet, or the physical router's or the DUT's ARP table size is less than the test subnet address count.

If your test subnet address is different from the physical router's or DUT's subnet address, and if you don't use the virtual router, you must add a physical router in the test network. This would increase network latency while using the virtual would not, thus ensuring the accuracy of test data. The DUT only requests the virtual router IP’s MAC address, so it reduces the MAC address entries in the DUT MAC address table.

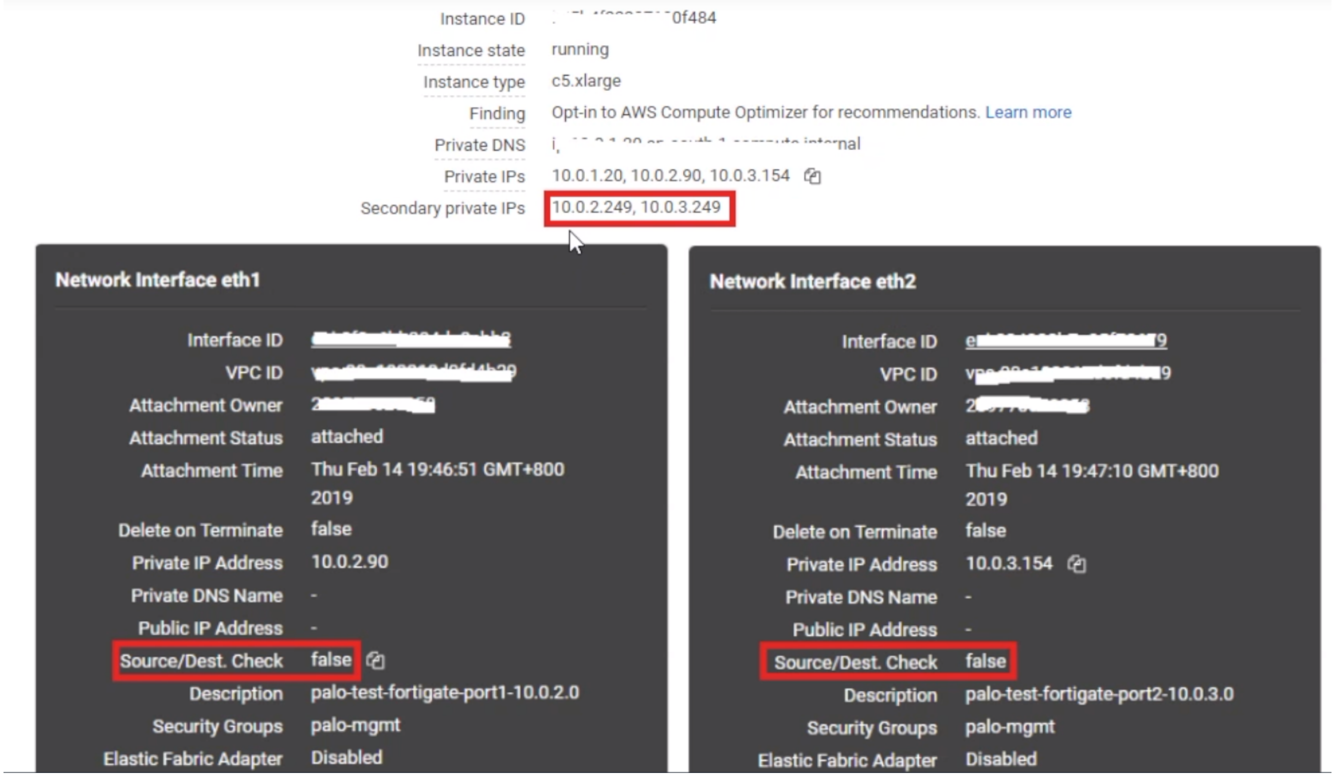


Destination	Gateway	Interface
IPv4 (4)		
17.1.0.0/16	10.0.2.41	port2
18.1.0.0/16	10.0.3.117	port3

In the DUT the static routes point to either end of the ForiTester, one to the 17.1 network, and the other to the 18.1 network.

Here the virtual router IP is 10.0.2.41 will be on the client side. On the server side the virtual router IP is 10.0.3.117.

FortiGate interface settings on AWS



Instance ID	[redacted]0f484
Instance state	running
Instance type	c5.xlarge
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Private DNS	i[redacted]nal
Private IPs	10.0.1.20, 10.0.2.90, 10.0.3.154
Secondary private IPs	10.0.2.249, 10.0.3.249

Network Interface eth1

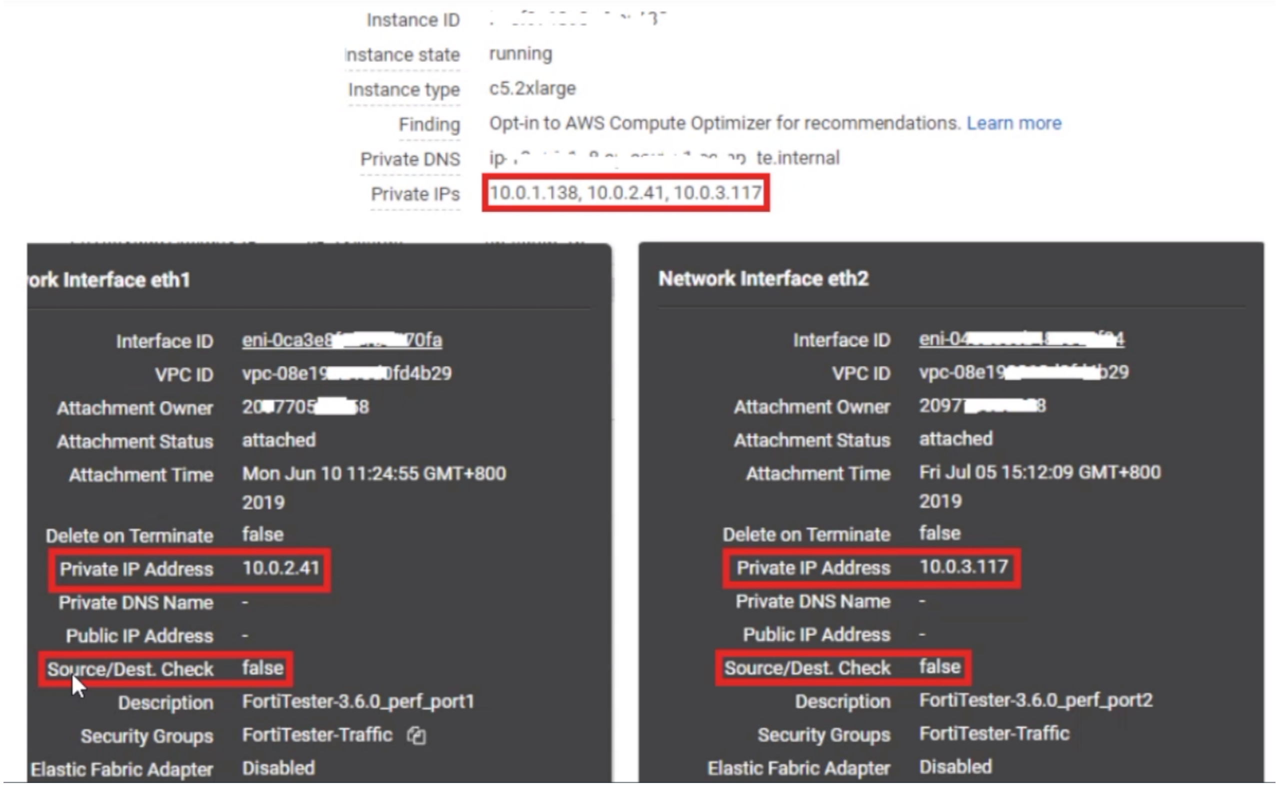
Interface ID	[redacted]
VPC ID	[redacted]
Attachment Owner	[redacted]
Attachment Status	attached
Attachment Time	Thu Feb 14 19:46:51 GMT+800 2019
Delete on Terminate	false
Private IP Address	10.0.2.90
Private DNS Name	-
Public IP Address	-
Source/Dest. Check	false
Description	palo-test-fortigate-port1-10.0.2.0
Security Groups	palo-mgmt
Elastic Fabric Adapter	Disabled

Network Interface eth2

Interface ID	[redacted]
VPC ID	[redacted]
Attachment Owner	[redacted]
Attachment Status	attached
Attachment Time	Thu Feb 14 19:47:10 GMT+800 2019
Delete on Terminate	false
Private IP Address	10.0.3.154
Private DNS Name	-
Public IP Address	-
Source/Dest. Check	false
Description	palo-test-fortigate-port2-10.0.3.0
Security Groups	palo-mgmt
Elastic Fabric Adapter	Disabled

In AWS, the two interfaces are eth 1 and eth2. The secondary private addresses are 10.0.2.249 and 10.0.3.249, corresponding to the diagram shown earlier. In order to use the virtual router, the source/destination check in both interfaces have to be set to false.

FortiTester interface settings on AWS



Instance ID	[redacted]
Instance state	running
Instance type	c5.2xlarge
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Private DNS	ip-[redacted]te.internal
Private IPs	10.0.1.138, 10.0.2.41, 10.0.3.117

ork Interface eth1

Interface ID	eni-0ca3e8[redacted]70fa
VPC ID	vpc-08e19[redacted]0fd4b29
Attachment Owner	20[redacted]7705[redacted]8
Attachment Status	attached
Attachment Time	Mon Jun 10 11:24:55 GMT+800 2019
Delete on Terminate	false
Private IP Address	10.0.2.41
Private DNS Name	-
Public IP Address	-
Source/Dest. Check	false
Description	FortiTester-3.6.0_perf_port1
Security Groups	FortiTester-Traffic
Elastic Fabric Adapter	Disabled

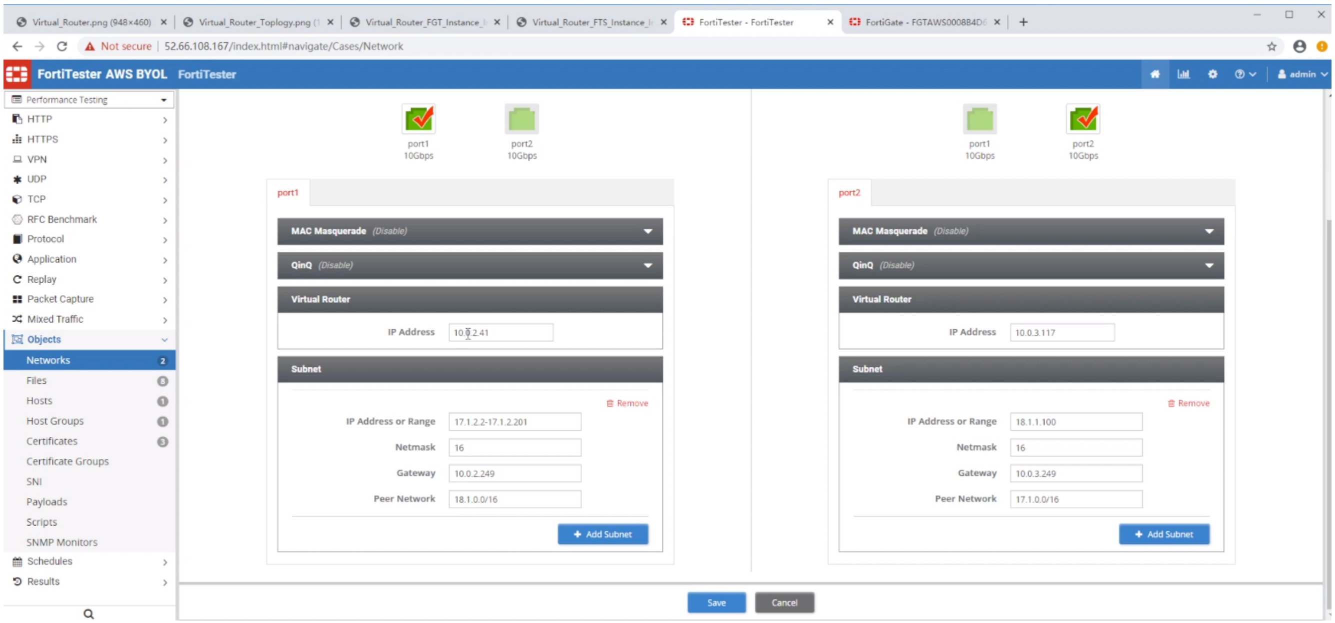
Network Interface eth2

Interface ID	eni-04[redacted]4
VPC ID	vpc-08e19[redacted]b29
Attachment Owner	2097[redacted]8
Attachment Status	attached
Attachment Time	Fri Jul 05 15:12:09 GMT+800 2019
Delete on Terminate	false
Private IP Address	10.0.3.117
Private DNS Name	-
Public IP Address	-
Source/Dest. Check	false
Description	FortiTester-3.6.0_perf_port2
Security Groups	FortiTester-Traffic
Elastic Fabric Adapter	Disabled

Here there are two ports for testing traffic: 10.0.2.41 and 10.0.3.117. Set the source/dest check to false in order to set the virtual router.

FortiTester network object settings example

1. Log onto FortiTester.
2. Go to **FortiTester > Performance Testing > Objects > Networks** to display the following page.



port1

MAC Masquerade (Disable)

QinQ (Disable)

Virtual Router

IP Address	10.0.2.41

Subnet

IP Address or Range	17.1.2.2-17.1.2.201
Netmask	16
Gateway	10.0.2.249
Peer Network	18.1.0.0/16

port2

MAC Masquerade (Disable)

QinQ (Disable)

Virtual Router

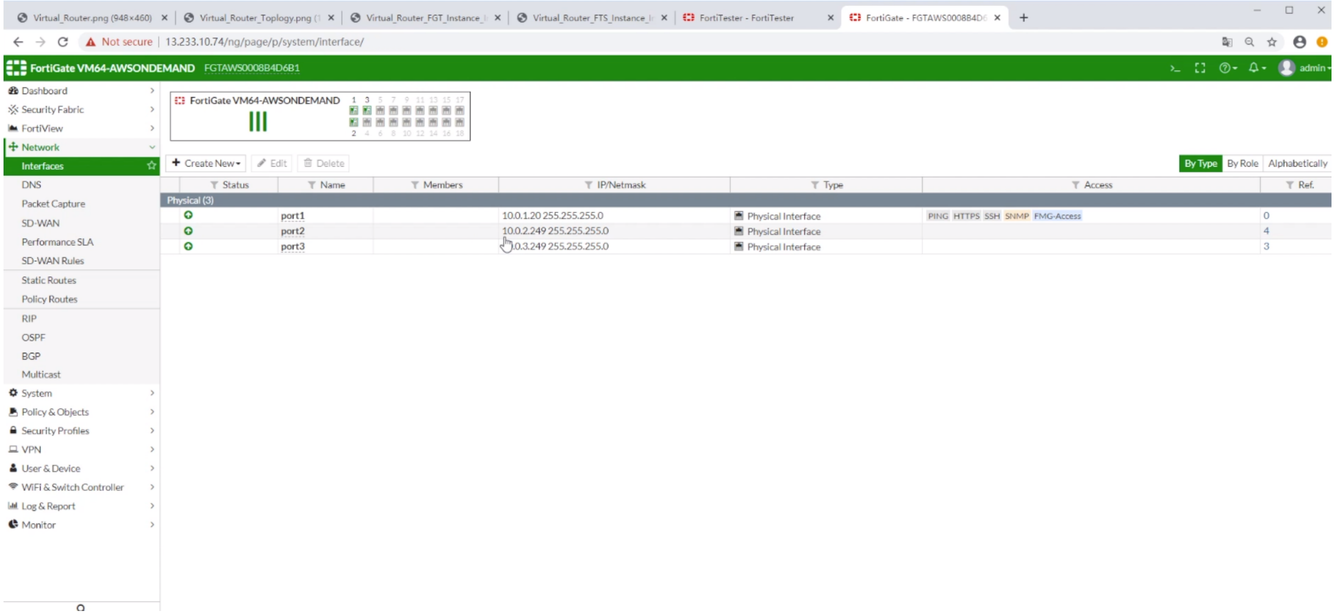
IP Address	10.0.3.117

Subnet

IP Address or Range	18.1.1.100
Netmask	16
Gateway	10.0.3.249
Peer Network	17.1.0.0/16

- The client, server Virtual Router IP Addresses correspond to AWS eth1, eth2 address (10.0.2.41 10.0.3.117).
- The gateway address corresponds to FortiGate interface Port2, Port3 address (10.0.2.249, 10.0.3.249).
- The Client Peer Network address corresponds to the server subnet.
- The Server Peer Network address corresponds to the client subnet.

FortiGate on AWS

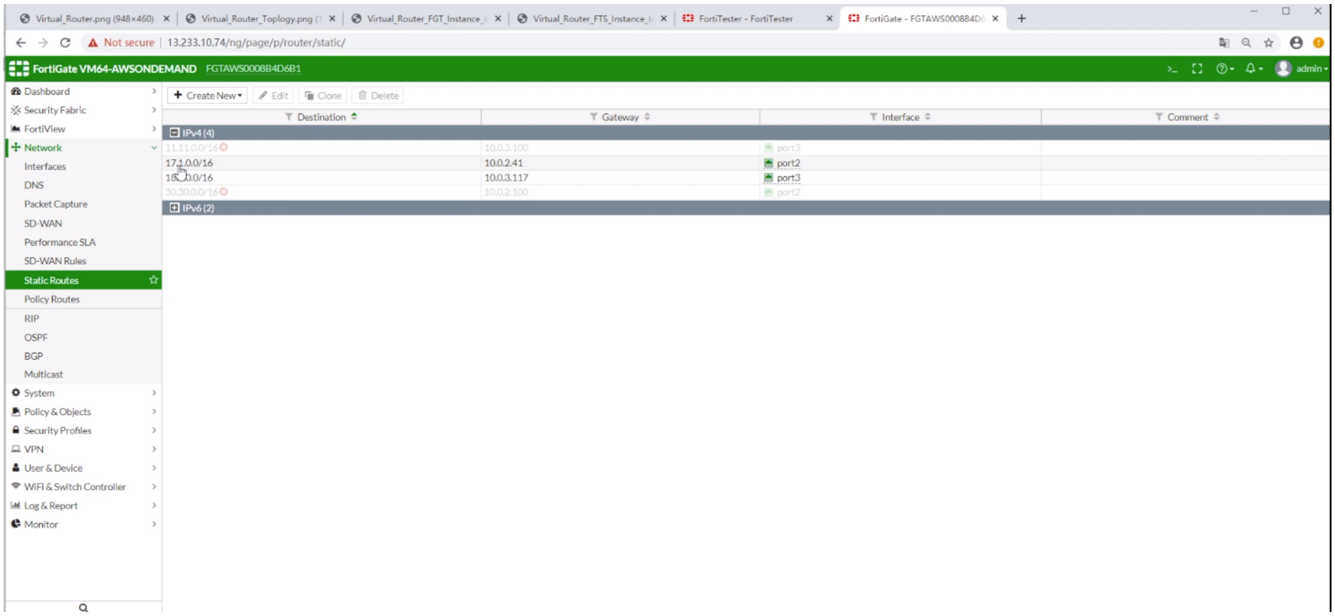


Status	Name	Members	IP/Netmask	Type	Access	Ref.
Physical (3)						
○	port1		10.0.1.20 255.255.255.0	Physical Interface	PING HTTPS SSH SNMP FMG-Access	0
○	port2		10.0.2.249 255.255.255.0	Physical Interface		4
○	port3		10.0.3.249 255.255.255.0	Physical Interface		3

Here the network interfaces correspond to AWS interface eth1, eth2 with the IP addresses we configured earlier. The virtual router subnets are pointing to FortiGate gateways.

Now, go to **FortiGate > Network > Static Routes**.

Remember that the DUT needs to point both the static route to the 17 network and the 18 network to the client server side of FortiTester, so you need to set the static route pointing to the virtual router IP addresses.



Destination	Gateway	Interface	Comment
IPv4 (4)			
11.11.0.0/16	10.0.3.100	port3	
17.1.0.0/16	10.0.2.41	port2	
18[illegible]0.0/16	10.0.3.117	port3	
30.30.0.0/16	10.0.2.100	port2	
IPv6 (2)			

This should match up with the FortiTester interface settings from earlier.

Now that we have finished configuring the network objects, we can use it on a test case with HTTP/CPS.

