



FortiTester Release Notes

VERSION 7.1.0

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



December 8, 2021

FortiTester 7.1.0 Release Notes

Change Log

Date	Change Description
December 8, 2021	FortiTester 7.1.0 initial release.

Introduction

FortiTester™ appliances offer enterprises and service providers a cost-effective solution for performance testing and validating their network security infrastructure and services, providing a comprehensive range of application test cases to evaluate equipment and right-size infrastructure. All test functionality is included in one simple device-based license.

FortiTester provides powerful yet easy-to-use test cases that simulate many stateful applications and malicious traffic. Built-in reporting provides comprehensive information about the tests, including SNMP stats from the device under test (DUT). It enables you to establish performance standards and conduct audits to validate that they continue to be met. A single 40-GE appliance allows over 20 million concurrent connections and new HTTP connection rates greater than 1 million/second; hardware-based acceleration supports new HTTPS connection rates above 20,000/second. Up to 8 appliances can be grouped in Test Center mode to massively scale performance. 40-GE device interfaces can be split to 4x 10-GE SFP+ for additional testing flexibility. 100- and 10-GE devices and their VM versions complete the Tester range, offering competitive price points for their target customers.

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

This *Release Notes* covers the new features, enhancements, known and resolved issues, and upgrade instructions about FortiTester Version 7.1.0, Build 0016.

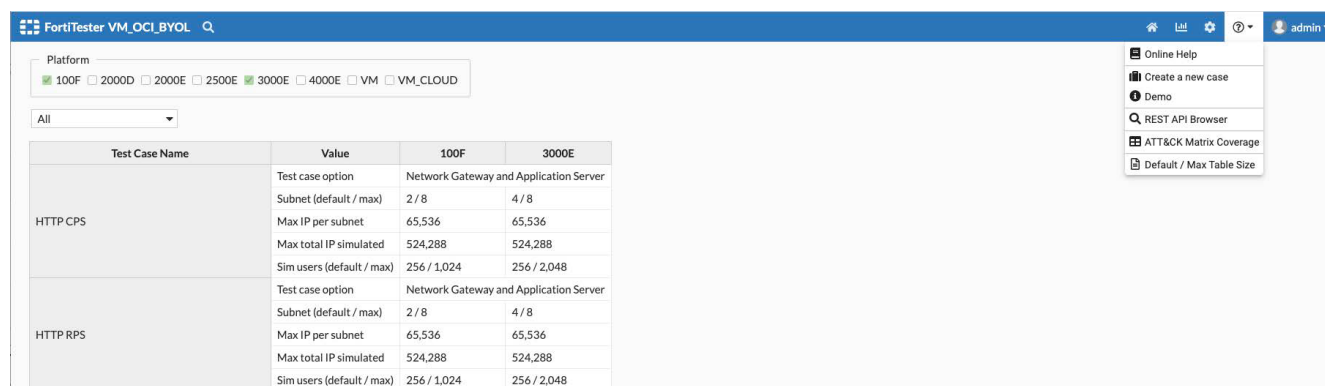
For additional documentation, please visit: <http://docs.fortinet.com/fortitester>.

What's new

FortiTester 7.1.0 offers the following new features and enhancements:

Default and Maximum values table

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 now 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.



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

Out of Order Reset flag

Often in performance testing, the DUT might have ASIC (e.g. nturbo) or engines enabled which might affect packet orders. In this version, FortiTester added an "Out of Order Reset" flag for ALL TCP related cases. If enabled, this option sets the "Out of Order Reset" flag in both client and server sides for TCP Options.

Note: If enabled with this option, FortiTester will send Reset packet to close the TCP session which has occurred in the out of order sequence.

