FortiOS - Release Notes

Version 6.2.8

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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

April 26, 2021
FortiOS 6.2.8 Release Notes
01-628-687669-20210426

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-04-26	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 6.2.8 build 1232.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.2.8 supports the following models.

FortiGate	FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30E-MG, FG-40F, FG-40F-3G4G, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-81E, FG-81E-POE, FG-81F, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-40F, FWF-40F-3G4G, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60F, FGR-60F-3G4G, FGR-90D
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special branch supported models

The following models are released on a special branch of FortiOS 6.2.8. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 1232.

FG-200F	is released on build 7088.
FG-201F	is released on build 7088.

Special notices

New Fortinet cloud services

FortiOS 6.2.0 introduced several new cloud-based services listed below. The new services require updates to FortiCare and Fortinet's FortiCloud single sign-on (SSO) service.

- Overlay Controller VPN
- FortiGuard Cloud-Assist SD-WAN Interface Bandwidth Monitoring
- FortiManager Cloud
- FortiAnalyzer Cloud

FortiGuard Security Rating Service

Not all FortiGate models can support running the FortiGuard Security Rating Service as a Fabric "root" device. The following FortiGate platforms can run the FortiGuard Security Rating Service when added to an existing Fortinet Security Fabric managed by a supported FortiGate model:

- FGR-30D
- FGR-35D
- FGT-30E
- FGT-30E-MI
- FGT-30E-MN
- FGT-50E
- FGT-51E
- FGT-52E

- FWF-30E
- FWF-30E-MI
- FWF-30E-MN
- FWF-50E
- FWF-50E-2R
- FWF-51E

Using FortiManager as a FortiGuard server

If you use FortiManager as a FortiGuard server, and you configure the FortiGate to use a secure connection to FortiManager, you must use HTTPS with port 8888. HTTPS with port 53 is not supported.

FortiGate hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D does not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
  set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

NP4lite platforms

FortiOS 6.2 and later does not support NP4lite platforms.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

L2TP over IPsec on certain mobile devices

Bug ID	Description
459996	Samsung Galaxy Tab A 8 and Android 9.0 crash after L2TP over IPsec is connected.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`:
  - in FortiOS 6.2.6 and later, set `unsupported-ssl` to `block`.
  - in FortiOS 6.4.3 and later, set `unsupported-ssl-negotiation` to `block`.

FortiGate 80D boot failure

The FortiGate 80D may fail to boot when the bootloader attempts to load the increased kernel size into the memory.

New features or enhancements

Bug ID	Description
634006	OpenSSL updated to 1.1.1j for security fixes.

638352	To avoid large number of new IKEv2 negotiations from starving other SAs from progressing to established states, the following enhancements have been made to the IKE daemon:
	• Prioritize established SAs.
	• Offload groups 20 and 21 to CP9.
	• Optimize the default embryonic limits for mid- and high-end platforms.
	The IKE embryonic limit can now be configured in the CLI:
	`config system global`
	`  set ike-embryonic-limit <integer>`
	`end`

644218	The host protection engine (HPE) has been enhanced to add monitoring and logging capabilities when the HPE is triggered. Users can enable or disable HPE monitoring, and configure intervals and multipliers for the frequency when event logs and attack logs are generated. These logs and monitors help administrators analyze the frequency of attack types and fine-tune the desired packet rates in the HPE shaper.
	`config monitoring npu-hpe`
	`  set status {enable | disable}`
	`  set interval <integer>`
	`  set multipliers <m1>, <m2>, ... <m12>`
	`end`
	The interval is set in seconds (1 - 60, default = 1). The multiplies are twelve integers ranging from 1 - 255, the default is `4, 4, 4, 4, 8, 8, 8, 8, 8, 8, 8, 8`.
	An event log is generated after every (interval × multiplier) seconds for any HPE type when drops occur for that HPE type. An attack log is generated after every (4 × multiplier) number of continuous event logs.

660596	Because pre-standard POE devices are uncommon in the field, `poe-pre-standard-detection` is set to `disable` by default. Upgrading from previous builds will carry forward the configured value.

