CIS FortiGate 7.4.x Benchmark

v1.0.1 - 01-07-2026

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completes successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for Fortinet FortiGate devices running the Fortinet OS version 7.4.0 or above. This guide was tested against FortiOS 7.4.5. To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for security administrators, IT auditors, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Fortinet OS on Fortinet network devices.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not negatively inhibit the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is paramount
  - acts as a defense in depth measure
  - may negatively inhibit the utility or performance of the technology.

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Eric Leong

Contributor
Daniel Brown
Robert Loehmann
Eric Leong
Darren Stevenson
Tabitha Haug

Recommendations

1 Network Settings

This section provides best practices related to Network/IP, DNS settings, DHCP server, static routing, Policy routing, and dynamic routing.

1.1 Ensure DNS server is configured (Automated)

Profile Applicability:

- Level 1

Description:

Fortinet uses the Domain Name Service (DNS) to translate host names into IP addresses. To enable DNS lookups, you must specify the primary DNS server for your system. You can also specify secondary and tertiary DNS servers. When resolving host names, the system consults the primary name server. If a failure or time-out occurs, the system consults the secondary name server.

For security purpose, trusted DNS servers should be configured to prevent man-in-the-middle attacks.

Rationale:

The purpose is to perform the resolution of system hostnames to Internet Protocol (IP) addresses using trusted DNS servers.

Audit:

In CLI:

```
FGT1 # config system dns
FGT1 (dns) # show
config system dns
    set primary <ip_address>
    set secondary <ip_address>
    ...
end
```

In the GUI, go to Networks > DNS. The FortiGate uses either the default FortiGuard DNS or customized DNS

Remediation:

In this example, we will assign 8.8.8.8 as primary DNS and 8.8.4.4 as secondary DNS.

In CLI:

```
FGT1 # config system dns
FGT1 (dns) # set primary 8.8.8.8
FGT1 (dns) # set secondary 8.8.4.4
FGT1 (dns) # end
FGT1 #
```

In the GUI, go to Networks > DNS. Click on "Specify" and put in 8.8.8.8 as "Primary DNS Server" and 8.8.4.4 as "Secondary DNS Server"

Default Value:

Default primary DNS server is 96.45.45.45. Default secondary DNS server is 96.45.46.46.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.0/administration-guide/903162

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.9 Configure Trusted DNS Servers on Enterprise Assets Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

1.2 Ensure intra-zone traffic is not always allowed (Manual)

Profile Applicability:

- Level 1

Description:

This is to make sure that only specific, authorized traffic is allowed between networks in the same zone.

Rationale:

This adds an extra layer of protection between different networks.

Audit:

In this example, we'll verify the zone DMZ. In CLI:

```
FGT1 # config system zone
FGT1 (zone) # edit DMZ
FGT1 (DMZ) # show full
config system zone
    edit "DMZ"
        ...
        set intrazone deny
        ...
    next
end
```

In the GUI, click on Network -> Interfaces, select the zone and click on "Edit". Make sure that the option "Block intra-zone traffic" is enabled.

Remediation:

In this example, we'll turn off intra-zone traffic in the zone DMZ. In CLI:

```
FGT1 # config system zone
FGT1 (zone) # edit DMZ
FGT1 (DMZ) # set intrazone deny
FGT1 (DMZ) # end
FGT1 #
```

In the GUI, click on Network -> Interfaces, select the zone and click on "Edit" and turn on "Block intra-zone traffic"

Default Value:

By default, intra-zone traffic is blocked

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/314783845/config-system-zone
2. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/116821

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	2.10 Physically or Logically Segregate High Risk Applications Physically or logically segregated systems should be used to isolate and run software that is required for business operations but incur higher risk for the organization.			●

1.3 Disable all management related services on WAN port (Manual)

Profile Applicability:

- Level 1

Description:

Enabling any management related services on WAN interface is high risk. Management related services such as HTTPS, HTTP, ping, SSH, SNMP, and Radius should be disabled on WAN.

Rationale:

Management related services should only be enabled on management interface. This is part of defending the firewall from attacks and reducing the attack surface. For WAN related services such as IPsec and SSLVPN, make use of local-in-policy (refer to CIS Section 2.4) to tighten firewall defenses.

Impact:

Enabling management related services on WAN port is convenient, but it exposes the firewall to unnecessary risks. Vulnerabilities found on vendor devices are commonly related to management services, and opening access to these allows attackers to exploit its vulnerabilities.

Audit:

On GUI:

```
Go to "Network" > "Interfaces".

Identify WAN interface and validate that HTTPS, HTTP, PING, SSH, SNMP, and
Radius Accounting is not enabled in "Administrative Access" section.
```

On CLI:

```
`FGT1 # show system interface`
```

Identify WAN interface and validate that "set allowaccess" does not include ping, https, http, ssh, snmp or radius-acct configured.

Remediation:

On GUI:

```
Go to "Network" > "Interfaces".
```

Review WAN interface and disable HTTPS, HTTP, ping, SSH, SNMP, and Radius services.

On CLI:

```
FGT1 # config system interface
FGT1 (interface) # edit "port1"
FGT1 (port1) # unselect allowaccess ping https ssh snmp http radius-acct
```

Note:

1. Interface name may differ based on deployment. For this example, port1 is deployed as WAN interface.
2. "unselect allowaccess" will only show services that you have enabled. If you have not enabled snmp on that interface, then snmp option will not be available.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	1.6 Address Unauthorized Assets Ensure that unauthorized assets are either removed from the network, quarantined or the inventory is updated in a timely manner.	●	●	●

2 System Settings

This topic contains information and best practices about FortiGate administration and system configuration.

2.1 General Settings

2.1.1 Ensure 'Pre-Login Banner' is set (Automated)

Profile Applicability:

- Level 1

Description:

Configure a pre-login banner, ideally approved by the organization's legal team. This banner should, at minimum, prohibit unauthorized access, provide notice of logging or monitoring, and avoid using the word "welcome" or similar words of invitation.

Rationale:

Through a properly stated login banner, the risk of unintentional access to the device by unauthorized users is reduced. Should legal action take place against a person accessing the device without authorization, the login banner greatly diminishes a defendant's claim of ignorance.

Impact:

Login banners provide a definitive warning to any possible intruders who may want to access the FortiGate that certain types of activity are illegal. At the same time, it also advises the authorized and legitimate users of their obligations relating to acceptable use.

Audit:

Run the following command in the CLI to verify the pre-login-banner is enabled:

```
FG1 # get system global
        ...
        pre-login-banner    : enable
        ...
end
```

In the GUI, to verify the content of the pre-login disclaimer message:

```
1) Go to 'System' -> 'Replacement Messages'
2) From the top right side, select 'Extended View'
3) Find 'Pre-login Disclaimer Message'
```

Remediation:

Run the following command in the CLI to enable the pre-login-banner:

```
FG1 # config system global
FG1 (global) # set pre-login-banner enable
FG1 (global) # end
FG1 #
```

In the GUI, to edit the content of the pre-login disclaimer message:

1. Go to 'System' -> 'Replacement Messages' -> 'Extended View' -> 'Pre-login Disclaimer Message'. The edit screen is on the bottom right corner of the page. Click on "Save" after the editing is done.

Default Value:

the 'Pre-Login Banner' is disabled by default

```
FG1 # config system global
FG1 (global) # show
config system global
        ...
        set pre-login-banner disable
        ...
end
```

the warning message default value is as follows:

```
PRE WARNING:
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action. All use of this system constitutes consent to
monitoring at all times and users are not entitled to any
expectation of privacy. If monitoring reveals possible evidence
of violation of criminal statutes, this evidence and any other
related information, including identification information about
the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or
unauthorized use, employees who violate security regulations or
make unauthorized use of this system are subject to appropriate
disciplinary action.
```

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-admin-disclaimer-page/ta-p/198609?externalID=FD33887

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.2 Ensure 'Post-Login-Banner' is set (Automated)

Profile Applicability:

- Level 1

Description:

Sets the banner after users successfully log in. This is equivalent to Message of the Day (MOTD) in some other systems.

Rationale:

Network banners are electronic messages that provide notice of legal rights to users of computer networks. From a legal standpoint, banners have four primary functions:

First, banners may be used to generate consent to real-time monitoring under Title III. Second, banners may be used to generate consent to the retrieval of stored files and records pursuant to ECPA. Third, in the case of government networks, banners may eliminate any Fourth Amendment "reasonable expectation of privacy" that government employees or other users might otherwise retain in their use of the government's network under O'Connor v.

Impact:

When post-login banner is enabled, some automated-script might be affected because both CLI and GUI need an acceptance action (press "A" or "Accept") to continue.

Audit:

Run the following command in the CLI to verify the post-login-banner is enabled:

```
FG1 # get system global
        ...
        post-login-banner    : enable
        ...
```

In the GUI, to verify the content of the post-login disclaimer message:

```
1) Go to 'System' -> 'Replacement Messages'
2) From the top right side, select 'Extended View'
3) Find 'Post-login Disclaimer Message'
```

Remediation:

Run the following command in the CLI to enable the post-login-banner:

```
FG1 # config system global
FG1 (global) # set post-login-banner enable
FG1 (global) # end
FG1 #
```

In the GUI, to edit the content of the post-login disclaimer message, go to

```
System -> Replace Messages -> Extended View -> "Post-login Disclaimer
Message". The edit screen is on the bottom right corner of the page. Click on
"Save" after the editing is done.
```

Default Value:

POST WARNING: This is a private computer system. Unauthorized access or use is prohibited and subject to prosecution and/or disciplinary action. All use of this system constitutes consent to monitoring at all times and users are not entitled to any expectation of privacy. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of this system are subject to appropriate disciplinary action.

%%LAST_SUCCESSFUL_LOGIN%% %%LAST_FAILED_LOGIN%%

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuring-admin-disclaimer-page/ta-p/198609?externalID=FD33887

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.3 Ensure timezone is properly configured (Automated)

Profile Applicability:

- Level 1

Description:

Sets the local time zone information so that the time displayed by the device is more relevant to those who are viewing it.

Rationale:

Having a correct time set on the device is important for two main reasons. The first reason is that digital certificates compare this time to the range defined by their Valid From and Valid To fields to define a specific validity period. The second reason is to have relevant time stamps when logging information. Whether you are sending messages to a Syslog server, sending messages to an SNMP monitoring station, or performing packet captures, timestamps have little usefulness if you cannot be certain of their accuracy.

Impact:

For many features to work, including scheduling, logging, and SSL-dependent features, the FortiOS system time must be accurate.

Audit:

In the CLI, do the following command and check the result of **timezone** filed in the output

```
FGT1 # get system global
...
timezone            : (GMT-8:00) Pacific Time (US & Canada)
...
```

Or from GUI, do the following:

```
1) Login to FortiGate
2) Go to 'System' -> 'Settings'.
3) Time Zone and NTP settings are under 'System Time'
```

Remediation:

In this example, we will set Eastern Timezone (GMT-5:00) for the Fortigate. Each timezone will have its corresponding ID. To find the correct ID, when you type in the command "set timezone ", also type the question mark '?' to list all of the available timezones and their IDs. The ID of the Eastern Timezone is 12 In the CLI:

```
FGT1 # config system global
FGT1 (global) # set timezone 12
FGT1 (global) # end
FGT1 #
```

In the GUI, do the following:

```
1) After login to fortigate, go to 'System' -> 'Settings'
2) Select '(GMT-5:00) Eastern Time (US & Canada)' under 'System Time'
```

Default Value:

Default value is (GMT-8:00) Pacific Time (US & Canada)

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Setting-the-system-time/ta-p/192907?externalID=FD49018
2. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/512210

Additional Information:

Daylight savings time is enabled by default, and can only be configured in the CLI.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.1.4 Ensure correct system time is configured through NTP (Manual)

Profile Applicability:

- Level 1

Description:

You can either manually set the FortiOS system time, or configure the device to automatically keep its system time correct by synchronizing with a Network Time Protocol (NTP) server.

These settings enable the use of primary and secondary NTP servers to provide redundancy in case of a failure involving the primary NTP server.

Rationale:

NTP enables the device to maintain accurate time and date when receiving updates from a reliable NTP server. Accurate timestamps are critical when correlating events with other systems, troubleshooting, or performing investigative work. Logs and certain cryptographic functions, such as those utilizing certificates, rely on accurate time and date parameters. In addition, rules referencing a Schedule object will not function as intended if the device's time and date are incorrect. For additional security, authenticated NTP can be utilized. If Symmetric Key authentication is selected, only SHA1 should be used, as MD5 is considered severely compromised.

Impact:

For many features to work, including scheduling, logging, and SSL-dependent features, the FortiOS system time must be accurate.

Audit:

In the CLI:

```
FGT1 # diag sys ntp status
synchronized: yes, ntpsync: enabled, server-mode: enabled

ipv4 server(ntp2.fortiguard.com) 208.91.114.23 -- reachable(0xff) S:3 T:54
    server-version=4, stratum=1
    reference time is e12361d5.f27e0322 -- UTC Wed Sep 11 12:06:45 2019
    clock offset is -0.001569 sec, root delay is 0.000000 sec
    root dispersion is 0.010269 sec, peer dispersion is 19 msec

ipv4 server(ntp1.fortiguard.com) 208.91.115.123 -- reachable(0xff) S:3 T:54
selected
    server-version=4, stratum=1
    reference time is e12361d4.4f8b22a5 -- UTC Wed Sep 11 12:06:44 2019
    clock offset is -0.000652 sec, root delay is 0.000000 sec
    root dispersion is 0.010284 sec, peer dispersion is 8 msec

ipv4 server(ntp2.fortiguard.com) 208.91.113.71 -- reachable(0xff) S:3 T:54
    server-version=4, stratum=2
    reference time is e12361d6.4caf57ab -- UTC Wed Sep 11 12:06:46 2019
    clock offset is -0.004814 sec, root delay is 0.000137 sec
    root dispersion is 0.011154 sec, peer dispersion is 3 msec

ipv4 server(ntp1.fortiguard.com) 208.91.113.70 -- reachable(0xff) S:3 T:54
    server-version=4, stratum=2
    reference time is e123617b.c98e2059 -- UTC Wed Sep 11 12:05:15 2019
    clock offset is -0.005106 sec, root delay is 0.000122 sec
    root dispersion is 0.013382 sec, peer dispersion is 6 msec
```

Remediation:

You can only customize NTP setting using CLI. In this example, we'll assign pool.ntp.org as primary NTP server and 1.1.1.1 as secondary NTP server.

```
FGT1 # config system ntp
FGT1 (ntp) # set type custom
FGT1 (ntp) # config ntpserver
FGT1 (ntpserver) # edit 1
FGT1 (1) # set server pool.ntp.org
FGT1 (1) # next
FGT1 (ntpserver) # edit 2
FGT1 (2) # set server 1.1.1.1
FGT1 (2) # end
FGT1 (ntp) # end
FGT1 #
```

Default Value:

By default, Fortinet uses the NTPs server of the FortiGuard

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Setting-the-system-time/ta-p/192907?externalID=FD49018
2. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/512210

Additional Information:

Daylight savings time is enabled by default, and can only be configured in the CLI.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 Standardize Time Synchronization Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●
v7	6.1 Utilize Three Synchronized Time Sources Use at least three synchronized time sources from which all servers and network devices retrieve time information on a regular basis so that timestamps in logs are consistent.		●	●

2.1.5 Ensure hostname is set (Automated)

Profile Applicability:

- Level 1

Description:

Changes the device default hostname.

