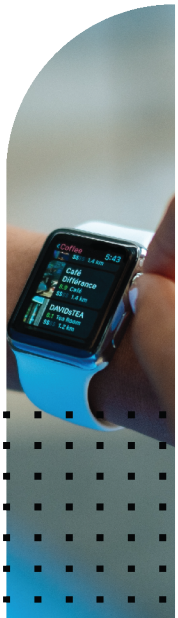
Release Notes

FortiOS 7.0.11



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

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

March 27, 2023
FortiOS 7.0.11 Release Notes
01-7011-889684-20230327

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-03-16	Initial release.
2023-03-17	Updated Resolved issues on page 24, Known issues on page 38, and Built-in AV engine on page 45.
2023-03-21	Updated Introduction and supported models on page 7.
2023-03-22	Added VDOM link and policy configuration is lost after upgrading if VDOM and VDOM link have the same name on page 20. Updated Known issues on page 38.
2023-03-24	Updated Product integration and support on page 21 and Known issues on page 38.
2023-03-27	Updated Known issues on page 38.

Introduction and supported models

This guide provides release information for FortiOS 7.0.11 build 0489.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 7.0.11 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 7.0.11. To confirm that you are running the correct build, run the CLI command `get system status` and check that the `Branch point` field shows 0489.

FG-80F-DSL	is released on build 4997.
FGR-70F	is released on build 6585.
FGR-70F-3G4G	is released on build 6585.

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.

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 7.0.11 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-3500F, FG-3501F, FG-4200F, FG-4201F, FG-4400F, and FG-4401F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For more information, refer to the Hyperscale Firewall Release Notes.

Changes in CLI

Bug ID	Description
816604	Remove the `purge` command under `endpoint-control fctems`.

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description
836613	Add CLI option for each FortiClient EMS connector (`trust-ca-cn`). This option is enabled by default. When enabled, the CA and CN information is stored with the connector, which allows the FortiGate to automatically approve an updated certificate as long as it has the same CA and CN. `config endpoint-control fctems` `edit <ems-id>` `set trust-ca-cn {enable | disable}` `next` `end`
841928	In some scenarios where it is necessary to simulate a system crash, the following commands allow a super_admin administrator to safely trigger a kernel crash using a SysRq key. `# diagnose debug kernel sysrq status` `# diagnose debug kernel sysrq {enable | disable}` `# diagnose debug kernel sysrq command crash` A kernel crash dump is outputted to the console. The FortiGate reboots and recovers without losing any functionality. This is only supported on FortiGate VMs.
854704	FortiGate VMs with eight or more vCPUs can be configured to have a minimum of eight cores to be eligible to run the full extended database (DB). Any FortiGate VM with less than eight cores will receive a slim version of the extended DB. This slim-extended DB is a smaller version of the full extended DB, and it is designed for customers who prefer performance over security.
855561	Use API endpoint domain name from instance metadata to support FortiOS VM OCI DRCC region.

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

FortiAnalyzer	• 7.0.7
FortiManager	• 7.0.7
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 15
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 7.0.11. When Security Fabric is enabled in FortiOS 7.0.11, all FortiGate devices must be running FortiOS 7.0.11.

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.

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"` **`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`	`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"`

Old configuration	New configuration
`        set poolname "test-ippool6-1"` `    next` `end`	`        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` `    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`

Old configuration	New configuration
	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 7.0.11 product integration and support information:

Web browsers	• Microsoft Edge 111 • Mozilla Firefox version 111 • Google Chrome version 111 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 111 • Mozilla Firefox version 111 • Google Chrome version 111 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 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	• 6.00286
IPS Engine	• 7.00159

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 105 Google Chrome version 107
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 105 Google Chrome version 107
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 105 Google Chrome version 107
macOS Monterey 12.4	Apple Safari version 15 Mozilla Firefox version 105 Google Chrome version 107
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 7.0.11. To inquire about a particular bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
818092	CDR archived files are deleted at random times and not retained.
845960	Flow mode opens port 8008 over the AV profile that does not have HTTP scan enabled.
849020	FortiGate enters conserve mode and the console prints a `fork()` failed message.

