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 :

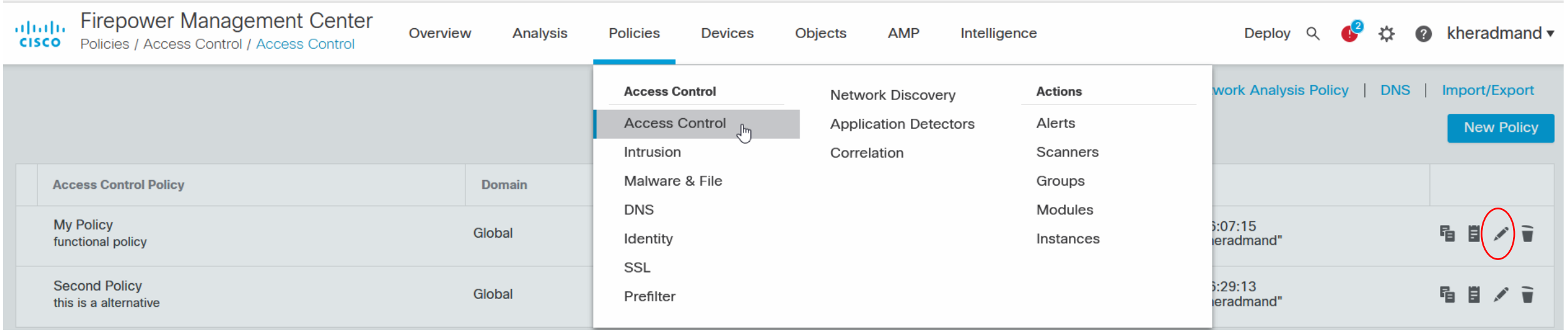
Access Control Policy Editor : set of rules , applicable to a threat defense

