Security Intelligence Blacklisting

The following topics provide an overview of Security Intelligence, including use for blacklisting and whitelisting traffic and basic configuration.

Security Intelligence Basics

As a first line of defense against malicious Internet content, the Firepower System includes the Security Intelligence feature, which allows you to immediately blacklist (block) connections based on the latest reputation intelligence, removing the need for a more resource-intensive, in-depth analysis.

Security Intelligence works by blocking traffic to or from IP addresses, URLs, or domain names that have a known bad reputation. This traffic filtering takes place **before** any other policy-based inspection, analysis, or traffic handling (although it does occur after hardware-level handling, such as fast-pathing).

Note that you could create access control rules that perform a similar function to Security Intelligence filtering by manually restricting traffic by IP address or URL. However, access control rules are wider in scope, more complex to configure, and cannot automatically update using dynamic feeds.

Traffic blacklisted by Security Intelligence is immediately blocked and therefore is not subject to any further inspection—not for intrusions, exploits, malware, and so on, but also not for network discovery. You can override blacklisting with whitelisting to force access control rule evaluation, and, recommended in passive deployments, you can use a "monitor-only" setting for Security Intelligence filtering. This allows the system to analyze connections that would have been blacklisted, but also logs the match to the blacklist and generates an end-of-connection security intelligence event.

⚠ **Caution** For traffic handled by many devices, the system processes certain Trust rules before an access control policy's Security Intelligence blacklist, which can allow blacklisted traffic to pass uninspected. For more information, see Limitations to Trusting or Blocking Traffic.

Security Intelligence Configuration

If you want to whitelist, blacklist, or monitor specific IP addresses, URLs, or domain names, you must configure custom objects, lists, or feeds. You have the following options:

- To configure network, URL, or DNS feeds, see Creating Security Intelligence Feeds.
- To configure network, URL, or DNS lists, see Updating Security Intelligence Lists.
- To configure network objects and object groups, see Creating Network Objects.
- To configure URL objects and object groups, see Creating URL Objects.

Blacklisting, whitelisting, or monitoring traffic based on a DNS list or feed also requires that you:

- 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.

Security Intelligence Strategies

For your convenience, Cisco provides feeds containing IP addresses, domain names, and URLs with poor reputation, as determined by Talos:

- the *Intelligence Feed*, which comprises several regularly updated collections of IP addresses.
- the *DNS and URL Intelligence Feed*, which comprises several regularly updated collections of domain names and URLs.

The Intelligence Feeds keep track of open relays, known attackers, bogus IP addresses (bogon), and so on. Because the Intelligence Feeds are regularly updated, using them ensures that the system uses up-to-date information to filter your network traffic. Malicious IP addresses, domain names, and URLs that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and deploy new policies.

You can also customize the feature to suit the unique needs of your organization, for example:

- **third-party feeds—**you can supplement the Intelligence Feeds with third-party reputation feeds, which are dynamic lists that the Firepower Management Center downloads from the internet on a regular basis
- **global blacklist and custom blacklists—**the system allows you to manually blacklist specific IP addresses, URLs, or domain names in many ways depending on your needs
- **whitelisting to eliminate false positives—**when a blacklist is too broad in scope, or incorrectly blocks traffic that you want to allow (for example, to vital resources), you can override a blacklist with a custom whitelist
- **enforcing blacklisting by security zone—**to improve performance, you may want to target enforcement, for example, restricting spam blacklisting to a zone that handles email traffic

- **monitoring instead of blacklisting**—especially useful in passive deployments and for testing feeds before you implement them; you can merely monitor and log the violating sessions instead of blocking them, generating end-of-connection events

Note In passive deployments, to optimize performance, Cisco recommends that you always use monitor-only settings. 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.

Example: Whitelisting

If a reputable feed improperly blocks your access to vital resources but is overall useful to your organization, you can whitelist only the improperly classified IP addresses, rather than removing the whole feed from the blacklist.

Example: Security Intelligence by Zone

You can whitelist an improperly classified URL, but then restrict the whitelist 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 whitelisted URLs. Or, you could use a third-party spam feed to blacklist traffic on an email server security zone.

Example: Monitor-Only Blacklisting

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.

Security Intelligence in Access Control Policies

Access control policies and their associated DNS policies use Security Intelligence whitelists and blacklists to quickly filter networks and URLs. The system provides default lists that apply to any zone. These lists are populated by your analysts, who can quickly add individual IP addresses, URLs, and domain names using the context menu. You can opt not to use these default lists on a per-policy basis.

