CIS Fortigate Benchmark

v1.1.0 - 04-03-2023

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/

Table of Contents

Overview

All CIS 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 for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

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

This document provides prescriptive guidance for establishing a secure configuration posture for Fortinet FortiGate devices running the Forinet OS version 6.4 or above. This guide was tested against FortiOS 6.4.5. 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, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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

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

Rationale:

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

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 208.91.112.53. Default secondary DNS server is 208.91.112.52

References:

1. https://docs.fortinet.com/document/fortigate/6.4.1/administration-guide/903162/important-dns-cli-commands

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 are 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 of 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/6.2.0/cookbook/116821/zone

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
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 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 have 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.

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 that may want to access the FortiGate that certain types of activity are illegal, but 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://kb.fortinet.com/kb/documentLink.do?externalID=FD33887

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

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

Profile Applicability:

- Level 1

Description:

Sets the banner after users successfully login. 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://kb.fortinet.com/kb/documentLink.do?externalID=FD33887

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

2.1.3 Ensure timezone is properly configured (Manual)

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://kb.fortinet.com/kb/documentLink.do?externalID=FD49018
2. https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/512210/setting-the-system-time
3. https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/512210/setting-the-system-time

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 (Automated)

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://docs.fortinet.com/document/fortigate/6.2.0/cookbook/512210/setting-the-system-time
2. https://kb.fortinet.com/kb/documentLink.do?externalID=FD49018

3.

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, but also 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, go to 'System' -> 'Settings', 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 #
```

or In GUI, go to 'System' -> 'Settings', update the field 'Hostname' with the new hostname, and click "Apply"

Default Value:

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

References:

1. https://kb.fortinet.com/kb/documentLink.do?externalID=FD48765

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 <u>Establish and Maintain a Secure Configuration Process for Network Infrastructure</u> Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 <u>Establish Secure Configurations</u> Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.1.6 Ensure the latest firmware is installed (Manual)

Profile Applicability:

- Level 2

Description:

Check against 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 which will gives you the latest version available.
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:

```
go to Dashboard -> Status -> System information and 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, click on

```
System -> Firmware, then click on "Browse" to select the next firmware file.
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://kb.fortinet.com/kb/documentLink.do?externalID=10948

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
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 from being connected 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:

config system auto-install set auto-install-config enable set auto-install-image enable end

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 disable is set)
```

Remediation:

CLI:

```
config system global

set ssl-static-key-ciphers disable

end
```

Default Value:

set ssl-static-key-ciphers enable

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 : enable

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.

Impact:

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

Audit:

currently implemented password policy can be shown from GUI or CLI
From CLI, type

```
get system password-policy
```

From GUI,
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
```

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 8
        set min-lower-case-letter 1
        set min-upper-case-letter 1
        set min-non-alphanumeric 1
        set min-number 1
        set expire-status enable
        set expire-day 90
        set reuse-password disable
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 '8'
6) Enable 'Character requirements'
7) set minimum '1' in the filed of 'Upper Case', 'Lower Case', 'Numbers (0-
9)' and 'Special'
8) Disable 'Allow password reuse'
9) Enable 'Password expiration' and set it to 90
```

Default Value:

By Default, Password Policy is disabled, 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://kb.fortinet.com/kb/documentLink.do?externalID=FD31021
2. https://docs.fortinet.com/document/fortigate/7.0.0/cli-reference/11620/config-system-password-policy
3. https://docs.fortinet.com/document/fortigate/7.0.0/administration-guide/364729/password-policy

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.

- Use numbers in place of letters, for example: passw0rd.
- Administrator passwords can be up to 64 characters.
- Include a mixture of numbers, symbols, and upper and lower case letters.
- Use multiple words together, or possibly even a sentence, for example: correcthorsebatterystaple.
- Use a password generator.
- Change the password regularly and always make the new password unique and not a variation of the existing password. for example, do not change from password to password1.
- 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.