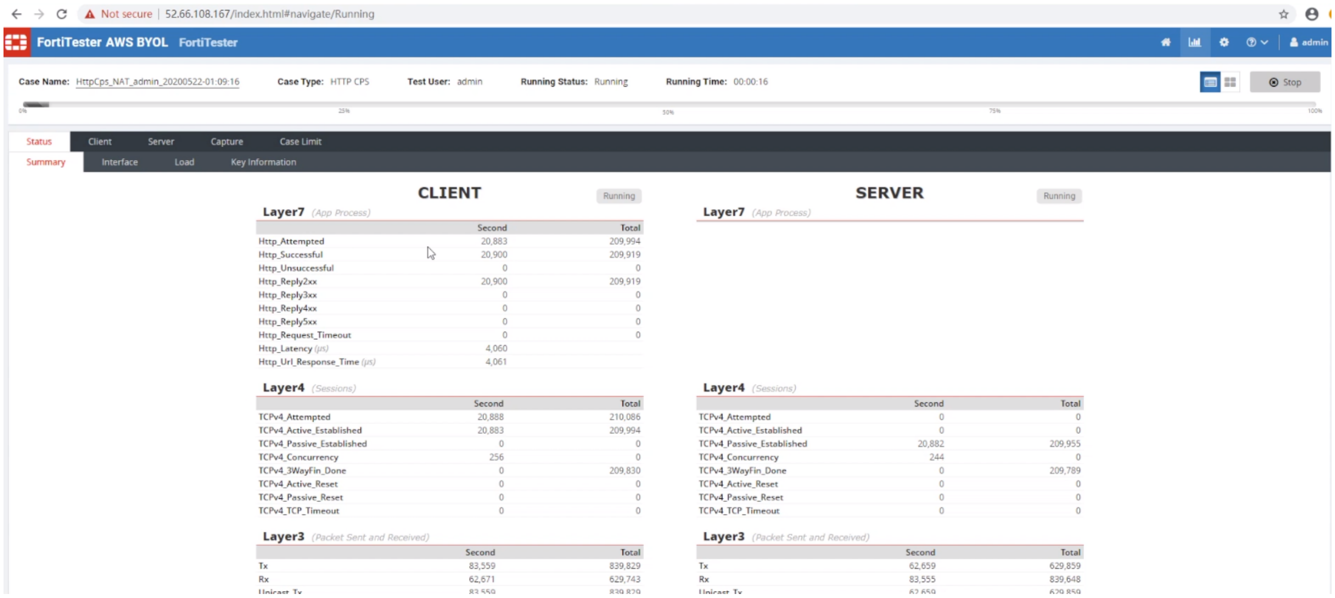
To start an HTTPS CPS test:

1. Go to **Cases > Performance Testing > HTTPS > CPS** to display the test case summary page.
2. Click **+ Create New** to display the **Select case options** dialog box.
3. In the popup dialog, for the **Network Config** option, make sure to select virtual router.
4. Click **OK** to continue.
5. Use the default settings for HTTP/CPS case.
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.

You can choose how long you want to run the test case in FortiTester.

Test results



Case Name: HttpCps_NAT_admin_20200522-01:09:16 **Case Type:** HTTP CPS **Test User:** admin **Running Status:** Running **Running Time:** 00:00:16

CLIENT Running

Layer7 *(App Process)*

	Second	Total
Http_Attempted	20,883	209,994
Http_Successful	20,900	209,919
Http_Unsuccessful	0	0
Http_Reply2xx	20,900	209,919
Http_Reply3xx	0	0
Http_Reply4xx	0	0
Http_Reply5xx	0	0
Http_Request_Timeout	0	0
Http_Latency *(μs)*	4,060	
Http_Url_Response_Time *(μs)*	4,061	

Layer4 *(Sessions)*

	Second	Total
TCPv4_Attempted	20,888	210,086
TCPv4_Active_Established	20,883	209,994
TCPv4_Passive_Established	0	0
TCPv4_Concurrency	256	0
TCPv4_3WayFin_Done	0	209,830
TCPv4_Active_Reset	0	0
TCPv4_Passive_Reset	0	0
TCPv4_TCP_Timeout	0	0

Layer3 *(Packet Sent and Received)*

	Second	Total
Tx	83,559	839,829
Rx	62,671	629,743
Unicast_Tx	83,559	839,829

SERVER Running

Layer7 *(App Process)*

Layer4 *(Sessions)*

	Second	Total
TCPv4_Attempted	0	0
TCPv4_Active_Established	0	0
TCPv4_Passive_Established	20,882	209,955
TCPv4_Concurrency	244	0
TCPv4_3WayFin_Done	0	209,789
TCPv4_Active_Reset	0	0
TCPv4_Passive_Reset	0	0
TCPv4_TCP_Timeout	0	0

Layer3 *(Packet Sent and Received)*

	Second	Total
Tx	62,659	629,859
Rx	83,555	839,648
Unicast_Tx	62,659	629,859

Here the client is generating HTTP traffic and the server is receiving this traffic.

It's important to look for the HTTP_ Attempted and HTTP_Successful. Here, there are 0 unsuccessful requests, which means that the virtual router setup works on FortiTester.

Security testing

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

- DDoS
- Fuzzing
- IPS
- Malware
- Web Protection
- Mixed Traffic

Also, you can manage the following:

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

DDoS cases

The following types of DDoS cases are available:

- Single packet flood
- TCP session flood
- HTTP session flood
- Concurrent session flood
- UDP

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 DDoS single packet flood test:

1. In *Security Testing*, expand *DDoS* and click *Single Packet Flood*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.

5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

DDoS single packet flood test case options

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.
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.
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.
Network Settings	

Settings	Guidelines
If you have selected a network config template, the network settings automatically inherit the configurations in the template. See Using network configuration templates for the description of network settings.	
Load	
DDoS Type	
Packet Config	Default–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.
Packet Group	Advanced–This object represents one network packet. The user uses a Single Packet group to specify the packet types and percentages rather than select from a list of existing DDoS types (as in the "default" case). The user will be able to configure the packet details in *Security Testing > Objects > Single Packet Group*. The specific parameters depend on the packet type, which the user selects when creating the object. The payload contents of the packets will be random (excluding UDP VSE). For all of the packet types (excluding ARP, which is IPv4 only), the user also needs to specify the IP version. See: Single Packet Group.
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	

Settings	Guidelines
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 DDoS TCP session flood test:

1. In *Security Testing*, expand *DDoS* and click *TCP Session Flood*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

DDoS TCP session flood test case options

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.
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.
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.
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 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
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

Settings	Guidelines
	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 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
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **NOTE**: Setting this timer can adversely affect TCP performance.
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 DDoS HTTP session flood test:

1. In *Security Testing*, expand *DDoS* and click *HTTP Session Flood*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

DDoS HTTP session flood test case options

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 Scripts on page 187.
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 Hosts on page 184.
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 SNMP Monitors on page 188.
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 25 for the description of network settings.	
Load	

Settings	Guidelines
Simulated Users	Number of users to simulate.
Ramp Up Time	The duration in seconds for which new sessions can be opened, attempting to reach the desired Connections per Second configured. (Range: 0 - 300). **NOTE:** If FortiTester cannot reach the Connections per Second configured during the specified Ramp Up Time, it will keep the highest CPS it reached during the Ramp Up Time.
Ramp Down Time	The duration in second during which the device ramps down the number of connections it is making. 0 will cause the FortiTester to cease generating sessions. (Range: 0 - 300).
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.

Settings	Guidelines
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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **NOTE**: Setting this timer can adversely affect TCP performance.
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 DDoS concurrent session flood test:

1. In *Security Testing*, expand *DDoS* and click *Concurrent Session Flood*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

DDoS concurrent session flood test case options

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.

Settings	Guidelines
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates.
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.
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.
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 for the description of network settings.	
Load	
Simulated Users	Number of users to simulate.
Maximum Concurrent Connections	Determines the maximum number of concurrent TCP connections supported through or with the DUT/SUT. This test is intended to find the maximum number of entries the DUT/SUT can store in its connection table.
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

Settings	Guidelines
	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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
Client/Server Network	
Network MTU	The maximum transmission unit size.

Settings	Guidelines
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 DDoS UDP packet flood test:

1. In *Security Testing*, expand *DDoS* and click *UDP Packet Flood*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

DDoS UDP packet flood test case options

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.
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.
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.
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 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.
Frame Size	The user can select either RFC fixed frame size (64, 128, 256, 512, 1024, 1280 or 1518), or User Defined. In v7.0.0+ FortiTester allows “user defined” frame sizes. This is useful if devices in path add/remove to packet size, so you can adjust the frame size FortiTester sends out.
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	

Settings	Guidelines
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.

Starting a fuzzing test

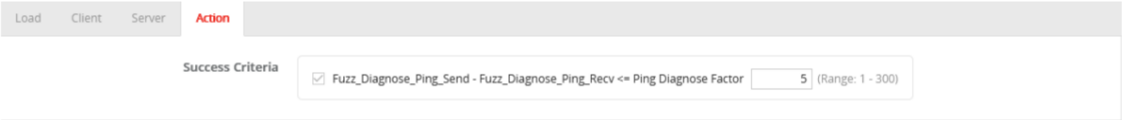
Fuzzing cases measure the device's ability to handle invalid IP, TCP, UDP, and ICMP packets, which send invalid fuzzed packets to DUT devices and validate whether the device continues to operate.

To start a fuzzing test:

1. Go to **Security Testing> Fuzzing** to display the test case summary page.
2. Click **+ Create New** to display the Case Options dialog box.
3. Configure the network settings and click **OK** to continue.
4. Set **Specifics > Load**: ICMP Options, TCP Options, UDP Options, Generic Options, IP Options.

ICMP Option	Enable ICMP–Control switch to enable ICMP protocol. ICMP Simuser–The count of simusers sending ICMP packets. ICMP Fuzz Fields includes “Bad ICMP Code”, “Bad ICMP Type” with a value from 0 to 100, which means the maximum percentage of packets transmitted has a randomized ICMP fields.
TCP Option	TCP control switch, simuser number and TCP Fuzz Fields.
UDP Option	UDP control switch, simuser number and UDP Fuzz Fields.
Generic Option	“Payload Size”, “Seed For The Pseudo-random Number Generator” and “Maximum Number of Simultaneous Corruption”.
IP Option	IP Fuzz Fields.

5. Set **Specifics > Action**: Success Criteria.



Success Criteria ☑ Fuzz_Diagnose_Ping_Send - Fuzz_Diagnose_Ping_Recv <= Ping Diagnose Factor 5 (Range: 1 - 300)

This field provides the judgement criteria of fuzzing test, which is succeed only if “Fuzz_Diagnose_Ping_Send” minus “Fuzz_Diagnose_Ping_Recv” is less than or equal to the input number “Ping Diagnose Factor” .

Starting a malware test

The Malware case sends files with HTTP/FTP/SMTP/IMAP/POP3/SMB protocol and detects viruses in files. Malware Strike packs are provided and refreshed regularly by FortiGuard updates.

Different tests can be run depending on the FortiGuard malware object group configuration (based on OS type, malware type e.g. ransomware, created date).

To start a malware test:

1. In Security Testing, expand *Malware* and click *Malware*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select the *Protocol* to use.

   If *HTTPS* is selected, you may specify ciphers and certificate groups for the SSL/TLS component and select a malware group object to be sent within the HTTPS traffic.
5. Select a *Certificate Group*, if applicable.
6. Click *OK*.
7. Configure the test case options described below.
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.

Malware test case options

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.
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.
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.
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 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 web application 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 acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
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	
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	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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
Client/Server Network	
Network MTU	The maximum transmission unit size.
TFTP Block Size	Specify a Block Size. The default is 512 bytes.
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	
Malware File Group	Select an existing malware file from the list or click *Manage Group* to upload new files.

IPS cases

The following types of IPS cases are available:

- Attack replay
- HTTP evasion

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. 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 IPS attack replay test:

1. In *Security Testing*, expand *IPS* and click *Attack Replay*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

IPS attack replay test case options

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.

Settings	Guidelines
Script Config	Select the script that will run before/after the test. To create a script, see Using script object templates.
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.
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.
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 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.
Maximum Timeout Packet Count	Option gives users finer control over the max packet loss (from 1-4294,967,295) before FortiTester stops sending packets in PCAP replay package.
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.
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

Settings	Guidelines
	traffic. See Managing the User Instruction group.

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. 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 IPS HTTP evasion test:

1. In *Security Testing*, expand *IPS* and click *HTTP Evasion*.
2. Click *Create New*.
3. Configure the network or select a network template. See Using network configuration templates for how to create a network template.
4. Select a *Certificate Group*, if applicable.
5. Click *OK*.
6. Configure the test case options described below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

IPS HTTP evasion test case options

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.
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.
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.
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 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.

Settings	Guidelines
Maximum Timeout Packet Count	Option gives users finer control over the max packet loss (from 1-4294,967,295) before FortiTester stops sending packets in pcap replay package.
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.

Web protection cases

The following types of web protection cases are available:

- Web protection
- Web crawler

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 *+ Create New* 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 25 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 below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Web Protection test case options

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.
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.
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.
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 25 for the description of network settings.	
Load	
Loops	Number of times to send the attacks. 0 means as many as possible.

Settings	Guidelines
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 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 acknowledgment is sent on the data frame, not in an individual frame. Otherwise, it sends an ACK frame individually. This feature only works with get/post requests.
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

Settings	Guidelines
	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.
FinACK Timer	This value measures the amount of time that a SimUser waits after it finishes its actions and before it directly breaks all of its TCP connections (that is, the time to wait to receive the LAST_ACK message for a FIN request). A value of 0 disables the timer. **Note**: Setting this timer can adversely affect TCP performance.
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.

Starting a Web protection 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 *+ Create New* 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 25 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 below.
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 1: You can 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.

Tip 2: You can add or edit a comment when the test is running. This comment can be used to search for the test result in the *Results* page. This is useful especially when the test runs for a long time.

Web protection web crawler test case options

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.

Settings	Guidelines
Capture Packet	
Capture Packet	Optional. 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.
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.

Managing security testing objects

The following types of security testing objects are available:

- Networks
- Certificates and certificate groups
- Payloads
- Scripts
- SNMP Monitors
- Single Packets
- Single Packet Group
- User Intrusion group
- FortiGuard Intrusion group
- User Malware group
- FortiGuard Malware Group
- Web protection group
- URL
- Custom traffic template

Networks

Networks defines the network connection topology of the FortiTester and DUT devices. Test case can reference a defined Network Topology object.

To create a network object:

1. Go to **Cases > Performance Testing > Objects > Networks**.
2. Click **+Create New** to create a network object.
3. Configure the options with the Network Configuration Templates. Click **OK**.
4. Name the Network object, set the Network Settings (see the Network Configuration Templates), click **Save**.
5. Repeat these steps to create more objects.

Certificates and 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 **+ Create New** 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 **+ Create New**.
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.

Payloads

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 **+ Create New** 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.

Scripts

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** or **Security Testing > Objects > Scripts**.
2. Click **+ Create New** 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.

SNMP Monitors

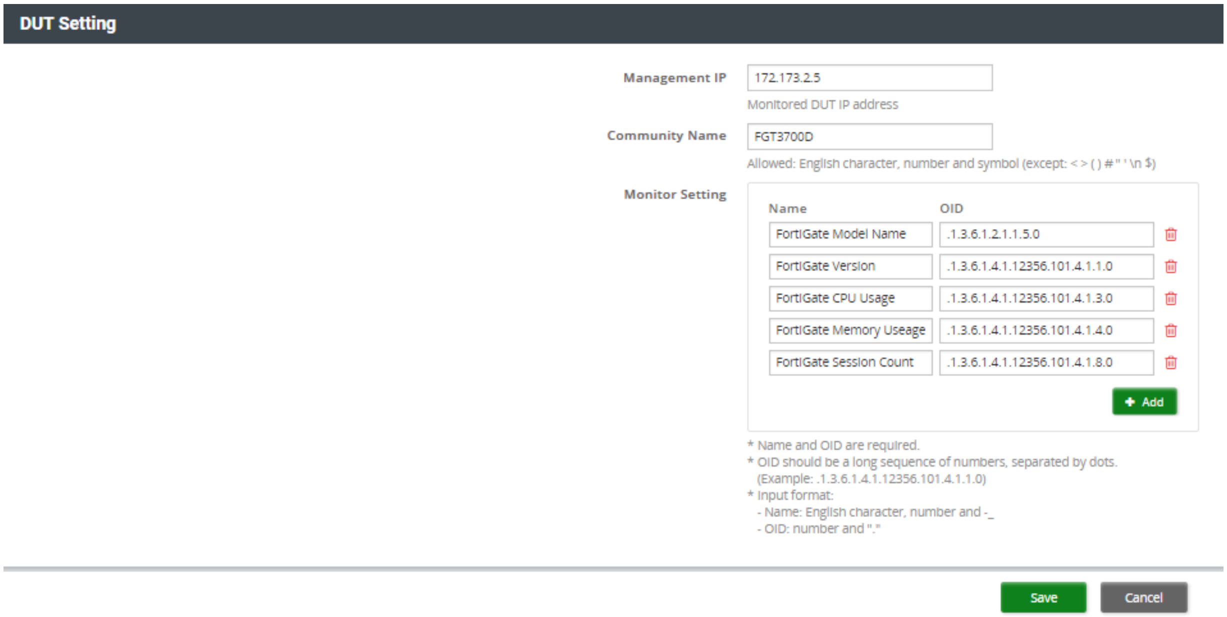
FortiTester allows you to monitor a FortiGate device under test (DUT) from the management interface. To do so, you must create a DUT monitor object template and then import it when you configure test settings.

To create a DUT monitor object template:

1. Go to **Performance Testing** or **Security Testing > Objects > SNMP Monitors**.
2. Click **+ Create New** 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 $)

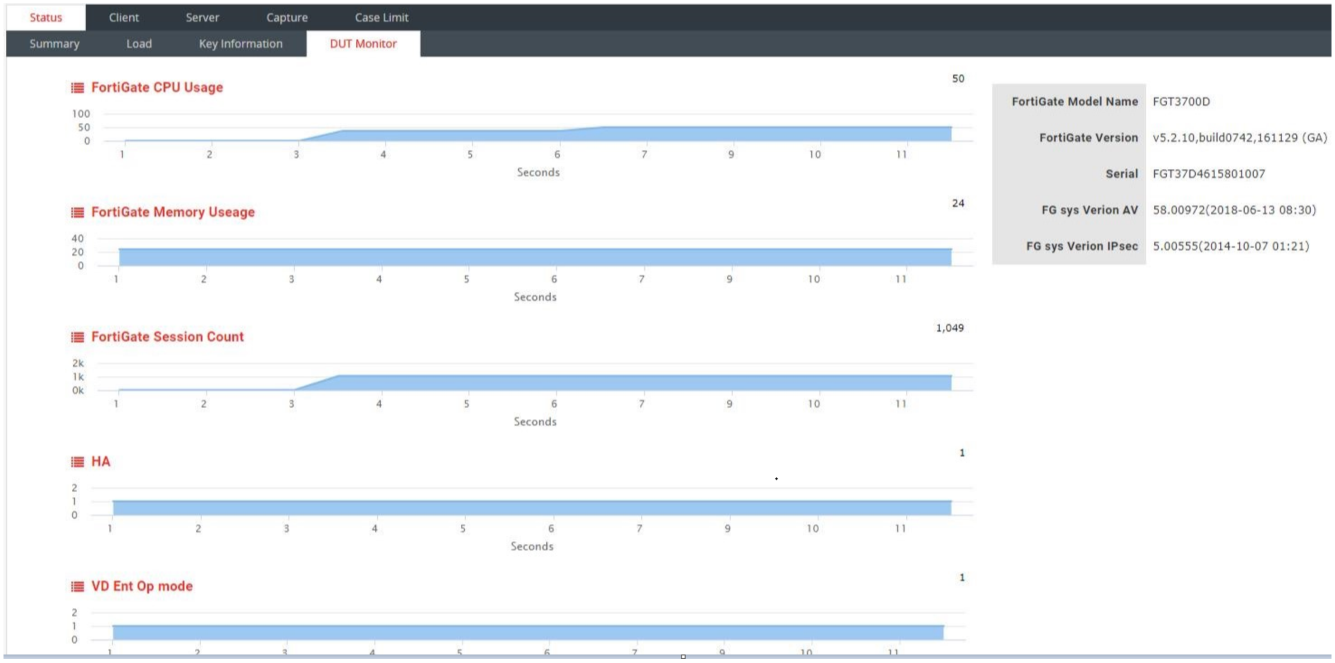
Monitor Setting

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)

Single Packets

The single packet defines the packet proportion that can be used in single packet groups.

To create a Single Packet:

1. Go to **Security Testing > Objects > Single Packets**.
2. Click **+ Create New** to display the configuration page.
3. Configure the following settings:
    - IP Version—The IP Version of your packet type. **NOTE:** ARP is IPv4 only.

