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:

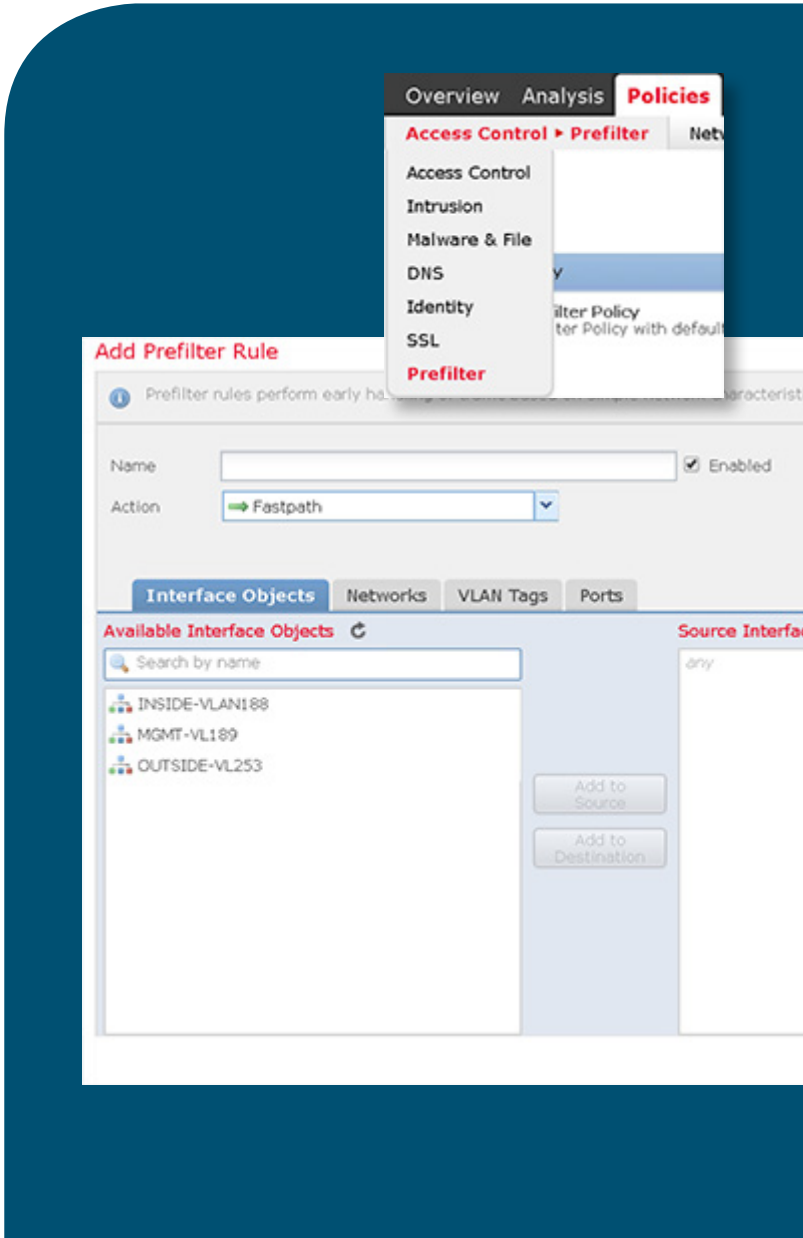
Access Policies

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

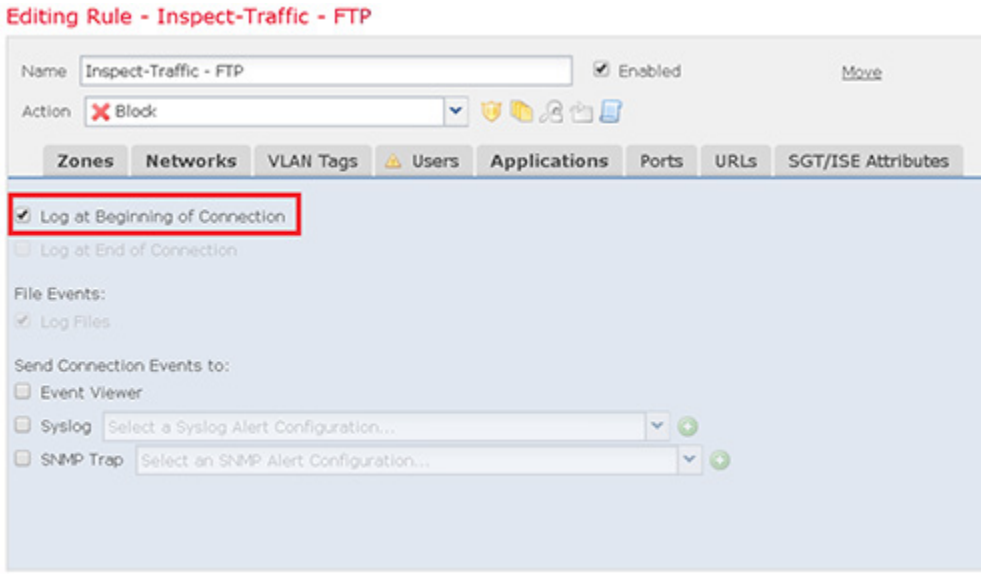
Connection Logging

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.



