

FMC GUIのUnified Event Viewerを使用したイベントのモニタ

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[探索](#)

[Unified Eventページの例](#)

[イベントの確認](#)

[列のパーソナライズ](#)

[列セットの保存](#)

[イベントの検索](#)

[検索の保存](#)

[タイムウィンドウ](#)

[稼働](#)

[カンマ区切り値\(CSV\)としてイベントをダウンロードする](#)

[関連情報](#)

はじめに

このドキュメントでは、Firewall Management Center(FMC)のグラフィカルユーザインターフェイス(GUI)でのUnified Event Viewer(CUGA)の使用について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Admin権限またはSecurity Analyst権限を使用したFMCへのアクセス
- バージョン7.0以降のFMC

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Firewall Management Center for VMware v7.2.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始して

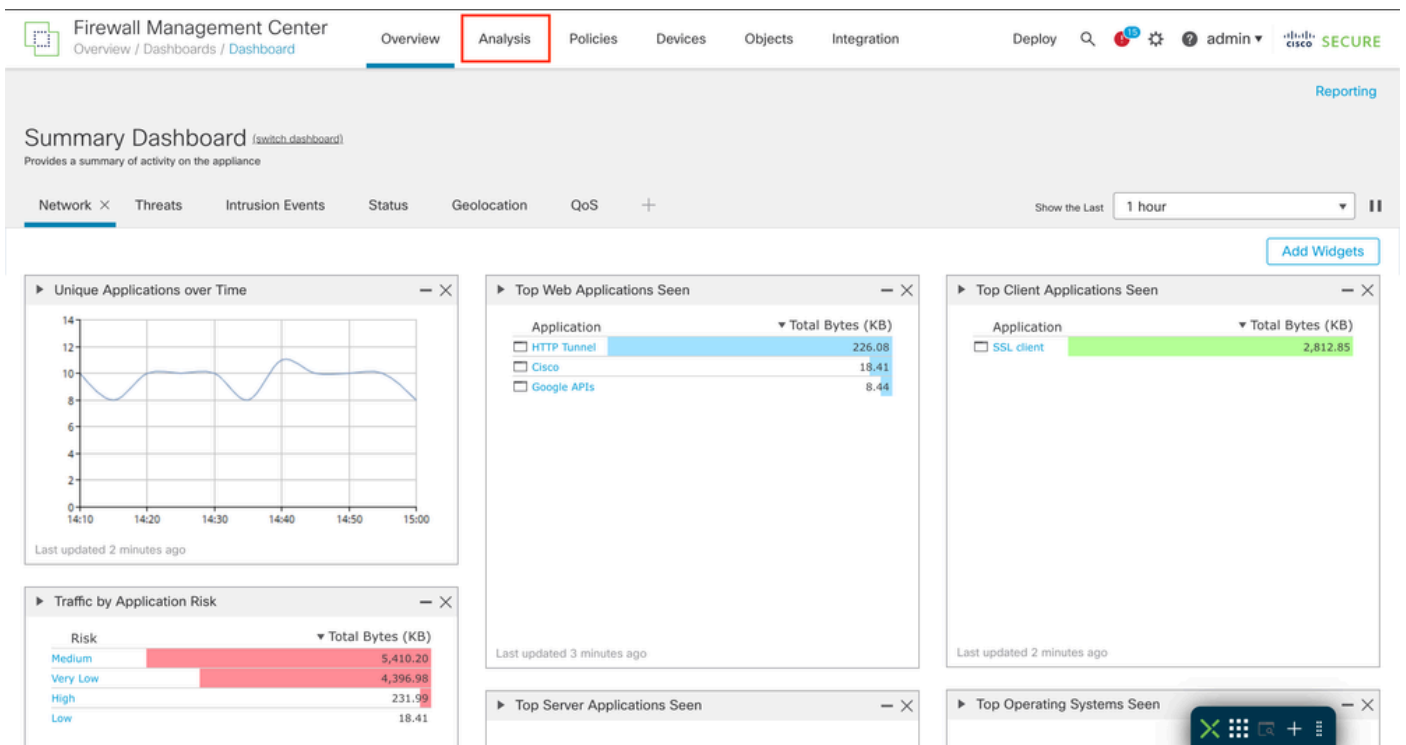
います。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

探索

ステップ 1 : FMCのGUIにログインします。



ステップ 2 Analysisタブに移動します。



ステップ 3 ドロップダウンメニューからUnified Eventsをクリックします。

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

14:10 14:20 14:30 14:40 14:50 15:00

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

Add Widgets

Total Bytes (KB)

2,812.85

Unified Eventページの例

Firewall Management Center
Analysis / Unified Events

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

Select...

