

# 在FMC GUI上使用統一事件檢視器監控事件

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[探索](#)

[統一事件頁面示例](#)

[審閱事件](#)

[個人化列](#)

[儲存列集](#)

[事件搜尋](#)

[儲存搜尋](#)

[時間段](#)

[啟用](#)

[以逗號分隔值\(CSV\)格式下載事件](#)

[相關資訊](#)

---

## 簡介

本文檔介紹如何在防火牆管理中心(FMC)的圖形使用者介面(GUI)上使用統一事件檢視器。

## 必要條件

### 需求

思科建議您瞭解以下主題：

- 使用管理員或安全分析師許可權訪問FMC
- FMC的版本等於或高於v7.0

### 採用元件

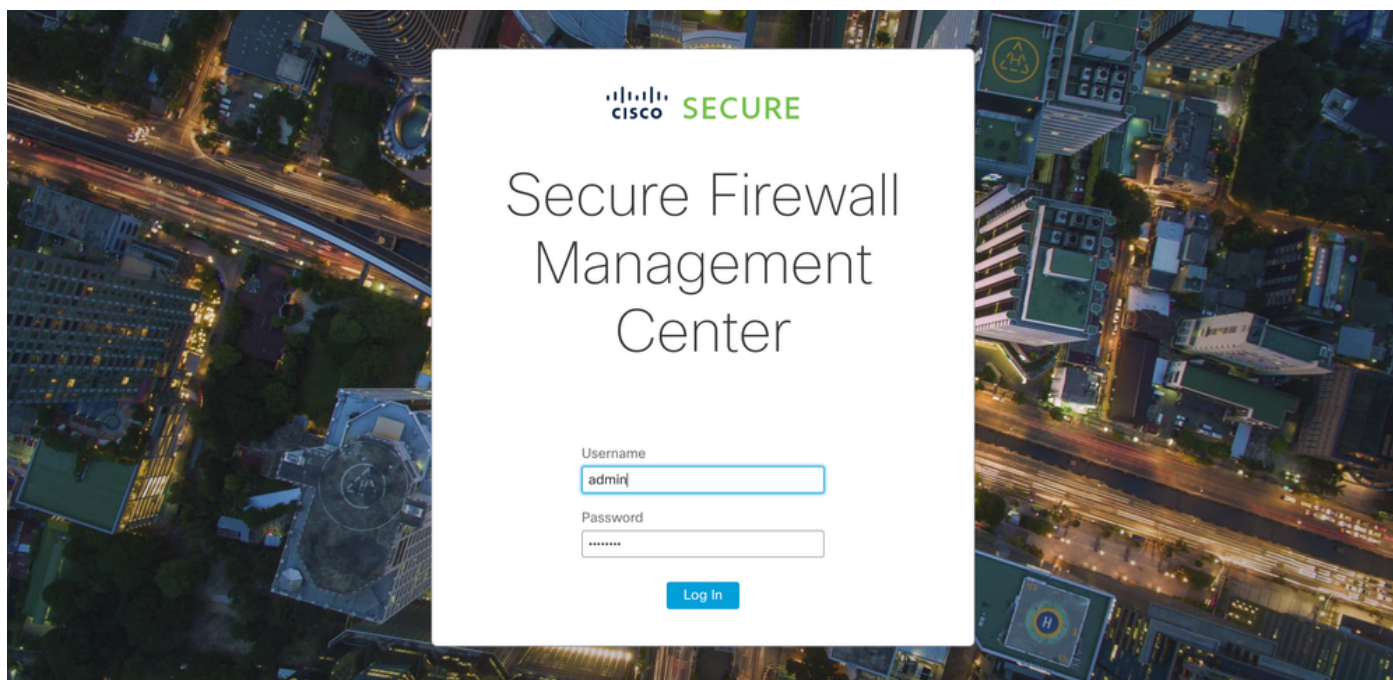
本文中的資訊係根據以下軟體和硬體版本：

- 適用於VMware v7.2.5的安全防火牆管理中心

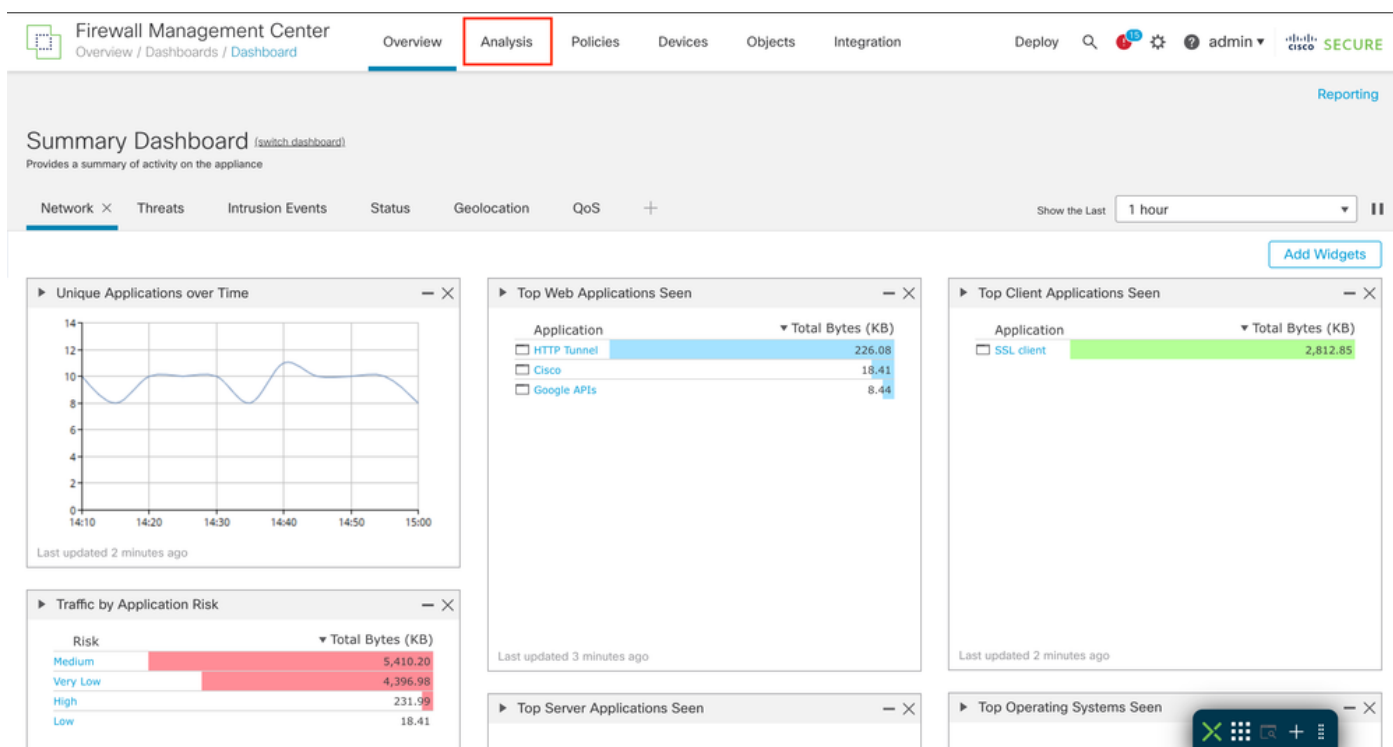
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

## 探索

步驟1.登入FMC GUI。



步驟2.定位至Analysis標籤。



步驟3.從下拉選單中，按一下Unified Events。

Firewall Management Center  
Overview / Dashboards / Dashboard

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

### Summary Dashboard (switch dashboard)

Provides a summary of activity on the appliance

Network × Threats Intrusion Events Status G

► Unique Applications over Time — ×

Last updated 2 minutes ago

► Traffic by Application Risk — ×

Context Explorer

Unified Events

Connections

Events

Security-Related Events

Intrusions

Events

Reviewed Events

Files

Malware Events

File Events

Captured Files

Network File Trajectory

Hosts

Network Map

Hosts

Indications of Compromise

Applications

Application Details

Servers

Host Attributes

Discovery Events

Vulnerabilities

Third-Party Vulnerabilities

Users

Indications of Compromise

Active Sessions

Users

User Activity

Correlation

Correlation Events

Allow List Events

Allow List Violations

Status

Advanced

Custom Workflows

Custom Tables

Geolocation

URL

Whois

Contextual Cross-launch

Search

Reporting

our

Add Widgets

en

▼ Total Bytes (KB)