      IP Parameters

IPv4	DSCP: 0 - 63 Identification: set value or random TTL: 1 - 255 DF: 0 - 1 MF: 0 - 1 Fragment Offset: 0 - 8189
IPv6	DSCP: 0 - 63 Hop Limit: 1 - 255 Fragment: toggle on/off Fragment Offset (if fragment): 0 - 8191

    - Packet Type

ARP	SMAC address prefix: xx-xx (the rest generated randomly), **NOTE:** IPv4 only.
DNS Query	IP parameters UDP parameters (see UDP type) but omit payload and payload size range. Domain Subdomain: specify or random
GRE/UDP	Outer IP parameters Inner IP parameters UDP parameters (see UDP below)
ICMP	IP parameters Payload Size: fixed value or range Message type: Echo
TCP	IP parameters Source Port: fixed value or range, available range 1 - 65,535 Destination Port: fixed value or range, available range 1 - 65,535 Payload Size: fixed value or range

	Flags: SYN, ACK, PSH, RST, FIN, URG, CWR, ECE (toggle on/off)
UDP	IP parameters Source port: fixed value or range, available range 1 - 65,535 Destination port: fixed value or range, available range 1 - 65,535 Payload: random or VSE Payload size (if random payload): fixed value or range IPv4 UDP checksum: toggle on/off

4. Click **Save**.

Single Packet Group

The single packet groups are used in DDoS Single Packet Flood cases. Each object in the group is associated with a percentage. Percentages should sum to 100. The Single Packet objects in same group should have the same IP version.

To create a Single Packet Group:

1. Go to **Security Testing > Objects > Single Packet Group**.
2. Click **+ Create New** to display the configuration page.
3. Configure the following settings:
   - Name—The name of your Single Packet Group
   - IP Version—The IP Version of your packet type. **NOTE:** ARP is IPv4 only.
4. Click **+ Create New** to add desired packets and set their weight. Create Single Packets in **Objects > Single Packets**.

User Intrusion group

You can use this service to manage the custom attack traffic and group. Upload pcap files that contain your customized attack traffic.

To create a user instruction group:

1. Go to **Cases > Security Testing > Objects > User Intrusion Group**.
2. Click **+ Create New** 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.

FGD Intrusion group

FortiGuard Intrusion Group allows you to create a customized group from FortiGuard intrusion services. It can be referenced by Attack Replay Profile.

To create a FGD Intrusion group:

1. Go to **Cases** > **Security Testing** > **Objects** > **FGD Intrusion Group**.
2. Click **+ Create New** to create a group to include the desired FDG instrusions. See FortiGuard updates on how to update the services.
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 **+ Create New**.
6. Select the FGD intrusions you want to include in this group.
7. Click **Save**.
8. Click **Close**.

User Malware group

Manage the Malware file and group. You can reference them in the Malware cases.

To create a malware file group:

1. Go to **Cases** > **Security Testing** > **Objects** > **User Malware Group**.
2. Click **+ Create New** 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 Malware files. Repeat this step to upload more files.

FGD Malware Group

FGD Malware group is the latest malware database (strike pack) provided by FortiGuard. It allows users to conduct security malware cases by stream malware via different network protocols such as HTTP/POP3/IMAP/SMB/SMTP/FTP to test DUT’s detection/blocking capabilities.

FGD Malware requires a subscription license. See: **System settings > System > FortiGuard.**

To create a FGD Malware group:

1. Go to **Cases** > **Security Testing** > **Objects** > **FGD Intrusion Group**.
2. Click **+ Create New** to create a group to include the desired Malware instrusions. See FortiGuard updates on how to update the services.
3. Enter a name for the group. Click **Add**.
4. Click **+ Create New** to create a new file. Under Manage Files, conduct searches based on criteria you specify.
5. Click **Save**.
6. Click **Close**.

Web protection group

Manage web protection group being referenced in the Web Protection cases.

To create a Web Protection group:

1. Go to **Cases** > **Security Testing** > **Objects** > **Web Protection Group**.
2. Click **+ Create New** to create a group where the uploaded files will be assigned.

3. Enter a name for the group. Click **Add**.
4. Click **Create New**.
5. Select the web protection signatures you want to include in this group.
6. Click **Save**.
7. Click **Close**.

URLs

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 **+ Create New** 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).

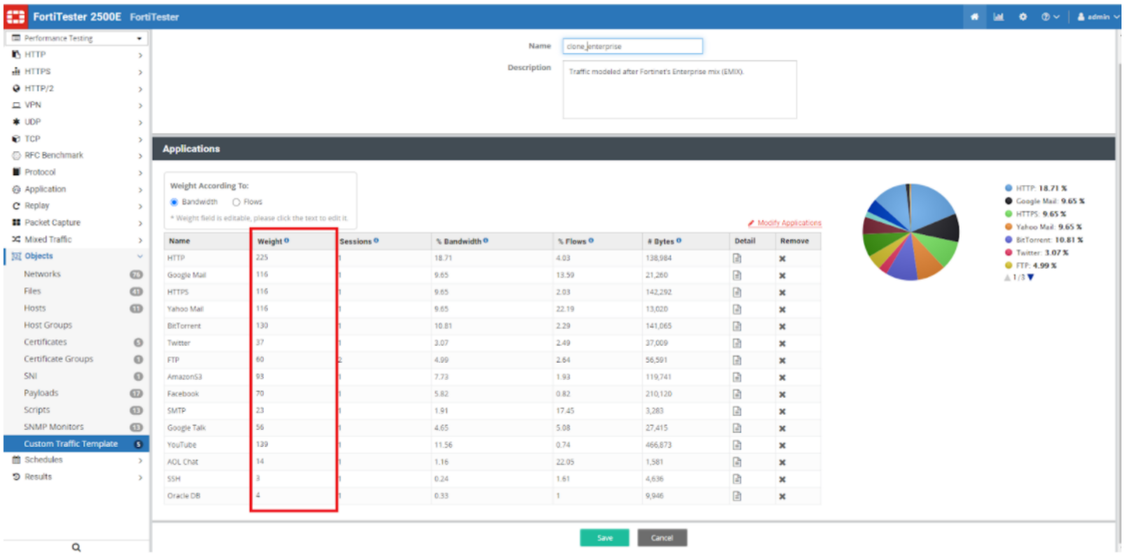
After you have created a URL list template, you can clone or export it as a zip file. This template can now be selected from the URL Group option on the popup dialogue when running a test.

Creating a custom traffic template

This service is used to manage the custom traffic template. It can be used in mixed traffic cases.

To create a custom traffic template

1. Go to **Performance Testing** or **Security Testing > Objects > Custom Traffic Template** to create custom template.
2. Click **+ Create New** and select the applications for the template.
3. Double click **Weight** to edit weights. Click the Detail icon to edit specifics. Don't forget to save.



Name: clone_enterprise

Description: Traffic modeled after Fortinet's Enterprise mix (EMIX).

Weight According To:
● Bandwidth ○ Flows

* Weight field is editable, please click the text to edit it.

Name	Weight	Sessions	% Bandwidth	% Flows	# Bytes	Detail	Remove
HTTP	225	1	18.71	4.03	138,984		✖
Google Mail	116	1	9.65	13.59	21,260		✖
HTTPS	116	1	9.65	2.03	142,292		✖
Yahoo Mail	116	1	9.65	22.19	13,020		✖
BitTorrent	130	1	10.81	2.29	141,065		✖
Twitter	37	1	3.07	2.49	37,009		✖
FTP	60	2	4.99	2.64	56,591		✖
AmazonS3	93	1	7.73	1.93	119,741		✖
Facebook	70	1	5.82	0.82	210,120		✖
SMTP	23	1	1.91	17.45	3,283		✖
Google Talk	56	1	4.65	5.08	27,415		✖
YouTube	139	1	11.56	0.74	466,873		✖
AOL Chat	14	1	1.16	22.05	1,581		✖
SSH	3	1	0.24	1.61	4,636		✖
Oracle DB	4	1	0.33	1	9,946		✖

4. Go to **Performance Testing** or **Security Testing > Mixed Traffic**, create a new case, select **Protocol** at **Mixed Traffic By**, and choose any Custom Traffic Template. Click Ok.
5. Go to **Specifics > Action**, and edit Bandwidth Upper Limit to determine maximum bandwidth.

Maintaining FortiGuard intrusion and webprotections 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.

Security testing cookbook

This section provides examples for running security tests.

Using an IPS Attack Replay case

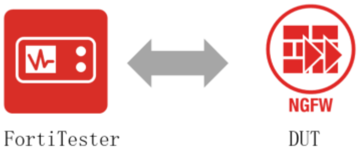
FortiTester can test security systems by replaying a FortiGuard intrusion pcaps or customized set of attack traffic. The FortiGuard intrusion package provides more than 1600 attack samples. The test result shows the CVE-ID, Application, Protocol, OS and Type, etc. for every attack. You can also see the attack list in the *Security Testing > Maintenance> Intrusion Definitions*.

You have to purchase the Premium or Standard intrusion service if you are going to use Fortinet IPS intrusion pcaps.

Before you begin:

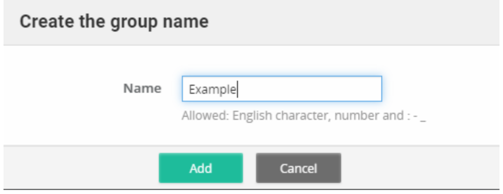
- Optional. If you want to test custom attack traffic, you must create a package of pcap files that can be replayed. Follow the file naming convention: `Description[_CVE-$CVEID].pcap`. Here "`[]`" means optional. The file type can be .pcap, .tgz, .tar.gz, or .zip. A .tgz, .tar.gz, or .zip file includes 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.

Topology



To configure a FortiGuard intrusion group:

1. Go to *Cases > Security Testing > Objects > FGD Intrusion Group.*
2. Click *+ Create New* then input the group name.

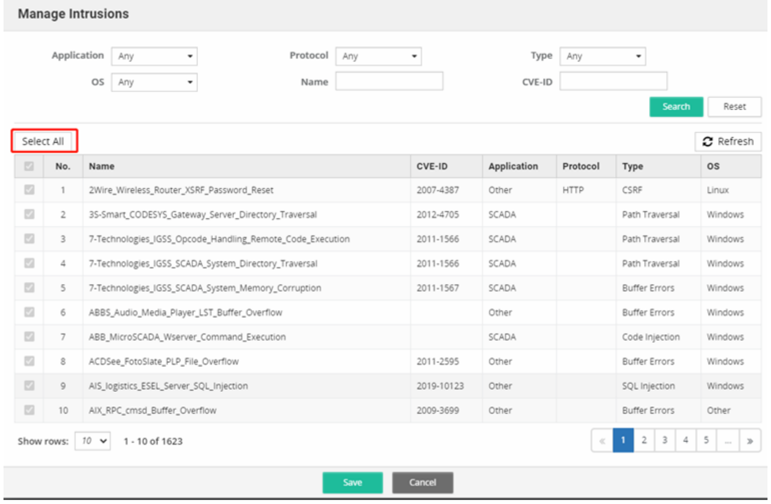


Create the group name

Name: Example

Allowed: English character, number and : - _

3. Click *+ Add*.
4. Click *Create New* to select the intrusions. You can click *Select All* to select all intrusions.



Manage Intrusions

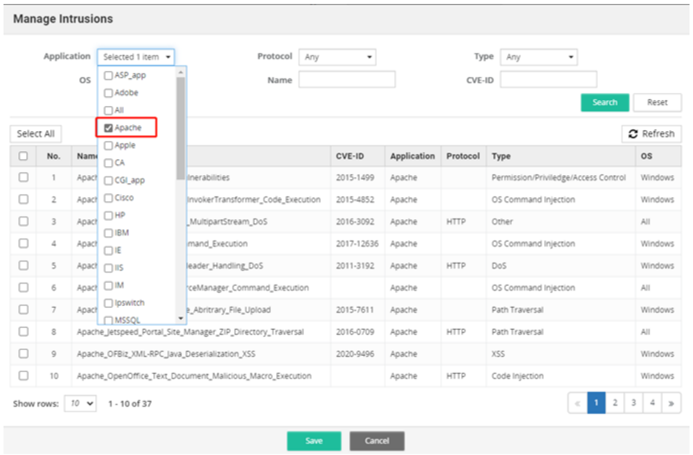
Application: Any — Protocol: Any — Type: Any

OS: Any — Name: — CVE-ID:

☑	No.	Name	CVE-ID	Application	Protocol	Type	OS
☑	1	2Wire_Wireless_Router_XSRF_Password_Reset	2007-4387	Other	HTTP	CSRF	Linux
☑	2	3S-Smart_CODESYS_Gateway_Server_Directory_Traversal	2012-4705	SCADA		Path Traversal	Windows
☑	3	7-Technologies_IGSS_Opcode_Handling_Remote_Code_Execution	2011-1566	SCADA		Path Traversal	Windows
☑	4	7-Technologies_IGSS_SCADA_System_Directory_Traversal	2011-1566	SCADA		Path Traversal	Windows
☑	5	7-Technologies_IGSS_SCADA_System_Memory_Corruption	2011-1567	SCADA		Buffer Errors	Windows
☑	6	ABBS_Audio_Media_Player_LST_Buffer_Overflow		Other		Buffer Errors	Windows
☑	7	ABB_MicroSCADA_Wserver_Command_Execution		SCADA		Code Injection	Windows
☑	8	ACDSee_FotoSlate_PLP_File_Overflow	2011-2595	Other		Buffer Errors	Windows
☑	9	AIS_logistics_ESEL_Server_SQL_Injection	2019-10123	Other		SQL Injection	Windows
☑	10	AIX_RPC_cmsd_Buffer_Overflow	2009-3699	Other		Buffer Errors	Other

Show rows: 10 — 1 - 10 of 1623

You can also apply filters from under Application, or from Protocol, Type, and so on.



Manage Intrusions

Application: Selected 1 item
Protocol: Any
Type: Any
OS
Name
CVE-ID

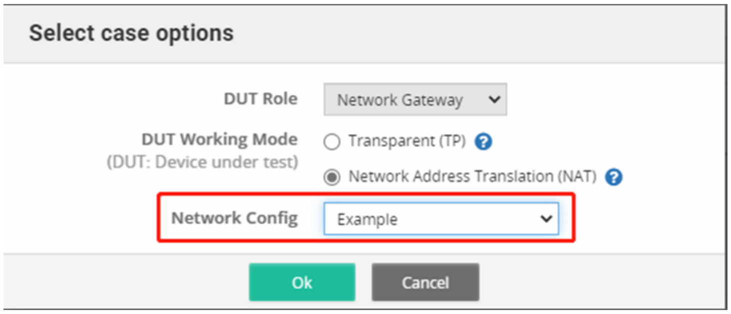
☐	No.	Name	CVE-ID	Application	Protocol	Type	OS
☐	1	Apach lnerabilities	2015-1499	Apache		Permission/Priviledge/Access Control	Windows
☐	2	Apach InvokerTransformer_Code_Execution	2015-4852	Apache		OS Command Injection	Windows
☐	3	Apach _MultipartStream_DoS	2016-3092	Apache	HTTP	Other	All
☐	4	Apach mand_Execution	2017-12636	Apache		OS Command Injection	Windows
☐	5	Apach leader_Handling_DoS	2011-3192	Apache	HTTP	DoS	Windows
☐	6	Apach rceManager_Command_Execution		Apache		OS Command Injection	All
☐	7	Apach e_Abritrary_File_Upload	2015-7611	Apache		Path Traversal	Windows
☐	8	Apache_Jetspeed_Portal_Site_Manager_ZIP_Directory_Traversal	2016-0709	Apache	HTTP	Path Traversal	All
☐	9	Apache_OFBiz_XML-RPC_Java_Deserialization_XSS	2020-9496	Apache		XSS	Windows
☐	10	Apache_OpenOffice_Text_Document_Malicious_Macro_Execution		Apache	HTTP	Code Injection	Windows

Show rows: 10   1 - 10 of 37

5. Click *Save*.

How to configure the Attack Replay case

1. Go to *Security Testing > IPS > Attack*.
2. Click the *Create New* then select the network object created before.



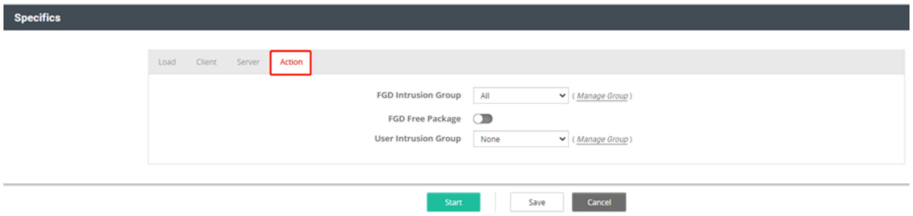
Select case options

DUT Role: Network Gateway

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

Network Config: Example

3. Use the group created before.



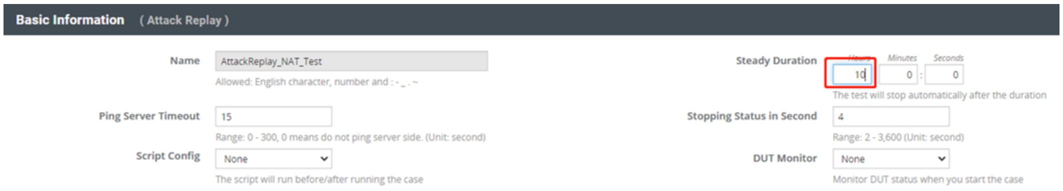
Specifics

FGD Intrusion Group: All (Manage Group)

FGD Free Package

User Intrusion Group: None (Manage Group)

In order to completely replay all pcaps, configure the case duration to a bigger number, for example 10 hours.



Basic Information (Attack Replay)

Name: AttackReplay_NAT_Test
Allowed: English character, number and : - _ . ~

Ping Server Timeout: 15
Range: 0 - 300, 0 means do not ping server side. (Unit: second)

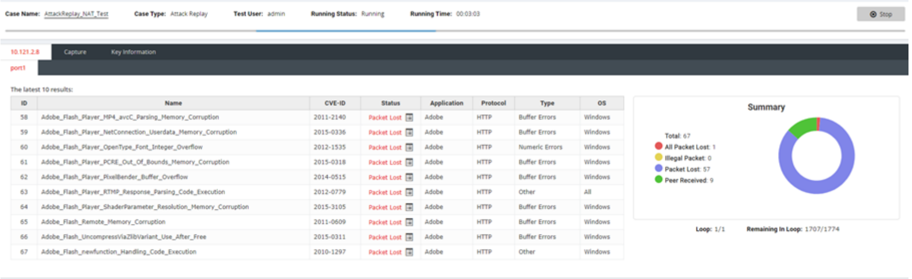
Script Config: None
The script will run before/after running the case

Steady Duration: Hours 10 : Minutes 0 : Seconds 0
The test will stop automatically after the duration

Stopping Status in Second: 4
Range: 2 - 3,600 (Unit: second)

DUT Monitor: None
Monitor DUT status when you start the case

4. Click *Start*.



Case Name: AttackReplay_NAT_Test **Case Type:** Attack Replay **Test User:** admin **Running Status:** Running **Running Time:** 00:03:03

The latest 10 results:

ID	Name	CVE-ID	Status	Application	Protocol	Type	OS
58	Adobe_Flash_Player_MP4_avcC_Parsing_Memory_Corruption	2011-2140	Packet Lost	Adobe	HTTP	Buffer Errors	Windows
59	Adobe_Flash_Player_NetConnection_Userdata_Memory_Corruption	2015-0336	Packet Lost	Adobe	HTTP	Buffer Errors	Windows
60	Adobe_Flash_Player_OpenType_Font_Integer_Overflow	2012-1535	Packet Lost	Adobe	HTTP	Numeric Errors	Windows
61	Adobe_Flash_Player_PCRE_Out_Of_Bounds_Memory_Corruption	2015-0318	Packet Lost	Adobe	HTTP	Buffer Errors	Windows
62	Adobe_Flash_Player_PixelBender_Buffer_Overflow	2014-0515	Packet Lost	Adobe	HTTP	Buffer Errors	Windows
63	Adobe_Flash_Player_RTMP_Response_Parsing_Code_Execution	2012-0779	Packet Lost	Adobe	HTTP	Other	All
64	Adobe_Flash_Player_ShaderParameter_Resolution_Memory_Corruption	2015-3105	Packet Lost	Adobe	HTTP	Buffer Errors	Windows
65	Adobe_Flash_Remote_Memory_Corruption	2011-0609	Packet Lost	Adobe	HTTP	Buffer Errors	Windows
66	Adobe_Flash_UncompressViaZlibVariant_Use_After_Free	2015-0311	Packet Lost	Adobe	HTTP	Buffer Errors	Windows
67	Adobe_Flash_newfunction_Handling_Code_Execution	2010-1297	Packet Lost	Adobe	HTTP	Other	Windows

Summary

Total: 67
● All Packet Lost: 1
● Illegal Packet: 0
● Packet Lost: 57
● Peer Received: 9

Loop: 1/1 **Remaining In Loop:** 1707/1774

Status	Meaning
● All Packet Lost	The client did not receive any packets sent by the server and the server did not receive any packets sent by the client.
● Illegal Packet	The package is identified as not a pcap format.
● Packet Lost	The client lost some packets sent by the server or the server lost some packets sent by the client.
● Peer Received	The client received all packets sent by the server and the server received all packets sent by the client.

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, you must install one of the following operating systems on each of the client devices.

