CIS OPNsense Benchmark

v1.0.0 - 03-26-2026

Terms of Use

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

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

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

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

Table of Contents

Overview

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

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

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

Important Usage Information

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

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

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

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

Key Stakeholders

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

Apply the Correct Version of a Benchmark

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

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

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

Exceptions

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

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

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

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

Remediation

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

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

The following is a reasonable remediation approach to follow:

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

Summary

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

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

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

Target Technology Details

This document provides prescriptive guidance for establishing a secure configuration posture for OPNsense. 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

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

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

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Profile 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.

- **Profile 2**

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

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

Acknowledgements

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

Author
Daniel Brown

Contributor
Darren Stevenson

Recommendations

1 General Setting Policy

1.1 Ensure SSH warning banner is configured (Manual)

Profile Applicability:

- Profile 1

Description:

Before authentication is allowed, a file containing its contents must be provided to the remote user, as specified by the Banner argument.

Rationale:

Banners are used to inform users who are connected of the specific site's connection rules. The prosecution of computer system intruders may be aided by the display of a warning message prior to the normal user login.

Audit:

In the CLI:

1. Run the following command and verify that output should contain 'Banner' parameter:

```
cat /etc/ssh/my_banner
```

Ensure a file exists in the /etc/ssh/ directory and that it contains the information you want in your ssh banner.

2. Run the following command and verify that a file exists, and that it references the above referenced "my_banner" file via a line such as:

```
Banner /etc/ssh/my_banner
```

Remediation:

In the CLI:

1. Create a banner file in the /etc/ssh/ directory via the following command

```
vi /etc/ssh/my_banner
```

2. To ensure your banner remains, you should utilize OPNsense's Targeted Overlays system by creating

   a file in the following directory:

```
vi /usr/local/etc/ssh/sshd_config.d/99-custom.conf
```

3. Then insert the following text in the 99-custom.conf file to reference your ssh banner file:

```
Banner /etc/ssh/my_banner
```

Save and exit the file

4. Restart OPNsense via the gui.

Default Value:

No banner is shown by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.1 Establish and Maintain a Security Awareness Program Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	17.3 Implement a Security Awareness Program Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	●	●	●

1.2 Ensure Backup count is set to 5 or more. (Manual)

Profile Applicability:

- Profile 1

Description:

OPNsense is able to store a user defined number of backups in a local cache.

Rationale:

An after-the-fact backup is taken after evaluating the change and ensuring it had the intended outcome. Periodic backups are also helpful, regardless of changes, especially in cases where a manual backup may be missed.

Audit:

In the GUI.

```
- Navigate to System -> Configuration -> Backups
```

Confirm "Backup Count" is set to 5 or more.

Remediation:

In the GUI.

```
- Navigate to System -> Configuration -> Backups
- Set the "Backup Count" to 5 or more.
- Click "Save"
```

Default Value:

Disabled

References:

1. https://docs.opnsense.org/manual/backups.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	10.1 Ensure Regular Automated Back Ups Ensure that all system data is automatically backed up on regular basis.	●	●	●

1.3 Ensure 'Message Of The Day (MOTD)' is set (Manual)

Profile Applicability:

- Profile 1

Description:

Sets the MOTD message.

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.

Audit:

In the OPNsense Shell type:

```
cat /var/run/motd
```

Remediation:

In the OPNsense Shell use vi to edit the message of the day:

```
vi /var/run/motd
```

Default Value:

```
root@OPNsense:~ # cat /var/run/motd
------------------------------------------------
|       Hello, this is OPNsense 25.7           |           :::::::.
|                                              |           :::::::::.
|  Website:     https://opnsense.org/          |        :::         :::
|  Handbook:    https://docs.opnsense.org/     |        :::         :::
|  Forums:      https://forum.opnsense.org/    |        :::         :::
|  Code:        https://github.com/opnsense    |         `:::::::::
|  Reddit:      https://reddit.com/r/opnsense  |           `:::::::
------------------------------------------------
root@OPNsense:~ #
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.1 Establish and Maintain a Security Awareness Program Establish and maintain a security awareness program. The purpose of a security awareness program is to educate the enterprise's workforce on how to interact with enterprise assets and data in a secure manner. Conduct training at hire and, at a minimum, annually. Review and update content annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	17.3 Implement a Security Awareness Program Create a security awareness program for all workforce members to complete on a regular basis to ensure they understand and exhibit the necessary behaviors and skills to help ensure the security of the organization. The organization's security awareness program should be communicated in a continuous and engaging manner.	●	●	●

1.4 Ensure Hostname is set (Automated)

Profile Applicability:

- Profile 1

Description:

Changes the device default hostname.

Rationale:

The device hostname is crucial for asset inventory and identification as a security need, as well as for the deployment of public keys and certificates and for comparing logs from various systems while handling an issue.

Audit:

In the CLI:

```
hostname
```

In the GUI:

```
- Navigate to System -> Settings -> General
- Check the Hostname Field
```

Remediation:

In the GUI:

```
- Navigate to System > Settings -> General
- Update the field 'Hostname' with the new hostname, and click "Save"
```

Default Value:

```
OPNsense.internal
```

References:

1. https://docs.opnsense.org/manual/settingsmenu.html#general

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	1.1 Establish and Maintain Detailed Enterprise Asset Inventory Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	●	●	●
v7	1.5 Maintain Asset Inventory Information Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.		●	●

1.5 Ensure DNS server is configured (Manual)

Profile Applicability:

- Profile 1

Description:

You must specify the main DNS server for your system in order to enable DNS lookups. Additionally, supplementary and third-party DNS servers can be specified. The system uses the main name server to resolve host names. The system examines the secondary name server, and if required, the tertiary, if a failure or time-out occurs.

Rationale:

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

Audit:

In the GUI:

```
- Navigate to System -> Settings -> General
- Check the 'DNS Server' Fields in the 'DNS Server' table under the
'Networking' section
```

Remediation:

In the GUI:

```
- Navigate to System -> Settings -> General
- Update the field 'DNS Servers' with the Your DNS Server, and click "Save"
```

Default Value:

By default it will be blank, unless the dynamic WAN type of DHCP is enabled then your ISP may assign these.

References:

1. https://docs.opnsense.org/manual/settingsmenu.html#general

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.		●	●

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

1.6 Ensure IPv6 is disabled if not used (Manual)

Profile Applicability:

- Profile 1

Description:

Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented.

Rationale:

If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Audit:

In the GUI:

```
Navigate to Interfaces -> Settings
```

Verify that 'Allow IPv6' is unchecked.

Remediation:

In the GUI:

```
Navigate to Interfaces -> Settings
Uncheck 'Allow IPv6'
```

Default Value:

In the GUI:

```
Interfaces -> Settings
'Allow IPv6' is checked.
```

CIS Controls:

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

Controls Version	Control	IG 1	IG 2	IG 3
v7	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.		●	●

1.7 Ensure 'Disable DNS Rebinding Checks' is unchecked (Manual)

Profile Applicability:

- Profile 1

Description:

Ensure that the 'Disable DNS Rebinding Checks' is unchecked to protect against DNS rebinding attacks.

Rationale:

Attackers can use DNS rebinding to exploit a DNS server's response to a domain name query that resolves to a private IP address. This could provide a hacker access to private network resources that shouldn't be made available to the general public. To defend against this kind of attack, OPNsense's "DNS Rebind Check" function disables private IP responses from DNS servers. As advised in the CIS benchmark, disabling this feature would expose the system to DNS rebinding attacks.

Audit:

In the GUI

```
- Navigate to System -> Settings -> Administration
- Verify that the 'Disable DNS Rebinding Checks' Field is unchecked
```

Remediation:

In the GUI

```
- Navigate to System -> Settings -> Administration
- uncheck the 'Disable DNS Rebinding Checks' Field
- Click save
```

Default Value:

By default the 'Disable DNS Rebinding Checks' is unchecked.

CIS Controls:

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

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

1.8 Ensure Web Management is Set to use HTTPS (Manual)

Profile Applicability:

- Profile 1

Description:

Web Admin Management Portal should only be accessed using HTTPS Protocol.

Rationale:

HTTP transmits all data (including passwords) in clear text over the network and provides no assurance of the identity of the hosts involved. Because of this HTTP should never be used for sensitive tasks such as managing network devices or entering login credentials and HTTPS should be configured for Web Portal Management instead

Audit:

In the GUI:

```
- Navigate to System -> Settings -> Administration
- Verify the 'Enable HTTP Strict Transport Security' option is enabled
```

Remediation:

In the GUI:

```
- Navigate to System -> Settings -> Administration
- Select the 'Enable HTTP Strict Transport Security' option
- Click 'Save'
```

Default Value:

In the GUI:

```
- System -> Settings -> Administration
- The 'Enable HTTP Strict Transport Security' option will be unchecked
```

CIS Controls:

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

Controls Version	Control	IG 1	IG 2	IG 3
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

2 Users Management

2.1 Ensure Sessions Timeout is set to less than or equal to 10 Minutes (Manual)

Profile Applicability:

- Profile 1

Description:

The session inactivity timeout setting represents the amount of time a user can be inactive before the user's session times out and closes. It only affects user browser sessions.

Rationale:

Indefinite or even long session timeout window increase the risk of attackers abusing abandoned sessions

Audit:

In GUI:

```
- Navigate to System > Settings > Administration
- Scroll to the 'Session Timeout'
- Check on the 'Session Timeout' field.
```

Remediation:

In GUI:

```
- Navigate to System > Settings > Administration
- Scroll to the 'Session Timeout'
- Set 10 in the 'Session Timeout' field
- Click Save
```

Default Value:

240 Minutes

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

2.2 Ensure LDAP or RADIUS server configured (Manual)

Profile Applicability:

- Profile 1

Description:

Configured the LDAP Servers or Radius server for central authentication.

Rationale:

Authentication, authorization and accounting (AAA) scheme provide an authoritative source for managing and monitoring access for devices.

Audit:

In the GUI:

```
- Navigate to System > Access > Servers
- See if an LDAP or RADIUS server have been configured
```

Remediation:

In the GUI:

```
- Navigate to System > Access > Servers
- Click the Orange Plus sign in the top right
- Enter the details needed for your LDAP server
- Click 'Save' at the bottom
```

Default Value:

Server Name: Local Database

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

2.3 Ensure Console Menu is Password Protected (Manual)

Profile Applicability:

- Profile 1

Description:

Set the Console Menu to password protected.

Rationale:

An unattended computer with an open Console Menu session to the device could allow an unauthorized user access to the firewall's management.

Audit:

In the GUI:

```
- Navigate to System > Settings > Administration
- Check "Console menu" Setting
```

Remediation:

In the GUI:

```
- Navigate to System > Settings > Administration
- Scroll to the 'Console' Section
- Ensure 'Password protect the console menu' is checked
- Click 'Save'
```

Default Value:

Default value is 'Checked'

CIS Controls:

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

2.4 Ensure all default accounts are either disabled or utilize strong passwords (Manual)

Profile Applicability:

- Profile 1

Description:

Disable the known default accounts configured. Note: The default admin account must remain enabled for high availability synchronization to work. Disabling it could cause issues.

Rationale:

Default accounts are accounts with predefined usernames and passwords that are typically included with software and hardware devices. Attackers often target default accounts because they are widely known and can be used to gain unauthorized access to a system. To prevent unauthorized access, all default accounts should either be disabled or have their passwords changed.

Audit:

In GUI:

```
- Navigate to System > Access > Users
- View the default users
```

Remediation:

In GUI:

```
- Navigate to System > Access > Users
- Remove any default users that are not used.
```

Note: The default admin account must remain enabled for high availability synchronization to work. Disabling it could cause issues.

Default Value:

The only default user is the "root" user.

Additional Information:

The known default accounts are often (without limiting to) the following: 'admin', 'guest', 'user', 'root', 'administrator', 'operator', 'supervisor', and 'demo'. It is important to change the passwords of these accounts to prevent attackers from using them to gain unauthorized access to the system. The use of strong, unique passwords for all user accounts is also recommended to further enhance security.

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	16.9 Disable Dormant Accounts Automatically disable dormant accounts after a set period of inactivity.	●	●	●

3 Password Policy

3.1 Ensure 'Local Account status' is set to 'Disabled' (Manual)

Profile Applicability:

- Profile 1

Description:

Disable the 'Local User' account except for the admin user.

Rationale:

Local accounts pose a threat to system security since the users are not manageable from the LDAP server.

Audit:

Need to manually check each account.

Remediation:

Disabled Local User Account.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	16.9 Disable Dormant Accounts Automatically disable dormant accounts after a set period of inactivity.	●	●	●

3.2 Ensure Login Protection methods are enabled. (Manual)

Profile Applicability:

- Profile 1

Description:

OPNsense strongly recommends enabling two-factor authentication (e.g., using TOTP) to protect user accounts, which is highly effective against password-based brute-force attacks.

Rationale:

Audit:

```
- Navigate to System > Access > Servers
- Check if there is a TOTP Server Configured
```

Remediation:

```
- Navigate to System > Access > Servers
- Click the Plus Sign to add a TOTP Server
- Give the server a descriptive name
- Select the TOTP Server Type
- Select a Token Length of 6
- Install Google Authenticator on your phone
- Add a user from System > Access > Users
- Enter a Username and Password and fill in the other fields just as you
would do for any other user. Then select the Generate new (160bit) secret
under OTP seed.
- Click Save
- For testing the user authentication, OPNsense offers a simple tester. Go to
System ▸ Access ▸ Tester
- Select the Authentication server you have configured, and enter the user
name. Then enter the *token + password, remember the order is token and then
password in the same field.
- Hit the test button and if all goes well you should see successfully
authenticated.
- Per default the system validates user credentials against the "Local
Database". In System ▸ Settings ▸ Administration, section Authentication you
should change this to your newly added authentication server to make sure no
local user can gain access without 2FA.
```

Default Value:

2FA is not enabled.

References:

1. https://docs.opnsense.org/manual/how-tos/two_factor.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

3.3 Ensure default password of admin is changed (Manual)

Profile Applicability:

- Profile 1

Description:

Ensure the default password is changed for the root user.

Rationale:

Using default passwords for the 'root' account could cause a compromise to the system.

Impact:

Failing to change the default 'root' account's password creates high risk to the system as the 'root' account may be abused by unauthorized users, allowing them full root access to the system.

Audit:

Try to login to the GUI with: Username: root Password: opnsense

Remediation:

In the GUI:

```
- Navigate to System > Access > Users
- Click the Pencil Icon under 'Commands'
- Change the password of the default 'root' user account.
- Click 'Save' at the bottom of the page.
```

Default Value:

opnsense

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.	●	●	●

4 Firewall Policy

4.1 Firewall Rules Policy

4.1.1 Ensure Default Deny is Enforced on All Internal Interfaces (Manual)

Profile Applicability:

- Profile 1

Description:

You must enforce a default deny policy on all internal interfaces (e.g., LAN, VLANs, DMZ, VPN).

Rationale:

Default deny prevents accidental exposure and limits lateral movement.

Impact:

You may break undocumented application traffic until you explicitly permit it.

Audit:

```
- Navigate to Firewall → Rules
- Verify each internal interface contains only explicit allow rules and no
broad "any/any" permits.
- Confirm traffic not explicitly allowed is denied.
```

Remediation:

```
- Navigate to Firewall → Rules
- Verify each internal interface contains only explicit allow rules and no
broad "any/any" permits.
- Confirm traffic not explicitly allowed is denied.
- Remove broad allow rules.
- Replace with explicit allow rules using aliases.
```

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

4.1.2 Ensure Least Privilege is Applied to All Permit Rules (Manual)

Profile Applicability:

- Profile 1

Description:

All allow rules must restrict traffic by:

- Source
- Destination
- Protocol
- Port/service

Rationale:

Overly broad rules create hidden attack paths.

Impact:

More rules may be required initially.

Audit:

```
1. Navigate to Firewall → Rules
2. Identify allow rules with:
- Source = any
- Destination = any
- Port = any
3. Validate business justification exists.
```

Remediation:

```
1. Navigate to Firewall → Rules
2. Identify allow rules with:
- Source = any
- Destination = any
- Port = any
3. Validate business justification exists.
4. Replace broad rules with alias-driven scoped rules.
```

CIS Controls:

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

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

4.1.3 Ensure “Any → Any” Rules are Prohibited (Manual)

Profile Applicability:

- Profile 1

Description:

You must not deploy any rule that permits “any source → any destination → any port.”

Rationale:

This defeats segmentation and enables unrestricted lateral movement.

Impact:

Some legacy environments may require modernization of rule design.

Audit:

```
1. Navigate to Firewall → Rules → [All interfaces]
2. Identify rules where:
- Source = any
- Destination = any
- Destination port = any
```

Remediation:

```
1. Navigate to Firewall → Rules → [All interfaces]
2. Identify rules where:
- Source = any
- Destination = any
- Destination port = any
3. Remove the rule.
- Replace with explicit rules using aliases.
```

Default Value:

IPv4 'Default allow LAN to any rule' IPv6 'Default allow LAN IPv6 to any rule'

CIS Controls:

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

4.1.4 Ensure Every Rule Has a Description Using a Standard Format (Manual)

Profile Applicability:

- Profile 1

Description:

Every firewall rule must include a description using the format: <ZONE> → <DEST> : <SERVICE> (Purpose)

Rationale:

Descriptions are required for auditability and safe change control.

Audit:

```
1. Navigate to Firewall → Rules
2. Verify no rule has an empty description field.
3. Verify descriptions are meaningful and standardized.
```

Remediation:

```
1. Navigate to Firewall → Rules
2. Verify no rule has an empty description field.
3. Verify descriptions are meaningful and standardized.
4. Update any rules that do not comply
5. Save each rule
```

CIS Controls:

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

4.1.5 Ensure Aliases are Used for Hosts, Networks, and Port Groups (Manual)

Profile Applicability:

- Profile 1

Description:

You must use aliases for:

- Any host referenced more than once
- Any port group referenced more than once
- All VLANs / security zones

Rationale:

Aliases reduce errors and simplify audits.

Impact:

Initial setup time increases slightly.

Audit:

```
1. Navigate to Firewall → Aliases
2. Confirm:
- Networks are defined as aliases
- Common port groups exist (DNS, NTP, Web, AD, etc.)

