

Firewall Bible
FMC/FTD 7.0.1

Setting up FMC + FMC configuration

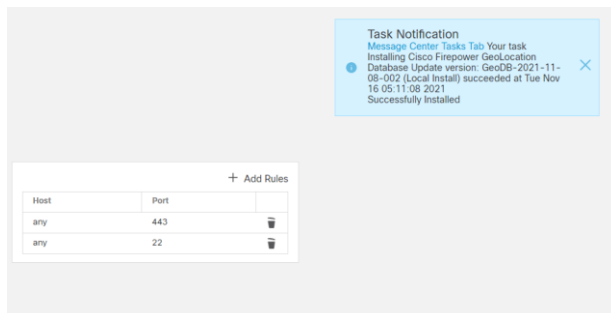
- Deploy OVA/Upgrade HW FMC to latest Gold-star FMC version
- Create local admin for config and 2nd admin for API use
- License FMC
- Install latest patches and hotfixes
- Base Configuration (SNMP, SMTP, NTP)
- Setup external auth + user roles (RADIUS)
- Setup recurring rule and Geolocation updates
- Configure/Join AD realm, pxgrid integration with ISE
- Configure eStreamer with Splunk
- Build AMP and Threat grid Connections to FMC
- Configure Backup/restore under Tools
- Realm integration

Screenshots of FMC standard config:

FMC Initial Configuration:

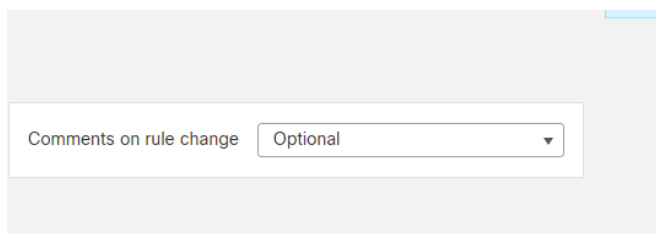
Access List:

Control which computers can access the system on specific ports



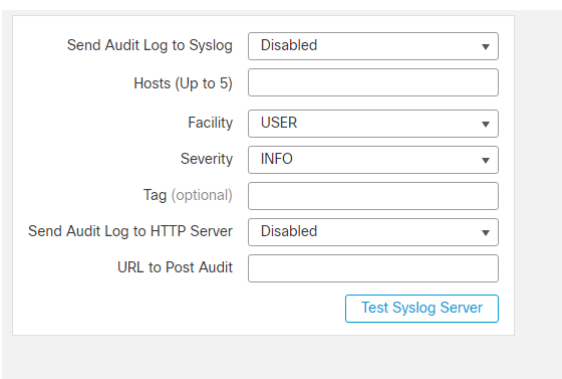
Access Control Preferences:

Configure the system to prompt users for a comment when they add or modify an access control policy



Audit Log:

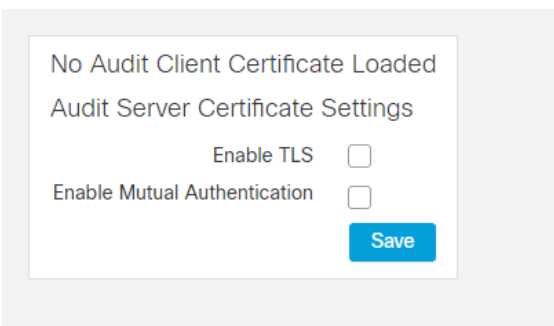
Configure the system to send an audit log to an external host



The screenshot shows a configuration panel for the audit log. It includes several settings: 'Send Audit Log to Syslog' is set to 'Disabled'; 'Hosts (Up to 5)' is an empty text field; 'Facility' is set to 'USER'; 'Severity' is set to 'INFO'; 'Tag (optional)' is an empty text field; 'Send Audit Log to HTTP Server' is set to 'Disabled'; and 'URL to Post Audit' is an empty text field. A blue button labeled 'Test Syslog Server' is located at the bottom right of the configuration area.

Audit Log Certificate:

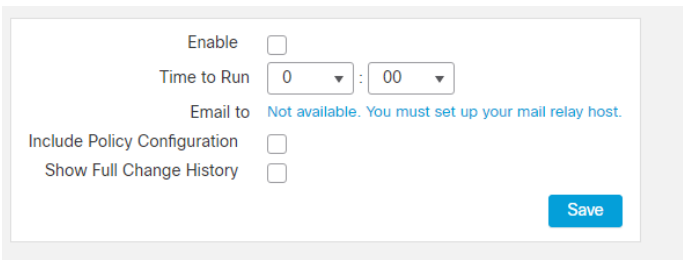
As part of audit log secure streaming, require mutual authentication between Classic devices and the audit log server



The screenshot shows a configuration panel titled 'No Audit Client Certificate Loaded' and 'Audit Server Certificate Settings'. It contains two checkboxes: 'Enable TLS' and 'Enable Mutual Authentication', both of which are currently unchecked. A blue 'Save' button is positioned at the bottom right of the panel.

Change Reconciliation:

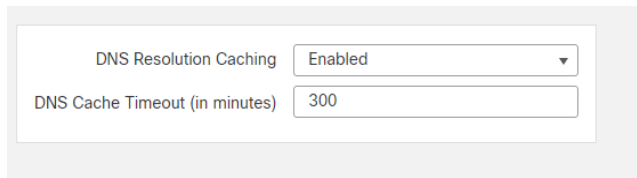
Configure the system to send a detailed report of changes to the system over the last 24 hours



The screenshot shows a configuration panel for change reconciliation. It includes an 'Enable' checkbox which is unchecked. Below it, 'Time to Run' is set to '0' hours and '00' minutes. The 'Email to' field displays the message 'Not available. You must set up your mail relay host.' There are also two unchecked checkboxes for 'Include Policy Configuration' and 'Show Full Change History'. A blue 'Save' button is located at the bottom right.

DNS Cache:

Configure the system to resolve IP addresses automatically on event view pages



The screenshot shows a configuration panel for the DNS Cache. It contains two settings: 'DNS Resolution Caching' is set to 'Enabled' via a dropdown menu, and 'DNS Cache Timeout (in minutes)' is set to '300' in a text input field.

Dashboard:

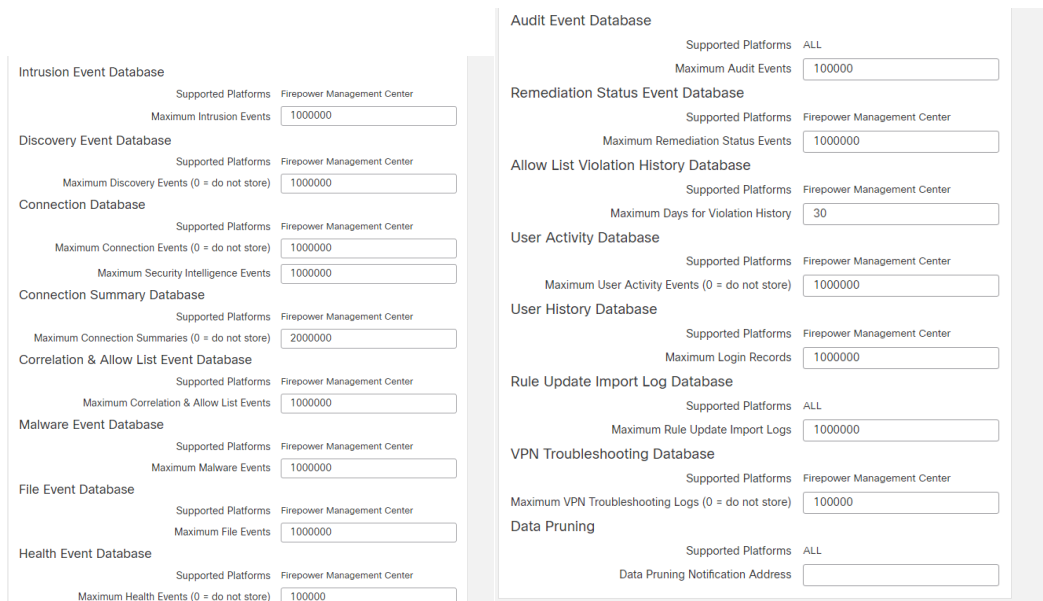
Enable Custom Analysis widgets on the dashboard



The screenshot shows a configuration panel for the Dashboard. It contains a single setting: 'Enable Custom Analysis Widgets' with a checked checkbox.

Database:

Specify the maximum number of each type of event that the Firepower Management Center can store



The screenshot shows a configuration panel for the Database, divided into two columns. Each setting includes a 'Supported Platforms' dropdown (mostly set to 'Firepower Management Center' or 'ALL') and a text input for the maximum number of events.

Database Type	Supported Platforms	Maximum Events
Intrusion Event Database	Firepower Management Center	1000000
Discovery Event Database	Firepower Management Center	1000000
Connection Database	Firepower Management Center	1000000
Connection Summary Database	Firepower Management Center	2000000
Correlation & Allow List Event Database	Firepower Management Center	1000000
Malware Event Database	Firepower Management Center	1000000
File Event Database	Firepower Management Center	1000000
Health Event Database	Firepower Management Center	100000
Audit Event Database	ALL	100000
Remediation Status Event Database	Firepower Management Center	1000000
Allow List Violation History Database	Firepower Management Center	30
User Activity Database	Firepower Management Center	1000000
User History Database	Firepower Management Center	1000000
Rule Update Import Log Database	ALL	1000000
VPN Troubleshooting Database	Firepower Management Center	100000
Data Pruning	ALL	

Email Notification:

Configure a mail host, select an encryption method, and supply authentication credentials for email-based notifications and reporting

Mail Relay Host	<input type="text"/>
Port Number	<input type="text" value="25"/>
Encryption Method	<input type="text" value="TLS"/>
From Address	<input type="text"/>
Use Authentication	<input type="checkbox"/>

[Test Mail Server Settings](#)

External Database Access:

Enable external read-only access to the database, and provide a client driver to download

External Database Access	
Allow External Database Access	<input type="checkbox"/>
Server Hostname	<input type="text"/>
Client JDBC Driver	Download

[Refresh](#) [Save](#)

HTTPS Certificate:

Request an HTTPS server certificate, if needed, from a trusted authority and upload certificates to the system

Current HTTPS Server Certificate				
Subject	commonName firepower	countryName US	organizationName Cisco Systems, Inc	organizationalUnitName Intrusion Management System
Issuer	commonName firepower	countryName US	organizationName Cisco Systems, Inc	organizationalUnitName Intrusion Management System
Validity	Not Before Sep 1 17:25:46 2021 GMT	Not After Nov 11 17:25:46 2023 GMT		
Version	3			
Serial Number	OCB9C18A119D857FED6D47655A5703B855E1CC19			
Signature Algorithm	sha256WithRSAEncryption			

[Renew HTTPS Certificate](#)

HTTPS Client Certificate Settings	
Enable Client Certificates	<input type="checkbox"/>

[Save](#)

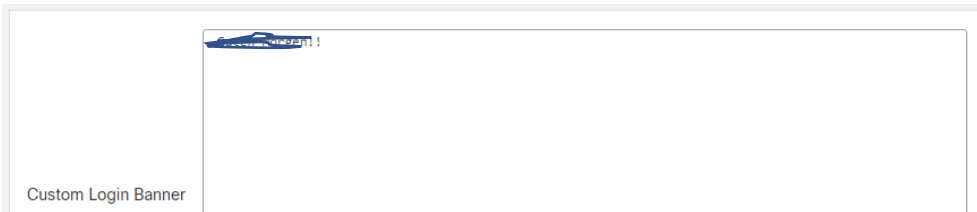
Intrusion Policy Preferences:

Configure the system to prompt users for a comment when they modify an intrusion policy

Comments on policy change	<input type="text" value="Optional"/>
Write changes in Intrusion Policy to audit log	<input checked="" type="checkbox"/>
Retain user overrides for deleted Snort 3 rules	<input checked="" type="checkbox"/>

Login Banner:

Create a custom login banner that appears when users log in



Management Interfaces:

Change options such as the IP address, hostname, and proxy settings of the appliance

▼ Interfaces

Link	Name	Channels	MAC Address	IP Address	
✓	eth0	Management Traffic Event Traffic			

▼ Routes

IPv4 Routes

Destination	Netmask	Interface	Gateway	
*				

IPv6 Routes

Destination	Prefix Length	Interface	Gateway	

▼ Shared Settings

Hostname

Domains

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

Remote Management Port

▼ ICMPv6

Allow Sending Echo Reply Packets

Allow Sending Destination Unreachable Packets

▼ Proxy

Enabled

Cancel

Save

Network Analysis Policy Preferences:

Configure the system to prompt users for a comment when they modify a network analysis policy

Comments on policy change

Optional

Write changes in Network Analysis Policy to audit log

Process:

Shut down, reboot, or restart Firepower System-related processes

Name	
Shutdown Management Center	→ Run Command
Reboot Management Center	→ Run Command
Restart Management Center Console	→ Run Command

REST API Preferences:

Enabling the REST API

Enable REST API ☒

Remote Storage Device:

Configure remote storage for backups and reports

Storage Type Local (No Remote Storage) ▼

Test
Save

SNMP:

Enable Simple Network Management Protocol (SNMP) polling

SNMP Version Version 2 ▼

Community String [REDACTED]

Session Timeout:

Leave default, at 60 for browser session and 0 for CLI.

Time:

View the current time setting and, if the time synchronization setting in the current system configuration is set to Manually in Local Configuration, change the time

Either use Defaults or if they have NTP servers, place them here.

Time Synchronization:

Manage time synchronization on the system








Serve Time via NTP Enabled

Set My Clock

Manually in Local Configuration ☐

Via NTP ☒

☐ Use the authenticated NTP server only + Add

NTP Server	Authentication	Action
	N/A	  
	N/A	  

UCAPL/CC Compliance:

Enable UCAPL/CC Compliance None

User Configuration:

Password Reuse Limit
Limit (0 = no limit)

Track Successful Logins
Days (0 = no tracking, 365 = max value)

Max Number of Login Failures
Maximum number of failures before temporary lockout (0 = no lockout, 999 = max value)

Set Time in Minutes to Temporarily Lockout Users
Minutes (0 = no wait time, 1440 = max value, 1 day)

Max Concurrent Sessions Allowed
Maximum sessions for users with Read Only privileges (0 = no limit, 1024 = max value)

Maximum sessions for users with Read/Write privileges/CLI users (0 = no limit, 1024 = max value)

VMware Tools:

Enable and use VMware Tools on a Firepower Management Center Virtual

VMware Tools

Enable VMware Tools ☐

Save

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Management_Center_System_Configuration.html#ID-2241-00000a50

Vulnerability Mapping:

Map vulnerabilities to a host IP address for any application protocol traffic received or sent from that address

Name	Description	<input checked="" type="checkbox"/>	Enabled
------	-------------	-------------------------------------	---------

Web Analytics:

Web Analytics

☒ Share usage information with Cisco

Save

Users:

Username	Real Name	Roles	Authentication Method	Password Lifetime	Enabled	Actions
admin		Administrator	Internal	Unlimited	<input type="checkbox"/>	
API_Admin	API Admin	Administrator	Internal	Unlimited	<input checked="" type="checkbox"/>	
		Administrator	Internal	Unlimited	<input checked="" type="checkbox"/>	
nbrinkley	Nick Brinkley	Administrator	Internal	Unlimited	<input type="checkbox"/>	

Users User Roles External Authentication Single Sign-On (SSO)

			Configure Permission Escalation	Create User Role
User Role			Enabled	Actions
Access Admin System-Provided			<input checked="" type="checkbox"/>	
Administrator System-Provided			<input checked="" type="checkbox"/>	
Discovery Admin System-Provided			<input checked="" type="checkbox"/>	
External Database User (Read Only) System-Provided			<input checked="" type="checkbox"/>	
Intrusion Admin System-Provided			<input checked="" type="checkbox"/>	
Maintenance User System-Provided			<input checked="" type="checkbox"/>	
Network Admin System-Provided			<input checked="" type="checkbox"/>	
Security Analyst System-Provided			<input checked="" type="checkbox"/>	
Security Analyst (Read Only) System-Provided			<input checked="" type="checkbox"/>	
Security Approver System-Provided			<input checked="" type="checkbox"/>	
Threat Intelligence Director (TID) User System-Provided			<input checked="" type="checkbox"/>	

Users User Roles External Authentication Single Sign-On (SSO)

Save Cancel Save and Apply

Default User Role: None Shell Authentication Disabled

+ Add External Authentication Object

Name	Method	Enabled
No data to Represent		

Users User Roles External Authentication Single Sign-On (SSO)

Single Sign-On (SSO) Configuration ☐

This feature is currently disabled.

Domains:

Domain configuration is up to date. Save Cancel Add Domain			
Name	Description	Devices	
Global		1 Device*	Edit Delete

Integration – Cloud Services:

We want these cloud services on so we can connect to the Cisco cloud for URL filtering, AMP for networks, and also our event configuration.

[Cloud Services](#) [Realms](#) [Identity Sources](#) [High Availability](#) [eStreamer](#) [Host Input Client](#) [Smart Software Manager On-Prem](#)

URL Filtering

Last URL Filtering Update: 2021-11-16 05:22:58 [Update Now](#)

☒ Enable Automatic Updates

☒ Query Cisco Cloud for Unknown URLs

Cached URLs Expire

[Dispute URL categories and reputations](#)

[Save](#)

AMP for Networks

Last Local Malware Detection Update: 2021-11-15 15:51:44

☒ Enable Automatic Local Malware Detection Updates

☐ Share URI from Malware Events with Cisco

[Save](#)

Cisco Cloud Region

Region

This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools.

[Save](#)

Cisco Cloud Event Configuration

☒ Send Intrusion Events to the cloud

☒ Send File and Malware Events to the cloud

Send Connection Events to the cloud:

☐ None ☒ Security Events ☐ All

[Click here](#) to view your Cisco Cloud configuration.
[Click here](#) to view your events in SecureX.

[Save](#)

Integration – Realms:

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. 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, a TS Agent, or ISE/ISE-PIC.

You can add multiple domain controllers as directories in a realm, but they must share the same basic realm information. The directories in a realm must be exclusively LDAP or exclusively Active Directory (AD) servers. After you enable a

realm, your saved changes take effect next time the Firepower Management Center queries the server.

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Host Input Client

Smart Software Manager On-Prem

Realms

Realm Sequences

Sync Results

Compare Realms

Add Realm

Name	Description	Type	Domain	AD Primary Domain	Base DN	State
[REDACTED]	Connection to DC	AD	Global	[REDACTED]	[REDACTED]	Enabled

Group and user sync

Directory

Realm Configuration

AD Primary Domain

[REDACTED]

E.g. domain.com

Enter query to look for users and groups

Enter the directory tree on the server where the Firepower Management Center should begin searching for user and group data.

Base DN

[REDACTED]

E.g. ou=group,dc=cisco,dc=com

Group DN

[REDACTED]

E.g. ou=group,dc=cisco,dc=com

Load Groups

Available Groups

Limit the groups to use in policy by moving them to either the Included Groups or Excluded Groups list. Moving one group to the Included Groups list, for example, allows that group only to be used in policy. [Learn more](#)

Available Groups (All groups are included by default)

Search

Anesthetists

Included Groups and Users

All except excluded

Excluded Groups and Users

None

Connection to DC

Group and User Sync

Directory

Realm Configuration

Directory Username*

[REDACTED]

E.g. user@domain.com

Directory Password*

Add Directory

Hostname/IP Address and Port	Encryption
dc2016dns.[REDACTED]:636	LDAPS
DCSecondary.[REDACTED]:636	LDAPS

Integration – Identity Sources:

If they have ISE. If not, leave as none.

Cloud Services

Realms

Identity Sources

High Availability

eStreamer

Identity Sources

Service Type

None

Identity Services Engine

No identity source active

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-24/214481-configure-ise-2-4-and-fmc-6-2-3-pxgrid-i.html>

Integration – High Availability:

HA for FMC. Most cases, we only have one instance. Leave as standalone.

Cloud Services	Realms	Identity Sources	High Availability	eStreamer	Host Input Client	Smart Software Manager On-Prem
----------------	--------	------------------	-------------------	-----------	-------------------	--------------------------------

Select a role for this Management Center and specify peer details to setup high availability.

Role For This FMC:

☒ Standalone (No High Availability)

☐ Primary

Integration – eStreamer:

Before the Management Center or managed device you want to use as an eStreamer server can begin streaming events to a client application, you must configure the eStreamer server to send events to clients, provide information about the client, and generate a set of authentication credentials to use when establishing communication. You can perform all of these tasks from the Management Center or managed device user interface.

As of now, we do not configure for most customers unless specifically asked.

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/api/eStreamer/EventStreamerIntegrationGuide/ConfiguringEstreamer.html>

Integration - Host Input Client:

In addition to accepting host input commands from users on the Management Center, the Management Center's host input service also accepts batch import files from authenticated host input clients on external hosts. You can use a host input client to process import files created for the host input import tool and then send the data to the Management Center to add the information to your network map.

Most customers we leave default (turned off) unless specifically asked about it.

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/api/host-input/HostInputAPIGuide/Configuring-HostInputClient.html>

Integration – Smart Software Manager On-Prem:

Input Client

Smart Software Manager On-Prem

Smart Software Manager On-Prem Configuration

☒ Connect directly to Cisco Smart Software Manager

☐ Connect to Cisco Smart Software Manager On-Prem Server

URL

SSL Certificate

Please select a certificate

Apply













Updates – Product Updates:

Here you can upload and download new updates to FMC/FTD.

Currently running software version: 6.6.1

Upload Update


































Updates

Type	Version	Date	Release Notes	Reboot	
Cisco Vulnerability And Fingerprint Database Updates	339	Thu Nov 5 21:41:04 UTC 2020		No	 
Cisco FTD SSP FP1K Upgrade	6.6.5-81	Wed Jul 28 04:59:26 UTC 2021		Yes	 
Cisco Firepower Mgmt Center Upgrade	6.6.5-81	Wed Jul 28 04:47:00 UTC 2021		Yes	 
Cisco FTD SSP FP2K Upgrade	6.6.5-81	Wed Jul 28 04:51:33 UTC 2021		Yes	 
Cisco FTD SSP FP1K Upgrade	6.6.4-64	Thu Apr 29 00:08:57 UTC 2021		Yes	 
Cisco FTD SSP FP2K Upgrade	6.6.4-59	Thu Apr 22 03:23:10 UTC 2021		Yes	 

Updates – Rule Updates:

You can update rules for snort rule update versioning here. You can also see the rule updates log.