Access Policies

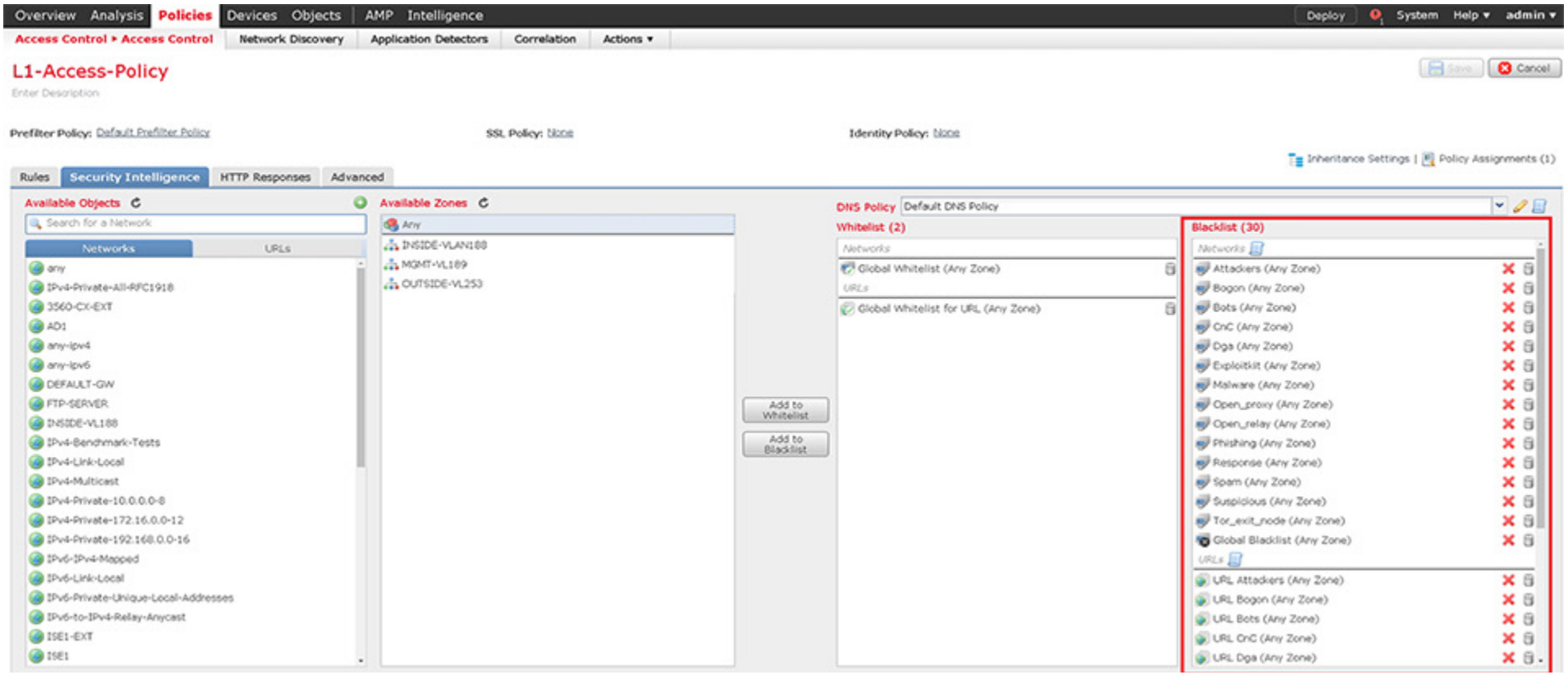
Defining Flows

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

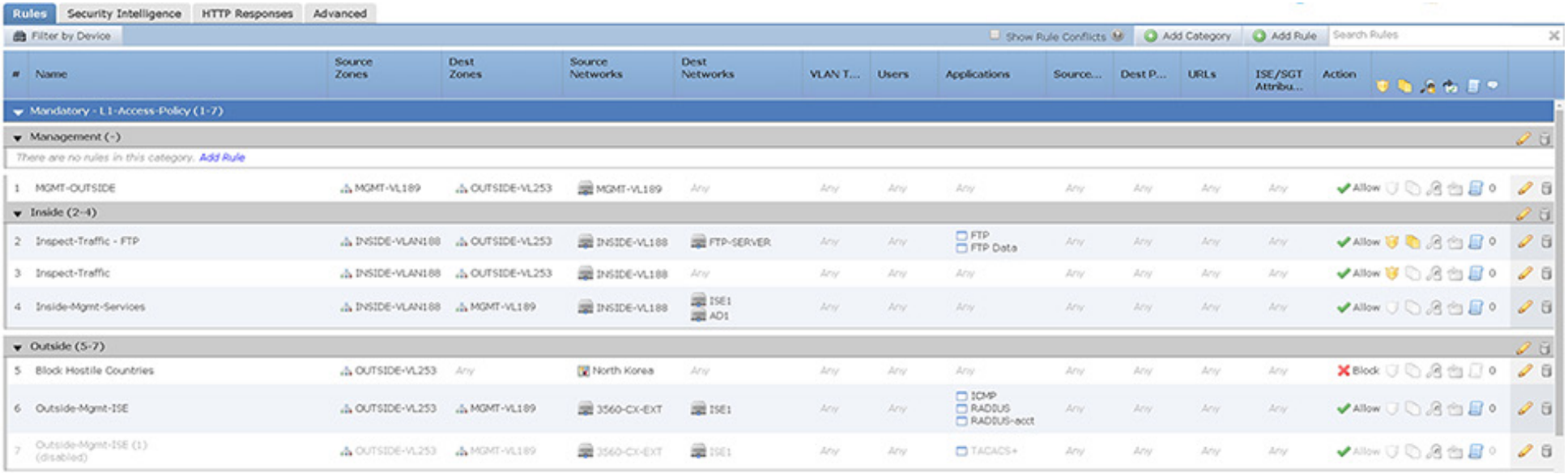
It's always a good idea to block known sources of bad traffic with Security Intelligence, and you don't need to process additional rule sets to do so. Plus, removing the bad actors from the beginning further optimizes the performance of Cisco FTD and reduces the overall risk to your organization.