3. Confirm rules reference aliases instead of raw IPs repeatedly.
```

Remediation:

```
1. Navigate to Firewall → Aliases
2. Confirm:
- Networks are defined as aliases
- Common port groups exist (DNS, NTP, Web, AD, etc.)
3. Confirm rules reference aliases instead of raw IPs repeatedly.
4. Create aliases and update rules accordingly.
```

CIS Controls:

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

4.1.6 Ensure Rules are Implemented on the Ingress Interface (Manual)

Profile Applicability:

- Profile 1

Description:

You must define rules on the interface where traffic enters the firewall.

Rationale:

OPNsense evaluates rules based on ingress interface. Misplaced rules cause bypass or failure.

Impact:

May require refactoring if rules were implemented incorrectly.

Audit:

```
1. Navigate to Firewall → Rules
2. Validate each rule exists on the correct ingress interface.
```

Remediation:

```
1. Navigate to Firewall → Rules
2. Validate each rule exists on the correct ingress interface.
3. Move rules to the correct interface, if they are on the wrong one.
```

CIS Controls:

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

4.1.7 Ensure Standard Rule Ordering is Used Per Interface (Manual)

Profile Applicability:

- Profile 1

Description:

Rules must be ordered as follows:

1. Management / anti-lockout
2. Infrastructure (DNS/DHCP/NTP)
3. Internal access rules
4. Internet access rules
5. Explicit block rules (logged)

Rationale:

Consistent ordering improves readability and reduces mistakes.

Audit:

```
- Navigate to Firewall → Rules → [Interface]
- Confirm Ordering matches the standard
```

Remediation:

```
- Navigate to Firewall → Rules → [Interface]
- Confirm Ordering matches the standard
- Reorder rules that do not comply
```

CIS Controls:

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

4.1.8 Ensure Floating Rules are Restricted to Cross-Zone Policy Use Cases (Manual)

Profile Applicability:

- Profile 1

Description:

Floating rules must be used only when:

- Policy must apply across multiple interfaces
- “Quick” evaluation is required

Rationale:

Floating rules can override interface policy and cause unexpected behavior.

Impact:

May require moving rules back to interfaces.

Audit:

```
1. Navigate to Firewall → Rules → Floating
2. Validate each floating rule has:
- documented justification
- limited scope
```

Remediation:

```
1. Navigate to Firewall → Rules → Floating
2. Validate each floating rule has:
- documented justification
- limited scope
3. Move rules to interface rulesets when possible.
```

CIS Controls:

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

5 Service Configuration

5.1 NTP Service Policy

5.1.1 Ensure time zone is properly configured (Manual)

Profile Applicability:

- Profile 1

Description:

Sets the local time zone information so that the device's time display is more accurate for viewers.

Rationale:

The device's time setting needs to be accurate for two reasons in particular. The first is that digital certificates use this time to compare the validity period they specify in their Valid From and Valid To fields to a range of times. The second justification is the need for accurate time stamps when logging data. When doing packet captures, delivering messages to a Syslog server, SNMP monitoring stations, or other tasks, timestamps are only meaningful if you can be certain of their accuracy.

Audit:

```
In the GUI:
- Navigate to Services > Network Time > General
- Verify NTP Servers are configured properly and one is checked as 'Prefer'
```

Remediation:

```
In the GUI:
- Navigate to Services > Network Time > General
- Add NTP servers under 'Time Servers'
- Select one as preferred by checking 'Prefer'
- Click 'Save'
```

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.		●	●

5.2 DNS Service Policy

5.2.1 Ensure 'DNSSEC' is Enable on DNS Service (Manual)

Profile Applicability:

- Profile 1

Description:

Enable the "DNSSEC" in the DNS Service Configuration.

Rationale:

Enable DNSSEC Support. DNSSEC is a means of protecting DNS data from attacks which use forged or manipulated DNS data, such as DNS cache poisoning.

Audit:

```
In the GUI:
- Navigate to Services > Unbound DNS > General
- Verify if 'Enable DNSSEC Support' is checked
```

Remediation:

```
In the GUI:
- Navigate to Services > Unbound DNS > General
- Check next to 'Enable DNSSEC Support'
- Click 'Apply'
```

CIS Controls:

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

5.3 VPN Configuration

5.3.1 Ensure WireGuard is used as the default VPN method (Manual)

Profile Applicability:

- Profile 1

Description:

WireGuard must use a dedicated RFC1918 subnet that is not reused by any internal VLAN. Additionally, WireGuard must remain disabled unless explicitly required for approved remote access or site-to-site VPN use cases.

Rationale:

Impact:

No VPN access is available until enabled.

Audit:

```
1. Navigate to VPN → WireGuard
2. Confirm no WireGuard instances are enabled unless required.
```

Remediation:

```
1. Navigate to VPN → WireGuard → Instances
2. Click the Plus Sign to add a WireGuard Instance
3. Click 'Save' when all of your instance details are entered
```

Default Value:

No VPNs enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.7 Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure Require users to authenticate to enterprise-managed VPN and authentication services prior to accessing enterprise resources on end-user devices.		●	●
v7	12.12 Manage All Devices Remotely Logging into Internal Network Scan all enterprise devices remotely logging into the organization's network prior to accessing the network to ensure that each of the organization's security policies has been enforced in the same manner as local network devices.			●

6 Logging

6.1 Ensure Logging is Enabled for Inter-Zone Deny Rules (Manual)

Profile Applicability:

- Profile 1

Description:

All deny rules that enforce segmentation between VLANs/zones must have logging enabled.

Rationale:

Inter-zone denies are high-signal and reveal lateral movement attempts.

Impact:

Moderate log volume increase.

Audit:

```
1. Navigate to Firewall → Rules
2. Identify deny rules between VLANs
3. Confirm "Log" is enabled on each
```

Remediation:

```
1. Navigate to Firewall → Rules
2. Identify deny rules between VLANs
3. Enable logging for segmentation deny rules.
```

Default Value:

No Logging Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2 Ensure Logging is Enabled for Management Plane Deny Rules (Manual)

Profile Applicability:

- Profile 1

Description:

All deny rules targeting firewall management services or MGMT networks must be logged.

Rationale:

Management targeting is a high-risk indicator and should generate security alerts.

Impact:

Low log volume increase.

Audit:

Verify deny rules for MGMT subnets and firewall GUI/SSH ports have logging enabled.

Remediation:

Enable logging on MGMT deny rules.

Default Value:

Not Enabled by default

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	8.8 Enable Command-line Audit Logging Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.		●	●

6.3 Ensure Remote Syslog is Configured (Manual)

Profile Applicability:

- Profile 1

Description:

OPNsense must forward logs to a remote log server or SIEM using syslog.

Rationale:

Local-only logs can be erased during compromise and are not sufficient for enterprise IR.

Impact:

Requires syslog receiver and storage.

Audit:

```
1. Navigate to System → Settings → Logging / Targets (or Syslog depending on
build)
2. Confirm at least one remote syslog target exists.
3. Confirm logs are received by the SIEM.
```

Remediation:

```
1. Navigate to System → Settings → Logging / Targets (or Syslog depending on
build)
2. Configure syslog target(s) to an enterprise log platform.
```

Default Value:

Empty

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**General Setting Policy**		
1.1	Ensure SSH warning banner is configured (Manual)	☐	☐
1.2	Ensure Backup count is set to 5 or more. (Manual)	☐	☐
1.3	Ensure 'Message Of The Day (MOTD)' is set (Manual)	☐	☐
1.4	Ensure Hostname is set (Automated)	☐	☐
1.5	Ensure DNS server is configured (Manual)	☐	☐
1.6	Ensure IPv6 is disabled if not used (Manual)	☐	☐
1.7	Ensure 'Disable DNS Rebinding Checks' is unchecked (Manual)	☐	☐
1.8	Ensure Web Management is Set to use HTTPS (Manual)	☐	☐
2	**Users Management**		
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes (Manual)	☐	☐
2.2	Ensure LDAP or RADIUS server configured (Manual)	☐	☐
2.3	Ensure Console Menu is Password Protected (Manual)	☐	☐
2.4	Ensure all default accounts are either disabled or utilize strong passwords (Manual)	☐	☐
3	**Password Policy**		
3.1	Ensure 'Local Account status' is set to 'Disabled' (Manual)	☐	☐
3.2	Ensure Login Protection methods are enabled. (Manual)	☐	☐
3.3	Ensure default password of admin is changed (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4	**Firewall Policy**		
4.1	**Firewall Rules Policy**		
4.1.1	Ensure Default Deny is Enforced on All Internal Interfaces (Manual)	☐	☐
4.1.2	Ensure Least Privilege is Applied to All Permit Rules (Manual)	☐	☐
4.1.3	Ensure “Any → Any” Rules are Prohibited (Manual)	☐	☐
4.1.4	Ensure Every Rule Has a Description Using a Standard Format (Manual)	☐	☐
4.1.5	Ensure Aliases are Used for Hosts, Networks, and Port Groups (Manual)	☐	☐
4.1.6	Ensure Rules are Implemented on the Ingress Interface (Manual)	☐	☐
4.1.7	Ensure Standard Rule Ordering is Used Per Interface (Manual)	☐	☐
4.1.8	Ensure Floating Rules are Restricted to Cross-Zone Policy Use Cases (Manual)	☐	☐
5	**Service Configuration**		
5.1	**NTP Service Policy**		
5.1.1	Ensure time zone is properly configured (Manual)	☐	☐
5.2	**DNS Service Policy**		
5.2.1	Ensure 'DNSSEC' is Enable on DNS Service (Manual)	☐	☐
5.3	**VPN Configuration**		
5.3.1	Ensure WireGuard is used as the default VPN method (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6	**Logging**		
6.1	Ensure Logging is Enabled for Inter-Zone Deny Rules (Manual)	☐	☐
6.2	Ensure Logging is Enabled for Management Plane Deny Rules (Manual)	☐	☐
6.3	Ensure Remote Syslog is Configured (Manual)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	☐	☐
1.2	Ensure Backup count is set to 5 or more.	☐	☐
1.3	Ensure 'Message Of The Day (MOTD)' is set	☐	☐
1.5	Ensure DNS server is configured	☐	☐
1.7	Ensure 'Disable DNS Rebinding Checks' is unchecked	☐	☐
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	☐	☐
2.4	Ensure all default accounts are either disabled or utilize strong passwords	☐	☐
3.1	Ensure 'Local Account status' is set to 'Disabled'	☐	☐
3.3	Ensure default password of admin is changed	☐	☐
5.2.1	Ensure 'DNSSEC' is Enable on DNS Service	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	☐	☐
1.2	Ensure Backup count is set to 5 or more.	☐	☐
1.3	Ensure 'Message Of The Day (MOTD)' is set	☐	☐
1.4	Ensure Hostname is set	☐	☐
1.5	Ensure DNS server is configured	☐	☐
1.6	Ensure IPv6 is disabled if not used	☐	☐
1.7	Ensure 'Disable DNS Rebinding Checks' is unchecked	☐	☐
1.8	Ensure Web Management is Set to use HTTPS	☐	☐
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	☐	☐
2.2	Ensure LDAP or RADIUS server configured	☐	☐
2.3	Ensure Console Menu is Password Protected	☐	☐
2.4	Ensure all default accounts are either disabled or utilize strong passwords	☐	☐
3.1	Ensure 'Local Account status' is set to 'Disabled'	☐	☐
3.3	Ensure default password of admin is changed	☐	☐
4.1.1	Ensure Default Deny is Enforced on All Internal Interfaces	☐	☐
5.1.1	Ensure time zone is properly configured	☐	☐
5.2.1	Ensure 'DNSSEC' is Enable on DNS Service	☐	☐
6.1	Ensure Logging is Enabled for Inter-Zone Deny Rules	☐	☐
6.2	Ensure Logging is Enabled for Management Plane Deny Rules	☐	☐
6.3	Ensure Remote Syslog is Configured	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	☐	☐
1.2	Ensure Backup count is set to 5 or more.	☐	☐
1.3	Ensure 'Message Of The Day (MOTD)' is set	☐	☐
