Center for Internet Security®

CIS Benchmarks™

CIS Cisco Firepower Threat Defense Benchmark

v1.0.0 - 11-30-2023

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 *5*

Intended Audience **5**

Consensus Guidance **6**

Typographical Conventions **7**

Recommendation Definitions *8*

Title **8**

Assessment Status **8**

Automated **8**

Manual **8**

Profile **8**

Description **8**

Rationale Statement **8**

Impact Statement **9**

Audit Procedure **9**

Remediation Procedure **9**

Default Value **9**

References **9**

CIS Critical Security Controls® (CIS Controls®) **9**

Additional Information **9**

Profile Definitions **10**

Acknowledgements **11**

Recommendations *12*

1 Management Plane **12**

1.1 Identity **13**

1.1.1 Local Credentials **14**

1.1.1.1 Restrict access to the local Admin account (Manual) 15

1.1.1.2 Do not use the default "admin" account (Manual) 17

1.1.2 External Authentication **19**

1.1.2.1 Use an External Authentication Source for Administrative Logins (Manual) 20

1.1.2.2 Enable SSHv2 (Automated) 23

1.1.3 User Roles for Administrative Access (Authorization) **24**

1.1.3.1 Set Appropriate Roles for all Administrative Users (Manual) 25

1.1.3.2 Use Dedicated User Accounts for API Access (Manual) 27

1.1.3.3 Restrict access to the FMC CLI (Manual) 30

1.1.4 User Identification **32**

1.1.4.1 Realm Configuration (User to Group Mapping, Active Logins) ... 33
1.1.4.1.1 Create a Realm (Manual) ... 34
1.1.4.1.2 Create an Identity Policy (Manual) ... 36
1.1.4.1.3 Create an Identity Rule (Manual) ... 38
1.1.4.1.4 Manage a Realm (Manual) ... 41
1.1.4.1.5 Compare Realms (Manual) ... 43
1.1.4.1.6 Manage an Identity Policy (Manual) ... 45
1.1.4.1.7 Manage an Identity Rule (Manual) ... 47
1.2 Backups ... 49
1.2.1 Create Periodic Backups of Firepower Management Center (Automated) ... 50
1.3 Scheduled Updates ... 53
1.3.1 Scheduled Rule Updates (Automated) ... 54
1.3.2 Scheduled Geolocation Updates (Automated) ... 56
1.3.3 Update of URL Filtering Database (Automated) ... 58
1.3.4 Regularly update the FMC Server Version (Manual) ... 60
1.3.5 Regularly update the Firepower Sensors (Automated) ... 62
1.4 Monitoring ... 65
1.4.1 Health Policy ... 66
1.4.1.1 Create a Health Policy for your FMC Server (Automated) ... 67
1.4.1.2 Ensure that the Health Policy is assigned to the managed Firepower Appliances (Automated) ... 73
1.4.1.3 Ensure that the Health Policy is assigned to all FMC Servers (Automated) ... 75
1.4.2 Platform Logging and Time ... 76
1.4.2.1 Configure Central Logging for FMC (Automated) ... 77
1.4.2.2 Configure Central Logging for FMC Managed Devices (Automated) ... 80
1.4.2.3 Monitor for Clock Drift within the Firepower Infrastructure (Automated) ... 82
1.4.2.4 Set FMC Time Synchronization to Multiple Reliable NTP Source(s) (Automated) ... 84
1.4.2.5 Set Firepower Sensor / Devices to Synchronize time to FMC (Automated) ... 86
1.4.2.6 Configure Audit Logging to be Sent to Syslog (Automated) ... 88
1.4.3 SNMP ... 90
1.4.3.1 If SNMP is configured, ensure that SNMP v3 only is used to Manage your FMC Server (Manual) ... 91
1.4.3.2 If SNMP is configured, ensure that SNMP v3 only is used to Manage your Firepower Managed Devices (Manual) ... 93
1.5 Triggered Actions ... 95
1.5.1 Scanning ... 96
1.5.1.1 Run Scheduled Nmap Scans (Manual) ... 97
1.6 Database Settings ... 99
1.6.1 Set Database Retention Policies (Manual) ... 100

2 Data Plane ... 103
2.1 Policies ... 104
2.1.1 Access Policy Default Logging (Manual) ... 105
2.1.2 Create an outbound SSL Policy (Manual) ... 108
2.1.3 Intrusion prevention policy (Automated) ... 111
2.1.4 Enable TLS server identity discovery (Automated) ... 112
2.1.5 Access Policy File Policy (Manual) ... 114
2.1.6 Decrypt traffic (Automated) ... 116
2.1.7 Access Policy - URL Filtering (Manual) ... 118
2.1.8 Enable secure VPN anyconnect tunnelling protocols (Manual) ... 121
2.1.9 Enable secure Site to Site VPN tunnelling protocols (Manual) ... 123
2.1.10 Access Policy Application Settings should be set (Manual) ... 125

3 Control Plane ... 127
3.1 Secure local network infrastructure ... 128
3.1.1 Secure the Network Time Protocol Server (Manual) ... 129
3.1.2 Secure the Domain Name System (DNS) (Manual) ... 131

3.2 Harden Network Protocol Settings **133**
3.2.1 Disable fragment reassembly (Automated) 134
3.2.2 Block older SSL and TLS versions (Automated) 135
3.3 Configure default action to Block (Automated) 137
Appendix: Summary Table ***139***
Appendix: CIS Controls v7 IG 1 Mapped Recommendations ***143***
Appendix: CIS Controls v7 IG 2 Mapped Recommendations ***144***
Appendix: CIS Controls v7 IG 3 Mapped Recommendations ***146***
Appendix: CIS Controls v7 Unmapped Recommendations ***148***
Appendix: CIS Controls v8 IG 1 Mapped Recommendations ***149***
Appendix: CIS Controls v8 IG 2 Mapped Recommendations ***150***
Appendix: CIS Controls v8 IG 3 Mapped Recommendations ***152***
Appendix: CIS Controls v8 Unmapped Recommendations ***154***
Appendix: Change History ***155***

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, Security Configuration Benchmark for Cisco Firepower Threat Defense 6.x or 7.x, provides prescriptive guidance for establishing a secure configuration posture for Cisco Devices running Cisco Firepower Threat Defense (FTD).
This document is targeted towards a recommended Firepower Threat Defense configuration, that is:

- Cisco Firepower Threat Defense (FTD) running versions 6.x or 7.x
- Firepower devices managed by Firepower Management Center (FMC)

To obtain the complete benchmark and or the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Cisco Firepower.

Consensus Guidance

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

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

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

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

Title

Concise description for the recommendation's intended configuration.

Assessment Status

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

Automated

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

Manual

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

Profile

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

Description

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

Rationale Statement

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

Impact Statement

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

Audit Procedure

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

Remediation Procedure

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

Default Value

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

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

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

Additional Information

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

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide a clear security benefit; and
  - not 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 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:

Contributor
Rob Vandenbrink
Darren Freidel
Daniele Bartoli
Paul Beyer
Daniel Brown

Recommendations

1 Management Plane

Services, settings and data streams related to setting up and examining the static configuration of the firewall, and the authentication and authorization of firewall administrators. Examples of management plane services include: administrative device access (telnet, ssh, http, and https), SNMP, and security protocols like RADIUS and TACACS+.

1.1 Identity

1.1.1 Local Credentials

1.1.1.1 Restrict access to the local Admin account (Manual)

Profile Applicability:

- Level 1

Description:

The default Admin user should never be used for anything outside of initial setup.

Rationale:

Default admin is the only account on the device on initial setup. Access to this account should be restricted. Utilizing individual accounts allow for more accurate logging.

Impact:

Using the default admin account for day to day tasks opens it to potential compromise. In the event of compromise it would be difficult to track where the compromise came from using logging. Default admin has root access and all accounts should be as needed.

Audit:

Review the FMC Syslog logs, looking for events similar to:

```
2021-12-25 13:31:11     User.Info       s-hof-fpmgt.mscu.com    Dec 25
18:31:11 mojo_server.pl: s-hof-fpmgt: admin@127.0.0.1, Login, Login
Success<000>x0a<000>x00
```

Remediation:

Set up alerts on the FMC Syslog logs, looking for events similar to:

```
2021-12-25 13:31:11     User.Info       s-hof-fpmgt.mscu.com    Dec 25
18:31:11 mojo_server.pl: s-hof-fpmgt: admin@127.0.0.1, Login, Login
Success<000>x0a<000>x00
```

Default Value:

The admin user is the only default account on the system.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.1.1.2 Do not use the default "admin" account (Manual)

Profile Applicability:

- Level 1

Description:

The use of named accounts is recommended for all access to the Firepower interface. The default "admin" account should only be used in exceptional circumstances.

Rationale:

The built in "admin" account has full rights to all facets of the Firepower platform. If a change is made by this account, linking this change back to an actual person or automated process can be difficult or impossible. For this reason, it is recommended that all accounts that access the Firepower be named accounts that are easily linked back to the people assigned for their use. Accounts used for automation should be similarly named for easy identification.

Impact:

Changing the default "admin" account on a Cisco Firepower firewall is a crucial security measure to protect your network infrastructure. To change the default "admin" account, you'll need to create a new user and disable or delete the default "admin" account.

Audit:

1. Access the Firepower Management Center (FMC): You can access the FMC using a web browser by entering its IP address in the address bar. Make sure you have administrative privileges to perform this task.
2. Log in to the FMC: Use the default "admin" account to log in.

If this succeeds you have verified that the "admin" account is active.

Remediation:

1. Create a New User:

```
- Go to "System" in the FMC navigation menu.
- Under "System Configuration," click on "Users."
- Click the "Add" button to create a new user account.
- Enter the new user's details, including a unique username and password.
- Assign the appropriate role and permissions to the new user, such as
Administrator or another custom role with the necessary privileges.
```

2. Disable or Delete the Default "admin" Account:

```
- While still in the "Users" section, locate the "admin" account.
- You can either disable or delete the "admin" account. Disabling is a safer
option in case you need to revert changes later, but deletion is more secure.
To disable the account, simply uncheck the "Enable" option next to the
"admin" account. To delete the account, select the "admin" account and click
the "Delete" button.
```

3. Log Out and Log Back In: Log out of the FMC, and then log back in using the new user account you created.
4. Test the New User Account: Verify that the new user account has the necessary privileges and access to perform administrative tasks on the Cisco Firepower firewall.
5. Update Documentation: Ensure that you document the changes you've made, including the new user account details and any changes to the "admin" account.

Default Value:

The admin user is the only default account on the system.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v8	17.5 Assign Key Roles and Responsibilities Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			

1.1.2 External Authentication

1.1.2.1 Use an External Authentication Source for Administrative Logins (Manual)

Profile Applicability:

- Level 1

Description:

By default, the Firepower administrative account is set during installation (commonly to "admin", but any value appropriate to the organization is fine), and is locally defined. It is recommended that a back-end directory be used to authenticate all other administrative access of all levels.

Rationale:

If the single "admin" account is used, only a single administrator can access the FMC console at one time, subsequent logins will disconnect the currently active session. More importantly, using generic accounts means that any changes cannot be tied to any specific administrator. This means that tracking change control requests is not practical in the default configuration, nor is tieing configuration errors to specific users.

Just as important, if an administrator leaves the organization it can be difficult to "find" all of the things that they administered in a timely manner, and disable their access. Using a back-end directory means that disabling a single account will disable all of their access. Similarly, controlling access by group means that moving a user account into or out of that group controls their access.

Impact:

Without external authentication defined, it is common to see these systems controlled by a single user - "admin". The defaults also have none of the common account management policies defined (enforcing periodic password changes, password complexity, preventing password re-use etc).

The result of this is that no changes can be connected to any specific person. Also, if an administrator should change roles or departments, they still have this default set of credentials.

If this approach is used for all network infrastructure, changing these credentials as people come and go is also difficult, it's very common to forget one or more devices during a password change. In the worst case, at some point in the future accessing that missed device might be impossible, as no-one in the team will remember what "the password" was 8 cycles ago.

Finally, if an attacker should compromise this password on one platform, all platforms are now accessible.

Audit:

In the FMC Console:

```
Navigate to System / Users
Verify that all administrative user accounts have "External" as their
Authentication Method
Note that the default administrative user that was defined during the
installation (often this found to be "admin") will remain in this list as an
Internal user.  It is recommended to keep this user in place, in the event
that the external authentication service is not available.
```

Remediation:

First create an External Authentication Object:

```
- Navigate to System / Users / External Authentication.
- Create an External Authentication Object (RADIUS or LDAP)
- Whichever method is defined, be sure to configure both a Primary and a
Backup server for redundant authentication
- On the External Authentication service, it's recommended to control access
by directory Groups rather than by user account (this is easily done in both
RADIUS and in LDAP)
- For both RADIUS or LDAP, the various administrative users should be
populated in their respective RBAC roles.  In a smaller environment, it is
common to see all administrators be populated in the "Administrator"
category, which gives them full administrative (read/write) rights.  If this
is not done, a "Default User Role" should be selected.
- If it is desired to restrict Shell Access to specific users only, in
earlier versions of FMC add them in the Shell Access Filter section.  In
later versions (6.4 or later), you can control this access using RADIUS
Attributes (Service Type: Administrative)
```

Default Value:

By default, a single administrative account (admin) is locally defined.

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/user_accounts_fmc.html#id_63531

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.1.2.2 Enable SSHv2 (Automated)

Profile Applicability:

- Level 1

Description:

SSHv2 is the preferred choice for secure remote access. Once configured it allows for an encrypted connection to the remote device.

Rationale:

SSHv1 is deprecated and is no longer recommended.

Audit:

```
Devices > Platform Settings > Secure Shell
```

Remediation:

```
Devices > Platform Settings > Secure Shell
1. Click Add
2. Enter in IP addresses or Range
3. Select Zone/Interface
```

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	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.1.3 User Roles for Administrative Access (Authorization)

1.1.3.1 Set Appropriate Roles for all Administrative Users (Manual)

Profile Applicability:

- Level 1

Description:

The Firepower Management platform has the ability to assign roles (RBAC) to each administrative user.

Rationale:

In smaller environments it is common to see all administrative users with full read/write access, but as organizations grow, it is recommended that people who only need reporting or other read-only access be assigned to more restrictive roles. In all environments, the roles of each user should be assessed to ensure only appropriate access is granted.

Impact:

If available, RBAC (Role Based Access Controls) are an important part of any configuration. A properly configured RBAC configuration ensures that full environment administrators have appropriate (full) access, but also properly limits people like managers, who may only need reports. In between these two extremes you will most often find Helpdesk and SOC analysts who require access to the Analysis functions of Firepower to resolve issues or investigate possible security incidents. To one side of this spectrum you generally find auditors, who need read-only access to the entire configuration to ensure that things like the Access Policy are appropriately configured, or that appropriate security controls are applied (for instance as described in this document).

Audit:

Navigate to System / Users
Verify that all user accounts have appropriate Roles assigned (in the Roles column), matching their job requirements.

Remediation:

Navigate to System / Users
Edit the target user.
Select any of the following Roles either singly or in combination, as required:

- Administrator (Externally Set)
- External Database User (Read Only)
- Security Analyst
- Security Analyst (Read Only)

- Security Approver
- Intrusion Admin
- Access Admin
- Network Admin
- Maintenance User
- Discovery Admin
- Threat Intelligence Director (TID) User

Default Value:

By default no User Role is assigned, at least one must be assigned at the time of user creation. If external authentication is configured (for instance RADIUS), often the role of "Administrator" is assigned by the external system (for instance with RADIUS Attribute-Value pairs).

