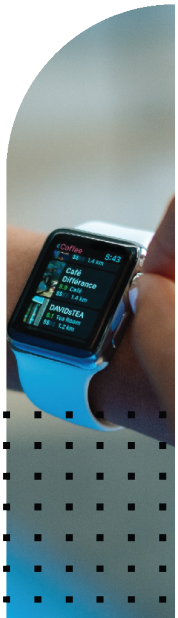
Release Notes

FortiOS 7.0.12



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/training-certification

FORTINET TRAINING 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

June 8, 2023
FortiOS 7.0.12 Release Notes
01-7012-902137-20230608

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-06-08	Initial release.

Introduction and supported models

This guide provides release information for FortiOS 7.0.12 build 0523.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.12 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-70F, FG-71F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300E, FG-301E, FG-400E, FG-400E-BP, FG-400F, FG-401F, FG-401E, FG-500E, FG-501E, FG-600E, FG-601E, FG-600F, FG-601F, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3000F, FG-3001F, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3500F, FG-3501F, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
FortiGate VM	FG-ARM64-AWS, FG-ARM64-KVM, FG-ARM64-OCI, FG-VM64, FG-VM64-ALI, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VM64-SVM, FG-VM64-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 7.0.12. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0523.

FG-80F-DSL	is released on build 6689.
FG-1000F	is released on build 6681.

FG-1001F	is released on build 6681.
FG-3200F	is released on build 6675.
FG-3201F	is released on build 6675.
FG-3700F	is released on build 6675.
FG-3701F	is released on build 6675.
FG-4800F	is released on build 6675.
FG-4801F	is released on build 6675.
FGR-70F	is released on build 6685.
FGR-70F-3G4G	is released on build 6685.

Special notices

Azure-On-Demand image

Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For ONDEMAND models before 6.4.2, upgrade to 6.4.2 using the FG-VM64-AZUREONDEMAND image. Then, upgrade to a later build using the FG-VM64-AZURE image.

GCP-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-GCPONDEMAND image is no longer provided. Both GCP PAYG and GCP BYOL models will share the same FG-VM64-GCP image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FG-VM64-GCPONDEMAND image. Then, upgrade to 7.0.x using the FG-VM64-GCP image.

ALI-On-Demand image

Starting from FortiOS 7.0.0, the FG-VM64-ALIONDEMAND image is no longer provided. Both ALI PAYG and ALI BYOL models will share the same FG-VM64-ALI image for upgrading and new deployments. Remember to back up your configuration before upgrading.

For PAYG models with a 6.2.x build, upgrade to the latest 6.4.x build (6.4.5 or later) using the FGT-VM64-ALIONDEMAND image. Then, upgrade to 7.0.x using the FGT-VM64-ALI image.

Unsupported websites in SSL VPN web mode

The following websites are not supported in SSL VPN web mode in FortiOS 7.0.1:

- Facebook
- Gmail
- Office 365
- YouTube

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 7.0.1.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

FEC feature design change

The FEC feature design has the following changes starting in FortiOS 7.0.2:

- FEC enabled on FortiGates running 7.0.2 is not backward compatible with FEC enabled on FortiGates running previous versions.
- In addition to enabling FEC on IPsec interfaces in previous versions, there is a new option, `fec`, that should also be enabled under the related firewall policy so the feature works:

```
config firewall policy
    edit <id>
        set fec enable
    next
end
```

- The `fec` option is not automatically enabled in a firewall policy when upgrading from a previous version. It must be enabled manually.

Hyperscale incompatibilities and limitations

See Hyperscale firewall incompatibilities and limitations in the Hyperscale Firewall Guide for a list of limitations and incompatibilities with FortiOS 7.0.12 features.

New features or enhancements

More detailed information is available in the New Features Guide.

