

# Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Overview of Security Intelligence feed](#)

[Manually add IP addresses to Global-Blacklist and Global-Whitelist](#)

[Create the Custom list of blacklist IP Address](#)

[Configure the Security Intelligence](#)

[Deploy Access Control Policy](#)

[Security Intelligence's events Monitoring](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

## Introduction

This document describes Cisco Security Intelligence/IP address reputation and configuration of IP blacklisting (Blocking) while using custom/auto feed of low reput IP address.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of ASA (Adaptive Security Appliance) firewall, ASDM (Adaptive Security Device Manager)
- FirePOWER appliance knowledge

**Note:** Security Intelligence filtering requires a Protection license.

### Components Used

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

- ASA FirePOWER modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X ) running software version 5.4.1 and above
- ASA FirePOWER module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) running software version 6.0.0 and above

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.

## Background Information

Cisco Security Intelligence comprises of several regularly updated collections of IP addresses that are determined to have a poor reputation by the Cisco TALOS Team. Cisco TALOS team determines the low reputation if any malicious activity is originated from those IP addresses such as spams, malware, phishing attacks etc.

Cisco IP Security Intelligence feed tracks the database of Attackers, Bogon, Bots, CnC, Dga, ExploitKit, Malware, Open\_proxy, Open\_relay, Phishing, Response, Spam, Suspicious. Firepower module does provide the option to create the custom feed of low repute IP address.

## Overview of Security Intelligence feed

Here is some more information about the type of IP address collections which can be classified as different categories in the Security Intelligence.

**Attackers:** Collection of IP addresses that are continually scanning for vulnerabilities or attempting to exploit other systems.

**Malware:** Collection of IP addresses that are attempting to propagate malware or are actively attacking anyone who visits them.

**Phishing:** Collection of hosts that are actively attempting to trick end users into entering confidential information like usernames and passwords.

**Spam:** Collection of hosts that have been identified as the source of sending spam email messages.

**Bots:** Collection of hosts that are actively participating as part of a botnet, and are being controlled by a known bot net controller.

**CnC:** Collection of hosts that have been identified as the controlling servers for a known Botnet.

**OpenProxy:** Collection of hosts that are known to run Open Web Proxies and offer anonymous web browsing services.

**OpenRelay:** Collection of hosts that are known to offer anonymous email relaying services used by spam and phishing attackers.

**TorExitNode:** Collection of hosts that are known to offer exit node services for the Tor Anonymizer network.

**Bogon:** Collection of IP Addresses that are not allocated but are sending traffic.

**Suspicious:** Collection of IP Addresses that are displaying suspicious activity and are under active investigation.

**Response:** Collection of IP Addresses that have been repeatedly observed engaged in the

suspicious or malicious behavior.

## Manually add IP addresses to Global-Blacklist and Global-Whitelist

Firepower module allows you to add certain IP addresses to Global-Blacklist when you know that they are part of some malicious activity. IP addresses can also be added to Global-Whitelist, if you want to allow the traffic to certain IP addresses which are blocked by blacklist IP addresses. If you add any IP address to Global-Blacklist/Global-Whitelist, it takes effect immediately without the need to apply the policy.

In order to add the IP address to Global-Blacklist/ Global-Whitelist, navigate to **Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**, hover the mouse on connection events and select **View Details**.

You can add either source or destination IP address to the Global-Blacklist/ Global-Whitelist. Click on **Edit** button and select **Whitelist Now/Blacklist Now** to add the IP address to the respective list, as shown in the image.

**Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**

Real Time Eventing

+ All ASA FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter  
Rule Action=Allow \*

Pause Refresh Rate 5 seconds 1/25/16 9:11:25 AM (IST)

Receive Times	Action	First Packet	Last Packet	Reason
1/25/16 9:09:50 AM	Allow	1/25/16 9:09:48 AM	1/25/16 9:09:49 AM	
1/25/16 9:07:36 AM	Allow	1/25/16 9:07:05 AM	1/25/16 9:07:03 AM	
1/25/16 9:07:07 AM	Allow	1/25/16 9:07:06 AM	1/25/16 9:07:06 AM	

**Monitoring > ASA FirePOWER Monitoring > Real Time Eventing**

Real Time Eventing

Initiator		Responder		Edit
Initiator IP	192.168.20.3	Responder IP	10.106.44.55	
Initiator Country and Continent	not available	Responder Country and Continent	not available	
Source Port/ICMP Type	60297	Destination Port/ICMP	49153	

In order to verify that source or destination IP address is added to the Global-Blacklist/ Global-Whitelist, navigate to **Configuration > ASA Firepower Configuration > Object Management >**

**Security Intelligence > Network Lists and Feeds** and edit **Global-Blacklist/ Global Whitelist**. You can also use the delete button to remove any IP address from the list.

## Create the Custom list of blacklist IP Address

Firepower allows you to create custom Network/IP addresses list which can be used in blacklisting (blocking). There are three option to do this:

1. You can write the IP addresses to a text file (One IP address per line) and can upload the file to Firepower Module. In order to upload the file, navigate to **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** and then click **Add Network Lists and Feeds** **Name:** Specify the name of Custom list. **Type:** Select **List** from the drop-down list. **Upload List:** Choose **Browse** to locate the text file in your system. Select option **Upload** to upload the file.
2. You can use any third-party IP database for the custom list for which Firepower module contacts the third party server to fetch the IP address list. In order to configure this, navigate to **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** and then click **Add Network Lists and Feeds** **Name:** Specify the name of the Custom Feed.

**Type:** Select option **Feed** from the drop-down list.

**Feed URL:** Specify the URL of the server to which Firepower module should connect and download the feed.

**MD5 URL:** Specify the hash value to validate the Feed URL path.

**Update Frequency:** Specify the time interval in which system connect to URL Feed server.

The image displays two screenshots of the Cisco Firepower configuration interface, specifically the 'Add Network Lists and Feeds' dialog box. The top screenshot shows the configuration for a 'List' type. The 'Name' field is 'Custom\_Feed', the 'Type' is 'List', and the 'Upload List' field contains the path 'C:\fakepath\Custom\_IP\_Feed.'. The bottom screenshot shows the configuration for a 'Feed' type. The 'Name' field is 'Custom\_Network\_Feed', the 'Type' is 'Feed', the 'Feed URL' is 'http://192.168.30.1/blacklist-IP.txt', the 'MD5 URL' is '(optional)', and the 'Update Frequency' is '30 minutes'.