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			
v7	16 Account Monitoring and Control Account Monitoring and Control			

1.1.3.2 Use Dedicated User Accounts for API Access (Manual)

Profile Applicability:

- Level 2

Description:

Keeping standard admin users (who use the UI or occassionally the CLI) separate from accounts that are used for scripting and automation is a key security principal.

Rationale:

Keeping interactive and automated access separate is key in most situations that involve automation, in particular if automation is used to enforce policy.

An account that logs in interactively and makes a deliberate change is most likely a change that is purposefully done (whether by the person who owns the account or be a compromised account), and should be treated as such.

Scripting accounts are often used for audit purposes, often because getting management approval for automated firewall changes can be a problem in many organizations. These accounts should be configured with read-only privileges.

At this time, automated read-write access in many organizations is often within a larger automation platform (such as Teraform or Ansible, both of which support Firepower). This approach is excellent, as firewall changes are not treated as standalone updates, but are usually part of larger deploys - for instance they can be tied to service deployments and configurations. In these situations the use of a native password "vault" or "safe" is recommended. Tools of this type are often run periodically, re-executing their playbooks that define the environment. In the event that an execution like this finds a change to make, it means one of two things:

- This is a new change that is scheduled and approved
- This "run" of the playbooks should be considered a finding - it has found either a conflict within the playbooks, or has found a manual change that has just been reversed.

In the second situation particularly, the difference between an interactive account and an automation account can be critical - knowing if you have a scripting error or an admin who is operating outside of the automation framework is a key consideration in remediation of this finding.

If an interactive account was used to run the automation playbook, working out if this is an automation error or an admin who is operating outside of the approved processes and procedures can be much more difficult.

Audit:

Review the assigned users, and collect the privilege level for each.
Manual Method:
Automated method:
https://www.cisco.com/c/en/us/td/docs/security/firepower/ftd-api/guide/ftd-rest-api/external-users-ftd-api.html
Review the login date/time for each account, and verify that these are appropriate. Inactive accounts should be deactivated, and accounts operating outside of approved times or source IP ranges should be investigated.

Remediation:

Default Value:

There is no default value for account rights, these are explicitly assigned during creation. That being said, it's common to see all accounts with full administrative rights - in other words, more rights than are required especially for audit-only accounts.

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/660/api/REST/firepower_management_center_rest_api_quick_start_guide_660/About_The_Firepower_Management_Center_REST_API.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v8	17.5 Assign Key Roles and Responsibilities Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

1.1.3.3 Restrict access to the FMC CLI (Manual)

Profile Applicability:

- Level 1

Description:

By default, there is one admin user with full administrator rights to the FTD CLI command line. This admin user can create multiple accounts and grant them either basic, which is read-only, or config, which is read-write, access levels.

Rationale:

Appropriate access levels should be administered depending on the user's role. Access to the CLI should be restricted to lower the overall attack surface.

Impact:

Decreasing the number of users with config access instead of granting all users config access, significantly reduces the chances of a compromised system.

Audit:

Users with config level access can use the CLI command `expert` to access the Linux shell. This is available to the admin account, local users, and external users with config level access.

Remediation:

To block access to the Linux shell, administrators can use the `system lockdown-sensor` command. Once this command is used, any non-administrator user who logs in will only have access to the FTD CLI command.

Default Value:

By default, there is one admin user with full administrator rights to the FTD CLI command line.

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/user_accounts_for_management_access.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v8	17.5 Assign Key Roles and Responsibilities Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			

1.1.4 User Identification

1.1.4.1 Realm Configuration (User to Group Mapping, Active Logins)

1.1.4.1.1 Create a Realm (Manual)

Profile Applicability:

- Level 1

Description:

A realm consists of one or more LDAP or Microsoft Active Directory servers that share the same directory credentials. You must configure a realm to perform user and user group queries, user control, or to configure an authoritative identity source.

Rationale:

Realms are connections between the Firepower Management Center and the user accounts on the servers you monitor. They specify the connection settings and authentication filter settings for the server.

Impact:

Realms can:

- Specify the users and user groups whose activity you want to monitor.
- Query the user repository for user metadata on authoritative users, as well as some non-authoritative users: POP3 and IMAP users detected by traffic-based detection and users detected by traffic-based detection, a user agent, or ISE.

Audit:

```
1. Log in to the Firepower Management Center.
2. Click System > Integration.
3. Click Realms.
```

Verify that documented Realms exist.

Remediation:

```
1. To create a new realm, click Add Realm.
2. To perform other tasks (such as enable, disable, or delete a realm), see
Manage a Realm.
3. Enter the following realm information:
```

- Name: A unique name for the realm. The system supports alphanumeric and special characters.
- Description: (Optional.) Enter a description of the realm.
- Type: The type of realm, AD for Microsoft Active Directory or LDAP for other supported LDAP repositories.
- AD Primary Domain: For Microsoft Active Directory realms only. Domain for the Active Directory server where users should be authenticated.

- Directory Username and Directory Password: For Microsoft Active Directory realms only. Domain for the Active Directory server where users should be authenticated.
- Base DN (Distinguished Name): The directory tree on the server where the Firepower Management Center should begin searching for user data.
- Group DN: The directory tree on the server where the Firepower Management Center should search for users with the group attribute
- Group Attribute (Optional): The group attribute for the server, Member or Unique Member.

```
4. Click OK.
5. Configure at least one directory as discussed in [Configure a Realm
Directory](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/confi
guration/guide/fpmc-config-guide-
v601/Identity_Policies_and_Realms.html#task_EBC16C6927ED4A33BBEE039547353F99)
.
6. Configure user and user group download (required for access control) as
discussed in [Download Users and
Groups](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configur
ation/guide/fpmc-config-guide-
v601/Identity_Policies_and_Realms.html#task_828D5C71131C4501AB4FE34423CD6349)
.
7. Click Realm Configuration.
8. Enter user session timeout values, in minutes, for Authenticated Users,
Failed Authentication Users, and Guest Users.
9. When you're finished configuring the realm, click Save.
```

Default Value:

There are no default Realms.

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Identity_Policies_and_Realms.html#task_EBC16C6927ED4A33BBEE039547353F99

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	16.1 Maintain an Inventory of Authentication Systems Maintain an inventory of each of the organization's authentication systems, including those located onsite or at a remote service provider.		●	●

1.1.4.1.2 Create an Identity Policy (Manual)

Profile Applicability:

- Level 1

Description:

An identity policy associates traffic on your network with an authoritative identity source and a realm.

Rationale:

After configuring one or more identity policies, you can associate one with an access control policy and deploy the access control policy to a managed device. Identity policies contain identity rules. Identity rules associate sets of traffic with a realm and an authentication method: passive authentication, active authentication, or no authentication.

Impact:

If you do not configure an identity policy, the system does not perform user authentication.

Audit:

```
1. Log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity
```

Verify that all documented Identity Policies are in place.

Remediation:

```
1. Log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity and click New Policy.
3. Enter a Name and, optionally, a Description.
4. Click Save.
5. To add a rule to the policy, click Add Rule as described in [Create an
Identity
Rule](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configurat
ion/guide/fpmc-config-guide-
v601/Identity_Policies_and_Realms.html#task_A2FCBE057F6A42D598D24C5280D0C238)
6. To create a rule category, click Add Category.
7. To configure captive portal active authentication, click Active
Authentication as described in [Configure the Captive Portal Part 1: Create
an Identity
Policy.](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configu
ration/guide/fpmc-config-guide-v601/User_Identity_Sources.html#id_61520)
8. Click Save to save the identity policy.
```

Default Value:

By default there is no Identity Policy.

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Identity_Policies_and_Realms.html#task_33C92E69A3F8487BAC3CBCB849102892

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.		●	●

1.1.4.1.3 Create an Identity Rule (Manual)

Profile Applicability:

- Level 1

Description:

These are the Rules that will be applied within your Identity Policy.

Rationale:

Identity Rules are the actions that are performed on users in the specified realms.

Impact:

Provides the ability to enforce a form of authentication for users as well as specify which realm contains the users you want to perform the Action on.

Audit:

```
1. Log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity
```

Verify that all documented Identity Policies are in place and that they have applicable rules.

Remediation:

```
1. If you haven't done so already, log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity .
3. Click Edit (edit icon) next to the identity policy to which to add the
identity rule.
4. If View (view button) appears instead, the configuration belongs to an
ancestor domain, or you do not have permission to modify the configuration.
5. Click Add Rule.
6. Enter a Name.
7. Specify whether the rule is Enabled.
8. To add the rule to an existing category, indicate where you want to Insert
the rule. To add a new category, click Add Category.
9. Choose a rule Action from the list.
10. Click Realms & Settings.
11. Choose a realm for the identity rule from the Realms list. You must
associate a realm with every identity rule.
12. The only exception to the realm requirement is implementing user control
using only the ISE SGT attribute tag. In this case, you do not need to
configure a realm for the ISE server. ISE SGT attribute conditions can be
configured in policies with or without an associated identity policy.
13. If you're configuring captive portal, see [How to Configure the Captive
Portal for User
Control.](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/config
uration/guide/fpmc-config-guide-
v601/User_Identity_Sources.html#task_B09D4711593E4506890BB8BE25B39B31)
14. (Optional) To add conditions to the identity rule, see [Rule Condition
Types](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configura
tion/guide/fpmc-config-guide-v601/fpmc-config-guide-
v601_chapter_01010111.html#id_16297).
15. Click Add.
16. In the policy editor, set the rule position. Click and drag or use the
right-click menu to cut and paste. Rules are numbered starting at 1. The
system matches traffic to rules in top-down order by ascending rule number.
The first rule that traffic matches is the rule that handles that traffic.
Proper rule order reduces the resources required to process network traffic
and prevents rule preemption.
17. Click Save.
```

Default Value:

There are no default rules set.

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Identity_Policies_and_Realms.html

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	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

1.1.4.1.4 Manage a Realm (Manual)

Profile Applicability:

- Level 1

Description:

This section describes how to perform various maintenance tasks for a realm using controls on the Realms page.

Rationale:

As a network administrator it is critical that you are able to administrate your realms, rules and identities.

Impact:

If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Audit:

```
1. Log in to the Firepower Management Center.
2. Click System > Integration.
3. Click Realms.
```

View all of your available Realms.

Remediation:

```
1. Log in to the Firepower Management Center.
2. Click System > Integration.
3. Click Realms.
4. To delete a realm, click Delete (delete icon).
5. To edit a realm, click Edit (edit icon) next to the realm and make changes
as described in [Create a
Realm](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configura
tion/guide/fpmc-config-guide-
v601/Identity_Policies_and_Realms.html#task_F9ED2AF84F604438ACDC2124237DC518)
.
6. To enable a realm, slide State to the right; to disable a realm, slide it
to the left.
7. To download users and user groups, click Download (download icon).
8. To copy a realm, click Copy (copy icon).
```

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Identity_Policies_and_Realms.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	11.7 Manage Network Infrastructure Through a Dedicated Network Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

1.1.4.1.5 Compare Realms (Manual)

Profile Applicability:

- Level 1

Description:

Utilize this technique to find differences between your Realms. You must be an Admin, Access Admin, Network Admin, or Security Approver to perform this task.

Rationale:

Important task for an Administrator.

Impact:

Allows you to identify differences between Realms.

Audit:

```
1. Log in to the Firepower Management Center.
2. Click System > Integration.
3. Click Realms.
4. Click System > Integration.
5. Click Realms.
6. Click Compare Realms.
```

Remediation:

```
1. Log in to the Firepower Management Center.
2. Click System > Integration.
3. Click Realms.
4. Click System > Integration.
5. Click Realms.
6. Click Compare Realms.
7. Choose Compare Realm from the Compare Against list.
8. Choose the realms you want to compare from the Realm A and Realm B lists.
9. Click OK.
10. To navigate individually through changes, click Previous or Next above
the title bar.
11. (Optional.) Click Comparison Report to generate the realm comparison
report.
12. (Optional.) Click New Comparison to generate a new realm comparison view.
```

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Identity_Policies_and_Realms.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	11.7 Manage Network Infrastructure Through a Dedicated Network Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.		●	●

1.1.4.1.6 Manage an Identity Policy (Manual)

Profile Applicability:

- Level 1

Description:

In a multidomain deployment, the system displays policies created in the current domain, which you can edit. It also displays policies created in ancestor domains, which you cannot edit. To view and edit policies created in a lower domain, switch to that domain.

Rationale:

Impact:

Important task for an organizations network administrators.

Audit:

```
1. If you haven't done so already, log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity
```

Remediation:

```
1. If you haven't done so already, log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity .
3. To delete a policy, click Delete (delete icon). If the controls are
dimmed, the configuration belongs to an ancestor domain, or you do not have
permission to modify the configuration.
4. To edit a policy, click Edit (edit icon) next to the policy and make
changes as described in [Create an Identity
Policy](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configur
ation/guide/fpmc-config-guide-
v601/Identity_Policies_and_Realms.html#task_33C92E69A3F8487BAC3CBCB849102892)
. If View (view button) appears instead, the configuration belongs to an
ancestor domain, or you do not have permission to modify the configuration.
5. To copy a policy, click Copy (copy icon).
6. To generate a report for the policy, click Report (Report icon) as
described in [Generating Current Policy
Reports](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configu
ration/guide/fpmc-config-guide-
v601/Policy_Management.html#task_CCED983433824793AF09203FDAD1AF53).
7. To compare policies, see [Comparing
Policies](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/config
uration/guide/fpmc-config-guide-
v601/Policy_Management.html#task_ABA1FE48DBBB44BC9FF40243FCC58BF6).
```

Default Value:

N/A

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Identity_Policies_and_Realms.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	5.2 Maintain Secure Images Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.		●	●

1.1.4.1.7 Manage an Identity Rule (Manual)

Profile Applicability:

- Level 1

Description:

Describes the technique and ability to manage Identity Rule's.

Rationale:

Important task for an administrator of an organization.

Audit:

```
1. If you haven't already done so, log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity
```

View your Identity Rule's.

Remediation:

```
1. If you haven't already done so, log in to the Firepower Management Center.
2. Click Policies > Access Control > Identity .
3. Click Edit (edit icon) next to the policy you want to edit. If View (view
button) appears instead, the configuration belongs to an ancestor domain, or
you do not have permission to modify the configuration.
4. To edit an identity rule, click Edit (edit icon) and make changes as
described in [Create an Identity
Policy](https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configur
ation/guide/fpmc-config-guide-
v601/Identity_Policies_and_Realms.html#task_33C92E69A3F8487BAC3CBCB849102892)
.
5. To delete an identity rule, click Delete (delete icon).
6. To create a rule category, click Add Category and choose the position and
the rule.
7. Click Save.
```

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Identity_Policies_and_Realms.html

CIS Controls:

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

1.2 Backups

As in all infrastucture, it is wise to plan for the worst, whether that is a regular instance where a database is corrupted, a patch that doesn't apply correctly, or an actual security event that compromises one or more Firepower components. The first line of defense in many if not all of these situations is good, recent backups that can be used to recover affected components.

1.2.1 Create Periodic Backups of Firepower Management Center (Automated)

Profile Applicability:

- Level 1

Description:

At a minimum, backing up the FMC server configuration is recommended. Backing up managed devices is usually not critical, the quickest recovery of a compromised Firepower device is to re-install it from scratch, then to use FMC to configure it by deploying the appropriate policies to it.

