

Securing Networks with
Cisco FTD

Chapter 8

Access Control Policy

Mohsen Kheradmand

Access Control Policy

Allows you to create access control rules to match traffic and apply an action on matched traffic

There are 2 editor :

Access Control Policy Editor : set of rules , applicable to a threat defense

Access Control Rule Editor : group of setting to allow, deny , and log traffic

- The other security policies, such as intrusion policies and file policies, have their own policy editors

Policy Editor

Policies > Access Control

The screenshot displays the Cisco Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and a breadcrumb trail "Policies / Access Control / Access Control". The main navigation menu contains tabs for Overview, Analysis, Policies (selected), Devices, Objects, AMP, and Intelligence. On the right, there are links for Deploy, a search icon, a notification bell with a "2" badge, a settings gear, a help icon, and the user name "kheradmand".

The "Policies" dropdown menu is open, showing a list of policy types: Access Control (highlighted with a mouse cursor), Network Discovery, Application Detectors, Correlation, Intrusion, Malware & File, DNS, Identity, SSL, and Prefilter. To the right of this menu, there is a section for "Actions" with a list: Alerts, Scanners, Groups, Modules, and Instances.

Below the navigation, a table lists existing policies:

Access Control Policy	Domain
My Policy functional policy	Global
Second Policy this is a alternative	Global

On the right side of the interface, there is a "New Policy" button and a list of policies. The first policy is "Network Analysis Policy | DNS | Import/Export". Below it, two policy entries are visible, each with a pencil icon circled in red, indicating the edit function:

- Policy 1: "6:07:15 kheradmand" with a pencil icon circled in red.
- Policy 2: "6:29:13 kheradmand" with a pencil icon circled in red.

- Click the pencil icon next to a policy name to open it in the policy editor
- If no access control policy has been created yet, you can create a new one by clicking the New Policy button

Policy Editor

Access control rule editor

 Firepower Management Center

Overview

Analysis

Policies

Devices

Objects

AMP

Intelligence

Deploy     kheradmand

Second Policy

this is a alternative

Analyze Hit Counts Save Cancel

[Inheritance Settings](#) | [Policy Assignments \(0\)](#)

Rules

Security Intelligence

HTTP Responses

Logging

Advanced

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

[Filter by Device](#)  ☐ Show Rule Conflicts  + [Add Category](#) [+ Add Rule](#)

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action	       
Mandatory - Second Policy (1-2)															
1	clients-server	Inside-LAN	Servers	Clients	Servers	Any	Any	Any	Any	Any	Any	Any	Any	 Monitor       0  	
2	Sale-to-SRVs	LAN	Servers	R2	Servers	Any	Any	Any	FTP HTTP HTTPS	FTP HTTP HTTPS	Any	Any	Any	 Allow       0  	
Default - Second Policy (-)															
There are no rules in this section. Add Rule or Add Category															

Policy Editor

Summary of some of the options:

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 5 ⚙️ ? kheradmand ▼

Second Policy

this is a alternative

Analyze Hit Counts Save Cancel

[Inheritance Settings](#) | [Policy Assignments \(0\)](#)

Rules Security Intelligence HTTP Responses Logging Advanced

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

[Filter by Device](#) 🔍 Search Rules × ☐ Show Rule Conflicts ⓘ + Add Category + Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action	Icons
▼ Mandatory - Second Policy (1-2)															
1	clients-server	Inside-LAN	Servers	Clients	Servers	Any	Any	Any	Any	Any	Any	Any	Any	Monitor	Icons
2	Sale-to-SRV	LAN	Servers	R2	Servers	Any	Any	Any	FTP HTTP HTTPS	FTP HTTP HTTPS	Any	Any	Any	Allow	Icons
▼ Default - Second Policy (-)															
There are no rules in this section. Add Rule or Add Category															

- **Rules:** To view the access control rules with their rule conditions. Traffic is evaluated in top-down order.
- **Security Intelligence:** To block connections based on reputation and intelligence data.
- **HTTP Responses:** To display a response page when a threat defense detects an attempt to access a website.
- **Logging:** To set up destinations for syslog messages
- **Advanced:** To configure advanced options that can influence the performance of a threat defense

Policy Editor

- **Policy Assignment:** you can create and save many access control policies on your FMC ,but you can deploy only one access control policy to your FTD at any time.

