FortiTester Release Notes

VERSION 4.2.0

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

April 13, 2021
FortiTester 4.2.0 Release Notes

Change Log

Date	Change Description
April 13, 2021	FortiTester 4.2.0 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 4 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 4.2.0, Build 0035.

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

What’s new

FortiTester 4.2.0 offers the following new features and enhancements:

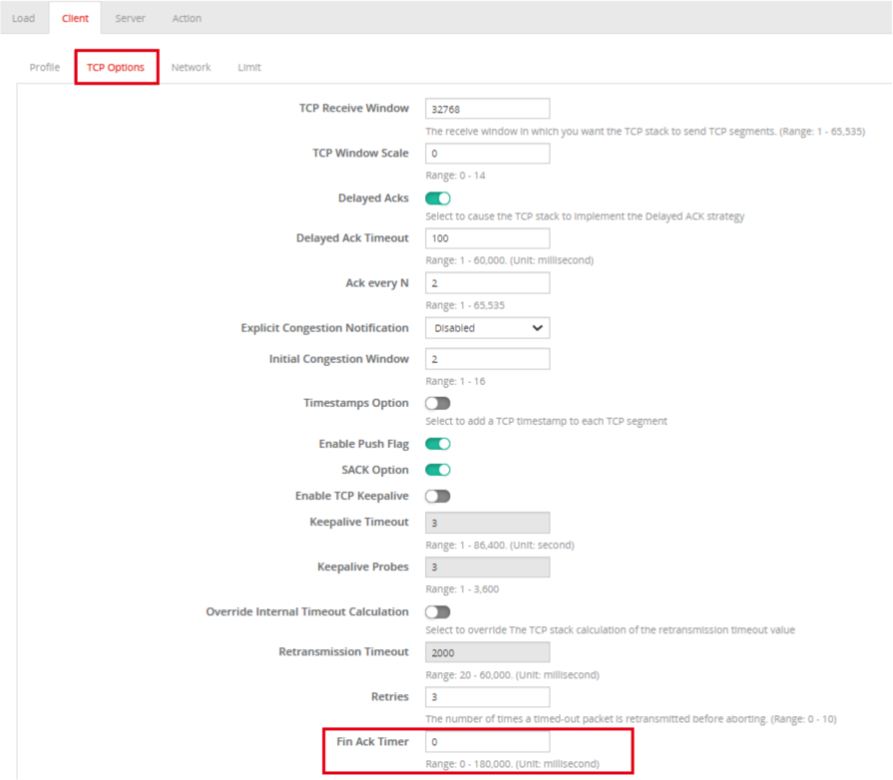
Added FinACK Timer

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.

Setting this timer can adversely affect TCP performance.

Configuration steps

Go to **Specifics > Client/Server > TCP Options > FinACK Timer.**



TCP Receive Window: 32768
The receive window in which you want the TCP stack to send TCP segments. (Range: 1 - 65,535)

TCP Window Scale: 0
Range: 0 - 14

Delayed Acks: ☑
Select to cause the TCP stack to implement the Delayed ACK strategy

Delayed Ack Timeout: 100
Range: 1 - 60,000. (Unit: millisecond)

Ack every N: 2
Range: 1 - 65,535

Explicit Congestion Notification: Disabled

Initial Congestion Window: 2
Range: 1 - 16

Timestamps Option: ☐
Select to add a TCP timestamp to each TCP segment

Enable Push Flag: ☑

SACK Option: ☑

Enable TCP Keepalive: ☐

Keepalive Timeout: 3
Range: 1 - 86,400. (Unit: second)

Keepalive Probes: 3
Range: 1 - 3,600

Override Internal Timeout Calculation: ☐
Select to override The TCP stack calculation of the retransmission timeout value

Retransmission Timeout: 2000
Range: 20 - 60,000. (Unit: millisecond)

Retries: 3
The number of times a timed-out packet is retransmitted before aborting. (Range: 0 - 10)