FortiGate allows you to create a password policy for administrators and IPsec pre-shared keys. With this policy, you can enforce regular changes and specific criteria for a password policy, including:

- The minimum length, between 8 and 64 characters.
- If the password must contain uppercase (A, B, C) and/or lowercase (a, b, c) characters.
- If the password must contain numbers (1, 2, 3).
- If the password must contain special or non-alphanumeric characters: !, @, #, $, %, ^, &, *, (, and)
- Where the password applies (admin or IPsec or both).
- The duration of the password before a new one must be specified.
- The minimum number of unique characters that a new password must include.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 <u>Use Unique Passwords</u> 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 <u>Use Unique Passwords</u> 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 login and fail to enter the correct password you could be a valid user, or a hacker attempting to gain access. For this reason, best practices dictate to limit the number of failed attempts to login before a lockout period where you cannot login for a certain period of time. lockout period will minimize the hacker attempts to gain access to 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
admin-lockout-threshold and **admin-lockout-duration**

Remediation:

To configure the lockout options, from CLI:

```
config system global
        set admin-lockout-threshold 3
        set admin-lockout-duration 60
end
```

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).

To configure the lockout options, from CLI:

```
config system global
        set admin-lockout-threshold 3
        set admin-lockout-duration 60
end
```

References:

1. https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/631730/setting-the-administrator-password-retries-and-lockout-time

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 SNMP agent is disabled (Automated)

Profile Applicability:

- Level 1

Description:

The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system.

Rationale:

The SNMP server can communicate using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used. If SNMP is required the server should be configured to use only SNMPv3.

Impact:

SNMP servers will not be able to query the Fortigate devices that have SNMP agents disabled.

Audit:

on CLI, run the following commands to check whether SNMP agent is disabled.

```
FGT1 # config system snmp sysinfo
FGT1 (sysinfo) # show full
config system snmp sysinfo
    set status disable
    ...
end
```

On the GUI, select System -> SNMP, make sure that SNMP Agent is disabled.

Remediation:

On the CLI, run the following command to disable the agent

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

On the GUI, select System -> SNMP, disable SNMP agent

Default Value:

SNMP agent is disabled by default.

References:

1. https://kb.fortinet.com/kb/documentLink.do?externalID=FD45755

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	**4.1 Establish and Maintain a Secure Configuration Process** Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	**5.1 Establish Secure Configurations** Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.3.2 Ensure only SNMPv3 is enabled (Automated)

Profile Applicability:

- Level 2

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 server 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

```
System -> SNMP. Make sure that SNMP agent is enabled.  Make sure that there
is not any SNMPv1/2c community. 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

```
FGT1 # config system snmp community
FGT1 (community) # delete public
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

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

Default Value:

By default, SNMP agent is disabled.

References:

1. https://kb.fortinet.com/kb/documentLink.do?externalID=FD45755
2. https://docs.fortinet.com/document/fortigate/6.4.0/administration-guide/457149/snmp-v3-users

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	11.5 Manage Network Devices Using Multi-Factor Authentication and Encrypted Sessions Manage all network devices using multi-factor authentication and encrypted sessions.		●	●

2.4 Administrators and Admin Profiles

2.4.1 Ensure default 'admin' password is changed (Manual)

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:

In the CLI, to change the password of account "admin"

```
FG1 # config system admin
FG1 (admin) # edit "admin"
FG1 (admin) # set password <your passwords>
FG1 (admin) # end
FG1 #
```

To change the default password in the GUI:

```
1) Login to FortiGate with admin account
2) Go to System > Administrators.
3) Edit the admin account.
4) Click Change Password.
5) If applicable, enter the current password in the Old Password field.
6) Enter a password in the New Password field, then enter it again in the
Confirm Password field.
7) Click OK.
```

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.	●	●	●
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 ensure that no one from anywhere else on the network able to login even with correct credentials.

