FortiOS - Best Practices

Version 6.0.4

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 COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdocs@fortinet.com

April 8, 2019
FortiOS 6.0.4 Best Practices
01-604-481057-20190408

TABLE OF CONTENTS

Best practices

This FortiGate Best Practices document is a collection of guidelines to ensure the most secure and reliable operation of FortiGate units in a customer environment. It is updated periodically as new issues are identified.

General considerations

1. For security purposes, NAT mode is preferred because all of the internal or DMZ networks can have secure private addresses. NAT mode policies use network address translation to hide the addresses in a more secure zone from users in a less secure zone.
2. Use virtual domains (VDOMs) to group related interfaces or VLAN subinterfaces. Using VDOMs will partition networks and create added security by limiting the scope of threats.
3. Use transparent mode when a network is complex and does not allow for changes in the IP addressing scheme.

Customer service and technical support

For antivirus and IPS updates, firmware updates, updated product documentation, technical support information, and other resources, visit the Fortinet Support website at https://support.fortinet.com. You can also register Fortinet products and service contracts and change your registration information at any time.

When requesting technical support, for optimum results you should provide as much of the following information as possible:

- Your name, and your company's name and location
- Your email address and/or telephone number
- Your support contract number (if applicable)
- The product name and model number
- The product serial number (if applicable)
- The software or firmware version number
- A detailed description of the problem

Fortinet Knowledge Base

The most recent Fortinet technical documentation is available from the Fortinet Knowledge Base. The knowledge base contains short how-to articles, FAQs, technical notes, product and feature guides, and much more. Visit the Fortinet Knowledge Base at http://kb.fortinet.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

System and performance

By implementing the following best practices for system and performance, you will ensure maximum efficiency of your FortiGate device. Be sure to read everything carefully, particularly the section that concerns shutting down the FortiGate system, in order to avoid potential hardware issues.

Performance

- Disable any management features you do not need. If you don't need SSH or SNMP, disable them. SSH also provides another possibility for would-be hackers to infiltrate your FortiGate unit.
- Put the most used firewall rules to the top of the interface list.
- Log only necessary traffic. The writing of logs, especially if to an internal hard disk, slows down performance.
- Enable only the required application inspections.
- Keep alert systems to a minimum. If you send logs to a syslog server, you may not need SNMP or email alerts, making for redundant processing.
- Establish scheduled FortiGuard updates at a reasonable rate. Daily updates occurring every 4-5 hours are sufficient for most situations. In more heavy-traffic situations, schedule updates for the evening when more bandwidth can be available.
- Keep security profiles to a minimum. If you do not need a profile on a firewall rule, do not include it.
- Keep VDOMs to a minimum. On low-end FortiGate units, avoid using them if possible.
- Avoid traffic shaping if you need maximum performance. Traffic shaping, by definition, slows down traffic.

Shutting down

Always shut down the FortiGate operating system properly before turning off the power switch to avoid potentially catastrophic hardware problems.

To power off the FortiGate unit - GUI:

1. Go to **Dashboard**.
2. In the **System Resources** widget, select **Shutdown**.

To power off the FortiGate unit – CLI:

```
execute shutdown
```

Once this has been done, you can safely turn off the power switch or disconnect the power cables from the power supply.

Migration

Network administrators are often reluctant to change firewall vendors due to the perception that the migration process is difficult. Indeed, there is no point hiding the fact that moving to a new vendor requires careful consideration. But concern over the potential pain of migration should not stand in the way of adopting new security technologies. The purpose of this chapter is to describe the best practices for performing such migrations and ultimately to ease the migration process itself.

Information gathering

It is always best practice to perform a full network audit prior to any migration. This should include:

- Full back up of all security systems (including switches, routers) in case a back-out needs to be performed.
- Physical and logical network diagram with visual audit

Understanding exactly where cables run in the network and verifying they are all correctly labeled is essential to avoid mistakes and unnecessary downtime during the upgrade. Don't overlook simple things such as:

- Do I have enough spare interfaces on my switches?
- Do I have the right fiber (single/multi mode) and right connectors (LC, FC, MTRJ, SC, ST)?
- Do I have spare cables? (in the heat of the moment, it is a simple mistake to break an RJ-45 connector or damage a fiber)
- Do I have space in the rack for the new equipment?
- Do I have enough power sockets?

No matter how securely a FortiGate is configured in the network, it cannot help if it has been bypassed; visually checking where the device sits in the network in relation to other devices will ensure you are maintaining security and verify the network diagram is 'as built'. Details of all networks including subnet masks should be documented at this point to ensure that the replacement device is configured with the correct information.

Object and policy migration

Whilst we have suggested some level of manual review is included in the policy migration, it can be useful to be able to automatically migrate simply between another vendor's format and the FortiGate format. The FortiGate policy format is text based and can easily be cut and pasted into from other vendor formats however, responding to the high customer demand to migrate away from other vendors, Fortinet have released an automatic configuration migration tool at http://convert.fortinet.com to simplify this process. Supporting Cisco ACLs, PIX, ASA, Check Point, and Juniper, the Converter can securely upload and convert the policy into the Fortinet format.

Testing and validation

This is an important process and should be tested offline first wherever possible i.e. configure the policy in the lab or on a test network and verify that the required access permissions are being implemented. To really test the solution out, the FortiGate can be implemented on the live network with a different gateway IP and the selected user pointed to the new gateway. This allows a staged approach to migrating the new platform into the network ensuring that the process does not interrupt day to day operations.

Going live and obtaining feedback

If testing and validation is successful at this point, you can migrate to the new firewall either by switching IP's and removing the old devices or by changing the default gateway in DHCP. Once the firewall is in place, acceptance testing will of course need to be carried out and an iterative process of tuning undertaken to finalize the configuration.

Adding new services

The Fortinet solution will have a plethora of additional features compared to your previous vendor and it is very tempting to start switching them on but it is a good idea to wait and validate the new firewall as was previously configured before adding new functions as this simplifies testing and problem diagnosis. Finally complete the migration (don’t forget about the Plan Do Check Act Cycle) by adding any new services that were requested and learn about the multiple features you have available with the FortiGate appliance.

Environmental specifications

Keep the following environmental specifications in mind when installing and setting up your FortiGate unit.

- Operating temperature: 32 to 104°F (0 to 40°C). Temperatures may vary, depending on the FortiGate model.
- If you install the FortiGate unit in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient temperature.Therefore, make sure to install the equipment in an environment compatible with the manufacturer's maximum rated ambient temperature.
- Storage temperature: -13 to 158°F (-25 to 70°C). Temperatures may vary, depending on the FortiGate model.
- Humidity: 5 to 90% non-condensing.
- Air flow - For rack installation, make sure that the amount of air flow required for safe operation of the equipment is not compromised.
- For free-standing installation, make sure that the appliance has at least 1.5 in. (3.75 cm) of clearance on each side to allow for adequate air flow and cooling.