- Windows 7, 8, 8.1 or 10, 64 bit
- Linux
- Mac

Installing FortiAgent

FortiAgent facilitates communication between FortiTester and the Remote Access Tools (RATs). Install the FortiAgent client on every target host that is taking part in the adversary emulation operation. Once installed, it will communicate with FortiTester and interact with the RATs to participate in the adversary operation.

The FortiAgent client supports the following platforms:

- Windows
- Linux-AMD64
- Linux-ARM64
- Mac-AMD64
- Mac-ARM64

To install FortiAgent on target hosts:

1. Download the latest release of FortiAgent from FortiTester.
    1. Go to *ATT&CK Testing > Maintenance > Resources*.
    2. In the *Available Clients* table, click the *Download* icon to download the appropriate *FortiAgent* for the target platform.
    3. Download the appropriate *conf.yml* for the target platform.
2. Extract the files from the downloaded archive and save the executable, along with *conf.yml*, to the installation location.
3. Follow the installation and usage instructions in the *README.md* file.
4. After FortiAgent is successfully started on the target hosts, it is listed on the *Agent Monitor* page in FortiTester (*ATT&CK Testing > Monitor > Agent Monitor*).
5. Repeat these steps 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 *+ Create New*.
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 *+ Create New*.
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 *+ Create New*.
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 *+ Create New*.
4. Enter a name for the ability group.
5. Click *OK*.
6. Click *+ Create New*.
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 *+ Create New*.
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.

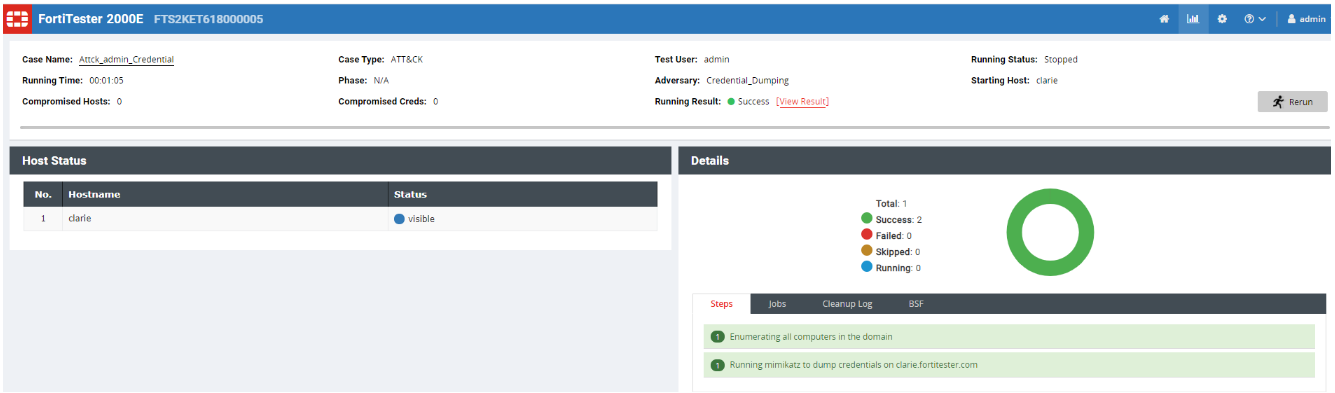
Name	Enter a name for this case.
Adversary	Select the adversary which will perform a collection of operations on the target hosts.
Hosts	Select the host group which includes a collection of target hosts.
Starting Host	Select on which host the adversary actions begins.
Start Method	• Existing RAT: The 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.
Parameter	Select the parameter group to use to locate specific types of files. Parameters must first be created in *ATT&CK Testing > ATT&CK Cases > Parameters*.
Max Fact Execution limitation	Set a maximum number of facts to limit the number of times an ability will process previously discovered facts.
Run As	Enter the username and password of the user on the FortiAgent endpoint.
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.



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

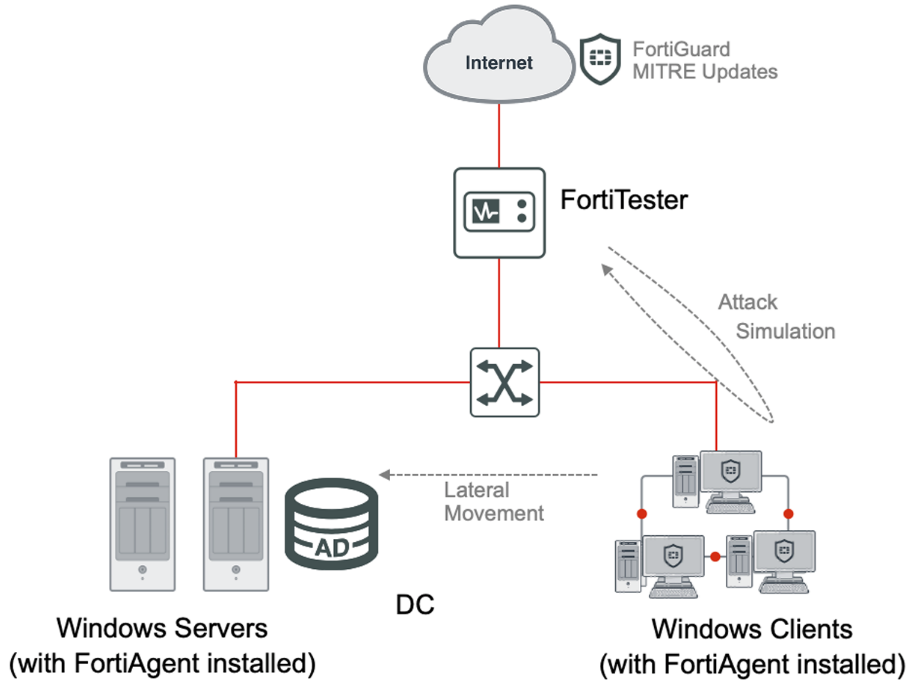
1 Enumerating all computers in the domain

1 Running mimikatz to dump credentials on clarie.fortitester.com

MITRE ATT&CK Breach simulation examples

FortiTester Mitre ATT&CK has the ability to simulate adversarial attacks upon your enterprise network while remaining in a controlled environment. ATT&CK does not just send attacks. It actually can allow your network to simulate what it would be like were it to already be compromised by an attack; for example, the software is already on your network and is collecting your credentials, lateral movements etc.

Topology


Internet
FortiGuard MITRE Updates
FortiTester
Attack Simulation
Lateral Movement
AD
DC
Windows Servers (with FortiAgent installed)
Windows Clients (with FortiAgent installed)

FortiTester provides the MITRE ATT&CK framework, allowing enterprises to simulate breaches and measure defense effectiveness against endpoints.

In the following example, you will see how FortiTester can be configured to perform the following:

- *Credential Dumping* - Uses Mimikatz to dump all windows login across ALL domain machines.
- *Scheduled Task* - Attacker schedules tasks to run, not just on the desktop, but on a higher value target like Windows Server.
- *Exfiltrate* - Attacker will extract information/files out of victims' PCs.
- *Running Powershell* - Run Powershell program on victims' PC, which is a common technique used in attacks.
- *Execution via Win API* - Use Win API to run code on victims' PC.

The following are required to run this example:

- 1 FortiTester
- 1 Windows Client
- 1 Windows Server (to simulate lateral movement)
- Both PC joint AD
- Administration rights on both Windows PC's (to install FortiAgent)

ATT&CK abilities

To view ATT&CK abilities, go to *Maintenance > View 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. 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.

These attacks are updated according to subscription services.

ATT&CK has a rich variety of different techniques, as can be seen below.

The ATT&CK Matrix is version 10 by default, but you can choose to view previous versions from the dropdown in the top right corner.

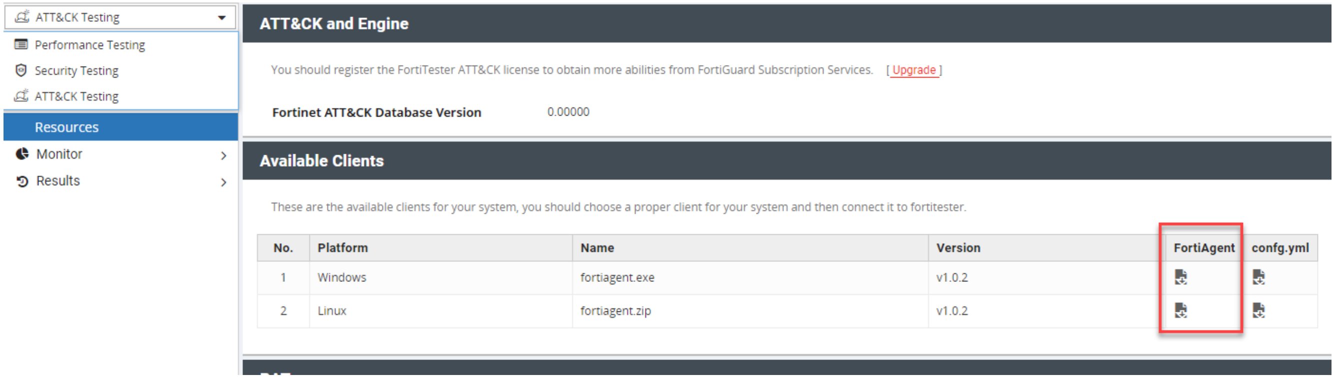
To run a MITRE ATT&CK case:

1. Download lightweighted windows agents onto two hosts. One is on the desktop, the other is on the windows server, yldp.

To install FortiAgent onto windows, administrative rights are required.

2. Go to *Maintenance > Resources* to find the agents and download the one for use. These are installed under FortiAgent folders.

Administration rights are required to install the agent.



ATT&CK and Engine

You should register the FortiTester ATT&CK license to obtain more abilities from FortiGuard Subscription Services. [Upgrade]

Fortinet ATT&CK Database Version 0.00000

Available Clients

These are the available clients for your system, you should choose a proper client for your system and then connect it to fortitester.

No.	Platform	Name	Version	FortiAgent	confg.yml
1	Windows	fortiagent.exe	v1.0.2		
2	Linux	fortiagent.zip	v1.0.2		

3. Download cnfg.yml and place it in the same directory. You also need to edit cofig.yml and fill in the "logging_path" item. Otherwise, the client cannot connect to the server.

4. The installation service will bring up the command box. Run the following command to install FortiAgent:

```
FortiAgent.exe --startup auto install
```

Run the following command to start FortiAgent:

```
FortiAgent.exe start
```

4. After agents are installed they will appear under *Monitor > Agent Monitor* in FortiTester.

5. Now install the second agent on the window's server

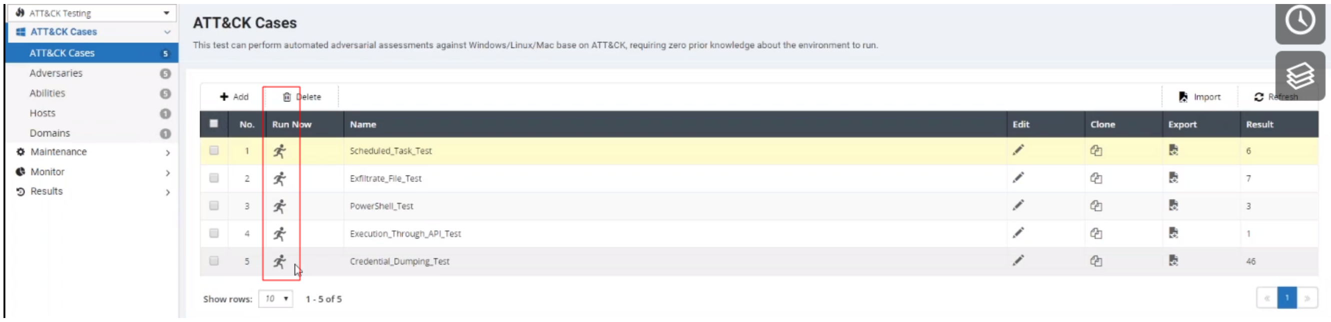
6. Go to *Maintenance > Resources* to downloads the agents onto your PC, then go to the FortiAgent folder and install it.

7. After FortiAgent is successfully started on the target hosts, it is listed on Agent Monitor page on FortiTester (*ATT&CK > ATT&CK Cases > Monitor*). The domain and host configuration specify which domain name this attack will test, as well as which hosts on the domain you are including in the test.

Using attack cases

To run ATT&CK cases, you will need to click on the ATT&CK icon in the GUI upon login, then create a few test cases using the techniques required for this example, as below.

To run an ATT&CK case, go to *ATT&CK Cases > ATT&CK Cases* and select one of the tests. Then click *Run Now*.



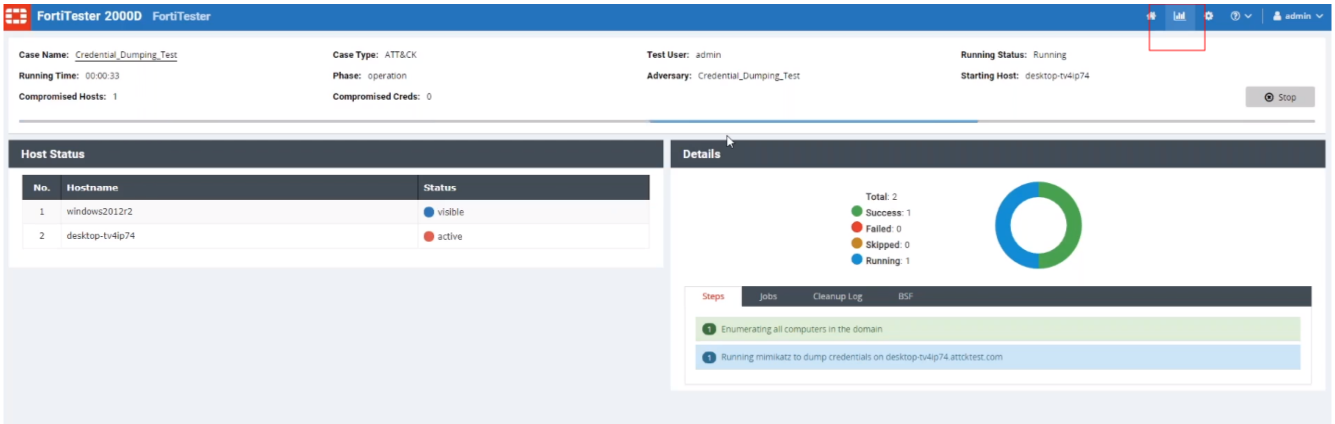
ATT&CK Cases

This test can perform automated adversarial assessments against Windows/Linux/Mac base on ATT&CK, requiring zero prior knowledge about the environment to run.

■	No.	Run Now	Name	Edit	Clone	Export	Result
□	1		Scheduled_Task_Test				6
□	2		Exfiltrate_File_Test				7
□	3		PowerShell_Test				3
□	4		Execution_Through_API_Test				1
□	5		Credential_Dumping_Test				46

Show rows: 10 ▾ 1 - 5 of 5

As FortiTester is running this test, click on the top right for the statistics metric.



Case Name: Credential_Dumping_Test
Case Type: ATT&CK
Test User: admin
Running Status: Running
Running Time: 00:00:33
Phase: operation
Adversary: Credential_Dumping_Test
Starting Host: desktop-tv4ip74
Compromised Hosts: 1
Compromised Creds: 0

Host Status

No.	Hostname	Status
1	windows2012r2	● visible
2	desktop-tv4ip74	● active

Details

Total: 2
Success: 1
Failed: 0
Skipped: 0
Running: 1

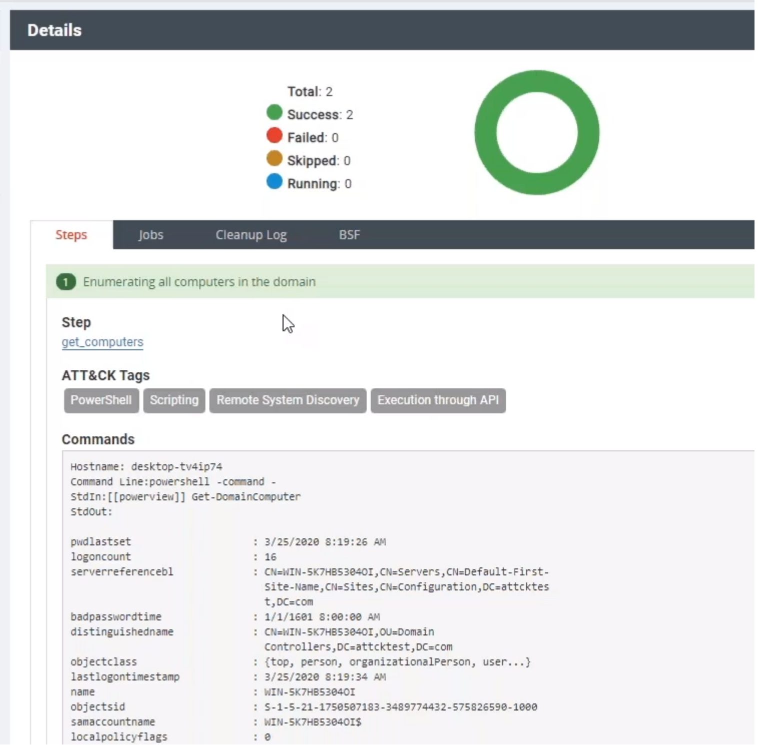
1 Enumerating all computers in the domain

1 Running mimikatz to dump credentials on desktop-tv4ip74.attcktest.com

Credential_Dumping_Test

Here we see two successful attempts on the DUT. The test uses Mimikatz that dumps passwords from memory.

FortiTester uses the `get_computer` function to extract all the hosts available in the domain, including both the desktop and the server, and sensitive information such as logon information, timing, etc.



1 Enumerating all computers in the domain

Step

get_computers

ATT&CK Tags

PowerShell | Scripting | Remote System Discovery | Execution through API

Commands

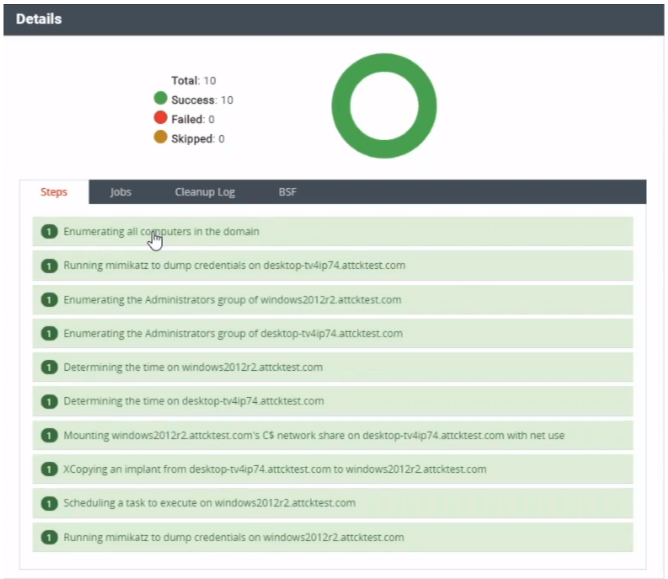
```
Hostname: desktop-tv4ip74
Command Line:powershell -command -
StdIn:[[powerview]] Get-DomainComputer
StdOut:

pwdlastset                   : 3/25/2020 8:19:26 AM
logoncount                   : 16
serverreferencebl            : CN=WIN-5K7HB5304OI,CN=Servers,CN=Default-First-
                               Site-Name,CN=Sites,CN=Configuration,DC=attcktes
                               t,DC=com
badpasswordtime              : 1/1/1601 8:00:00 AM
distinguishedname            : CN=WIN-5K7HB5304OI,OU=Domain
                               Controllers,DC=attcktest,DC=com
objectclass                  : {top, person, organizationalPerson, user...}
lastlogontimestamp           : 3/25/2020 8:19:34 AM
name                         : WIN-5K7HB5304OI
objectsid                    : S-1-5-21-1750507183-3489774432-575826590-1000
samaccountname               : WIN-5K7HB5304OI$
localpolicyflags             : 0
```

This `credential_dump` attack is across all machines in the domain.

Scheduled_Task_Test

The hacker has the ability to schedule an attack on the victim's computer to run. If you've already run the test before, FortiTester has the ability to save results. The results show, for example, if `get_computers` was successful.