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

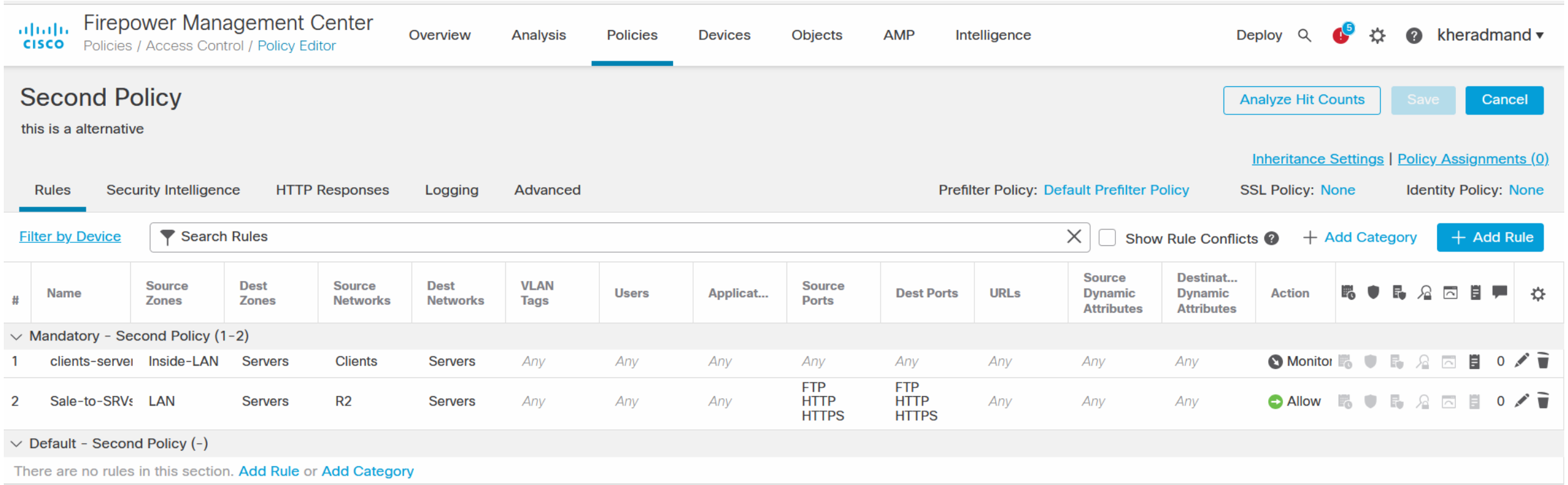
Policies > Access Control



- 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

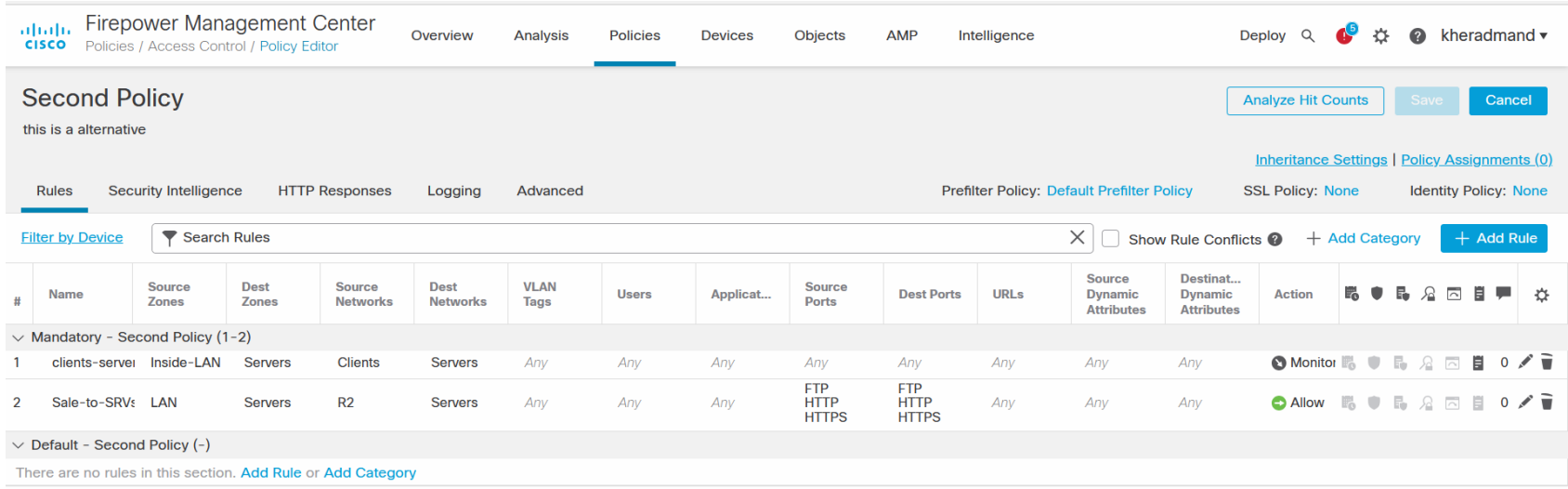
Policy Editor

Access control rule editor



Policy Editor

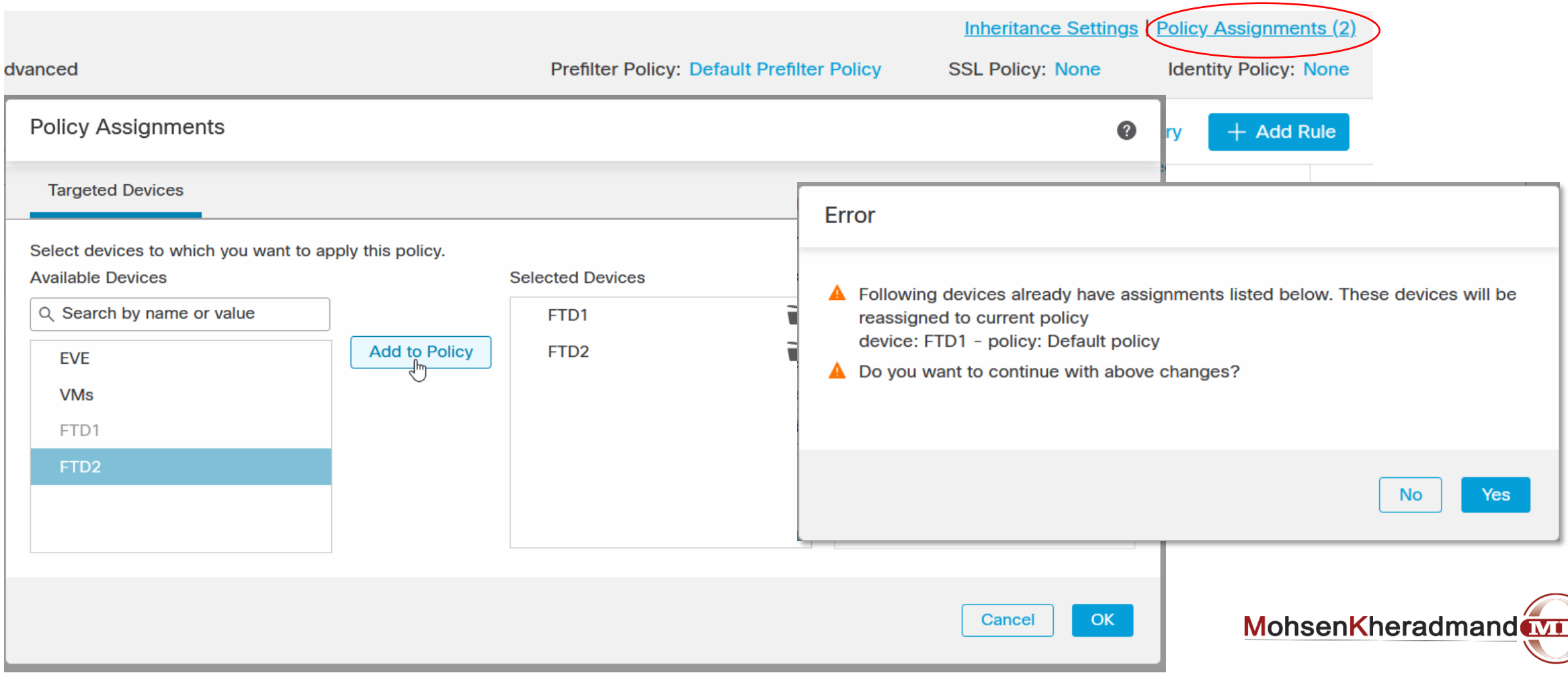
Summary of some of the options:



- 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.



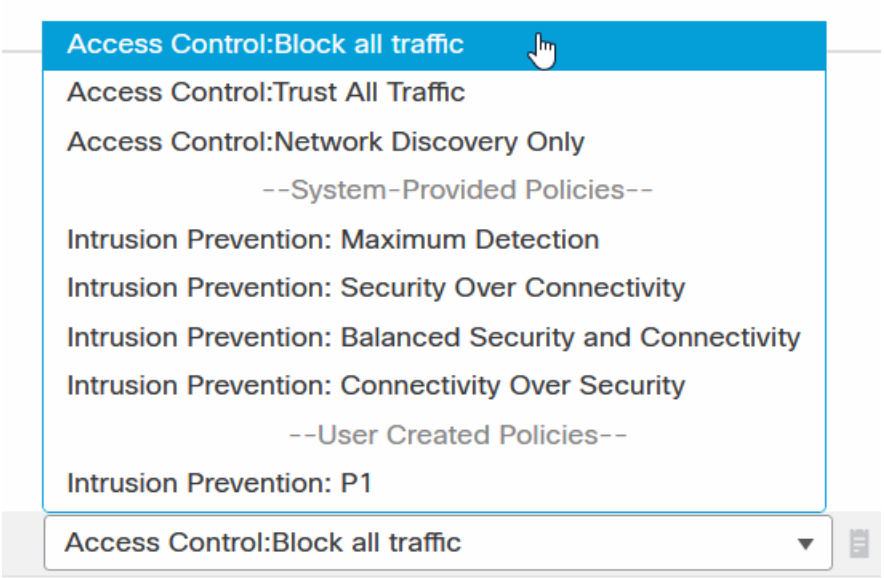
Policy Editor

- Default Action:

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

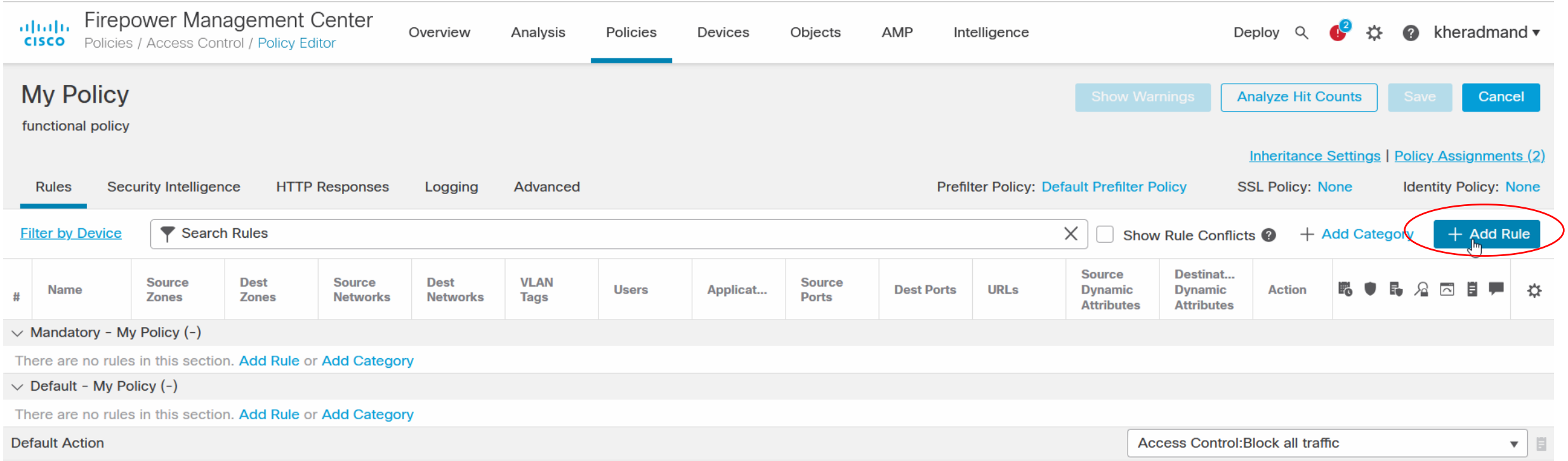
You can choose to apply one of the following actions to the remaining unmatched traffic:

- 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.