Impact:

All access, from legitimate or illegitimate users, outside of allowed segment will be stopped. 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, go to

```
System -> Administrators, select the account and click on edit. In the
account setting page, make sure that "Restrict login to trusted hosts" are
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 over-ride the existing host/network.
In the web GUI, go to

```
System -> Administrators, select the account and click on edit. In the
account setting page, make sure that "Restrict login to trusted hosts" are
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/6.0.0/cookbook/222079/using-a-trusted-host-optional

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 having 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, there are needs to create different levels of administrative accounts. For example, technicians from tier 1 support should not have total access to the system as compared with a tier 3 support.

Audit:

There are 2 stages to audit. **Stage 1: verify the profile**. Here is how to verify in the CLI:

```
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, I would like 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

```
System -> Admin Profiles, select "tier_1" and click "Edit". On "Firewall",
click on "Custom" and then click on "Read/Write" option for "Address".
```

In the next example, I would like to 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

```
System -> Administrators, select "support1" and click "Edit". Under
"Administrator Profile", select "tier_1".
```

Default Value:

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

References:

1. https://docs.fortinet.com/document/fortigate/latest/administration-guide/294491/administrator-profiles

Additional Information:

You cannot change the profile of the account which you are currently logging 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 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 settings admin idle timeout to prevent the risk of unauthorized access to the device by preventing someone from using a logged-in GUI on a PC that has been left unattended.

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/6.2.0/cookbook/215451/setting-the-idle-timeout-time

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	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

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" attack 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

```
Network -> Interfaces, select the interface and click "Edit". 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

```
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

```
Network -> Interfaces, select the interface and click "Edit". 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/6.0.0/handbook/909236/configuring-administrative-access-to-interfaces

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 (Manual)

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 so they can extend past "trusted host" configurations and can be configured with source and destination addresses as well as services specifically.

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 you can enable the feature to see them in the GUI by going to

```
System > Feature Visibility and 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

2.5 High Availability

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

2.5.1 Ensure High Availability Configuration (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:

```
Navigate to "System" and then "HA"
Ensure "Mode" is set to proper setting "Active-Active" or "Active-Passive"
Review Configuration settings
       "Cluster Name" must match on devices
       "Password" Must match on devices
       "Heartbeat Interfaces" need to be defined on devices
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:

```
Navigate to "System" and then "HA"
Ensure "Mode" is set to proper setting "Active-Active" or "Active-Passive"
Review Configuration settings
        "Cluster Name" must match on devices
        "Password" Must match on devices
        "Heartbeat Interfaces" need to be defined on devices
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/6.4.5/administration-guide/489119/ha-cluster-setup-examples

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 that the FortiGate is connected to.

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 it is not being monitored. Without the Interface monitoring enabled failover would be limited to hardware, system, or power faults.

Audit:

To Validate from GUI:

```
go to System - > HA
Under "Monitor Interfaces" validate all applicable interfaces are selected
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:

```
go to System - > HA
Under "Monitor Interfaces" select all applicable interfaces.
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

2.5.3 Ensure HA Reserved Management Interface is Configured (Manual)

Profile Applicability:

- Level 1

- Level 2

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:

```
go to System -> HA edit the "Master" device and 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 enable
and that config ha-mgmt-interfaces has at least one entry with an interface and gateway
defined

Remediation:

Remediate through the GUI:

```
go to System -> HA edit the "Master" device and 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

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.

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,

```
go to Policy & Objects -> IPv4 Policy. First 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 obviously 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.

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

Profile Applicability:

- Level 1

Description:

We want to make sure 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 mistakes.