Feature ID	Description
868164	Implement BIOS-level signature and file integrity checking for important system files and executables. Warn users of failed integrity checks, or prevent the system from booting depending on the severity and BIOS verification level. Kernel and userspace processes can also periodically verify the integrity of AV and IPS engine files, and other important system files and executables. FortiOS firmware and each release of an AV or IPS engine file are dually-signed by Fortinet CA and third-party CAs.

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*.

Fortinet Security Fabric upgrade

FortiOS 7.0.12 greatly increases the interoperability between other Fortinet products. This includes:

FortiAnalyzer	• 7.0.8
FortiManager	• 7.0.8
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 7.0 version.
FortiSwitch OS (FortiLink support)	• 6.4.6 build 0470 or later
FortiAP **FortiAP-S** **FortiAP-U** **FortiAP-W2**	• See Strong cryptographic cipher requirements for FortiAP on page 14
FortiClient* EMS	• 7.0.0 build 0042 or later
FortiClient* Microsoft Windows	• 7.0.0 build 0029 or later
FortiClient* Mac OS X	• 7.0.0 build 0022 or later
FortiClient* Linux	• 7.0.0 build 0018 or later
FortiClient* iOS	• 6.4.6 build 0507 or later
FortiClient* Android	• 6.4.6 build 0539 or later
FortiSandbox	• 2.3.3 and later

* If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.

When upgrading your Security Fabric, devices that manage other devices should be upgraded first.

When using FortiClient with FortiAnalyzer, you should upgrade both to their latest versions. The versions between the two products should match. For example, if using FortiAnalyzer 7.0.0, use FortiClient 7.0.0.

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. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC
13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice
17. FortiDeceptor
18. FortiAI/FortiNDR
19. FortiTester
20. FortiMonitor

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 7.0.12. When Security Fabric is enabled in FortiOS 7.0.12, all FortiGate devices must be running FortiOS 7.0.12.

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

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*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.4.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Strong cryptographic cipher requirements for FortiAP

FortiOS 7.0.0 has removed 3DES and SHA1 from the list of strong cryptographic ciphers. To satisfy the cipher requirement, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.3 and later
- FortiAP-S and FortiAP-W2 (E models): version 6.2.4, 6.4.1, and later
- FortiAP-U (EV and F models): version 6.0.3 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

If FortiGates running FortiOS 7.0.1 need to manage FortiAP models that cannot be upgraded or legacy FortiAP models whose names end with the letters B, C, CR, or D, administrators can allow those FortiAPs' connections with weak cipher encryption by using compatibility mode:

```
config wireless-controller global
    set tunnel-mode compatible
end
```

How VoIP profile settings determine the firewall policy inspection mode

When upgrading, all firewall policies with a VoIP profile selected will be converted to proxy-based inspection. All firewall policies that do not have a VoIP profile selected will remain in the same inspection mode after upgrading.

In the case when customers are using the following settings in 6.4:

```
config system settings
    set default-voip-alg-mode proxy-based
end
```

```
config firewall policy
    edit 0
        set inspection-mode flow
        unset voip-profile
    next
end
```

In 6.4, by default, SIP traffic is handled by proxy-based SIP ALG even though no VoIP profile is specified in a firewall policy.

After upgrading, the firewall policy will remain in `inspection-mode flow` but handled is by flow-based SIP inspection.

Due to the difference in which the SIP traffic is handled by flow-based SIP versus proxy-based SIP ALG inspection in 7.0.0 and later, if customers want to maintain the same behavior after upgrading, they can manually change the firewall policy's `inspection-mode` to `proxy`:

```
config firewall policy
    edit 0
        set inspection-mode proxy
        unset voip-profile
    next
end
```

Or prior to upgrading, they can assign a `voip-profile` to the firewall policies that are processing SIP traffic to force the conversion to `inspection-mode proxy` after upgrading.

L2TP over IPsec configuration needs to be manually updated after upgrading from 6.4.x or 7.0.0 to 7.0.1 and later

If the setting is not manually updated after upgrading, the VPN connection will be established, but it will not be accessible from the internal network (office network). This setting change is necessary regardless of whether route-based or policy-based IPsec is used.

