FORTINET

Best Practices

FortiManager 7.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
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 LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

March 21, 2024
FortiManager 7.2.0 Best Practices
02-720-0795934-20230421

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-04-11	Initial release.
2022-05-05	Added FortiManager performance and sizing in closed networks on page 26.
2022-06-09	Added Secure password storage on page 10
2022-09-08	Updated VM Size and License on page 25.
2022-09-16	Updated Security Best Practices on page 23.
2022-11-02	Updated Back up the configuration on page 10.
2023-03-01	Updated What to do when an object conflict occurs on page 14.
2024-03-21	Updated Reverting a FortiGate configuration on page 16.

Overview

This guide is a collection of best practices guidelines for using FortiManager. Use these best practices to help you get the most out of your FortiManager products, maximize performance, and avoid potential problems.

Additional information

For product and feature guides, go to the Fortinet Document Library at https://docs.fortinet.com.

For procedures on how to implement these best practices, see the *FortiManager Administration Guide* in the Fortinet Document Library.

For customer service and support, go to https://support.fortinet.com.

For technical notes, how-to articles, FAQs, and links to the technical forum and technical documentation, go to the Fortinet Community at https://community.fortinet.com/.

Installation

Plan your installation carefully and select the FortiManager model(s) that meet your requirements.

- Plan the size of your installation appropriately. Ensure you plan for future management and logging requirements, including consideration for:
  - The number of connected devices.
  - If applicable, log rates and analytic and archive retention periods.
- Ensure you have remote serial console or virtual console access.
- Ensure a local TFTP server is available on a network local to the FortiManager.

Business Continuity

- Set up and use High Availability (HA).
- Ensure there is no power interruption. A power loss could cause the loss of a FortiManager device's database integrity. See Maintain database integrity on page 11.
  - Always shut down or reboot the FortiManager gracefully. Removing power without a graceful shutdown might damage FortiManager databases.
  - Ensure the FortiManager environment has a stable and uninterruptible power supply.
- If an unexpected power loss occurs, revert to a known good backup of the configuration.
- Ensure there are spare parts on site, such as fans, power supplies, and hard disk drives.

Geographic redundancy

In order to increase resiliency, implement geographic redundancy when clustering FortiManager devices. That is, situate your FortiManager devices in locations that are not affected by the same conditions, such as power outages or floods.

In the event that the original primary FortiManager fails, the new primary FortiManager will attempt to contact all of the managed devices after the admin user has promoted the FortiManager to primary AND has issued the `exec fgfm reclaim` command. If any of your managed devices are behind a NAT device, the new primary FortiManager may be unable to connect to the managed devices, depending on whether that NAT is 1-to-1. In the event that FortiManager is unable to initiate a connection to managed devices, you must manually repoint the managed devices to the new primary FortiManager since they only have the IP address for the previous primary FortiManager.

1:1 NAT considerations

Applies to 1:1 NAT with public, static IP addresses; does not apply to 1:1 NAT with public, dynamic IP addresses.

Configure the management address setting on a FortiManager that is behind a NAT device so the FortiGate can use IP port 541 to initiate an FGFM tunnel to the FortiManager.

When a FortiGate is discovered by a FortiManager that is behind a NAT device, the FortiManager does NOT automatically set the IP Address on the FortiGate. This prevents the FortiGate from pointing to the FortiManager's private IP address and initiating the FortiGate-FortiManager (FGFM) tunnel to the FortiManager.

By configuring the management address setting in the CLI, FortiManager knows the public IP and can configure it on the FortiGate.

You can use the CLI to configure the management address when the NAT device in front of the FortiManager has a static 1:1 NAT rule

To configure the management address with the CLI:

```
config system admin setting
   set mgmt-addr "x.x.x.x"
   ** Detail **
```

General Maintenance

Perform general maintenance tasks such as backup and restore so you can revert to a previous configuration if necessary.

Back up the configuration

- Perform regular backups to ensure you have a recent copy of your FortiManager configuration.
- Verify the backup by comparing the checksum in the log entry with that of the backed up file.
- Set up a backup schedule so you always have a recent backup of the configuration.
  See the FortiManager Administration Guide.
- If your FortiManager is a virtual machine, you can also use VM snapshots.

If you use ADOMs, a large number of ADOMs can significantly increase the size of configuration files which increases backup and restore time. See ADOM considerations on page 17.

Secure password storage

Passwords, as well as the private keys used in certificates, are encrypted using a pre-defined private key when stored on the FortiManager, and encoded when displayed in the CLI and configuration file. This ensures that the password cannot be decrypted unless the private key is known, and the password is not displayed in clear text anywhere.

To enhance your password security, you should specify your own private key for the encryption process. This ensures that your key is unique and known only by you. The key is also required on other FortiManagers to restore the system from a configuration file. In HA clusters, the same key should be used on all of the units.