Rationale:

While backups be default configured to run weekly, a minimum cadence of daily backups is recommended in most environments to minimize the impact of deploying an older backup. Backups are recommended to be stored remotely so that in the event of a security incident, the attacker would need to compromise both the FMC server and the remote backup destination. If that remote backup destination is then part of a standard IT backup solution, that then makes a complete compromise of Firepower backups even more difficult.

Impact:

Backups are a critical part of system recovery, from either operational events that may affect operation of the Firepower System, or security incidents that may affect operation or may cast doubt on the integrity of the Firepower configuration or stored data.

Audit:

Navigate to:

```
- System (Gear Icon) > Backups
- Verify that backups are occurring and completing periodically, in the lower
part of this screen.
- At a minimum, backups should have a "Yes" in the "Configurations" column
- Select "Backup Profiles"
- For each Backup Profile, open the profile and verify that the backups are
configured to copy to a remote host.
```

Next, navigate to:

```
- System (Gear Icon) > Scheduling
- Verify that the backups are scheduled to run at a reasonable schedule
(daily in most environments)
- Select the last few backup jobs, and verify that the Last Run Status is
"Successful"
```

Remediation:

Navigate to

```
System (Gear Icon) > Backup / Restore > Backup Profiles
- Choose "Create Profile"
- Assign a descriptive name
- At a minimum, choose "Back Up Configuration"
- If space permits, it is advised that "Back Up Events" is also selected,
with "Back Up Threat Intelligence Director" as a second "if space permits"
recommendation.
- If only these fields are completed, the backups are only stored locally on
the FMC server.  This is not recommended, as any event that affects the FMC
server may make these backups unavailable, or in the case of a security event
the integrity of the information in the backups may be suspect.
- Because of this, choose "Copy when complete"
- Fill in the values for your site, which define an SCP / SFTP service in
your environment that will host your off-device backups
- You have the option of completing authentication for your backups as userid
/ password.  In a more secure implementation, you also have the option to use
SSH keys for authentication.
- When complete, select "Save as New"

Next, navigate to: System (Gear Icon) > Scheduling

- Select "Add Task"
- For Job Type, select "Backup"
- Choose "Recurring"
- Choose a start time in the future, preferably in an off-peak time window
- Give the job a descriptive name
- Choose "Management Center" as the Backup Type (in most environments no
critical data is hosted on the managed devices)
- Choose the Backup Profile that you have created.
- There is a comment field that can be used at your discretion.
- An "Email Status to" field is available if email is a convenient way to
track backup job status in your environment.
```

Default Value:

By default, backups are configured as "Configuration Only".

This default backup is scheduled to run to run weekly (each Sunday at 21:00), and is stored locally on the FMC server.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.2 Perform Automated Backups Perform automated backups of in-scope enterprise assets. Run backups weekly, or more frequently, based on the sensitivity of the data.	●	●	●
v7	10.1 Ensure Regular Automated Back Ups Ensure that all system data is automatically backed up on regular basis.	●	●	●

1.3 Scheduled Updates

1.3.1 Scheduled Rule Updates (Automated)

Profile Applicability:

- Level 1

Description:

The Snort Vulnerability database should be automatically downloaded and deployed at a reasonable cadence, preferably daily.

Rationale:

If the IPS Rule database is not updated frequently, then newer attacks may not be detected, and improved detections of existing attacks will not be used.

Impact:

There are a few different impacts to consider for this recommendation: On the positive side, it is definitely recommended to use the latest rule database to maximize the detection of malicious events and to minimize false positives. On the negative side, deploying the updated database to existing rulesets may cause unintended consequences - it is possible (though not probable) that deploying a new database to an existing ruleset without testing can result in affecting production traffic in unexpected ways. This negative consequence is generally deemed to be of low probability. For this reason it is recommended to both download the newest rule database at a frequent interval, but then also to deploy updated policies after the rule updates are completed. The only time this is not recommended is if there is an established manual procedure of testing before deploying after rule updates. In most environments this is too labor intensive to mitigate a risk that is considered to be both of low probability and low impact, so automated deploys are recommended.

Audit:

```
- Navigate to System (Gear Icon) > Updates
- Choose "Rule Updates"
- Under "Recurring Rule Update Imports", verify that "Enable Recurring Rule
Update Imports from the Support Site" is enabled
- Verify that the update frequency is set to "Daily", with a scheduled time
that complies with the policies of the organization.
- Ensure that "Policy Deploy" is selected, unless there is an equivalent
manual test / deploy procedure in place.
- At the top of the screen, verify that the "Running Snort Rule update
version" is the expected recent value.
- This version can also be found by Navigating to Overview > Dashboard >
Status
```

Remediation:

```
- Navigate to System (Gear Icon) > Updates
- Choose "Rule Updates"
- Under "Recurring Rule Update Imports", choose "Enable Recurring Rule Update
Imports from the Support Site"
- Choose an update frequency and schedule.  Daily updates are recommended,
the update time is should be schedule for an off-peak time window to minimize
the potential affect on traffic that IPS rule updates can have.  (note that
this impact is usually considered to be of low risk)
- Choose "Policy Deploy", unless there is an equivalent manual test / deploy
procedure in place.
```

Default Value:

By default, Rule Updates are not configured.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●

1.3.2 Scheduled Geolocation Updates (Automated)

Profile Applicability:

- Level 1

Description:

The Geo Location database should be automatically downloaded and deployed at a reasonable cadence, preferably daily.

Rationale:

Impact:

While the geo-location of IP addresses may not seem like a rapidly changing artifact, it actually can be, especially for IPv4. In today's world where the IPv4 address space is exhausted, it is common to see addresses change location, sometimes even change continents as subnets change hands. In addition, the larger Cloud Service Providers will often move subnets between geographically disparate datacenters to balance demand for address space with the subnets they own. Finally, many companies have Disaster Recovery strategies that have production (public) address spaces move to a DR location in some disaster scenarios

All of these common examples mean that any geo-location database will see multiple changes daily. As this database is used for both detection of events, enriching events with geo-location data and in many cases in firewall rules, keeping this database as up-to-date as possible is important for all organizations.

Audit:

```
- Navigate to System (Gear Icon) > Updates > Gelolocation Updates
- Under "recurring Geolocation Updates", ensure that "Enable Recurring Weekly
Updates from the Support Site" is selected
- Ensure that the scheduled day and time matches any policies your
organization may have in place.
- verify that the "Geolocation Update Version" (at the top of the screen)
matches the expected recent value.
- This version can also be found by Navigating to Overview > Dashboard >
Status
```

Remediation:

```
- Navigate to System (Gear Icon) > Updates
- Choose "Geolocation Updates"
- Under "Recurring Rule Update Imports", enable "Enable Recurring Weekly
Updates from the Support Site"
- Set the scheduled day and time to match any policies your organization may
have in place.
```

Default Value:

By default the Geolocation database is not updated automatically.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●

1.3.3 Update of URL Filtering Database (Automated)

Profile Applicability:

- Level 1

Description:

The URL Filtering database should be automatically downloaded and deployed at a reasonable cadence, at a minimum daily.

Rationale:

The categorization of websites of course lags behind the deployment of new sites. In addition, malicious sites often see changes in site names happen at an accelerated rate (fast flux DNS), to avoid being categorized as malicious. Another source of change is the end-users and administrators of deployed Firepower systems, who have the option of sending database corrections to Cisco directly.

Finally, periodically content categories are updated. For instance, in January 2021 15 new categories were added, many of which have proven useful in filtering or controlling access to various malicious or undesirable sites,

All of these reasons mean that keeping the URL database up to date is extremely important, the more out of date this database is, the less meaningful rules and detections based on it are.

Audit:

```
Navigate to System (Gear Icon) > Scheduling
```

Verify that there is a job scheduled at least daily to update the URL Database.
In the lower half of the screen, verify that the URL Database update job is running successfully, and that the cadence matches the desired frequency of updates.

Remediation:

```
Navigate to System (Gear Icon) > Scheduling
Choose "Add Task"
For "Job Type", select "Update URL Filtering Database"
Choose Recurring, with a cadence of one daily or less.  It may be desirable
to update this database more frequently.
Set the scheduled time to match your organizations policies.
Give the job a descriptive name.
Choose "Save"
```

Default Value:

By default the URL Filtering Database is not automatically updated.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●

1.3.4 Regularly update the FMC Server Version (Manual)

Profile Applicability:

- Level 1

Description:

The Firepower Infrastructure OS Components are updated frequently by Cisco. It is recommended that the version of the FMC Server be checked monthly at a minimum, and updated if recommended.

Rationale:

Impact:

Not updating the FMC server not only makes it less effective in preventing undesired traffic, it also means that bugs that may lead to a system compromise are not addressed.

It is routine in today's world that as patches are released, malicious actors will reverse-engineer those patches to try to deduce the bugs and other issues that are addressed, then create exploits based on those findings. In addition, if the bugs were found by researchers outside of the vendor team, it is common that at some point after updates or fixes are released that they will post their research, often with proof-of-concept code, which can be then used by malicious actors to write more robust exploits.

Audit:

```
Navigate to Overview > Dashboard > Status
Verify that the software version is at the desired level
```

Remediation:

Before updating, it is recommended that the release notes for the target version are reviewed to assess any potential new issues that may be introduced, or any new functions or behavior changes that need to be accounted for. The release notes will also often have update time estimates, which can help in appropriately scheduling maintenance windows.
It is also recommended that a formal testing procedure be written for Firepower, and that this procedure is executed after each update to ensure full functionality post update.
To update FMC:

```
- Navigate to System (Gear Icon) > Updates > Product Updates
- If needed, upload the required FMC Update to the update list
- Choose "Deploy" on the required update
- Select the FMC Server that is the target of the update
- Choose "Launch Readiness Check".  Note that this can take an extended
period of time.
- If this completes successfully, Choose "Install".  Note that this can take
an extended period of time, and will frequently take the FMC Server out of
service and/or reboot the server.  It is recommended that this only be done
in a scheduled maintenance window.
- Execute your testing procedure to ensure that there are no functional
changes that will affect the people or clients that use systems that are
protected by your FMC installation.
```

Default Value:

The update process is manual.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●

1.3.5 Regularly update the Firepower Sensors (Automated)

Profile Applicability:

- Level 1

Description:

The Firepower Infrastructure OS Components are updated frequently by Cisco. It is recommended that the version of the Firepower Sensors be checked monthly at a minimum, and updated if recommended. In most cases it is recommended that the Firepower Sensors be kept at the same version as the FMC Server. Because of the duration of the update process however, it is common to see the sensors "lag" slightly behind the FMC Server due to constraints in scheduling maintenance windows.

Rationale:

Impact:

Not updating the Firepower Sensors not only makes them less effective in preventing undesired traffic, it also means that bugs that may lead to a system compromise are not addressed.

It is routine in today's world that as patches are released, malicious actors will reverse-engineer those patches to try to deduce the bugs and other issues that are addressed, then create exploits based on those findings. In addition, if the bugs were found by researchers outside of the vendor team, it is common that at some point after updates or fixes are released that they will post their research, often with proof-of-concept code, which can be then used by malicious actors to write more robust exploits.

Audit:

```
- Navigate to Devices > Device Management
- Verify that the version of each sensor is at the desired level, and that
all sensors are at a consistent version
- Unless a different version is in use on one or more sensors for a
documented reason (for instance, a new version is being tested or the update
process is in progress but not complete), it is recommended that all sensors
run the same version, and that this version matches the FMC Server version
```

Remediation:

Before updating, it is recommended that the release notes for the target version are reviewed to assess any potential new issues that may be introduced, or any new functions or behavior changes that need to be accounted for. The release notes will also often have update time estimates, which can help in appropriately scheduling maintenance windows.
It is also recommended that a formal testing procedure be written for Firepower, and that this procedure is executed after each update to ensure full functionality post update.
To update a Firepower sensor:

```
- Navigate to System (Gear Icon) > Updates > Product Updates
- If needed, upload the required Sensor Update to the update list
- Choose "Deploy" on the required update
- Select the Sensor (or Sensors if multiple devices are being updated at
once) that is/are the target of the update
- Choose "Launch Readiness Check". Note that this can take an extended period
of time.
- If this completes successfully, Choose "Install". Note that this can take
an extended period of time, and will frequently take the Firepower Sensor(s)
out of service and/or reboot the sensor.
- Updating Firepower Sensors will almost always interrupt service, which
means that it is recommended that this only be done in a scheduled
maintenance window.
- If redundant sensors are deployed, usually only one sensor in a pair will
be updated at once to eliminate the service outage aspect of the update.
- Execute your testing procedure to ensure that there are no functional
changes that will affect the people or clients that use systems that are
protected by your Firepower installation.
```

Default Value:

The update process is manual.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v8	7.4 Perform Automated Application Patch Management Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	11.4 Install the Latest Stable Version of Any Security-related Updates on All Network Devices Install the latest stable version of any security-related updates on all network devices.	●	●	●

1.4 Monitoring

1.4.1 Health Policy

1.4.1.1 Create a Health Policy for your FMC Server (Automated)

Profile Applicability:

- Level 1

Description:

The Health Policy defines various settings indicating the overall health and resource utilization of the FMC Server and the Firepower Appliances.

Rationale:

The defaults are sufficient for many environments, but should be reviewed. In many environments it might be desired to lower some thresholds.

The ISE monitor is disabled by default, given that the User Agent method of correlating user accounts to IP addresses is retired in version 7, this setting should definitely be adjusted if the ISE or ISE/PIC service is in use.