Specifics	
Load	Client Server Action
Profile	TCP Options Network Limit
TCP Receive Window	32768 <small>The receive window in which you want the TCP stack to send TCP segments. (Range: 1 - 65,535)</small>
TCP Window Scale	0 <small>Range: 0 - 14</small>
Delayed Acks	<input checked="" type="checkbox"/> <small>Select to cause the TCP stack to implement the Delayed ACK strategy</small>
Delayed Ack Timeout	100 <small>Range: 1 - 60,000. (Unit: millisecond)</small>
Ack every N	2 <small>Range: 1 - 65,535</small>
Explicit Congestion Notification	Disabled
Initial Congestion Window	2 <small>Range: 1 - 16</small>
Timestamps Option	<input checked="" type="checkbox"/> <small>Select to add a TCP timestamp to each TCP segment</small>
Enable Push Flag	<input checked="" type="checkbox"/>
SACK Option	<input checked="" type="checkbox"/>
Enable TCP Keepalive	<input checked="" type="checkbox"/>
Keepalive Timeout	3 <small>Range: 1 - 86,400. (Unit: second)</small>
Keepalive Probes	3 <small>Range: 1 - 3,600</small>
Override Internal Timeout Calculation	<input checked="" type="checkbox"/> <small>Select to override The TCP stack calculation of the retransmission timeout value</small>
Retransmission Timeout	2000 <small>Range: 20 - 60,000. (Unit: millisecond)</small>
Retries	3 <small>The number of times a timed-out packet is retransmitted before aborting. (Range: 0 - 10)</small>
Fin Ack Timer	0 <small>Range: 0 - 180,000. (Unit: millisecond)</small>
Out of Order Reset	<input checked="" type="checkbox"/>

Internet Mix Option (IMIX)

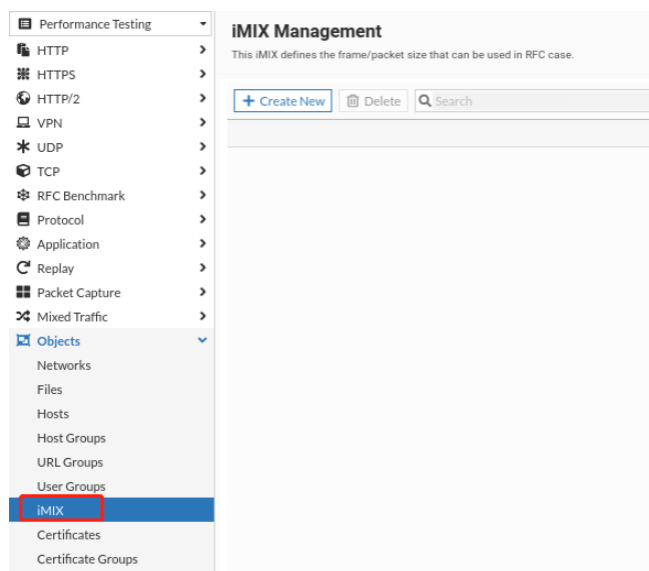
Internet Mix or IMIX refers to typical Internet traffic passing some network equipment such as routers, switches or firewalls. When measuring equipment performance using an IMIX of packets the performance is assumed to resemble what can be seen in "real-world" conditions.

For RFC2544 and RFC3511 throughput, frame size has added an IMIX option. If you choose IMIX, you need to reference IMIX objects.

Performance Testing		Specifics	
		Load	Client Server
HTTP	>		
HTTPS	>		
HTTP/2	>		
VPN	>		
UDP	>		
TCP	>		
RFC Benchmark	>		
RFC 2544	>		
Throughput	2		

Flows	128 <small>Range: min - 16,384. (min: the selected port pairs * cores per port)</small>
Traffic Direction	Both Unidirectional Bidirectional <small>Both of unidirectional and bidirectional traffic</small>
Frame Size	RFC 2544 User Defined iMIX
	Sample (Manage iMIX)
Traffic Cycle Time	30 <small>Traffic burst duration in seconds for each frame size. (Range: 2 - 3,600, unit: second)</small>

Before referencing iMIX, the iMIX object needs to be configured.



The Frame Size/ Packet Size and Weight can be configured. Frame size cannot be repeated, and currently supports up to 10 records.

No.	Packet Size	Frame Size	Percentage	Weight
1	1262	1280	25%	1
2	238	256	25%	1
3	110	128	25%	1
4	46	64	25%	1

URL Group in Action of HTTP cases

Before 7.1, FortiTester's action on HTTP/HTTP2/HTTPS test cases can be set to custom, while a request could have up to maximum of 32 URLs. Now in v7.1 FortiTester comes with a new "URL group" option, which allows users to configure/reuse a URL host group object of up to 1000 URLs.

