

Blacklisting Using Security Intelligence IP Address Reputation

As a first line of defense against malicious Internet content, the ASA FirePOWER module 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 filtering requires a Protection license.

Security Intelligence works by blocking traffic to or from IP addresses that have a known bad reputation. This traffic filtering takes place **before** any other policy-based inspection, analysis, or traffic handling.

Note that you could create access control rules that perform a similar function to Security Intelligence filtering by manually restricting traffic by IP address. 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. Optionally, 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.

For your convenience, Cisco provides the *Intelligence Feed* (sometimes called the *Sourcefire Intelligence Feed*), which is comprised of several regularly updated collections of IP addresses determined by the VRT to have a poor reputation. The Intelligence Feed tracks open relays, known attackers, bogus IP addresses (bogon), and so on. You can also customize the feature to suit the unique needs of your organization, for example:

- **third-party feeds**—you can supplement the Intelligence Feed with third-party reputation feeds, which the system can automatically update just as it does the Cisco feed
- **custom blacklists**—the system allows you to manually blacklist specific IP addresses in many ways depending on your needs
- **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 the violating sessions instead of blocking them, generating end-of-connection events
- **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

For detailed information on configuring your access control policy to perform Security Intelligence to perform Security Intelligence filtering and viewing the event data that this filtering produces, see the following sections:

- Choosing a Security Intelligence Strategy, page 5-2
- Building the Security Intelligence Whitelist and Blacklist, page 5-3
- Logging Security Intelligence (Blacklisting) Decisions, page 36-8

Choosing a Security Intelligence Strategy

License: Protection

The easiest way to construct a blacklist is to use the Intelligence Feed, which tracks IP addresses known to be open relays, known attackers, bogus IP addresses (bogon), and so on. Because the Intelligence Feed is regularly updated, using it ensures that the system uses up-to-date information to filter your network traffic. Malicious IP addresses that represent security threats such as malware, spam, botnets, and phishing may appear and disappear faster than you can update and apply new policies.

To augment the Intelligence Feed, you can perform Security Intelligence filtering using custom or third-party IP address lists and feeds, where:

- a *list* is a static list of IP addresses that you upload to the ASA FirePOWER module
- a *feed* is a dynamic list of IP addresses that the ASA FirePOWER module downloads from the Internet on a regular basis; the Intelligence Feed is a special kind of feed

For detailed information on configuring Security Intelligence lists and feeds, including Internet access requirements, see Working with Security Intelligence Lists and Feeds, page 3-4.

Using the Security Intelligence Global Blacklist

In the course of your analysis, you can build a *global blacklist*. For example, if you notice a set of routable IP addresses in intrusion events associated with exploit attempts, you can blacklist those IP addresses. The ASA FirePOWER module uses this global blacklist (and a related *global whitelist*) to perform Security Intelligence filtering in all access control policies. For information on managing these global lists, see Working with the Global Whitelist and Blacklist, page 3-6.

Note Although feed updates and additions to the global blacklist (or global whitelist; see below) automatically implement changes throughout your deployment, any other change to a Security Intelligence object requires you to reapply the access control policy. For more information, see Table 3-1 on page 3-5.

Using Network Objects

Finally, a simple way to construct a blacklist is to use *network objects or network object groups* that represent an IP address, IP address block, or collection of IP addresses. For information on creating and modifying network objects, see Working with Network Objects, page 3-3.

Using Security Intelligence Whitelists

In addition to a blacklist, each access control policy has an associated whitelist, which you can also populate with Security Intelligence objects. A policy's whitelist overrides its blacklist. That is, the system evaluates traffic with a whitelisted source or destination IP address using access control rules, even if the IP address is also blacklisted. In general, use the whitelist if a blacklist is still useful, but is too broad in scope and incorrectly blocks traffic that you want to inspect.

For example, 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.

Enforcing Security Intelligence Filtering by Security Zone

For added granularity, you can enforce Security Intelligence filtering based on whether the source or destination IP address in a connection resides in a particular security zone.

To extend the whitelist example above, you could whitelist the improperly classified IP addresses, but then restrict the whitelist object using a security zone used by those in your organization who need to access those IP addresses. That way, only those with a business need can access the whitelisted IP addresses. As another example, you could use a third-party spam feed to blacklist traffic on an email server security zone.

Monitoring—Rather than Blacklisting—Connections

If you are not sure whether you want to blacklist a particular IP address or set of addresses, you can use a "monitor-only" setting, which allows the system to pass the matching connection to access control rules, but also logs the match to the blacklist and generates an end-of-connection Security Intelligence event. Note that you cannot set the global blacklist to monitor-only.