Audit:

```
- Navigate to System (Gear logo) > Health > Policy
- Open the Health Policy in use
- Verify the settings below:
- ensure that the policy is set for all Firepower appliances and FMC servers
```

Default Settings:

- Policy Run Time Interval: 5 minutes (adjust downwards as needed, keeping available resources in mind)
- AMP For Endpoints Status: On
- AMP for Firepower Status: On
- Appliance Heartbeat: On
- Automatic Application Bypass Status: On
- Backlog Status: On
- CPU Usage: On (Warning = 80%, Critical = 90%, adjust downwards as needed)
- Appliance Configuration Resource Utilization
- Cluster/Failover Status: On
- Configuration Database: On (Warning = 15GB, Critical = 50GB, adjust downwards as needed)
- Disk Status: On
- Disk Usage: On (Warning = 85%, Critical = 90%, 2HD Warning = 97%, 2HD Critical = 99%, adjust downward as needed)
- FMC HA Status: On
- Hardware Alarms: On
- Health Monitor Process: On (Warning - 30 minutes since last event, Criticalk = 60 minutes, adjust downward as required)
- Host Limit: On (Warning = 50 hosts, Critical = 10, adjust upwards as needed)
- Inline Link Mismatch Alarms: On

- Interface Status: On
- Intrusion and File Event Rate: On (Warning Threshold = 30 events per second, Critical = 50, adjust downward as required)
- Link State Propagation: On
- Local Malware Analysis: On
- Memory Usage: On (Warning Threshold = 80%, Critical = 90%, adjust downward as required)
- Platform Faults: On (Severity is set to Critical, do not suggest changing this)
- Power Supply: On
- Process Status: On
- RRD Server Process: On (Warning = 2 restarts, Critical = 3, do not recommend adjusting)
- Realm: On (Warning mismatch at 50%, adjust downwards as required)
- Reconfiguring Detection: On
- Security Intelligence: On
- Smart License Monitor: On
- Snort Identity Memory Usage: On (Critical Threshold = 80%, adjust downward as required)
- Threat Data Updates on Devices: On (Warning = 1 hr, Critical = 24 hrs, adjust downward as required)
- Time Series Data Monitor: On
- Time Synchronization Status: On
- URL Filtering Monitor: On (Warning = hr, Critical = 24 hrs, adjust downward as required)
- User Agent Status (deprecated): On (if still in use, move to ISE/PIC)
- VPN Status: On

Non-Default Settings:

- ISE Connection Status Monitor: On (Only if ISE or ISE/PIC is deployed)
- Card Reset: On (Only for FMC instances running on physical hardware)

Notes:
"Host Limit" defines how many hosts can be monitored at one time by Firepower. The values in the Health Policy are how many host entries remain in the table before generating an alert. The total for the various FMC models are:

```
FMC Model  Hosts

MC750      2,000
MC1000    50,000
MC1500    50,000
FS2000   150,000
MC2500   150,000
MC3500   300,000
MC4000   600,000
MC4500   600,000
vFMC      50,000
```

"Configuration Database" limit is the size of the Config database at which the event is generated
In the Disk Usage Section, 2HD = Second SSD, used for On Platform Malware storage

Remediation:

```
- Navigate to System (Gear logo) > Health > Policy
- Create a New Policy or Edit the existing one
- Set the following Values:
```

Default Settings:

- Policy Run Time Interval: 5 minutes (adjust downwards as needed, keeping available resources in mind)
- AMP For Endpoints Status: On
- AMP for Firepower Status: On
- Appliance Heartbeat: On
- Automatic Application Bypass Status: On
- Backlog Status: On
- CPU Usage: On (Warning = 80%, Critical = 90%, adjust downwards as needed)
- Appliance Configuration Resource Utilization
- Cluster/Failover Status: On
- Configuration Database: On (Warning = 15GB, Critical = 50GB, adjust downwards as needed)
- Disk Status: On
- Disk Usage: On (Warning = 85%, Critical = 90%, 2HD Warning = 97%, 2HD Critical = 99%, adjust downward as needed)
- FMC HA Status: On
- Hardware Alarms: On
- Health Monitor Process: On (Warning - 30 minutes since last event, Criticalk = 60 minutes, adjust downward as required)
- Host Limit: On (Warning = 50 hosts, Critical = 10, adjust upwards as needed)
- Inline Link Mismatch Alarms: On
- Interface Status: On
- Intrusion and File Event Rate: On (Warning Threshold = 30 events per second, Critical = 50, adjust downward as required)
- Link State Propagation: On
- Local Malware Analysis: On

- Memory Usage: On (Warning Threshold = 80%, Critical = 90%, adjust downward as required)
- Platform Faults: On (Severity is set to Critical, do not suggest changing this)
- Power Supply: On
- Process Status: On
- RRD Server Process: On (Warning = 2 restarts, Critical = 3, do not recommend adjusting)
- Realm: On (Warning mismatch at 50%, adjust downwards as required)
- Reconfiguring Detection: On
- Security Intelligence: On
- Smart License Monitor: On
- Snort Identity Memory Usage: On (Critical Threshold = 80%, adjust downward as required)
- Threat Data Updates on Devices: On (Warning = 1 hr, Critical = 24 hrs, adjust downward as required)
- Time Series Data Monitor: On
- Time Synchronization Status: On
- URL Filtering Monitor: On (Warning = hr, Critical = 24 hrs, adjust downward as required)
- User Agent Status (deprecated): On (if still in use, move to ISE/PIC)
- VPN Status: On

Non-Default Settings:

- ISE Connection Status Monitor: On (Only if ISE or ISE/PIC is deployed)
- Card Reset: On (Only for FMC instances running on physical hardware)

Notes:
"Host Limit" defines how many hosts can be monitored at one time by Firepower. The values in the Health Policy are how many host entries remain in the table before generating an alert. The total for the various FMC models are:

```
FMC Model  Hosts

MC750       2,000
MC1000     50,000
MC1500     50,000
FS2000    150,000
MC2500    150,000
MC3500    300,000
MC4000    600,000
MC4500    600,000
vFMC       50,000
```

"Configuration Database" limit is the size of the Config database at which the event is generated
In the Disk Usage Section, 2HD = Second SSD, used for On Platform Malware storage

Default Value:

Default Set to ON:

- Policy Run Time Interval: 5 minutes (adjust downwards as needed, keeping available resources in mind)
- AMP For Endpoints Status: On
- AMP for Firepower Status: On
- Appliance Heartbeat: On
- Automatic Application Bypass Status: On
- Backlog Status: On
- CPU Usage: On (Warning = 80%, Critical = 90%, adjust downwards as needed)
- Appliance Configuration Resource Utilization
- Cluster/Failover Status: On
- Configuration Database: On (Warning = 15GB, Critical = 50GB, adjust downwards as needed)
- Disk Status: On
- Disk Usage: On (Warning = 85%, Critical = 90%, 2HD Warning = 97%, 2HD Critical = 99%, adjust downward as needed)
- FMC HA Status: On
- Hardware Alarms: On
- Health Monitor Process: On (Warning - 30 minutes since last event, Criticalk = 60 minutes, adjust downward as required)
- Host Limit: On (Warning = 50 hosts, Critical = 10, adjust upwards as needed)
- Inline Link Mismatch Alarms: On
- Interface Status: On
- Intrusion and File Event Rate: On (Warning Threshold = 30 events per second, Critical = 50, adjust downward as required)
- Link State Propagation: On
- Local Malware Analysis: On
- Memory Usage: On (Warning Threshold = 80%, Critical = 90%, adjust downward as required)
- Platform Faults: On (Severity is set to Critical, do not suggest changing this)
- Power Supply: On
- Process Status: On
- RRD Server Process: On (Warning = 2 restarts, Critical = 3, do not recommend adjusting)
- Realm: On (Warning mismatch at 50%, adjust downwards as required)
- Reconfiguring Detection: On
- Security Intelligence: On
- Smart License Monitor: On
- Snort Identity Memory Usage: On (Critical Threshold = 80%, adjust downward as required)
- Threat Data Updates on Devices: On (Warning = 1 hr, Critical = 24 hrs, adjust downward as required)
- Time Series Data Monitor: On
- Time Synchronization Status: On

- URL Filtering Monitor: On (Warning = hr, Critical = 24 hrs, adjust downward as required)
- User Agent Status (deprecated): On (if still in use, move to ISE/PIC)
- VPN Status: On

Default Set to OFF:

- ISE Connection Status Monitor: Off
- Card Reset: Off

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/health_monitoring.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

1.4.1.2 Ensure that the Health Policy is assigned to the managed Firepower Appliances (Automated)

Profile Applicability:

- Level 1

Description:

This checks to ensure that an appropriate Health Policy is assigned to all managed Firepower devices

Rationale:

Audit:

```
- Navigate to Devices > Device Management
- Select each device in turn
- Verify that under Device > Health, that the appropriate Health Policy is
applied (see Recommendation 1.4.1.1)
```

Alternatively:

```
- Navigate to System (Gear icon) > Health > Policy
- Click the "checkmark" icon next to the Policy being applied
- Verify that the Devices and FMC servers that you wish to apply this policy
to all have this policy applied (second column)
```

Remediation:

```
- Navigate to System (Gear icon) > Health > Policy
- Click the "checkmark" icon next to the Policy being applied
- Select the Devices and FMC servers that you wish to apply this policy to
- Press "Apply"
```

Default Value:

By default the Health Policy named "Initial_Health_Policy" is applied to all devices

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

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

1.4.1.3 Ensure that the Health Policy is assigned to all FMC Servers (Automated)

Profile Applicability:

- Level 1

Description:

This checks to ensure that an appropriate Health Policy is assigned to all managed Firepower devices

Rationale:

Audit:

```
- Navigate to System (Gear icon) > Health > Policy
- Click the "checkmark" icon next to the Policy being applied
- Verify that the Devices and FMC servers that you wish to apply this policy
to all have this policy applied (second column)
```

Remediation:

```
- Navigate to System (Gear icon) > Health > Policy
- Click the "checkmark" icon next to the Policy being applied
- Select the Devices and FMC servers that you wish to apply this policy to
- Press "Apply"
```

Default Value:

By default the Health Policy named "Initial_Health_Policy" is applied to all FMC Servers

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

1.4.2 Platform Logging and Time

1.4.2.1 Configure Central Logging for FMC (Automated)

Profile Applicability:

- Level 1

Description:

Syslog allows for central logging in almost every environment in a format that almost all logging infrastructure can consume. In higher security environments, SNMPv3 Traps should be used (see Recommendations in Section 1.4.3)

Rationale:

Central logging is critical in almost every environment. Central logging facilitates:

- detecting security events
- Incident response to security events
- detection of operational events and problems
- detection of trends in the environment, especially if a SIEM is one of the logging destinations

Syslog is the lower security protocol for central logging. Syslog is unencrypted, so if in use that fact should influence the network architecture, as the path from a syslog sender to the syslog server should be protected from unauthorized access.

SNMPv3 Traps allow for encryption of log messages, so is recommended in higher security environments (see Recommendations in Section 1.4.3)

Impact:

Without central logging, the only logs available in Firepower are those in the FMC "Analysis" section. Log retention of these logs is limited, usually to a short period depending on log volumes (under System > Configuration > Database), so log retention for longer periods depends on central logging.

Logs in the "Analysis" section do not contain FMC specific events, such as high CPU or Memory utilization or other critical operational events.

In addition, combining Firepower logs with logs of other devices is only practical in a central logging situation.

Finally, if a SIEM or log keyword alerting is used to identify security incidents in the organization, then Firepower logs must be sent to that logging destination, or any indicators detected by Firepower will not be relayed to the SIEM.

Audit:

First, verify a Syslog Alert Configuration:

```
- Navigate to Policies > Actions > Alerts > Alerts
- Verify that a Syslog destination is set correctly for your organization.

Next, navigate to Policies > Actions > Alerts > Impact Flag Alerts


- Verify that your created Syslog server is set as a target
- Verify email and SNMP alert destinations as appropriate to your
organization
- Verify that "Syslog" is set for all Alerts
- Verify that email and SNMP notifications for each as appropriate for your
organization

Next, navigate to Policies > Actions > Alerts > Discover Event Alerts


- Verify that your created Syslog server is set as a target
- Verify email and SNMP alert destinations as appropriate to your
organization
- Verify that "Syslog" is set for all Alerts
- Verify that email and SNMP notifications for each as appropriate for your
organization

Next, navigate to Policies > Actions > Alerts > Advanced Malware Protection
Alerts


- Verify that your created Syslog server is set as a target
- Verify email and SNMP alert destinations as appropriate to your
organization
- Verify that "Syslog" is set for all Alerts
- Verify that email and SNMP notifications for each as appropriate for your
organization
```

Remediation:

First, create a Syslog Alert Configuration:

```
- Navigate to Policies > Actions > Alerts > Alerts
- Create an Alert Configuration
- Set a Host Name, IP, Port (default 514) and Severity
- Choose "Save"
Next, navigate to Policies > Actions > Alerts > Impact Flag Alerts
```

- At a minimum, set your created Syslog server as a target
- Set email and SNMP alert destinations as appropriate to your organization
- Set destinations for all Impact Flags. Syslog should be set for all, set email and SNMP notifications for each as appropriate for your organization

```
Next, navigate to Policies > Actions > Alerts > Discover Event Alerts
```

- At a minimum, set your created Syslog server as a target
- Set email and SNMP alert destinations as appropriate to your organization

- Set destinations for all Events. Syslog should be set for all, set email and SNMP notifications for each as appropriate for your organization

```
Next, navigate to Policies > Actions > Alerts > Advanced Malware Protection
Alerts
```

- At a minimum, set your created Syslog server as a target
- Set email and SNMP alert destinations as appropriate to your organization
- Set destinations for all Events. Syslog should be set for all, set email and SNMP notifications for each as appropriate for your organization

Default Value:

By default no external alert destinations are configured. If a Syslog Alert destination is configured, all FMC alerts have this destination set

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

1.4.2.2 Configure Central Logging for FMC Managed Devices (Automated)

Profile Applicability:

- Level 1

Description:

Syslog allows for central logging in almost every environment. In higher security environments, SNMPv3 Traps should be used (see Recommendation x.x.x)

Rationale:

Central logging is critical in almost every environment. Central logging facilitates:

- detecting security events
- Incident response to security events
- detection of operational events and problems
- detection of trends in the environment, especially if a SIEM is one of the logging destinations

Syslog is the lower security protocol for central logging. Syslog is unencrypted, so if in use that fact should influence the network architecture, as the path from a syslog sender to the syslog server should be protected from unauthorized access.

SNMPv3 Traps allow for encryption of log messages, so is recommended in higher security environments (see Recommendation x.x.x)

Impact:

Without central logging, the only logs available in Firepower are those in the FMC "Analysis" section. Log retention of these logs is limited, usually to a short period depending on log volumes (under System > Configuration > Database), so log retention for longer periods depends on central logging.

In addition, combining Firepower logs with logs of other devices is only practical in a central logging situation.

Finally, if a SIEM or log keyword alerting is used to identify security incidents in the organization, then Firepower logs must be sent to that logging destination, or any indicators detected by Firepower will not be relayed to the SIEM.

Audit:

```
- Navigate to Devices / Platform settings
- For each Platform Settings Policy:
- Under Syslog, ensure that the following configuration changes are set:
- "Enable Logging" is enabled
- If applicable, set "Enable Logging on failover standby unit"
- Under "VPN Logging Settings", enable "Enable Logging to FMC" is set, with a
logging level of "Informational"
- Under "Logging Destinations" ensure that the logging destination is set to
"Syslog Servers" (lower security environments only)
- Understand that this setting sends the logs in clear text, so ensure that
the path between the logging devices and the syslog server is secured.
- Under "Syslog Servers" ensure that the server(s) IP addresses, Protocol and
Port match the syslog server.
- Under "Reachable By", ensure that the appropriate interface that should
send syslog logs is configured.
```

Remediation:

```
- Navigate to devices / platform settings
- Edit or create a Platform Settings Policy
- Under Syslog, make the following configuration changes:
- Set "Enable Logging"
- If applicable, set "Enable Logging on failover standby unit"
- Under "VPN Logging Settings", enable "Enable Logging to FMC", and set a
logging level of "Informational"
- Under "Logging Destinations" set the logging destination to "Syslog
Servers" in lower security environments.
- Understand that this setting sends the logs in clear text, so ensure that
you secure the path between the logging devices and the syslog server
- Under "Syslog Servers" set the server(s) IP addresses, Protocol and Port to
match your syslog server.
- Under "Reachable By", set the appropriate interface that should send syslog
logs.
```

Default Value:

By default, syslog is not configured

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.1 Centralize Security Event Alerting Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

1.4.2.3 Monitor for Clock Drift within the Firepower Infrastructure (Automated)

Profile Applicability:

- Level 1

Description:

This setting generates an alert if any of the various times in the Firepower infrastructure do not agree with each other.

Rationale:

Setting a reliable time source is critical for all security operations. A reliable time sync ensures that logs from disparate sources reflect the correct sequence of events, whether investigating from the point of view of a single device (and single log) or when consolidating logs for a more complete picture and event timeline. This setting looks for and logs clock differences between the various Firepower components in the infrastructure.

Impact:

Having one or more security devices with different times can make investigating events or using the resulting logs for operational purposes more difficult or even impossible.