2,812.85

## 統一事件頁面示例

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               |

## 審閱事件

步驟1. 按一下> 圖示。

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               |

步驟2.顯示事件的詳細資訊。

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: ApplID

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 |

## 個人化列

步驟1.按一下圖示

Firewall Management Center  
Analysis / Unified Events

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

步驟2.選擇您要在表上的事件欄位。

Firewall Management Center  
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | **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 | Reason | Source IP    | Destination IP | Source Port / ICMP Type | Destination Port / ICMP Code | Web App |
|---------------------|------------|--------|--------|--------------|----------------|-------------------------|------------------------------|---------|
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.111 | 10.1.8.107     | 55046 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.105 | 10.1.20.51     | 44563 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.166 | 142.250.72.202 | 53436 / tcp             | 443 (https) / tcp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.166 | 142.250.72.202 | 53437 / tcp             | 443 (https) / tcp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.105 | 10.27.20.51    | 57541 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.105 | 10.1.20.51     | 42318 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.110 | 10.1.9.38      | 38758 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.110 | 10.1.8.101     | 53922 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.105 | 10.27.20.51    | 52776 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.32  | 208.67.220.220 | 39366 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.111 | 10.1.8.101     | 47616 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.41  | 208.67.220.220 | 54037 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.230 | 173.37.87.157  | 60602 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 10.18.19.230 | 173.37.87.157  | 59309 / udp             | 53 (domain) / udp            |         |
| 2023-10-04 16:11:28 | Connection | Allow  |        | 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

步驟3. ( 可選 ) 搜尋欄位以簡化導覽。

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

|                                     |                                  |  |
|-------------------------------------|----------------------------------|--|
| <input checked="" type="checkbox"/> | Source IP                        |  |
| <input checked="" type="checkbox"/> | Source Port / ICMP Type          |  |
| <input type="checkbox"/>            | NAT Source IP                    |  |
| <input type="checkbox"/>            | NAT Source Port                  |  |
| <input type="checkbox"/>            | NetFlow Source Autonomous System |  |

Revert 7 selected Apply

步驟4.按一下事件欄位以禁用或啟用。

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

|                                     |                                  |  |
|-------------------------------------|----------------------------------|--|
| <input checked="" type="checkbox"/> | Source IP                        |  |
| <input type="checkbox"/>            | Source Port / ICMP Type          |  |
| <input type="checkbox"/>            | NAT Source IP                    |  |
| <input type="checkbox"/>            | NAT Source Port                  |  |
| <input type="checkbox"/>            | NetFlow Source Autonomous System |  |

Revert 6 selected Apply

步驟5.按一下Apply。

Saved Column Sets

Select...

Filter columns

Select none | Select default

☒ Event Type

☒ Action

☒ Destination Port / ICMP Code

☒ Source IP

☒ Device

Revert

6 selected

Apply

步驟6. ( 可選 ) 您可以將每個列拖動到不同的位置，以重新定位列。

Firewall Management Center

Analysis / Unified Events

Overview | Analysis | Policies | Devices | Objects | Integration

Deploy | admin

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

Go Live

Select...

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

Refresh

| 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               |

## 儲存列集

步驟1. 按一下 Saved Column Sets。

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 | 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

步驟2. 按一下Create column set from current selection。

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 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

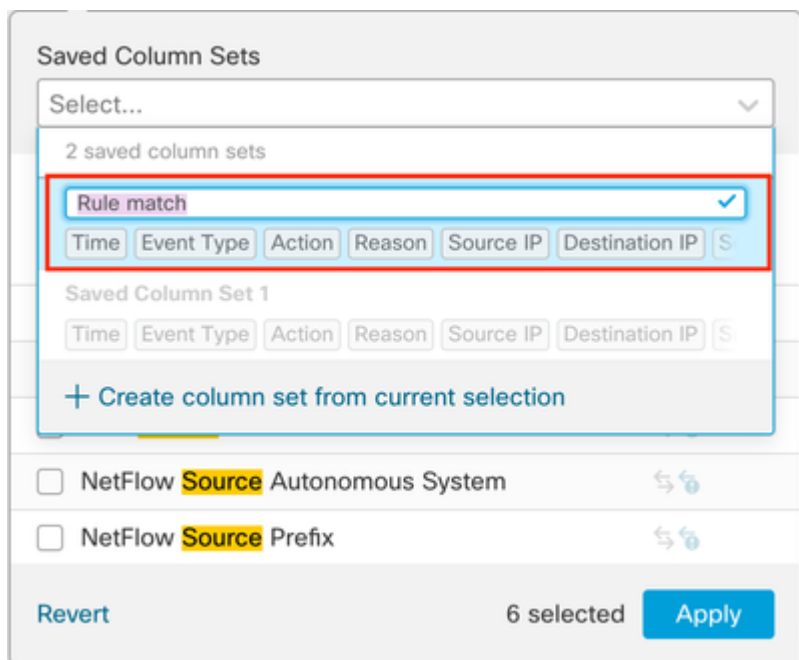
Time Event Type Action Reason Source IP Destination IP

