

Cisco Firepower Threat Defense Policy Management Common Practices



Cisco Firepower Threat Defense (FTD) policies help you flag specific network traffic patterns, create alerts and better control your network. Consider these common practices and recommendations when deploying Cisco FTD policies.

Policy Management Table of Contents:

1. Access Policies

- Rationalizing
- Connection Logging
- Defining Flows
- Blocking Bad Traffic
- Determining What Needs Encryption

2. IPS Policies

- Testing Policies
- Leveraging Firepower Recommendations
- Deploying Strict Controls
- Leverage X-Forwarding
- Fine-Tuning Rules

3. Malware Policies

4. SSL Policies

5. Identity Policies

6. Network Analysis Policies

Access Policies

Rationalizing

Whether migrating from an existing firewall platform or building a net-new configuration, it's a good idea to rationalize rule sets and streamline or optimize where appropriate. For example, determine whether you can eliminate any of the following:



Services that have been decommissioned and are no longer required.

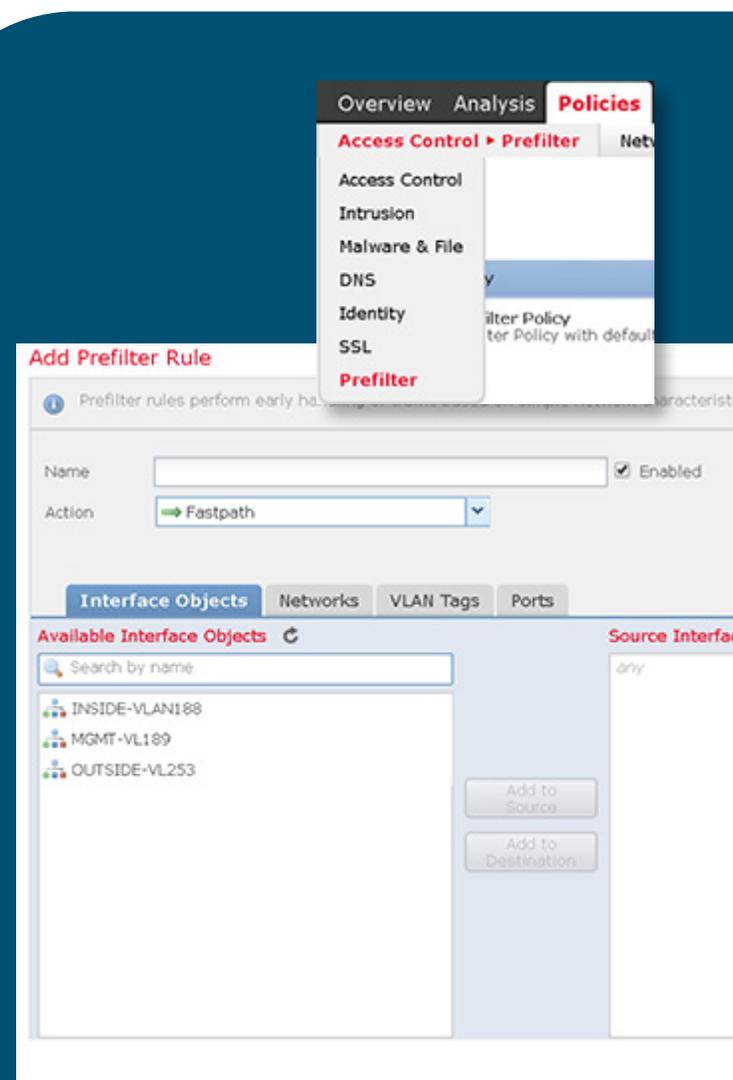


Policies that have grown too complex.



Rule sprawling, or when you have two rules with different ports or applications that can be combined under a single rule set.

Also, not all traffic needs a higher level of inspection. Use pre-filter policies to exclude traffic that doesn't need additional scrutiny, such as backups or highly critical flows that require low latency (think trading applications). Define these flows within the Cisco Firepower Management Center (FMC) pre-filter policy.



Access Policies

Connection Logging

While Connection Logging is a handy feature, it requires a lot of additional overhead and your security intelligence, Intrusion Prevention System (IPS), and malware events are already generated in threat data logging. You can always turn on Connection Logging as needed for troubleshooting later.

If you decide you want to perform Connection Logging, optimize your performance by either logging at the beginning or end of the connection—not both.

When logging with Block or Block with Reset, you can only log at the beginning of the connection. But if you want additional data such as traffic over the duration of the session, application details, etc., you should log at the end of connection.

If longer-term event storage is needed, you should consider external remote storage option such as external Security Information and Event Management (SIEM) and/or syslog infrastructure. Use e-streamer for advanced logging capabilities to external SIEM providers.