Data Leak Prevention

Bug ID	Description
873608	DLP blocking of SMB traffic gives unreliable results.

Endpoint Control

Bug ID	Description
834168	FortiGates get deauthorized on EMS.

Explicit Proxy

Bug ID	Description
823319	Authentication hard timeout is not respected for firewall users synchronized from WAD user.
842016	Client gets 304 response if a cached object has varying headers and is expired.
849794	Random websites are not accessible with proxy policy after upgrading to 6.4.10.
865135	Multipart boundary parsing failed with CRLF before the end of boundary 1.

Firewall

Bug ID	Description
728734	The VIP group hit count in the table (*Policy & Objects* > *Virtual IPs*) is not reflecting the correct sum of VIP members.
794901	Unable to create a `geography` type address object and get a `Can not be geography address when it is a member of addrgrp used by ipsec_tunnel!` error.
816493	The `set sub-type ems-tag` option is blocked in HA diff installation.
835413	Inaccurate sFlow interface data reported to PRTG after upgrading to 7.0.
840689	Virtual server aborts connection when `ssl-max-version` is set to `tls-1.3`.
847086	Unable to add additional MAC address objects in an address group that already has 152 MAC address objects.
852714	Making a full HTTP session is sometimes bypassed if `ssl-hsts` is enabled for a `server-load-balance` VIP.
854901	Full cone NAT (`permit-any-host enable`) causes TCP session clash.
856187	Explicit FTPS stops working with IP pool after upgrading.
860480	FG-3000D cluster kernel panic occurs when upgrading from 7.0.5 to 7.0.6 and later.
861990	Increased CPU usage in softIRQ after upgrading from 7.0.5 to 7.0.6.
865661	Standard and full ISDB sizes are not configurable on FG-101F.
875565	The policy or other cache lists are sometimes not freed in time. This may cause unexpected policies to be stored in the cache list.

FortiView

Bug ID	Description
804177	When setting the time period to the *now* filter, the table cannot be filtered by policy type.

GUI

Bug ID	Description
722358	When a FortiGate local administrator is assigned to more than two VDOMs and tries logging in to the GUI console, they get a command parse error when entering VDOM configuration mode.

Bug ID	Description
753328	Incorrect shortcut name shown on the *Network* > *SD-WAN* > *Performance SLAs* page.
773258	FortiAP icon cannot be moved once placed on the WiFi map.
833306	Intermittent error, *Failed to retrieve FortiView data*, appears on real-time *FortiView Sources* and *FortiView Destination* monitor pages.
837836	The *Network* > *Interfaces* faceplate shows two SFP interfaces, which do not exist on that FortiGate model.
845513	On G-model profiles, changing the platform mode change from single 5G (dedicated scan enabled) to dual 5G is not taking effect.
853414	*Dashboard* widgets are not loading when the FortiGate manages FortiSwitch with tenant ports (exported from root to other VDOM).
867589	Local VDOM administrator randomly sees a blank white page after logging in with the interface that belongs to the VDOM.
869138	Unable to select addresses in *FortiView* monitors.
870675	CLI console in GUI reports *Connection lost.* when the administrator has more than 100 VDOMs assigned.
872064	Creating a monitor from a dashboard widget in a non-root VDOM incorrectly uses the root VDOM.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
777394	Long-lasting sessions expire on the HA secondary in large session synchronization scenarios.
810175	`set admin-restrict-local` is not working for SSH.
813207	Virtual MAC address is sent inside GARP by the secondary unit after a reboot.
818432	When private data encryption is enabled, all passwords present in the configuration fail to load and may cause HA failures.
830879	Running `execute ha manage 0 <remote_admin>` fails and displays a `Permission denied, please try again.` error if the 169.254.0.0/16 local subnet is not in the trusted host list.
835331	Communication is disrupted when HA switching is performed in an environment where the VDOM is split to accommodate two IPoE lines.
837888	CLI deployment of a configuration to the secondary unit results in an unresponsive aggregate interface.
840305	Static ARP entry is removed after reboot or HA failover.

