

FMC GUI에서 Unified Event Viewer를 사용하여 이벤트 모니터링

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[탐색](#)

[Unified Event 페이지의 예](#)

[이벤트 검토](#)

[열 맞춤 설정](#)

[열 세트 저장](#)

[이벤트 검색](#)

[검색 저장](#)

[타임 윈도우](#)

[라이브](#)

[CSV\(선택표로 구분된 값\)로 이벤트 다운로드](#)

[관련 정보](#)

소개

이 문서에서는 FMC(Firewall Management Center)의 GUI(그래픽 사용자 인터페이스)에서 Unified Event Viewer를 사용하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 관리자 또는 보안 분석가 권한으로 FMC에 액세스
- 버전 v7.0 이상의 FMC

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Secure Firewall Management Center for VMware v7.2.5

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

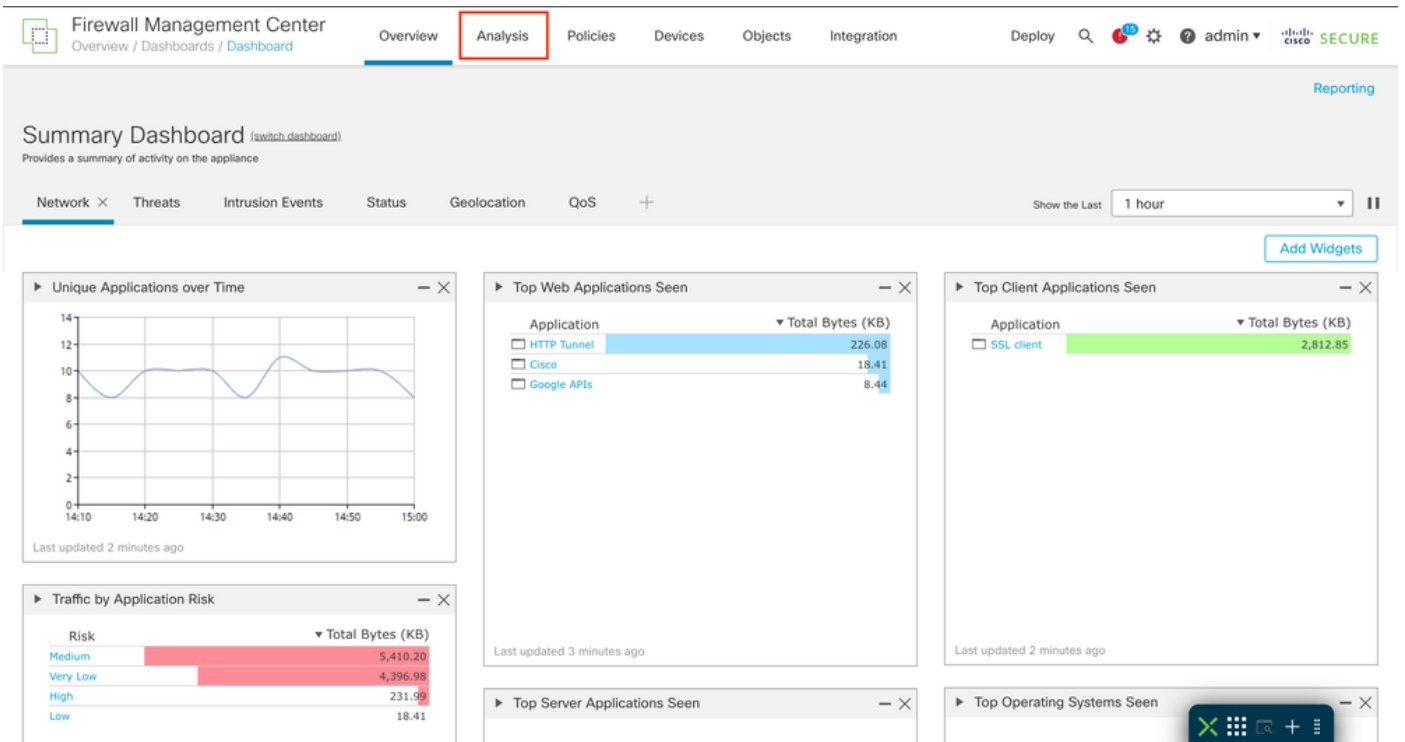
명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

탐색

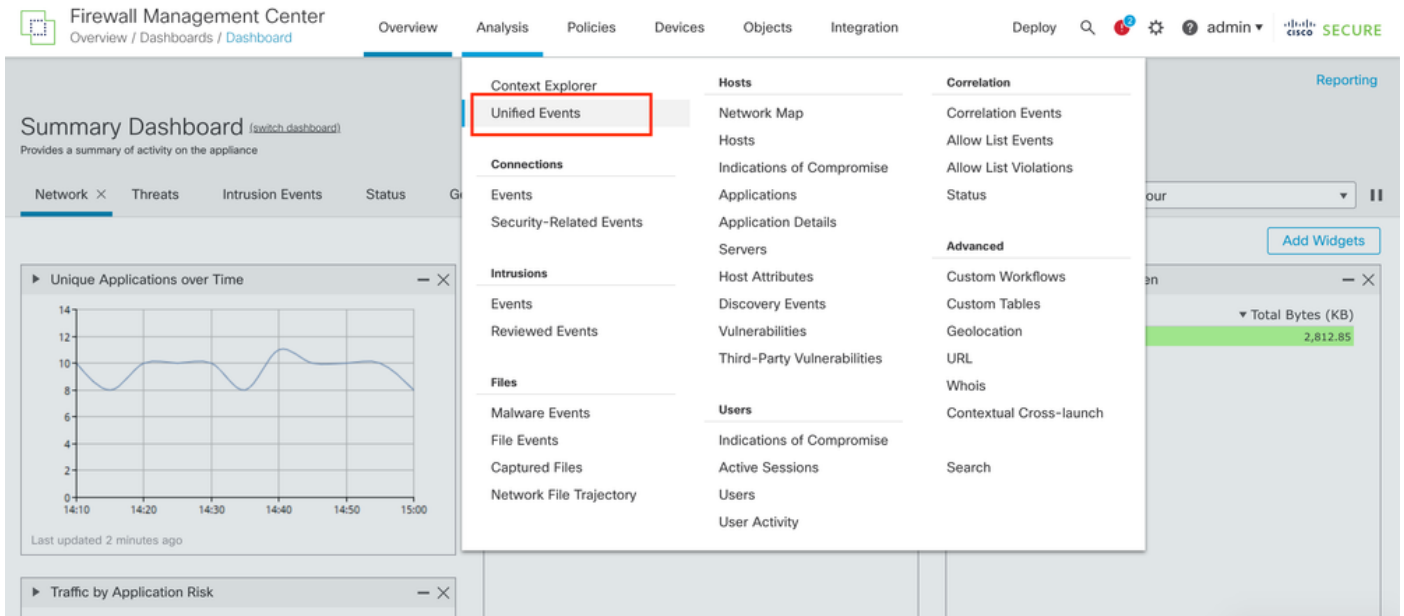
1단계. FMC GUI에 로그인합니다.



2단계. 분석 탭으로 이동합니다.



3단계. 드롭다운 메뉴에서 Unified Events를 클릭합니다.



Unified Event 페이지의 예

Firewall Management Center
Analysis / Unified Events

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

이벤트 검토

1단계. > 아이콘을 클릭합니다.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Select...

Refresh

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h

Go Live

	Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
>	2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
>	2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
>	2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
>	2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
>	2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

2단계. 이벤트의 세부 정보가 표시됩니다.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

SECURE

Select...

Refresh

Showing 10,000 events (of 10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h

Go Live

	Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
>	2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow

Event Type: Connection

Time: 2023-10-04 16:11:29

Last Packet: 2023-10-04 16:11:39

Action: Allow

Source IP: 10.18.19.111

Source User: Not Found

Destination IP: 10.1.8.107

Ingress Security Zone: inside

Egress Security Zone: outside

Source Port / ICMP Type: 55046 / udp

Destination Port / ICMP Code: 53 (domain) / udp

Client Application: DNS

Business Relevance: Very High

DNS Query: cloud-sa.amp.cisco.com

DNS Response: No Error

DNS Record Type: A

Intrusion Events: 0

Files: 0

Access Control Policy: t

Access Control Rule: allow

Network Analysis Policy: Balanced Security and Connectivity

Prefilter Policy: allow

QoS Policy: test

Domain: Global

Ingress Virtual Router: Global

Egress Virtual Router: Global

Initiator Packets: 2

Responder Packets: 0

QoS-Dropped Initiator Packets: 0

QoS-Dropped Responder Packets: 0

Initiator Bytes: 164

Responder Bytes: 0

QoS-Dropped Initiator Bytes: 0

QoS-Dropped Responder Bytes: 0

Detection Type: ApplD

NAT Source IP: 10.88.243.43

>	2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
>	2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
>	2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow

열 맞춤 설정

1단계. 아이콘을 클릭합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | CISCO SECURE

Q Select... Refresh

Showing 10,000 events (10,000) of tens of thousands 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

2단계. 테이블에서 원하는 이벤트 필드를 선택합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | CISCO SECURE

Q Select... Refresh

Showing 10,000 events (10,000) of tens of thousands 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Ac
		OW		10.18.19.111	10.1.8.107	55046 / udp	53 (domain) / udp	
		OW		10.18.19.105	10.1.20.51	44563 / udp	53 (domain) / udp	
		OW		10.18.19.166	142.250.72.202	53436 / tcp	443 (https) / tcp	
		OW		10.18.19.166	142.250.72.202	53437 / tcp	443 (https) / tcp	
		OW		10.18.19.105	10.27.20.51	57541 / udp	53 (domain) / udp	
		OW		10.18.19.105	10.1.20.51	42318 / udp	53 (domain) / udp	
		OW		10.18.19.110	10.1.9.38	38758 / udp	53 (domain) / udp	
		OW		10.18.19.110	10.1.8.101	53922 / udp	53 (domain) / udp	
		OW		10.18.19.105	10.27.20.51	52776 / udp	53 (domain) / udp	
		OW		10.18.19.32	208.67.220.220	39366 / udp	53 (domain) / udp	
		OW		10.18.19.111	10.1.8.101	47616 / udp	53 (domain) / udp	
		OW		10.18.19.41	208.67.220.220	54037 / udp	53 (domain) / udp	
		OW		10.18.19.230	173.37.87.157	60602 / udp	53 (domain) / udp	
		OW		10.18.19.230	173.37.87.157	59309 / udp	53 (domain) / udp	
		OW		10.18.19.111	10.1.8.101	39941 / udp	53 (domain) / udp	

Saved Column Sets

Select...

Filter columns

Select none Select default

- ☒ Event Type
- ☒ Action
- ☒ Reason
- ☒ Source IP
- ☒ Destination IP
- ☒ Source Port / ICMP Type
- ☒ Destination Port / ICMP Code

Revert 11 selected Apply

3단계. (선택 사항) 더 쉽게 탐색할 수 있도록 필드를 검색합니다.

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

☒	Source IP	
☒	Source Port / ICMP Type	
☐	NAT Source IP	
☐	NAT Source Port	
☐	NetFlow Source Autonomous System	

Revert 7 selected Apply

4단계. 비활성화하거나 활성화하려면 이벤트 필드를 클릭합니다.

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

☒	Source IP	
☐	Source Port / ICMP Type	
☐	NAT Source IP	
☐	NAT Source Port	
☐	NetFlow Source Autonomous System	

Revert 6 selected Apply

5단계. Apply(적용)를 클릭합니다.

Saved Column Sets

Select...

Filter columns

Select none

Select default

☒ Event Type

↔

🔍

🔖

🗑️

🔗

☒ Action

↔

🔍

🔖

🗑️

🔗

☒ Destination Port / ICMP Code

↔

🔍

🔖

🗑️

🔗

☒ Source IP

↔

🔍

🔖

🗑️

🔗

☒ Device

↔

🔍

🔖

🗑️

🔗

Revert

6 selected

Apply

6단계(선택 사항) 각 열을 다른 위치로 끌어 열 위치를 변경할 수 있습니다.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

Go Live

Select...

Refresh

Showing 10,000 events (10,000) of tens of thousands

2023-10-05 12:02:15 EDT → 2023-10-05 13:02:15 EDT 1h

Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Source IP	Device	Access Control Rule
2023-10-05 13:02:15	Connection	Allow	53 (domain) / udp	10.18.1	GW	allow
2023-10-05 13:02:15	Connection	Allow	53 (domain) / udp	10.18.19.110	GW	allow
2023-10-05 13:02:15	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:15	Connection	Allow	53 (domain) / udp	10.18.19.32	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.105	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.111	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.111	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:14	Connection	Allow	53 (domain) / udp	10.18.19.105	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.230	GW	allow
2023-10-05 13:02:14	Connection	Allow	443 (https) / tcp	10.18.19.166	GW	allow
2023-10-05 13:02:13	Connection	Allow	53 (domain) / udp	10.18.19.110	GW	allow
2023-10-05 13:02:13	Connection	Allow	53 (domain) / udp	10.18.19.230	GW	allow
2023-10-05 13:02:13	Connection	Allow	443 (https) / tcp	10.18.19.166	GW	allow
2023-10-05 13:02:13	Connection	Allow	443 (https) / tcp	10.18.19.166	GW	allow

열 세트 저장

1단계. Saved Column Sets(저장된 열 세트)를 클릭합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ admin | cisco SECURE

Q Select... Refresh

Showing 10,000 events (10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Ap
		OW		10.18.19.111	10.1.8.107	55046 / udp	53 (domain) / ud	
		OW		10.18.19.105	10.1.20.51	44563 / udp	53 (domain) / ud	
		OW		10.18.19.166	142.250.72.202	53436 / tcp	443 (https) / tcp	
		OW		10.18.19.166	142.250.72.202	53437 / tcp	443 (https) / tcp	
		OW		10.18.19.105	10.27.20.51	57541 / udp	53 (domain) / ud	
		OW		10.18.19.105	10.1.20.51	42318 / udp	53 (domain) / ud	
		OW		10.18.19.110	10.1.9.38	38758 / udp	53 (domain) / ud	
		OW		10.18.19.110	10.1.8.101	53922 / udp	53 (domain) / ud	
		OW		10.18.19.105	10.27.20.51	52776 / udp	53 (domain) / ud	
		OW		10.18.19.32	208.67.220.220	39366 / udp	53 (domain) / ud	
		OW		10.18.19.111	10.1.8.101	47616 / udp	53 (domain) / ud	
		OW		10.18.19.41	208.67.220.220	54037 / udp	53 (domain) / ud	
		OW		10.18.19.230	173.37.87.157	60602 / udp	53 (domain) / ud	
		OW		10.18.19.230	173.37.87.157	59309 / udp	53 (domain) / ud	
		OW		10.18.19.111	10.1.8.101	39941 / udp	53 (domain) / ud	

Filter columns

Select none Select default

Event Type Action Reason Source IP Destination IP Source Port / ICMP Type Destination Port / ICMP Code

Revert 11 selected Apply

2단계. 현재 선택에서 열 세트 생성을 클릭합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ admin | cisco SECURE

Q Select... Refresh

Showing 10,000 events (10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination IP	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
		OW	10.1.8.107	53 (domain) / ud	GW	10.18.19.111	55046 / udp	allow
		OW	10.1.20.51	53 (domain) / ud	GW	10.18.19.105	44563 / udp	allow
		OW	142.250.72.202	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
		OW	142.250.72.202	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
		OW	10.27.20.51	53 (domain) / ud	GW	10.18.19.105	57541 / udp	allow
		OW	10.1.20.51	53 (domain) / ud	GW	10.18.19.105	42318 / udp	allow
		OW	10.1.9.38	53 (domain) / ud	GW	10.18.19.110	38758 / udp	allow
		OW	10.1.8.101	53 (domain) / ud	GW	10.18.19.110	53922 / udp	allow
		OW	10.27.20.51	53 (domain) / ud	GW	10.18.19.105	52776 / udp	allow
		OW	208.67.220.220	53 (domain) / ud	GW	10.18.19.32	39366 / udp	allow
		OW	10.1.8.101	53 (domain) / ud	GW	10.18.19.111	47616 / udp	allow
		OW	208.67.220.220	53 (domain) / ud	GW	10.18.19.41	54037 / udp	allow
		OW	173.37.87.157	53 (domain) / ud	GW	10.18.19.230	60602 / udp	allow
		OW	173.37.87.157	53 (domain) / ud	GW	10.18.19.230	59309 / udp	allow
		OW	10.1.8.101	53 (domain) / ud	GW	10.18.19.111	39941 / udp	allow
		OW	108.156.211.71	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow

Filter columns

Select none Select default

Rule match

2 saved column sets

Rule match

Time Event Type Action Reason Source IP Destination IP

Saved Column Set 1

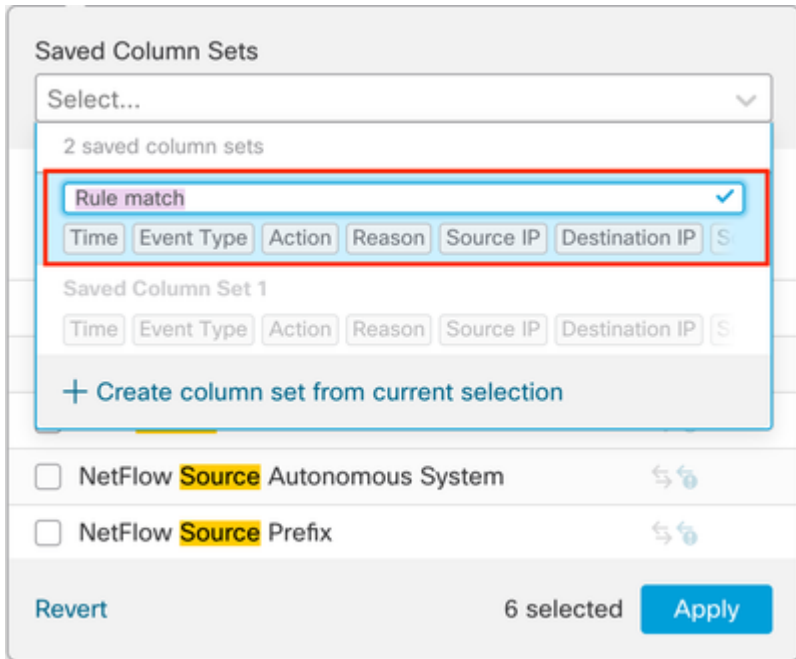
Time Event Type Action Reason Source IP Destination IP

+ Create column set from current selection

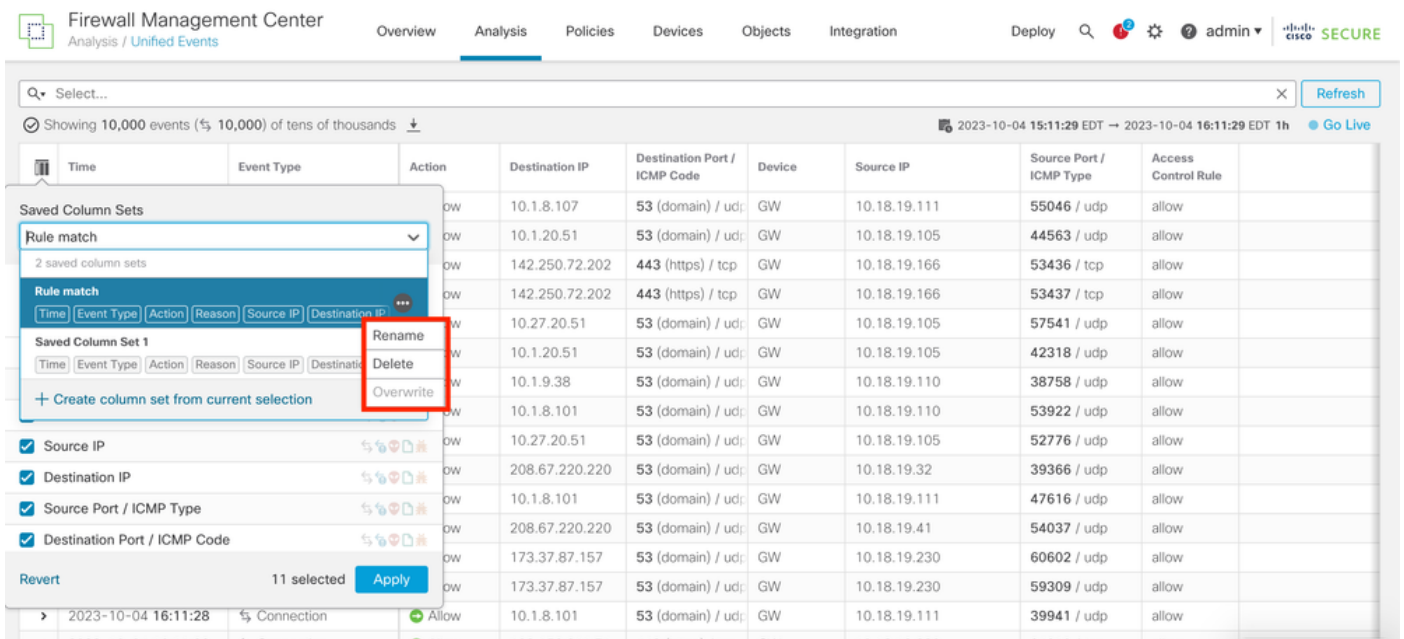
Source IP Destination IP Source Port / ICMP Type Destination Port / ICMP Code

Revert 11 selected Apply

3단계. (선택사항) 열 세트의 이름을 변경합니다.



4단계. 생략 부호(...)를 클릭하여 기존 집합을 편집할 수 있습니다.



이벤트 검색

1단계. 특정 이벤트 검색을 시작하려면 Select(선택)를 클릭합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Q Select... Refresh

Showing 10,000 events (of 10,000) of tens of thousands 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

	Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
>	2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
>	2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
>	2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
>	2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
>	2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

2단계. 필터를 적용할 필드를 선택합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

Q source Refresh

Showing 10,000 events (of 10,000) of tens of thousands 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

	Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
>	2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
>	2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
>	2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

3단계. 필터로 사용할 값을 작성합니다.

Q Source IP X Select...

4단계. Apply(적용)를 클릭하여 필터를 구성합니다.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔒

SECURE

🔍

Source IP 10.18.19.105

×

Select...

×

Apply

Cancel

🕒

Showing all 144 events (📄 144)

📅

2023-10-06 12:31:58 EDT → 2023-10-06 13:31:58 EDT 1h

Go Live

5단계. (선택 사항) 각 필터에 여러 값을 추가할 수 있습니다.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔒

SECURE

🔍

Source IP 10.18.19.111

×

10.18.19.105

×

Select...

×

Refresh

🕒

Showing 150 events (📄 150)

📅

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h

Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:27	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	46739 / udp	allow
2023-10-04 16:11:27	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	56045 / udp	allow
2023-10-04 16:11:27	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	43523 / udp	allow
2023-10-04 16:11:27	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	46938 / udp	allow
2023-10-04 16:11:26	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	41931 / udp	allow
2023-10-04 16:11:26	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.111	42734 / udp	allow
2023-10-04 16:11:25	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	54464 / udp	allow
2023-10-04 16:11:25	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	45681 / udp	allow
2023-10-04 16:11:25	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	50585 / udp	allow
2023-10-04 16:11:25	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	48789 / udp	allow
2023-10-04 16:11:24	🔗 Connection	🟢 Allow	53 (domain) / udp	GW	10.18.19.105	45203 / udp	allow

6단계. (선택 사항) 필요한 만큼 필터를 추가합니다.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔒

SECURE

🔍

Source IP 10.18.19.111

×

10.18.19.105

×

Destination Port / ICMP Code 8910

×

Select...

×

Refresh

🕒

Showing all 106 events (📄 106)

📅

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h

Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50786 / tcp	allow
2023-10-04 16:10:51	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45442 / tcp	allow
2023-10-04 16:10:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50784 / tcp	allow
2023-10-04 16:10:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45440 / tcp	allow
2023-10-04 16:09:21	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50782 / tcp	allow
2023-10-04 16:09:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45438 / tcp	allow
2023-10-04 16:08:31	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50780 / tcp	allow
2023-10-04 16:08:21	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45436 / tcp	allow
2023-10-04 16:07:41	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50778 / tcp	allow
2023-10-04 16:07:31	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45434 / tcp	allow
2023-10-04 16:06:51	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50776 / tcp	allow
2023-10-04 16:06:41	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45432 / tcp	allow
2023-10-04 16:06:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50774 / tcp	allow
2023-10-04 16:05:51	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45430 / tcp	allow
2023-10-04 16:05:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50772 / tcp	allow
2023-10-04 16:05:01	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45428 / tcp	allow
2023-10-04 16:04:21	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	50770 / tcp	allow
2023-10-04 16:04:11	🔗 Connection	🟢 Allow	8910 / tcp	GW	10.18.19.105	45426 / tcp	allow



팁: 값을 쓰는 동안 연산자(>, <, ! 등)를 사용할 수 있습니다.

검색 저장

생성한 필터를 다시 사용할 수 있도록 검색을 저장할 수 있습니다.

1단계. 돋보기 아이콘을 클릭합니다.

The screenshot shows the Firewall Management Center interface. At the top, there are tabs for Overview, Analysis, Policies, Devices, Objects, and Integration. The Analysis tab is selected. Below the tabs, there is a search bar with a magnifying glass icon highlighted by a red box. The search bar contains the text "Destination Port / ICMP Code 8910" and "Source IP 10.18.19.111 x 10.18.19.105 x". To the right of the search bar is a "Refresh" button. Below the search bar, there is a "Saved searches" panel on the left and a table of search results on the right. The "Saved searches" panel shows "0 saved searches" and a "+ Save search" button. The table of search results has columns for Source IP, Device, and Access Control Rule. The table contains 15 rows of data.

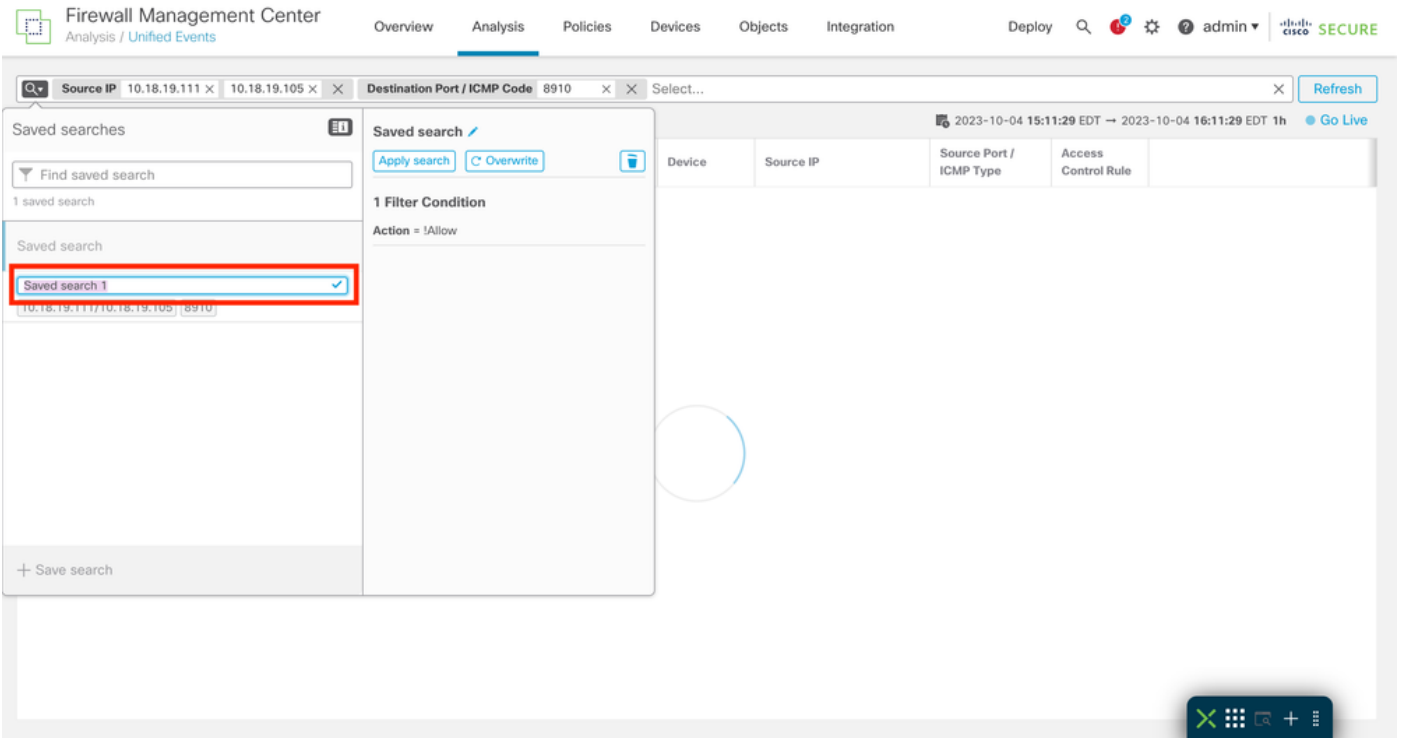
Source IP	Device	Access Control Rule
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow

2단계. 검색 저장을 클릭합니다.

The screenshot shows the Firewall Management Center interface, similar to the previous one. The "+ Save search" button in the "Saved searches" panel is highlighted by a red box. The table of search results is the same as in the previous screenshot.

Source IP	Device	Access Control Rule
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow

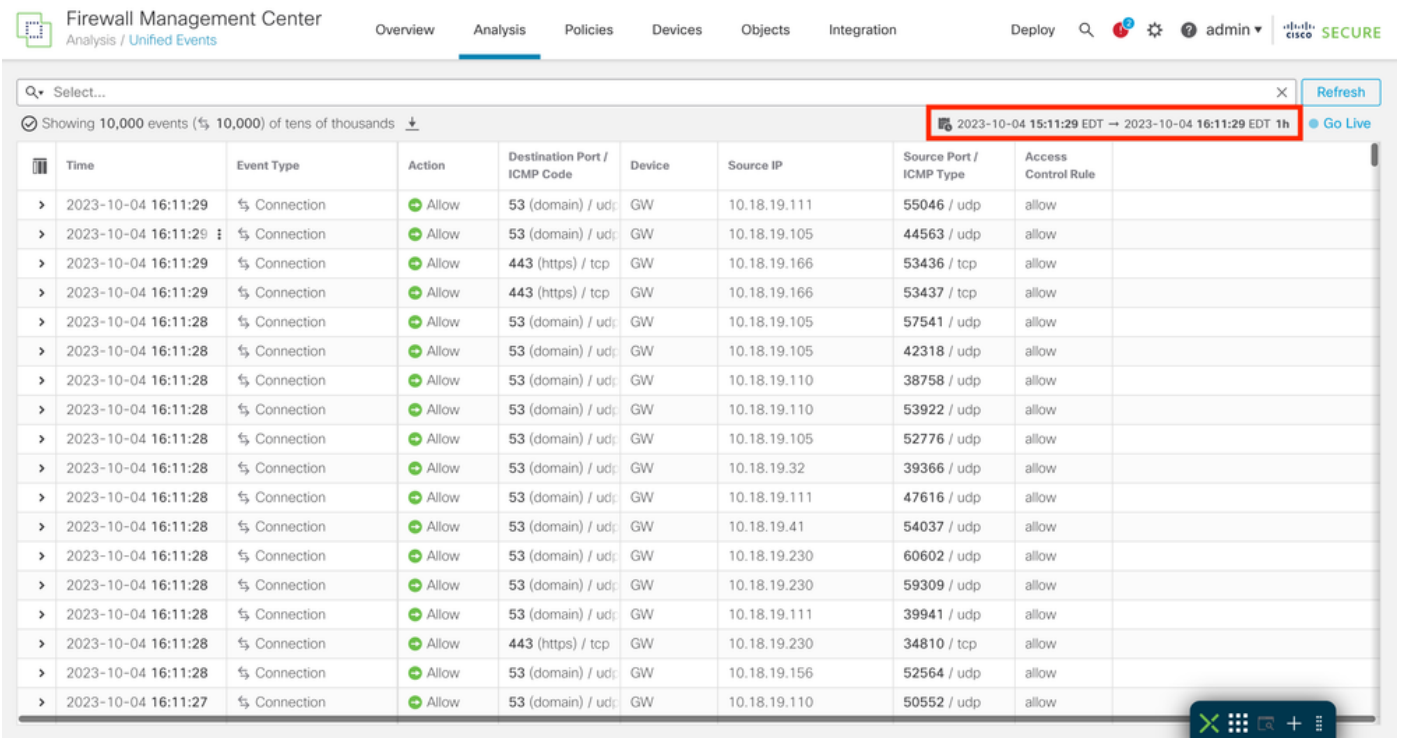
3단계. (선택 사항) 검색의 이름을 변경합니다.



타임 윈도우

타임 윈도우를 수정하여 특정 시간을 기준으로 관련 이벤트를 좁히는 것이 더 쉽습니다.

1단계. 이벤트의 창 프레임을 수정하려면 날짜 범위를 클릭합니다.



2단계. 팝업 창에서 시간 범위를 선택합니다.

[illegible]

3단계. (선택 사항) 슬라이딩 시간 범위를 사용하여 특정 시간부터 현재 시간까지의 이벤트를 표시합니다.

Fixed Time Range Sliding Time Range

Show the last

1

hour

second

minute

hour

day

week

month

Apply

18.19.110	allow
18.19.110	allow

4단계. 구성된 시간 범위에서 이벤트를 필터링하려면 Apply(적용)를 클릭합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ admin 🔒 cisco SECURE

Q Select... Refresh

Showing 8,317 events (8,317) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow

Fixed Time Range Sliding Time Range

Show the last 6 hours

Select last: 5 minutes, 1 hour, 6 hours, 1 day, 2 weeks, 1 month

Apply

라이브

Go Live 기능을 활성화하여 실시간으로 이벤트를 표시할 수 있습니다. 이벤트는 생성된 대로 표시 됩니다.

활성화하려면 Go Live를 클릭합니다.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ ⓘ admin 🔒 cisco SECURE

Q Select... Refresh

Showing 10,000 events (10,000) of tens of thousands

2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	Connection	Allow	443 (https) / tcp	GW	10.18.19.230	34810 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52564 / udp	allow
2023-10-04 16:11:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	50552 / udp	allow

Go Live

활성화된 후에는 Live라는 단어가 표시됩니다.

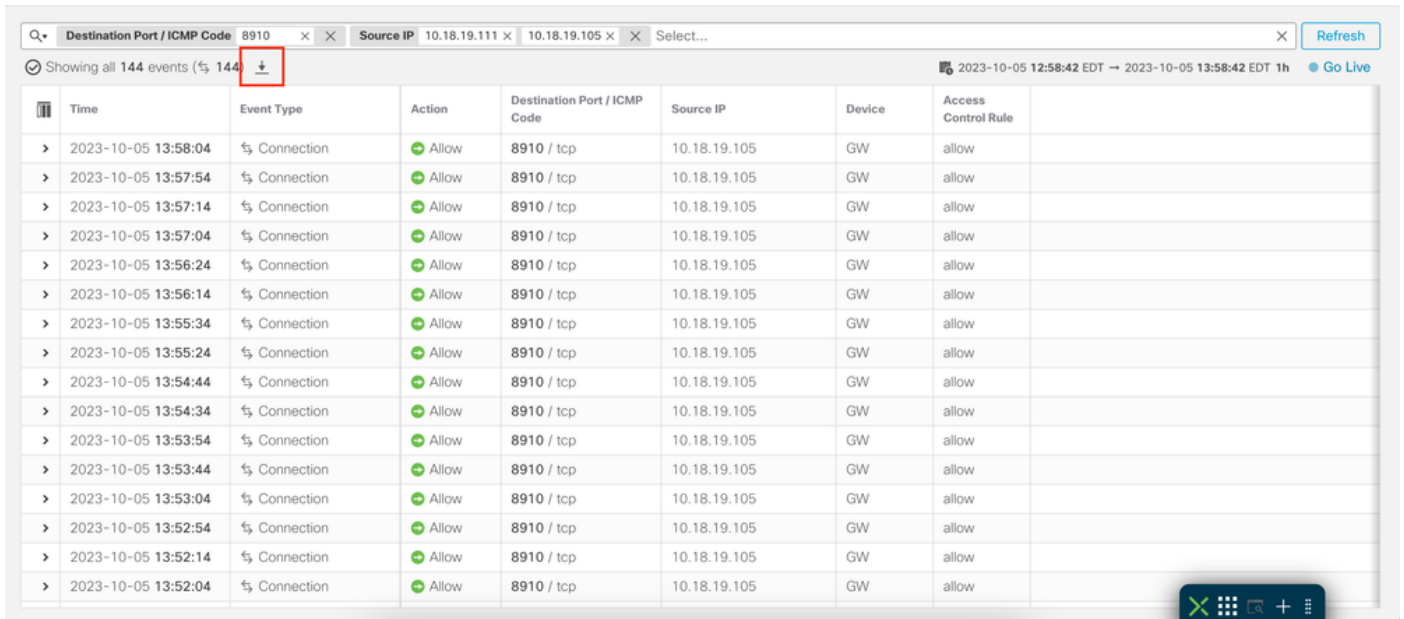
2023-10-05 21:55:25 EDT → 2023-10-05 21:56:04 EDT 39s Live



주의: Live가 활성화된 경우 타임 윈도우를 수정할 수 없습니다. 타임 윈도우를 수정하려면 먼저 라이브 옵션을 다시 클릭하여 비활성화하십시오.

이벤트 다운로드 형식 쉼표로 구분된 값(CSV)

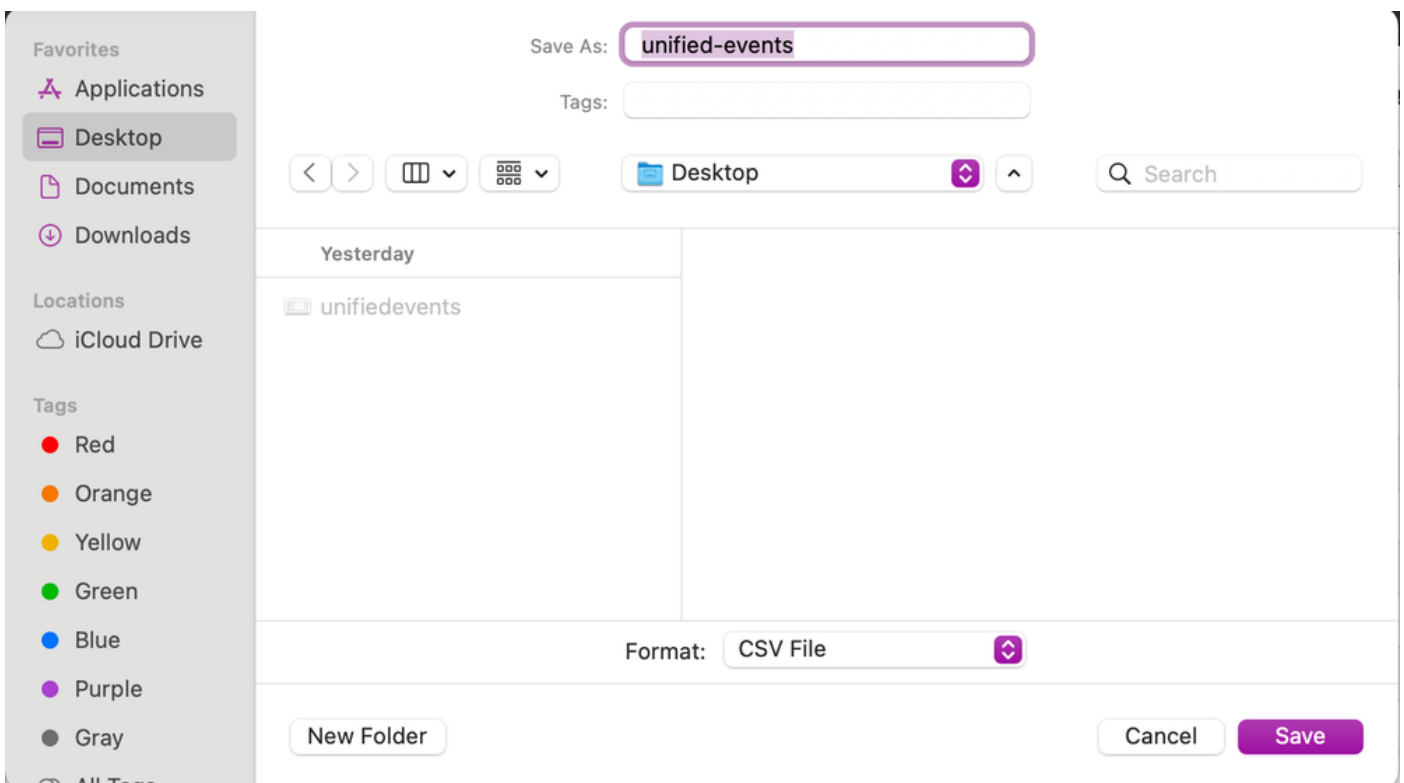
1단계. 다운로드 아이콘을 클릭하여 페이지에 현재 표시된 이벤트를 포함하는 파일을 생성합니다.



The screenshot shows a web interface for viewing event logs. At the top, there are filters for 'Destination Port / ICMP Code' (8910) and 'Source IP' (10.18.19.111, 10.18.19.105). A 'Refresh' button is on the right. Below the filters, it says 'Showing all 144 events (1/144)' and a download icon (a square with a downward arrow) is highlighted with a red box. The main area is a table with columns: Time, Event Type, Action, Destination Port / ICMP Code, Source IP, Device, and Access Control Rule. The table contains 14 rows of data, all showing 'Connection' events with 'Allow' actions. At the bottom right, there is a 'Go Live' button.

Time	Event Type	Action	Destination Port / ICMP Code	Source IP	Device	Access Control Rule
2023-10-05 13:58:04	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:57:54	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:57:14	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:57:04	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:56:24	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:56:14	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:55:34	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:55:24	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:54:44	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:54:34	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:53:54	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:53:44	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:53:04	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:52:54	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:52:14	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow
2023-10-05 13:52:04	Connection	Allow	8910 / tcp	10.18.19.105	GW	allow

2단계. 다운로드 폴더와 이름을 선택하고 저장을 클릭합니다.



The screenshot shows a file save dialog. On the left is a sidebar with 'Favorites' (Applications, Desktop, Documents, Downloads) and 'Locations' (iCloud Drive). Below that are 'Tags' (Red, Orange, Yellow, Green, Blue, Purple, Gray, All Tags). The main area has 'Save As:' with the text 'unified-events' in a purple box. Below it is a 'Tags:' field. There are navigation buttons (back, forward, list, grid) and a 'Desktop' button. A search bar is on the right. Below the search bar is a section for 'Yesterday' with a folder icon and the name 'unifiedevents'. At the bottom, there is a 'Format:' dropdown set to 'CSV File'. At the very bottom are 'New Folder', 'Cancel', and 'Save' buttons.

Save As: unified-events

Tags:

Desktop

Yesterday

unifiedevents

Format: CSV File

New Folder Cancel Save

3단계. CSV 파일을 확인합니다.

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	37412 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	54766 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.166	54279 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	55185 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	46312 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	36785 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	57394 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	57395 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	38278 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44865 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	58387 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	49873 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	51060 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	34103 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.31	60020 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	43410 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47406 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	43359 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	43336 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	42658 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52923 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	46485 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.201	52178 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55864 / udp	allow

관련 정보

- [Unified Event Viewer 작업](#)
- [Cisco Secure Firewall - Unified Events Viewer: 팁과 요령](#)
- [Cisco 기술 지원 및 다운로드](#)

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.

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.