Product Updates Rule Updates Geolocation Updates

Summary	Time	User ID	Status	
Snort Rule Update 2021 11 15 001 vrt Completed install of Snort Rule Update 2021-11-15-001-vrt	2021-11-17 01:02:30	admin		 
Snort Rule Update 2021 11 10 001 vrt Completed install of Snort Rule Update 2021-11-10-001-vrt	2021-11-11 01:02:17	admin		 
Snort Rule Update 2021 11 09 001 vrt Completed install of Snort Rule Update 2021-11-09-001-vrt	2021-11-10 01:04:50	admin		 
Snort Rule Update 2021 11 03 001 vrt Completed install of Snort Rule Update 2021-11-03-001-vrt	2021-11-05 01:03:19	admin		 
Snort Rule Update 2021 11 02 001 vrt Completed install of Snort Rule Update 2021-11-02-001-vrt	2021-11-03 01:02:43	admin		 
Snort Rule Update 2021 10 27 001 vrt Completed install of Snort Rule Update 2021-10-27-001-vrt	2021-10-29 01:01:57	admin		 
Snort Rule Update 2021 10 25 001 vrt Completed install of Snort Rule Update 2021-10-25-001-vrt	2021-10-27 01:02:06	admin		 
Snort Rule Update 2021 10 20 001 vrt Completed install of Snort Rule Update 2021-10-20-001-vrt	2021-10-22 01:03:00	admin		 
Snort Rule Update 2021 10 18 001 vrt Completed install of Snort Rule Update 2021-10-18-001-vrt	2021-10-20 01:02:49	admin		 
Snort Rule Update 2021 10 13 001 vrt Completed install of Snort Rule Update 2021-10-13-001-vrt	2021-10-15 01:02:15	admin		 
Snort Rule Update 2021 10 12 001 vrt Completed install of Snort Rule Update 2021-10-12-001-vrt	2021-10-13 01:02:44	admin		 

Updates – Geolocation updates:

You can import/install geolocation updates here.

The screenshot shows the 'Geolocation Updates' tab in the Cisco Smart Software Manager. At the top, it says 'Running geolocation update version: 2021-11-08-002'. Below this, there are two main sections: 'One-Time Geolocation Update' and 'Recurring Geolocation Updates'. The 'One-Time' section has a note that updates may be large and take up to 45 minutes. It offers two sources: 'Upload and install geolocation update' (selected) with a 'Choose File' button, and 'Download and install geolocation update from the Support Site'. An 'Import' button is at the bottom right. The 'Recurring' section has a checkbox 'Enable Recurring Weekly Updates from the Support Site' which is checked. Below this, there are dropdowns for 'Update Start Time' (Thursday), 'Time' (12:00), 'Period' (PM), and 'Timezone' (America/New York). 'Cancel' and 'Save' buttons are at the bottom right.

Licensing – Smart Licensing:

This page is pretty important. You can see all of your licensing structured and what licenses are good or need renewed. You can also sync your Cisco smart software manager as well to see product registration and usage registration.

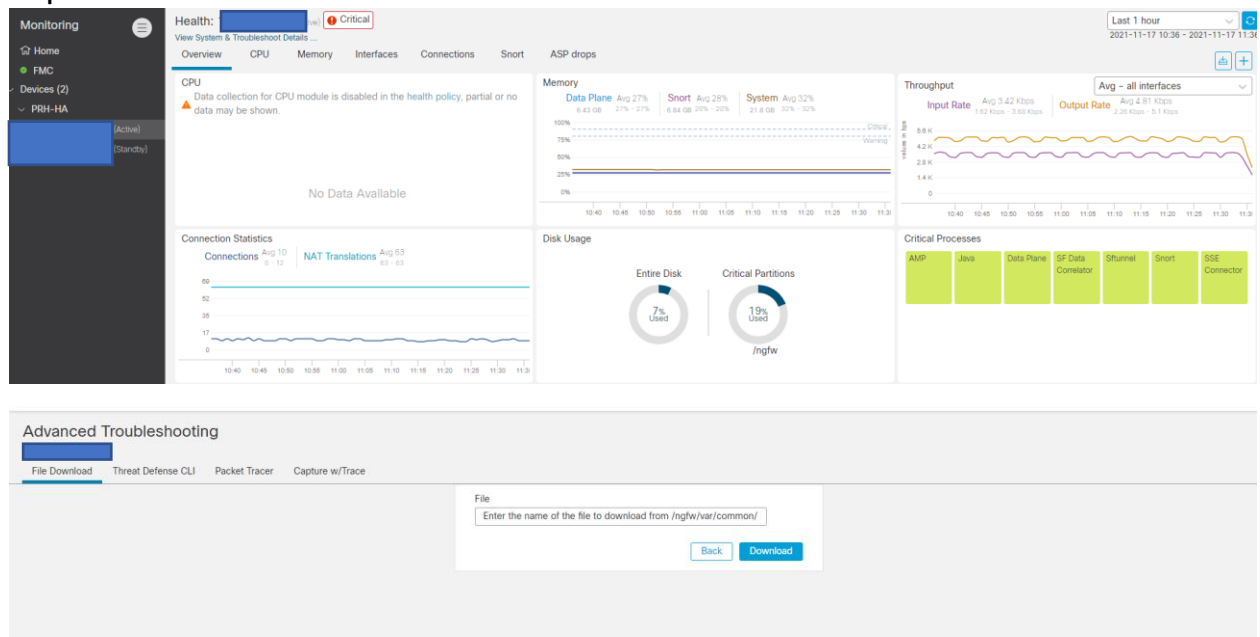
The screenshot shows the 'Smart License Status' and 'Smart Licenses' page. The 'Smart License Status' section on the left shows: Usage Authorization: Authorized (Last Synchronized On Nov 13 2021), Product Registration: Registered (Last Renewed On Dec 03 2020), Assigned Virtual Account: [redacted], Export-Controlled Features: Enabled, Cisco Success Network: Disabled, and Cisco Support Diagnostics: Disabled. The 'Smart Licenses' section on the right has a table with columns: License Type/Device Name, License Status, Device Type, Domain, and Group. The table lists several licenses, all with a green status icon. A 'Filter Devices...' button and an 'Edit Licenses' button are at the top right of the table.

License Type/Device Name	License Status	Device Type	Domain	Group
> Firepower Management Center/Virtual (3)	●			
> Base (3)	●			
> Malware (3)	●			
> Threat (3)	●			
> URL Filtering (3)	●			
AnyConnect Apex (0)				
> AnyConnect Plus (3)	●			
AnyConnect VPN Only (0)				

Health Monitor:

You can view the health of your FMC and any FTDs in this window. It will show any Health status errors, warnings, etc. You can then click on your FTDs and see a bunch of graphs with statistics for what the FTDs are using, critical processes, etc. If you go to View System & Troubleshooting details on the FTDs, there are two main areas that you need to know about. One is generating Troubleshooting Files. You will need to do this if problems occur and Cisco TAC gets involved and wants troubleshooting files. The other link is Advanced Troubleshooting. Here you can do file downloads, get into the FTD CLI, run packet tracers, and run packet

captures.



Health Policy:

We can see a multitude of categories in which monitoring is on for most by default. We can then go in and decide to either remove monitoring for that specific category or change thresholds related to that category.

The screenshot shows the 'Editing Policy' dialog box for the 'Initial_Health_Policy'. The dialog has a sidebar on the left with a list of categories: Backlog Status, CPU Usage (per core), CPU Usage Data Plane, CPU Usage Short, CPU Usage System, Card Reset, Chassis Status FTD, Cluster/Failover Status, Configuration Database, Configuration Memory Allocation, Connection Statistics, Critical Process Statistics, Deployed Configuration Statistics, and Disk Status. The main area of the dialog contains the following fields: 'Policy Name' (Initial_Health_Policy 2021-09-01), 'Policy Description' (Initial Health Policy), 'Description' (Statistics about deployed configuration such as number of ACEs, IPS rules), and 'Enabled' (On). At the bottom right, there are 'Cancel' and 'Save Policy and Exit' buttons.

Health Events:

Here we can see different health events such as memory usage, smart licensing monitoring, FMC HA status, etc.

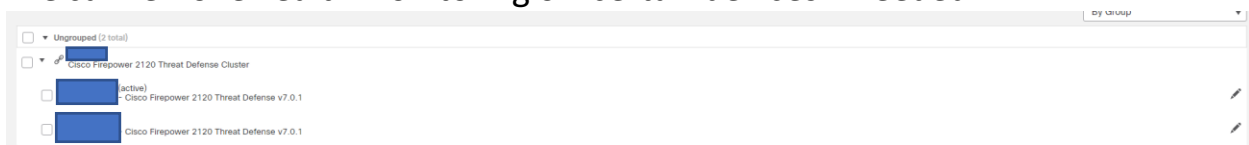
No Search Constraints ([Edit Search](#)) expanding

Health Monitor Table View of Health Events

<input type="checkbox"/> Module Name X	Test Name X	Time X	Description X	Value X	Units X	Status X	Device X
▼ <input type="checkbox"/> Memory Usage	Memory Usage - Memory Test	2021-11-17 11:45:03	Normal System Memory	31	n/a	●	
▼ <input type="checkbox"/> Memory Usage Data Plane	Memory Usage Data Plane - Memory Test for Lina	2021-11-17 11:45:03	Normal Lina Memory	26	n/a	●	
▼ <input type="checkbox"/> Memory Usage Snort	Memory Usage Snort - Memory Test for Snort	2021-11-17 11:45:03	Normal Snort Memory	27	n/a	●	
▼ <input type="checkbox"/> Memory Usage	Memory Usage - Memory Test	2021-11-17 11:44:55	Normal System Memory	30	n/a	●	
▼ <input type="checkbox"/> Memory Usage Data Plane	Memory Usage Data Plane - Memory Test for Lina	2021-11-17 11:44:55	Normal Lina Memory	27	n/a	●	
▼ <input type="checkbox"/> Memory Usage Snort	Memory Usage Snort - Memory Test for Snort	2021-11-17 11:44:55	Normal Snort Memory	28	n/a	●	
▼ <input type="checkbox"/> Backlog Status	Backlog Status	2021-11-17 11:44:12	No event backlog exists on any device	0		●	
▼ <input type="checkbox"/> Time Synchronization Status	Time Synchronization Status	2021-11-17 11:44:12	All devices are synchronized	0		●	

Health Exclude:

We can remove health monitoring off certain devices if needed.



Health Monitor Alerts:

We can configure our own Health monitor alerts by choosing the severity that triggers the alert, the module, and then the alert itself with an optional threshold timeout.

Active Health Alerts

Load

Delete

Configure Health Alerts

Health Alert Name

Severity

Critical

Warning

Normal

Error

Recovered

Threshold Timeout (Optional)

(in minutes)

Module

AMP Connection Status

AMP Threat Grid Status

AMP For Endpoints Status

AMP for Firepower Status

ASP Drop

Advanced Snort Statistics

Appliance Heartbeat

Automatic Application Bypass...

Backlog Status

CPU Usage (per core)

CPU Usage Data Plane

Alert

Save

Security Analytics and Logging:

This would be a Stealth watch integration where you can send your logging to an SMC or Stealth watch management console. Provides logging storage for centralized events. Or, you can send it to a Flow collector to a SMC.