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

イベントの確認

ステップ 1 : > アイコンをクリックします。

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

ステップ2 イベントの詳細情報が表示されます。

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

列のパーソナライズ

ステップ1: アイコンをクリックします。



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

ステップ2テーブルに表示するイベントフィールドを選択します。

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 Ac
2023-10-04 16:11:29	Connection	Allow		10.18.19.111	10.1.8.107	55046 / udp	53 (domain) / udp	
2023-10-04 16:11:29	Connection	Allow		10.18.19.105	10.1.20.51	44563 / udp	53 (domain) / udp	
2023-10-04 16:11:29	Connection	Allow		10.18.19.166	142.250.72.202	53436 / tcp	443 (https) / tcp	
2023-10-04 16:11:29	Connection	Allow		10.18.19.166	142.250.72.202	53437 / tcp	443 (https) / tcp	
2023-10-04 16:11:29	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

ステップ3: (オプション) フィールドを検索してナビゲーションを容易にします。

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

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

Revert 7 selected Apply

ステップ 4 イベントフィールドをクリックして、無効または有効にします。

Saved Column Sets

Select...

Source

Select 14 filtered | Select default

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

Revert 6 selected Apply

ステップ 5 次に、[Apply] をクリックします。

Saved Column Sets

Select...

Filter columns

Select none | Select default

☒ Event Type

☒ Action

☒ Destination Port / ICMP Code

☒ Source IP

☒ Device

Revert 6 selected **Apply**

ステップ6: (オプション) 各列を別の場所にドラッグして、列の位置を変更できます。

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy

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

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

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

列セットの保存

ステップ 1 : Saved Column Setsをクリックします。

Firewall Management Center
Analysis / Unified Events

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

Q Select... Refresh

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

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

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web Ap
2023-10-04 16:11:28	Connection	Allow		10.18.19.111	10.1.8.107	55046 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.105	10.1.20.51	44563 / udp	53 (domain) / ud	
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) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.105	10.1.20.51	42318 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.110	10.1.9.38	38758 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.110	10.1.8.101	53922 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.105	10.27.20.51	52776 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.32	208.67.220.220	39366 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.111	10.1.8.101	47616 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.41	208.67.220.220	54037 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.230	173.37.87.157	60602 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		10.18.19.230	173.37.87.157	59309 / udp	53 (domain) / ud	
2023-10-04 16:11:28	Connection	Allow		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

11 selected Apply

ステップ 2 Create column set from current selectionをクリックします。

Firewall Management Center
Analysis / Unified Events

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

Q Select... Refresh

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

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

Time	Event Type	Action	Destination IP	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-04 16:11:28	Connection	Allow	10.1.8.107	53 (domain) / ud	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.20.51	53 (domain) / ud	GW	10.18.19.105	44563 / udp	allow
2023-10-04 16:11:28	Connection	Allow	142.250.72.202	443 (https) / tcp	GW	10.18.19.166	53436 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	142.250.72.202	443 (https) / tcp	GW	10.18.19.166	53437 / tcp	allow
2023-10-04 16:11:28	Connection	Allow	10.27.20.51	53 (domain) / ud	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.20.51	53 (domain) / ud	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.9.38	53 (domain) / ud	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.8.101	53 (domain) / ud	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.27.20.51	53 (domain) / ud	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	208.67.220.220	53 (domain) / ud	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.8.101	53 (domain) / ud	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	208.67.220.220	53 (domain) / ud	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	173.37.87.157	53 (domain) / ud	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	173.37.87.157	53 (domain) / ud	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.8.101	53 (domain) / ud	GW	10.18.19.111	39941 / udp	allow
2023-10-04 16:11:28	Connection	Allow	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