+ Create column set from current selection

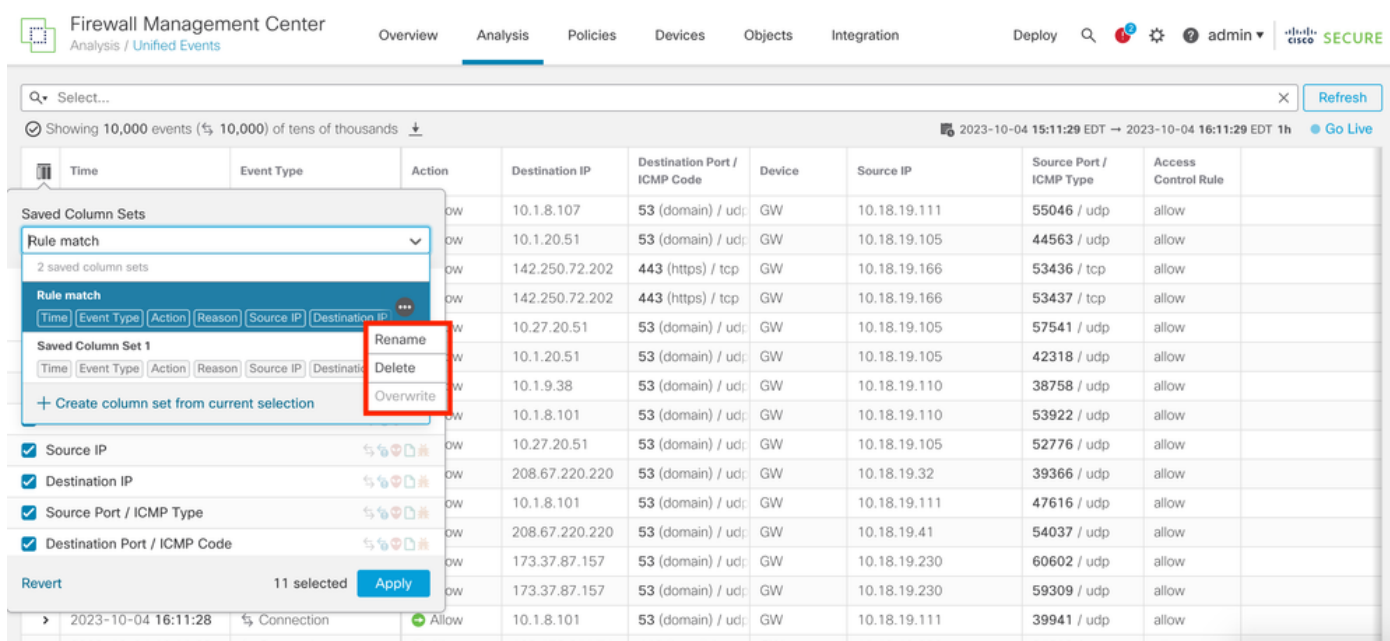
Source IP Destination IP Source Port / ICMP Type Destination Port / ICMP Code

Revert 11 selected Apply

步驟3. ( 可選 ) 更改列集的名稱。



步驟4.按一下省略號(...)可以編輯現有集。



## 事件搜尋

步驟1. 若要開始搜尋特定事件，請按一下「Select」。

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               |

步驟2.選擇要應用篩選器的欄位。

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

NAT Source IP  
 NAT Source Port  
 NetFlow Source Autonomous System  
 NetFlow Source Prefix  
 NetFlow Source ToS  
 Source Continent  
 Source Country  
 Source Device  
 Source Host Criticality  
**Source IP**

