# Monitore eventos usando o Unified Event Viewer na GUI do FMC

## Contents



## Introdução

Este documento descreve o uso do Unified Event Viewer em uma interface gráfica de usuário (GUI) no Firewall Management Center (FMC).

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso ao FMC com privilégios de administrador ou analista de segurança
- FMC com versão igual ou superior a v7.0

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

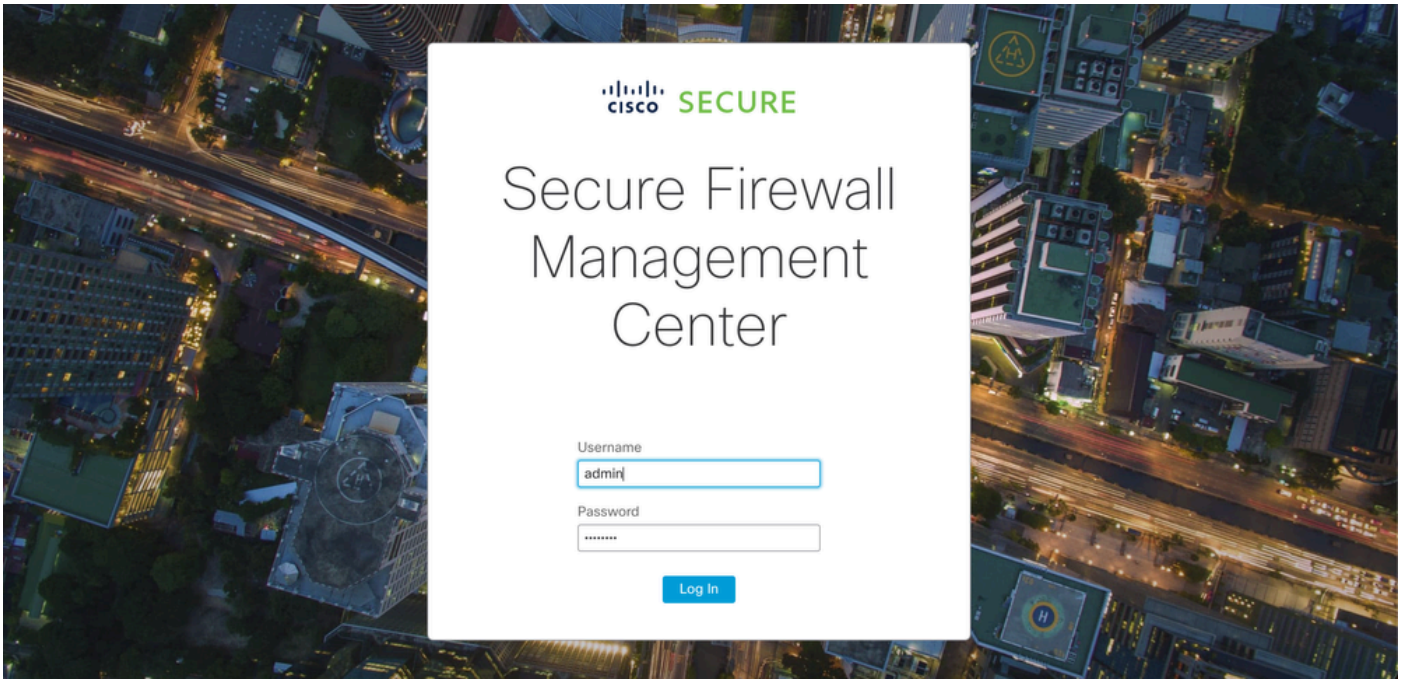
- Secure Firewall Management Center para VMware v7.2.5

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

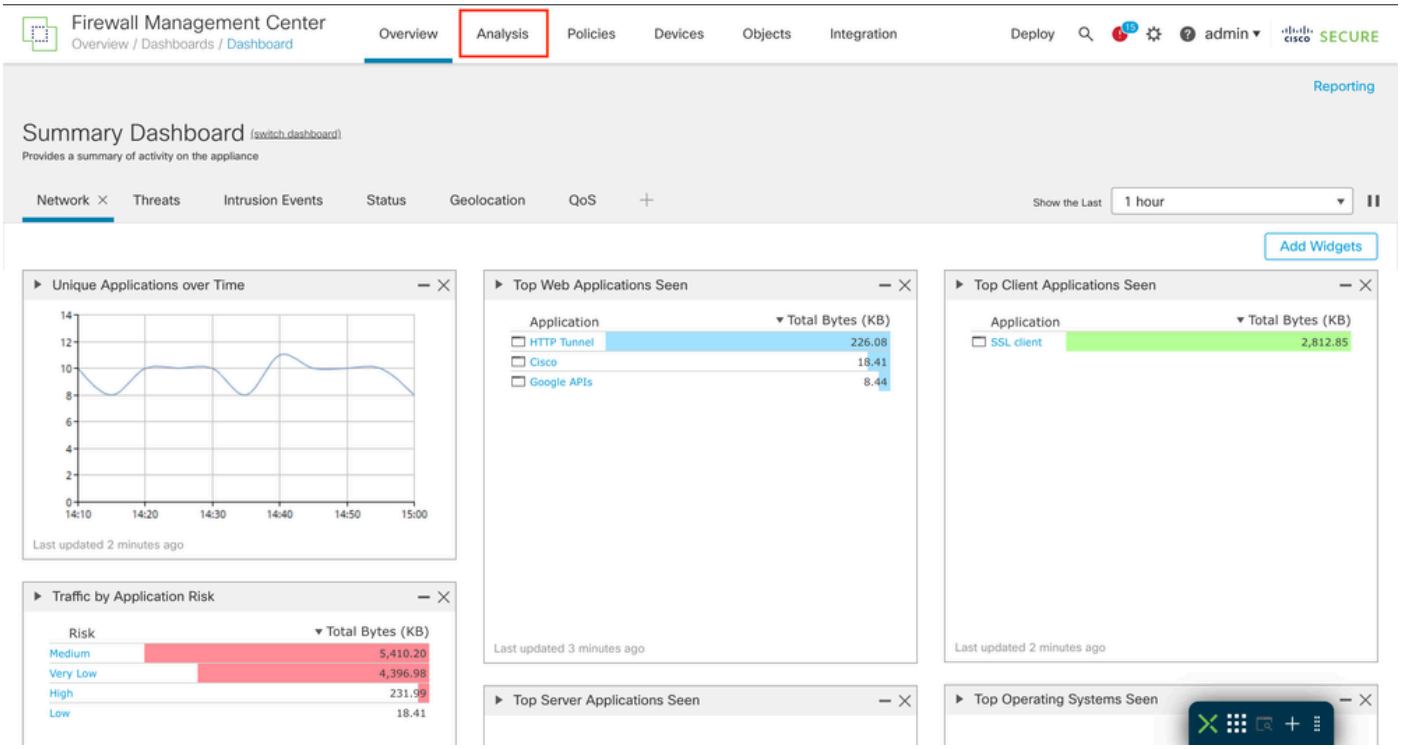
configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Explorar

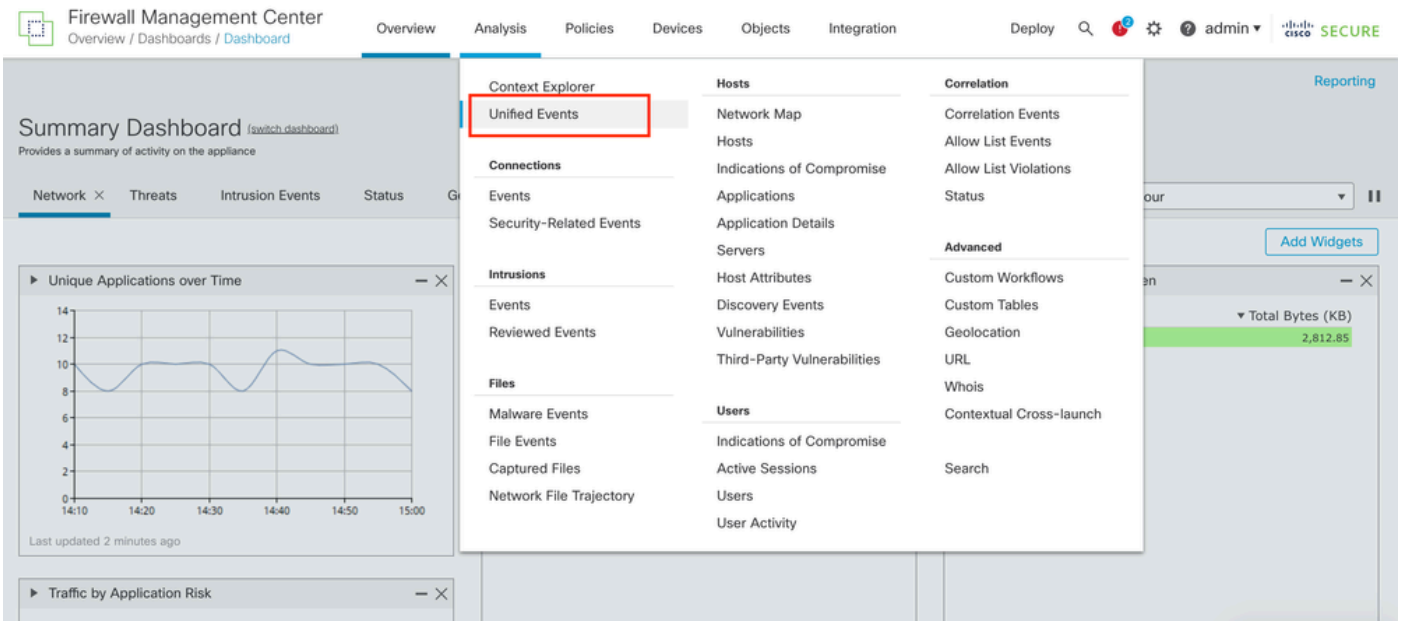
Etapa 1. Fazer login na GUI do FMC.