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.

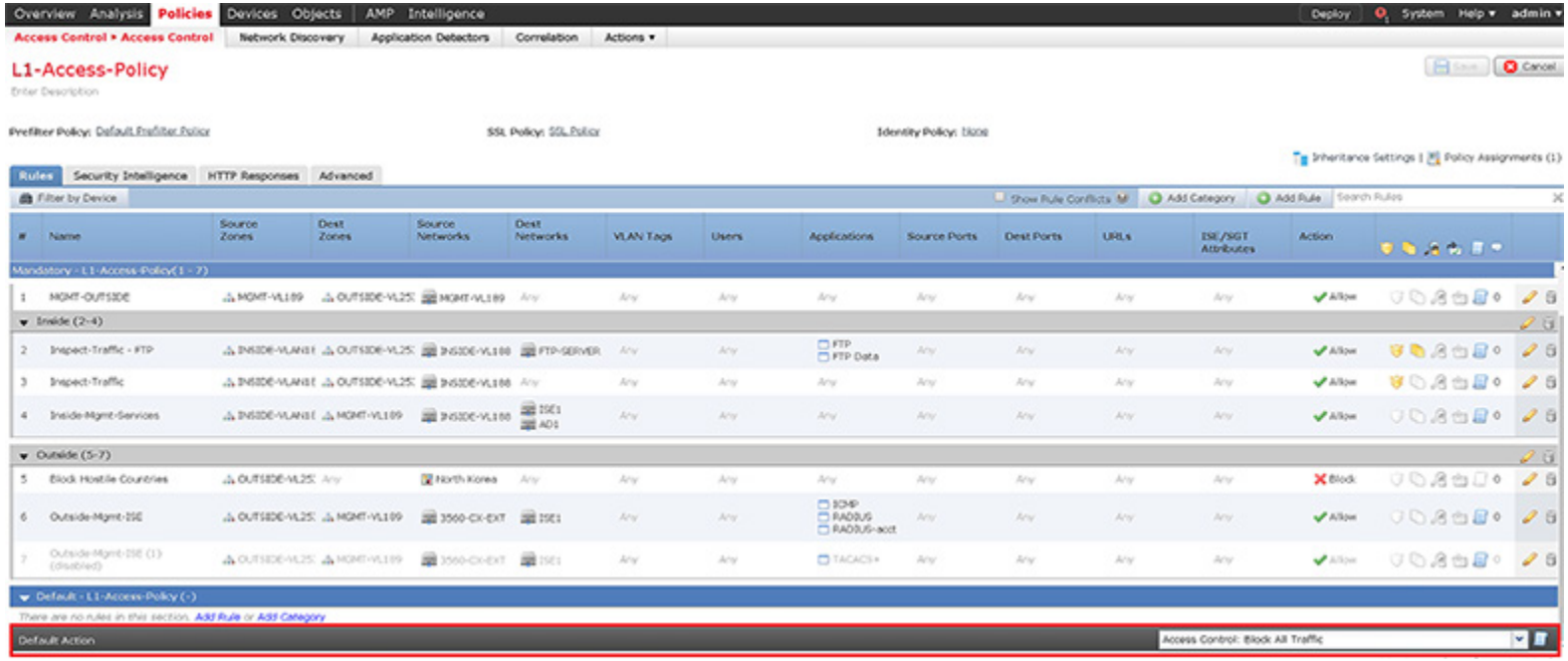


Access Policies

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.



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.

