

CIS pfSense Firewall Benchmark

v1.1.0 - 06-30-2023

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

Terms of Use	1
Table of Contents	2
Overview	4
Intended Audience.....	4
Consensus GUIDance.....	5
Typographical Conventions.....	6
Recommendation Definitions.....	7
Title.....	7
Assessment Status.....	7
Automated	7
Manual.....	7
Profile	7
Description.....	7
Rationale Statement	7
Impact Statement.....	8
Audit Procedure.....	8
Remediation Procedure.....	8
Default Value.....	8
References	8
CIS Critical Security Controls® (CIS Controls®).....	8
Additional Information.....	8
Profile Definitions	9
Acknowledgements	10
Recommendations	11
1 General Setting Policy.....	11
1.1 Ensure SSH warning banner is configured (Manual)	12
1.2 Ensure AutoConfigBackup is enable (Manual).....	14
1.3 Ensure 'Message Of The Day (MOTD)' is set (Manual)	16
1.4 Ensure Hostname is set (Manual)	18
1.5 Ensure DNS server is configured (Manual).....	20
1.6 Ensure IPv6 is disabled if not used (Manual)	21
1.7 Ensure 'DNS Rebind Check' is unchecked (Manual)	23
1.8 Ensure Web Management is Set to use HTTPS (Manual)	24
1.9 Ensure a synchronized High Availability peer is configured (Manual)	26
2 Users Management.....	27
2.1 Ensure Sessions Timeout is set to less than or equal to 10 Minutes (Manual)	28

2.2 Ensure LDAP or RADIUS server configured (Manual)	30
2.3 Ensure Console Menu is Password Protected (Manual)	31
2.4 Ensure all default accounts are either disabled or utilize strong passwords (Manual)	32
3 Password Policy	34
3.1 Ensure 'Local Account status' is set to 'Disabled' (Manual).....	35
3.2 Ensure Login Protection Threshold is set to 30 or less (Manual)	36
3.3 Ensure Allow access again after time is set to 300 or more second (Manual)	38
3.4 Ensure default password of admin is changed (Manual).....	39
4 Firewall Policy.....	41
4.1 Firewall Rules Policy	42
4.1.1 Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules (Manual)	43
4.1.2 Ensure no Allow Rule with Any in Source field present in the Firewall Rules (Manual).....	45
4.1.3 Ensure no Allow Rule with Any in Services field present in the Firewall Rules (Manual)	47
4.1.4 Ensure there are no Unused Policies (Manual).....	49
4.1.5 Ensure Logging is Enable for All Firewall Rules (Manual).....	50
4.1.6 Ensure ICMP Request is securely configured (Manual)	52
5 Service Configuration.....	54
5.1 SNMP Policy	55
5.1.1 Ensure SNMP traps receivers is set (Manual)	56
5.1.2 Ensure SNMP traps is enabled (Manual)	58
5.1.3 Ensure that the add-on package NET-SNMP is installed and configured securely (Manual).....	60
5.2 NTP Service Policy	61
5.2.1 Ensure time zone is properly configured (Manual)	62
5.3 DNS Service Policy	64
5.3.1 Ensure 'DNSSEC' is Enable on DNS Service (Manual)	65
5.4 VPN Configuration	66
5.4.1 Ensure RADIUS or LDAP are being used for VPN Authentication (Manual).....	67
5.4.2 Apply a Trusted Signed Certificate for VPN Portal (Manual)	68
5.4.3 Ensure that OpenVPN is configured to use TLS encryption for secure communications. (Manual) ...	70
5.5 OpenVPN	71
5.5.1 Ensure that OpenVPN use strong ciphers or hashing algorithms (Manual)	72
6 Logging	73
6.1 Ensure syslog is configured (Manual)	74
Appendix: Summary Table	76
Appendix: Change History	91

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 PfSense devices running version 2.5.0 or above. This Guide was tested against pfSense 2.5.0. 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
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<i><italic font in brackets></i>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	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

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

Touhid Shaikh

Contributor

Darren Freidel

Daniel Brown

Touhid Shaikh Senior Security Consultant in Securityium

Recommendations

1 General Setting Policy

1.1 Ensure SSH warning banner is configured (Manual)

Profile Applicability:

- Level 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:

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

```
grep "^Banner" /etc/ssh/sshd_config
```

Remediation:

In the CLI:




Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:




```
Banner /etc/issue.net
```

Default Value:

No banner is shown by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.1 <u>Establish and Maintain a Security Awareness Program</u> 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.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>17.3 Implement a Security Awareness Program</p> <p>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.</p>			

1.2 Ensure AutoConfigBackup is enable (Manual)

Profile Applicability:

- Level 1

Description:

Making a backup before and after each large change or series of changes, as well as after each little change, is the recommended practice. A first backup is typically prepared in case the change being done has unfavorable repercussions.

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 Services > Auto Config Backup.
```

Remediation:

In the GUI.