1 Enumerating all computers in the domain

1 Running mimikatz to dump credentials on desktop-tv4ip74.attcktest.com

1 Enumerating the Administrators group of windows2012r2.attcktest.com

1 Enumerating the Administrators group of desktop-tv4ip74.attcktest.com

1 Determining the time on windows2012r2.attcktest.com

1 Determining the time on desktop-tv4ip74.attcktest.com

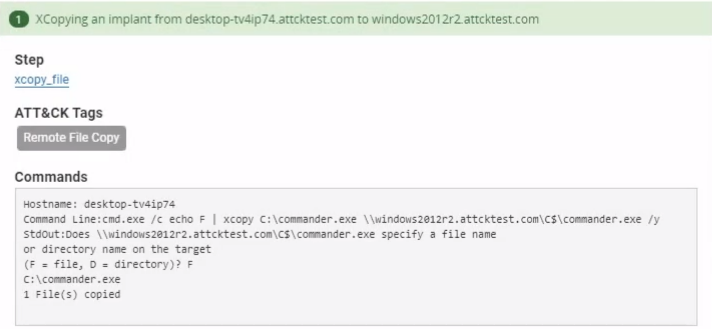
1 Mounting windows2012r2.attcktest.com's C$ network share on desktop-tv4ip74.attcktest.com with net use

1 XCopying an implant from desktop-tv4ip74.attcktest.com to windows2012r2.attcktest.com

1 Scheduling a task to execute on windows2012r2.attcktest.com

1 Running mimikatz to dump credentials on windows2012r2.attcktest.com

After `get_computers` and `get_credentials` are run, FortiTester can do an xcopy of a file from the desktop to the server, which is a higher value target. The following image shows that it has been successful in scheduling a task on the windows server.



1 XCopying an implant from desktop-tv4ip74.attcktest.com to windows2012r2.attcktest.com

Step

xcopy_file

ATT&CK Tags

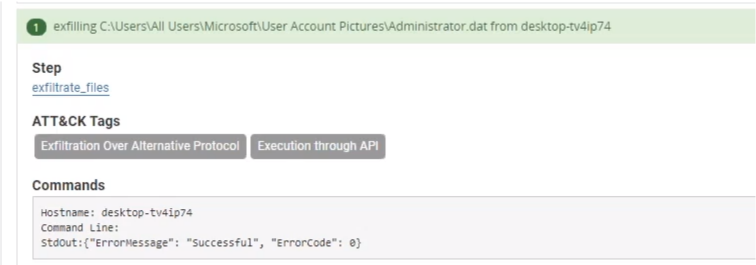
Commands

```
Hostname: desktop-tv4ip74
Command Line:cmd.exe /c echo F | xcopy C:\commander.exe \\windows2012r2.attcktest.com\C$\commander.exe /y
StdOut:Does \\windows2012r2.attcktest.com\C$\commander.exe specify a file name
or directory name on the target
(F = file, D = directory)? F
C:\commander.exe
1 File(s) copied
```

The user may look at the gray box to learn the techniques used.

Exfiltrate_File_Test

After the test is run successfully, FortiTester will retrieve various files from the user's PC.



1 exfilling C:\Users\All Users\Microsoft\User Account Pictures\Administrator.dat from desktop-tv4ip74

Step

exfiltrate_files

ATT&CK Tags

Commands

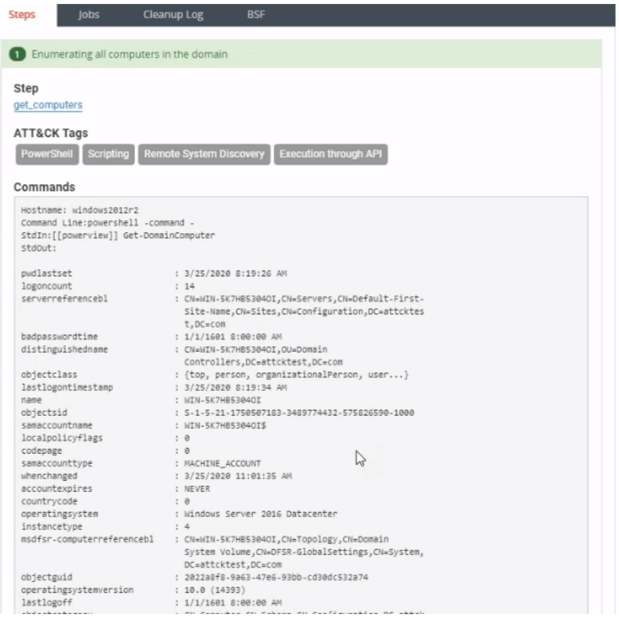
```
Hostname: desktop-tv4ip74
Command Line:
StdOut:{"ErrorMessage": "Successful", "ErrorCode": 0}
```

PowerShell_Test

Involves `get_admin`, which lists all the administrator accounts on the two hosts, including the domain and the local administrator on the victim's PC.

Execution_Through_API

This is similar to PowerShell_Test, where Windows API is used to extract information.



1 Enumerating all computers in the domain

Step
get_computers

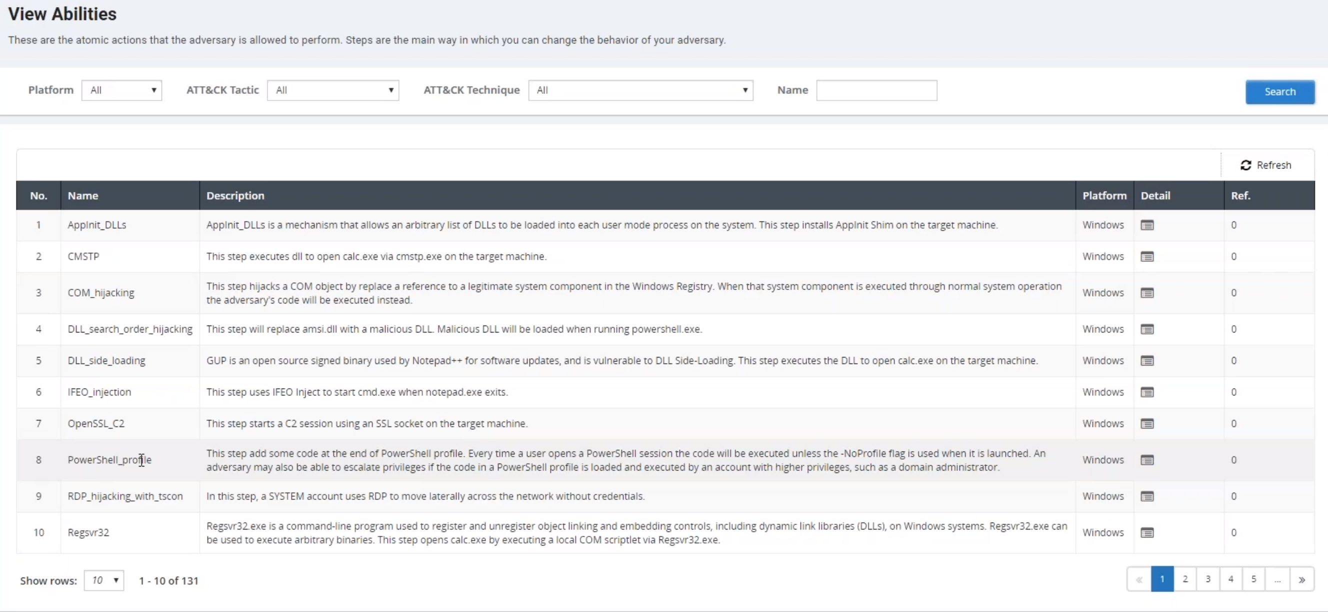
ATT&CK Tags
PowerShell | Scripting | Remote System Discovery | Execution through API

Commands

```
Hostname: windows2012r2
Command Line:powershell -command -
StdIn:[[powerview]] Get-DomainComputer
StdOut:

pwdlastset                  : 3/25/2020 8:19:26 AM
logoncount                  : 14
serverreferencebl           : CN=WIN-5K7HB53040I,CN=Servers,CN=Default-First-
                              Site-Name,CN=Sites,CN=Configuration,DC=attcktes
                              t,DC=com
badpasswordtime             : 1/1/1601 8:00:00 AM
distinguishedname           : CN=WIN-5K7HB53040I,OU=Domain
                              Controllers,DC=attcktest,DC=com
objectclass                 : {top, person, organizationalPerson, user...}
lastlogontimestamp          : 3/25/2020 8:19:34 AM
name                        : WIN-5K7HB53040I
objectsid                   : S-1-5-21-1750507183-3489774432-575826590-1000
samaccountname              : WIN-5K7HB53040I$
localpolicyflags            : 0
codepage                    : 0
samaccounttype              : MACHINE_ACCOUNT
whenchanged                 : 3/25/2020 11:01:35 AM
accountexpires              : NEVER
countrycode                 : 0
operatingsystem             : Windows Server 2016 Datacenter
instancetype                : 4
msdfsr-computerreferencebl  : CN=WIN-5K7HB53040I,CN=Topology,CN=Domain
                              System Volume,CN=DFSR-GlobalSettings,CN=System,
                              DC=attcktest,DC=com
objectguid                  : 2022a8f8-9a63-47e6-93bb-cd30dc532a74
operatingsystemversion      : 10.0 (14393)
lastlogoff                  : 1/1/1601 8:00:00 AM
```

Go to *Maintenance > View Abilities* to see the dependencies of each tactic and technique.



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:

No.	Name	Description	Platform	Detail	Ref.
1	AppInit_DLLs	AppInit_DLLs is a mechanism that allows an arbitrary list of DLLs to be loaded into each user mode process on the system. This step installs AppInit Shim on the target machine.	Windows	▤	0
2	CMSTP	This step executes dll to open calc.exe via cmstp.exe on the target machine.	Windows	▤	0
3	COM_hijacking	This step hijacks a COM object by replace a reference to a legitimate system component in the Windows Registry. When that system component is executed through normal system operation the adversary's code will be executed instead.	Windows	▤	0
4	DLL_search_order_hijacking	This step will replace amsi.dll with a malicious DLL. Malicious DLL will be loaded when running powershell.exe.	Windows	▤	0
5	DLL_side_loading	GUP is an open source signed binary used by Notepad++ for software updates, and is vulnerable to DLL Side-Loading. This step executes the DLL to open calc.exe on the target machine.	Windows	▤	0
6	IFEO_injection	This step uses IFEO Inject to start cmd.exe when notepad.exe exits.	Windows	▤	0
7	OpenSSL_C2	This step starts a C2 session using an SSL socket on the target machine.	Windows	▤	0
8	PowerShell_profile	This step add some code at the end of PowerShell profile. Every time a user opens a PowerShell session the code will be executed unless the -NoProfile flag is used when it is launched. An adversary may also be able to escalate privileges if the code in a PowerShell profile is loaded and executed by an account with higher privileges, such as a domain administrator.	Windows	▤	0
9	RDP_hijacking_with_tscon	In this step, a SYSTEM account uses RDP to move laterally across the network without credentials.	Windows	▤	0
10	Regsvr32	Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. Regsvr32.exe can be used to execute arbitrary binaries. This step opens calc.exe by executing a local COM scriptlet via Regsvr32.exe.	Windows	▤	0

Show rows: 10 1 - 10 of 131

Summary

Running the tests above shows the power of FortiTester MITRE ATT&CK abilties. You can also view other ATT&CK tactics under *Maintenance > View Abilities* as below, and see the dependencies of different attacks

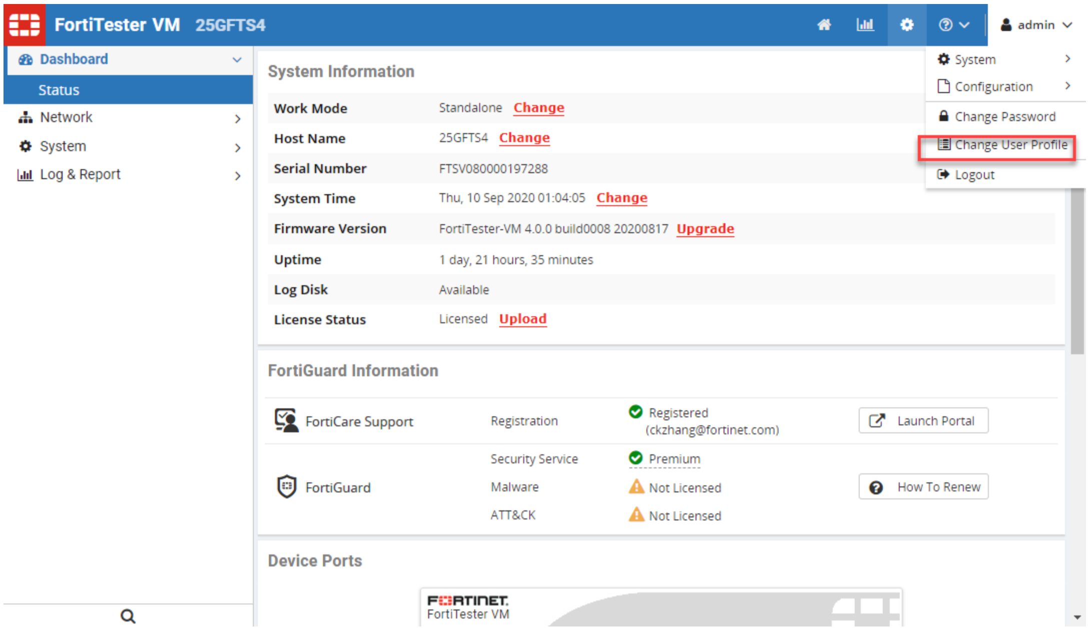
System administration

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, system resources, device ports, and alert message console.

System Information Overview



System Information

Work Mode	Standalone Change
Host Name	25GFTS4 Change
Serial Number	FTSV080000197288
System Time	Thu, 10 Sep 2020 01:04:05 Change
Firmware Version	FortiTester-VM 4.0.0 build0008 20200817 Upgrade
Uptime	1 day, 21 hours, 35 minutes
Log Disk	Available
License Status	Licensed Upload

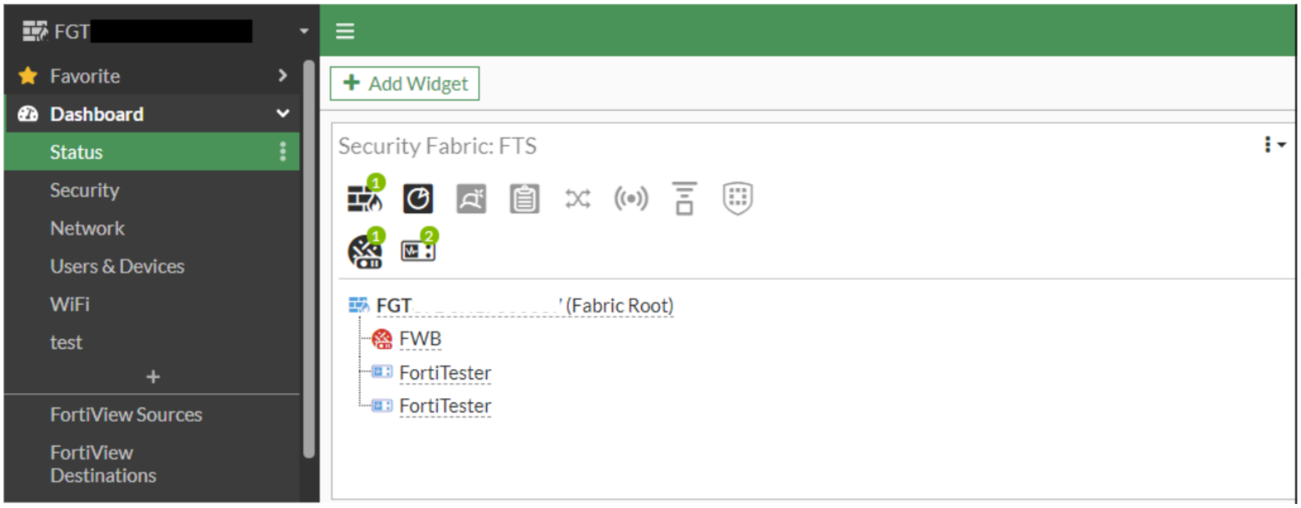
FortiGuard Information

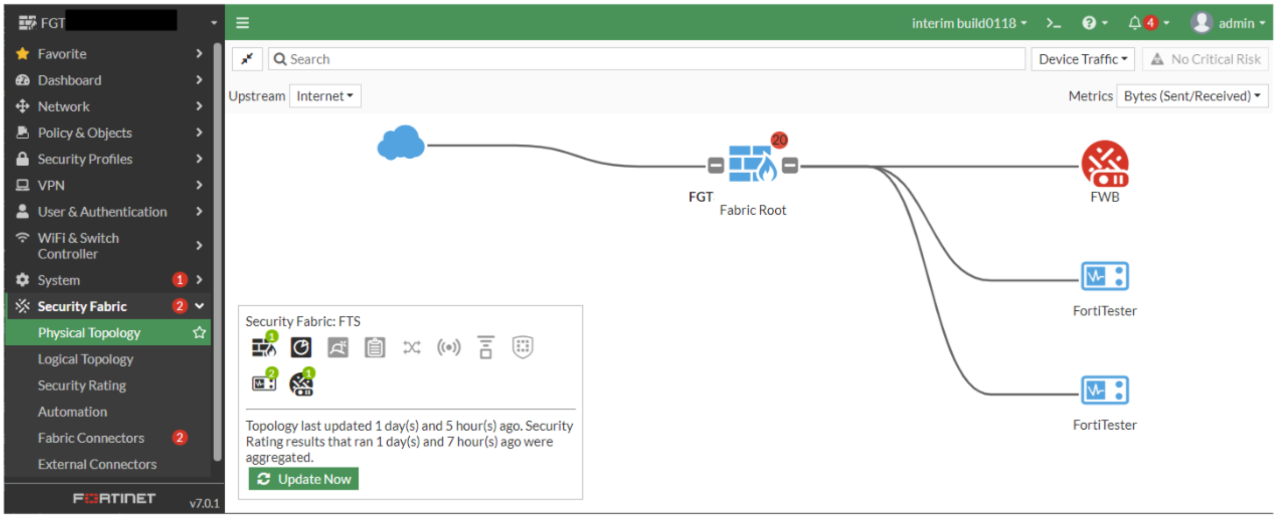
FortiCare Support	Registration	Registered (ckzhang@fortinet.com)	Launch Portal
FortiGuard	Security Service	Premium	How To Renew
	Malware	Not Licensed	
	ATT&CK	Not Licensed	

Security fabric

FortiTester v7.0.1+ allows users to join FortiTester to FortiOS Security Fabric via fabric protocol, thus allowing information exchange between FortiTester and FortiGates. Upon a successful connection, FortiOS will show FortiTester as an icon in physical and logical topology, as well as showing a widget in FortiOS dashboard with FortiTester system information.

FortiOS v7.0.1 showing FortiTester icon, as well as system information widget.

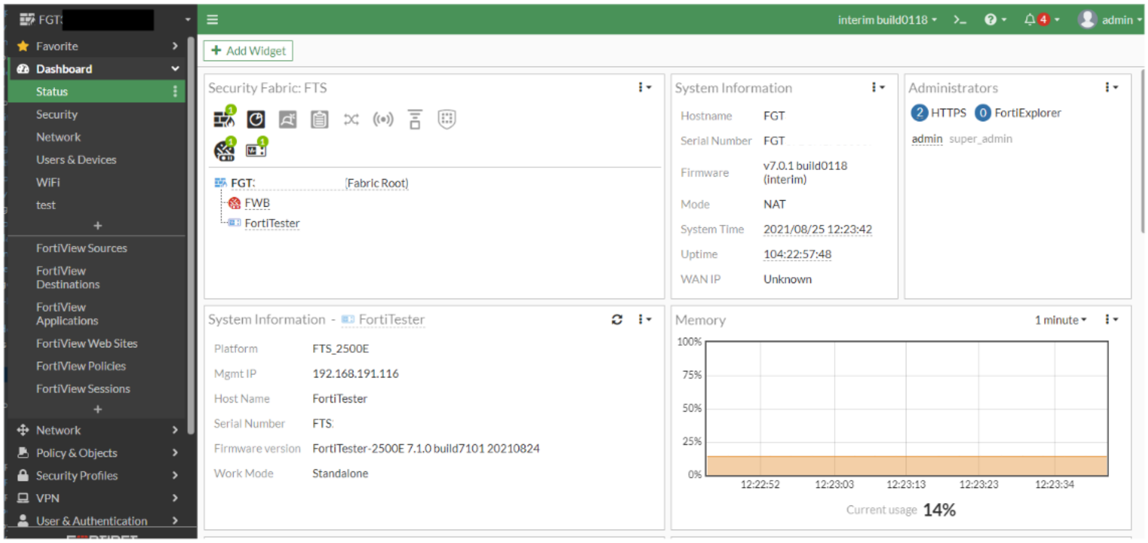




Topology last updated 1 day(s) and 5 hour(s) ago. Security Rating results that ran 1 day(s) and 7 hour(s) ago were aggregated.

For step by step configuration to connect FortiTester to FortiOS, please refer to FortiOS v7.0.0 documentation at: https://docs.fortinet.com/document/fortigate/7.0.0/new-features/943947/fortitester-as-a-security-fabric-device-7-0-1

After the connection is successful, you can optionally add a FortiTester system information widget on FortiOS dashboard, as follows:



Security Fabric: FTS

FGT: (Fabric Root)
FWB
FortiTester

System Information

Hostname FGT
Serial Number FGT
Firmware v7.0.1 build0118 (interim)
Mode NAT
System Time 2021/08/25 12:23:42
Uptime 104:22:57:48
WAN IP Unknown

Administrators

2 HTTPS 0 FortiExplorer
admin super_admin

System Information - FortiTester

Platform FTS_2500E
Mgmt IP 192.168.191.116
Host Name FortiTester
Serial Number FTS
Firmware version FortiTester-2500E 7.1.0 build7101 20210824
Work Mode Standalone

Memory

Current usage 14%

Tip 1: FortiTester needs to be fully licensed in order to authenticate successfully with Certificates.