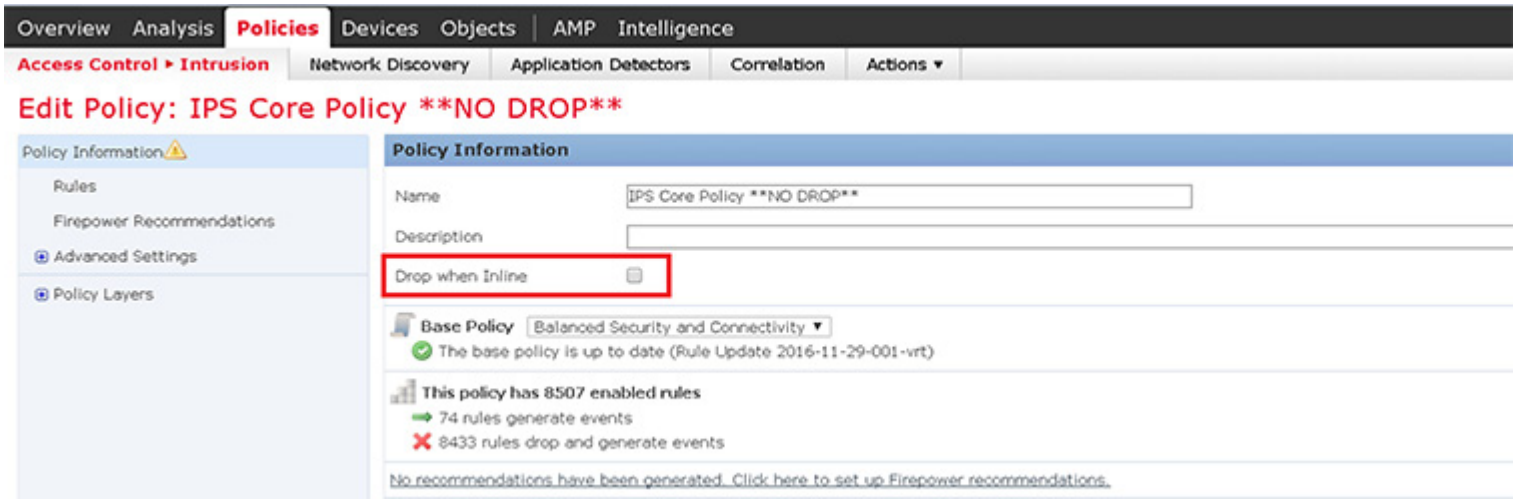
IPS Policies

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

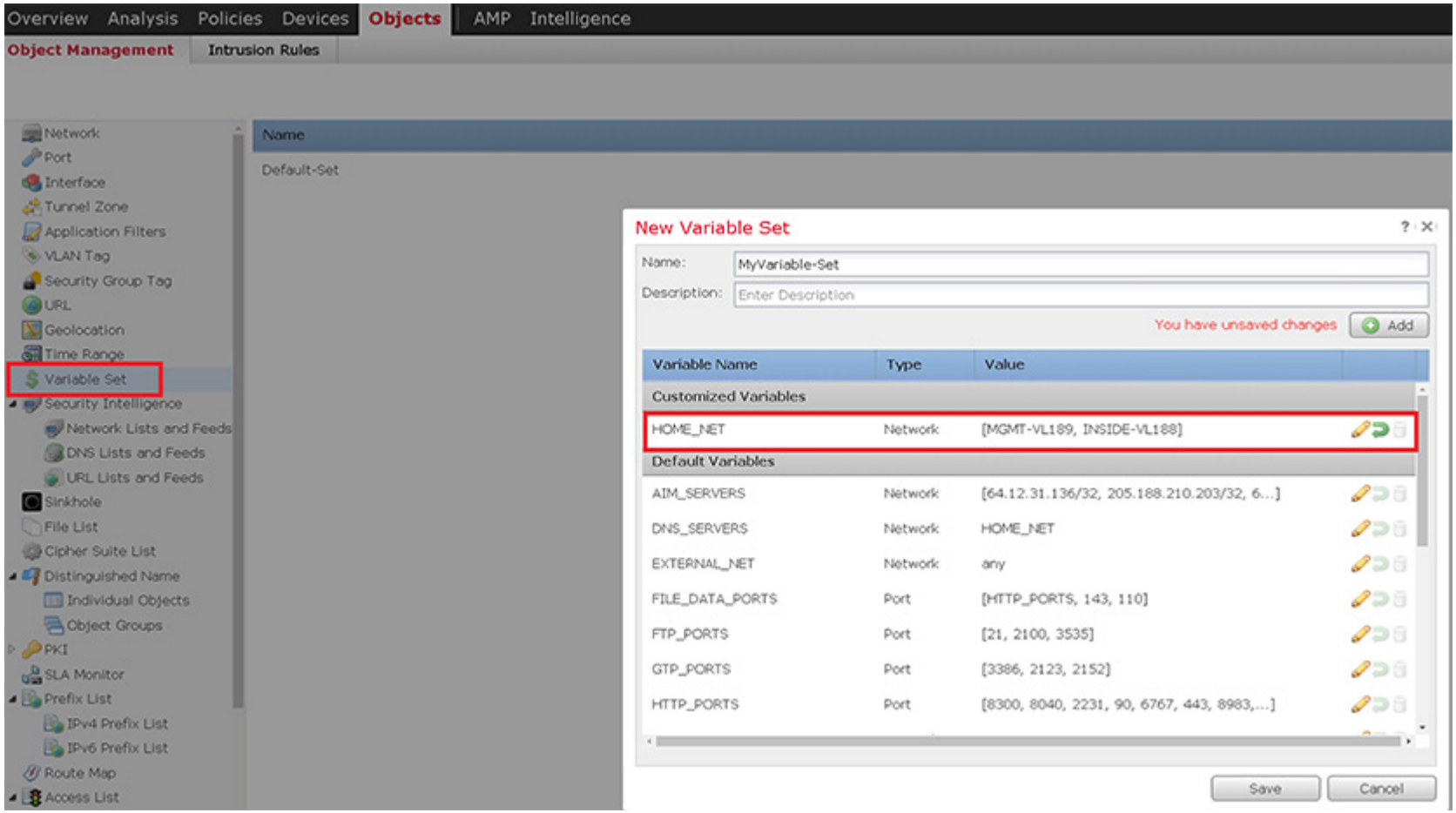
Consider testing IPS policies before deploying. This ensures that the policy is further optimized prior to moving the rule set into production. This can include passive or inline tap modes or inline mode with the “drop when inline” option unchecked.



IPS Policies

Configuring Variables Sets

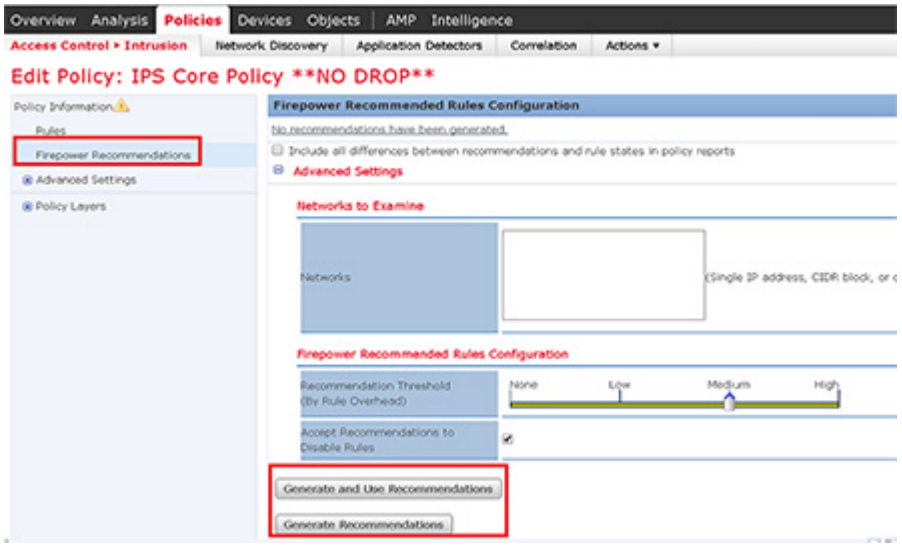
Variable sets provide deeper accuracy in terms of detection and reduce the amount of noise. It's critical that you populate the variable sets with information that reflects your environment, and you should also update your variable sets as your environment changes.



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.



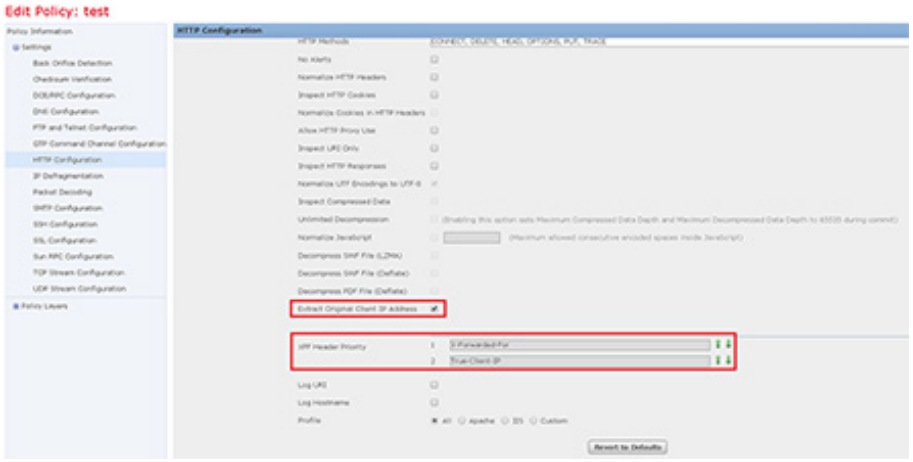
Deploying Strict Controls

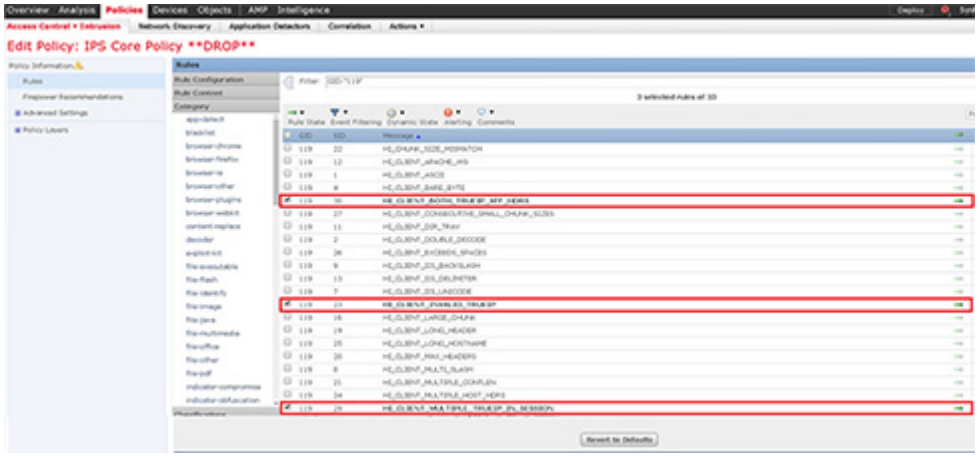
Define the critical and non-critical hosts within the environment and deploy strict controls for critical assets. This may include IPS and file/malware policies.

