Blocking Traffic with Security Intelligence

The following topics provide an overview of Security Intelligence, including use of lists for blocking and allowing traffic and basic configuration.

- About Security Intelligence, on page 1
- Best Practices for Security Intelligence, on page 2
- License Requirements for Security Intelligence, on page 2
- Requirements and Prerequisites for Security Intelligence, on page 3
- Security Intelligence Sources, on page 3
- Configure Security Intelligence, on page 4
- Security Intelligence Monitoring, on page 10
- Override Security Intelligence Blocking, on page 11
- Troubleshooting Security Intelligence, on page 12
- History for Security Intelligence Block Listing, on page 13

About Security Intelligence

As an early line of defense against malicious internet content, Security Intelligence uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domain names. This is called *Security Intelligence block listing*.

Security Intelligence is an early phase of access control, before the system performs more resource-intensive evaluation. Using a Block list improves performance by quickly excluding traffic that does not require inspection.

Note You cannot use a Block list to block fastpathed traffic. 8000 Series fastpathing and prefilter evaluation occur before Security Intelligence filtering. Fastpathed traffic bypasses all further evaluation, including Security Intelligence.

Although you can configure custom Block lists, Cisco provides access to regularly updated intelligence feeds. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations.

You can refine Security Intelligence Block listing with Do Not Block lists and monitor-only Block lists. These mechanisms exempt traffic from being blocked by a Block list, but do **not** automatically trust or fastpath

matching traffic. Traffic added to a Do Not Block list or monitored at the Security Intelligence stage is intentionally subject to further analysis with the rest of access control.

Related Topics

Security Intelligence Lists and Feeds
Other Connections You Can Log
Using Connection and Security Intelligence Event Tables

Best Practices for Security Intelligence

- Configure your access control policies to block threats detected by Cisco-provided Security Intelligence feeds. See Configuration Example: Security Intelligence Blocking, on page 9.
- If you want to supplement the Cisco-provided Security Intelligence feeds with custom threat data, or manually block emerging threats:
  - For IP addresses, use custom Security Intelligence lists and feeds, or Network objects or groups. To create these, see Security Intelligence Lists and Feeds and Network Objects, and their subtopics. To use them for Security Intelligence, see Configure Security Intelligence, on page 4.
  - For URLs and domains, use custom Security Intelligence lists and feeds, *not* objects or groups. See details at Manual URL Filtering Options.
  - You can also add entries to a Block list from events. See Global and Domain Security Intelligence Lists.
- To test new feeds, or for passive deployments, set the action from block to monitor only. See Security Intelligence Monitoring, on page 10.
- If you need to exclude specific sites or addresses from Security Intelligence blocking, see Override Security Intelligence Blocking, on page 11.
- System-provided Security Intelligence categories may change over time and without notification; you should plan to check periodically for changes, and modify your policies accordingly.
- You should also configure URL filtering, a separate feature with separate licensing requirements, for further protection against malicious sites. See URL Filtering.

License Requirements for Security Intelligence

FTD License

Threat

Classic License

Protection

Requirements and Prerequisites for Security Intelligence

Model Support

Any

Supported Domains

Any

User Roles

- Admin
- Access Admin
- Network Admin

Security Intelligence Sources

- System-provided feeds

  Cisco provides access to regularly updated intelligence feeds for domains, URLs and IP addresses. For more information, see Security Intelligence Lists and Feeds.

  If you see a feed with "TID" in the name, this feed is *not* used by Security Intelligence. Instead, this feed is used by the feature described in Threat Intelligence Director.

- Third-party feeds

  Optionally, supplement Cisco-provided feeds with third-party reputation feeds, which are dynamic lists that the Firepower Management Center downloads from the internet on a regular basis. See Custom Security Intelligence Feeds.

- Custom Block lists or feeds (or objects or groups)

  Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects or groups.)

  For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy, as described in Custom Security Intelligence Lists and Configure Security Intelligence, on page 4.