Bug ID	Description
853900	The administrator `password-expire` calculation on the primary and secondary returns a one-second diff, and causes HA to be out-of-sync.
854445	When adding or removing an HA monitor interface, the link failure value is not updated.
856004	Telnet connection running ping fails during FGSP failover for virtual wire pair with VLAN traffic.
856643	FG-500E interface stops sending IPv6 RAs after upgrading from 7.0.5 to 7.0.7.
860497	Output of `diagnose sys ntp status` is misleading when run on a secondary cluster member.
864226	FG-2600F kernel panic occurs after a failover on both members of the cluster.
885844	HA shows as being out-of-sync after upgrading due to a checksum mismatch for `endpoint-control fctems`.

Hyperscale

Bug ID	Description
807476	After packets go through host interface TX/RX queues, some packet buffers can still hold references to a VDOM when the host queues are idle. This causes a VDOM delete error with `unregister_vf`. If more packets go through the same host queues for other VDOMs, the issue should resolve by itself because those buffers holding the VDOM reference can be pushed and get freed and recycled.
824733	IPv6 traffic continues to pass through a multi-VDOM setup, even when the static route is deleted.
877696	Get KTRIE invalid node related error and kernel panic on standby after adding a second device into A-P mode HA cluster.

Intrusion Prevention

Bug ID	Description
845944	Firewall policy change causes high CPU spike with IPS engine.

IPsec VPN

Bug ID	Description
726326, 745331	IPsec server with NP offloading drops packets with an invalid SPI during rekey.
765174	Certain packets are causing IPsec tunnel drops on NP6XLite platforms after HA failover because the packet is not checked properly.
798045	FortiGate is unable to install SA (`failed to add SA, error 22`) when there is an overlap in configured selectors.
810833	IPsec static router gateway IP is set to the gateway of the tunnel interface when it is not specified.
822651	NP dropping packet in the incoming direction for SoC4 models.
842571	If `mode-cfg` is used, a race condition can result in an IP conflict and sporadic routing problems in an ADVPN/SD-WAN network. Connectivity can only be restored by manually flushing the IPsec tunnels on affected spokes.
848014	ESP tunnel traffic hopping from VRF.
855772	FortiGate IPsec tunnel role could be incorrect after rebooting or upgrading, and causes negotiation to be stuck when it comes up.
858715	IPsec phase 2 fails when both HA cluster members reboot at the same time.
869166	IPsec tunnel does not coming up after the upgrading firmware on the branch FortiGate (FG-61E).
873097	Phase 2 not initiating the rekey at soft limit timeout on new kernel platforms.
876795	RADIUS server will reject new authentication if a previous session is missing ACCT-STOP to terminate the session, which causes the VPN connection to fail.

Log & Report

Bug ID	Description
838357	A deny policy with log traffic disabled is generating logs.
860264	The miglogd process may send empty logs to other logging devices.
873987	High memory usage from miglogd processes even without traffic.
850519	*Log & Report* > *Forward Traffic* logs do not return matching results when filtered with *!<application name>*.

Proxy

Bug ID	Description
746587	WAD crashes during traffic scan in proxy mode.
769955	WAD process crashes (signal 11) with disclaimer and user authentication being applied to the web proxy.
781613	WAD crash occurs four times on FG-61F during stress testing.
818371	WAD process crashes with some URIs.
823078	WAD user-info process randomly consumes 100% CPU of one core.
825977	WAD crash occurs on FG-101F during stress testing.
834387	In a firewall proxy policy, the SD-WAN zone assigned to interface is not checked.
835745	WAD process is crashing after upgrading to FortiOS 7.2.1.
843318	If a client sends an HTTP request for a resource which is not yet cached by the FortiGate and the request header contains `Cache-Control: only-if-cached`, then the WAD worker process will crash with signal 11.
855853	WAD crashes frequently and utilizes high CPU.
855882	Increase in WAD process memory usage after upgrading.
856235	The WAD process memory usage gradually increases over a few days, causing the FortiGate to enter into conserve mode.
857368	WAD crash with signal 11 caused by a stack allocated buffer overflow when parsing Huffman-encoded HTTP header name if the header length is more than 256 characters.

