

クラウド配信ファイアウォールのアクティビティ検索でレポートを有効にする

内容

[はじめに](#)

[概要](#)

[解決方法](#)

はじめに

このドキュメントでは、ネットワークトンネルでクラウド配信ファイアウォールポリシーのレポートを有効にする方法について説明します。

概要

デフォルトでは、Umbrella Cloud-Delivered Firewallのレポートは有効になっていません。クラウド配信ファイアウォールポリシーのレポートを受信するには、各ネットワークトンネルでこの機能を手動で有効にする必要があります。

解決方法

ダッシュボードでレポートを有効にするには、次の手順に従います。

1. Policies > Firewallの順に移動します。
2. レポートを有効にするネットワークトンネルを選択します。
3. 選択したトンネルの右側にある3つのドットをクリックします。
4. レポートを有効にするには、ロギングのスイッチを切り替えます。

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

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	...

360055369031

5. ロギングのスイッチを有効に切り替えます。

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

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		Edit Duplicate Enabled Logging Block Delete
☐	2	Umbrella HQ - IP Blocking	Enabled	Block	Any	Any IPs Any Ports	1 IP Any Ports	▲ 0/24hrs		
☐	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	...

360055232232

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。