

Securing Networks with
Cisco FTD

Chapter 9

Prefilter Policy

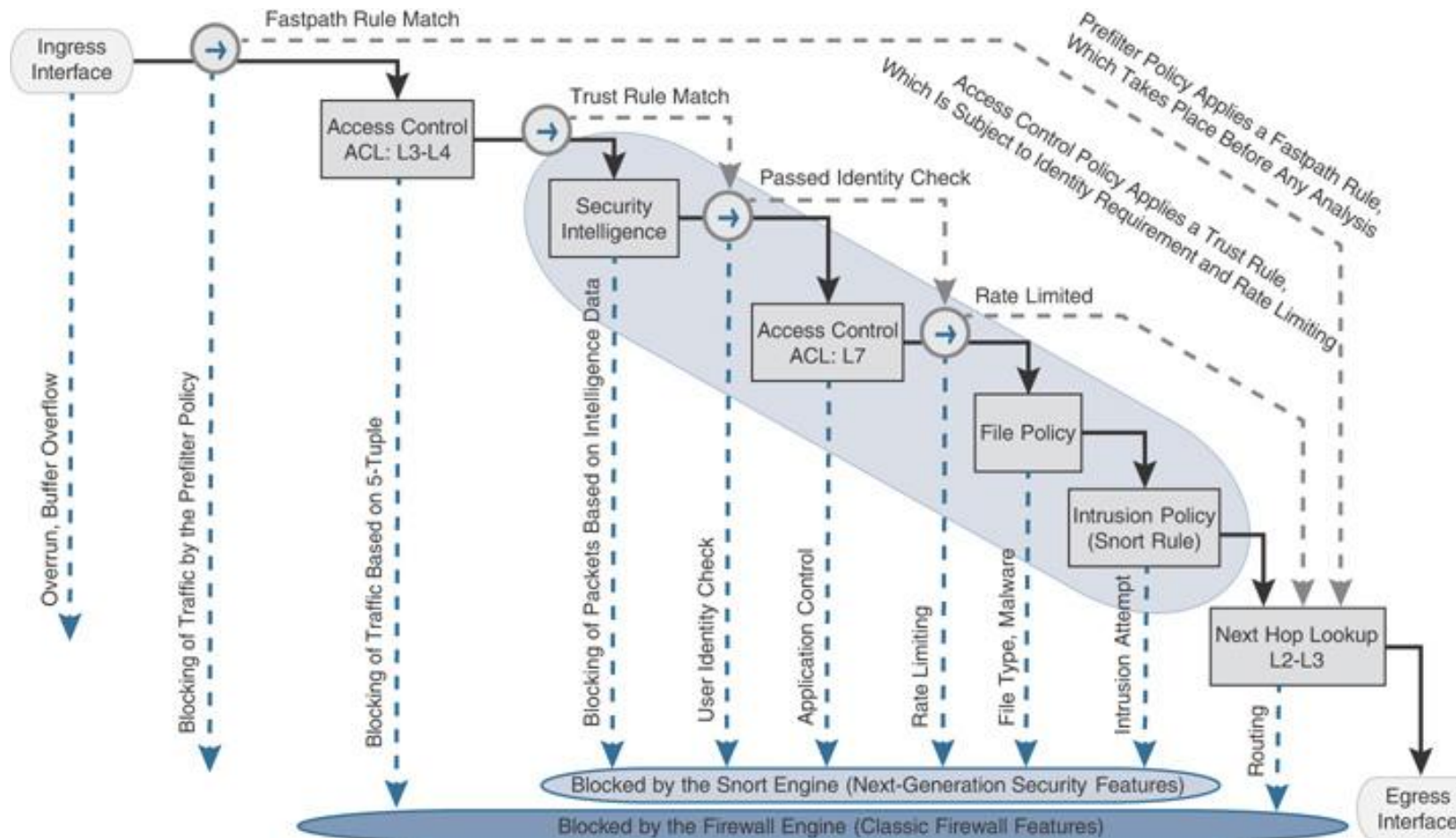
Mohsen Kheradmand

The objectives of this chapter are to learn about

- Configuration and deployment of prefilter policy
- Differences between prefilter policy and access control policy
- Different ways to bypass deep packet inspection
- Inspection of encapsulated traffic

Prefilter Policy: Rules and Actions

- A prefilter policy acts on traffic earlier and faster than the access control policy
- Prefilter Rule Can Filter Traffic Based on Interface, Network, VLAN, and Port



Potential Reasons for a Packet Drop by a Threat Defense

Prefilter Policy: Configuration

- Policies > Prefilter > New Policy
- Enter a name for new policy (or description) and save it