660624	When enabling the Security Fabric on the root FortiGate, the following FortiAnalyzer GUI behavior has changed:
	• If a FortiAnalyzer appliance is enabled, then the dialog will be for the *FortiAnalyzer* connector.
	• If a FortiAnalyzer appliance is disabled but *FortiAnalyzer Cloud* is enabled, then the dialog will be for the *Cloud Logging* connector.
	• If neither the FortiAnalyzer appliance or FortiAnalyzer Cloud are enabled:
	  • If the device has a FAZC (standard FortiAnalyzer Cloud subscription) or AFAC (premium subscription) entitlement, then the dialog will be for the *Cloud Logging* connector.
	  • If the device does not have a FAZC or AFAC entitlement, then the dialog will be for the *FortiAnalyzer* connector.

Bug ID	Description
	• When *FortiAnalyzer Cloud* is enabled and the FortiAnalyzer appliance is disabled, then the *Cloud Logging* connector will not let you switch to the *FortiGate Cloud* FortiAnalyzer.
670345	Support Strict-Transport-Security in HTTPS redirect.
673371	Support ICMP type 13 at local interface.
680599	Increase the ICMP rate limit to allow more ICMP error message to be sent by the FortiGate per second. The ICMP rate limit has changed from 1 second (100 jiffies) to 10 milliseconds (1 jiffy).

684133	Support site-to-site IPsec VPN in an asymmetric routing scenario with a loopback interface as a VPN bound interface.
	`config vpn ipsec phase1-interface`
	`edit <name>`
	`set interface "loopback"`
	`set loopback-asymroute {enable | disable}`
	`next`
	`end`

Changes in default behavior

Bug ID	Description
669018	Update link for Fortinet URL rating submission on web filter block/warning pages to point to https://globalurl.fortinet.net.
673609	The auto-join FortiCloud re-try timer has changed from 600 seconds to 60 seconds.

Upgrade Information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.2.8 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.2.5
- FortiClient EMS 6.2.3 and later
- FortiClient 6.2.3 and later
- FortiAP 5.4.4 and later
- FortiSwitch 3.6.11 and later

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. FortiGate devices
4. Managed FortiSwitch devices
5. Managed FortiAP devices
6. FortiClient EMS
7. FortiClient
8. FortiSandbox
9. FortiMail
10. FortiWeb
11. FortiADC
12. FortiDDOS
13. FortiWLC

If the Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.2.8. When the Security Fabric is enabled in FortiOS 6.2.8, all FortiGate devices must be running FortiOS 6.2.8.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.2.8 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.2.8 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.2.8 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.2.8 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.2.8, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.2.8.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

FortiView widgets have been rewritten in 6.2.8. FortiView widgets created in previous versions are deleted in the upgrade.

Product integration and support

The following table lists FortiOS 6.2.8 product integration and support information:

Web Browsers	• Microsoft Edge 44 • Mozilla Firefox version 76 • Google Chrome version 81 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 44 • Mozilla Firefox version 76 • Google Chrome version 81 • Microsoft Internet Explorer version 11 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 14. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 14. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.2.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 14 and Fortinet Security Fabric upgrade on page 14. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 5.6.0 and later are supported.
FortiClient iOS	• 6.2.0 and later
FortiClient Android and FortiClient VPN Android	• 6.2.0 and later
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0295 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2019 Standard
	  • Windows Server 2019 Datacenter
	  • Windows Server 2019 Core
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2016 Core
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Windows Server 2012 Core
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2008 Core
	  • Novell eDirectory 8.8

FortiExtender	• 4.1.2
AV Engine	• 6.00161
IPS Engine	• 5.00239
Virtualization Environments	
Citrix	• Hypervisor Express 8.1, build 2019-12-04
Linux KVM	• Ubuntu 18.04.3 LTS • QEMU emulator version 4.4.4 (Debian 1:4.0+dfsg-0ubuntu9.4) • libvirtd (libvirt) 4.0.0
Microsoft	• Hyper-V Server 2019
Open Source	• XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, and 6.7
VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel X520

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04 / 18.04 (32-bit & 64-bit)	2336. Download from the Fortinet Developer Network: https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 76 Google Chrome version 81
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 76 Google Chrome version 81
Linux CentOS 7/8	Mozilla Firefox version 68
OS X Catalina 10.15	Apple Safari version 13 Mozilla Firefox version 76 Google Chrome version 81
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

The following table lists the antivirus and firewall client software packages that are supported.