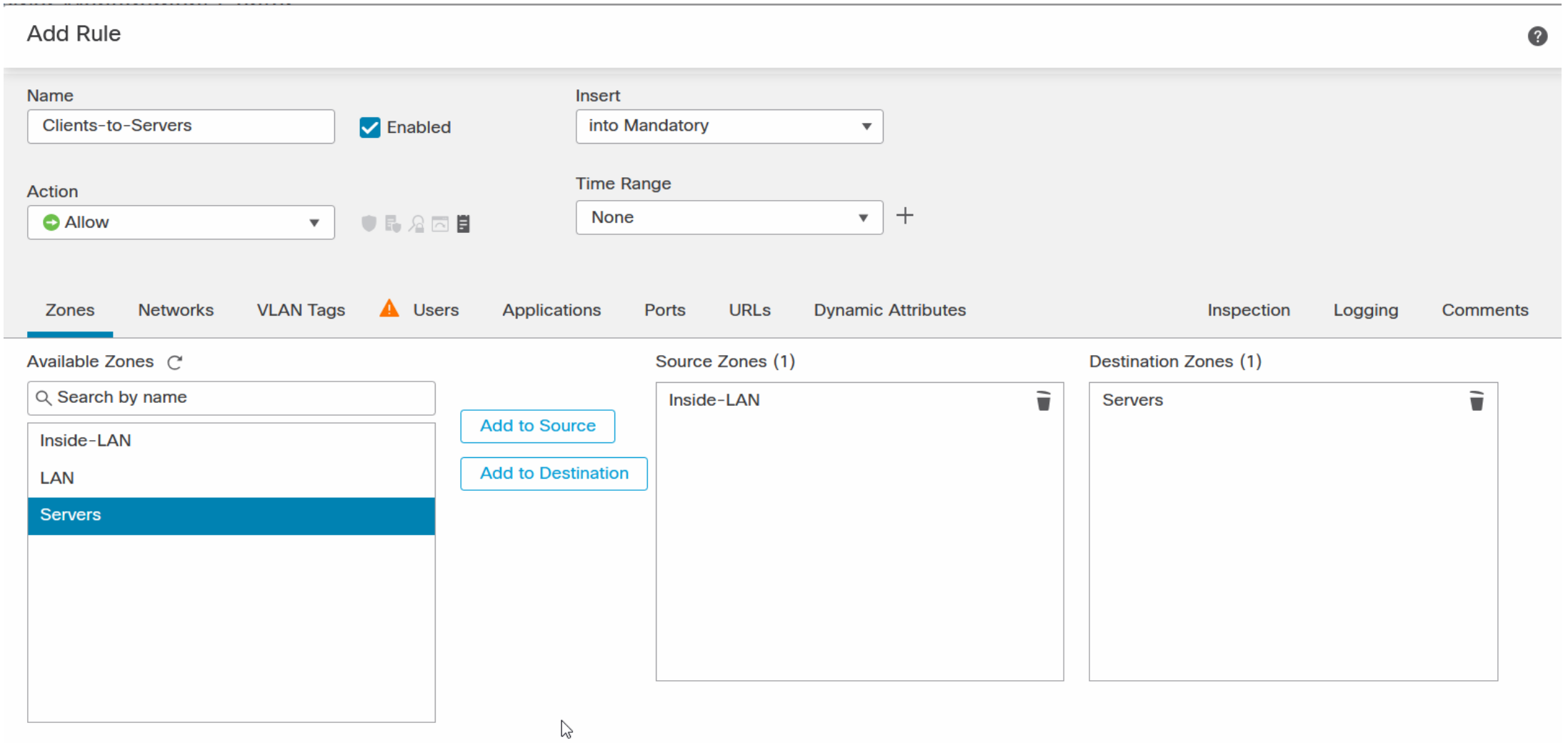
Rule Editor

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

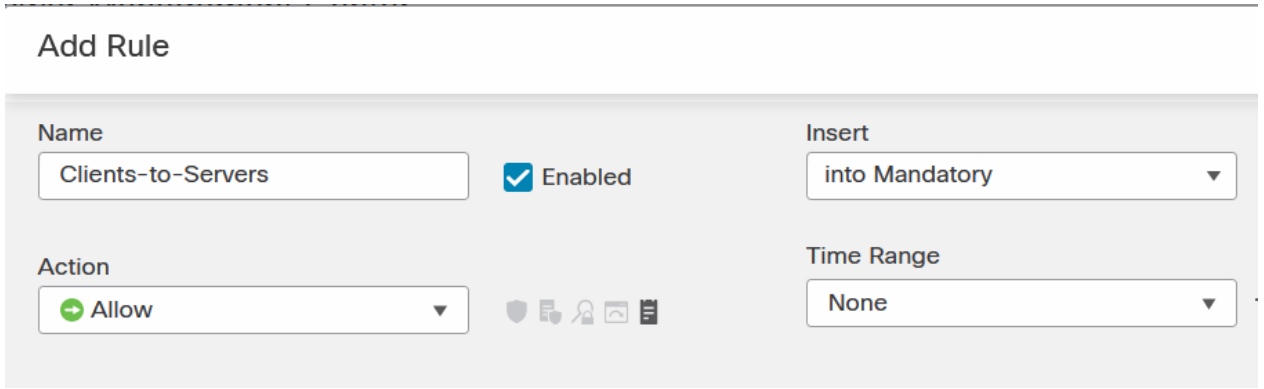


An access control rule can have single or multiple matching conditions

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



- 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.

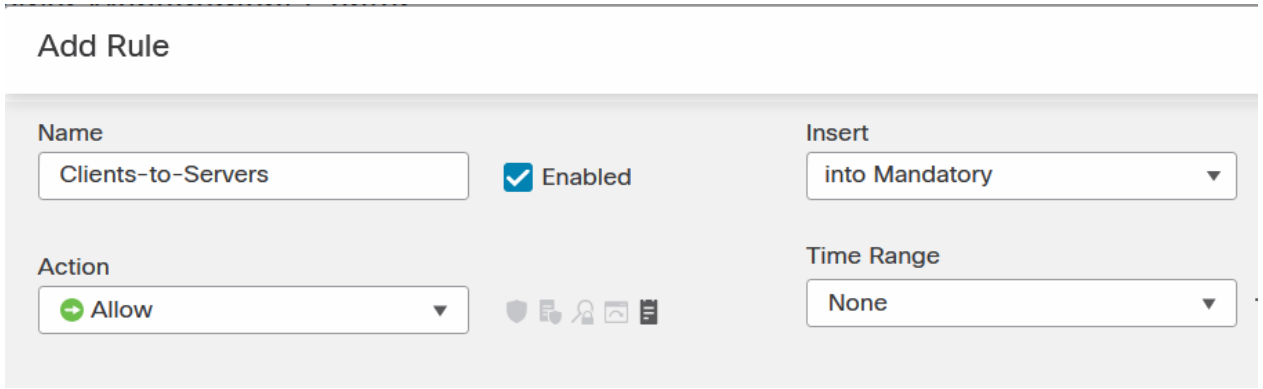
  Block: Drop the traffic unconditionally without inspection , which causes the connection to time out

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

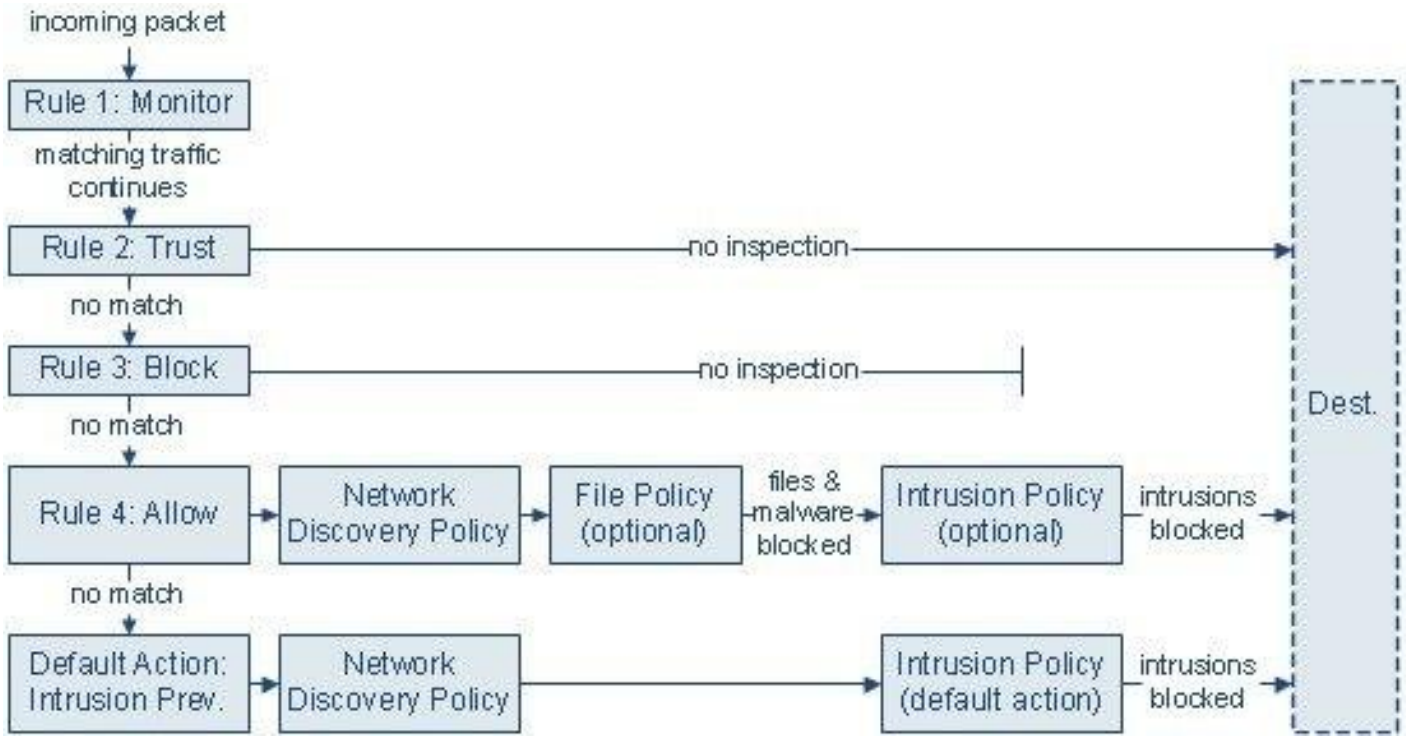
  Interactive Block : the web page will be blocked but user can decide to view the page. (displays a warning message)

