Common Acronyms

FDM – Firepower Device Management – On-Device Firewall management service, GUI based.

FMC – Firewall management Center – usually deployed in a remote network and used for firepower management across the general internet. GUI based. (Ignore most references to this, competitions will use FDM)

CDO – Cisco Defense Orchestrator – Enterprise level management, not needed

FTD – Firepower Threat Defense – The hardware or virtual firewall itself.

Password Reset:

https://www.cisco.com/c/en/us/support/docs/security/

Reset the Admin Password on the ASA 5512-X through ASA 5555-X and ASA 5506-X through ASA 5516-X (Software ASA Firepower Module) and ISA 3000 Devices

```
> session sfr do password-reset
```

Reset the Admin Password on the ASA 5585-X Series Devices (Hardware ASA Firepower Module)

```
> session 1 do password-reset
```

Change the CLI or Shell Admin Password for FMCs and NGIPSv

Use these instructions to reset a known password for these admin accounts:

- Firepower Management Center: admin password used to access the CLI or the shell.
- Next Generation Information Preservation System virtual (NGIPSv: admin password used to access the CLI.

Procedure:

1. Log into the appliance admin account by SSH or the console.
    a. For the Firepower Management Center:
    b. If your Firepower Management Center runs Firepower Version 6.2 or lower, the log in gives you direct access to the Linux shell.
    c. If your Firepower Management Center runs Firepower Version 6.3 or 6.4 and the Firepower Management Center CLI is not enabled, log in gives you direct access to the Linux shell.
    d. If your Firepower Management Center runs Firepower Version 6.3 or 6.4 and the Firepower Management CLI is enabled, log in gives you access to the Firepower Management Center CLI. Enter the expert command to access the Linux shell.
    e. If your Firepower Management Center runs Firepower Version 6.5+, log in gives you access to the Firepower Management Center CLI. Enter the expert command to access the Linux shell.
    f. For managed devices, log in gives you access to the device CLI. Enter the expert command to access the Linux shell.
2. At the shell prompt enter this command: sudo passwd admin.
3. When prompted, enter the current admin password to elevate privilege to root access.

4. In response to prompts, enter the new admin password twice.

More cases are covered in cisco link above ^

Firepower Management Center (FMC) is a Linux box. Sudo rules apply in CLI, not in webGUI

> sudo configure network

Management interface configuration (IPv4 and IPv6)

Check for admin user accounts

> System > Users

Check for licensing

> System > Licenses > Smart licenses (or Licenses)

- Base – everything but what is covered by other licensing
- Malware – required for Advanced Malware Protection (AMP) and AMP Threat Grid
- Threat – checks for file types and intrusion and exploit alerts
- URL Filtering – filters URLs based on 'reputation'
- RA VPN – needed for anyConnect VPN configuration

Routed vs Transparent Mode

Routed Mode

- Each interface connects to its own subnet.
- Each interface is the gateway for the subnet attached to it.
- This will be the mode for Regionals
- Configure firewall using FDM