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,

```
go to Policy & Objects -> IPv4 Policy.
```

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

Remediation:

In this example, we will 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,

```
click on Policy & Objects -> IPv4 Policy. Select the policy, click "Edit". 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
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 Policies are Uniquely Named (Manual)

Profile Applicability:

- Level 2

Description:

Ensure Policies are uniquely named

Rationale:

Uniquely named policies allow for better auditing and prevent multiple policies performing the same actions existing and possibly introducing misconfigurations

Audit:

Review firewall policies and validate that all policies are uniquely named

Remediation:

Provide all firewall policies with a unique name

3.4 Ensure there are no Unused Policies (Manual)

Profile Applicability:

- Level 2

Description:

Ensure that there are no firewall policies that are unused

Rationale:

Unused policies may provide unintended or anticipated access to services or hosts

Audit:

Review all Firewall policies for use and validate the purpose of the policy

Remediation:

Disable and then delete any used firewall policies

3.5 Ensure firewall policy denying all traffic to/from Tor or malicious server IP addresses using ISDB (Manual)

Profile Applicability:

- Level 1

Description:

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

Rationale:

FortiGate includes Tor or malicious server related IP address using ISDB. The idea is to filter out malicious traffics using firewall policies as first level filtering. This is done without involving more resource intensive process 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", 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" and "Malicious-Malicious.Server".

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", 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" and "Malicious-Malicious.Server"
Schedule: Always
Action: Deny
Log Violation Traffic: Enabled
Enable this policy: Enabled
```

3.6 Ensure logging is enabled on all firewall policies (Manual)

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), but this option should be enabled out of best practice and with assumption that no other data sources is available.

Impact:

By default, when creating firewall policies, logging option is not enabled. Also, the default implicit deny policy is not logged. This creates 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:
For allowed policies, "Log Allowed Traffic" is set on "All Sessions" option
For denied policies, "Log Violation Traffic" is enabled.

Default Value:

Disabled

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 (Manual)

Profile Applicability:

- Level 2

Description:

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

Rationale:

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

Audit:

Review all firewall policies that have a "WAN" interface as the destination and ensure that an IPS sensor with "Scan Outgoing Connections to Botnet Sites" is set to "Block"

Remediation:

Apply an IPS Sensor with "Scan Outgoing Connections to Botnet Sites" set to "Block" on all firewall policies with traffic exiting the network to a "WAN" interface.

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:

GUI (FortiOS 6):

```
Access the FortiGate administrative web access page and go to System >
FortiGuard under "FortiGuard Updates" validate "Accept push updates"  is
enabled.
```

GUI (FortiOS 7):

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

CLI (FortiOS 6):

```
config system autoupdate push-update
get (Validate status is enable)
```

CLI (FortiOS 7):

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

Remediation:

GUI (FortiOS 6):

```
Access the FortiGate administrative web access page and go to System >
FortiGuard under 'FortiGuard Updates" enable "Accept push updates".
```

GUI (FortiOS 7):

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

CLI (FortiOS 6):

```
config system autoupdate
set status enable
end
```

CLI (FortiOS 7):

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

Default Value:

Disable (on FortiOS 6)

Enabled and set to automatic (on FortiOS 7)

References:

1. https://docs.fortinet.com/document/fortigate/7.0.10/administration-guide/547335

4.2.2 Apply Antivirus Security Profile to Policies (Manual)

Profile Applicability:

- Level 2

Description:

Ensuring that traffic traversing between networks on the FortiGate have 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

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:

GUI:

```
Go to "Security Profiles" > "AntiVirus" > select AV profile
```

Validate that "Use FortiGuard outbreak prevention database" is enabled.
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/7.0.9/administration-guide/889364/fortiguard-outbreak-prevention

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 FortiOS 6.4.x

```
FGT1 # show antivirus heuristic
```

Validate that it is in "block" mode.
On FortiOS 7.x:

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

Validate that it is enabled.

Remediation:

```
FGT1 # config antivirus settings

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

Default Value:

Disabled (for version 6.4.x)

Enabled (for version 7.x)

References:

1. https://docs.fortinet.com/document/fortigate/6.4.11/cli-reference/517620/config-antivirus-heuristic
2. https://docs.fortinet.com/document/fortigate/7.0.0/new-features/773410/ai-based-malware-detection

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:

```
FGT1 # config antivirus settings

FGT1 (settings) # set grayware enable
```

Default Value:

Enabled

References:

1. https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuration-options-about-antivirus/ta-p/191939

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:

GUI:

```
Review DNS filters under Security Profiles > DNS Filter and ensure that
"redirect botnet C&C requests to Block portal" is enabled and that policies
allowing DNS traffic have a DNS Filter Security profile applied
```

Remediation:

Review DNS Filter Security Profiles and validate that "Redirect botnet C&C requests to Block Portal" is enabled and that firewall policies that have DNS traffic have a DNS Filter security profile applied with that option enabled

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

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 if the DNS category is blocked, monitored, or allowed). 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), but this option should be enabled out of best practice and with assumption that no other data sources is available.

Impact:

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

Audit:

GUI:

```
Go to "Security Profiles" > "DNS Filter" > select 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

4.4 Application Control

Application Control Security profiles

4.4.1 Block high risk categories on Application Control (Manual)

Profile Applicability:

- Level 1

Description:

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

Rationale:

High risk applications such as those in "P2P" and "Proxy" are known for spreading malwares. Other than that, some of these 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" requires to be allowed based on organization's policy, that specific application needs to be under "Monitor" mode in the "Application and Filter Override" configuration.

Audit:

GUI:

```
Go to "Security Profiles" > "Application Control" > 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:

Disabled on default profile

4.4.2 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 application 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 attacker starts a rogue HTTPS server on port 10443, it could be used for data exfiltration.

Audit:

GUI:

```
Go to "Security Profiles" > "Application Control" > select App Control
profile
```

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

Remediation:

GUI:

```
Go to "Security Profiles" > "Application Control" > select App Control
profile

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

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://attack.mitre.org/techniques/T1571/

4.4.3 Ensure all Application Control related traffic are 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 visibility gap on security investigation. This includes "Unknown Applications" category.

Impact:

Visibility gap, affects incident forensics and response.

Audit:

GUI:

```
Go to "Security Profiles" > "Application Control" > select App Control
profile
```

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

Remediation:

Review Application Control Security Profiles and validate that no "Allow" action is set on any categories.

Default Value:

"Unknown Applications category is set as "Allow"

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.

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 disable
        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

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 (Automated)

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

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:

```
To Validate root FortiGate status go to "Security Fabric" -> Fabric
Connectors and then select "Security Fabric Setup"
Validate that the root FortiGate has status set to enabled and the Security
Fabric Role set to "Serve as Fabric Root"
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:

```
To configure root FortiGate status go to "Security Fabric" -> Fabric
Connectors and then select "Security Fabric Setup"
On the root FortiGate set the status to enabled and the Security Fabric Role
to "Serve as Fabric Root"

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

6 VPN

6.1 SSL VPN

SSL VPN Best Practices

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

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:

```
Access the FortiGate administrative web access page and 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

```
System > Certificates > Import and 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 Certifcate"
```

Default Value:

Self Signed Factory installed certificate

6.1.2 Enable Limited TLS Versions for SSL VPN (Manual)

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 ssl-max-prot-ver and ssl-min-proto-ver as well as algorithm and
banned-cipher)
```

Remediation:

CLI:

```
config vpn ssl settings
set ssl-max-prot-ver *** {Configure max TLS Version supported}
set ssl-min-proto ver *** {set minimum support TLS version}
set banned-cipher *** {add cipher suite to banned list and prevent it from
being used}
set algorithm high {use high algorithms}
```

Default Value:

ssl-max-proto-ver : tls1-3 ssl-min-proto-ver : tls1-2 banned-cipher : algorithm : high

7 Users and Authentication

This section provides best practice related to Users and devices including:

- Endpoint control and compliance
- Users and user Groups Definition
- Guest Management
- LDAP, RADIUS, and TACACS+ Servers
- Authentication Settings
- FortiTokens
- PKI
- Configuring the maximum login attempts and lockout period

7.1 Configuring the maximum login attempts and lockout period (Automated)

Profile Applicability:

- Level 2

Description:

Configure maximum user log in attempts and lockout period

Rationale:

Failed user log in attempts can indicate an attempt to gain access to the network. Limiting the number of attempts before the account is locked for a determined amount of time helps slow down brute force attempts and impedes malicious attempts to access user accounts.