The screenshot displays the Cisco FMC Policy Editor interface. At the top, navigation links include [Inheritance Settings](#) and [Policy Assignments \(2\)](#), with the latter circled in red. Below these, status indicators show: Prefilter Policy: [Default Prefilter Policy](#), SSL Policy: [None](#), and Identity Policy: [None](#). The main section is titled "Policy Assignments" and features a "Targeted Devices" tab. A message prompts the user to "Select devices to which you want to apply this policy." The interface is divided into "Available Devices" and "Selected Devices" columns. In the "Available Devices" list, "EVE", "VMs", "FTD1", and "FTD2" are shown, with "FTD2" highlighted. An "Add to Policy" button is positioned between the columns, with a mouse cursor hovering over it. The "Selected Devices" column currently lists "FTD1" and "FTD2". An "Error" dialog box is overlaid on the right, containing the following text: "Following devices already have assignments listed below. These devices will be reassigned to current policy" and "device: FTD1 - policy: Default policy". It then asks, "Do you want to continue with above changes?" with "No" and "Yes" buttons. At the bottom of the main interface, "Cancel" and "OK" buttons are visible.

Policy Editor

- Default Action:
 - To define how the traffic that does not match any existing access control rule conditions is handled by FTD

You can choose to apply one of the following actions to the remaining unmatched traffic:

- Block all the remaining unmatched traffic.
- Trust all the remaining unmatched traffic.
- Discover only the host, user, and application details.
- Inspect traffic against an intrusion policy.



Rule Editor

Select the policy and Click the Add Rule button on the policy editor.

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis **Policies** Devices Objects AMP Intelligence

Deploy 🔍 2 ⚙️ ? kheradmand ▼

My Policy
functional policy

Show Warnings Analyze Hit Counts Save Cancel

[Inheritance Settings](#) | [Policy Assignments \(2\)](#)

Rules Security Intelligence HTTP Responses Logging Advanced

Filter by Device 🔍 Search Rules X ☐ Show Rule Conflicts ? + Add Category **+ Add Rule**

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source Dynamic Attributes	Destinat... Dynamic Attributes	Action	🛡️ 🛡️ 🛡️ 🛡️ 🛡️ 🛡️ ⚙️
▼ Mandatory - My Policy (-)															
There are no rules in this section. Add Rule or Add Category															
▼ Default - My Policy (-)															
There are no rules in this section. Add Rule or Add Category															
Default Action														Access Control:Block all traffic ▼ 📄	

An access control rule can have single or multiple matching conditions

Rule Editor

Add Rule ?

Name

Clients-to-Servers

Enabled

☒

Insert

into Mandatory

Action

Allow



Time Range

None

+

Zones

Networks

VLAN Tags

 Users

Applications

Ports

URLs

Dynamic Attributes

Inspection

Logging

Comments

Available Zones 

Search by name

Inside-LAN

LAN

Servers

Add to Source

Add to Destination

Source Zones (1)

Inside-LAN 

Destination Zones (1)

Servers 

Rule Editor

Add Rule

Name	Clients-to-Servers	☒ Enabled	Insert	into Mandatory
Action	Allow		Time Range	None

- Type a **name** for new rule

- **Action :**

Allow : permit traffic but there may be more inspections, such as Intrusion and File policies.

Trust—Allow traffic without further inspection of any kind

Monitor : log the traffic and then continue to the rest of rules.