To enable and enter your own private encryption key:

```
config system global
set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
0123456789abcdef0123456789abcdef
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0123456789abcdef0123456789abcdef
Your private data encryption key is accepted.
```

This is an example. Using `0123456789abcdef0123456789abcdef` as your private key is not recommended.

Schedule maintenance tasks for off-peak hours

Fortinet recommends scheduling maintenance tasks for off-peak hours whenever possible, including tasks such as:

- Configuration backup.
- Log deletion (if FortiAnalyzer features are enabled).
- Log rolling and related log upload (if FortiAnalyzer features are enabled).

Maintain database integrity

To maintain database integrity, never power off a FortiManager unit without a graceful shutdown. Removing power without a proper shutdown can damage FortiManager databases.

Always use the following CLI command to shutdown the device before removing power:

```
execute shutdown
```

Fortinet highly recommends connecting FortiManager units to an uninterruptible power supply (UPS) to prevent unexpected power issues that might damage internal databases.

Replace managed device

When you replace a standalone FortiGate device, the usual and recommended method in FortiManager is to use `execute device replace sn`.

When you replace a FortiGate cluster member, you don't need to use `execute device replace sn` because the cluster updates FortiManager about the new cluster member.

If the new cluster member appears in FortiManager as unregistered, delete it from the unregistered device list so that FortiManager can discover the new device as a cluster member.

If the FortiAnalyzer feature set is used and you need to replace a standalone FortiGate device or a cluster member, the best practice is to add the new device as a new member so as to preserve existing logs. Consider adding the old and new FortiGate devices into a group for reporting purposes.

Replace the FortiManager device

If the FortiAnalyzer feature set is enabled and you need to move logs to a new FortiManager device, use log aggregation. If the FortiManager being replaced is the primary, after replacing it, use `execute fgfm reclaim-dev-tunnel` to force FortiGates to connect to the new FortiManager.

Upgrading firmware on managed devices

After a firmware upgrade, the FortiGate configuration may change due to syntax differences between the versions. FortiManager will detect this and perform an auto-retrieve operation to obtain a full copy of the FortiGate's current configuration. See *FortiManager Operations* in the *FortiManager Administration Guide*.

Whenever a retrieve or auto-retrieve operation occurs, the policy package status for that device is automatically flagged as unknown until the next install confirms its status and FortiManager can confirm that the package aligns with what the device database has.

To correct the policy package status after a firmware upgrade, perform an *Install Policy Package*, making sure to check the *Install Preview* carefully prior to completing the install. In many cases, the *Install Preview* will show "Nothing to Install". See Installing policy packages on page 15

Completing the install will correct the policy package status even if no configuration changes are pushed to the FortiGate.

Configuration Management

If there is more than one admin account per ADOM, enable workspace - either normal or workflow to control concurrent operator usage. See Concurrent administrators on page 13.

Use FortiManager to make FortiGate changes, rather than making changes in the FortiGate GUI. If changes will by made in the FortiGate GUI, use *Backup Mode*. See Normal versus Backup Mode on page 13.

When importing policy packages:

- Be careful when handling object conflicts: Choosing the FortiGate value will override the FortiManager value and might affect other FortiGates in that ADOM. See What to do when an object conflict occurs on page 14.
- Include unused objects if you think you might use them in the future: FortiManager will remove unused objects on the FortiGate during the next install. Note that periodic cleanup of unused objects at the ADOM level is recommended. See What to do with unused objects on page 14.
- Download the Import Policy Report if you need a record of the import, including any changes made to objects to resolve object conflicts. See Import report on page 15.

When installing policy packages (see Installing policy packages on page 15):

- Each managed device should only have one policy package associated with it. This reduces the chances of administrative error when installing a policy package.
- When installing a policy package, review the *Install Preview* before completing the install.

Concurrent administrators

To prevent multiple administrators from making changes to the FortiManager database at the same time and causing conflicts, the workspace function should be enabled. This feature requires admin users to lock ADOMs and policy packages and/or objects before making changes to the database.

Normal versus Backup Mode

Once FortiGates are managed by a FortiManager that is operating in Normal Mode, whenever possible, configuration changes should be made on the FortiManager and not the FortiGate.

This is particularly true for changes to policies or objects that affect the *Policies & Objects* pane on the FortiManager. Any such changes made directly on a FortiGate will require manual changes to resynchronize the FortiManager with the FortiGate. Although the *Device Manager* pane will learn about the changes, these changes will be overridden by the next policy package installation, unless the ADOM level *Policy & Objects* have been updated.

If you intend to regularly make changes directly on the FortiGate, and only need FortiManager to act as a configuration repository, it is recommended that you use FortiManager in Backup Mode.

When FortiManager is in Normal Mode, GUI access to managed FortiGates is restricted to Read-Only mode in order to limit the number of changes made directly on the FortiGate. Super_User accounts have the option of switching to Read-Write mode.