| Action | Destination Port / ICMP Code | Device | Source IP    | Source Port / ICMP Type | Access Control Rule |
|--------|------------------------------|--------|--------------|-------------------------|---------------------|
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.111 | 55046 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.105 | 44563 / tcp             | allow               |
| Allow  | 443 (https) / tcp            | GW     | 10.18.19.166 | 53436 / tcp             | allow               |
| Allow  | 443 (https) / tcp            | GW     | 10.18.19.166 | 53437 / tcp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.105 | 57541 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.105 | 42318 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.110 | 38758 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.110 | 53922 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.105 | 52776 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.32  | 39366 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.111 | 47616 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.41  | 54037 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.230 | 60602 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.230 | 59309 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.111 | 39941 / udp             | allow               |
| Allow  | 443 (https) / tcp            | GW     | 10.18.19.230 | 34810 / tcp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 | 52564 / udp             | allow               |
| Allow  | 53 (domain) / udp            | GW     | 10.18.19.110 | 50552 / udp             | allow               |

步驟3.寫入要用作篩選器的值。

Q Source IP  X Select...

步驟4.按一下Apply以設定篩選條件。

Firewall Management Center  
Analysis / Unified Events

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

Q 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

步驟5. ( 可選 ) 可以向每個篩選器新增多個值。

Firewall Management Center  
Analysis / Unified Events

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

Q 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               |

步驟6. ( 可選 ) 根據需要新增多個篩選條件。

Firewall Management Center  
Analysis / Unified Events

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

Q 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               |



提示：編寫值時可以使用運算子 ( >、<、! 等 )。

## 儲存搜尋

可以儲存搜尋，以便您可以重複使用已建立的過濾器。

步驟1. 按一下放大鏡圖示。

The screenshot shows the Firewall Management Center interface. At the top, there's a navigation bar with tabs: Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Analysis' tab is selected. Below the navigation bar, there's a search bar with a magnifying glass icon and a 'Refresh' button. The search bar contains the text 'Destination Port / ICMP Code: 8910' and 'Source IP: 10.18.19.111 x 10.18.19.105 x'. Below the search bar, there's a 'Saved searches' panel on the left. The panel has a search input field and a '+ Save search' button. The main area on the right shows a table of search results. The table has columns: Source IP, Device, Access Control Rule, and a fourth column. The table contains 12 rows of data. The first row is highlighted. The table is titled '2023-10-05 12:58:42 EDT → 2023-10-05 13:58:42 EDT 1h' and has a 'Go Live' button.

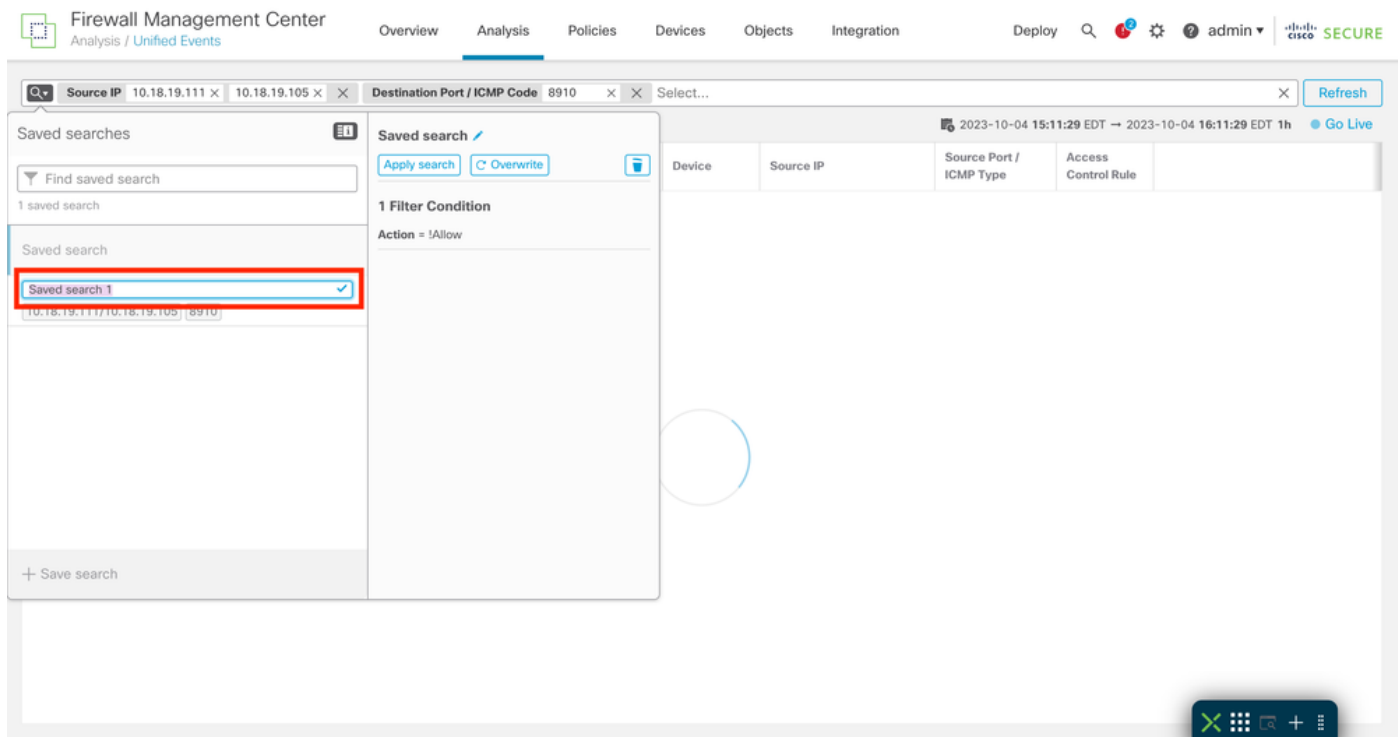
| Source IP    | Device | Access Control Rule |  |
|--------------|--------|---------------------|--|
| 10.18.19.105 | GW     | allow               |  |
| 10.18.19.105 | GW     | allow               |  |
| 10.18.19.105 | GW     | allow               |  |
| 10.18.19.105 | GW     | allow              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