Audit:

```
- Navigate to System (Gear Icon) > Health > Policy
- Create a Policy or Edit the existing Policy
- Choose "Time Synchronization Status"
- Ensure that this setting is set to "Enabled"
- Under "Deploy > Deployment History, ensure that all managed devices have
had a recent deploy that includes this setting
```

Remediation:

```
- Navigate to System (Gear Icon) > Health > Policy
- Create a Policy or Edit the existing Policy
- Choose "Time Synchronization Status"
- Choose "Enabled"
- Save the Policy change, this applies the change to the FMC server
- Deploy the policy to Deploy this change to all managed devices.
```

Default Value:

The default value for this setting is "Off"

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.		●	●

1.4.2.4 Set FMC Time Synchronization to Multiple Reliable NTP Source(s) (Automated)

Profile Applicability:

- Level 1

Description:

Configure the FMC Server to acquire it's time from a reliable source, consistent with your organization's policies.

Rationale:

Setting a reliable time source is critical for all security operations. A reliable time sync ensures that logs from disparate sources reflect the correct sequence of events, whether investigating from the point of view of a single device (and single log) or when consolidating logs for a more complete picture and event timeline.

Impact:

Having one or more security devices with different times can make investigating events or using the resulting logs for operational purposes more difficult or even impossible.

Audit:

```
- Navigate to: System (Gear Icon) > Configuration > Time
- Ensure that reliable time sources are configured, matching the policy of
your organization
- Ensure that all "Offset" values in this list are less than 5 milliseconds
```

Remediation:

```
- Navigate to: System (Gear Icon) > Configuration > Time Synchronization
- Set "Serve Time via NTP" to "Enabled"
- Configure "Set My Clock" to "Via NTP"
- Ensure that multiple independent NTP sources are in the NTP Server List in
this window
- Depending on your organization, your policy may be to use internal NTP
Servers, external NTP Servers or some mix of the two.
```

Default Value:

By default the FMC Server synchronizes its clock via NTP, using the servers 0.sourcefire.pool.ntp.org and 1.sourcefire.pool.ntp.org

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.		●	●

1.4.2.5 Set Firepower Sensor / Devices to Synchronize time to FMC (Automated)

Profile Applicability:

- Level 1

Description:

Set all managed Firepower devices to acquire their time synchronization from the FMC Server.

Rationale:

Setting a reliable, consistent time source is critical for all security operations. A reliable time sync ensures that logs from disparate sources reflect the correct sequence of events, whether investigating from the point of view of a single device (and single log) or when consolidating logs for a more complete picture and event timeline. This setting ensures that all managed Firepower devices have their time set from the same FMC Server, so all Firepower logs should have consistent time.

Impact:

Having one or more security devices with different times can make investigating events or using the resulting logs for operational purposes more difficult or even impossible.

Audit:

```
- Navigate to Devices > Device Management
- Edit each device in turn
- Under the "System" section, verify that the correct time and correct
timezone for your organization's policies are shown.
```

Also:

```
- In this same page, under "Device" > Applied Policies, ensure that a
Platform Settings Policy is applied.
- Select that Platform Settings Policy
- Under Time Synchronization ensure that "Set My Clock" is set to "Via NTP
from Management Center"
```

Remediation:

```
Navigate to Devices > Platform Settings

Edit or create a Platform Settings Policy
Under Time Synchronization, Change "Set My Clock" to "Via NTP from Management
Center"
Save this change
Select "Policy Assignments" (top right of the page)
Ensure that the appropriate devices are in the "Selected Devices" column for
this Policy.
Repeat for all managed devices if multiple policies are required to cover all
devices.
Again, save your change
Deploy to apply the change to all devices
```

Default Value:

By default there is no Platform Settings Policy. However, when a Platform Settings Policy is created, it's default setting is that "Set My Clock" is set to "Via NTP from Management Center"

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.		●	●

1.4.2.6 Configure Audit Logging to be Sent to Syslog (Automated)

Profile Applicability:

- Level 1

Description:

Audit Logging logs the details of all configuration changes.

Rationale:

Logging configuration changes facilitates troubleshooting of any resulting issues that might happen post change. From a security perspective, if a configuration change should result in a security exposure or event, the audit log will help define the time window of the exposure or event, as well as the party responsible for the change (if RBAC is configured, see Recommendation 1.1.3.1)

In addition, sending the Audit Log to a central Syslog server allows Firepower changes to be reconciled to the Change Control Procedure, especially if a SIEM and appropriate event ticketing is configured.

Impact:

Without audit logging enabled, the configuration cannot be "back-tracked" to define when any configuration issues might have been made. This may make defining the start and end of a security exposure either much less reliable (if only manual tracking is available) or impossible (if the change was made outside of the change control procedure)

Audit:

```
- Navigate to System (Gear Icon) > Configuration > Audit Log
- Ensure that "Send Audit Log to Syslog" is enabled
- Ensure that the Host field is set to the correct Syslog Host
- Ensure that "Severity" is set to "INFO" (the default value)
```

Remediation:

```
- Navigate to System (Gear Icon) > Configuration > Audit Log
- Set "Send Audit Log to Syslog" to enabled
- Set the "Host" field to the correct Syslog Host
- Set the "Severity" value to "INFO" (the default value)
```

Default Value:

The Audit log is not sent to Syslog by default.

If logging is enabled, the default Severity is set to "INFO"

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

1.4.3 SNMP

1.4.3.1 If SNMP is configured, ensure that SNMP v3 only is used to Manage your FMC Server (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that if SNMP is configured, that only SNMPv3 is enabled for FMC

Rationale:

SNMP is commonly used to manage an alert on common device metrics such as CPU Utilization, Link Utilization and Temperature. Older versions of SNMP (1,2,2c) were all unencrypted, and often used default "string" values to authenticate, allowing disclosure of sensitive information or in some cases permitting configuration changes. Ensuring that only SNMPv3 is configured allows this desired management function, but encrypts the associated data.

Impact:

If older versions of SNMP are configured, any captured SNMP traffic is in clear text, disclosing sensitive device information. In addition, older versions of SNMP often used default authentication "strings", which if configured allowed full access to the device SNMP information.

Finally, if an older SNMP version is compromised, it gives a malicious actor an excellent "traffic multiplier" situation, where small requests resulted in much larger responses. This in combination with the UDP protocol used by these protocols allowed for this multiplied traffic to be spoofed, such that the spoofed (target) IP address could be subject to enough traffic to result in a denial of service condition. Using appropriate passwords and encryption in SNMPv3 makes this type of attack much more difficult, as the credentials must be compromised before the traffic multiplier issue is in play.

Audit:

```
- Navigate to System (Gear Icon) / SNMP
- Ensure that the SNMP Version is set to "Version 3"
- Ensure that SNMPv3 Users exist such that:
- if applicable, the "Encryption Password Type" is set to "Encrypted"
- if applicable, the "Auth Algorithm Type" is set to SHA or SHA256
- if applicable, the "Encryption Type" is set to AES256
```

Remediation:

```
- Navigate to System (Gear Icon) / SNMP
- Set the SNMP Version to "Version 3"
- Choose "Add User"
- Configure SNMPv3 Users such that:
- If applicable, set the "Encryption Password Type" is set to "Encrypted"
- If applicable, set the "Auth Algorithm Type" to SHA or SHA256
- If applicable, set the "Encryption Type" to AES256
- Save your changes
```

Default Value:

By default SNMP is not configured.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
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.		●	●
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

1.4.3.2 If SNMP is configured, ensure that SNMP v3 only is used to Manage your Firepower Managed Devices (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that if SNMP is configured, that only SNMPv3 is enabled.

Rationale:

SNMP is commonly used to manage an alert on common device metrics such as CPU Utilization, Link Utilization and Temperature. Older versions of SNMP (1,2,2c) were all unencrypted, and often used default "string" values to authenticate, allowing disclosure of sensitive information or in some cases permitting configuration changes. Ensuring that only SNMPv3 is configured allows this desired management function, but encrypts the associated data.

Impact:

If older versions of SNMP are configured, any captured SNMP traffic is in clear text, disclosing sensitive device information. In addition, older versions of SNMP often used default authentication "strings", which if configured allowed full access to the device SNMP information.

Finally, if an older SNMP version is compromised, it gives a malicious actor an excellent "traffic multiplier" situation, where small requests resulted in much larger responses. This in combination with the UDP protocol used by these protocols allowed for this multiplied traffic to be spoofed, such that the spoofed (target) IP address could be subject to enough traffic to result in a denial of service condition. Using appropriate passwords and encryption in SNMPv3 makes this type of attack much more difficult, as the credentials must be compromised before the traffic multiplier issue is in play.

Audit:

```
- Navigate to devices / platform settings
- Ensure that there is a Platform Settings Policy
- Edit each Policy in Turn
- Under "SNMP", ensure that "Enable SNMP Servers" is enabled
- Ensure that the "Read Community String" field is empty
- Under "Users" verify that at least one SNMPv3 user is created
- If applicable, set the "Encryption Password Type" is set to "Encrypted"
- If applicable, set the "Auth Algorithm Type" to SHA or SHA256
- If applicable, set the "Encryption Type" to AES256
- Under the "Hosts" tab:
- Verify that the IP address of your SNMP Server is configured to restrict
access
- Verify that the SNMP Version is set to 3
- Ensure that appropriate Usernames (as assessed above) are set
- Ensure that Polling Hosts are set to "Poll"
- Ensure that logging hosts are set to "Trap"
- Ensure that appropriate interfaces are set to send or receive requests
- Under "Policy Assignments" (upper right of this display), ensure that the
"Selected Devices" column contains all applicable devices for this policy.
- Ensure that all managed devices are governed by a Platform Settings Policy
as described above.
```

Remediation:

```
- Navigate to devices / platform settings
- Edit or create a Platform Settings Policy
- Under "SNMP", ensure that "Enable SNMP Servers" is enabled
- Ensure that the "Read Community String" field is empty
- Under "Users" configure the Username
- If applicable, set the "Encryption Password Type" is set to "Encrypted"
- If applicable, set the "Auth Algorithm Type" to SHA or SHA256
- If applicable, set the "Encryption Type" to AES256
- Under the "Hosts" tab:
- Set the IP address of your SNMP Server
- Set the SNMP Version to 3
- Set the Username that was configured above
- Set polling hosts with a permission of "Poll"
- Set logging hosts with a permission of "Trap"
- Set the interface that will be allowed to send or receive SNMPv3 requests
- Under "Policy Assignments" (upper right of this display), ensure that the
"Selected Devices" column contains all applicable devices for this policy.
- Ensure that all managed devices are governed by a Platform Settings Policy
as described above.
```

- Save your changes

Default Value:

By default SNMP is not configured.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
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.		●	●
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

1.5 Triggered Actions

1.5.1 Scanning

1.5.1.1 Run Scheduled Nmap Scans (Manual)

Profile Applicability:

- Level 2

Description:

Internal subnets should be scanned periodically to discover new hosts and services, also to identify when services or hosts are retired.

Rationale:

Running Nmap scans can help detect unauthorized devices or services that may have been added to your network without prior knowledge.

Audit:

To verify the configuration of the scans:

```
- Navigate to Policies > Network Discovery > Actions > Scanners
- Verify that an Nmap Scanner is defined
- Navigate to Policies > Network Discovery > Actions > Scanners > Targets
- Verify that a "Scan Target" exists
- Edit the target, ensure that all reachable internal subnets are fully
represented.
- In the "Ports" field, ensure that the port range is 1-65535.
- Navigate to System > Tools > Scheduling
- Verify that a periodic "Nmap Scan" task exists
- Edit the task, verify that this task is scheduled for regular production
hours
- Verify that the task is scheduled to run periodically, once per day if
possible.
- In the Target field, ensure that this has the value of the "all subnets"
target above
- In the "Remediation" field, ensure that the value is the Nmap Scanner
instance defined above
```

To verify successful completion of scans:

```
- Navigate to Policies > Network Discovery > Actions > Scanners > Scan
Results to verify that scans are completing successfully and consistently
```

Remediation:

```
- Navigate to Policies > Network Discovery > Actions > Scanners
- Choose "Add Nmap Instance"
- Give your scanner a meaningful name
- The scan defaults are generally reasonable, but can be adjusted in any way
that optimizes the scan duration and impact for your environment.  The
important thing is that the scan occurs.
- Press Save
- Navigate to Policies > Network Discovery > Actions > Scanners > Targets
- Choose "Create Scan Target"
- Give the target a meaningful name
- In the IP Range, add all target subnets.  Be sure to limit this scope such
that the scan will complete in a reasonable time.
- In the "Ports" field, the default port range is 1-1024.  This is a good
default for an initial scan, but should be expanded to include all ports once
you have a better gauge of  the scan times and impacts.
- After the first test scans are complete, this field should be changed to 1-
65535.  However this is not a good range for the initial scan(s).
- Under System > Tools > Scheduling
- Select "Add Task"
- Choose "Nmap Scan"
- Give the Nmap Scan a meaningful name
- Choose "Recurring"
- Repeat every "1" days
- Run during production hours, the goal being to discover all servers and
workstations, not just the ones on the network during off hours
- For the Target, choose the one that is defined above
- For the "Remediation", choose the Nmap Scanner instance that is defined
above
- Press "Save"
```

Default Value:

By default Nmap scans are not defined

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

1.6 Database Settings

1.6.1 Set Database Retention Policies (Manual)

Profile Applicability:

- Level 1

Description:

The various databases within Firepower are set to maximum values of events rather than time periods, with an overall maximum count. These values vary by model (see the "defaults" section in this recommendation)

Rationale:

These database retention values often need adjustment, to prevent one database (often the Connection Database from filling up prematurely, while other databases (such as the Intrusion or Malware Databases) remain empty or nearly so.

Impact:

This adjustment of database limits is quite often specific to each organization. Care should be taken that while the Intrusion or Malware databases are often reduced in size, that they won't reach an "overflow" condition in the event of an actual Intrusion or Malware event.

Audit:

```
System > Configuration > Database
```

Verify that the settings are appropriate to your environment and event volumes

Remediation:

```
System > Configuration > Database
```

These values are often set to values that don't reflect day-to-day working environments for many organizations.
In many environments, these settings can be adjusted down as these event volumes are usually lower:

- Health Event Database
- Audit Event Database
- White List Violation History Database
- Remediation Status Event Database

If no VPN is configured (such as in a FirePower Services installation) then that database is not needed at all. Similarly, if a feature is not licensed (for instance the Malware license, which uses the Malware and File databases), those databases can be reduced or zero'd out (note that the minimum value for the Malware Events Database is 10,000, even in the absence of a license)
In a storage constrained setting (such as when using the Virtual FMC), these settings can often also be considered for reduction:

- Intrusion Event Database
- Malware Event Database

After reductions are completed, the Connection Database and Connection Summary Database will often be increased.
The goal is usually to have each event Database hold roughly the same time-period of events. In most environments, it is desired to have a longer retention of "catastrophic" events such as those stored in the Intrusion or Malware databases than "operational" events such as those in the Connection database. However, the Connection database is the one most often referenced to troubleshoot rule issues or monitor behaviours, so in most environments at least 1-4 weeks is desired in that database.
This makes for an interesting "tightrope" of configurations that can take an extended period of time to optimize for many organizations.

Default Value:

The default values for database retention will vary by model. For instance, the defaults for the FMCv (the most widely deployed model) are:

```
Intrusion Events                                    1,000,000
Discovery Event Database                            1,000,000
Connection Database (Connection Events)             1,000,000
Connection Database (Security Intelligence Events)  1,000,000
Connection Summary Database                         2,000,000
Correltion & White List Database                    1,000,000
Malware Database                                    1,000,000
File Event Database                                 1,000,000
Health Event Database                                 100,000
Audit Event Database                                  100,000
Remediation Status Database                         1,000,000
White List Violation History                               30
User Activity                                       1,000,000
Rule Import Log                                     1,000,000
VPN Troubleshooting                                   100,000
```

The maximum event count will also vary by model:

```
FMCv        10 million
FMCv300     60 million
FMC1600     30 million
FMC2600     60 million
FMC 4600   300 million
```

Note that the default maximum settings for each individual database exceed the maximum total.