Block: Drop the traffic unconditionally without inspection , which causes the connection to time out

Block with reset : Drop the traffic, but sends a TCP reset (connection is closed immediately without time out)

Interactive Block : the web page will be blocked but user can decide to view the page. (displays a warning message)

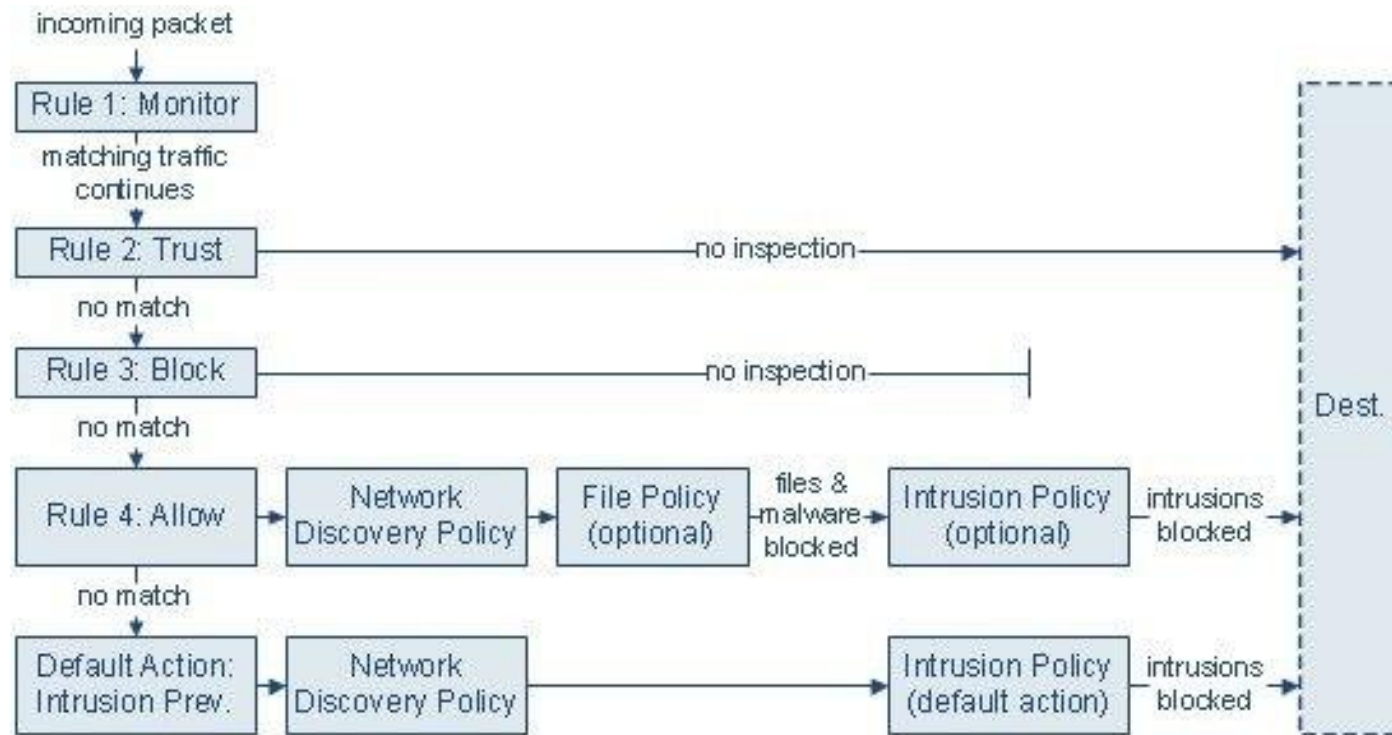
Interactive Block with Reset : like interactive block displays a warning message to the client but send a TCP reset to both sides when it is not accepted. The “interactive block” message can be customized.