Supported Microsoft Windows XP antivirus and firewall software

Product	Antivirus	Firewall
Symantec Endpoint Protection 11	✓	✓
Kaspersky Antivirus 2009	✓	
McAfee Security Center 8.1	✓	✓
Trend Micro Internet Security Pro	✓	✓
F-Secure Internet Security 2009	✓	✓

Supported Microsoft Windows 7 32-bit antivirus and firewall software

Product	Antivirus	Firewall
CA Internet Security Suite Plus Software	✓	✓
AVG Internet Security 2011		
F-Secure Internet Security 2011	✓	✓
Kaspersky Internet Security 2011	✓	✓
McAfee Internet Security 2011	✓	✓
Norton 360™ Version 4.0	✓	✓
Norton™ Internet Security 2011	✓	✓
Panda Internet Security 2011	✓	✓
Sophos Security Suite	✓	✓
Trend Micro Titanium Internet Security	✓	✓
ZoneAlarm Security Suite	✓	✓
Symantec Endpoint Protection Small Business Edition 12.0	✓	✓

Resolved issues

The following issues have been fixed in version 6.2.8. For inquires about a particular bug, please contact Customer Service & Support.

DNS Filter

Bug ID	Description
511729	Domain filter entries whose action is set to allow should not be logged.

Explicit Proxy

Bug ID	Description
624513	IP pool address in proxy policy is not used sometimes when enabling a security profile.
662931	Browsers change default `SameSite` cookie settings to `Lax`, and Kerberos authentication does not work in transparent proxy.
664548	When the FortiGate is configured as an explicit proxy and AV is enabled on the proxy policy, users cannot access certain FTP sites.
681054	Web proxy users are disconnected due to external resource update flushing the user even if they do not have an authentication rule using the related proxy address or IP list.
689002	Proxy traffic failed after modifying resource setting in external connector.
697566	Explicit proxy unable to access a particular URL (https://***.my.salesforce.com) after upgrading from 5.6.12 to 6.2.7.

Firewall

Bug ID	Description
474612	SNAT is using low ports below 1023 for NTP.
611781	Search option on IPv4 policy page not working; after typing in the search bar, no results are displayed.
616220	ICMP reply packets are dropped by the FortiGate.

Bug ID	Description
643446	Fragmented UDP traffic is silently dropped when fragments have different ECN values.
661014	FortiCarrier has GTP dropped packet log after configuring GTP allow list.
675353	Security policy (NGFW mode) flow-based UTM logs are still generated when policy traffic log is disabled.
682956	ISDB is empty/crashes after upgrading from 6.2.4/6.2.5 to 6.2.6.
683426	No hit counts on policy for DHCP broadcast packets in transparent mode.
683604	When changing a policy and creating a firewall sniffer concurrently, there is traffic that is unrelated to the policy that is being changed and matching the implicit deny policy. Some IPv4 firewall policies were missing after the change.
699785	Firewall performance may degrade when thousands of VIPs are configured.

FortiView

Bug ID	Description
628225	*Compromised Hosts* dashboard cannot show data if FortiAnalyzer is configured using the FQDN address in the log setting. FortiAnalyzer configured with an IP address does not have this issue.

GUI

Bug ID	Description
592854	An address created by the VPN wizard cannot save changes due to an incorrect validation check for parentheses, *()*, in the *Comments* field.
593860	When central management is enabled, users can bypass GUI read-only restrictions and apply policy changes.
601879	When logging in to the dashboard after a factory reset, the dashboard displays *The web page cannot be found*.
631041	Adding an RSSO group to the firewall policy does not enable RSSO on the policy.
639617	On *Explicit Web Proxy Policy* page, unable to change *Outgoing Source IP* option from *IP Pools* to *Proxy Default* or *Original Source IP*. CLI does not have this issue.
650708	When the client browser is in a different time zone from the FortiGate, the *Guest Management* page displays an incorrect expiry time for guest users. The CLI returns the correct expiry.
654626	Unable to change the action setting of *Freeware and Software Downloads* using the *FortiGuard Category Based Filter* of the DNS filter profile.