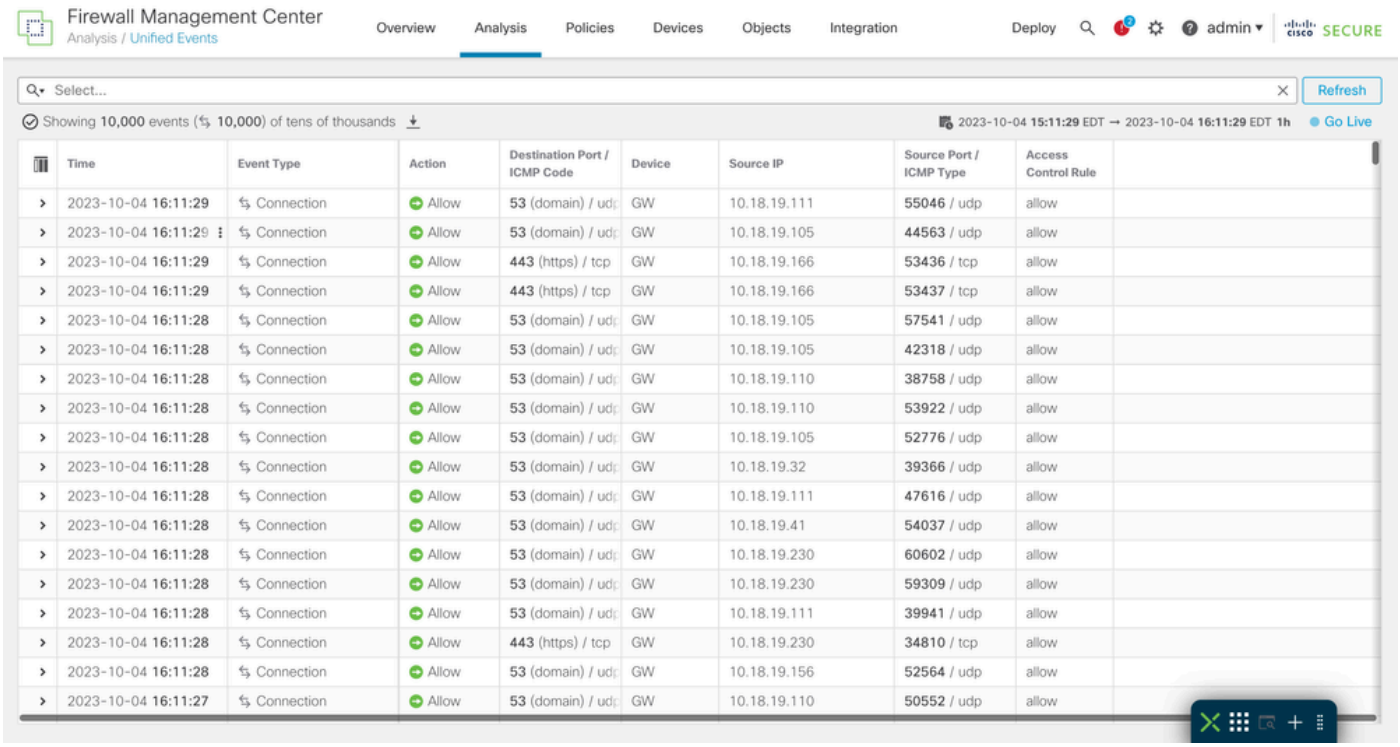

Etapa 2. Navegue até a guia Análise.




Etapa 3. No menu suspenso, clique em Unified Events.