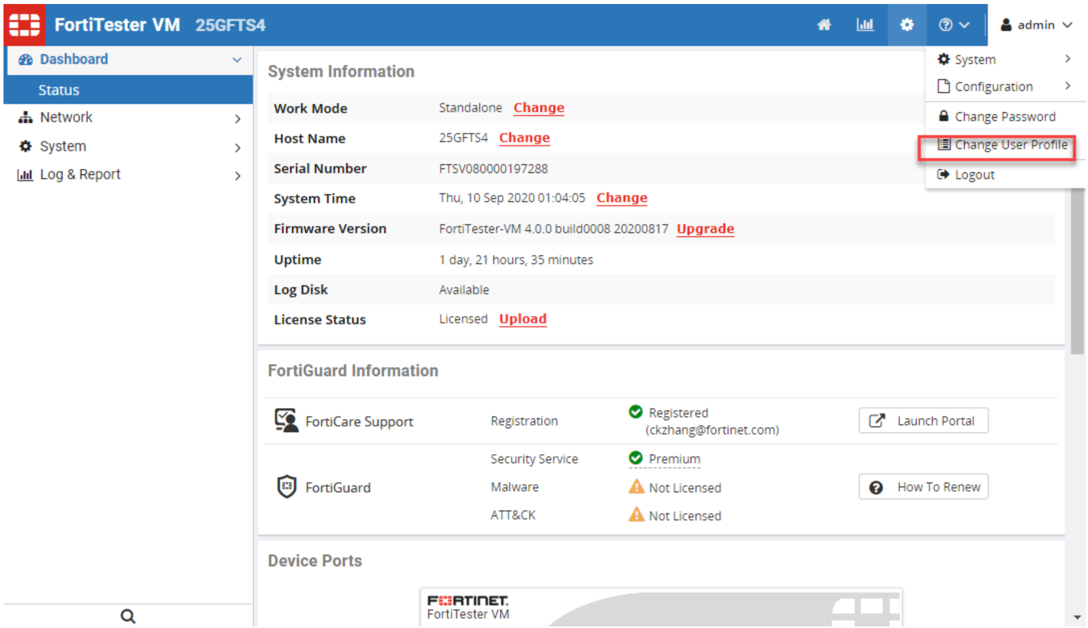
Tip 2: FortiOS will use TCP port 443 to communicate to FortiTester. FortiTester will use TCP port 8013 to connect to FortiOS.

Tip 3: If there are multiple FortiTester connected to same fabric, deauthenticating one will deauthenticate all FortiTesters in Security Fabric.

Setting password

To reset the password:

1. Go to *System Settings > Dashboard > Status.* Click on the top right, under admin, to change the user profile.



System Information

Work Mode	Standalone Change
Host Name	25GFTS4 Change
Serial Number	FTSV080000197288
System Time	Thu, 10 Sep 2020 01:04:05 Change
Firmware Version	FortiTester-VM 4.0.0 build0008 20200817 Upgrade
Uptime	1 day, 21 hours, 35 minutes
Log Disk	Available
License Status	Licensed Upload

FortiGuard Information

FortiCare Support	Registration	✓ Registered (ckzhang@fortinet.com)
FortiGuard	Security Service	✓ Premium
	Malware	⚠ Not Licensed
	ATT&CK	⚠ Not Licensed

Device Ports

2. You will be directed to the homepage of your choice after you login again.

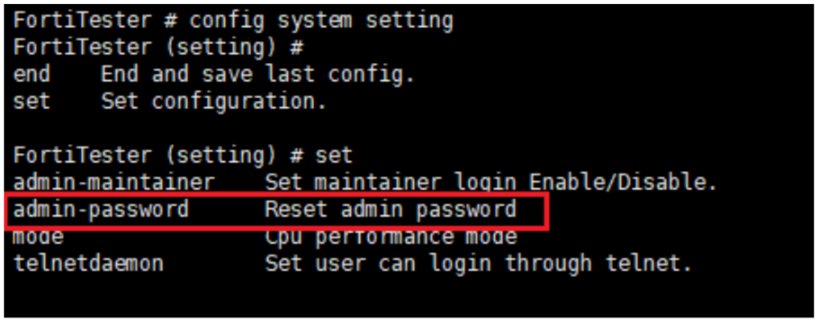
CLI command for maintainer account

Maintainer access is also supported on serial port terminals. You can login with ‘maintainer’ account shortly after FortiTester boots. The password would be bcpb plus the serial number of the FortiTester. Example: bcpbFTS4KET618000005. After a short period of time, you will no longer be able to login with maintainer account. You might want to reboot FortiTester to try again.

The Serial Number can be found at *Dashboard > Serial Number.*

You can reset the password of admin account with the maintainer's login with

```
config system setting
set admin-password <passwd>
end
```

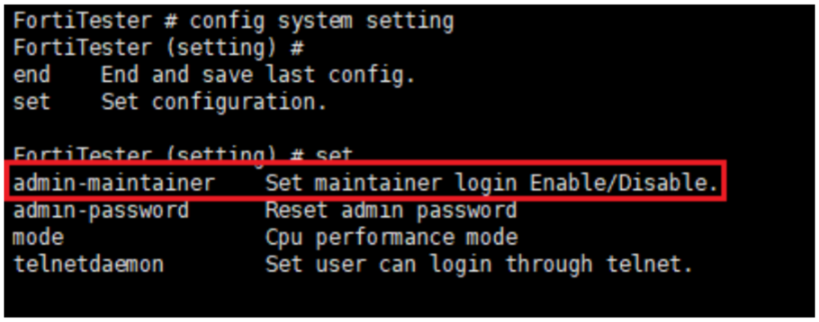


```
FortiTester # config system setting
FortiTester (setting) #
end     End and save last config.
set     Set configuration.

FortiTester (setting) # set
admin-maintainer     Set maintainer login Enable/Disable.
admin-password       Reset admin password
mode                 Cpu performance mode
telnetdaemon         Set user can login through telnet.
```

If the maintainer login is no longer needed, you are free to disable it by login ssh/telnet terminal with any administration account, by using the following command:

```
config system setting
set admin-maintainer disable
end
```



```
FortiTester # config system setting
FortiTester (setting) #
end     End and save last config.
set     Set configuration.

FortiTester (setting) # set
admin-maintainer     Set maintainer login Enable/Disable.
admin-password       Reset admin password
mode                 Cpu performance mode
telnetdaemon         Set user can login through telnet.
```

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

FortiTester does not support downgrading to previous firmware versions. Users have the option to backup configuration and test cases before upgrade, or restoring older firmware and configurations.

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.

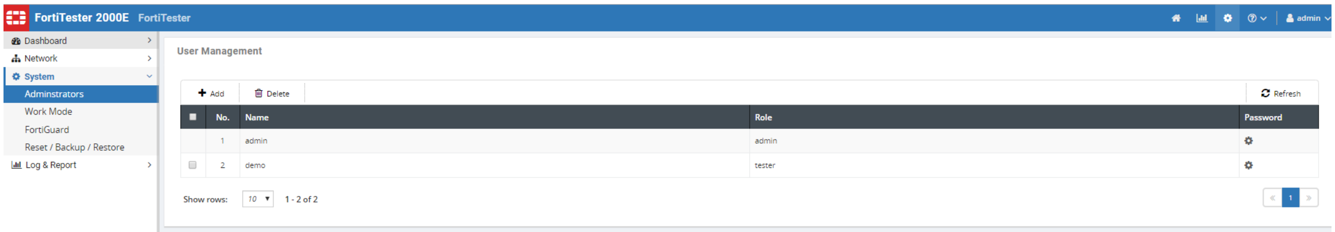
Configuring specific settings

In this section, you can configure the following:

Administration settings	
HTTPS Server Certificate	Select the TLS certificates uploaded in *System* > *Certificates*.
Idle Timeout	Define the idle timeout period to expire a FortiTester GUI session.
View settings	
Theme	Configure the theme for the system. This applies to the entire system, not just the user account.
Hardware settings	
Enable SSL Accelerator	Enable or disable the SSL Accelerator card.
Enable VLAN Offload	Enable to strip the double-tagged VLAN packet's S-Tag at the receiver end.
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	40G interface can fan out into 4x10G ports. • Only supported by the FortiTester 3000E model

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.



User Management

■	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

FortiTester can receive updates from either FortiGuard Networks (if FortiTester has connectivity to Internet directly or via proxy), manual updates from support website (https://support.fortinet.com). Updates are important for security services tests making sure FortiTester has the latest intrusion, web protection signatures, malware strike pack and MITRE ATT&CK signatures Updates.

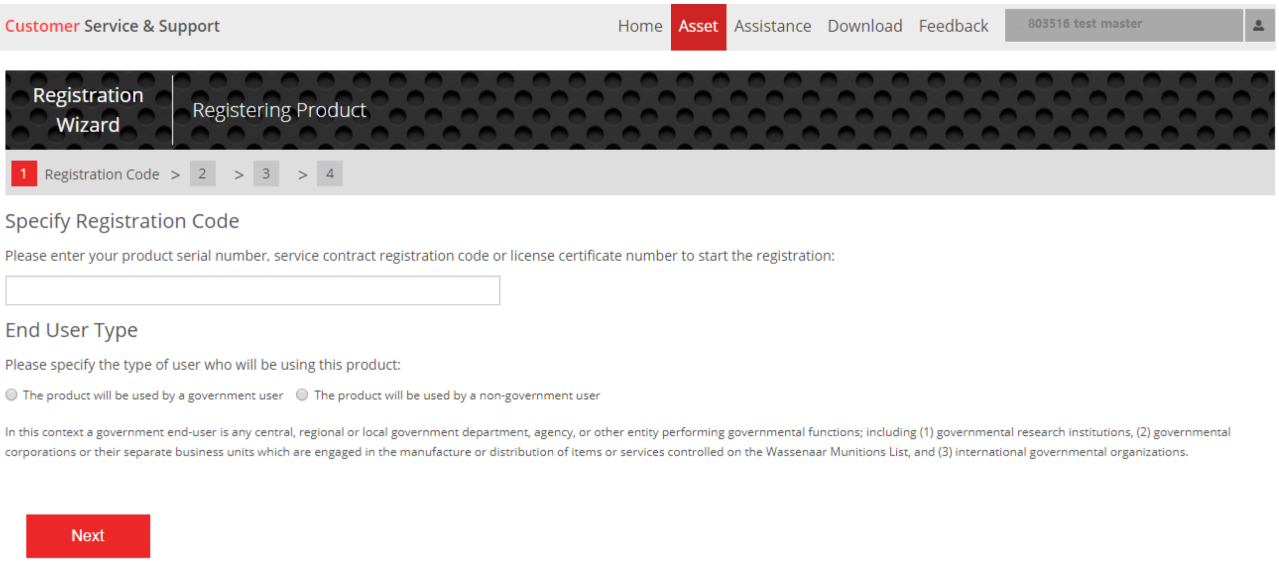
With older FortiTester versions v3.x and 4.x, users can see there is a standard vs premium package where basic package provides monthly updates, and premium contains bi-monthly updates.

Services could be renewed via Fortinet authorised partners and distributors.

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:

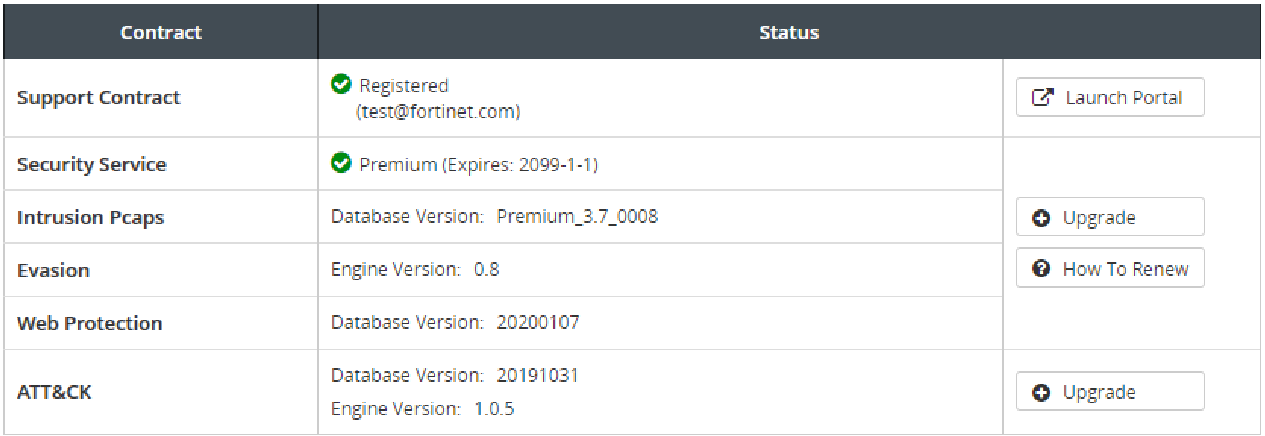
End User Type

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

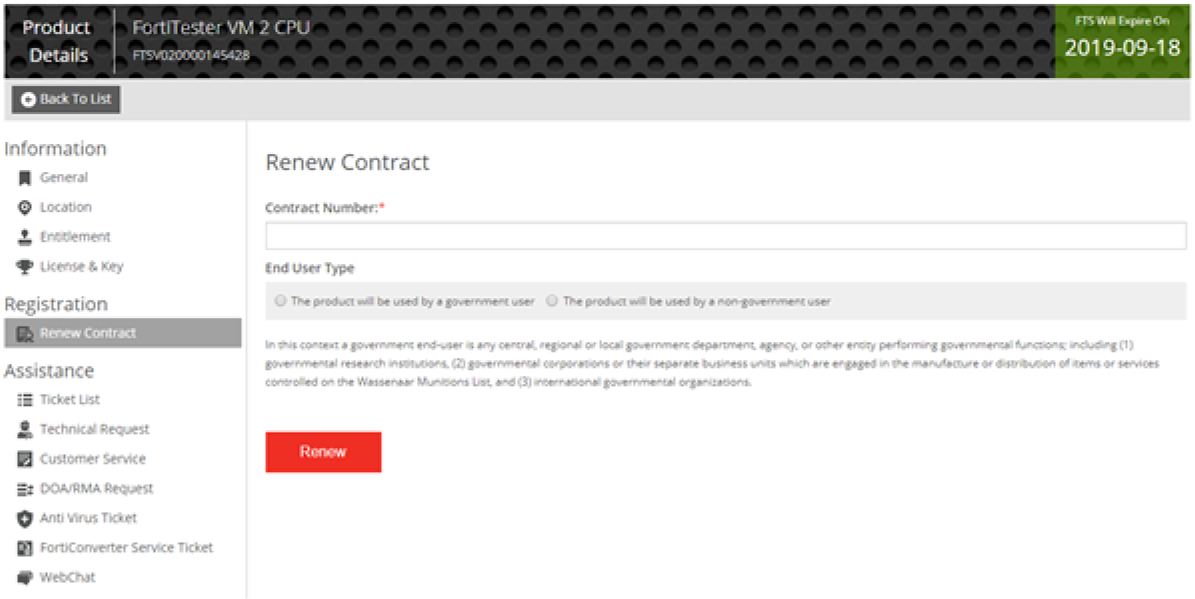
In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions; including (1) governmental research institutions, (2) governmental corporations or their separate business units which are engaged in the manufacture 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:
    - *Cases > Security Testing > Maintenance > FGD Intrusion Service.*
    - *Cases > Security Testing > Maintenance > Web Protection Service.*
    - *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.

Scheduled updates for FortiGuard

Go to *System > Fortiguard > Malware & IPS & ATT&CK Updates*. If you enable *Scheduled Updates*, you can click *Upgrade Malware & IPS & ATT&CK Definitions* to update instantly.

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.
4.

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.

5. Click *Apply*.

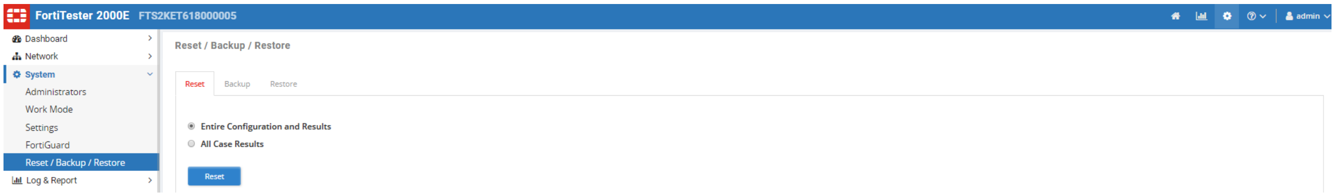
Malware & IPS & ATT&CK Updates

Enable *Scheduled Updates* and set the frequency of the update, or manually update it.

Reset, back up, restore, or downgrade 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.

Backup CLI

FortiTester # execute backup

```
all Backup all config to tftp server.
case Backup case config to tftp server.
history Backup history config to tftp server.
system Backup system config to tftp server.
```

Example

```
Backup case configuration
execute backup case tftp Case Configuration 10.121.1.206
```

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.

Downgrade

Downgrade steps

Generally, downgrade is NOT supported with FortiTester. Please do not hesitate to contact us should you have any problems with using FortiTester.

If you must downgrade you must perform the following checks and operations.

1. Check the console port connectivity. You must be able to configure the FortiTester on console port.
2. Backup the files you want to back up.
3. Execute command "execute reboot" then enter "y".
4. After showing "Press any key to display configuration menu", press <Enter> to display the configuration menu.

Example

```
Press any key to display configuration menu...
...
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[B]: Boot with backup firmware and set as default.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
Enter Selection [G]:
Enter G,F,B,Q,or H:
```

5. Enter G, TFTP server address, local address (FortiTester mgmt port addresss) and image name(downgrade version example 100F.out).

   Example

   ```
   Please connect TFTP server to Ethernet port "MGMT".
   Enter TFTP server address [192.168.1.168]: 10.121.1.206
   Enter local address [192.168.1.188]: 10.121.2.25
   Enter firmware image file name [image.out]: 100F.out
   MAC:000D484B2571
   #################################################################
   ```

   Note: If you enter the wrong address or image name you can use Ctrl+Backspace to delete before typing <Enter>.

   If you see #######, FortiTester is downloading image.
6. After showing "Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?" enter "D".
7. After rebooting, log onto the FortiTester CLI.
8. Execute command "execute factoryreset" then enter "y:.
9. After rebooting, configure the mgmt port address and gateway. **Note**: the password is empty.

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.
Subnet statistics	If enabled, reports calculate and display statistics based on subnets.

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

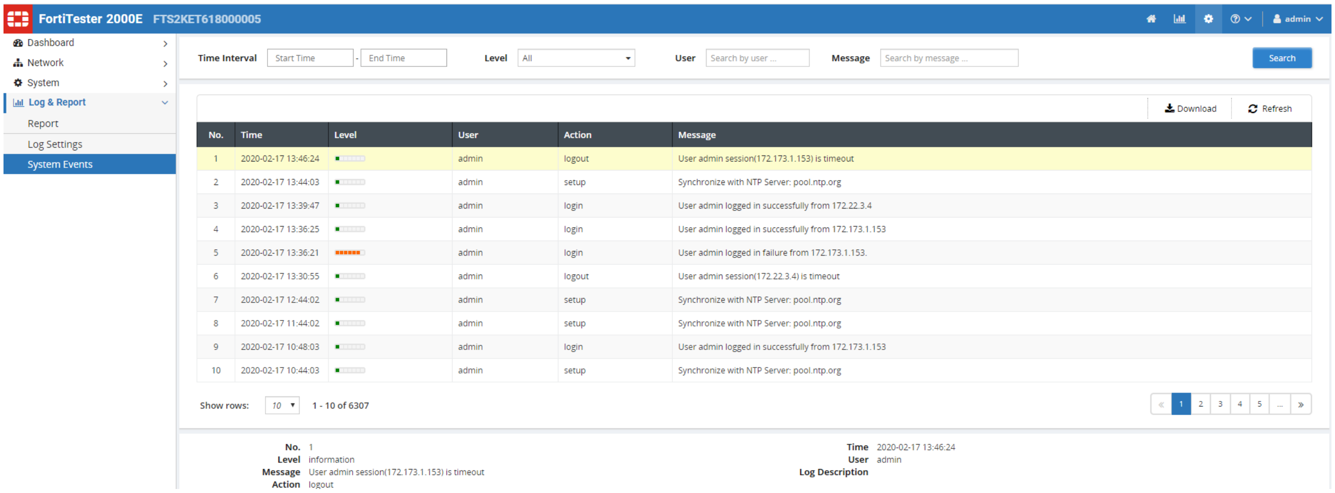
Select the events that will be reported in **System Events**.