1. Create a URL Group object.

Performance Testing

- HTTP
- HTTPS
- HTTP/2
- VPN
- UDP
- TCP
- RFC Benchmark
- Protocol
- Application
- Replay
- Packet Capture
- Mixed Traffic
- Objects
 - Networks 17
 - Files 1
 - Hosts 4
 - Host Groups 5
 - URL Groups 22

URL Group Options

Name

Allowed: English character, number and . - _

2. A special feature allows the user to add URL Group hosts using existing Host Groups.



After being created, this imported Host Group has no relationship with the URL Group anymore.

One URL Group can have up to 1000 URL's.

Performance Testing

- HTTP
- HTTPS
- HTTP/2
- VPN
- UDP
- TCP
- RFC Benchmark
- Protocol
- Application
- Replay
- Packet Capture
- Mixed Traffic
- Objects
 - Networks 17
 - Files 1
 - Hosts 4
 - Host Groups 5
 - URL Groups 22

Basic Information

Name

Sample

URL Management

Create New

Delete

Search

No.	Hostname	Method	URI	Body	Edit
No results					

3. Open the Action tab in the HTTP-based case. Choose "**Custom**" in **Method** and the **URL Group** will be selectable.

FortiTester 4000E

Performance Testing

- HTTP
 - CPS 37
 - RPS 7
 - CC 8
 - Throughput 4
- HTTPS
- HTTP/2
- VPN
- UDP
- TCP
- RFC Benchmark
- Protocol
- Application
- Replay
- Packet Capture

Network Settings

VLAN ID: 1 (Range: 1 - 4,094)

IP Address or Range: 17.4.2.2-17.4.2.201

Netmask: 16

VLAN ID: 1 (Range: 1 - 4,094)

Specifics

Load Client Server **Action**

Method: Custom

Type: Request Pages **URL Group**

URL Group: **Sample** (Manage Groups)

SSLVPN case enhancement

1. Add HTTP RPS within the inner tunnel for SSL-VPN Throughput.



The user can configure Requests Per Connection to determine how many HTTP Requests are sent on one TCP session, and then close it.

FortiTester 2000D

Select case options

Inner Traffic: **HTTP RPS**

IP Version: v4

DUT Role: Network Gateway

DUT Working Mode (DUT: Device under test): Transparent (TP)

Network Address Translation (NAT): Network Address Translation (NAT)

Network Config: Default

Ok Cancel

VPN

- IPsec
- SSL-VPN
 - CPS 15
 - RPS 1
 - CC 14
 - Throughput 10**
- UDP
- TCP

Performance Testing

HTTP

HTTPS

HTTP/2

VPN

IPsec

SSL-VPN

CPS

RPS

CC

Throughput

UDP

TCP

RFC Benchmark

Protocol

Application

Replay

Packet Capture

Mixed Traffic

Objects

Schedules

Results

Network Settings

Capture Packet

QinQ (Disable)

Subnet

IP Address or Range

17.1.2.2-17.1.2.201

Netmask

16

VPN Gateway

17.1.1.1

Peer Network

19.10.0/16

VLAN ID

1

Range: 1 - 4,094

IP Address or Range

17.2.2.2-17.2.2.201

Netmask

16

VPN Gateway

17.2.1.1

Peer Network

19.2.0.0/16

VLAN ID

1

Range: 1 - 4,094

Load Client HTTP RPS

Load Client Server Action

Mode

Simuser

Simulated Users

1

Range: 1 - 32

Requests per Connection

0

Range: 0 - 50,000

HTTP Request Time Out

5

Range: 1 - 3,600. (Unit: second)

2. To support FortiTester ports configured in a trunk 802.1x environment, FortiTester added the ability to add QinQ and VLAN tag field in the network setting for SSLVPN test.

In all SSL-VPN(CPS/RPS/CC/Throughput) cases, create the Tag ID in the **Port > Subnet** configuration items.

Performance Testing

HTTP

HTTPS

HTTP/2

VPN

IPsec

SSL-VPN

CPS

RPS

CC

Throughput

UDP

TCP

RFC Benchmark

Protocol

Application

Replay

Packet Capture

Mixed Traffic

Objects

Schedules

Results

Basic Information (SSL-VPN CPS)

