在安全终端云控制台中配置IP允许和阻止列表

目录

简介

本文档介绍思科安全终端中的IP允许/阻止功能。

先决条件

要求

思科建议您有权访问思科安全终端门户。

使用的组件

本文档中的信息基于Secure Endpoint console。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

使用安全终端配置IP允许/阻止列表

什么是IP允许/阻止列表？

IP块和允许列表与设备流关联一起使用，用于定义自定义IP地址检测。创建列表后，可以在策略中定义这些列表，以除思科情报源之外或单独使用它们。 这些列表可以定义为使用单个IP地址、CIDR块或IP地址和端口组合。当您提交列表时，会在后端合并冗余地址。

IP地址示例

如果将这些条目添加到列表：

- 192.0.2.0/24
- 192.0.2.15
- 192.0.2.135
- 192.0.2.200

列表的净结果为：

- 192.0.2.0/24

但是，如果还包括端口，结果会有所不同：

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

列表的净结果为：

- 192.0.2.0/24
- 192.0.2.15:80

什么是IP允许列表？

通过IP允许列表，可以指定您不想检测的IP地址。您的IP允许列表中的条目会在IP阻止列表和思科情报源中创建覆盖。您可以选择添加单个IP地址、整个CIDR块，或者使用端口号指定IP地址。

什么是IP阻止列表？

通过IP阻止列表，您可以指定任何计算机连接到它们时想要检测的IP地址。您可以选择添加单个IP地址、整个CIDR块，或者使用端口号指定IP地址。当计算机连接到您列表中的IP地址时，采取的操作取决于您在策略的“网络”部分中指定的内容。

什么是隔离IP允许列表？

Isolation IP allow列表指定在隔离期间未被阻止的IP地址。 隔离IP允许列表与隔离IP允许列表中的IP允许列表不同，因为隔离IP允许列表不支持规则中的端口号。

创建IP允许/阻止列表

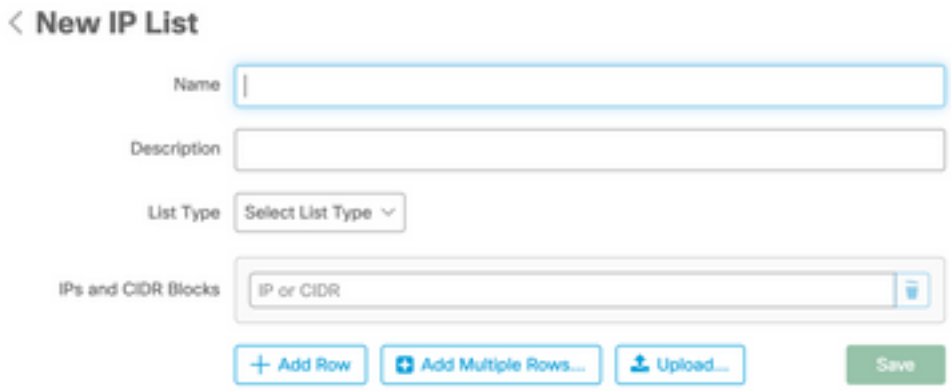
步骤1:要创建IP列表，请导航至Secure Endpoint门户中的**Outbreak Control**，然后单击**IP Block & Allow Lists**选项，如图所示。

IP阻止和允许列表

第二步：选择**Create IP List**功能，如图所示。

创建IP列表

第三步：系统随即会显示“新建IP列表”页面。输入新列表的名称和说明，然后从List Type下拉列表中选择**Allow**、**Block**或**Isolation**Allow，如图所示。



IP列表配置

第四步：您可以输入每行一个IP地址或CIDR块。您可以选择输入IP地址：

- 您可以单击**Add Row**添加单个行。
- 如果选择**Add Multiple Rows**，您还可以快速添加多个IP地址和CIDR块。
- 然后，您可以在对话框中输入或粘贴IP地址和CIDR块列表，然后在完成时单击**Add Rows**。
- 您还可以上传包含以换行符分隔的IP地址和CIDR块的CSV文件。要上传文件，单击**Upload**，然后单击Browse选择CSV文件，然后单击**Upload**。对于列表类型，选择是希望此列表为允许列表、阻止列表还是隔离允许。

第五步：完成后，保存IP地址列表配置。

其他配置示例

要将端口添加到阻止或允许列表（不考虑IP地址），可以向相应的列表中添加两个条目，其中XX是要阻止的端口号：

- 0.0.0.1/1:XX
- 128.0.0.1/1:XX

注意：上传的IP列表最多可包含100,000行或最大大小为2 MB。当前仅支持IPv4地址。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。