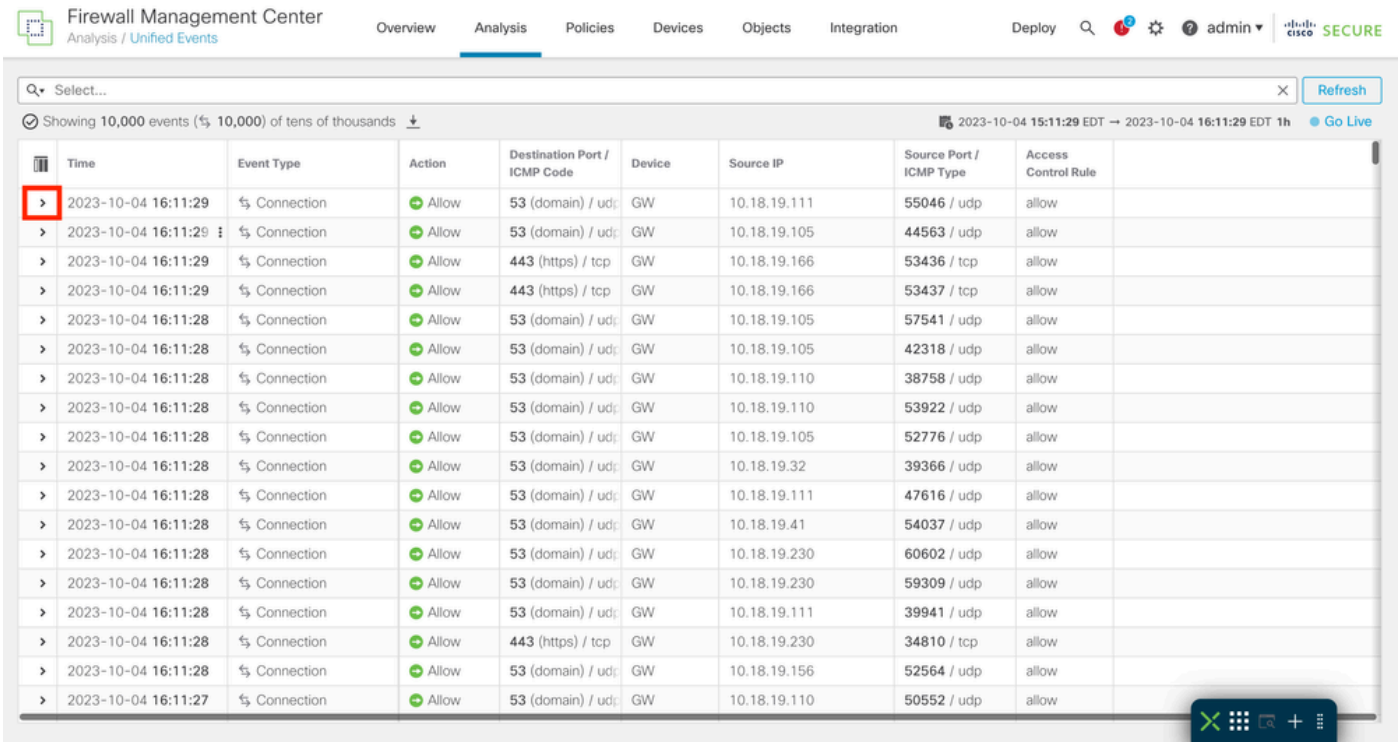



Exemplo da página de eventos unificados

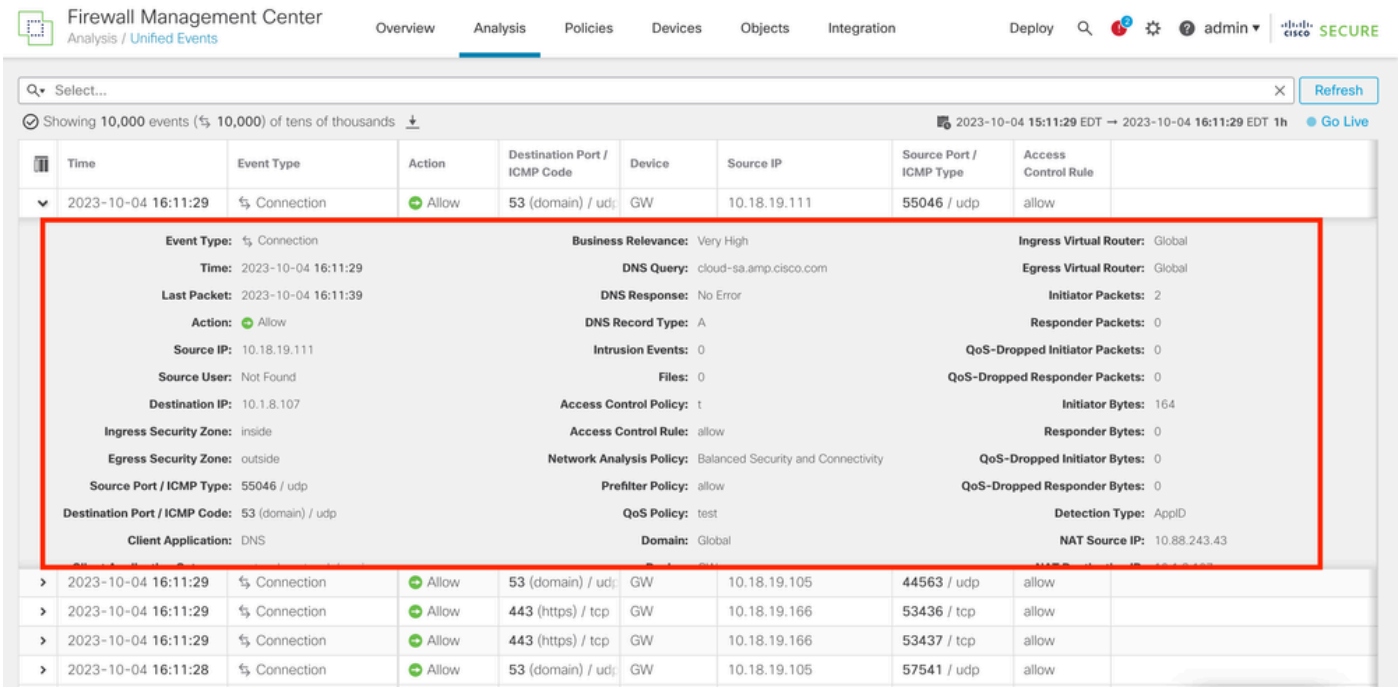



# Revisar eventos

Etapa 1. Clique no ícone > .

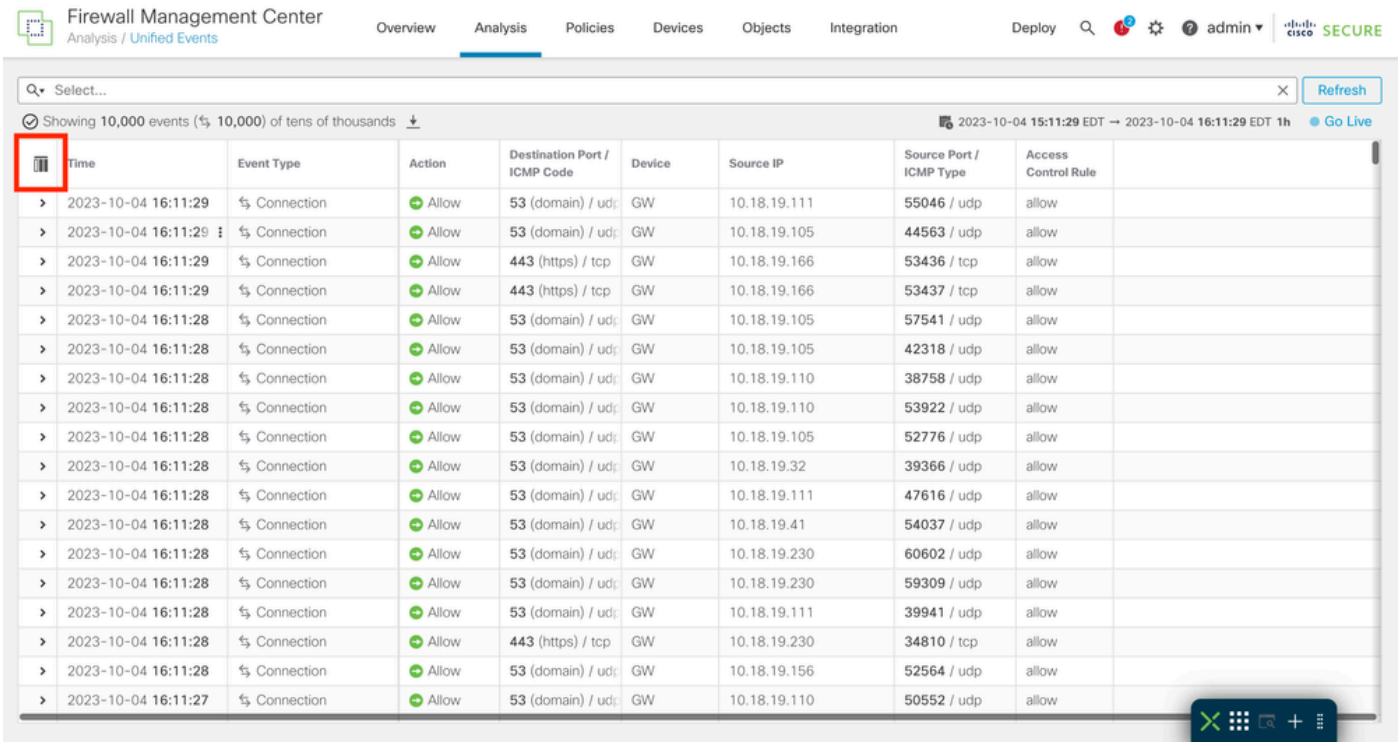



Etapa 2. As informações detalhadas do evento são exibidas.

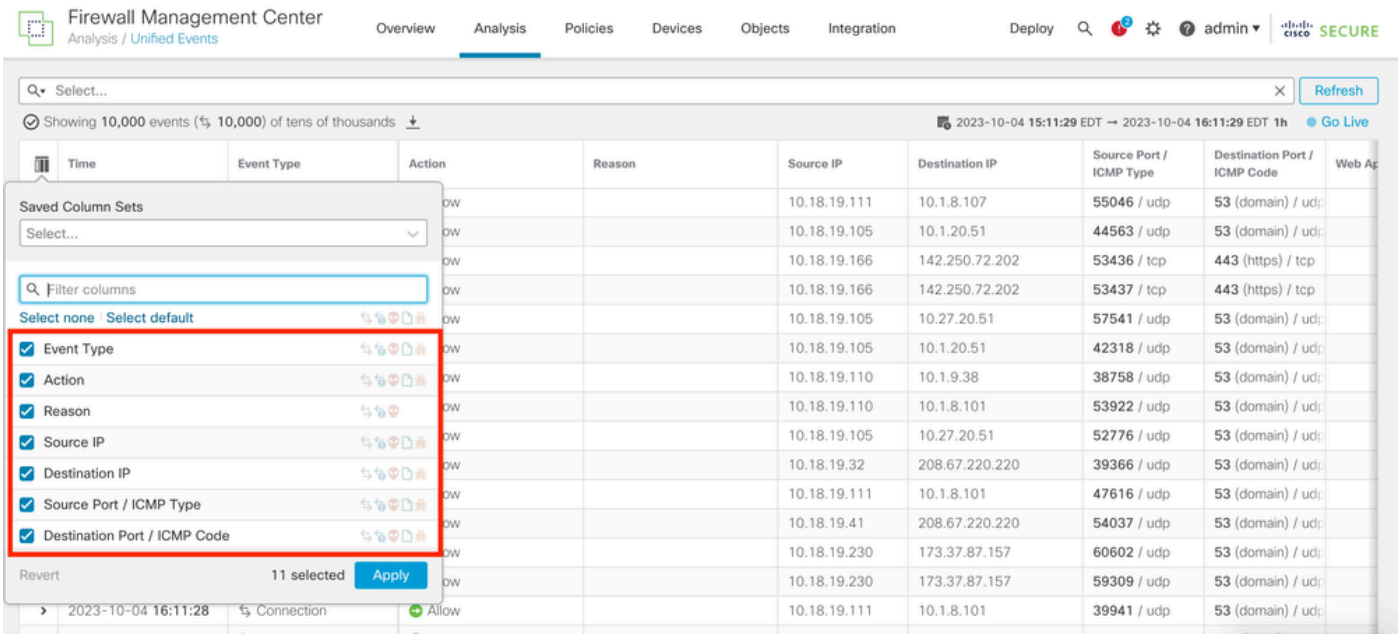



# Personalizar Colunas

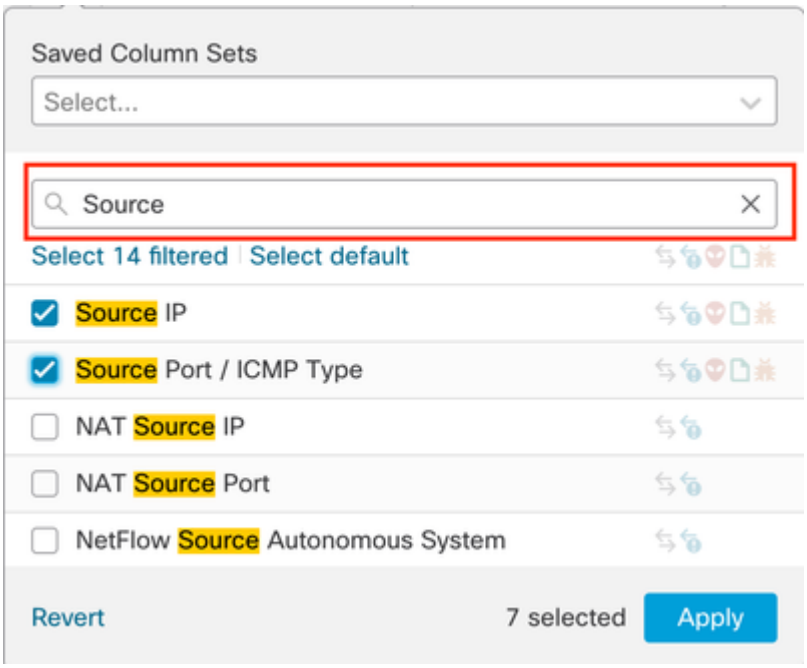
Etapa 1. Clique no ícone .