Rationale:

The device hostname plays an important role in asset inventory and identification as a security requirement. It is also crucial in the public keys and certificate deployments, as well as when correlating logs from different systems during an incident handling.

Audit:

In CLI

```
get system global
        ...
        hostname             : FG1
        ...
```

In GUI

```
1) Go to 'System' > 'Settings'
2) Check the field 'Hostname'
```

Remediation:

In CLI, set the hostname to 'New_FGT1' as follows:

```
FGT1 # config system global
FGT1 (global) # set hostname "New_FGT1"
FGT1 (global) # end
New_FGT1 #
```

In GUI

```
1) Go to 'System' > 'Settings'
2) Update the field 'Hostname' with the new hostname
3) click 'Apply'
```

Default Value:

The default value of the hostname is the model number of the unit. Example: 'FortiGate 2000E'

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Renaming-the-hostname/ta-p/198521?externalID=FD48765

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.6 Ensure the latest firmware is installed (Manual)

Profile Applicability:

- Level 2

Description:

Check against the Fortinet website to make sure that the latest stable firmware is installed.

Rationale:

Fortinet periodically updates the FortiGate firmware to include new features and resolve important issues. After you have registered your FortiGate unit, firmware updates can be downloaded from the Fortinet Customer Service & Support website.

It is important to constantly keep the firmware up to date to prevent any new well-known exploitation.

Audit:

First, check for the latest firmware version available by going to https://docs.fortinet.com/upgrade-tool, select your product from the Current Product drop-down menu, then select the upgrade to FortiOS Version for the latest available version.

Second, verify the current firmware on your system. In the CLI:

```
FGT1 # get system status
...
Version: Fortigate-100D v6.2.7,build1190,201216 (GA)
...
FGT1 #
```

In the GUI:

```
1. Go to Dashboard > Status > System information
2. Check for firmware.
```

At the same time, go to https://www.fortiguard.com/psirt?product=FortiOS and check for vulnerabilities that your existing version might have.

Remediation:

First, determine the upgrade path recommended by Fortinet. If you have not upgraded the system for a long time, it is not recommended to upgrade straight to the latest version, as the configuration could be lost. Fortinet provides a tool to recommend an upgrade path for all of its products.

Go to https://docs.fortinet.com/upgrade-tool. Choose your product from the "Current Product" drop-down menu, the "current FortiOS version", and the latest firmware version available for that model from "Upgrade to FortiOS Version". Click "Go". Write down the path and then click on "Download" to download all the necessary versions.

The second step is to download the required FortiOS firmware/s. Go to https://support.fortinet.com and login. Go to Support -> Firmware Download. Once there, select the product and click on "Upgrade Path". Choose the specific model of the hardware, the current firmware version and the latest firmware version available for that model. Click "Go". Write down the path and then click on "Download" to download all the necessary versions.

The last step is to install the new firmwares in the order provided by the "Upgrade tool". It is recommended to use GUI to perform this task as it would be much easier.

In the GUI

```
1. Go to System > Fabric Management
2. Right click on device that needs to be upgraded.
3. Then click on "Upgrade". You might have to perform this step multiple
times if you follow the upgrade path.
```

Default Value:

There is no default firmware. The hardware comes with the latest firmware at the time it was manufactured.

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-upgrade-FortiGate-firmware/ta-p/194980?externalID=10948

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●

2.1.7 Disable USB Firmware and configuration installation (Automated)

Profile Applicability:

- Level 2

Description:

Disable USB port auto install feature for config and firmware.

Rationale:

Disabling USB port for auto install prevents a USB with a manipulated configuration or incorrect firmware from being connected and loaded automatically.

Audit:

CLI:

```
config system auto-install
get
```

Verify that set `auto-install-config` and set `auto-install-image` are disabled

Remediation:

CLI:

```
config system auto-install
    set auto-install-config disable
    set auto-install-image disable
end
```

Default Value:

`auto-install` is enabled by default.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/304730529/config-system-auto-install

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

2.1.8 Disable static keys for TLS (Automated)

Profile Applicability:

- Level 2

Description:

Disable support for static keys on TLS sessions terminating on the FortiGate

Rationale:

Prevent TLS sessions terminating on the FortiGate from using static SSL keys

Audit:

CLI:

```
config system global
get
```

Validate that `ssl-static-key-ciphers` disabled.

Remediation:

CLI:

```
config system global
set ssl-static-key-ciphers disable

end
```

Default Value:

`ssl-static-key-ciphers` is enabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/339914554/config-system-global

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

2.1.9 Enable Global Strong Encryption (Automated)

Profile Applicability:

- Level 2

Description:

Enable FortiOS to only use strong encryption and allow only strong ciphers for communication

Rationale:

Audit:

CLI:

```
config system global
get
```

Validate `strong-crypto` is enabled.

Remediation:

CLI:

```
config system global
set strong-crypto enable

end
```

Default Value:

`strong-crypto` is enabled by default.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/339914554/config-system-global

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	18.5 Use Only Standardized and Extensively Reviewed Encryption Algorithms Use only standardized and extensively reviewed encryption algorithms.		●	●

2.1.10 Ensure management GUI listens on secure TLS version (Automated)

Profile Applicability:

- Level 1

Description:

As we move towards better encryption capabilities, we need to also ensure GUI access is properly secured. TLS 1.3 is currently the most secure SSL/TLS supported version for SSL-encrypted administrator access (at this time of writing).

Rationale:

Use higher version of SSL/TLS to prevent MiTM attacks.

Audit:

CLI:

```
config system global
get
```

Verify if `set admin-https-ssl-versions tlsv1-3` is configured.

Remediation:

CLI:

```
config system global
set admin-https-ssl-versions tlsv1-3
```

Default Value:

FortiOS 7.x - TLS 1.2 and 1.3 enabled

FortiOS 6.x - TLS 1.1, 1.2, and 1.3 enabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/339914554/config-system-global

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			

Controls Version	Control	IG 1	IG 2	IG 3
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.1.11 Ensure CDN is enabled for improved GUI performance (Automated)

Profile Applicability:

- Level 2

Description:

To improve GUI performance, an option is added to enable loading static GUI artifacts cached in CDN (content delivery network) servers closer to the user rather than from the FortiGate. On failure, the files can fall back to loading from the FortiGate.

Rationale:

When accessing a remote FortiGate, GUI might experience some slowness due to geographical distance. For this case, loading static GUI artifacts cached in CDN servers will provide a better GUI / web management experience.

Impact:

This is not a security control recommendation. Hence, there is no impact if this is not enabled.

Audit:

On CLI:

```
config system global
get
```

Ensure that `gui-cdn-usage` is enabled.

Remediation:

On CLI:

```
config system global
    set gui-cdn-usage enable
end
```

Default Value:

Enabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/205105/loading-artifacts-from-a-cdn

2.1.12 Ensure single CPU core overloaded event is logged (Automated)

Profile Applicability:

- Level 1

Description:

Add log-single-cpu-high option under config system global. When enabled, CPU single core usage will be polled every three seconds, and any single CPU core usage above the CPU usage threshold will report an event log. If a core is reported, that core will not be checked again for the next 30 seconds.

Rationale:

There are instances where overall CPU usage is low, but there is a single CPU core that is overloaded. But because reporting and dashboard in FortiGate shows the overall CPU usage, a single CPU core spike may get overlooked on a FortiGate with multiple CPU cores. This causes performance issues where there are instances which traffic has been stopped processing.

Audit:

On CLI:

```
config system global
get
```

Ensure that `log-single-cpu-high` is enabled.

Remediation:

On CLI:

```
config system global
    set log-single-cpu-high enable
end
```

Default Value:

Disabled

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Enable-logging-for-single-core-CPU-spike-against/ta-p/293010
2. https://docs.fortinet.com/document/fortigate/7.2.4/fortios-release-notes/743723/new-features-or-enhancements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

2.1.13 Ensure Hostname is Not Displayed On Login GUI (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that the device hostname is not displayed on the GUI login page

Rationale:

The hostname of the device may be displayed on the GUI login page which may provide information for reconnaissance

Audit:

From the CLI run the command:

```
FGT1 # get system global | grep -f gui-display
gui-display-hostname: disable  <---
```

If "gui-display-hostname" is set to disable the hostname will not be displayed on the login screen

Remediation:

To disable "gui-display-hostname"

In the CLI:

```
FGT1 # config system global
FGT1 (global) # set gui-display-hostname disable
FGT1 (global) # end
FGT1 #
```

Default Value:

Default Value for "gui-display-hostname" is disable

2.2 Password Policy

This Section contains criteria for local passwords such as complexity and restrictions. The best practice is to use named accounts, and if possible a back-end authentication solution such as Active Directory or (best case) a two-factor authentication solution. However, local credentials will always exist, if only to account for the failure of a back-end authentication solution.

2.2.1 Ensure 'Password Policy' is enabled (Automated)

Profile Applicability:

- Level 1

Description:

It is important to use secure and complex passwords for preventing unauthorized access to the FortiGate device.

Rationale:

Attackers can use brute force password software to launch more than just dictionary attacks. Such attacks can discover common passwords where a letter is replaced by a number or symbol. Center for Internet Security (CIS) recommends that passwords should be at least 14 characters long with no limit on the enforced maximum number of characters

Impact:

Weak passwords can be easily discovered by hackers, which leads to unauthorized access to FortiGate. Depending on the access privilege of the compromised account, the attacker may modify important settings.

Audit:

Currently implemented password policy can be shown from GUI or CLI

From CLI, type:

```
get system password-policy
```

Or from GUI as follows:

```
1) Log in to FortiGate with a user with at least read-only privileges
2) Go to 'System' > 'Settings'
3) Find and check the status of the 'Password Policy' Section
4) Ensure 'Password scope' is 'Both'
5) Ensure 'Minimum length' to '14'
```

The recent update by NIST on password policy has shifted focus to password length, since longer passwords are harder to crack with brute-force attacks. Not enforcing password complexity such as symbols and numbers can be easier for users to remember without being predictable.

NIST also is now recommending password resets in the case of a credential breach only.

Remediation:

Can be modified from CLI or GUI.

From CLI, do the following:

```
config system password-policy
        set status enable
        set apply-to admin-password ipsec-preshared-key
        set minimum-length 14
end
```

Or from GUI, do the following:

```
1) Log in to FortiGate as Super Admin
2) Go to 'System' > 'Settings'
3) Find the 'Password Policy' section
4) Default 'Password scope' is 'Off', change it to 'Both'
5) set 'Minimum length' to '14'
```

Default Value:

By default, 'Password Policy' is disabled. It can be checked from CLI as follows:

```
config system password-policy
    set status disable
end
```

Or from GUI as follows:

```
1) Log in to FortiGate as Super Admin
2) Go to 'System' > 'Settings'
3) Find the 'Password Policy' section
4) Default 'Password scope' is 'Off'
```

References:

1. https://pages.nist.gov/800-63-4/sp800-63b.html
2. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/127236326/config-system-password-policy
3. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/364729

Additional Information:

Consider the following to ensure better security:

- Do not use passwords that are obvious, such as the company name, administrator names, or other obvious words or phrases.
- Administrator passwords can be up to 64 characters.
- Use multiple words together, or possibly even a sentence, for example: correcthorsebatterystaple.
- Make note of the password and store it in a safe place away from the management computer, in case you forget it; or ensure at least two people know the password in the event one person becomes unavailable. Alternatively, have two different admin logins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.2.2 Ensure administrator password retries and lockout time are configured (Automated)

Profile Applicability:

- Level 1

Description:

Failed login attempts can indicate malicious attempts to gain access to your network. To prevent this security risk, FortiGate is preconfigured to limit the number of failed administrator login attempts. After the maximum number of failed login attempts is reached, access to the account is blocked for the configured lockout period.

Rationale:

When you log in and fail to enter the correct password, you could potentially be a valid user or a hacker attempting to gain access. For this reason, best practice dictates limiting the number of failed login attempts before a lockout period in which you cannot log in for a certain period of time. Lockout period will minimize hacker attempts to gain access to the firewall.

Impact:

Attackers will keep attempting to access the device through brute force attacks without any interruption, which may lead to a successful login.

Audit:

To check the lockout options, from CLI:

```
get system global
```

from the output, check the value of the below fields:

1. `admin-lockout-threshold`
2. `admin-lockout-duration`

Ensure that `admin-lockout-threshold` is set at 3 or less and `admin-lockout-duration` is set at 900 or less

Remediation:

To configure the lockout options, from CLI:

```
config system global
        set admin-lockout-threshold 3
        set admin-lockout-duration 900
end
```

Lockout affects the offending IP address, not the entire account.

Default Value:

By default, the number of password retry attempts is set to three, allowing the administrator a maximum of three attempts at logging in to their account before they are locked out for a set amount of time (by default, 60 seconds).

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/339914554/config-system-global

Additional Information:

The number of attempts and the default wait time before the administrator can try to enter a password again can be configured using the CLI.

A maximum of ten retry attempts can be configured, and the lockout period can be 1 to 2147483647 seconds (over 68 years).

The higher the retry attempts, the higher the risk that someone might be able to guess the password.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.3 SNMP

2.3.1 Ensure only SNMPv3 is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Ensuring that only SNMPv3 service is enabled and SNMPv1, SNMPv2c are disabled.

Rationale:

SNMP Version 3 provides security enhancements that are not available in SNMP Version 1 or SNMP Version 2c. SNMP Versions 1 and 2c transmit data between the SNMP server and SNMP agent in clear text. SNMP Version 3 adds authentication and privacy options to secure protocol operations. Some firewalls need to be constantly monitored of its performance and status, especially if the firewalls are critical to the operation. Enabling SNMPv3 will ensure that the firewall is monitored properly.

Impact:

Some older SNMP servers that only run SNMPv1 or SNMPv2c will not be able to query to this firewall.

Audit:

From CLI, check to make sure that there is not any community for SNMPv1 or SNMPv2c and only SNMPv3 users are there. Also make sure that SNMP Agent is enabled:

```
FGT1 # config system snmp sysinfo
FGT1 (sysinfo) # show
config system snmp sysinfo
        set status enable
        ...
end
FGT1 (sysinfo) # end
FGT1 # config system snmp community
FGT1 (community) # show
config system snmp community
end
FGT1 (community) # end
FGT1 # config system snmp user
FGT1 (user) # show
config system snmp user
    edit "snmp_test"
        set security-level auth-priv
        set auth-proto sha256
        set auth-pwd ENC xxxxxx
        set priv-proto aes256
        set priv-pwd ENC xxxxxx
    next
end
```

In the GUI, go to:

```
1. System > SNMP. Make sure that SNMP agent is enabled.
2. Make sure that there is not any SNMPv1/2c community.
3. Make sure that there is at least 1 SNMPv3 user in the list.
```

Remediation:

To enable SNMP agent in CLI:

```
FGT1 # config system snmp sysinfo
FGT1 (sysinfo) # set status enable
FGT1 (sysinfo) # end
```

In GUI, go to System > SNMP and enable SNMP Agent.