Editing Rule - Inspect-Traffic - FTP

The screenshot shows the configuration for a rule named "Inspect-Traffic - FTP". The rule is enabled and has an action of "Block". The "Log at Beginning of Connection" checkbox is checked and highlighted with a red box. Other options include "Log at End of Connection", "File Events", and "Send Connection Events to".

Editing Rule - Inspect-Traffic - FTP

Name: Enabled [Move](#)

Action:

Zones **Networks** **VLAN Tags** **Users** **Applications** **Ports** **URLs** **SGT/ISE Attributes**

Log at Beginning of Connection

Log at End of Connection

File Events:

Log Files

Send Connection Events to:

Event Viewer

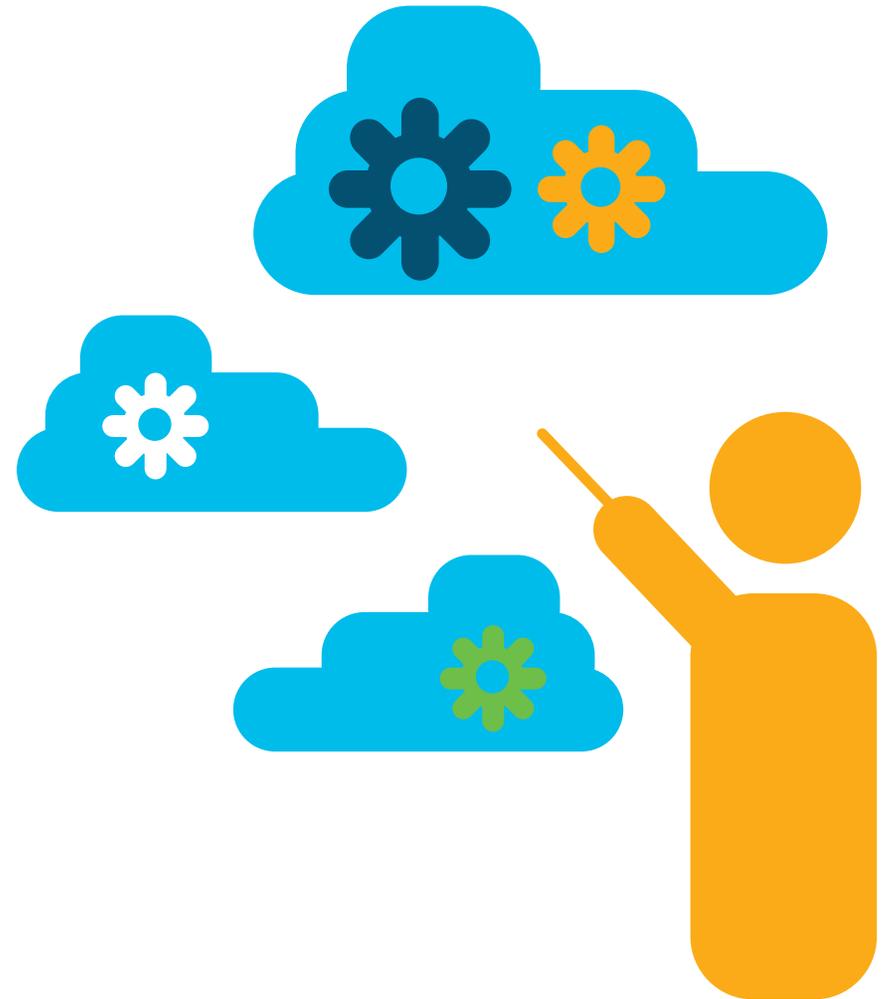
Syslog

SNMP Trap

Access Policies

Defining Flows

You can also simplify the critical and non-critical hosts within the environment and deploy strict controls for critical assets. Start by defining which flows require malware inspection. Then, optimize malware policies for the specific flow required. For example, if the flow requires you to inspect FTP traffic that contains document type files, then your malware policy should reflect the proper protocol and file type. This may include IPS and file/malware policies. Malware and IPS Policies will also reiterate this statement.



Access Policies

Blocking Bad Traffic

It's always a good idea to block known sources of bad traffic with Security Intelligence, and you don't need to process additional rule sets to do so. Plus, removing the bad actors from the beginning further optimizes the performance of Cisco FTD and reduces the overall risk to your organization.

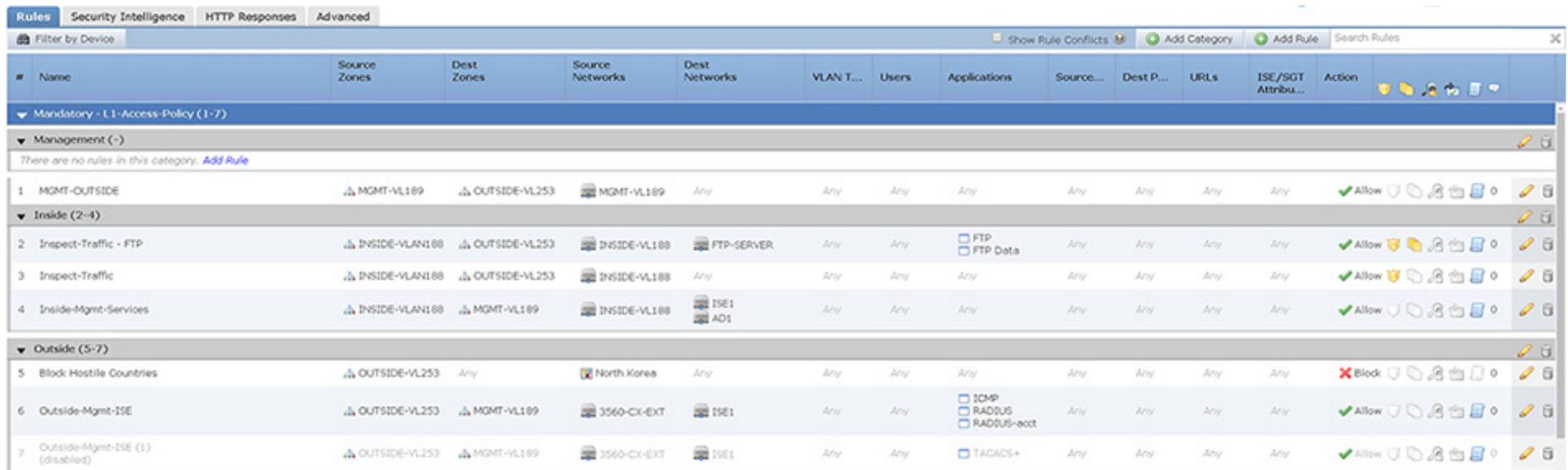
The screenshot displays the Cisco FTD configuration interface for an L1-Access-Policy. The interface is divided into several sections:

- Navigation Bar:** Overview, Analysis, Policies (selected), Devices, Objects, AMP, Intelligence. Sub-panels include Access Control, Network Discovery, Application Detectors, Correlation, and Actions.
- Policy Configuration:** Prefilter Policy: Default Prefilter Policy, SSL Policy: None, Identity Policy: None.
- Security Intelligence Section:** Includes tabs for Rules, Security Intelligence (selected), HTTP Responses, and Advanced.
- Available Objects:** A list of network objects such as any, IPv4-Private-All-RFC1918, 3560-CX-EXT, AD1, any-ipv4, any-ipv6, DEFAULT-GW, FTP-SERVER, INSIDE-VL100, IPv4-Benchmark-Tests, IPv4-Link-Local, IPv4-Multicast, IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16, IPv6-IPv4-Mapped, IPv6-Link-Local, IPv6-Private-Unique-Local-Addresses, IPv6-to-IPv4-Relay-Anycast, ISE1-EXT, and ISE1.
- Available Zones:** A list of zones including Any, INSIDE-VLAN100, MGMT-VL109, and OUTSIDE-VL253.
- DNS Policy:** Default DNS Policy. Includes a Whitelist (2) with items like Global Whitelist (Any Zone) and Global Whitelist for URL (Any Zone). It also features 'Add to Whitelist' and 'Add to Blacklist' buttons.
- Blacklist (30):** A list of 30 items, including Attackers (Any Zone), Bogon (Any Zone), Bots (Any Zone), CnC (Any Zone), Dga (Any Zone), Exploitkit (Any Zone), Malware (Any Zone), Open_proxy (Any Zone), Open_relay (Any Zone), Phishing (Any Zone), Response (Any Zone), Spam (Any Zone), Suspicious (Any Zone), Tor_exit_node (Any Zone), and Global Blacklist (Any Zone). Each item has a red 'X' icon and a trash icon.

Access Policies

Blocking Bad Traffic Continued

When building rules, use the minimum number of attributes to define the traffic of interest. Less is more. This helps to further optimize the rule sets and increase performance. Attributes include zones, networks, GEO location, VLAN tags, user/group, applications, ports, URLs and SGTs.