```
- Navigate to Services > Auto Config Backup.  
- Click the Setting at the top.  
- Check on the Enable ACB.  
- Click Save
```

Default Value:




Disabled

References:

1. <https://docs.netgate.com/pfsense/en/latest/backup/autoconfigbackup.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 <u>Ensure Regular Automated Back Ups</u> 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:

- Level 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 pfSense Shell type:

```
cat /etc/motd
```

Remediation:

In pfSense Shell:

```
Type 'Message Of The Day (MOTD)' message here
vi /etc/motd
```

Default Value:

```
[2.5.0-RELEASE][admin@pfSense.home.arpa]/root: cat /etc/motd
FreeBSD ?..? (UNKNOWN)

Welcome to FreeBSD!







Release Notes, Errata: https://www.FreeBSD.org/releases/
Security Advisories:  https://www.FreeBSD.org/security/
FreeBSD Handbook:    https://www.FreeBSD.org/handbook/
FreeBSD FAQ:          https://www.FreeBSD.org/faq/
Questions List:       https://lists.FreeBSD.org/mailman/listinfo/freebsd-questions/
FreeBSD Forums:       https://forums.FreeBSD.org/

Documents installed with the system are in the /usr/local/share/doc/freebsd/
directory, or can be installed later with:  pkg install en-freebsd-doc
For other languages, replace "en" with a language code like de or fr.

Show the version of FreeBSD installed:  freebsd-version ; uname -a
Please include that output and any error messages when posting questions.
Introduction to manual pages:  man man
FreeBSD directory layout:      man hier

Edit /etc/motd to change this login announcement.
[2.5.0-RELEASE][admin@pfSense.home.arpa]/root:
```

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.1 <u>Establish and Maintain a Security Awareness Program</u> 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 <u>Implement a Security Awareness Program</u> 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 (Manual)

Profile Applicability:

- Level 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 > General Setup
- Check the Hostname Field

Remediation:

In the GUI:

- Navigate to System > General Setup
- Update the field 'Hostname' with the new hostname, and Click "Save"






Default Value:

pfSense

References:

1. <https://docs.netgate.com/pfsense/en/latest/config/general.html>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><u>1.1 Establish and Maintain Detailed Enterprise Asset Inventory</u></p> <p>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.</p>			
v7	<p><u>1.5 Maintain Asset Inventory Information</u></p> <p>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.</p>			

1.5 Ensure DNS server is configured (Manual)

Profile Applicability:

- Level 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 > General Setup
- Check the 'DNS Servers' Field in 'DNS Server Settings' table

Remediation:






In the GUI:

- Navigate to System > General Setup
- 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.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.9 Configure Trusted DNS Servers on Enterprise Assets</u> 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	<u>7.7 Use of DNS Filtering Services</u> Use DNS filtering services to help block access to known malicious domains.			

1.6 Ensure IPv6 is disabled if not used (Manual)

Profile Applicability:

- Level 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 CLI:

```
cat /etc/sysctl.conf
```

check below entries:

- net.ipv6.conf.all.disable_ipv6=1
- net.ipv6.conf.default.disable_ipv6=1
- net.ipv6.conf.lo.disable_ipv6 = 1

In the GUI:

```
Navigate to System > Advanced > Networking
```

Check if 'Allow IPv6' is checked.

Remediation:

In the CLI:

```
Add below in the `/etc/sysctl.conf` file and reboot.  
- net.ipv6.conf.all.disable_ipv6=1  
- net.ipv6.conf.default.disable_ipv6=1  
- net.ipv6.conf.lo.disable_ipv6 = 1
```

In the GUI:





```
Navigate to System > Advanced > Networking  
Uncheck 'Allow IPv6'
```

Default Value:

In the GUI:

System > Advanced > Networking
'Allow IPv6' is checked.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

1.7 Ensure 'DNS Rebind Check' is unchecked (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the 'DNS Rebind Check' feature 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, pfSense'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 > Advance
- Check the 'DNS Rebind Check' Field

Remediation:







In the GUI

- Navigate to System > Advance
- Uncheck on 'DNS Rebind Check' Field

Default Value:

By default the 'DNS Rebind Check' is unchecked.

CIS Controls:

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

- Level 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 > Advance > Admin Access
- Check the 'webConfigurator' Table for HTTPS Enable.

Remediation:

In the GUI:



- Navigate to System > Advanced > Admin Access
- Select 'HTTPS' in the 'webConfigurator'.
- CLick 'Save'

Default Value:

In the GUI:

System > Advanced > Admin Access
'Protocol' will be 'HTTPS (SSL/TLS)'

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	<p><u>11.1 Maintain Standard Security Configurations for Network Devices</u></p> <p>Maintain standard, documented security configuration standards for all authorized network devices.</p>		●	●

1.9 Ensure a synchronized High Availability peer is configured (Manual)

Profile Applicability:

- Level 1

Description:

Ensure a High Availability peer is fully synchronized and in a passive or active state.

Rationale:

To ensure availability of both the firewall and the resources it protects, a High Availability peer is required. In the event a single firewall fails, or when maintenance such as a software update is required, the HA peer can be used to automatically fail over session states and maintain overall availability

Audit:

In the GUI:

- Navigate to System > High Avail. Sync
- Check "Synchronize Config to IP" is configured.

Remediation:






In the GUI:

- Navigate to System > High Avail. Sync
- Setup each field and Hit Save

Default Value:

All fields are blank

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 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	<u>11.1 Maintain Standard Security Configurations for Network Devices</u> 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:

- Level 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 > User Manager
- Click the Setting at the top.
- Check on the 'Session Timeout' field.

Remediation:




In GUI:

- Navigate to System > User Manager
- Click the Setting at the top.
- set 10 in the 'Session Timeout' field.
- Click Save

Default Value:

Username listed will be: 'admin'

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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:

- Level 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 > User Manager.
- Click the Authentication Servers at the top.
- Check "Authentication Servers" Setting

Remediation:





In the GUI:

- Navigate to System > User Manager.
- Click the Authentication Servers at the top.
- Configure "Authentication Servers" Setting

Default Value:

'Server Name' will be '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:

- Level 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 > Advanced > Admin Access.
- Check "Console Options" Setting

Remediation:






In the GUI:

- Navigate to System > Advanced > Admin Access.
- Set "Console Options" Setting
- Click "Save"

Default Value:

'Console menu' will be unchecked

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:

- Level 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 > User Manager > Users
- View the default users

Remediation:

In GUI:

- Navigate to System > User Manager > 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 "admin" 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	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> 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	<u>16.9 Disable Dormant Accounts</u> 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:

- Level 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 <u>Disable Dormant Accounts</u> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.			
v7	16.9 <u>Disable Dormant Accounts</u> Automatically disable dormant accounts after a set period of inactivity.			

3.2 Ensure Login Protection Threshold is set to 30 or less (Manual)

Profile Applicability:

- Level 1

Description:

The Login Protection Threshold is a score-based system that helps to prevent unauthorized access to the pfSense firewall. This score is based on various criteria, including the number of unsuccessful login attempts from a specific IP address. This control ensures that the Login Protection Threshold is set to a value of 30 or less.

Rationale:

Setting the Login Protection Threshold to a value of 30 or less helps to prevent attackers from brute-forcing their way into the system. The default value is 30, and this is a reasonable value for most situations. By limiting the number of unsuccessful login attempts, the system can protect against unauthorized access and improve security.

Audit:

In the GUI:



- Navigate to System > Advanced
- Check the 'Login Protection' > 'Threshold' Field

Remediation:

In the GUI:

- Navigate to System > Advanced
- Set 30 in the 'Login Protection' > 'Threshold' Field
- Click 'Save'

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p>4.10 Enforce Automatic Device Lockout on Portable End-User Devices</p> <p>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.</p>			

Controls Version	Control	IG 1	IG 2	IG 3
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 Allow access again after time is set to 300 or more second (Manual)

Profile Applicability:

- Level 2

Description:

Account password lockout \geq 300 seconds. Allow access again after a user has been locked out (due to failed login attempts). The user is allowed access after the configured time if there have been no login attempts during that time).

Rationale:

the Allow access again after the time setting determines the number of seconds.

Audit:

In GUI:

- Navigate to System > Advanced > Admin Access
- Check the 'Login Protection' options.
- Check 'Blocktime' value is greater than 300 seconds.

Remediation:




In GUI:

- Navigate to System > Advanced > Admin Access
- set the 'Login Protection' options.
- set 'Blocktime' value to 300.
- Click Save

Default Value:

'Blocktime' will be blank

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.			

3.4 Ensure default password of admin is changed (Manual)

Profile Applicability:

- Level 1

Description:

To assist users in changing the default password for 'admin' account.

Rationale:

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

Impact:

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

Audit:

Try to login to the GUI with:

Username: admin

Password: pfsense

Remediation:

In the GUI:







- Navigate to System > User Manager
- Click the Pencil Icon under 'Actions'
- Change the password of the default 'admin' user account.
- Click 'Save' at the bottom of the page.

Default Value:

Default Values:

User: admin
Password: pfsense

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> 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	<u>4.2 Change Default Passwords</u> 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 no Allow Rule with Any in Destination Field present in the Firewall Rules (Manual)

Profile Applicability:

- Level 1

Description:

The Firewall Rules with Any in Source field allows all the IP Addresses of the Network to access the specified destination configured in the Firewall rules for specific services.

Rationale:

In any properly designed and implemented Milner Firewall architecture the connection that loads the service should be explicitly allowed from the IP source address to the specific IP destination address. This services abolishes the chances of an exploit because of service misconfigurations.

Audit:

Verify there are no allowed rules present in the firewall which has Any used in the Destination field

In CLI:

```
pfctl -sr
```

Remediation:




Delete or Disable the rule from the firewall which has Any used in the Destination field.












Default Value:

Default "Allow Any" rule to prevent lockout.

Default "Allow Any" rules on LAN Interfaces to allow network connectivity within the LAN.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 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.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> 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	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.1 <u>Maintain Standard Security Configurations for Network Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.			

4.1.2 Ensure no Allow Rule with Any in Source field present in the Firewall Rules (Manual)

Profile Applicability:

- Level 1

Description:

The Firewall Rules with Any in the Destination field allows accessing all the IP Addresses of Network from specified Sources configured in the Firewall rules for specific services

Rationale:

Ideally, the traffic should be explicitly allowed from the specific Source to specific Destination for the required services. This provides better control over the traffic passes through the firewall and reduce the chances of an exploit because of service misconfiguration.

Audit:

Verify there are no allowed rules present in the firewall which has Any used in the Source field. If there is any such rule present in the firewall, it should have a business justification and also it should be documented
In CLI:

```
pfctl -sr
```

Remediation:




Delete the rule from the firewall which has Any used in the Source field.












Default Value:

Default "Allow Any" rule to prevent lockout.

Default "Allow Any" rules on LAN Interfaces to allow network connectivity within the LAN.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 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.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> 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	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.1 <u>Maintain Standard Security Configurations for Network Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.			

4.1.3 Ensure no Allow Rule with Any in Services field present in the Firewall Rules (Manual)

Profile Applicability:

- Level 1

Description:

The Firewall Rules with Any in the Service field allows accessing all the Services from specified Source to specified Destination configured in the Firewall rules.

Rationale:

Many services, including telnet, FTP, and TFTP, have security problems. Attackers can utilize these services to their advantage in order to access computers, obtain credentials, or launch DoS attacks. These services must be set up in accordance with the requirements of the company.

Audit:

Verify there are no allowed rules present in the firewall which has Any used in the Service field.

In CLI:

```
pfctl -sr
```

Remediation:




Delete the rule from the firewall which has Any used in the Service field.












Default Value:

Default "Allow Any" rule to prevent lockout.

Default "Allow Any" rules on LAN Interfaces to allow network connectivity within the LAN.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.2 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.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 <u>Implement and Manage a Firewall on Servers</u> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	4.5 <u>Implement and Manage a Firewall on End-User Devices</u> 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	9.4 <u>Apply Host-based Firewalls or Port Filtering</u> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v7	11.1 <u>Maintain Standard Security Configurations for Network Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.			

4.1.4 Ensure there are no Unused Policies (Manual)

Profile Applicability:

- Level 1

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 unused firewall policies.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software</u> Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.			
v7	<u>11.1 Maintain Standard Security Configurations for Network Devices</u> Maintain standard, documented security configuration standards for all authorized network devices.			

4.1.5 Ensure Logging is Enable for All Firewall Rules (Manual)

Profile Applicability:

- Level 1

Description:

Ensure all firewall rules have logging enable.

Rationale:

The event log of firewall rules helps in identifying the allowed and blocked traffic and also helps in troubleshooting and forensic investigation. It is always good to enable logging for all the firewall rules, but by logging multiple firewall rules results in a huge log files, which requires huge disk space and management operations. Logs play an important role in security auditing, incident response, system maintenance and forensic investigation, and should be configured as per the business needs.

Audit:

In the GUI:

- Navigate to Status > System Logs > Settings
- Verify Desired Logging Options are enabled

Remediation:

In the GUI:

- Navigate to Status > System Logs > Settings
- Check Desired Logging Options to enable.

Default Value:

The following log options are enabled by default: Log firewall default blocks:

- Log packets matched from the default block rules in the ruleset
- Log packets blocked by 'Block Bogon Networks' rules
- Log packets blocked by 'Block Private Networks' rules Web Server Log:
- Log errors from the web server process Log Configuration Changes:
- Generate log entries when making changes to the configuration.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.8 <u>Document Data Flows</u> Document data flows. Data flow documentation includes service provider data flows and should be based on the enterprise's data management process. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 <u>Enable Detailed Logging</u> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.1.6 Ensure ICMP Request is securely configured (Manual)

Profile Applicability:

- Level 1

Description:

ICMP (Internet Control Message Protocol) is used by network devices to communicate with each other. While ICMP is essential for network management and troubleshooting, allowing all types of ICMP requests may increase the risk of attacks such as Ping Flood and ICMP Redirect. Therefore, it is recommended to securely configure the allowed types of ICMP requests on the firewall.

Rationale:

Allowing all types of ICMP requests may increase the risk of attacks such as Ping Flood and ICMP Redirect. To mitigate these risks, it is recommended to securely configure the allowed types of ICMP requests on the firewall.

Audit:

In GUI:





```
- Navigate to Firewall > Rules
- Review the firewall rules to determine if any ICMP request rules are present.
- Review the firewall rules to determine if any ICMP request rules are present.
- Check the configured ICMP request types for each rule to ensure that only necessary types are allowed
```

Remediation:

In GUI:

- Navigate to Firewall > Rules
- Review the firewall rules to determine if any ICMP request rules are present.
- Review the firewall rules to determine if any ICMP request rules are present.
- Check the configured ICMP request types for each rule to ensure that only necessary types are allowed

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.6 <u>Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			
v7	9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

5 Service Configuration

5.1 SNMP Policy

5.1.1 Ensure SNMP traps receivers is set (Manual)

Profile Applicability:

- Level 1

Description:

Enables SNMP traps receivers where traps are sent.

Rationale:

The purpose of the SNMP service is to monitor in real-time the events occurring on systems in order to meet the security requirement of the availability of systems and services. The traps are SNMP notifications sent to the NMS or SNMP traps receivers and should be enabled in order to be sent and processed by the NMS. The NMS or SNMP traps receivers will then provide a comprehensive aggregation and reporting of events generated, thus helping the administrator. Additionally, the add on package NET-SNMP (when configured appropriately) can satisfy this as well.

Audit:

In GUI:

- Navigate to Services > SNMP.
- Check "SNMP Traps Enable" is enabled.
- Check on the "SNMP Trap Settings" is configured.

Remediation:

In GUI:







- Navigate to Services > SNMP.
- Check "SNMP Traps Enable" is enable.
- Configured the "SNMP Trap Settings" value.
- CLick Save

Default Value:

In GUI:

- Under 'SNMP Daemon Settings'
- 'Enable' box will not be checked.

CIS Controls:

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

5.1.2 Ensure SNMP traps is enabled (Manual)

Profile Applicability:

- Level 1

Description:

Enables SNMP traps to be sent to the Network Management Station (NMS)

Rationale:

The purpose of the SNMP service is to monitor in real-time the events occurring on systems in order to meet the security requirement of the availability of systems and services. The traps are SNMP notifications sent to the NMS and should be enabled in order to be sent and processed by the NMS. The NMS will then provide a comprehensive aggregation and reporting of events generated, thus helping the administrator.

Audit:

IN GUI:

- Navigate to Services > SNMP.
- Check "SNMP Traps Enable" is enabled.

Remediation:

IN GUI:




- Navigate to Services > SNMP.
- set checkbox "SNMP Traps Enable".
- Click on Save




Default Value:

In GUI:

- Under 'SNMP Daemon Settings'
- 'Enable' box will not be checked.

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.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			

5.1.3 Ensure that the add-on package NET-SNMP is installed and configured securely (Manual)

Profile Applicability:

- Level 2

Description:

The add-on package NET-SNMP provides Simple Network Management Protocol (SNMP) functionality on pfSense. SNMP is used for network management and monitoring, allowing administrators to collect and view information about devices on the network. This rule ensures that the NET-SNMP package is installed and securely configured.

Rationale:

SNMP is a widely used protocol for network management and monitoring, and it is important to ensure that it is securely configured on pfSense. If SNMP is not properly secured, it can allow unauthorized access to network devices and sensitive information. By ensuring that the NET-SNMP package is installed and configured securely, administrators can monitor network devices while also maintaining the security of their network.

Audit:

- Check if the NET-SNMP package is installed on pfSense.
- Verify that SNMPv3 is enabled and configured with strong encryption and authentication settings.
- Verify that SNMP access is restricted to authorized hosts only.
- Verify that default community strings have been removed or changed.

Remediation:

5.2 NTP Service Policy

5.2.1 Ensure time zone is properly configured (Manual)

Profile Applicability:

- Level 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 > NTP
- verify the 'Enable NTP Server' Field

Remediation:

In the GUI:

- Navigate to Services > NTP
- Checked the 'Enable NTP Server' Field
- Click 'Save'

Default Value:

Default value is 'NTP Server Configuration'

- 'Enable' will be checked

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.4 <u>Standardize Time Synchronization</u> Standardize time synchronization. Configure at least two synchronized time sources across enterprise assets, where supported.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>6.1 Utilize Three Synchronized Time Sources</p> <p>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.</p>		●	●

5.3 DNS Service Policy

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

Profile Applicability:

- Level 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 > DNS Resolver > General DNS Resolver Options
- Verify if "DNSSEC" is checked or not.

Remediation:







In the GUI:

- Navigate to Services > DNS Resolver > General DNS Resolver Options
- Check the box next to 'DNSSEC' and set Enable
- CLick 'Save'

Default Value:

The DNS Resolver is enabled by default.

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.			

5.4 VPN Configuration

5.4.1 Ensure RADIUS or LDAP are being used for VPN Authentication (Manual)

Profile Applicability:

- Level 1

Description:

Set backed authentication for VPN User to LDAP server. Configured the LDAP Servers 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 > User Manager.
- CLick the Authentication Servers at the top.
- Check 'Authentication Servers' Setting

Remediation:

In the GUI:

- Navigate to System > User Manager.
- CLick the Authentication Servers at the top.
- Configure 'Authentication Servers' Setting

Default Value:

Default Authentication Servers is: 'Local Database'

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
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.		●	●

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

Profile Applicability:

- Level 1

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:

In GUI:

- Navigate to System > Cert. Manager > CAs
- Check the 'Issuer' Column

Remediation:

In GUI:



- Navigate to System > Cert. Manager > CAs
- Click "Add"
- In "Method" use the 'Import an existing Certificate Authority'
- Fill Textbox and Hit save.

Default Value:

There are no default certificates.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	1.8 Utilize Client Certificates to Authenticate Hardware Assets Use Client certificates to authenticate hardware assets connecting to the organization's trusted network.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.2 <u>Configure Centralized Point of Authentication</u> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.			

