

Enable Reporting In Activity Search for Cloud-Delivered Firewall

Contents

[Introduction](#)

[Overview](#)

[Solution](#)

Introduction

This document describes how to enable reporting for Cloud-Delivered Firewall policies on network tunnels.

Overview

By default, reporting for Umbrella Cloud-Delivered Firewall is not enabled. You must manually enable the feature on each network tunnel to receive reports for Cloud-Delivered Firewall policies.

Solution

To enable reporting on the Dashboard:

1. Navigate to **Policies > Firewall**.
2. Select the network tunnel to enable reporting.
3. Click the three dots on the right-hand side of the selected tunnel.
4. Toggle the switch for **Logging** to enable reporting.

The screenshot shows the Cisco Umbrella dashboard for Firewall Policy management. The left sidebar contains the navigation menu with 'Policies' and 'Firewall Policy' highlighted. The main content area displays a table of firewall rules. The first rule, 'Umbrella HQ - Port Blocking', is selected, and its configuration details are shown on the right. The 'Logging' toggle is visible and enabled.

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 k/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. Toggle the switch for Logging to enable.

Cisco Umbrella

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	A Edit
☐	2 Umbrella HQ - IP Blocking	Enabled	Block	Any	Any IPs Any Ports	1 IP Any Ports	0/24hrs	A Duplicate Enabled
☐	3 Allow Umbrella Resolvers	Enabled	Allow	Any	Any IPs Any Ports	2 IPs Any Ports	30.5 k/24hrs	A Logging Block
☐	4 Block SSH to SQL Server	Enabled	Block	Any	Any IPs Any Ports	1 IP 1 Port	0/24hrs	A Delete
☐	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