  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.

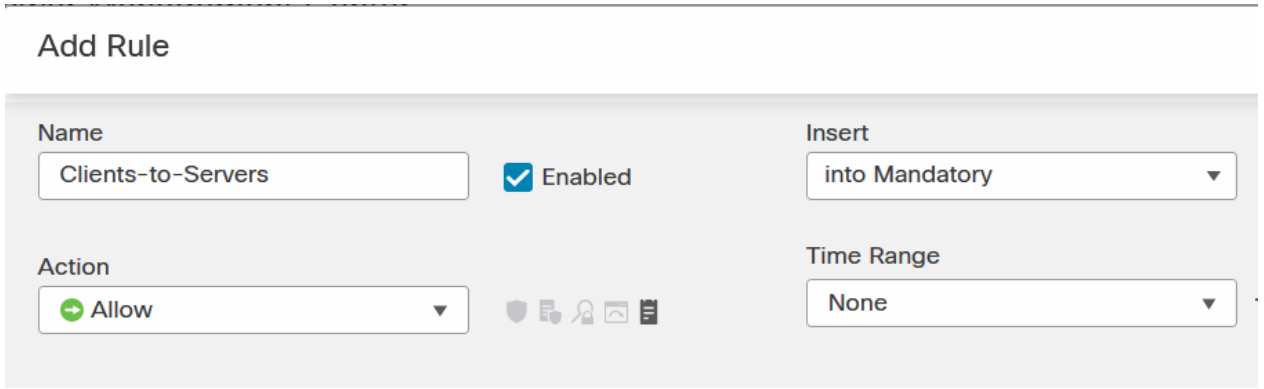
Rule Editor



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



Rule Editor



Insert :

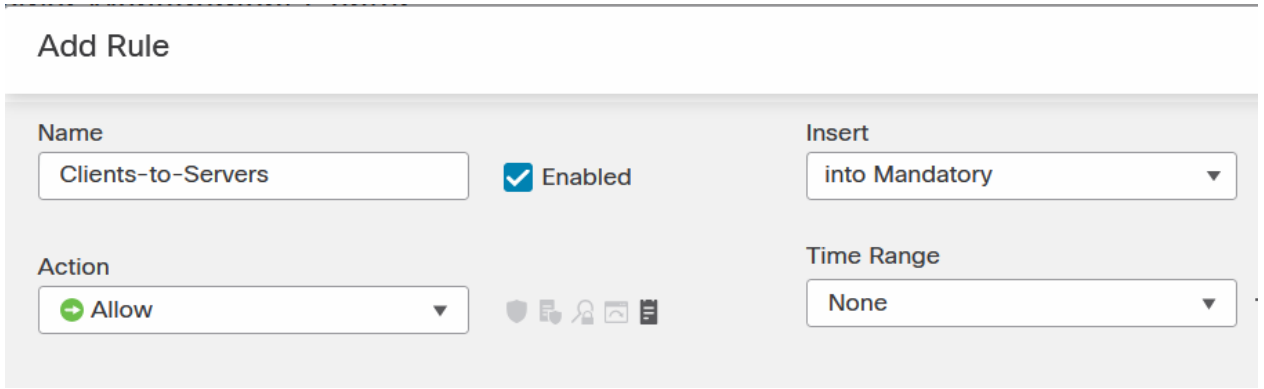
✓ The main purpose of the mandatory and default rule sections is to create a hierarchy of access control policies

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

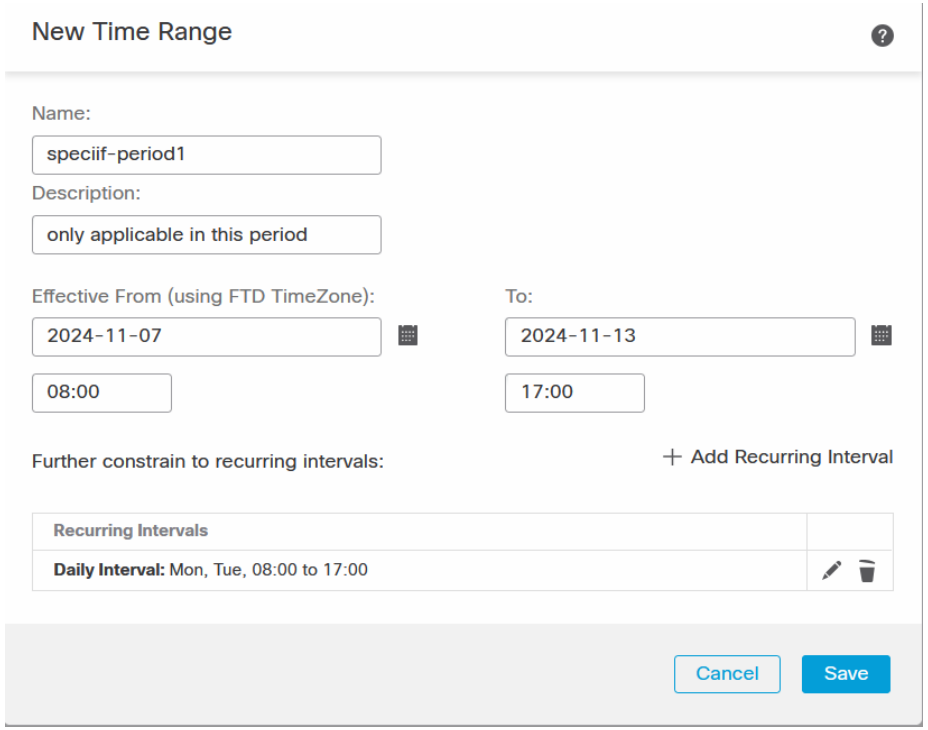
Into default : May contain more general rules that apply to all traffic at last