Bug ID	Description
655255	FortiGuard resource retrieval delay causes GUI pages to respond slowly. Affected pages include: *Firewall Policy*, *Settings* (log and system), *Explicit Proxy* (web and FTP), *System Global*, and *System CSF*.
656599	Automation CLI script should support setting an administrator profile to restrict access.
656668	On the *System* > *HA page*, GUI tooltip for the reserved management interface incorrectly shows the connecting IP address instead of the configured IP address.
661703	High latency accessing *Security Fabric* > *Physical Topology/Logical Topology* pages in Firefox.
662640	Some GUI pages (dashboard, topology, policy list, interface list) are slow to load on low-end platforms when there are many concurrent HTTPSD requests.
665597	User credentials test from web UI and CLI are inconsistent.
666500	The *Confirm version downgrade* warning message is not displayed when a user downgrades firmware between minor patch release versions using the manual upload option. Firmware downgrades from FortiGuard do not have this issue.
667863	GUI does not display FortiSwitch ports when multiple FortiLink interfaces are configured. FortiOS 6.4.0 and later supports multiple FortiLink configurations via the GUI.
672906	GUI does not redirect to the system reboot progress page after successfully restoring a configuration.
689605	On some browser versions, the GUI displays a blank dialog when creating custom application or IPS signatures. Affected browsers: Firefox 85.0, Microsoft Edge 88.0, and Chrome 88.0.
691277	When logs are retrieved from FortiAnalyzer, the GUI displays the same traffic logs for primary and secondary HA devices.

HA

Bug ID	Description
540600	The HA `hello-holddown` value is divided by 10 in the hatalk daemon, which makes the `hello-holddown` time 10 times less than the configuration.
609631	Both nodes in HA simultaneous reboot when `gtp-enhance-mode` is enabled or disabled.
627851	After the HA peer node has been replaced, there needs to be a way to reset the HA health status back to OK.
650624	HA GARP sending was delayed due to lots of transceiver reading.
652507	Sessions with `syn_ses` flags are not synced after reboot.
653095	Inband management IP connection breaks when failover occurs (only in virtual cluster setup).
657376	VLAN interfaces are created on a different virtual cluster primary instead of the root primary do not sync.

Bug ID	Description
678309	Cluster is out of sync because of `config vpn certificate ca` after upgrade.
690248	Malicious certificate database is not getting updated on the secondary unit.
693223	hasync crashes with signal 11 in `ha_same_fosver_with_manage_master`.

Intrusion Prevention

Bug ID	Description
657541	On FG-80D, the IPS engine daemon count drops to 0 when the CPU number is 4.
668631	IPS is constantly crashing, and ipshelper has high CPU when IPS extended database has too many rules (more than 256) sharing the same pattern. Affected models: SoC3-based FortiGates.
686301	ipshelper CPU spikes when configuration changes are made.
689259	Flow-based AV scanning does not send specific extension files to FortiSandbox.
689590	IP quarantine is not working on FG-80D.
691395	Signature false positives causing outage after IPS database update.

IPsec VPN

Bug ID	Description
566076	IKED process signal 11 crash in an ADVPN and BGP scenario.
597246	When disabling and re-enabling OCVPN after HA failover, the IPsec tunnel cannot be established.
631804	OCVPN errors showing in logs when OCVPN is disabled.
638352	In extreme situations when thousands of tunnels are negotiating simultaneously (IKEv2), iked process gets exhausted and stuck.
642543	IPsec did not rekey when keylife expired after back-to-back HA failover.
650599	IKE HA sync truncates phase 2 options flags after the first eight bits.
655895	Unable to route traffic to a spoke VPN site from the hub FortiGate when the dialup IPsec VPN interface is dual stacked (IPv4/IPv6).
666693	If NAT-T IP changes, the dynamic IPsec spoke add route entry is stuck on the hub.
678800	Kernel may crash on link event update with `net-device` enabled.
684133	Site-to-site IPsec VPN cannot establish in asymmetric routing scenario where the IPsec VPN bound interface is a loopback interface.