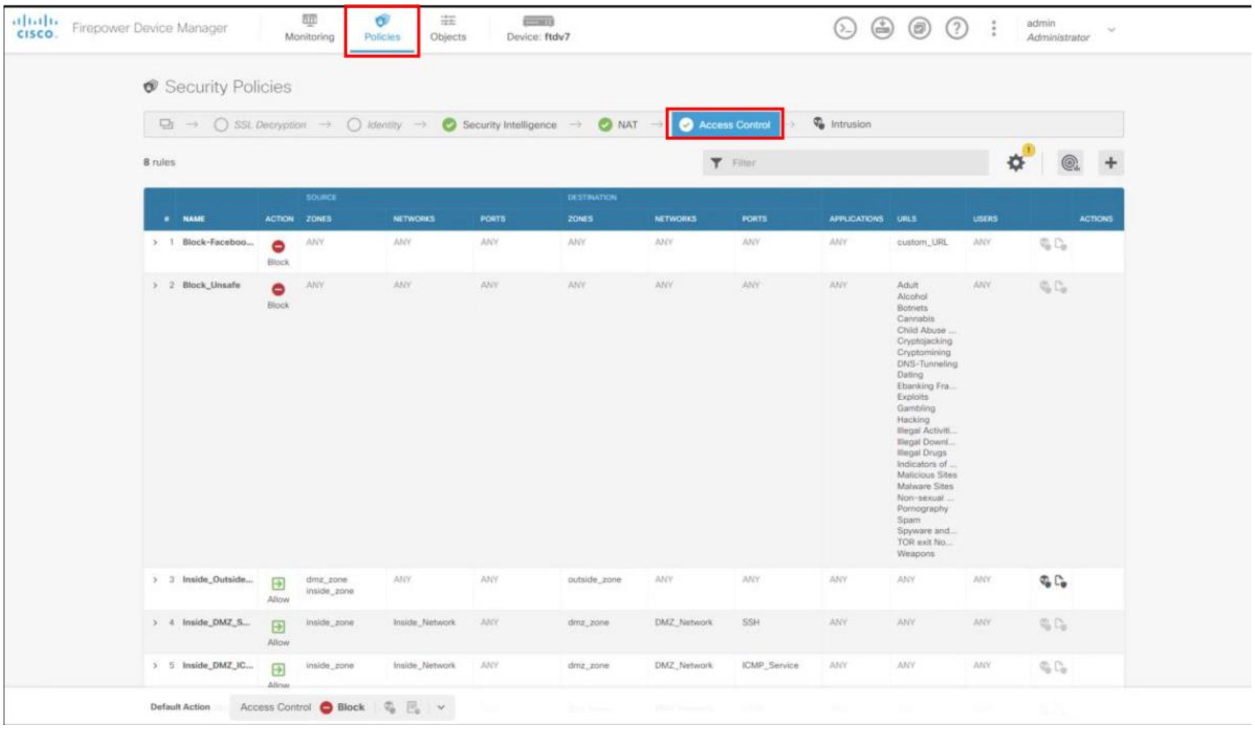
Transparent Mode

- FTD sits as a mitm, invisible to the client machines
- Requires a layer 3 router to route traffic
- Configure firewall using FMC

Access Control

Very similar to security policies on Palo Alto NGFW

Priority is given top to bottom and the rule applied to traffic is the first one it matches.



8 rules

			SOURCE			DESTINATION						
#	NAME	ACTION	ZONES	NETWORKS	PORTS	ZONES	NETWORKS	PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Block-Faceboo...	Block	ANY	ANY	ANY	ANY	ANY	ANY	ANY	custom_URL	ANY	
2	Block_Unsafe	Block	ANY	ANY	ANY	ANY	ANY	ANY	ANY	Adult Alcohol Botnets Cannabis Child Abuse ... Cryptojacking Cryptomining DNS-Tunneling Dating Ebanking Fra... Exploits Gambling Hacking Illegal Activiti... Illegal Downl... Illegal Drugs Indicators of ... Malicious Sites Malware Sites Non-sexual ... Pornography Spam Spyware and... TOR exit No... Weapons	ANY	
3	Inside_Outside...	Allow	dmz_zone inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	
4	Inside_DMZ_S...	Allow	inside_zone	Inside_Network	ANY	dmz_zone	DMZ_Network	SSH	ANY	ANY	ANY	
5	Inside_DMZ_IC...	Allow	inside_zone	Inside_Network	ANY	dmz_zone	DMZ_Network	ICMP_Service	ANY	ANY	ANY	

