

# 在 FMC GUI 上使用 Unified Event Viewer 监控事件

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[探索](#)

[统一事件页面示例](#)

[查看事件](#)

[个性化列](#)

[保存列集](#)

[事件搜索](#)

[保存搜索](#)

[时间段](#)

[正式启用](#)

[以逗号分隔值\(CSV\)格式下载事件](#)

[相关信息](#)

---

## 简介

本文档介绍如何在防火墙管理中心(FMC)的图形用户界面(GUI)上使用统一事件查看器。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 使用管理员或安全分析员权限访问FMC
- 版本等于或高于v7.0的FMC

### 使用的组件

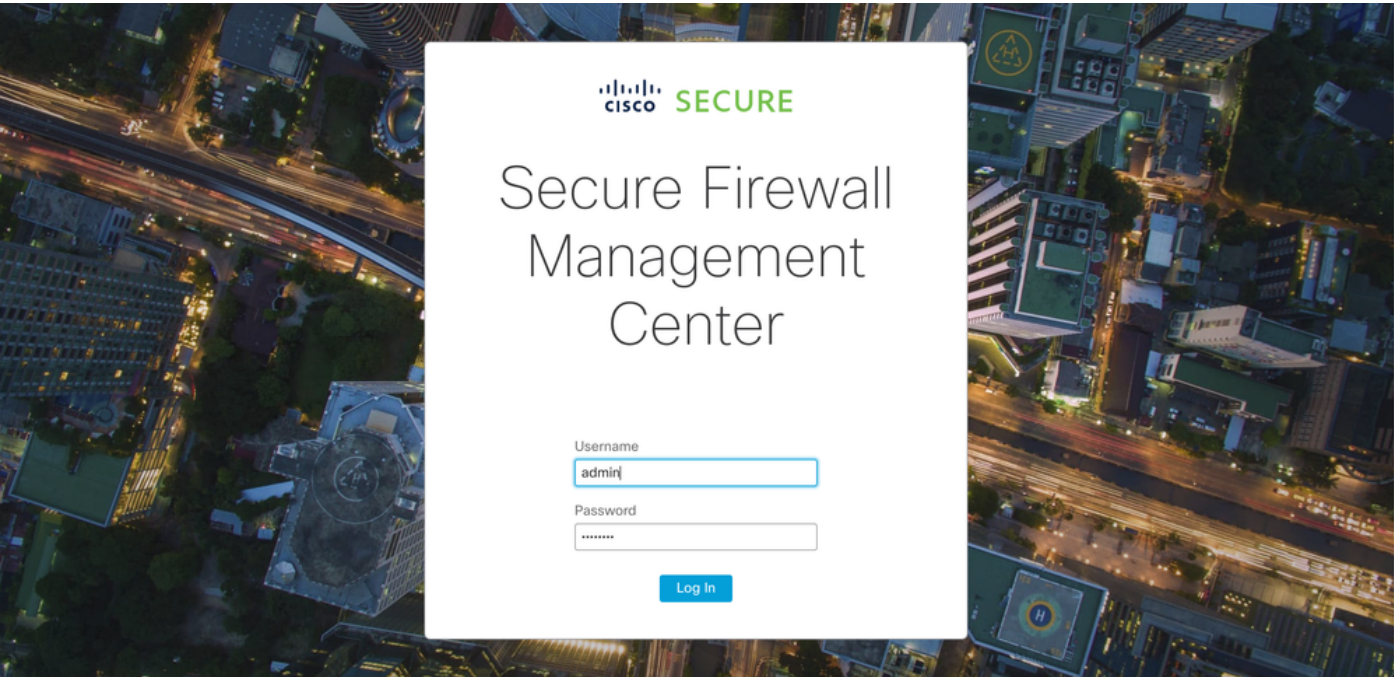
本文档中的信息基于以下软件和硬件版本：

- 适用于VMware v7.2.5的安全防火墙管理中心

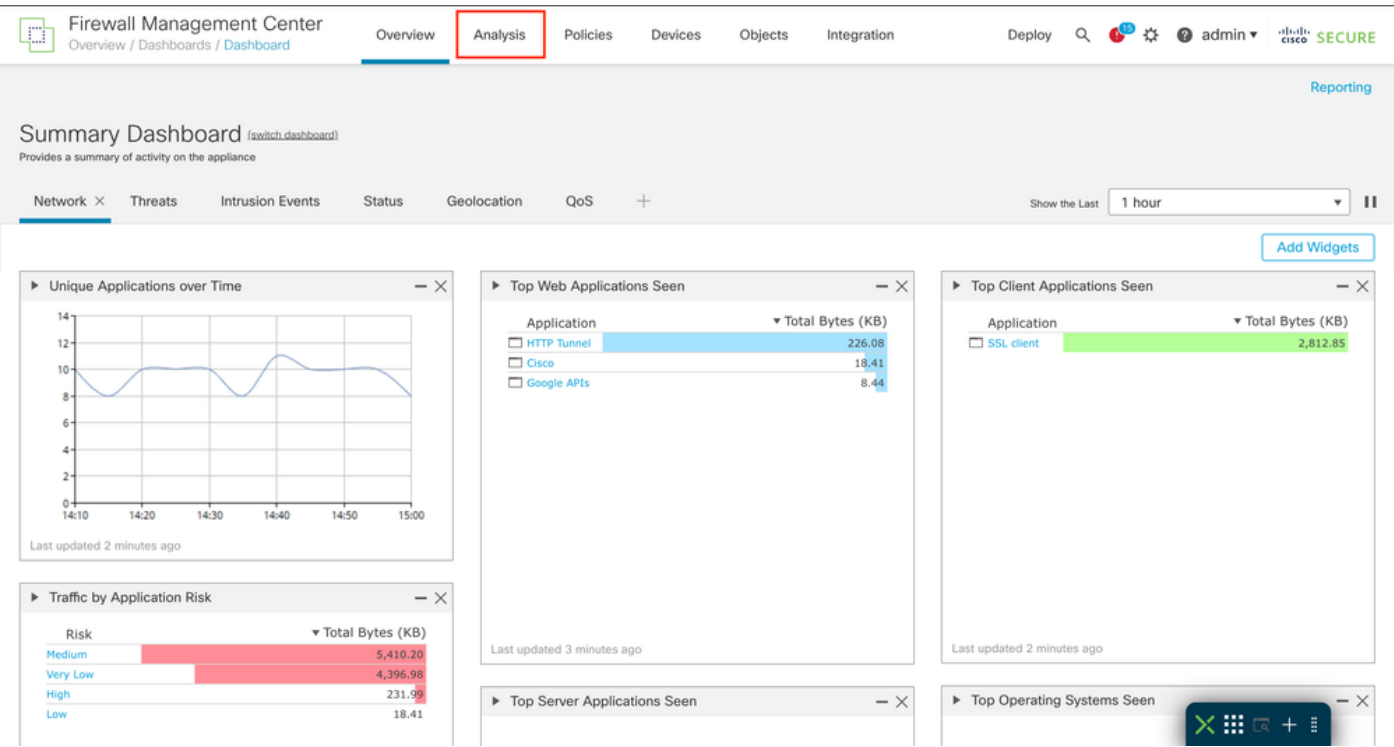
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