References:

1. https://www.cisco.com/c/en/us/products/collateral/security/firesight-management-center/datasheet-c78-736775.html
2. https://<FMCAddress>/help_files/index.html#!r_database_event_limits.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.4 Enforce Data Retention Retain data according to the enterprise's data management process. Data retention must include both minimum and maximum timelines.	●	●	●
v8	8 Audit Log Management Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.			
v8	8.10 Retain Audit Logs Retain audit logs across enterprise assets for a minimum of 90 days.		●	●
v7	18.11 Use Standard Hardening Configuration Templates for Databases For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.		●	●

2 Data Plane

Services and settings related to the data passing through the router (as opposed to direct to it). The data plane is for everything not in control or management planes. Settings on a router concerned with the data plane include interface access lists, firewall functionality (e.g. CBAC), NAT, and IPSec. Settings for traffic-affecting services like unicast RPF verification and CAR/QoS also fall into this area.

2.1 Policies

2.1.1 Access Policy Default Logging (Manual)

Profile Applicability:

- Level 1

Description:

Each Access Policy should have it's default logging set to send all events to both Syslog and the FMC Events Database. While it is also recommended that each rule have logging explicitly defined, this recommendation is to prevent a situation where a misconfigured rule results in matching traffic not being properly logged.

Rationale:

The default setting for logging when creating a new rule is ***check this **** This recommendation ensures that logging still occurs for traffic matching any rule where adjusting this default is missed.

Impact:

The impact of not configuring this setting means that when investigating an incident, it would be entirely possible that critical log data would not be sent, which would of course impeded that investigation.

Audit:

GUI Audit Procedure:

```
Device > Platform Setting > Threat Defense Policy > Syslog > Logging
Destinations
```

API Audit Procedure (Python Example):

```
apireq =
"/api/fmc_config/v1/domain/"+domainuuid+"/policy/accesspolicies?expanded=true
"
apiheaders =  {'Accept': 'application/json', 'X-auth-access-token':
accesstoken}
r = requests.get(baseuri+apireq, headers=apiheaders, verify = False )
retvals = json.loads(r.text)['items']

policylist = []
for x in range(len(retvals)):
    try:
        print(retvals[x]['defaultAction']['syslogConfig']['name'])
    except:
        tempval2 = "UNDEFINED"
    else:
        tempval2 = retvals[x]['defaultAction']['syslogConfig']['name']

policylist = []
for x in range(len(retvals)):
    tempval = {'id': retvals[x]['id'],
        'name': retvals[x]['name'],
        'defaultaction.logbegin': retvals[x]['defaultAction']['logBegin'],
        'defaultaction.logend': retvals[x]['defaultAction']['logEnd'],
        'defaultaction.tofmc':
retvals[x]['defaultAction']['sendEventsToFMC'],
        'defaultaction.logend': retvals[x]['defaultAction']['logEnd'],
        'defaultaction.syslogserver': tempval2,
        'defaultaction.intrusionpolicy':
retvals[0]['defaultAction']["intrusionPolicy"]["name"]
        }
    policylist.append(tempval)
```

To be compliant:

- policylist[defaultaction.syslogserver] must have a value that is not "UNDEFINED"
- policylist[defaultaction.logbegin] must have a value of "TRUE"
- policylist[defaultaction.logend] must have a value of "TRUE"
- policylist[defaultaction.tofmc] must have a value of "TRUE"

Remediation:

In the GUI

```
Device > Platform Setting > Threat Defense Policy > Syslog > Logging
Destinations
```

Default Value:

Not Defined.

CIS Controls:

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

2.1.2 Create an outbound SSL Policy (Manual)

Profile Applicability:

- Level 1

Description:

As time moves forward, we see more and more traffic that was previously in clear text now being implemented with encryption. This makes inspecting that traffic for malicious activity more and more complex. Decrypting traffic for inspection makes that process much easier, however, privacy and legal factors should be considered before implementing such as process. Decryption is governed by the "SSL Policy". In addition to site categories or individual sites, rules within that policy can be assigned by user accounts, workstation names, subnets or applications as in most other Firepower policies.

Rationale:

Standard HTTPS traffic is a good target for decryption, as configuring Firepower to decrypt, inspect then re-encrypt traffic is fairly straightforward.
In most cases, the following site categories should not be decrypted:

- Finance
- Government and Law
- Health and Medicine

Essentially, any site that might be subject to Privacy legislation should not be decrypted.

Impact:

This function involves configuring the FirePower system with a Certificate Authority (CA) that is trusted in your organization. This means that workstations within your organization will need that CA Certificate in their list of trusted Certificate Authorities.

What this means is that only managed workstations can effectively have their traffic decrypted. "Guest" workstations that are not centrally managed (which includes personal cell phones in many organizations) will not have the correct CA Certificate list, so cannot be subject to a decryption policy.

Audit:

- Verify that you have a written policy that permits decryption that has been communicated to the people that are affected by that policy.
- Navigate to Policies > SSL
- Verify that, at a minimum the site categories: "Finance", "Government and Law", "Health and Medicine" have a "Do not decrypt" action assigned to them
- Assess other "Decrypt - Resign" and "Do not Decrypt" assignments for compliance to your policy

- Verify that any sites assigned a "Do not decrypt" action for performance or operational reasons (such as pinned certificates) still fall within the parameters of your policy
- Verify that your SSL Policy is assigned in the Access Policy (Policies > Access Control > <Your Access Policy> > SSL Policy)

Remediation:

- Verify that you have a written policy that permits decryption that has been communicated to the people that are affected by that policy.
- Navigate to Policies > SSL
- Create rules to define what is exempted from decryption. At a minimum the site categories: "Finance", "Government and Law", "Health and Medicine" should have a "do not decrypt" action assigned to them
- Assess other "Decrypt - Resign" and "Do not Decrypt" assignments for compliance to your policy
- Verify that any sites assigned a "Do not decrypt" action for performance or operational reasons still fall within the parameters of your policy
- In most rulesets, there will be a "default" rule at the bottom of the list, which will either decrypt all other sites, or exempt all other sites from decryption.
- Verify that your SSL Policy is assigned in the Access Policy (Policies > Access Control > <Your Access Policy> > SSL Policy)

Default Value:

By default no SSL Policy is created or implemented.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.3 Deploy a Network Intrusion Detection Solution Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service.		●	●
v8	13.8 Deploy a Network Intrusion Prevention Solution Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			●
v8	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	12.10 Decrypt Network Traffic at Proxy Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.			●

2.1.3 Intrusion prevention policy (Automated)

Profile Applicability:

- Level 2

Description:

Intrusion policies are sets of intrusion detection and prevention setting that inspect traffic for violations and in the case of inline deployments can block malicious traffic. These policies are the system's last line of defense before traffic transitions to its destination.

Rationale:

The Firepower System delivers several base intrusion policies, which enable you to take advantage of the experience of the Cisco Talos Intelligence Group (Talos). Ensuring that the base policies give you the ability to block or mitigate malicious traffic.

Audit:

```
Policies > Access Control > Intrusion
```

Compare Intrusion policies. Ensure base policy is applied

Remediation:

```
Policies > Access Control > Intrusion
```

Create Policy using a minimum of the Base Policy.

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.8 Deploy a Network Intrusion Prevention Solution Deploy a network intrusion prevention solution, where appropriate. Example implementations include the use of a Network Intrusion Prevention System (NIPS) or equivalent CSP service.			●
v7	12.7 Deploy Network-Based Intrusion Prevention Systems Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries.			●

2.1.4 Enable TLS server identity discovery (Automated)

Profile Applicability:

- Level 1

Description:

TLS server identity discovery is the process by which a FTD verifies the identity of the server that is trying to make a secure connection via TLS or SSL. This is vital for ensuring the security and authenticity of the server.

Rationale:

Determining that the incoming traffic is originated from a secure server is important to the safety of your network. Enabling TLS server identity discovery allows FTD to determine if the source of traffic is communicating through a secure server.

Audit:

```
Policies > Access Control > Advanced
```

View your access control policies
Go to advanced settings
Verify TLS Server Identity Discovery is selected

Remediation:

```
Policies > Access Control > Advanced
```

Check TLS Server Identity Discovery

Default Value:

Not Enabled.

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/getting_started_with_access_control_policies.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

2.1.5 Access Policy File Policy (Manual)

Profile Applicability:

- Level 1

Description:

FirePower allows detection of files by type, then imposing an action on detected files, which can consist of any or all of: Block Malware Detect Files Block Files Malware Cloud Lookup

With in these categories, processing options include: Spero Analysis for MSEXE Dynamic Analysis Capacity Handling (if busy, store suspect files for later processing) Local Malware Analysis Reset Connection

These values are configurable by Application Protocol and Direction of Transfer.

Rationale:

Files downloaded from the public internet, via email or direct download are a prime source of malware in most organizations today. For an initial infection vector, the most common by far is Office documents that have embedded macros or other active content. Subsequent stages of infection however will download true executable files or scripts (often PowerShell, Python or Javascript, but certainly not limited to these) which will then execute the malicious intent of the malware campaign.

Impact:

Configuring a File Policy helps to make downloading (or sending or uploading) malware more difficult.

Audit:

- Verify that your organization has a written and approved policy that has been communicated to the people affected by that policy.
- Navigate to Policies > Malware and File
- Edit your file policy
- Verify that your file policy implements the written policy as closely as possible.
- Verify that this file policy to all "Permit" rules in the Access Control Policy (Policies > Access Control)

Remediation:

- Verify that your organization has a written and approved policy that has been communicated to the people affected by that policy.
- Navigate to Policies > Malware and File
- Edit or Create your file policy
- Verify that your file policy implements the written policy as closely as possible.

- Apply this file policy to all "Permit" rules in the Access Control Policy (Policies > Access Control)

Default Value:

By default no File Policy exists.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.7 Allowlist Authorized Scripts Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●
v8	9.6 Block Unnecessary File Types Block unnecessary file types attempting to enter the enterprise's email gateway.		●	●
v7	7.9 Block Unnecessary File Types Block all e-mail attachments entering the organization's e-mail gateway if the file types are unnecessary for the organization's business.		●	●

2.1.6 Decrypt traffic (Automated)

Profile Applicability:

- Level 2

Description:

SSL decryption policies turn encrypted traffic into plaintext traffic. This allows the FTD device to apply URL filtering, intrusion and malware control as well as services that require deep packet inspection. If your policies allow the traffic it is then re-encrypted before it leaves the device.

Rationale:

Encrypted traffic can hide malicious content or activities. By decrypting the traffic, the firewall can inspect it for malware or other threats. Decryption allows the firewall to analyze web pages, applications and files.

Impact:

Traffic decryption can be resource intensive. When enabling this on your FTD device ensure that you have a robust architecture to handle the additional CPU and memory usage.

Audit:

Verify ssl decryption is enabled.

```
Policy > SSL Decryption > SSL Decryption.
```

After you enable SSL decryption

```
Policy > SSL Decryption > configure default action for policy.
```

Remediation:

```
Policy > SSL Decryption > enable SSL Decryption.
```

After you enable SSL decryption

```
Policy > SSL Decryption > configure default action for policy.
```

Default Value:

Not Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	12.10 Decrypt Network Traffic at Proxy Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use whitelists of allowed sites that can be accessed through the proxy without decrypting the traffic.			●

2.1.7 Access Policy - URL Filtering (Manual)

Profile Applicability:

- Level 1

Description:

Firepower allows restriction of sites by category and reputation. For instance, allowing "hacking" sites of good reputation only would likely permit information security blogs and tools, but block sites that post pirated software or key generation tools. Permitting social media sites of good reputation only would permit mainstream sites such as LinkedIn, Facebook, Instagram or Twitter, but would block social media sites that have more extremist content.

Rationale:

Site categories can be blocked for many reasons. In most organizations, these can be divided into "Human Resources" and "IT" reasons.

The first category will include things like sites that by their nature are outright illegal to access in the workplace, as well as sites that violate community standards within the organization. The "community standards" list will of course vary between organizations, so this list is of course somewhat fluid, and should be set by a written policy within your organization before implementation.

Site Categories often blocked for "Human Resources" Reasons:

- Pornography
- Adult
- Cheating and Plagarism
- Dating
- Gambling
- Lotteries
- Hate Speech
- Illegal Activities
- Illegal Downloads
- Illegal Drugs
- Child Abuse Content
- Terrorism and Violent Extremism
- Extreme
- Ebanking Fraud

Less commonly in recent times, some organizations have policies that block social media, games and recreation sites for "productivity" reasons.

At the other end of the spectrum, there are site categories that allow blocking of sites that seek to infect or compromise hosts, supply malware or tools that might not be desired in the organization, or facilitate avoidance of acceptable use policies within the organization.

Site Categories that are blocked for these "IT Reasons" can often include:

- Spam
- Peer File Transfer
- Spyware and Adware
- Botnets
- Hacking
- Open HTTP Proxy
- Parked Domains
- Filter Avoidance
- Cryptojacking
- Cryptomining
- Domain Generated Algorithm
- Malware Sites
- Malicious Sites
- Personal VPN

Impact:

Not having a written policy that governs internet access by category in your organization means that any enforcement doesn't have an "legs to stand on" - without a written policy that is approved by Sr Management effective enforcement simply is not possible.

Not blocking sites for the various "HR Reasons" exposes the organization to legal action due to access of illegal content. Not blocking sites that fall into the "community standards" category exposes the organization to HR complaints around workplace standards and appropriate behaviour.

At the other end of the spectrum, not blocking the various "IT Reasons" sites exposes the organization's servers and workstations to actual malicious activity. Sites in these categories seek to infect or compromise hosts, download or otherwise supply supply malware, or facilitate avoidance of acceptable use policies within the organization. In addition, sites that host legitimate security tools might need to be restricted to specific, authorized groups in many organizations.

Audit:

- Verify that a written policy is in place to restrict access to internet sites by category.
- Navigate to Policies > Access Control.
- Edit the Access Control Policy
- Verify that one or more "block by category" rules exist, and ensure that they provide complete coverage (and no more) when compared to the written policy.

Remediation:

- Verify that a written policy is in place to restrict access to internet sites by category.
- Navigate to Policies > Access Control.
- Edit the Access Control Policy
- Create one or more "block by category" rules, with blocked categories in compliance with the written policy.

Default Value:

By default there is no block rules in the Access Policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.7 Collect URL Request Audit Logs Collect URL request audit logs on enterprise assets, where appropriate and supported.		●	●
v8	9.3 Maintain and Enforce Network-Based URL Filters Enforce and update network-based URL filters to limit an enterprise asset from connecting to potentially malicious or unapproved websites. Example implementations include category-based filtering, reputation-based filtering, or through the use of block lists. Enforce filters for all enterprise assets.		●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●
v7	7.6 Log all URL requests Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		●	●

2.1.8 Enable secure VPN anyconnect tunnelling protocols (Manual)

Profile Applicability:

- Level 1

Description:

A secure VPN uses strong encryption protocols making it difficult for anyone to intercept data. Traffic is masked to prevent leakage. Strong encryption is recommended with the VPN tunneling. The IKEv2 policy should include AES-256 or AES-GCM-256 for encryption, a Diffie-Hellman group of 20, a SHA-384 or SHA-512 integrity hash, and a Pseudo Random Function (PRF) hash of SHA-384 or SHA-512.

