National Security Agency
Cybersecurity Technical Report

Cisco Firepower Hardening Guide

[August 2023]
U/OO/183115-23
PP-23-2153

Notices and history

Document change history

Date	Version	Description
August 2023	1.0	Initial Publication

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademark recognition

Cisco Firepower is a registered trademark of Cisco Technology, Inc.

Publication information

Author(s)

National Security Agency
Cybersecurity Directorate
Network Infrastructure Security

Contact information

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
General Cybersecurity Inquiries: Cybersecurity_Requests@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions. This includes its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense information systems, and the Defense Industrial Base, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Executive summary

The Cisco Firepower device, now known as *Cisco Secure Firewall* [1], is a Next-Generation Firewall (NGFW) that blocks updated threats, malware, and application layer exploitation techniques. This cybersecurity technical report (CTR) is a guide of best practices for network and system administrators who are using Cisco Firepower Threat Defense (FTD). This report provides configurations that will assist network and system administrators in tailoring and inspecting network traffic, as well as hardening the device along with its provided default policies and rulesets.

As network administrators start to deploy Cisco Firepower devices, proper configuration is essential in mitigating vulnerabilities and ensuring the security of the network. Access control rules manage network traffic flow and minimize unauthorized access to infrastructure devices. When network administrators configure the Cisco Firepower device to prevent unauthorized traffic, they must know that securing user access to the device is just as important in preventing unauthorized access through traffic.

At minimum, network administrators should configure user accounts that contain restricted privileges, a strong password policy, and passive authentication. Linux shell and command line interface (CLI) access must be restricted to prevent users from implementing configurations that could lead to a compromised network. Undesirable traffic can be detected as early as possible by correctly configuring access control policies, creating appropriate URL filtering rules, and utilizing file and intrusion policies, which minimizes the risk of network security compromise.

Network administrators should implement configurations for encrypted traffic to create more streamlined and desired traffic. As SSL/TLS policies and separate HTTP and HTTPS access control policies are properly configured, the policies pass through authorized traffic and filter out malicious traffic that may be obscured by encryption. As network administrators configure virtual private networks (VPN) with secure hashing and encryption algorithms, traffic is routed privately and securely to prevent unauthorized users and access to sensitive data.

Creating malware and file policies allows the device to capture and detect files that are harmful to the network. Resetting session connections prevent harmful sessions from remaining open and leading to a compromise in the network.

Network administrators need to harden the underlying operating system, FXOS, on Firepower compatible devices [2] to minimize attack surfaces. Strong SSH algorithms, HTTPS options, and TLS versions should be configured in order to enable secure sessions between authorized users and the device. This configuration not only limits the number of users that can access the FXOS but prevents unsecured access into the device.

Contents

Table of Figures

1. Overview

Cisco Firepower is a Next-Generation Firewall (NGFW) with a combined operating system that has application-layer Firepower features and network-layer Cisco Adaptive Security Appliance (ASA) features. It runs the Firepower Threat Defense (FTD) operating system. Along with the stateful firewall features of the ASA, FTD implements application visibility and control (AVC), URL filtering, user identity and authentication, malware protection, and intrusion prevention.

The Firepower Management Center (FMC) is designed to centralize management functions for multiple FTD devices. The FMC contains similar configuration features as the standalone Firepower device as well as other configurations that are unique to FMC. This document establishes a best practice guide for essential configurations of the FTD system. The purpose of these configurations is to enhance network traffic security and visibility along with other network-specific configurations that were created based on the needs of the organization. At the time this document was written, the Cisco suggested release version of FTD was 7.0.5 and of FMC was 7.0.5 [3].

2. Implementing access control

Access control rules are created to refine and control desired traffic flow, minimize unauthorized access, and prevent undesirable traffic from accessing and compromising the network, while also allowing users to access intended and authorized sites. Access control policies protect the network by restricting users from accessing specifically configured external or internal network resources, while also providing the appropriate connectivity to users within defined security zones of the network. A best practice for access control configuration is to create rules that are as specific and succinct as possible and in the proper order. Following this practice will minimize the processing power required, the amount of rules the device needs to evaluate, and the increased risk of rule redundancy.

In FTD, access control rules can indicate the type of traffic as well as how it is blocked, allowed, logged, or inspected. Configured rules can restrict specific ports, URLs, file types, network ranges, and parts of or entire applications to regulate the flow of traffic within a network. An access control policy can be applied to one or more FTD devices when multiple FTD devices are managed with the FMC.

2.1. Configure default action to "Block"

The *default action* handles all of the 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.

NSA recommends setting the default action to *Block* with *Connection Events Logging: At Beginning and End of Connection* selected with additional rules created in an "allow-listing" method, as shown in the following figure. Enabling detailed logging in a firewall can potentially impact the performance of the firewall, especially during high traffic periods. However, these devices can significantly scale in high-traffic environments. Intensive logging can introduce additional latency into network communications. Each logged event requires processing and storage, which can add a delay in the packet forwarding process.

The default action of *Block* is configured as follows: *Policies* > *Access Control* > in the *Default Action* dropdown at the bottom, select *Block* > select the *At Beginning and End of Connection* radio button > *OK*.

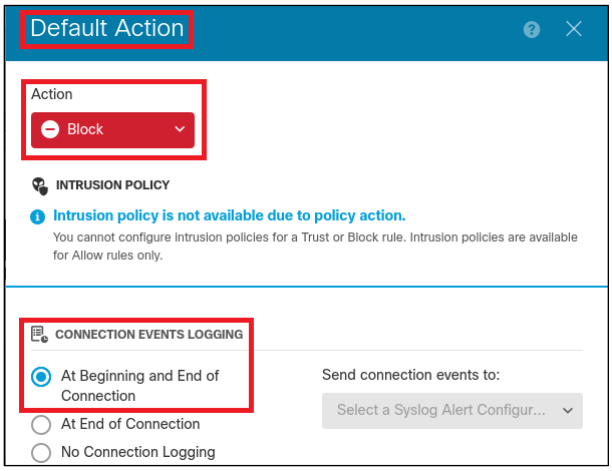

Figure 1: Default access control option (FDM)

Since the default access control option is set to *Block*, an *Allow* access rule set is required to access the public Internet. This can be configured as follows: *Policies* > *Access Control* > *Add Rule* (the '+' button) > Source Networks: *[Desired Source Network]* > Destination Networks: *[Desired Destination Network]*, as shown in the following figure:

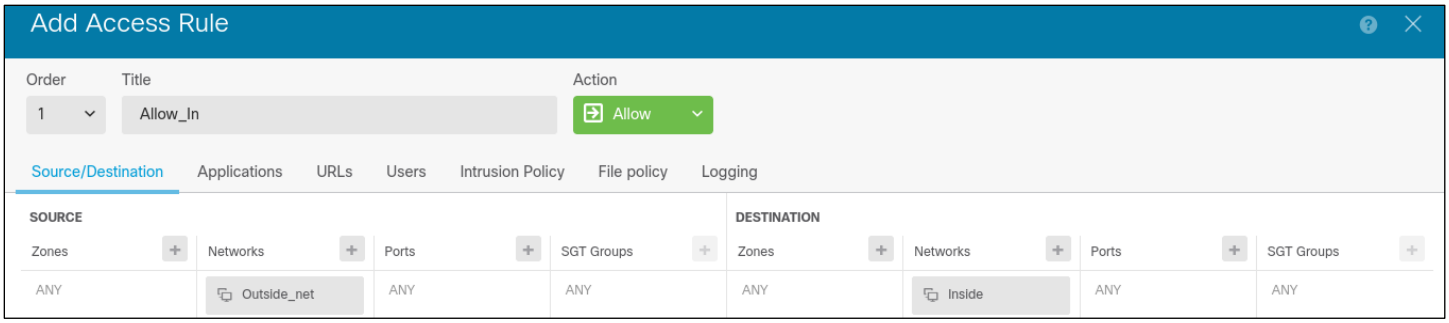

Figure 2: Add Allow access rule

2.2. Ensure rule priority placement

Proper configuration of access control rules ensures only explicitly allowed traffic can reach the network. Access control rules are processed against the defined rules in a top-down, sequential order evaluation method. As packets flow through the system, they are compared against the rules in the specific order that they are defined. Once a packet matches a rule, the evaluation process is concluded, even if subsequent, more specific rules are later defined.

Since packets are processed according to the first matched rule, NSA recommends placing specific access control policies before generalized rules, to ensure critical, undesirable traffic is detected as early as possible. If access control rules are improperly configured or placed in an incorrect order, a rule that is

higher up could block subsequent rules from allowing desirable traffic through, potentially jeopardizing the availability of the network.

The following figure shows *incorrectly* configured access control rules. Rule #1, a *general* rule, *allows* access to the entirety of the Facebook Application. Rule #2, a *specific* rule, *blocks* Facebook Apps and Facebook Games. Since Rule #1 *allows* all of Facebook, Rule #2 would not be evaluated when a user attempts to visit Facebook Apps and Facebook Games, therefore improperly *allowing* the User access.

Figure 3: Incorrectly configured access rules

The specific rule of *NO FB Games* should be set as Rule #1 and the general rule of *Allow FB* should be set to Rule #2, to correctly configure these access control rules. This change results in blocking access to Facebook Apps and Facebook Games but allowing users access to the rest of Facebook. The evaluation order of the rules can be changed by either dragging a rule to the desired position within the rule list, or by selecting *Edit* (pencil icon) and then changing the *Order* number in the dropdown in the upper-left corner, as shown in the following figures:

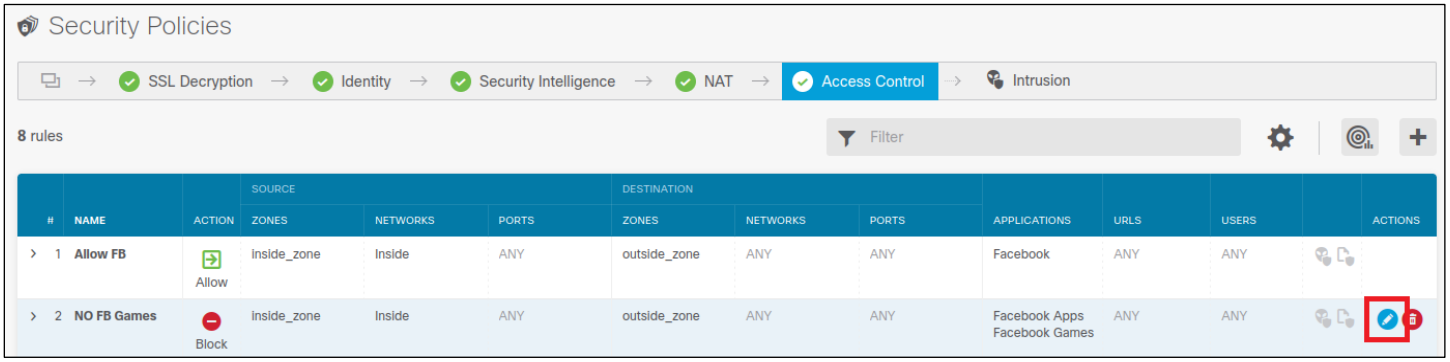

Figure 4: Edit access rule

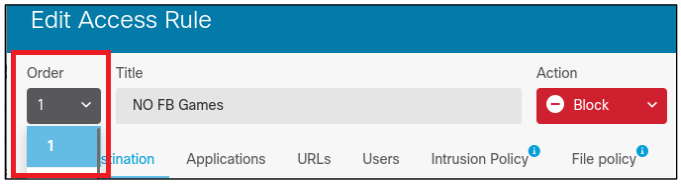

Figure 5: Change access rule order

Figure 6: Correctly configured access rules

While this specific example is an illustration of how to configure access control rules in a NGFW with rule priority placement in mind, this product does still offer the traditional access control functionality options that specifically address IPv4 or IPv6 traffic, as well as rules that specify protocols or ports. The user can refer to the NIST recommendations for further guidelines on traditional firewall policies [4].