5.4.3 Ensure that OpenVPN is configured to use TLS encryption for secure communications. (Manual)

Profile Applicability:

- Level 2

Description:

Configure OpenVPN to use TLS encryption for secure communication with Clients and servers.

Rationale:**Audit:****Remediation:**

In GUI

- Open the pfSense web interface and navigate to VPN > OpenVPN.
- Click on the server configuration you want to configure.
- Under the "Cryptographic Settings" section, set the "TLS Configuration" option to "Enable".
- Choose the appropriate TLS key length, key direction, and digest algorithm.
- Click "Save" to save the changes.

5.5 OpenVPN

5.5.1 Ensure that OpenVPN use strong ciphers or hashing algorithms (Manual)

Profile Applicability:

- Level 1

Description:

This rule aims to prevent the use of weak cryptographic algorithms in OpenVPN, which could be exploited by attackers to compromise the confidentiality, integrity, and availability of the VPN traffic. Specifically, this rule requires that only strong and secure cryptographic ciphers and hashing algorithms are used in OpenVPN.

Rationale:

Weak cryptographic algorithms are more susceptible to attacks such as brute-force attacks, known-plaintext attacks, and man-in-the-middle attacks. By ensuring that only strong cryptographic algorithms are used in OpenVPN, the VPN traffic will be better protected against unauthorized access and modification.

Impact:

Implementing this rule may impact the performance of the OpenVPN service, as strong cryptographic algorithms can be more computationally intensive than weaker ones. However, this impact can be minimized by selecting the appropriate cryptographic algorithms for the underlying hardware and network environment.

Audit:**Remediation:**

6 Logging

6.1 Ensure syslog is configured (Manual)

Profile Applicability:

- Level 1

Description:

Syslog logging is a standard logging protocol that is widely supported. It is recommended for a level 1 deployment only, as syslog does not support encryption

Rationale:

Sending all system logs to a remote host is recommended to provide protected, long term storage and archiving. This also places a copy of the logs in a second location, in case the primary (on the firewall) logs are compromised. Storing logs on a remote host also allows for more flexible log searches and log processing, as well as many methods of triggering events or scripts based on specific log events or combinations of events. Finally, remote logging provides many organizations with the opportunity to combine logs from disparate infrastructure in a SIEM (Security Information and Event Management) system.

Logging to an external system is also usually required by most regulatory frameworks.

Impact:

Failure to properly store and archive logs for critical infrastructure leaves an organization without the tools required to establish trends in events or activity, or to retrospectively analyze security or operational events beyond the log timespan stored on the firewall. Not having remote logs also puts many organizations outside of compliance with many regulatory frameworks.

Audit:

In GUI:

- Navigate to Status > System Logs > Settings.
- Check 'Enable Remote Logging' Options

Remediation:

In GUI:

- Navigate to Status > System Logs > Settings.
- Configure 'Enable Remote Logging' Options












Default Value:

By default no external logging is defined.

Additional Information:

- <https://docs.netgate.com/pfsense/en/latest/monitoring/logs/index.html>
- <https://docs.rapid7.com/insightidr/pfsense-firewall/>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 <u>Collect Detailed Audit Logs</u> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v8	8.12 <u>Collect Service Provider Logs</u> Collect service provider logs, where supported. Example implementations include collecting authentication and authorization events, data creation and disposal events, and user management events.			
v7	6.2 <u>Activate audit logging</u> Ensure that local logging has been enabled on all systems and networking devices.			
v7	6.3 <u>Enable Detailed Logging</u> 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)	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure AutoConfigBackup is enable (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure 'Message Of The Day (MOTD)' is set (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure Hostname is set (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure DNS server is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure IPv6 is disabled if not used (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure 'DNS Rebind Check' is unchecked (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure Web Management is Set to use HTTPS (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure a synchronized High Availability peer is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2	Users Management		
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure LDAP or RADIUS server configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure Console Menu is Password Protected (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure all default accounts are either disabled or utilize strong passwords (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3	Password Policy		
3.1	Ensure 'Local Account status' is set to 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.2	Ensure Login Protection Threshold is set to 30 or less (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure Allow access again after time is set to 300 or more second (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure default password of admin is changed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4	Firewall Policy		
4.1	Firewall Rules Policy		
4.1.1	Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Allow Rule with Any in Source field present in the Firewall Rules (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure no Allow Rule with Any in Services field present in the Firewall Rules (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure there are no Unused Policies (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure Logging is Enable for All Firewall Rules (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ICMP Request is securely configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5	Service Configuration		
5.1	SNMP Policy		
5.1.1	Ensure SNMP traps receivers is set (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure SNMP traps is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure that the add-on package NET-SNMP is installed and configured securely (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.2	NTP Service Policy		
5.2.1	Ensure time zone is properly configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.3	DNS Service Policy		
5.3.1	Ensure 'DNSSEC' is Enable on DNS Service (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	VPN Configuration		
5.4.1	Ensure RADIUS or LDAP are being used for VPN Authentication (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Apply a Trusted Signed Certificate for VPN Portal (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure that OpenVPN is configured to use TLS encryption for secure communications. (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5	OpenVPN		