Depending on your device, the FortiGate may generate, use, and even radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Explosion is a serious risk if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions. To reduce the risk of fire, use only No. 26 AWG or larger UL Listed or CSA Certified Telecommunication Line Cord.

Grounding

- Ensure the FortiGate unit is connected and properly grounded to a lightning and surge protector. WAN or LAN connections that enter the premises from outside the building should be connected to an Ethernet CAT5 (10/100 Mb/s) surge protector.
- Shielded Twisted Pair (STP) Ethernet cables should be used whenever possible rather than Unshielded Twisted Pair (UTP).
- Do not connect or disconnect cables during lightning activity to avoid damage to the FortiGate unit or personal injury.

Rack mounting

- **Elevated Operating Ambient** - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tmax) specified by the manufacturer.
- **Reduced Air Flow** - Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- **Mechanical Loading** - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- **Circuit Overloading** - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Earthing** - Reliable earthing of rack-mounted equipment should be maintained.

Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

Firmware

Firmware upgrading and downgrading sounds pretty simple, anyone can do it, right? The mark of a professional is not that they can do something correctly, or even do it correctly over and over again. A professional works in such a way that, if anything goes wrong they are prepared and able to quickly get things back to normal. Firmware updates can go wrong just like anything else. So a real professional does things in a way that minimizes their risk and follows some best practices, as listed below.

Firmware change management

Consider the following five points when performing firmware upgrades, not only in FortiOS but in general. This applies to pretty much any change you have to do in a production environment.

Understanding the new version first

Before attempting any changes in production, first make sure you set up a laboratory where you can freely play with the new features, and understand them with enough time and no pressure. Read the Release Notes, Manuals, and other documentation like presentations, videos, or podcasts about the new version.

You are ready to explain the need for an upgrade once you understand:

- The differences and the enhancements between the new version and the previous version(s).
- The impact of the upgrade on customers and the users of the operating platform.
- The known limitations that might affect your environment.
- The potential risks when performing the upgrade.
- The licensing changes that may apply.

Never attempt to upgrade to a version you don't fully understand (both on features and known limitations), and on which you have no operational experience.

Have a valid reason to upgrade

The reason can NOT be “Because I want to have the latest version”. The reason has to be explained in terms of business, technical, and/or operational improvement.

Affirmative answers to the following questions are valid reasons to upgrade:

- Does the new version have a feature that helps to ensure compliance?
- Does the new version have an enhancement that allows 40% decrease (40% improvement) on the time to perform a certain operation?
- Does the new feature correct a known defect/bug found on a previous version that affects the company business/operations?

- Will the new version allow your organization to deploy new services that will help to gain new customers or increase loyalty of existing ones?
- Is the vendor cutting support for the version your organization is currently using?

If the best reason to upgrade is “Because the new features seem to be cool” or “Because I want to have the latest version”, a little more understanding and planning may be necessary.

Prepare an upgrade plan

If you choose to upgrade because you found a valid reason to do so, make sure you create a plan that covers business, technical, and operational aspects of the upgrade:

Business:

Proper planning and justification for an upgrade should be proportional to how critical the system is to the business.

- Make sure you can clearly articulate the benefits of the upgrade in business terms (time, money, and efficiency).
- Understand the business processes that will be affected by the change.
- Make sure the upgrade maintenance window is not close to a business-critical process (such as quarterly or monthly business closure).
- Obtain executive and operational approval for the maintenance window. The approval must come from the owners of ALL the systems/information affected by the upgrade, not only from those that own the system being upgraded. The approval must be done in a formal (written or e-mail) form.

Technical and operational:

- Re-read the Release Notes for the technology you are upgrading. Supported hardware models, upgrade paths, and known limitations should be clearly understood.
- Make sure your upgrade maintenance window does not overlap with any other maintenance window on your infrastructure.
- If you have any premium support offer (such as TAM, Premium Support), do a capacity planning exercise to ensure the new firmware/software version does not take more hardware resources than you currently have.
- Create a backup, whether or not you have scheduled backups. Create a new fresh backup.
- Obtain offline copies of both the currently installed firmware and the new version.
- Create a list of systems with inter-dependencies to the system you are upgrading. For example, if you are upgrading a FortiGate; understand the impact on any FortiAP, FortiAuthenticator, FortiToken, FortiManager, or FortiAnalyzer you have on your environment.
- Ensure you have a list of adjacent devices to the upgrading platform and have administrative access to them, just in case you need to do some troubleshooting. Are you upgrading FortiWeb? Make sure you can administratively access the Web Applications. Are you upgrading a FortiGate? Make sure you can administratively access the surrounding switches and routers.
- Have a step-by-step plan on how to perform and test the upgrade. You want to make sure you think of the worst situation before it happens, and have predefined courses of action, instead of thinking under pressure when something already went wrong.
- Define a set of tests (that include critical business applications that should be working) to make sure the upgrade went fine. If any test does not go well, define which ones mandate a rollback and which ones can be tolerated for further troubleshooting. This set of tests should be run before and after the upgrade to compare results, and they should be the same.

- Define a clear rollback plan. If something goes wrong with the upgrade or the tests, the rollback plan will help you get your environment back to a known and operational status. The plan must clearly state the conditions under which the rollback will be started.
- Declare configuration freezes. A little bit before and after the upgrade. The idea is to reduce the amount of variables to take into consideration if something goes wrong.
- Perform a “Quality Assurance” upgrade. Grab a copy of the production configuration, load it on a non-production box and execute the upgrade there to see if there are any issues on the process. Then adjust your plan according to the results you obtained.
- Have a list of information elements to be gathered if something goes wrong. This ensures that, even if the upgrade fails, you will collect enough information so you can troubleshoot the issue without needing to repeat the problem. Get help from Fortinet Support if you need to check what else could be missing on your list.
- Define a test monitoring period after the change was completed. Even if the upgrade went smoothly, something could still go wrong. Make sure you monitor the upgraded system for at least one business cycle. Business cycles may be a week, a month, or a quarter, depending on your organization’s business priorities.

Execute the upgrade plan

Execution of an upgrade is just as key as planning.

Once you are performing the upgrade, the pressure will rise and stress might peak. This is why you should stick to the plan you created with a cool head.

Resist the temptation to take decisions while performing the upgrade, as your judgment will be clouded by the stress of the moment, even if a new decision seems to be “obvious” at such time. If your plan says you should rollback, then execute the rollback despite the potential “We-can-fix-this-very-quickly” mentality.

While performing the upgrade, make sure all the involved components are permanently monitored before, during, and after the upgrade, either via monitoring systems, SNMP alerts, or at least with tools like a ping. Critical resources like CPU, memory, network, and/or disk utilization must also be constantly monitored.

To avoid misunderstandings, when performing the tests for each critical application defined on the planning, make sure there are formal notifications on the results for each user area, service, system, and/or application tested.

Regardless if you have to rollback or not, if a problem occurs, make sure you gather as much information about the problem as possible, so you can later place a Support ticket to find a solution.