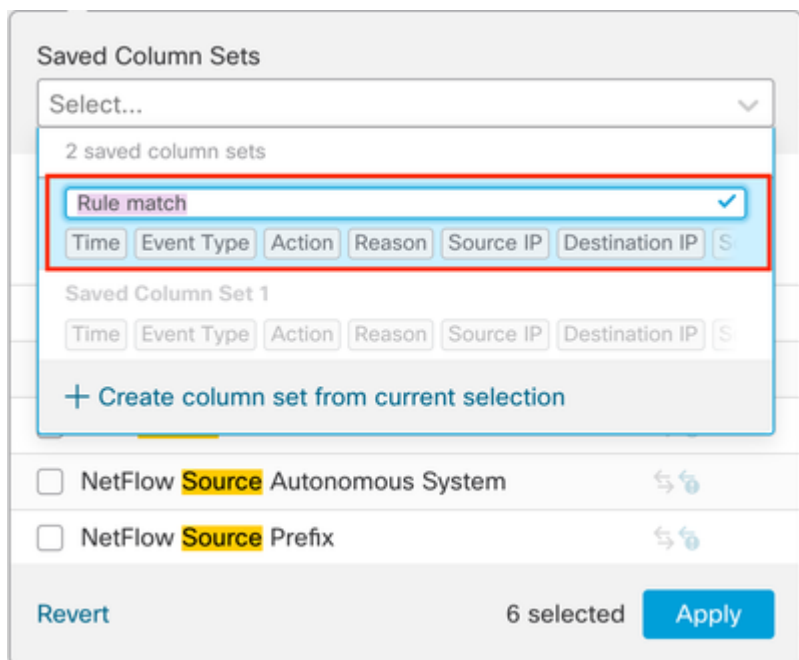
Saved Column Set 1

Time Event Type Action Reason Source IP Destination IP

+ Create column set from current selection

11 selected Apply

ステップ3: (オプション) 列セットの名前を変更します。



ステップ 4 省略記号(...)をクリックすると、既存のセットを編集できます。

Firewall Management Center
Analysis / Unified Events

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

Select... Refresh

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

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

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

Saved Column Sets

Rule match (selected) 2 saved column sets

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

Rename Delete Overwrite

Revert 11 selected Apply

2023-10-04 16:11:28 🔗 Connection 🟢 Allow 10.1.8.101 53 (domain) / udp GW 10.18.19.111 39941 / udp allow

イベントの検索

ステップ 1：特定のイベントの検索を開始するには、Selectをクリックします。

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

ステップ2フィルタを適用するフィールドを選択します。

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 / udp	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

ステップ3フィルタとして使用する値を記述します。

Q Source IP X Select...

