FortiTester Release Notes

VERSION 7.0.0

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

FORTINET®

August 9, 2021
FortiTester 7.0.0 Release Notes

Change Log

Date	Change Description
August 9, 2021	FortiTester 7.0.0 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 malicous 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 7.0.0, Build 0008.

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

What’s new

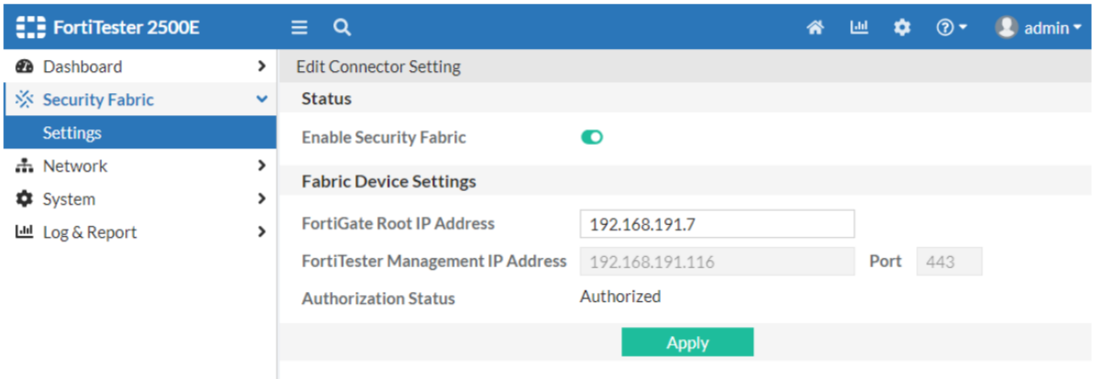
FortiTester 7.0.0 offers the following new features and enhancements:

New GUI

FortiTester v7.0 has a brand new GUI interface for enhanced usability and experience. While most items are unchanged but users will find a similar “FortiOS” experience in selection and searching. Noticeably multi-selection will involve the use of mouse and the shift key, rather than use of checkboxes in previous versions.

Support for Fortinet Security Fabric

FortiTester 7.0.0 will have the ability to connect to FortiOS security Fabric and display data such as system information in FortiOS as a widget, which will also appear in physical and logical topology in FortiOS. For detailed configuration, please refer to the administration guide. Here are some key settings in FortiTester and how it appears in FortiGate.



Edit Connector Setting

Status

Enable Security Fabric ●

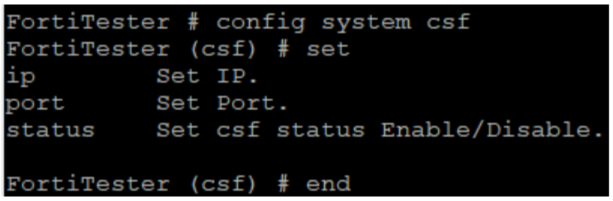
Fabric Device Settings

FortiGate Root IP Address: 192.168.191.7

FortiTester Management IP Address: 192.168.191.116 Port: 443

Authorization Status: Authorized

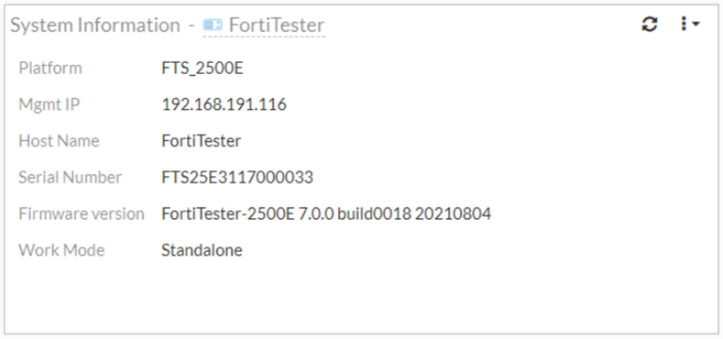
You can set the configuration up in the console.



```
FortiTester # config system csf
FortiTester (csf) # set
ip         Set IP.
port       Set Port.
status     Set csf status Enable/Disable.

FortiTester (csf) # end
```

Screen on FortiGate:



System Information - FortiTester

Platform	FTS_2500E
Mgmt IP	192.168.191.116
Host Name	FortiTester
Serial Number	FTS25E3117000033
Firmware version	FortiTester-2500E 7.0.0 build0018 20210804
Work Mode	Standalone

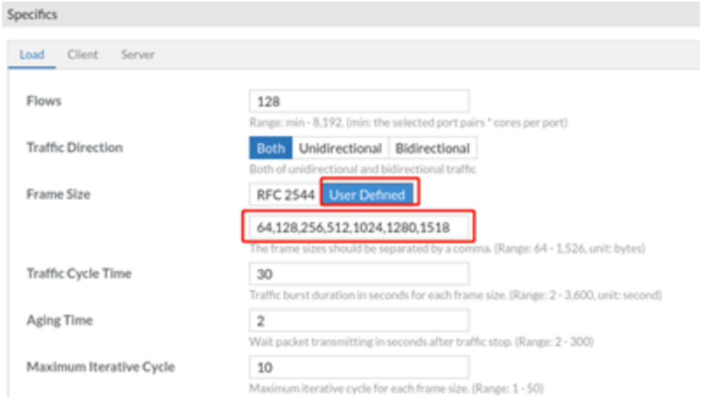
Function Enhancement

With RFC2544 performance testing in Cloud environments such as AWS/Azure, often MTU could be smaller than FortiTester default MTU of 1500 bytes (which cannot be change along with Cloud platforms), and hence maximum frame size could not be tested. In this version, FortiTester allows users to specify frame sizes to cater for different path MTU.

