

Beheben Sie die Inaktivität des Netzwerk-Tunnels auf dem Umbrella Dashboard.

Inhalt

[Einleitung](#)

[Problem](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird die Fehlerbehebung bei Netzwerk-tunneln beschrieben, die im Umbrella Dashboard als inaktiv angezeigt werden.

Problem

Nach dem Hinzufügen von Netzwerk-Tunneln werden die Tunnel im Umbrella Dashboard als inaktiv angezeigt.

Fehlerbehebung

1. Aktivieren Sie die Protokollierung für die standardmäßige Cloud-Delivered Firewall (CDFW)-Richtlinie, um Netzwerk-tunnel zu aktivieren. Ihre Netzwerk-Tunnel werden nur dann als "aktiv" angezeigt, wenn die Protokollierung für die standardmäßige Cloud-Delivered Firewall (CDFW)-Richtlinie aktiviert ist:

Cisco Umbrella

Overview

Deployments

Policies

Management

DNS Policies

Firewall Policy

Web Policies

Policy Components

Destination Lists

Content Categories

Application Settings

Tenant Controls

Security Settings

Block Page Appearance

Integrations

Selective Decryption Lists

Reporting

Admin

Investigate

Demo User

dCloud Demo (cisco)

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

7 Total

☐	Priority	Name	Status	Action	Applications	Protocol	Source Criteria	Destination Criteria	Hit Count	Last Hit	
☐	1	Umbrella Branch - App Blocking	Enabled	Block	bittorrent bittorrent-networking 3 more	Any	Any IPs Any Ports	Any IPs Any Ports	0/24hrs	Jul 18, 2020 - 06:41pm	...
☐	2	Umbrella HQ - Port Blocking	Enabled	Block	Any Application	Any	Any IPs Any Ports	Any IPs 3 Ports	318.0 /24hrs	Jul 21, 2020 - 11:14pm	...
☐	3	Umbrella HQ - IP Blocking	Enabled	Block	Any Application	Any	Any IPs Any Ports	1 IP Any Ports	0/24hrs	Jun 29, 2020 - 06:10pm	...
☐	4	Allow Umbrella Resolvers	Enabled	Allow	Any Application	Any	Any IPs Any Ports	2 IPs Any Ports	25.2 k/24hrs	Jul 21, 2020 - 11:16pm	...
☐	5	Block SSH to SQL Server	Enabled	Block	Any Application	Any	Any IPs Any Ports	1 IP 1 Port	0/24hrs	No Hits	...
☐	6	Block High Ports	Enabled	Block	Any Application	Any	Any IPs Any Ports	Any IPs 1 Port	0/24hrs	No Hits	...
☐	7	Default Rule	Enabled	Allow	Any Application	Any	Any IPs Any Ports	Any IPs Any Ports	14.7 k/24hrs		...

Edit

Duplicate

Logging

Allow

360062629451

2. Wenn die Protokollierung aktiviert ist, führen Sie diesen Befehl auf dem Router aus, auf dem die Netzwerktunnel konfiguriert sind:

<#root>

show crypto ikev2 sa

Stellen Sie sicher, dass es sich bei der Quell-IP-Adresse um eine interne IP-Adresse aus dem Anwendernetzwerk gemäß RFC 1918 handelt. Überprüfen Sie Ihre Konfiguration gemäß diesem Leitfaden: [Network Tunnel Configuration](#). Wenn der Fehler weiterhin auftritt, erstellen Sie ein Ticket mit dem Befehl show crypto ikev2 sa sowie den CDFW-Protokollen an unser Support-Team.

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.