Audit:

CLI:

```
config user setting
get (Validate auth-lockout-threshold *  the number of attempts before locking
out the account and auth-lockout duration * the duration of the lockout once
the failed attempts is met)
```

Remediation:

CLI:

```
config user setting

set auth-lockout-threshold 5

end

config user setting

set auth-lockout-duration 300

end
```

Default Value:

auth-lockout-threshold: 3 auth-lockout-duration: 0

8 Logs and Reports

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

8.1 Enable Logging

How to enable logging on the FortiGate device.

8.1.1 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 event is enabled)
end
```

Remediation:

Access the FortiGate administrative web access page and go to
Log & Report > Log Settings enable Event Logging.
CLI:

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

8.2 Encrypt Logs Sent to FortiAnalyzer / FortiManager

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

8.2.1 Encrypt Log Transmission to FortiAnalyzer / FortiManager (Automated)

Profile Applicability:

- Level 2

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)
end
```

Remediation:

GUI:

```
Access the FortiGate administrative web access page and go to Log & Report >
Log Settings and when configuring Remote logging to
FortiAnalyzer/FortiManager select "Encrypt log transmission"
```

CLI:

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

8.3 Centralized Logging and Reporting

Logging and Reporting should be done to a Centralized device

8.3.1 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:

```
Review log settings through the administrative web page go to Log & Report >
Log Settings and validate under "Remote Logging and Archiving" that logs are
being offloaded to another device.
```

Remediation:

Configure a remote server for logs to be sent to.

```
Access the FortiGate administrative web access page and to to Log & Report >
Log Settings and under "Remote Logging and Archiving" configure a remote
server to send logs to.
```

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 (Manual)	☐	☐
2.1.4	Ensure correct system time is configured through NTP (Automated)	☐	☐
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)	☐	☐
2.2	**Password Policy**		
2.2.1	Ensure 'Password Policy' is enabled (Automated)	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.3	**SNMP**		
2.3.1	Ensure SNMP agent is disabled (Automated)	☐	☐
2.3.2	Ensure only SNMPv3 is enabled (Automated)	☐	☐
2.4	**Administrators and Admin Profiles**		
2.4.1	Ensure default 'admin' password is changed (Manual)	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled (Manual)	☐	☐
2.4.3	Ensure admin accounts with different privileges having their correct profiles assigned (Manual)	☐	☐
2.4.4	Ensure idle timeout time is configured (Automated)	☐	☐
2.4.5	Ensure only encrypted access channels are enabled (Automated)	☐	☐
2.4.6	Apply Local-in Policies (Manual)	☐	☐
2.5	**High Availability**		
2.5.1	Ensure High Availability Configuration (Automated)	☐	☐
2.5.2	Ensure "Monitor Interfaces" for High Availability Devices is Enabled (Automated)	☐	☐
2.5.3	Ensure HA Reserved Management Interface is Configured (Manual)	☐	☐
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 Policies are Uniquely Named (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.4	Ensure there are no Unused Policies (Manual)	☐	☐
3.5	Ensure firewall policy denying all traffic to/from Tor or malicious server IP addresses using ISDB (Manual)	☐	☐
3.6	Ensure logging is enabled on all firewall policies (Manual)	☐	☐
4	**Security Profiles**		
4.1	**Intrusion Prevention System (IPS)**		
4.1.1	Detect Botnet Connections (Manual)	☐	☐
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)	☐	☐
4.3	**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 (Manual)	☐	☐
4.4	**Application Control**		
4.4.1	Block high risk categories on Application Control (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.4.2	Block applications running on non-default ports (Automated)	☐	☐
4.4.3	Ensure all Application Control related traffic are logged (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 (Automated)	☐	☐
6	**VPN**		
6.1	**SSL VPN**		
6.1.1	Apply a Trusted Signed Certificate for VPN Portal (Manual)	☐	☐
6.1.2	Enable Limited TLS Versions for SSL VPN (Manual)	☐	☐
7	**Users and Authentication**		
7.1	Configuring the maximum login attempts and lockout period (Automated)	☐	☐
8	**Logs and Reports**		
8.1	**Enable Logging**		
8.1.1	Enable Event Logging (Automated)	☐	☐
8.2	**Encrypt Logs Sent to FortiAnalyzer / FortiManager**		
8.2.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.3	**Centralized Logging and Reporting**		
8.3.1	Centralized Logging and Reporting (Automated)	☐	☐