 Firepower Management Center

Policies / Access Control / Prefilter

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligence

Deploy 🔍 ⓘ ⚙️ ? admin ▼

Prefilter Policy

Custom Prefilter-1

Default Prefilter Policy

Access Control

Access Control

Intrusion

Malware & File

DNS

Identity

SSL

Prefilter

Network Discovery

Application Detectors

Correlation

Actions

Alerts

Scanners

Groups

Modules

Instances

Object Management | Access Control

New Policy

New Policy ⓘ

Name:

Servers Prefilter

Description:

must be applied to server zone

Cancel

Save

MohsenKheradmand



Prefilter Policy: Configuration

Firepower Management Center
Policies / Access Control / Tunnel Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy Search 1 ? admin

Servers Prefilter

must be applied to server zone

Analyze Hit Counts Save Cancel

Rules

+ Add Tunnel Rule + Add Prefilter Rule Search Rules X

#	Name	Rule Type	Source Interface Obje...	Destination Interface Obje...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone			
There are no rules. Add Tunnel Rule Add Prefilter Rule														
Non-tunneled traffic is allowed														
Default Action: Tunnel Traffic														
Analyze all tunnel traffic														
Analyze all tunnel traffic														
Block all tunnel traffic														

There are three ways to assign an action to the traffic:

- **Tunnel rule**
Filters tunnel traffic that is encapsulated by an additional IP header (i.e. : GRE, IP-in-IP, and IPv6-in-IP)
- **Prefilter rule**
Filter traffic based on basic networking constraints (IP address, port number ,VLAN tag, and interface)
- **Default action**
 - Act on a traffic that is not matched to Tunnel rules (it is applicable only for tunnel traffic)

Prefilter Policy: Configuration

Both a tunnel rule and prefilter rule offer three types of actions:

➤ Analyze

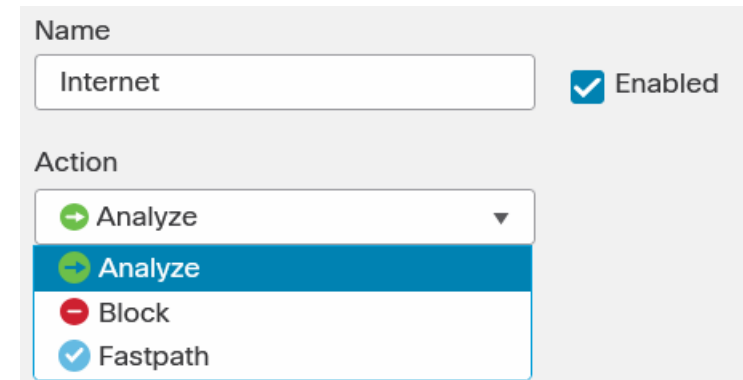
- Allows a threat defense to perform further analysis on matching traffic
- Inspected and controlled by access control policies, intrusion policies, and malware and file policies

➤ Block

- This action blocks matching traffic immediately
- No further inspection is performed by any policy

➤ Fastpath

- This action bypasses any further security analysis
- The matching traffic is no longer subject to rate limit and identity requirements



The screenshot shows a configuration window for a Prefilter Policy. It has a 'Name' field containing 'Internet' and an 'Enabled' checkbox which is checked. Below this is an 'Action' dropdown menu. The dropdown is open, showing three options: 'Analyze' (with a green right-pointing arrow icon), 'Block' (with a red left-pointing arrow icon), and 'Fastpath' (with a blue checkmark icon). The 'Analyze' option is currently selected and highlighted with a blue background.

Bypassing Deep Packet Inspection

Secure Firewall offers two types of rule actions to bypass deep packet inspection :

➤ Fastpath action:

- A prefilter rule with the Fastpath action, bypass the traffic before a packet reaches the firewall engine and Snort engine

➤ Trust action

- An access control rule with the Trust action allows a threat defense to bypass deep packet inspection
- Trusted traffic checks for identity and quality of service (QoS) requirements as configured in their respective policies
- Access control policy rules offer more filtering capability. i.e. you can filter traffic based on applications, URLs, users,

Prefilter Policy: Configuration

➤ In this example we need to allow management traffic pass via SSH and HTTPS (without deep inspection)

