

在活动搜索中为云交付的防火墙启用报告

目录

- [简介](#)
- [概述](#)
- [解决方案](#)

简介

本文档介绍如何在网络隧道上启用云交付的防火墙策略报告。

概述

默认情况下，未启用Umbrella云交付防火墙的报告。必须在每个网络隧道上手动启用该功能，才能接收云交付防火墙策略的报告。

解决方案

要在控制面板上启用报告，请执行以下操作：

1. 导航到策略>防火墙。
2. 选择网络隧道以启用报告。
3. 单击所选隧道右侧的三个点。
4. 切换日志记录以启用报告。

Cisco Umbrella

Overview

Deployments

1 Policies

Management

DNS Policies

Firewall Policy

Web Policies

Policy Components

Destination Lists

Content Categories

Application Settings

Security Settings

Block Page Appearance

Integrations

Selective Decryption Lists

Reporting

Admin

Investigate

Policies / Management

Firewall Policy

Use this policy to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. For more information about Firewall Policy, view [Manage Firewall](#).

FILTERS

Q Search Firewall Rule names or descriptions

1 Selected SELECT ALL 6

EXPORT

ENABLE RULES

DISABLE RULES

...

	Priority	Name	Status	Action	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit	
☒	1	Umbrella HQ - Port Blocking	Enabled	Block	Any	Any IPs Any Ports	Any IPs 3 Ports	663.0 /24hrs	Apr 23, 2020 - 02:21pm	3...
☐	2	Umbrella HQ - IP Blocking	Enabled	Block	Any	Any IPs Any Ports	1 IP Any Ports	0/24hrs	Apr 09, 2020 - 12:10am	...
☐	3	Allow Umbrella Resolvers	Enabled	Allow	Any	Any IPs Any Ports	2 IPs Any Ports	30.5 k/24hrs	Apr 23, 2020 - 02:21pm	...
☐	4	Block SSH to SQL Server	Enabled	Block	Any	Any IPs Any Ports	1 IP 1 Port	0/24hrs	No Hits	...
☐	5	Block High Ports	Enabled	Block	Any	Any IPs Any Ports	Any IPs 1 Port	0/24hrs	No Hits	...
☐	6	Default Rule	Enabled	Allow	Any	Any IPs Any Ports	Any IPs Any Ports	11.9 k/24hrs	Apr 23, 2020 - 02:21pm	...

5.切换要启用日志记录的交换机。

Cisco Umbrella

Overview

Deployments

Policies

Management

DNS Policies

Firewall Policy

Web Policies

Policy Components

Destination Lists

Content Categories

Application Settings

Security Settings

Block Page Appearance

Integrations

Selective Decryption Lists

Reporting

Admin

Investigate

Policies / Management

Firewall Policy

Use this policy to control network traffic based on IP, port, and protocol. Rules are evaluated from the top down. For more information about Firewall Policy, view [Manage Firewall](#).

FILTERS

Q Search Firewall Rule names or descriptions

1 Selected [SELECT ALL 6](#)

EXPORT

ENABLE RULES

DISABLE RULES

...

	Priority	Name	Status	Action	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit
☒	1	Umbrella HQ - Port Blocking	Enabled	Block	Any	Any IPs Any Ports	Any IPs 3 Ports	663.0 /24hrs	A
☐	2	Umbrella HQ - IP Blocking	Enabled	Block	Any	Any IPs Any Ports	1 IP Any Ports	▲ 0/24hrs	A
☐	3	Allow Umbrella Resolvers	Enabled	Allow	Any	Any IPs Any Ports	2 IPs Any Ports	30.5 k/24hrs	
☐	4	Block SSH to SQL Server	Enabled	Block	Any	Any IPs Any Ports	1 IP 1 Port	▲ 0/24hrs	▲
☐	5	Block High Ports	Enabled	Block	Any	Any IPs Any Ports	Any IPs 1 Port	▲ 0/24hrs	▲ No Hits
☐	6	Default Rule	Enabled	Allow	Any	Any IPs Any Ports	Any IPs Any Ports	11.9 k/24hrs	Apr 23, 2020 - 02:21pm

Edit

Duplicate

Enabled

Logging

Block

Delete

360055232232

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）。