Rule Editor



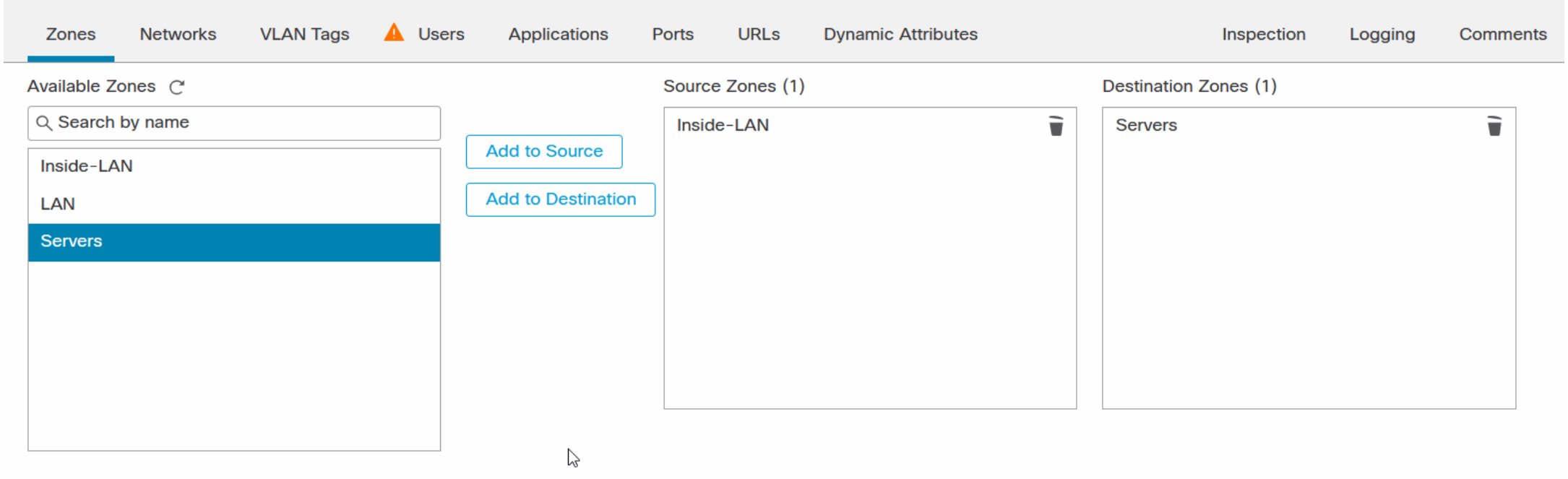
- Time Range ：

  Applicable time period for this rule



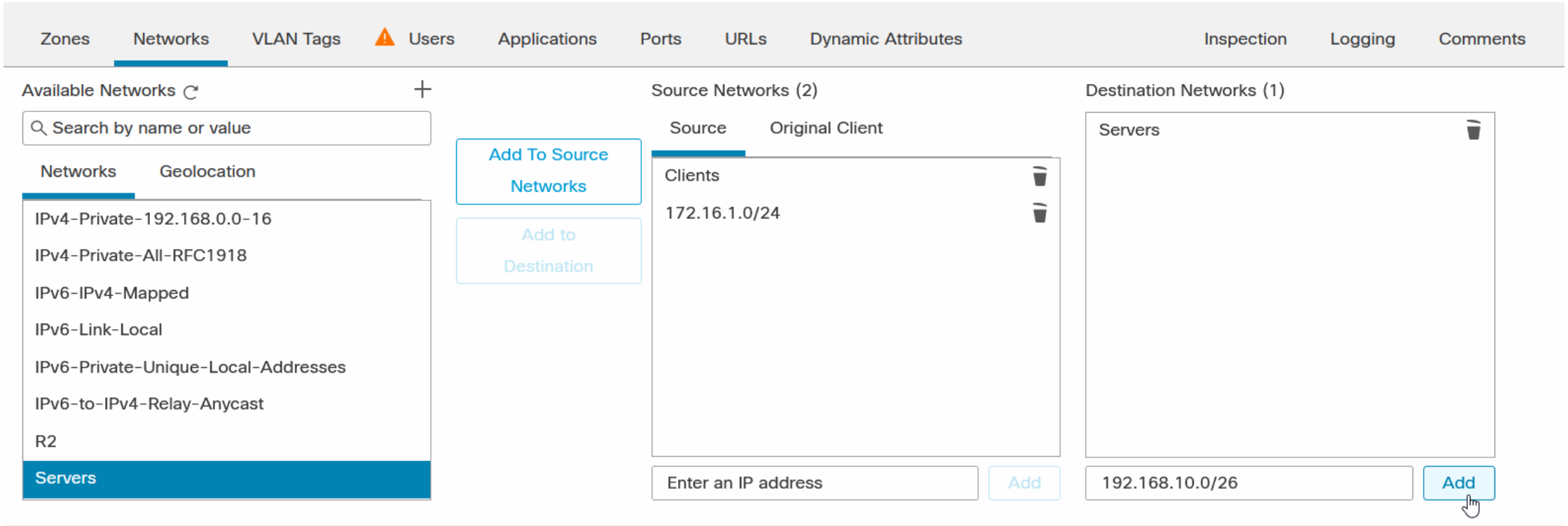
Rule Editor

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



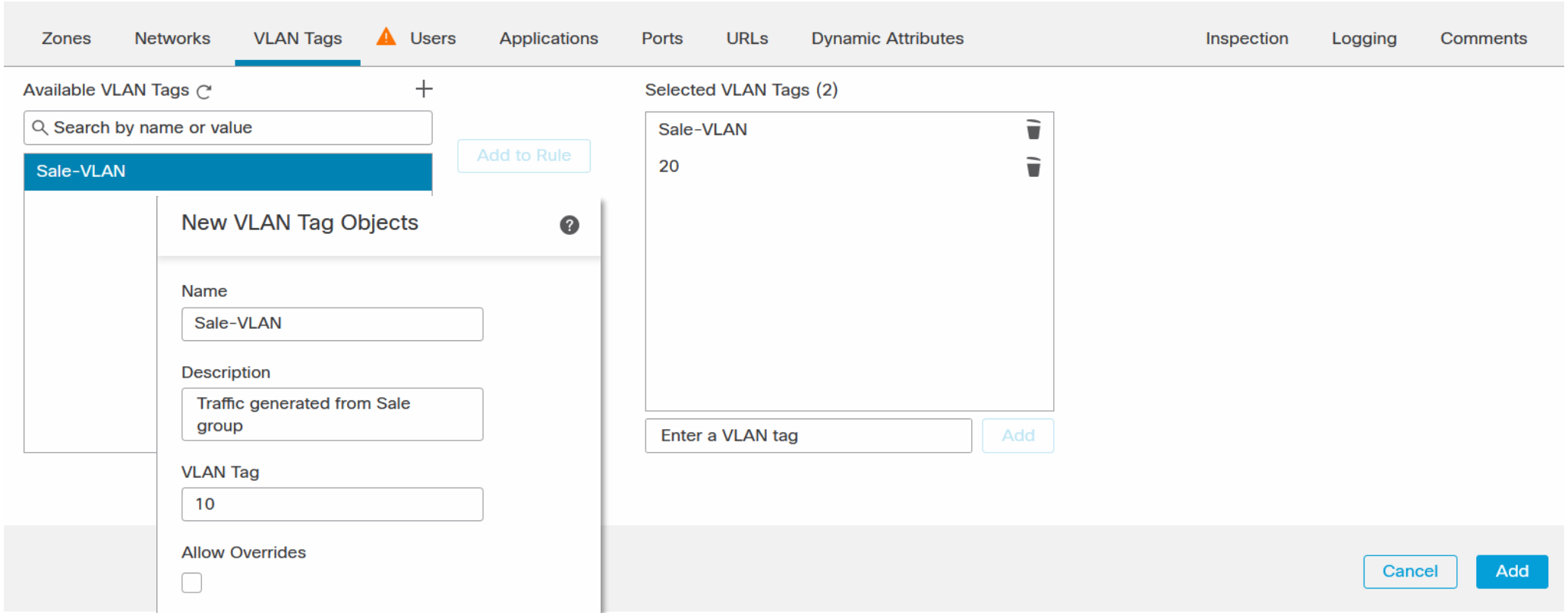
Rule Editor

- 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



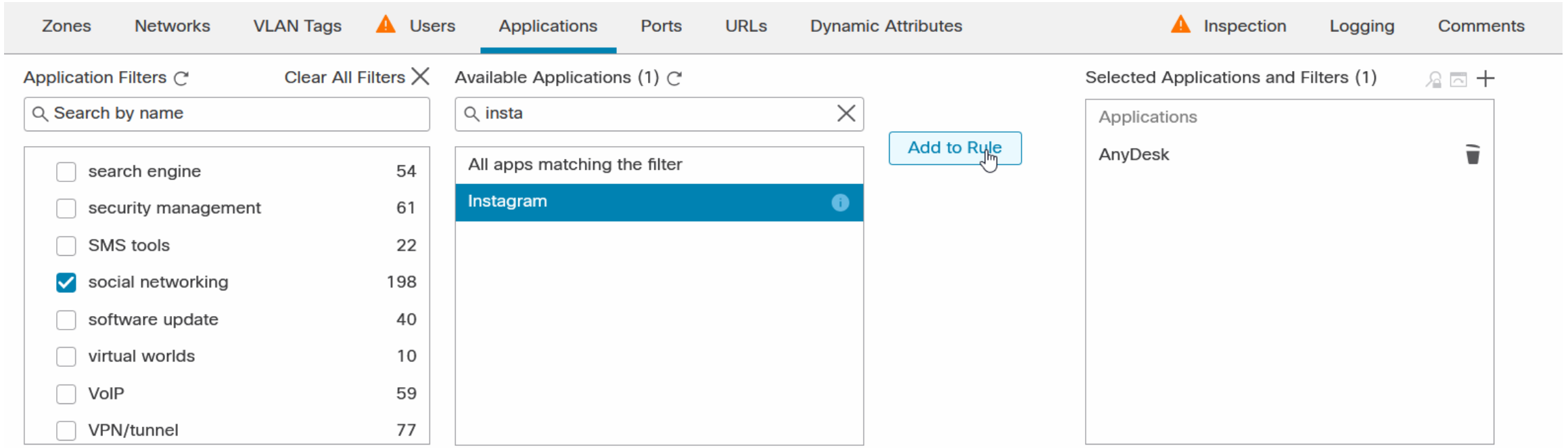
Rule Editor

- 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