Import policy

When using the *Add Device Wizard*, importing policies and related objects to the *Policies & Objects* level is the final step. Such an import can also be separately initiated for a device.

This step ensures that the ADOM database (*Policies & Objects* pane) is populated with the information needed for managing firewall policies on managed devices in that ADOM. It also helps to ensure that interface mapping is properly configured.

During the import, objects being imported may differ from objects of the same name that already exist in that ADOM database.

What to do when an object conflict occurs

The admin user must choose to either keep the FortiManager version of the conflicted object, or replace it with the FortiGate version.

If this is the first device that an import is being performed on in this ADOM, it is reasonable to choose the FortiGate version of the object if the syntax or value of this object is typical for other devices that will be imported.

If other devices have already been imported, choose the FortiManager version of the object so that existing managed devices are not negatively affected.

Shared object conflicts when auto-importing VDOMs

When adding a new FortiGate device and choosing to *automatically import VDOMs*, existing FortiGate devices that share the same objects may become in conflict.
This occurs if there are differences in the shared object's values between FortiGate and the FortiManager, for example when the *Comments* section differs. FortiManager automatically imports the object from FortiGate, overriding the existing object in the FortiManager's database which causes existing devices using that object to display a conflict.
The recommended practice when adding a new FortiGate device with shared objects is to *import each VDOM step by step* in order to override the shared object's values with FortiManager's.

What to do with unused objects

By default, FortiManager will only import objects associated with the policies being imported. The admin user is given the opportunity to import objects not yet associated with policies.

If you anticipate using many of the unassociated objects in future policies, you can chose to import them. Note that importing unused objects will increase the size of the database.

Periodic cleanup of unused objects at the ADOM level is recommended.

Import report

Save a copy of the import report at the end of the import process. Otherwise, these details are not saved for reference purposes. An import policy report may be useful if contacting Fortinet technical support in the future.

Installing policy packages

Each policy package is intended to reflect the complete security policies for one or more managed FortiGates.

The following guidelines are intended to reduce the likelihood of administrative errors when installing configuration changes to FortiGates:

- Each managed device should only have one policy package associated with it. This will help to ensure that the wrong policy package is not mistakenly installed to a FortiGate.
- When installing a policy package, be sure to review the *Install Preview* before completing the installation. This is particularly important during the initial installation of a policy package to a FortiGate.

Consolidated policy package installation

Manually select specific installation targets by selecting *Install On* and perform the installation with the following guidelines:

- For a mix of SD-WAN and non SD-WAN devices, *Install On* must only reference devices with a SD-WAN interface.
- For a mix of FortiWiFi and FortiGate devices, *Install On* must only reference devices with a WiFi interface.

Adding Devices

When initially adding a device to a FortiManager, there are several steps that should be followed before the FortiGate is considered synchronized.

To synchronize FortiGate with FortiManager:

1. Ensure a policy package is assigned to this device using *Import Policy*.

2. Perform an *Install Policy Package* to ensure that FortiGate and FortiManager are properly synchronized.

As a result, the Config Status and Policy Package Status will show as *Synchronized*.

The above procedure does not apply to the Backup Mode.

Ensuring that a FortiGate is synchronized sets a good foundation for future configuration changes to be pushed to the FortiGate.

Reverting a FortiGate configuration

You can use FortiManager to revert the configuration of a FortiGate to a previous revision. The revert operation does not affect the policy package stored in the FortiManager ADOM database.

In order to align the policy information stored in the ADOM database with the reverted FortiGate configuration in the device database, you should perform the following actions after reverting the configuration:

1. Import the configuration from the managed FortiGate to synchronize the policy package stored in the ADOM database.
2. Re-install the policy package from FortiManager.

By importing and reinstalling the policy package, the device database and policies within the ADOM database are synchronized.

For more information, see the following topics in the FortiManager Administration Guide:

- Device database (DB)
- Revert
- Reverting to another configuration file
- Viewing configuration revision history

ADOM Design

Enable ADOMs to support devices other than FortiGates, upgrades of FortiGates not supported by ADOM migration, and upgrading policy package versions. See When to enable ADOMs on page 17.

When upgrading FortiGate versions, if possible, use the same ADOM. See Upgrading the firmware of managed devices on page 17.

Upgrade in the following order:

1. FortiGate.
2. ADOM.
3. Global (if used).

Before upgrading the FortiGate, confirm that the current FortiManager version is compatible with the new FortiGate version. If not, upgrade the FortiManager first.

ADOM revisions (see ADOM revisions on page 18):

- Use for significant changes.
- Implement a deletion policy to limit the number of retained revisions.

Periodically clean up unused objects. See What to do with unused objects on page 14.

For more information, see the *FortiManager Administration Guide*.

ADOM considerations

A large number of ADOMs can significantly increase the size of configuration files which increases backup and restore time. Do not create more ADOMs than your business needs.

When to enable ADOMs

By default, FortiManager manages all FortiGate devices in a common ADOM called the root ADOM.