# 探索

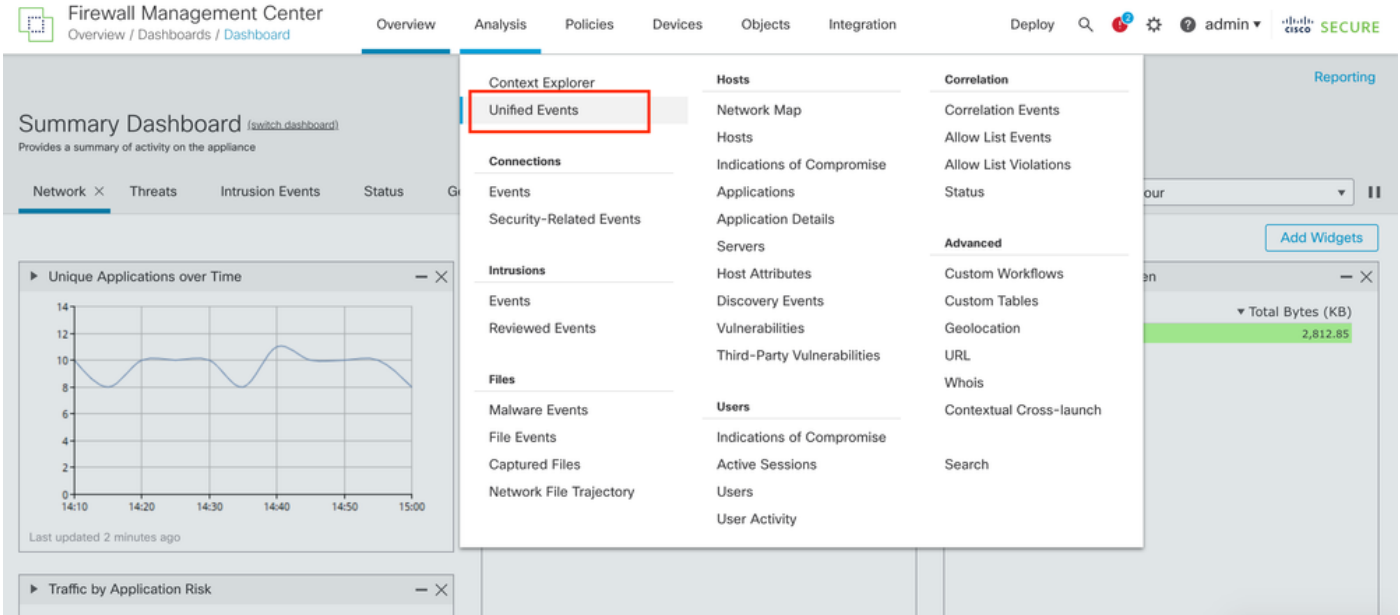
步骤1.登录FMC GUI。



步骤2.定位至分析标签。



步骤3.从下拉菜单中，单击Unified Events。



## 统一事件页面示例

The screenshot shows the 'Unified Events' page in the Firewall Management Center. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects, and Integration. The 'Analysis' tab is selected. The page displays a table of events with columns: Time, Event Type, Action, Destination Port / ICMP Code, Device, Source IP, Source Port / ICMP Type, and Access Control Rule. The table shows a list of connection events from 2023-10-04 16:11:29 to 2023-10-04 16:11:27. The events are filtered to show 10,000 events (of tens of thousands). The table is sorted by Time in descending order. The table is followed by a 'Go Live' button and a 'Refresh' button.

| 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               |

## 查看事件

步骤1.单击>图标。

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               |  |

步骤2.显示事件的详细信息。

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               |  |

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 |  |

## 个性化列

步骤1.点击图标

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               |

步骤2.选择您要在表上显示的事件字段。

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 | Reason | Source IP    | Destination IP | Source Port / ICMP Type | Destination Port / ICMP Code | Web A |
|------|------------|--------|--------|--------------|----------------|-------------------------|------------------------------|-------|
|      |            | 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             |       |

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

步骤3. ( 可选 ) 搜索字段以简化导航。

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

步骤4. 点击事件字段以禁用或启用。

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

步骤5. 单击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

步骤6. ( 可选 ) 您可以将每个列拖动到不同的位置来重新定位列。

Firewall Management Center

Analysis / Unified Events

OverviewAnalysisPoliciesDevicesObjectsIntegration

Deploy

admin

Go Live

Select...