Configure Security Analytics and Logging (SAL) Integration

Select the setup that best represents your system:

One Box

Firepower Management Center
Provides centralized management for Firepower Threat Defense devices

Stealthwatch Management Console
Provides logging storage and centralized Eventing display

Firepower Threat Defense devices
Version 7.0 or higher

- 1 **Configure Host**
Provide SMC hostname or IP address
- 2 **Confirm Settings**
Confirm the host settings
- 3 **Establish Query Credentials**
Log in to the SMC to establish credentials

Start

Flow Collector

Firepower Management Center
Provides centralized management for Firepower Threat Defense devices

Stealthwatch Management Console
Provides centralized Eventing display

Firepower Threat Defense devices
Version 7.0 or higher

Flow Collectors
Provides logging storage

- 1 **Configure Host**
Provide SMC hostname or IP address
Provide Flow Collector IP address
- 2 **Confirm Settings**
Confirm the host settings
- 3 **Establish Query Credentials**
Log in to the SMC to establish credentials

Start

Monitoring Audit:

Your traditional audit log with GET requests show activity.

<input type="checkbox"/>	Time x	User x	Subsystem x	Message x
▼	2021-11-17 11:48:05	nbrinkley	API	
▼	2021-11-17 11:47:58	nbrinkley	System > Health > Monitor Alerts	Page View
▼	2021-11-17 11:47:16	nbrinkley	System > Health > Exclude	Page View
▼	2021-11-17 11:46:25	nbrinkley	System > Health > Events	Page View

Monitoring Syslog:

Monitoring syslog events.

Messages
Nov 17 2021 11:55:23
Nov 17 2021 11:55:23
Nov 17 2021 11:55:20
Nov 17 2021 11:55:01
Nov 17 2021 11:55:01

Monitoring statistics:

Can view memory usage, load average, disk usage, and other statistics here.



Tools – Backup/Restore:

Here we can set up Backup profiles to backup the FMC and FTDs. Then, you can manually download the backups to your PC. I would recommend always having a backup downloaded to the PC and not just storing the backups on the device you are taking a backup from. Storage location is set to default at `/var/sf/backup/`.

<input type="checkbox"/>	System Information	Date Created	File Name	VDB Version	Location	Size (MB)	Configurations	Events	TID
<input type="checkbox"/>	10.111.111.5								
<input type="checkbox"/>	Cisco Firepower 2120 Threat Defense v7.0.1	2021-11-16 17:13:29	10.111.111.5_Secondary_20211116171149.tar	build 347	Local	105	Yes	No	No
<input type="checkbox"/>	10.111.111.4								
<input type="checkbox"/>	Cisco Firepower 2120 Threat Defense v7.0.1	2021-11-16 17:13:25	10.111.111.4_Primary_20211116171145.tar	build 347	Local	105	Yes	No	No

Download Delete Move

Tools – Scheduling:

Here, you can schedule events such as Backups, deploying policies, Nmap scanning, installing latest updates, etc.

New Task

Job Type

Backup

Backup

Download CRL

Deploy Policies

NMap Scan

Report

Firepower Recommended Rules

Download Latest Update

Install Latest Update

Push Latest Update

Update URL Filtering Database

Schedule task to run

Current time

Start Time

Job Name

Backup Type

Backup Profile

Comment

021

12:00

Pm

America/New York

Management Center

Device

Config only backup

Not available. You must set up your mail relay host.

Cancel

Save

Tools – Import/Export:

Here we can import/export a multitude of things such as Dashboard statistics, different policies, NAT, SSL, ACP, and more.

Access Control Policy	Access Control Policy	2021-11-17 03:31:58
Contextual Cross-launch		
<input type="checkbox"/> Alexa Domain	Contextual Cross-launch	2021-09-01 13:26:11
<input type="checkbox"/> AlienVault Domain	Contextual Cross-launch	2021-09-01 13:26:10
<input type="checkbox"/> AlienVault IP	Contextual Cross-launch	2021-09-01 13:26:10
<input type="checkbox"/> AlienVault SHA256	Contextual Cross-launch	2021-09-01 13:26:10
<input type="checkbox"/> AMP for Endpoints File Trajectory	Contextual Cross-launch	2021-09-01 13:26:10
<input type="checkbox"/> AMP for Endpoints SHA256	Contextual Cross-launch	2021-09-01 13:26:10
<input type="checkbox"/> IBM X-Force Exchange Domain	Contextual Cross-launch	2021-09-01 13:26:11
<input type="checkbox"/> IBM X-Force Exchange IP	Contextual Cross-launch	2021-09-01 13:26:10
<input type="checkbox"/> IBM X-Force Exchange SHA256	Contextual Cross-launch	2021-09-01 13:26:11

Data Purge:

You can purge Discovery and Identity events, hosts, user activity, connection events, connection summary events, and SI events.

Data Purge

Discovery and Identity

☐ Network Discovery Events

☐ Hosts

☐ User Activity

☐ User Identities

Connections

☐ Connection Events

☐ Connection Summary Events

☐ Security Intelligence Events

Purge Selected Events

AFTER FMC CONFIGURATION

Putting Base IP config on FTDs that customer sends in workbooks

Joining FTDs to FMC (configure manager add)

Upgrade FTD/FMC to compatible versioning

Licensing (checking if connected to EA/smart account, licensing is correct)

If you were sold HA pair, bring up FTDs into HA.

HA Pair:

Follow the screenshot to what config to put. You can use the exact IPv6 addresses in the screenshot as your failover/state link. Change interfaces when needed.

Running Migration tool... (Everything should be migrated other than S2S as of version 2.4.1)

After Migration tool is ran.....

POLICIES

ACLS:

Rules-

Making sure all destination zones are inputted in the rules after the migration. Combining/deleting any rules that can be combined or removed. Creating categories and organizing ACLs based off of Zones.

Best Practice to add for inside – outside ACLs for every customer. See SS below.

Search												
6 rules												
#	Name	Action	Source				Destination				Layer 7	
			Zones	Networks	Ports	SGT Groups	Zones	Networks	Ports	SGT Groups	Applications	URLs
1	Block URLs	Block	inside_zone	Any	Any	Any	outside	Any	Any	Any	Any	Adult (Any Reputation) Banking Fraud (Any Reputation) Exploits (Any Reputation) Hate Speech (Any Reputation)
2	Block Geolocation	Block	inside_zone	Any	Any	Any	outside	12.12.12.12 China North Korea Russian Federation	Any	Any	Any	Any
3	Block Applications	Block	inside_zone	Any	Any	Any	outside	Any	Any	Any	BitTorrent Netflix Netflix stream	Any
4	Allow DNS	Allow	inside_zone	Any	Any	Any	outside	Any	DNS over TCP DNS over UDP	Any	DNS	Any
5	Allow Applications	Allow	inside_zone	Any	Any	Any	outside	Any	Any	Any	Office 365 Office 365 Planner Office365 Admin p... OneDrive Sharepoint Sharepoint Online Skype Skype Auth Skype for Business	Any
6	Allow HTTP and HTTPS	Allow	inside_zone	Any	Any	Any	outside	Any	HTTP HTTPS	Any	Any	Any

Make sure when all of your policies are created, add your intrusion/malware and file policies to your specific rules that you want the policies on. (Add IPS rules on pretty much all the allow rules. File/malware rules will be applied on any catch all rules or rules regarding not encrypted/secure protocols like http, ftp, etc.



Also add your Prefilter Policy, SSL policy, and Identity Policy if you have one to the ACP.

Security Intelligence –

Make sure you block the appropriate Networks and URLs and put them in your DNS policy Block list. See screenshot below.

(From Attackers to Tor_exit_node in the list)


Prefilter Policy: [Default Prefilter Policy](#)
SSL Policy: [None](#)
Identity Policy: [PRH-Identity](#)

DNS Policy  


Default DNS Policy

Do-Not-Block List(2)


Networks



Global Do-Not-Block List (Any Zone) 



URLs



Global Do-Not-Block List for URL (Any Zone) 



Block List(46)



Networks 



Attackers (Any Zone)  



Banking_fraud (Any Zone)  



Bogon (Any Zone)  



Bots (Any Zone)  



CnC (Any Zone)  



Cryptomining (Any Zone)  



Dga (Any Zone)  

Exploitkit (Any Zone)  

High_risk (Any Zone)  

loc (Any Zone)  

Link_sharing (Any Zone)  

Malicious (Any Zone)  

HTTP Responses –

This can be default, make sure System-provided is selected in the interactive block response page.

Rules
Security Intelligence
HTTP Responses
Logging
Advanced

Inheritance Settings | Policy Assignments (11)

Prefilter Policy: [Default Prefilter Policy](#)
SSL Policy: [None](#)
Identity Policy: [PRH-Identity](#)

Block Response Page

This page will be displayed when HTTP traffic is blocked.

None

Interactive Block Response Page

This page will be displayed when HTTP traffic is blocked, but the user may choose to continue.

System-provided

Logging –

Check the syslog settings configured in the FTD platform Settings policy deployed on the device. (I would use the severity of EMERG)

Enter Description

You have unsaved changes

Show Warnings

Analyze Hit Counts

Save

Cancel

Rules

Security Intelligence

HTTP Responses

Logging

Advanced

Inheritance Settings

Policy Assignments (1)

Prefilter Policy: Default Prefilter Policy

SSL Policy: None

Identity

Default Syslog Settings:

The following configuration will be used for all syslog destinations in this AC policy and all included SSL, Prefilter and Intrusion policies unless explicitly overridden.

☐ Send using specific syslog alert

Syslog Alert

☒ Use the syslog settings configured in the FTD Platform Settings policy deployed on the device

Syslog Severity

EMERG

IPS Settings

☐ Send Syslog messages for IPS events

Default syslog settings configured above are used for syslog destinations for IPS events

Show Overrides

File and Malware Settings

☐ Send Syslog messages for File and Malware events

Default syslog settings configured above are used for syslog destinations for File and Malware events

Show Overrides

Rules				Security Intelligence	HTTP Responses	Logging	Advanced	Inheritance Settings Policy Assignments	
				Prefilter Policy: Default Prefilter Policy		SSL Policy: None		Identity Policy: Default Identity Policy	
General Settings						Intelligent Application Bypass Settings			
Maximum URL characters to store in connection events				1024		Intelligent Application Bypass Settings		Off	
Allow an interactive block to bypass blocking for (seconds)				600		Total Apps and Filters Configured		All applications including unidentified applications	
Retry URL cache miss lookup				Yes		Transport/Network Layer Preprocessor Settings			
Enable Threat Intelligence Director				Yes		Ignore the VLAN header when tracking connections		No	
Enable reputation enforcement on DNS traffic				Yes		Detection Enhancement Settings			
Inspect traffic during policy apply				Yes		Adaptive Profiles		Enabled	
Identity Policy Settings						Adaptive Profiles - Enable profile updates		Enabled	
Identity Policy				PRH-Identity		Adaptive Profiles - Attribute Update Interval		60	
SSL Policy Settings						Adaptive Profiles - Networks		0 0 0 0/0	
SSL Policy to use for inspecting encrypted connections				None		Performance Settings			
TLS Server Identity Discovery						Pattern Matching Limits - Max Pattern Match States to Analyze Per Packet		5	
Early application detection and URL categorization				Disabled		Performance Statistics - Sample Time (seconds)		300	
Prefilter Policy Settings						Regular Expression - Limit		Default Value	
Prefilter Policy used before access control				Default Prefilter Policy		Regular Expression - Recursion Limit		Default Value	
Network Analysis and Intrusion Policies						Intrusion Event Logging Limits - Max Events Stored Per Packet		8	
Prefilter Policy used before access control				Default Prefilter Policy		Regular Expression - Recursion Limit		Default Value	
Network Analysis and Intrusion Policies						Intrusion Event Logging Limits - Max Events Stored Per Packet		8	
Intrusion Policy used before Access Control rule is determined				No Rules Active		Latency-Based Performance Settings			
Intrusion Policy Variable Set				Default-Set		Applied from Installed Rule Update		true	
Default Network Analysis Policy				Balanced Security and Connectivity		Packet Handling		Disabled	
Threat Defense Service Policy						Rule Handling		Enabled	
Threat Defense Service Rule(s)				0		Rule Handling - Threshold (microseconds)		512	
Files and Malware Settings						Rule Handling - Consecutive Threshold Violations Before Suspending Rule		3	
Limit the number of bytes inspected when doing file type detection				1460		Rule Handling - Suspension Time (seconds)		10	
Allow file if cloud lookup for Block Malware takes longer than (seconds)				2					
Do not calculate SHA256 hash values for files larger than (n bytes)				10485760					
Minimum file size for advanced file inspection and storage (bytes)				6144					
Maximum file size for advanced file inspection and storage (bytes)				1048576					
Minimum file size for dynamic analysis testing (bytes)				6144					
Maximum file size for dynamic analysis testing (bytes)				1048576					

Intrusion Policy:

Create an Intrusion Policy Best practice in SS.