Appendix: CIS Controls *v7* IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure 'Pre-Login Banner' is set	☐	☐
2.1.5	Ensure hostname is set	☐	☐
2.1.6	Ensure the latest firmware is installed	☐	☐
2.2.2	Ensure administrator password retries and lockout time are configured	☐	☐
2.3.1	Ensure SNMP agent is disabled	☐	☐
2.4.1	Ensure default 'admin' password is changed	☐	☐
2.4.3	Ensure admin accounts with different privileges having their correct profiles assigned	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure DNS server is configured	☐	☐
2.1.1	Ensure 'Pre-Login Banner' is set	☐	☐
2.1.2	Ensure 'Post-Login-Banner' is set	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.5	Ensure hostname is set	☐	☐
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	☐	☐
2.3.1	Ensure SNMP agent is disabled	☐	☐
2.3.2	Ensure only SNMPv3 is enabled	☐	☐
2.4.1	Ensure default 'admin' password is changed	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges having their correct profiles assigned	☐	☐
2.4.4	Ensure idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐
3.2	Ensure that policies do not use "ALL" as Service	☐	☐

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	☐	☐
2.1.1	Ensure 'Pre-Login Banner' is set	☐	☐
2.1.2	Ensure 'Post-Login-Banner' is set	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.5	Ensure hostname is set	☐	☐
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	☐	☐
2.3.1	Ensure SNMP agent is disabled	☐	☐
2.3.2	Ensure only SNMPv3 is enabled	☐	☐
2.4.1	Ensure default 'admin' password is changed	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges having their correct profiles assigned	☐	☐
2.4.4	Ensure idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐
3.2	Ensure that policies do not use "ALL" as Service	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.3	Disable all management related services on WAN port	☐	☐
2.1.7	Disable USB Firmware and configuration installation	☐	☐
2.1.8	Disable static keys for TLS	☐	☐
2.1.9	Enable Global Strong Encryption	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.5.1	Ensure High Availability Configuration	☐	☐
2.5.2	Ensure "Monitor Interfaces" for High Availability Devices is Enabled	☐	☐
2.5.3	Ensure HA Reserved Management Interface is Configured	☐	☐
3.1	Ensure that unused policies are reviewed regularly	☐	☐
3.3	Ensure Policies are Uniquely Named	☐	☐
3.4	Ensure there are no Unused Policies	☐	☐
3.5	Ensure firewall policy denying all traffic to/from Tor or malicious server IP addresses using ISDB	☐	☐
3.6	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	☐	☐
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter	☐	☐
4.3.2	Ensure DNS Filter logs all DNS queries and responses	☐	☐
4.4.1	Block high risk categories on Application Control	☐	☐
4.4.2	Block applications running on non-default ports	☐	☐
4.4.3	Ensure all Application Control related traffic are logged	☐	☐
5.1.1	Enable Compromised Host Quarantine	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.1.1	Ensure Security Fabric is Configured	☐	☐
6.1.1	Apply a Trusted Signed Certificate for VPN Portal	☐	☐
6.1.2	Enable Limited TLS Versions for SSL VPN	☐	☐
7.1	Configuring the maximum login attempts and lockout period	☐	☐
8.1.1	Enable Event Logging	☐	☐
8.2.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager	☐	☐
8.3.1	Centralized Logging and Reporting	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.2	Ensure intra-zone traffic is not always allowed	☐	☐
2.1.1	Ensure 'Pre-Login Banner' is set	☐	☐
2.1.2	Ensure 'Post-Login-Banner' is set	☐	☐
2.1.5	Ensure hostname is set	☐	☐
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	☐	☐
2.3.1	Ensure SNMP agent is disabled	☐	☐
2.4.1	Ensure default 'admin' password is changed	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges having their correct profiles assigned	☐	☐
2.4.4	Ensure idle timeout time is configured	☐	☐