Rule Editor

Add Rule

Name	Clients-to-Servers	☒ Enabled	Insert	into Mandatory
Action	Allow		Time Range	None

➤ note that you cannot associate an intrusion or file policy when the Block action is selected



Rule Editor

Add Rule

Name	Clients-to-Servers	☒ Enabled	Insert	into Mandatory
Action	Allow		Time Range	None

Insert :

- ✓ The main purpose of the mandatory and default rule sections is to create a hierarchy of access control policies

Into mandatory : are rules that are enforced first and should be used for override rules if needed.

- Often contains specific elements that may be exceptions to the overall policy

Into default : May contain more general rules that apply to all traffic at last

Rule Editor

Add Rule

Name

Clients-to-Servers

☒ Enabled

Insert

into Mandatory

Action

Allow

Time Range

None

- Time Range :
Applicable time period for this rule

New Time Range

Name:

speciif-period1

Description:

only applicable in this period

Effective From (using FTD TimeZone):

2024-11-07

08:00

To:

2024-11-13

17:00

Further constrain to recurring intervals:

+ Add Recurring Interval

Recurring Intervals

Daily Interval: Mon, Tue, 08:00 to 17:00

Cancel

Save

Rule Editor

- You can select the source / destination zones where traffic flows

Zones

Networks

VLAN Tags

 Users

Applications

Ports

URLs

Dynamic Attributes

Inspection

Logging

Comments

Available Zones 

Search by name

Inside-LAN

LAN

Servers

Add to Source

Add to Destination

Source Zones (1)

Inside-LAN 

Destination Zones (1)

Servers 

Rule Editor

- You can select the source / destination Networks (IP addresses) where traffic flows
- You can select the networks from defined objects or enter new IP address of the network / clients

Zones

Networks

VLAN Tags

⚠ Users

Applications

Ports

URLs

Dynamic Attributes

Inspection

Logging

Comments

Available Networks ↻

Q Search by name or value

Networks

Geolocation

IPv4-Private-192.168.0.0-16

IPv4-Private-All-RFC1918

IPv6-IPv4-Mapped

IPv6-Link-Local

IPv6-Private-Unique-Local-Addresses

IPv6-to-IPv4-Relay-Anycast

R2

Servers

Add To Source Networks

Add to Destination

Source Networks (2)

Source

Original Client

Clients

172.16.1.0/24

Destination Networks (1)

Servers

Enter an IP address

Add

192.168.10.0/26

Add

Rule Editor

- You can select the VLAN tag of the traffic from predefined VLAN tags(or create one)
- You can also enter the tag manually and add it to list

The screenshot displays the 'Rule Editor' interface with the 'VLAN Tags' tab selected. The top navigation bar includes 'Zones', 'Networks', 'VLAN Tags', 'Users', 'Applications', 'Ports', 'URLs', 'Dynamic Attributes', 'Inspection', 'Logging', and 'Comments'. The 'Available VLAN Tags' section on the left features a search bar and a list with 'Sale-VLAN' selected. An 'Add to Rule' button is next to it. A modal window titled 'New VLAN Tag Objects' is open, containing fields for 'Name' (Sale-VLAN), 'Description' (Traffic generated from Sale group), 'VLAN Tag' (10), and an 'Allow Overrides' checkbox. The 'Selected VLAN Tags (2)' section on the right lists 'Sale-VLAN' and '20', each with a trash icon. Below this is an 'Enter a VLAN tag' input field and an 'Add' button. At the bottom right, there are 'Cancel' and 'Add' buttons. The bottom left of the modal has 'Cancel' and 'Save' buttons.