To delete SNMPv1/2c communities. In this example, we'll delete community "public" in CLI:

First, to identify the community, run

```
FGT1 # config system snmp community
FGT1 (community) # show
config system snmp community
    edit 1
        set name "public"
        config hosts
            edit 1
            next
        end
    next
end
```

This shows that the community public has ID 1

```
FGT1 # config system snmp community
FGT1 (community) # delete 1
FGT1 (community) # end
FGT #
```

In the GUI, go to:

```
System > SNMP, select the community and click on the Delete button.
```

To add SNMPv3 user in CLI:

```
FGT1 # config system snmp user
FGT1 (user) # edit "snmp_test"
FGT1 (snmp_test) # set security-level auth-priv
FGT1 (snmp_test) # set auth-proto sha256
FGT1 (snmp_test) # set auth-pwd xxxx
FGT1 (snmp_test) # set priv-proto aes256
FGT1 (snmp_test) # set priv_pwd xxxx
FGT1 (snmp_test) # end
FGT1 #
```

In the GUI, go to:

```
1. System > SNMP, under SNMPv3, click on "Create New" button.
2. Select "Authentication" and choose SHA256 as Authentication algorithm.
3. Click "Change" to type in the password.
4. Also select option "Private", choose AES256 as Encryption Algorithm.
5. Click on "Change" to change the password. Click "OK" to add the new user.
6. Click apply to apply the new setting into the current config.
```

Default Value:

By default, SNMP agent is disabled.

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-Configure-FortiGate-SNMP-Agent-for/ta-p/196866?externalID=FD45755
2. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/325005/basic-configuration

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions Manage all network devices using multi-factor authentication and encrypted sessions.		●	●

2.3.2 Allow only trusted hosts in SNMPv3 (Manual)

Profile Applicability:

- Level 2

Description:

Ensuring that only certain hosts are able to conduct SNMP GET or receive SNMP Trap.

Rationale:

SNMP offers rich information that can be useful for reconnaissance activity. Hence, limiting this information to only relevant devices such as NMS (Network Monitoring System) or other SNMP servers is necessary.

Audit:

From CLI:

```
FGT1 # show system snmp user
config system snmp user
    edit "snmp_test"
        set notify-hosts 192.168.1.101
        set security-level auth-priv
        set auth-proto sha512
        set auth-pwd ENC xxxxx
        set priv-proto aes256
        set priv-pwd ENC xxxxx
    next
end
```

Validate that "notify-hosts" is configured with specific IP address, and there is no "0.0.0.0" configured.

From GUI:

```
1. System > SNMP.
2. On SNMPv3 section, double click on the configured SNMPv3 settings.
3. Ensure that "Hosts" is configured with specific IP address, and there is
no "0.0.0.0" configured.
```

Remediation:

To remove 0.0.0.0 from trusted hosts in CLI:

```
FGT1 # config system snmp user
FGT1 (user) # edit "snmp_test"
FGT1 (snmp_test) # unselect notify-hosts 0.0.0.0
FGT1 (snmp_test) # end
FGT1 #
```

From GUI:

```
1. System > SNMP.
2. On SNMPv3 section, double click on the configured SNMPv3 settings.
3. Remove 0.0.0.0 from "Hosts" option.
```

Default Value:

By default, no SNMP is configured.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/325005/basic-configuration

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●
v7	12.2 Scan for Unauthorized Connections across Trusted Network Boundaries Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.		●	●

2.3.3 Disable SNMPv3 Query Per User (Automated)

Profile Applicability:

- Level 2

Description:

Disabling SNMP query for SNMPv3 Users that only need to receive SNMP traps

Rationale:

SNMP can contain information that is useful for reconnaissance, SNMP queries allow devices to send requests for information, disabling this on SNMPv3 users that do not need to query and only need to receive SNMP traps is necessary.

Audit:

```
From CLI:
config system snmp user
    edit "snmp_test"
        set queries disable
        set notify-hosts 192.168.1.101
        set security-level auth-priv
        set auth-proto sha512
        set auth-pwd ENC xxxxxx
        set priv-proto aes256
        set priv-pwd ENC xxxxxx
    next
end
```

Validate that "set queries" is disabled

```
From GUI:
1. System > SNMP
2. On SNMPv3 settings double click on the SNMPv3 user to modify
3. Ensure that the slider for "Queries" is disabled
```

Remediation:

To disable Queries for a specific SNMPv3 User in CLI:

{snmp_test is the example SNMPv3 username}

```
FGT1 # config system snmp user
FGT1 (user) # edit snmp_test
FGT1 (snmp_test) # set queries disable
FGT1 (snmp_test) # next
FGT1 (user) # end
```

To disable Queries for a specific SNMPv3 User in GUI:

```
1. System > SNMP
2. Under the SNMPv3 section select the specific user and double click or
single click and select edit
3. Under the Queries section click the slider for "Enabled" so it is turned
off
```

Default Value:

By Default SNMPv3 Users allow Queries

2.3.4 Enabling SNMP trap for memory usage (Automated)

Profile Applicability:

- Level 1

Description:

Enabling SNMP traps for memory usage monitoring helps detect anomalies and ensure critical security features remain operational. This proactive approach enhances system reliability by alerting administrators to potential resource issues.

Rationale:

Monitoring memory usage via SNMP traps ensures that critical security processes have sufficient resources to operate effectively. This helps prevent performance degradation or failures that could expose the system to security risks.

Impact:

Memory usage reaching critical status will automatically turn FortiGates into conserve mode which will impact security inspection.

Audit:

In the example below, SNMP trap will trigger once memory usage is above 80% (less than 20% free memory), and the freeable memory is more than 35% (memory that can be reclaimed by the system when needed).

From CLI, enable SNMP trap trap-free-memory-threshold and trap-freeable-memory-threshold.

```
FGT1 # config system snmp sysinfo
FGT1 (sysinfo) # show
config system snmp sysinfo
    set status enable
    set trap-free-memory-threshold 20
    set trap-freeable-memory-threshold 50
end
```

Remediation:

To configure SNMP trap trap-free-memory-threshold and trap-freeable-memory-threshold. From CLI:

```
FGT1 # config system snmp sysinfo
FGT1 (sysinfo) # show
config system snmp sysinfo
    set status enable
    set trap-free-memory-threshold 20
    set trap-freeable-memory-threshold 50
end
```

Default Value:

trap-free-memory-threshold is set to 5 trap-freeable-memory-threshold is set to 60

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/943586

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

2.4 Administrators and Admin Profiles

2.4.1 Remove default admin user and create one with other name (Automated)

Profile Applicability:

- Level 1

Description:

Before deploying any new FortiGate, it is important to change the password of the default admin account.

It is also recommended that you change even the user name of the default admin account, However, since you cannot change the user name of an account that is currently in use, a second administrator account must be created in order to do this.

Rationale:

Default credentials are well documented by most vendors, including Fortinet. Therefore, it will be one of the first things that will be tried to illegally gain access to the system.

Impact:

If not changed, then any scripts that use default credentials will be able to access the system.

Audit:

Using both CLI and GUI, in the username field put in "admin", leave the password field blank and proceed. If it's checked out, it means that the default password is still in place and needs to be changed.

Remediation:

First create an other local admin account, for example mycompanyadmin.

```
#if VDOM enabled
config global
#configure new admin
config system admin
     edit "mycompanyadmin"
         set password
         set accprofile "super_admin"
     next
end
```

Verify if the newly created login works by opening another CLI session, do not logout of your current session.

Once validated, logout with the default local admin account and use the CLI session with mycompanyadmin to delete the default local admin account.

Please make sure there are no references in the configuration to the account (groups, etc.)

```
#if VDOM enabled
config global
 config system admin
     delete "admin"
 end
```

To change the default password in the GUI:

```
Global (if VDOM enabled) > System > Administrators
```

Create New admin account (mycompanyadmin) Verify if you can login with that account via another browser session (eg. incognito mode).

Remove default admin

```
System > Administrators menu
```

Default Value:

By default, your FortiGate has an administrator account set up with the username admin and no password. In order to prevent unauthorized access to FortiGate, it is highly recommended that you add a password to this account.

Username: admin **The default admin account does not have any password. Just leave it blank**

References:

1. https://kb.fortinet.com/kb/documentLink.do?externalID=FD48763
2. https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/99980/default-administrator-password

Additional Information:

In FortiOS 6.2.1 and later, adding a password to the admin administrator is mandatory. You will be prompted to configure it the first time you log in to the FortiGate using that account, after a factory reset, and after a new image installation.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●

2.4.2 Ensure all the login accounts having specific trusted hosts enabled (Manual)

Profile Applicability:

- Level 1

Description:

Configure an administrative account to be accessible only to someone who is using a trusted host. You can set a specific IP address for the trusted host or use a subnet.

Rationale:

Access to a firewall to perform administrative tasks should only come from specific network segments reserved for administrators only. This additional layer of security ensures that no one from anywhere else on the network is able to log in, even with correct credentials.

Impact:

All access outside of the allowed segment will be stopped, including from both legitimate and illegitimate users. Thus, administrators working remotely will have to make sure that they have access to jump hosts that sit in the allowed segment.

Audit:

This example is to check if trusted hosts option is enabled for account "test_admin" and which trusted hosts are in the list:

```
FG1 # config system admin
FG1 (admin) # edit "test_admin"
FG1 (test_admin) # show
config system admin
        edit "test_admin"
                ...
                set trusthost1 10.0.0.0 255.255.255.0
                set trusthost2 192.168.10.0 255.255.255.0
                ...
        next
end
```

In the Web GUI:

```
1. System > Administrators.
2. Select the account and click on edit.
3. In the account setting page, make sure that "Restrict login to trusted
hosts" is enabled and all the allowed hosts / subnets are in the list of
trusted host.
```

Please take note that certain versions of FortiOS will only show the first 3 trusted hosts in the list. If you want to see more, you have to click on the "+" sign as if you're adding a new item into the list. Keep clicking until you see an empty field of trusted host. That's when you know that you have reached the bottom of the list.

Remediation:

To remove a trusted host item from the list in CLI:

```
FG1 # config system admin
FG1 (admin) # edit "test_admin"
FG1 (test_admin) # unset trusthost1
FG1 (test_admin) # end
FG1 #
```

To add a trusted host into the list in CLI:

```
FG1 # config system admin
FG1 (admin) # edit "test_admin"
FG1 (test_admin) # set trusthost6 1.1.1.1 255.255.255.255
FG1 (test_admin) # end
FG1 #
```

Before adding an item, please make sure that it does not already exist. For example, if trusthost3 is already in the list, using it again will override the existing host/network.

In the Web GUI:

```
1. System > Administrators.
2. select the account and click on edit.
3. In the account setting page, make sure that "Restrict login to trusted
hosts" is enabled and all the allowed hosts / subnets are in the list of
trusted host.
```

Please take note that certain versions of FortiOS will only show the first 3 trusted hosts in the list. If you want to see more, you have to click on the "+" sign as if you're adding a new item into the list. Keep clicking until you see an empty field of trusted host. That's when you know that you have reached the bottom of the list. To add another trusted host, fill in the empty field of the new "Trusted Host". To remove a trusted host, simply erase everything in the field of that corresponding host.

Default Value:

By default, each account is accessible from everywhere. The host value is 0.0.0.0/0

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/14906

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●
v7	11.6 Use Dedicated Machines For All Network Administrative Tasks Ensure network engineers use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be segmented from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.		●	●
v7	11.7 Manage Network Infrastructure Through a Dedicated Network Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

2.4.3 Ensure admin accounts with different privileges have their correct profiles assigned (Manual)

Profile Applicability:

- Level 1

Description:

Verify that users with access to the Fortinet should only have the minimum privileges required for that particular user.

Rationale:

In some organizations, it is necessary to create different levels of administrative accounts. For example, technicians from tier 1 support should not have total access to the system compared to a tier 3 support.

Audit:

There are 2 stages to audit. Here is how to verify in the CLI:

Stage 1: Verify the profile.

```
FGT1 # config system accprofile
FGT1 (accprofile) # edit "tier_1"
FGT1 (tier_1) # show full
config system accprofile
    edit "tier_1"
        set comments ''
        set secfabgrp read
        set ftviewgrp read
        set authgrp none
        set sysgrp none
        set netgrp read
        set loggrp none
        set fwgrp custom
        set vpngrp none
        set utmgrp none
        set wifi none
        set admintimeout-override disable
        config fwgrp-permission
            set policy none
            set address none
            set service none
            set schedule none
        end
    next
end
FGT1 (tier_1) #
```

If the following privileges are set to "custom", please also check the sub-privileges of the customized ones to make sure that only the right privileges are allowed: fwgrp, sysgrp, netgrp, loggrp, utmgrpset.

In the GUI, go to:

```
System > Admin Profiles, select the profile and click on "Edit".
```

Stage 2: Verify the admin accounts.

In the CLI:

```
FGT1 #config system admin
FGT1 (admin) # edit "support1"
FGT1 (support1) # show full
config system admin
  edit "support1"
    ...
    set accprofile "tier_1"
    ...
  next
end
```

In the GUI, go to:

```
System > Administrators, select the account and click "Edit"
```

Remediation:

In this example, the goal is to provide the profile "tier_1" the ability to view and modify address objects. This sub-privilege is under fwgrp privilege.

In CLI:

```
FGT1 # config system accprofile
FGT1 (accprofile) # edit "tier_1"
FGT1 (tier_1) # set fwgrp custom
FGT1 (tier_1) # config fwgrp-permission
FGT1 (fwgrp-permission) # set address read-write
FGT1 (fwgrp-permission) # end
FGT1 (tier_1) # end
FGT1 #
```

For the GUI, go to:

```
1. System > Admin Profiles, select "tier_1" and click "Edit".
2. On "Firewall", click on "Custom".
3. Click on "Read/Write" option for "Address".
```

In the next example, assign the profile "tier_1" to the account "support1".

In the CLI:

```
FGT1 # config system admin
FGT1 (admin) # edit "support1"
FGT1 (support1) # set accprofile "tier_1"
FGT1 (support1) # end
FGT1 #
```

For the GUI, go to:

```
1. System > Administrators.
2. Select "support1" and click "Edit".
3. Under "Administrator Profile", select "tier_1".
```

Default Value:

By default, there are only 2 profiles: prof_admin and super_admin. You must select a profile to create an admin account. The system will not automatically choose for you.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/294491

Additional Information:

You cannot change the profile of the account you are already logged in as.

The profile "super_admin" cannot be deleted or modified.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.4.4 Ensure Admin idle timeout time is configured (Automated)

Profile Applicability:

- Level 1

Description:

The idle timeout period is the amount of time that an administrator will stay logged in to the GUI without any activity.

Rationale:

Best practice dictates setting admin idle timeout to prevent the risk of unauthorized access to the device, such as someone using a logged-in GUI on a PC that has been left unattended.

For security reasons, the Center for Internet Security (CIS) recommends that administrator sessions should automatically timeout after a period of inactivity, with a maximum recommended time of 15 minutes or less

Impact:

This is to prevent someone from accessing the FortiGate if the management PC is left unattended.

