Access Control Using Intrusion and File Policies

The following topics describe how to configure access control policies to use intrusion and file policies:

Intrusions and Malware Inspection Overview

Intrusion and file policies work together as the last line of defense before traffic is allowed to its destination:

- *Intrusion policies* govern the system's intrusion prevention capabilities.
- *File policies* govern the system's file control and AMP for Firepower capabilities.

All other traffic handling occurs **before** network traffic is examined for intrusions, prohibited files, and malware. This traffic handling includes hardware-based fast-pathing, Security Intelligence-based traffic filtering (blacklisting), SSL inspection-based decisions, and traffic decoding and preprocessing. Then, access control rules and the access control default action determine which traffic is inspected by intrusion and file policies.

By associating an intrusion or file policy with an access control rule, you are telling the system that before it passes traffic that matches the access control rule's conditions, you first want to inspect the traffic with an intrusion policy, a file policy, or both.

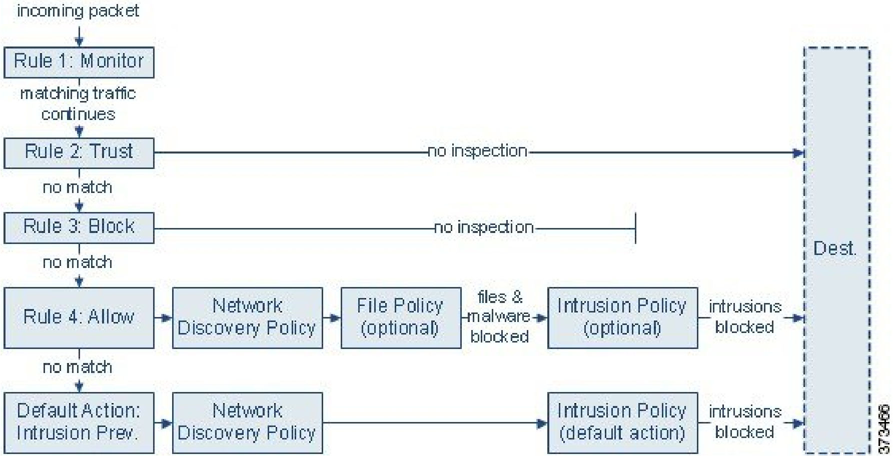
Note By default, the system disables intrusion and file inspection of encrypted payloads. This helps reduce false positives and improve performance when an encrypted connection matches an access control rule that has intrusion and file inspection configured.

The Firepower Management Center can also receive AMP for Endpoints data from the AMP cloud. The Firepower Management Center presents this data alongside any AMP for Firepower data. Importing endpoint-based malware events and indications of compromise (IOC) data does not require a license.

Access Control Traffic Handling

Access control rules provide a granular method of handling network traffic across multiple managed devices. The system matches traffic to access control rules in the order you specify. In most cases, the system handles network traffic according to the *first* access control rule where *all* the rule's conditions match the traffic. An access control rule's *action* determines how the system handles matching traffic. You can monitor, trust, block, or allow (with or without further inspection) matching traffic.

The following diagram shows the flow of traffic in an inline intrusion prevention and AMP for Firepower deployment, as governed by an access control policy that contains four different types of access control rules and a default action.



In the scenario above, the first three access control rules in the policy—Monitor, Trust, and Block—cannot inspect matching traffic. Monitor rules track and log but do not inspect network traffic, so the system continues to match traffic against additional rules to determine whether to permit or deny it. Trust and Block rules handle matching traffic without further inspection of any kind, while traffic that does not match continues to the next access control rule.

The fourth and final rule in the policy, an Allow rule, invokes various other policies to inspect and handle matching traffic, in the following order:

- **Discovery: Network Discovery Policy**—First, the network discovery policy inspects traffic for discovery data. Discovery is passive analysis and does not affect the flow of traffic. Although you do not explicitly enable discovery, you can enhance or disable it. However, allowing traffic does not automatically guarantee discovery data collection. The system performs discovery only for connections involving IP addresses that are explicitly monitored by your network discovery policy.

- **AMP for Firepower and File Control: File Policy**—After traffic is inspected by discovery, the system can inspect it for prohibited files and malware. AMP for Firepower detects and optionally blocks malware in many types of files, including PDFs, Microsoft Office documents, and others. If your organization wants to block not only the transmission of malware files, but all files of a specific type (regardless of whether the files contain malware), *file control* allows you to monitor network traffic for transmissions of specific file types, then either block or allow the file.

- **Intrusion Prevention: Intrusion Policy**—After file inspection, the system can inspect traffic for intrusions and exploits. An intrusion policy examines decoded packets for attacks based on patterns, and can block or alter malicious traffic. Intrusion policies are paired with *variable sets*, which allow you to use named values to accurately reflect your network environment.