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

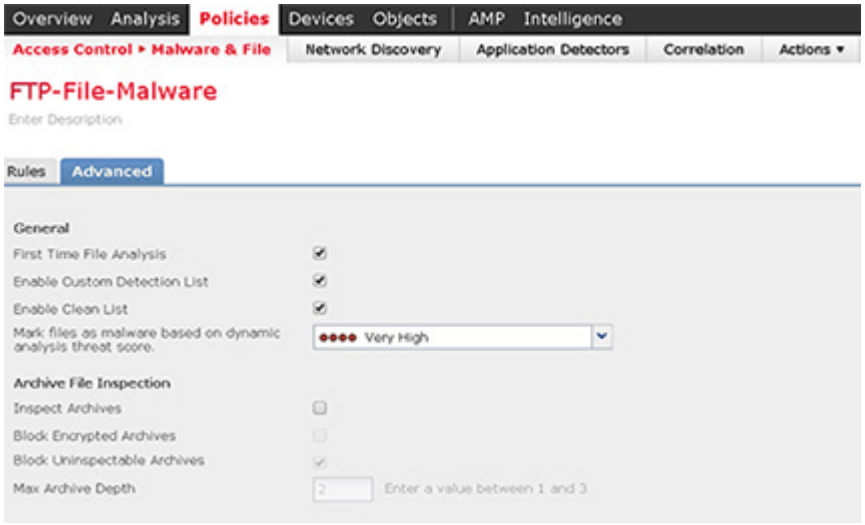
Fine-Tuning Rules

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.