Rationale:

Secure VPN settings are important to protect privacy and data. Secure settings ensure that your online activities are encrypted and anonymized

Audit:

```
Device > VPN settings
```

Verify VPN settings

Remediation:

Follow Cisco's Guidance

```
https://www.cisco.com/c/en/us/support/docs/security-vpn/secure-socket-layer-ssl/217040-configure-ssl-anyconnect-management-vpn.html#anc0
```

Default Value:

N/A

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●

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.		●	●

2.1.9 Enable secure Site to Site VPN tunnelling protocols (Manual)

Profile Applicability:

- Level 1

Description:

A secure VPN uses strong encryption protocols making it difficult for anyone to intercept data. Traffic is masked to prevent leakage. Strong encryption is recommended with the VPN tunneling. The IKEv2 policy should include AES-256 or AES-GCM-256 for encryption, a Diffie-Hellman group of 20, a SHA-384 or SHA-512 integrity hash, and a Pseudo Random Function (PRF) hash of SHA-384 or SHA-512.

Rationale:

Secure VPN settings are important to protect privacy and data. Secure settings ensure that your online activities are encrypted and anonymized

Audit:

```
Navigate to Devices > VPN > Site To Site. Under Add VPN, click Firepower
Threat Defense Device
```

Remediation:

Follow Cisco's Guidance

```
https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-
ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html#toc-hId--
1324915693
```

Default Value:

Not Configured

References:

1. https://media.defense.gov/2023/Aug/02/2003272858/-1/-1/0/CTR_CISCO_FIREPOWER_HARDENING_GUIDE.PDF
2. https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/215470-site-to-site-vpn-configuration-on-ftd-ma.html#toc-hId--1324915693

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).		●	●
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			
v7	9.1 Associate Active Ports, Services and Protocols to Asset Inventory Associate active ports, services and protocols to the hardware assets in the asset inventory.		●	●
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.		●	●

2.1.10 Access Policy Application Settings should be set (Manual)

Profile Applicability:

- Level 1

Description:

When creating a rule, where possible the "Application" field should be preferred for use over the traditional "Dest Port" fields. Even when the destination port is known, the Application value should be added for each rule.

Rationale:

This preference makes things like Data Exfiltration or Beaconing to Command and Control servers more difficult for malicious actors. Masquerading traffic of this type over port 53 (usually used for DNS) or as unencrypted traffic using 443/tcp is a common practice for malware.

Impact:

Supplying both the Destination Port and the Application fields for each rule in the Access Policy makes data exfiltration and beaconing that much more difficult for malicious actors.

Unfortunately, current malware routinely uses valid HTTPS traffic for these purposes, but the more "speed bumps" that can be implemented at the perimeter the better.

Audit:

For each rule in the Access Policy (especially perm,it rules), ensure that the Application field is filled in. Even if the destination port is "known" for any particular rule, the application should still be filled in.

Remediation:

For each Access Policy Rule:

- Choose "Edit"
- Choose the "Applications" tab for that rule
- Select all applications that are applicable for that rule

Note that if any application other than "Any" is selected, then the application list must be complete, or some desired traffic will be blocked (or undesired traffic will be permitted). This means that this is often an iterative process.
A common method is to have a rule with the Application list implemented, then follow that rule with an identical one, but with "Any" selected for the application field. This second rule will log differently - with a higher severity or to a different log server, so that as the second rule triggers, exceptions are easily seen and the first rule can be adjusted. After some period of time the second rule will no longer trigger and will be deleted.

Default Value:

The value of "Any" is the default for any new Access Policy Rule.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.6 Establish and Maintain an Inventory of Authentication and Authorization Systems Establish and maintain an inventory of the enterprise's authentication and authorization systems, including those hosted on-site or at a remote service provider. Review and update the inventory, at a minimum, annually, or more frequently.		●	●
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

3 Control Plane

The control plane covers monitoring, route table updates, and generally the dynamic operation of the router. Services, settings, and data streams that support and document the operation, traffic handling, and dynamic status of the router. Examples of control plane services include: logging (e.g. Syslog), routing protocols, status protocols like CDP and HSRP, network topology protocols like STP, and traffic security control protocols like IKE. Network control protocols like ICMP, NTP, ARP, and IGMP directed to or sent by the router itself also fall into this area.

3.1 Secure local network infrastructure

3.1.1 Secure the Network Time Protocol Server (Manual)

Profile Applicability:

- Level 1

Description:

Network Time Protocol (NTP) is intended to synchronize all participating devices to within a few milliseconds of Coordinated Universal Time (UTC). NTP is important for correct logging and tracking of events.

Rationale:

Synchronizing the system time on the management center and its managed devices is essential to successful operation of Firepower. We strongly recommend using a secure and trusted Network Time Protocol (NTP) server to synchronize system time on the management center and the devices it manages.

Impact:

When multiple devices are in usage, without time synchronization, each resource will think the correct time is different. If you try to compare logs between resources, none of the timestamps line up. If the data is aggregated to a log server or security information event manager, the events will appear jumbled, and analytics and correlation engines will not be able to process the data for unusual behavior or indicators of compromise.

Audit:

```
Devices > Platform Settings > Time Synchronization (verify NTP server)
```

Remediation:

```
Devices > Platform Settings > Time Synchronization >
**_Configure one of the following clock options:_**

**Via NTP from Defense Center—(Default)**. The managed device gets time from
the NTP servers you configured for the management center (except for
authenticated NTP servers) and synchronizes time with those servers directly.
However, if any of the following are true, the managed device synchronizes
time from the management center:
The management center's NTP servers are not reachable by the device.

The management center has no unauthenticated servers.

**Via NTP from**—If your management center is using NTP servers on the
network, select this option and enter the fully-qualified DNS name (such as
ntp.example.com), or IPv4 or IPv6 address, of the same NTP servers you
specified in System > Configuration > Time Synchronization. If the NTP
servers are not reachable, the management center acts as an NTP server.
```

Default Value:

NTP from Defense Center

References:

1. https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/interfaces-settings-platform.html?bookSearch=true

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4 Secure Configuration of Enterprise Assets and Software Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).			
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.		●	●

3.1.2 Secure the Domain Name System (DNS) (Manual)

Profile Applicability:

- Level 1

Description:

Devices communicating with each other over a network generally rely on DNS to translate hostnames to IP addresses. Certain FTD functions use DNS examples include NTP, access control policies, VPN services provided by the threat defense, ping, or traceroute

Rationale:

Audit:

```
Devices > Platform Settings > DNS > DNS Settings (verify DNS Server Settings)
```

Remediation:

```
Devices > Platform Settings > DNS > DNS Settings >
Check Enable DNS name resolution by device
Configure the DNS Server Groups
```

Default Value:

no setting

References:

1. https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/720/management-center-device-config-72/interfaces-settings-platform.html?bookSearch=true#id_74914

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.		●	●
v8	8.6 Collect DNS Query Audit Logs Collect DNS query audit logs on enterprise assets, where appropriate and supported.		●	●

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.	●	●	●
v7	8.7 Enable DNS Query Logging Enable Domain Name System (DNS) query logging to detect hostname lookups for known malicious domains.		●	●

3.2 Harden Network Protocol Settings

3.2.1 Disable fragment reassembly (Automated)

Profile Applicability:

- Level 2

Description:

Rationale:

Attackers use fragmentation to evade security systems such as firewalls or IPS because the checks are usually performed on the first fragment. They can then put malicious payload in the other fragments to perform DoS against internal systems. Disabling the fragmentation on the security appliance implies changing its default behavior from accepting up to 24 fragments in a packet to accepting only 1 fragment in a packet.

Impact:

You might need to allow fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, fragmented packets are often used in Denial of Service (DoS) attacks, so we recommend that you do not allow fragments.

Audit:

```
Device>Platform settings>(FTD Policy)>Fragment settings>Chain=1
```

Remediation:

```
Devices > Platform Settings > create an FTD policy > Fragment Settings > set
Chain (Packet) to '1' > Save and Deploy
```

Default Value:

By default the threat defense device allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4 Secure Configuration of Enterprise Assets and Software Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).			
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

3.2.2 Block older SSL and TLS versions (Automated)

Profile Applicability:

- Level 1

Description:

Transport Layer Protocol or TLS utilities cryptography to encrypt web traffic. Firepower Threat Defense can block older TLS and SSL version to help protect the network from compromise. It is recommended that you move to TLS 1.3 for your enterprise.

Rationale:

By using TLS 1.3 you can enhance the security and performance of you network communications while maintaining privacy and complying with modern standards.

Audit:

```
Policies > Access Control > SSL
```

Ensure that a rule exists blocking older versions of SSL and TLS.

Remediation:

```
Policies > Access Control > SSL
1. Click add rule
2. In the _Name_ field enter a name for the rule
3. From the _Action_ list select **Block** or **Block with reset**
4. Click _Version_
5. Select older versions of TLS
6. Save Rule
```

Because this is a specific rule, order it earlier in your policy than more general rules such as application-matching rules.

Default Value:

not configured

References:

1. https://www.cisco.com/c/en/us/td/docs/security/firepower/70/configuration/guide/fpmc-config-guide-v70/understanding_traffic_decryption.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.8 Uninstall or Disable Unnecessary Services on Enterprise Assets and Software Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.		●	●
v7	7.2 Disable Unnecessary or Unauthorized Browser or Email Client Plugins Uninstall or disable any unauthorized browser or email client plugins or add-on applications.		●	●

3.3 Configure default action to Block (Automated)

Profile Applicability:

- Level 1

Description:

The default action handles traffic that does not match any of the rulesets created by network administrators. A Block default configuration ensures only permitted and desired traffic passes through the network, minimizing unauthorized access and preventing potentially malicious traffic from accessing and compromising the network.

Rationale:

Block for all actions that aren't defined by rulesets is similar to the Deny Any/Any in an ASA. It is important to prevent traffic not defined by rulesets from gaining access to the network.

Impact:

Setting default block with logging can cause some issues with latency in high traffic networks. It is important to have adequate storage for the logs.

Audit:

In the GUI

```
Policies > Access Control > in the Default Action dropdown at the bottom,
ensure Block is selected> Verify At Beginning and End of Connection radio
button is selected
```

In the API
HTTP GET `/policy/accesspolicies`
Look for:

```
            "defaultAction": {
                "action": "DENY",
                "eventLogAction": "LOG_BOTH"
```

Remediation:

In the GUI

```
Policies > Access Control > in the Default Action dropdown at the bottom,
select Block > select the At Beginning and End of Connection radio button >
OK
```

In the API
HTTP PUT /policy/accesspolicies/{objId}

```
{
    "name": "NGFW-Access-Policy",
    "version": "<version>",
    "defaultAction": {
      "action": "DENY",
      "eventLogAction": "LOG_BOTH",
      "type": "accessdefaultaction"
    },
    "type": "accesspolicy"
  }
```

Default Value:

Not Enabled.

References:

1. https://media.defense.gov/2023/Aug/02/2003272858/-1/-1/0/CTR_CISCO_FIREPOWER_HARDENING_GUIDE.PDF

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	7.4 Maintain and Enforce Network-Based URL Filters Enforce network-based URL filters that limit a system's ability to connect to websites not approved by the organization. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.		●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Management Plane**		
1.1	**Identity**		
1.1.1	**Local Credentials**		
1.1.1.1	Restrict access to the local Admin account (Manual)	☐	☐
1.1.1.2	Do not use the default "admin" account (Manual)	☐	☐
1.1.2	**External Authentication**		
1.1.2.1	Use an External Authentication Source for Administrative Logins (Manual)	☐	☐
1.1.2.2	Enable SSHv2 (Automated)	☐	☐
1.1.3	**User Roles for Administrative Access (Authorization)**		
1.1.3.1	Set Appropriate Roles for all Administrative Users (Manual)	☐	☐
1.1.3.2	Use Dedicated User Accounts for API Access (Manual)	☐	☐
1.1.3.3	Restrict access to the FMC CLI (Manual)	☐	☐
1.1.4	**User Identification**		
1.1.4.1	**Realm Configuration (User to Group Mapping, Active Logins)**		
1.1.4.1.1	Create a Realm (Manual)	☐	☐
1.1.4.1.2	Create an Identity Policy (Manual)	☐	☐
1.1.4.1.3	Create an Identity Rule (Manual)	☐	☐
1.1.4.1.4	Manage a Realm (Manual)	☐	☐
1.1.4.1.5	Compare Realms (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.1.4.1.6	Manage an Identity Policy (Manual)	☐	☐
1.1.4.1.7	Manage an Identity Rule (Manual)	☐	☐
1.2	**Backups**		
1.2.1	Create Periodic Backups of Firepower Management Center (Automated)	☐	☐
1.3	**Scheduled Updates**		
1.3.1	Scheduled Rule Updates (Automated)	☐	☐
1.3.2	Scheduled Geolocation Updates (Automated)	☐	☐
1.3.3	Update of URL Filtering Database (Automated)	☐	☐
1.3.4	Regularly update the FMC Server Version (Manual)	☐	☐
1.3.5	Regularly update the Firepower Sensors (Automated)	☐	☐
1.4	**Monitoring**		
1.4.1	**Health Policy**		
1.4.1.1	Create a Health Policy for your FMC Server (Automated)	☐	☐
1.4.1.2	Ensure that the Health Policy is assigned to the managed Firepower Appliances (Automated)	☐	☐
1.4.1.3	Ensure that the Health Policy is assigned to all FMC Servers (Automated)	☐	☐
1.4.2	**Platform Logging and Time**		
1.4.2.1	Configure Central Logging for FMC (Automated)	☐	☐
1.4.2.2	Configure Central Logging for FMC Managed Devices (Automated)	☐	☐
1.4.2.3	Monitor for Clock Drift within the Firepower Infrastructure (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.4.2.4	Set FMC Time Synchronization to Multiple Reliable NTP Source(s) (Automated)	☐	☐
1.4.2.5	Set Firepower Sensor / Devices to Synchronize time to FMC (Automated)	☐	☐
1.4.2.6	Configure Audit Logging to be Sent to Syslog (Automated)	☐	☐
1.4.3	**SNMP**		
1.4.3.1	If SNMP is configured, ensure that SNMP v3 only is used to Manage your FMC Server (Manual)	☐	☐
1.4.3.2	If SNMP is configured, ensure that SNMP v3 only is used to Manage your Firepower Managed Devices (Manual)	☐	☐
1.5	**Triggered Actions**		
1.5.1	**Scanning**		
1.5.1.1	Run Scheduled Nmap Scans (Manual)	☐	☐
1.6	**Database Settings**		
1.6.1	Set Database Retention Policies (Manual)	☐	☐
2	**Data Plane**		
2.1	**Policies**		
2.1.1	Access Policy Default Logging (Manual)	☐	☐
2.1.2	Create an outbound SSL Policy (Manual)	☐	☐
2.1.3	Intrusion prevention policy (Automated)	☐	☐
2.1.4	Enable TLS server identity discovery (Automated)	☐	☐
2.1.5	Access Policy File Policy (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.6	Decrypt traffic (Automated)	☐	☐
2.1.7	Access Policy - URL Filtering (Manual)	☐	☐
2.1.8	Enable secure VPN anyconnect tunnelling protocols (Manual)	☐	☐
2.1.9	Enable secure Site to Site VPN tunnelling protocols (Manual)	☐	☐
2.1.10	Access Policy Application Settings should be set (Manual)	☐	☐
3	**Control Plane**		
3.1	**Secure local network infrastructure**		
3.1.1	Secure the Network Time Protocol Server (Manual)	☐	☐
3.1.2	Secure the Domain Name System (DNS) (Manual)	☐	☐
3.2	**Harden Network Protocol Settings**		
3.2.1	Disable fragment reassembly (Automated)	☐	☐
3.2.2	Block older SSL and TLS versions (Automated)	☐	☐
3.3	Configure default action to Block (Automated)	☐	☐