5.5.1	Ensure that OpenVPN use strong ciphers or hashing algorithms (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
6	Logging		
6.1	Ensure syslog is configured (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure AutoConfigBackup is enable	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure 'Message Of The Day (MOTD)' is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure DNS server is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure 'DNS Rebind Check' is unchecked	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure all default accounts are either disabled or utilize strong passwords	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure 'Local Account status' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure Allow access again after time is set to 300 or more second	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure default password of admin is changed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Allow Rule with Any in Source field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure no Allow Rule with Any in Services field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure Logging is Enable for All Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure SNMP traps receivers is set	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure SNMP traps is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Ensure 'DNSSEC' is Enable on DNS Service	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure syslog is configured	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure AutoConfigBackup is enable	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure 'Message Of The Day (MOTD)' is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure Hostname is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure DNS server is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure IPv6 is disabled if not used	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure 'DNS Rebind Check' is unchecked	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure Web Management is Set to use HTTPS	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure a synchronized High Availability peer is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure LDAP or RADIUS server configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure Console Menu is Password Protected	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure all default accounts are either disabled or utilize strong passwords	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure 'Local Account status' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure Allow access again after time is set to 300 or more second	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure default password of admin is changed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Allow Rule with Any in Source field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure no Allow Rule with Any in Services field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure there are no Unused Policies	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure Logging is Enable for All Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ICMP Request is securely configured	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.1	Ensure SNMP traps receivers is set	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure SNMP traps is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure time zone is properly configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Ensure 'DNSSEC' is Enable on DNS Service	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure RADIUS or LDAP are being used for VPN Authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Apply a Trusted Signed Certificate for VPN Portal	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure syslog is configured	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure AutoConfigBackup is enable	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure 'Message Of The Day (MOTD)' is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure Hostname is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure DNS server is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure IPv6 is disabled if not used	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure 'DNS Rebind Check' is unchecked	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure Web Management is Set to use HTTPS	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure a synchronized High Availability peer is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure LDAP or RADIUS server configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure Console Menu is Password Protected	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure all default accounts are either disabled or utilize strong passwords	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure 'Local Account status' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Login Protection Threshold is set to 30 or less	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure Allow access again after time is set to 300 or more second	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure default password of admin is changed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Allow Rule with Any in Source field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure no Allow Rule with Any in Services field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure there are no Unused Policies	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure Logging is Enable for All Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
4.1.6	Ensure ICMP Request is securely configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure SNMP traps receivers is set	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure SNMP traps is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure time zone is properly configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Ensure 'DNSSEC' is Enable on DNS Service	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure RADIUS or LDAP are being used for VPN Authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Apply a Trusted Signed Certificate for VPN Portal	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure syslog is configured	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
