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

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。

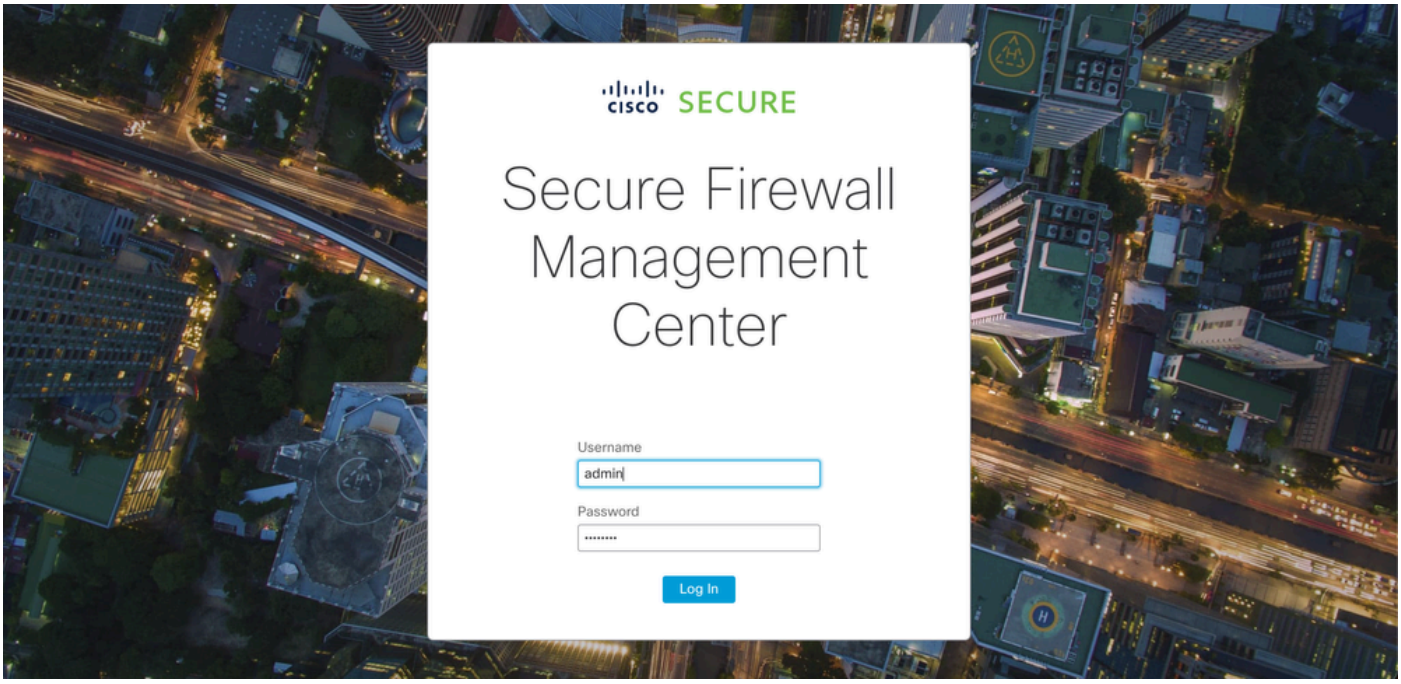
- Secure Firewall Management Center for VMware v7.2.5

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

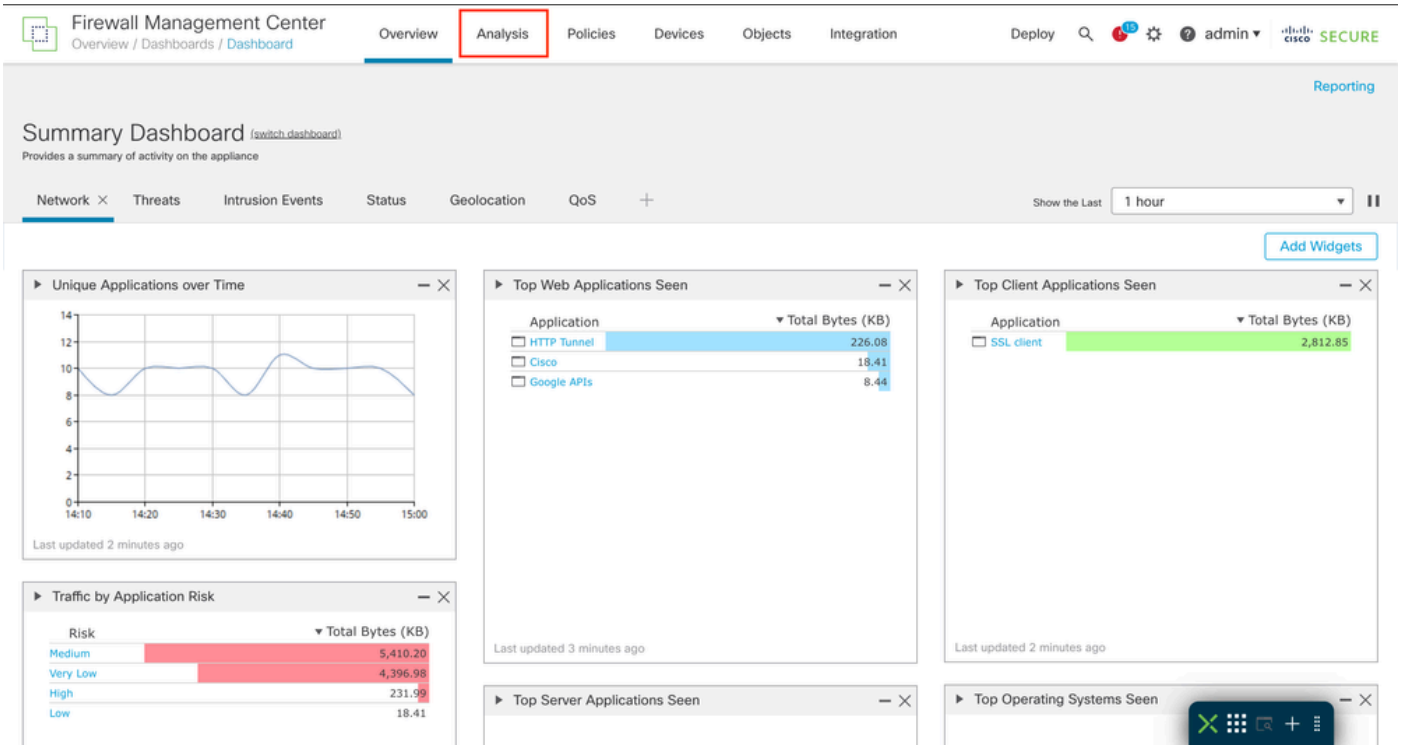
います。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

探索

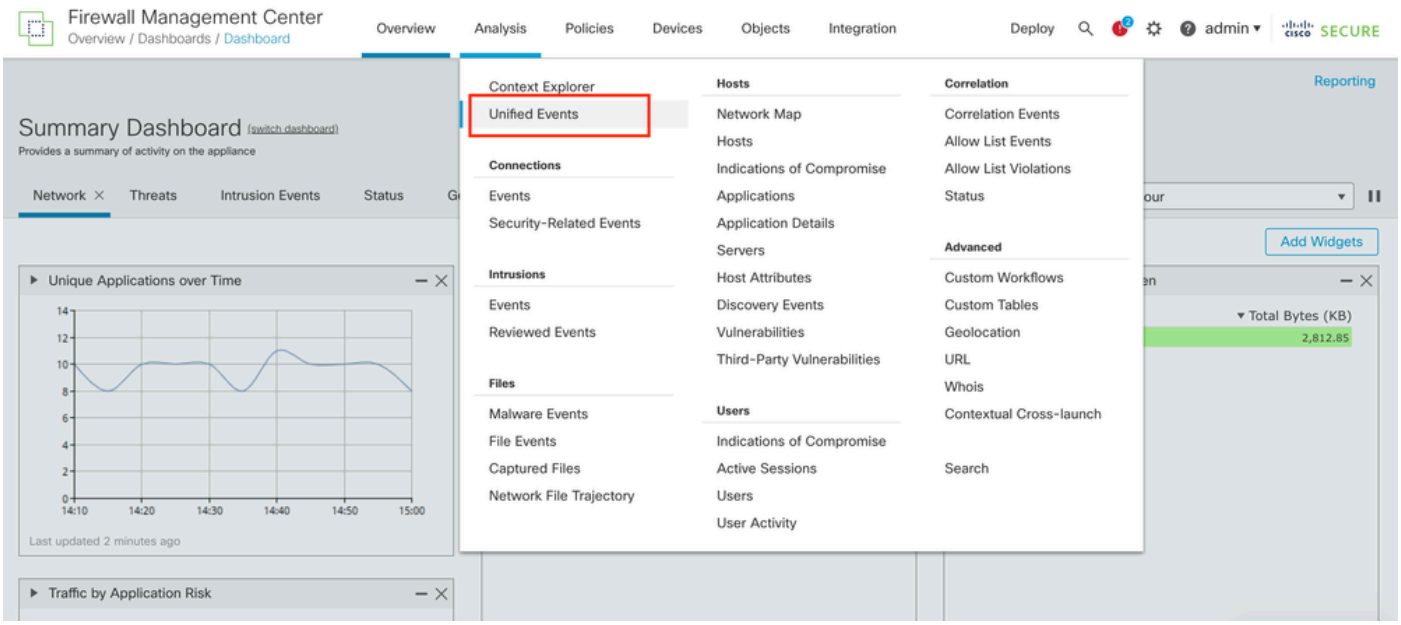
ステップ 1：FMCのGUIにログインします。



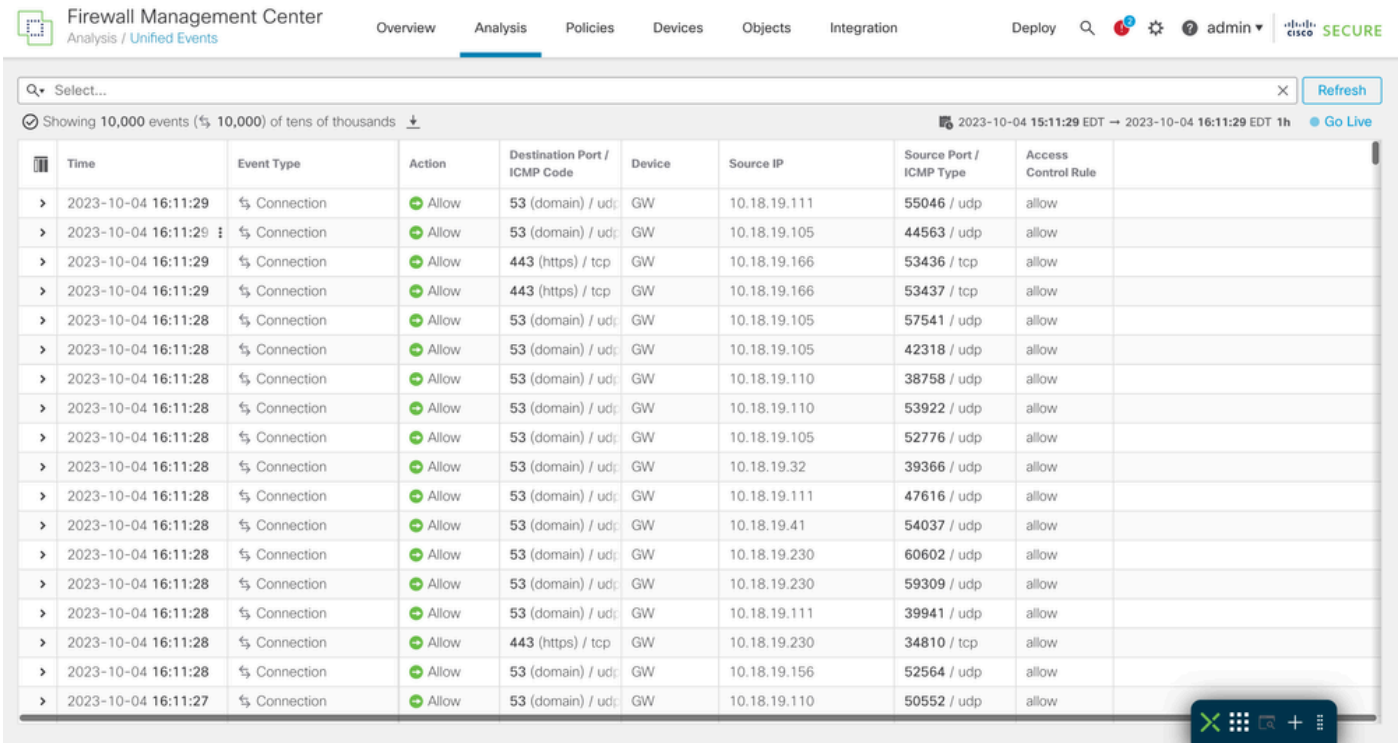
ステップ 2Analysisタブに移動します。



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。

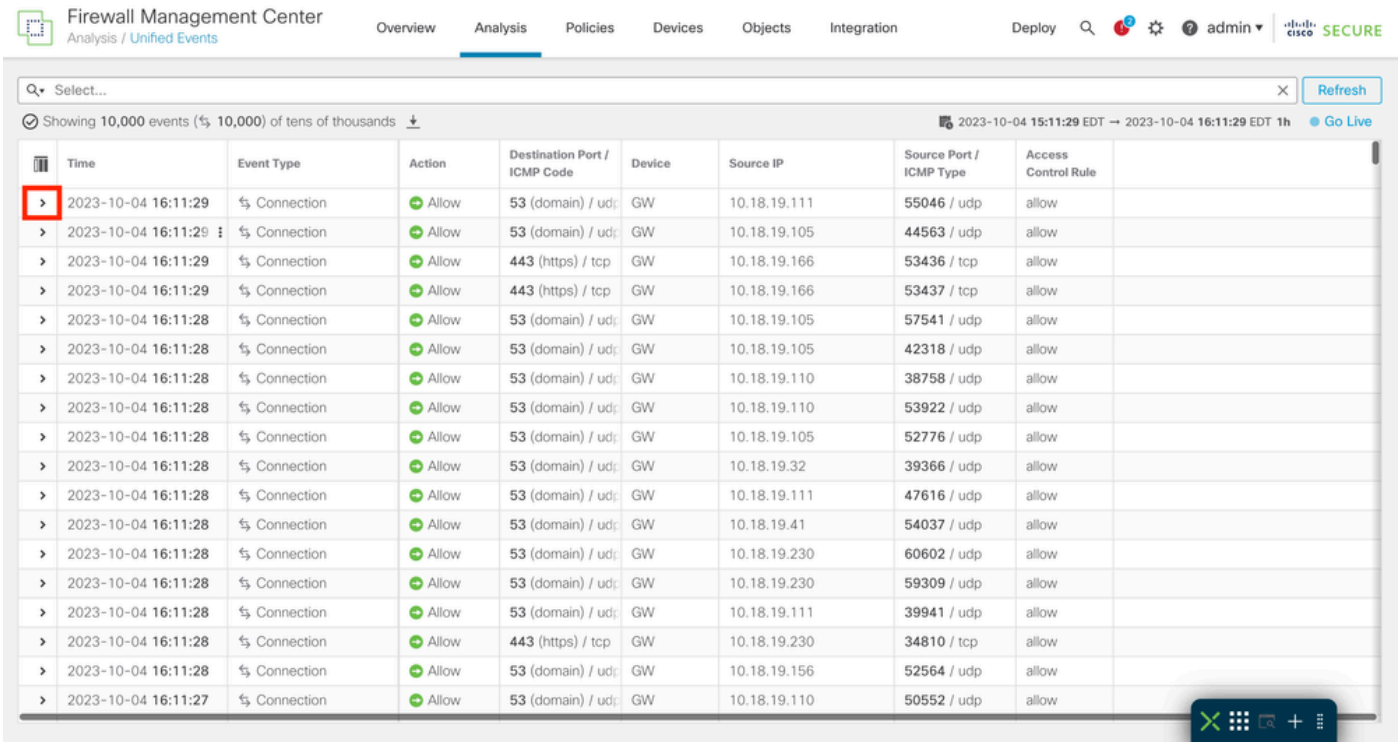


Unified Eventページの例

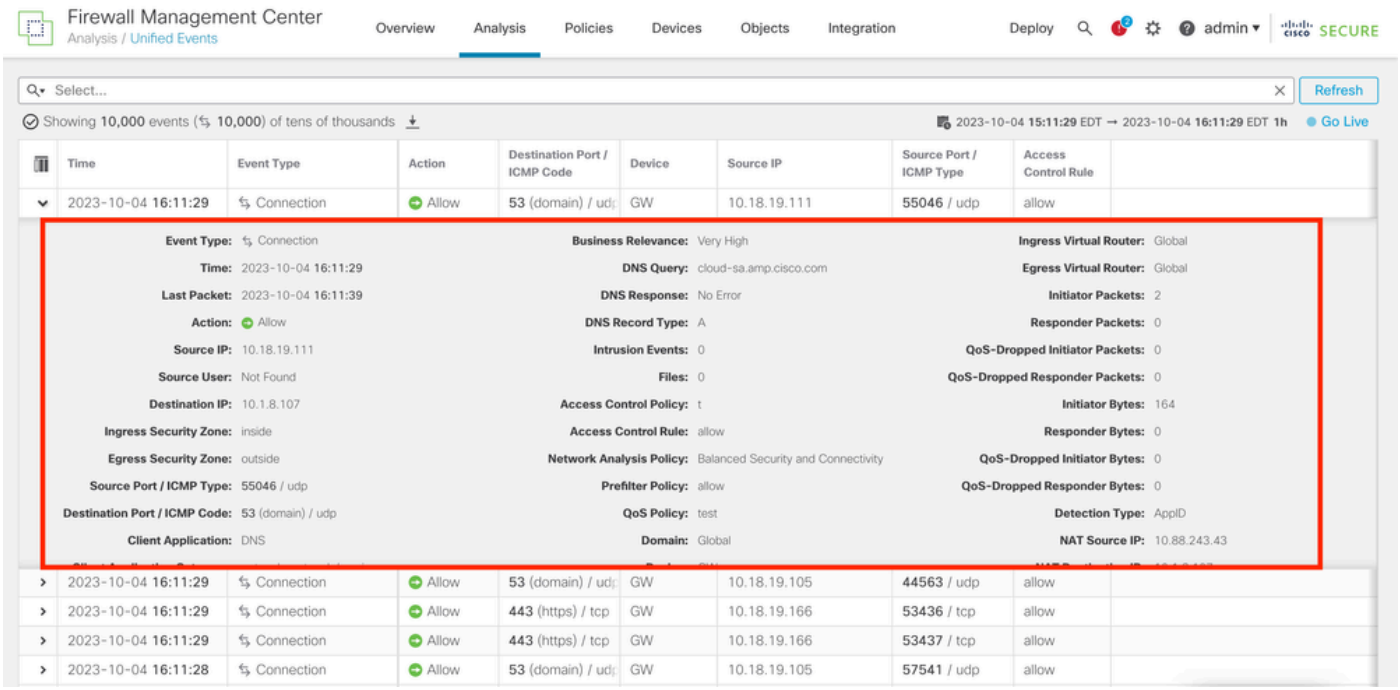


イベントの確認

ステップ 1 : > アイコンをクリックします。

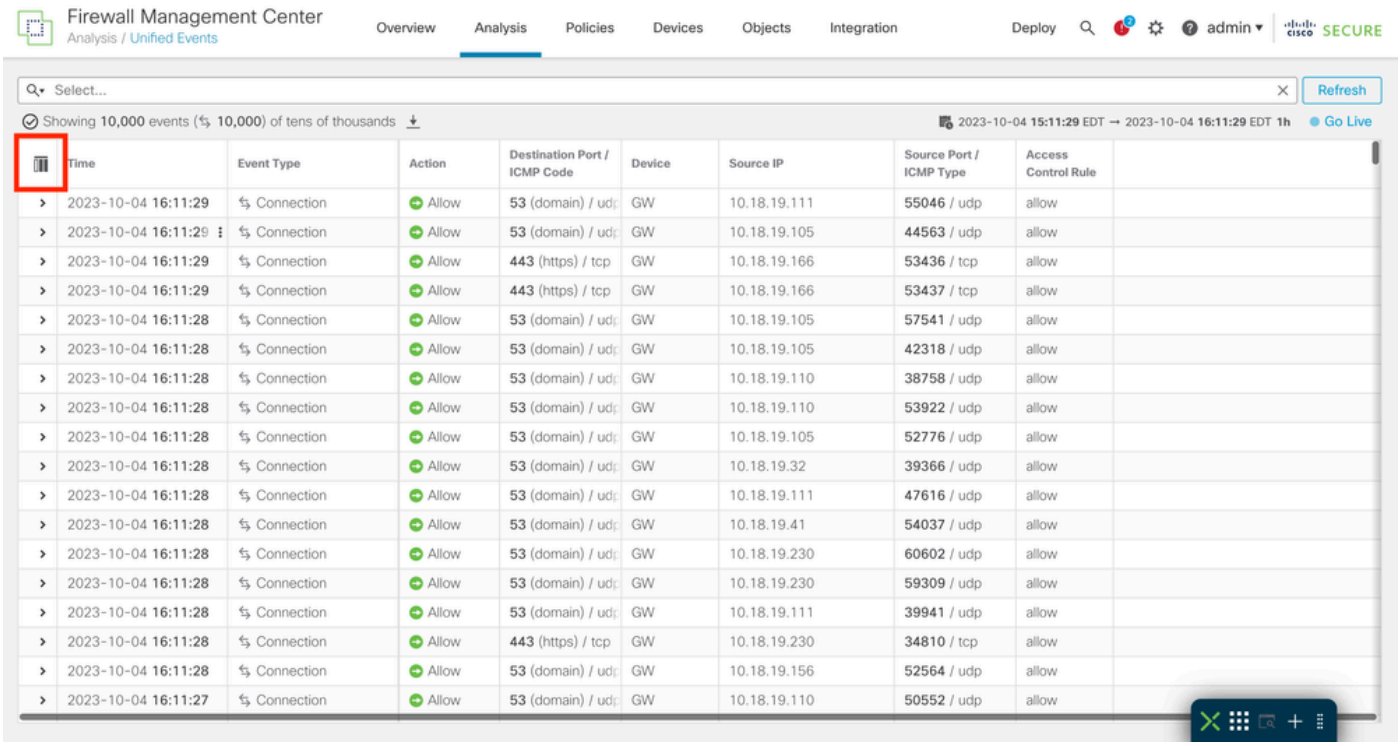


ステップ 2イベントの詳細情報が表示されます。

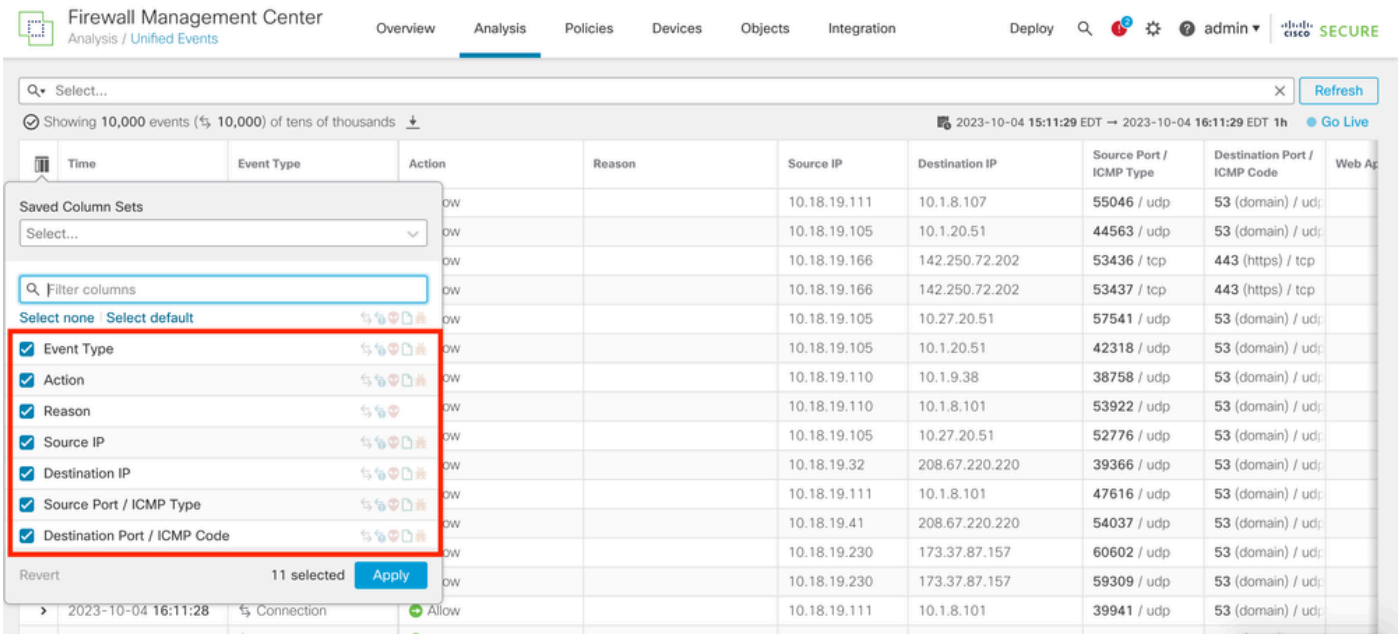


列のパーソナライズ

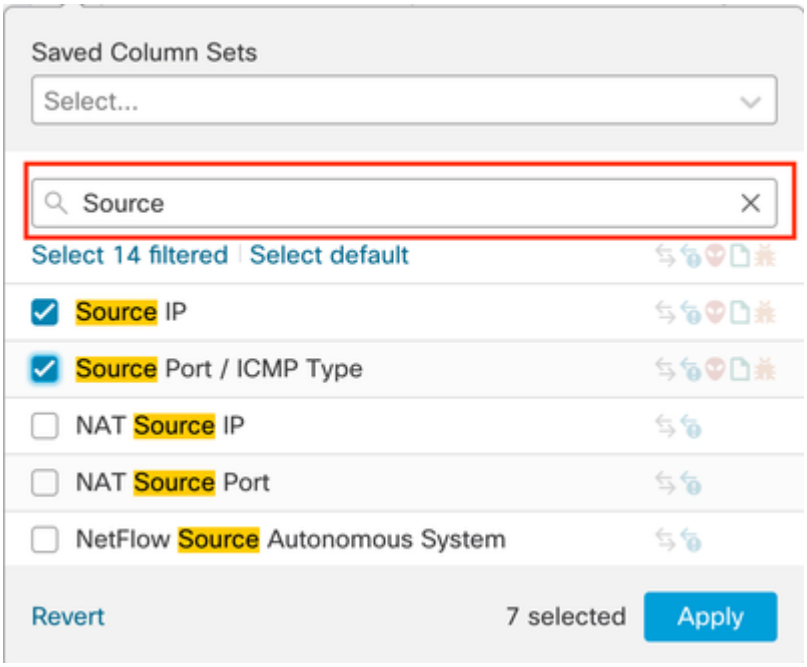
ステップ 1：アイコンをクリックします。  .



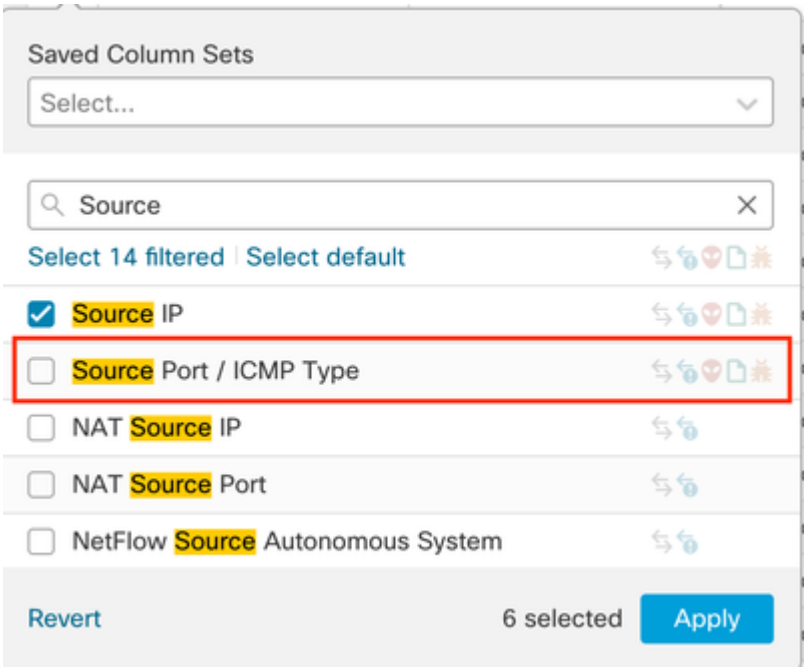
ステップ 2テーブルに表示するイベントフィールドを選択します。



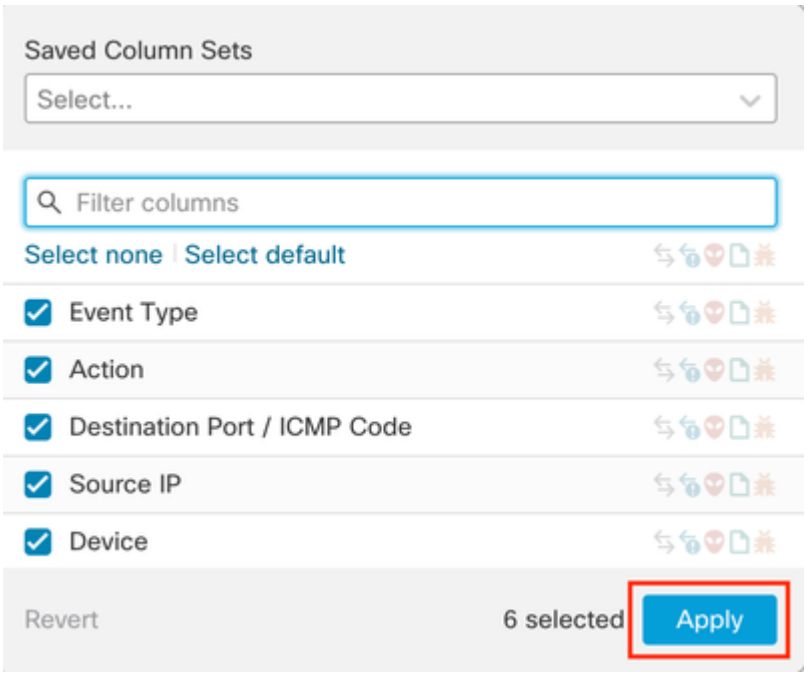
ステップ3: (オプション) フィールドを検索してナビゲーションを容易にします。



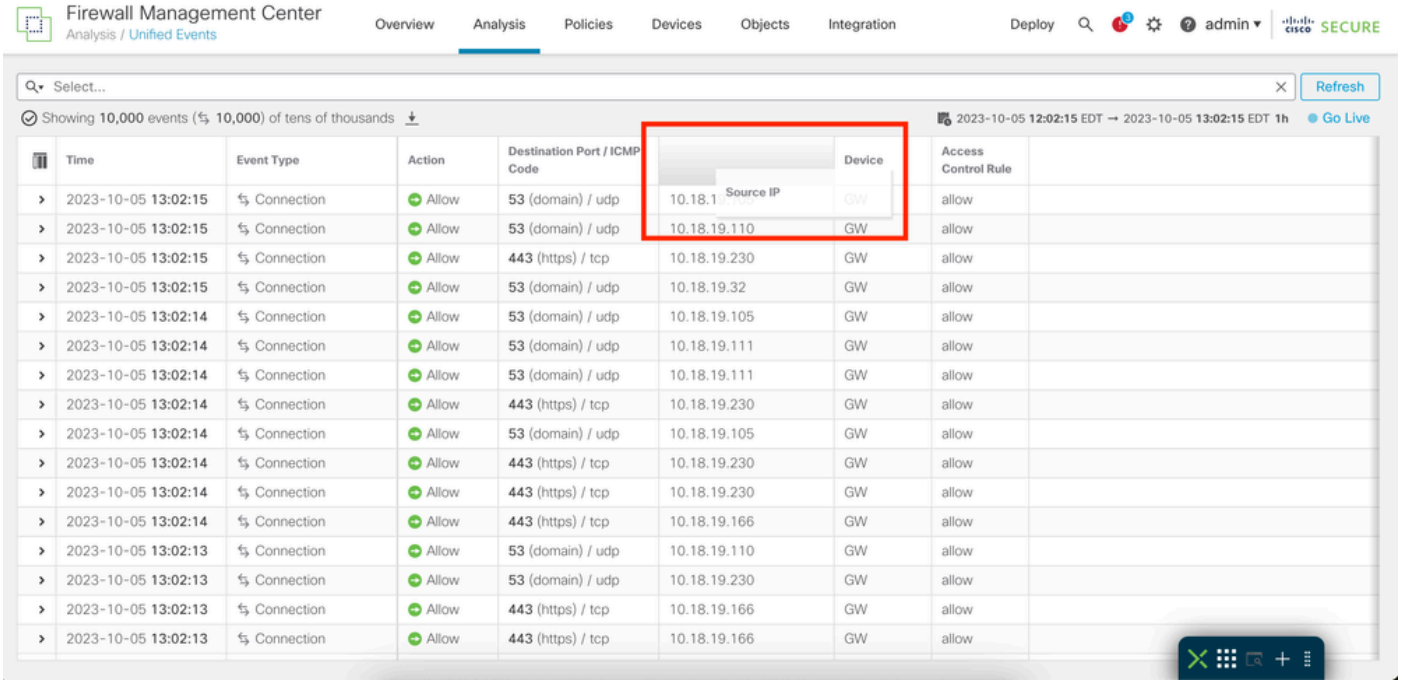
ステップ 4イベントフィールドをクリックして、無効または有効にします。



ステップ 5次に、[Apply] をクリックします。

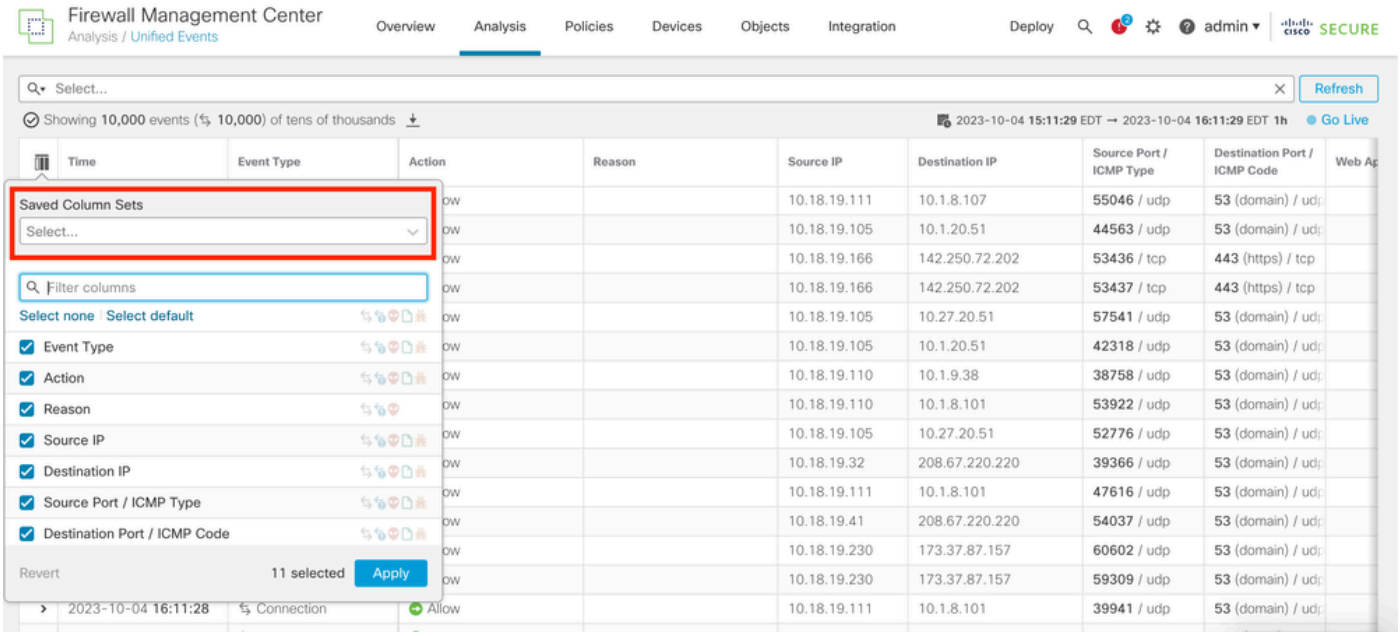


ステップ6:（オプション）各列を別の場所にドラッグして、列の位置を変更できます。

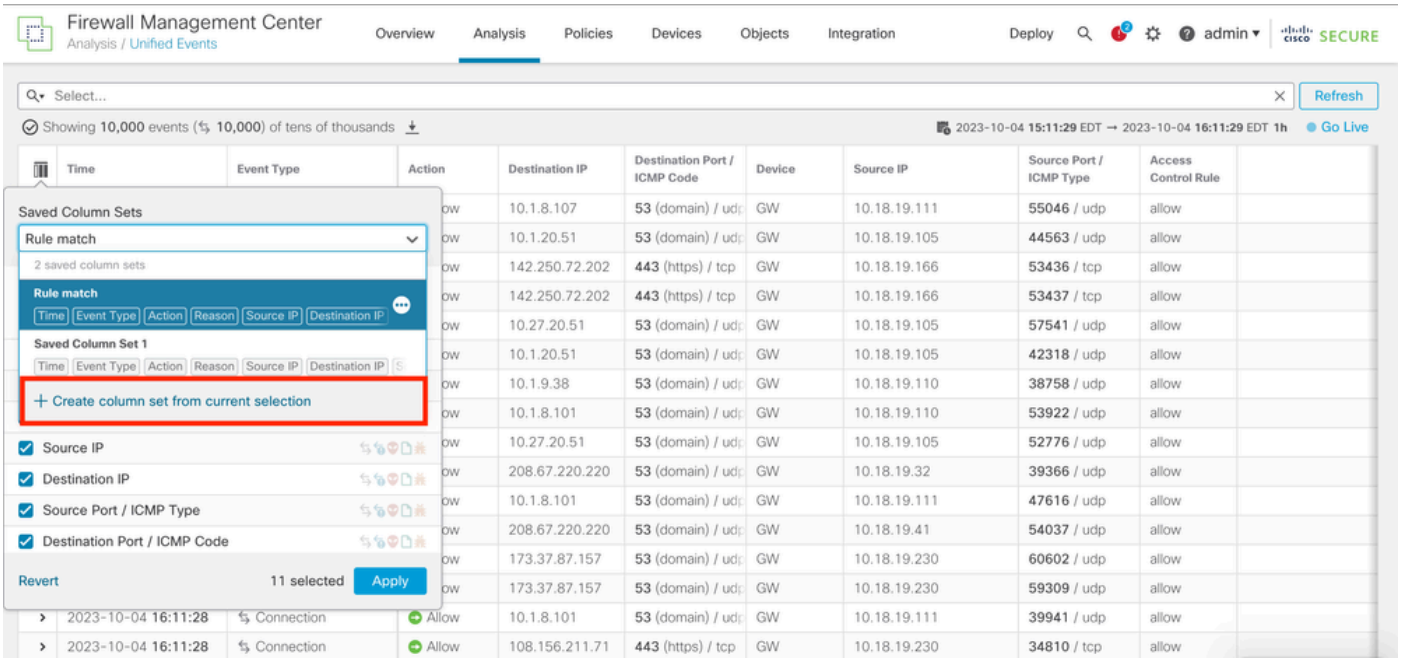


列セットの保存

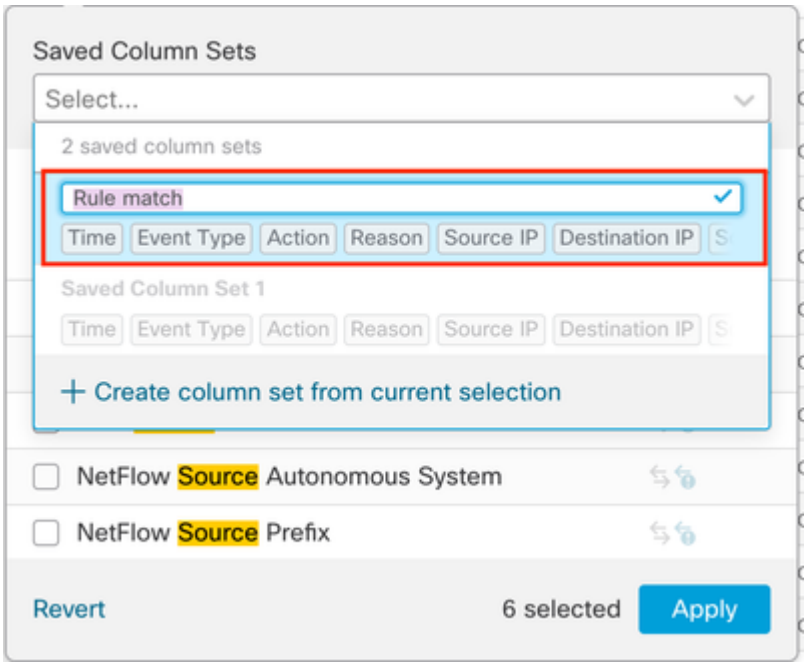
ステップ 1：Saved Column Setsをクリックします。



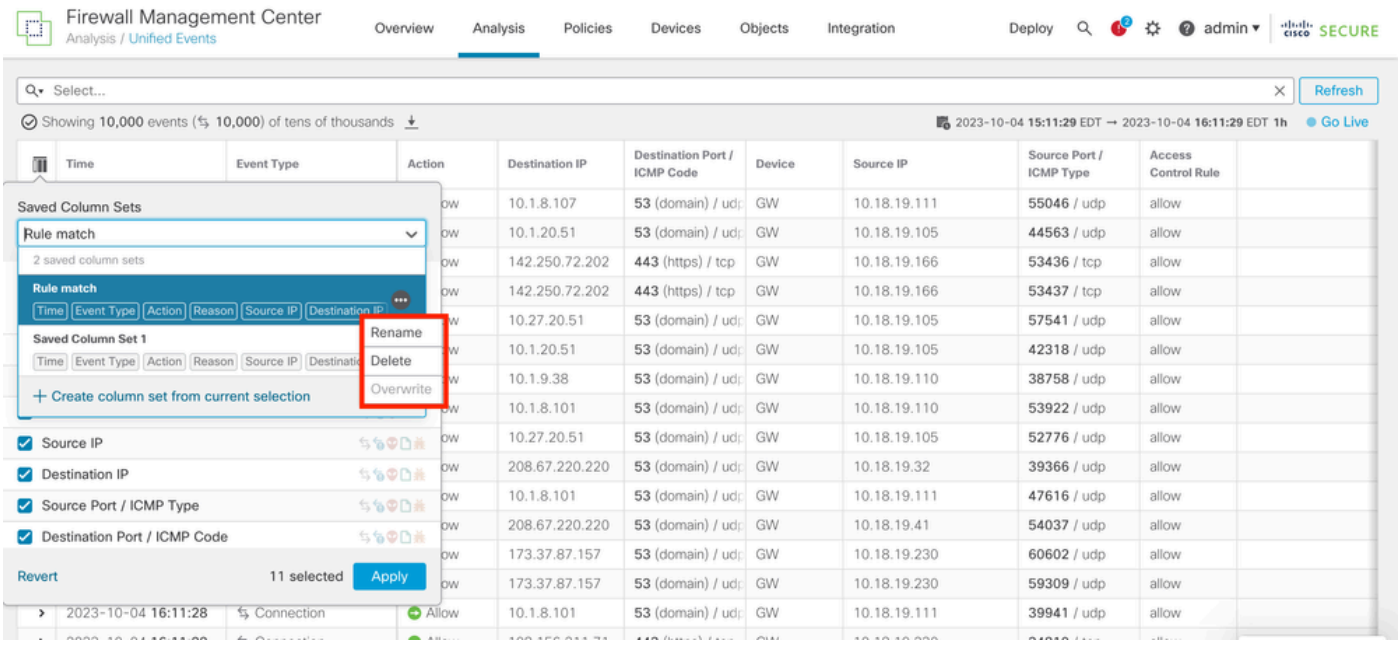
ステップ 2Create column set from current selectionをクリックします。



ステップ3: (オプション) 列セットの名前を変更します。

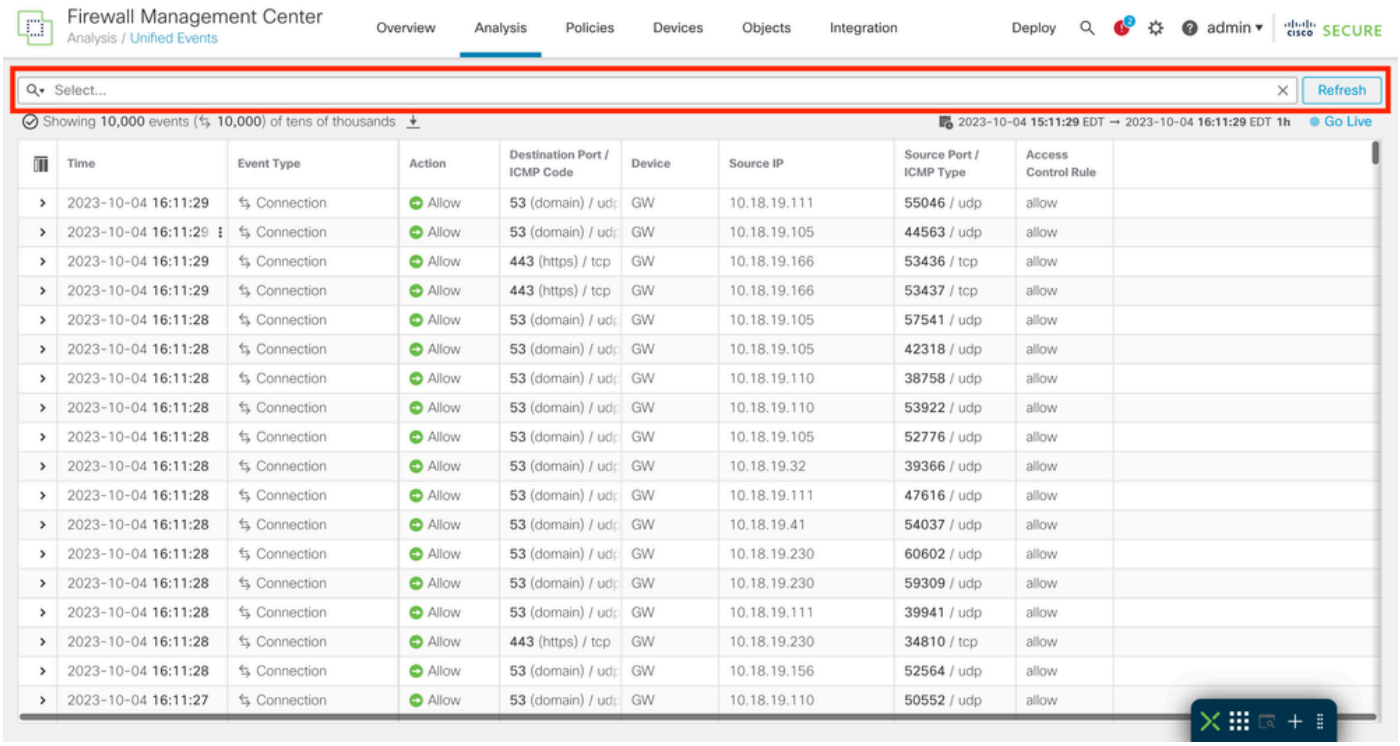


ステップ 4省略記号(...)をクリックすると、既存のセットを編集できます。

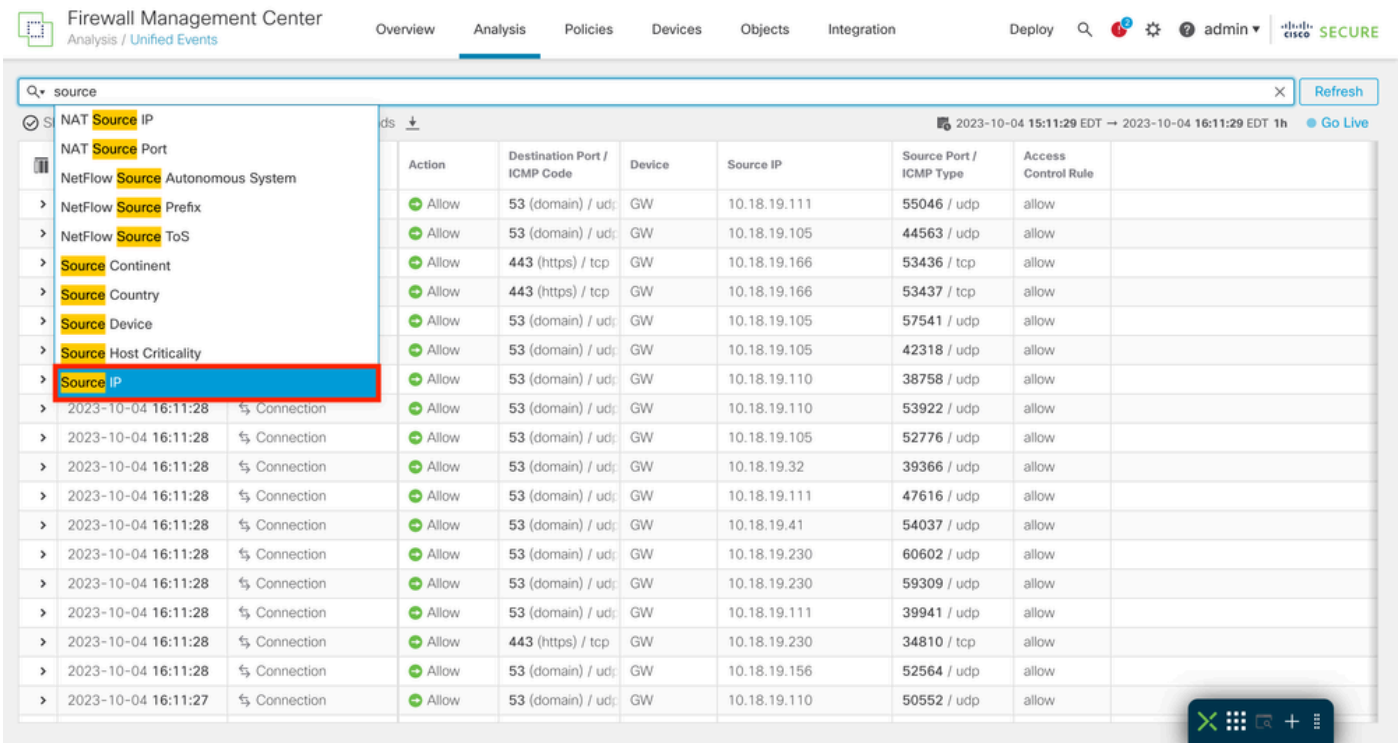


イベントの検索

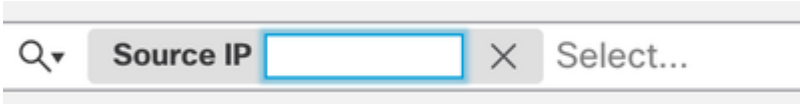
ステップ 1：特定のイベントの検索を開始するには、Selectをクリックします。



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。

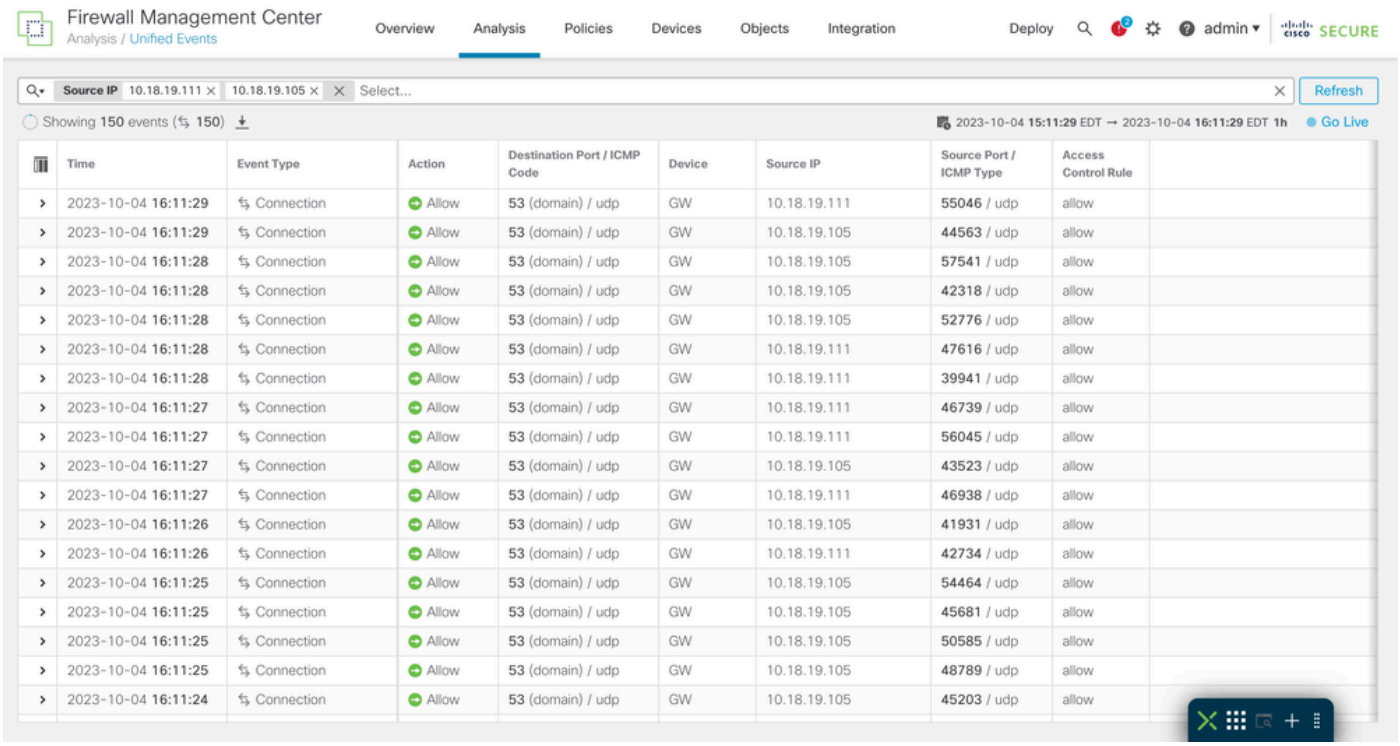


ステップ 3フィルタとして使用する値を記述します。

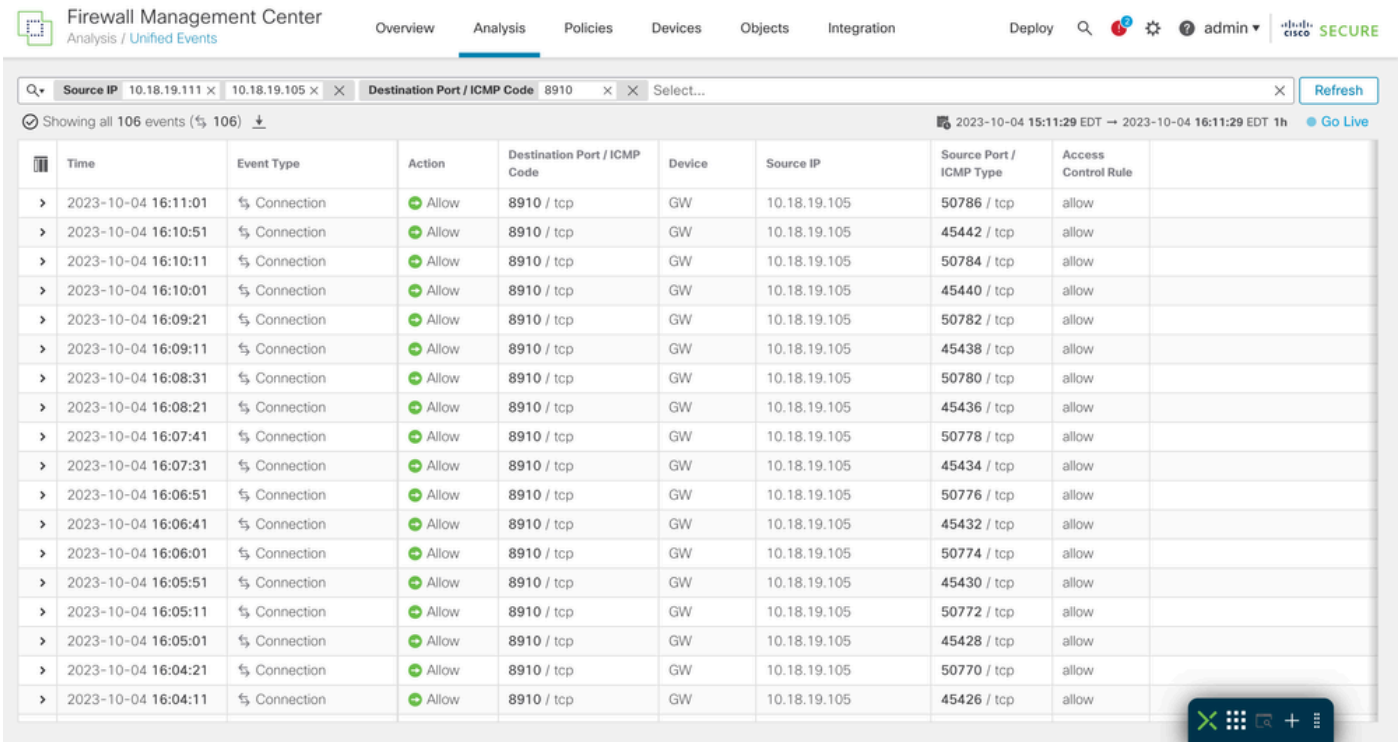


ステップ 4Applyをクリックして、フィルタを設定します。

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。



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。

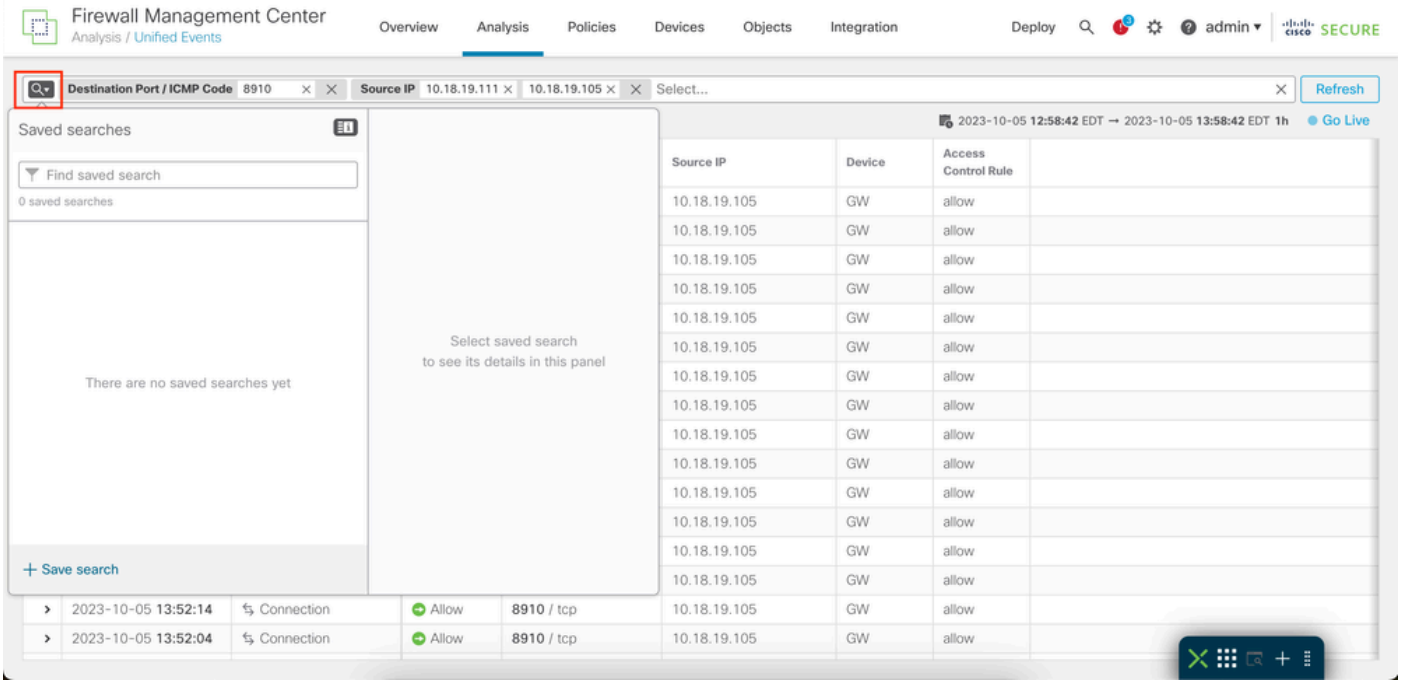


ヒント：値の書き込み時に演算子（>、<、！など）を使用できます。

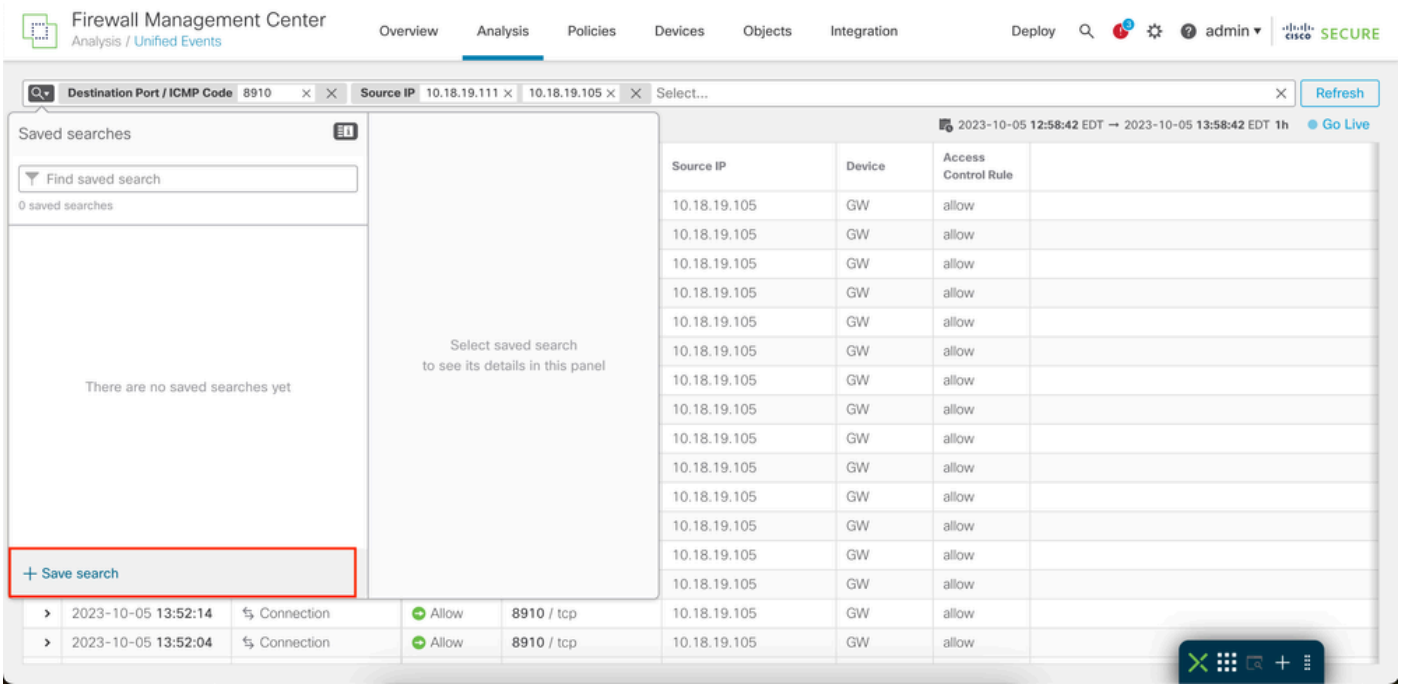
検索の保存

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。

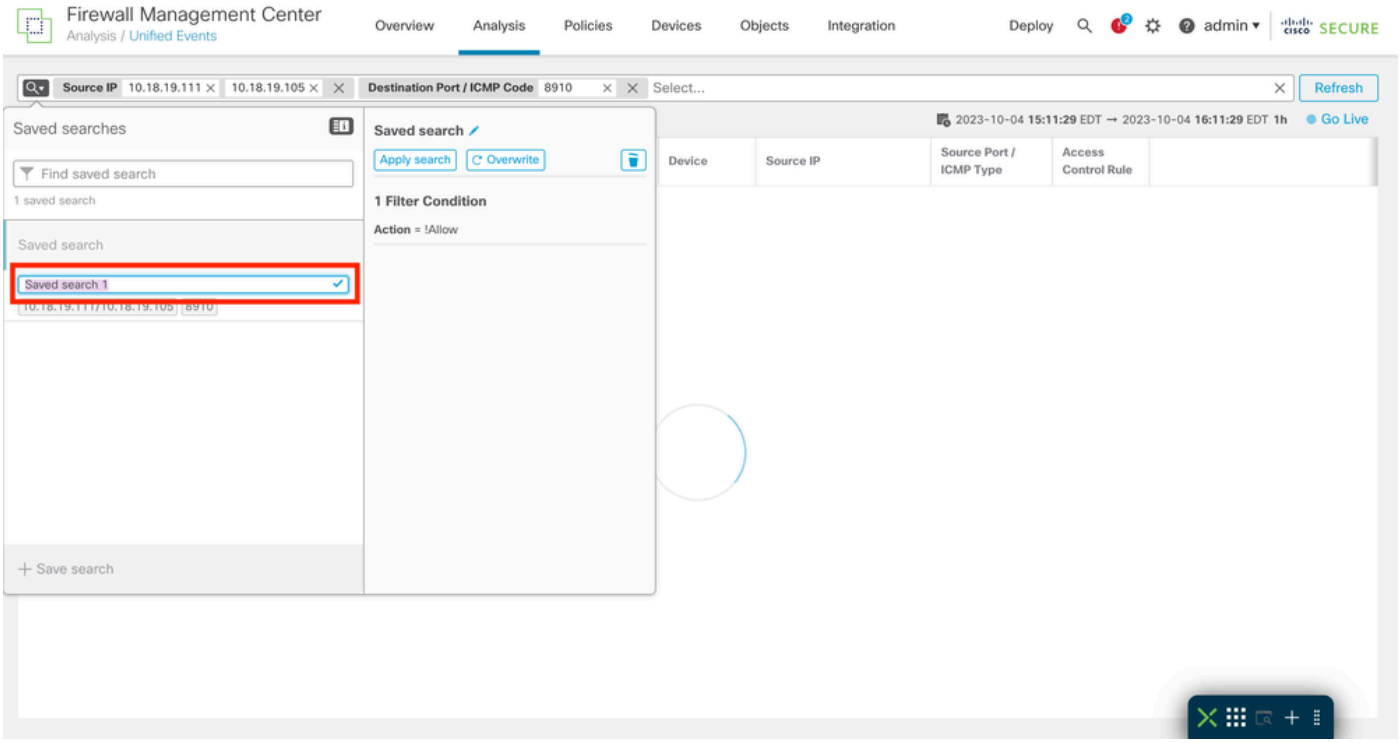
ステップ 1：虫めがねアイコンをクリックします。



ステップ 2Save Searchをクリックします。



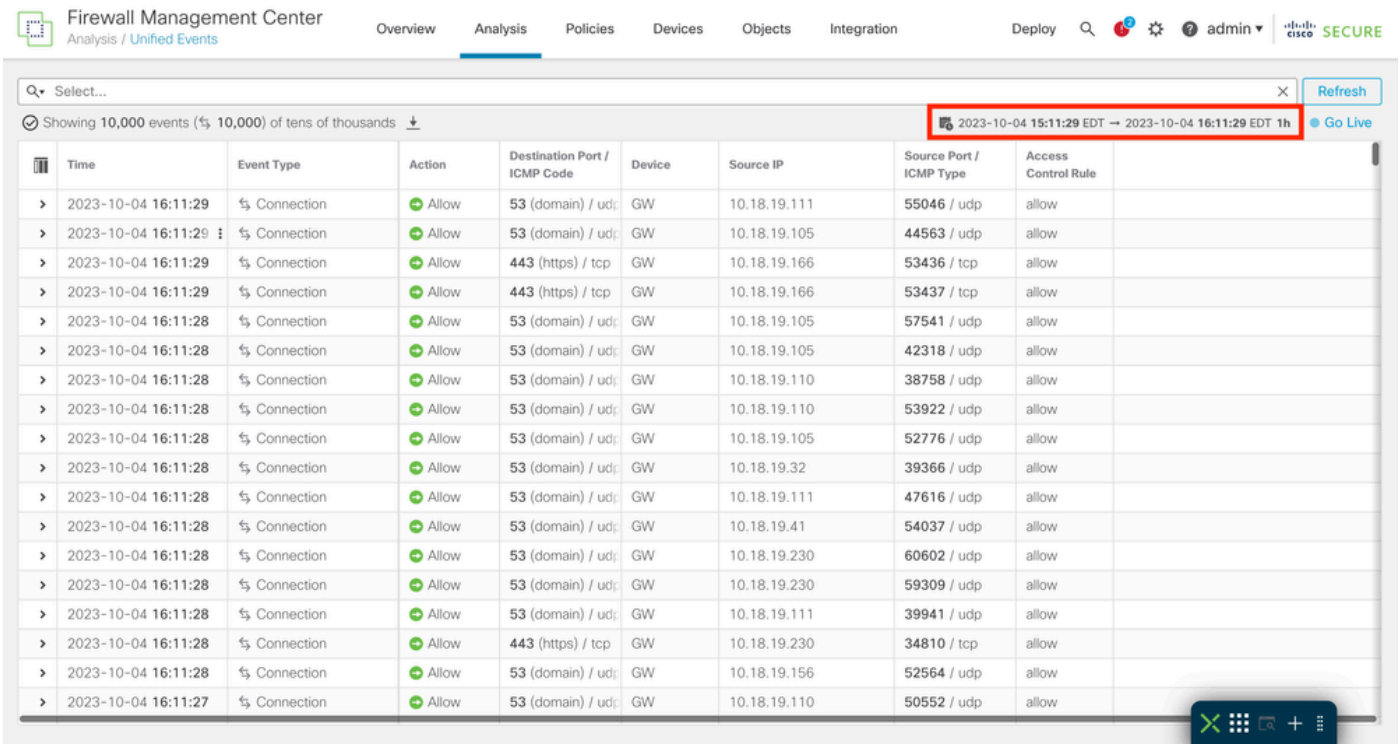
ステップ3:（オプション）検索名を変更します。



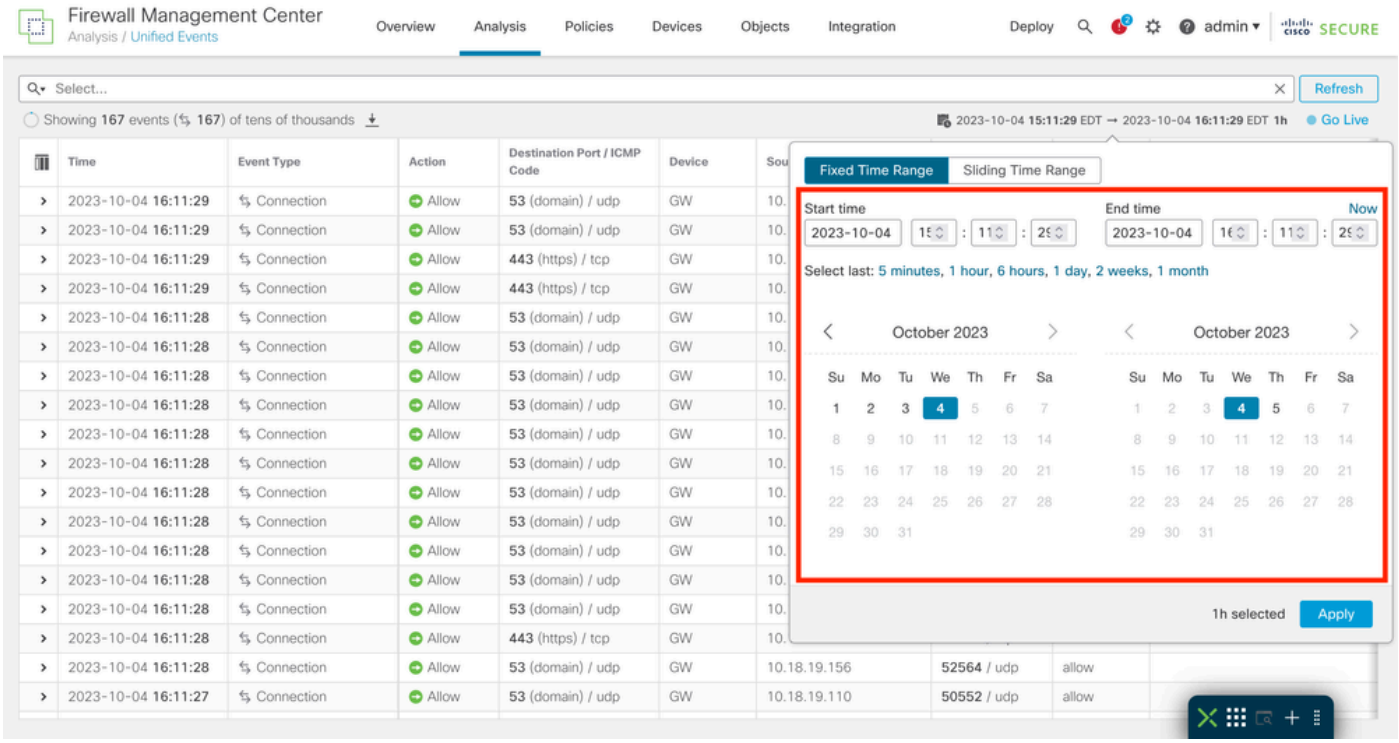
タイムウィンドウ

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。

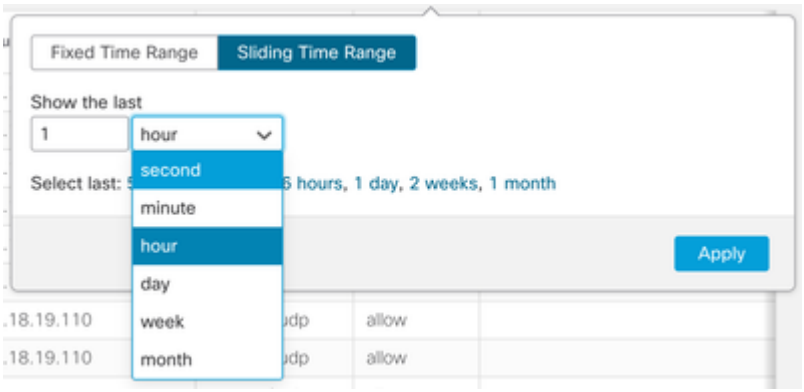
ステップ 1：イベントのウィンドウフレームを変更するには、日付範囲をクリックします。



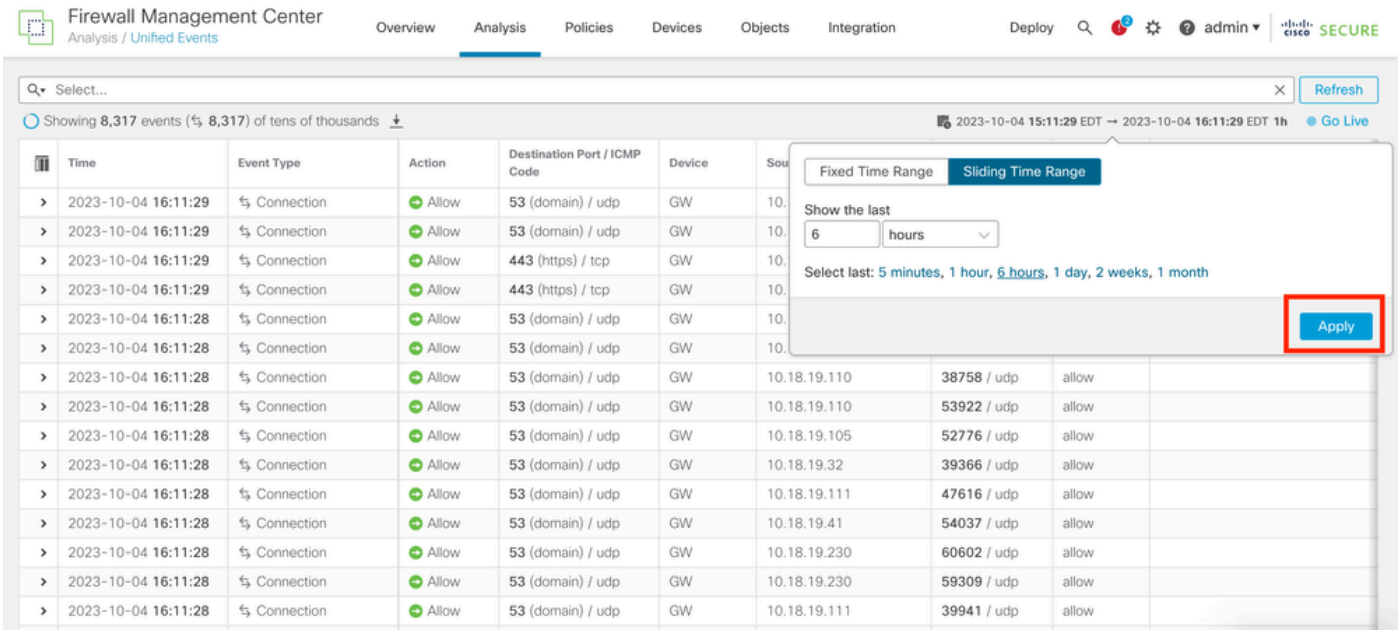
ステップ 2ポップアップウィンドウで時間の範囲を選択します。



ステップ3: (オプション) スライディング時間範囲を使用して、特定の時間から現在の時間までのイベントを表示します。



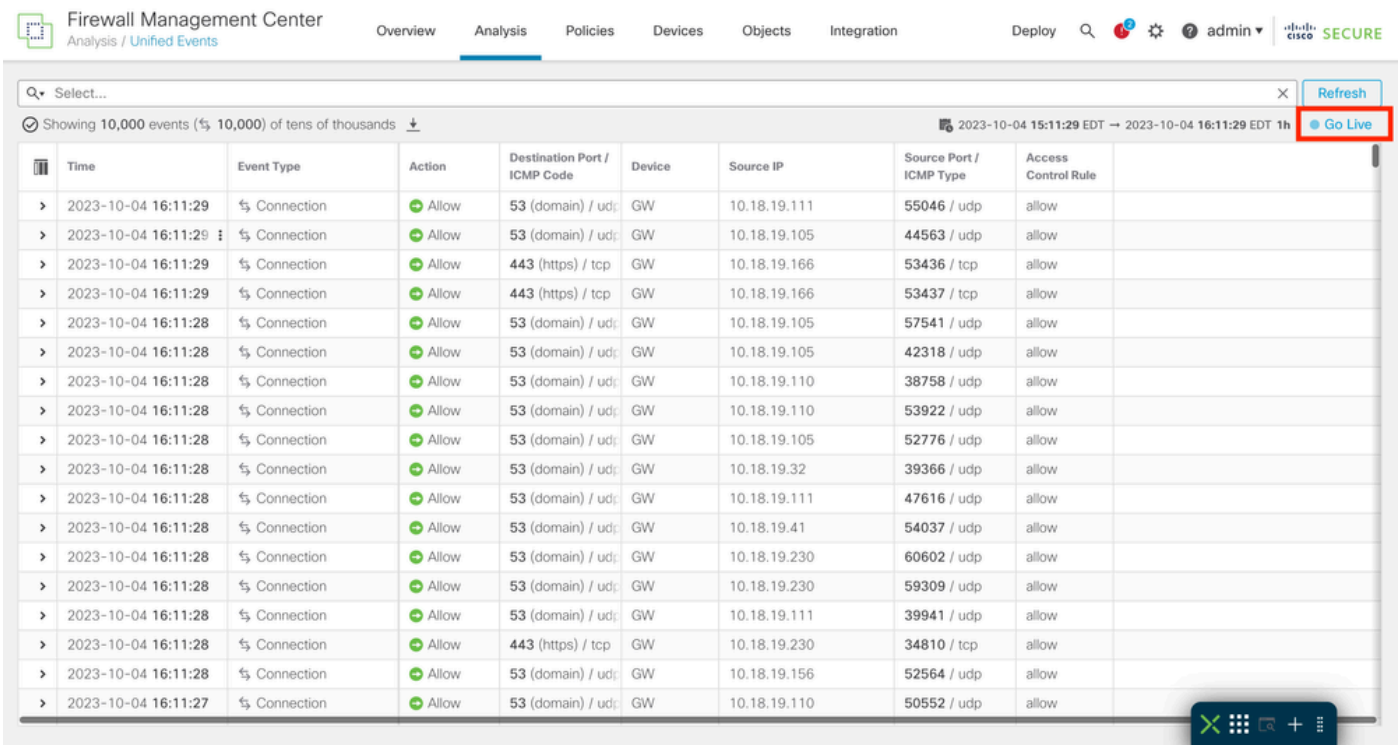
ステップ 4Applyをクリックして、設定した時間範囲でイベントをフィルタリングします。



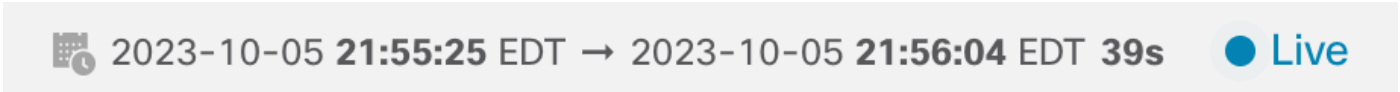
稼動

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。



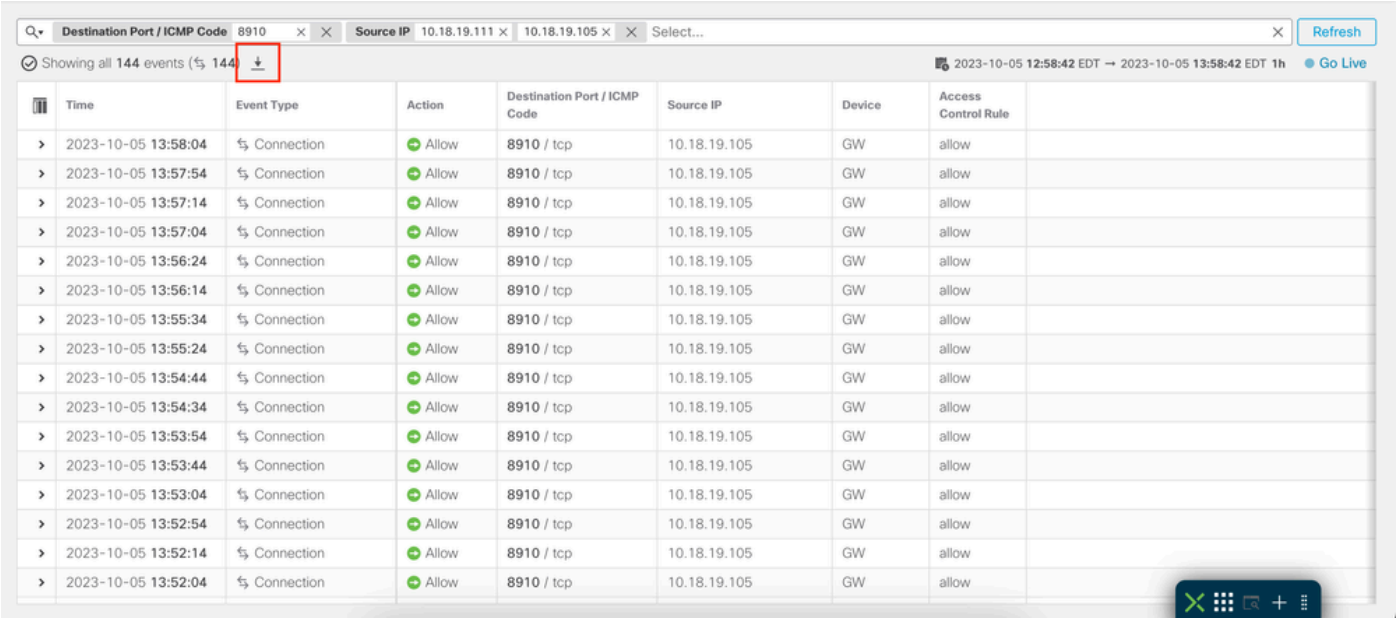
有効にすると、Liveという単語が表示されます。



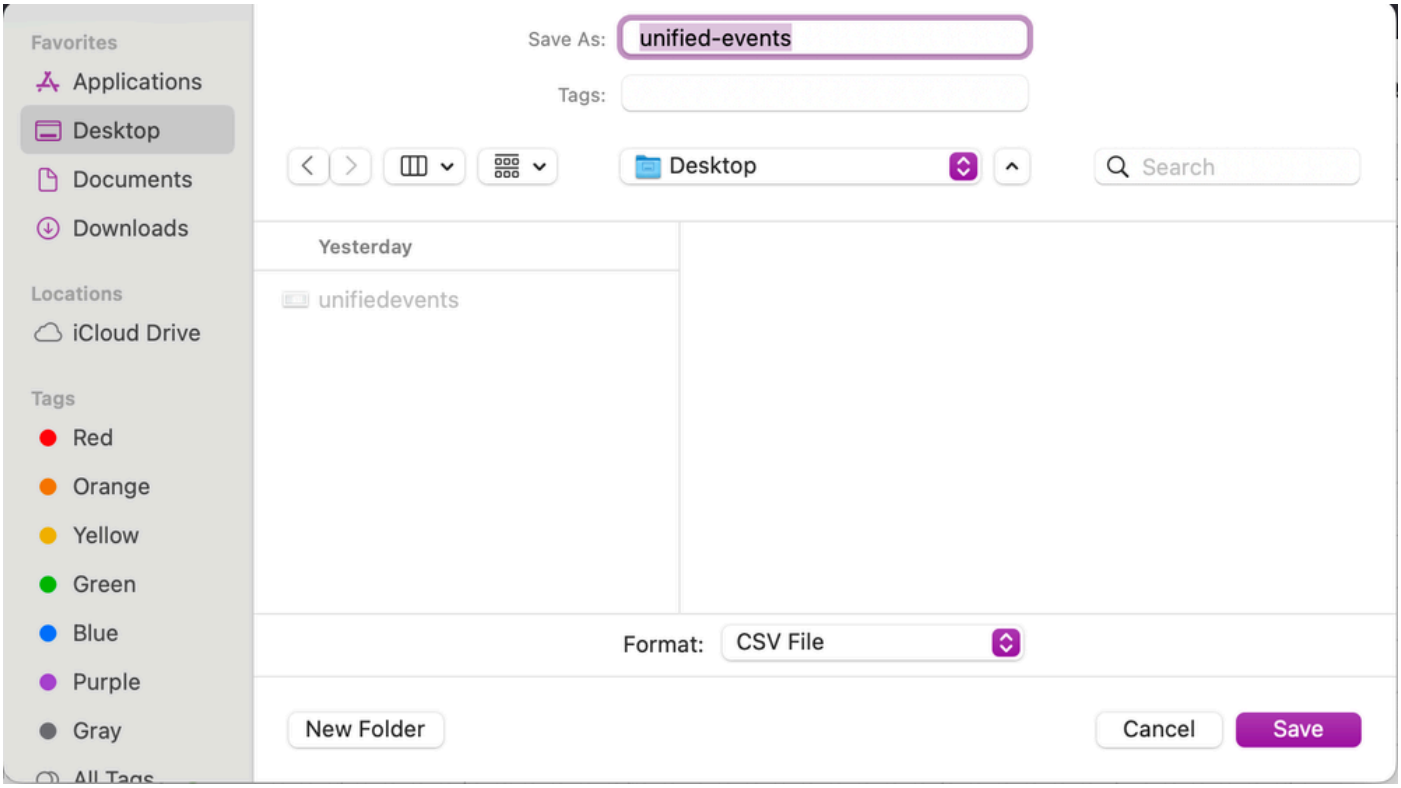
⚠ 注意:Liveが有効になっていると、時間帯を変更できません。タイムウィンドウを変更するには、まず再度クリックしてライブオプションを無効にします。

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。



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 3CSV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。