Edit Intrusion Policy ×

Name*

Description

Inspection Mode
☐ Detection ☒ Prevention

Intrusion rule actions are always applied. Connections that match a drop rule are blocked.

Base Policy

Cancel Save

After creating intrusion policy to screenshot above, we will come back to applying/editing the policy. We need traffic to start flowing so it can be analyzed. Then, we can go into snort 3 later to see what Cisco recommends as best practice to remove/add snort rules in based off the traffic it sees.

Malware & File Policy:

Create your Malware & File Policy Best practice in screenshot below.

MalwareFile

Enter Description

Rules

Advanced

General

☒ First Time File Analysis

☒ Enable Custom Detection List

☒ Enable Clean List

If AMP Cloud disposition is Unknown, override disposition based upon threat score

Disabled

Archive File Inspection

☐ Inspect Archives

☐ Block Encrypted Archives

☒ Block Uninspectable Archives

Max Archive Depth

Enter a value between 1 and 3

2

DNS Policy:

Identity Policy:

See screenshots below for the passive identity rule in our policy.

[illegible]

Rules
Active Authentication
Identity Source

Server Certificate *
None
+

Port *
885
(885 or 1025 - 65535)

Maximum login attempts *
3
(0 or greater. Use 0 to indicate unlimited login attempts)

Active Authentication Response Page

This page will be displayed if a user triggers an identity rule with HTTP Response Page as the Authentication Type.

System-provided

* Required when using Active Authentication

This is all we need to do for best practice. You can use identity policies to detect the user who is associated with a connection. By identifying the user, you can correlate threat, endpoint, and network intelligence with user identity information. By linking network behavior, traffic, and events directly to individual users, the system can help you identify the source of policy breaches, attacks, or network vulnerabilities. All you need is a realm configured first (in configuration, integration, then realms in the fmc cog wheel) Once a realm is configured, then you can create a rule in the policy, name it passive identity, then connect the rule with the action of passive authentication and the realm you are using.

SSL Policy:

How you handle SSL and encrypted traffic on the network. The SSL policy will handle the decryption of encrypted traffic coming in on TCP connections only.

Generally skipped, however is customer wants this policy to be applied, you can follow this here to build a policy out (You need a cert built out as well):

<http://www.labminutes.com/sec0228 asa firepower 60 ssl decryption 1>

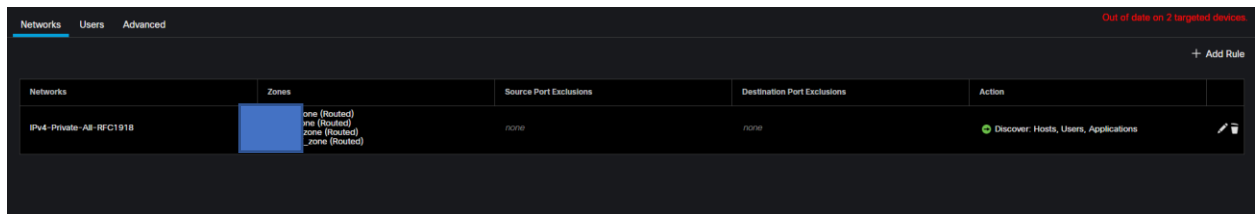
Prefilter Policy:

Make sure a default prefilter policy is created and applied to ACP. Can add rules in per customer request. (For instance, offsite backups.)

Like an ACL however it provides early access control which allows a flow to bypass the snort engine completely. Traffic will not be analyzed by the snort engine.

<https://www.cisco.com/c/en/us/support/docs/security/firepower-management-center/212700-configuration-and-operation-of-ftd-prefi.html>

Network Discovery:



Best practice ^ The rest is default under Users and Advanced as well. Its applied to your FMC, does not need to be pushed down to a device. Policy is applied by default.

Application Detectors:

Correlation:

DEVICES

Device Management:

Device Upgrade:

NAT:

VPN – S2S:

First step would be going to the ASA and running the command “show vpn-sessiondb detail l2l”. Log all the active connections to notepad ++. Then, go into object management, network, and start creating a list of all the objects. Here is a picture for example.

Source zone is outside, destination zone is inside. Source network is your peer's local network object you are trying to reach. Your destination object is your local network object it needs to reach. Enable IPS inspection and make sure it is in the right ACL category. Save your rule. Then, you need to check NAT. Usually the NAT rules are migrated successfully, however, it is good to check just in case. It should look like this just like the example...

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options	
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services		
6	→	Static	Inside_lg	Outside_lg	ObixVPN	ObixRemote		ObixVPN	ObixRemote		Ons: false no-proxy-arp	

After making sure NAT is good, you have successfully created a s2s tunnel with an attached ACL and NAT rule!

VPN-RA:

Dynamic Access Policy:

Troubleshooting:

Qos:

Platform Settings:

ARP Inspection:

(Usually not set up unless specifically asked)

By default, all ARP packets are allowed between bridge group members. You can control the flow of ARP packets by enabling ARP inspection.

ARP inspection prevents malicious users from impersonating other hosts or routers (known as ARP spoofing). ARP spoofing can enable a “man-in-the-middle” attack. For example, a host sends an ARP request to the gateway router; the gateway router responds with the gateway router MAC address. The attacker, however, sends another ARP response to the host with the attacker MAC address instead of the router MAC address. The attacker can now intercept all the host traffic before forwarding it on to the router.

Procedure

- Step 1** Select **Devices > Platform Settings** and create or edit a FTD policy.
- Step 2** Select **ARP Inspection**.
- Step 3** Add entries to the **ARP Inspection** table.
- Click **Add** to create a new entry, or click **Edit** if the entry already exists.
 - Select **in desired options**.
 - Inspect Enabled**—To perform **ARP Inspection** on the selected interfaces and zones.
 - Flood Enabled**—Whether to flood ARP requests that do not match static ARP entries out all interfaces other than the originating interface or the dedicated management interface. This is the default behavior.
If you do not elect to flood ARP requests, then only those requests that exactly match static ARP entries are allowed.
 - Security Zones**—Add the zones that contain the interfaces on which to perform the selected actions. The zones must be switched zones. For interfaces not in a zone, you can type the interface name into the field below the Selected Security Zone list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.
 - Click **OK**.
- Step 4** Add static ARP entries according to **Add a Static ARP Entry**.
- Step 5** Click **Save**.
You can now click **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

DNS:

(Usually not set up unless specifically asked to)

Configure DNS

The Domain Name System (**DNS**) servers are used to resolve hostnames to IP addresses. There are two **DNS** server settings that apply to different types of traffic: data and special management traffic. Data traffic includes any services that use **FQDNs** for which a **DNS** lookup is necessary, such as Access Control Rules and Remote Access VPN. Special management traffic includes traffic originating on the Management interface such as FMC management and database updates. This procedure only applies to **data DNS** servers. For **management DNS** settings, see the CLI **configure network dns servers** and **configure network dns searchdomains** commands.

To determine the correct interface for **DNS** server communications, the FTD uses a routing lookup, but which routing table is used depends on the interfaces for which you enable **DNS**. See the interface settings below for more information.

Before you begin

- Ensure you have created a **DNS** server group. For instructions, see **Creating DNS Server Group Objects**.
- Ensure that the FTD has appropriate static or dynamic routes to access the **DNS** servers.

Procedure

- Step 1** Select **Devices > Platform Settings** and create or edit a Firepower Threat Defense policy.
- Step 2** Click **DNS**.
- Step 3** Check **Enable DNS name resolution by device**.
- Step 4** Choose the **DNS Server Group** that you have already created.
- Step 5** (Optional) Enter the **Expiry Entry Timer** and **Poll Timer** values in minutes.
These options apply to **FQDNs** that are specified in network objects only. These do not apply to **FQDNs** used in other features.
- Expire Entry Timer** specifies the time limit to remove the IP address of a resolved FQDN from the **DNS** lookup table after its time-to-live (TTL) expires. Removing an entry requires the table to be recompiled, so frequent removals can increase the processing load on the device. This setting virtually extends the TTL.
 - Poll Timer** specifies the time limit after which the device queries the **DNS** server to resolve the FQDN that was defined in a network object. An FQDN is resolved periodically either when the poll timer has expired, or when the TTL of the resolved IP entry has expired, whichever occurs first.
- Step 6** Enable **DNS** lookups on all interfaces or on specific interfaces. These choices also affect which routing tables are used.
Note that enabling **DNS** lookups on an interface is not the same as specifying the source interface for lookups. The FTD always uses a route lookup to determine the source interface.
- No interfaces selected—Enables **DNS** lookups on all interfaces, including Management and management-only interfaces. The FTD checks the data routing table, and if no route is found, falls back to the management-only routing table.
 - Specific interfaces selected but not the **Enable DNS Lookup via diagnostic interface also** option—Enables **DNS** lookups on the specified interfaces. The FTD checks the data routing table only.
 - Specific interfaces selected plus the **Enable DNS Lookup via diagnostic interface also** option—Enables **DNS** lookups on the specified interfaces and the interface. The FTD checks the data routing table, and if no route is found, falls back to the management-only routing table.
 - Only the **Enable DNS Lookup via diagnostic interface also** option—Enables **DNS** lookups on . The FTD checks only the management-only routing table. Be sure to configure an IP address for the Diagnostic interface on the **Devices > Device Management > edit device > Interfaces** page.
- Step 7** Click **Save**.

External Authentication:

This would be for your configuration with ISE to do any external authentication.

Manage External Authentication Server						
Name	Description	Method	Server:Port	Encryption	Enabled	
ISE		RADIUS		no	<input checked="" type="checkbox"/>	

Fragment Settings:

By default, the FTD device allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly. You might need to let fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, if you do not have an application that fragments traffic, we recommend that you do not allow fragments by setting Chain to 1. Fragmented packets are often used as Denial of Service (DoS) attacks.

Size (Block)	<input type="text" value="200"/>	(1 - 30000)
Chain (Packet)	<input type="text" value="24"/>	(1 - 8200)
Timeout (Sec)	<input type="text" value="5"/>	(1 - 30)

HTTP:

If you want to allow HTTPS connections to one or more interfaces on the FTD device, configure HTTPS settings. You can use HTTPS to download packet captures for troubleshooting.