Bug ID	Description
687749	iked HA sync crashed on secondary with authenticated user group in firewall policy.
691878	Creating or updating a user with two-factor authentication causes dialup VPN traffic to stop.
694992	Issue establishing IPsec and L2TP tunnel with Chromebook behind NAT.
710961	Hub is dropping packets due to `Failed to find IPsec Common` after upgrading from 6.2.6 to 6.2.7.

Log & Report

Bug ID	Description
623471	FortiGate did not change the time after daylight saving time.
654363	Traffic log shows *Policy violation* for traffic hitting the allow policy in NGFW policy mode.
667274	FortiGate does not have log disk auto scan failure status log.
675347	When searching for some rarely-found logs within a large volume of logs, there is a long period of time before the results are returned. During the waiting period, if any new requests arrive, the old search session cannot be cleared. There is then a risk that multiple processes exist together, which may cause performance issues.
677540	First TCP connection to syslog server is not stable.
682444	No event log generated when log disk needs format.
694296	Memory leak issue in miglogd when log daemon has connection issue or FortiAnalyzer setting changes.
710344	Reliable syslog is sent in the wrong format when flushing the logs queued in the log daemon when working in TCP reliable mode.

Proxy

Bug ID	Description
603195	Multiple WAD crashes with signal 11.
633108	When FOH server is disconnected from a HTTP session, the HTTP session client port peer is not cleared. After this, the HTTP client port shutdown causes a crash because the peer port is freed.
655356, 660857	Proxy deep inspection fails if server uses TLS 1.3 cookies or record padding.

Bug ID	Description
661063	If a client sends an RST to a WAD proxy, the proxy can close the connection to the server. In this case, the relatively long session expiration (which is usually 120 seconds by default) could lead to session number spikes in some tests.
675525	No WAD sessions displayed when running `diagnose wad filter`.
680651	Memory leak when retrieving the thumbnailPhoto information from the LDAP server.
681134	Proxy-based SSL certification inspection session hangs if the outbound probe connection has no routes.
693951	Cannot access Java-based application in proxy mode.

Routing

Bug ID	Description
579884	VRF configuration in WWAN interface has no effect after reboot.
628896	DHCP relay does not match the SD-WAN policy route.
687034	bgpd memory leak if running BGP on 6.2.7 and 6.4.4.
692241	BGP daemon consumes high CPU in ADVPN setup when disconnecting after socket writing error.

Security Fabric

Bug ID	Description
649556	FortiNAC requests to FortiGate can timeout on low-end models when there are many concurrent requests.
660624	FortiAnalyzer Cloud should be taken into consideration when doing CLI check for CSF setting.

SSL VPN

Bug ID	Description
602480	Use jQuery to customize FortiGate SSL VPN log in page.
608195	AngularJS web application cannot load via SSL VPN web mode.
610905	SSL VPN bypassing logon count limit with different case in user name.