- **Destination—**Traffic that passes all the checks described above passes to its destination.

An Interactive Block rule (not shown in the diagram) has the same inspection options as an Allow rule. This is so you can inspect traffic for malicious content when a user bypasses a blocked website by clicking through a warning page.

Traffic that does not match any of the non-Monitor access control rules in the policy is handled by the default action. In this scenario, the default action is an Intrusion Prevention action, which allows traffic to its final destination as long as it is passed by the intrusion policy you specify. In a different deployment, you might have a default action that trusts or blocks all traffic without further inspection. Note that the system can inspect traffic allowed by the default action for discovery data and intrusions, but not prohibited files or malware. You **cannot** associate a file policy with the access control default action.

Note Sometimes, when a connection is analyzed by an access control policy, the system must process the first few packets in that connection, **allowing them to pass**, before it can decide which access control rule (if any) will handle the traffic. However, so these packets do not reach their destination uninspected, you can use an intrusion policy—called the default intrusion policy—to inspect them and generate intrusion events.

File and Intrusion Inspection Order

In your access control policy, you can associate multiple Allow and Interactive Block rules with different intrusion and file policies to match inspection profiles to various types of traffic.

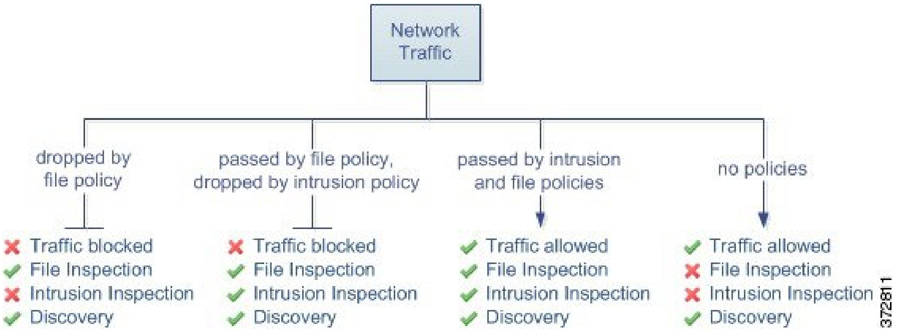
Note Traffic allowed by an Intrusion Prevention or Network Discovery Only default action can be inspected for discovery data and intrusions, but cannot be inspected for prohibited files or malware. You **cannot** associate a file policy with the access control default action.

You do not have to perform both file and intrusion inspection in the same rule. For a connection matching an Allow or Interactive Block rule:

- without a file policy, traffic flow is determined by the intrusion policy
- without an intrusion policy, traffic flow is determined by the file policy
- without either, allowed traffic is inspected by network discovery only

Tip The system does not perform any kind of inspection on trusted traffic. Although configuring an Allow rule with neither an intrusion nor file policy passes traffic like a Trust rule, Allow rules let you perform discovery on matching traffic.

The diagram below illustrates the types of inspection you can perform on traffic that meets the conditions of either an Allow or user-bypassed Interactive Block access control rule. For simplicity, the diagram displays traffic flow for situations where both (or neither) an intrusion and a file policy are associated with a single access control rule.



For any single connection handled by an access control rule, file inspection occurs before intrusion inspection. That is, the system does not inspect files blocked by a file policy for intrusions. Within file inspection, simple blocking by type takes precedence over malware inspection and blocking.

For example, consider a scenario where you normally want to allow certain network traffic as defined in an access control rule. However, as a precaution, you want to block the download of executable files, examine downloaded PDFs for malware and block any instances you find, and perform intrusion inspection on the traffic.

You create an access control policy with a rule that matches the characteristics of the traffic you want to provisionally allow, and associate it with both an intrusion policy and a file policy. The file policy blocks the download of all executables, and also inspects and blocks PDFs containing malware:

- First, the system blocks the download of all executables, based on simple type matching specified in the file policy. Because they are immediately blocked, these files are subject to neither malware nor intrusion inspection.
- Next, the system performs malware cloud lookups for PDFs downloaded to a host on your network. Any PDFs with a malware disposition are blocked, and are not subject to intrusion inspection.
- Finally, the system uses the intrusion policy associated with the access control rule to inspect any remaining traffic, including files not blocked by the file policy.

Note Until a file is detected and blocked in a session, packets from the session may be subject to intrusion inspection.

Access Control Rule Configuration to Perform File Control and Malware Protection

An access control policy can have multiple access control rules associated with file policies. You can configure file inspection for any Allow or Interactive Block access control rule, which permits you to match different file and malware inspection profiles against different types of traffic on your network before it reaches its final destination.