2.3. Secure user access

When signing in for the first time, the local user *admin* is created by default and contains all privileges available to configure the Firepower device. NSA recommends adding *local user* objects, which creates separate, non-administrative accounts with unique usernames for each user. This can be configured as follows: *Objects* > *Users* > *Add Local User* (the '+' button) > Service Types: *RA-VPN* > input new User's Name and Password > *OK*, as shown in the following figure. Notice that the only available *Service Type* option is *RA-VPN* for local users added through this workflow.

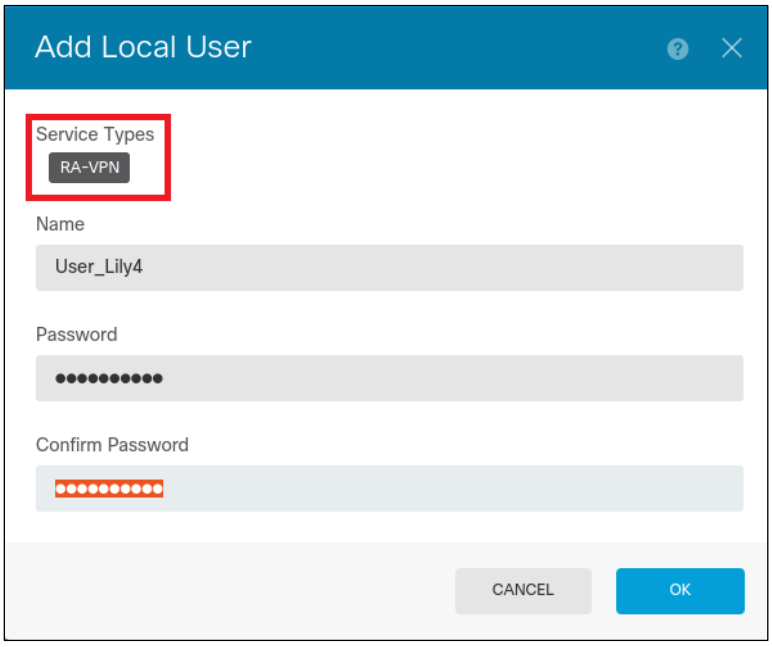

Figure 7: Add local user

The new accounts will limit the users' privileges, preventing them from logging in and accessing the administrative FDM portal, as shown in the following figure:

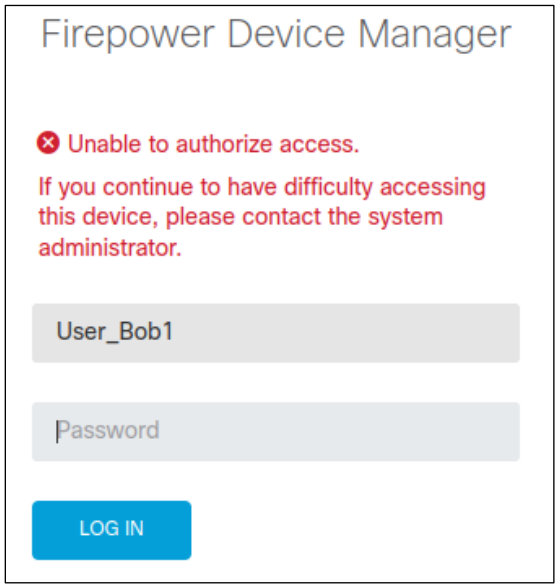

Figure 8: Local user login to FDM

Once the Service Types is configured to RA-VPN, configuring a RADIUS server serves as access protection for the FTD remote access VPN. On the RADIUS server, the different levels of access rights can be provided from a single authentication source as opposed to separate local user accounts.

NSA recommends enabling a RADIUS server for authentication and authorization as well as creating user accounts with appropriate access rights to prevent needing multiple users to log in via the admin account. Whether a user is gaining access through HTTPS or SSH, role-based access control (RBAC) attributes should be updated for the appropriate accounts.

A RADIUS server such as Cisco Identity Services Engine (ISE), allows network administrators to approve access by implementing attributes with authorization policies. Within ISE, go to *Policy* > *Policy Elements* > *Authorization* > *Authorization Profiles*. Within the authorization profile, scroll to *Advanced Attributes Settings* and click on the appropriate attribute with its value.

To provide HTTPS access, NSA recommends defining the *cisco-av-pair* attribute within a user account. The following are supported values for this attribute:

- ***fdm.userrole.authority.ro***: This value only provides *read-only* access. The users can view configurations and dashboards but are unable to make changes.
- ***fdm.userrole.authority.rw*****:** This value provides *read-write* access. These users are able to execute all the actions a *read-only* user can do, but can and also edit and deploy the configuration. These users are restricted to upgrades, viewing the audit logs, creating and restoring backups, and ending user sessions on the device.

- ***fdm.userrole.authority.admin***: This value provides full *administrator* access. These users are able to implement all actions that the local *admin* user is able to do.

To provide RBAC for SSH access, NSA recommends defining the user account attribute as *Service-Type* on the RADIUS server. If a user account does not have this attribute defined on the RADIUS server, SSH access will be denied. The following are values for this attribute:

- ***Administrative (6)***: This value provides *config* access to the CLI. Users with this value are able to use all commands in the CLI.
- ***NAS Prompt (7)* or any value other than *(6)***: Users with this value have basic authorization to the CLI. These users will only be able to use *read-only* commands such as the `show` command.

The password for the *admin* account should be changed to a complex password and stored in a secure storage location. The account should only be used in case of an emergency when no other means of accessing the device are available.

2.4. Restrict configuration privileges

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.

NSA recommends restricting the number of users who will obtain *config* access to the FTD system. Appropriate access levels should be administered depending on the user's role. Decreasing the number of users with *config* access instead of granting all users *config* access, significantly reduces the chances of a compromised system.

2.5. Restrict Linux shell access

CLI access is obtained through the management interface from an SSH connection. 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.

NSA recommends not adding new user accounts directly in the Linux shell, but to instead create new accounts using the `configure user add` command on the FTD CLI. 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.

However, once this command is applied, the results cannot be reversed without a hotfix from the Cisco technical assistance center. Use the command `configure ssh-access-list` in the FTD CLI to limit the number of IP addresses from which the device will accept SSH connections on the management interface.

2.6. Change the password policy for each user

Every user account should contain enforced password and login policies. The *configure user* command, within the FTD CLI, enforces the user's password and login configurations. NSA recommends hardening each user account using the following *configure user* commands. Properly implementing these settings can prevent the system from being compromised through web interface login mechanisms and SSH sessions:

- ***configure user maxfailedlogins***: maximum number of failed logins before a user is locked out.
- ***configure user minpasswdlen***: enforces a minimum password length.
- ***configure user strengthcheck***: enforces strong passwords.
- ***configure user access***: assigns user access privileges based on the user's requirements.
- ***configure user forcereset***: forces the user to reset the password on the next login.

2.7. Enable logging and configure a Syslog server

NSA recommends enabling connection logging and configuring an external syslog server to record traffic and events that may be of interest as traffic passes through the device. The logging configuration for an individual access rule determines whether connection events are created for traffic that matches a specific rule. Logging must be enabled to see events related to the rule in the *Event Viewer*. Logging must also be enabled to match traffic that will be reflected in the dashboards used to monitor the system.

NSA recommends logging events that are critical for analysis, at the discretion of network administrators, but not to log debug and informational traffic that would affect system performance with numerous similar events. For example, logging events of blocked TCP connections for a Denial of Service (DoS) attempt may overwhelm the database with multiple similar events.

For different types of policies, there are additional logging options to log *At Beginning and End of Connection* or *At End of Connection*, as shown in the following figure:

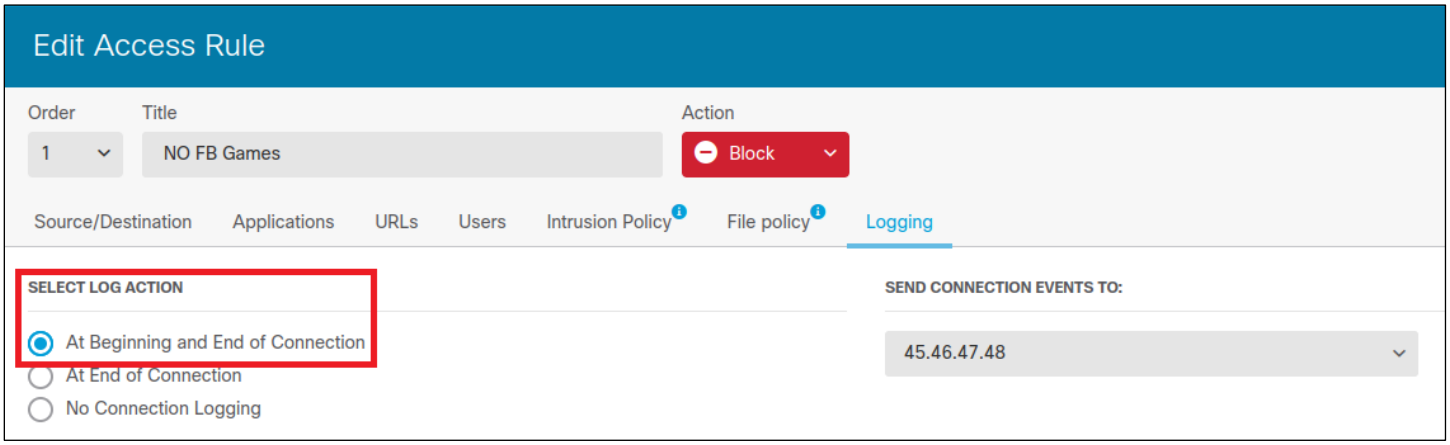

Figure 9: Log action At Beginning and End of Connection

NSA recommends selecting the log action *At Beginning and End of Connection*, which will log blocked traffic at the beginning of a connection and log allowed traffic both at the beginning and end of a connection. Blocked traffic is typically logged at the beginning, since it is denied immediately with no further inspection of the packets. Logging should be set to *End of Connection* when connection logging is enabled in an SSL policy, because the system is unable to determine if the connection is encrypted, using the first packet in the session.