Some reasons for enabling ADOMs are:

- Support for devices other than FortiGates.
- Organizing devices by administrative group, customer, or geographic location.

Upgrading the firmware of managed devices

Each ADOM has a firmware version associated with it. FortiGates must be running firmware in the same maintenance release to be added to the ADOM.

When you upgrade a FortiGate, it is not necessary to move it to a new ADOM, provided that ADOM upgrade is supported to the next FortiOS version level. Instead, you can upgrade the firmware of that FortiGate to the next higher maintenance release. Once all the FortiGates in an ADOM have been upgraded to the new maintenance release, you can upgrade the ADOM itself.

Using the ADOM upgrade option is recommended in most scenarios because it is much simpler than moving the devices to a new ADOM. Moving devices to a new ADOM requires importing policies for each moved device, and the creation of a new policy package in the new ADOM.

You might decide to move upgraded devices to a new ADOM if you are deploying new devices in the field anyway.

ADOM revisions

It is possible to keep a revision history of changes made at the policy and objects level. However, unlike at the device level, the revision history at this level can significantly increase the overall size of your configuration backup.

Guidelines for use of ADOM revision history:

- Use for significant changes only.
- Implement a deletion policy to limit the number of revisions retained.
- Using the install wizard does not automatically add an ADOM revision.

Log Management

Set up a log management strategy that gives a good balance of redundancy and performance. Retain logs log enough for business requirements and archive older logs for better performance.

This is only applicable when FortiAnalyzer features are enabled. See the *FortiManager Administration Guide* for details.

Set up a log backup strategy

- Set up a backup strategy for logs.
- Set up a schedule to roll and upload logs. You can use the GUI or CLI to set this up. For details, see the *System Settings > Device logs* section in the *FortiManager Administration Guide*.
  - You can also back up logs using the `execute backup logs` command. For details, see the *FortiManager CLI Reference*.

Set up redundancy

- For log storage redundancy, you can set this up at the disk level by selecting an appropriate RAID level.
- For log delivery redundancy, set FortiGates to send log to multiple devices, provided the FortiGate models support this function.

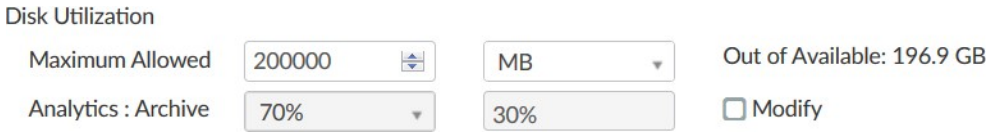
Set disk size and RAID level

Fortinet recommends using the default RAID level specified in the FortiManager data sheet, that is, RAID 50. If your configuration does not meet RAID 50 requirements, consider upgrading your hardware.

When planning for disk space requirements, consider future storage needs. Adding disks to an existing RAID array requires rebuilding the RAID array and restoring backed up logs.

The disk space available for you to set log quotas depends on the RAID level and the reserved space for temporary files. Temporary files are needed for indexing, reporting, and file management. In your planning, include both the disk space for the original logs FortiManager receives (Archive) and the space required to index the logs (Analytics).

Fortinet recommends using the default ratio of *Analytics : Archive* for most deployments. If you plan to retain archive logs for a much longer period than your analytical data, you might allocate a higher percentage to Archive.



If you need more disk space for a VM, add a virtual disk rather than change the size of an existing virtual disk. Use the `execute lvm extend` command to add a virtual disk. See the *FortiManager CLI Reference*.

Set log retention and storage

Determine the logs needed to meet business requirements

Consider carefully which types of logs to store on FortiManager. In some cases, you can be more selective about the type and volume of logs sent from FortiGate to FortiManager. Reducing the type and volume of logs gives FortiManager more resources to process the logs that meet your log storage, forensic, and reporting needs.

Allocate quota and set log retention policy

Ensure your quota settings is sufficient to fulfill your log retention policy. You must keep enough log data to meet your organization's reporting requirements. Configure quota settings and the log retention policy to ensure there is enough time to generate all scheduled reports.

Log View > *Storage Statistics* shows graphs with trends to help you with this planning.

If you are using ADOMs, ensure the quota is sufficient for every ADOM. Allocating insufficient quota to an ADOM might cause the following issues:

- Prevent you from meeting your log retention objective.
- Waste CPU resources enforcing quotas with log deletion and database trims.
- Adversely affect reporting when quota enforcement acts on analytical data before a report is complete.

For analytics, ensure the quota is sufficient and the retention period is long enough to complete all scheduled reports. When reports are generated and the log retention period is past, there is no need to keep analytical data since it can be regenerated from the original archived log data.

It is recommended that archive data be retained for a longer period than the analytic log data. The archive data is needed to regenerate analytic data in the event of a rebuild, such as may occur automatically during firmware upgrade.