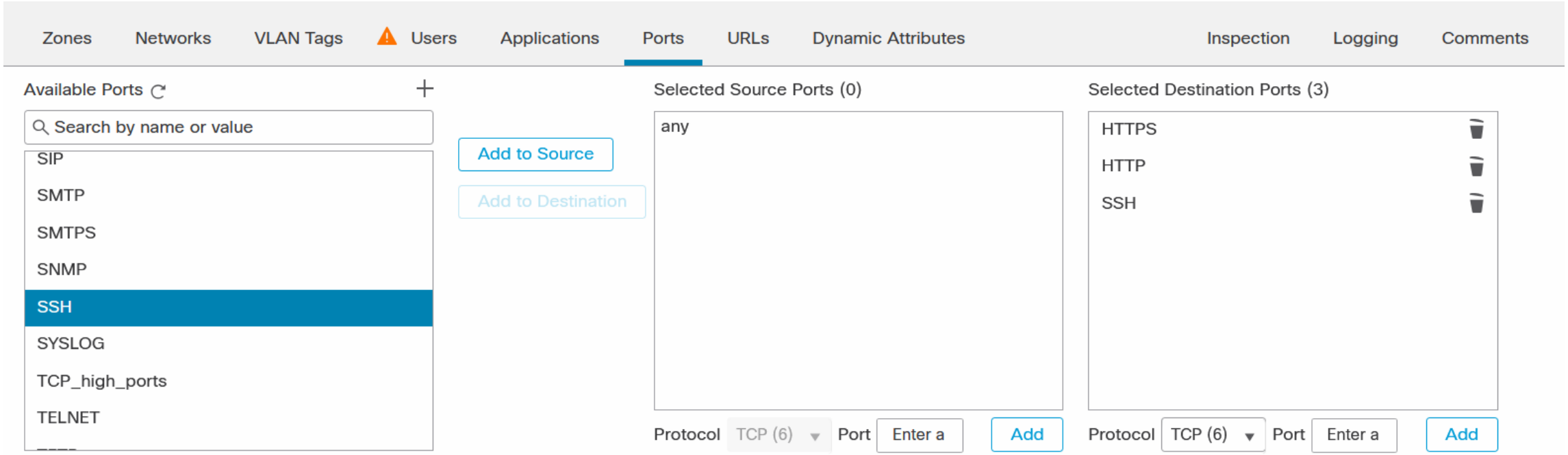
Rule Editor

- You can act to traffic based on application signature



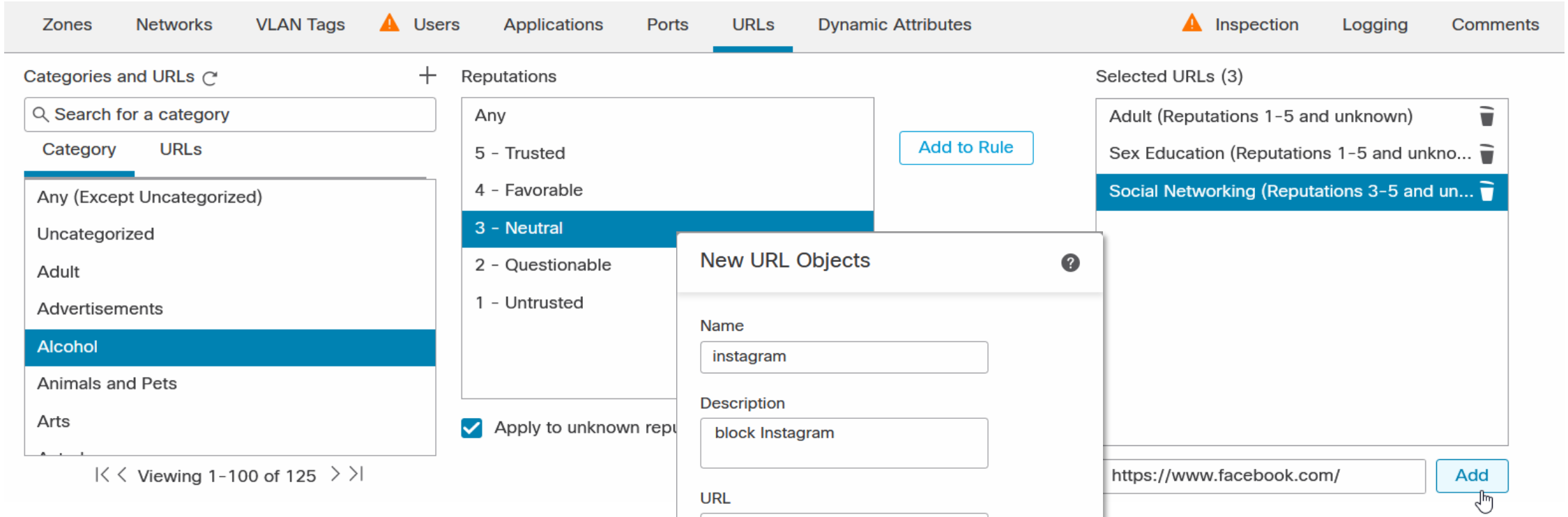
Rule Editor

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



Rule Editor

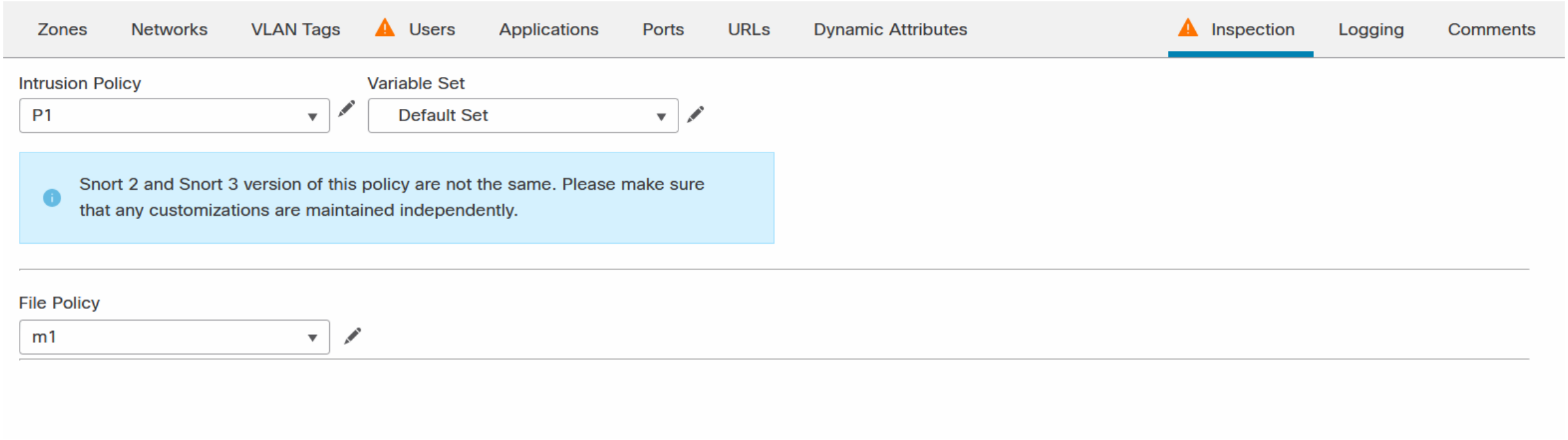
- You can filter traffic based on its URL , by predefined Category and Reputations , customized URL or enter manual URL