NSA recommends streaming logs to an external source rather than logging on the device itself. Sending events to an external syslog server yields more available disk space on the device and helps maintain the integrity of security logs. This external source creates an extra layer of redundancy, which mitigates the risk of adversaries accessing and manipulating the security logs, covering their tracks. The syslog server must be configured in the intrusion policy settings to send intrusion events to the syslog server. This can be configured as follows: *Device* > *System Settings*: *Logging Settings* > toggle the *Data Logging* switch, as shown in the following figure:

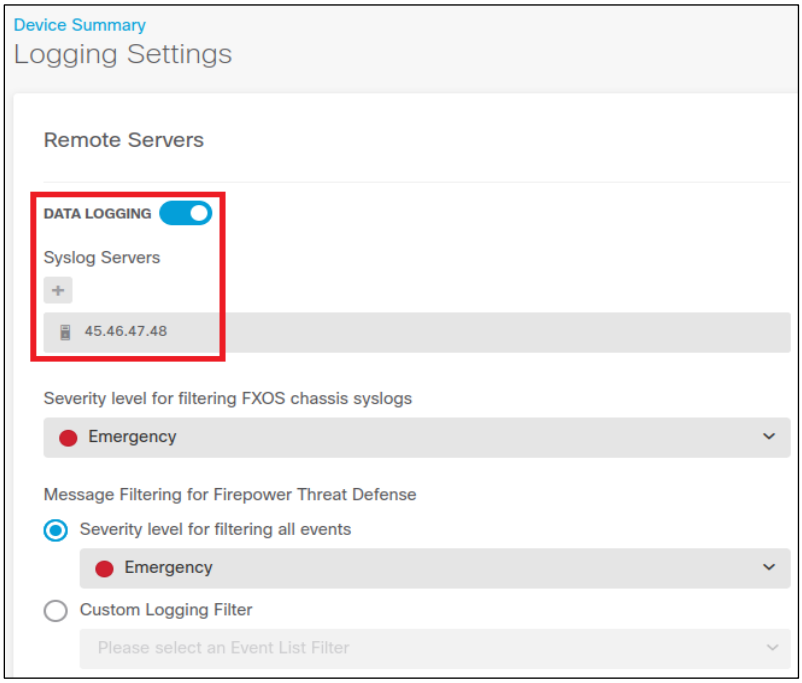

Figure 10: Data logging settings

File and malware events can also be sent to the external syslog server by configuring logging settings; however, the network administrator must first configure file policies on one or more access control rules before file logging can be enabled. This can be configured as follows: *Policies* > *Edit* (pencil icon) > *File Policy* > select either the *Block Malware All* or *Malware Cloud Lookup - No Block* option from the dropdown, as shown in the following figure:

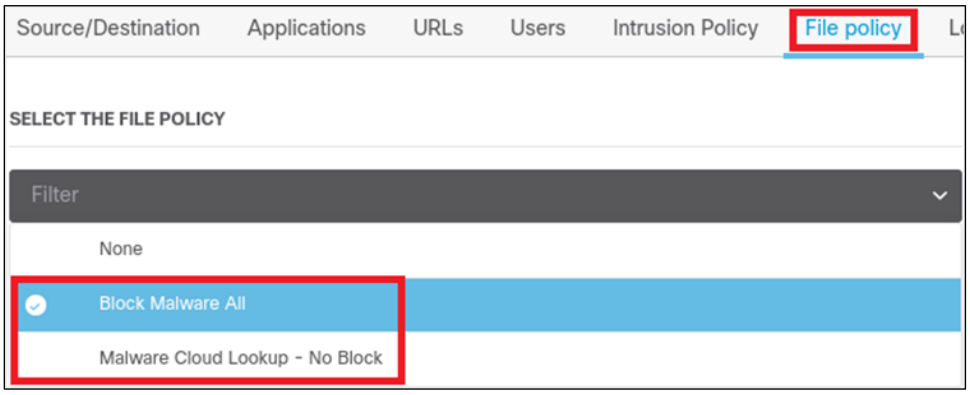

Figure 11: Configure file policy

Still within the *Edit Access Rule* workflow, logging is then enabled as follows: *Logging* (the tab next to *File Policy*) > *File Events* > *Log Files* > *OK*, as shown in the following figure:

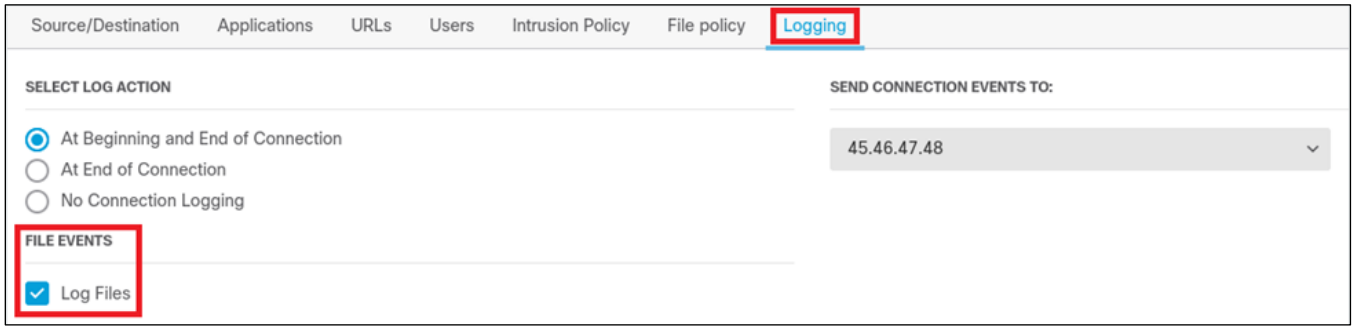

Figure 12: Enable logging

Once the applicable access control rules have been configured, file and malware logging can then be configured as follows: *Device* > *System Settings: Logging Settings* > toggle the *File/Malware Logging* switch > select the applicable *Syslog Server* from the dropdown > *Save*, as shown in the following figures:

Figure 13: Enable file/malware logging

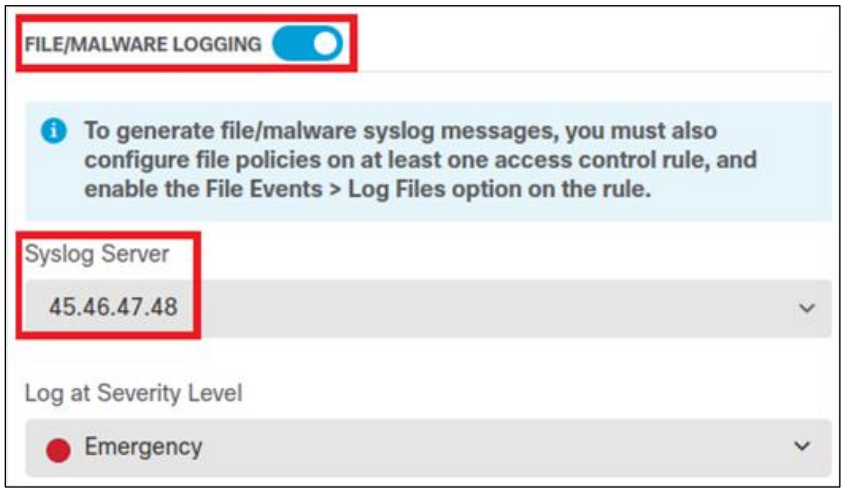

Figure 14: Select Syslog server

2.8. Create identity policies with passive authentication

An identity policy authenticates users by associating an IP address with a username within the system. When a service is permitted or denied for a particular user, that service is applied to the IP address of the associated user.

NSA recommends creating identity policies with passive authentication to link abnormal network behavior directly with individual users. Obtaining user information can be done through either passive or active authentication. Passive authentication is recommended due to the identity source being separate from the FTD device, and allows user identification to be obtained from another authentication service such as an Identity Services Engine (ISE). The system obtains identity mappings based upon the identity sources that were specified. Active authentication is for HTTPS connections only. A username and password is prompted and authenticated against the specified identity source.

To create a passive authentication identity source, the policy would need to be enabled. Once the policy is enabled, *passive authentication* should be specified and ISE should be integrated with the appropriate server, as shown in the following figures:

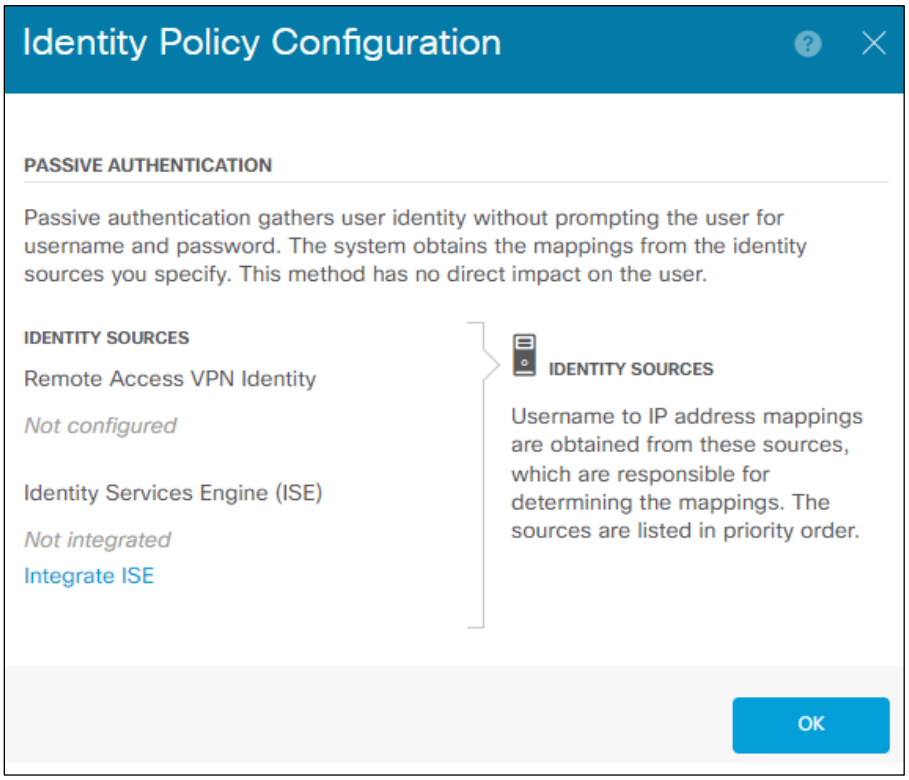

Figure 15: Passive authentication

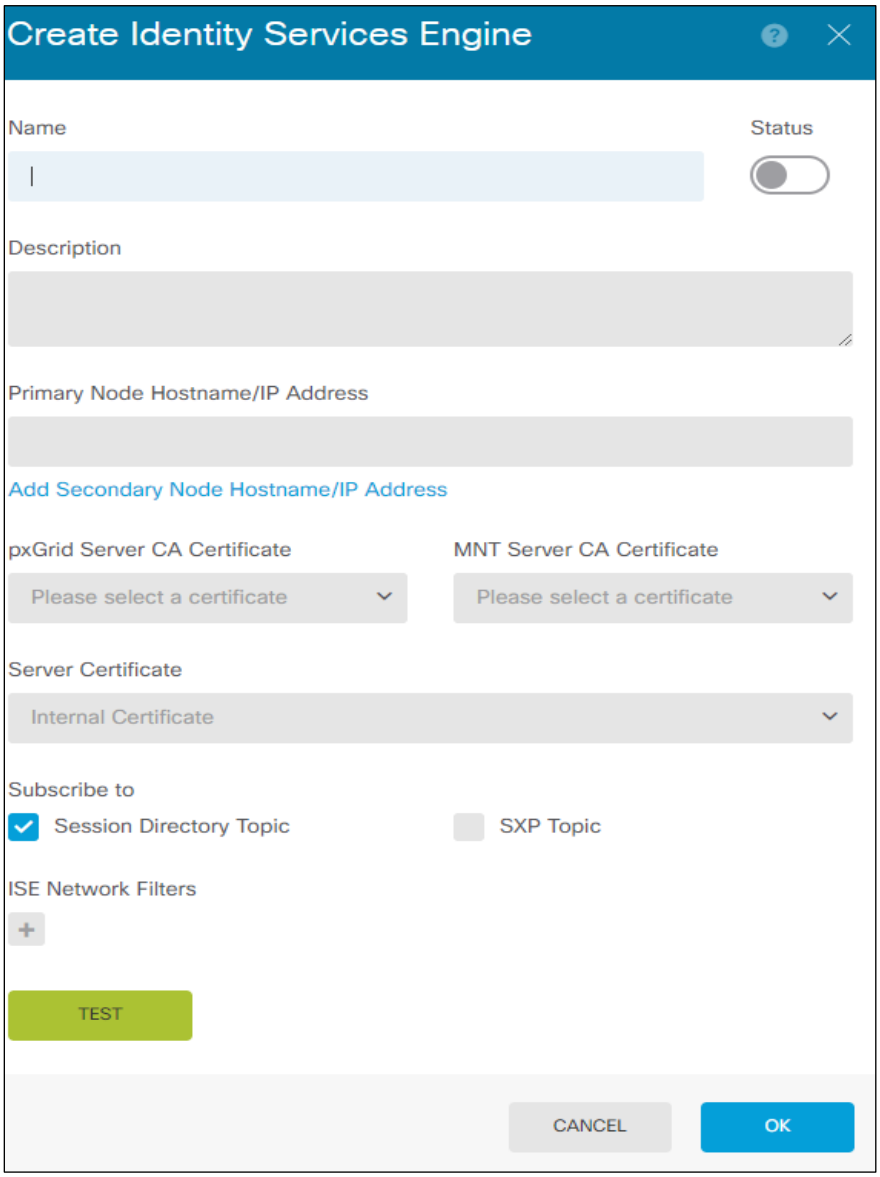

Figure 16: ISE integration

2.9. Disable fragment reassembly

In *Fragment Settings*, the default setting allows up to 24 fragments for each packet and up to 200 fragments awaiting reassembly. Limiting how the device fragments packets can prevent exploitation, such as in a DoS attempt, and prevent extended downtime of critical infrastructure and services. For normal traffic that is fragmented, the system will attempt to reassemble the packets. If the system is able to reassemble the fragmented packets, this traffic will not be dropped. If the packets cannot be reassembled, then the packets will be dropped.