Use Fetcher Management for log fetching

To generate a report for a time period not covered by current analytical data:

- Use log fetching (*Fetcher Management*) to fetch archived logs to generate reports.
- Import log data from an external backup to generate reports.

Log fetching simplifies generating reports from log data for the following reasons:

- Log fetching allows you to specify the devices and time periods to be indexed.
- You can pull indexed logs into an ADOM with quota and log retention settings specifically set up to generate report on older logs.
- Log fetching helps to avoid duplications that might occur with importing data from an external backup.

For information on *Fetcher Management* (log fetching) and importing a log file, see the *FortiManager Administration Guide*.

Rebuild SQL database

Some firmware upgrades might change the SQL schema that indexes logs (analytics). If so, FortiManager automatically rebuilds the SQL database. During the rebuild, searching and reporting functions are limited.

You rarely need to manually rebuild an SQL database. If you think there might be problems with the SQL database, contact Customer Service & Support before considering a manual rebuild.

You might consider rebuilding the SQL database in the following situations:

- After moving a device to a new ADOM, you might need to rebuild the SQL database in the new ADOM.
- If disk space is running low, you might rebuild the SQL database to try free up disk space.

Report Performance

This is only applicable when FortiAnalyzer features are enabled. See the *FortiManager Administration Guide* for details.

For reports that you run regularly, set up the following:

- Put those reports into a group.
- Schedule those reports. If possible, schedule reports to run at off-peak hours and do not schedule reports to run at the same time as log maintenance tasks.
- Enable auto-cache for those reports.

Grouping reports has these advantages:

- Reduce the number of *hcache* tables.
- Improve *auto-cache* completion time.
- Improve report performance and reduce report completion time.

Consider grouping reports in these conditions:

- If you use the same or a similar report template for different FortiGates in the same ADOM.
- If you regularly use different filters on your reports.

Other ways to improve report performance include:

- Avoid running reports at the same time as log aggregation or log transfer.
- Avoid queries to external sources such as DNS (for name resolution) or LDAP (for obtaining a user list).

For more information, see the *FortiManager Administration Guide*.

Security Best Practices

For stronger security, implement the following security best practices.

Administrator access best practices

- Enable password policy and set requirements for the administrator password. The password policy lets you specify the administrator's password minimum length, type of characters it must contain, and the number of days to password expiry.
- Use CLI commands to configure the administrator's password lockout and retry attempts.
  For example, to set the lockout duration to two attempts and set a two minute duration before the administrator can log in again, enter the following CLI commands:

```
config system global
   set admin-lockout-threshold 2
   set admin-lockout-duration 120
end
```

- Set a lower idle timeout so that unattended workstations are logged out.
- Use multi-factor authentication and RADIUS authentication for administrators. For more information, see the *FortiAuthenticator Administration Guide* in the Fortinet Document Library.
- Limit administrator access. For example, configure trusted hosts and allowaccess.

Encryption best practices

Set a strong encryption level. Use the SSL protocol version (TLS version) that meets PCI compliance or your organization's security requirements. For example:

```
config system global
   set enc-algorithm high
   set fgfm-ssl-protocol tlsv1.2
   set oftp-ssl-protocol tlsv1.2
   set ssl-protocol tlsv1.2
   set webservice-proto tlsv1.2
   set ssl-low-encryption disable
end

config fmupdate fds-setting
   set fds-ssl-protocol tlsv1.2
end
```

The `enc-algorithm` setting allows you to specify the security levels for cipher suites.

- `set enc-algorithm low` uses all OpenSSL ciphers.
- `set enc-algorithm medium` uses high and medium OpenSSL ciphers.
- `set enc-algorithm high` (default) uses only high OpenSSL ciphers.

Other security best practices

- Disable unused interfaces.
- Upgrade firmware to the latest version.
- Install physical devices in a restricted area.
- Place the FortiManager behind a firewall, such as a FortiGate, to limit attempts to access the FortiManager device.

When FortiManager is behind a FortiGate, AV and IPS features can be enabled on the FortiGate to further protect FortiManager from malware or intrusion attacks. See the FortiGate Administration Guide.

If the firewall in front of the FortiManager is NATing the traffic, configure the FortiManager with the dedicated public IP (see the following Fortinet Community article). This ensures that FortiGate devices are able to initiate communications (FGFM tunnels) to the FortiManager.

- Set up NTP. For example:

```
config system ntp
   set status enable
   set sync_interval 60
   config ntpserver
      edit 1
         set server {<address_ipv4> | <fqdn_str>}
      end
   end
end
```

- For audit purposes:
  - Use named accounts wherever possible.
  - Send logs to a central log destination, like FortiAnalyzer.

Do not lose the administrator log in information as there is no password recovery mechanism in FortiManager 5.4.0 and later.

VM Size and License

When using VMs, implement the following:

- Allocate sufficient CPU and memory resources to all VMs based on the number of devices and enabled features.
- Ensure the VM license meets your requirements for daily log rate (GB/day) and log storage capacity.