-
- Step 1** Select **Devices > Platform Settings** and create or edit an FTD policy.
- Step 2** Select **HTTP**.
- Step 3** Enable the HTTPS server by clicking **Enable HTTP server**.
- Step 4** (Optional) Change the HTTPS port. The default is 443.
- Step 5**
- Identify the interfaces and IP addresses that allow HTTPS connections.
- Use this table to limit which interfaces will accept HTTPS connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.
- a. Click **Add** to add a new rule, or click **Edit** to edit an existing rule.
- b. Configure the rule properties:
- **IP Address**—The network object that identifies the hosts or networks you are allowing to make HTTPS connections. Choose an object from the drop-down menu, or add a new network object by clicking **+**.
 - **Security Zones**—Add the zones that contain the interfaces to which you will allow HTTPS connections. For interfaces not in a zone, you can type the interface name into the field below the Selected Security Zone list and click **Add**. These rules will be applied to a device only if the device includes the selected interfaces or zones.
- c. Click **OK**.
- Step 6**
- Click **Save**.
- You can now click **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

ICMP:

To protect the device from attacks, you can use ICMP rules to limit ICMP access to interfaces to particular hosts, networks, or ICMP types. ICMP rules function like

access rules, where the rules are ordered, and the first rule that matches a packet defines the action.

If you configure any ICMP rule for an interface, an implicit deny ICMP rule is added to the end of the ICMP rule list, changing the default behavior. Thus, if you want to simply deny a few message types, you must include a permit any rule at the end of the ICMP rule list to allow the remaining message types.

ICMP UnReachable

Rate Limit

1
(1 - 100)

Burst Size

1
(1 - 10)

+ Add

Action	ICMP Service	Interface	Network
No records to display			

Secure Shell:

You can add SSH tunnels to your available Zones/interfaces.

Add Secure Shell Configuration

IP Address* +

Available Zones C

Q Search

AVGDMZ

CUST-EDGE

dmz1

dmz2

dmzsw

inside

outside

Add

Selected Zones/Interfaces

Interface Name Add

Cancel OK

SMTP Server:

You must identify an SMTP server if you configure email alerts in the Syslog settings. The source email address you configure for Syslog must be a valid account on the SMTP servers.

Primary Server Ip Address +

Secondary Server Ip Address +

SNMP:

Simple Network Management Protocol (SNMP) defines a standard way for network management stations running on PCs or workstations to monitor the health and status of many types of devices, including switches, routers, and security appliances. You can use the SNMP page to configure a firewall device for monitoring by SNMP management stations.

The Simple Network Management Protocol (SNMP) enables monitoring of network devices from a central location. Cisco security appliances support network monitoring using SNMP versions 1, 2c, and 3, as well as traps and SNMP read access.

☒ Enable SNMP Servers

Read Community String

Confirm*

System Administrator Name

IT x5850

Location

Spokane, WA







Listen Port

161

(1 - 65535)

HostsUsersSNMP Traps

+ Add

Interface	Network	SNMP Version	Poll/Trap	Trap Port	Username	
inside		2c	Poll	162		 
inside		2c	Poll	162		 
inside		2c	Poll	162		 

SSL:

Procedure

- Step 1** Select **Devices > Platform Settings** and create or edit a Firepower Threat Defense policy.
- Step 2** Select **SSL**.
- Step 3** Add entries to the **Add SSL Configuration** table.
- Click **Add** to create a new entry, or click **Edit** if the entry already exists.
 - Select the required security configurations from the drop-down list .
 - Protocol Version**—Specifies the TLS protocols to be used while establishing remote access VPN sessions.
 - Security Level**—Indicates the kind of security positioning you would like to set up for the SSL.
- Step 4** Select the **Available Algorithms** based on the protocol version that you select and click **Add** to include them for the selected protocol. For more information, see [About SSL Settings](#)
- The algorithms are listed based on the protocol version that you select. Each security protocol identifies unique algorithm for setting up the security level.
- Step 5** Click **OK** to save the changes.

Syslog:

Here, we can add our Syslog servers.

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
S

Basic Logging Settings

☒ Enable Logging
☐ Enable Logging on the failover standby unit
☐ Send syslogs in EMBLEM format
☐ Send debug messages as syslogs

Memory Size of the Internal Buffer

1048576

(4096-52428800 Bytes)

VPN Logging Settings

☒ Enable Logging to FMC

Logging Level

errors

Specify FTP Server Information

☐ FTP Server Buffer Wrap

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
Syslog Settings
Syslog Servers

☒ Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)*

512

(0 - 8192 messages). Use 0 to indicate unlimited Queue Size

+ Add

Interface	IP Address	Protocol	Port	EMBLEM	SECURE	
inside		UDP	514	false	false	
inside		UDP	514	false	false	

Timeouts:

These consist of SIP timeouts, console timeouts, Connection timeouts, etc.
Choose your liking.

Console Timeout*

0

(0 - 1440 mins)

Translation Slot(xlate)

Default

3:00:00

(3:0:0 or 0:1:0 - 1193:0:0)

Connection(Conn)

Default

1:00:00

(0:0:0 or 0:5:0 - 1193:0:0)

Half-Closed

Default

0:10:00

(0:0:0 or 0:30 - 1193:0:0)

UDP

Default

0:02:00

(0:0:0 or 0:1:0 - 1193:0:0)

ICMP

Default

0:00:02

(0:0:2 or 0:0:2 - 1193:0:0)

RPC/Sun RPC

Default

0:10:00

(0:0:0 or 0:1:0 - 1193:0:0)

H.225

Default

1:00:00

(0:0:0 or 0:0:0 - 1193:0:0)

H.323

Default

0:05:00

(0:0:0 or 0:0:0 - 1193:0:0)

SIP

Default

0:30:00

(0:0:0 or 0:5:0 - 1193:0:0)

SIP Media

Default

0:02:00

(0:0:0 or 0:1:0 - 1193:0:0)

SIP Disconnect:

Default

0:02:00

(0:02:0 or 0:0:1 - 0:10:0)

SIP Invite

Default

0:03:00

(0:1:0 or 0:1:0 - 0:30:0)

SIP Provisional Media

Default

0:02:00

(0:2:0 or 0:1:0 - 0:30:0)


Time Synchronization:

Can either set NTP from Management Center or if you have NTP servers, set it to there.

Set My Clock

☒ Via NTP from Management Center

☐ Via NTP from


 This setting is unsupported on firepower 9300 and Firepower 4100 platforms. Please use Firepower Chassis Manager instead to set NTP time synchronization.

Time Zone:


Generally, you can leave blank and it will default to UTC. If not, you can specify your time zone.

Time Zone:

 +

 Time-based rules in supported policies are applied based on the time zone assigned to the device.

 Time Zone setting is supported on FTD version 6.6.0 and above.

 If no Time Zone is selected, Time Zone will be UTC Time Zone (UTC + 00:00).

FlexConfig:

Certificates:

Objects

Object Management:

Access List:

You can put standard/extended access lists in these categories revolving around your objects/object groups.

Address Pools:

These will usually contain your VPN pools.

IPv4 Pools			
IPv4 pool contains list of IPv4 addresses, it is used for diagnostic interface with clustering, or for VPN remote access profiles.			
		Add IPv4 Pools	<input type="text" value="Filter"/>
Name	Value	Override	
VPN-Pool			

Application filters:

You can organize your applications by creating a filter based on certain characteristics.

AS Path:

Mandatory for BGP config, don't need unless you are doing BGP. AS path is a sequence of AS numbers between source and destination routers that form a directed route for packets to travel.

Cipher Suite List:

Object comprised of several cipher suites. Each cipher suite value represents a cipher suite used to negotiate SSL or TLS encryption sessions. You can use these cipher suite lists in SSL rules to control encrypted traffic based on whether the client and server negotiated the SSL session using that suite.

Community List:

Transitive BGP attribute. Groups of destinations that share some common attribute, used for route tagging. The community list is an ordered list of matching statements. Destinations are matched against the rules until a match is found.

Individual Objects:

Distinguished name object represents the distinguished name listed for a public key certificate's subject or issuer. You can use distinguished name objects in SSL rules to control encrypted traffic based on whether the client and server negotiated the SSL session using a server certificate with the distinguished name as subject or issuer.

Object Groups:

Each distinguished name object represents the distinguished name listed for a public key certificate's subject or issuer. You can use distinguished name object groups in SSL rules to control encrypted traffic based on

whether the client and server negotiated the SSL session using a server certificate with the distinguished name as subject or issuer.

DNS Server Group:

A DNS server group is a list of one or more DNS servers and connection settings to use for connecting.

File list:

If you use AMP for Firepower, and the AMP cloud incorrectly identifies a file's disposition, you can add the file to a file list to better detect the file in the future. There are two predefined categories of file lists, Clean List - System treats it as if the AMP cloud assigned a clean disposition Custom Detection List - System treats it as if the AMP cloud assigned a malware disposition.

FlexConfig object:

FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig policies.

FlexConfig Text Object:

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Geolocation:

Geolocation represents one or more countries or continents that the system has identified as the source or destination of traffic on your monitored network. It is used in various places like access control policies, SSL policies, and event searches.

Interface:

Interface objects segment your network to help you manage and classify traffic flow. An interface object simply groups interfaces. These groups may span multiple devices; you can also configure multiple interface objects on a single device.

You want to make sure the zones we create are tied to the correct interface group. Afterwards, go to your device management and look at your ftd's interfaces. Make sure the zone matches your interface group.

Key Chain:



A list of keys that allows you to use in different policies.

Network:

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

PKI Cert enrollment:

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Cert Enrollment			
			Add Cert Enrollment <input type="text" value="Filter"/>
A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).			
Name	Type	Override	
	PKCS12 File		 

Edit Cert Enrollment

Name* [Redacted]
Description [Redacted]

CA Information Certificate Parameters **Key** Revocation

Enrollment Type: [Redacted]
PKCS12 File: [Redacted] [Browse PKCS12 File](#)
Passphrase: [Redacted]

☐ Allow Overrides

Cancel Save

Key Type:
☒ RSA ☐ ECDSA
Key Name: * <Default-RSA-Key>
Key Size: 2048

Advanced Settings
☐ Ignore IPsec Key Usage
Do not validate values in the Key Usage and extended Key Usage extensions of IPsec remote client
☐ Allow Overrides

Cancel Save

CA Information Certificate Parameters **Key** **Revocation**

☐ Enable Certificate Revocation Lists (CRL)
☒ Use CRL distribution point from the certificate
☐ User static URL configured
CRL Server URLs: * [Redacted]
☐ Enable Online Certificate Status Protocol (OCSP)
☐ Allow Overrides

Cancel Save

External Cert Groups:

External certificate object represents a server public key certificate that does not belong to your organization. You can use external certificate objects in SSL rules to control traffic encrypted with the server certificate.

External Certs:

External certificate object represents a server public key certificate that does not belong to your organization. You can use external certificate objects in SSL rules to control traffic encrypted with the server certificate.

Internal CA Groups:

Internal certificate authority (CA) object represents the CA public key certificate of a CA your organization controls. You can use internal CA objects in SSL rules to decrypt outgoing encrypted traffic by re-signing the server certificate with the internal CA.

Internal CAs:

Internal certificate authority (CA) object represents the CA public key certificate of a CA your organization controls. You can use internal CA objects in SSL rules to decrypt outgoing encrypted traffic by re-signing the server certificate with the internal CA.

Internal Cert Groups:

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Internal Certs:

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Trusted CA Groups:

Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.

Trusted CAs:

Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.

Policy List:

Policy list objects is used when configuring route maps. When a policy list is referenced within a route map, all of the match statements within the policy list are evaluated and processed.