Network Settings

CLIENT

SERVER

port1

port2

port3

port4

port1

port2

port3

port4

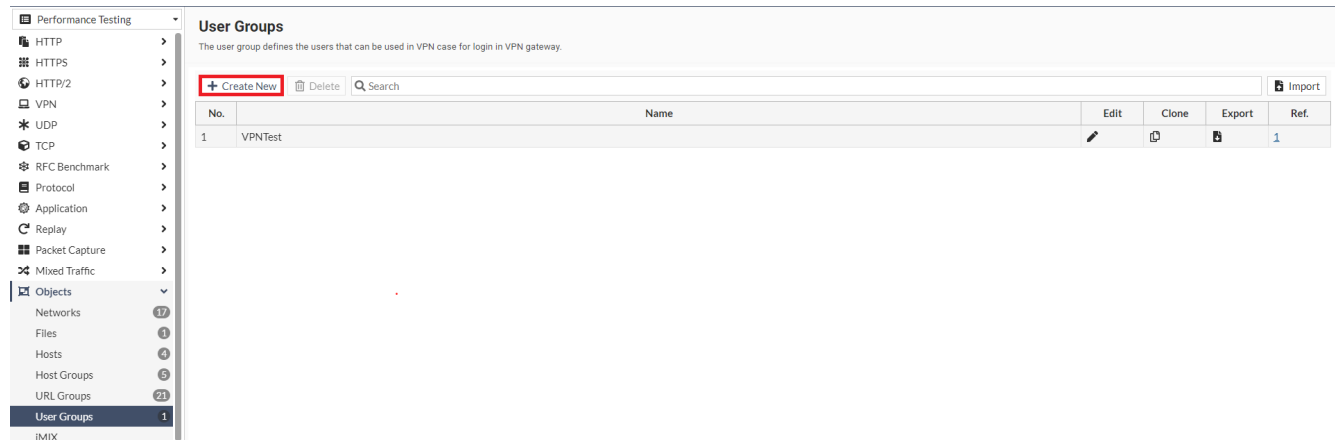
Start

Save

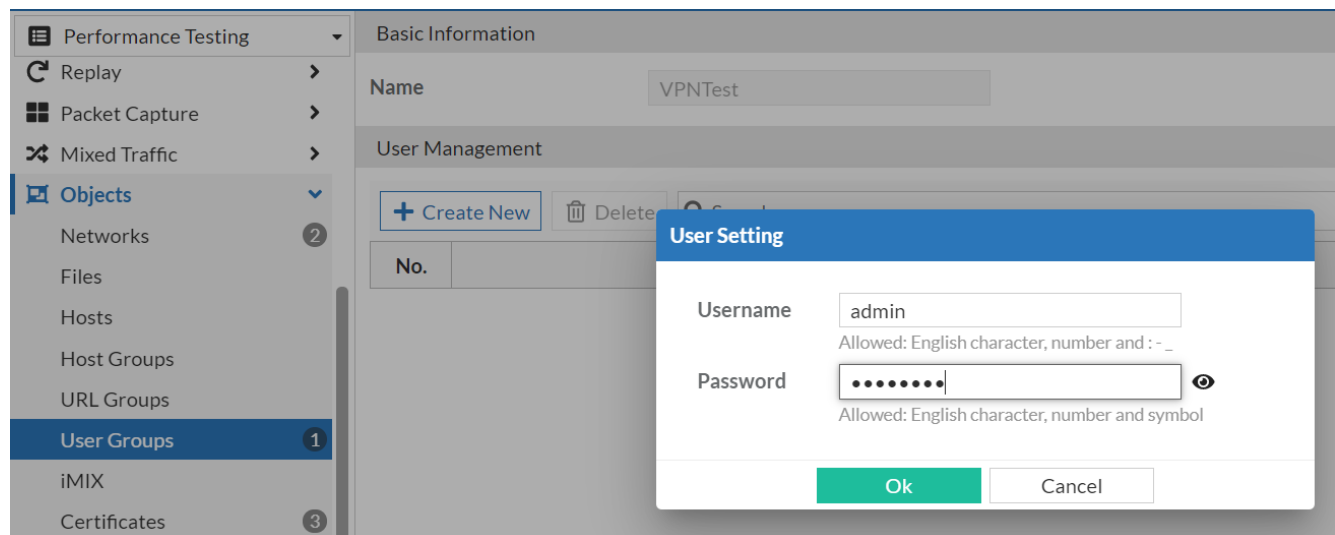
Cancel

3. Before v7.1 FortiTester had the ability to simulate a single username login for tunnel mode. Now in 7.1, FortiTester provides the ability to simulate multiple user names. This allows FortiView to populate with more rich user name information, for example.

a. Go to **Objects > User Groups > Create New** to create a user group object.



b. Click **Create New** to create multiple users/password pairs to the current **User Group Object**.



c. 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 a.