  For IP addresses, you can optionally use network objects rather than lists or feeds for this purpose; for information, see Network Objects. (For URLs, using lists and feeds is strongly recommended over other methods.)

- Custom Do Not Block lists or feeds

  Override Security Intelligence blocking for specific sites or addresses. See Override Security Intelligence Blocking, on page 11.

- Global Block lists (one each for Network, URL and DNS)

While reviewing events, you can immediately add an event's IP address, URL, or domain to the applicable Global Block List so that Security Intelligence will handle future traffic from that source. See Global and Domain Security Intelligence Lists.

- Global Do Not Block lists (one each for Network, URL and DNS)

  While reviewing events, you can immediately add an event's IP address, URL, or domain to the applicable Global Do Not Block List if you do not want Security Intelligence to block future traffic from that source. See Global and Domain Security Intelligence Lists.

Configure Security Intelligence

Each access control policy has Security Intelligence options. You can add network objects, URL objects and lists, and Security Intelligence feeds and lists to a Block list or Do Not Block list, and constrain any of these by security zone. You can also associate a DNS policy with your access control policy, and add domain names to a Block or Do Not Block list.

The number of objects in the Do Not Block lists plus the number in the Block lists cannot exceed 125 network objects, or 32767 URL objects and lists.

Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

Caution From Security Intelligence in an access control policy, adding multiple objects to a Block or Do Not Block list, or deleting multiple objects, sometimes 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 how the target device handles traffic. See Snort® Restart Traffic Behavior for more information. Note that whether the Snort process restarts can vary by device, depending on the memory available for inspection.

Before you begin

- Tip: For guidance on minimum configuration recommendations, see also Configuration Example: Security Intelligence Blocking, on page 9.
- To ensure that all options are available to select, add at least one managed device to your management center.
- In passive deployments, or if you want to set Security Intelligence filtering to monitor-only, enable logging; see Logging Connections with Security Intelligence.
- Configure a DNS policy to take Security Intelligence action for domains. For more information, see DNS Policies.

Procedure

Step 1 In the access control policy editor, click **Security Intelligence**.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 2 You have the following options:

- Click **Networks** to add network objects (IP addresses).
- Click **URLs** to add URL objects.

Step 3 Find the **Available Objects** you want to add to the Block or Do Not Block list. You have the following options:

- Search the available objects by typing in the **Search by name or value** field. Clear the search string by clicking **Reload** ( ) or **Clear** ( ).
- If no existing list or feed meets your needs, click **Add** ( ), select **New Network List** or **New URL List**, and proceed as described in Creating Security Intelligence Feeds or Uploading New Security Intelligence Lists to the Firepower Management Center.
- If no existing object meets your needs, click **Add** ( ), select **New Network Object** or **New URL Object**, and proceed as described in Creating Network Objects.

Security Intelligence ignores IP address blocks using a `/0` netmask.

Step 4 Choose one or more **Available Objects** to add.

Step 5 (Optional) Choose an **Available Zone** to constrain the selected objects by zone.

You cannot constrain system-provided Security Intelligence lists by zone.

Step 6 Click **Add to Do Not Block list** or **Add to Block list**, or click and drag the selected objects to either list.

To remove an object from a Block or Do Not Block list, click **Delete** ( ) To remove multiple objects, choose the objects and right-click to **Delete Selected**.

Step 7 (Optional) Set objects on the Block list to monitor-only by right-clicking the object under **Block List**, then choosing **Monitor-only (do not block)**.

You cannot set system-provided global Security Intelligence lists to monitor only.

Step 8 Choose a DNS policy from the **DNS Policy** drop-down list.

Step 9 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Related Topics

Security Intelligence Lists and Feeds
Snort® Restart Scenarios

Security Intelligence Options

Use the Security Intelligence tab in the access control policy editor to configure network (IP address) and URL Security Intelligence, and to associate the access control policy with a DNS policy in which you have configured Security Intelligence for domains.