Last but not least, document the upgrade:

- Enable your terminal emulation program to leave trace of all the commands executed and all the output generated. If you are performing steps via GUI, consider using a video capture tool to document it.
- Document any command or change performed over the adjacent/interdependent systems. Make sure they are acknowledged by the relevant administrators
- Document any deviations performed over the upgrade plan. This is planned-versus-actual.

Learn more about change management

Change Management and Change Control are huge knowledge areas in the field of Information Systems and Computer/Network Security.

This document is by no means a comprehensive list on what you should do when performing an upgrade, with either Fortinet or any other technology. It is merely a list of important things you should take into consideration when

performing upgrades which are the result of years of experience dealing with changes on critical environments, as it is common that security devices are protecting critical applications and processes.

There are vast resources on the topic: books, public white papers, blog entries, etc. If you search the Internet for the “Change Control Best Practices” or “Change Management Best Practices” you will get many interesting documents.

Changes on production IT infrastructure are critical to the business. Make sure they play in your favor and not against you.

Performing a firmware upgrade

Upgrading a firewall is something that should be compared to upgrading the operating system on your computer. It’s not to be taken lightly! You want to make sure everything is backed up and you have some options available if things go awry. Assuming it all seems to work you also want a list of things to do in order to confirm everything is working properly. Finally, you need enough time to do it. All really simple stuff, but what does this mean in relation to upgrading your FortiGate? It means, you follow these simple steps:

1. **Backup and store old configuration (full configuration backup from CLI).**
   Digging into this a little, step 1 is easy to understand. Do a full backup of your old configuration. This is all part of your disaster recovery plan. If the upgrade fails in some way you need to make sure you can get the Firewall back up and running. The best way to do this is to get it back to a state where you know what the behavior was. For more information, refer to Performing a configuration backup on page 17.
2. **Have copy of old firmware available.**
   Step 2, is also part of your disaster recovery. If the upgrade fails you might be able to switch the active partition. But as a Professional, you need to be prepared for the worst case scenario where you can’t do that. Which means you’ll need your old firmware.
3. **Have disaster recovery option on standby -- especially if remote.**
   Step 3, is your plan for what to do in the event of a critical failure. As we’re talking FortiGate this means that your firewall doesn’t come back after the upgrade. What this means is that you need to be able to get to the console port in order to find out why. Maybe it’s DHCP and the IP changed, maybe the OS is corrupt, who knows? Get to the console and find out.
   There could be a simple fix. If there’s not, then be prepared for a format and TFTP reload.
4. **Read the release notes, including the upgrade path and bug information.**
   Step 4, READ THE RELEASE NOTES. They contain all kinds of information, known bugs, fixed bugs even upgrade issues like lost configuration settings. Not all upgrade information is ever contained in any products release notes. That does not mean they are devoid of good/useful information. Read them, digest them, then a few days later read them again.
5. **Double check everything.**
   Step 5, do a double check of everything. Is your TFTP server working, does your console connection function, is there anything in the release notes that could impact your upgrade procedure, do you have your configuration backed up? Make sure you’ve done everything.
6. **Upgrade.**
   Step 6, do the upgrade. Doing an upgrade doesn’t take very long, a few minutes (less a lot of times) but make sure you schedule enough time for it. At the end of the day an upgrade can succeed or fail. If it succeeds you want some

time to check/confirm that any important features you have are working (VPNs etc). If it fails you'll need time to sort things out.

Performing a firmware downgrade

Just like upgrading, you need to make sure it's done properly. While similar, the steps are somewhat different since there are other pitfalls in this case.

1. **Locate pre-upgrade configuration file.**
   Step 1 is very important. This is why, when you upgrade you make a backup of your old configuration and save it. If you don't, then you'll need to rebuild manually.
2. **Have copy of old firmware available.**
   Step 2 is fairly obvious. Even with devices that have multiple partitions and your downgrade process is simply going to be to switch the active partition, this could go wrong. In which case, you may be without Internet access. A professional has a plan for when things go wrong.
3. **Have disaster recovery option on standby -- especially if remote.**
   Step 3 is no different from before. Hopefully you don't need to format the unit, but be prepared for that, just in case.
4. **Read the release notes -- is a downgrade possible, or necessary?**
   Step 4, once again, is to READ THE RELEASE NOTES. In this case, you will need to do this for the version you are on, and the version you are downgrading too, and everything in between (if you are going back multiple major releases or patches). Maybe the OS switched from 32 to 64 bits somewhere between the two firmware releases. In order to make sure you don't get nailed by something like that you need to check the upgrade and downgrade information in every major release and patch, as it may have a direct impact on your options.
5. **Double check everything.**
6. **Downgrade -- all settings, except those needed for access, are lost.**
   Step 5 and 6 are the same as before. Double check everything, then downgrade.
7. **Restore pre-upgrade configuration.**
   Step 7 is new. Obviously most settings are lost when you downgrade so in order to get back up and running you will need to restore your old configuration file.

Performing a configuration backup

Once you configure the FortiGate unit and it is working correctly, it is extremely important that you backup the configuration. In some cases, you may need to reset the FortiGate unit to factory defaults or perform a TFTP upload of the firmware, which will erase the existing configuration. In these instances, the configuration on the device will have to be recreated, unless a backup can be used to restore it.

It is also recommended that once any further changes are made that you backup the configuration immediately, to ensure you have the most current configuration available. Also, ensure you backup the configuration before upgrading the FortiGate unit's firmware. Should anything happen during the upgrade that changes the configuration, you can easily restore the saved configuration.

Always backup the configuration and store it on the management computer or off-site. You have the option to save the configuration file to various locations including the local PC, USB key, FTP and TFTP site.The latter two are configurable through the CLI only.

If you have VDOMs, you can back up the configuration of the entire FortiGate unit or only a specific VDOM. Note that if you are using FortiManager or FortiCloud, full backups are performed and the option to backup individual VDOMs will not appear.

To back up the FortiGate configuration - GUI:

1. Go to **Dashboard**.
2. On the **System Information** widget, select **Backup** next to **System Configuration**.
3. Select to backup to your **Local PC** or to a **USB Disk**.
   The **USB Disk** option will be grayed out if no USB drive is inserted in the USB port. You can also backup to the FortiManager using the CLI.
4. If VDOMs are enabled, select to backup the entire FortiGate configuration (**Full Config**) or only a specific VDOM configuration (**VDOM Config**).
5. If backing up a VDOM configuration, select the VDOM name from the list.
6. Select **Encrypt configuration file**.
   Encryption must be enabled on the backup file to back up VPN certificates.
7. Enter a password and enter it again to confirm it. You will need this password to restore the file.
8. Select **Backup**.
9. The web browser will prompt you for a location to save the configuration file. The configuration file will have a .conf extension.