Port:

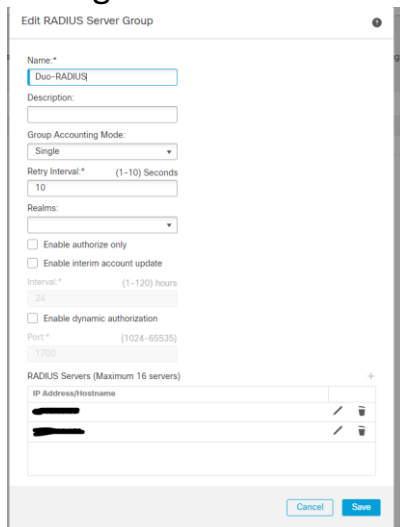
Port objects or groups represent different protocols. You can use port objects and groups in various places in the systems web interface, including access control policies, identity rules, network discovery rules, port variables, and event searches.

IPv4 Prefix List:

Prefix lists work like access lists for route advertisements (prefixes). You can create prefix list objects for IPv4 to use when you are configuring route maps, policy maps, OSPF Filtering, or BGP Neighbor Filtering

Radius Server Group:

RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.



The screenshot shows the 'Edit RADIUS Server Group' configuration window. It includes fields for 'Name' (set to 'Duo-RADIUS'), 'Description', 'Group Accounting Mode' (set to 'Single'), 'Retry Interval' (set to '10' seconds), 'Realms', and checkboxes for 'Enable authorize only', 'Enable interim account update', and 'Enable dynamic authorization'. There are also fields for 'Interval' (set to '24' hours) and 'Port' (set to '1700'). At the bottom, there is a section for 'RADIUS Servers (Maximum 16 servers)' with a table for adding servers, including columns for 'IP Address/hostname' and 'Port'. The 'Cancel' and 'Save' buttons are at the bottom right.

Route Map:







Route maps are used when redistributing routes into any routing process. They are also used when generating a default route into a routing process. A route map defines which of the routes from the specified routing protocol are allowed to be redistributed into the target routing process.

Security Group Tag:

A Security Group Tag (SGT) object specifies a single SGT value. You can use SGT objects in rules to control traffic with SGT attributes that were not assigned by Cisco ISE. You cannot group or override SGT objects.


DNS Lists and Feeds:

DNS lists and feeds helps you quickly filter traffic by collecting Domain Names. Its used in DNS policies to blacklist and whitelist as part of Security Intelligence

Name	Type	
Cisco-DNS-and-URL-Intelligence-Feed Last Updated: 2021-11-15 18:10:01	Feed	 
Global-Blacklist-for-DNS	List	 
Global-Whitelist-for-DNS	List	 

Network Lists and Feeds:

Network lists and feeds helps you quickly filter traffic by collecting IP address and address blocks. Its used in access control policies to blacklist and whitelist as part of Security Intelligence.

Name	Type	
Cisco-Intelligence-Feed Last Updated: 2021-11-15 18:09:59	Feed	 
Cisco-TID-Feed Last Updated: 2021-11-15 19:01:27	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

URL Lists and Feeds:

URL lists and feeds help you quickly filter traffic by collecting URLs. Its used in access control policies to blacklist and whitelist as part of Security Intelligence. You can also use URL lists in access control and QoS rules, whose analysis and traffic handling phases occur after Security Intelligence.

Name	Type	
Global-Blacklist-for-URL	List	 
Global-Whitelist-for-URL	List	 

Sinkhole:

A sinkhole object represents either a DNS server that gives non-routeable addresses for all domain names within the sinkhole, or an IP address that does not resolve to a server. You can reference the sinkhole object within a DNS policy rule to redirect matching traffic to the sinkhole.

SLA Monitor:

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Time Range:

Time range object represents the time interval. You can use it to apply a policy only during times you specify.

Time Zone:

Time range objects in supported policies are applied based on the time zone specified in device platform settings.

Tunnel Zone:

A tunnel zone represents certain types of plaintext, passthrough tunnels that you explicitly tag for special analysis. A tunnel zone is not an interface object, even though you can use it as an interface constraint in some configurations.

URL:

URL object represents a single URL or IP address. You can use URL objects and groups in various places, including access control policies and event searches. For example, you could write an access control rule that blocks a specific website.

URL			
		Add URL	Q Filter
URL object represents a single URL or IP address. You can use URL objects and groups in various places, including access control policies and event searches. For example, you could write an access control rule that blocks a specific website.			
Name	Value	Override	
Duo	https://vpn. [REDACTED]		/ [REDACTED]
TeamViewer	https://login.teamviewer.com		/ [REDACTED]
[REDACTED]			/ [REDACTED]

Variable Set:

Variables represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppressions, adaptive profile updates, and dynamic rule states.

Edit Variable Set Cerium-Variable-Set

Name:

Description:

Enter Description

Add

Variable Name	Type	Value	
Customized Variables			
EXTERNAL_NET	Network	!!IPv4-Private-All-RFC1918	/C
HOME_NET	Network	[IPv4-Private-All-RFC1918, !CUST-EDGE-1...]	/C
Default Variables			
DNS_SERVERS	Network	HOME_NET	/C
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	/C
FTP_PORTS	Port	[21, 2100, 3535]	/C
GTP_PORTS	Port	[3386, 2123, 2152]	/C
HTTP_PORTS	Port	[8300, 8040, 36099, 2231, 90, 16995, 67...]	/C

Cancel
Save

Variable Name	Type	Value	
HTTP_SERVERS	Network	HOME_NET	/C
ORACLE_PORTS	Port	any	/C
SHELLCODE_PORTS	Port	!80	/C
SIP_PORTS	Port	[5600, 5061, 5060]	/C
SIP_SERVERS	Network	HOME_NET	/C
SMTP_SERVERS	Network	HOME_NET	/C
SNMP_SERVERS	Network	HOME_NET	/C
SQL_SERVERS	Network	HOME_NET	/C
SSH_PORTS	Port	22	/C

VLAN Tag:

VLAN tag object represents a VLAN tag or range of tags.

VPN AnyConnect File:

File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.













AnyConnect File			Add AnyConnect File	Filter
File objects represent files used in configurations, typically for remote access VPN policies. They can contain AnyConnect Client Profile and AnyConnect Client Image files.				
Name	Value	Type		
Anyconnect	anyconnect-win-4.9.05042-webdeploy-k9.pkg	AnyConnect Client...	↓	✕
anyconnect-linux64-4.9.05042-webdeploy-k9.pkg	anyconnect-linux64-4.9.05042-webdeploy-k9.pkg	AnyConnect Client...	↓	✕
anyconnect-macos-4.9.05042-webdeploy-k9.pkg	anyconnect-macos-4.9.05042-webdeploy-k9.pkg	AnyConnect Client...	↓	✕
Anyconnect_4.9.06037	anyconnect-win-4.9.06037-webdeploy-k9.pkg	AnyConnect Client...	↓	✕

VPN Certificate Map:

Certificate Map Object is used to provide an association between a received certificate and a Remote Access VPN connection profile. If a received certificate matches the rules contained in the certificate map, the connection is associated with the specified connection profile.









VPN Group Policy:

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Group Policy	
A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience. The RADIUS authorization server assigns the group profile.	
Name	
	 
Contractor	 
DfltGrpPolicy	 
Employee	 
Engineer	 
MnlGrpPolicy	 

IKEv1 IPsec Proposal:

IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv1 IPsec Proposal object, single encryption and Hash algorithm is allowed.

IKEv1 IPsec Proposal	
IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv1 IPsec Proposal object, single encryption and Hash algorithm is allowed.	
Name	
tunnel_aes128_sha	 
tunnel_aes192_sha	 
tunnel_aes256_sha	 
tunnel_des_sha	 

IKEv1 Policy:

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). IKEv1, IKE proposals contain a single set of algorithms and a modulus group.

IKEv2 IPsec Proposal:

IPsec security association negotiation with ISAKMP, the peers agree to use a particular proposal to protect a particular data flow. In IKEv2 IPsec Proposal object, you can select multiple encryption and Hash Algorithms are allowed. During IKEv2 negotiations, the peers select the most appropriate options that each support.

IKEv2 Policy:

Internet Key Exchange (IKE) is a key management protocol that is used to authenticate IPsec peers, negotiate and distribute IPsec encryption keys, and automatically establish IPsec security associations (SAs). IKEv2 proposal, you can select multiple algorithms and modulus groups in one policy

Intrusion Rules:

You can view the exact rules here if you want to manually touch them. However, it is best just to go to your intrusion policy and edit rules there.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Tuning_Intrusion_Policies_Using_Rules.html

AMP

AMP Management:

Connects to the US Cloud for AMP for Endpoints/AMP for Networks. (Sometimes, you may need to remove the AMP cloud connection and re-initiate it for it to sync properly) Sign into your CCO account and the integration will take place.

Dynamic Analysis Connections:

Connects to Threat-grid for dynamic analysis and sending SHAs to sandboxes for further inspection. You can hit the associate button to sign

into your CCO account to initiate the integration between firepower and Threat-grid.

Intelligence

Incidents:

Sources:

Elements:

Settings:

Analysis

Context Explorer:

Acts like a main summary page of all the analysis subsections of events. Includes context about the status of your network. Includes graphs about indications of compromise, network information, application protocol information, security intelligence, intrusion information, etc.

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using the Context Explorer.html>

Connection Events:

This is where you can see all of your connections with application details. You can see the first to last packet, initiator and responder IPs, ingress and egress security zones, ports, application protocol, etc. This can be a super helpful area if you are doing threat hunting and wanted to search a specific traffic flow that happened.

You can also click on a specific host profile and see things like the Device name, Mac addresses, loc, Operating system, servers it has touched, Applications it has touched, etc.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/connection_and_security_intelligence_events.html

Connection Security Intelligence Events:

These events are focused on your blocks. If you have geolocation on for instance, it will show mostly blocked IPs from countries you don't want connections to. (Ex. Russia IP attempts, North Korea IP connection attempts, etc.) You can see the initiator IP, responder IP, and the type of intelligence category that was blocked. You can also see the egress/ingress zones as well as the port.

You can also open the host view as well from the received IP and see any IOC, device name, MAC address, etc that was involved in the blocking event.

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

Intrusion Events:

All of your intrusion events will be in this section. There you can go into threat hunting to analyze who was the target, what exactly was vulnerable, what was the vulnerability, was the event blocked/stopped, etc. You can then use the Intrusion event packet view. The packet view indicates why a specific packet was captured by providing information about the intrusion event that the packet triggered, including the event's time stamp, message, classification, priority, and, if the event was generated by a standard text rule, the rule that generated the event. The packet view also provides general information about the packet, such as its size.

If intrusion events occur... It is best practice to go into your intrusion policy to add any rules to the drop and generate event rule section to make sure the intrusion event that occurred does not occur again. You will also see a Firepower Recommendations section that can help auto update your rules as well to match the traffic/events you have been seeing.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110000.html

Intrusion Reviewed Events:

Once an event goes under some analysis, you can push that intrusion event to your reviewed events for organization. You can also make notes to what you have done such as added an intrusion policy rule after seeing the event, etc.

Intrusion Clipboard:

Clipboard — To add an event to the clipboard so you can transfer it to the incidents at a later time, click Copy to copy the event whose packet you are viewing or click Copy All to copy all the events whose packets you previously selected.