1) Add Prefilter Rule

- Type a name for rule
- Action = Fastpath
- Destination port= SSH

The screenshot shows the configuration page for a Prefilter Policy. At the top, the 'Name' field contains 'SSH-Trust', and the 'Enabled' checkbox is checked. The 'Insert' dropdown is set to 'below rule' with a position of '0'. The 'Action' dropdown is set to 'Fastpath'. The 'Time Range' dropdown is set to 'None'. Below these fields are tabs for 'Interface Objects', 'Networks', 'VLAN Tags', and 'Ports', with 'Ports' being the active tab. A search bar is present with the text 'Search by name or value'. Under 'Available Ports', a list includes RIP, SIP, SMTPS, SMTP, SNMP, SSH (highlighted), SYSLOG, and TCP high ports. To the right of this list are buttons for 'Add to Source' and 'Add to Destination'. Further right, there are two boxes: 'Selected Source Ports (0)' containing 'any', and 'Selected Destination Ports (1)' containing 'SSH'. At the bottom, there are two identical input sections for 'Protocol' (set to 'TCP (6)') and 'Port' (with a placeholder 'Enter a'), each followed by an 'Add' button.

✓ It means traffic destined to SSH port are trusted and not inspected

Prefilter Policy: Configuration

1) Add Prefilter Rule

Name

SSH-Trust

☒ Enabled

Action

Fastpath

Insert

below rule

0

Time Range

None

+

Interface Objects

Networks

VLAN Tags

Ports

Comment

Logging

Available Networks

Search by name or value

any

IPv4-Private-All-RFC1918

admin-PCs

any-ipv4

any-ipv6

FMC-FTD

IPv4-Benchmark-Tests

IPv4-Link-Local

Add to Source

Add to Destination

Source Networks (1)

admin-PCs

Enter an IP address

Add

Destination Networks (1)

FMC-FTD

Enter an IP address

Add

- Optionally you can Select source and destination traffic and add to source/destination network

Prefilter Policy: Configuration

1) Add Prefilter Rule

Name

SSH-Trust

☒ Enabled

Insert

below rule

0

Action

Fastpath

Time Range

None

+

Interface Objects

Networks

VLAN Tags

Ports

Comment

Logging

☐ Log at Beginning of Connection

☒ Log at End of Connection

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

+

- Optionally, enable logging to enable the FTD to send logs of matched traffic to FMC

Prefilter Policy: Configuration

Finally click Add

Servers Prefilter

must be applied to server zone

Rules

You have unsaved changes

Analyze Hit Counts

Save

Cancel

+ Add Tunnel Rule

+ Add Prefilter Rule

Search Rules

X

#	Name	Rule Type	Source Interface Obje...	Destination Interface Obje...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone			
1	SSH-Trust	Prefilter	any	any	admin-PCs	FMC-FTD	any	SSH	any	Fastpath	na			0

Non-tunneled traffic is allowed

Default Action: Tunnel Traffic

Analyze all tunnel traffic

- Leave the Default Action Tunnel Traffic to Analyze all tunnel traffic
- Click save
- Note : Do not deploy a new prefilter policy at this stage.(next section , invoke this prefilter to access control policy)

Prefilter Policy: Configuration

2) Invoking a Prefilter Policy into an Access Control Policy

- Policies > Access Control > Access Control

 Firepower Management Center

Policies / Access Control / Access Control

OverviewAnalysisPoliciesDevicesObjectsAMPIntelligence

Deploy 🔍 🔔 ⚙️ ? admin ▾

Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export

New Policy

Access Control Policy	Domain	Status	Last Modified	
FTD1-Policy applicable to FTD1	Global	Targeting 1 devices <i>Up-to-date on all targeted devices</i>	2024-12-02 13:52:14 Modified by "admin"	   

- Edit desired Access control policy

Prefilter Policy: Configuration

2) Invoking a Prefilter Policy into an Access Control Policy

- Click the Default Prefilter Policy to change it

FTD1-Policy
applicable to FTD1

Show Warnings Analyze Hit Counts Save Cancel

[Inheritance Settings](#) | [Policy Assignments \(1\)](#)

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

[Filter by Device](#) Search Rules

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users
✓	Mandatory - FTD1-Policy (-)						

Prefilter Policy

The prefilter policy performs early traffic handling using simple network characteristics, including non-encrypted encapsulation. (Firepower Threat Defense only.)

Default Prefilter Policy Servers Prefilter Custom Prefilter-1 Default Prefilter Policy

Cancel OK

- Select the Prefilter Policy (created in last step)
- Click Save
- Now you can Deploy the Policy to the FTD

Trust Rule via Access Control Policy

- ✓ As I mentioned in the last step we want to allow HTTPS traffic to pass through as well , without deep inspection
 - ✓ But other facilities like : Security Intelligence data, application fingerprints, URL filtering, user identities are needed
- Policies > Access Control > Access Control.