Available Objects

Available objects include:

- Security Intelligence categories populated by the system-provided feed.

  For details, see Security Intelligence Categories, on page 7.

- System-provided Global Block and Do Not Block lists.

  For descriptions, see Security Intelligence Sources, on page 3.

- Security Intelligence lists and feeds that you create under Object > Object Management > Security Intelligence.

  For descriptions, see Security Intelligence Sources, on page 3.

- Network and URL objects and groups that are configured on the respective pages under Object > Object Management. These are different from the Security Intelligence objects in the previous bullet.

  For details about network objects, see Network Objects. (For URLs, use Security Intelligence lists or feeds rather than objects or groups.)

Available Zones

Except for the system-provided Global lists, you can constrain Security Intelligence filtering by zone.

For example: To improve performance, you may want to target enforcement. As a more specific example, you can block spam only for a security zone that handles email traffic.

To enforce Security Intelligence filtering for an object on multiple zones, you must add the object to the Block or Do Not Block list separately for each zone.

DNS Policy

In order to match DNS traffic using Security Intelligence, you must select a DNS policy for your Security Intelligence configuration.

Using Block or Do Not Block lists, or monitoring traffic based on a DNS list or feed, also requires that you:

- Configure DNS Security Intelligence lists and feeds. See Security Intelligence Lists and Feeds.
- Create a DNS policy. See Creating Basic DNS Policies for more information.
- Configure DNS rules that reference your DNS lists or feeds. See Creating and Editing DNS Rules for more information.
- Because you deploy the DNS policy as part of your access control policy, you must associate both policies. See DNS Policy Deploy for more information.

Do Not Block List

See Override Security Intelligence Blocking, on page 11.

To select all objects in the list, right-click an object.

Block List

See Configuration Example: Security Intelligence Blocking, on page 9 and other topics in this chapter.

For explanations of the visual indicators in the Block list, see Block List Icons, on page 9.

To select all objects in the list, right-click an object.

Logging

Security Intelligence logging, enabled by default, logs all blocked and monitored connections handled by an access control policy's target devices. However, the system does not log Do Not Block list matches; logging of connections on the Do Not Block list depends on their eventual disposition. Logging must be enabled for connections on the Block list before you can set objects on that list to monitor-only.

To enable, disable, or view logging settings, right-click an object in the Block list.

Related Topics

Global and Domain Security Intelligence Lists
Security Intelligence Lists and Multitenancy

Security Intelligence Categories

Security Intelligence categories are determined by the system-provided feeds described in Security Intelligence Lists and Feeds.

These categories are used in the following locations:

- The Networks sub-tab on the Security Intelligence tab of an access control policy
- The URLs sub-tab beside the Networks tab on the Security Intelligence tab of an access control policy
- In a DNS policy on the DNS tab in the DNS rule configuration page
- In events generated when traffic matches Block or Monitor configurations in the above locations

Note If your organization is using Threat Intelligence Director: When viewing events, you may see categories that indicate that the action was taken by TID, such as `TID URL Block`.

Categories are updated by Talos from the cloud, and this list may change independently of Firepower releases.

Table 1: Cisco Talos Intelligence Group (Talos) Feed Categories

Security Intelligence Category	Description
Attackers	Active scanners and hosts known for outbound malicious activity