Default Action Access Control Block

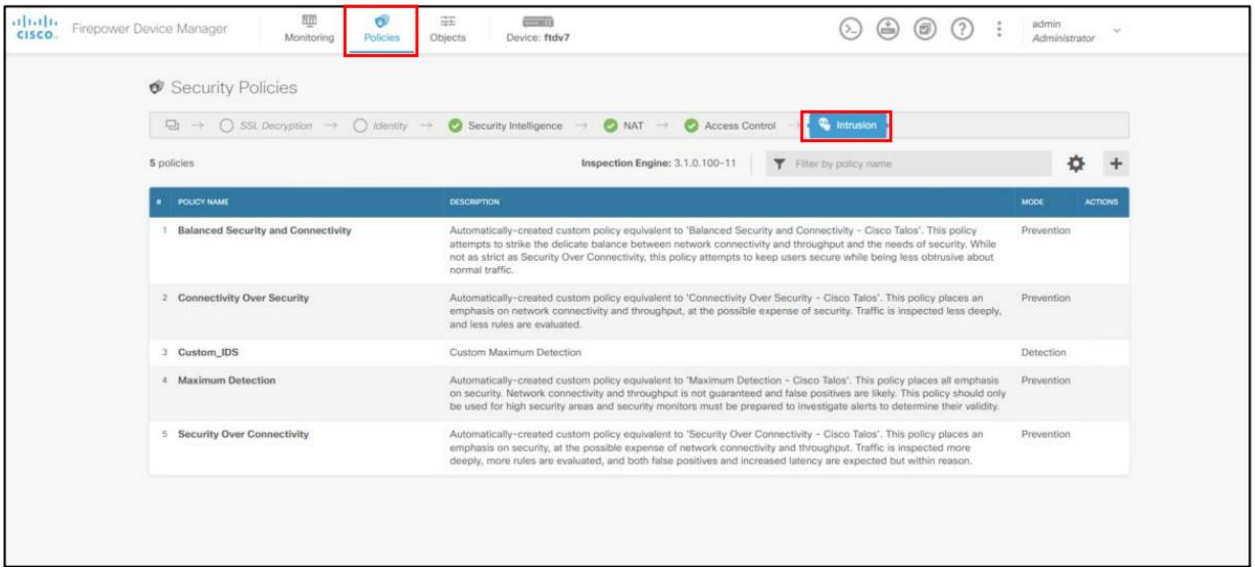
Intrusion Detection

Network analysis policies (NAP) and intrusion policies work together

A network analysis policy (NAP) governs how traffic is decoded and preprocessed so that it can be further evaluated, especially for anomalous traffic that might signal an intrusion attempt.

An intrusion policy uses intrusion and preprocessor rules, which are collectively known as intrusion rules, to examine the decoded packets for attacks based on patterns. The rules can either prevent (drop) the threatening traffic and generate an event, or simply detect (alert) it and generate an event only.

As the system analyzes traffic, the network analysis decoding and preprocessing phase occurs before and separately from the intrusion prevention phase. Together, network analysis and intrusion policies provide broad and deep packet inspection. They can help you detect, alert on, and protect against network traffic that could threaten the availability, integrity, and confidentiality of hosts and their data.