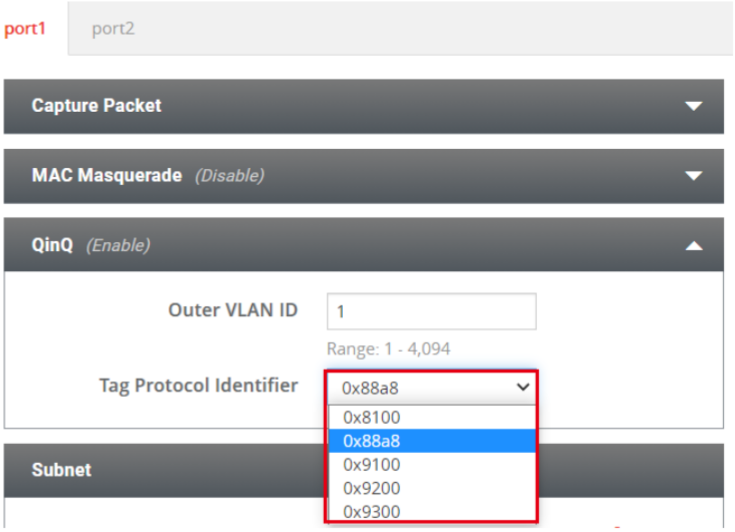
Fin Ack Timer: 0
Range: 0 - 180,000. (Unit: millisecond)

Added an option to select EtherType for QinQ packets

QinQ support 5 EtherTypes : 0x88a8, 0x8100, 0x9100, 0x9200, 0x9300.

Configuration steps

Go to **Network Setting > port > QinQ.**



Outer VLAN ID: 1

Range: 1 - 4,094

Tag Protocol Identifier: 0x88a8

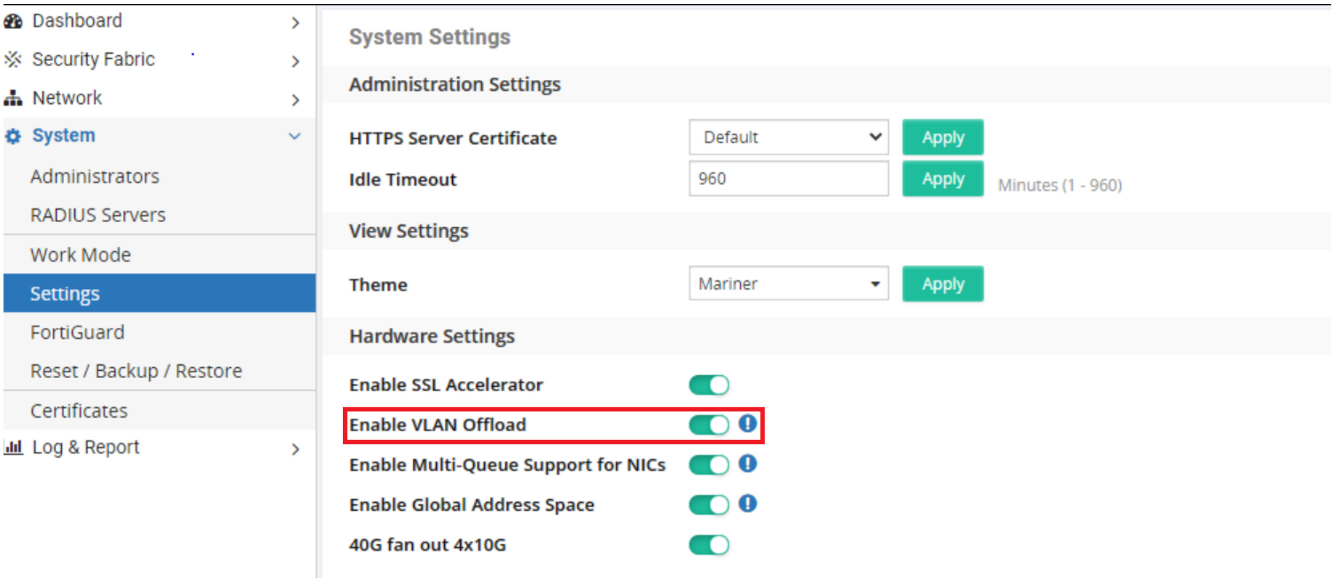
Added a VlanOffload Switch

When VlanOffload is enabled, the double-tagged VLAN packet's S-Tag will get stripped at the receiver end.