Security Intelligence Category	Description
Banking_fraud	Sites that engage in fraudulent activities that relate to electronic banking
Bogon	Bogon networks and unallocated IP addresses
Bots	Sites that host binary malware droppers
CnC	Sites that host command-and-control servers for botnets
Cryptomining	Hosts providing remote access to pools and wallets for the purpose of mining cryptocurrency
Dga	Malware algorithms used to generate a large number of domain names acting as rendezvous points with their command-and-control servers
Exploitkit	Software kits designed to identify software vulnerabilities in clients
High_risk	Domains and hostnames that match against the OpenDNS predictive security algorithms from security graph
Ioc	Hosts that have been observed to engage in Indicators of Compromise (IOC)
Link_sharing	Websites that share copyrighted files without permission
Malicious	Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category
Malware	Sites that host malware binaries or exploit kits
Newly_seen	Domains that have recently been registered, or not yet seen via telemetry. **Attention** Currently, this category does not have any active feed and is reserved for future use.
Open_proxy	Open proxies that allow anonymous web browsing
Open_relay	Open mail relays that are known to be used for spam
Phishing	Sites that host phishing pages
Response	IP addresses and URLs that are actively participating in malicious or suspicious activity
Spam	Mail hosts that are known for sending spam
Spyware	Sites that are known to contain, serve, or support spyware and adware activities
Suspicious	Files that appear to be suspicious and have characteristics that resemble known malware
Tor_exit_node	Hosts known to offer exit node services for the Tor Anonymizer network

Block List Icons

The following visual indicators may appear in the Block list on the Security Intelligence tab in an access control policy:

Icon or Visual Indicator	Description
Block ( )	The object is set to block.
Monitor ( )	The object is set to monitor-only. See Security Intelligence Monitoring, on page 10
An object is displayed in strikethrough text	The same object is also on the Do Not Block list, which overrides the block.

Configuration Example: Security Intelligence Blocking

Configure your access control policy to block all threats detectable by the system's regularly updated Security Intelligence feeds.

The number of objects in the Block lists plus the number in the Do Not Block lists cannot exceed 125 network objects, or 32767 URL objects and lists.

Note The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

Caution From Security Intelligence in an access control policy, adding multiple objects to a Do Not Block list or Block list, or deleting multiple objects, sometimes 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 how the target device handles traffic. See Snort® Restart Traffic Behavior for more information. Note that whether the Snort process restarts can vary by device, depending on the memory available for inspection.

Before you begin

- To ensure that all options are available to select, add at least one managed device to your management center.
- Configure a DNS policy to block all Security Intelligence threat categories for domains. For more information, see DNS Policies.
- If you have, or will have, custom lists of entities to block, create a Security Intelligence object of each type (URLs, DNS, Networks.) See Security Intelligence Lists and Feeds.

Procedure

Step 1 Click **Policies** > **Access Control**.

Step 2 Create a new access control policy or edit an existing policy.

Step 3 In the access control policy editor, click **Security Intelligence**.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

Step 4 Click **Networks** to add blocking criteria for IP addresses.

a) Scroll down in the Networks list and select all of the threat categories listed below the Global lists.
b) If applicable, select the security zones for which you want to block these threats.
c) Click **Add to Block List**.
d) If you have created custom lists or feeds with addresses to block, add those to the Block List using the same steps as above.

Step 5 Click **URLs** to add blocking criteria for URLs, and repeat the steps you followed for Networks.

Step 6 Choose a DNS policy from the **DNS Policy** drop-down list; see DNS Policy Overview.

Step 7 Click **Save**.

What to do next

- Enable logging for these connections; see Logging Connections with Security Intelligence.
- Deploy configuration changes; see Deploy Configuration Changes.
- For additional protection, configure URL filtering to block malicious URLs. See URL Filtering.

Security Intelligence Monitoring

Monitoring logs connection events for traffic that would have been blocked by Security Intelligence, but does not block the traffic. Monitoring is especially useful for:

- Testing feeds before you implement them.

  Consider a scenario where you want to test a third-party feed before you implement blocking using that feed. When you set the feed to monitor-only, the system allows connections that would have been blocked to be further analyzed by the system, but also logs a record of each of those connections for your evaluation.

- Passive deployments, to optimize performance.

  Managed devices that are deployed passively cannot affect traffic flow; there is no advantage to configuring the system to block traffic. Additionally, because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection.

Note If configured, Threat Intelligence Director may impact the action taken (Monitor or Block.) For more information, see TID-Firepower Management Center Action Prioritization.