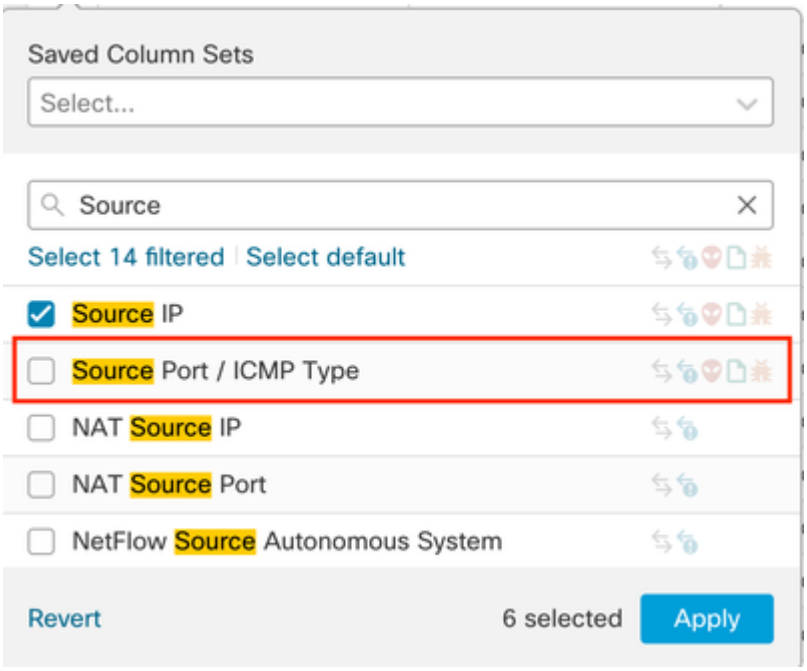

Etapa 2. Selecione os campos de evento desejados na tabela.



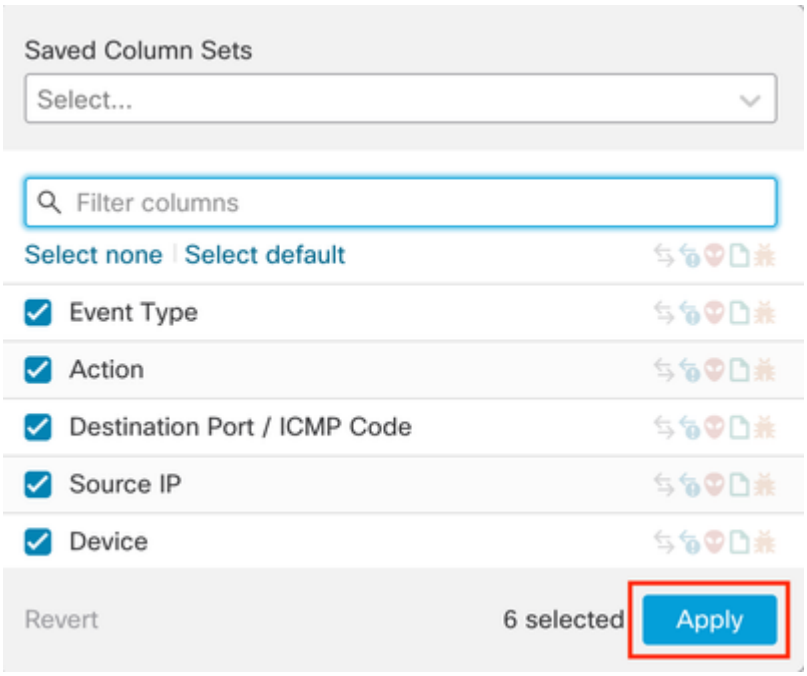

Etapa 3. (Opcional) Procure o campo para facilitar a navegação.



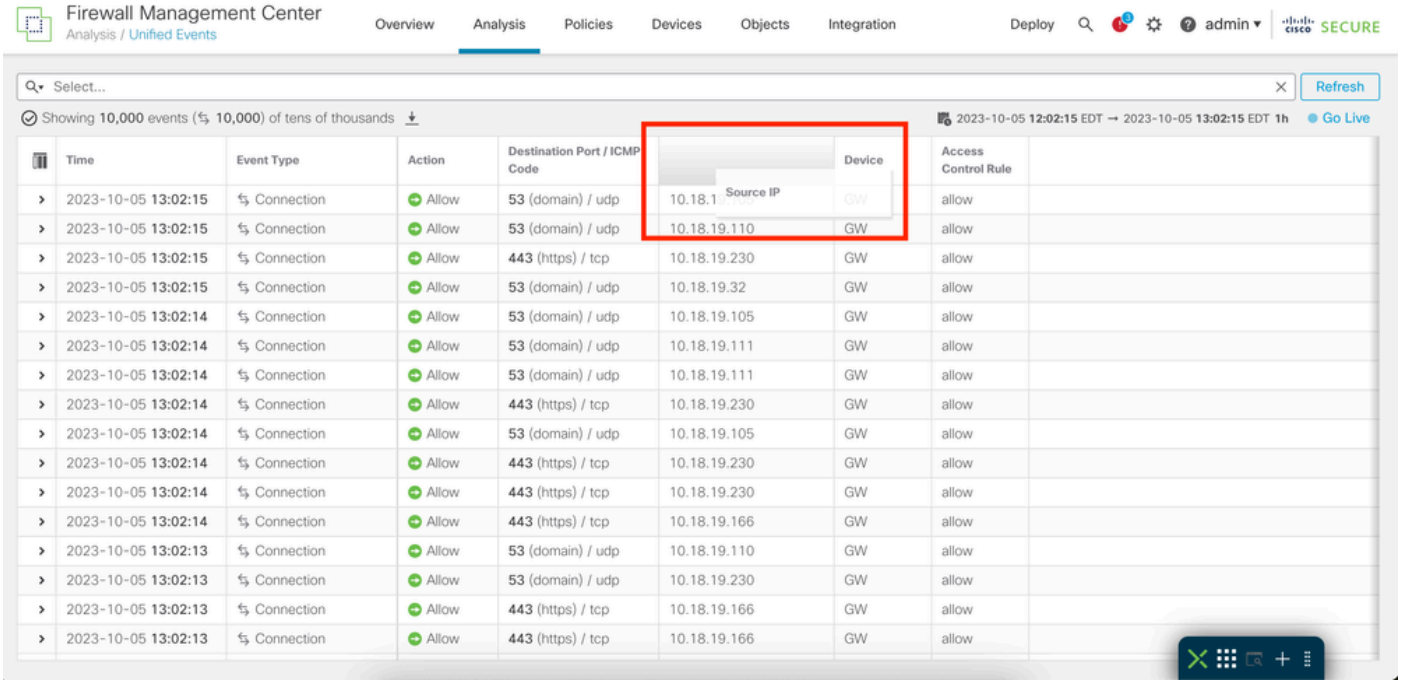

Etapa 4. Clique em um campo de evento para desativar ou ativar.




Etapa 5. Clique em Apply.

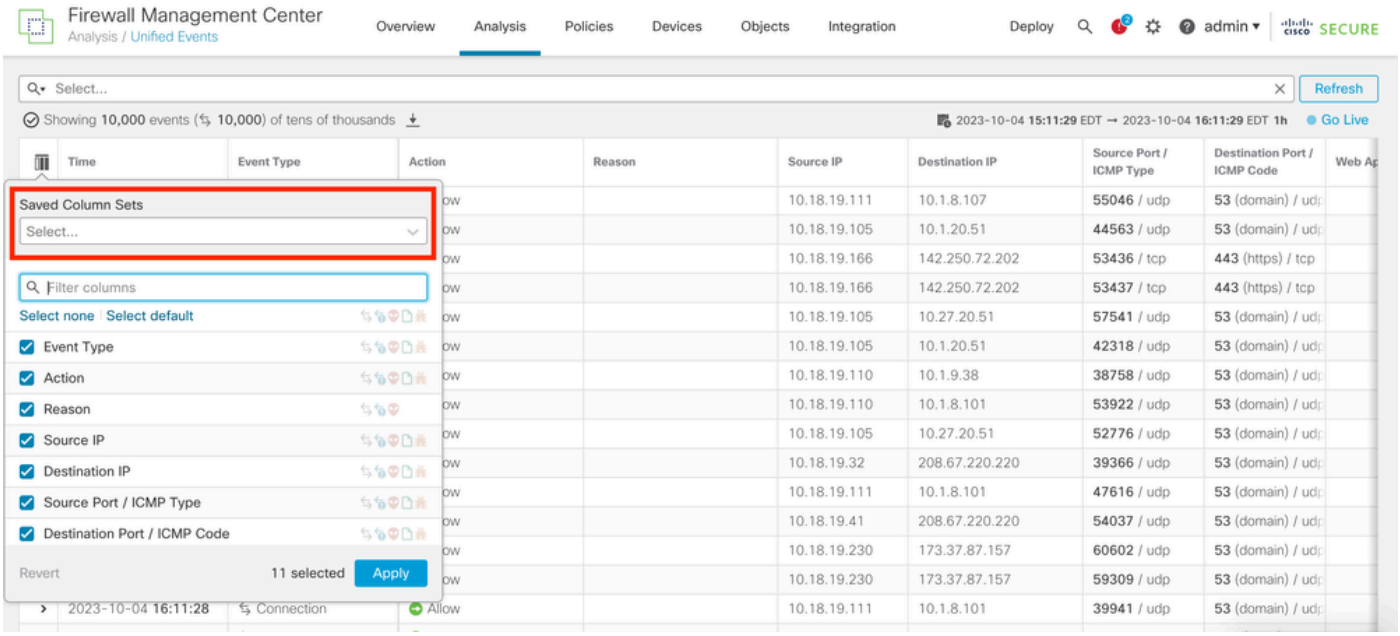



Etapa 6. (Opcional) Você pode reposicionar as colunas arrastando cada uma delas para um local diferente.