NSA recommends disabling the packet fragment reassembly in FMC and setting the *Chain (fragment)* option to *1* to not fragments. This can be configured as follows: *Devices* > *Platform Settings* > create an

FTD policy > Fragment Settings > set *Chain (Packet)* to '*1*' > *Save and Deploy*, as shown in the following figure:

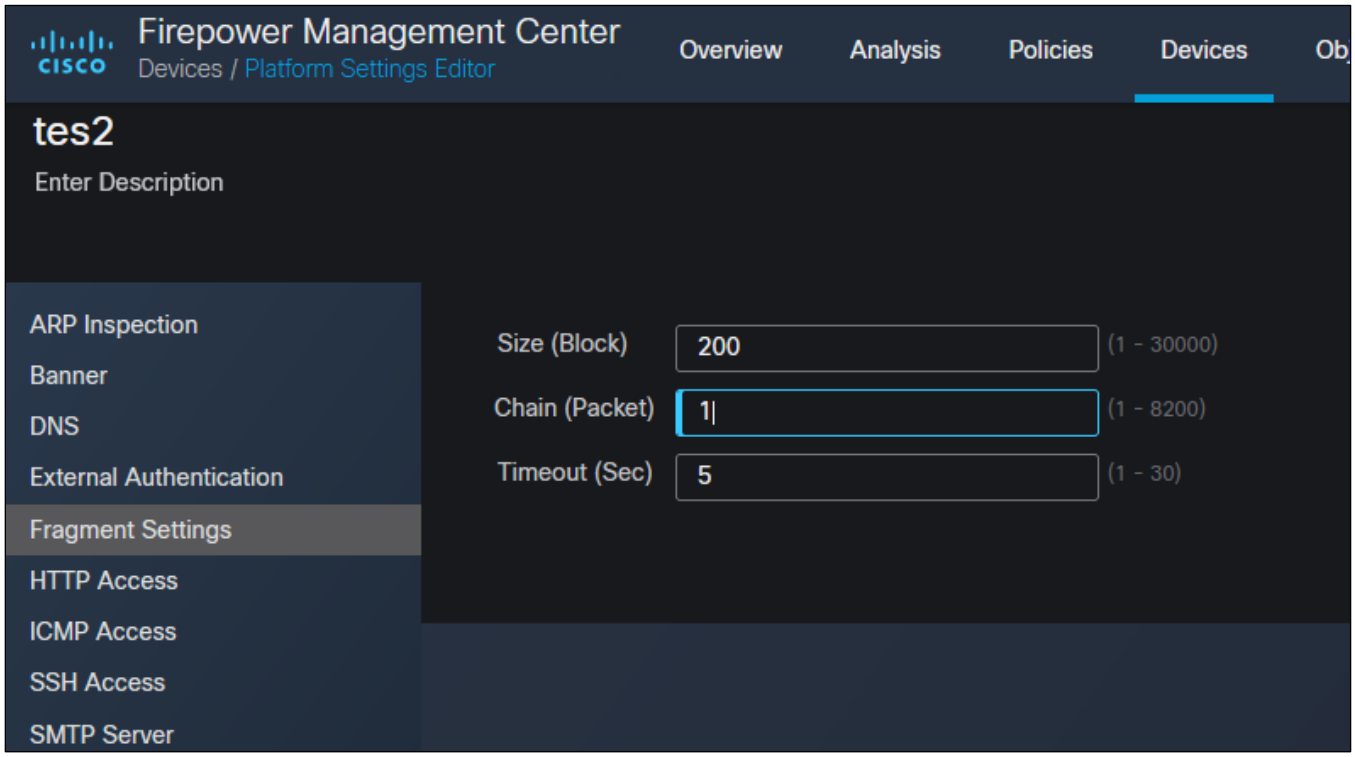

Figure 17: Fragment settings (FMC)

2.10. Enable SNMPv3 access

NSA recommends administrators enable SNMPv3 when using SNMP to monitor the health of FTD. While FTD supports versions 1, 2c, and 3, SNMP version 3 should be the only version used. Only SNMPv3 supports *read-only* users and encryption with AES-256. This means that users can only poll or send SNMP traps for alerts. In FMC, go to *Devices*, then *Platform Settings* and select *SNMP*. Once in the SNMP setting, enable the *SNMP* checkbox, *Enable SNMP Servers*, then configure the below options.

As shown in the following figure, the password for the community string is used by the SNMP management station when sending requests to the FTD device. This password should be unique; contain uppercase and lowercase letters, numbers, and symbols; kept secret; and changed at regular intervals. The security level should be configured to *Priv* when creating SNMP users, which enables authentication and privacy so that SNMP messages are encrypted and authenticated. The type of password encryption should be set to *encrypted* because passwords should not be transmitted without encryption.

The *Auth Algorithm Type* should be set to *SHA-256*, since MD5 was deprecated in 2008 due to both the risk of collisions and it no longer being considered reliable or recommended for use. The *Encryption Type* for the password should be set to *AES-256.* 3DES is a weak encryption algorithm that should not be used, and increases the chance of an adversary decrypting the data.

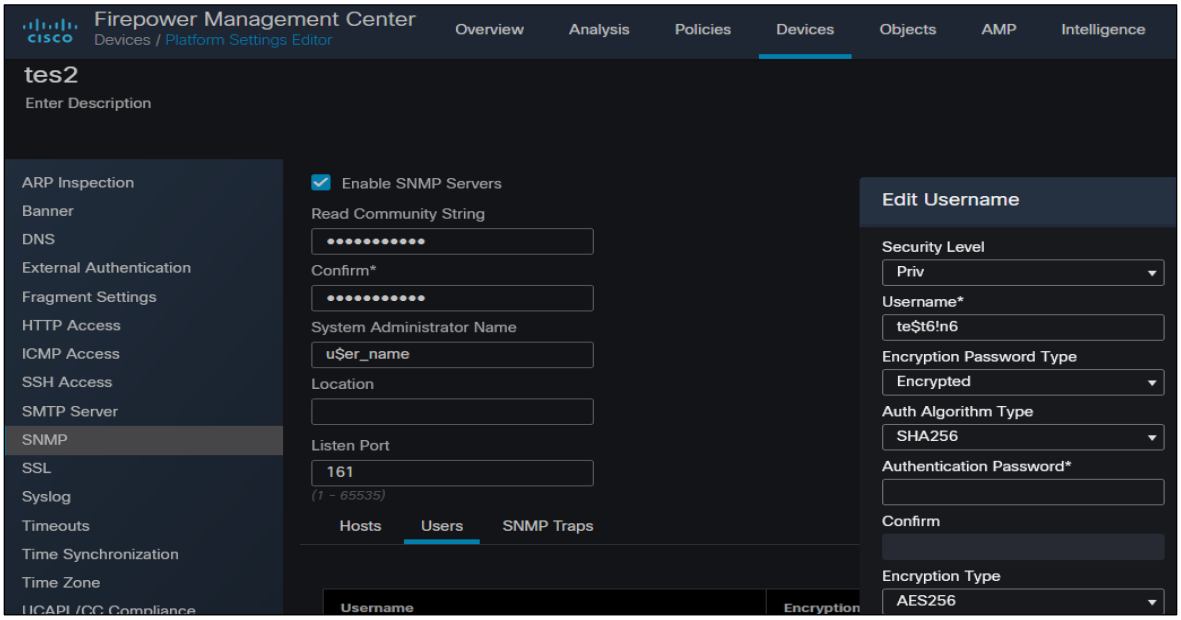

Figure 18: Configure SNMP

The SNMP host entries represent the SNMP management stations that can access the FTD device. As polls and traps are enabled, select *Device Management Interface* when choosing an option on how to reach the device from the SNMP Management Station, as shown in the following figure. This confines access from the management station by the interface instead of by a subnet or security zone.

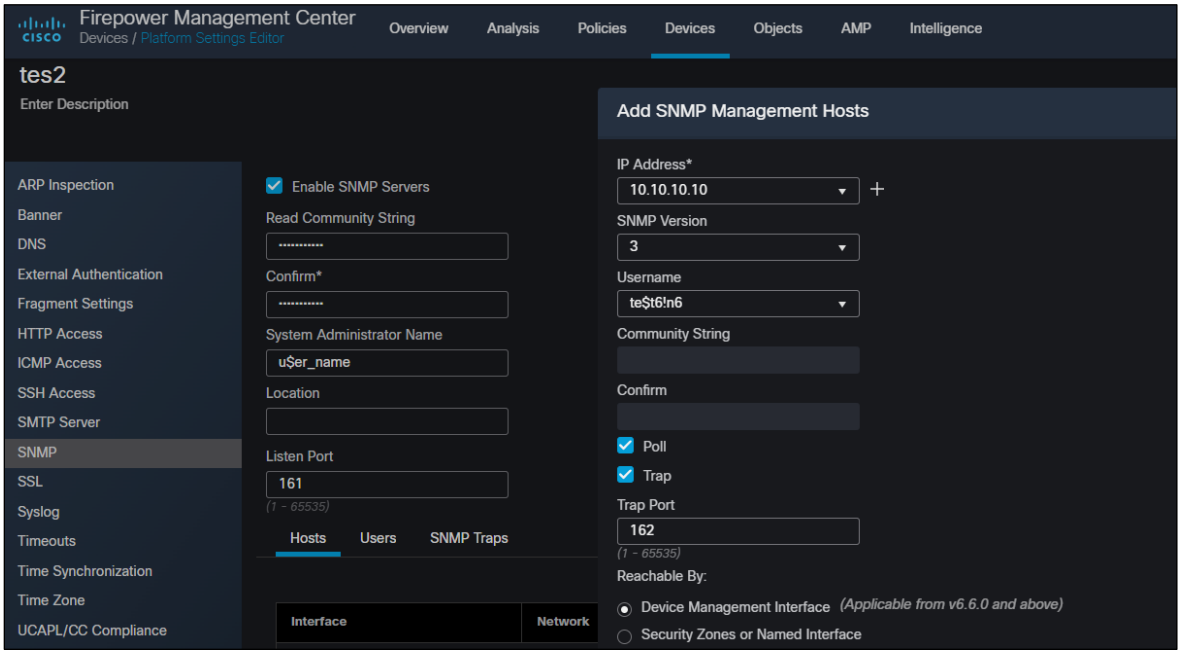

Figure 19: Add SNMP management hosts

2.11. Create application filter objects for efficient policy creation

Application filters can be used to control the flow for multiple applications at a time. An application filter object defines the applications that are used in a connection or a filter-defining application by category, type, tag, business relevance, or risk.

NSA recommends creating application filter objects if multiple policies must include the same group of applications. Applications and filters can be specified directly in each policy, but using objects helps to simplify complex rule creation and helps the system stay within the 50 items per criteria limit.