MohsenKheradmand MK

Rule Editor

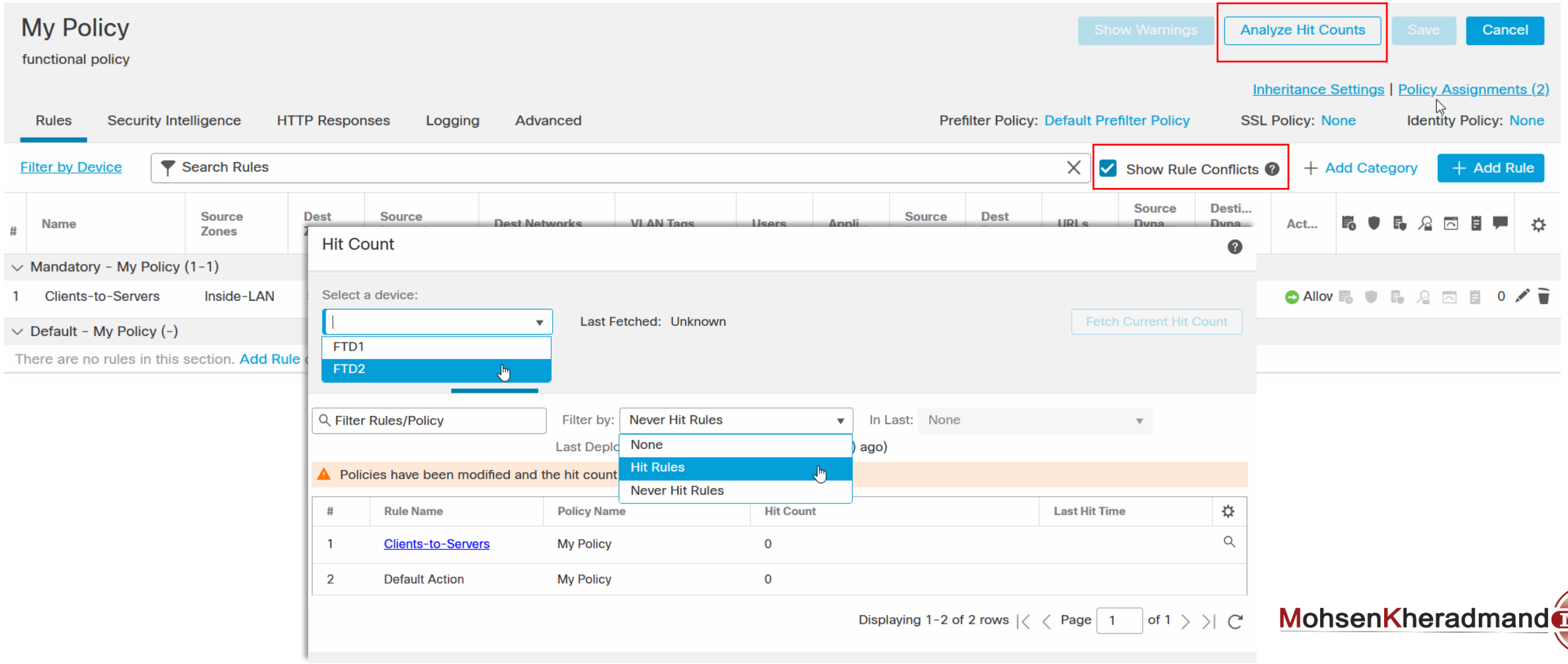
- On the Inspection tab, you can use the Intrusion Policy and File Policy to select desired next-generation security policies.



Rule Editor

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

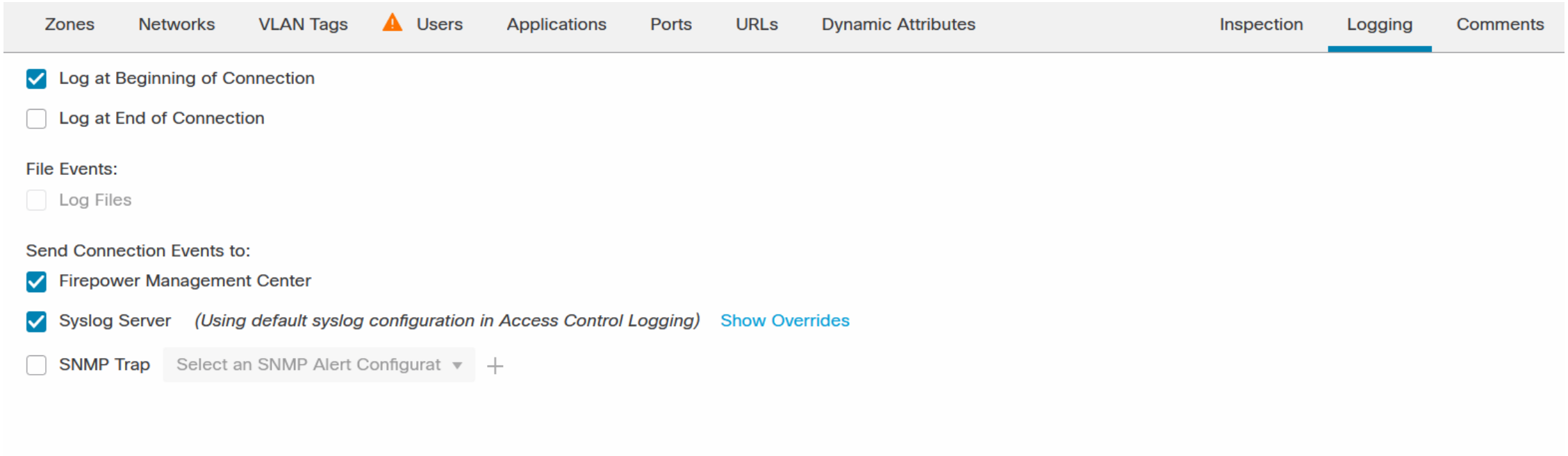
Analyze Hit Counts : to determine if there are any rules that never hit any traffic or matches and hit traffic