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	☐	☐
2.1.1	Ensure 'Pre-Login Banner' is set	☐	☐
2.1.2	Ensure 'Post-Login-Banner' is set	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.5	Ensure hostname is set	☐	☐
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	☐	☐
2.3.1	Ensure SNMP agent is disabled	☐	☐
2.3.2	Ensure only SNMPv3 is enabled	☐	☐
2.4.1	Ensure default 'admin' password is changed	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges having their correct profiles assigned	☐	☐
2.4.4	Ensure idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐

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	☐	☐
2.1.1	Ensure 'Pre-Login Banner' is set	☐	☐
2.1.2	Ensure 'Post-Login-Banner' is set	☐	☐
2.1.3	Ensure timezone is properly configured	☐	☐
2.1.4	Ensure correct system time is configured through NTP	☐	☐
2.1.5	Ensure hostname is set	☐	☐
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	☐	☐
2.3.1	Ensure SNMP agent is disabled	☐	☐
2.3.2	Ensure only SNMPv3 is enabled	☐	☐
2.4.1	Ensure default 'admin' password is changed	☐	☐
2.4.2	Ensure all the login accounts having specific trusted hosts enabled	☐	☐
2.4.3	Ensure admin accounts with different privileges having their correct profiles assigned	☐	☐
2.4.4	Ensure idle timeout time is configured	☐	☐
2.4.5	Ensure only encrypted access channels are enabled	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

	Recommendation	Set Correctly	
		Yes	No
1.3	Disable all management related services on WAN port	☐	☐
2.1.7	Disable USB Firmware and configuration installation	☐	☐
2.1.8	Disable static keys for TLS	☐	☐
2.1.9	Enable Global Strong Encryption	☐	☐
2.4.6	Apply Local-in Policies	☐	☐
2.5.1	Ensure High Availability Configuration	☐	☐
2.5.2	Ensure "Monitor Interfaces" for High Availability Devices is Enabled	☐	☐
2.5.3	Ensure HA Reserved Management Interface is Configured	☐	☐
3.1	Ensure that unused policies are reviewed regularly	☐	☐
3.2	Ensure that policies do not use "ALL" as Service	☐	☐
3.3	Ensure Policies are Uniquely Named	☐	☐
3.4	Ensure there are no Unused Policies	☐	☐
3.5	Ensure firewall policy denying all traffic to/from Tor or malicious server IP addresses using ISDB	☐	☐
3.6	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	☐	☐
4.3.1	Enable Botnet C&C Domain Blocking DNS Filter	☐	☐
4.3.2	Ensure DNS Filter logs all DNS queries and responses	☐	☐
4.4.1	Block high risk categories on Application Control	☐	☐
4.4.2	Block applications running on non-default ports	☐	☐
4.4.3	Ensure all Application Control related traffic are logged	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1	Enable Compromised Host Quarantine	☐	☐
5.2.1.1	Ensure Security Fabric is Configured	☐	☐
6.1.1	Apply a Trusted Signed Certificate for VPN Portal	☐	☐
6.1.2	Enable Limited TLS Versions for SSL VPN	☐	☐
7.1	Configuring the maximum login attempts and lockout period	☐	☐
8.1.1	Enable Event Logging	☐	☐
8.2.1	Encrypt Log Transmission to FortiAnalyzer / FortiManager	☐	☐
8.3.1	Centralized Logging and Reporting	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Apr 3, 2023	1.1.0	Use TLSv1.2 for Admin Access (Ticket 14490)