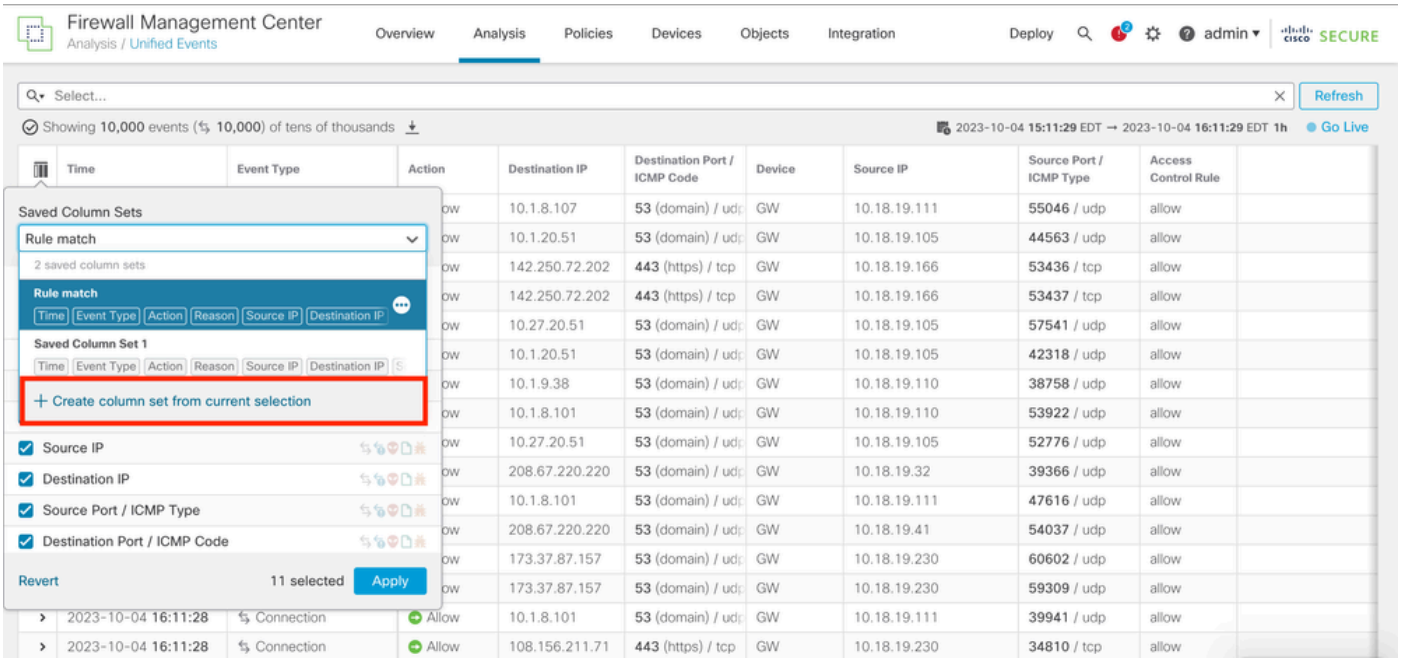



## Salvar Conjunto de Colunas

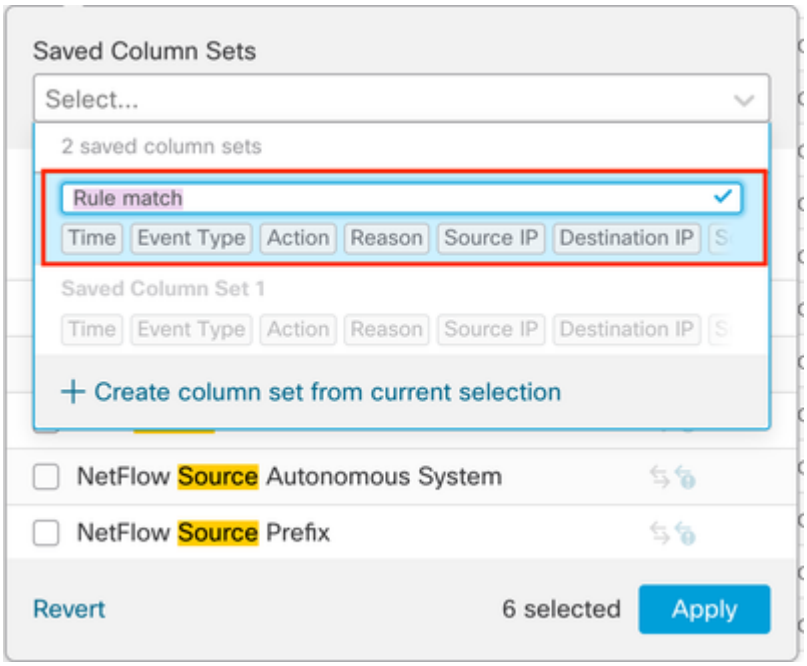
Etapa 1. Clique em Conjuntos de Colunas Salvas.



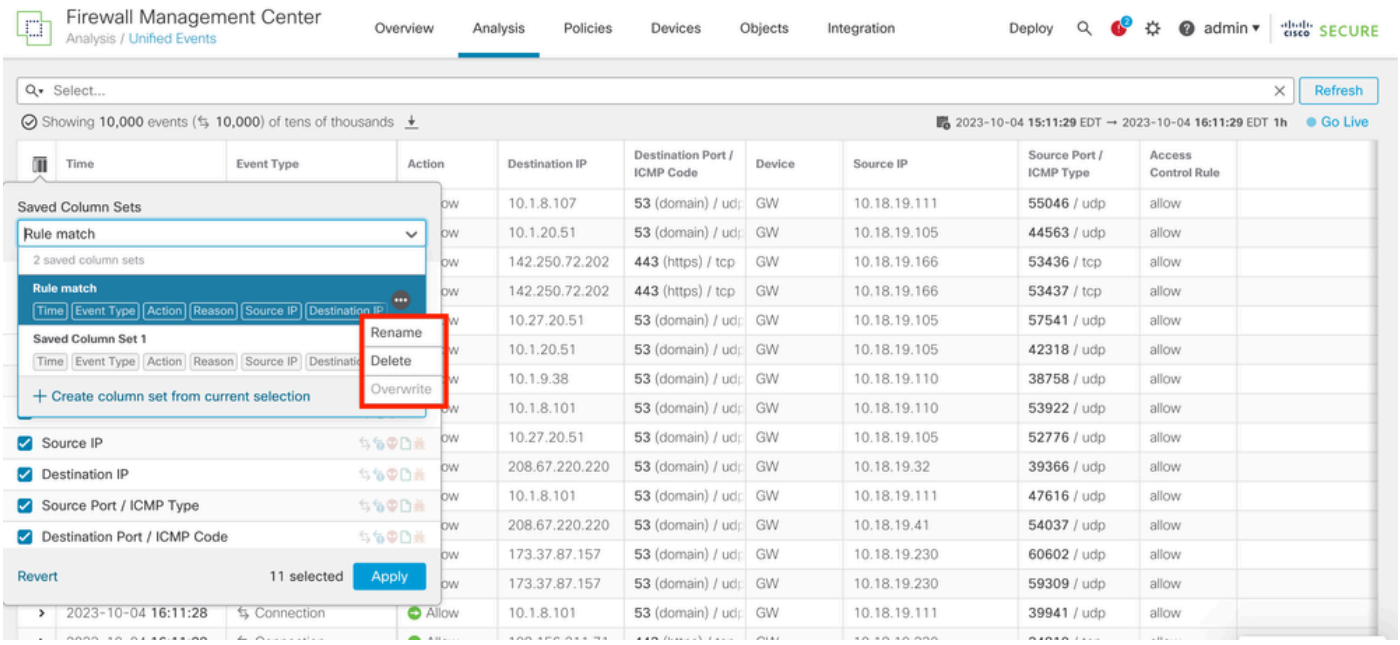

Etapa 2. Clique em Criar conjunto de colunas a partir da seleção atual.




Etapa 3. (Opcional) Altere o nome do conjunto de colunas.