Audit:

To check the idle timeout in the GUI:

```
1) Login to FortiGate
2) Go to 'System' > 'Settings'.
3) In the 'Administration Settings' section, check the 'Idle timeout' value
in minutes.
```

To check the idle timeout in the CLI:

```
get system global
```

check the value of `admintimeout` in minutes

Remediation:

To change the idle timeout in the GUI:

```
1) Login to FortiGate with Super Admin privileges
2) Go to 'System' > 'Settings'.
3) In the 'Administration Settings' section, set the 'Idle timeout' value to
five minutes by typing 5.
4) Click Apply.
```

To change the idle timeout in the CLI:

```
config system global
        set admintimeout 5
end
```

Default Value:

By default, it is set to five minutes.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/215451

Additional Information:

A setting of higher than 15 minutes will have a negative effect on a security rating score.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.4.5 Ensure only encrypted access channels are enabled (Automated)

Profile Applicability:

- Level 1

Description:

Allow only HTTPS access to the GUI and SSH access to the CLI.

Rationale:

By only allowing encrypted access, we are making it harder to use "Man in the Middle" attacks to sniff login credentials.

Audit:

In the CLI, when verifying the network interface, make sure that http and telnet are not in the `allowaccess` list:

```
FG1 # config system interface
FG1 (interface) # edit port1
FG1 (port1) # show
config system interface
        edit "port1"
                ...
                set allowaccess ssh https ping snmp
                ...
        next
end
```

In the web GUI, click on:

```
1. Network > Interfaces, select the interface and click "Edit".
2. In the interface setting page, make sure that HTTP and Telnet are not
selected in the section "Administrative Access"
```

Remediation:

If HTTP or Telnet is in the `allowaccess` list, you will have to set that list again with the same elements except for http or telnet.

On CLI:

```
FG1 # config system interface
FG1 (interface) # edit port1
FG1 (port1) # set allowaccess ssh https ping snmp
FG1 (port1) # end
FG1 #
```

In the web GUI, click on:

```
1. Network > Interfaces, select the interface and click "Edit".
2. In the interface setting page, uncheck HTTP and Telnet in the section
"Administrative Access".
```

Default Value:

By default, HTTP and Telnet are not enabled on any interface.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/574723

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

2.4.6 Apply Local-in Policies (Automated)

Profile Applicability:

- Level 1

Description:

Configure Local-in Policies to control inbound traffic that is destined to a FortiGate interface.

Rationale:

Local-in Policies allow for more granular and specific control of all types of traffic that are destined for a FortiGate interface. They are not limited to management-only protocols, therefore they can extend past "trusted host" configurations and be configured with source and destination addresses as well as specific services.

Impact:

Local-in Policies are processed before "trusted host" configurations, so it is important to validate that management access will be maintained once the Local-in policies are put in place.

Audit:

To review Local-in Policies in the GUI, go to:

```
1. System > Feature Visibility.
2. Turning on "Local-in policies" under the Additional Features Section.
```

This will then add the section under "Policies and Objects" there will now be a section for "Local-in Policies"

It can also be viewed through the CLI:

```
config firewall local-in-policy
show
```

Remediation:

Local-in Policies can only be configured through the CLI:

```
config firewall {local-in-policy | local-in-policy6}
    edit <policy_number>
        set intf <interface>
        set srcaddr <source_address> [source_address] ...
        set dstaddr <destination_address> [destination_address] ...
        set action {accept | deny}
        set service <service_name> [service_name] ...
        set schedule <schedule_name>
        set comments <string>
    next
end
```

For example, to prevent the source subnet 10.10.10.0/24 from pinging port1, but allow administrative access for PING on port1:

```
config firewall address
    edit "10.10.10.0"
        set subnet 10.10.10.0 255.255.255.0
    next
end
config firewall local-in-policy
    edit 1
        set intf "port1"
        set srcaddr "10.10.10.0"
        set dstaddr "all"
        set service "PING"
        set schedule "always"
    next
end
```

Default Value:

There are no Local-in Policies in place by default.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/363127

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.4.7 Ensure default Admin ports are changed (Automated)

Profile Applicability:

- Level 1

Description:

FortiGate admin ports listen on the common ports of 80 and 443. This is default behavior. While interface access is controlled by configuring network interfaces, the FortiGate still listens on the admin ports that have been configured, which can also cause a conflict should 80 or 443 be needed as part of additional configuration later on.

Rationale:

To increase security of the FortiGate Admin Ports, changing it from the default ports will reduce the attack surface should FortiGate Admin Access be targeted. As mentioned, a possible port conflict can also be avoided.

Impact:

Unauthorized access to a FortiGate or any firewall could prove very costly. While this is a single hardening step of many, it is an important one when hardening any firewall.

Audit:

Log in to the GUI and click on System > Settings > Review the ports under 'Administration Settings' section.

Remediation:

```
config system global
    set admin-https-redirect disable
    set admin-port 8082 **(or any other uncommon port)**
    set admin-server-cert "self-sign"
    set admin-sport 4343 **(or any other uncommon port)**
end
```

OR

From Web GUI:

```
1. System > Settings
2. Change the ports/settings under 'Administration Settings' section.
```

NOTE: https redirection must be turned off as well as changing port 80. This is due to the nature of how browser port redirection works. The browser will be redirected from port 80 to port 443 or whichever 'admin-sport' is configured, meaning that it will still listen on port 80 even when the port has been reconfigured.

Default Value:

```
config system global
    set admin-https-redirect enable
    set admin-port 80
    set admin-server-cert "self-sign"
    set admin-sport 443
```

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/616955
2. https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-change-the-port-for-the-admin-access-to/ta-p/192295?externalID=FD46981

Additional Information:

TIP: Don't choose these ports:

```
8080/8081 - These are very common browser proxy ports.
4433 - This is the FortiGate default FTM push port.
10443 - This is the FortiGate default SSL VPN port.
```

Other Admin Ports such as 22 and 23 can also be changed as required.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

2.4.8 Virtual patching on the local-in management interface (Automated)

Profile Applicability:

- Level 1

Description:

Allow virtual patching to be applied to traffic destined to the FortiGate by applying IPS signatures to the local in interface using local in policies. Attacks geared towards GUI and SSH management access, for example, can be mitigated using IPS signatures pushed from FortiGuard, thereby virtually patching these vulnerabilities.

The FortiGate must have a valid FMWR (Firmware) license to install the FMWP database. The FMWP database can be viewed by running the `diagnose autoupdate versions` command.

Rationale:

Patches require scheduling of downtime, which means there is some attack window from the time Fortinet announced the vulnerability to when patch is applied. To minimise the risk, virtual patching on GUI and SSH management access is needed.

Audit:

On CLI:

```
config firewall local-in-policy
show
```

Ensure that `virtual-patch` is enabled for those policy that is allowing traffic.

Remediation:

On CLI:

```
config firewall local-in-policy
    edit <id>
        set virtual-patch enable
    next
end
```

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/393161

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.5 Deploy Automated Software Patch Management Tools Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●

2.5 High Availability

High Availability (HA) subsection includes configurations for High Availability between FortiGate devices

2.5.1 Ensure High Availability configuration is enabled (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that FortiGate devices are configured for High Availability (HA).

Rationale:

Configuring High Availability (HA) increases system availability as well as decreases impact of routine maintenance (Firmware updates, cable moves, etc.) and the the impact of device failure.

Impact:

Not having High Availability (HA) configured correctly and synced properly impacts the availability of the FortiGate devices as well as any systems that require traversing the FortiGates. With properly configured HA in place outages can be minimized during firmware updates as well as if there are power outages or device failures.

Audit:

In GUI:

```
1. Navigate to "System" and then "HA"
2. Ensure "Mode" is set to proper setting "Active-Active" or "Active-Passive"
3. Review Configuration settings:
        - "Cluster Name" must match on devices
        - "Password" Must match on devices
        - "Heartbeat Interfaces" need to be defined on devices
4. Click "OK" to save changes and exit
```

In CLI:

```
FGT1 # config system ha
FGT1 (ha) # set mode a-p                        ###(Active-Passive)
FGT1 (ha) # set group-name "FGT-HA"             ###(Set cluster name)
FGT1 (ha) # set password *******                ###(Set password)
FGT1 (ha) # set hbdev port10 50                         ###(Set Heartbeat
Interface and priority)
FGT1 (ha) # end
```

To review configuration in CLI:

```
FGT1 # config system ha
FGT1 (ha) # show
config system ha
    set group-name "FGT-HA"
    set mode a-p
    set password ENC
enrwD467hJmO6j6YW/l6FEOa1YNVYdo8Z5mCcTDEKUFpOVXcNYnPBmQDGX//ViXk6TkwNH0il5aJr
/fZY25lq+husndQHZVWp2LIlXmCv/n81U43nkZUWaIKvqkellGFbhv0/IHoOLzQPCsVcBbyrsgopr
YMvh6w7F06+nRriBtMNQxpOV5V+e388EcwsOOMsXBZOw==
    set hbdev "port10" 50
    set override disable
end
```

Remediation:

In GUI:

```
1. Navigate to "System" and then "HA"
2. Ensure "Mode" is set to proper setting "Active-Active" or "Active-Passive"
3. Review Configuration settings:
        - "Cluster Name" must match on devices
        - "Password" Must match on devices
        - "Heartbeat Interfaces" need to be defined on devices
4. Click "OK" to save changes and exit
```

In CLI:

```
FGT1 # config system ha
FGT1 (ha) # set mode a-p                        ###(Active-Passive)
FGT1 (ha) # set group-name "FGT-HA"             ###(Set cluster name)
FGT1 (ha) # set password *******                ###(Set password)
FGT1 (ha) # set hbdev port10 50                         ###(Set Heartbeat
Interface and priority)
FGT1 (ha) # end
```

To review configuration in CLI:

```
FGT1 # config system ha
FGT1 (ha) # show
config system ha
    set group-name "FGT-HA"
    set mode a-p
    set password ENC
enrwD467hJmO6j6YW/l6FEOa1YNVYdo8Z5mCcTDEKUFpOVXcNYnPBmQDGX//ViXk6TkwNH0il5aJr
/fZY25lq+husndQHZVWp2LIlXmCv/n81U43nkZUWaIKvqkellGFbhv0/IHoOLzQPCsVcBbyrsgopr
YMvh6w7F06+nRriBtMNQxpOV5V+e388EcwsOOMsXBZOw==
    set hbdev "port10" 50
    set override disable
end
```

Default Value:

N/A

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/357558
2. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/900885

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.2 Ensure "Monitor Interfaces" for High Availability devices is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Configure Interface Monitoring within High Availability settings. `Interface Monitoring` should be enabled on all critical interfaces.

Rationale:

With `Interface Monitoring` enabled on devices, failover can occur if there are physical media issues or issues with the specific port to which the FortiGate is connected.

Impact:

Not configuring Interface Monitoring can directly impact services due to a failure to trigger a High Availability failover if an interface is impacted only on the primary device and is not being monitored. Without the `Interface Monitoring` enabled, failover would be limited to hardware, system, or power faults.

Audit:

To validate from GUI:

```
1. Go to System > HA.
2. Under "Monitor Interfaces" validate all applicable interfaces are
selected.
3. Select "OK".
```

To validate from CLI:

```
FGT1 # config system ha
FGT1 (ha) # show
config system ha
    set group-name "FGT-HA"
    set mode a-p
    set password ENC
enrwD467hJmO6j6YW/l6FEOa1YNVYdo8Z5mCcTDEKUFpOVXcNYnPBmQDGX//ViXk6TkwNH0il5aJr
/fZY25lq+husndQHZVWp2LIlXmCv/n81U43nkZUWaIKvqkellGFbhv0/IHoOLzQPCsVcBbyrsgopr
YMvh6w7F06+nRriBtMNQxpiTE+12xAHz7lA3EoYZzf8A==
    set override disable
    set monitor "port6" "port7"   ###Validate proper interfaces are present
end
```

Remediation:

To remediate from GUI:

```
1. Go to System > HA.
2. Under "Monitor Interfaces" select all applicable interfaces.
3. Select "OK".
```

To validate from CLI:

```
FGT1 # config system ha
FGT1 (ha) # set monitor "port6" "port7"
FGT1 (ha) # show  ###To Review changes to monitored interfaces before
applying
config system ha
    set group-name "FGT-HA"
    set mode a-p
    set password ENC
enrwD467hJmO6j6YW/l6FEOa1YNVYdo8Z5mCcTDEKUFpOVXcNYnPBmQDGX//ViXk6TkwNH0il5aJr
/fZY25lq+husndQHZVWp2LIlXmCv/n81U43nkZUWaIKvqkellGFbhv0/IHoOLzQPCsVcBbyrsgopr
YMvh6w7F06+nRriBtMNQxpiTE+12xAHz7lA3EoYZzf8A==
    set override disable
    set monitor "port6" "port7"
end
```

Default Value:

N/A

References:

1. https://docs.fortinet.com/document/fortigate/6.0.0/best-practices/498515/interface-monitoring-port-monitoring

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.3 Ensure HA Reserved Management Interface is configured (Automated)

Profile Applicability:

- Level 1

Description:

Ensure `Reserved Management Interfaces` are configured on HA devices.

Rationale:

To be able to access both the primary and secondary firewalls in an HA cluster, `Reserved Management Interfaces` need to be configured to prevent them from syncing with HA and sharing a virtual MAC address.

Impact:

Not configuring `Reserved Management Interfaces` impacts the ability to access secondary devices directly due to the primary and secondary devices syncing configuration exactly and floating a virtualized mac address between them for failover.

Audit:

Review through the GUI:

```
1. Go to System > HA edit the "Master" device.
2. Verify that "Management Interface Reservation" is selected and there is an
interface, and gateway defined.
```

Review through the CLI:

```
FGT1 #config system ha
FGT1 (ha) # show
config system ha
    set group-name "FGT-HA"
    set mode a-p
    set password ENC
enrwD467hJmO6j6YW/l6FEOa1YNVYdo8Z5mCcTDEKUFpOVXcNYnPBmQDGX//ViXk6TkwNH0il5aJr
/fZY25lq+husndQHZVWp2LIlXmCv/n81U43nkZUWaIKvqkellGFbhv0/IHoOLzQPCsVcBbyrsgopr
YMvh6w7F06+nRriBtMNQxpiTE+12xAHz7lA3EoYZzf8A==
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port6"
            set gateway 10.10.10.1
        next
    end
    set override disable
end
```

Validate that `set ha-mgmt-status` is enabled and that `config ha-mgmt-interfaces` has at least one entry with an interface and gateway defined.

Remediation:

Remediate through the GUI:

```
1. Go to System > HA edit the "Master" device.
2. Enable "Management Interface Reservation" once this is enabled select an
an interface, and configure the appropriate gateway.
```

Remediate through the CLI:

```
FGT1 #config system ha
FGT1 (ha) # set ha-mgmt-status enable
FGT1 (ha) # config ha-mgmt-interfaces
FGT1 (ha-mgmt-interfaces) # edit 1
new entry '1' added
FGT1 (1) # set interface port6
FGT1 (1) # set gateway 10.10.10.1
FGT1 (1) # end
FGT1 (ha) # show
config system ha
    set group-name "FGT-HA"
    set mode a-p
    set password ENC
enrwD467hJmO6j6YW/l6FEOa1YNVYdo8Z5mCcTDEKUFpOVXcNYnPBmQDGX//ViXk6TkwNH0il5aJr
/fZY25lq+husndQHZVWp2LIlXmCv/n81U43nkZUWaIKvqkellGFbhv0/IHoOLzQPCsVcBbyrsgopr
YMvh6w7F06+nRriBtMNQxpiTE+12xAHz7lA3EoYZzf8A==
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port6"
            set gateway 10.10.10.1
        next
    end
    set override disable
end
FGT1 (ha) # end
```

Default Value:

N/A

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/313152

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

2.5.4 Ensure High Availability Group-ID is configured (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that FortiGate High Availability (HA) configuration has non-default "Group-ID"

Rationale:

High Availability (HA) allows a FortiGate cluster to float a virtual MAC address between devices to minimize downtime if there is a failover event. This Virtual MAC address is generated using the GROUP-ID so to prevent possible duplicate MAC addresses on Layer 2 of the network configuring a non-default Group-ID is needed.

Impact:

Not modifying the Group-ID attribute in HA could allow a duplicate MAC address from another default FortiGate having HA configured which can cause problems if they are both within the same network

Audit:

In the CLI:

```
FGT1 # show sys ha
config system ha
    set group-id 10
    set group-name "HAGROUP"
    set mode a-p
    set password ENC xxxxxxxx
    set hbdev "port7" 50
    set session-pickup enable
    set override disable
    set priority 200
end
```

Validate that "group-id" is present and not configured for the default of 0

```
In the GUI:

1. System > HA
2. Select the primary device and either double click to open or single click
and select edit
3. Under "Cluster Settings" Validate that "Group ID" is not 0 and has been
configured
```

Remediation:

To modify High Availability (HA) Group-ID

From the CLI:

```
FGT1 # config system ha
FGT1 (ha) # set group-id 10
FGT1 (ha) # end
FGT1 #
```

The Group ID can be any integer value from 0-1023

From the GUI:

```
1. System > HA
2. Select Primary device and either double click or single click and select
"Edit"
3. Under Cluster Settings enter a value in the "Group ID"
4. Click OK to apply
```

The Group ID can be any integer value from 0-1023

Default Value:

The default "Group-ID" value is set to 0

3 Policy and Objects

This section contains best practices related to configuring firewall policies, Objects and traffic shaping

3.1 Ensure that unused policies are reviewed regularly (Manual)

Profile Applicability:

- Level 2

Description:

All firewall policies should be reviewed regularly to verify the business purpose. Unused policies should be disabled and logged.

Recommendation to review twice per year or inline with BCP practice (Business Continuity Plan). Some of the firewall policies will only be used during BCP, hence, the hit count might show 0 if the review is done too often.

Rationale:

By reviewing policies regularly, we can determine if the policies are still needed by the business purpose. Thus, we can keep the firewall policies lean and efficient. It also prevents traffic being allowed or blocked accidently.

Audit:

In CLI, type "diag firewall iprope show 100004 <policy_id>". In this example, we'll verify policy with ID of 32. We'll also need to clear the counter after each review so that we can tell if the policy is still being used for the next review :

```
FGT1 # diag firewall iprope show 100004 32
idx=2 pkts/bytes=144967/135758174 asic_pkts/asic_bytes=0/0 flag=0x0 hit
count:663
FGT1 # diag firewall iprope clear 100004 32
```

In the GUI,

```
1. Go to Policy & Objects.
2. Click on Firewall Policy.
3. Make sure that either the columns "Bytes" or "Hit Count" are visible. To
display either one of them, move the cursor to the top row where all the
columns names are. Right click and select "Bytes" or "Hit Count" and click
OK. To clear the counter, right click on the "Bytes" or "Hit Count" columns
of that policy and click on "Clear Counters".
```

Remediation:

The remediation is to review and decide if you should delete unused policies.

Default Value:

By default, the hit count value is 0 at the beginning.

References:

1. https://kb.fortinet.com/kb/documentLink.do?externalID=FD44631

Additional Information:

The CLI commands are only available after FortiOS 6.0. Before that, please use GUI.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

3.2 Ensure that policies do not use "ALL" as Service (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all security policies in effect clearly state which protocols / services they are allowing.

Rationale:

This is to make sure that the firewall do not allow traffic with unauthorized protocols/services by mistake.

Audit:

In CLI:

```
FGT1 # config firewall policy
FGT1 (policy) # show
TEST-FG-Third (policy) # show
config firewall policy
    edit 1
        set uuid d0eed832-bb73-51e6-c3da-3cd2ec201608
        set srcintf "internal"
        set dstintf "wan"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set service "HTTPS" "HTTP"
        set ssl-ssh-profile "__tmp_no-inspection"
        set nat enable
    next
end
```

In the GUI,

```
1. Go to Policy & Objects.
2. Click on Firewall Policy.
```

Make sure that none of the policies use "ALL" as its service.

Remediation:

This is an example showing how to modify policy with ID of 2 to change the service from "ALL" to FTP and SNMP.

In CLI:

```
FGT1 # config firewall policy
FGT1 (policy) # edit 2
FGT1 (2) # set service "FTP" "SNMP"
FGT1 (2) # end
FGT1 #
```

In the GUI,

```
1. Go to Policy & Objects.
2. Click on Firewall Policy.
3. Select the policy, click "Edit".
4. In the Service section, click on it and select FTP and SNMP. Click OK.
```

Default Value:

By default, all new policy will have "ALL" in its service field.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

3.3 Ensure firewall policy denying all traffic to/from Tor, malicious server, or scanner IP addresses using ISDB (Automated)

Profile Applicability:

- Level 1

Description:

Firewall policies should include a deny rule for traffic going to/from Tor, malicious server, or scanner IP addresses using ISDB (Internet Service Database).

Rationale:

FortiGate includes Tor or malicious server related IP address using ISDB. The idea is to filter out malicious traffic using firewall policies as first level filtering. This is done without involving more resource intensive processes such as IPS inspection, hence optimizing FortiGate's performance.

Audit:

Go to "Policy & Objects".

Validate that there is a firewall policy created to block inbound connections from sources named "Tor-Exit.Node", "Tor-Relay.Node", "Censys-Scanner", "Shodan-Scanner", "Botnet-C&C.Server", "Phishing-Phishing.Server", "Proxy-Proxy.Server", "Spam-Spamming.Server", "VPN-Anonymous.VPN", and "Malicious-Malicious.Server" on "All" services.

Validate that there is a firewall policy created to block outbound connections to destination named "Tor-Relay.Node", "Botnet-C&C.Server", "Phishing-Phishing.Server", "Proxy-Proxy.Server", "Spam-Spamming.Server", "VPN-Anonymous.VPN", and "Malicious-Malicious.Server".

Note that these ISDBs is recommended as of December 2024 (FortiOS 7.4.5). Fortinet might rollout additional ISDBs to be blocked in newer versions that is not covered in this benchmark.

Remediation:

Review firewall policies and ensure there are:

1. A firewall policy created to block inbound connections with these settings:

```
From: Any
To: Any
Source: "Tor-Exit.Node", "Tor-Relay.Node", "Censys-Scanner", "Shodan-
Scanner", "Botnet-C&C.Server", "Phishing-Phishing.Server", "Proxy-
Proxy.Server", "Spam-Spamming.Server", "VPN-Anonymous.VPN", and "Malicious-
Malicious.Server"
Destination: all
Schedule: Always
Services: All
Action: Deny
Log Violation Traffic: Enabled
Enable this policy: Enabled
```

2. A firewall policy created to block outbound connections with these settings:

```
From: Any
To: Any
Source: All
Destination: "Tor-Relay.Node", "Botnet-C&C.Server", "Phishing-
Phishing.Server", "Proxy-Proxy.Server", "Spam-Spamming.Server", "VPN-
Anonymous.VPN", and "Malicious-Malicious.Server"
Schedule: Always
Action: Deny
Log Violation Traffic: Enabled
Enable this policy: Enabled
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	12.2 Scan for Unauthorized Connections across Trusted Network Boundaries Perform regular scans from outside each trusted network boundary to detect any unauthorized connections which are accessible across the boundary.		●	●
v7	12.3 Deny Communications with Known Malicious IP Addresses Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each of the organization's network boundaries,.		●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

3.4 Ensure logging is enabled on all firewall policies (Automated)

Profile Applicability:

- Level 1

Description:

Logging should be enabled for all firewall policies including the default implicit deny policy.

Rationale:

Firewall policies should log for all traffic (both allow and deny policies). This enables SOC or security analyst to do further investigations on security incidents especially on threat hunting or incident response activities. Although there are many data sources that can provide DNS query logs (AD or EDR), this option should be enabled out of best practice and with assumption that no other data sources are available.

Impact:

By default, when creating firewall policies, a logging option is not enabled. Also, the default implicit deny policy is not logged. This creates a data gap in threat hunting or incident response activities.

Audit:

Go to "Policy & Objects" > "Firewall Policy".

Validate that logging is enabled on all firewall policies.

Remediation:

Review firewall policies and ensure that:

1. For allowed policies, "Log Allowed Traffic" is set on "All Sessions" option.
2. For denied policies, "Log Violation Traffic" is enabled.

Default Value:

Logging is disabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	12.5 Configure Monitoring Systems to Record Network Packets Configure monitoring systems to record network packets passing through the boundary at each of the organization's network boundaries.		●	●
v7	12.8 Deploy NetFlow Collection on Networking Boundary Devices Enable the collection of NetFlow and logging data on all network boundary devices.		●	●

4 Security Profiles

This section contains best practices related to FortiGate security features, including:

- Inspection modes
- Antivirus
- Web filter
- Filtering based on YouTube channel
- DNS filter
- Application control
- Intrusion prevention
- File filter
- Email filter
- Data leak prevention
- VoIP solutions
- ICAP
- Web application firewall
- SSL & SSH Inspection
- Custom signatures
- Overrides

4.1 Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) Security profiles

4.1.1 Detect Botnet connections (Automated)

Profile Applicability:

- Level 2

Description:

Interfaces which are classified as "WAN" and are used by a policy should use an IPS sensor which blocks or monitors outgoing connections to botnet sites.

Rationale:

Blocking outgoing connections to known Botnets should be utilized in a Defense In Depth network design.

Audit:

On GUI:

```
1. Ensure that relevant IPS profile is configured with "Scan Outgoing
Connections to Botnet Sites" set to "Block".
2. Review all firewall policies that have a "WAN" interface as the
destination.
```

Remediation:

On GUI:

```
1. Configure relevant IPS profiles with "Scan Outgoing Connections to Botnet
Sites" set to "Block".
2. Apply relevant IPS profile on all firewall policies with traffic exiting
the network to a "WAN" interface.
```

Default Value:

"Scan Outgoing Connections to Botnet Sites" is disabled on default profile.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/668865

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.7 Deploy a Host-Based Intrusion Prevention Solution Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.			●

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.8 Deploy a Network Intrusion Prevention Solution Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			●
v7	12.7 Deploy Network-Based Intrusion Prevention Systems Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.			●
v7	15.3 Use a Wireless Intrusion Detection System Use a wireless intrusion detection system (WIDS) to detect and alert on unauthorized wireless access points connected to the network.		●	●

4.1.2 Apply IPS Security Profile to Policies (Manual)

Profile Applicability:

- Level 1

Description:

Ensuring that traffic traversing between networks on the FortiGate have an IPS security profile inspecting it.

Rationale:

Traffic moving between "interfaces" on the FortiGate should have firewall policies applied with an IPS security profile applied.

Audit:

Review **all** firewall policies and ensure that traffic has an `IPS` security profile assigned for inspection.

Remediation:

Configure on **all** "Allowed" firewall policies to have an appropriate `IPS` security profile applied to policies.

Default Value:

Not Configured

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/243446

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	12.7 Deploy Network-Based Intrusion Prevention Systems Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.			●

4.2 Antivirus

4.2.1 Ensure Antivirus Definition Push Updates are Configured (Automated)

Profile Applicability:

- Level 2

Description:

Ensure FortiGate is configured to accept antivirus definition push updates.

Rationale:

Ensure that the FortiGate will accept push updates from FortiGuard to ensure the most up to date signature databases are present on the device.

Audit:

On GUI:

```
1. Access the FortiGate administrative web access page and go to System >
FortiGuard.
2. Under "FortiGuard Updates" ensure that the "Scheduled updates" is set to
"Automatic".
```

On CLI:

```
config system autoupdate schedule
show (Validate that there are no output, meaning it is already set as
"automatic"
```

Remediation:

On GUI:

```
1. Access the FortiGate administrative web access page and go to System >
FortiGuard.
2. Under "FortiGuard Updates" ensure that the "Scheduled updates" is set to
"Automatic".
```

On CLI:

```
config system autoupdate schedule
set status enable
set frequency automatic
end
```

Default Value:

Enabled and set to automatic.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/547335

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●

4.2.2 Apply Antivirus Security Profile to Policies (Manual)

Profile Applicability:

- Level 2

Description:

Ensuring that traffic traversing between networks on the FortiGate has an Antivirus Security profile inspecting it.

Rationale:

Traffic moving between "interfaces" on the FortiGate should have firewall policies applied with an antivirus security profile applied.

Audit:

Review all firewall policies and ensure that traffic has an antivirus security profile assigned for inspection.

Remediation:

Review firewall policies and apply an appropriate antivirus security profile to policies.

Default Value:

No security inspection on firewall policies.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/243446

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●

4.2.3 Enable Outbreak Prevention Database (Automated)

Profile Applicability:

- Level 2

Description:

Ensure FortiGate AV inspection uses outbreak prevention database as an added layer of protection on top of antivirus' signature-based detection.

Rationale:

Antivirus mainly uses signature for malware blocking. By enabling "FortiGuard outbreak prevention database", FortiGate can leverage on 3rd party malware hash signatures curated by the FortiGuard as an additional protection layer.

The hash signatures are obtained from FortiGuard's Global Threat Intelligence database. The antivirus database queries FortiGuard with the hash of a scanned file. If FortiGuard returns a match, the scanned file is deemed to be malicious.

Audit:

On GUI:

```
1. Go to "Security Profiles" > "AntiVirus".
2. Select AV profile.
```

Validate that "Use FortiGuard outbreak prevention database" is enabled.

On CLI:

```
FGT1 # config antivirus profile

FGT1 (profile) # show
```

Validate that for each traffic protocol, "set outbreak-prevention block" is configured.

Remediation:

Review Antivirus Security Profiles and validate that "Use FortiGuard outbreak prevention database" is enabled.

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/889364

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●
v7	8.6 Centralize Anti-malware Logging Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		●	●

4.2.4 Enable AI /heuristic based malware detection (Automated)

Profile Applicability:

- Level 2

Description:

AI /heuristic based detection should be enabled.

Rationale:

The AV Engine AI malware detection model integrates into regular AV scanning to help detect potentially malicious Windows Portable Executables (PEs) in order to mitigate zero-day attacks. It is an additional layer of protection on top of traditional antivirus protection.

In version 6.x, it is named "Heuristic detection". On version 7.x, Fortinet has renamed this to AI based detection.

Audit:

Configuration and verification can be only done on CLI.

On CLI:

```
FGT1 # show antivirus settings | grep machine-learning-detection
```

Validate that it is enabled.

Remediation:

On CLI:

```
FGT1 # config antivirus settings
FGT1 (settings) # set machine-learning-detection enable
```

Default Value:

Enabled.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/252375733/config-antivirus-settings

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.7 Use Behavior-Based Anti-Malware Software Use behavior-based anti-malware software.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

4.2.5 Enable grayware detection on antivirus (Automated)

Profile Applicability:

- Level 2

Description:

Grayware detection should be enabled.

Rationale:

Usage of grayware is generally not allowed in strict company policies and some graywares can be used for malicious intent. If the file passes the virus scan, it can be checked for grayware. Grayware signatures are kept up to date in the same manner as the antivirus definitions.

Audit:

CLI:

```
FGT1 # show antivirus settings | grep grayware
```

Validate that grayware detection is enabled.

Remediation:

On CLI:

```
FGT1 # config antivirus settings
FGT1 (settings) # set grayware enable
```

Default Value:

Enabled in 7.4 or newer. Older versions the default is disabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/252375733/config-antivirus-settings

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	10.6 Centrally Manage Anti-Malware Software Centrally manage anti-malware software.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●

4.2.6 Ensure inline scanning with FortiGuard AI-Based Sandbox Service is enabled (Automated)

Profile Applicability:

- Level 1

Description:

Inline scanning is supported when the FortiGate is licensed with the FortiGuard AI-Based Sandbox Service (FAIS). It works similar to inline scanning for the FortiSandbox appliance, by holding a file up to 50 seconds for the verdict to be returned. Timed out scans can either be set to block, log, or ignore. Inline scanning can be enabled from the GUI on the Cloud Sandbox configuration page.

Rationale:

With FAIS, unknown malware can be detected and blocked using cloud sandboxing technology. Using inline scanning with FAIS, patient zero can also be prevented. This complements the existing antivirus signature-based detection and also acts as an additional layer of defense on top of FortiGate's AV heuristics feature.

Audit:

On CLI:

```
config system fortiguard
get
```

Verify if `sandbox-inline-scan` is enabled. Note that, `sandbox-inline-scan` will only show up after sandbox region is set (this is done during initial setup). If there is no `sandbox-inline-scan` in the output, it means that this feature is not enabled.

If `sandbox-inline-scan` is enabled, check on CLI if it is enforced on AV security profile:

```
config antivirus profile
show
```

Verify if `fortisandbox-mode inline` is set and on each traffic protocol, `fortisandbox block` is set.

On GUI:

```
1. Go to Security Fabric > Fabric Connectors and double-click the Cloud
Sandbox card.
```

Verify if "Inline scan" is enabled.

If "Inline scan" is enabled, then:

```
1. Go to Security Profiles > AntiVirus and double-click the relevant AV
profile.
```

Verify if `Scan strategy` is set as "Inline" and `Action` is set as "Block"

Remediation:

On GUI:

Enable the FortiGate Cloud feature visibility:

```
1. Go to System > Feature Visibility.
2. In the Additional Features section, enable FortiGate Cloud Sandbox.
3. Click Apply.
```

Configure the Cloud Sandbox Fabric connector:

```
1. Go to Security Fabric > Fabric Connectors and double-click the Cloud
Sandbox card.
2. Set the Type to FortiGate Cloud.
3. Select a Region.
4. Enable Inline scan.
5. Click OK.
```

Configure the antivirus profile:

```
1. Go to Security Profiles > AntiVirus and click Create New.
2. Set the Feature set to Proxy-based.
3. Enable the protocols to inspect.
4. Enable Send files to FortiSandbox for inspection.
5. Set the Scan strategy to Inline, and set the Action to Block.
6. Click OK.
```

On CLI: Disable FortiSandbox appliance and FortiSandbox Cloud:

```
config system fortisandbox
    set status disable
end
```

Configure FortiGate Cloud Sandbox (example given is setting it as "Global" region):

```
# execute forticloud-sandbox region
0  Global
1  Europe
2  Japan
3  US
Please select cloud sandbox region[0-3]:0
Cloud sandbox region is selected: Global
```

Enable inline scanning for FortiGate Cloud:

```
config system fortiguard
    set sandbox-region "Global"
    set sandbox-inline-scan enable
end
```

Enforced on AV security profile:

```
config antivirus profile
    edit <profile name>
        set feature-set proxy
        set fortisandbox-mode inline
 config http
        set fortisandbox block
        end
 config ftp
        set fortisandbox block
        end
 config imap
        set fortisandbox block
        end
 config pop3
        set fortisandbox block
        end
 config mapi
        set fortisandbox block
        end
 config nntp
        set fortisandbox block
        end
 config cifs
        set fortisandbox block
        end
 config ssh
        set fortisandbox block
        end
    next
end
```

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/571153/using-fortisandbox-inline-scanning-with-antivirus

4.2.7 Enable CDR for proxy mode on XLSB, OpenOffice, and RTF files (Automated)

Profile Applicability:

- Level 2

Description:

Enabling Content Disarm & Reconstruction (CDR) for proxy mode on XLSB, OpenOffice, and RTF files enhances security by sanitizing potentially malicious content in these file types. This helps prevent threats embedded in documents while maintaining usability.

Note that, this is only applicable for AV profiles and firewall policies in "Proxy mode".

Rationale:

Enabling Content Disarm & Reconstruction (CDR) for XLSB, OpenOffice, and RTF files mitigates the risk of embedded malware by sanitizing potentially harmful content before it reaches the user. This proactive approach reduces the attack surface while ensuring business continuity.

Impact:

Without CDR, malicious payloads hidden in these document formats could bypass traditional security measures, leading to data breaches or system compromise.

Audit:

Ensure CDR is configured from GUI:

```
1. Go to Security Profiles > AntiVirus and click Create New.
2. Enable AntiVirus scan, and select Block.
3. Set Feature set to Proxy-based.
4. Under Inspected Protocols, enable one or more protocols that support
proxy-based antivirus scanning.
5. Under APT Protection Options, enable Content Disarm and Reconstruction,
and select Apply CDR to office files to disarm Microsoft Office and
OpenOffice files, including RTF (Rich Text Format) and XLSB (Excel Binary
Workbook) files.
```

Remediation:

To configure antivirus CDR in the GUI:

```
1. Go to Security Profiles > AntiVirus and click Create New.
2. Enable AntiVirus scan, and select Block.
3. Set Feature set to Proxy-based.
4. Under Inspected Protocols, enable one or more protocols that support
proxy-based antivirus scanning.
5. Under APT Protection Options, enable Content Disarm and Reconstruction,
and select Apply CDR to office files to disarm Microsoft Office and
OpenOffice files, including RTF (Rich Text Format) and XLSB (Excel Binary
Workbook) files.
```

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.0/new-features/920942/support-xlsb-openoffice-and-rtf-files-for-cdr-in-antivirus-profiles-7-4-4

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

4.3 DNS Filter

4.3.1 Enable Botnet C&C Domain Blocking DNS Filter (Automated)

Profile Applicability:

- Level 2

Description:

Enable Botnet C&C domain blocking to block botnet access at the DNS name resolving stage.

Rationale:

Blocking botnet website access at the DNS resolution stage provides an additional layer of defense.

Audit:

On GUI:

```
1. Review DNS filters under Security Profiles > DNS Filter and ensure that
"Redirect botnet C&C requests to Block Portal" is enabled.
2. Ensure that firewall policies allowing DNS traffic have a DNS Filter
Security profile applied.
```

Remediation:

On GUI:

```
1. Go to Security Profiles > DNS Filter.
2. On the relevant security profile name, double click. Enable "Redirect
botnet C&C requests to Block Portal".
2. Ensure that firewall policies that have DNS traffic have a DNS Filter
security profile applied with that option enabled.
```

Default Value:

"Redirect botnet C&C requests to Block Portal" is enabled on default profile.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/105208

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 Use DNS Filtering Services Use DNS filtering services on all enterprise assets to block access to known malicious domains.	●	●	●
v7	8.6 Centralize Anti-malware Logging Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		●	●
v7	8.7 Enable DNS Query Logging Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		●	●

4.3.2 Ensure DNS Filter logs all DNS queries and responses (Automated)

Profile Applicability:

- Level 1

Description:

DNS filter should log all DNS queries and responses.

Rationale:

DNS filter should log all DNS queries and responses (whether the DNS category is blocked, monitored, or allowed). This enables SOC or security analysts to do further investigations on security incidents, especially on threat hunting or incident response activities. Although there are many data sources that can provide DNS query logs (AD or EDR), this option should be enabled out of best practice and with the assumption that no other data source is available.

Impact:

By default, allowed DNS is not logged. This creates a data gap in threat hunting or incident response activities.

Audit:

GUI:

```
1. Go to "Security Profiles" > "DNS Filter".
2. Select relevant DNS Filter profile.
```

Validate that "Log all DNS queries and responses" is enabled.

CLI:

```
FGT1 # config dnsfilter profile

FGT1 (profile) # show
```

Validate that "set log-all-domain enable" is configured on DNS Filter profile.

Remediation:

Review DNS Filter Security Profiles and validate that "Log all DNS queries and responses" is enabled.

Default Value:

Disabled

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-Static-DNS-filter-behavior-in-logging/ta-p/223110

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.6 Collect DNS Query Audit Logs Collect DNS query audit logs on enterprise assets, where appropriate and supported.		●	●
v7	8.7 Enable DNS Query Logging Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		●	●

4.3.3 Apply DNS Filter Security Profile to Policies (Automated)

Profile Applicability:

- Level 1

Description:

Ensuring that traffic traversing to the Internet on the FortiGate has a DNS Filter security profile inspecting it.

Rationale:

Traffic outbound to the Internet on the FortiGate should have firewall policies applied with an DNS Filter security profile applied.

Audit:

Review firewall policies that handle traffic **outbound to Internet** has an `DNS Filter` security profile assigned for inspection.

Remediation:

Configure on "Allowed" firewall policies that handle traffic **outbound to Internet** to have an appropriate `DNS Filter` security profile applied to policies.

Default Value:

Not Configured

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/243446

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	9.2 Use DNS Filtering Services Use DNS filtering services on all enterprise assets to block access to known malicious domains.	●	●	●
v7	7.7 Use of DNS Filtering Services Use DNS filtering services to help block access to known malicious domains.	●	●	●

4.4 Web Filtering

4.4.1 Create a Web Filtering Profile (Automated)

Profile Applicability:

- Level 1

Description:

Ensure FortiGuard Category-based Web filtering is blocking Security Risk categories

Rationale:

Websites categorized under "Security Risk" pose significant threats to an organization's network and users. Categories such as "Dynamic DNS", "Malicious Websites", "Phishing", and "Spam URLs" are often associated with cyber threats and serve as initial access vectors for attacks such as malware distribution, phishing schemes, command-and-control activities, and data theft.

If any websites or web pages that fall under the FortiGuard URL Database Categories "Dynamic DNS", "Newly Observed Domains", or "Newly Registered Domains" are required to be allowed, this based on an organization's policy, those specific entries should be configured under "Monitor" action in the web filter configuration.

Impact:

Setting the FortiGuard URL Database Categories "Newly Observed Domains" or "Newly Registered Domains" to "Block" action, can significantly impact user access to websites, particularly newly created website and/or uncategorized websites while it's relation to unrated category.

Audit:

GUI:

```
Go to Security Profiles > Web Filter. Select the relevant web filter profile,
if applicable. Validate that, within the "Security Risk" section, categories
such as "Malicious Websites", "Phishing", and "Spam URLs" are set to the
action "Block".
```

Remediation:

Apply Web Filter profile to the firewall policy or SD-WAN and ensure that the Security Risk categories, including Malicious Websites, Phishing, and Spam URLs, are configured to Block.

Default Value:

By default, all categories under "Security Risk" and "Unrated" are set to Block.

References:

1. https://docs.fortinet.com/document/fortigate/7.6.2/administration-guide/267887/configuring-a-web-filter-profile

4.5 Application Control

Application Control Security profiles

4.5.1 Block high risk categories on Application Control (Manual)

Profile Applicability:

- Level 1

Description:

Ensure FortiGate Application Control blocks high risk applications to reduce attack surface.

Rationale:

High risk applications such as those in "P2P" and "Proxy" are known for spreading malware. Some of this traffic is encrypted and therefore is able to bypass network security inspection (for those without decryption implemented). Blocking these applications from running eliminates this risk.

If any application that falls under "P2P" and "Proxy" is required to be allowed based on an organization's policy, that specific application needs to be under "Monitor" mode in the "Application and Filter Override" configuration.

Audit:

GUI:

```
1. Go to "Security Profiles" > "Application Control".
2. Select App Control profile.
```

Validate that "P2P" and "Proxy" category is blocked.

Remediation:

Review Application Control Security Profiles and validate that "P2P" and "Proxy" category is blocked.

Default Value:

All application category "Action" is set as "Monitor" by default.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/19814

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			●
v7	9.5 Implement Application Firewalls Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			●

4.5.2 Block applications running on non-default ports (Automated)

Profile Applicability:

- Level 2

Description:

Ensure FortiGate Application Control blocks applications running on non-default ports.

Rationale:

Running applications on non-default ports is not directly a threat, but can be an indication of something unexpected. For example, HTTPS runs on port 443. Potentially, if an attacker starts a rogue HTTPS server on port 10443, it could be used for data exfiltration.

Audit:

On GUI:

```
1. Go to "Security Profiles" > "Application Control".
2. Select relevant App Control profile.
```

Validate that "Block applications detected on non-default ports" option is enabled.

Remediation:

GUI:

```
1. Go to "Security Profiles" > "Application Control".
2. Select relevant App Control profile.
```

Enable "Block applications detected on non-default ports" option.

On CLI:

```
FGT1 # config application list

FGT1 (list) # edit <profile name>

FGT1 (<profile name>) # set enforce-default-app-port enable
```

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/66882

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

4.5.3 Ensure all Application Control related traffic is logged (Manual)

Profile Applicability:

- Level 1

Description:

Ensure no category is set to "Allow" on FortiGate Application Control.

Rationale:

Any category that is set as "Allow" on Application Control will not be logged. This creates a visibility gap on security investigation. This includes "Unknown Applications" category.

Impact:

Visibility gap, which affects incident forensics and response.

Audit:

On GUI:

```
1. Review "Security Profiles" > "Application Control".
2. Select the relevant App Control profile.
```

Validate that no "Allow" action is set on any categories.

Remediation:

On GUI:

```
1. Go to "Security Profiles" > "Application Control".
2. Select the relevant App Control profile.
3. Change any categories with "Allow" action to "Monitor".
```

Default Value:

"Unknown Applications" category is set as "Allow".

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/19814

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.5.4 Apply Application Control Security Profile to Policies (Manual)

Profile Applicability:

- Level 1

Description:

Ensuring that traffic traversing between networks on the FortiGate have an Application Control security profile inspecting it.

Rationale:

Traffic moving between "interfaces" on the FortiGate should have firewall policies applied with an Application Control security profile applied.

Audit:

Review **all** firewall policies and ensure that traffic has an `Application Control` security profile assigned for inspection.

Remediation:

Configure on **all** "Allowed" firewall policies to have an appropriate `Application Control` security profile applied to policies.

Default Value:

Not Configured

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/243446

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	9.5 Implement Application Firewalls Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	18.10 Deploy Web Application Firewalls (WAFs) Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.			

5 Security Fabric

This Section provides best practice related to configuring Fortinet Security Fabric.

5.1 Automation

5.1.1 Enable Compromised Host Quarantine (Automated)

Profile Applicability:

- Level 1

Description:

Default automation trigger configuration for when a high severity compromised host is detected.

Rationale:

By enabling this feature you protect your environment against compromised hosts. Default automation stitch to quarantine a high severity compromised host on FortiAPs, FortiSwitches, and FortiClient EMS.

Please note that this is only applicable if you have Fortinet's solution ecosystem (FortiGate with FortiAP, FortiSwitches, or FortiClient EMS).

Audit:

GUI

```
Security Fabric > Automation
```

Verify Compromised Host Quarantine is enabled.

Remediation:

GUI

```
Security Fabric > Automation
```

Edit and change Disabled to Enabled

CLI

```
config system automation-action
    edit "Quarantine on FortiSwitch + FortiAP"
        set description "Default automation action configuration for
quarantining a MAC address on FortiSwitches and FortiAPs."
        set action-type quarantine
    next
    edit "Quarantine FortiClient EMS Endpoint"
        set description "Default automation action configuration for
quarantining a FortiClient EMS endpoint device."
        set action-type quarantine-forticlient
    next
end
config system automation-trigger
    edit "Compromised Host - High"
        set description "Default automation trigger configuration for when a
high severity compromised host is detected."
    next
end
config system automation-stitch
    edit "Compromised Host Quarantine"
        set description "Default automation stitch to quarantine a high
severity compromised host on FortiAPs, FortiSwitches, and FortiClient EMS."
        set status enable
        set trigger "Compromised Host - High"
        config actions
            edit 1
                set action "Quarantine on FortiSwitch + FortiAP"
            next
            edit 2
                set action "Quarantine FortiClient EMS Endpoint"
            next
        end
    next
end
```

Default Value:

Not enabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		●	●
v8	13.9 Deploy Port-Level Access Control Deploy port-level access control. Port-level access control utilizes 802.1x, or similar network access control protocols, such as certificates, and may incorporate user and/or device authentication.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●
v7	8.3 Enable Operating System Anti-Exploitation Features/ Deploy Anti-Exploit Technologies Enable anti-exploitation features such as Data Execution Prevention (DEP) or Address Space Layout Randomization (ASLR) that are available in an operating system or deploy appropriate toolkits that can be configured to apply protection to a broader set of applications and executables.		●	●

5.2 Fabric Connectors

Security Fabric Connector Configuration

5.2.1 Configure Root FortiGate for Security Fabric

Configuring and identifying the root FortiGate within the Security Fabric

5.2.1.1 Ensure Security Fabric is Configured (Manual)

Profile Applicability:

- Level 2

Description:

Ensure Root FortiGate is configured as security fabric root.

Rationale:

Without a root FortiGate configured, the security fabric is not functional and can not be leveraged.

Please note that this is only applicable if security fabric function within FortiGate is used.

Impact:

Without Security Fabric enabled, visibility and management of traffic throughout an organization is decreased and individual FortiGate management becomes more intensive.

Audit:

Review through the GUI:

```
1. Go to "Security Fabric" -> Fabric Connectors and then select "Security
Fabric Setup".
2. Validate that the root FortiGate has status set to enabled and the
Security Fabric Role set to "Serve as Fabric Root".
3. Ensure that FortiAnalyzer settings are correct and that there is a defined
Fabric name as well as interfaces selected that will "Allow other Security
Fabric Devices to Join".
```

Remediation:

Remediation through the GUI:

```
1. Go to "Security Fabric" -> Fabric Connectors and then select "Security
Fabric Setup".
2. On the root FortiGate, set the status to enabled and the Security Fabric
Role to "Serve as Fabric Root".
3. Configure FortiAnalyzer settings when prompted and define a Fabric name as
well as interfaces that will "Allow other Security Fabric Devices to Join".
```

Default Value:

Disabled

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	0.0 Explicitly Not Mapped Explicitly Not Mapped			
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

6 VPN

6.1 SSL VPN

SSL VPN Best Practices

6.1.1 Apply a Trusted Signed Certificate for VPN Portal (Automated)

Profile Applicability:

- Level 2

Description:

Apply a signed certificate from a trusted Certificate Authority (CA) to the SSL VPN portal to allow users to connect securely with confidence.

Rationale:

Having an unsigned or self signed certificate leaves connections open to man-in-the-middle attacks and could allow users to connect to untrusted servers.

Audit:

GUI:

```
1. Access the FortiGate administrative web access page.
2. Go to VPN > SSL-VPN Settings and assign a signed certificate in the
dropdown for "Server Certificate".
```

Remediation:

Import a signed certificate from a trusted CA through the GUI:

```
1. Go to System > Certificates > Import.
2. Then assign the certificate to the SSL VPN portal by going to VPN > SSL-
VPN Settings and selecting the proper certificate in the dropdown for "Server
Certificate".
```

Default Value:

Self Signed Factory installed certificate

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	1.8 Utilize Client Certificates to Authenticate Hardware Assets Use client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

6.1.2 Enable Limited TLS Versions for SSL VPN (Automated)

Profile Applicability:

- Level 2

Description:

Enable and disable TLS versions and Cipher suites for more granular control of SSL VPN connections and enforcing more secure connections.

Rationale:

Limiting TLS versions to more secure versions as well as enforcing stronger ciphers increases the security of the SSL VPN connections.

Audit:

CLI:

```
config vpn ssl settings
get
```

Validate that:

`ssl-max-prot-ver` is set to tls1-3.

`ssl-min-proto-ver` is set to tls1-2.

`algorithm` is set to high.

Remediation:

CLI:

```
config vpn ssl settings
set ssl-max-proto-ver tls1-3
set ssl-min-proto-ver tls1-2
set algorithm high
```

Default Value:

ssl-max-proto-ver : tls1-3

ssl-min-proto-ver : tls1-2

algorithm : high

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/cli-reference/114404382/config-vpn-ssl-settings

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		●	●
v7	0.0 Explicitly Not Mapped Explicitly Not Mapped			

7 Logs and Reports

This section provides best practices related to logging and reporting in FortiGate.

7.1 Enable Logging

How to enable logging on the FortiGate device.

7.1.1 Enable Event Logging (Automated)

Profile Applicability:

- Level 2

Description:

Enabling event logging to allow for log generation and review.

Rationale:

Enabling event logging generates logs that can be stored for later review or auditing or can be ingested by another system (SIEM, Analyzer) for monitoring and response.

Audit:

CLI:

```
config log eventfilter
get
```

Validate that all event types are enabled.

Remediation:

On GUI:

```
1. Go to Log & Report > Log Settings.
2. Enable "All" Event Logging.
```

On CLI:

```
config log eventfilter
set event enable
end
```

Default Value:

Enabled

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/250999

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	8.8 Enable Command-line Audit Logging Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.		●	●

7.2 Centralized Logging and Reporting

Logging and Reporting should be done to a Centralized device

7.2.1 Centralized Logging and Reporting (Automated)

Profile Applicability:

- Level 2

Description:

Device logs should be sent to a centralized device for log collection, retention, and reporting. This could be a SIEM. syslog device, FortiAnalyzer, FortiManager, etc.

Rationale:

Centralized logging allows for more reliable log retention and more enriched log data for review and reporting.

Audit:

On GUI:

```
1. Go to Log & Report > Log Settings.
2. Validate under "Syslog logging" that logs are being offloaded to another
device.
```

Remediation:

Configure a remote server for logs to be sent to:

```
1. Go to Log & Report > Log Settings.
2. Under "Syslog logging" configure a remote server to send logs to.
```

Default Value:

Not configured.

References:

1. https://docs.fortinet.com/document/fortigate/7.4.5/administration-guide/250999

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	8.6 Centralize Anti-malware Logging Send all malware detection events to enterprise anti-malware administration tools and event log servers for analysis and alerting.		●	●

7.3 Encrypt Logs in Transit

Ensure that logs sent to FortiAnalyzer or FortiManager are encrypted during transmission.

7.3.1 Encrypt Log Transmission to FortiAnalyzer / FortiManager (Automated)

Profile Applicability:

- Level 1

Description:

Enable encryption for logs that are sent to FortiAnalyzer or FortiManager.

Rationale:

Provides encryption for logs that are sent to FortiAnalyzer or FortiManager to prevent logs being collected and viewed as they traverse the network.

Audit:

CLI:

```
config log fortianalyzer setting
get
```

Validate `enc-algorithm` is set to high.

Validate `reliable` is set enabled.

Remediation:

Secure log transfer settings can only be configured on CLI:

```
config log fortianalyzer setting
set reliable enable
set enc-algorithm high
end
```

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortianalyzer/7.4.5/administration-guide/410387

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

7.3.2 Encrypt Log Transmission to Syslog (Manual)

Profile Applicability:

- Level 1

Description:

Enable encryption for logs that are sent to FortiAnalyzer or FortiManager.

Rationale:

Provides encryption for logs that are sent to syslog to prevent logs being collected and viewed as they traverse the network.

Audit:

CLI:

```
config log syslog setting
get
```

Validate `enc-algorithm` is set to high.

Validate `reliable` is set enabled.

Remediation:

Secure log transfer settings can only be configured on CLI:

```
config log syslog setting
set reliable enable
set enc-algorithm high
end
```

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortianalyzer/7.4.5/administration-guide/410387

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

7.3.3 Encrypt Log Transmission to Syslog (Manual)

Profile Applicability:

- Level 1

Description:

Enable encryption for logs that are sent to FortiAnalyzer or FortiManager.

Rationale:

Provides encryption for logs that are sent to syslog to prevent logs being collected and viewed as they traverse the network.

Audit:

CLI:

```
config log syslog setting
get
```

Validate `enc-algorithm` is set to high.

Validate `reliable` is set enabled.

Remediation:

Secure log transfer settings can only be configured on CLI:

```
config log syslog setting
set reliable enable
set enc-algorithm high
end
```

Default Value:

Disabled

References:

1. https://docs.fortinet.com/document/fortianalyzer/7.4.5/administration-guide/410387

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Network Settings**		
1.1	Ensure DNS server is configured (Automated)	☐	☐
1.2	Ensure intra-zone traffic is not always allowed (Manual)	☐	☐
1.3	Disable all management related services on WAN port (Manual)	☐	☐
2	**System Settings**		
2.1	**General Settings**		
2.1.1	Ensure 'Pre-Login Banner' is set (Automated)	☐	☐
2.1.2	Ensure 'Post-Login-Banner' is set (Automated)	☐	☐
2.1.3	Ensure timezone is properly configured (Automated)	☐	☐
2.1.4	Ensure correct system time is configured through NTP (Manual)	☐	☐
2.1.5	Ensure hostname is set (Automated)	☐	☐
2.1.6	Ensure the latest firmware is installed (Manual)	☐	☐
2.1.7	Disable USB Firmware and configuration installation (Automated)	☐	☐
2.1.8	Disable static keys for TLS (Automated)	☐	☐
2.1.9	Enable Global Strong Encryption (Automated)	☐	☐
2.1.10	Ensure management GUI listens on secure TLS version (Automated)	☐	☐
2.1.11	Ensure CDN is enabled for improved GUI performance (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.12	Ensure single CPU core overloaded event is logged (Automated)	☐	☐
2.1.13	Ensure Hostname is Not Displayed On Login GUI (Automated)	☐	☐
2.2	**Password Policy**		
2.2.1	Ensure 'Password Policy' is enabled (Automated)	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured (Automated)	☐	☐
2.3	**SNMP**		
2.3.1	Ensure only SNMPv3 is enabled (Automated)	☐	☐
2.3.2	Allow only trusted hosts in SNMPv3 (Manual)	☐	☐
2.3.3	Disable SNMPv3 Query Per User (Automated)	☐	☐
2.3.4	Enabling SNMP trap for memory usage (Automated)	☐	☐
2.4	**Administrators and Admin Profiles**		
2.4.1	Remove default admin user and create one with other name (Automated)	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled (Manual)	☐	☐
2.4.3	Ensure admin accounts with different privileges have their correct profiles assigned (Manual)	☐	☐
2.4.4	Ensure Admin idle timeout time is configured (Automated)	☐	☐
2.4.5	Ensure only encrypted access channels are enabled (Automated)	☐	☐
2.4.6	Apply Local-in Policies (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.4.7	Ensure default Admin ports are changed (Automated)	☐	☐
2.4.8	Virtual patching on the local-in management interface (Automated)	☐	☐
2.5	**High Availability**		
2.5.1	Ensure High Availability configuration is enabled (Automated)	☐	☐
2.5.2	Ensure "Monitor Interfaces" for High Availability devices is enabled (Automated)	☐	☐
2.5.3	Ensure HA Reserved Management Interface is configured (Automated)	☐	☐
2.5.4	Ensure High Availability Group-ID is configured (Automated)	☐	☐
3	**Policy and Objects**		
3.1	Ensure that unused policies are reviewed regularly (Manual)	☐	☐
3.2	Ensure that policies do not use "ALL" as Service (Automated)	☐	☐
3.3	Ensure firewall policy denying all traffic to/from Tor, malicious server, or scanner IP addresses using ISDB (Automated)	☐	☐
3.4	Ensure logging is enabled on all firewall policies (Automated)	☐	☐
4	**Security Profiles**		
4.1	**Intrusion Prevention System (IPS)**		
4.1.1	Detect Botnet connections (Automated)	☐	☐
4.1.2	Apply IPS Security Profile to Policies (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.2	**Antivirus**		
4.2.1	Ensure Antivirus Definition Push Updates are Configured (Automated)	☐	☐
4.2.2	Apply Antivirus Security Profile to Policies (Manual)	☐	☐
4.2.3	Enable Outbreak Prevention Database (Automated)	☐	☐
4.2.4	Enable AI /heuristic based malware detection (Automated)	☐	☐
4.2.5	Enable grayware detection on antivirus (Automated)	☐	☐
4.2.6	Ensure inline scanning with FortiGuard AI-Based Sandbox Service is enabled (Automated)	☐	☐
4.2.7	Enable CDR for proxy mode on XLSB, OpenOffice, and RTF files (Automated)	☐	☐
4.3	**DNS Filter**		
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter (Automated)	☐	☐
4.3.2	Ensure DNS Filter logs all DNS queries and responses (Automated)	☐	☐
4.3.3	Apply DNS Filter Security Profile to Policies (Automated)	☐	☐
4.4	**Web Filtering**		
4.4.1	Create a Web Filtering Profile (Automated)	☐	☐
4.5	**Application Control**		
4.5.1	Block high risk categories on Application Control (Manual)	☐	☐
4.5.2	Block applications running on non-default ports (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.5.3	Ensure all Application Control related traffic is logged (Manual)	☐	☐
4.5.4	Apply Application Control Security Profile to Policies (Manual)	☐	☐
5	**Security Fabric**		
5.1	**Automation**		
5.1.1	Enable Compromised Host Quarantine (Automated)	☐	☐
5.2	**Fabric Connectors**		
5.2.1	**Configure Root FortiGate for Security Fabric**		
5.2.1.1	Ensure Security Fabric is Configured (Manual)	☐	☐
6	**VPN**		
6.1	**SSL VPN**		
6.1.1	Apply a Trusted Signed Certificate for VPN Portal (Automated)	☐	☐
6.1.2	Enable Limited TLS Versions for SSL VPN (Automated)	☐	☐
7	**Logs and Reports**		
7.1	**Enable Logging**		
7.1.1	Enable Event Logging (Automated)	☐	☐
7.2	**Centralized Logging and Reporting**		
7.2.1	Centralized Logging and Reporting (Automated)	☐	☐
7.3	**Encrypt Logs in Transit**		
7.3.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.3.2	Encrypt Log Transmission to Syslog (Manual)	☐	☐
7.3.3	Encrypt Log Transmission to Syslog (Manual)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.3	Disable all management related services on WAN port	☐	☐
2.1.6	Ensure the latest firmware is installed	☐	☐
2.1.8	Disable static keys for TLS	☐	☐
2.1.12	Ensure single CPU core overloaded event is logged	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured	☐	☐
2.3.4	Enabling SNMP trap for memory usage	☐	☐
2.4.1	Remove default admin user and create one with other name	☐	☐
2.4.3	Ensure admin accounts with different privileges have their correct profiles assigned	☐	☐
2.4.4	Ensure Admin idle timeout time is configured	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.4.7	Ensure default Admin ports are changed	☐	☐
2.4.8	Virtual patching on the local-in management interface	☐	☐
4.2.1	Ensure Antivirus Definition Push Updates are Configured	☐	☐
4.2.2	Apply Antivirus Security Profile to Policies	☐	☐
4.2.3	Enable Outbreak Prevention Database	☐	☐
4.2.4	Enable AI /heuristic based malware detection	☐	☐
4.2.5	Enable grayware detection on antivirus	☐	☐
4.3.3	Apply DNS Filter Security Profile to Policies	☐	☐
7.1.1	Enable Event Logging	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure DNS server is configured	☐	☐
1.3	Disable all management related services on WAN port	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.6	Ensure the latest firmware is installed	☐	☐
2.1.7	Disable USB Firmware and configuration installation	☐	☐
2.1.8	Disable static keys for TLS	☐	☐
2.1.9	Enable Global Strong Encryption	☐	☐
2.1.12	Ensure single CPU core overloaded event is logged	☐	☐
2.2.1	Ensure 'Password Policy' is enabled	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured	☐	☐
2.3.1	Ensure only SNMPv3 is enabled	☐	☐
2.3.2	Allow only trusted hosts in SNMPv3	☐	☐
2.3.4	Enabling SNMP trap for memory usage	☐	☐
2.4.1	Remove default admin user and create one with other name	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges have their correct profiles assigned	☐	☐
2.4.4	Ensure Admin idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.4.7	Ensure default Admin ports are changed	☐	☐
2.4.8	Virtual patching on the local-in management interface	☐	☐
3.1	Ensure that unused policies are reviewed regularly	☐	☐
3.2	Ensure that policies do not use "ALL" as Service	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure firewall policy denying all traffic to/from Tor, malicious server, or scanner IP addresses using ISDB	☐	☐
3.4	Ensure logging is enabled on all firewall policies	☐	☐
4.1.1	Detect Botnet connections	☐	☐
4.2.1	Ensure Antivirus Definition Push Updates are Configured	☐	☐
4.2.2	Apply Antivirus Security Profile to Policies	☐	☐
4.2.3	Enable Outbreak Prevention Database	☐	☐
4.2.4	Enable AI /heuristic based malware detection	☐	☐
4.2.5	Enable grayware detection on antivirus	☐	☐
4.2.7	Enable CDR for proxy mode on XLSB, OpenOffice, and RTF files	☐	☐
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter	☐	☐
4.3.2	Ensure DNS Filter logs all DNS queries and responses	☐	☐
4.3.3	Apply DNS Filter Security Profile to Policies	☐	☐
4.5.3	Ensure all Application Control related traffic is logged	☐	☐
5.1.1	Enable Compromised Host Quarantine	☐	☐
7.1.1	Enable Event Logging	☐	☐
7.2.1	Centralized Logging and Reporting	☐	☐
7.3.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager	☐	☐
7.3.2	Encrypt Log Transmission to Syslog	☐	☐
7.3.3	Encrypt Log Transmission to Syslog	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure DNS server is configured	☐	☐
1.2	Ensure intra-zone traffic is not always allowed	☐	☐
1.3	Disable all management related services on WAN port	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.6	Ensure the latest firmware is installed	☐	☐
2.1.7	Disable USB Firmware and configuration installation	☐	☐
2.1.8	Disable static keys for TLS	☐	☐
2.1.9	Enable Global Strong Encryption	☐	☐
2.1.12	Ensure single CPU core overloaded event is logged	☐	☐
2.2.1	Ensure 'Password Policy' is enabled	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured	☐	☐
2.3.1	Ensure only SNMPv3 is enabled	☐	☐
2.3.2	Allow only trusted hosts in SNMPv3	☐	☐
2.3.4	Enabling SNMP trap for memory usage	☐	☐
2.4.1	Remove default admin user and create one with other name	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges have their correct profiles assigned	☐	☐
2.4.4	Ensure Admin idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.4.7	Ensure default Admin ports are changed	☐	☐
2.4.8	Virtual patching on the local-in management interface	☐	☐
3.1	Ensure that unused policies are reviewed regularly	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.2	Ensure that policies do not use "ALL" as Service	☐	☐
3.3	Ensure firewall policy denying all traffic to/from Tor, malicious server, or scanner IP addresses using ISDB	☐	☐
3.4	Ensure logging is enabled on all firewall policies	☐	☐
4.1.1	Detect Botnet connections	☐	☐
4.1.2	Apply IPS Security Profile to Policies	☐	☐
4.2.1	Ensure Antivirus Definition Push Updates are Configured	☐	☐
4.2.2	Apply Antivirus Security Profile to Policies	☐	☐
4.2.3	Enable Outbreak Prevention Database	☐	☐
4.2.4	Enable AI /heuristic based malware detection	☐	☐
4.2.5	Enable grayware detection on antivirus	☐	☐
4.2.7	Enable CDR for proxy mode on XLSB, OpenOffice, and RTF files	☐	☐
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter	☐	☐
4.3.2	Ensure DNS Filter logs all DNS queries and responses	☐	☐
4.3.3	Apply DNS Filter Security Profile to Policies	☐	☐
4.5.1	Block high risk categories on Application Control	☐	☐
4.5.3	Ensure all Application Control related traffic is logged	☐	☐
4.5.4	Apply Application Control Security Profile to Policies	☐	☐
5.1.1	Enable Compromised Host Quarantine	☐	☐
6.1.1	Apply a Trusted Signed Certificate for VPN Portal	☐	☐
7.1.1	Enable Event Logging	☐	☐
7.2.1	Centralized Logging and Reporting	☐	☐
7.3.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager	☐	☐
7.3.2	Encrypt Log Transmission to Syslog	☐	☐
7.3.3	Encrypt Log Transmission to Syslog	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.11	Ensure CDN is enabled for improved GUI performance	☐	☐
2.1.13	Ensure Hostname is Not Displayed On Login GUI	☐	☐
2.3.3	Disable SNMPv3 Query Per User	☐	☐
2.5.4	Ensure High Availability Group-ID is configured	☐	☐
4.2.6	Ensure inline scanning with FortiGuard AI-Based Sandbox Service is enabled	☐	☐
4.4.1	Create a Web Filtering Profile	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.6	Ensure the latest firmware is installed	☐	☐
2.2.1	Ensure 'Password Policy' is enabled	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured	☐	☐
2.3.4	Enabling SNMP trap for memory usage	☐	☐
2.4.1	Remove default admin user and create one with other name	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges have their correct profiles assigned	☐	☐
2.4.4	Ensure Admin idle timeout time is configured	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.4.7	Ensure default Admin ports are changed	☐	☐
2.4.8	Virtual patching on the local-in management interface	☐	☐
3.2	Ensure that policies do not use "ALL" as Service	☐	☐
3.4	Ensure logging is enabled on all firewall policies	☐	☐
4.2.1	Ensure Antivirus Definition Push Updates are Configured	☐	☐
4.2.2	Apply Antivirus Security Profile to Policies	☐	☐
4.2.3	Enable Outbreak Prevention Database	☐	☐
4.2.5	Enable grayware detection on antivirus	☐	☐
4.2.7	Enable CDR for proxy mode on XLSB, OpenOffice, and RTF files	☐	☐
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter	☐	☐
4.3.3	Apply DNS Filter Security Profile to Policies	☐	☐
4.5.4	Apply Application Control Security Profile to Policies	☐	☐
7.1.1	Enable Event Logging	☐	☐
7.2.1	Centralized Logging and Reporting	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure DNS server is configured	☐	☐
1.2	Ensure intra-zone traffic is not always allowed	☐	☐
1.3	Disable all management related services on WAN port	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.6	Ensure the latest firmware is installed	☐	☐
2.1.7	Disable USB Firmware and configuration installation	☐	☐
2.1.8	Disable static keys for TLS	☐	☐
2.1.12	Ensure single CPU core overloaded event is logged	☐	☐
2.2.1	Ensure 'Password Policy' is enabled	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured	☐	☐
2.3.1	Ensure only SNMPv3 is enabled	☐	☐
2.3.2	Allow only trusted hosts in SNMPv3	☐	☐
2.3.4	Enabling SNMP trap for memory usage	☐	☐
2.4.1	Remove default admin user and create one with other name	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges have their correct profiles assigned	☐	☐
2.4.4	Ensure Admin idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.4.7	Ensure default Admin ports are changed	☐	☐
2.4.8	Virtual patching on the local-in management interface	☐	☐
3.1	Ensure that unused policies are reviewed regularly	☐	☐
3.2	Ensure that policies do not use "ALL" as Service	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure firewall policy denying all traffic to/from Tor, malicious server, or scanner IP addresses using ISDB	☐	☐
3.4	Ensure logging is enabled on all firewall policies	☐	☐
4.1.2	Apply IPS Security Profile to Policies	☐	☐
4.2.1	Ensure Antivirus Definition Push Updates are Configured	☐	☐
4.2.2	Apply Antivirus Security Profile to Policies	☐	☐
4.2.3	Enable Outbreak Prevention Database	☐	☐
4.2.4	Enable AI /heuristic based malware detection	☐	☐
4.2.5	Enable grayware detection on antivirus	☐	☐
4.2.7	Enable CDR for proxy mode on XLSB, OpenOffice, and RTF files	☐	☐
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter	☐	☐
4.3.2	Ensure DNS Filter logs all DNS queries and responses	☐	☐
4.3.3	Apply DNS Filter Security Profile to Policies	☐	☐
4.5.3	Ensure all Application Control related traffic is logged	☐	☐
4.5.4	Apply Application Control Security Profile to Policies	☐	☐
5.1.1	Enable Compromised Host Quarantine	☐	☐
6.1.1	Apply a Trusted Signed Certificate for VPN Portal	☐	☐
6.1.2	Enable Limited TLS Versions for SSL VPN	☐	☐
7.1.1	Enable Event Logging	☐	☐
7.2.1	Centralized Logging and Reporting	☐	☐
7.3.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager	☐	☐
7.3.2	Encrypt Log Transmission to Syslog	☐	☐
7.3.3	Encrypt Log Transmission to Syslog	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure DNS server is configured	☐	☐
1.2	Ensure intra-zone traffic is not always allowed	☐	☐
1.3	Disable all management related services on WAN port	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.6	Ensure the latest firmware is installed	☐	☐
2.1.7	Disable USB Firmware and configuration installation	☐	☐
2.1.8	Disable static keys for TLS	☐	☐
2.1.12	Ensure single CPU core overloaded event is logged	☐	☐
2.2.1	Ensure 'Password Policy' is enabled	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured	☐	☐
2.3.1	Ensure only SNMPv3 is enabled	☐	☐
2.3.2	Allow only trusted hosts in SNMPv3	☐	☐
2.3.4	Enabling SNMP trap for memory usage	☐	☐
2.4.1	Remove default admin user and create one with other name	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges have their correct profiles assigned	☐	☐
2.4.4	Ensure Admin idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.4.7	Ensure default Admin ports are changed	☐	☐
2.4.8	Virtual patching on the local-in management interface	☐	☐
3.1	Ensure that unused policies are reviewed regularly	☐	☐
3.2	Ensure that policies do not use "ALL" as Service	☐	☐

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure firewall policy denying all traffic to/from Tor, malicious server, or scanner IP addresses using ISDB	☐	☐
3.4	Ensure logging is enabled on all firewall policies	☐	☐
4.1.1	Detect Botnet connections	☐	☐
4.1.2	Apply IPS Security Profile to Policies	☐	☐
4.2.1	Ensure Antivirus Definition Push Updates are Configured	☐	☐
4.2.2	Apply Antivirus Security Profile to Policies	☐	☐
4.2.3	Enable Outbreak Prevention Database	☐	☐
4.2.4	Enable AI /heuristic based malware detection	☐	☐
4.2.5	Enable grayware detection on antivirus	☐	☐
4.2.7	Enable CDR for proxy mode on XLSB, OpenOffice, and RTF files	☐	☐
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter	☐	☐
4.3.2	Ensure DNS Filter logs all DNS queries and responses	☐	☐
4.3.3	Apply DNS Filter Security Profile to Policies	☐	☐
4.5.1	Block high risk categories on Application Control	☐	☐
4.5.3	Ensure all Application Control related traffic is logged	☐	☐
4.5.4	Apply Application Control Security Profile to Policies	☐	☐
5.1.1	Enable Compromised Host Quarantine	☐	☐
6.1.1	Apply a Trusted Signed Certificate for VPN Portal	☐	☐
6.1.2	Enable Limited TLS Versions for SSL VPN	☐	☐
7.1.1	Enable Event Logging	☐	☐
7.2.1	Centralized Logging and Reporting	☐	☐
7.3.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager	☐	☐
7.3.2	Encrypt Log Transmission to Syslog	☐	☐
7.3.3	Encrypt Log Transmission to Syslog	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.11	Ensure CDN is enabled for improved GUI performance	☐	☐
2.1.13	Ensure Hostname is Not Displayed On Login GUI	☐	☐
2.3.3	Disable SNMPv3 Query Per User	☐	☐
2.5.4	Ensure High Availability Group-ID is configured	☐	☐
4.2.6	Ensure inline scanning with FortiGuard AI-Based Sandbox Service is enabled	☐	☐
4.4.1	Create a Web Filtering Profile	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Dec 6, 2025	1.0.1	4.2.6 Ensure inline scanning with FortiGuard AI-Based Sandbox Service is enabled (Ticket 26643)
Dec 6, 2025	1.0.1	Create Automated Content for CISCAT assessment tool (Ticket 26793)