ステップ4Applyをクリックして、フィルタを設定します。

Firewall Management Center
Analysis / Unified Events

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

ステップ5: (オプション) 各フィルタに複数の値を追加できます。

Firewall Management Center
Analysis / Unified Events

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

ステップ6: (オプション) 必要な数のフィルタを追加します。

Firewall Management Center
Analysis / Unified Events

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

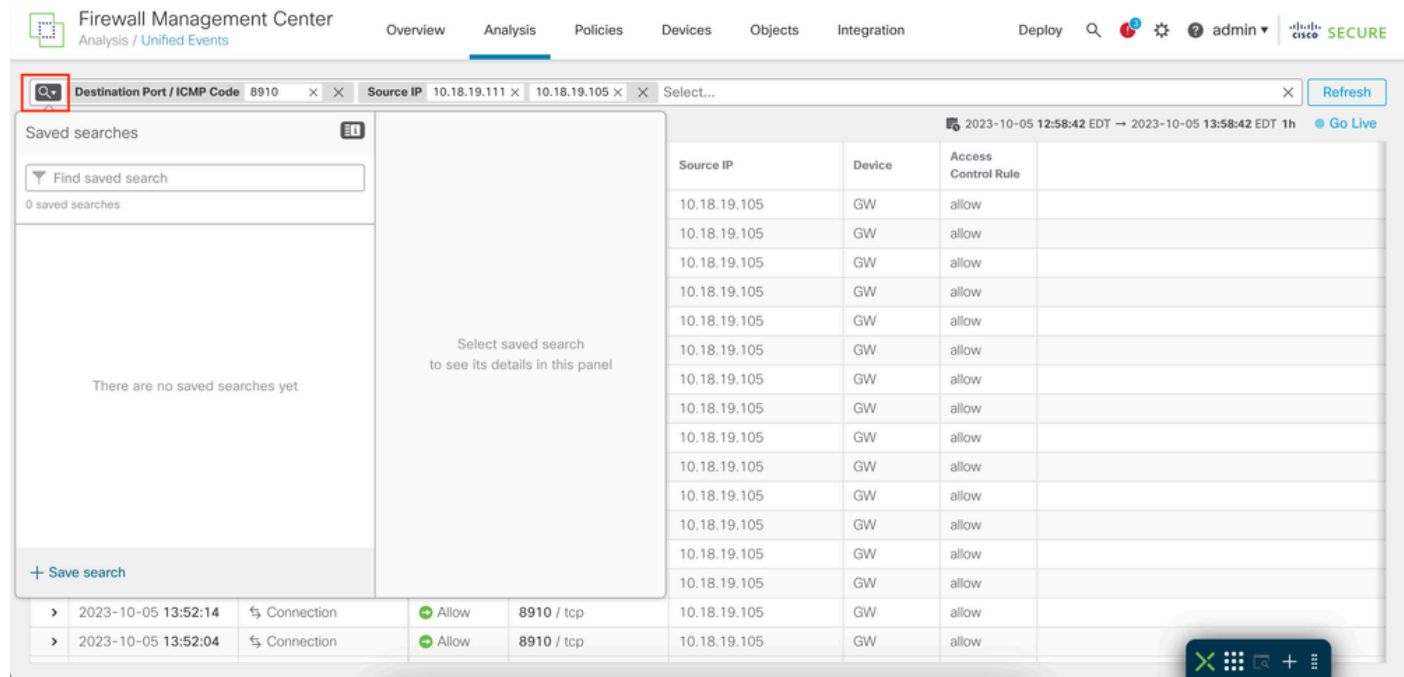


ヒント：値の書き込み時に演算子（>、<、！など）を使用できます。

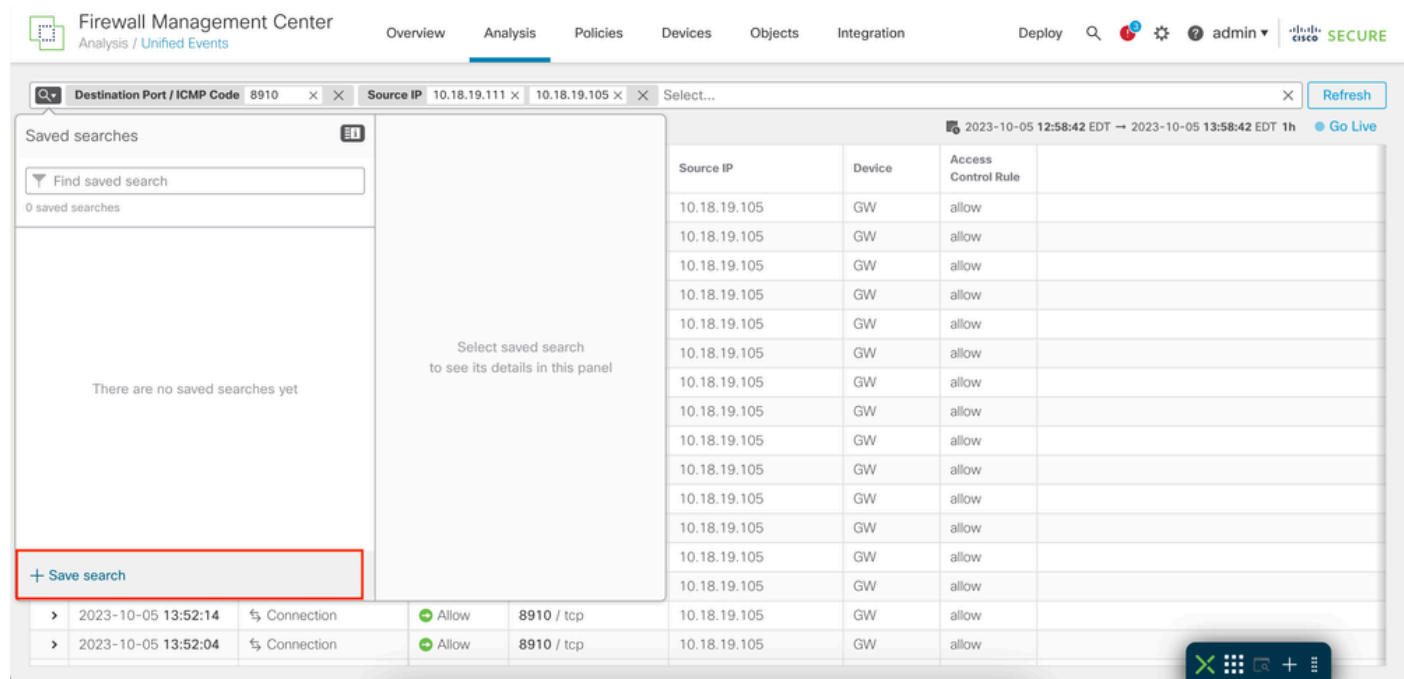
検索の保存

検索を保存して、作成したフィルタを再利用することができます。

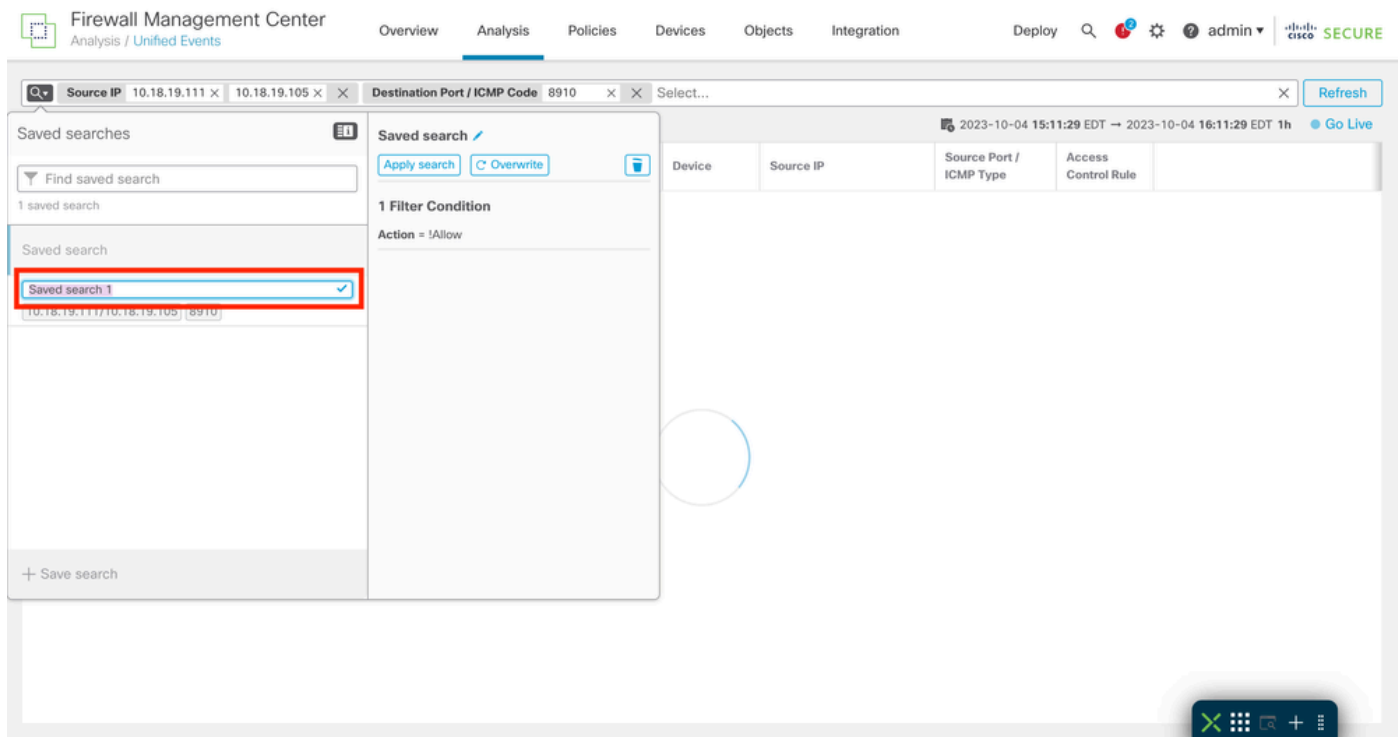
ステップ 1: 虫めがねアイコンをクリックします。



ステップ 2 Save Searchをクリックします。



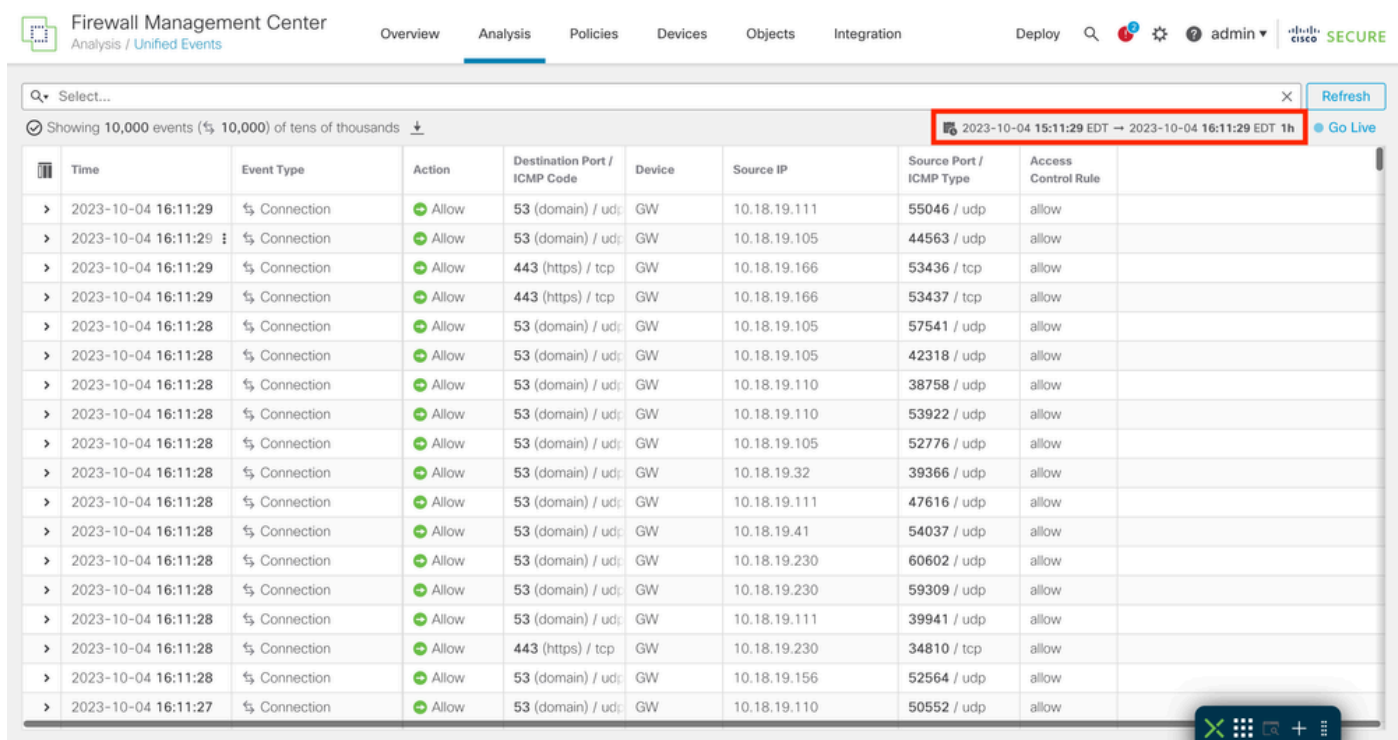
ステップ3: (オプション) 検索名を変更します。



タイムウィンドウ

タイムウィンドウを変更すると、特定の時間に基づいて関連するイベントを絞り込みやすくなります。

ステップ 1: イベントのウィンドウフレームを変更するには、日付範囲をクリックします。



ステップ 2 ポップアップウィンドウで時間の範囲を選択します。

Firewall Management Center
Analysis / Unified Events

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

Q Select... Refresh

Showing 8,317 events (8,317) of tens of thousands 2023-10-04 15:11:29 EDT → 2023-10-04 16:11:29 EDT 1h Go Live

