

Aktivieren von Berichten bei der Aktivitätssuche nach über die Cloud bereitgestellten Firewalls

Inhalt

[Einleitung](#)

[Überblick](#)

[Lösung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Berichterstellung für Cloud-basierte Firewall-Richtlinien in Netzwerktunneln aktivieren.

Überblick

Standardmäßig ist die Berichterstellung für Umbrella Cloud-basierte Firewalls nicht aktiviert. Sie müssen die Funktion in jedem Netzwerktunnel manuell aktivieren, um Berichte für Firewall-Richtlinien zu erhalten, die über die Cloud bereitgestellt werden.

Lösung

So aktivieren Sie das Reporting auf dem Dashboard:

1. Navigieren Sie zu Richtlinien > Firewall.
2. Wählen Sie den Netzwerktunnel aus, um die Berichterstellung zu aktivieren.
3. Klicken Sie auf die drei Punkte auf der rechten Seite des ausgewählten Tunnels.
4. Schalten Sie den Switch für die Protokollierung um, um die Berichterstellung zu aktivieren.

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. Schalten Sie den Switch für die Protokollierung ein, um ihn zu aktivieren.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.