It is not possible to increase FortiManager's logging capabilities past what is included in the base license. For additional logging, see FortiAnalyzer.

For details, see *FortiManager Private Cloud*.

FortiManager performance and sizing in closed networks

Here you can find best practice information about sizing a FortiManager that is acting as a FortiGuard Distribution Server (FDS) in closed networks.

When operating in a closed network, FortiGate devices are not connected to the Internet. This is a protective measure that adds security, but it means that FortiGate devices cannot retrieve updates directly from FortiGuard. FortiGate devices can instead get the latest FortiGuard updates through an Internet connected FortiManager acting as a FDS. When FortiManager is acting is as a FDS, it will process the updates for AV/IPS, Web Filtering database, and license checks.

A closed network configuration with a FortiManager FDS can be set up in either a cascade or air-gapped mode.

Network design and process

In the examples below, the following scenario is used:

- 24 x FortiGate 1800F devices across four data centers.
- One FortiManager cluster per data center.
- FortiGates use FortiManagers as the FDS for AV/IPS, license checks, and the Web Filtering database.

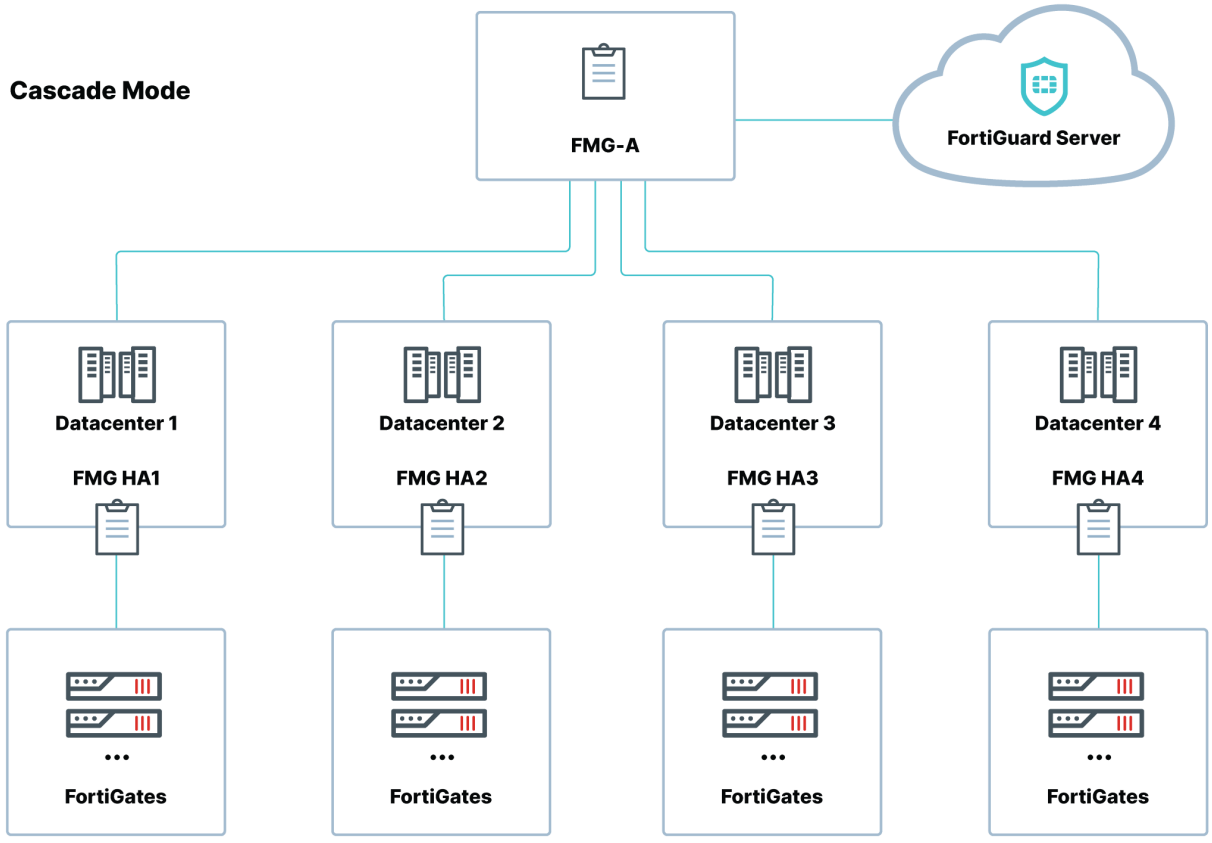
Two network design modes are demonstrated:

- Cascade mode on page 26
- Air gap mode on page 27

Cascade mode

Design:

The following topology diagram demonstrates the network design using cascade mode where FortiManager-A is connected to the Internet, and FortiManager HA 1-4 are not connected to the Internet. The FortiManager HA 1-4 clusters override to use FortiManager-A as the FDS to download package and database updates, and provide update and rating services to FortiGate devices.