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. **Note**: FortiSiem v5.3+ is supported.

Send logs to syslog	Enable to send the log to the syslog server when saving logs.
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 ...

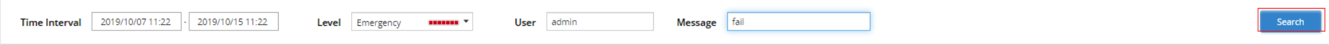
No.	Time	Level	User	Action	Message
1	2020-02-17 13:46:24	■	admin	logout	User admin session(172.173.1.153) is timeout
2	2020-02-17 13:44:03	■	admin	setup	Synchronize with NTP Server: pool.ntp.org
3	2020-02-17 13:39:47	■	admin	login	User admin logged in successfully from 172.22.3.4
4	2020-02-17 13:36:25	■	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 8 appliances or VMs:

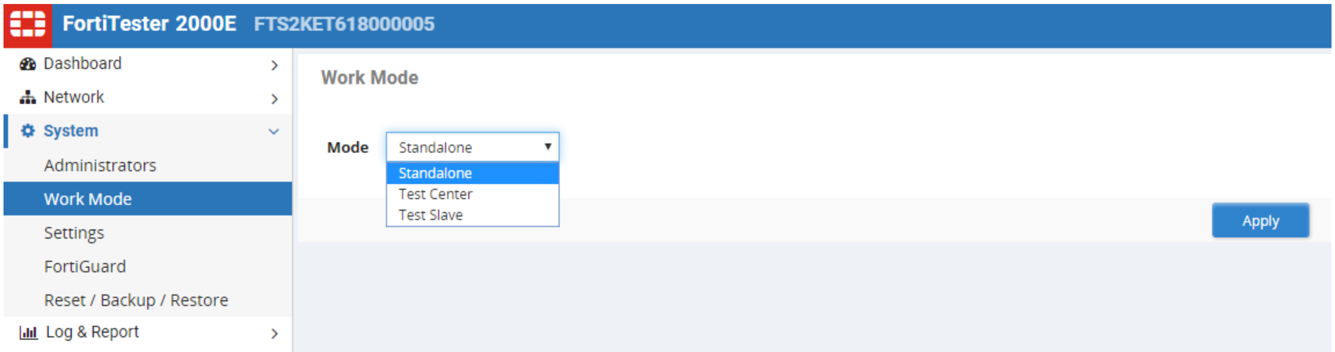
- In NAT or TP mode, you can configure at most 4 servers and 4 clients.
- In Application mode, you can configure at most 8 clients.

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/Client must have the same vCPU number, VM type, port number.
- Software - Center/Client 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/Client must have the same fanout mode (e.g. 3000E can break out 2 x 40G into 8 x 10G)
- Center/Client must be in the same group i.e.:
  - "2K": ["FTS_2000D", "FTS_2000E", "FTS_2500E", FTS_2000F],
  - "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"],
  - "IBM_BYOL": ["FTS_VM_IBM_BYOL"]

Configuring work mode settings

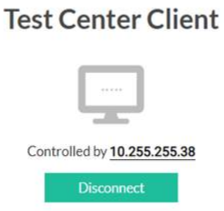
The work mode settings determine whether the FortiTester operates as a standalone appliance or is joined with other FortiTester appliances to form a Test Center.



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 server appliance; the others are Test Center clients. You manage test cases from the Test Center appliance management interface; the web UI is not available for an appliance in Test Client work mode. When you enter the web UI address for the Test Client appliance, it displays the following page instead.

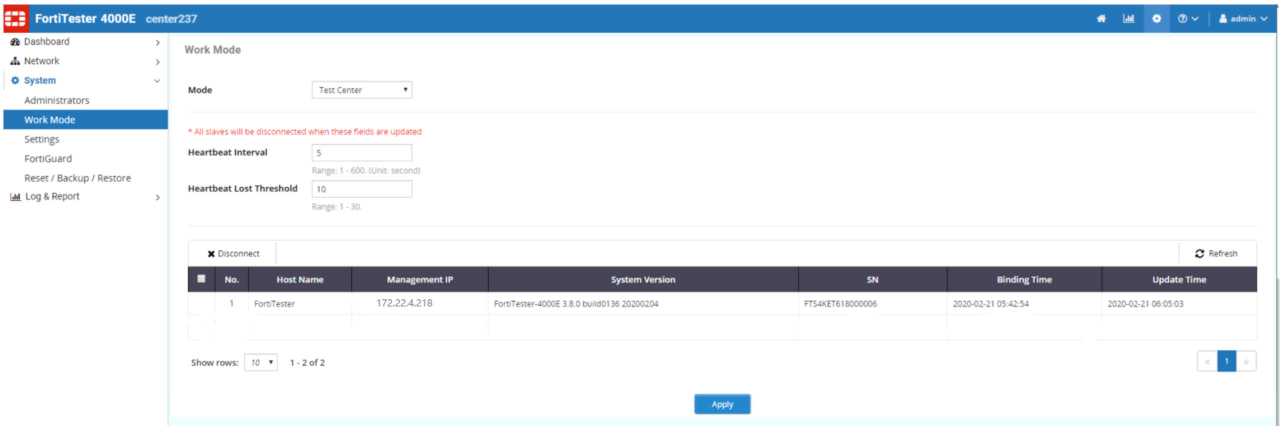
Test Client Mode



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 server. 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 Client*.
8. Enter the IP address of the Test Center server and click *Connect*.
9. Return to the *Work Mode* page on the server 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 client Web GUI to return to Standalone mode.

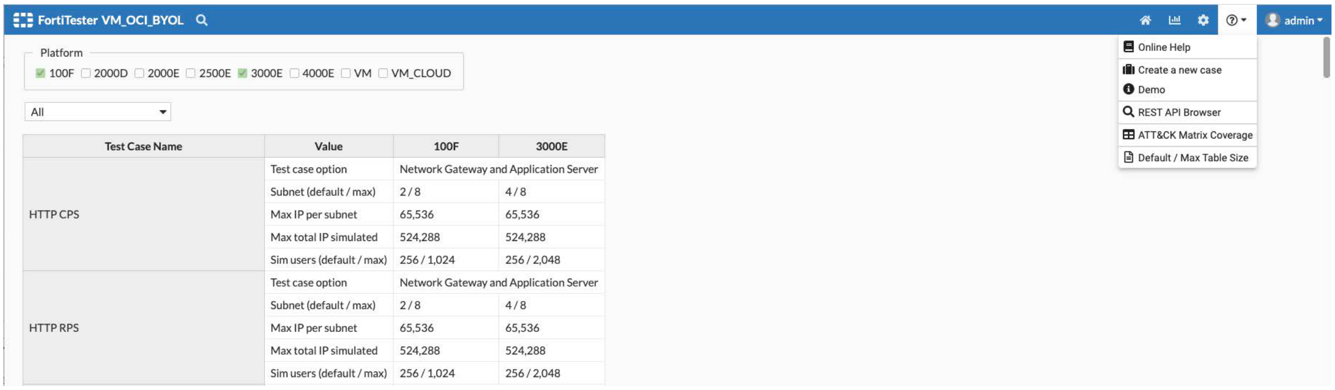
When the appliances have been added to the Test Center, you can select one or more FortiTester appliances to work as clients and others to work as servers when you create test cases. In this example, 172.22.4.217 has the client ports; 172.22.4.218 has the server ports. You can add up to four pairs of appliances to a Test Center.

10. Configure *Heartbeat Interval* and *Heartbeat Lost Threshold* to manage the heartbeat traffic between center and clients in Test Center mode.

> FortiTester uses HTTPS 443, tcp 2002 and tcp 2003 for heartbeat. FTS heartbeat is lost if the center does not receive the heartbeat packet from the client in the appropriate Heartbeat Interval; this interval is set in *Heartbeat Lost Threshold*.

Default and maximum values

Often when users are selecting FortiTester models to test, the user needs to know the max simusers, subnets configured (up to 8 on higher end models to generate more IPs). FortiTester shows a table of the default and maximum values for each test case that users can configure. This table can be shown by clicking on the top right of FortiTester GUI. Users can select the models and view the default and maximum configurable options.



Platform

☑ 100F □ 2000D □ 2000E □ 2500E ☑ 3000E □ 4000E □ VM □ VM_CLOUD

All

Test Case Name	Value	100F	3000E
HTTP CPS	Test case option	Network Gateway and Application Server	
	Subnet (default / max)	2 / 8	4 / 8
	Max IP per subnet	65,536	65,536
	Max total IP simulated	524,288	524,288
	Sim users (default / max)	256 / 1,024	256 / 2,048
HTTP RPS	Test case option	Network Gateway and Application Server	
	Subnet (default / max)	2 / 8	4 / 8
	Max IP per subnet	65,536	65,536
	Max total IP simulated	524,288	524,288
	Sim users (default / max)	256 / 1,024	256 / 2,048

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
- ALI BYOL

For more details about FortiTester-VM deployment, see the FortiTester Private Cloud Deployment Guides and the FortiTester Public Cloud Deployment Guides.

Deployment

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 Example
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 dropdown 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 example. 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 "Chapter 1 - Getting Started" on page 1 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*.

Glossary

A

AAA
Authentication, Authorization, and Accounting

AD
Active Directory

ADOM
Administrative Domain

AES
Advanced Encryption Standard

AMI
Amazon Machine Image

AP
Access Point

API
Application Programming Interface

APN
Access Point Name

APT
Advanced Persistent Threat

ATP
Advanced Threat Protection

AV
Antivirus

AVP
Attribute Value Pairs

AWS
Amazon Web Service

B

BGP
Border Gateway Protocol

C

C&C
Command and Control

CA
Certificate Authority

CASI
Cloud Access Security Inspection

CBC
Cipher Block Chaining

CHAP
Challenge-Handshake Authentication Protocol

CIDR
Classless Inter-Domain Routing

CLI
Command Line Interface

CN
Common Name

CoA
Change of Authorization

CPU
Central Processing Unit

CRL
Certificate Revocation List

CSR
Certificate Signing Request

CSV
Comma Separated Value

CVE
Common Vulnerabilities and Exposures

D

DC
Domain Controller, Direct Current

DES
Data Encryption Standard

DH
Diffie-Hellman

DHCP
Dynamic Host Configuration Protocol

DLL
Dynamic-Link Library

DLP
Data Loss Prevention

DN
Distinguished Name

DNAT
Destination Network Address Translation

DNS
Domain Name System

DSCP
Differentiated Services Code Point

DSRI
Disable Server Response Inspection

DTLS
Datagram Transport Layer Security

E

EA
E-mail Address

EAPOL
Extensible Authentication Protocol over LAN (Local Area Network)

EC
Endpoint Control

EC2
Elastic Compute Cloud

EGP
Exterior Gateway Protocol

EMS
Enterprise Management Server

ESD
Electrostatic Discharge

ESP
Encapsulated Security Payload

F

FAZ
FortiAnalyzer

FCT
FortiClient

FDN
FortiGuard Distribution Network

FDS
FortiGuard Distribution Servers

FG
FortiGate

FGFM
FortiGate-FortiManager

FMG
FortiManager

FQDN
Fully Qualified Domain Name

FSA
FortiSandbox

FSSO
Fortinet Single Sign-On

FTP
File Transfer Protocol

G

GCF
Gatekeeper Confirm

GPRS
General Packet Radio Service

GRE
Generic Routing Encapsulation

GTP
GPRS Tunneling Protocol

GUI
Graphical User Interface

GUID
Globally Unique Identifier

H

HA
High Availability

hcache
Hard Cache

HDD
Hard Disk Drive

HTML
HyperText Markup Language

HTTP
HyperText Transfer Protocol

I

I/O
Input / Output

IBP
Identity-based Policy

ICAP
Internet Content Adaptation Protocol

ICMP
Internet Control Message Protocol

IGP
Interior Gateway Protocol

IKE
Internet Key Exchange

IMAP
Internet Message Access Protocol

IOC
Indicators of Compromise

IP
Internet Protocol

IPS
Intrusion Prevention System

IPsec
Internet Protocol Security

ISDB
Internet Service Database

ISP
Internet Service Provider

IV
Initialization Vector

J

JSON
JavaScript Object Notation

L

L2TP
Layer 2 Tunneling Protocol

LACP
Link Aggregation Control Protocol

LAN
Local Area Network

LDAP
Lightweight Directory Access Protocol

M

MAC
Media Access Control

MD5
Message Digest 5

MGCP
Media Gateway Controller Protocol

MIB
Management Information Base

MMC
Microsoft Management Console

MSCHAP
Microsoft Challenge-Handshake Authentication Protocol

MSS
Maximum Segment Size

N

NAC
Network Access Control or Compliance

NAS
Network Access Server

NAT
Network Address Translation

NAT-PT
Network Address Translation (NAT) Port Translation

NDcPP
Network Device Collaborative Protection Profile

NGFW
Next-Generation Firewall

NNTP
Network News Transfer Protocol

NOC
Network Operations Center

NPU
Network Processing Unit

NTLM
NT LAN Manager

NTP
Network Time Protocol

O

OCSP
Online Certificate Status Protocol

OFTP
Odette File Transfer Protocol

ONC-RPC
Open Network Computing Remote Procedure Call

OSPF
Open Shortest Path First

OTP
One-time Password

OU
Organization Unit

OUI
Organizationally Unique Identifier

OVF
Open Virtualization Format

P

PAP
Password Authentication Protocol

PAT
Port Address Translation

PEM
Power Entry Module

PFS
Perfect Forward Secrecy

PKCS
Public Key Cryptography Standards

PKI
Public Key Infrastructure

PoE
Power over Ethernet

POP3
Post Office Protocol 3

PPP
Point-to-Point Protocol

PPPoE
Point-to-Point Protocol over Ethernet

PPTP
Point-to-Point Tunneling Protocol

PSK
Pre-Shared Key

R

RADIUS
Remote Authentication Dial-In User

RAID
Redundant Array of Independent Disks

RAM
Random Access Memory

RAS
Registration, Admission, and Status

RBAC
Role Based Access Control

RCF
Registration Confirm

RDP
Remote Desktop Protocol

REST
Representational State Transfer

RFC
Remote Function Call

RSH
Remote Shell

RSSO
RADIUS Single Sign-On

RTM
Real-Time Monitor

RTP
Real-Time Protection

RTSP
Real-Time Streaming Protocol

S

SAN
Storage Area Network

SAP
Shelf Alarm Panel

SCEP
Simple Certificate Enrollment Protocol

SCP
Secure Copy

SCVP
Server-based Certificate Validation Protocol

SDK
Software Development Kit

SDN
Software-Defined Networking

SFTP
Secure (or SSH) File Transfer Protocol

SHA1
Secure Hash Algorithm 1

SIP
Session Initiation Protocol

SMTP
Simple Mail Transfer Protocol

SNAT
Secure Network Address Translation

SNI
Server Name Indication

SNMP
Simple Network Management Protocol

SOC
Security Operations Center

SQL
Structured Query Language

SSH
Secure Shell

SSID
Service Set Identifier

SSL
Secure Sockets Layer

SSO
Single Sign-On

T

TACACS+
Terminal Access Controller Access-Control System

Tcl
Tool Command Language

TCP
Transmission Control Protocol

TFTP
Trivial File Transfer Protocol

TLS
Transport Layer Security

TNS
Transparent Network Substrate

TTL
Time-to-live

U

UDP
User Datagram Protocol

UID
Unique Identifier

URI
Uniform Resource Identifier

URL
Uniform Resource Locator

UTM
Unified Threat Management

UUID
Universally Unique Identifier

V

VDOM
Virtual Domain

VHD
Virtual Hard Disk

VIP
Virtual Internet Protocol

VLAN
Virtual Local Area Network

VM
Virtual Machine

VMDK
Virtual Machine Disk

VoIP
Voice over Internet Protocol

VPC
Virtual Private Cloud

VPN
Virtual Private Network

VSA
Vendor Specific Attribute

W

WAF
Web Application Firewall

WAN
Wide Area Network

WCCP
Web Cache Communication Protocol

WIDS
Wireless Intrusion Detection System

WPA
Wi-Fi Protected Access

WPA2
Wi-Fi Protected Access II

WSDL
Web Services Description Language

WTP
Wireless Transaction Protocol

X

XAuth
Extended Authentication

XML
eXtensible Markup Language

XSS
Cross-site Scripting

XVA
XenServer Virtual Appliance

FAQ

Table of contents

1. Does FortiTester VM supports SR-IOV?
2. How do I replay large PCAPs in FortiTester?
3. Can FortiTester run more than one case at a time?
4. Does FortiTester support API?
5. What are the supported hardware & port density?
6. What are the limitations on CPU, RAM and Storage for different VM licenses?
7. Where can I download the attack package?
8. What are Test Centre model running conditions? Can they be different models?
9. How can we reset FortiTester admin password? Is there a maintainer account like FortiGate?
10. How do you calculate max bandwidth in TestCenter mode?
11. SSL CPS VPN test - is there a way NOT to send the ping to FortiTester server side when starting the case?
12. Why is the Trunk status of the device that connected to FortiTester down?
13. How many MAX end points / unique IP's can FortiTester generate?
14. How does FortiTester run offline?
15. What is the difference between Connections per Second and Simulated Users?
16. How to redirect GUI access to HTTPS from HTTP? on page 285

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.

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 42.

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.

What are the supported hardware & port density?

- FortiTester 100F-3x GE RJ45, 2x 1GE SFP, 2x 10 GE SFP+, 1 TB HDD storage
- FortiTester 2000D - 1x GE RJ45, 4x 10 GE SFP+, 120GB 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 2000F - 1x GE RJ45, 4x 10 GE SFP+, 2TB HDD Storage

- FortiTester 3000E - 1x GE RJ45, 2x 40 GE QSFP, 2TB HDD storage
- FortiTester 4000E - 1x GE RJ45, 1x 100 GE QSFP28, 2TB 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 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/Client must have the same vCPU number, VM type, port number.
- Software - Center/Client 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/Client must have the same fanout mode (e.g. 3000E can break out 2 x 40G into 8 x 10G)
- Center/Client must be in the same group i.e.:
  - "2K": ["FTS_2000D", "FTS_2000E", "FTS_2500E", FTS_2000F],
  - "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"]
  - "IBM_BYOL": ["FTS_VM_IBM_BYOL"]

How can we reset FortiTester admin password? Is there a maintainer account like FortiGate?

FortiTester does have a maintainer account, can be used to change password, but you must connect FortiTester console port.

Please refer to the following steps

1. **Connect** FortiTester console port.
2. **Reboot** FortiTester then get the SN.

   FortiBootLoader

   - FortiTester-4000E (23:46-06.26.2017)
   - Ver:00010001

   FortiTester-4000E (17:33-08.28.2017)

   Ver:00010002

   Serial number:FTS4KET618000005

   Total RAM: 131072MB

   Boot up, boot device capacity: 1960MB.

   Press any key to display configuration menu...

Login with maintainer user.

3. After the FortiTester boots, a timpe period of only 300 seconds will be permitted to type in the username and password.

   The password is bcpb plus the serial number of the FortiTester. Example bcpbFTS4KET618000005.

   center237 login: maintainer

   Password:

   Welcome !

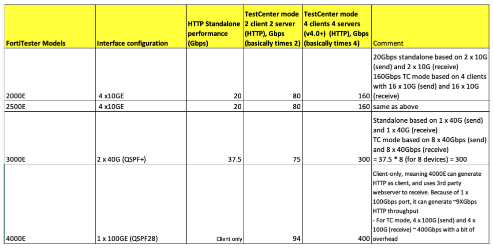
   For interactive help, Please type "?".
4. Change admin user password.

```
center237 # config system setting
center237 (setting) #
center237 (setting) # set admin-
      password fts@ftnt
Reset password success
center237 (setting) # end
center237 #
```

See Setting Password for more information.

How do you calculate max bandwidth in TestCenter mode?

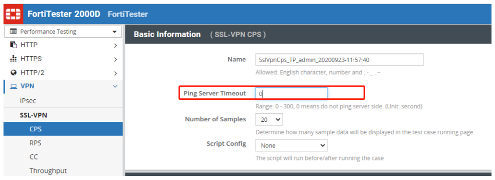
This is dependent on interfaces on FTS e.g. 10/40/100G and how much traffic it can generate. The example below is based on HTTP throughput.