Bug ID	Description
610995	SSL VPN web mode gets error when accessing internal website at https://st***.st***.ca/.
619296	FortiGate reverts default values of text on buttons in SSL VPN log on page.
620946	All sslvpnd daemons use 99.9% CPU when policy is being updated.
628597	Unable to load the SSL VPN bookmark internal website, https://fi***.co.nz.
646339	SSL-SSH inspection profile changes to `no-inspection` after device reboots.
649197	Unable to use editor in Atlassian internal Confluence portal over SSL VPN web mode.
659322	SSL VPN will disconnect all connections after new address is added to IP pool.
661290	https://mo***.be site is non-accessible in SSL VPN web mode.
662042	The https://outlook.office365.com and https://login.microsoft.com websites cannot be accessed in the SSL VPN web portal.
662871	SSL VPN web mode has problems accessing some pages on FortiAnalyzer 6.2.
670731	Internal application server/website bookmark (https://***.***.***.***:****/nexgen/) not working in SSL VPN web mode.
672743	sslvpnd segmentation fault crash due to old DNS entries in cache that cannot be released if the same results were added into the cache but in a different order.
673320	Pop-up window does not load correctly when accessing internal application at https://re***.wo***.nl using SSL VPN web mode.
677167	SSL VPN web mode has problem accessing Sapepronto server.
678132	SSL VPN web portal SSO credentials for alternative option are not working.
680711	Unable to access OWA web server on mobile device in SSL VPN web mode.
681764	Video could not load for https://le***.sm***.ca in SSL VPN web mode.
683601	Changing DNS or WINS server under VPN SSL settings logs off connected users.
685269	SSL VPN web mode is not working properly for aw***.co***.com website.
688023	SSL VPN bookmarked website shows empty page after logging in to SSL VPN gateway https://vd***.vi***.com.
696009	Tunnel IP pool leak when DTLS tunnel user session is deleted due to timeout (idle or authentication).
706270	sslvpnd `signal 11 (Segmentation fault) received` caused by a pointer arithmetic error.

Switch Controller

Bug ID	Description
700842	FortiSwitch MAC delete logs are not being generated.

System

Bug ID	Description
488400	FGFM sessions timeout when the sessions between two non-VLAN ID EMAC VLANs are offloaded.
521213	Read-only administrators should be able to run `diagnose sniffer packet` command.
564477	VLAN switch creation fails every other time on FG-140D-POE.
584622	SNMP trap cannot display FortiGate model in OSPF trap information.
598527	ISDB may cause crashes after downgrading FortiGate firmware.
618158	DHCP client cannot get IP address when NTP server option in DHCP server settings is set to *Same as System NTP*.
620902	Application fgfmsd crashed and signal 11 received `__cmdb_config_write_by_fname + 0x01cd`.
627629	DHCP client sent invalid DHCPREQUEST format during INIT state.
628642	Issue when packets from the same session are forwarded to each LACP member when NPx offloading is enabled.
642005	FortiGate does not send `service-account-id` to FortiManager via fgfm tunnel when FortiCloud is activated directly on the FortiGate.
643033	`get system interface transceiver port1` should return RX power and TX power for all Ch0[1-4] with a 0 value or N/A when the admin port is down on one side and the link status is down.
644616	NP6 does not update session timers for traffic IPsec tunnel if established over one pure EMAC VLAN interface.
650878	DHCP relay will honor the broadcast flag set to 0 (unicast) in only one VDOM at a time in a multi-VDOM environment.
654131	No statistics for TX and RX counters for VLAN interfaces.
659539	FortiGate running 6.2.7 GA cannot validate license via FortiManager due to FortiManager hardware missing Fortinet_CA2 and Fortinet_SUBCA2001.
664279	snmpd crashes when sorting a list-based ARP table if it has about 50,000 or more entries.
665332	When VDOM has large number of VIPs and policies, any firewall policy change causes cmdbsvr to become busy and use high CPU.
665550	Fragmented UDP traffic does not assemble on the FortiGate and does not forward out.
666418	SFP interfaces on FG-330xE do not show link light.
667722	VLAN interface created on top of a 10 GB interface is not showing the actual TX/RX counters.
668856	Offloaded traffic passing through two VDOMs connected with EMAC-VLANs is sometimes dropped.
668856	Offloaded traffic passing through two VDOMs connected with EMAC-VLANs is sometimes dropped.
669914	No statistics for TX and RX counters for VLAN interfaces.

Bug ID	Description
670897	Update GTP code to be compatible with newer versions (GTPv1 and GTPv2).
670962	Packet loss occurs when traffic flow between VLAN interfaces is created under 10G LACP link.
672011	LTE DHCP IP addressing not installed in the routing table.
672183	UDP 4500 inter-VDOM traffic is not offloaded, causing BFD/IPsec to drop.
673263	High memory issue is caused by heavy traffic on the VDOM link.
673609	The auto-join FortiCloud re-try timer 600 second value is too large.
673918	Read-only administrator with packet capture read-write permission cannot run `diagnose sniffer` command.
675171	L2TP enabled status should be configured before EIP and SIP.
677568	Failed to parse `execute restore config` properly when the command is from a FortiManager script.
678809	dhcpd crashes with signal 6 because the timer is not canceled before calling the free release function.
680881	Rebooting device causes interface mode to change from static to DHCP.
686442	Traffic was stopped because PBA IP pool has the wrong relationship information.
690797	Huawei E8372h-320 LTE modem does not receive IP on FG-30E.
693757	Secondary FG-5001D blades in SLBC cluster do not show updated contract dates.
698014	When running `execute speed-test` command, it shows all VLAN and SSL interfaces from other VDOMs.

User & Device

Bug ID	Description
643191	FSSO TS-Agent is not working properly when FortiGates use NGFW policy-based mode.
658794	FortiGate sent CSR certificate instead of signed certificate to FortiManager when retrieve is performed.
662391	Persistent sessions for de-authenticated FSSO users.
675226	The `ssl-ocsp-source-ip` setting not configurable in non-management VDOMs.
675539	FSSO collector status is down, despite that it is reported as connected by authd in a multi-VDOM environment.

VM

Bug ID	Description
627106	FG-VM64 console shows `hw csum failure` for VLAN interface on mlx5_core PF.
711525	FG-VM-AWS PAYG instance randomly loses license after reboot.

Web Filter

Bug ID	Description
593203	Cannot enter a name for the web rating override or save it due to name input error.
668325	Hanging FortiGuard connection is not torn down in some situations.
676403	Replacement message pictures (FortiGuard web filter) are not displayed in Chrome.
678467	Safe search URL option is not working while the original query in Google Images has the same parameter name.

WiFi Controller

Bug ID	Description
621346	Dynamic VLAN on SSID cannot pass traffic through FG-100F/101F and FG-60F/61F when offloading is enabled.
698961	FWF-60F/61F and FWF-40F encounters kernel panic (`LR is at capwap_find_sta_by_mac`) when one managed FortiAP is authenticating WiFi clients.
707635	AP with MAC E0-23-FF not coming online through mesh with FortiWiFi radio set to root.

Known issues

The following issues have been identified in version 6.2.8. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

DNS Filter

Bug ID	Description
582374	License shows expiry date of `0000-00-00`.

Explicit Proxy

Bug ID	Description
540091	Cannot access explicit FTP proxy via VIP.

Firewall

Bug ID	Description
654356	In NGFW policy mode, sessions are not re-validated when security policies are changed. **Workaround**: clear the session after policy change.

FortiView

Bug ID	Description
635309	When choosing to view *Compromised Hosts*, FortiGate returns an error 500 when FQDN is set in `config log fortianalyzer setting`.
673225	FortiView *Top Traffic Shaping* widget does not show data for outbound traffic if the source interface's role is WAN. Data is displayed if the source interface's role is LAN, DMZ, or undefined.

GUI

Bug ID	Description
354464	Antivirus archive logging enabled from the CLI will be disabled by editing the antivirus profile in the GUI, even if no changes are made.
514632	Inconsistent reference count when using ports in HA `session-sync-dev`.
529094	When creating an anti-spam block/allowlist entry, *Mark as Reject* should be grayed out.
535099	The SSID dialog page does not have support for the new MAC address filter.
541042	Log viewer forwarded traffic does not support multiple filters for one field.
584915	*OK* button missing from many pages when viewed in Chrome on an Android device.
584939	VPN event logs are incorrectly filtered when there are two *Action* filters and one of them contains "-".
602102	Warning message is not displayed when a user configures an interface with a static IP address that is already in use.
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.
621254	When creating or editing an IPv4 policy or address group, firewall address searching does not work if there is an empty wildcard address due to a configuration error.
664007	GUI incorrectly displays the warning, *Botnet package update unavailable, AntiVirus subscription not found.*, when the antivirus entitlement is expiring within 30 days. The actual botnet package update still works within the active entitlement duration.
672599	After performing a search on firewall *Addresses*, the matched count over total count displayed for each address type shows an incorrect total count number. The search functionality still works correctly.
682440	On *Firewall Policy* list, the tooltip for *IP Pool* incorrectly shows *Port Block Allocation* as being exhausted if there are expiring PBAs available to be reallocated.
688994	The *Edit Web Filter Profile* page incorrectly shows that a URL filter is configured (even though it is not) if the URL filter entry has the same name as the web filter profile in the CLI.

HA

Bug ID	Description
695067	When there are more than two members in a HA cluster and the HA interface is used for the heartbeat interface, some RX packet drops are observed on the HA interface. However, no apparent impact is observed on the cluster operation. **Workaround**: do not use the HA interface as a heartbeat interface.
700271	Non-hyperscale license system's secondary device responds to ARP queries. Affected platforms: all NP7 platforms (FG-180XF, FG-260XF, FG-420XF, FG-440XF) that were released on 6.2.6.

Intrusion Prevention

Bug ID	Description
565747	IPS engine 5.00027 has signal 11 crash.
590087	When IPS pcap is enabled, traffic is intermittently disrupted after disk I/O reaches IOPS limit.

IPsec VPN

Bug ID	Description
644780	Rectify the consequences if password renewal on FortiClient is canceled.

Log & Report

Bug ID	Description
606533	User observes `FGT internal error` while trying to log in or activate FortiGate Cloud from the web UI.
713014	Cannot perform disk scan after enabling disk raid.

Proxy

Bug ID	Description
604681	WAD process with SoC SSL acceleration enabled consumes more memory usage over time, which may lead to conserve mode. **Workaround**: disable SoC SSL acceleration under the firewall SSL settings.

REST API

Bug ID	Description
584631	REST API admin with token unable to configure HA setting (via login session works).
663441	REST API unable to change status of interface when VDOMs are enabled.

Bug ID	Description
714075	When CORS is enabled for REST API administrators, POST and PUT requests with body data do not work with CORS due to the pre-flight requests being handled incorrectly. This only impacts newer browser versions that use pre-flight requests.

Routing

Bug ID	Description
537354	BFD/BGP dropping when `outbandwidth` is set on interface.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.

SSL VPN

Bug ID	Description
505986	On IE 11, SSL VPN web portal displays blank page title *{{::data.portal.heading}}* after authentication.

Switch Controller

Bug ID	Description
588584	GUI should add support to allow using switch VLAN interface under a tenant VDOM on a managed switch VDOM.
605864	If the firewall is downgraded from 6.2.3 to 6.2.2, the FortiLink interface loses its CAPWAP setting.

System

Bug ID	Description
464340	EHP drops for units with no NP service module.
578031	FortiManager Cloud cannot be removed once the FortiGate has trouble with contract.
600032	SNMP does not provide routing table for non-management VDOM.
607565	Interface `emac-vlan` feature does not work on SoC4 platform.
694202	`stpforward` does not work with LAG interfaces on a transparent VDOM.
695803	Unable to reorder firewall DoS policy in GUI or CLI.

Upgrade

Bug ID	Description

658664	FortiExtender status becomes `discovered` after upgrading from 6.0.10 (build 0365).
	Workaround: change the `admin` from `discovered` to `enable` after upgrading.
	`config extender-controller extender`
	`edit <id>`
	`set admin enable`
	`next`
	`end`

User & Device

Bug ID	Description
595583	Device identification via LLDP on an aggregate interface does not work.

VM

Bug ID	Description
587757	FG-VM image unable to be deployed on AWS with additional HDD (st1) disk type.

Bug ID	Description
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
605511	FG-VM-GCP reboots a couple of times due to kernel panic.
608881	IPsec VPN tunnel not staying up after failing over with AWS A-P cross-AZ setup.
640436	FortiGate AWS bootstrapped from configuration does not read SAML settings.
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.

WiFi Controller

Bug ID	Description
676689	RADIUS traffic not matching SD-WAN rule when using wpad daemon for wireless connection.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.

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.