- FMG HA 1-4 connected with FMG-A
- FMG HA 1-4 override to FMG-A download pkg/DB

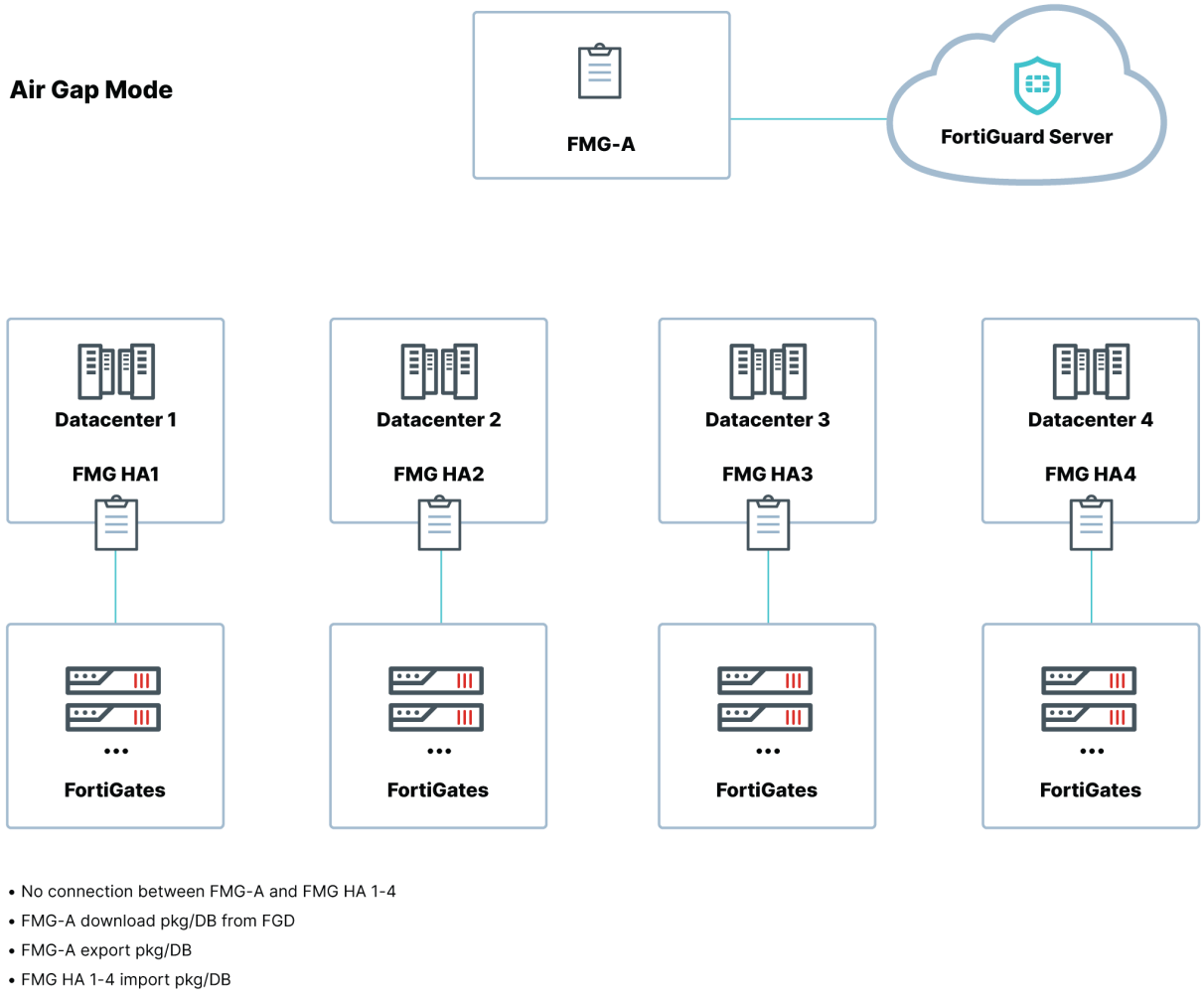
Process:

1. FortiManager-A connects to the FDS to download AV/IPS packages, contracts, and Web Filtering database.
2. FortiManager HA 1-4 have no Internet (FGD) access and override to use FortiManager-A to download the packages and database updates.
3. FortiManager HA 1-4 provide update and rating services to the FortiGates.

Air gap mode

Design:

The following topology diagram demonstrates the network design using air-gap mode where there is no connection between FortiManager-A and the FortiManager HA 1-4 clusters. The FortiGuard update package must be imported on each FortiManager cluster using an internal-access only FTP server.



Process:

1. In an air-gaped deployment mode, there is no connection between FortiManager-A and the FortiManager clusters.
2. FortiManager-A downloads the updates from FortiGuard.
3. FortiManager-A exports the downloaded packages.
4. The FortiManager cluster imports the packages. This process must use an internal-access only FTP server.