To make L2TP over IPsec work after upgrading:

1. Add a static route for the IP range configured in `vpn l2tp`. For example, if the L2TP setting in the previous version's root VDOM is:

```
config vpn l2tp
    set eip 210.0.0.254
    set sip 210.0.0.1
    set status enable
    set usrgrp "L2tpusergroup"
end
```

   Add a static route after upgrading:

```
config router static
    edit 1
        set dst 210.0.0.0 255.255.255.0
        set device "l2t.root"
    next
end
```

2. Change the firewall policy source interface tunnel name to `l2t.VDOM`.

Add interface for NAT46 and NAT64 to simplify policy and routing configurations

This update simplifies the policy and routing of NAT46 and NAT64 policies by adding the NAT tunnel interface and options in `firewall vip/vip6` and `firewall policy` settings. The `policy46` and `policy64` settings have been merged into `policy`, and `vip46` and `vip64` into `vip` and `vip6`. Most firewall policy options can now be used in policies with NAT46 and NAT64 options enabled.

Upgrading

When upgrading from FortiOS 6.4.x or 7.0.0 to 7.0.1 and later, the old configurations for `vip46`, `vip64`, `policy46`, `policy64`, `nat64`, and `gui-nat46-64` will be removed. All objects in them will be removed.

The following CLI commands have been removed:

- `config firewall vip46`
- `config firewall vip64`

- `config firewall policy46`
- `config firewall policy64`
- `config system nat64`
- `set gui-nat46-64 {enable | disable}` (under `config system settings`)

The following GUI pages have been removed:

- *Policy & Objects* > *NAT46 Policy*
- *Policy & Objects* > *NAT64 Policy*
- NAT46 and NAT64 VIP category options on *Policy & Objects* > *Virtual IPs* related pages

During the upgrade process after the FortiGate reboots, the following message is displayed:

```
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log read'
```

The following output is displayed after running the diagnose command:

```
# diagnose debug config-error-log read
>>> "config" "firewall" "policy64" @ root:command parse error (error -
61)
>>> "config" "firewall" "policy46" @ root:command parse error (error -
61)
```

Creating new policies

After upgrading FortiOS 6.4.x or 7.0.0 to 7.0.1, you will need to manually create new `vip46` and `vip64` policies.

- Create a `vip46` from `config firewall vip` and enable the `nat46` option.
- Create a `vip64` from `config firewall vip6` and enable the `nat64` option.
- Create or modify `ippool` and `ippool6`, and enable the `nat64` or `nat46` option.
- Create a policy and enable the `nat46` option, apply the `vip46` and `ippool6` in a policy.
- Create a policy and enable the `nat64` option, apply the `vip64` and `ippool` in policy.
- Ensure the routing on the client and server matches the new `vip`/`vip6` and `ippool`/`ippool6`.

Example configurations

`vip46` object:

Old configuration	New configuration

`config firewall vip46`
`edit "test-vip46-1"`
`set extip 10.1.100.155`
`set mappedip 2000:172:16:200::55`
`next`
`end`
	`config firewall vip`
	`edit "test-vip46-1"`
	`set extip 10.1.100.150`
	`set nat44 disable`
	`set nat46 enable`
	`set extintf "port24"`

Old configuration	New configuration
	set ipv6-mappedip 2000:172:16:200::55 next end

`ippool6` object:

Old configuration	New configuration
config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 next end	config firewall ippool6 edit "test-ippool6-1" set startip 2000:172:16:201::155 set endip 2000:172:16:201::155 **set nat46 enable** next end

NAT46 policy:

Old configuration	New configuration
config firewall policy46 edit 1 set srcintf "port24" set dstintf "port17" set srcaddr "all" set dstaddr "test-vip46-1" set action accept set schedule "always" set service "ALL" set logtraffic enable set ippool enable set poolname "test-ippool6-1" next end	config firewall policy edit 2 set srcintf "port24" set dstintf "port17" set action accept **set nat46 enable** set srcaddr "all" set dstaddr "test-vip46-1" set srcaddr6 "all" set dstaddr6 "all" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname6 "test-ippool6-1" next end

`vip64` object

Old configuration	New configuration
config firewall vip64 edit "test-vip64-1" set extip 2000:10:1:100::155 set mappedip 172.16.200.155 next end	config firewall vip6 edit "test-vip64-1" set extip 2000:10:1:100::155 set nat66 disable **set nat64 enable** **set ipv4-mappedip 172.16.200.155**

Old configuration	New configuration
	next end

`ippool` object

Old configuration	New configuration
config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 next end	config firewall ippool edit "test-ippool4-1" set startip 172.16.201.155 set endip 172.16.201.155 **set nat64 enable** next end

NAT64 policy:

Old configuration	New configuration
config firewall policy64 edit 1 set srcintf "wan2" set dstintf "wan1" set srcaddr "all" set dstaddr "test-vip64-1" set action accept set schedule "always" set service "ALL" set ippool enable set poolname "test-ippool4-1" next end	config firewall policy edit 1 set srcintf "port24" set dstintf "port17" set action accept **set nat64 enable** set srcaddr "all" set dstaddr "all" set srcaddr6 "all" set dstaddr6 "test-vip64-1" set schedule "always" set service "ALL" set logtraffic all set ippool enable set poolname "test-ippool4-1" next end

ZTNA configurations and firewall policies

Since FortiOS 7.0.2, ZTNA configurations no longer require a firewall policy to forward traffic to the access proxy VIP. This is implicitly generated based on the ZTNA rule configuration.

When upgrading from FortiOS 7.0.1 or below:

- If an `access-proxy` type `proxy-policy` does not have a `srcintf`, then after upgrading it will be set to `any`.
- To display the `srcintf` as *any* in the GUI, *System* > *Feature Visibility* should have *Multiple Interface Policies*

enabled.
- All full ZTNA firewall policies will be automatically removed.

Default DNS server update

If both primary and secondary DNS servers are set to use the default FortiGuard servers prior to upgrading, the FortiGate will update them to the new servers and enable DoT after upgrading. If one or both DNS servers are not using the default FortiGuard server, upgrading will retain the existing DNS servers and DNS protocol configuration.

VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name

Affected versions:

- FortiOS 6.4.9 and later
- FortiOS 7.0.6 and later
- FortiOS 7.2.0 and later

When upgrading to one of the affected versions, there is a check within the set `vdom-links` function that rejects `vdom-links` that have the same name as a VDOM. Without the check, the FortiGate will have a kernel panic upon bootup during the upgrade step.

A workaround is to rename the `vdom-links` prior to upgrading, so that they are different from the VDOMs.

Product integration and support

The following table lists FortiOS 7.0.12 product integration and support information:

Web browsers	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
Explicit web proxy browser	• Microsoft Edge 114 • Mozilla Firefox version 113 • Google Chrome version 114 Other browser versions have not been tested, but may fully function. Other web browsers may function correctly, but are not supported by Fortinet.
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C

Fortinet Single Sign-On (FSSO)	• 5.0 build 03010 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2022 Standard
	  • Windows Server 2022 Datacenter
	  • 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 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
	  • Windows Server 2008 Core (requires Microsoft SHA2 support package)
	  • Novell eDirectory 8.8

AV Engine	• 6.00288
IPS Engine	• 7.00167

Virtualization environments

The following table lists hypervisors and recommended versions.

Hypervisor	Recommended versions
Citrix Hypervisor	• 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS • Red Hat Enterprise Linux release 8.4 • SUSE Linux Enterprise Server 12 SP3 release 12.3
Microsoft Windows Server	• 2012R2 with Hyper-V role
Windows Hyper-V Server	• 2019
Open source XenServer	• Version 3.4.3 • Version 4.1 and later
VMware ESX	• Versions 4.0 and 4.1
VMware ESXi	• Versions 6.5, 6.7, and 7.0.