The screenshot displays the Cisco ISE Access Policy configuration interface. The top navigation bar includes tabs for 'Rules', 'Security Intelligence', 'HTTP Responses', and 'Advanced'. Below the navigation bar, there are options to 'Filter by Device', 'Show Rule Conflicts', 'Add Category', 'Add Rule', and a search box for 'Search Rules'. The main area shows a list of rules organized into categories: 'Mandatory - L1-Access-Policy (1-7)', 'Management (-)', 'Inside (2-4)', and 'Outside (5-7)'. Each rule row contains columns for Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN T..., Users, Applications, Source..., Dest P..., URLs, ISE/SGT Attribu..., Action, and a set of icons for editing and deleting the rule.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN T...	Users	Applications	Source...	Dest P...	URLs	ISE/SGT Attribu...	Action	Icons
▼ Mandatory - L1-Access-Policy (1-7)														
▼ Management (-)														
There are no rules in this category. Add Rule														
1	MGMT-OUTSIDE	MGMT-VL189	OUTSIDE-VL253	MGMT-VL189	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Icons
▼ Inside (2-4)														
2	Inspect-Traffic - FTP	INSIDE-VLAN188	OUTSIDE-VL253	INSIDE-VL188	FTP-SERVER	Any	Any	FTP FTP Data	Any	Any	Any	Any	Allow	Icons
3	Inspect-Traffic	INSIDE-VLAN188	OUTSIDE-VL253	INSIDE-VL188	Any	Any	Any	Any	Any	Any	Any	Any	Allow	Icons
4	Inside-Mgmt-Services	INSIDE-VLAN188	MGMT-VL189	INSIDE-VL188	ISE1 AD1	Any	Any	Any	Any	Any	Any	Any	Allow	Icons
▼ Outside (5-7)														
5	Block Hostile Countries	OUTSIDE-VL253	Any	North Korea	Any	Any	Any	Any	Any	Any	Any	Any	Block	Icons
6	Outside-Mgmt-ISE	OUTSIDE-VL253	MGMT-VL189	3560-CX-EXT	ISE1	Any	Any	ICMP RADIUS RADIUS-eoctl	Any	Any	Any	Any	Allow	Icons
7	Outside-Mgmt-ISE (1) (disabled)	OUTSIDE-VL253	MGMT-VL189	3560-CX-EXT	ISE1	Any	Any	TACACS+	Any	Any	Any	Any	Allow	Icons

Access Policies

Determining What Needs Encryption

Ascertain which kinds of traffic need decryption and define an SSL decryption policy. Again, when defining the flow, leverage the minimum number of attributes to uniquely classify the traffic. You'll also need to consider corporate policy when decrypting traffic. Many customers exclude flows such as banking, health, and finance based on internal corporate policies.

Additionally, make sure that you set your default action in correspondence with your security posture.

The screenshot shows the Palo Alto Networks configuration interface for the 'L1-Access-Policy'. The interface includes a navigation bar at the top with tabs for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The main content area is titled 'L1-Access-Policy' and shows a table of rules. The table has the following columns: #, Name, Source Zones, Dest Zones, Source Networks, Dest Networks, VLAN Tags, Users, Applications, Source Ports, Dest Ports, URLs, SSL/SIGT Attributes, and Action. The rules are grouped into sections: Mandatory (1-7), Inside (2-4), and Outside (5-7). The default action is set to 'Access Control: Block All Traffic'.

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	SSL/SIGT Attributes	Action
1	MGMT-OUTSIDE	MGMT-VL189	OUTSIDE-VL25	MGMT-VL189	Any	Any	Any	Any	Any	Any	Any	Any	Allow
▼ Inside (2-4)													
2	Inspect-Traffic - FTP	INSIDE-VLAN81	OUTSIDE-VL25	INSIDE-VL188	FTP-SERVER	Any	Any	FTP FTP Data	Any	Any	Any	Any	Allow
3	Inspect-Traffic	INSIDE-VLAN81	OUTSIDE-VL25	INSIDE-VL188	Any	Any	Any	Any	Any	Any	Any	Any	Allow
4	Inside-Mgmt-Services	INSIDE-VLAN81	MGMT-VL189	INSIDE-VL188	ISE1 AD1	Any	Any	Any	Any	Any	Any	Any	Allow
▼ Outside (5-7)													
5	Block Hostile Countries	OUTSIDE-VL25	Any	North Korea	Any	Any	Any	Any	Any	Any	Any	Any	Block
6	Outside-Mgmt-ISE	OUTSIDE-VL25	MGMT-VL189	3500-CK-EXT	ISE1	Any	Any	SDP RADIUS RADIUS-act	Any	Any	Any	Any	Allow
7	Outside-Mgmt-ISE (1) (disabled)	OUTSIDE-VL25	MGMT-VL189	3500-CK-EXT	ISE1	Any	Any	TACACS+	Any	Any	Any	Any	Allow
▼ Default - L1-Access-Policy (-)													
There are no rules in this section. Add Rule or Add Category													
Default Action													Access Control: Block All Traffic

Review the available settings under Advanced > Access Control Policy and select the value that is best suited for your environment. You can see detailed information about each setting from the Help > Online utility.