步驟2. 按一下 Save Search。

The screenshot shows the Firewall Management Center interface, similar to the previous one. The 'Saved searches' panel on the left is highlighted with a red box, and the '+ Save search' button is also highlighted with a red box. The main area on the right shows the same table of search results.

| 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               |  |

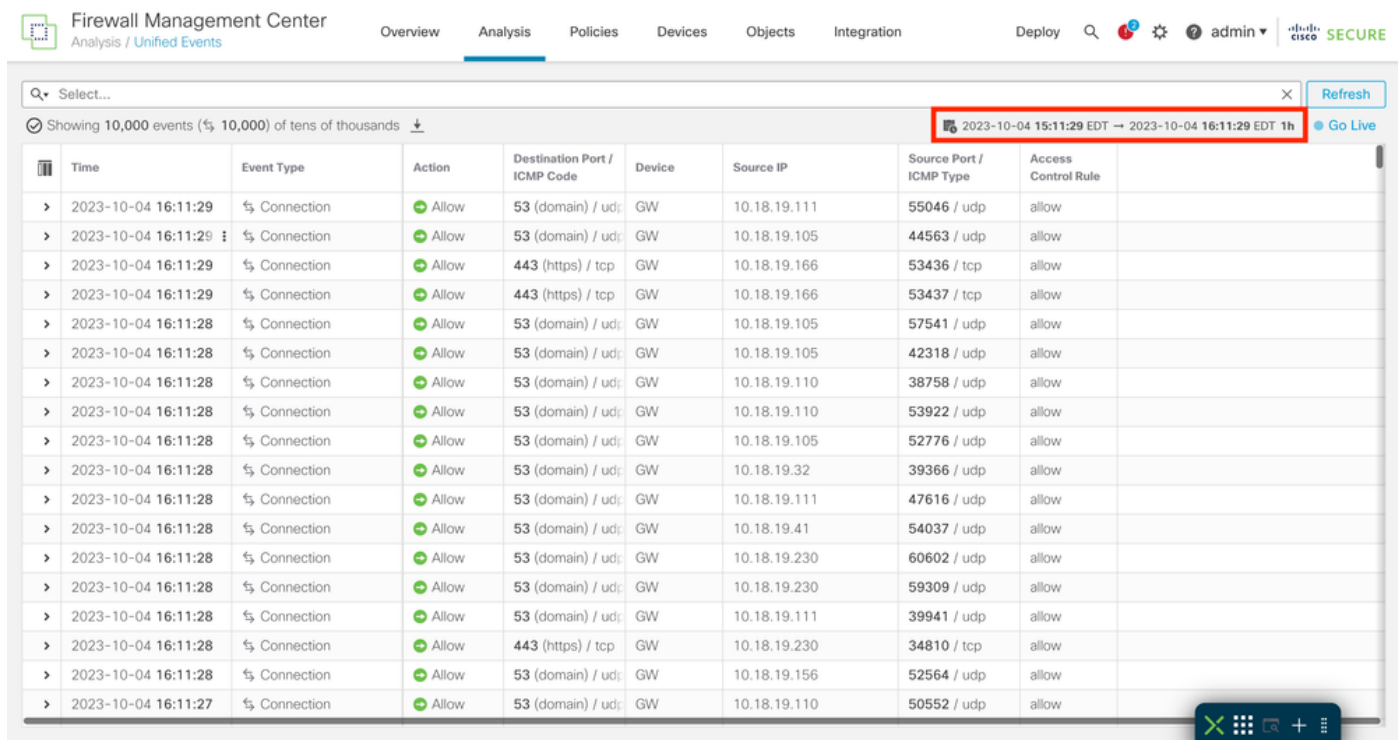
步驟3. ( 可選 ) 更改搜尋的名稱。



## 時間段

通過修改時間視窗，可以更容易地根據特定時間縮小相關事件的範圍。

步驟1. 若要修改事件的視窗框架，請按一下日期範圍。



步驟2. 在彈出視窗中選擇時間範圍。

Q Select...

Showing 167 events (167) 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       |
|---------------------|------------|--------|------------------------------|--------|--------------|
| 2023-10-04 16:11:29 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:29 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:29 | Connection | Allow  | 443 (https) / tcp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:29 | Connection | Allow  | 443 (https) / tcp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 443 (https) / tcp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.156 |
| 2023-10-04 16:11:27 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.18.19.110 |

Fixed Time Range Sliding Time Range

Start time

2023-10-04 15:11:29

End time

2023-10-04 16:11:29

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

October 2023

October 2023

1h selected

Apply

步驟3. (可選) 使用滑動時間範圍顯示從特定時間到當前時間的事件。



Fixed Time Range

步驟4.按一下Apply以過濾所設定時間範圍的事件。

**Q** Select... [Refresh](#)

Showing 8,317 events (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 | Sou          | Source IP   | Destination IP | Port | Protocol | Action |
|-----------------------|------------|--------|------------------------------|--------|--------------|-------------|----------------|------|----------|--------|
| > 2023-10-04 16:11:29 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.          |             |                |      |          |        |