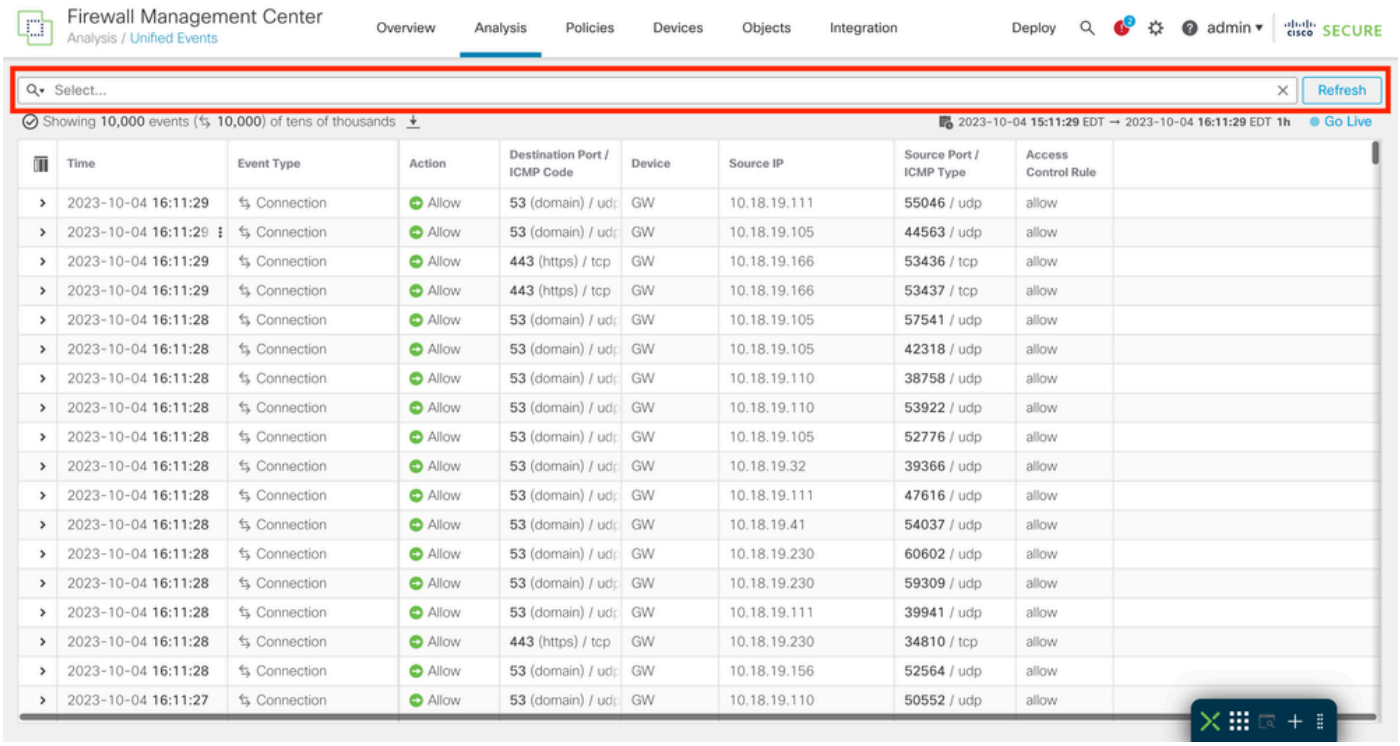



Etapa 4. Você pode editar um conjunto existente clicando nas reticências (...).

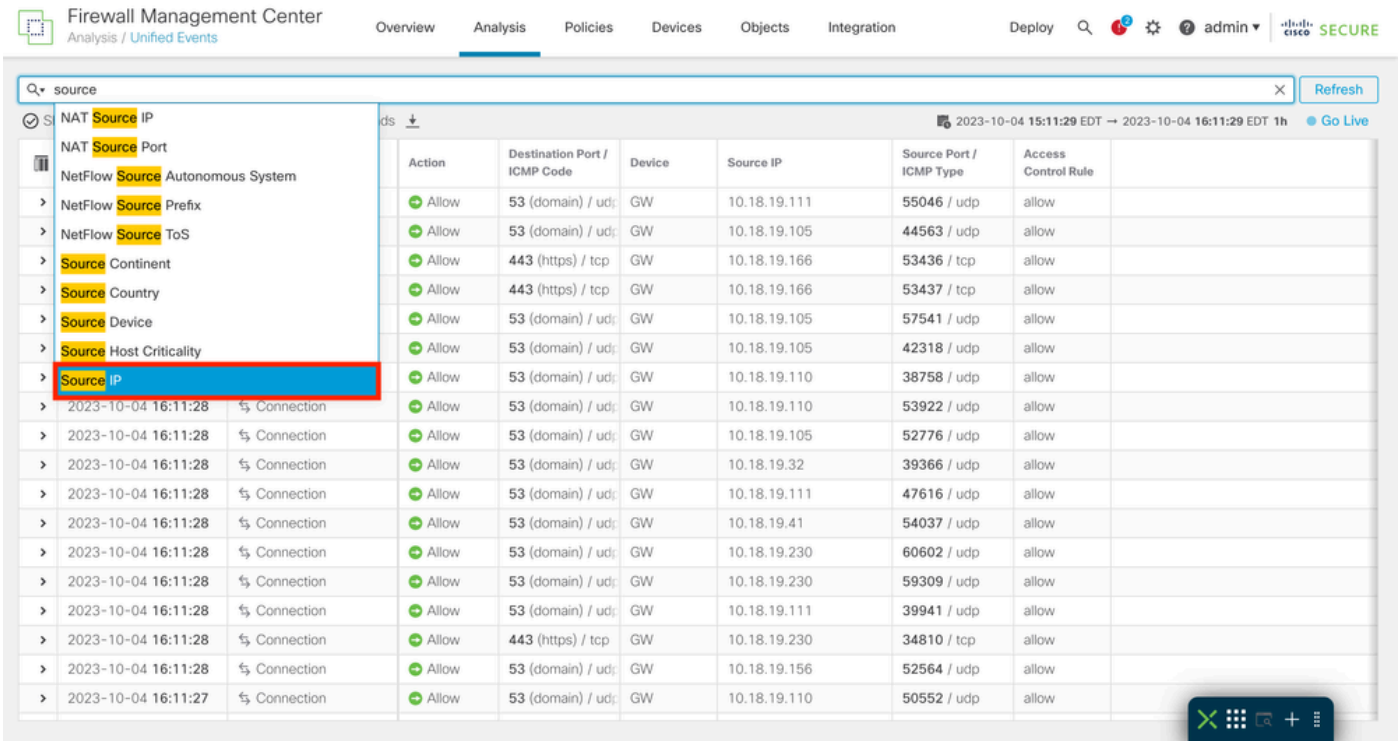



# Pesquisa de evento

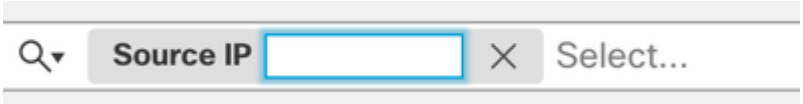
Etapa 1. Para começar a procurar eventos específicos, clique em Selecionar.




Etapa 2. Selecione o campo onde deseja aplicar o filtro.