Example

Assume an RFC default MTU size as 1500 bytes. If Cloud MTU path is 1480, then 1480 bytes + 18 bytes (frame header+CRC) = 1498 bytes as the maximum frame size.

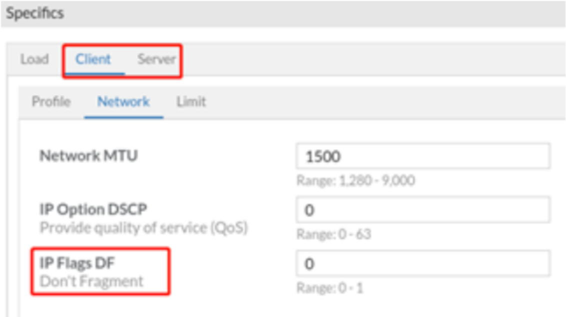
1. For the RFC2544 case, add Frame Size config by a user. Go to **Specifics > Load > Frame Size > UserDefined**.



Specifics

Flows	128 Range: min - 8,192. (min: the selected port pairs * cores per port)
Traffic Direction	Both | Unidirectional | Bidirectional Both of unidirectional and bidirectional traffic
Frame Size	RFC 2544 | User Defined 64,128,256,512,1024,1280,1518 The frame sizes should be separated by a comma. (Range: 64 - 1,526, unit: bytes)
Traffic Cycle Time	30 Traffic burst duration in seconds for each frame size. (Range: 2 - 3,600, unit: second)
Aging Time	2 Wait packet transmitting in seconds after traffic stop. (Range: 2 - 300)
Maximum Iterative Cycle	10 Maximum iterative cycle for each frame size. (Range: 1 - 50)

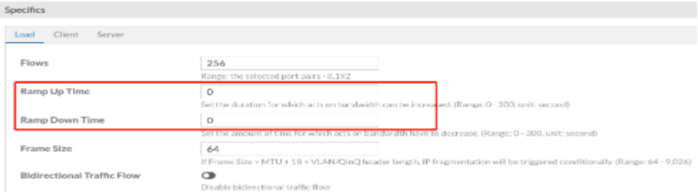
2. **Add** an option to set the "do not fragment" flag in both client and server sides for IPv4.



Specifics

Network MTU	1500 Range: 1,280 - 9,000
IP Option DSCP Provide quality of service (QoS)	0 Range: 0 - 63
IP Flags DF Don't Fragment	0 Range: 0 - 1

3. **Add** ramp up/down for UDP PPS based on flow.



Specifics

Flows: 256
Range: the selected port pairs - 8,192

Ramp Up Time: 0
Set the duration for which acts on bandwidth can be increased. (Range: 0 - 300, unit: second)

Ramp Down Time: 0
Set the amount of time for which acts on bandwidth have to decrease. (Range: 0 - 300, unit: second)

Frame Size: 64
If Frame Size > MTU + 18 + VLAN/QinQ header length, IP fragmentation will be triggered conditionally. (Range: 64 - 9,026)

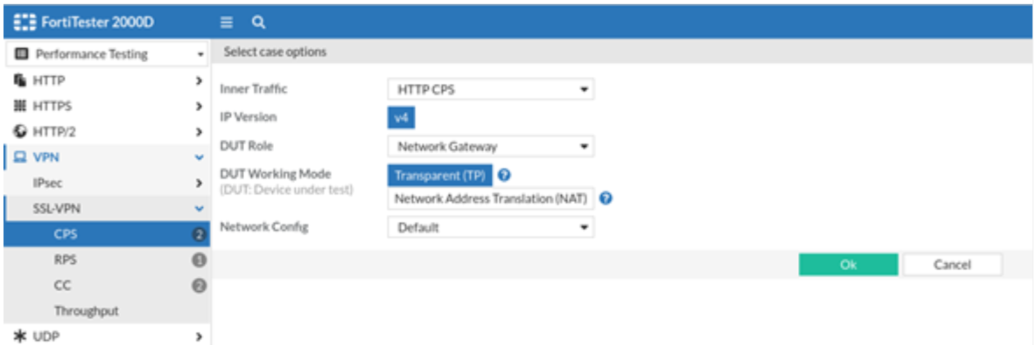
Bidirectional Traffic Flow
Disable bidirectional traffic flow

SSL-VPN SNI function support

The SNI (Server Name Indication) function of SSLVPN case supports deploying an Intermediate equipment, such as FortiSASE, between FortiTester and FortiGate. The FortiTester sendsan SSL VPN tunnel connection request containing SNI extension field to the intermediate device, which parses the extension and forwards message to the desired FortiGate.