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 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 113 Google Chrome version 113
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 113 Google Chrome version 113
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 113 Google Chrome version 113
macOS Ventura 13	Apple Safari version 15 Mozilla Firefox version 113 Google Chrome version 113
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.

Resolved issues

The following issues have been fixed in version 7.0.12. To inquire about a particular bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
857632	Unable to access to some websites when application control with deep inspection is enabled.

DNS Filter

Bug ID	Description
871854	DNS UTM log still presents unknown FortiGuard category even when the DNS proxy received a rating value.
878674	Forward traffic log is generated for allowed DNS traffic if the DNS filter is enabled but the policy is set to log security events only.

Firewall

Bug ID	Description
804603	An httpsd singal 6 crash occurs due to `/api/v2/monitor/license/forticare-resllers`.

GUI

Bug ID	Description
750727	Applying a negate for the *Application Name* column in the log viewer is not working as expected.
827893	Security rating test for *FortiCare Support* fails when connected to FortiManager Cloud or FortiAnalyzer Cloud.

Bug ID	Description
862474	IPsec tunnel interface *Bandwidth* widget inbound is zero and outbound value is lower than the binding interface.
890683	GUI being exposed to port 80 on the interfaces defined in the ACME settings, even if administrative access is disabled on the interface.
897004	On rare occasions, the GUI may display blank pages when the user navigates from one menu to another if there is a managed FortiSwitch present.
899434	A `super_admin` login is logged in the console logs when remotely logging in to a FortiGate with the FortiCloud portal using a `prof_admin` profile.

HA

Bug ID	Description
846015	First ICMP redirected from FGSP secondary is dropped on FGSP primary when UTM is enabled.
868622	The session is not synchronized after HA failover by detecting monitored interface as down.
872686	Configuration backup on standby unit fails when using SFTP.
881847	HA interfaces flapping on FG-3401E.
883546	In HA, sending lot of CLI configurations causes the creation of a VDOM on the secondary unit.

Intrusion Prevention

Bug ID	Description
839170	IPS engine may crash (`SIGALRM`) when the system is busy because it might not receive enough run time.

IPsec VPN

Bug ID	Description
788751	IPsec VPN Interface shows incorrect TX/RX counter.
855705	NAT detection in shortcut tunnel sometimes goes wrong.
858681	When upgrading from 6.4.9 to 7.0.6 or 7.0.8, the traffic is not working between the spokes on the ADVPN environment.

Bug ID	Description
873097	Phase 2 not initiating the rekey at soft limit timeout on new kernel platforms.
885818	If a tunnel in an IPsec aggregate is down but its DPD link is on, the IPsec aggregate interface may still forward traffic to a down tunnel causing traffic to drop.
891462	The *Peer ID* field in the *IPsec* widget should not show a warning message that *Two-factor authentication is not enabled*.
892699	In an HA cluster, static routes via the IPsec tunnel interface are not inactive in the routing table when the tunnel is down.

Log & Report

Bug ID	Description
823183	FortiGates are showing *Logs Queued* in the GUI after a FortiAnalyzer reboot, even tough the queued logs were actually all uploaded to FortiAnalyzer and cleared when the connection restores.
837116	FortiCloud log statistics chart on the *Log Settings* page shows incorrect data.
838253	FortiAnalyzer log statistics chart on the *Log Settings* page shows incorrect data.
857573	Log filter with negation of destination IP display all logs.
860141	Syslog did not update the time after daylight saving time (DST) adjustment.
864219	A miglogd crash occurs when creating a dynamic interface cache on an ADVPN environment.
901545	FG-40F/FWF-61F halts after upgrading.