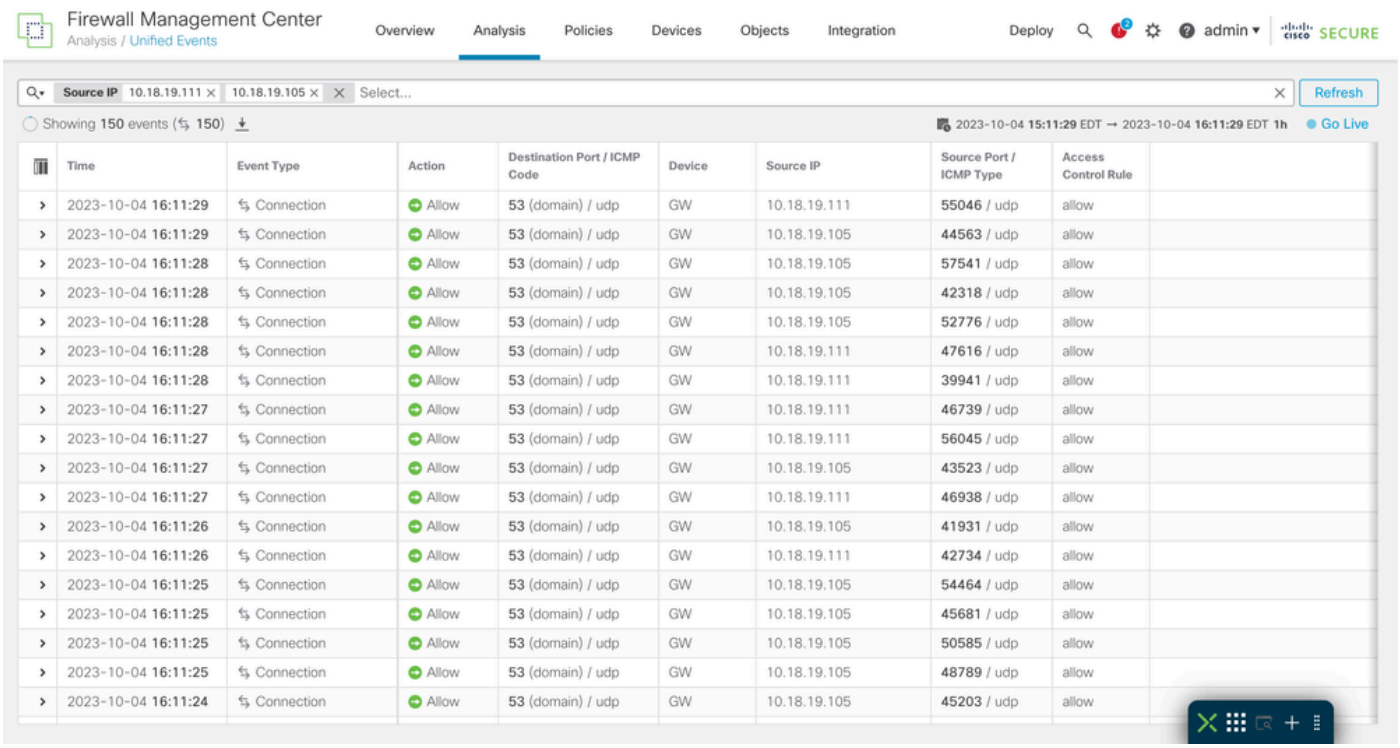



Etapa 3. Escreva os valores a serem usados como filtro.

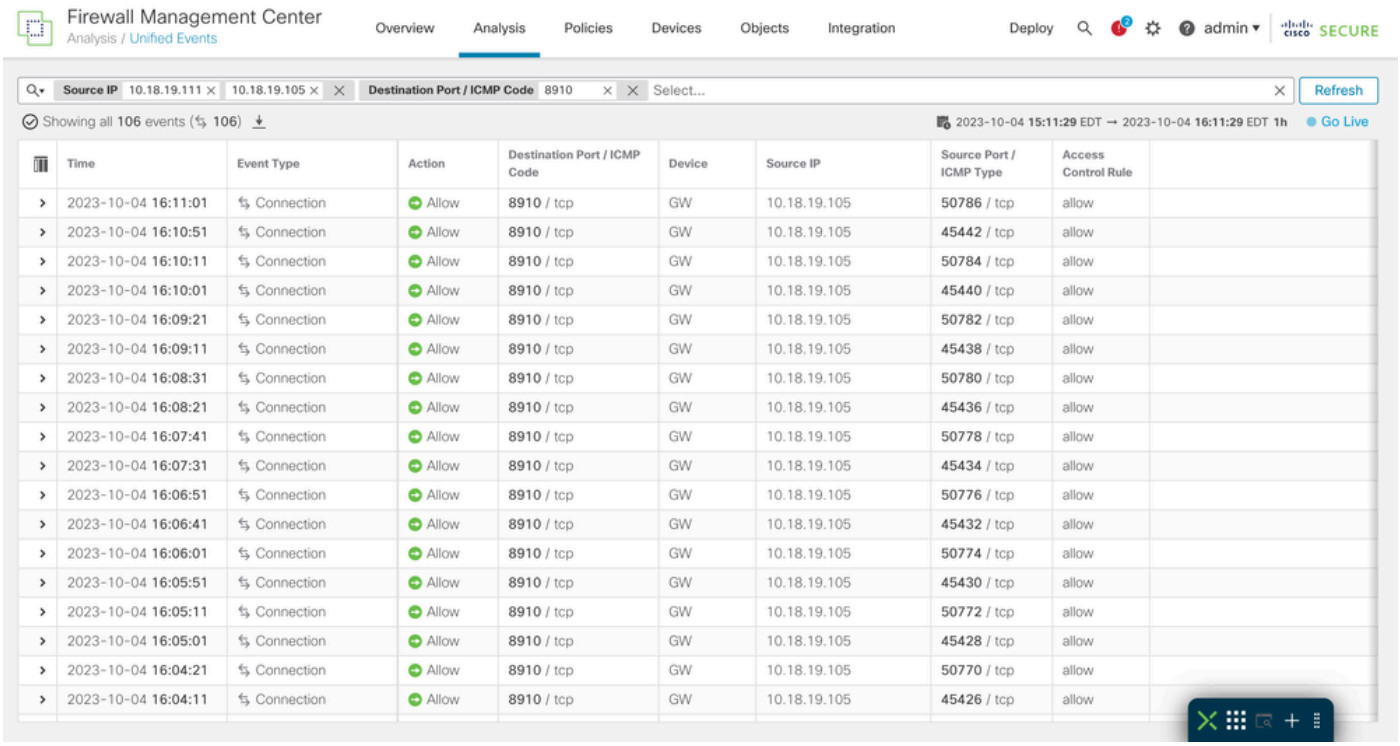



Etapa 4. Clique em Apply para configurar o filtro.


Etapa 5. (Opcional) Você pode adicionar vários valores a cada filtro.




Etapa 6. (Opcional) Adicione quantos filtros forem necessários.

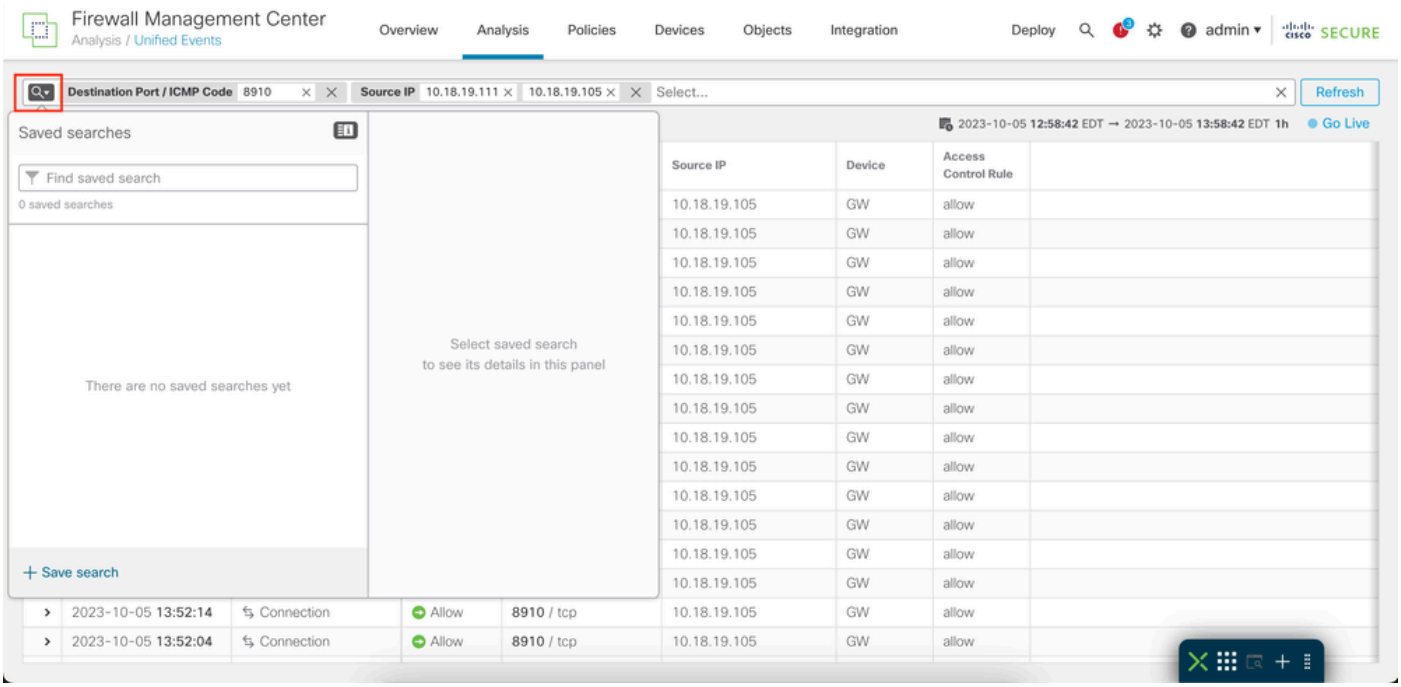


Tip: Você pode usar operadores ( >,<, ! e assim por diante) ao escrever os valores.