To back up the FortiGate configuration - CLI:

```
execute backup config management-station <comment>
```

… or …

```
execute backup config usb <backup_filename> [<backup_password>]
```

… or for FTP (note that port number, username are optional depending on the FTP site)…

```
execute backup config ftp <backup_filename> <ftp_server> [<port>] [<user_name>] [<password>]
```

… or for TFTP …

```
execute backup config tftp <backup_filename> <tftp_servers> <password>
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config vdom
   edit <vdom_name>
```

Backing up a configuration file using SCP

You can use secure copy protocol (SCP) to download the configuration file from the FortiGate unit as an alternative method of backing up the configuration file or an individual VDOM configuration file. This is done by enabling SCP for and administrator account and enabling SSH on a port used by the SCP client application to connect to the FortiGate unit. SCP is enabled using the CLI commands:

```
config system global
   set admin-scp enable
end
```

Use the same commands to backup a VDOM configuration by first entering the commands:

```
config global
   set admin-scp enable
end
config vdom
   edit <vdom_name>
```

Security Profiles (AV, Web Filtering etc.)

Infection can come from many sources and have many different effects. Because of this, there is no single means to effectively protect your network. Instead, you can best protect your network with the various UTM tools your FortiGate unit offers.

Firewall

- Be careful when disabling or deleting firewall settings. Changes that you make to the firewall configuration using the GUI or CLI are saved and activated immediately.
- Arrange firewall policies in the policy list from more specific to more general. The firewall searches for a matching policy starting from the top of the policy list and working down. For example, a very general policy matches all connection attempts. When you create exceptions to a general policy, you must add them to the policy list above the general policy.
- Avoid using the All selection for the source and destination addresses. Use addresses or address groups.
- If you remove all policies from the firewall, there are no policy matches and all connections are dropped.
- If possible, avoid port ranges on services for security reasons.
- The settings for a firewall policy should be as specific as possible. Do not use 0.0.0.0 as an address. Do not use Any as a service. Use subnets or specific IP addresses for source and destination addresses and use individual services or service groups.
- Use a 32-bit subnet mask when creating a single host address (for example, 255.255.255.255).
- Use logging on a policy only when necessary and be aware of the performance impact. For example, you may want to log all dropped connections but can choose to use this sparingly by sampling traffic data rather than have it continually storing log information you may not use.
- It is possible to use security policies based on 'any' interface. However, for better granularity and stricter security, explicit interfaces are recommended.
- Use the comment field to input management data, for example: who requested the rule, who authorized it, etc.
- Avoid FQDN addresses if possible, unless they are internal. It can cause a performance impact on DNS queries and security impact from DNS spoofing.
- For non vlan interfaces, use zones (even if you have only one single interface for members) to allow:
- An explicit name of the interface to use in security policies ('internal' is more explicit than 'port10').
- A split between the physical port and its function to allow port remapping (for instance moving from a 1G interface to a 10G interface) or to facilitate configuration translation, as performed during hardware upgrades.

Security

- Use NTP to synchronize time on the FortiGate and the core network systems, such as email servers, web servers, and logging services.
- Enable log rules to match corporate policy. For example, log administration authentication events and access to systems from untrusted interfaces.

- Minimize adhoc changes to live systems, if possible, to minimize interruptions to the network. When not possible, create backup configurations and implement sound audit systems using FortiAnalyzer and FortiManager.
- If you only need to allow access to a system on a specific port, limit the access by creating the strictest rule possible.

Authentication

- You must add a valid user group to activate the Authentication check box on the firewall policy configuration page.
- Users can authenticate with the firewall using HTTP or FTP. For users to be able to authenticate, you must add an HTTP or FTP policy that is configured for authentication.

Antivirus

- Enable antivirus scanning at the network edge for all services.
- Use FortiClient endpoint antivirus scanning for protection against threats that get into your network.
- Subscribe to FortiGuard AntiVirus Updates and configure your FortiGate unit to receive push updates. This will ensure you receive antivirus signature updates as soon as they are available.
- To ensure that all AV push updates occur, ensure you have an AV profile enabled in a security policy.
- Enable only the protocols you need to scan. If you have antivirus scans occurring on the SMTP server, or use FortiMail, it is redundant to have scanning occur on the FortiGate unit as well.
- Reduce the maximum file size to be scanned. Viruses usually travel in small files of around 1 to 2 megabytes.
- Do not quarantine files unless you regularly monitor and review them. This is otherwise a waste of space and impacts performance.
- Examine antivirus reports and log messages periodically. Take particular notice of repeated detections. For example, repeated virus detection in SMTP traffic could indicate a system on your network is infected and is attempting to contact other systems to spread the infection using a mass mailer.

Antispam

- If possible use, a FortiMail unit. The antispam engines are more robust.
- Use fast DNS servers.
- Use specific security profiles for the rule that will use antispam.
- DNS checks may cause false positive with HELO DNS lookup.
- Content analysis (banned words) may impose performance overhead.

Intrusion Prevention System (IPS)

Your FortiGate's IPS system can detect traffic attempting to exploit this vulnerability. IPS may also detect when infected systems communicate with servers to receive instructions. Refer to the following list of best practices regarding IPS.

- Enable IPS scanning at the network edge for all services.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to FortiGuard IPS Updates and configure your FortiGate unit to receive push updates. This will ensure you receive IPS signature updates as soon as they are available.
- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to Block.
- Create and use security profiles with specific signatures and anomalies you need per-interface and per-rule.
- Do not use predefined or generic profiles. While these profiles are convenient to supply immediate protection, you should create profiles to suit your network environment.
- If you do use the default profiles, reduce the IPS signatures/anomalies enabled in the profile to conserve processing time and memory.
- If you are going to enable anomalies, make sure you tune thresholds according to your environment.
- If you need protection, but not audit information, disable the logging option.
- Tune the IP-protocol parameter accordingly.

Blocking Skype using CLI options for improved detection

If you want to identify or block Skype sessions, use the following CLI command with your FortiGate's public IP address to improve detection (FortiOS 4.3.12+ and 5.0.2+):

```
config ips global
   set skype-client-public-ipaddr 198.51.100.0,203.0.113.0
end
```

Note that the above syntax is configured using multiple public IP addresses, where a single public IP address may suffice depending on your network configuration.

Email filter

Spam is a common means by which attacks are delivered. Users often open email attachments they should not, and infect their own machine.

- Enable email filtering at the network edge for all types of email traffic.
- Use FortiClient endpoint IPS scanning for protection against threats that get into your network.
- Subscribe to the FortiGuard AntiSpam Service.

URL filtering

Best practices for URL filtering can be divided into four categories: flow-based versus proxy based filtering; local category/rating feature; URL filter 'Exempt' action; and Deep Scan.

Flow-based versus proxy-based

Try to avoid mixing flow-based and proxy-based features in the same profile if you are not using IPS or Application Control.

Local category/rating feature

Local categories and local rating features consume a large amount of CPU resources, so use these features as little as possible. It is better to use Local categories instead of using the 'override' feature, since the 'override' feature is more complicated and more difficult to troubleshoot.

URL filter 'Exempt' action

When using the URL filter 'Exempt' option,webfilter, antivirus and dlp scans are bypassed by default, so use this option only for trusted sites.