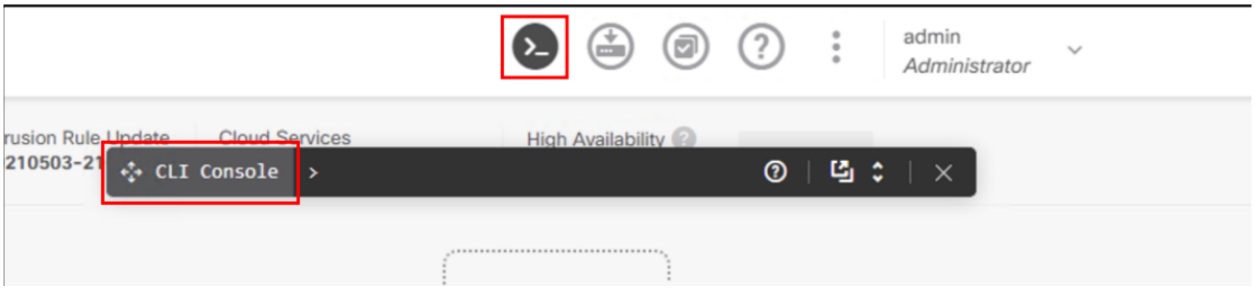
5 policies

Inspection Engine: 3.1.0.100-11

#	POLICY NAME	DESCRIPTION	MODE	ACTIONS
1	Balanced Security and Connectivity	Automatically-created custom policy equivalent to 'Balanced Security and Connectivity - Cisco Talos'. This policy attempts to strike the delicate balance between network connectivity and throughput and the needs of security. While not as strict as Security Over Connectivity, this policy attempts to keep users secure while being less obtrusive about normal traffic.	Prevention	
2	Connectivity Over Security	Automatically-created custom policy equivalent to 'Connectivity Over Security - Cisco Talos'. This policy places an emphasis on network connectivity and throughput, at the possible expense of security. Traffic is inspected less deeply, and less rules are evaluated.	Prevention	
3	Custom_IDS	Custom Maximum Detection	Detection	
4	Maximum Detection	Automatically-created custom policy equivalent to 'Maximum Detection - Cisco Talos'. This policy places all emphasis on security. Network connectivity and throughput is not guaranteed and false positives are likely. This policy should only be used for high security areas and security monitors must be prepared to investigate alerts to determine their validity.	Prevention	
5	Security Over Connectivity	Automatically-created custom policy equivalent to 'Security Over Connectivity - Cisco Talos'. This policy places an emphasis on security, at the possible expense of network connectivity and throughput. Traffic is inspected more deeply, more rules are evaluated, and both false positives and increased latency are expected but within reason.	Prevention	

CLI Commands

Cisco is lazy so they implemented a ssh cli console on their webGUI, crazy I know.



> ?

> ping

Both will be your friend as normal cisco cli configuration rules apply. Example:

> show running-config

> show interface ip brief

Cisco has all commands listed over 12 different pages - good luck finding a command without the name: https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense/tz.html

Figure 1: If you are limited to the CLI I wish you good luck

Basic Configuration

Security policies are based on security zones, (like Palo Altos), found under Objects > Security Zones

Basic Security Policies:

SSL Decryption - to inspect encrypted connections (such as HTTPS) for intrusions, malware, and so forth, you must decrypt the connections.

Identity – User ID equivalent – not necessary for regionals

Security Intelligence – blocking based on blacklists

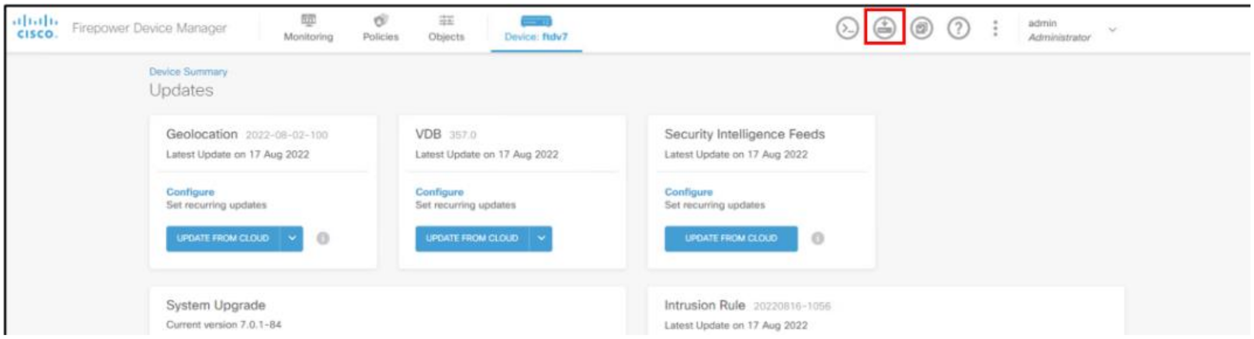
Nat – should already exist

Access Control – Intrusion and file policies are applied using access control policies. Application and port controls are also applied with access control policies

Intrusion – known threat policies

Commit Changes

Press Deploy Now button to commit



Updates

Geolocation 2022-08-02-100
Latest Update on 17 Aug 2022
Set recurring updates

VDB 357.0
Latest Update on 17 Aug 2022
Set recurring updates

Security Intelligence Feeds
Latest Update on 17 Aug 2022
Set recurring updates

System Upgrade
Current version 7.0.1-84

Intrusion Rule 20220816-1056
Latest Update on 17 Aug 2022

Cli: each of these are valid ways to commit changes but vary depending on the device and software.

```
# copy running-config startup-config

# write memory

# commit
```

Configuring Access Control Rules

1. Select Policies > Access Control.
2. Do any of the following:
   - To create a new rule, click the + button.
   - To edit an existing rule, click the edit icon ( ) for the rule.
3. Select where you want to insert the rule in the ordered list of rules.