IPS Policies

Start with the proper default policy and ensure that the network analysis policy uses the same approach. For example, if you build an IPS policy with balanced connectivity and security, then your Network Analysis policy should use the same approach.

The most common approach used by customers is to start with Balanced and tweak from there.



Testing Policies

Consider testing IPS policies before deploying. This ensures that the policy is further optimized prior to moving the rule set into production. This can include passive or inline tap modes or inline mode with the “drop when inline” option unchecked.

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this, there are sub-tabs for 'Access Control', 'Intrusion', 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions'. The main heading is 'Edit Policy: IPS Core Policy **NO DROP**'. On the left, there is a sidebar with 'Policy Information' (selected), 'Rules', 'Firepower Recommendations', 'Advanced Settings', and 'Policy Layers'. The main content area shows the 'Policy Information' section with the following details:

- Name: IPS Core Policy **NO DROP**
- Description: (empty field)
- Drop when Inline: (highlighted with a red box)
- Base Policy: Balanced Security and Connectivity
- Status: The base policy is up to date (Rule Update 2016-11-29-001-vrt)
- Summary: This policy has 8507 enabled rules
 - 74 rules generate events
 - 8433 rules drop and generate events
- Footer: No recommendations have been generated. [Click here to set up Firepower recommendations.](#)

IPS Policies

Configuring Variables Sets

Variable sets provide deeper accuracy in terms of detection and reduce the amount of noise. It's critical that you populate the variable sets with information that reflects your environment, and you should also update your variable sets as your environment changes.

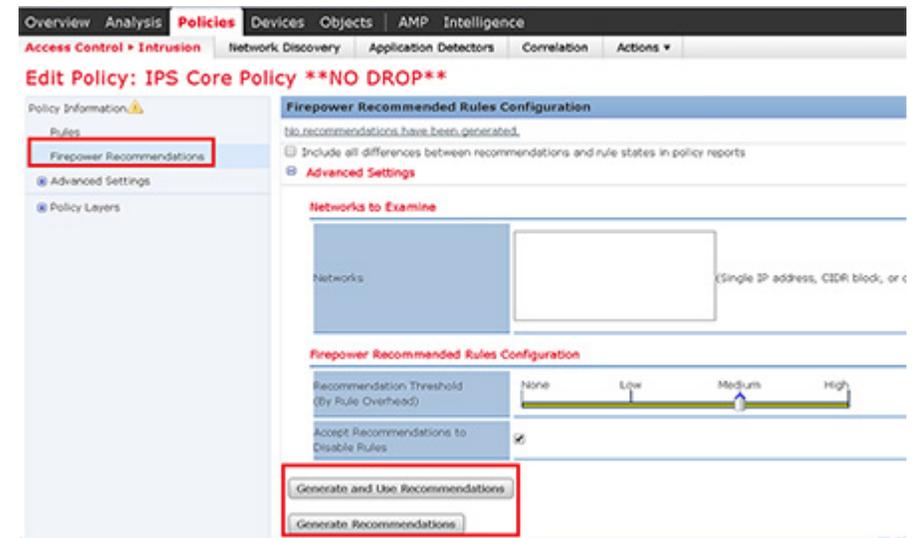
The screenshot displays a network management interface with a sidebar on the left and a main content area. The sidebar contains a tree view of objects, with 'Variable Set' highlighted in a red box. The main content area shows a 'New Variable Set' dialog box. The dialog box has a title bar with a question mark and a close button. It contains a 'Name' field with the value 'MyVariable-Set' and a 'Description' field with the placeholder text 'Enter Description'. Below the fields is a red notification that says 'You have unsaved changes' and an 'Add' button. The main part of the dialog is a table with three columns: 'Variable Name', 'Type', and 'Value'. The table is divided into two sections: 'Customized Variables' and 'Default Variables'. The 'HOME_NET' variable is highlighted in a red box. The 'Default Variables' section includes variables like 'AIM_SERVERS', 'DNS_SERVERS', 'EXTERNAL_NET', 'FILE_DATA_PORTS', 'FTP_PORTS', 'GTP_PORTS', and 'HTTP_PORTS'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Variable Name	Type	Value
Customized Variables		
HOME_NET	Network	[MGMT-VL189, INSIDE-VL188]
Default Variables		
AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6...]
DNS_SERVERS	Network	HOME_NET
EXTERNAL_NET	Network	any
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]
GTP_PORTS	Port	[3386, 2123, 2152]
HTTP_PORTS	Port	[8300, 8040, 2231, 90, 6767, 443, 8983,...]