Configuration notes: You need to configure 'Exempt' actions in the URL filter if you want to bypass the FortiGuard Web Filter.You can configure which particular inspection(s) you want to bypass using the `set exempt` command in `config webfilter urlfilter`.

Deep Scan

The 'Deep Scan' feature is much heavier on resources than 'HTTPS URL Scan Only'. Deep Scan is much more accurate, since many sites (such as various Google applications) cannot be scanned separately without deep scanning enabled.

Note: If you configure Deep Scan in the SSL profile and then configure 'Enable HTTPS URL Scan Only' in the web filter profile, then Deep Scan is not performed.

Web filtering

FortiGuard Web Filtering can help stop infections from malware sites and help prevent communication if an infection occurs.

- Enable FortiGuard Web Filtering at the network edge.
- Install the FortiClient application and use FortiGuard Web Filtering on any systems that bypass your FortiGate unit.
- Block categories such as Pornography, Malware, Spyware, and Phishing. These categories are more likely to be dangerous

Patch management

When vulnerabilities are discovered in software, the software vendors release updates that fix these problems. Keeping your software and operating system up-to-date is a vital step to prevent infection and defend against attacks.

- Follow the latest advisories and reports on the FortiGuard webpage.
- Apply updates to all software as the updates become available.
- FortiGuard Vulnerability Management can help identify security weaknesses in your network. This subscription service is available through FortiScan and FortiAnalyzer units.
- Apply firmware updates to your FortiGate unit as they are released.
- Subscribe to FortiGuard AntiVirus and IPS services, so that AntiVirus and IPS scanning engines are automatically updated when new version are released.

Policy configuration

Configuring the FortiGate unit with an ‘allow all’ traffic policy is very undesirable. While this does greatly simplify the configuration, it is less secure. As a security measure, it is best practice for the policy rulebase to ‘deny’ by default, and not the other way around.

Policy configuration changes

On a heavy-loaded system, plan configuration changes during low usage periods in order to minimize impact on CPU usage and established sessions. In this scenario, it is considered a best practice to de-accelerate the hardware-accelerated sessions.

You can configure de-accelerated behaviour on hardware-accelerated sessions using CLI commands to control how the processor manages policy configuration changes. The following CLI commands are to be used:

```
config system settings
   set firewall-session-dirty { check-all | check-new | check-policy-option }
end
```

where you want the following to be true:

`check-all`	CPU flushes all current sessions and re-evaluates them. This is the default option.
`check-new`	CPU keeps existing sessions and applies policy changes to new sessions only. This reduces CPU load and the possibility of packet loss.
`check-policy-option`	Use the option selected in the `firewall-session-dirty` field of the firewall policy (`check-all` or `check-new`, as above, but per policy).

Policy whitelisting

- Allow only the necessary inbound and outbound traffic.
- If possible, limit traffic to specific addresses or subnets. This allows the FortiGate unit to drop traffic to and from unexpected addresses.

IPS and DoS policies

- Because it is critical to guard against attacks on services that you make available to the public, configure IPS signatures to block matching signatures. For example, if you have a web server, configure the action of web server signatures to Block.
- Your FortiGate unit includes IPS signatures written to protect specific software titles from DoS attacks. Enable the signatures for the software you have installed and set the signature action to Block.
- DoS attacks are launched against vulnerabilities. Maintain a FortiGuard IPS subscription to ensure your FortiGate unit automatically receives new and updated IPS signatures as they are released.

- Use and configure DoS policies to appropriate levels based on your network traffic and topology. This will help drop traffic if an abnormal amount is received. The key is to set a good threshold. The threshold defines the maximum number of sessions/packets per second of normal traffic. If the threshold is exceeded, the action is triggered. Threshold defaults are general recommendations, but your network may require very different values. One way to find the correct values for your environment is to set the action to Pass and enable logging. Observe the logs and adjust the threshold values until you can determine the value at which normal traffic begins to generate attack reports. Set the threshold above this value with the margin you want. Note that the smaller the margin, the more protected your system will be from DoS attacks, but your system will also be more likely to generate false alarms.

Networking

When configuring your network, ensure that there is no ‘back door’ access to the protected network. For example, if there is a wireless access point, it must be appropriately protected with password and encryption.

Be sure to also maintain an up-to-date network diagram which includes IP addressing, cabling, and network elements.

Routing configuration

- Always configure a default route.
- Add blackhole routes for subnets reachable using VPN tunnels. This ensures that if a VPN tunnel goes down, traffic is not mistakingly routed to the Internet unencrypted.

Policy routing

Keep the number of policy routes to a minimum to optimize performance in route lookup and to simplify troubleshooting.

Dynamic routing

- Select a Router ID that matches an IP assigned to an interface. This avoids the likelihood of having two devices with the same router ID.
- For routing over an IPsec tunnel, assign IP addresses to both ends of the tunnel.

Advanced routing

Use the following best practices for advanced routing when dealing with Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF).

Border Gateway Protocol (BGP)

If you are using BGP, it is recommended that you enable soft-reconfiguration. This has two benefits:

- It allows you to perform ‘soft clear’ of peers after a change is made to a BGP policy.
- It provides greater visibility into the specific prefixes learned from each neighbor.

Leave soft-reconfiguration disabled if your FortiGate does not have much unused memory. Soft-reconfiguration requires keeping separate copies of prefixes received and advertised, in addition to the local BGP database.

Open Shortest Path First (OSPF)

- Avoid use of passive interfaces wherever possible.
- Avoid use of virtual links to connect areas. All areas should be designed to connect directly to the backbone area.
- Ensure that all backbone routers have a minimum of two peering connections to other backbone neighbors.
- An entire OSPF domain should be under common administration.

Network Address Translation (NAT)

- Beware of misconfiguring the IP Pool range. Double-check the start and end IP addresses of each IP pool. The IP pool should not overlap with addresses assigned to FortiGate interfaces or to any hosts on directly connected networks.
- If you have internal and external users accessing the same servers, use split DNS to offer an internal IP to internal users so that they don't have to use the external-facing VIP.

Configuring NAT

Do not enable NAT for inbound traffic unless it is required by an application. If, for example, NAT is enabled for inbound SMTP traffic, the SMTP server might act as an open relay.

Transparent Mode

- Do not connect two ports to the same VLAN on a switch or to the same hub. Some Layer 2 switches become unstable when they detect the same MAC address originating on more than one switch interface or from more than one VLAN.
- If you operate multiple VLANs on your FortiGate unit, assign each VLAN id to its own forwarding domain to ensure that the scope of the broadcast does not extend beyond the VLAN it originated in.

To protect against Layer 2 loops:

- Enable `stpforward` on all interfaces.
- Use separate VDOMs for production traffic (TP mode VDOM) and management traffic (NAT mode VDOM).
- Only place those interfaces used for production in the TP mode VDOM. Place all other interfaces in the NAT mode VDOM. This protects against potential Layer 2 loops.

Using virtual IPs (VIPs)

- Use the external IP of 0.0.0.0 when creating a VIP for a FortiGate unit where the external interface IP address is dynamically assigned.

