Security Intelligence

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. The following topics explain how to implement Security Intelligence.

About Security Intelligence

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. The system drops this unwanted traffic before evaluating it with the access control policy, thus reducing the amount of system resources used.

You can block traffic based on the following:

- Cisco Talos Intelligence Group (Talos) feeds—Talos provides access to regularly updated security 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. The system downloads feed updates regularly, and thus new threat intelligence is available without requiring you to redeploy the configuration.

Note Talos feeds are updated by default every hour. You can change the update frequency, and even update the feeds on demand, from the **Device** > **Updates** page.

- Network and URL objects—If you know of specific IP addresses or URLs you want to block, you can create objects for them and add them to the blocked list or the exception list. Note that you cannot use network objects with FQDN or range specifications.

You create separate lists for IP addresses (networks) and URLs.

Note If an HTTP/HTTPS request is to a URL that uses an IP address instead of a hostname, the system looks up the IP address reputation in the network address lists. You do not need to duplicate IP addresses in the network and URL lists.

Making Exceptions to the Block Lists

For each block list, you can create an associated exception list, also known as the do not block list. The only purpose of the exception list is to exempt IP addresses or URLs that appear in the block list. That is, if you find an address or URL you need to use, and you know to be safe, is in a feed configured on the block list, you can exempt that network/URL without completely removing the category from the block list.

Exempted traffic is subsequently evaluated by the access control policy. The ultimate decision on whether the connections are allowed or dropped is based on the access control rule the connections match. The access rule also determines whether intrusion or malware inspection is applied to the connection.

Security Intelligence Feed Categories

The following table describes the categories available in the Cisco Talos Intelligence Group (Talos) feeds. These categories are available for both network and URL blocking.

These categories can change over time, so a newly-downloaded feed might have category changes. When configuring Security Intelligence, you can click the info icon next to a category name to see a description.

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

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

Security Intelligence Category	Description
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
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

License Requirements for Security Intelligence

You must enable the **Threat** license to use Security Intelligence. See Enabling or Disabling Optional Licenses.

Configuring Security Intelligence

The Security Intelligence policy gives you an early opportunity to drop unwanted traffic based on source/destination IP address or destination URL. Any allowed connections are still evaluated by access control policies and might eventually be dropped. You must enable the Threat license to use Security Intelligence.

Procedure

Step 1 Select **Policies** > **Security Intelligence**.

Step 2 If the policy is not enabled, click the **Enable Security Intelligence** button.

You can disable the policy at any time by clicking the **Security Intelligence** toggle to **Off**. Your configuration is preserved, so that when you enable the policy again you do not need to reconfigure it.

Step 3 Configure Security Intelligence.

There are separate block lists for Networks (IP addresses) and URLs.

a) Click the **Network** or **URL** tab to display the list you want to configure.

b) In the block/drop list, click **+** to select the objects or feeds whose connections you want to drop immediately.

The object selector organizes the objects and feeds on separate tabs by type. If the object you want does not yet exist, click the **Create New Object** link at the bottom of the list and create it now. For a description of the Cisco Talos Intelligence Group (Talos) feeds, click the **i** button next to the feed. See also Security Intelligence Feed Categories, on page 2.

Note Security Intelligence ignores IP address blocks using a /0 netmask. This includes the any-ipv4 and any-ipv6 network objects. Do not select these objects for network blocking.

c) In the do not block list, click **+** and select any exceptions to the block list.

The only reason to configure this list is to make exceptions for IP addresses or URLs that are in the block list. Exempted connections are subsequently evaluated by your access control policy, and might be dropped anyway.

d) Repeat the process to configure the other block list.

Step 4 (Optional.) Click the **Edit Logging Settings** button (⚙) to configure logging.

If you enable logging, any matches to block list entries are logged. Matches to exception entries are not logged, although you get log messages if exempted connections match access control rules with logging enabled.

Configure the following settings:

- **Connection Events Logging**—Click the toggle to enable or disable logging.
- **Syslog**—If you want to send a copy of the events to an external syslog server, select this option and select the server object that defines the syslog server. If the required object does not already exist, click **Add Syslog Server** and create it.

  Because event storage on the device is limited, sending events to an external syslog server can provide more long term storage and enhance your event analysis.

Monitoring Security Intelligence

If you enable logging for the Security Intelligence policy, the system generates Security Intelligence events for each connection that matches an item on a block list. There are matching connection events for these connections.

Statistics for dropped connections appear in the various dashboards available on the Monitoring page.

The **Monitoring** > **Access and SI Rules** dashboard shows the top access rules and Security Intelligence rule-equivalents that are matching traffic.

In addition, you can select **Monitoring** > **Events**, then the **Security Intelligence** view, to see the Security Intelligence events, as well as the related connection events on the **Connection** tab.

- The SI Category ID field in an event indicates the object matched in the block list, such as a network or URL object or feed.

- The Reason field in a connection event explains why the action shown in the event was applied. For example, a Block action paired with reasons such as IP Block or URL Block indicates that a connection was dropped by Security Intelligence.

Examples for Security Intelligence

The use case chapter includes an example of implementing Security Intelligence policies. Please see How to Block Threats.