Intrusion Incidents:

These are intrusion events that you suspect are involved in a possible violation of your security. This leads into the topic of incident handling which can be more discussed here:

<https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/incidents.html>

File Malware Events:

These are different events that will show attempted malware in your environment caught by the fmc. It will show the file name, file SHA256, file type, and hit count. If you click into the file name, you will see the receiving IP, the user who tried to access it, the event type (blocked or allowed), the event subtype, and more.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110001.html

File events:

Similar to malware events, file events show a type of file, disposition, action, and hit count of them. You can then click on the type and see all the malware cloud lookups for that file. It will show you the sending IP, country, receiving IP, port, receiving protocol, user, the file name, and the cloud disposition of the SHA lookup.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110001.html

File captured files:

This shows a summary of your captured files, each with a rating threat score of low to high. It shows you the type of file and the category the file belongs in, as well as the hit count. If you click on the type or category, you can then filter your events by that attribute to see all the file names, SHAs, threat score, types, etc your fmc has found sifting through traffic.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110001.html

File Network File Trajectory:

To further target your analysis, you can use a malware file's network file trajectory (a map of how the file traversed your network, passing among hosts, as well as various file properties) to track the spread of an individual threat across hosts over time, allowing you to concentrate outbreak control and prevention efforts where most useful.

If you configure local malware analysis or dynamic analysis in a file rule, the system preclassifies files matching the rule and generates a file composition report.

If your organization has deployed AMP for Endpoints and integrated that deployment with your Firepower Management Center, you can also import records of scans, malware detections, and quarantines, as well as indications of compromise (IOC) identified by that product. This data is displayed alongside event data gathered by Firepower for a more complete picture of malware on your network.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/fpmc-config-guide-v60_chapter_01110001.html#concept_5511F4FCC2504C54A8A759136F7FE17D

Hosts Network Map:

Here, you can see all of your hosts based on the IP, IPv6, or MAC. You can then click on a certain IP and it will list its host profile, IOC, OS, applications, etc.

Network devices contains the same layout except with this case, it is network devices, not hosts. You can also search IPs for mobile hosts as well to see any devices that are phones attached to your network, given an IP in your subnet.

Can search by Indications of Compromise as well, application protocols, vulnerabilities, and host attributes.

<https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Using the Network Map.html#ID-2222-00000068>

Hosts:

The host category breaks hosts down in groups. You start with a summary of OS names, then OS version, down to OS details with IP, and then

whatever host is connected with that IP. It is a really great category to see what OS versions are connected in your network if your IT department is trying to get rid of WIN 7 machines and needs to tie it to a host for example.

Indications of Compromise:

Here, you can see categories and hit counts of IoC. Some categories will be malware Downloaded, CnC connected, impact 2 attacks, malware detection and malware execution, etc. You can then click on the category and see all of your IP addresses that match that category of compromise. It will list the event type, description, first seen and last seen time variables.

From here, you can see the exact IPs with these compromised events. You will want to click on the red host profile. You will be able to do a deep dive on the IoC event to further threat hunt.

Applications:

You can see all the applications that your FMC/FTDs have identified. It will also show the host count that have hit those applications such as SSL clients, Microsoft apps, O365 apps, etc.

Application Details:

This section is just like the Application section however it specifies the web application, application protocol, and client group with the hit count. (Not just the application and hit count)

Servers:

The Servers Section of the host profile lists servers either detected on hosts on your monitored network, added from exported NetFlow records, or added through an active source like a scanner or the host input feature. The list can include up to 100 servers per host. After that limit is reached, new server information from any source, whether active or passive, is discarded until you delete a server from the host or a server times out.

If you scan a host using Nmap, Nmap adds the results of previously undetected servers running on open TCP ports to the Servers list. If you perform an Nmap scan or import Nmap results, an expandable Scan Results section also appears in the host profile, listing the server information detected on the host by the Nmap scan. In addition, if the host is deleted from the network map, the Nmap scan results for that server for the host are discarded.

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/using_host_profiles.html#ID-2218-00000207

Host Attributes:

You can use host attributes to classify hosts in ways that are important to your network environment. The Firepower Management Center provides two predefined host attributes:

Host Criticality

Use this attribute to designate the business criticality of a given host and to tailor correlation responses to host criticality. For example, if you consider your organization's mail servers more critical to your business than a typical user workstation, you can assign a value of High to your mail servers and other business-critical devices and Medium or Low to other hosts. You can then create a correlation policy that launches different alerts based on the criticality of an affected host.

Notes

Use this host-specific attribute to record information about the host that you want other analysts to view. For example, if you have a computer on the network that has an older, unpatched version of an operating system that you use for testing, you can use the Notes feature to indicate that the system is intentionally unpatched.

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/using_host_profiles.html#ID-2218-00000493

Discovery Events:

The Discovery Statistics page displays a summary of the hosts, events, protocols, application protocols, and operating systems detected by the system.

The page lists statistics for the last hour and the total accumulated statistics. You can choose to view statistics for a particular device, or all devices. You can also view events that match the entries on the page by clicking the event, server, operating system, or operating system vendor listed within the summary.

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/working_with_discovery_events.html

Vulnerabilities:

Here we can see all the vulnerabilities that the snort engine has gathered by analyzing traffic/packets. You can also see vulnerabilities in detail and “on the network” as well. It will list an IP address, the snort ID, title of the CVE, vulnerability impact, description, etc. You can click on the specific vulnerability to filter all the IPs that have it or you can filter based on vulnerability impact score and tackle each one from there.

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/configuration/guide/fpmc-config-guide-v64/using_host_profiles.html#ID-2218-000006a7

Third-Party Vulnerabilities:

Same as above except more focused on adding a mapping to a vulnerability. If you had more information about a CVE from a third party

resource, you can create a new vulnerability map set and enter the identification of the vulnerability ID and enter a description.

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/host_identity_sources.html#ID-2219-00000344

Users Active Sessions:

Here, you will be able to see VPN authentication types. Whenever a user signs onto the vpn, it will log it in the Users active sessions area. You can see current IPs, time stamps, and discover identities of the user. You can also see the discovery application (most likely LDAP if it is a vpn authentication) and the device (most likely firewall).

User:

This is a list of discovered users in your network, found by the FTDs and mapping logon usernames to the discovery application.

User Activity:

Like above, you can see users signing into an application with the VPN authentication type. It will contain time stamps, event types, users, discovery application, IP addresses, the VPN session type, what VPN group policy attached, VPN connection profile, vpn client public IP, etc.

User indications of Compromise:

Same as the other indications of compromise category except specifically with users.

Correlation Events:

You can use the correlation feature to respond in real time to threats to your network, using correlation policies. A correlation policy violation occurs when the activity on your network triggers either a correlation rule or compliance white list within an active correlation policy. For example,

you can create a correlation rule that a discovery event occurs and an new IP host is detected and it meets the following conditions: IP address is in 10.4.0.0/16. Generally used for creating whitelists as well.

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/Correlation_Policies.html#ID-2204-0000011a

Allow List Events:

Events that hit the allowed list.

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

Allow List Violations:

Events that violated the allow list.

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

Status:

Shows current status of events.

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

Advanced Custom Workflows:

If the predefined and Cisco-provided custom workflows do not meet your needs, you can create and manage custom workflows.

Custom workflows are workflows that you create to meet the unique needs of your organization. When you create a custom workflow, you choose the kind of event (or database table) on which the workflow is based. On the Firepower Management Center, you can base a custom workflow on a custom table. You can also choose the pages a custom workflow contains; custom workflows can contain drill-down, table view, and host or packet view pages. Defaults are down below...

Table 1. Saved Custom Workflows

Workflow Name	Description
Events by Impact, Priority, and Host Criticality	<p>You can use this workflow to quickly pick out and focus in on hosts that are important to your network, currently vulnerable, and possibly currently under attack.</p> <p>This workflow is based on the Intrusion Events with Destination Criticality custom table.</p>
Events by Priority and Classification	<p>This workflow lists events and their type in order of event priority, along with a count showing how many times each event has occurred.</p> <p>This workflow is based on the Intrusion Events custom table.</p>
Events with Destination, Impact, and Host Criticality	<p>You can use this workflow to find the most recent attacks on hosts that are important to your network and currently vulnerable.</p> <p>This workflow is based on the Intrusion Events with Destination Criticality custom table.</p>
Hosts with Servers Default Workflow	<p>You can use this workflow to quickly view the basic information in the Hosts with Servers custom table.</p> <p>This workflow is based on the Hosts with Servers custom table.</p>
Intrusion Events with Destination Criticality Default Workflow	<p>You can use this workflow to quickly view the basic information in the Intrusion Events with Destination Criticality custom table.</p> <p>This workflow is based on the Intrusion Events with Destination Criticality custom table.</p>
Intrusion Events with Source Criticality Default Workflow	<p>You can use this workflow to quickly view the basic information in the Intrusion Events with Source Criticality custom table.</p> <p>This workflow is based on the Intrusion Events with Source Criticality custom table.</p>
Server and Host Details	<p>You can use this workflow to determine what servers are most frequently used on your network and which hosts are running those servers.</p> <p>This workflow is based on the Hosts with Servers custom table.</p>

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

Custom Tables:

You can create custom tables in Analysis, advanced, custom tables. Click view to see the custom table you want to view, then customize the table. If you want to create your own, at the top right, you can click create your own custom table. You can then select fields such as applications, business relevance, versioning, web applications, etc.

https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/custom_workflows.html#D-2191-00000bf5

GeoLocation:

You can search up specific IPs to find the country, country code, continent, etc of a public IP.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/using_lookups.html

URL:

You can search urls to get a reputation score as well as a category list. For instance, you can enter google.com. The category will come up as a search engine and the reputation comes up as Trusted.

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/using_lookups.html

Whois:

Can enter in a public ip address to get a whole whois report on the public IP. Everything from ISP provider name, address information, org handlers, CIDR range, etc.

https://www.cisco.com/c/en/us/td/docs/security/firepower/622/configuration/guide/fpmc-config-guide-v622/using_lookups.html

Contextual Cross-Launch:

Allows for boosted threat hunting by increasing our threat research vector by combining cisco/third party security solutions to gather more data. This makes external integrations with the FMC event views possible. There are dozens of cross-launch integration links included and you can even create your own custom links. Very handy for pivoting to other systems to gain additional context around a Firepower event.

https://www.cisco.com/c/en/us/td/docs/security/firepower/630/configuration/guide/fpmc-config-guide-v63/analyze_events_using_external_tools.html

<https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/BRKSEC-3328.pdf>

Troubleshooting Commands for Cut:

packet-tracer input INSIDE icmp 192.168.103.1 80 192.168.101.1
packet-tracer input (interface) (protocol) (source address) (icmp type) (icmp code) (destination IP address)

capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
capture (name of capture) interface (name of interface) match (protocol) host (Source IP)

Turn crypto debugging on, then generate your packet tracer.

Show Commands for ASA/FTD commands for IPsec VPN:

show crypto ipsec stats
show vpn-sessiondb license-summary
show Version
show run crypto map
more system:running-config
show run crypto ikev2
show crypto isakmp sa
show vpn-sessiondb anyconnect
show vpn-sessiondb detail I2I

IKE S2S w/ IPsec show commands:

show crypto isakmp policy

show crypto engine connections active
show crypto isakmp keys
show crypto map
show crypto isakmp sa
debug crypto isakmp
debug crypto ipsec

DMVPN Show commands:

show dmvpn
show ip nhrp
show crypto engine connections active
show ip route
show crypto map
show ip cef [network]
show crypto ipsec sa
show crypto isakmp sa

Flex VPN:

show crypto ikev2 proposal
show crypto ikev2 sa
show crypto ipsec transform-set
show crypto ipsec profile
show crypto ipsec sa
show crypto map

GET VPN w/ Key Server:

show crypto gdoi
show crypto gdoi ks
show crypto isakmp sa detail
show crypto ipsec sa

Remote Access VPNs:

show crypto pki cert
show ip int bri
show ip route
show crypto ikev2 sa

```
show vpn-sessiondb remote
```