Rules are applied on a first-match basis, so you must ensure that rules with highly specific traffic matching criteria appear above policies that have more general criteria that would otherwise apply to the matching traffic.

The default is to add the rule to the end of the list. If you want to change a rule's location later, edit this option.

4. In Title, enter a name for the rule.
5. Select the action to apply to matching traffic.
   - Trust: Allow traffic without further inspection of any kind.
   - Allow: Allow the traffic subject to the intrusion and other inspection settings in the
   - policy.
   - Block: Drop the traffic unconditionally. The traffic is not inspected.

Step 6 - Define the traffic matching criteria using any combination of the following tabs:

- Action:
  - Trust—Allow traffic without further inspection of any kind.
  - Allow—Allow the traffic subject to the intrusion policy.
  - Block—Drop the traffic unconditionally. The traffic is not inspected.
- Source/Destination Zones
- Source/Destination Networks

- Source/Destination Ports/Protocols
- Source/Destination SGT Groups (Security Group Tag)
  - You must define an ISE (Identity Services Engine) identity source; otherwise, this section will not appear
- Applications
  - Relationship between filters is AND, relationship between single criteria is OR
  - Risk is High OR Medium AND Business Relevance is Low OR Very Low
- URLs
- Users
- Intrusion Policy
  - Just turn on and select either Maximum Security or Security over Connectivity
    - Which ever one is chosen above should be used in all other available locations per best practices. (Network Analysis Policy (NAP) & Intrusion Policy)
  - Management Interface must have internet access to update definitions from AMP Cloud
- File Policy
  - Enable "Block Malware All"
  - "Cloud Lookup All" will only log all files and not block any.
  - Possible outcomes of a file lookup:
    - Malware: The AMP cloud categorized the file as malware. An archive file (e.g. a zip file) is marked as malware if any file within it is malware.
    - Clean: The AMP cloud categorized the file as clean, containing no malware. An archive file is marked as clean if all files within it are clean.
    - Unknown: The AMP cloud has not assigned a disposition to the file yet. An archive file is marked as unknown if any file within it is unknown.
    - Unavailable: The system could not query the AMP cloud to determine the file's disposition. You may see a small percentage of events with this disposition; this is expected behavior. If you see several "unavailable" events in succession, ensure that the Internet connection for the management address is functioning correctly.
- Logging
  - Cisco only allows Beginning & End of connection logging for block rules
  - Log at End of Connection is recommended for allowed traffic
  - No logging is the default

Best Practices

1. Configure the default action for the policy.
2. Click the Access Policy Settings button and enable the TLS Server Identity Discovery option.
3. Create as few access control rules as possible.
4. Enabling logging on your access control rules.
5. Put very specific rules at the top of the policy.
6. Pair Block and Allow rules to target subsets of traffic.
7. Target traffic regardless of IP address or port.
   a. Specifically, Application and URL filtering – user filtering may not be possible
8. Apply intrusion inspection to all your Allow rules.
9. Configure the Security Intelligence policy to block unwanted IP addresses and URLs.

    a. Policies > Access Control > Security Intelligence

10. Implement the SSL Decryption policy.
    a. Intrusion policies do not work without SSL Decryption

Intrusion Policies

System Provided Policies: Pick one and use it across all other references to an intrusion policy. They are meant to be used together as they are configured together by Cisco Talos Intelligence Group.