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

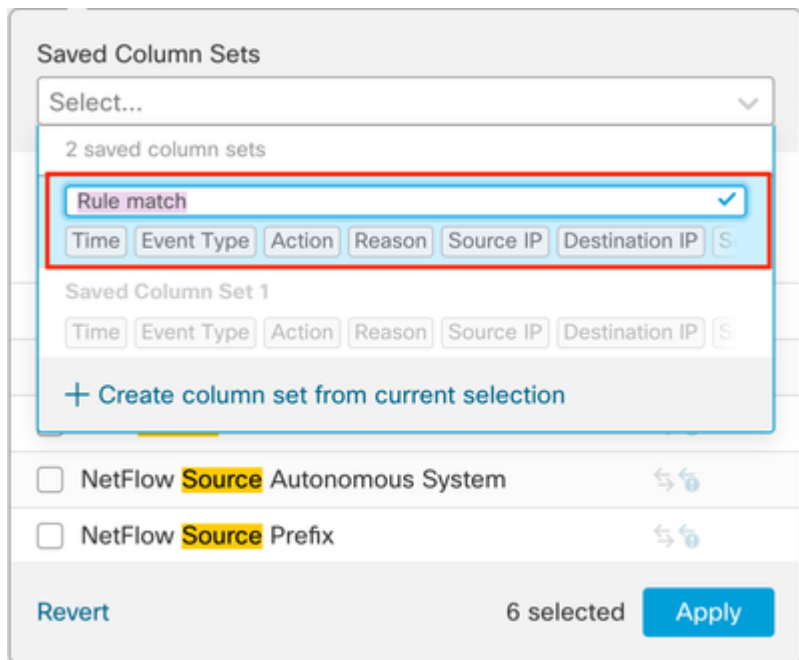
Refresh

| 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               |

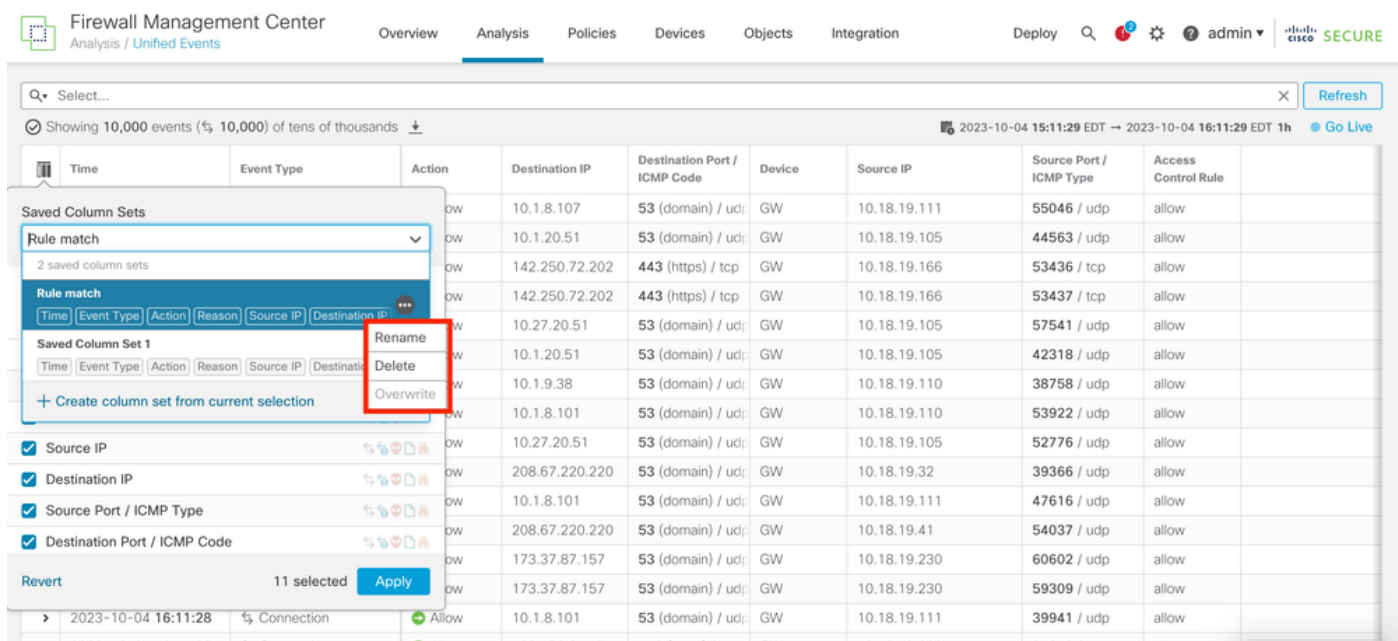
## 保存列集

步骤1. 点击保存的列集。





步骤4.单击省略号(...)可以编辑现有集。



## 事件搜索

步骤1.要开始搜索特定事件，请点击选择。

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               |

步骤2.选择要应用过滤器的字段。

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               |

步骤3.编写要用作过滤器的值。

Q Source IP Select...