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.

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

Building the Security Intelligence Whitelist and Blacklist

License: Protection

To build a whitelist and blacklist, you populate them with any combination of network objects and groups, as well as Security Intelligence feeds and lists, all of which you can constrain by security zone.

By default, access control policies use the ASA FirePOWER module's global whitelist and blacklist, which apply to any zone. These lists are populated by your analysts. You can opt not to use these global lists on a per-policy basis.



Note You cannot apply an access control policy that uses a populated global whitelist or blacklist to a device not licensed for Protection. If you added IP addresses to either global list, you **must** remove the non-empty list from the policy's Security Intelligence configuration before you can apply the policy. For more information, see Working with the Global Whitelist and Blacklist, page 3-6.

After you build your whitelist and blacklist, you can log blacklisted connections. You can also set individual blacklisted objects, including feeds and lists, to monitor-only. This allows the system to handle connections involving blacklisted IP addresses using access control, but also logs the connection's match to the blacklist.

Use the Security Intelligence tab in the access control policy to configure the whitelist, blacklist, and logging options. The page lists the Available Objects you can use in either the whitelist or blacklist, as well as the Available Zones you can use to constrain whitelisted and blacklisted objects. Each type of object or zone is distinguished with an different icon. The objects marked with the Cisco icon ( ) represent the different categories in the Intelligence Feed.

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.

You can add up to a total of 255 objects to the whitelist and the blacklist. That is, the number of objects in the whitelist plus the number in the blacklist cannot exceed 255.

Note that although you can add network objects with a netmask of `/0` to the whitelist or blacklist, address blocks using a `/0` netmask in those objects will be ignored and whitelist and blacklist filtering will not occur based on those addresses. Address blocks with a `/0` netmask from Security Intelligence feeds are also ignored. If you want to monitor or block all traffic targeted by a policy, use an access control rule with the **Monitor** or **Block** rule action, respectively, and a default value of **any** for the **Source Networks** and **Destination Networks**, instead of Security Intelligence filtering.

To build the Security Intelligence whitelist and blacklist for an access control policy:

Step 1 Select **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to configure.

The access control policy editor appears.

Step 3 Select the **Security Intelligence** tab.

Security Intelligence settings for the access control policy appear.

Step 4 Optionally, click the logging icon ( ) to log blacklisted connections.

You must enable logging before you can set blacklisted objects to monitor-only. For details, see Logging Security Intelligence (Blacklisting) Decisions, page 36-8.

Step 5 Begin building your whitelist and blacklist by selecting one or more **Available Objects**.

Use Shift and Ctrl to select multiple objects, or right-click and **Select All**.

Tip You can search for existing objects to include, or create objects on the fly if no existing objects meet the needs of your organization. For more information, see Searching for Objects to Whitelist or Blacklist, page 5-5.

Step 6 Optionally, constrain the selected objects by zone by selecting an **Available Zone**.

By default, objects are not constrained, that is, they have a zone of `Any`. Note that other than using **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 global whitelist or blacklist cannot be constrained by zone.

Step 7 Click **Add to Whitelist** or **Add to Blacklist**.

You can also click and drag the selected objects to either list.

The objects you selected are added to the whitelist or blacklist.

Tip To remove an object from a list, click its delete icon ( ). Use Shift and Ctrl to select multiple objects, or right-click and **Select All**, then right-click and select **Delete Selected**. If you are deleting a global list, you must confirm your choice. Note that removing an object from a whitelist or blacklist does not delete that object from the ASA FirePOWER module.

Step 8 Repeat steps 5 through 7 until you are finished adding objects to your whitelist and blacklist.

Step 9 Optionally, set blacklisted objects to monitor-only by right-clicking the object under **Blacklist**, then selecting **Monitor-only (do not block)**.

In passive deployments, Cisco recommends you set all blacklisted objects to monitor-only. Note, however, that you cannot set the global blacklist to monitor-only.

Step 10 Click **Store ASA FirePOWER Changes**.

You must apply the access control policy for your changes to take effect; see Deploying Configuration Changes, page 4-11.

Searching for Objects to Whitelist or Blacklist

License: Protection

If you have multiple network objects, groups, feeds, and lists, use the search feature to narrow the objects you want to blacklist or whitelist.

To search for objects to whitelist or blacklist:

Step 1 Type your query in the **Search by name or value** field.

The Available Objects list updates as you type to display matching items. To clear the search string, click the reload icon ( ) above the search field or click the clear icon ( ) in the search field.

You can search on network 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`.