Routing

Bug ID	Description
618684	When HA failover is performed to the other cluster member that is not able to reach the BFD neighbor, the BFD session is down as expected but the static route is present in the routing table.
708904	`No IGMP-IF for ifindex` log points to multicast enabled interface.
809321	IS-IS LSP packets do not include the checksum and the authentication key (`[Checksum: [missing]], [Checksum Status: Not present] and authentication "hmac-md5 (54), message digest]`).
816582	IPv6 connected subnet in VRF, other than VRF 0, gets an RPF failure after HA failover.
846107	IPv6 VRRP backup is sending RA, which causes routing issues.

Bug ID	Description
847037	When the policy route has a set gateway, the FortiGate is not following the policy route to forward traffic and sends unreasonable ARP requests.
848270	Reply traffic from the DNS proxy (DNS database) is choosing the wrong interface.
848310	IPsec traffic sourced from a loopback interface does not follow the policy route or SD-WAN rules.
850862	GUI does not allow an AS path to be to configured with multiple similar AS numbers.
852525	When enabled, FEC is not effectively reducing packet loss when behind NAT.
860075	Traffic session is processed by a different SD-WAN rule and randomly times out.
862165	FortiGate does not add the route in the routing table when it changes for SD-WAN members.
862418	Application VWL crash occurs after FortiManager configuration push causes an SD-WAN related outage.
862573	SD-WAN GUI does not load, and the lnkmtd process crashes frequently.
865914	When BSM carries multiple CRPs, PIM might use the incorrect prefix to update the mroute's RP information.

Security Fabric

Bug ID	Description
798795	API that registers appliances to the Fabric stopped working.
801048	During the FortiOS initialization process, there is a small chance that other services using UDP take the specific port that caused csfd initialization to fail.
814674	*Failed to retrieve upgrade progress* message appears when upgrading a FortiAP or FortiSwitch that is connected to a downstream FortiGate.
835765	Automation stitch trigger is not working when the threshold based email alert is enabled in the configuration.
839258	Unable to add another FortiGate to the Security Fabric after updating to the latest patch.
870527	FortiGate cannot display more than 500 VMs in a GCP dynamic address.

SSL VPN

Bug ID	Description
746230	SSL VPN web mode cannot display certain websites that are internal bookmarks.

Bug ID	Description
748085	Authentication request of SSL VPN realm can now only be sent to user group, local user, and remote group that is mapped to that realm in the SSL VPN settings. The authentication request will not be applied to the user group and remote group of non-realm or other realms.
783167	Unable to load GitLab through SSL VPN web portal.
803576	Comments in front of `<html>` tag are not handled well in HTML file in SSL VPN web mode.
808107	FortiGate is not sending Accounting-Request packet that contains the Interim-Update AVP when two-factor authentication is assigned to a user (defined on the FortiGate) while connecting using SSL VPN.
810239	Unable to view PDF files in SSL VPN web mode.
819754	Multiple DNS suffixes cannot be set for the SSL VPN portal.
825750	VMware vCenter bookmark in not working after logging in to SSL VPN web mode.
825810	SSL VPN web mode is unable to access EMS server.
828194	SSL VPN stops passing traffic after some time.
831069	A blank page displayed after logging in to the back-end server in SSL VPN web mode.
848067	RDP over VPN SSL web mode stops work after upgrading.
850898	OS checklist for the SSL VPN in FortiOS does not include macOS Ventura (13).
852566	User peer feature for one group to match to multiple user peers in the authentication rules is broken.
854143	Unable to access Synology NAS server through SSL VPN web mode.
854642	Internal website with JavaScript is proxying some functions in SSL VPN web mode, which breaks them.
863860	RDP over SSL VPN web mode to a Windows Server changes the time zone to GMT.
864096	EcoStruxure Building Operations 2022 does not render using SSL VPN bookmark.
864417	In the second authentication of RADIUS two-factor authentication, the `acct-update-interval` returned is `0`. SSL VPN uses the second return and not send RADIUS `acct-interim-update` packet.
876683	SSL VPN web mode has issue accessing specific URL, https://gt***.si***.fr.
877896	When accessing the VDOM's GUI in SSL VPN web mode, policies are only shown for a specific VDOM instead of all VDOMs.