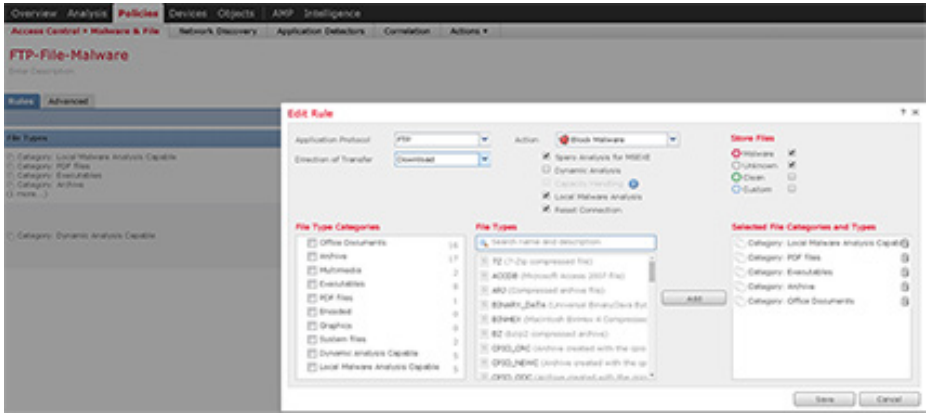
Malware Policies

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



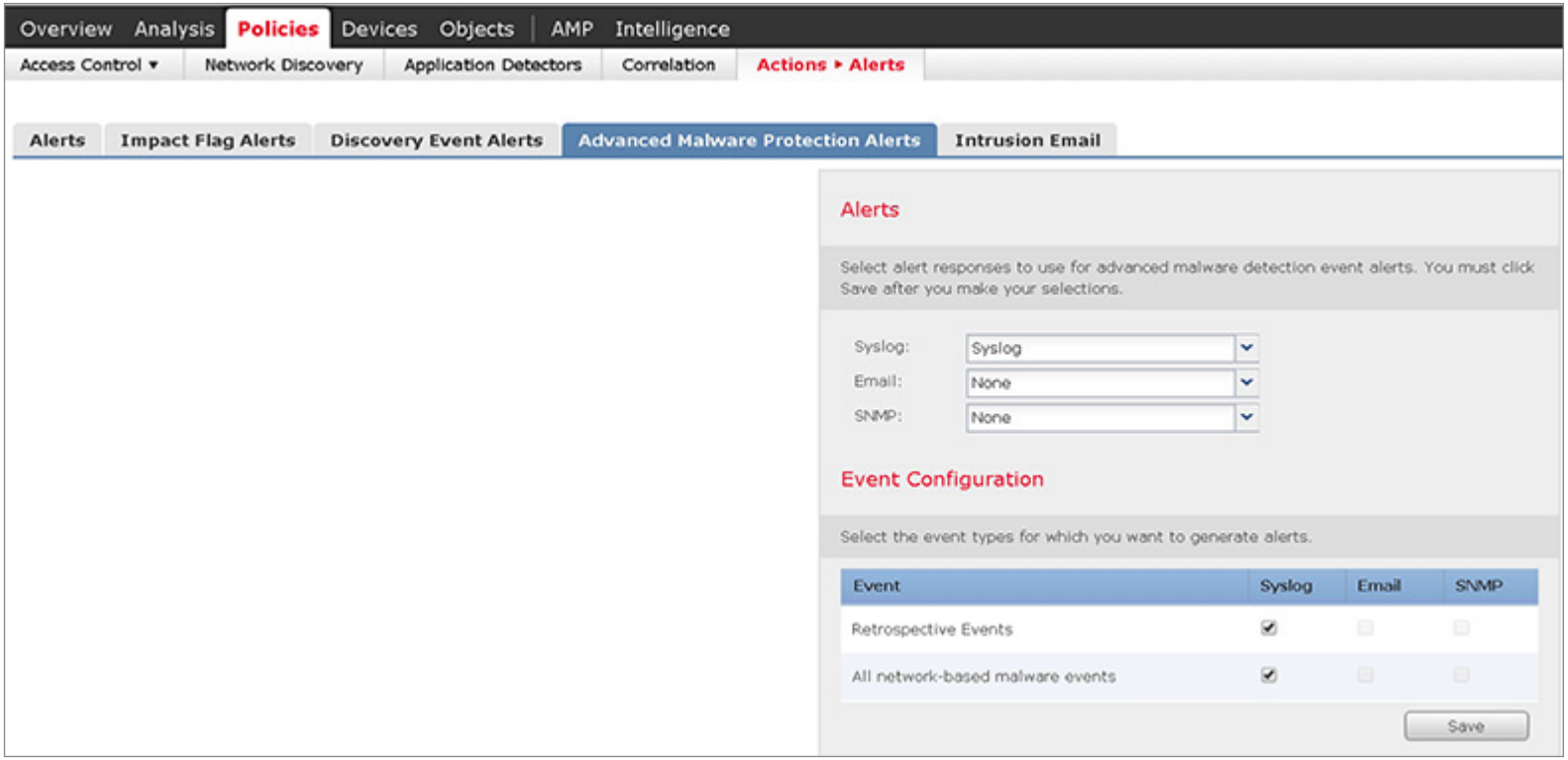
You’ll also want to define which flows require malware inspection and optimize malware policies for the specific flow required. For example, if the flow requires that you inspect FTP traffic that contains document type files, then your malware policy should reflect the proper protocol and file type. 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.

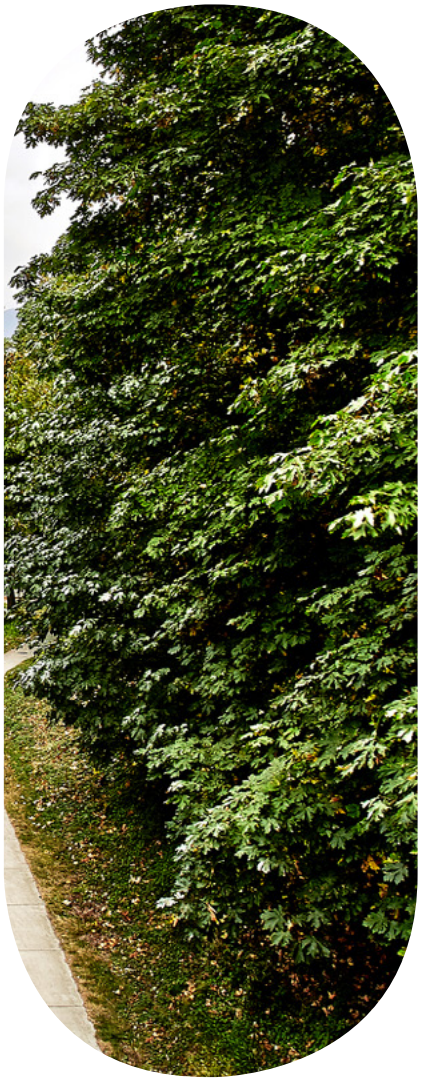


Lastly, enable the reset connection option for Block Files and/or Block Malware. This terminates the connection.