Performance Testing

HTTP

HTTPS

HTTP/2

VPN

IPsec

SSL-VPN

CPS

RPS

CC

Throughput

UDP

TCP

RFC Benchmark

Protocol

Application

Replay

Packet Capture

Mixed Traffic

Objects

Schedules

Results

Network Settings

Netmask

16

VPN Gateway

1.4.1.1

Peer Network

2.4.0.0/16

VLAN ID

1

Range: 1 - 4,094

Specifics

Load

Client

HTTP CPS

Mode

Simuser

Simulated Users

512

Range: the selected port pairs - 4,096

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)

VPN Gateway Port

10443

Range: 0 - 65,535

Enable User Group

☒

User Group

VPNTTest

(Manage Groups)

Tunnel Mode

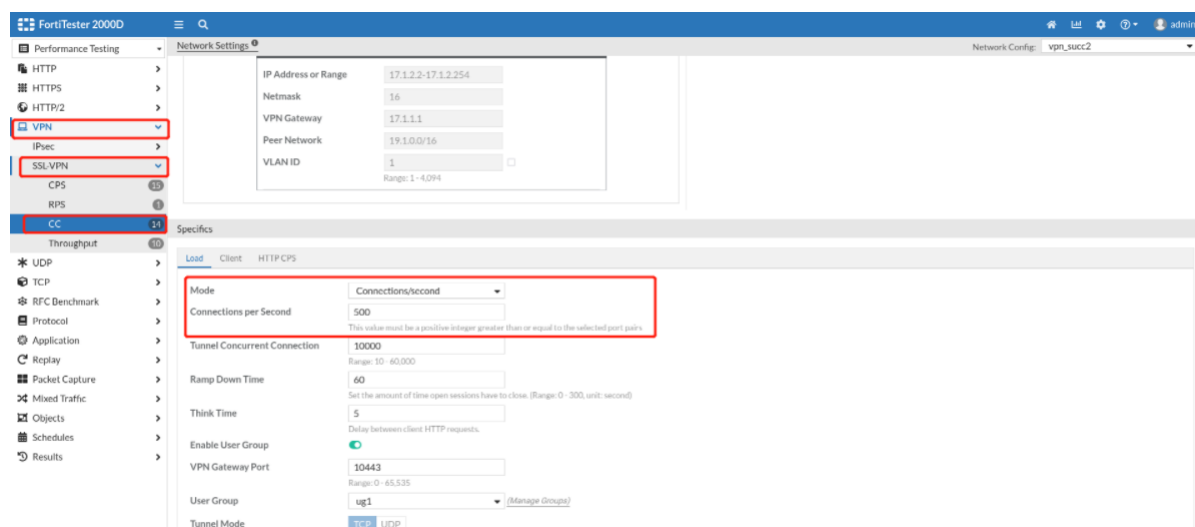
TCP

UDP

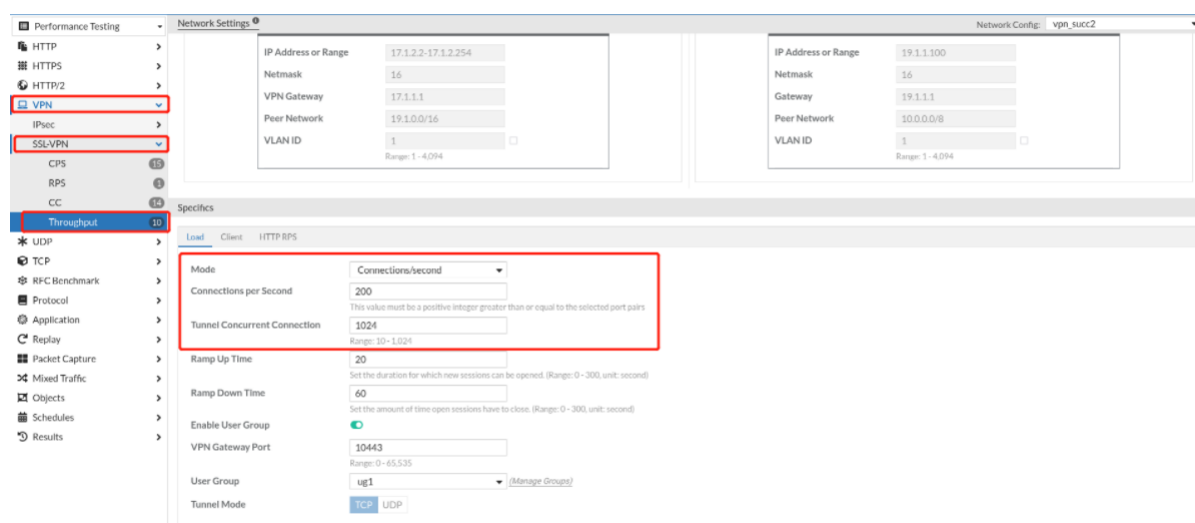
Add Connections per Second (CPS) to all SSLVPN