Switch Controller

Bug ID	Description
762615, 765283	FortiLink flcfgd crash occurs when pushing all configurations to FortiSwitch, which includes quarantined MACs.
857778	VLAN changes on FortiGate are pushed to FortiSwitch, but they are not taking effect.
876021	FortiLink virtually managed switch port status is not getting pushed after the FortiGate reboots.

System

Bug ID	Description
550701	WAD daemon signal 11 causes cmdbsvr deadlock.
649729	HA synchronization packets are hashed to a single queue when `sync-packet-balance` is enabled.
700621	The forticron daemon is constantly being restarted.
722273	SA is freed while its timer is still pending, which leads to a kernel crash.
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.
757482	When `fastpath` is disabled, counters in the dashboard are showing 0 bytes TX/RX for a VLAN interface configured on an LACP interface.
778794	Incorrect values in NP7/hyperscale DoS policy anomaly logs. For packet rate-based meter log, the repeated numbers do not reflect the amount of dropped packets for a specific anomaly/attack; for the session counter meter log, the `pps` number is negative.
784169	When a virtual switch member port is set to be an alternate by STP, it should not reply with ARP; otherwise, the connected device will learn the MAC address from the alternate port and send subsequent packets to the alternate port.
795104	A member of an LAG interface is not coming up due to a different actor key.
799487	The debug zone uses over 400 MB of RAM.
799570	High memory usage occurs on FG-200F.
807629	NP7 `dos-offload` triggers an established TCP session to have synproxy process issues.
810137	Scheduled speed test crash is caused by adding the same object to a list twice.
813162	Kernel panic occurs after traffic goes through IPsec VPN tunnel and EMAC VLAN interface.
813607	LACP interfaces are flapping after upgrading to 6.4.9.

Bug ID	Description
815937	FCLF8522P2BTLFTN transceiver is not working after upgrade.
818452	The `ifLastChange` SNMP OID only shows zeros.
819667	1G copper SFP port is always up on FG-260xF.
819724	LTE fails to connect after the firewall reboots. Multiple reboots are required to bring back connectivity.
824543	The `reply-to` option in the email server settings is no longer visible in a default server configuration on FortiOS 7.2.0.
826490	NP7 platforms may reboot unexpectedly when unable to handle kernel null pointer de-reference.
827240	FortiGate in HA may freeze and reboot. Before the reboot, softIRQ may be seen as high. This leads to a kernel panic.
827241	Unable to resolve sp***.saas.ap***.com on a specific VDOM.
833062	FortiGate becomes unresponsive, and there are many WAD and forticron crashes.
840960	When kernel debug level is set to `>=KERN_INFO` on NP6xLite platforms, some tuples missing debug messages may get flooded and cause the system ti get stuck.
841932	The GUI and API stopped working after loading many interfaces due to httpsd stuck in a D state (kernel I/O socket).
845736	After rebooting the FortiGate, the MTU value on the VXLAN interface was changed.
845781	Kernel panic and regular reboots occur on NP7 platforms, which are caused by FortiOS trying to offload a receiving ESP packet from the EMAC VLAN interface and convert to an IPv6 destination address with NAT46 NPU offloaded sessions.
847077	`Can't find xitem. Drop the response.` error appears for DHCPOFFER packets in the DHCP relay debug.
847314	NP7 platforms may encounter random kernel crash after reboot or factory reset.
849186	Unexpected console error appears: `unregister_netdevice: waiting for pim6reg1 to become free. Usage count = 3`.
850683	Console keeps displaying `bcm_nl.nr_request_drop ...` after the FortiGate reboots because of the `cfg-save revert` setting under `config system global`. Affected platforms: FG-10xF and FG-20xF.
850688	FG-20xF system halts if setting `cfg-save` to `revert` under `config system global` and after the `cfg-revert-timeout` occurs.
853144	Network device kernel null pointer is causing a kernel crash.
853794	Issue with the `server_host_key_algorithm` compatibility when using SSH on SolarWinds.
853811	Fortinet 10 GB transceiver LACP flapping when shut/no shut was performed on the interface from the switch side.

Bug ID	Description
854388	Configuring `set src-check disable` is not persistent in the kernel after rebooting for GRE interfaces.
855573	False alarm of the PSU2 occurs with only one installed.
856202	Random reboots and kernel panic on NP7 cluster when the FortiGate sends a TCP RST packet and IP options are missing in the header.
858633	When any 10 Gigabit (SFP+) port is connected a switch, all configurations related to the 10 Gigabit ports is removed (trunks) when traffic is flowing upon boot. Affected platforms: FG-40xF, FG-60xF, FG-300xF.
859717	The FortiGate is only offering the `ssh-ed25519` algorithm for an SSH connection.
860385	IPv6 BGP session drops when passing through a FortiGate configured with VRF.
861144	`execute ping-option interface` cannot specific an interface name of `a`.
868225	After a cold reboot (such as a power outage), traffic interfaces may not come up with a possible loss of VLAN configurations.
869599	Forticron memory is leaking.
870381	Memory corruption or incorrect memory access when processing a bad WQE.
873805	CPSS usage goes to 99% and causes initiation issues when traffic is flowing upon boot. Affected platforms: FG-40xF, FG-60xF, FG-300xF.
877154	FortiGate with new kernel crashes when starting debug flow.
877240	Get `zip conf file failed -1` error message when running a script configuring the FortiGate.
880290	NP7 is not configured properly when the ULL ports are added to LAG interface, which causes accounting on the LAG to not work.

Upgrade

Bug ID	Description
850691	The `endpoint-control fctems` entry `0` is added after upgrading from 6.4 to 7.0.8 when the FortiGate does not have EMS server, which means the `endpoint-control fctems` feature was not enabled previously. This leads to a FortiManager installation failure.
854550	After upgrading to 7.0.8, `replacemsg utm` parameters are not taken over and revert to the default. Affected replacement messages under `config system replacemsg utm`: `virus-html`, `virus-text`, `dlp-html`, `dlp-text`, and `appblk-html`.

User & Authentication

Bug ID	Description
751763	When MAC-based authentication is enabled, multiple RADIUS authentication requests may be sent at the same time. This results in duplicate sessions for the same device.
835859	Incorrect source MAC address is used in LLDP TX packet when the interface has `https` in `allowaccess`.
839801	FortiToken purge in a VDOM clears all FortiToken statuses in the system.
842517	Adding a local user to a group containing many users causes a delay in GUI and CLI due to cmdbsvr (high CPU).
843528	RADIUS MAC authentication using ClearPass is intermittently using old credentials.
851233	FortiToken activation emails should include HTTPS links to documentation instead of HTTP.
853793	FG-81F 802.1X MAC authentication bypass (MAB) failed to authenticate Cisco AP.
872051	When the LDAP server has a huge amount of LDAP groups configured, it might return `LDAP_SIZELIMIT_EXCEEDED` to indicate not all results from SearchResultEntries were returned. The user-info daemon does not handle this error code correctly, and causes a huge amount of LDAP traffic.

VM

Bug ID	Description
740796	IPv6 traffic triggers `<interface>: hw csum failure` message on CLI console.
764392	Incorrect VMDK file size in the OVF file for hw13 and hw15.
856645	Session is not crated over NSX imported object when traffic starts to flow.
859165	Unable to enable FIPS cipher mode on FG-VM-ARM64-AWS.
860096	CPU spike observed on all the cores in a GCP firewall VM.
868698	During a same zone AWS HA failover, moving the secondary IP will cause the EIP to be in a disassociated state.
869359	Azure auto-scale HA shows certificate error for secondary VM.
885829	Azure SDN connector stopped processing when Azure returned `NotFound` error for VMSS interface from an AD DS-managed subscription.

VoIP

Bug ID	Description
757477	PRACK will cause voipd crashes when the following conditions are met: `block-unknown` is disabled in the SIP profile, the PRACK message contains SDP, and PRACK fails to find any related previous transactions (this is not a usual case).

Web Filter

Bug ID	Description
856793	In flow mode, URL filter configuration changes cause a spike in CPU usage of the IPS engine process.

WiFi Controller

Bug ID	Description
807605	FortiOS exhibits segmentation fault on hostapd on the secondary controller configured in HA.
828901	Connectivity loss occurs due to switch and FortiAPs (hostapd crash).
831736	Application hostapd crash found on FG-101F.
834644	A hostapd process crash is shown in device crash logs.
856830	HA FortiGate encounters multiple hostapd crashes.
857084	Console exhibits hostapd segmentation fault with `signal 6:R28: 0000000002b4e120: $d at fgtassert.c:?.`
857140	Hostapd segmentation fault signal 11 occurs upon RF chamber setup.
858653	Invalid wireless MAC OUI detected for a valid client on the network.
865260	Incorrect source IP in the self-originating traffic to RADIUS server.
868022	Wi-Fi clients on a RADIUS MAC MPSK SSID get prematurely de-authenticated by the secondary FortiGate in the HA cluster.
882551	FortiWiFi fails to act as the root mesh AP, and leaf AP does not come online.

ZTNA

Bug ID	Description
832508	The EMS tag name (defined in the EMS server's *Zero Trust Tagging Rules*) format changed in 7.0.8 from `FCTEMS<serial_number>_<tag_name>` to `EMS<id>_ZTNA_<tag_name>`. After upgrading, the EMS tag format was converted properly in the CLI configuration, but the WAD daemon is unable to recognize this new format, so the ZTNA traffic will not match any ZTNA policies with EMS tag name checking enabled.
863057	ZTNA real server address group gets unset once the FortiGate restarts.
865316	Adding an EMS tag on the *Policy & Objects* > *Firewall Policy* edit page for a normal firewall policy forces NAT to be enabled.

Known issues

The following issues have been identified in version 7.0.11. To inquire about a particular bug or report a 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.

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.

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.

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.
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.
827893	Security rating test result incorrectly shows *Failed* for FortiManager Cloud FortiCare support.
843554	The ALL service object is changed when a new object is created.
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.
892207	Unable to authorize a newly discovered FortiAP from the *WiFi Controller* > *Managed FortiAPs* page.

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.
846015	First ICMP redirected from FGSP secondary is dropped on FGSP primary when UTM is enabled.

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.
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.
892699	In an HA cluster, static routes via the IPsec tunnel interface are not inactive in the routing table when the tunnel is down. **Workaround**: in an SD-WAN scenario, a health check for the IPsec tunnel (SD-WAN member) with `update-static-route enable` is required. `config system sdwan` `  config health-check`

Bug ID	Description
	`` edit <name> set server <string> next end end ``` In a non-SD-WAN scenario, a link health monitor configuration is required. ``` config system link-monitor edit <name> set srcintf <IPsec_phase1-interface_name> set server <address> set source-ip <IPsec_tunnel_IP or internal_interface_IP) next end ```

Log & Report

Bug ID	Description
850642	Logs are not seen for traffic passing through the firewall.