Use the **Security Intelligence** tab in the access control policy editor to configure network and URL Security Intelligence, and to associate the access control policy with a DNS policy.

You can set network and URL blacklisted objects, including feeds and lists, to monitor-only. This allows the system to handle connections involving blacklisted IP addresses and URLs using access control, but also logs the connection’s match to the blacklist.

Security Intelligence Options

Object, Zone, and Blacklist Icons

On the Security Intelligence tab of the access control policy editor, each type of object or zone is distinguished with an different icon.

In the blacklist, objects set to block are marked with the block icon (✖) while monitor-only objects are marked with the monitor icon (⬇). Because the whitelist overrides the blacklist, if you add the same object to both lists, the system displays the blacklisted object with a strikethrough.

Security Intelligence in a Multidomain Deployment

In a multidomain deployment, the Global domain owns the Global blacklists and whitelists. Only Global administrators can add to or remove items from the Global lists. So that subdomain users can whitelist and blacklist networks, domain names, and URLs, multitenancy uses the concepts of Domain lists and Descendant Domain lists:

- A Domain list is a whitelist or blacklist whose contents apply to a particular subdomain only. The Global lists are Domain lists for the Global domain.
- A Descendant Domain list is a whitelist or blacklist that aggregates the Domain lists of the current domain.

Search Syntax for Network Objects

You can search on network and URL object names and on the values configured for those objects. For example, if you have an individual network object named Texas Office with the configured value 192.168.3.0/24, and the object is included in the group object US Offices, you can display both objects by typing a partial or complete search string such as Tex, or by typing a value such as 3.

Security Intelligence Zone Constraints

By default, Security Intelligence filtering is not constrained by zone, that is, Security Intelligence objects have an associated zone of Any. You can constrain by only one zone. To enforce Security Intelligence filtering for an object on multiple zones, you must add the object to the whitelist or blacklist separately for each zone. Also, the default whitelist or blacklist cannot be constrained by zone.

Security Intelligence 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 whitelist matches; logging of whitelisted connections depends on their eventual disposition. You must enable logging for blacklisted connections before you can set blacklisted objects to monitor-only.

Security Intelligence Categories

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

Security Intelligence Category	Description
Malware	Sites that host malware binaries or exploit kits
Phishing	Sites that host phishing pages
Spam	Mail hosts that are known for sending spam
Bots	Sites that host binary malware droppers
CnC	Sites that host command and control servers for botnets
OpenProxy	Open proxies that allow anonymous web browsing
OpenRelay	Open mail relays that are known to be used for spam
TorExitNode	Tor exit nodes
Bogon	Bogon networks and unallocated IP addresses

Configuring Security Intelligence

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

Each access control policy has Security Intelligence options. You can whitelist or blacklist network objects, URL objects and lists, and Security Intelligence feeds and lists, all of which you can constrain by security zone. You can also associate a DNS policy with your access control policy, and whitelist or blacklist domain names.

Caution Changing a Security Intelligence list, except the Whitelist Now or Blacklist Now options from the right-click context menu, 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.

You can add up to a total of 255 network objects and 32767 URL objects and lists to the whitelists and blacklists. That is, the number of objects in the whitelists plus the number in the blacklists cannot exceed 255 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.

Before You Begin

- In passive deployments, or if you want to set Security Intelligence filtering to monitor-only, enable logging; see Logging Blacklisted Connections.

Procedure

Step 1 In the access control policy editor, click the **Security Intelligence** tab.
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 the **Networks** tab to add network objects.
- Click the **URLs** tab to add URL objects.

Step 3 Find the **Available Objects** you want to add to the whitelist or blacklist. 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 the add icon (⊕), 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 the add icon (⊕), 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 Select one or more **Available Objects** to add.

Step 5 Optionally, constrain the selected objects by zone by selecting an **Available Zone**.
You cannot constrain system-provided Security Intelligence lists by zone.

Step 6 Click **Add to Whitelist** or **Add to Blacklist**, or click and drag the selected objects to either list.

To remove an object from a whitelist or blacklist, click its delete icon (🗑) To remove multiple objects, select them and right-click to **Delete Selected**.

Step 7 Optionally, set blacklisted objects to monitor-only by right-clicking the object under **Blacklist**, then selecting **Monitor-only (do not block)**.
You cannot set system-provided Security Intelligence lists to monitor only.

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

Caution Associating a custom DNS policy with Security Intelligence 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.

Step 9 Click **Save**.

What to Do Next

- Deploy configuration changes; see Deploying Configuration Changes.