FortiTester v7.1.0 added CPS (connections per second) test mode (along with existing simusers) for SSLVPN CC and Throughput cases. All 4 SSLVPN cases (CPS, CC, RPS and Throughput) support simusers and CPS mode to control the rate of setup of SSLVPN tunnels.

1. In SSL-VPN cases, go to the **VPN > SSL-VPN > CC > Load tab > Mode** dropdown menu, select **Connections/second** and fill in the rate.



2. In Throughput case, go to the **VPN > SSL-VPN > Throughput > Load tab > Mode** dropdown menu, select **Connections/second** and fill in the rate.



The "Tunnel Concurrent Connection" item is the total number of tunnels created in the Throughput case.

Added "Maximum Timeout Packet Count"

Added "Maximum Timeout Packet Count" to Attack/HTTP Evasion/GTP cases.

Before v7.1, FortiTester devices conducting PCAP replay in ATTACK/HTTP Evasion and GTP will not send further packets if the packet loss count is more than 20. Now, in v7.1, users will have finer control over the max packet loss (from 1-4294,967,295) before FortiTester stops sending packets in PCAP replay package.

Security Testing
DDoS
Fuzzing
IPS
Attack 3
HTTP Evasion 1
Malware
Web Protection
Mixed Traffic
Objects
Maintenance
Schedules
Results

Network Settings

Subnet
IP Address 1.1.2.2
Netmask 16
Gateway 1.1.1.1
Peer Network 2.1.0.0/16
VLAN ID 1
Range: 1 - 4,094

Specifics

Load	Client	Server	Action
Loops	1	Range: 0 means unlimited, 0 - 10,000,000.	
Delay	0	Delay between each loop. (Range: 0 - 120,000, Unit: millisecond)	
TCP Replay Time Out	200	Range: 1 - 600,000. (Unit: millisecond)	
Break Once Packet Lost	No	Break the pcap replay when packet lost	
Maximum Timeout Packet Count	20	Range: 0 - 4,294,967,295.	

New OpenAPI

FortiTester v7.1 supports new OPENAPI format. API browser in GUI has been improved to allow users to try out the API in GUI. Users can also find FortiTester API documentation on FNDN (Fortinet Developer Network).

FortiTester VM_OCI_BYOL
APIs
User Management
System Management
System RADIUS Server Management
Object Management
Case Management
Case History
Case Intrusion
Case Intrusion Report
Case User Intrusions
Case User Malware Group Management
Case FGD Malware Management
Case Web Protection Management
Case Web Crawler Management
ATT&CK

FortiTester API Documentation

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

Hardware support

This release supports the following hardware models:

- FortiTester 100F
- FortiTester 2000D
- FortiTester 2000E
- FortiTester 2500E
- FortiTester 3000E
- FortiTester 4000E
- FortiTester VM (VMware ESX/ESXi, KVM, OpenStack, AWS, AZURE, GCP, OCI, and ALI)

System integration and support

FortiTester v7.1.0 can integrate with the following products:

- FortiOS v7.0.1 Security Fabric Integration
- FortiManager v6.4.6 and 7.0.1 License activation and FortiGuard server updates
- FortiSIEM v5.3.0 log integration
- SYSLOG to other product

Upgrade/downgrade instructions

You can use FortiTester's web UI to upgrade the firmware image.

Before you begin:

- Back up your configuration (From the GUI, click **System > Reset/Backup/Restore > Backup**).
- Record the current version your system is running before upgrade. This can be found in **GUI > Dashboard**, or from CLI "get system status".
- Download the image file from the Fortinet support website.
- Read the *Release Notes* for the version you plan to install.
- Upgrade the firmware from the System page.

