IP Address is Blocked or Blacklisted by the Security Intelligence of a Cisco FireSIGHT System

Contents

Introduction

The Security Intelligence feature allows you to specify the traffic that can traverse your network based on the source or destination IP address. This is especially useful if you want to blacklist - deny traffic to and from - specific IP addresses, before the traffic is subjected to analysis by access control rules. This documents describes how to handle scenarios when an IP address is being blocked or blacklisted by a Cisco FireSIGHT System.

Prerequisites

Requirements

Cisco recommends that you have knowledge on Cisco FireSIGHT Management Center.

Components Used

The information in this document is based on these hardware and software versions:

- Cisco FireSIGHT Management Center
- Cisco Firepower Appliance
- Cisco ASA with Firepower (SFR) module

- Software Version 5.2 or later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Difference Between Intelligence Feed and Intelligence List

There are two ways to use the Security Intelligence feature in a FireSIGHT System:

Security Intelligence Feed

A Security Intelligence feed is a dynamic collection of IP addresses that the Defense Center downloads from an HTTP or HTTPS server. To help you build blacklists, Cisco provides the *Security Intelligence Feed*, which represents IP addresses determined by the Vulnerability Research Team (VRT) to have a poor reputation.

Security Intelligence List

A Security Intelligence list, contrasted with a feed, is a simple static list of IP addresses that you manually upload to the FireSIGHT Management Center.

Legitimate IP Address is Blocked or Blacklisted

Verify if an IP Address is in the Security Intelligence Feed

If an IP address is being blocked by the Security Intelligence Feed blacklist, you can follow the steps below to verify this:

Step 1: Access the CLI of the Firepower appliance or service module.

Step 2: Run the following command. Replace `<IP_Address>` with the IP address that you want to search for:

```
admin@Firepower:~$ grep <IP_Address> /var/sf/iprep_download/*.blf
```

For example, If you want to search for IP Address 198.51.100.1, run the following command:

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

If this command returns any match for the IP address you provided, it indicates that the IP address is present on the Security Intelligence Feed blacklist.

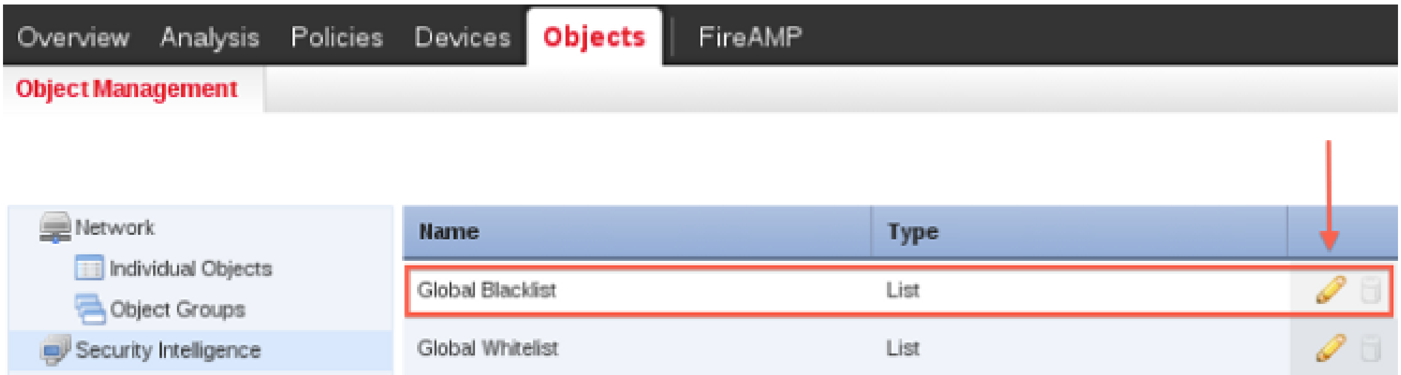
Check the Blacklist

To find a list of the IP addresses that might be blacklisted, follow the steps below:

Step 1: Access to the web interface of the FireSIGHT Management Center.

Step 2: Navigate to **Objects > Object Management > Security Intelligence**.

Step 3: Click on the *pencil* icon to open or edit the **Global Blacklist**. A pop up window with a list of IP addresses appears.



Name	Type
Global Blacklist	List
Global Whitelist	List

Work with a Blocked or Blacklisted IP Address

If a particular IP address is blocked or blacklisted by Security Intelligence Feed, you can consider any of the following options to allow it.

Option 1: Security Intelligence Whitelists

You can whitelist an IP address that is blacklisted by Security Intelligence. A whitelist overrides its blacklist. The FireSIGHT system evaluates traffic with a whitelisted source or destination IP address using access control rules, even if an IP address is also blacklisted. Therefore, you can use a whitelist when 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 a vital resource but is overall useful to your organization, you can whitelist the improperly classified IP addresses only, rather than removing the whole feed from the blacklist.

> **Caution**: After you make any change in an Access Control policy, you must reapply the policy to the managed devices.

Option 2: Enforce Security Intelligence Filter 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 might want to use a third-party spam feed to blacklist traffic on an email server security zone.

Option 3: Monitor, Rather than Blacklist

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. 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.

Steps to configure the Security Intelligence with "monitor-only" setting:

1. On the **Security Intelligence** tab in an access control policy, click the logging icon. The Blacklist Options dialog box appears.
2. Select the **Log Connections** check box to log beginning-of-connection events when traffic meets Security Intelligence conditions.
3. Specify where to send connection events.
4. Click **OK** to set your logging options. The Security Intelligence tab appears again.
5. Click **Save**. You must apply the access control policy for your changes to take effect.

Option 4: Contact Cisco Technical Assistance Center

You can always contact Cisco Technical Assistance Center, if:

- You have questions with the above options 1, 2 or 3.
- You want further research and analysis on an IP address that is blacklisted by Security Intelligence.
- You want an explanation why the IP address is blacklisted by Security Intelligence.