Rule Editor

- You can act to traffic based on application signature

Zones

Networks

VLAN Tags

 Users

Applications

Ports

URLs

Dynamic Attributes

 Inspection

Logging

Comments

Application Filters 

Clear All Filters 

Available Applications (1) 

Selected Applications and Filters (1)   

Q Search by name

☐ search engine 54

☐ security management 61

☐ SMS tools 22

☒ social networking 198

☐ software update 40

☐ virtual worlds 10

☐ VoIP 59

☐ VPN/tunnel 77

Q insta

All apps matching the filter

Instagram 

Add to Rule

Applications

AnyDesk 

Rule Editor

- You can enter the source / destination port (well-known ports or custom port) to act based on this

Zones

Networks

VLAN Tags

 Users

Applications

Ports

URLs

Dynamic Attributes

Inspection

Logging

Comments

Available Ports 

+

Q Search by name or value

SIP

SMTP

SMTPS

SNMP

SSH

SYSLOG

TCP_high_ports

TELNET

Add to Source

Add to Destination

Selected Source Ports (0)

any

Protocol TCP (6) Port Enter a

Add

Selected Destination Ports (3)

HTTPS

HTTP

SSH

Protocol TCP (6) Port Enter a

Add

MohsenKheradmand 

Rule Editor

- You can filter traffic based on its URL , by predefined Category and Reputations , customized URL or enter manual URL

The screenshot displays the 'Rule Editor' interface with the 'URLs' tab selected. The top navigation bar includes tabs for Zones, Networks, VLAN Tags, Users, Applications, Ports, URLs, Dynamic Attributes, Inspection, Logging, and Comments. The main area is divided into three sections: 'Categories and URLs', 'Reputations', and 'Selected URLs (3)'. The 'Categories and URLs' section has a search bar and a list of categories, with 'Alcohol' selected. The 'Reputations' section shows a list of reputation levels, with '3 - Neutral' selected. A 'New URL Objects' dialog box is open, allowing the user to add a new URL object. The dialog box contains fields for Name, Description, URL, and Allow Overrides. The 'Name' field is filled with 'instagram', the 'Description' field with 'block Instagram', and the 'URL' field with 'https://www.instagram.com/'. The 'Allow Overrides' checkbox is unchecked. The 'Add to Rule' button is visible in the 'Reputations' section. The 'Selected URLs (3)' section shows a list of selected URLs, including 'Adult (Reputations 1-5 and unknown)', 'Sex Education (Reputations 1-5 and unknown)', and 'Social Networking (Reputations 3-5 and unknown)'. The 'Add' button is visible in the 'Selected URLs (3)' section.

Categories and URLs + Reputations

Search for a category

Category URLs

Any (Except Uncategorized)

Uncategorized

Adult

Advertisements

Alcohol

Animals and Pets

Arts

Viewing 1-100 of 125

Any

5 - Trusted

4 - Favorable

3 - Neutral

2 - Questionable

1 - Untrusted

☒ Apply to unknown reputations

Add to Rule

New URL Objects ?

Name

instagram

Description

block Instagram

URL

https://www.instagram.com/

Allow Overrides

☐

Cancel Save

Selected URLs (3)

Adult (Reputations 1-5 and unknown)

Sex Education (Reputations 1-5 and unknown)

Social Networking (Reputations 3-5 and unknown)

https://www.facebook.com/ Add

Rule Editor

- On the Inspection tab, you can use the Intrusion Policy and File Policy to select desired next-generation security policies.

Zones

Networks

VLAN Tags

 Users

Applications

Ports

URLs

Dynamic Attributes

 Inspection

Logging

Comments

Intrusion Policy

P1

▼



Variable Set

Default Set

▼





Snort 2 and Snort 3 version of this policy are not the same. Please make sure that any customizations are maintained independently.