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

Fixed Time Range Sliding Time Range

Show the last 6 hours

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

Apply

稼動

Go Live機能を有効にすると、イベントをリアルタイムで表示できます。イベントは生成されるとおりに表示されます。

有効にするには、Go Liveをクリックします。

Firewall Management Center
Analysis / Unified Events

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

Q Select... Refresh

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

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

Go Live

有効にすると、Liveという単語が表示されます。

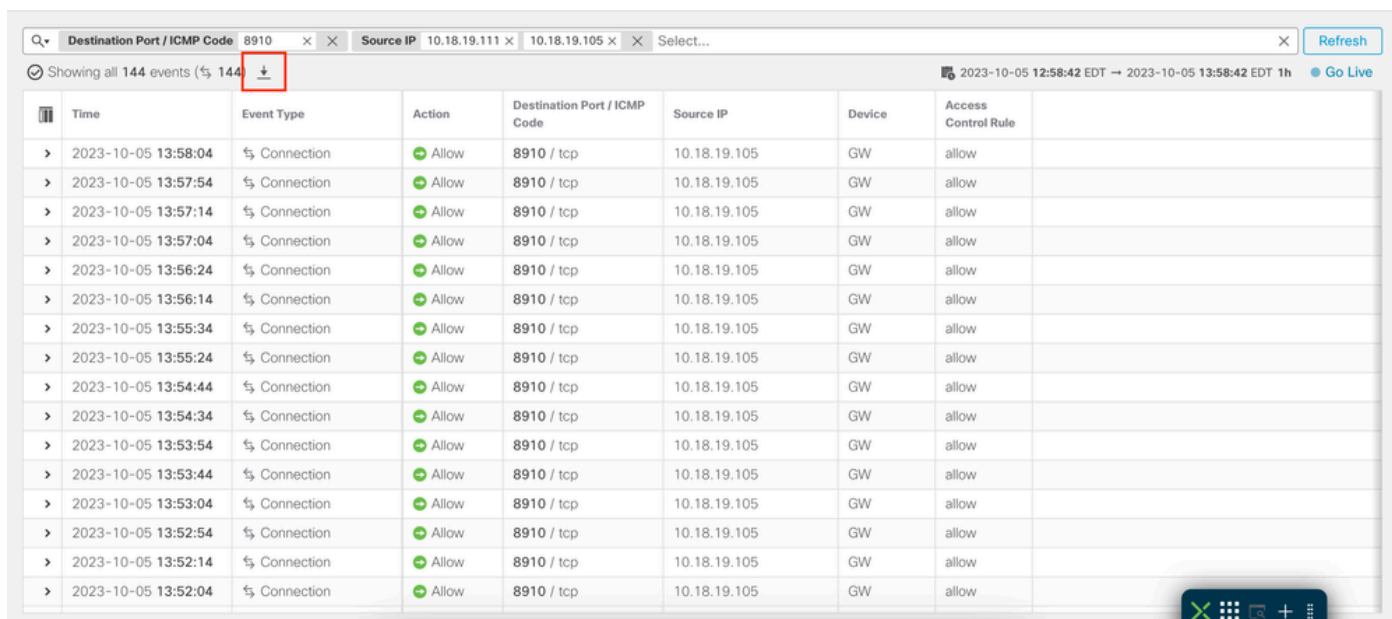
2023-10-05 21:55:25 EDT → 2023-10-05 21:56:04 EDT 39s Live



注意:Liveが有効になっていると、時間帯を変更できません。タイムウィンドウを変更するには、まず再度クリックしてライブオプションを無効にします。

イベントのダウンロード カンマ区切り値 (CSV)