Proxy

Bug ID	Description
727629	WAD encounters signal 11 crash.
857507	WAD encounters signal 11 crash after upgrading to 7.0.8.
874563	WAD has signal 11 crash when attempting to merge user information attributes.
901296	WAD crash with HTTP forward request.

Routing

Bug ID	Description
821149	Early packet drop occurs when running UTM traffic on virtual switch interface.
858299	Redistributed BGP routes to the OSPF change its forward address to the tunnel ID.
863318	Application forticron signal 11 (Segmentation fault) occurs.
864626	FortiGate local traffic does not follow SD-WAN rules.
883918	Delay in joining `(S,G)` in PIM-SM.
884372	All BGP routes in dual ADVPN redundant configuration are not getting updated to the correct WAN interface post-rollback to WAN failover.
890379	After upgrading, SD-WAN is unable to fail over the traffic when one interface is down.
897940	Link monitor's probe timeout value range is not appropriate when the user decreases the minimum interval.

Security Fabric

Bug ID	Description
825291	Security rating test for *FortiAnalyzer* fails when connected to FortiAnalyzer Cloud.
853406	External resource full certificate check does not validate certificate when URI is an IP address.

SSL VPN

Bug ID	Description
781581	Customer internal website is not shown correctly in SSL VPN web mode.
868491	SSL VPN web mode connection to VMware vCenter 7 is not working.
871039	Internal website is not displaying user-uploaded PDF files when visited through SSL VPN web mode.
872745	SSL VPN web mode to RDP broker leads to connection being closed.
873313	SSL VPN policy is ignored if no user or user group is set and the FSSO group is set.
873995	Problem with the internal website using SSL VPN web mode.
877124	RDP freezes in web mode with high CPU usage of SSL VPN process.

Bug ID	Description
884860	SSL VPN tunnel mode gets disconnected when SSL VPN web mode is disconnected by `limit-user-logins`.
896007	Specific SAP feature is not working with SSL VPN web mode.

System

Bug ID	Description
666664	Interface belonging to other VDOMs should be removed from interface list when configuring a GENEVE interface.
724085	Traffic passing through an EMAC VLAN interface when the parent interface is in another VDOM is blocked if NP7 offloading is enabled. If `auto-asic-offload` is disabled in the firewall policy, then the traffic flows as expected.
766834	forticron allocates over 700 MB of memory, causes the FortiGate to go into conserve mode, and causes kernel panic due to 100 MB of configured CRL.
796094	Egress traffic on EMAC VLAN is using base MAC address instead.
805122	In FIPS-CC mode, if `cfg-save` is set to `revert`, the system will halt a configuration change or certificate purge.
812957	When setting the `speed` of 1G SFP ports on FG-180xF platforms to `1000full`, the interface does not come up after rebooting.
820268	VIP traffic access to the EMAC VLAN interface uses incorrect MAC address on NP7 platform.
821000	QSFP and QSFP+ Fortinet transceivers are not operational on FG-3401E.
859795	High CPU utilization occurs when relay is enabled on VLAN, and this prevents users from getting an IP from DHCP.
869305	SNMP multicast counters are not increasing.
878400	When traffic is offloaded to an NP7 source MAC, the packets sent from the EMAC VLAN interface are not correct.
881094	FG-3501F NP7 is dropping all traffic after it is offloaded.
882187	FortiGate enters conserve mode in a few hours after enabling UTM on the policies.
883071	Kernel panic occurs due to null pointer dereference.
887268	Unable to configure `dscp-based-priority` when `traffic-priority dscp` is configured under `system global`.
892195	LAG interface has `NOARP` flag after interface settings change.
899884	FG-3000F reboots unexpectedly with NULL pointer dereference.
909345	Kernel panic occurs when receiving ICMP redirect messages.

Upgrade

Bug ID	Description
900761	FG-601E crashes randomly after upgrading to 7.0.8 and 7.0.11.

Web Filter

Bug ID	Description
863728	The urlfilter process causes a memory leak, even when the firewall policy is not using the web filter feature.