File Policy

m1

▼



Rule Editor

Rule Conflict : to determine if there are any duplicate or overlapping rules (Shadowed rule conflicts)

Analyze Hit Counts : to determine if there are any rules that never hit any traffic or matches and hit traffic

The screenshot displays the Palo Alto Networks Rule Editor interface. At the top, the 'My Policy' header is visible, along with buttons for 'Show Warnings', 'Analyze Hit Counts' (highlighted with a red box), 'Save', and 'Cancel'. Below the header, there are tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', 'Logging', and 'Advanced'. The 'Rules' tab is active, showing a list of rules. A search bar and a 'Filter by Device' dropdown are present. A red box highlights the 'Show Rule Conflicts' checkbox, which is checked. Below the rules list, a 'Hit Count' modal is open, showing a dropdown for 'Select a device' with options 'FTD1' and 'FTD2'. The modal also includes a 'Fetch Current Hit Count' button. At the bottom of the modal, there is a table with columns: '#', 'Rule Name', 'Policy Name', 'Hit Count', and 'Last Hit Time'. The table contains two rows: '1 Clients-to-Servers My Policy 0' and '2 Default Action My Policy 0'. A warning message states: 'Policies have been modified and the hit count has been reset. Please refresh the hit counts.' The footer of the modal shows 'Displaying 1-2 of 2 rows' and 'Page 1 of 1'.

My Policy
functional policy

Show Warnings **Analyze Hit Counts** Save Cancel

[Inheritance Settings](#) | [Policy Assignments \(2\)](#)

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [None](#)

[Filter by Device](#) Search Rules X ☒ Show Rule Conflicts ? + Add Category + Add Rule

#	Name	Source Zones	Dest	Source	Dest Networks	VLAN Tags	Users	Appli	Source	Dest	URLs	Source Dyna	Desti...	Act...
▼ Mandatory - My Policy (1-1)														
1	Clients-to-Servers	Inside-LAN												
▼ Default - My Policy (-)														
There are no rules in this section. Add Rule														

Hit Count

Select a device: Last Fetched: Unknown [Fetch Current Hit Count](#)

FTD1 FTD2

Filter Rules/Policy Filter by: Never Hit Rules In Last: None

Last Deplo None ago)

⚠ Policies have been modified and the hit count has been reset. Please refresh the hit counts.

#	Rule Name	Policy Name	Hit Count	Last Hit Time
1	Clients-to-Servers	My Policy	0	
2	Default Action	My Policy	0	

Displaying 1-2 of 2 rows < < Page 1 of 1 > > ↻

Rule Editor

On the **Logging** tab, you can enable Log at Beginning/End of Connection to log the connections (helpful for troubleshooting)

Zones	Networks	VLAN Tags	 Users	Applications	Ports	URLs	Dynamic Attributes	Inspection	Logging	Comments
-------	----------	-----------	---	--------------	-------	------	--------------------	------------	----------------	----------

☒ Log at Beginning of Connection

☐ Log at End of Connection

File Events:

☐ Log Files

Send Connection Events to:

☒ Firepower Management Center

☒ Syslog Server *(Using default syslog configuration in Access Control Logging)* [Show Overrides](#)

☐ SNMP Trap

Select an SNMP Alert Configurat ▼

 +

Note : in block action rules , You cannot enable *Log at End of Connection* because blocked traffic is denied instantaneously without further inspection at the beginning of connections

Rule Editor

Click *HTTP Responses* tab to select The “interactive block” message or create a customized message to display

The screenshot shows the 'Rule Editor' interface with the 'HTTP Responses' tab selected. The main panel displays two options for the block response page: 'Block Response Page' (Custom...) and 'Interactive Block Response Page' (System-provided). A modal dialog titled 'Edit Block Response Page' is open, showing a text area with the following HTML code:

```
<!DOCTYPE html>
<html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body sans-serif; h1 null p null strong null</style>
</head>
<body>
<h1>Access Denied</h1>
<p>
<strong>You are attempting to access a forbidden site.</strong><br/><br/>
Consult your system administrator for details.
</p>
</body>
</html>
```

Below the text area, it indicates '386 of 49892 characters used'. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Rule Editor

Consider the following best practices when you configure an access control policy:

- 1) Place the rules with block actions at the top of the access control policy
- 2) Place the precisely defined rules before a broader rule
- 3) Rules that **are not** associated with an intrusion policy or file policy should be placed before other rules
- 4) If you want to allow or block traffic just based on 5-tuple (source and destination IP address/port number and protocol), consider using a prefilter rule for them. It improves system performance
- 5) After adding all the access control rules, use the **Show Rule Conflict** check box to determine if there are any duplicate or overlapping rules (also known as shadowed rules).
- 6) Once an access control policy is deployed and running for some time, use the **Analyze Hit Counts** option to determine if there are any rules that never matched any traffic.