5.1.3	Ensure that the add-on package NET-SNMP is installed and configured securely	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure that OpenVPN is configured to use TLS encryption for secure communications.	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1	Ensure that OpenVPN use strong ciphers or hashing algorithms	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure AutoConfigBackup is enable	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure 'Message Of The Day (MOTD)' is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure Hostname is set	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure 'DNS Rebind Check' is unchecked	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure a synchronized High Availability peer is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure Console Menu is Password Protected	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure all default accounts are either disabled or utilize strong passwords	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure 'Local Account status' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure default password of admin is changed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Allow Rule with Any in Source field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure no Allow Rule with Any in Services field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure Logging is Enable for All Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure SNMP traps receivers is set	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure SNMP traps is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Ensure 'DNSSEC' is Enable on DNS Service	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure syslog is configured	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure AutoConfigBackup is enable	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure 'Message Of The Day (MOTD)' is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure Hostname is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure DNS server is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure IPv6 is disabled if not used	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure 'DNS Rebind Check' is unchecked	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure Web Management is Set to use HTTPS	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure a synchronized High Availability peer is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure LDAP or RADIUS server configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure Console Menu is Password Protected	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure all default accounts are either disabled or utilize strong passwords	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure 'Local Account status' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Login Protection Threshold is set to 30 or less	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure default password of admin is changed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Allow Rule with Any in Source field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure no Allow Rule with Any in Services field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure there are no Unused Policies	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure Logging is Enable for All Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ICMP Request is securely configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure SNMP traps receivers is set	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.2	Ensure SNMP traps is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure time zone is properly configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Ensure 'DNSSEC' is Enable on DNS Service	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure RADIUS or LDAP are being used for VPN Authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Apply a Trusted Signed Certificate for VPN Portal	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure syslog is configured	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1	Ensure SSH warning banner is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.2	Ensure AutoConfigBackup is enable	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure 'Message Of The Day (MOTD)' is set	<input type="checkbox"/>	<input type="checkbox"/>
1.4	Ensure Hostname is set	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure DNS server is configured	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure IPv6 is disabled if not used	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure 'DNS Rebind Check' is unchecked	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure Web Management is Set to use HTTPS	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure a synchronized High Availability peer is configured	<input type="checkbox"/>	<input type="checkbox"/>
2.1	Ensure Sessions Timeout is set to less than or equal to 10 Minutes	<input type="checkbox"/>	<input type="checkbox"/>
2.2	Ensure LDAP or RADIUS server configured	<input type="checkbox"/>	<input type="checkbox"/>
2.3	Ensure Console Menu is Password Protected	<input type="checkbox"/>	<input type="checkbox"/>
2.4	Ensure all default accounts are either disabled or utilize strong passwords	<input type="checkbox"/>	<input type="checkbox"/>
3.1	Ensure 'Local Account status' is set to 'Disabled'	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure Login Protection Threshold is set to 30 or less	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure default password of admin is changed	<input type="checkbox"/>	<input type="checkbox"/>
4.1.1	Ensure no Allow Rule with Any in Destination Field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Allow Rule with Any in Source field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.3	Ensure no Allow Rule with Any in Services field present in the Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure there are no Unused Policies	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure Logging is Enable for All Firewall Rules	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure ICMP Request is securely configured	<input type="checkbox"/>	<input type="checkbox"/>
5.1.1	Ensure SNMP traps receivers is set	<input type="checkbox"/>	<input type="checkbox"/>

Recommendation		Set Correctly	
		Yes	No
5.1.2	Ensure SNMP traps is enabled	<input type="checkbox"/>	<input type="checkbox"/>
5.2.1	Ensure time zone is properly configured	<input type="checkbox"/>	<input type="checkbox"/>
5.3.1	Ensure 'DNSSEC' is Enable on DNS Service	<input type="checkbox"/>	<input type="checkbox"/>
5.4.1	Ensure RADIUS or LDAP are being used for VPN Authentication	<input type="checkbox"/>	<input type="checkbox"/>
5.4.2	Apply a Trusted Signed Certificate for VPN Portal	<input type="checkbox"/>	<input type="checkbox"/>
6.1	Ensure syslog is configured	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.3	Ensure Allow access again after time is set to 300 or more second	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure that the add-on package NET-SNMP is installed and configured securely	<input type="checkbox"/>	<input type="checkbox"/>
5.4.3	Ensure that OpenVPN is configured to use TLS encryption for secure communications.	<input type="checkbox"/>	<input type="checkbox"/>
5.5.1	Ensure that OpenVPN use strong ciphers or hashing algorithms	<input type="checkbox"/>	<input type="checkbox"/>

Appendix: Change History

Date	Version	Changes for this version
Jun 27, 2023	1.1.0	4.1.1 & 4.1.2 are identical (Ticket 17745)
Jun 30, 2023	1.1.0	Include information on using LDAP for password complexity (Ticket 17045)
Jun 30, 2023	1.1.0	3.2 Ensure Maximum number of failed attempts allowed is set to 5 or fewer (Manual) (Ticket 17742)
Jun 30, 2023	1.1.0	4.1.7 Ensure ICMP Request in not enable on Firewall (Manual) (Ticket 17743)
Jun 30, 2023	1.1.0	1.7 - Ensure 'DNS Rebind Check' is set (Ticket 17738)
Jun 30, 2023	1.1.0	2.4 Ensure known default accounts do not exist or disabled (Manual) (Ticket 17740)