步骤4.单击Apply配置过滤器。

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

步骤5. ( 可选 ) 可以向每个过滤器添加多个值。

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               |

步骤6. ( 可选 ) 根据需要添加多个过滤器。

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

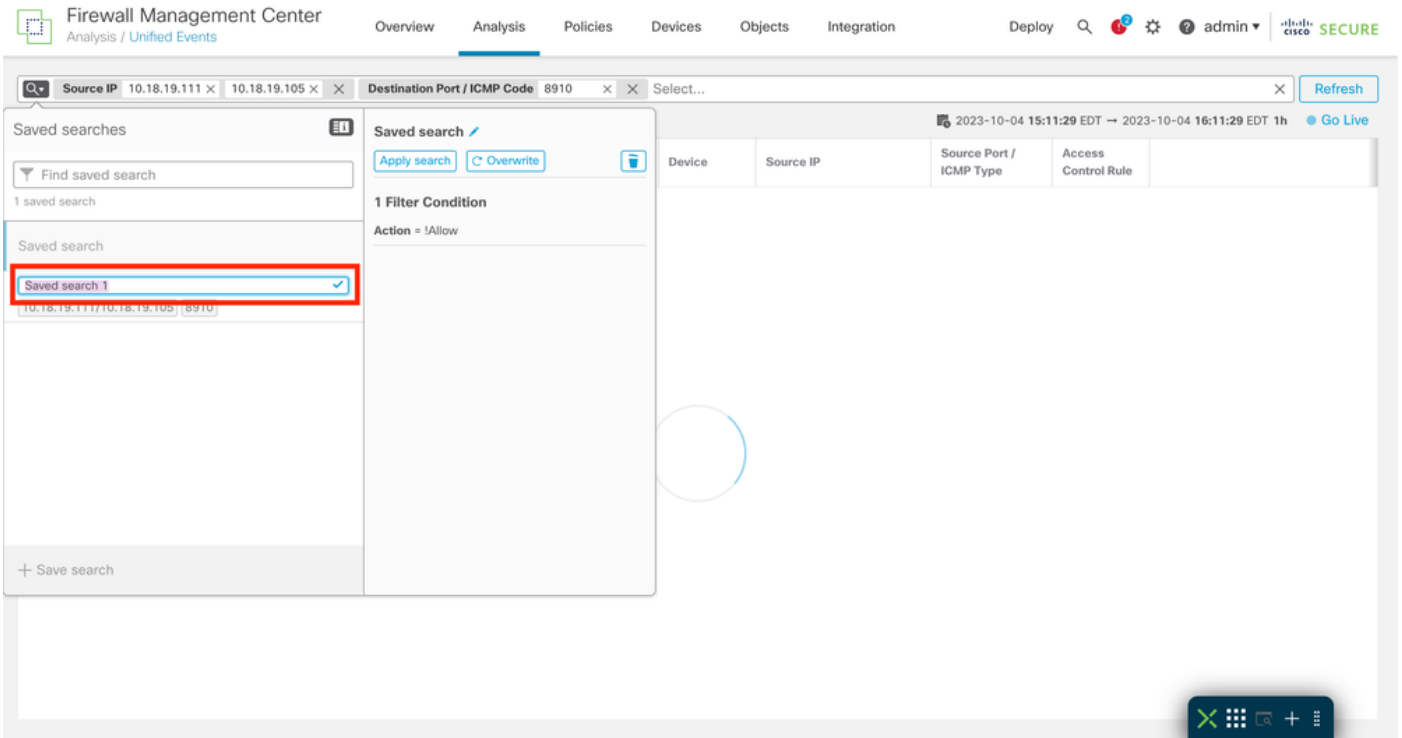
Showing all 106 events (106)