Known issues

The following issues have been identified in version 7.0.12. To inquire about a particular bug or report a bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
877613	*Mark as Reject* can be still chosen as an *Action* in an *Anti-Spam Block/Allow List* in the GUI.

Endpoint Control

Bug ID	Description
730767	The new HA primary FortiGate cannot get EMS Cloud information when HA switches over. **Workaround**: delete the EMS Cloud entry then add it back.

Explicit Proxy

Bug ID	Description
817582	When there are many users authenticated by an explicit proxy policy, the *Firewall Users* widget can take a long time to load. This issue does not impact explicit proxy functionality.

Firewall

Bug ID	Description
719311	On the *Policy & Objects* > *Firewall Policy* page in 6.4.0 onwards, the IPv4 and IPv6 policy tables are combined but the custom section name (global label) is not automatically checked for duplicates. If there is a duplicate custom section name, the policy list may show empty for that section. This is a display issue only and does not impact policy traffic. **Workaround**: rename the custom section to unique name between IPv4 and IPv6 policies.

Bug ID	Description

843554	If the first firewall service object in the service list (based on the order in the command line table) has a protocol type of *IP*, the GUI may incorrectly modify its protocol number whenever a new firewall service of the same protocol type *IP* is created in the GUI.
	This silent misconfiguration can result in unexpected behavior of firewall policies that use the impacted service. For example, some 6K and 7K platforms have firewall service *ALL* (protocol type *IP*) as the first service, and this can cause the *ALL* service to be modified unexpectedly.
	Workaround: create a new service in the CLI, or move a non-IP type services to the top of the firewall service list. For example, if `ALL` is the first firewall service in the list:
	`config firewall service custom`
	`edit "unused"`
	`set tcp-portrange 1`
	`next`
	`move "unused" before "ALL"`
	`end`

897849	*Firewall Policy* list may show empty sequence grouping sections if multiple policies are sharing the same `global-label`. **Workaround**: drag and drop the policy to the correct sequence group in the GUI, or remove the `global-label` for each member policy in the group except for the leading policy. For example, in the configuration, policy 2 will be automatically grouped under `group1` without the need of adding the same `global-label`. • Policy 1 (`global-label "group"`) • Policy 2 • Policy 3 (`global-label "group2"`) • Policy 4

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
677806	On the *Network* > *Interfaces* page when VDOM mode is enabled, the *Global* view incorrectly shows the status of IPsec tunnel interfaces from non-management VDOMs as up. The VDOM view shows the correct status.
685431	On the *Policy & Objects* > *Firewall Policy* page, the policy list can take around 30 seconds or more to load when there is a large number (over 20 thousand) of policies. **Workaround**: use the CLI to configure policies.

Bug ID	Description
707589	*System* > *Certificates* list sometimes shows an incorrect reference count for a certificate, and incorrectly allows a user to delete a referenced certificate. The deletion will fail even though a success message is shown. Users should be able to delete the certificate after all references are removed.
708005	When using the SSL VPN web portal in the Firefox, users cannot paste text into the SSH terminal emulator. **Workaround**: use Chrome, Edge, or Safari as the browser.
755177	When upgrading firmware from 7.0.1 to 7.0.2, the GUI incorrectly displays a warning saying this is not a valid upgrade path.
810225	An *undefined* error is displayed when changing an administrator password for the first time. Affected models: NP7 platforms.
853352	On the *View/Edit Entries* slide-out pane (*Policy & Objects* > *Internet Service Database* dialog), users cannot scroll down to the end if there are over 100000 entries.
898902	In the *System* > *Administrators* dialog, when there are a lot of VDOMs (over 200), the dialog can take more than one minute to load the *Two-factor Authentication* toggle. This issue does not affect configuring other settings in the dialog. **Workaround**: use the CLI to configure `two-factor-authentication` under `config system admin`.

HA

Bug ID	Description
810286	FGSP local sessions exist after rebooting an HA pair with A-P mode, and the HW SSE/session count is incorrect.
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.