IPS Policies

Leveraging Firepower Recommendations

Firepower Recommendations uses the data passively collected about the operating systems, servers, and client applications within the environment and then associates specific rules to protect these assets. Some organizations also run Firepower Recommendations after every new service brought online and will incorporate this into the change management process. You can also run Firepower Recommendations on a regular cadence (monthly, quarterly) to be sure that the IPS rule set is always optimized.



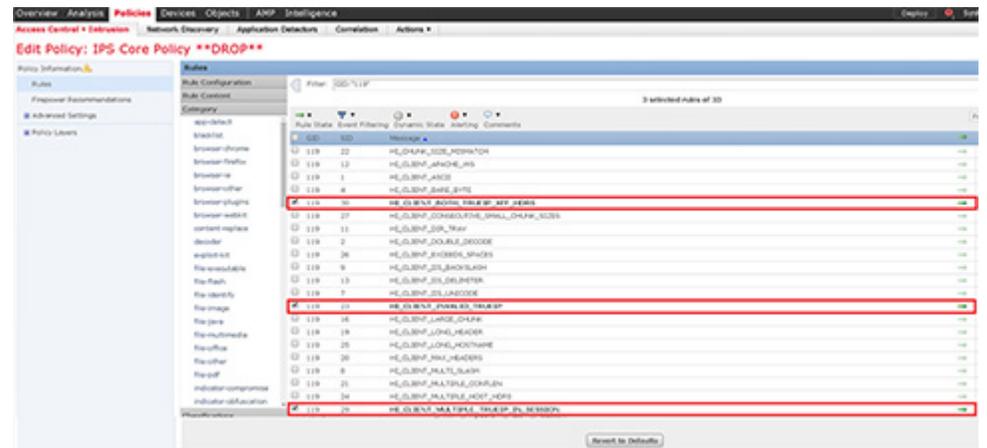
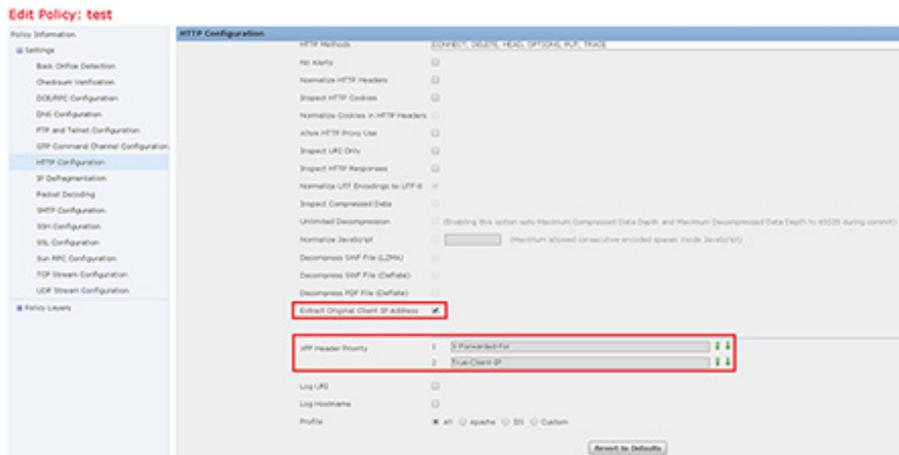
Deploying Strict Controls

Define the critical and non-critical hosts within the environment and deploy strict controls for critical assets. This may include IPS and file/malware policies.

IPS Policies

Leverage X-Forwarding

If you have a proxy server deployed, leverage x-forwarding. This needs to be enabled on both the proxy and Firepower Device.