Verification

Analysis / Connections / Events

Connection Events Confirm the Actions by the Access Control Policy

The screenshot displays the Cisco FMC Events interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, and a search icon. The 'Analysis' tab is selected. Below the navigation bar, there are links for 'Bookmark This Page', 'Reporting', 'Dashboard', 'View Bookmarks', and 'Search'. A 'Predefined Searches' dropdown menu is also present. The main heading is 'Connection Events' with a '(switch workflow)' link. A time range filter is set to '2021-09-22 15:34:58 - 2021-09-22 18:06:01' with an 'Expanding' status. Below this, there is a 'No Search Constraints (Edit Search)' link. Two tabs are visible: 'Connections with Application Details' and 'Table View of Connection Events', with the latter being the active tab. A 'Jump to...' input field is located above the table. The table itself has columns for selection, timestamp, action, initiator IP, responder IP, source port / ICMP type, destination port / ICMP code, access control policy, and access control rule. Three rows of data are shown, each with a dropdown arrow and a checkbox in the selection column. The data rows show various actions (Allow, Allow, Block) and rules (Default Action, Web Traffic, Telnet Traffic). At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying rows 1-3 of 3 rows'. Two buttons, 'View' and 'View All', are located at the bottom left.

	☐	↓ First Packet x	Action x	Initiator IP x	Responder IP x	Source Port / ICMP Type x	Destination Port / ICMP Code x	Access Control Policy x	Access Control Rule x
▼	☐	2021-09-22 18:05:46	Allow	172.16.1.200	192.168.1.2	35852 / tcp	22 (ssh) / tcp	AC Policy	Default Action
▼	☐	2021-09-22 18:04:03	Allow	172.16.1.200	192.168.1.2	57732 / tcp	80 (http) / tcp	AC Policy	Web Traffic
▼	☐	2021-09-22 18:02:40	Block	172.16.1.200	192.168.1.2	38966 / tcp	23 (telnet) / tcp	AC Policy	Telnet Traffic

Or On the policy editor page, select the Analyze Hit Counts button

Verification

Alternatively, you can view all the access control rules and hit counts by the CLI of the threat defense

```
<show access-list
```

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
  alert-interval 300
access-list CSM_FW_ACL_; 9 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998
(hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535
rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544
rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0)
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998
(hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268443648: ACCESS POLICY: AC Policy - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268443648: L4 RULE: Telnet Traffic
access-list CSM_FW_ACL_ line 10 advanced deny tcp any any object-group TELNET
rule-id 268443648 event-log flow-start
(hitcnt=7) 0xae7f8544
```

Verification

You can debug the operation of the FTD security engines to see the details behind the processing of traffic flowing

<system support firewall-engine-debug

Please specify an IP protocol: tcp

Please specify a client IP address:

Please specify a client port:

Please specify a server IP address:

Please specify a server port:

Monitoring firewall engine debug
messages

.

.

! Client attempts to connect to the
server using Telnet service

.

172.16.1.200-41090 > 192.168.1.2-23 6 AS 1-1 | 1 Got start of flow event from hardware with flags 00020001

172.16.1.200-41090 > 192.168.1.2-23 6 AS 1-1 | 1 Logging SOF for event from hardware with rule_id =
268443648 ruleAction = 4 ruleReason = 0

.

.

! Client uses a browser to access the web server

Access Control Policy