Hyperscale

Bug ID	Description
795853	VDOM ID and IP addresses in the IPL table are incorrect after disabling EIF/EIM.
811109	FortiGate 4200F, 4201F, 4400F, and 4401F HA1, HA2, AUX1, and AUX2 interfaces cannot be added to an LAG.

Bug ID	Description
836976	Sessions being processed by hyperscale firewall policies with hardware logging may be dropped when dynamically changing the `log-processor` setting from `hardware` to `host` for the hardware log sever added to the hyperscale firewall policy. To avoid dropping sessions, change the `log-processor` setting during quiet periods.
838654	Hit count not ticking for implicit deny policy for hardware session in case of NAT46 and NAT64 traffic.
839958	`service-negate` does not work as expected in a hyperscale deny policy.
842659	`srcaddr-negate` and `dstaddr-negate` are not working properly for IPv6 traffic with FTS.
843132	Access control list (ACL) policies added to a hyperscale firewall VDOM that is processing traffic may take longer than expected to become effective. During a transition period, traffic that should be blocked by the new ACL policy will be allowed.
843197	Output of `diagnose sys npu-session list/list-full` does not mention policy route information.
843266	Diagnose command should be available to show `hit_count/last_used` for policy route and NPU session on hyperscale VDOM.
843305	Get `PARSE SKIP ERROR=17 NPD ERR PBR ADDRESS` console error log when system boots up.
844421	The `diagnose firewall ippool list` command does not show the correct output for overload type IP pools.
846520	NPD/LPMD process killed by out of memory killer after running mixed sessions and HA failover.

IPsec VPN

Bug ID	Description
761754	IPsec aggregate static route is not marked inactive if the IPsec aggregate is down.

Log & Report

Bug ID	Description
850642	Logs are not seen for traffic passing through the firewall.
860822	When viewing logs on the *Log & Report* > *System Events* page, filtering by *domain\username* does not display matching entries. **Workaround**: use a double backslash (*domain\\username*) while filtering or searching by username only without the domain.

Proxy

Bug ID	Description
836101	FortiGate is entering conserve mode due to a WAD memory leak.
837724	WAD crash occurs.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
794703	Security Rating report for *Rogue AP Detection* and *FortiCare Support* checks show incorrect results.

System

Bug ID	Description
847664	Console may display `mce: [Hardware Error]` error message after fresh image burn or reboot.
884023	When a user is logged in as a VDOM administrator with restricted access and tries to upload a certificate (*System* > *Certificates*), the *Create* button on the *Create Certificate* pane is greyed out.
900670	QSFP/QSFP+ port23/port24 are down after upgrading to 7.0.11 on FG-3401E.
903397	After upgrading to 7.0.11, FortiOS cannot display QSFP+ transceiver information. Affected platforms: FG-110xE, FG-220xE, FG-330xE, FG-340xE, and FG-360xE.

User & Authentication

Bug ID	Description
765184	RADIUS authentication failover between two servers for high availability does not work as expected.

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.

WiFi Controller

Bug ID	Description
814541	When there are extra large number of managed FortiAP devices (over 500) and large number of WiFi clients (over 5000), the *Managed FortiAPs* page and *FortiAP Status* widget can take a long time to load. This issue does not impact FortiAP operation.
904349	Unable to create FortiAP profile in the GUI for dual-5G mode FortiAP U231F/U431F models. **Workaround**: use the CLI to update the profile to dual-5G mode.

ZTNA

Bug ID	Description
848222	ZTNA TCP forwarding is not working when a real server is configured with an FQDN address type. An FQDN address type that can resolve public IPs is not recommended for ZTNA TCP forwarding on real servers because the defined internal DNS database zone is trying to override it at the same time. By doing so, the internal private address may not take effect after rebooting, and causes a ZTNA TCP forwarding failure due to the real server not being found.

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.

www.fortinet.com