- Be sure to select the correct external interface when creating a new virtual IP (VIP). The external interface should be set to the interface at which the FortiGate unit receives connection requests from external networks.

FGCP high availability

Fortinet suggests the following practices related to high availability:

- Use Active-Active HA to distribute TCP and UTM sessions among multiple cluster units. An active-active cluster may have higher throughput than a standalone FortiGate unit or than an active-passive cluster.
- Use a different host name on each FortiGate unit when configuring an HA cluster. Fewer steps are required to add host names to each cluster unit before configuring HA and forming a cluster.
- Consider adding an Alias to the interfaces used for the HA heartbeat so that you always get a reminder about what these interfaces are being used for.
- Enabling `load-balance-all` can increase device and network load since more traffic is load-balanced. This may be appropriate for use in a deployment using the firewall capabilities of the FortiGate unit and IPS but no other content inspection.
- An advantage of using session pickup is that non-content inspection sessions will be picked up by the new primary unit after a failover. The disadvantage is that the cluster generates more heartbeat traffic to support session pickup as a larger portion of the session table must be synchronized. Session pickup should be configured only when required and is not recommended for use with SOHO FortiGate models. Session pickup should only be used if the primary heartbeat link is dedicated (otherwise the additional HA heartbeat traffic could affect network performance).
- If session pickup is not selected, after a device or link failover all sessions are briefly interrupted and must be re-established at the application level after the cluster renegotiates. For example, after a failover, users browsing the web can just refresh their browsers to resume browsing. Users downloading large files may have to restart their download after a failover. Other protocols may experience data loss and some protocols may require sessions to be manually restarted. For example, a user downloading files with FTP may have to either restart downloads or restart their FTP client.
- If you need to enable session pickup, consider enabling `session-pickup-delay` to improve performance by reducing the number of sessions that are synchronized. See Improving session synchronization performance on page 1.
- Consider using the `session-sync-dev` option to move session synchronization traffic off the HA heartbeat link to one or more dedicated session synchronization interfaces. See Improving session synchronization performance on page 1.
- To avoid unpredictable results, when you connect a switch to multiple redundant or aggregate interfaces in an active-passive cluster you should configure separate redundant or aggregate interfaces on the switch; one for each cluster unit.
- Use SNMP, syslog, or email alerts to monitor a cluster for failover messages. Alert messages about cluster failovers may help find and diagnose network problems quickly and efficiently.

Heartbeat interfaces

Fortinet suggests the following practices related to heartbeat interfaces:

Do not use a FortiGate switch port for the HA heartbeat traffic. This configuration is not supported.

- Configure at least two heartbeat interfaces and set these interfaces to have different priorities.
- For clusters of two FortiGate units, as much as possible, heartbeat interfaces should be directly connected using patch cables (without involving other network equipment such as switches). If switches have to be used they should not be used for other network traffic that could flood the switches and cause heartbeat delays.
- If you cannot use a dedicated switch, the use of a dedicated VLAN can help limit the broadcast domain to protect the heartbeat traffic and the bandwidth it creates.
- For clusters of three or four FortiGate units, use switches to connect heartbeat interfaces. The corresponding heartbeat interface of each FortiGate unit in the cluster must be connected to the same switch. For improved redundancy use a different switch for each heartbeat interface. In that way if the switch connecting one of the heartbeat interfaces fails or is unplugged, heartbeat traffic can continue on the other heartbeat interfaces and switch.
- Isolate heartbeat interfaces from user networks. Heartbeat packets contain sensitive cluster configuration information and can consume a considerable amount of network bandwidth. If the cluster consists of two FortiGate units, connect the heartbeat interfaces directly using a crossover cable or a regular Ethernet cable. For clusters with more than two units, connect heartbeat interfaces to a separate switch that is not connected to any network.
- If heartbeat traffic cannot be isolated from user networks, enable heartbeat message encryption and authentication to protect cluster information. See Enabling or disabling HA heartbeat encryption and authentication on page 1.
- Configure and connect redundant heartbeat interfaces so that if one heartbeat interface fails or becomes disconnected, HA heartbeat traffic can continue to be transmitted using the backup heartbeat interface. If heartbeat communication fails, all cluster members will think they are the primary unit resulting in multiple devices on the network with the same IP addresses and MAC addresses (condition referred to as *Split Brain*) and communication will be disrupted until heartbeat communication can be reestablished.
- Do not monitor dedicated heartbeat interfaces; monitor those interfaces whose failure should trigger a device failover.
- Where possible at least one heartbeat interface should not be connected to an NP4 or NP6 processor to avoid NP4 or NP6-related problems from affecting heartbeat traffic.
- Where possible, the heartbeat interfaces should not be connected to an NP4 or NP6 processor that is also processing network traffic.
- Where possible, each heartbeat interface should be connected to a different NP4 or NP6 processor.
- Any FortiGate interface can be used as a heartbeat interface including 10/100/1000Base-T, SFP, QSFP fiber and copper, and so on. If you set up two or more interfaces as heartbeat interfaces each interface can be a different type and speed.

Interface monitoring (port monitoring)

Fortinet suggests the following practices related to interface monitoring (also called port monitoring):

- Wait until a cluster is up and running and all interfaces are connected before enabling interface monitoring. A monitored interface can easily become disconnected during initial setup and cause failovers to occur before the cluster is fully configured and tested.
- Monitor interfaces connected to networks that process high priority traffic so that the cluster maintains connections to these networks if a failure occurs.
- Avoid configuring interface monitoring for all interfaces.
- Supplement interface monitoring with remote link failover. Configure remote link failover to maintain packet flow if a link not directly connected to a cluster unit (for example, between a switch connected to a cluster interface and the network) fails. See Remote link failover on page 1.

WAN Optimization

WAN Optimization features require significant memory resources and generate a high amount of I/O on disk. Before enabling WAN Optimization, ensure that the memory usage is not too high. If possible, avoid other disk-intensive features such as heavy traffic logging on the same disk as the one configured for WAN Optimization needs.

In general, it is preferable to enable the Transparent Mode checkbox and ensure that routing between the two endpoints is acceptable. Some protocols may not work well without enabling Transparent Mode.

Other best practices for utilizing the WAN Optimization feature follow.

Sharing the WAN Opt. tunnel for traffic of the same nature

WAN optimization tunnel sharing is recommended for similar types of WAN optimization traffic (such as CIFS traffic from different servers). However, tunnel sharing for different types of traffic is not recommended. For example, aggressive and non-aggressive protocols should not share the same tunnel.

Ordering WAN Opt. rules appropriately

- Precise, port specific WAN Optimization rules should be at the top of the list.
- Generic rules, such as overall TCP, should be at the bottom of the list.

Avoiding mixing protocols in a WAN Opt. tunnel

Different protocols may be more or less talkative or interactive . Mixing protocols in a tunnel may result in a delay for some of them. It is recommended to define protocol specific wan-optimization rules and restrict the ports to the necessary ones only for performance reasons.