Note: If you are using the Test Center feature, Test Center Clients will be disconnected during the upgrade, and must be reconnected after the upgrade is completed.

To upgrade the firmware:

Note that CLI is the only way to upgrade FortiTester--2000D from any pre-2.7.0 version. The Web UI does not support this upgrade. Connect to the CLI through a terminal emulator such as Putty using the following steps:

1. Start a terminal emulation program on the management computer, select the COM port, and set the baud rate as 9600.
2. Press Enter on your keyboard to connect to the CLI.
3. Login with the username - **admin** and its password.
4. Reboot the system using command `execute reboot`.
5. Select **F** to format the boot device.
6. Select **G** to download the image from the TFTP server mentioned in "Before you begin". You will be required to specify IP addresses of the TFTP server and the FortiTester appliance (management port). Make sure that both of the IP addresses are in the same subnet.
7. Select **D** to save the image file as "Default firmware" for upgrading.
8. System starts rebooting. During the rebooting process, the system will take 2~3 minutes to replace the firmware on the active partition (the message "Reading boot image ... bytes." appears). Please be patient while the system is rebooting.
9. After reboot, IP address of the management port is set to a default of 192.168.1.99. It can be changed through the following commands:

```
FAD15D3114000001 # config system interface
FAD15D3114000001 (interface) # edit mgmt
FAD15D3114000001 (mgmt) # set ip <IP_Address> <Netmask>
FAD15D3114000001 (mgmt) # end
FAD15D3114000001 #
```
10. Firmware upgrade is completed. Access the Web UI through the management port. You might need to refresh the Web UI pages by pressing **Ctrl+F5**.



FortiTester v7.1.0 does not support downgrading to previous releases. Users have the option of backup configuration and tests cases before upgrading, or restoring older firmware and configuration if necessary.

Note: If the user wants to upgrade to 7.1.0, it's best to come from version 7.0.0. Users with versions before 7.0.0 should first upgrade to 4.x then to 7.0.0, before upgrading to 7.1.0

Accelerator cards

All hardware models of FortiTester except 100F and 2000E have a performance-enhancing SSL acceleration. This helps accelerate SSL traffic in the handshake stage.

To check which card and card model your device uses:

Enter the following CLI command:

```
diagnose hardware info
```

The following information will be displayed:

```
...  
[Accelerator info]  
SSL Accelerator Model<Model number>
```

Model III represents the Cavium Nitrox III card, model V represents the Cavium Nitrox V card, and model VI represents the Intel QAT card.

Resolved issues

The following table lists the major issues that have been resolved in this release. The resolved issues listed below do not list every bug that has been corrected with this release. For inquiries about a particular bug, please contact Fortinet Customer Service & Support at <https://support.fortinet.com>.

Bug ID	Description
760542	error: Invalid 'Min Server IP Address' IP address: x.x.x.x (network address)
750922	While running Fortinet EMIX traffic test using FTS4000E, FortiGate reports IPS signature attack for FTP traffic
749512	Security Testing Fuzzing ICMP/TCP/UDP Bad code ranges are not settable.
711104	Suggestion that FortiTester be able to generate traffic load at a configured rate.
708574	In SSL/VPN throughput tests, all HTTP traffic continue in the same sessions during the whole test.
708571	No Vlan tag field in the network setting for the SSL/VPN test.

Known issues

The table below lists the major known issues discovered in this release. For inquiries about a particular bug, please contact Fortinet Customer Service & Support: <https://support.fortinet.com>.

Bug ID	Description
761629	Ramp up spike
758550	Lot of packet loss due to retransmission - Proxy HTTP 64K test
751949	EMIX throughput using Fortinet EMIX Traffic template gives lot more lower results compares to Ixia /BP EMIX Traffic profile.
738156	Fortitester agent is not digital signed and will be detected by FortiEDR as suspicious file
512700	B0095: Only one IP address in server subnet IP address range is used during explicit proxy test
697147	FortiTester SSL/VPN test does not reflect the FortiClient connections.
705388	Test import fails if the test exists in another work mode or fanout mode.

Change Log

Date	Change Description
December 8, 2021	FortiTester 7.1.0 initial release.



FORTINET®



Copyright© 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.