When the system detects a prohibited file (including malware) according to the settings in the file policy, it automatically logs an event to the Firepower Management Center database. If you do not want to log file or malware events, you can disable this logging on a per-access-control-rule basis.

The system also logs the end of the associated connection to the Firepower Management Center database, regardless of the logging configuration of the invoking access control rule.

Configuring an Access Control Rule to Perform File Control and Malware Protection

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat (file control) Malware (AMP)	Protection (file control) Malware (AMP)	Any	Any	Admin/Access Admin/Network Admin

Caution Associating a file policy with an access control rule, or subsequently dissociating the policy by selecting **None**, restarts the Snort process and interrupts traffic when you deploy configuration changes. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic.

Procedure

Step 1 In the access control policy editor, create a new rule or edit an existing rule; see Access Control Rule Components.

Step 2 Ensure the rule action is set to **Allow**, **Interactive Block**, or **Interactive Block with reset**.

Step 3 Click the **Inspection** tab.

Step 4 Choose a **Malware Policy** to inspect traffic that matches the access control rule, or choose **None** to disable file inspection for matching traffic.

Step 5 Optionally, but not recommended, disable logging of file or malware events for connections matching the rule. Click the **Logging** tab and uncheck the **Log Files** check box, as described in File and Malware Event Logging for Allowed Connections.

Step 6 Click **Save** to save the rule.

Step 7 Click **Save** to save the policy.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes.

Access Control Rule Configuration to Perform Intrusion Prevention

An access control policy can have multiple access control rules associated with intrusion policies. You can configure intrusion inspection for any Allow or Interactive Block access control rule, which permits you to match different intrusion inspection profiles against different types of traffic on your network before it reaches its final destination.

Whenever the system uses an intrusion policy to evaluate traffic, it uses an associated *variable set*. Variables in a set represent values commonly used in intrusion rules to identify source and destination IP addresses and ports. You can also use variables in intrusion policies to represent IP addresses in rule suppressions and dynamic rule states.

Tip Even if you use system-provided intrusion policies, Cisco **strongly** recommends you configure the system's intrusion variables to accurately reflect your network environment. At a minimum, modify default variables in the default set.

Understanding System-Provided and Custom Intrusion Policies

Cisco delivers several intrusion policies with the Firepower System. By using system-provided intrusion policies, you can take advantage of the experience of theCisco Talos Security Intelligence and Research Group (Talos). For these policies, Talos sets intrusion and preprocessor rule states, as well as provides the initial configurations for advanced settings. You can use system-provided policies as-is, or you can use them as the base for custom policies. Building custom policies can improve the performance of the system in your environment and provide a focused view of the malicious traffic and policy violations occurring on your network.

Connection and Intrusion Event Logging

When an intrusion policy invoked by an access control rule detects an intrusion and generates an intrusion event, it saves that event to the Firepower Management Center. The system also automatically logs the end of the connection where the intrusion occurred to the Firepower Management Center database, regardless of the logging configuration of the access control rule.

Access Control Rule Configuration and Intrusion Policies

In addition to custom intrusion policies that you create, the system provides two custom policies: Initial Inline Policy and Initial Passive Policy. These two intrusion policies use the Balanced Security and Connectivity intrusion policy as their base. The only difference between them is their **Drop When Inline** setting, which enables drop behavior in the inline policy and disables it in the passive policy.

The number of unique intrusion policies you can use in a single access control policy depends on the model of the target devices; more powerful devices can handle more. Every unique **pair** of intrusion policy and variable set counts as one policy. Although you can associate a different intrusion policy-variable set pair with each Allow and Interactive Block rule (as well as with the default action), you cannot deploy an access control policy if the target devices have insufficient resources to perform inspection as configured.

Configuring an Access Control Rule to Perform Intrusion Prevention

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin

⚠ **Caution** Associating an intrusion policy with an access control rule, or subsequently dissociating the policy by selecting **None**, restarts the Snort process and interrupts traffic when you deploy configuration changes. Whether this interruption drops traffic or passes traffic without inspection depends on the model of the managed device and how it handles traffic.

Procedure

Step 1 In the access control policy editor, create a new rule or edit an existing rule; see Access Control Rule Components.

Step 2 Ensure the rule action is set to **Allow**, **Interactive Block**, or **Interactive Block with reset**.

Step 3 Click the **Inspection** tab.

Step 4 Choose a system-provided or custom **Intrusion Policy**, or choose **None** to disable intrusion inspection for traffic that matches the access control rule.

Caution Do **not** use the `Maximum Detection` policy unless instructed to by Support. Cisco uses this policy for testing.

Step 5 If you want to change the variable set associated with the intrusion policy, choose a value from the **Variable Set** drop-down list.

Step 6 Click **Save** to save the rule.

Step 7 Click **Save** to save the policy.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes.