

# 클라우드 제공 방화벽에 대한 활동 검색에서 보고 활성화

## 목차

---

[소개](#)

[개요](#)

[솔루션](#)

---

## 소개

이 문서에서는 네트워크 터널에서 클라우드 제공 방화벽 정책에 대한 보고를 활성화하는 방법에 대해 설명합니다.

## 개요

기본적으로 Umbrella Cloud-Delivered Firewall에 대한 보고는 활성화되지 않습니다. 클라우드 제공 방화벽 정책에 대한 보고서를 받으려면 각 네트워크 터널에서 기능을 수동으로 활성화해야 합니다.

## 솔루션

대시보드에서 보고를 활성화하려면

1. Policies(정책) > Firewall(방화벽)로 이동합니다.
2. 보고를 활성화하려면 네트워크 터널을 선택합니다.
3. 선택한 터널의 오른쪽에 있는 점 3개를 클릭합니다.
4. 보고를 활성화하려면 Logging(로깅) 스위치를 토글합니다.

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
<input checked="" type="checkbox"/>	1 Umbrella HQ - Port Blocking	Enabled	Block	Any	Any IPs Any Ports	Any IPs 3 Ports	663.0 /24hrs	Apr 23, 2020 - 02:21pm <b>3...</b>
<input type="checkbox"/>	2 Umbrella HQ - IP Blocking	Enabled	Block	Any	Any IPs Any Ports	1 IP Any Ports	▲ 0/24hrs	Apr 09, 2020 - 12:10am ...
<input type="checkbox"/>	3 Allow Umbrella Resolvers	Enabled	Allow	Any	Any IPs Any Ports	2 IPs Any Ports	30.5 k/24hrs	Apr 23, 2020 - 02:21pm ...
<input type="checkbox"/>	4 Block SSH to SQL Server	Enabled	Block	Any	Any IPs Any Ports	1 IP 1 Port	▲ 0/24hrs	▲ No Hits ...
<input type="checkbox"/>	5 Block High Ports	Enabled	Block	Any	Any IPs Any Ports	Any IPs 1 Port	▲ 0/24hrs	▲ No Hits ...
<input type="checkbox"/>	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. Logging(로깅) 스위치를 활성화하려면 전환합니다.

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
<input checked="" type="checkbox"/>	1 Umbrella HQ - Port Blocking	Enabled	Block	Any	Any IPs Any Ports	Any IPs 3 Ports	663.0 /24hrs	<div style="border: 1px solid #ccc; padding: 2px;">             Edit              Duplicate              Enabled <input type="checkbox"/>  <b>Logging</b> <input checked="" type="checkbox"/>              Block <input type="checkbox"/>              Delete           </div>
<input type="checkbox"/>	2 Umbrella HQ - IP Blocking	Enabled	Block	Any	Any IPs Any Ports	1 IP Any Ports	▲ 0/24hrs	
<input type="checkbox"/>	3 Allow Umbrella Resolvers	Enabled	Allow	Any	Any IPs Any Ports	2 IPs Any Ports	30.5 k/24hrs	
<input type="checkbox"/>	4 Block SSH to SQL Server	Enabled	Block	Any	Any IPs Any Ports	1 IP 1 Port	▲ 0/24hrs	▲ No Hits ...
<input type="checkbox"/>	5 Block High Ports	Enabled	Block	Any	Any IPs Any Ports	Any IPs 1 Port	▲ 0/24hrs	▲ No Hits ...
<input type="checkbox"/>	6 Default Rule	Enabled	Allow	Any	Any IPs Any Ports	Any IPs Any Ports	11.9 k/24hrs	Apr 23, 2020 - 02:21pm ...

360055232232

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.