FortiTester Release Notes

VERSION 7.2.0

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

August 23, 2022
FortiTester 7.2.0 Release Notes

Change Log

Date	Change Description
August 23, 2022	FortiTester 7.2.0 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 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 7.2.0, Build 0328.

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

What's new

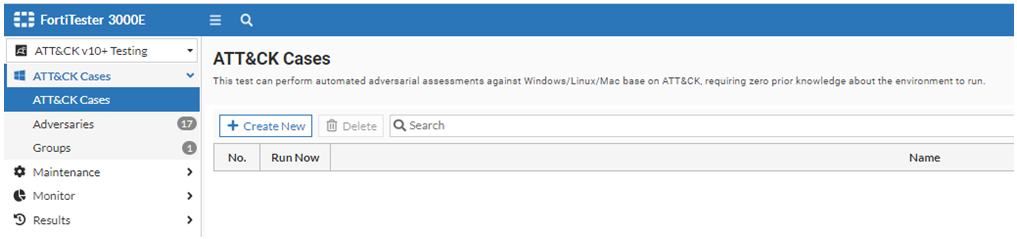
FortiTester 7.2.0 offers the following new features and enhancements:

Support ATT&CK V10 Breach Simulation

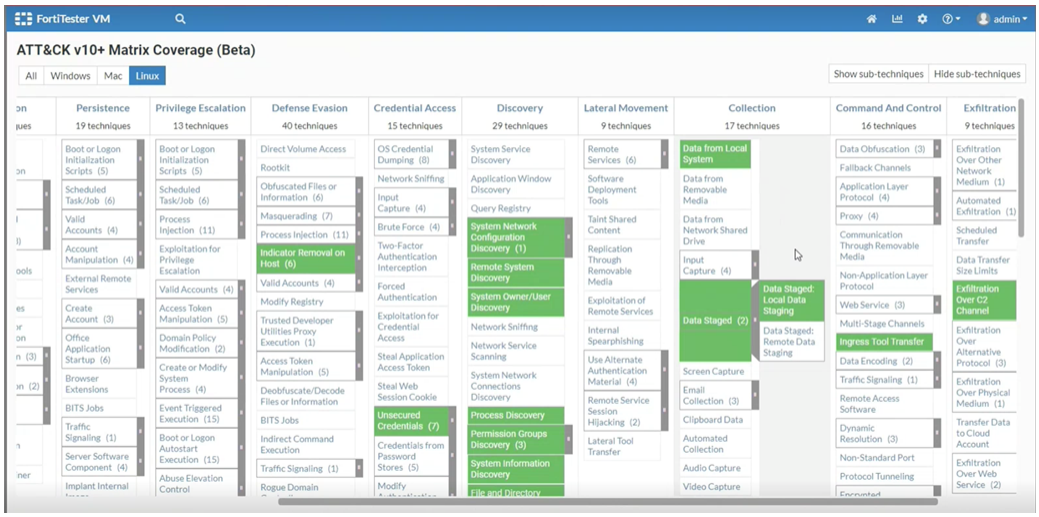
FortiTester v7.2 comes with a new MITRE ATT&CK framework supporting MITRE matrix v10 and sub-techniques, released as beta and running concurrently with the previous v6 matrix. Users are encouraged to try and migrate to this version. **Note**: The two versions (v6 and v10) are not compatible. Here's an overview of differences between different versions:

	FortiTester v3.9/4.x/7.0/7.1	FortiTester v7.2	Comments
MITRE ATT&CK matrix version	V6	V10	
Sub-techniques support	No	Yes	
End point agents support	Windows only	Windows / MAC / Linux	
Number of techniques (Abilities)	26 default 300+ total	95 default 200+ total	More updates will be made available for v10 via FortiGuard
Default Campaigns (Adversaries)	4 (Credential Dumping, Execution_ Through_API, PowerShell, Scheduled_Task)	8 (Check Systems Environment, Create Exfiltrate Directory, User and Domain information Extraction, Process Enumeration, Signed Binary Proxy Execution, Find and Exfiltrate files, Install Powershell, Bypass UAC User Access control on Windows)	
Exfiltrate files	Separate server on network	FortiTester	

New ATT&CK v10 menu



MITRE v10 with sub-techniques support:



Separation of Test Case ports and physical ports

This new feature allows configuration export/import between different models.

Previous v7.2 Fortitester configuration could only be exported/imported between the same model. In v7.2 this limitation is removed, made possible with the use of Test Case ports mapping to physical ports in tests. With this change, FortiTester introduces new objects, such as port mapping and port settings.

Allocation of extra vCPUs for VMs

FortiTester v7.2 allows for the allocation of two extra vCPUs more than total licensed vCPU for system management. For example, a VM04 can use 4 vCPU for traffic generation and an extra 2 vCPU's for system management.

Support of Virtual Router in SSLVPN testing

SSLVPN case include CPS, RPS, CC and Throughput now supports Virtual Router. VR is useful in public cloud testing where IP assignment is limited (e.g. AWS public cloud). Now, many SSLVPN client IP's can be simulated using VR.

Improved Report generation time

Report generation for longer tests cases (e.g. couple of hours up to days) received improvements in report generation time.

New DNS Zone Transfer support

Added DNS-AXFR case. This simulates attacker use of AXFR zone transfer as an attack vector for DDoS attacks. This new feature establishes a TCP connection (three-way handshake), simulates a DNS zone transfer (AXFR), and closes the TCP connection.

Single Packet control for DDoS testing

In previous version DDoS tests uses system default 'mix' of attacks (such as SYN_flood, FIN_Flood etc). Some parameters were set and not configurable by the user. In v7.2 a new single packet case option allows an advanced configuration item to refer Single Packet Group object. This feature is used to simulate a DDoS attack, specially related to the MIRAI attacks simulation.

Supports IBM Public cloud platform

New platform IBM released for FortiTester.

New ICMP test

Added ICMP Case. This allows FortiTester to generate ICMP traffic with different settings such as packet size etc, to test DUT's capability to parse/route ICMP traffic, offering a 'flood' option to send simultaneous pings within configured time interval (up to 600ms).

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, IBM, and ALI)

System integration and support

FortiTester v7.2.0 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 inquires about a particular bug, please contact Fortinet Customer Service & Support at https://support.fortinet.com.

Bug ID	Description
775972	IGMP Test is generating an invalid IPv4 Header Checksum
780285	Cannot fanout FTS3KE
512700	B0095: Only one IP address in server subnet IP address range is used during explicit proxy test
761629	Ramp up spike
823322	Multiple Unauthenticated command injection
822808	Unauthenticated command injection
803658	Upgrade of Glibc libraries
824612	Authenticated command injection in certificate import feature
824616	Missing account lockout - telnet
827744	Multiple command injection vulnerabilities in GUI and API
796092	command injection in "execute ping" CLI command
822806	Unauthenticated command injection
796091	command injection in "execute restore/backup" CLI commands
830511	Removed remote admin access for troubleshooting
669462	Resolved Glibc vulnerability after upgrade
747235	Pillow--- Precaution upgrade
750520	TCPReply precaution update
755943	StrongSwan ---Precaution Upgrade
756761	DropBear precaution upgrade
761946	Busybox - precautions upgrade
792118	Upgraded openSSL library
797244	Upgraded zilb library
799415	Upgraded pillow library
799811	Upgraded curl library
800743	Upgraded tcpdump library

Bug ID	Description
805710	Updated kernel
806011	Resolved ncurses security issue
811434	Upgraded libpng library
811673	Upgraded openSSH
816373	Upgraded numpy
824615	Missing account lockout - SSH

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
815376	The performance of some cases is lower than in version 7.1.0
758945	Cannot run/create case if TC_Client connects to TC_Sever by Public IP
751949	EMIX throughput using Fortinet EMIX Traffic template gives lower results compared to Ixia /BP EMIX Traffic profile.
738156	FortiTester agent is not digitally signed and will be detected by FortiEDR as a suspicious file
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
August 23, 2022	FortiTester 7.2.0 initial release.

Copyright© 2022 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.