IPS Policies

Fine-Tuning Rules

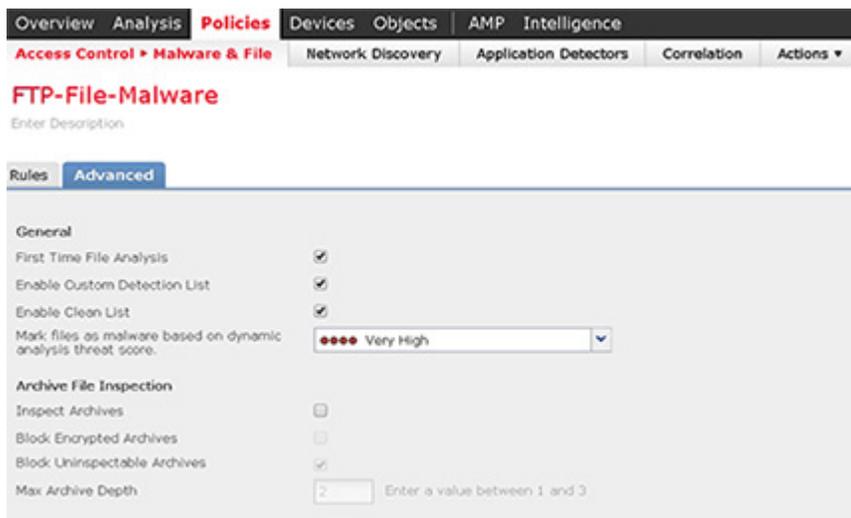
When enabling pre-processors, you'll also need to enable the corresponding IPS signatures of interest (see screenshots from X-Forwarding). It's recommended that you do not enable all the intrusion rules within an intrusion policy, as this will degrade performance and may increase false positives. Tuning is key, and Firepower Recommendations further help streamline this process.

Be careful when importing a rule update with new or updated shared object rules, which are binaries. This restarts the Snort process when you deploy configuration changes, temporarily interrupting traffic inspection. Whether traffic drops during this interruption or passes without further inspection depends on the model of the managed device and how it handles traffic. Make sure your process for downloading and installing rule updates complies with your security policies. In addition, intrusion rule updates may be large, so import rules during periods of low network use.



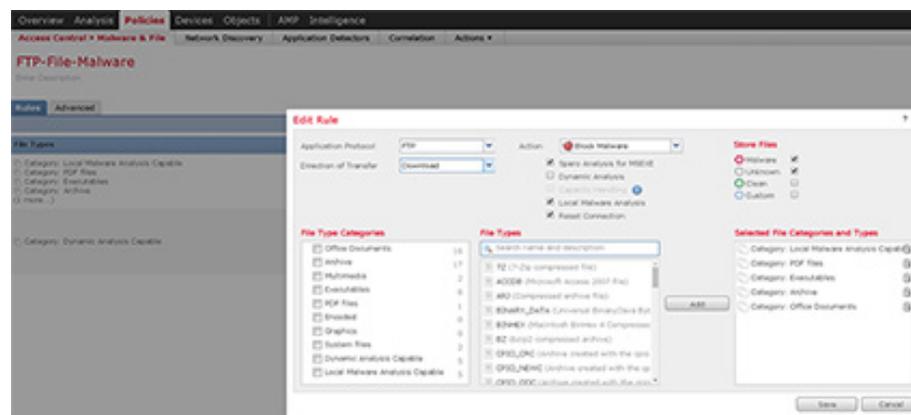
Malware Policies

You should leverage the default value under “Advanced” unless your environment dictates otherwise.



You’ll also want to define which flows require malware inspection and optimize malware policies for the specific flow required. For example, if the flow requires that you inspect FTP traffic that contains document type files, then your malware policy should reflect the proper protocol and file type. This may include IPS and file/malware policies. Malware and IPS Policies will also reiterate this statement.

You can define the critical and non-critical hosts within the environment and deploy strict controls for critical assets. This may include IPS and file/malware policies.



Malware Policies

Additionally, Malware alerts should be enabled based on your security policy.

The screenshot shows the configuration page for Malware Policies. The navigation bar includes Overview, Analysis, Policies (selected), Devices, Objects, AMP, and Intelligence. Below this, there are tabs for Access Control, Network Discovery, Application Detectors, Correlation, and Actions > Alerts. The main content area has tabs for Alerts, Impact Flag Alerts, Discovery Event Alerts, Advanced Malware Protection Alerts (selected), and Intrusion Email.

Alerts

Select alert responses to use for advanced malware detection event alerts. You must click Save after you make your selections.

Syslog: Syslog
Email: None
SNMP: None

Event Configuration

Select the event types for which you want to generate alerts.

Event	Syslog	Email	SNMP
Retrospective Events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All network-based malware events	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Save

Lastly, enable the reset connection option for Block Files and/or Block Malware. This terminates the connection.