Proxy

Bug ID	Description
727629	WAD encounters signal 11 crash.
836101	FortiGate is entering conserve mode due to a WAD memory leak.
837724	WAD crash occurs.

Routing

Bug ID	Description
839784	DHCP relay packets are not being sent out of the WWAN interface.
863318	Application forticron signal 11 (Segmentation fault) occurs.
864626	FortiGate local traffic does not follow SD-WAN rules.
875668	SD-WAN SLA log information has incorrect inbound and outbound bandwidth values.

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.
825291	FortiAnalyzer connection security rating fails for 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.
873313	SSL VPN policy is ignored if no user or user group is set and the FSSO group is set.

Switch Controller

Bug ID	Description
813216	FortiLink goes down when CAPWAP offloading is enabled or disabled.

System

Bug ID	Description
666664	Interface belonging to other VDOMs should be removed from interface list when configuring a GENEVE interface.
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.
812957	When setting the `speed` of 1G SFP ports on FG-180xF platforms to `1000full`, the interface does not come up after rebooting.
847664	Console may display `mce: [Hardware Error]` error message after fresh image burn or reboot.

User & Authentication

Bug ID	Description
679016	A fnbamd crash is caused by the LDAP server being unreachable
765184	RADIUS authentication failover between two servers for high availability does not work as expected.
836082	LLDP packets are not being received if mgmt is used as an HA management reservation interface.

WAN Optimization

Bug ID	Description
728861	HTTP/HTTPS traffic cannot go through when `wanopt` is set to manual mode and an external proxy is used. **Workaround**: set `wanopt` to automatic mode, or `set transparent disable` in the `wanopt profile`.

Web Filter

Bug ID	Description
766126	Block replacement page is not pushed automatically to replace the video content when using a video filter.
829704	Web filter not logging all URLs properly.

WiFi Controller

Bug ID	Description
875382	*Managed FortiAPs* GUI page takes a long time to load.

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.

Built-in AV engine

Resolved engine issues

Bug ID	Description
849020	FortiGate enters conserve mode and the console prints a `fork()` failed message.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
773711	HTTPS sessions to some internal destinations are randomly dropped for users from the same group set.
808961	IPS engine stalled and caused packet drops.
822551	EICAR virus test file HTTPS traffic cannot be blocked, even when there is a block IPS log.
836955	Primary and secondary units of HA cluster are not accessible and drop traffic.
838514	File filter is not consistently blocking files in NGFW policy mode.
838875	Application control `filename` field has unexpected character and breaks the syslog format.
839671	IPS engine is crashing.
847129	IPS engine crashes and FortiGate enters conserve mode. IPS engine stalled and IPS fail-open is triggered.
848003	FG-200E memory is not released and enters conserve mode, even after the traffic stopped.
848368	IPS is causing high memory (FortiOS 6.4.8).
849030	IPS engine libips.so process crashes with signal 11 at `sock_read_stop` on FortiOS 6.4.10.
854254	FG-1200D cannot transmit the push ACK packet.
855301	IPS engine is consuming high memory.
856616	High IPS engine memory usage after device upgrade.
856793	In flow mode, URL filter configuration changes cause a spike in CPU usage of the IPS engine process.
859675	Traffic from an untrusted external IP addresses is not dropped, and presents the server's certificate.
863074	Both `block` and `passthrough` logs are sent out by the web filter override function.
870243	ZIP file block does not work as expected with flow-mode DLP.
872062	Flow-based DNS filter with `safe-search` enabled returns a record of `0.0.0.0` for redirected FQDNs (IPS 7.00149 and later).
873153	URLs longer than 8000 characters are unable to get a FortiGuard rating with flow-based URL filter.
879555	FortiGate is querying the web filtering service over 2.5 billion times per day.

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