FortiTester Models	Interface configuration	HTTP Standalone performance (Gbps)	TestCenter mode 2 client 2 server (HTTP), Gbps (basically times 2)	TestCenter mode 4 clients 4 servers (v4.0+) (HTTP), Gbps (basically times 4)	Comment
2000E	4 x10GE	20	80	160	20Gbps standalone based on 2 x 10G (send) and 2 x 10G (receive) 160Gbps TC mode based on 4 clients with 16 x 10G (send) and 16 x 10G (receive)
2500E	4 x10GE	20	80	160	same as above
3000E	2 x 40G (QSPF+)	37.5	75	300	Standalone based on 1 x 40G (send) and 1 x 40G (receive) TC mode based on 8 x 40Gbps (send) and 8 x 40Gbps (receive) = 37.5 * 8 (for 8 devices) = 300
4000E	1 x 100GE (QSPF28)	Client only	94	400	Client-only, meaning 4000E can generate HTTP as client, and uses 3rd party webserver to receive. Because of 1 x 100Gbps port, it can generate ~9XGbps HTTP throughput - For TC mode, 4 x 100G (send) and 4 x 100G (receive) ~ 400Gbps with a bit of overhead

SSL CPS VPN test - is there a way NOT to send the ping to FortiTester server side when starting the case? (if PING is not successful through the FG [requires another policy] SSLVPN case would not run.

Yes it's possible not to send the ping, by setting ping timeout to 0, as below:



Basic Information (SSL-VPN CPS)

Name: SslVpnCps_TP_admin_20200923-11:57:40

Allowed: English character, number and : - _ . ~

Ping Server Timeout: 0

Range: 0 - 300, 0 means do not ping server side. (Unit: second)

Number of Samples: 20

Determine how many sample data will be displayed in the test case running page

Script Config: None

The script will run before/after running the case

Why is the Trunk status of the device that connected to FortiTester down?

The test configuration on FortiTester is only a test template without activating the configuration. The admin can pre-stage multiple test cases with different network configuration for individual port-based or bond-based testing.

Only when the tester runs a bond-based test will FortiTester activate the bond, then the status of the connected trunk or aggregate interface on FortiSwitch or FortiGate will also change to "up."

How many MAX end points / unique IP's can FortiTester generate?

Each Test case limitation is different. Take HTTP CPS for example:

There are a few concepts which are important to understand.

Subnet settings

These control how many subnets FortiTester will create with a virtual router. In an HTTP CPS case you can create up to 16 subnets, each with 4096 IPs each. For example, 16 subnets x 65,536 IPs = 1,048,576 unique IPs

However, in the testing selection, you can either choose **SimUsers (max 1024)** OR **Connection per sec (max 9,999,999)**. The simple analogy is:

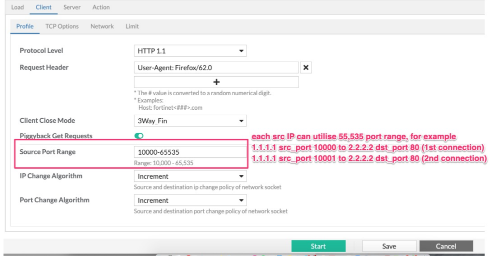
Sim users - FortiTester will send X number of runners from starting line to finish (to fetch something from finish line), the runners comes back with the objects, and start the run again (until test time finishes).

DUT (e.g. FG) might hold up the users (runner).

Connections per second - FortiTester will send X number of runners per Y seconds (e.g. 100 runners per second). FortiTester does not care whether the users come back or not (result will be measured at the end). If the DUT allows them to return in time, that DUT can 'sustain' this CPS rate.

- Understand that EACH IP, you can also use SOURCE PORT to distribution sessions. FortiTester **will FIRST use unique IP's first BEFORE source port**. Let's take a look at an extreme case:

FortiTester can use 1 IPs (controlled by subnet settings) and generate 55,535 (65,535 minus 10,000) connections to 1 destination, with use of source port. This settings can be found under client tab as below:



Protocol Level: HTTP 1.1

Request Header: User-Agent: Firefox/62.0

* The # value is converted to a random numerical digit.
* Examples:
Host: fortinet<###>.com

Client Close Mode: 3Way_Fin

Piggyback Get Requests

Source Port Range: 10000-65535
Range: 10,000 - 65,535

each src IP can utilise 55,535 port range, for example
1.1.1.1 src_port 10000 to 2.2.2.2 dst_port 80 (1st connection)
1.1.1.1 src_port 10001 to 2.2.2.2 dst_port 80 (2nd connection)

IP Change Algorithm: Increment
Source and destination ip change policy of network socket

Port Change Algorithm: Increment
Source and destination port change policy of network socket

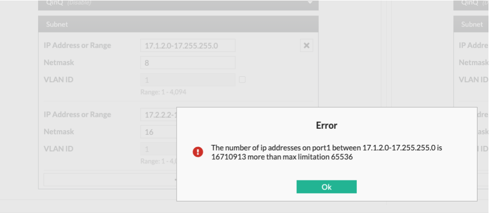
Therefore if both subnets and source port are configured (or left as default i.e. two subnets in certain models, higher end will have 4 subnets for default, and a source port of 10,000-65,535), FortiTester will distribute the sessions across the configured IP range and ports.

So to answer the original question: How many unique IP's can FortiTester generate?

The simple answer is: for HTTP CPS, FortiTester can generate 16 subnets x 65,536 IPs = 1,048,576 IPs on each end. However, the load, controlled by 'connections/secs' or simusers can be adjusted (or greater than the IP configured).

- It was mentioned earlier **for each case it's slightly different**. To explain further:

For HTTP CPS - if you set subnet to /8 (i.e. more hosts), when you click **save**, FortiTester does NOT allow you to go over the maximum of 65,535 (this is the MAX IP per subnet for HTTP CPS).



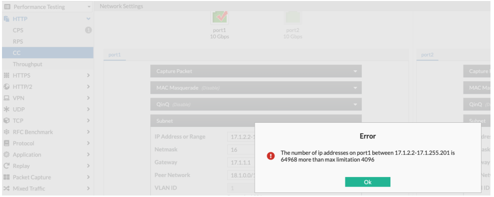
IP Address or Range: 17.1.2.0-17.255.255.0
Netmask: 8
VLAN ID: 1
Range: 1 - 4,094

IP Address or Range: 17.2.2.2-1
Netmask: 16
VLAN ID: 1
Range: 1 - 4,0

Error

The number of ip addresses on port1 between 17.1.2.0-17.255.255.0 is 16710913 more than max limitation 65536

But for HTTP CC (Concurrent session), a different test altogether, the max limitation of IP is 4,096. See error screenshot below (if your subnet/IP configured goes over the max value).



IP Address or Range: 17.1.2.2-1
Netmask: 16
Gateway: 17.1.1.1
Peer Network: 18.1.0.0/1
VLAN ID: 1

Error

The number of ip addresses on port1 between 17.1.2.2-17.1.255.201 is 64968 more than max limitation 4096

In the future we hope to document each case clearly for the maximum configured value.

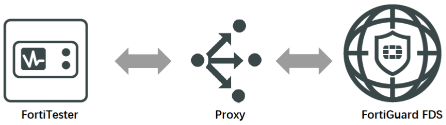
How does FortiTester run offline?

There are a few scenarios to cover:

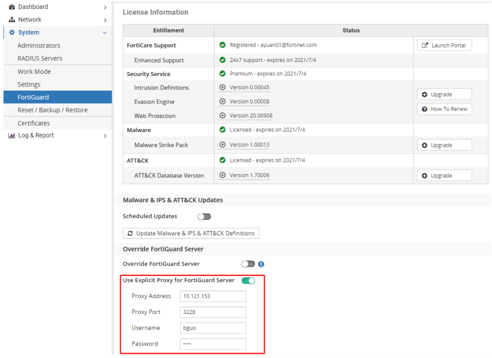
1. Without FortiManager

- FortiTester VMs requires Internet for periodic license validation. Once it validates, if VM goes offline, the license will be valid for 3 days before it requires validation again (goes into trial mode if fails).
- FortiTester appliances will work without internet; however, updates via internet are impacted (users can download updates manually via support website).
- FortiTester has 'HTTPS proxy feature' to allow FortiTester to reach internet via proxy, as below:

Topology



To configure on FortiTester GUI, go to **System > FortiGuard.**



License Information

Entitlement	Status	
FortiCare Support	Registered - ayuan01@fortinet.com	Launch Portal
Enhanced Support	24x7 support - expires on 2021/7/4	
Security Service	Premium - expires on 2021/7/4	
Intrusion Definitions	Version 0.00045	Upgrade
Evasion Engine	Version 0.00008	How To Renew
Web Protection	Version 20.00908	
Malware	Licensed - expires on 2021/7/4	
Malware Strike Pack	Version 1.00013	Upgrade
ATT&CK	Licensed - expires on 2021/7/4	
ATT&CK Database Version	Version 1.70006	Upgrade

Malware & IPS & ATT&CK Updates

Scheduled Updates

Update Malware & IPS & ATT&CK Definitions

Override FortiGuard Server

Override FortiGuard Server

Use Explicit Proxy for FortiGuard Server

Proxy Address: 10.121.153

Proxy Port: 3228

Username: bguo

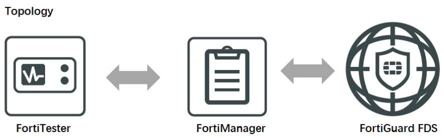
Password: ····

2a. With FortiManager (Online)

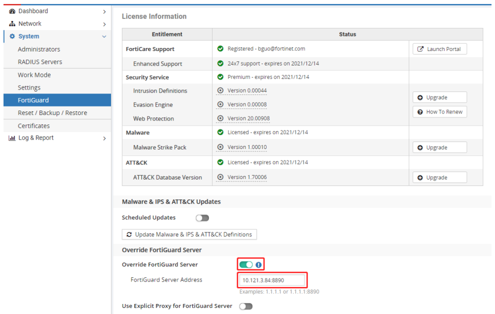
FortiManager v6.4.6+ and v7.0.1+ supports the following functions:

- FortiTester license verification
- FortiTester Update packages (malware / IPS / web protection updates)

Topology



To configure on FortiTester GUI, go to **System** > **FortiGuard**, then input FortiManager IP in FortiGuard IP address field.



License Information

Entitlement	Status	
FortiCare Support	Registered - bguo@fortinet.com	Launch Portal
Enhanced Support	24x7 support - expires on 2021/12/14	
Security Service	Premium - expires on 2021/12/14	
Intrusion Definitions	Version 0.00044	Upgrade
Evasion Engine	Version 0.00008	How To Renew
Web Protection	Version 20.00908	
Malware	Licensed - expires on 2021/12/14	
Malware Strike Pack	Version 1.00010	Upgrade
ATT&CK	Licensed - expires on 2021/12/14	
ATT&CK Database Version	Version 1.70006	Upgrade

Malware & IPS & ATT&CK Updates

Scheduled Updates

Update Malware & IPS & ATT&CK Definitions

Override FortiGuard Server

Override FortiGuard Server

FortiGuard Server Address: 10.121.3.84:8890

Examples: 1.1.1.1 or 1.1.1.1:8890

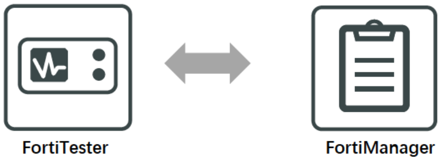
Use Explicit Proxy for FortiGuard Server

2b. With FortiManager (offline)

Purpose

- FMG01 to act as a licensing server (like FDS), enable web service on FortiManager interface
- FMG02 to get the packages from online FDS, export the packages and import back into FortiManager 01
- Users import license (from support.fortinet.com) into FMG01 to validate FortiTester

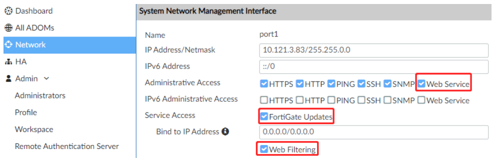
Topology



FortiManger Offline Mode

Tp enable service update, go to **ADOM Fabric > System Settings > Network.**

You must get entitlement from support.forinet.com if you use FortiManager OFFLINE mode.



System Network Management Interface

Name: port1

IP Address/Netmask: 10.121.3.83/255.255.0.0

IPv6 Address: ::/0

Administrative Access: ☑HTTPS ☑HTTP ☑PING ☑SSH ☑SNMP ☑Web Service

IPv6 Administrative Access: □HTTPS □HTTP □PING □SSH □SNMP □Web Service

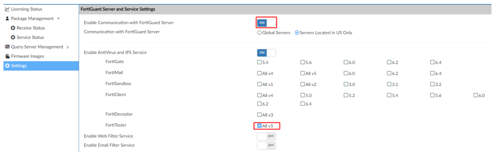
Service Access: ☑FortiGate Updates

Bind to IP Address: 0.0.0.0/0.0.0.0

☑Web Filtering

Configure ONLINE mode on FMG01 (This FortiManager can reach the internet.)

Go to **ADOM Fabric > FortiGuard > Settings.**



FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server: ON

Communication with FortiGuard Server: ○Global Servers ●Servers Located in US Only

Enable AntiVirus and IPS Service: ON

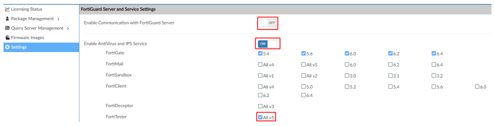
FortiGate	□5.4	□5.6	□6.0	□6.2	□6.4	
FortiMail	□All v4	□All v5	□6.0	□6.2	□6.4	
FortiSandbox	□All v1	□All v2	□3.0	□3.1	□3.2	
FortiClient	□All v4	□5.0	□5.2	□5.4	□5.6	□6.0
	□6.2	□6.4				
FortiDeceptor	□All v3					
FortiTester	☑All v5					

Enable Web Filter Service: OFF

Enable Email Filter Service: OFF

Configure offline mode on FMG02 (This FortiManager cannot reach the internet.)

Go to **ADOM Fabric > FortiGuard > Settings.**



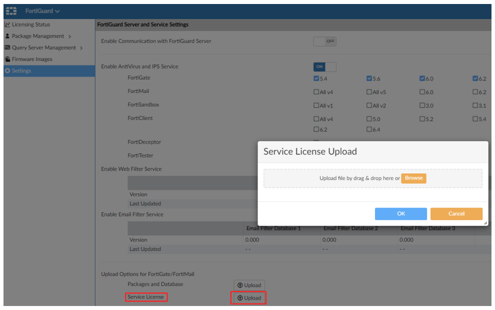
FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server: OFF

Enable AntiVirus and IPS Service: ON

FortiGate	☑5.4	☑5.6	☑6.0	☑6.2	☑6.4	
FortiMail	□All v4	□All v5	□6.0	□6.2	□6.4	
FortiSandbox	□All v1	□All v2	□3.0	□3.1	□3.2	
FortiClient	□All v4	□5.0	□5.2	□5.4	□5.6	□6.0
	□6.2	□6.4				
FortiDeceptor	□All v3					
FortiTester	☑All v5					

Import FortiTester entitlement into FMG02 (FortiManager that has no Internet access).



FortiGuard Server and Service Settings

Enable Communication with FortiGuard Server: OFF

Enable AntiVirus and IPS Service: ON

FortiGate	☑ 5.4	☑ 5.6	☑ 6.0	☑ 6.2
FortiMail	☐ All v4	☐ All v5	☐ 6.0	☐ 6.2
FortiSandbox	☐ All v1	☐ All v2	☐ 3.0	☐ 3.1
FortiClient	☐ All v4 ☐ 6.2	☐ 5.0 ☐ 6.4	☐ 5.2	☐ 5.4
FortiDeceptor				
FortiTester				

Enable Web Filter Service

Version

Last Updated

Enable Email Filter Service

	Email Filter Database 1	Email Filter Database 2	Email Filter Database 3
Version	0.000	0.000	0.000
Last Updated	- -	- -	- -

Upload Options for FortiGate/FortiMail

Packages and Database: Upload

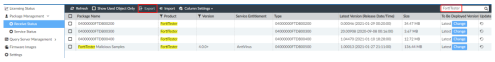
Service License: Upload

Service License Upload

Upload file by drag & drop here or Browse

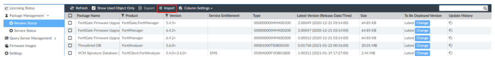
OK Cancel

Export service package from an ONLINE FortiManager (FMG01).



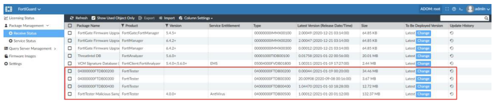
☐	Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Version	Update
☐	04000000FTDB00200	FortiTester			04000000FTDB00200	0.00046 (2021-01-29 00:20:00)	34.47 MB	Latest Change	
☐	04000000FTDB00300	FortiTester			04000000FTDB00300	20.00908 (2020-09-08 00:16:00)	3.67 MB	Latest Change	
☐	04000000FTDB00400	FortiTester			04000000FTDB00400	1.04470 (2021-01-10 18:28:00)	12.72 MB	Latest Change	
☐	FortiTester Malicious Samples	FortiTester	4.0.0+	AntiVirus	04000000FTDB00500	1.00013 (2021-01-27 21:11:00)	136.44 MB	Latest Change	

Import the service package in FMG02 (OFFLINE FortiManager).



☐	Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Version	Update History
☐	FortiGate Firmware Upgra	FortiGate;FortiManager	5.4.5+		00000000IMMX00100	2.00049 (2020-12-21 03:14:00)	64.85 KB	Latest Change	
☐	FortiGate Firmware Upgra	FortiManager	6.4.2+		00000000IMMX00200	2.00047 (2020-12-21 03:14:00)	64.85 KB	Latest Change	
☐	FortiGate Firmware Upgra	FortiManager	6.4.2+		00000000IMMX00300	0.00012 (2020-12-21 03:14:00)	64.85 KB	Latest Change	
☐	ThreatIntel DB	FortiAnalyzer	5.6.0+		00001000TIDB00100	0.01758 (2021-01-22 00:56:00)	20.01 MB	Latest Change	
☐	VCM Signature Database (	FortiClient;FortiAnalyzer	5.4.0+;5.6.0+	EMS	05004000FVDB01800	1.00311 (2021-01-19 17:27:00)	2.44 MB	Latest Change	

After it will show the FortiTester service package after import on FortiManager GUI



☐	Package Name	Product	Version	Service Entitlement	Type	Latest Version (Release Date/Time)	Size	To Be Deployed Version	Update History
☐	FortiGate Firmware Upgra	FortiGate;FortiManager	5.4.5+		00000000IMMX00100	2.00049 (2020-12-21 03:14:00)	64.85 KB	Latest Change	
☐	FortiGate Firmware Upgra	FortiManager	6.4.2+		00000000IMMX00200	2.00047 (2020-12-21 03:14:00)	64.85 KB	Latest Change	
☐	FortiGate Firmware Upgra	FortiManager	6.4.2+		00000000IMMX00300	0.00012 (2020-12-21 03:14:00)	64.85 KB	Latest Change	
☐	ThreatIntel DB	FortiAnalyzer	5.6.0+		00001000TIDB00100	0.01758 (2021-01-22 00:56:00)	20.01 MB	Latest Change	
☐	VCM Signature Database (	FortiClient;FortiAnalyzer	5.4.0+;5.6.0+	EMS	05004000FVDB01800	1.00311 (2021-01-19 17:27:00)	2.44 MB	Latest Change	
☐	04000000FTDB00200	FortiTester			04000000FTDB00200	0.00044 (2021-01-19 00:20:00)	34.46 MB	Latest Change	
☐	04000000FTDB00300	FortiTester			04000000FTDB00300	20.00908 (2020-09-08 00:16:00)	3.67 MB	Latest Change	
☐	04000000FTDB00400	FortiTester			04000000FTDB00400	1.04470 (2021-01-10 18:28:00)	12.72 MB	Latest Change	
☐	FortiTester Malicious Samp	FortiTester	4.0.0+	AntiVirus	04000000FTDB00500	1.00012 (2021-01-20 01:12:00)	132.37 MB	Latest Change	

Configure FortiTester to use FortiManager 02 (offline FortiManager).

What is the difference between Connections per Second and Simulated Users?

The following analogy may be helpful:

Simulated Users - FortiTester will send X number of runners from starting line to finish (to fetch something from the finish line). The runner comes back with the objects, and starts the run again (until test time finishes). The DUT (e.g. FG) might or might not be able to hold up the users (runners).

Connections per Second - FortiTester will send X number of runners per Y seconds (e.g. 100 runners per second). FortiTester does not care whether the users come back or not (the result will be measured at the end). If the DUT allows them to return in time, that DUT can 'sustain' this CPS rate.

How to redirect GUI access to HTTPS from HTTP?

FortiTester disabled the HTTP access by default from version 7.3.0. The following CLI command can enable HTTPS redirect.

```
FortiTester # config system web-service
```

```
FortiTester (web-service) # set https-redirect-status enable
```

```
FortiTester (web-service) # set https-redirect-host www.fts.fortinet.com
```

```
FortiTester (web-service) # end
```

```
FortiTester #
```

Parameter	Description	Type	Default
https-redirect-status	Enable/disable redirect HTTPS from HTTP	option	disable
https-redirect-host	FortiTester's domain/IP	string	IP of management interface

www.fortinet.com

Copyright© 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.