Application Filters can be configured as follows: *Policies* > *Access Control* > *Edit* (pencil icon) > *Applications* > *Add Application* (the '+' button) > *Advanced Filter*. The user will see pre-defined filter criteria which help filter out specific applications that will be added to the application object, as shown in the following figure:

- ***Risks (1)***: The likelihood of the specific application undermining an organization's security policies. This criteria ranges from *Very Low* to *Very High*.
- ***Business Relevance (2)***: The likelihood of the specific application aligning with the business needs and operations of the organization. This criteria ranges from *Very Low* to *Very High*.
- ***Types (3)***: Defines the type of application which consists of either *Application Protocol*, *Client Protocol*, or *Web Application*.
    - ***Application Protocol***: The communication between hosts (e.g., HTTP, SSH).
    - ***Client Protocol***: Communication from the software, running on the host (e.g., web browsers, email clients).
    - ***Web Application*****:** Content or HTTP / HTTPS traffic from a requested URL.
- ***Categories (4)***: General application classification, describing its most essential functions.
- ***Tags (5)***: Information that describes the application (e.g., for encrypted traffic, only applications tagged with SSL Protocol can be identified and filtered; without the tag, only unencrypted / decrypted traffic can be detected.)

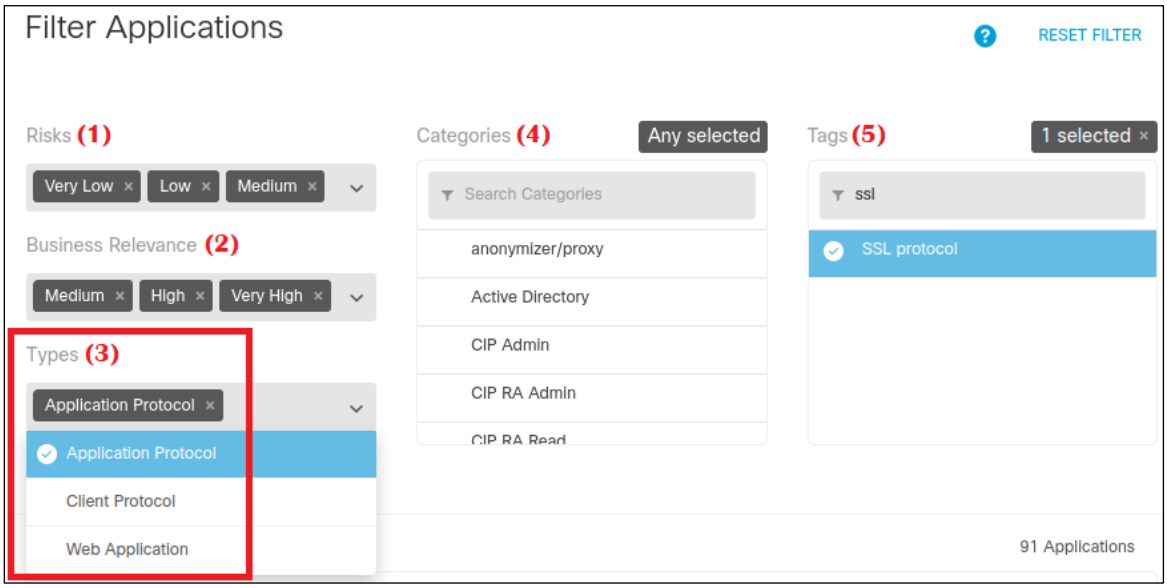

Figure 20: Filter applications (FDM)

FTD provides a search option that helps users identity predefined, available applications. This can be configured from within the *Filter Applications* submenu as shown in the following figures: In the *Filter the list of applications* text box, input the name of the application to be filtered and added to the object > select the desired applications > Add > click on *Save as Filter* > input the desired filter name > *OK*.

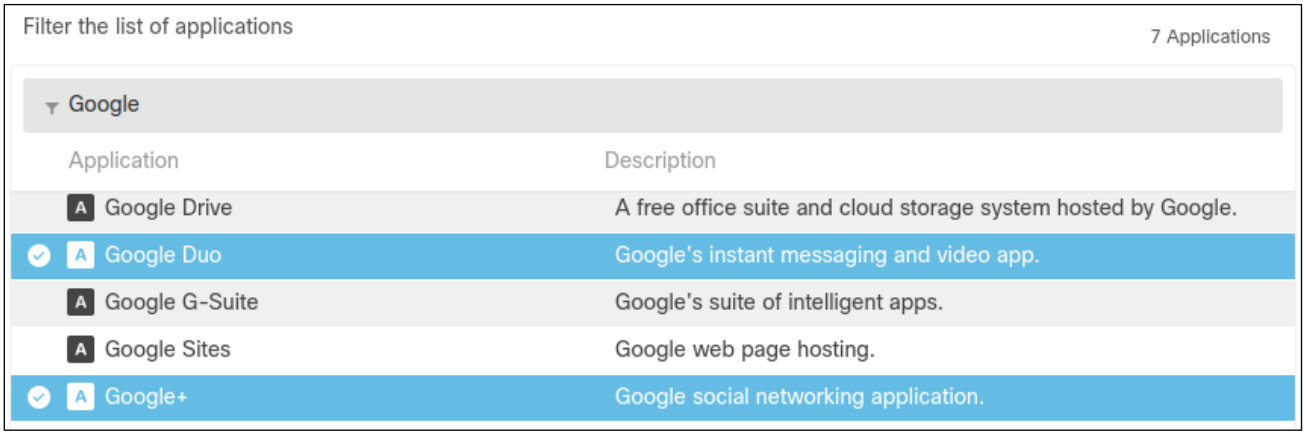

Figure 21: Filter list of applications

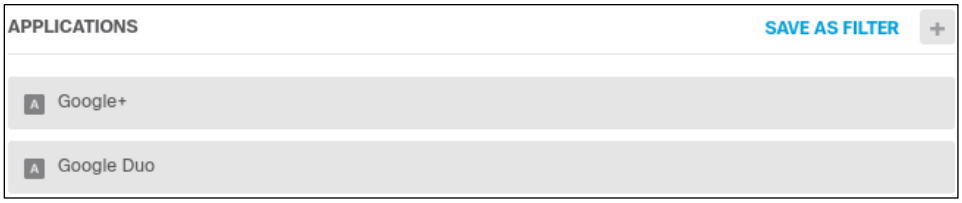

Figure 22: Selected applications

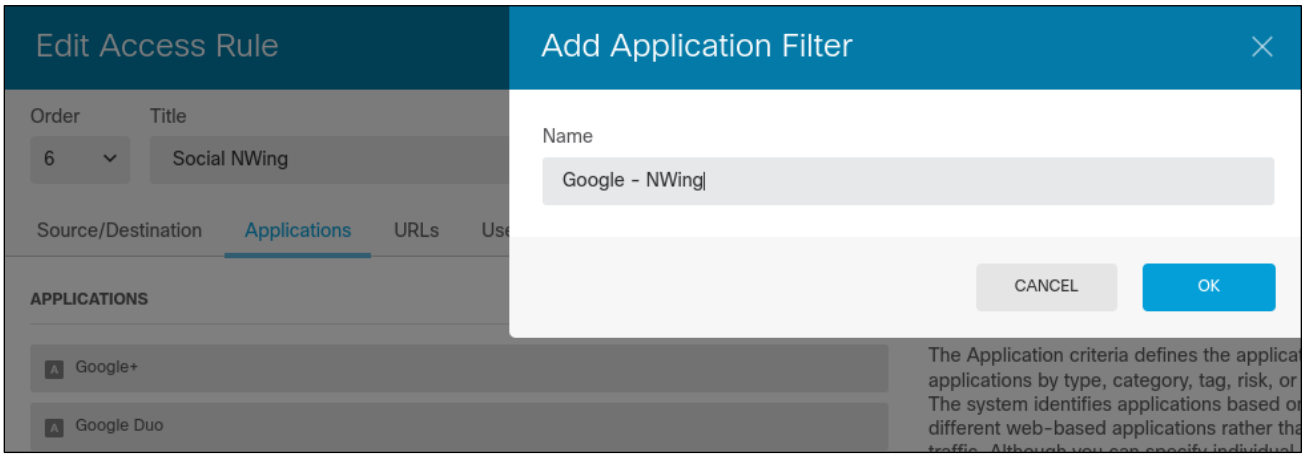

Figure 23: Create application filter

Once the filter name has been saved, it can be applied to other access control rules. In the selected list of *Applications*, the '*A*' icon changes to a filter icon and the list of application names is replaced with the filter name, as shown in the following figure:

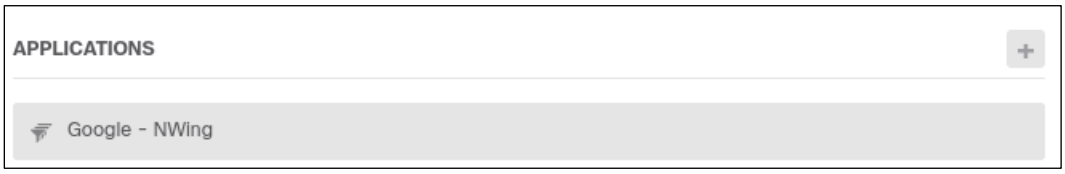

Figure 24: Application filter

This filter can also be edited by accessing *Objects* > *Application Filters* > *Edit* (pencil icon), as shown in the following figure:

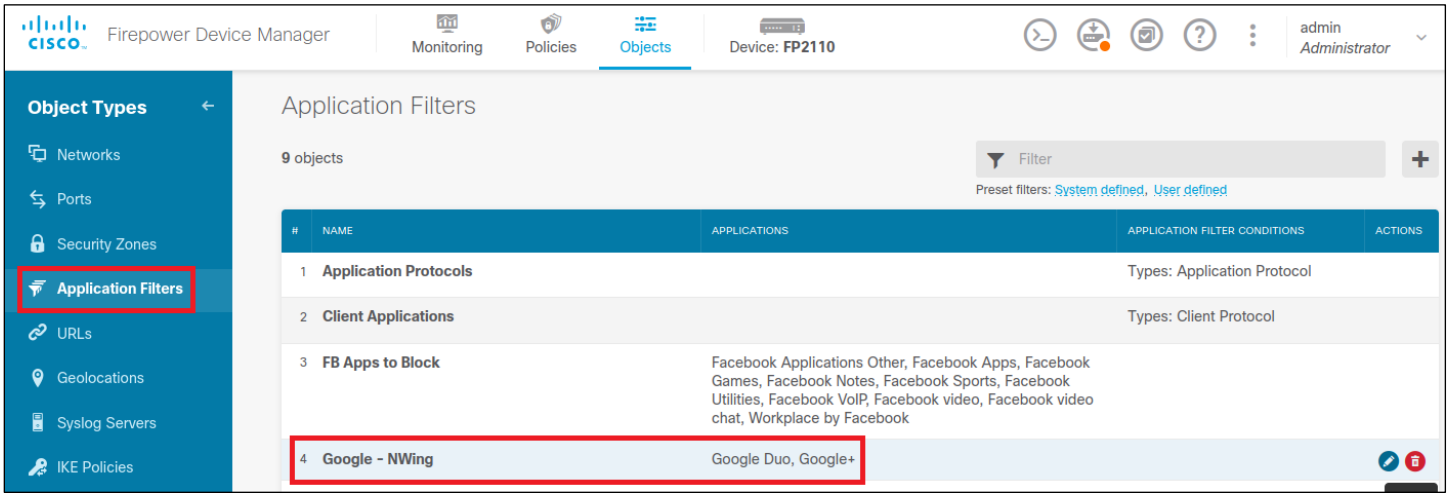

Figure 25: Application filter objects

Application filters can also be applied to access control rules, configured as follows: *Policies* > *Access Control* > *Edit* (pencil icon) > *Applications* > *Add Application* (the '+' button) > *Application Filters* > select the applicable filter(s) > *OK* > *OK*.

Traffic can also be filtered by the URL within an HTTPS or HTTP connection. URL filtering can occur using categories and reputations, which outline a URL's general classification and risk level, respectively. A category classification is a general identification for a URL. For example, *Facebook.com* belongs in the *Social Networking* category and *indeed.com* belongs in the *Job Search* category, but URLs can belong to more than one category.