Setting correct configuration options for CIFS WAN Opt.

Ensure that the WAN Optimization rules cover TCP ports 139 and 445 (on the same or two different rules). Also ensure that Transparent Mode is selected.

Setting correct configuration options for MAPI WAN Opt.

For MAPI WAN Optimization, only specify a rule with TCP port 135 (unless the MAPI control port is configured differently). Derived data sessions using other random ports will be handled by the CIFS wan-optimization daemon even with only the control port configured.

Testing WAN Opt. in a lab

- Ensure that WAN emulators are used to simulate the WAN. If no WAN emulator is used, it is expected to have better results without WAN Optimization than with WAN Optimization.
- To test the difference between cold transfers (first-time transfers) and warm transfers, it is recommended to generate a random file of the cold transfer to ensure that the test is the first time that the file has been seen.

Regarding byte compression and type of file

Enabling byte compression on file transfers already compressed (.jpeg files, compressed archive, etc.) won't provide any performance increase and could be seen as a misuse of CPU resources.

Regarding network address translation (NAT)

Selecting the NAT feature in a security policy does not have any influence on WAN Optimization traffic.

High Availability

There is no benefit to using active-active mode, so for pure WAN Optimization needs, use active-passive mode. Refer to the FGCP high availability section for other best practices related to HA.

Authentication with specific peers

Configure WAN optimization authentication with specific peers. Accepting any peer is not recommended as this can be less secure.

Virtual Domains (VDOMs)

VDOMs can provide separate firewall policies and, in NAT mode, completely separate configurations for routing and VPN services for each connected network or organization. This section provides a list of best practices for configuring VDOMs.

Per-VDOM resource settings

While Global resources apply to resources shared by the whole FortiGate unit, per-VDOM resources are specific to only one Virtual Domain.

By default all the per-VDOM resource settings are set to no limits. This means that any single VDOM can use up all the resources of the entire FortiGate unit if it needs to do so. This would starve the other VDOMs for resources to the point where they would be unable to function. For this reason, it is recommended that you set some maximums on resources that are most vital to your customers.

Virtual domains in NAT mode

Once you have enabled virtual domains and created one or more VDOMs, you need to configure them. It is recommended that you perform the following tasks in the order given (while you may not require all for your network topology):

1. Change the management virtual domain.
2. Configure FortiGate interfaces for your VDOMs in NAT mode.
3. Configure VDOM routing.
4. Configure security policies for VDOMs in NAT mode.
5. Configure UTM profiles for VDOMs in NAT mode.
6. Test the configuration.

Virtual clustering

If you decide to disable override for clurstering, as a result of persistent renegotiating, you should disable it for both cluster units.

Explicit proxy

- For explicit proxies, when configuring limits on the number of concurrent users, you need to allow for the number of users based on their authentication method. Otherwise you may run out of user resources prematurely.
- Each session-based authenticated user is counted as a single user using their authentication membership (RADIUS, LDAP, FSSO, local database etc.) to match users in other sessions. So one authenticated user in multiple sessions is still one user.
- For all other situations, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user.
- Set the explicit web proxy and explicit FTP proxy Default Firewall Policy Action to Deny. This means that a firewall policy is required to use these explicit proxies, allowing you to control access and impose security features.
- Do not enable the explicit web or FTP proxy on an interface connected to the Internet. This is a security risk because anyone on the Internet who finds the proxy could use it to hide their source address. If you must enable the proxy on such an interface make sure authentication is required to use the proxy.

Wireless

The following section contains a list of best practices for wireless network configurations with regard to encryption and authentication, geographic location, network planning, power usage, client load balancing, local bridging, SSIDs, and the use of static IPs.

Encryption and authentication

It is best practice to always enable the strongest user authentication and encryption method that your client supports. Fortinet recommends the following security, in order of strongest to weakest:

- WPA2 - Enterprise 802.1x/EAP - Personal pre-shared key (8-63 characters)
- WPA - Enterprise 802.1x/EAP - Personal pre-shared key (8-63 characters)
- WEP128 - 26 Hexadecimal digit key
- WEP64 - 10 Hexadecimal digit key
- None - Open system

Geographic location

Ensure that the FortiGate wireless controller is configured for your geographic location. This ensures that the available radio channels and radio power are in compliance with the regulations in your region.

The maximum allowed transmitter power and permitted radio channels for Wi-Fi networks depend on the region in which the network is located. By default, the WiFi controller is configured for the United States. If you are located in any other region, you need to set your location before you begin configuring wireless networks.

The location setting can only be changed from CLI. To change the country to France, for example, enter the following:

```
config wireless-controller setting
   set country FR
end
```

To see the list of country codes, enter a question mark ('?') in place of the country code.

Using an incorrect geographic location is a common error that can lead to unpredicable results on the client side.

Network planning

It is recommended that you perform a proper site survey prior positioning the wireless access point. In order to evaluate the coverage area environment, the following criteria must be taken into account:

- Size of coverage area
- Bandwidth required
- Client wireless capabilities

After completing a RF site survey, you'll have a good idea of the number and location of access points needed to provide users with adequate coverage and performance.

However, prior to installing the access points, be sure to determine the RF channel(s) you plan to use. This will ensure that users can roam throughout the facility with substantial performance.

To avoid co-channel interference, adjacent Wi-Fi APs must be configured to use non-overlapping channels. Otherwise, you'll find poor performance will degrade because of interference between access points.

It is recommended to statically configure the non-overlapping channels on every access point, using one Custom AP profile per AP (or group of APs). If static configuration cannot be used, the FortiOS Wi-Fi Controller includes the Automatic Radio Resource Provisioning (ARRP) feature.

Lowering the power level to reduce RF interference

Relevant Product(s): FortiAP

Reducing power reduces unwanted coverage and potential interference to other WLANs. Areas of unwanted coverage are a potential security risk. If possible, reduce the transmitter power of your wireless access point so that the signal is not available beyond the areas where it is needed. Auto Tx Power Control can be enabled to automatically adjust the transmit power.

In cases where customers complain about slow wireless traffic through a FortiAP, it might be necessary to try to reduce the possibility of RF interference. It is best practice not to locate FortiAPs near steel beams or other interfering materials. You can try using a wireless sniffer tool to collect the wireless packets and then analyze the extent of air interference.

A common mistake is spacing FortiAPs based upon the 5Ghz radio frequency. The 2.4Ghz signal travels further.

You have two options when confronted with slow wireless traffic through a FortiAP:

Option #1: Reducing transmit power

Perform a speed test and record the results. Set one of the radios on a FortiAP to be in dedicated monitoring mode. Then observe how many APs are detected. If the number of APs is too high (i.e., greater than 20), try reducing the transmit power in the WTP profile for the FortiAPs until the number of dedicated APs has dropped significantly.

Repeat the speed test.

Option #2: Ensuring that VAPs are distributed over the available channels

No built-in tools are available to measure RF interference directly. However, FortiOS 5.0 does allow for automatic power adjustment, which should minimize the occurrence of RF interference.