Performance testing

The performance testing below was done using FortiManager and FortiOS devices running versions 7.0.0 or later.

Web Filtering performance test case and results:

In a closed network, FortiManager will need to download the Web Filtering database and upgrade it in memory. The current Web Filtering database size is 7.5 GB, so the FortiManager will need (2 x 7.5 GB) + (8 GB) system memory, which is a minimum of 23 GB.

Some FortiManager units which do not meet the memory requirements, such as FortiManager 300E which includes 8GB of memory, cannot be used for this purpose.

FortiManager Platform	CPU	Memory	Cache	CPU usage	Max URL rating/s	CPU	Loss Rate <%
FMG3900E	24	128G	7G	70.00%	90k	64-bit	0.0200
FMG3000F	32	64G	7G	45.00%	80k	64-bit	0.0200
FMG3700F	40	386G	7G	72.00%	90k	64-bit	0.023
FMG3000G	32	128G	7.3G	74%	90k	64-bit	0.01

AV/IPS performance test case and results:

FortiManager has no concurrent connection limitation, and the bottleneck for FortiGate updates from FortiManager is based on the available bandwidth for the network interface and the number of FDS workers configured to process download requests on the FortiManager.

The following scenarios demonstrate how various configurations of FDS workers and network ports affect the update time per FortiGate device as well as the FortiManager CPU usage.

The following performance testing was completed on a FortiManager-3000G with a 32-bit CPU, 128 GB of memory, and running version 7.0.2.

The update package size used to calculate CPU usage below is based on the first time update to download the full AV/IPS package.

Scenario 1

Number of FortiGates	Update Time Per FortiGate	FortiManager CPU Usage		Network Bandwidth (port2 1Gbps)	Max Concurrent Connections	Update Package Size
		FortiGuard Update Service Daemon	FDS Worker=1			
1000	14 minutes	< 1%	98%	960M	1000	110M

In the first scenario, there are 1000 FortiGate devices, one FDS worker is configured to process download requests on FortiManager, and *port2* is used which supports speeds up to 1 Gbps. In this example, each FortiGate takes approximately 14 minutes to update, and the process uses 98% of the CPU on the FortiManager. With only one FDS worker and limited network bandwidth over *port2*, the AV/IPS update process becomes resource intensive on the FortiManager. Additional resources are recommended.

Scenario 2

Number of FortiGates	Update Time Per FortiGate	FortiManager CPU Usage		Network Bandwidth (port4 25Gbps)	Max Concurrent Connections	Update Package Size
		FortiGuard Update Service Daemon	FDS Worker=10			
1000	4 - 20 seconds	< 1%	15%	20G	1000	110M

In the second scenario, the number of supported FortiGates remain the same, but by changing the number of available FDS workers to 10 and using *port4* which supports speeds up to 25 Gbps, each FortiGate is updated in only 4 to 20 seconds instead of 14 minutes, and the FortiManager CPU usage is 15% instead of 98%. The FortiManager in this scenario is suitably configured to support the AV/IPS updates for the number of FortiGates in the closed network.

By increasing the available FDS workers and choosing a network port that supports greater speeds, the load on the FortiManager CPU and the time to update each FortiGate is reduced.

Scenario 3

Number of FortiGates	Update Time Per FortiGate	FortiManager CPU Usage		Network Bandwidth (port4 25Gbps)	Max Concurrent Connections	Update Package Size
		FortiGuard Update Service Daemon	FDS Worker=10			
3000	100 - 120 seconds	< 10%	50-95%	20G	3000	110M

The third scenario uses the same port and number of FDS workers that are used in the second scenario but the number of FortiGate devices has been increased to 3000. The update time per FortiGate is increased to 100 - 120 seconds, and the FortiManager CPU usage is increased to between 50 and 95%.

As the number of supported FortiGate devices increases, the CPU usage and total time to update each FortiGate also increase.

To set the maximum number of FDS workers:

```
config fmupdate fds-setting
   set max-work {1-32}
end
```

`max-work` = The maximum number of worker processing download requests (1 - 32, default = 1).

Conclusion

The following table provides recommendations about the FDS worker settings that should be configured based on the number of FortiGate devices in your environment. You can see the expected CPU usage and time to update each FortiGate device based on the recommended settings.

Number of FortiGate	Recommended number of FDS workers	CPU Usage	Time to update all FortiGate devices
1 - 50 devices	Use default setting (1 FDS Worker)	20 - 50%	30 seconds
50 - 1000 devices	Change max-worker to 10	50 - 90%	1 minute
1000 - 3000 devices	Change max-worker to 24	50 - 90%	5 minutes
3000 + devices	Keep the max-worker set to 24. While you can configure the FDS worker setting up to 32, there is no benefit to CPU load beyond 24 in this scenario.	-	-

www.fortinet.com