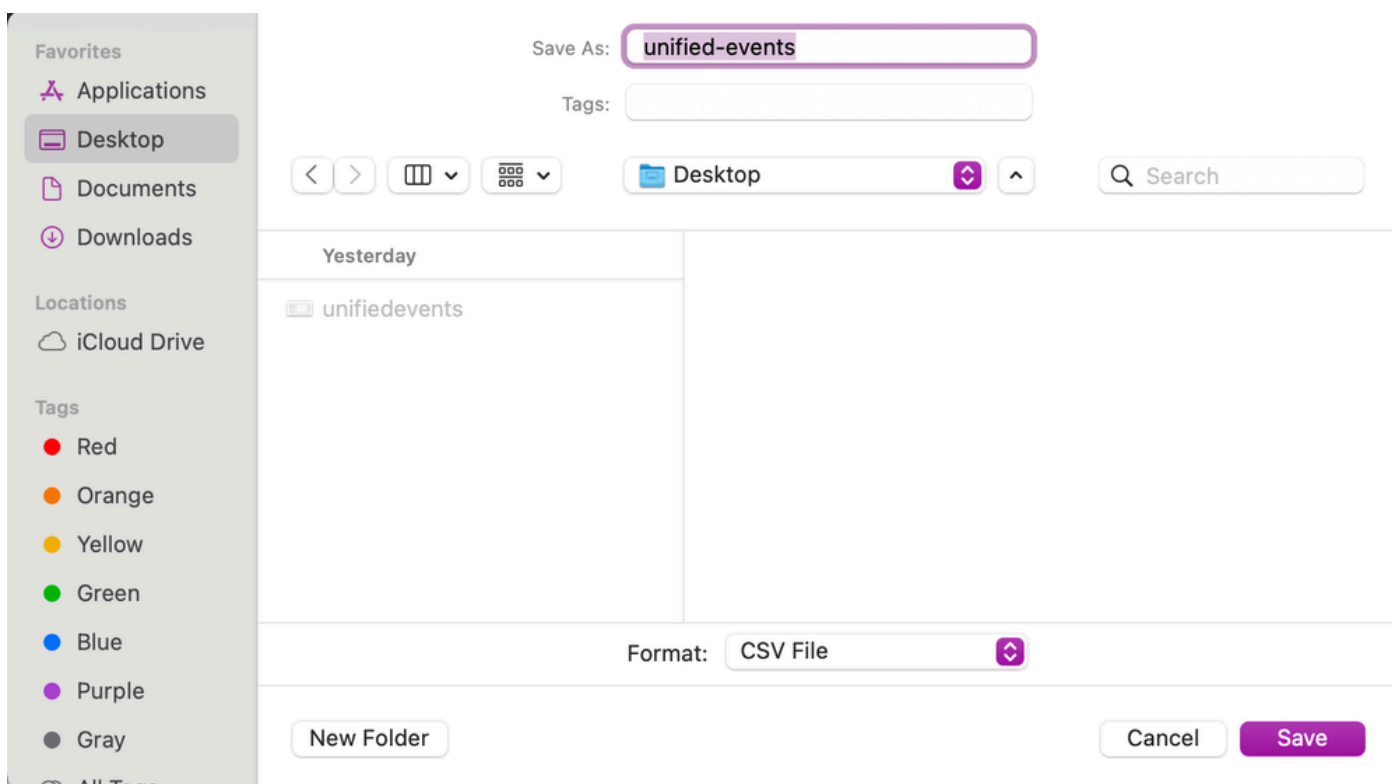
ステップ 1: ダウンロードアイコンをクリックして、ページに現在表示されているイベントを含むファイルを生成します。



The screenshot shows a web interface for viewing event logs. At the top, there are filters for 'Destination Port / ICMP Code' (8910) and 'Source IP' (10.18.19.111, 10.18.19.105). A 'Refresh' button is on the right. Below the filters, it says 'Showing all 144 events (1/144)'. A red box highlights a download icon (a square with a downward arrow) next to the event count. The main area is a table with columns: Time, Event Type, Action, Destination Port / ICMP Code, Source IP, Device, and Access Control Rule. The table contains 14 rows of data, all showing 'Connection' events with 'Allow' actions on 'GW' devices. The time range is from 2023-10-05 12:58:42 EDT to 2023-10-05 13:58:42 EDT. A 'Go Live' button is in the top right corner.

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

ステップ 2ダウンロードフォルダを選択し、名前を付けてSaveをクリックします。



ステップ 3 CSV ファイルを確認します。

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

関連情報

- [Unified Event Viewerの操作](#)
- [Cisco Secure Firewall - Unified Events Viewer : ヒント](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。