FTD1-Policy

applicable to FTD1

Show Warnings

Analyze Hit Counts

Save

Cancel

Inheritance Settings

Policy Assignments (1)

Rules

Security Intelligence

HTTP Responses

Logging

Advanced

Prefilter Policy: Servers Prefilter

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								
Mandatory - FTD1-Policy (-)																						

- Click Add Rule

Trust Rule via Access Control Policy

- Enter a name for Rule
- Action = trust
- Select HTTP/HTTPS ports
- Add selected ports to destination ports

Add Rule

Name: ☒ Enabled

Action:

Insert:

Time Range:

Ports

Available Ports (0):

- BitTorrent
- DNS_over_TCP
- DNS_over_UDP
- FTP
- HTTP**
- HTTPS**
- IMAP
- LDAP

Selected Source Ports (0):

Selected Destination Ports (2):

- HTTP
- HTTPS

Protocol: TCP (6) Port: Enter a

Protocol: TCP (6) Port: Enter a

Trust Rule via Access Control Policy

You can also :

- Select the source traffic and Add to source network

The screenshot shows the 'Add Rule' configuration window. The rule name is 'Web Access', it is enabled, and the action is 'Trust'. The 'Networks' tab is selected, showing a list of available networks. The network 'IPv4-Private-192.168.0.0-16' is selected and highlighted in blue. A red circle with the number '1' points to the 'Trust' action dropdown. A red circle with the number '2' points to the selected network in the list. A red circle with the number '3' points to the 'Add To Source Networks' button. The 'Source Networks (1)' list shows the selected network. The 'Destination Networks (0)' list is empty. The 'Add' button is at the bottom right.

Finally :

- Add
- Click Save
- And Deploy the policy to FTD

Verification

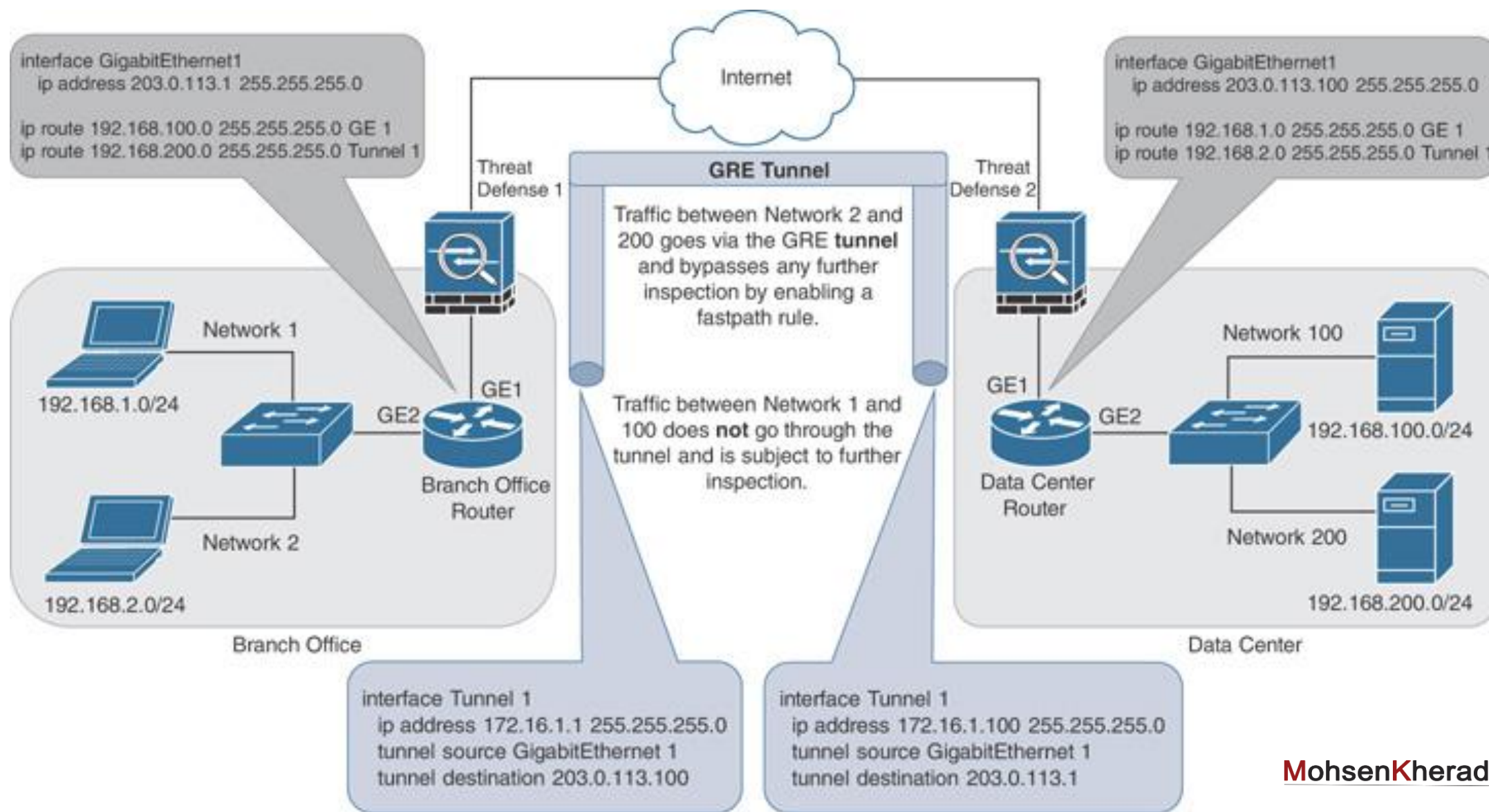
Verify the actions of prefilter and access control rules on live traffic

Analysis > Connections > Events

The screenshot displays the Cisco FMC Events page. 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 '2021-09-30 08:15:24 - 2021-09-30 09:25:31' with an 'Expanding' status. Below this, it says 'No Search Constraints (Edit Search)'. There are two tabs: 'Connections with Application Details' and 'Table View of Connection Events', with the latter being selected. A 'Jump to...' input field is located above the table. The table has columns: a checkbox, 'First Packet x', 'Action x', 'Initiator IP x', 'Responder IP x', 'Source Port / ICMP Type x', 'Destination Port / ICMP Code x', 'Access Control Rule x', and 'Tunnel/Prefilter Rule x'. Two rows of data are shown. The first row has a dropdown arrow, a checkbox, the timestamp '2021-09-30 09:25:13', the action 'Trust', initiator IP '192.168.1.2', responder IP '172.16.1.200', source port '45854 / tcp', destination port '80 (http) / tcp', and the rule 'Web Access'. The second row has a dropdown arrow, a checkbox, the timestamp '2021-09-30 09:23:59', the action 'Fastpath', initiator IP '192.168.1.2', responder IP '172.16.1.200', source port '45636 / tcp', destination port '22 (ssh) / tcp', and the rule 'Shell Prefilter'. At the bottom, there is a pagination bar showing 'Page 1 of 1' and 'Displaying rows 1-2 of 2 rows'. Below the pagination bar are two buttons: 'View' and 'View All'.

	☐	First Packet x	Action x	Initiator IP x	Responder IP x	Source Port / ICMP Type x	Destination Port / ICMP Code x	Access Control Rule x	Tunnel/Prefilter Rule x
▼	☐	2021-09-30 09:25:13	Trust	192.168.1.2	172.16.1.200	45854 / tcp	80 (http) / tcp	Web Access	
▼	☐	2021-09-30 09:23:59	Fastpath	192.168.1.2	172.16.1.200	45636 / tcp	22 (ssh) / tcp		Shell Prefilter

Managing Encapsulated Traffic inspection



Managing Encapsulated Traffic inspection

Click Prefilter policy > edit

Servers Prefilter

must be applied to server zone

Analyze Hit Counts Save Cancel

Rules

+ Add Tunnel Rule + Add Prefilter Rule Search Rules X

#	Name	Rule Type	Source Interface Obje...	Destination Interface Obje...	Source Networks	Destination Networks	Source Port	Destination Port	VLAN Tag	Action	Tunnel Zone	
1	SSH-Trust	Prefilter	any	any	admin-PCs	FMC-FTD	any	SSH	any	Fastpath	na	

Non-tunneled traffic is allowed

Default Action: Tunnel Traffic Analyze all tunnel traffic

Click Add Tunnel Rule

Managing Encapsulated Traffic inspection

Add Tunnel Rule

Tunnel rules perform early handling of non-encrypted encapsulated traffic, using outer IP headers. Fastpathed traffic bypasses access control and QoS.

NameGRE☒ Enabled

Action☒ Fastpath

☒ Match tunnels only from source (X)
☐ Match tunnels from source and destination (↔)

Insertbelow rule1

Assign Tunnel ZoneSelect a Tunnel Zone+

Time RangeNone+

Interface ObjectsTunnel EndpointsVLAN TagsEncapsulation & PortsCommentLogging

Encapsulation Protocols:
☒ GRE
☐ IP-in-IP
☐ IPv6-in-IP
☐ Teredo Port (3544)

CancelAdd