To set up the SSL-VPN SNI function:

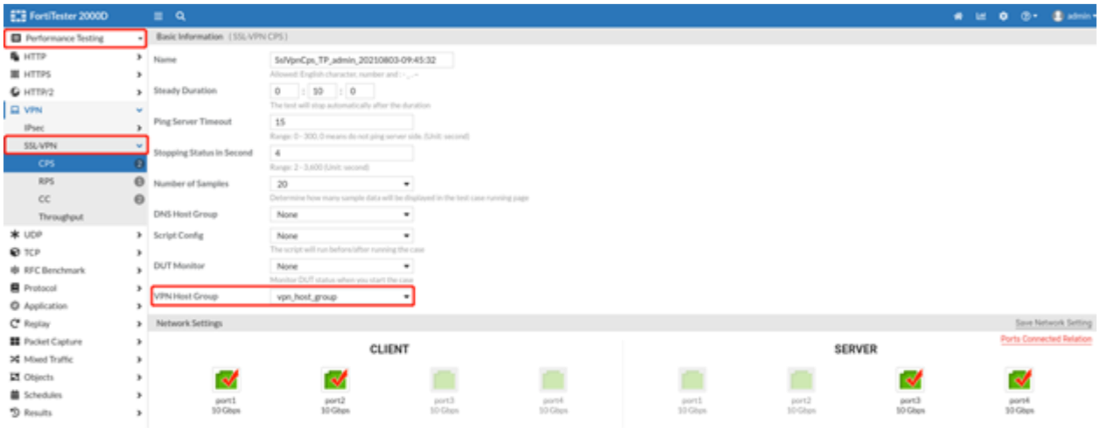
1. Go to **Cases > Performance Testing > Objects > Hosts** to display the Hosts Management page.
2. Click **+ Create New** to add maps between hostnames to IP addresses.
3. Go to **Cases > Performance Testing > Objects > Host > Host Groups** to display the Host Groups page.
4. Click **+ Create New** to add maps between ports and hosts.
5. Go to **Cases > Performance Testing > VPN > SSL-VPN > CPS(RPS/CC/Throughput)** to select case options and click on OK button.



Select case options

Inner Traffic: HTTP CPS
IP Version: v4
DUT Role: Network Gateway
DUT Working Mode (DUT: Device under test): Transparent (TP) | Network Address Translation (NAT)
Network Config: Default

6. Select the VPN Host Group and select the Host Group which is set in step 4.



Basic Information (SSL-VPN CPS)

Name: SslVpnCps_TP_admin_20210803-09:45:32
Allowed: English character, number and : - _ . ~

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

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

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

Number of Samples: 20
Determine how many sample data will be displayed in the test case running page

DNS Host Group: None

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

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

VPN Host Group: vpn_host_group

Network Settings

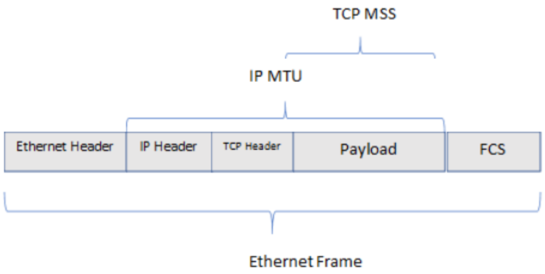
Tip on using Frame size with RFC2544 testing

While FortiTester complies with RFC2544 when sending out fixed frame size, in certain environment such as public cloud, sending 1500 MTU packet size will cause a problem as cloud networking devices might have MTU less than 1500 (e.g. 1480 bytes), and making transmission impossible. Hence users can use “User Defined” packet size such as 1498 (this includes 18 bytes frame header + CRC) to allow maximum packet size (1498-18 = 1480) to be tested in cloud environment.

Example

Cloud MTU = 1480 = IP MTU (set by cloud devices)

FortiTester sends out 1498 frame size = Ethernet frame size (minus 18bytes = 1480, the maximum packet size sent)



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 v7.0.0 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 v7.0 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 7.0.0, it's best to come from version 4.x. Users with versions before 4.x should first upgrade to 4.x, before upgrading to 7.0.0

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 inquires about a particular bug, please contact Fortinet Customer Service & Support at https://support.fortinet.com.

Bug ID	Description
0736157	RFC2544 test has lower limits in 4.2 compared with 3.9.
0738275	Certificates with dots or periods in their filename do not display in the GUI.

Known issues

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

Bug ID	Description
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.
697147	FortiTester SSL/VPN test does not reflect the FortiClient connections.
708571	No Vlan tag field in the network setting for the SSL/VPN test.
705388	Test import fails if the test exists in another work mode or fanout mode.

Change Log

Date	Change Description
August 9, 2021	FortiTester 7.0.0 initial release.