Configuration steps

Go to **System > Settings > VlanOffload.**

The function is only in hardware platform.



System Settings

Administration Settings

HTTPS Server Certificate: Default

Idle Timeout: 960 Minutes (1 - 960)

View Settings

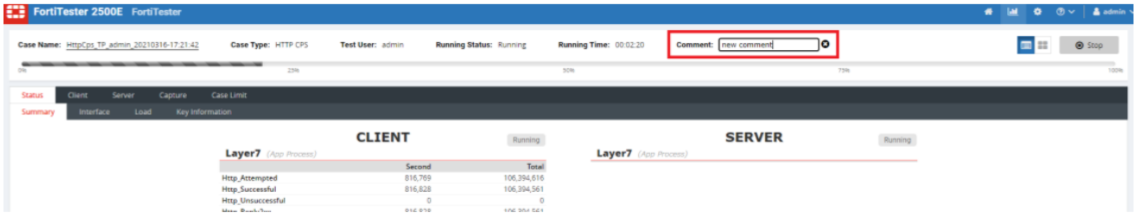
Theme: Mariner

Hardware Settings

Enable SSL Accelerator
Enable VLAN Offload
Enable Multi-Queue Support for NICs
Enable Global Address Space
40G fan out 4x10G

Added comment configuration in the running page

Supports a function to add/edit the comment when a test is running. It can be used for searching the test result in the Results page.



Case Name: HttpCps_TP_admin_20210316-17:21:42 Case Type: HTTP CPS Test User: admin Running Status: Running Running Time: 00:02:20 Comment: new comment

CLIENT

Layer7 (App Process)

	Second	Total
Http_Attempted	816,769	106,394,616
Http_Successful	816,828	106,394,561
Http_Unsuccessful	0	0

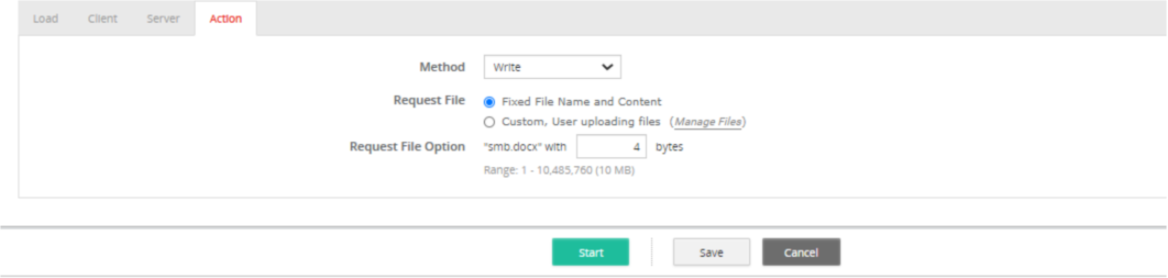
SERVER

Layer7 (App Process)

Added Samba upload feature

The "Write" method is added in the action tab of "CIFS/SMB" test case, so the user can trigger SMB upload traffic via this method.

To configure, go to **Performance Testing > Protocol > TCP > CIFS/SMB.**



Method: Write

Request File: ● Fixed File Name and Content
○ Custom, User uploading files (*Manage Files*)

Request File Option: "smb.docx" with 4 bytes

Range: 1 - 10,485,760 (10 MB)

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)

Upgrade 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**).
- 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 Slaves 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**.

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
705325	FortiTester sent a TCP packet with the wrong MAC address.
692793	In Testcenter mode you cannot exclude one FortiTester.
691810	FortiTester server side active RST issue.
690198	Includes secp384r1 in TLS1.2 VPN test.
688894	Unable to update IPS after upgrade.
681075	API endpoint for network config object returns multiple versions of object.
678827	Disabled DNS request for FTSVM0UNLICENSED
674595	Frame size in load setting; MTU size in network setting should not include VLAN 4Bytes header size.
654226	Need an option to select EtherType for QinQ packets.
654225	Double Tagged VLAN packet's S-Tag shouldn't get stripped at receiver end.

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	Suggest 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: the 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
April 13, 2021	FortiTester 4.2.0 initial release.