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               |

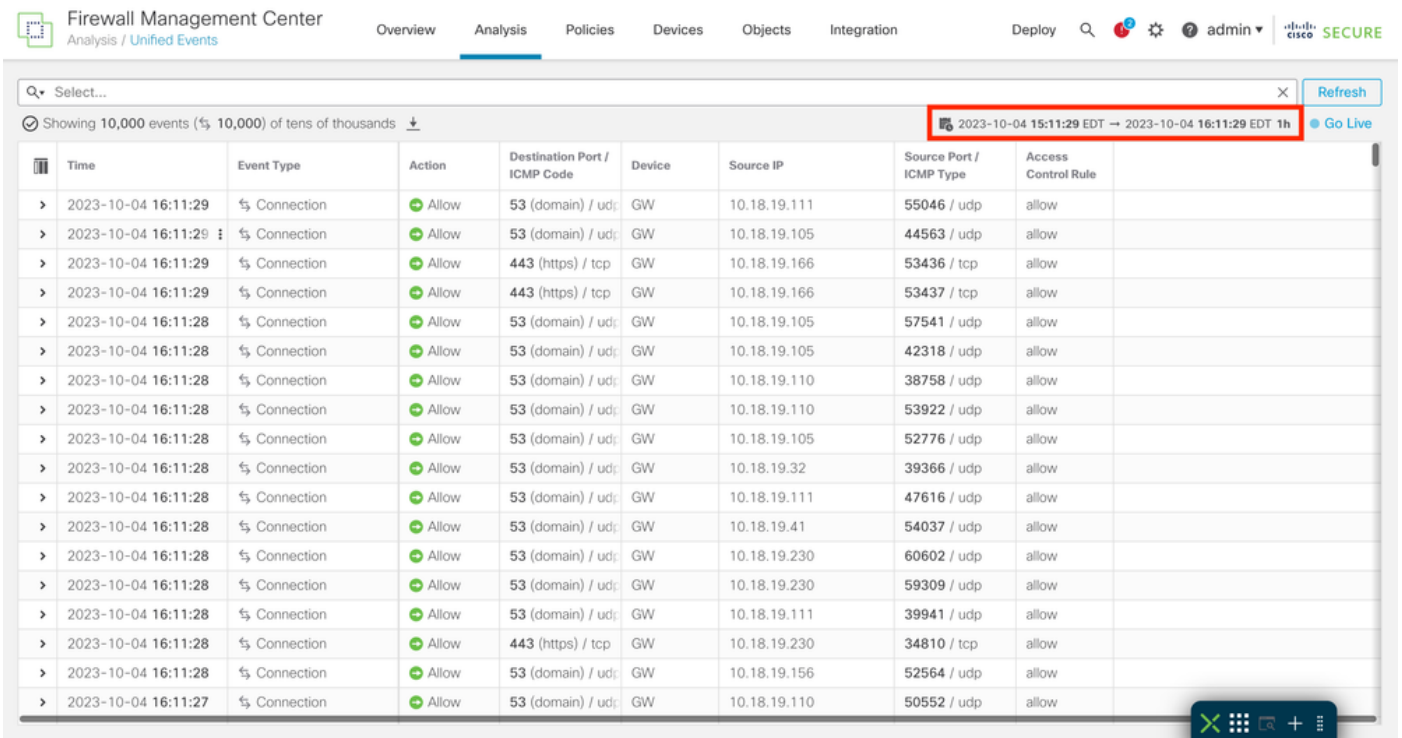
步骤3. ( 可选 ) 更改搜索的名称。



## 时间段

通过修改时间窗口，可以更容易地根据特定时间缩小相关事件的范围。

步骤1.要修改事件的窗口框架，请单击日期范围。



步骤2.在弹出窗口中选择时间范围。



要启用，请点击上线。

启用后，它会显示Live一词。



**警告：**启用Live后，无法修改时间段。要修改时间段，请先再次点击禁用Live选项。

步骤1.点击下载图标，生成包含当前显示在页面上的事件的文件。

🔍

Destination Port / ICMP Code 8910

×

×

Source IP 10.18.19.111

×

10.18.19.105

×

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               |  |

✕

📄

🔗

+

📄

步骤2.选择下载文件夹、名称并单击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

步骤3.检验CSV文件。

| 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               |

## 相关信息

- [使用统一事件查看器](#)
- [Cisco Secure Firewall - Unified Events Viewer:提示和诀窍](#)
- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。