Configure IP Allow and Block List in the Secure Endpoint Cloud Console

Contents

Introduction

This document describes the IP Allow/Block feature within Cisco Secure Endpoint.

Prerequisites

Requirements

Cisco recommends that you have access to the Cisco Secure Endpoints portal.

Components Used

The information in this document is based on the Secure Endpoint console.

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, ensure that you understand the potential impact of any command.

Configure an IP Allow/Block List with Secure Endpoint

What is an IP Allow/Block List?

IP block and allow lists are used with device flow correlation to define custom IP address detections. After you have created your lists, you can then define in the policy to use them in addition to the Cisco Intelligence Feed or on their own. The lists can be defined to use individual IP addresses, CIDR blocks, or IP address and port combinations. When you submit a list, redundant addresses are combined on the back end.

IP Addresses Examples

If you add these entries to a list:

- 192.0.2.0/24
- 192.0.2.15
- 192.0.2.135
- 192.0.2.200

The list is processed with a net result of:

- 192.0.2.0/24

However, if you also include ports the result is different:

- 192.0.2.0/24
- 192.0.2.15:80
- 192.0.2.135
- 192.0.2.200

The list is processed with a net result of:

- 192.0.2.0/24
- 192.0.2.15:80

What is an IP Allow List?

An IP allow list enables you to specify IP addresses you never want to detect. Entries in your IP allowed list create an override in your IP blocked list as well as the Cisco Intelligence Feed. You can choose to add single IP addresses, entire CIDR blocks, or specify IP addresses with port numbers.

What is an IP Block List?

An IP block list allows you to specify IP addresses you want to detect any time one of your computers connects to them. You can choose to add single IP addresses, entire CIDR blocks, or specify IP addresses with port numbers. When a computer makes a connection to an IP address in your list the action taken depends on what you have specified in the Network section of your policy.

What is an Isolation IP Allow List?

An Isolation IP allow list specifies the IP addresses that are not blocked during isolation. Isolation IP allow lists are different from IP Allow Lists in that Isolation IP allow lists do not support port numbers in the rule.

Create an IP Allow/Block List

Step 1. In order to create an IP list, navigate to **Outbreak Control** in the Secure Endpoint portal and click **IP Block & Allow Lists** option, as shown in the image.

Outbreak Control

CUSTOM DETECTIONS

Simple

Advanced

Android

APPLICATION CONTROL

Blocked Applications

: Uploaded IP lists can contain up to 10,000 lines or be a maximum of 2 MB in size. Only IPv4 addresses are currently supported. To improve performance and include more addresses, use CIDR blocks.