SSL Policies

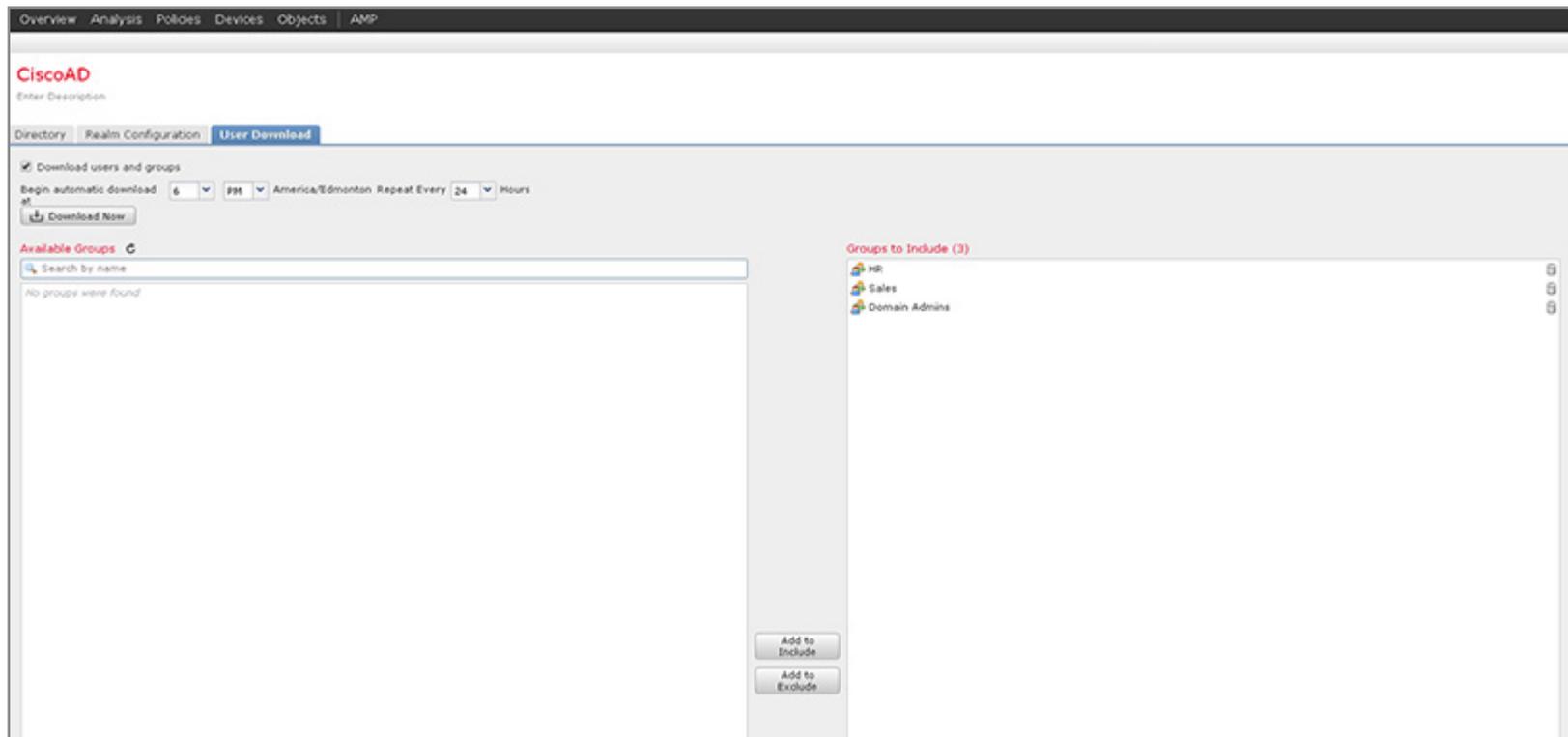
Determine which traffic flows need decryption and define an SSL decryption policy. Again when defining the flow, leverage the minimum number of attributes to uniquely classify the traffic.

Consider corporate policy when decrypting traffic. Just like with Access Policies, many customers exclude flows such as banking, health, and finance based on internal corporate policies. Also, make sure that you set your default action in correspondence with your security posture and that the CA you use for Decrypt Resign is signed by a corporate CA and installed in users' browsers, or you should only target users that have this CA installed as a trusted CA.



Identity Policies

If using passive authentication with the Cisco Firepower User Agent, make sure that all domain servers are targeted. Only include groups in realm that are needed for policy enforcement. This will limit the number of users and groups that have to be downloaded and post-processed from AD.



Consider leveraging Cisco ISE or Cisco ISE Passive Identity Connector with integrated user- or device-based policies. This allows synergy across multiple Cisco security platforms.

Network Analysis Policies

Start with a base policy that reflects your security posture as mentioned in the IPS Policies section. Remember, if you build an IPS policy with balanced connectivity and security, then your Network Analysis policy should use the same approach.

If inline normalization is enabled in your Network Analysis Policy, make sure that the GID 129 rules are enabled in IPS policies, so that you're alerted when Inline Normalization is dropping traffic. Otherwise, traffic will be dropped silently with no explanation.



Author: Jason Maynard, CSE Cybersecurity, Cisco.