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Restrict access to the local Admin account	☐	☐
1.1.2.1	Use an External Authentication Source for Administrative Logins	☐	☐
1.1.2.2	Enable SSHv2	☐	☐
1.1.3.2	Use Dedicated User Accounts for API Access	☐	☐
1.2.1	Create Periodic Backups of Firepower Management Center	☐	☐
1.3.2	Scheduled Geolocation Updates	☐	☐
1.3.3	Update of URL Filtering Database	☐	☐
1.3.4	Regularly update the FMC Server Version	☐	☐
1.3.5	Regularly update the Firepower Sensors	☐	☐
1.4.1.1	Create a Health Policy for your FMC Server	☐	☐
1.4.1.2	Ensure that the Health Policy is assigned to the managed Firepower Appliances	☐	☐
1.4.1.3	Ensure that the Health Policy is assigned to all FMC Servers	☐	☐
3.1.2	Secure the Domain Name System (DNS)	☐	☐
3.2.1	Disable fragment reassembly	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Restrict access to the local Admin account	☐	☐
1.1.2.1	Use an External Authentication Source for Administrative Logins	☐	☐
1.1.2.2	Enable SSHv2	☐	☐
1.1.3.2	Use Dedicated User Accounts for API Access	☐	☐
1.1.4.1.1	Create a Realm	☐	☐
1.1.4.1.2	Create an Identity Policy	☐	☐
1.1.4.1.3	Create an Identity Rule	☐	☐
1.1.4.1.4	Manage a Realm	☐	☐
1.1.4.1.5	Compare Realms	☐	☐
1.1.4.1.6	Manage an Identity Policy	☐	☐
1.1.4.1.7	Manage an Identity Rule	☐	☐
1.2.1	Create Periodic Backups of Firepower Management Center	☐	☐
1.3.1	Scheduled Rule Updates	☐	☐
1.3.2	Scheduled Geolocation Updates	☐	☐
1.3.3	Update of URL Filtering Database	☐	☐
1.3.4	Regularly update the FMC Server Version	☐	☐
1.3.5	Regularly update the Firepower Sensors	☐	☐
1.4.1.1	Create a Health Policy for your FMC Server	☐	☐
1.4.1.2	Ensure that the Health Policy is assigned to the managed Firepower Appliances	☐	☐
1.4.1.3	Ensure that the Health Policy is assigned to all FMC Servers	☐	☐
1.4.2.1	Configure Central Logging for FMC	☐	☐
1.4.2.2	Configure Central Logging for FMC Managed Devices	☐	☐
1.4.2.3	Monitor for Clock Drift within the Firepower Infrastructure	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.4.2.4	Set FMC Time Synchronization to Multiple Reliable NTP Source(s)	☐	☐
1.4.2.5	Set Firepower Sensor / Devices to Synchronize time to FMC	☐	☐
1.4.2.6	Configure Audit Logging to be Sent to Syslog	☐	☐
1.4.3.1	If SNMP is configured, ensure that SNMP v3 only is used to Manage your FMC Server	☐	☐
1.4.3.2	If SNMP is configured, ensure that SNMP v3 only is used to Manage your Firepower Managed Devices	☐	☐
1.5.1.1	Run Scheduled Nmap Scans	☐	☐
1.6.1	Set Database Retention Policies	☐	☐
2.1.1	Access Policy Default Logging	☐	☐
2.1.5	Access Policy File Policy	☐	☐
2.1.7	Access Policy - URL Filtering	☐	☐
2.1.9	Enable secure Site to Site VPN tunnelling protocols	☐	☐
3.1.1	Secure the Network Time Protocol Server	☐	☐
3.1.2	Secure the Domain Name System (DNS)	☐	☐
3.2.1	Disable fragment reassembly	☐	☐
3.2.2	Block older SSL and TLS versions	☐	☐
3.3	Configure default action to Block	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Restrict access to the local Admin account	☐	☐
1.1.2.1	Use an External Authentication Source for Administrative Logins	☐	☐
1.1.2.2	Enable SSHv2	☐	☐
1.1.3.2	Use Dedicated User Accounts for API Access	☐	☐
1.1.4.1.1	Create a Realm	☐	☐
1.1.4.1.2	Create an Identity Policy	☐	☐
1.1.4.1.3	Create an Identity Rule	☐	☐
1.1.4.1.4	Manage a Realm	☐	☐
1.1.4.1.5	Compare Realms	☐	☐
1.1.4.1.6	Manage an Identity Policy	☐	☐
1.1.4.1.7	Manage an Identity Rule	☐	☐
1.2.1	Create Periodic Backups of Firepower Management Center	☐	☐
1.3.1	Scheduled Rule Updates	☐	☐
1.3.2	Scheduled Geolocation Updates	☐	☐
1.3.3	Update of URL Filtering Database	☐	☐
1.3.4	Regularly update the FMC Server Version	☐	☐
1.3.5	Regularly update the Firepower Sensors	☐	☐
1.4.1.1	Create a Health Policy for your FMC Server	☐	☐
1.4.1.2	Ensure that the Health Policy is assigned to the managed Firepower Appliances	☐	☐
1.4.1.3	Ensure that the Health Policy is assigned to all FMC Servers	☐	☐
1.4.2.1	Configure Central Logging for FMC	☐	☐
1.4.2.2	Configure Central Logging for FMC Managed Devices	☐	☐
1.4.2.3	Monitor for Clock Drift within the Firepower Infrastructure	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.4.2.4	Set FMC Time Synchronization to Multiple Reliable NTP Source(s)	☐	☐
1.4.2.5	Set Firepower Sensor / Devices to Synchronize time to FMC	☐	☐
1.4.2.6	Configure Audit Logging to be Sent to Syslog	☐	☐
1.4.3.1	If SNMP is configured, ensure that SNMP v3 only is used to Manage your FMC Server	☐	☐
1.4.3.2	If SNMP is configured, ensure that SNMP v3 only is used to Manage your Firepower Managed Devices	☐	☐
1.5.1.1	Run Scheduled Nmap Scans	☐	☐
1.6.1	Set Database Retention Policies	☐	☐
2.1.1	Access Policy Default Logging	☐	☐
2.1.2	Create an outbound SSL Policy	☐	☐
2.1.3	Intrusion prevention policy	☐	☐
2.1.5	Access Policy File Policy	☐	☐
2.1.6	Decrypt traffic	☐	☐
2.1.7	Access Policy - URL Filtering	☐	☐
2.1.9	Enable secure Site to Site VPN tunnelling protocols	☐	☐
3.1.1	Secure the Network Time Protocol Server	☐	☐
3.1.2	Secure the Domain Name System (DNS)	☐	☐
3.2.1	Disable fragment reassembly	☐	☐
3.2.2	Block older SSL and TLS versions	☐	☐
3.3	Configure default action to Block	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.8	Enable secure VPN anyconnect tunnelling protocols	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.2	Do not use the default "admin" account	☐	☐
1.1.2.1	Use an External Authentication Source for Administrative Logins	☐	☐
1.1.3.1	Set Appropriate Roles for all Administrative Users	☐	☐
1.1.3.2	Use Dedicated User Accounts for API Access	☐	☐
1.1.3.3	Restrict access to the FMC CLI	☐	☐
1.1.4.1.7	Manage an Identity Rule	☐	☐
1.2.1	Create Periodic Backups of Firepower Management Center	☐	☐
1.3.1	Scheduled Rule Updates	☐	☐
1.3.2	Scheduled Geolocation Updates	☐	☐
1.3.3	Update of URL Filtering Database	☐	☐
1.3.4	Regularly update the FMC Server Version	☐	☐
1.3.5	Regularly update the Firepower Sensors	☐	☐
1.4.1.1	Create a Health Policy for your FMC Server	☐	☐
1.4.1.2	Ensure that the Health Policy is assigned to the managed Firepower Appliances	☐	☐
1.4.1.3	Ensure that the Health Policy is assigned to all FMC Servers	☐	☐
1.6.1	Set Database Retention Policies	☐	☐
2.1.1	Access Policy Default Logging	☐	☐
2.1.4	Enable TLS server identity discovery	☐	☐
2.1.8	Enable secure VPN anyconnect tunnelling protocols	☐	☐
3.1.2	Secure the Domain Name System (DNS)	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.2	Do not use the default "admin" account	☐	☐
1.1.2.1	Use an External Authentication Source for Administrative Logins	☐	☐
1.1.2.2	Enable SSHv2	☐	☐
1.1.3.1	Set Appropriate Roles for all Administrative Users	☐	☐
1.1.3.2	Use Dedicated User Accounts for API Access	☐	☐
1.1.3.3	Restrict access to the FMC CLI	☐	☐
1.1.4.1.1	Create a Realm	☐	☐
1.1.4.1.2	Create an Identity Policy	☐	☐
1.1.4.1.3	Create an Identity Rule	☐	☐
1.1.4.1.4	Manage a Realm	☐	☐
1.1.4.1.5	Compare Realms	☐	☐
1.1.4.1.6	Manage an Identity Policy	☐	☐
1.1.4.1.7	Manage an Identity Rule	☐	☐
1.2.1	Create Periodic Backups of Firepower Management Center	☐	☐
1.3.1	Scheduled Rule Updates	☐	☐
1.3.2	Scheduled Geolocation Updates	☐	☐
1.3.3	Update of URL Filtering Database	☐	☐
1.3.4	Regularly update the FMC Server Version	☐	☐
1.3.5	Regularly update the Firepower Sensors	☐	☐
1.4.1.1	Create a Health Policy for your FMC Server	☐	☐
1.4.1.2	Ensure that the Health Policy is assigned to the managed Firepower Appliances	☐	☐
1.4.1.3	Ensure that the Health Policy is assigned to all FMC Servers	☐	☐
1.4.2.1	Configure Central Logging for FMC	☐	☐
1.4.2.2	Configure Central Logging for FMC Managed Devices	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.4.2.3	Monitor for Clock Drift within the Firepower Infrastructure	☐	☐
1.4.2.4	Set FMC Time Synchronization to Multiple Reliable NTP Source(s)	☐	☐
1.4.2.5	Set Firepower Sensor / Devices to Synchronize time to FMC	☐	☐
1.4.2.6	Configure Audit Logging to be Sent to Syslog	☐	☐
1.4.3.1	If SNMP is configured, ensure that SNMP v3 only is used to Manage your FMC Server	☐	☐
1.4.3.2	If SNMP is configured, ensure that SNMP v3 only is used to Manage your Firepower Managed Devices	☐	☐
1.5.1.1	Run Scheduled Nmap Scans	☐	☐
1.6.1	Set Database Retention Policies	☐	☐
2.1.1	Access Policy Default Logging	☐	☐
2.1.2	Create an outbound SSL Policy	☐	☐
2.1.4	Enable TLS server identity discovery	☐	☐
2.1.5	Access Policy File Policy	☐	☐
2.1.6	Decrypt traffic	☐	☐
2.1.7	Access Policy - URL Filtering	☐	☐
2.1.8	Enable secure VPN anyconnect tunnelling protocols	☐	☐
2.1.9	Enable secure Site to Site VPN tunnelling protocols	☐	☐
2.1.10	Access Policy Application Settings should be set	☐	☐
3.1.1	Secure the Network Time Protocol Server	☐	☐
3.1.2	Secure the Domain Name System (DNS)	☐	☐
3.2.2	Block older SSL and TLS versions	☐	☐
3.3	Configure default action to Block	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
1.1.1.1	Restrict access to the local Admin account	☐	☐
1.1.1.2	Do not use the default "admin" account	☐	☐
1.1.2.1	Use an External Authentication Source for Administrative Logins	☐	☐
1.1.2.2	Enable SSHv2	☐	☐
1.1.3.1	Set Appropriate Roles for all Administrative Users	☐	☐
1.1.3.2	Use Dedicated User Accounts for API Access	☐	☐
1.1.3.3	Restrict access to the FMC CLI	☐	☐
1.1.4.1.1	Create a Realm	☐	☐
1.1.4.1.2	Create an Identity Policy	☐	☐
1.1.4.1.3	Create an Identity Rule	☐	☐
1.1.4.1.4	Manage a Realm	☐	☐
1.1.4.1.5	Compare Realms	☐	☐
1.1.4.1.6	Manage an Identity Policy	☐	☐
1.1.4.1.7	Manage an Identity Rule	☐	☐
1.2.1	Create Periodic Backups of Firepower Management Center	☐	☐
1.3.1	Scheduled Rule Updates	☐	☐
1.3.2	Scheduled Geolocation Updates	☐	☐
1.3.3	Update of URL Filtering Database	☐	☐
1.3.4	Regularly update the FMC Server Version	☐	☐
1.3.5	Regularly update the Firepower Sensors	☐	☐
1.4.1.1	Create a Health Policy for your FMC Server	☐	☐
1.4.1.2	Ensure that the Health Policy is assigned to the managed Firepower Appliances	☐	☐
1.4.1.3	Ensure that the Health Policy is assigned to all FMC Servers	☐	☐
1.4.2.1	Configure Central Logging for FMC	☐	☐

Recommendation		Set Correctly	
		Yes	No
1.4.2.2	Configure Central Logging for FMC Managed Devices	☐	☐
1.4.2.3	Monitor for Clock Drift within the Firepower Infrastructure	☐	☐
1.4.2.4	Set FMC Time Synchronization to Multiple Reliable NTP Source(s)	☐	☐
1.4.2.5	Set Firepower Sensor / Devices to Synchronize time to FMC	☐	☐
1.4.2.6	Configure Audit Logging to be Sent to Syslog	☐	☐
1.4.3.1	If SNMP is configured, ensure that SNMP v3 only is used to Manage your FMC Server	☐	☐
1.4.3.2	If SNMP is configured, ensure that SNMP v3 only is used to Manage your Firepower Managed Devices	☐	☐
1.5.1.1	Run Scheduled Nmap Scans	☐	☐
1.6.1	Set Database Retention Policies	☐	☐
2.1.1	Access Policy Default Logging	☐	☐
2.1.2	Create an outbound SSL Policy	☐	☐
2.1.3	Intrusion prevention policy	☐	☐
2.1.4	Enable TLS server identity discovery	☐	☐
2.1.5	Access Policy File Policy	☐	☐
2.1.6	Decrypt traffic	☐	☐
2.1.7	Access Policy - URL Filtering	☐	☐
2.1.8	Enable secure VPN anyconnect tunnelling protocols	☐	☐
2.1.9	Enable secure Site to Site VPN tunnelling protocols	☐	☐
2.1.10	Access Policy Application Settings should be set	☐	☐
3.1.1	Secure the Network Time Protocol Server	☐	☐
3.1.2	Secure the Domain Name System (DNS)	☐	☐
3.2.2	Block older SSL and TLS versions	☐	☐
3.3	Configure default action to Block	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8.0	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Aug 7, 2023	1.0.0	Change Name to current CISCO branding (Ticket 19412)
Oct 20, 2023	1.0.0	Rename Title of Benchmark (Ticket 20098)
Oct 20, 2023	1.0.0	Update Overview (Ticket 20099)