2.12. Configure URL category reputation

The Cisco Talos Web Reputation Threat Level refers to the risk of visiting a website or an IP address and can range from *Trusted* (exceptional safety) to *Untrusted* (exceptionally bad, malicious, or undesirable) or have an *Unknown* threat level, as shown in the following figure:

NEW THREAT LEVEL	DESCRIPTION
Trusted	Displaying behavior that indicates exceptional safety
Favorable	Displaying behavior that indicates a level of safety
Neutral	Displaying neither positive or negative behavior. However, has been evaluated.
Questionable	Displaying behavior that may indicate risk, or could be undesirable
Untrusted	Displaying behavior that is exceptionally bad, malicious, or undesirable
Unknown	Not previously evaluated, or lacking features to assert a threat level verdict

Figure 26: Web reputation levels (Cisco Talos)

When a category is selected, the default reputation risk is set to *Any and Unknown*, as shown in the following figure:

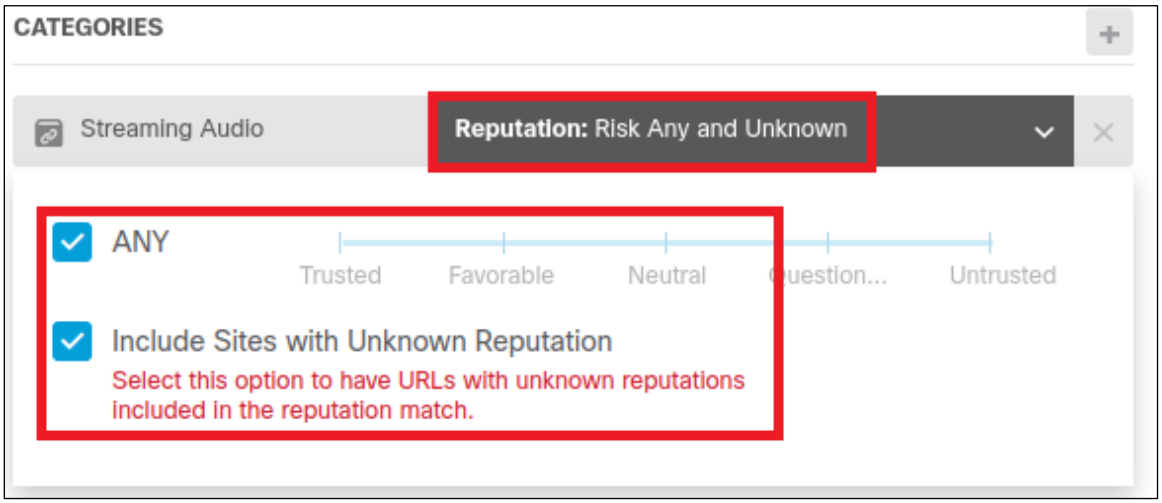

Figure 27: Default reputation risk (FDM)

NSA recommends *unchecking* the *ANY* box (which will automatically uncheck the *Include Sites with Unknown Reputation* box) and selecting the *Trusted* reputation level, as shown in the following figure:

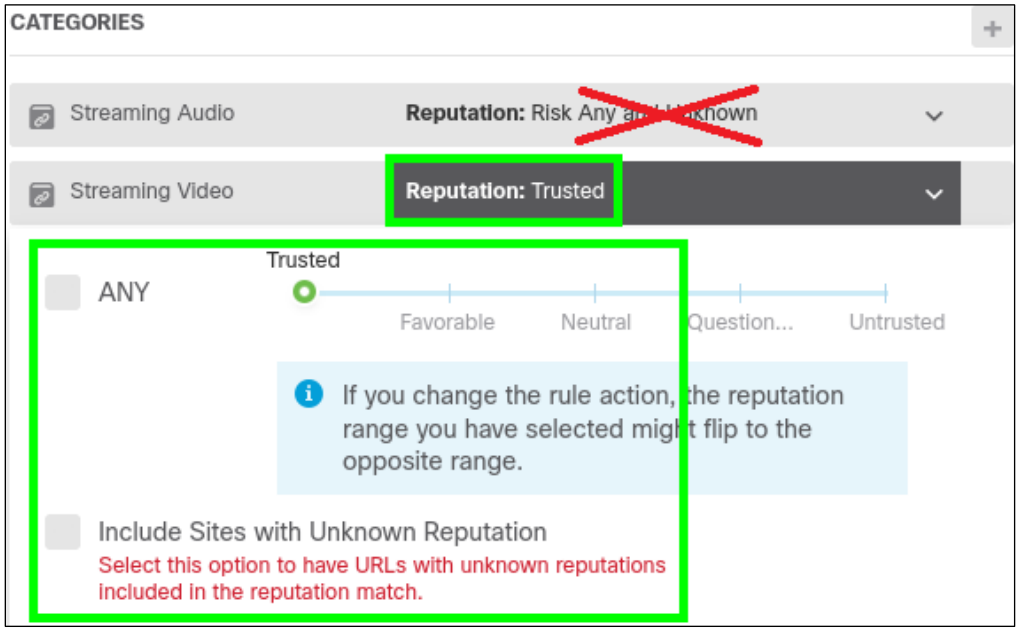

Figure 28: Recommended reputation risk settings

2.13. Enable reputation enforcement on DNS traffic

In DNS request filtering, the system looks up the category and reputation of specific websites when the system sees the DNS lookup request for the fully qualified domain name. If the DNS/URL filtering rule for the returned category/reputation is a *Block* rule within the access control policy, then the system blocks the DNS reply leading to a failed connection attempt.

NSA recommends enabling the *Reputation Enforcement on DNS traffic* option within the access policy settings, as shown in the following figure, to stop connections at the DNS phase. Go to *Access Control*

Policy Settings, and enable the setting by clicking on the button until it turns blue. Enabling this option improves HTTPS traffic filtering which is encrypted. As the control rules match HTTPS traffic, the DNS reply is blocked before the HTTPS connection is started.

Figure 29: Enable reputation enforcement on DNS traffic setting

2.14. Create separate URL filtering mechanism rules for HTTP and HTTPS traffic

As HTTPS traffic is filtered, subdomains within URLs are disregarded when the system determines the subject common name. For example, the URL *yoururlhere.com* should be used instead of the URL *www.yoururlhere.com*. Network administrators should examine the contents of the certificates used by sites to verify that the correct subdomain is used.

When the system is performing URL filtering, the HTTP and HTTPS traffic from the same website are both filtered when access control rules allow or block a specific URL. To distinguish between HTTP and HTTPS traffic from the same website, separate rules must be configured to match the HTTP or HTTPS traffic separately.

NSA recommends creating separate rules to block inbound and outbound HTTP traffic, and to allow authorized HTTPS traffic. This provides greater control and restrictions over the network accessing unencrypted protocols.

Creating a *Block HTTP* traffic rule can be configured as follows: *Policies* > *Access Control* > *Add Rule* (the '+' button) > Action: *Block* > add the applicable Zones and Networks for the Source and Destination traffic > add *HTTP* as the destination port to be blocked > *OK*, as shown in the following figure:

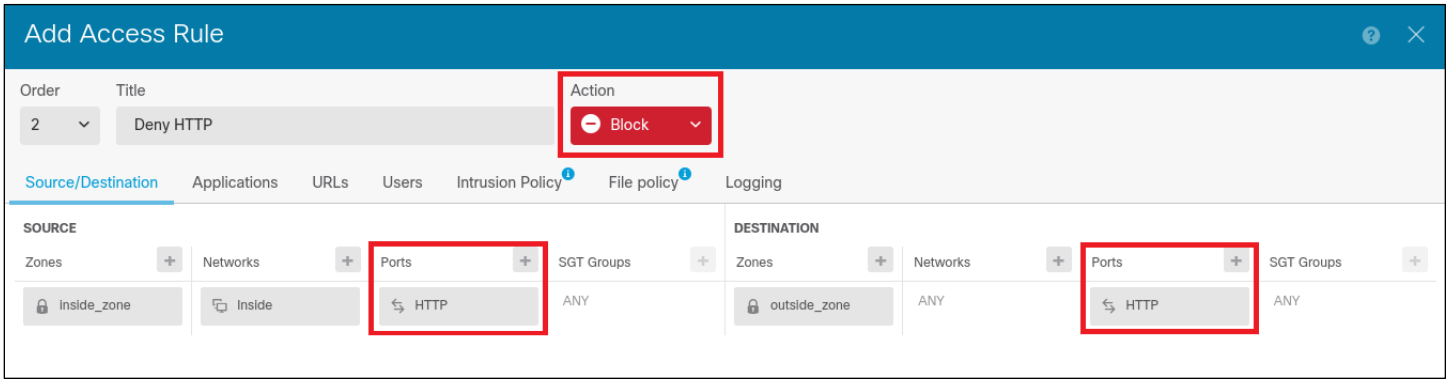

Figure 30: Select ports for block access rule

Similarly, an *Allow HTTPS* rule can be configured as shown in the following figure: *Policies* > *Access Control* > *Add Rule* (the '+' button) > Action: *Allow* > add the applicable Zones and Networks for the Source and Destination traffic > add *HTTPS* as the destination port to be permitted > *OK*.

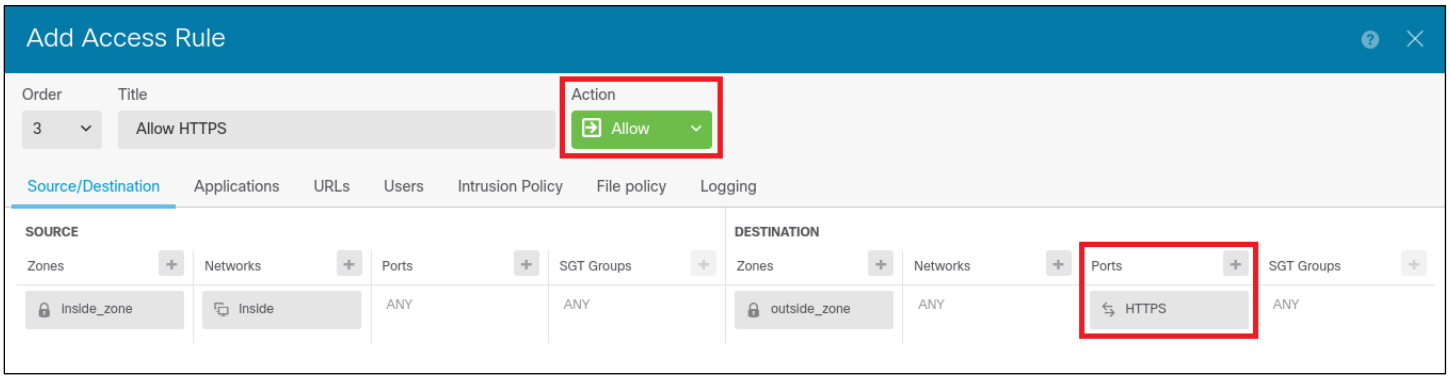

Figure 31: Create Allow access rule

An alternate method of configuring a *Block HTTP* rule is to select *HTTP* as an Application. This can be configured as shown in the following figure: *Policies* > *Access Control* > *Add Rule* (the '+' button) > Action: *Block* > add the applicable Zones and Networks for the Source and Destination traffic > click on the *Applications* tab > *Add application* (the '+' button) > select *HTTP* from the dropdown > *OK* > *OK*.