MohsenKheradmand MK

Rule Editor

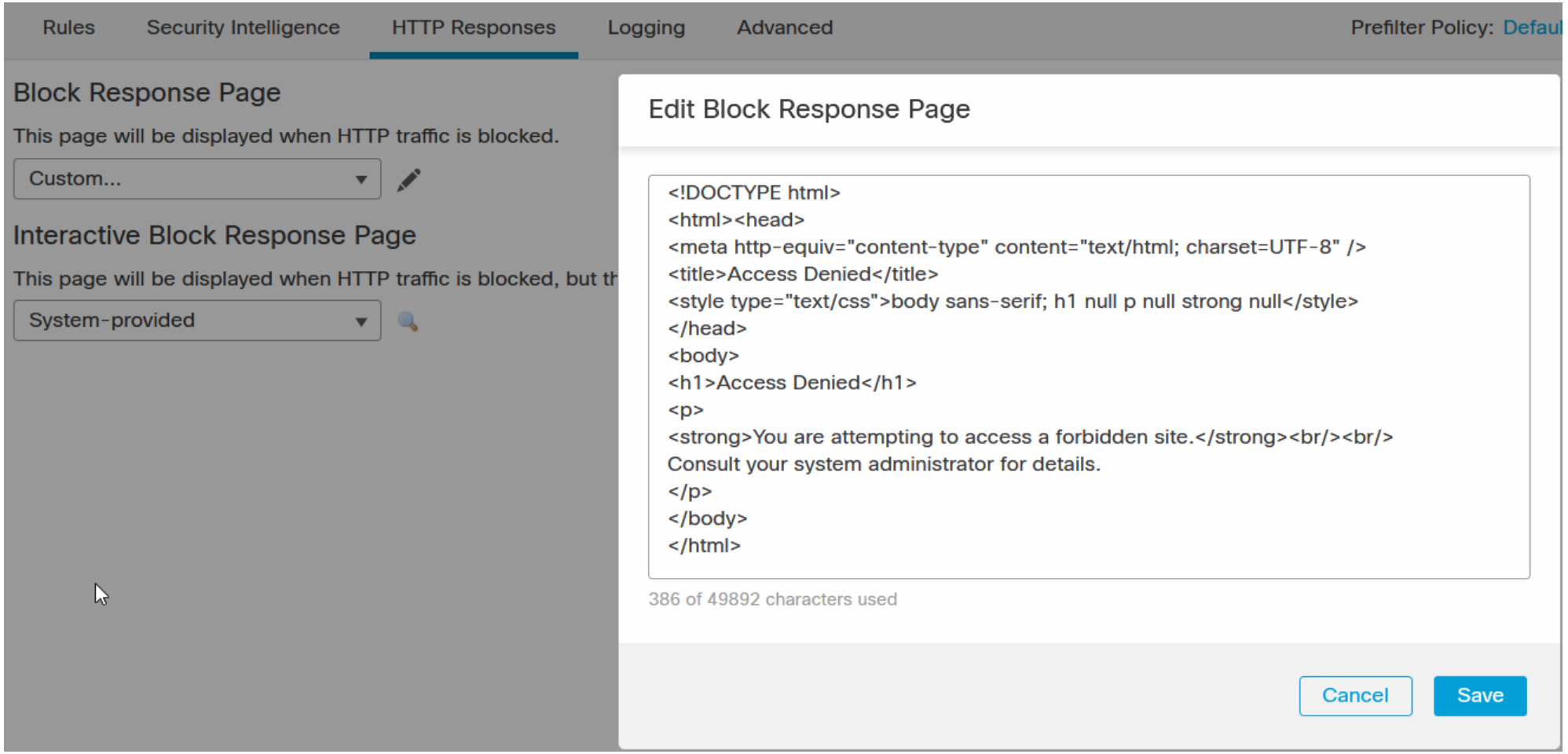
On the Logging tab, you can enable Log at Beginning/End of Connection to log the connections (helpful for troubleshooting)



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



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

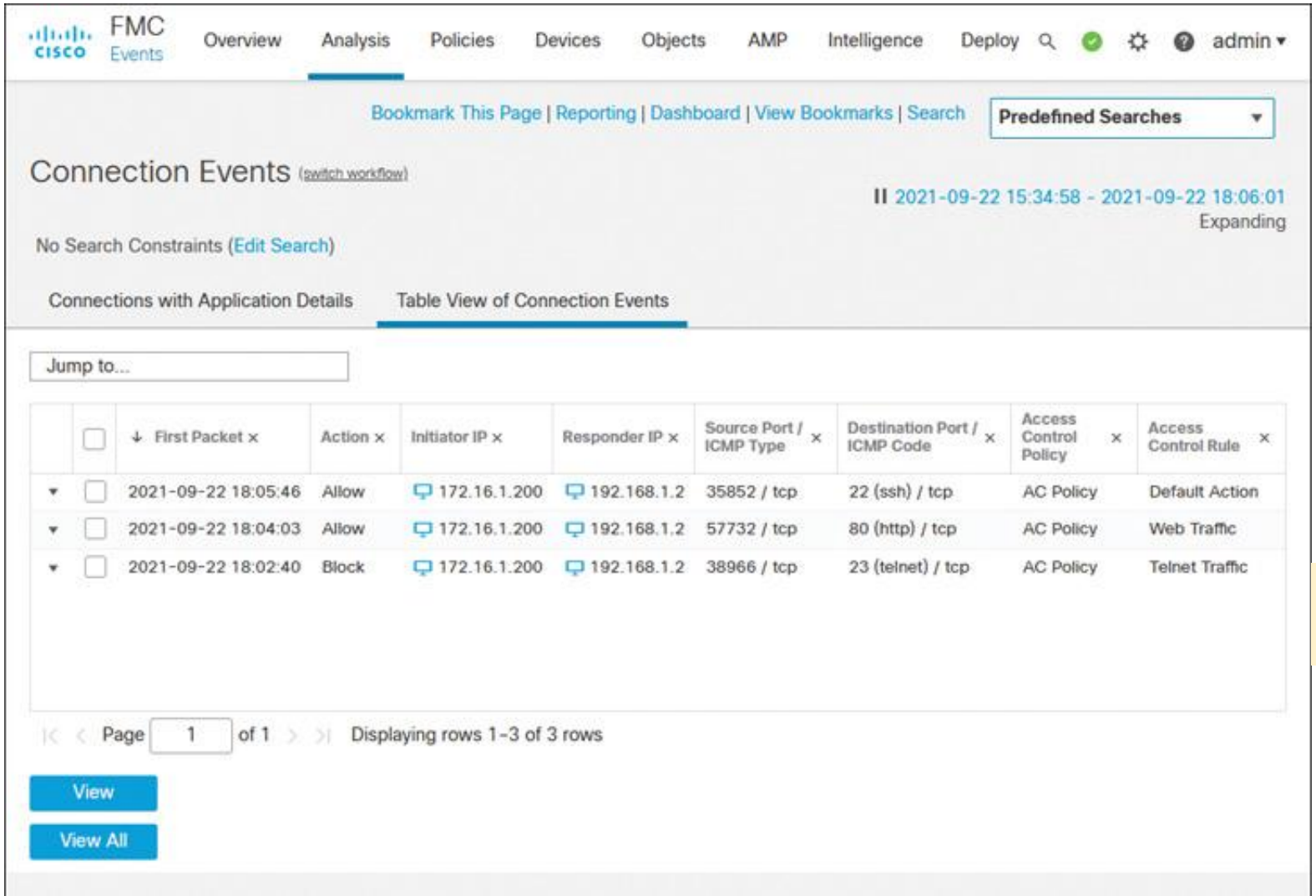
5) After adding all the access control rules, use the **Show Rule Conflict** check box to determine if there are any duplicate or overlapping rules (also known as shadowed rules).

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



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 I 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 I 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