1.4	Ensure Hostname is set	☐	☐
1.5	Ensure DNS server is configured	☐	☐
1.6	Ensure IPv6 is disabled if not used	☐	☐
1.7	Ensure 'Disable DNS Rebinding Checks' is unchecked	☐	☐
1.8	Ensure Web Management is Set to use HTTPS	☐	☐
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	☐	☐
2.2	Ensure LDAP or RADIUS server configured	☐	☐
2.3	Ensure Console Menu is Password Protected	☐	☐
2.4	Ensure all default accounts are either disabled or utilize strong passwords	☐	☐
3.1	Ensure 'Local Account status' is set to 'Disabled'	☐	☐
3.2	Ensure Login Protection methods are enabled.	☐	☐
3.3	Ensure default password of admin is changed	☐	☐
4.1.1	Ensure Default Deny is Enforced on All Internal Interfaces	☐	☐
5.1.1	Ensure time zone is properly configured	☐	☐
5.2.1	Ensure 'DNSSEC' is Enable on DNS Service	☐	☐
5.3.1	Ensure WireGuard is used as the default VPN method	☐	☐
6.1	Ensure Logging is Enabled for Inter-Zone Deny Rules	☐	☐
6.2	Ensure Logging is Enabled for Management Plane Deny Rules	☐	☐
6.3	Ensure Remote Syslog is Configured	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	☐	☐
1.2	Ensure Backup count is set to 5 or more.	☐	☐
1.3	Ensure 'Message Of The Day (MOTD)' is set	☐	☐
1.4	Ensure Hostname is set	☐	☐
1.7	Ensure 'Disable DNS Rebinding Checks' is unchecked	☐	☐
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	☐	☐
2.3	Ensure Console Menu is Password Protected	☐	☐
2.4	Ensure all default accounts are either disabled or utilize strong passwords	☐	☐
3.1	Ensure 'Local Account status' is set to 'Disabled'	☐	☐
3.3	Ensure default password of admin is changed	☐	☐
4.1.1	Ensure Default Deny is Enforced on All Internal Interfaces	☐	☐
5.2.1	Ensure 'DNSSEC' is Enable on DNS Service	☐	☐
6.2	Ensure Logging is Enabled for Management Plane Deny Rules	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	☐	☐
1.2	Ensure Backup count is set to 5 or more.	☐	☐
1.3	Ensure 'Message Of The Day (MOTD)' is set	☐	☐
1.4	Ensure Hostname is set	☐	☐
1.5	Ensure DNS server is configured	☐	☐
1.6	Ensure IPv6 is disabled if not used	☐	☐
1.7	Ensure 'Disable DNS Rebinding Checks' is unchecked	☐	☐
1.8	Ensure Web Management is Set to use HTTPS	☐	☐
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	☐	☐
2.2	Ensure LDAP or RADIUS server configured	☐	☐
2.3	Ensure Console Menu is Password Protected	☐	☐
2.4	Ensure all default accounts are either disabled or utilize strong passwords	☐	☐
3.1	Ensure 'Local Account status' is set to 'Disabled'	☐	☐
3.2	Ensure Login Protection methods are enabled.	☐	☐
3.3	Ensure default password of admin is changed	☐	☐
4.1.1	Ensure Default Deny is Enforced on All Internal Interfaces	☐	☐
5.1.1	Ensure time zone is properly configured	☐	☐
5.2.1	Ensure 'DNSSEC' is Enable on DNS Service	☐	☐
5.3.1	Ensure WireGuard is used as the default VPN method	☐	☐
6.1	Ensure Logging is Enabled for Inter-Zone Deny Rules	☐	☐
6.2	Ensure Logging is Enabled for Management Plane Deny Rules	☐	☐
6.3	Ensure Remote Syslog is Configured	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	☐	☐
1.2	Ensure Backup count is set to 5 or more.	☐	☐
1.3	Ensure 'Message Of The Day (MOTD)' is set	☐	☐
1.4	Ensure Hostname is set	☐	☐
1.5	Ensure DNS server is configured	☐	☐
1.6	Ensure IPv6 is disabled if not used	☐	☐
1.7	Ensure 'Disable DNS Rebinding Checks' is unchecked	☐	☐
1.8	Ensure Web Management is Set to use HTTPS	☐	☐
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	☐	☐
2.2	Ensure LDAP or RADIUS server configured	☐	☐
2.3	Ensure Console Menu is Password Protected	☐	☐
2.4	Ensure all default accounts are either disabled or utilize strong passwords	☐	☐
3.1	Ensure 'Local Account status' is set to 'Disabled'	☐	☐
3.2	Ensure Login Protection methods are enabled.	☐	☐
3.3	Ensure default password of admin is changed	☐	☐
4.1.1	Ensure Default Deny is Enforced on All Internal Interfaces	☐	☐
5.1.1	Ensure time zone is properly configured	☐	☐
5.2.1	Ensure 'DNSSEC' is Enable on DNS Service	☐	☐
5.3.1	Ensure WireGuard is used as the default VPN method	☐	☐
6.1	Ensure Logging is Enabled for Inter-Zone Deny Rules	☐	☐
6.2	Ensure Logging is Enabled for Management Plane Deny Rules	☐	☐
6.3	Ensure Remote Syslog is Configured	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	☐	☐

Appendix: Change History

Date	Version	Changes for this version