To Configure Security Intelligence Monitoring:

After you configure Security Intelligence blocking following the instructions in Configuration Example: Security Intelligence Blocking, on page 9, right-click each applicable object in the Block list and choose **Monitor-only**. You cannot set system-provided Security Intelligence lists to monitor only.

Override Security Intelligence Blocking

Optionally, you can use Do Not Block lists to exempt specific domains, URLs, or IP addresses from being blocked by Security Intelligence lists or feeds.

For example, you can:

- Override the occasional false-positive block in a reputable Security Intelligence feed
- Inspect specific traffic in depth instead of blocking it early based on reputation
- Exempt otherwise-restricted transactions based on zone from Security Intelligence blocking

  For example, you can add an improperly classified URL to a Do Not Block list, but then restrict the Do Not Block list object using a security zone used by those in your organization who need to access those URLs. That way, only those with a business need can access the URLs on the Do Not Block list.

Note Entries on a Do Not Block list are *not* automatically trusted or fastpathed; this traffic is intentionally subject to further analysis with the rest of access control.

Procedure

Step 1 Option 1: Add an IP address, URL, or domain from an event to the Global Do Not Block List. See Global and Domain Security Intelligence Lists.

Step 2 Option 2: Use a custom Security Intelligence list or feed.

a) Create the custom Security Intelligence list or feed. See Custom Security Intelligence Lists or Creating Security Intelligence Feeds.
b) For IP addresses (Networks) and URLs: Edit your access control policy, click the Security Intelligence tab, then click the custom list or feed in the Networks or URLs sub-tab, then click **Add to Do Not Block List**.
c) Save your changes.
d) For domains (DNS): See the "DNS Policy" section in the Security Intelligence Options, on page 6 topic.
e) Deploy your changes.

Troubleshooting Security Intelligence

Security Intelligence Categories Are Missing from the Available Options List

Symptoms: On the Security Intelligence tab of the access control policy, Security Intelligence categories (such as CnC or Exploitkit) are not displayed in the Networks tab under Available Options.

Cause:

- These categories do not appear until you have added at least one managed device to your management center. You must add a device in order to pull all TALOS feeds.
- The URL filtering feature uses a different set of categories than the Security Intelligence feature; the category that you expect to see may be a URL filtering category. To see URL filtering categories, look at the **URLs** tab in an access control rule.

Troubleshooting Memory Use

Symptoms: Connections that should be blocked by a Security Intelligence Block list are instead evaluated by access control rules. The Security Intelligence health module alerts that it is out of memory.

Cause: Memory limitations. Cisco Intelligence Feeds are based on the latest threat intelligence from Cisco Talos Intelligence Group (Talos). These feeds tend to get larger as time passes. When a Firepower device receives a feed update, it loads as many entries as it can into the memory it has allocated for Security Intelligence. When a device cannot load all the entries, it may not block traffic as expected. Some connections that should be blocked by a Block list instead continue to be evaluated by access control rules.

Affected platforms: Lower-memory devices are most likely to have this issue, especially if your Block list includes a lot of Security Intelligence categories or you also filter URLs based on category and reputation. These devices include Firepower 7010, 7020, and 7030; ASA 5506-X, 5508-X, 5516-X, 5512-X , 5515-X, and 5525-X; NGIPSv.

Workaround: If you think this is happening, redeploy configurations to the affected devices. This can allocate more memory to Security Intelligence. If the issue persists, contact Cisco Technical Assistance Center (TAC), who can help you verify the issue and propose a solution appropriate to your deployment.

History for Security Intelligence Block Listing

Feature	Version	Details
New Security Intelligence categories	All	Talos has added the following new Security Intelligence categories: • banking_fraud • ioc • high_risk • link_sharing • malicious • newly_seen • spyware You should update your access control and DNS policies to address the new categories, and check periodically for future changes. New/modified pages: Security Intelligence tab, Networks and URLs sub-tabs; DNS rules in DNS policies Supported platforms: FMC