| > 2023-10-04 16:11:29 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.          |             |                |      |          |        |
| > 2023-10-04 16:11:29 | Connection | Allow  | 443 (https) / tcp            | GW     | 10.          |             |                |      |          |        |
| > 2023-10-04 16:11:29 | Connection | Allow  | 443 (https) / tcp            | GW     | 10.          |             |                |      |          |        |
| > 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.          |             |                |      |          |        |
| > 2023-10-04 16:11:28 | Connection | Allow  | 53 (domain) / udp            | GW     | 10.          |             |                |      |          |        |
| > 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

啟用

您可以啟用「啟用」功能以即時顯示事件。事件在生成時顯示。

要啟用，請按一下啟用。

Firewall Management Center  
Analysis / Unified Events

OverviewAnalysisPoliciesDevicesObjectsIntegrationDeploy

admin

Go Live

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               |

啟用後，它會顯示Live一詞。

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

Live

**注意：**啟用Live後，無法修改時間視窗。要修改時間視窗，請先再次按一下以禁用「即時」選項。

將事件下載為 逗號分隔值(CSV)

步驟1.按一下下載圖示以生成包含當前顯示在頁面上的事件的檔案。

🔍

Destination Port / ICMP Code 8910 x x

Source IP 10.18.19.111 x 10.18.19.105 x

Select...

✕

Refresh

🕒

Showing all 144 events (📄 144)

📅 2023-10-05 12:58:42 EDT → 2023-10-05 13:58:42 EDT 1h

🔗 Go Live

| 📄 | 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               |  |

✕

📄

🔗

+

📄

步驟2.選擇下載資料夾和名稱，然後按一下Save。

Favorites

Applications

Desktop

Documents

Downloads

Locations

iCloud Drive

Tags

Red

Orange

Yellow

Green

Blue

Purple

Gray

All Tags

Save As: unified-events

Tags:

<>[icon] [icon]

Desktop

Search

Yesterday

unifiedevents

Format: CSV File

New Folder

Cancel

Save

步驟3.驗證CSV檔案。

| 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               |

## 相關資訊

- [使用統一事件檢視器](#)
- [思科安全防火牆 — 統一事件檢視器：提示與訣竅](#)
- [思科技術支援與下載](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。