Security Over Connectivity network analysis and intrusion policies

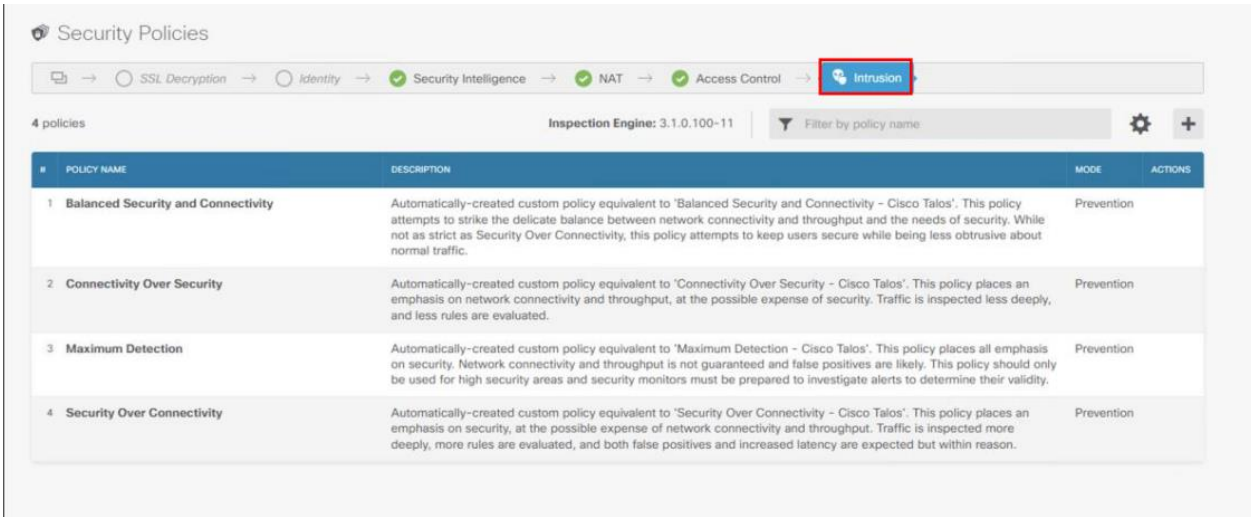
> These policies are built for networks where network infrastructure security takes precedence over user convenience. The intrusion policy enables numerous network anomaly intrusion rules that could alert on or drop legitimate traffic.

Maximum Detection network analysis and intrusion policies

> These policies are built for networks where network infrastructure security is given even more emphasis than is given by the Security Over Connectivity policies, with the potential for even greater operational impact. For example, the intrusion policy enables rules in many threat categories including malware, exploit kit, old and common vulnerabilities, and known in-the-wild exploits

By default, all intrusion policies operate in Prevention mode to implement an Intrusion Prevention System (IPS). In the Prevention inspection mode, if a connection matches an intrusion rule whose action is to drop traffic, the connection is actively blocked.

Detection mode changes dropped traffic to “would have blocked” which is bad.



4 policies

Inspection Engine: 3.1.0.100-11

#	POLICY NAME	DESCRIPTION	MODE	ACTIONS
1	Balanced Security and Connectivity	Automatically-created custom policy equivalent to 'Balanced Security and Connectivity - Cisco Talos'. This policy attempts to strike the delicate balance between network connectivity and throughput and the needs of security. While not as strict as Security Over Connectivity, this policy attempts to keep users secure while being less obtrusive about normal traffic.	Prevention	
2	Connectivity Over Security	Automatically-created custom policy equivalent to 'Connectivity Over Security - Cisco Talos'. This policy places an emphasis on network connectivity and throughput, at the possible expense of security. Traffic is inspected less deeply, and less rules are evaluated.	Prevention	
3	Maximum Detection	Automatically-created custom policy equivalent to 'Maximum Detection - Cisco Talos'. This policy places all emphasis on security. Network connectivity and throughput is not guaranteed and false positives are likely. This policy should only be used for high security areas and security monitors must be prepared to investigate alerts to determine their validity.	Prevention	
4	Security Over Connectivity	Automatically-created custom policy equivalent to 'Security Over Connectivity - Cisco Talos'. This policy places an emphasis on security, at the possible expense of network connectivity and throughput. Traffic is inspected more deeply, more rules are evaluated, and both false positives and increased latency are expected but within reason.	Prevention	

Creating IPSec VPN Tunnel

1. Configuring IKE and IPSec Settings
    a. Define IKE settings including pre-shared key, encryption, integrity, DH group, lifetime, and authentication method.

   b. Configure IPSec settings including encryption, integrity, lifetime, and authentication.

2. Defining Local and Remote Subnets
   a. Specify the local subnet of your FTD device and the remote subnet(s) you want to connect to.
3. Creating Access Control Rules
   a. Create access control rules that permit traffic through the VPN tunnel.
   b. Allow traffic from the local subnet to the remote subnet and vice versa.