Wireless client load balancing

Wireless load balancing allows your wireless network to more efficiently distribute wireless traffic among wireless access points and available frequency bands. FortiGate wireless controllers support the following types of client load balancing:

- **Access Point Hand-off** - The wireless controller signals a client to switch to another access point.
- **Frequency Hand-off** - The wireless controller monitors the usage of 2.4GHz and 5GHz bands, and signals clients to switch to the lesser-used frequency.

Local bridging

Whenever possible, use local bridging to offload the CAPWAP tunnel. Note that in this case, Wi-Fi client devices obtain IP addresses from the same DHCP server as wired devices on the LAN. The vlan ID can only be configured from the CLI:

```
config wireless-controller vap
   edit "vaplocalbridge"
      set vdom "root"
      set ssid "testvaplocalbridge"
      set local-bridging enable
      set vlanid 40 ---> only available in CLI
   next
end
```

Advertising SSIDs

- It is highly recommended to advertise the SSID. It makes it easier for customers and wireless clients. Also, if you 'hide' the SSID (known as ‘network cloaking’), then clients will always look for it when they're outside the coverage area, which searches for known SSIDs, in effect leaking the SSID anyway. Refer to RFC 3370. Furthermore, many of the latest Broadcom drivers do not support hidden SSID for WPA2.
- For security reason, you might want to prevent direct communication between your wireless clients. In this case, enable Block Intra-SSID Traffic (in the SSID configuration).
- In a network with multiple wireless controllers, you need to change the mesh SSID so that each mesh root has a unique SSID. Other controllers using the same mesh root SSID might be detected as fake or rogue APs. Go to **WiFi & Switch Controller > SSID** to change the SSID. Fortinet also recommends that you create a new preshared key instead of using the default.

Using static IPs in a CAPWAP configuration

In a large FortiAP deployment with more than 20 FortiAPs connecting to a Fortigate Wireless Controller (AC), it is recommended to use static IPs on the access points instead of DHCP, setting the AC IP statically and the AC discovery type to static (Type 1), instead of learning it through broadcast, multicast, or DHCP.

This makes management of the APs easier since you know the exact IP of each access point. Troubleshooting also becomes easier as the debug of the AC controller won't continuously attempt the different discovery methods in sequence (broadcast > multicast > static).

Logging and reporting

The default log device settings must be modified so that system performance is not compromised. The FortiGate unit, by default, has all logging of FortiGate features enabled, except for traffic logging. The default logging location will be either the FortiGate unit's system memory or hard disk, depending on the model. Units with a flash disk are not recommended for disk logging.

Log management

When the FortiGate unit records FortiGate activity, valuable information is collected that provides insight into how to better protect network traffic against attacks, including misuse and abuse. There is a lot to consider before enabling logging on a FortiGate unit, such as what FortiGate activities to enable and which log device is best suited for your network's logging needs. A plan can help you in deciding the FortiGate activities to log, a log device, as well as a backup solution in the event the log device fails.

This plan should provide you with an outline, similar to the following:

- What FortiGate activities you want and/or need logged (for example, security features).
- The logging device best suited for your network structure.
- If you want or require archiving of log files.
- Ensuring logs are not lost in the event a failure occurs.

After the plan is implemented, you need to manage the logs and be prepared to expand on your log setup when the current logging requirements are outgrown. Good log management practices help you with these tasks.

Log management practices help you to improve and manage logging requirements. Logging is an ever-expanding tool that can seem to be a daunting task to manage. The following management practices will help you when issues arise, or your logging setup needs to be expanded.

- Revisit your plan on a yearly basis to verify that your logging needs are being met by your current log setup. For example, your company or organization may require archival logging, but not at the beginning of your network's lifespan. Archival logs are stored on a FortiGate unit's local hard drive, a FortiAnalyzer unit, or a FortiCloud server, in increasing order of size.
- Configure an alert message that will notify you of activities that are important to be aware about. For example: if a branch office does not have a FortiGate administrator, you will need to know at all times that the IPsec VPN tunnel is still up and running. An alert email notification message can be configured to send only if IPsec tunnel errors occur.
- If your organization or company uses peer-to-peer programs such as Skype or other instant messaging software, use the IM usage dashboard widget or the Executive Summary's report widget (Top 10 Application Bandwidth Usage Per Hour Summary) to help you monitor the usage of these types of instant messaging software. These widgets can help you in determining how these applications are being used, including if there is any misuse and abuse. Their information is taken from application log messages; however, application log messages should be viewed as well since they contain the most detailed information.
- Ensure that your backup solution is up-to-date. If you have recently expanded your log setup, you should also review your backup solution. The backup solution provides a way to ensure that all logs are not lost in the event that the log device fails or issues arise with the log device itself.

- When downloading log messages and viewing them on a computer, the log file will be downloaded like any other file. Log file names contain their log type and date in the name, so it is recommended to create a folder in which to archive your log messages, as they can be sorted easily.

System memory and hard disks

If the FortiGate unit has a hard disk, it is enabled by default to store logs. This also means that you do not have to enable this and configure the settings for logging to the hard disk, but modify these settings so that it is configured for your network logging requirements.

If the FortiGate unit has only flash memory, disk logging is disabled by default, as it is not recommended. Constant rewrites to flash drives can reduce the lifetime and efficiency of the memory. It must be enabled in the CLI under config log disk setting.

For some low-end models, disk logging is unavailable. Check a product's Feature Matrix for more information. In either case, Fortinet recommends using either a FortiAnalyzer unit or the FortiCloud service.

Comparison of inspection types

The tables in this section show how different security functions map to different inspection types.

Mapping security functions to inspection types

The table below lists FortiOS security functions and shows whether they are applied by the kernel, flow-based inspection or proxy-based inspection.

FortiOS security functions and inspection types

Security Function	Kernel (Stateful inspection)	Flow-based inspection	Proxy-based inspection
Firewall	yes		
IPsec VPN	yes		
Traffic Shaping	yes		
User Authentication	yes		
Management Traffic	yes		
SSL VPN	yes		
IPS		yes	
Antivirus		yes	yes
Application Control		yes	
Web filtering		yes	yes
DLP		yes	yes
Email Filtering			yes
VoIP inspection			yes
ICAP			yes

More information about inspection methods

The three inspection methods each have their own strengths and weaknesses. The following table looks at all three methods side-by-side.

Inspection methods comparison

Feature	Stateful	Flow	Proxy
Inspection unit per session	first packet	selected packets, single pass architecture, simultaneous application of configured inspection methods	complete content, configured inspection methods applied in order
Memory, CPU required	low	medium	high
Level of threat protection	good	better	best
Authentication	yes		
IPsec and SSL VPN	yes		
Antivirus protection		yes	yes
Web Filtering		yes	yes
Data Leak Protection (DLP)		yes	yes
Application control		yes	
IPS		yes	
Delay in traffic	minor	no	small
Reconstruct entire content		no	yes