SSL Policies

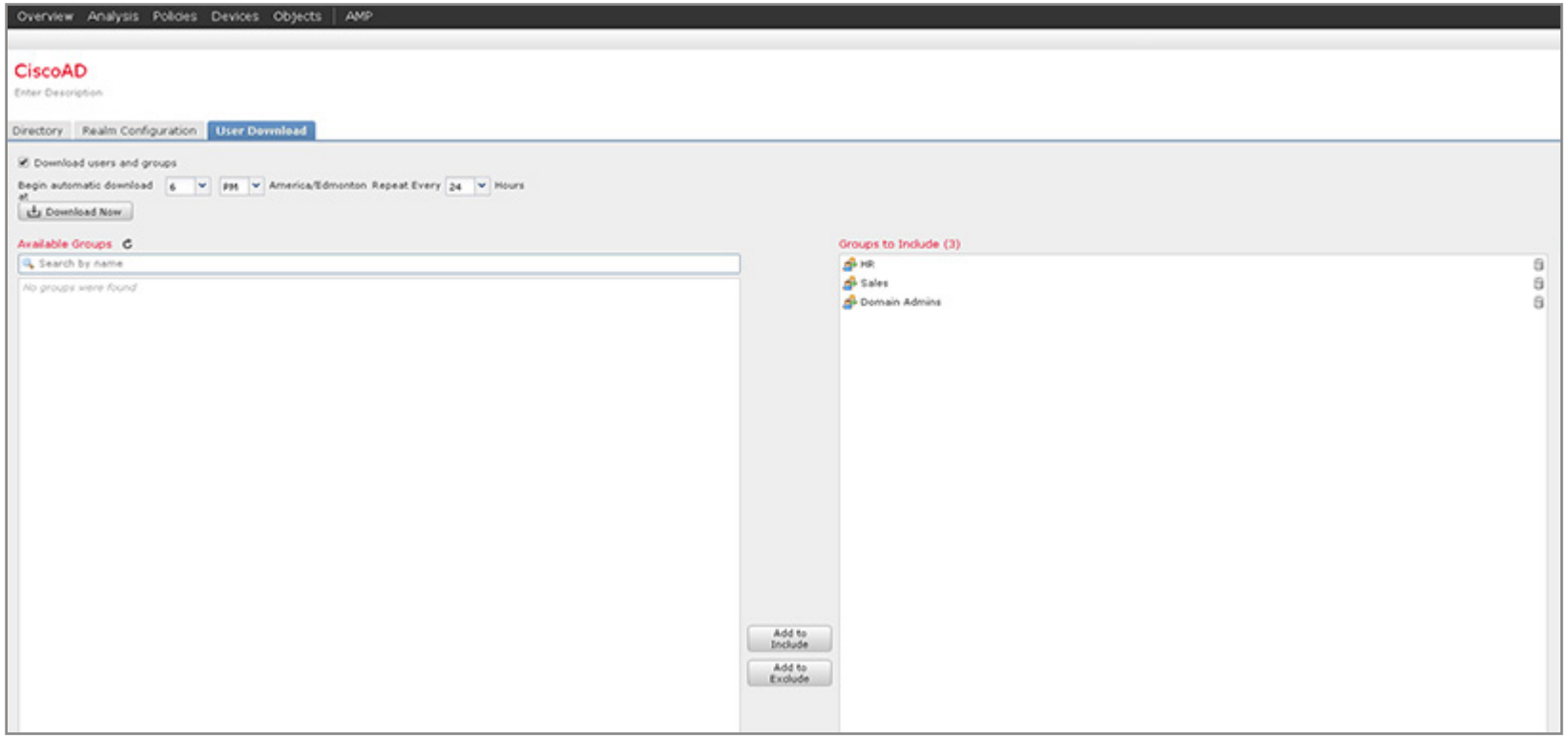
Determine which traffic flows need decryption and define an SSL decryption policy. Again when defining the flow, leverage the minimum number of attributes to uniquely classify the traffic.

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 form AD.

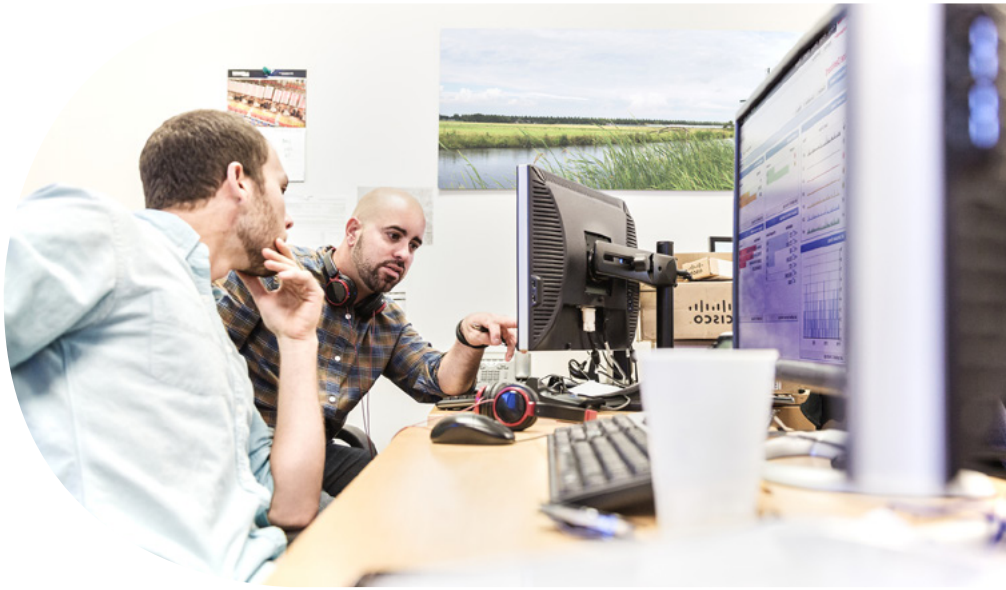


Consider leveraging Cisco ISE or Cisco ISE Passive Identity Connector with integrated user- or device-based policies. This allows synergy across multiple Cisco security platforms.

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.