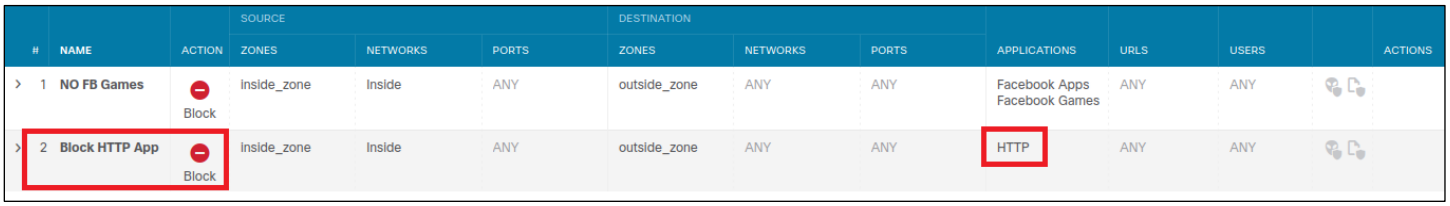

Figure 32: Select application for block access rule

2.15. Create separate access control policy rules for URL and application filtering

NSA recommends creating separate application and URL access control policy rules. Combining both URL and application criteria in the same rule can cause the unintended result of the rule not functioning, permitting undesirable traffic to pass through the network. URL filtering rules block specific web servers, whereas application filtering rules target specific applications regardless of the web server.

2.16. Configure the URL time to live

The *URL Time to Live* (TTL) duration determines how long to cache URL category and lookup values before a new category and reputation lookup is executed. This option is enabled when the *Query Cisco CSI for Unknown URLs* option is selected, which can be configured by navigating to: *Device* > System Settings: *See more* > *URL Filtering Preferences* > Click on *Query Cisco CSI for Unknown URLs*, as shown in the following figure.

The option *Query Cisco CSI for Unknown URLs* is used for URLs with neither a reputation nor a category classification in the URL filtering database. If lookup results return reputation or category results, they will be used when URL conditions are processed within their respective access rules. This option should be enabled to label URLs with a category and reputation, and use the URL TTL.

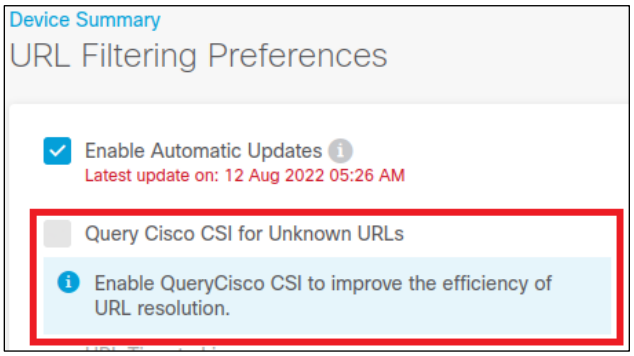

Figure 33: Enable Query Cisco CSI for Unknown URLs option

A shorter TTL duration produces more accurate URL filtering results and a longer duration yields better performance for *Unknown* URLs. NSA recommends changing the TTL from the default setting *Never,* to an option that provides a balance between accurate filtering and better performance, as shown in the following figure. If accurate filtering is a priority, administrators should increase the TTL to a longer time which extends up to a week. If performance is not a concern then administrators are encouraged to shorten this TTL according to their network requirements.

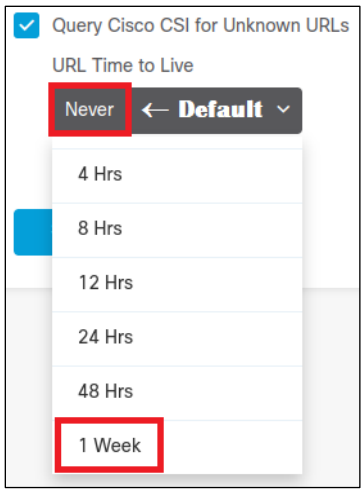

Figure 34: Time to Live (TTL) setting

3. Implementing intrusion prevention policies

IDS or IPS inspection on traffic is controlled by intrusion policies. These policies inherit settings from one of the four Cisco Talos base policy templates: *Balanced Security and Connectivity*, *Connectivity over Security*, *Maximum Detection*, and *Security over Connectivity*, as shown in the following figure:

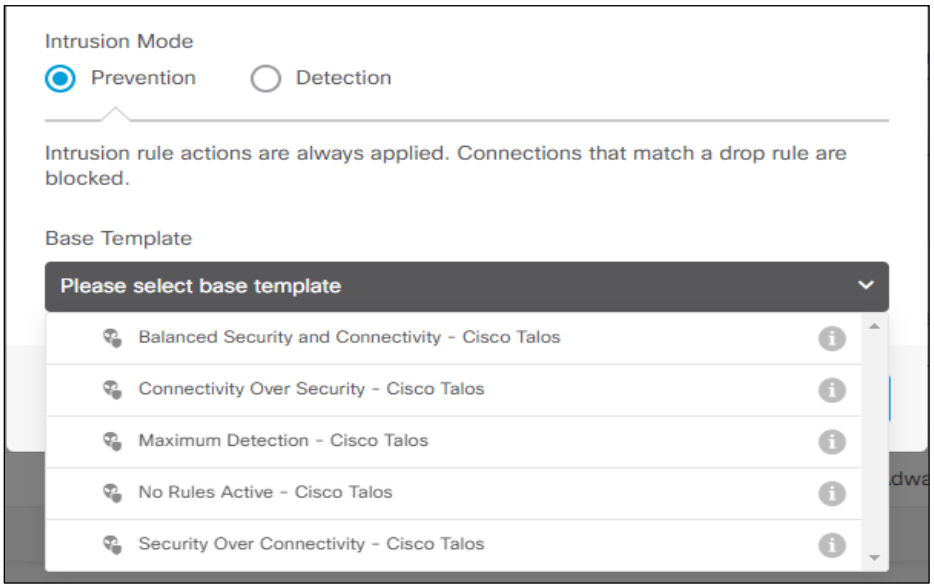

Figure 35: Intrusion Prevention base template options

Individual rules within policies can be configured to generate events, drop traffic and generate events, or be disabled. Rules can also be grouped for easier configuration and management, and deep packet inspection is performed by the engine from pattern matching. Snort is the main inspection engine for the system and the rules within the policies are a collection of Snort rules evaluated against traffic flows.

3.1. Implement "Balanced Security and Connectivity" as a base policy

The Firepower contains combined intrusion and network analysis-based policies that enable the system to preprocess and handle traffic. NSA recommends the network analysis base policy to be *Balanced Security and Connectivity*, which attempts to keep users secure while not being too aggressive and possibly dropping normal traffic. The other base policies contain an emphasis on network infrastructure over security and connectivity.

Once the base policy is chosen, administrators are able to modify rules within the intrusion policy. The action for each rule can be changed to alert, drop, or disable depending on network requirements. Custom rules can also be uploaded and applied to an intrusion policy based on traffic analysis. The security level for each subgroup can be modified within each intrusion policy to enforce rule processing so connectivity or security is emphasized in the network. Rules are organized into various signature groups with respect to intrusion type. Each group has subgroups that contain the signatures and an action of alert, drop, or disable. The security level for each subgroup can also be modified to enforce the rule groups.

4. Implementing SSL policies

Secure Socket Layer (SSL) policies control inspection and decryption of encrypted traffic. SSL decryption within the device mostly targets Transport Layer Security (TLS). The three components of SSL decryption are a TLS proxy, the session setup, and the application data. The session setup involves the asymmetric key while the application data involves the symmetric key for encryption/decryption. The actions related to

this policy include decrypt - resign, decrypt - known key, do not decrypt, block, block with reset, and monitor. The encryption/decryption is only available on hardware for ASA 5525-X, 5555-X, 5545-X, Firepower 2100, 4100, and 9300 series versions 6.2.3 and up.

4.1. Enable TLS server identity discovery

Decrypting traffic from the Internet presents a number of issues as this traffic is coming inbound to the internal network. Within network traffic, even when not decrypting traffic, the certificate is required to match application and URL filtering criteria in the access control rule.

NSA recommends enabling the TLS Server Identity Discovery option to enable policy enforcement without affecting performance or risking compliance, as with full decryption [5]. Go to access policy Settings and click on the TLS Server Identity Discovery button. Once this option is enabled, as shown in the following figure, the device will identify the server's certificate without decrypting the entire session. This allows encrypted connections to match the correct access control rules.

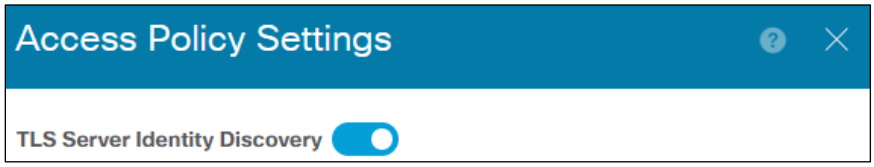

Figure 36: Enable TLS Server Identity Discovery setting

4.2. Decrypt specific traffic instead of all traffic

It is easier to process traffic when there is no encryption or obfuscation. Unlike plaintext traffic, encrypted connections, such as HTTPS, cannot be examined fully by network administrators. Since most legitimate connections are encrypted, adversaries can hide harmful traffic within encrypted traffic.

NSA recommends using the *Decrypt - Resign* action to inspect encrypted traffic when decrypting. The system re-signs the certificate of the website once traffic matches the rule. Separate sessions for decryption and re-encryption are created with respective cryptographic connections. Certificate objects and ciphers added to the policy must also match the CA certificate and encryption algorithm. If objects and ciphers do not match, encryption and decryption will be unsuccessful. Decrypting all traffic will hinder performance on the device. Depending on the flow of traffic within the network, only decrypt abnormal traffic outgoing from the internal network or other traffic that may be of interest. Select *Decrypt Re-Sign* from the action list when creating an SSL rule, as shown in the following figure:

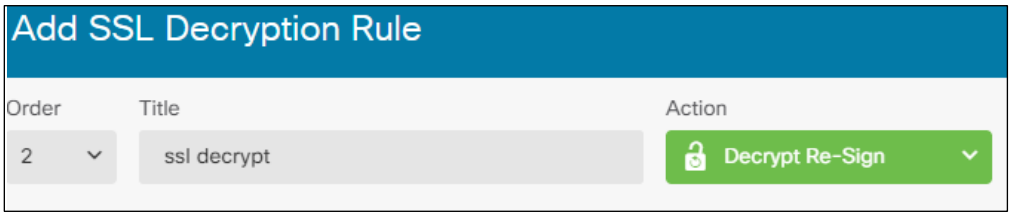

Figure 37: Create SSL Decryption Rule

5. Implementing malware and file policies

File and malware policies indicate the type of files that are allowed, blocked, or inspected from all types of traffic that pass through the device. Different actions available for incoming files are detect files, block files, malware cloud lookup, and block malware. When files and malware are to be inspected, this includes static, dynamic, and local analysis. Below are a few guidelines when configuring these policies.

5.1. Enable reset connection

File or malware policies contain rules that involve blocking harmful files and malware. In FMC, under the action criteria, there are other options as to what should be done after those harmful files or malware are blocked as seen below.

NSA recommends enabling the *reset connection* option under the action, which will prevent a blocked application session from remaining open, as shown in *Figure 15*. If the connection is not reset, the session can remain open and connected. This setting resets the TCP connection and prevents malicious actions from an unauthorized host.

5.2. Do not store all files within local storage

High volume within a network increases the chances of encountering malicious files or executables. The system stores files or malware for further analysis that match criteria within a rule. NSA recommends not to store all of the files for analysis on the device. Storing all files on the system will not only affect storage space, but system performance can be affected as well.

As shown in the following figure, enabling the *Store Files* options allows the system to allocate space on the device's hard drive to store those files. Once the space on the hard drive is at capacity, the system begins to delete the oldest set of files first. This will continue until the threshold for adequate hard drive space is reached. An alternative to permanently storing captured files on the device's hard drive is to download the files from the device's file storage to another protected system for further manual analysis. Another option is to submit captured files to the AMP cloud lookup service for dynamic analysis.