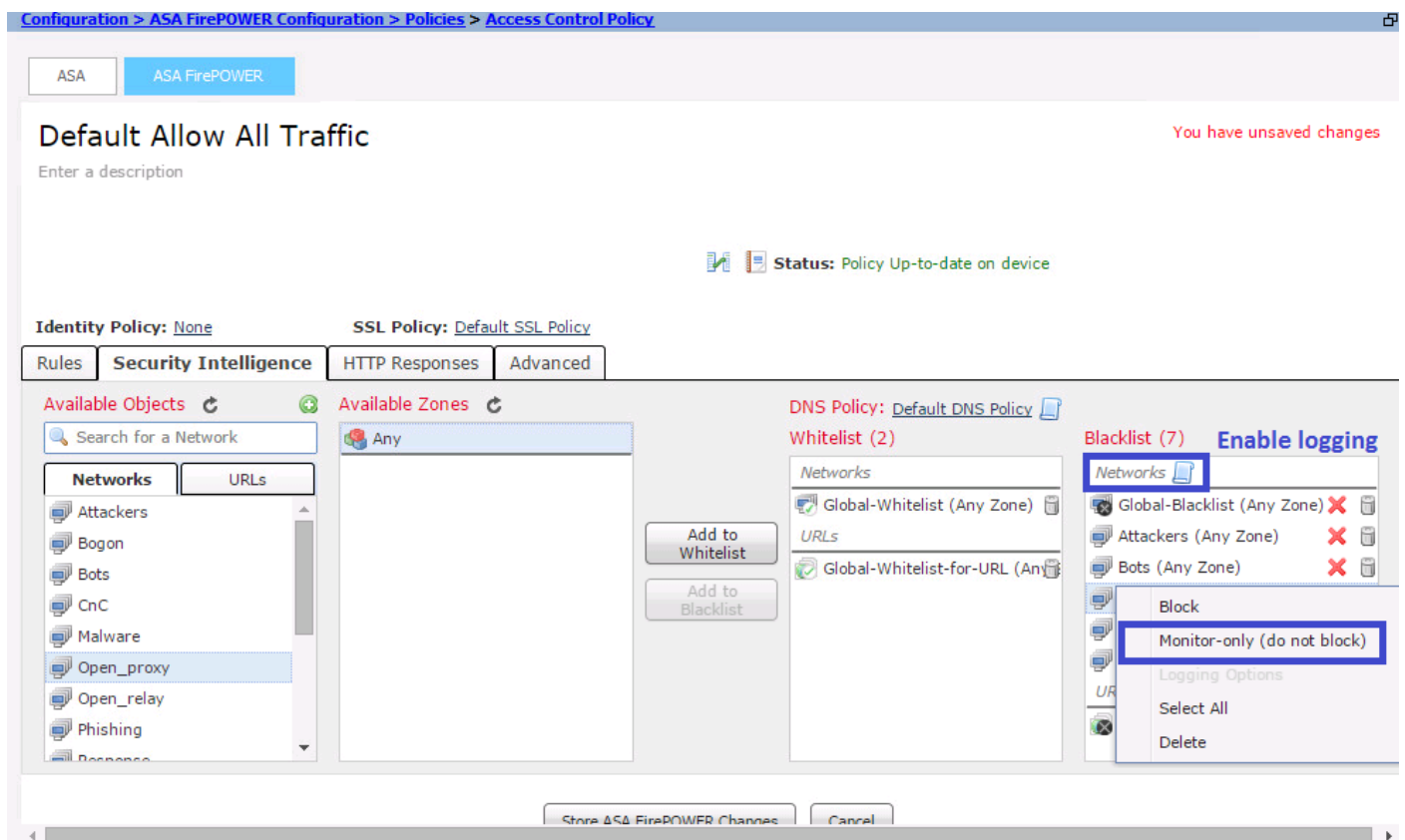
# Configure the Security Intelligence

In order to Configure Security Intelligence, navigate to **Configuration > ASA Firepower Configuration > Policies > Access Control Policy**, select **Security Intelligence** tab.

Choose the feed from the Network Available Object, move to **Whitelist/ Blacklist** column to allow/block the connection to the malicious IP address.

You can click the icon and enable logging as specified in the image.

If you just want to generate the event for malicious IP connections instead of blocking the connection, then right-click on the feed, choose **Monitor-only (do not block)**, as shown in the image:

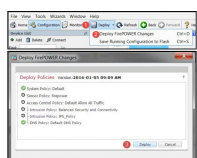


Choose option Store ASA Firepower Changes to save the AC policy changes.

## Deploy Access Control Policy

For the changes to take effect, you must deploy the Access Control policy. Before you apply the policy, see an indication that whether the Access Control Policy is out-of-date on the device or not.

To deploy the changes to the sensor, click **Deploy** and choose **Deploy FirePOWER Changes** then select **Deploy** in the pop-up window to deploy the changes.











**Verify** the changes by the Firepower Tool Module, navigate to **Monitoring > ASA events Monitoring** and select **Security Intelligence** tab. This will

**and Feeds** and check the time when the feed was last updated. You can choose the Edit button to set the frequency of feed update.

Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds

Update Feeds   Add Network Lists and Feeds   Filter

Name	Type	
Cisco-Intelligence-Feed <i>Last Updated: 2016-02-08 10:03:14</i>	Feed	 
Custom_Feed	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

Ensure that Access Control Policy deployment has completed successfully.

Monitor the security intelligence to see if traffic is blocking or not.

## Related Information

- [Cisco ASA FirePOWER Module Quick Start Guide](#)
- [Technical Support & Documentation - Cisco Systems](#)