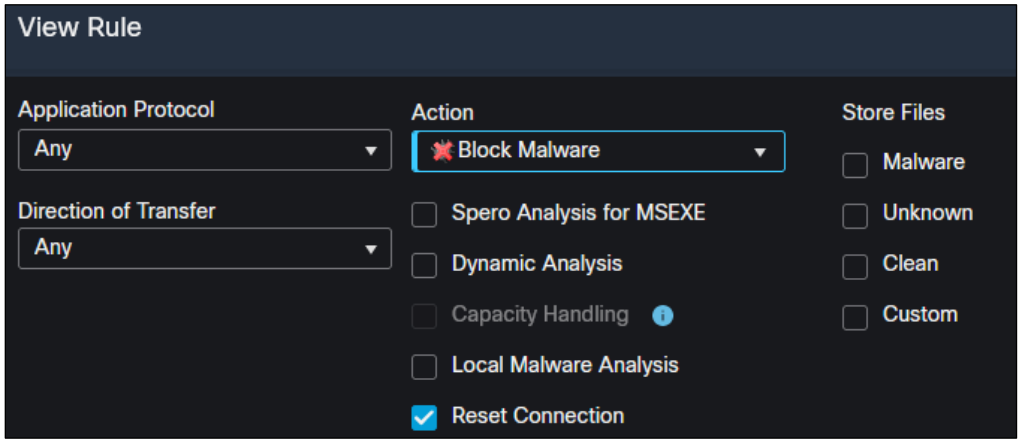

Figure 38: Configure Store Files options (FMC)

6. Enabling secure VPN settings

6.1. Use secure VPN tunneling protocols

The most secure protocol and strong encryption algorithms should be chosen when creating a VPN with this device. NSA recommends using the Internet Key Exchange (IKE) version 2 (IKEv2) key management protocol due to the IPsec and Security Association (SA) standards that allow a more secure connection by encrypting data between clients [6]. IKEv1 should be disabled due to implementation of insecure hashing and encryption algorithms [7]. 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 [8]. The IPsec proposal should include AES-256 or AES-GCM-256 encryption, SHA-384 or SHA-512 integrity hash, and an authentication type of Certificate [9].

7. Hardening FXOS

The Firepower device runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS), on top of which is the FTD image installed as a container. To prevent possible exploitation of known vulnerabilities, FXOS should be updated to the most recent version and configured so that only authorized users have management access. The following configurations show the NSA recommended baseline for SSH, HTTPS, and TLS access encryption and hashing algorithms.

7.1. Configure strong SSH algorithms

SSHv2 should be configured to the strongest algorithms for authorized users connecting to FXOS, as shown in the following figures. The commands are executed in the FXOS CLI, which puts the device in the system services mode and enables SSH.

Once the SSH server is enabled and the working directory has been placed in system services mode, NSA recommends configuring the SSHv2 encryption algorithm AES-CTR-256, following NSA and NIST guidance to retire the use of the deprecated 3DES-CBC algorithm. This configuration should be enabled on both the server and client to ensure a strong SSH encryption algorithm, as shown in the following figures:

```
> connect fxos
Firepower-module#
Firepower-module# scope system
Firepower-module /system# scope services
Firepower-module /system/services# enable ssh-server
Firepower-module /system/services#
```

Figure 39: Enable SSH

```
Firepower-module /system/services# set ssh-server encrypt-algorithm aes256-ctr
Firepower-module /system/services# set ssh-client encrypt-algorithm aes256-ctr
```

Figure 40: Configure AES-CTR-256 encryption

At a minimum, NSA recommends using the *diffie-hellman-group14-sha1* key exchange algorithm. This algorithm may be implemented to exchange a secure session with most devices [10]. The configuration in the following figure shows the commands to execute for both server and client.

```
Firepower-module /system/services# set ssh-server kex-algorithm diffie-hellman-group14-sha1
Firepower-module /system/services# set ssh-client kex-algorithm diffie-hellman-group14-sha1
```

Figure 41: Configure Diffie-Hellman key exchange algorithm

In order to verify data integrity within SSH, a Hash-based Message Authentication Code (HMAC) method must be specified to ensure both sender identity and that the message was not modified during transit. NSA recommends configuring the HMAC-SHA2-512 algorithm for both server and client, as shown in the following figure:

```
Firepower-module /system/services# set ssh-server mac-algorithm hmac-sha2-512
Firepower-module /system/services# set ssh-server mac-algorithm hmac-sha2-512
```

Figure 42: Configure HMAC algorithm

NSA recommends configuring an RSA host key of 3072 bits and a key ring maximum volume limit of 500,000, as showing in the following figures. A larger key modulus size makes it harder for adversaries to be able to derive the key, and each encryption key is used to protect no more than half a gigabyte of data. Rekeying occurs once this threshold is reached.

```
Firepower-module /system/services# set ssh-server host-key rsa 3072
Firepower-module /system/services# set ssh-client host-key rsa 3072
```

Figure 43: Configure RSA host key

```
Firepower-module /system/services# set ssh-server rekey-limit volume 500000
Firepower-module /system/services# set ssh-client rekey-limit volume 500000
```

Figure 44: Configure rekey limit

NSA recommends configuring a time limit of 60 minutes to prevent having an idle SSH session for long periods of time, as shown in the following figure. Once the time limit has been reached, FXOS disconnects the SSH session, and a rekey of session keys are generated

```
Firepower-module /system/services# set ssh-server rekey-limit time 60
Firepower-module /system/services# set ssh-client rekey-limit time 60
```

Figure 45: Configure rekey time limit

NSA recommends enabling a strict host key check to control SSH host key checking, as shown in the following figure. Enabling this option allows the system to reject a connection if the host key is not in the FXOS known host file.

```
Firepower-module /system/services# set ssh-client stricthostkeycheck enable
```

Figure 46: Configure strict host keycheck

NSA recommends configuring trusted subnets or hosts for SSH access with FXOS, as shown in the following figure. Known hosts or subnets should be configured to maintain strict limits on hosts that will have SSH access to FXOS.

```
Firepower-module /system/services# enter ip-block {ip_address} {prefix_length} ssh
```

Figure 47: Configure trusted hosts or subnets within the FXOS SSH known host file

7.2. Configure key ring

NSA recommends creating key rings of a minimum of 3072 bits. Including the default key ring, FXOS supports up to eight key rings. To create the HTTPS key rings, navigate to security mode and key in the commands as shown in the following figure:

```
Firepower-module# scope security
Firepower-module /security# create keyring {key_ring_name}
Firepower-module /security/keyring# set modulus mod3072
Firepower-module /security/keyring# commit-buffer
```

Figure 48: Configure key rings

While FXOS comes with a default key ring, NSA recommends regenerating the key ring if the certificate expires or the cluster name changes, as shown in the following figure:

```
Firepower-module /security # scope keyring default
Firepower-module /security/keyring# set regenerate yes
Firepower-module # commit-buffer
```

Figure 49: Configure key ring regeneration

NSA recommends creating a certificate request for a key ring to prepare for secure communications. In case the keys become compromised, a certificate authority (CA) and certificate revocation list (CRL) is also recommended, as this would allow the keys to be revoked, preventing them from being used. Usually devices contain a self-signed certificate which is not automatically trusted by other devices. A user's browser may display an authentication warning due to this self-signed certificate. Creating a new certificate from a CA allows devices to trust appropriate certificates and allow for secure and trusted communications.

Once the certificate has been generated, copy the text, including the BEGIN and END lines, and save this to a file. The file should be sent to a trusted certificate authority to obtain a certificate for the key ring. Then, create a trusted point containing the certificate chain for the key ring certificate, as shown in the following figure:

```
Firepower-module /security # scope keyring {keyring_name}
Firepower-module /security/keyring# create certreq ip {ipv4 or ipv6 address} subject-name {name}
Certificate request password:
Confirm certificate request password:
Firepower-module /security/keyring# commit-buffer
Certificate request subject name: {name}
…
-----BEGIN CERTIFICATE REQUEST-----
…..
-----END CERTIFICATE REQUEST-----

Firepower-module /security # create trustpoint {name_of_trustpoint]
Firepower-module /security /trustpoint# set certchain
Enter lines one at a time. Enter ENDOBUF to finish. Press ^C to abort
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIISDFNUSSDFIUNISUDNFKIBSEUIFBOSUEFHOSEHFOISEFSOEIJFOISEJ
>…
> -----END CERTIFICATE -----
> ENDOBUF
Firepower-module /security /trustpoint# commit-buffer
```

Figure 50: Create certificate request for key ring

7.3. Configure HTTPS options for secure communication

HTTPS uses Public Key Infrastructure (PKI) to create secure communication between the Firepower chassis and a user's browser. Before secure communication can take place, key rings and certificates must be created for devices on both ends to create trusted points and a secure channel. Once the certificates and trusted points are created, HTTPS is enabled and the previously created key ring is used.

NSA recommends configuring trusted subnets or hosts for HTTPS access with FXOS. Known hosts or subnets should be configured to maintain a strict limits on hosts that will have HTTPS access to FXOS.

```
Firepower-module /system/services# enter ip-block {ip_address} {prefix_length} https
Firepower-module /system/services# commit-buffer
```

Figure 51: Configure trusted hosts or subnets within the FXOS HTTPS known host file

7.4. Configure TLS to the latest versions

The Transport Layer Security (TLS) protocol provides data integrity and privacy between two communicating applications. The minimum TLS version configured in FXOS ensures external devices must also be configured with the same TLS version to open an HTTPS connection with FXOS. The device will also communicate with higher version levels, if both parties in the communication support the configured level.

Although the FXOS minimum default TLS version is 1.1, NSA recommends setting the minimum configuration to TLS 1.2, which allows the use of more secure hash algorithms and advanced cipher suites. TLS version 1.3 is also available and does not support many of the vulnerable cryptographic algorithms that TLS 1.2 can be configured to allow and often allows by default, thus making it more

secure by default. To configure the TLS version within FXOS, navigate to system mode as shown in the following figure:

```
Firepower-module /system# set services tls-ver v1_2
```

Figure 52: Configure TLS to the latest version

8. Works cited

[1] Cisco, "Introducing new Cisco Secure product names," 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/security/secure-names.html#~products. [Accessed 25 May 2023].

[2] Cisco, "Cisco Firepower 4100/9300 FXOS Compatibility," 1 December 2015. [Online]. Available: https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html. [Accessed 25 May 2023].

[3] Cisco, "Cisco Secure - Products, Solutions, and Platform," 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/security/secure-names.html#~products. [Accessed 25 May 2023].

[4] NIST, "Guidelines on Firewalls and Firewall Policy," September 2009. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf. [Accessed 25 May 2023].

[5] National Security Agency, "Managing Risk from Transport Layer Security Inspection," 16 December 2019. [Online]. Available: https://media.defense.gov/2019/Dec/16/2002225460/-1/-1/0/info%20sheet%20%20managing%20risk%20from%20transport%20layer%20security%20inspection.pdf. [Accessed 7 March 2023].

[6] National Security Agency, "Securing IPsec Virtual Private Networks," October 2020. [Online]. Available: https://media.defense.gov/2021/Sep/16/2002855930/-1/-1/0/securing_ipsec_virtual_private_networks_executive_summary_2020_07_01_final_release.pdf. [Accessed 7 March 2023].

[7] E. P. Wouters, "RFC 9395 Deprecation of the Internet Key Exchange Version (IKEv1) Protocol and Obselete Algorithms," April 2023. [Online]. Available: https://www.ietf.org/rfc/rfc9395.html. [Accessed June 2023].

[8] National Security Agency, "Commercial National Security Algorithm Suite 2.0," Spetember 2022. [Online]. Available: Avalilable: https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.pdf. [Accessed June 2023].

[9] National Security Agency, "RFC 9206 Commercial National Security Algorithm (CNSA) Suite Cryptography for Internet Protocol Security (IPsec)," February 2022. [Online]. Available: https://www.rfc-editor.org/rfc/rfc9206.pdf. [Accessed June 2023].

[10] M. Baushke, "Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH)," January 2022. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc9142. [Accessed July 2023].