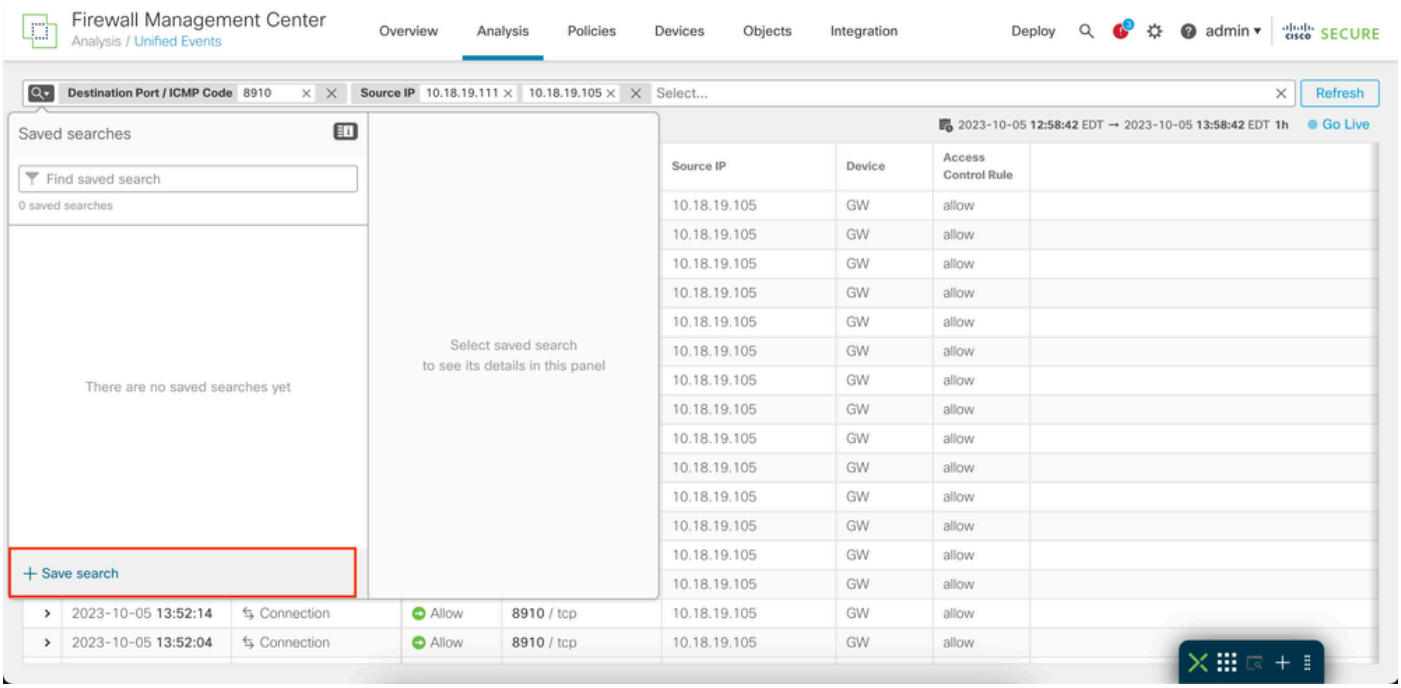
## Salvar pesquisa

É possível salvar pesquisas para que você possa reutilizar os filtros criados.

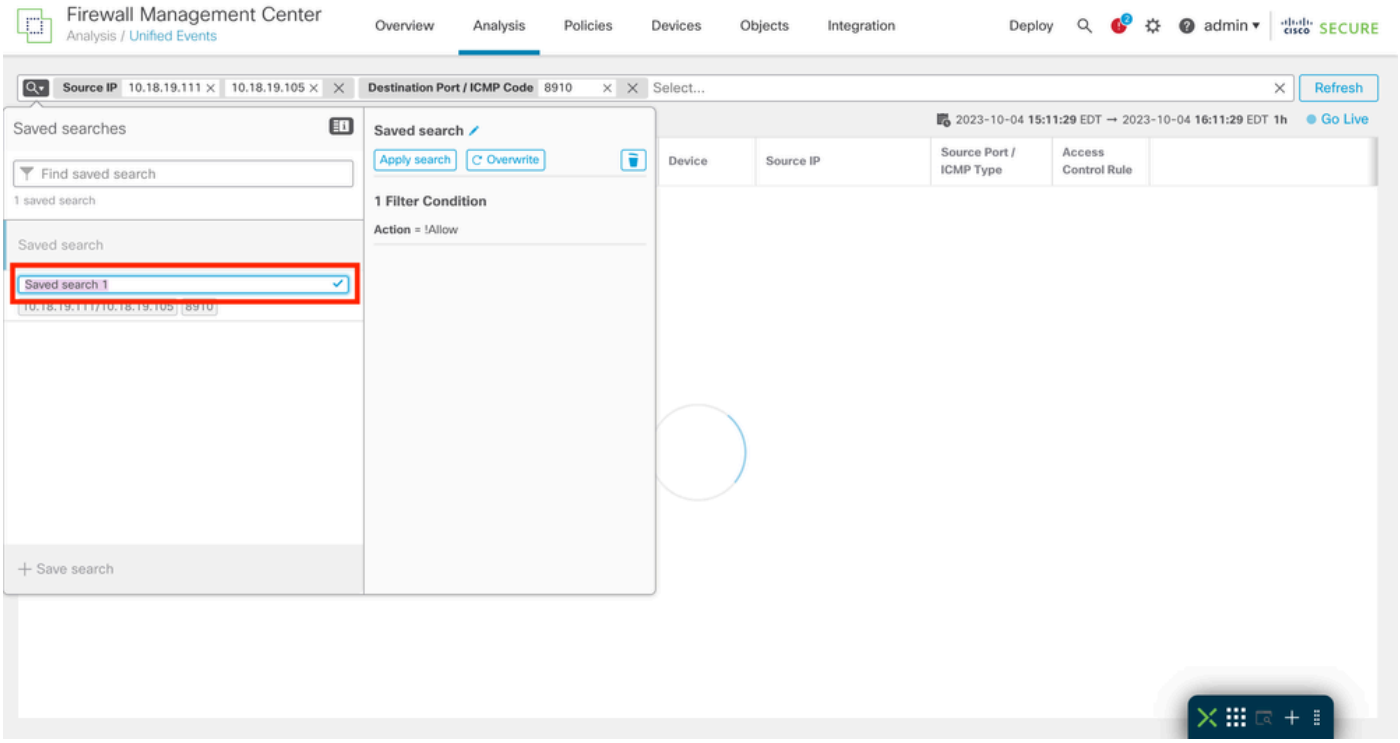
Etapa 1. Clique no ícone de lupa.




Etapa 2. Clique em Save Search.



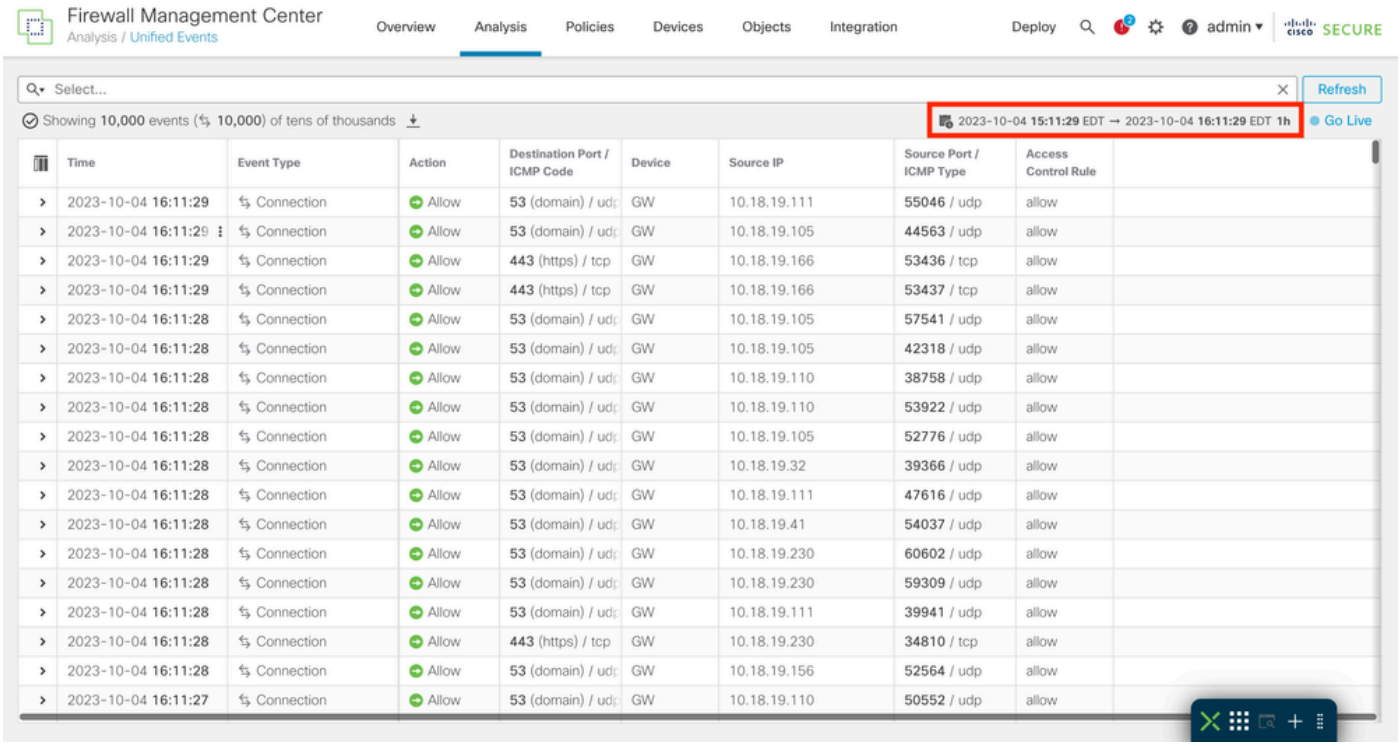

Etapa 3. (Opcional) Altere o nome da pesquisa.



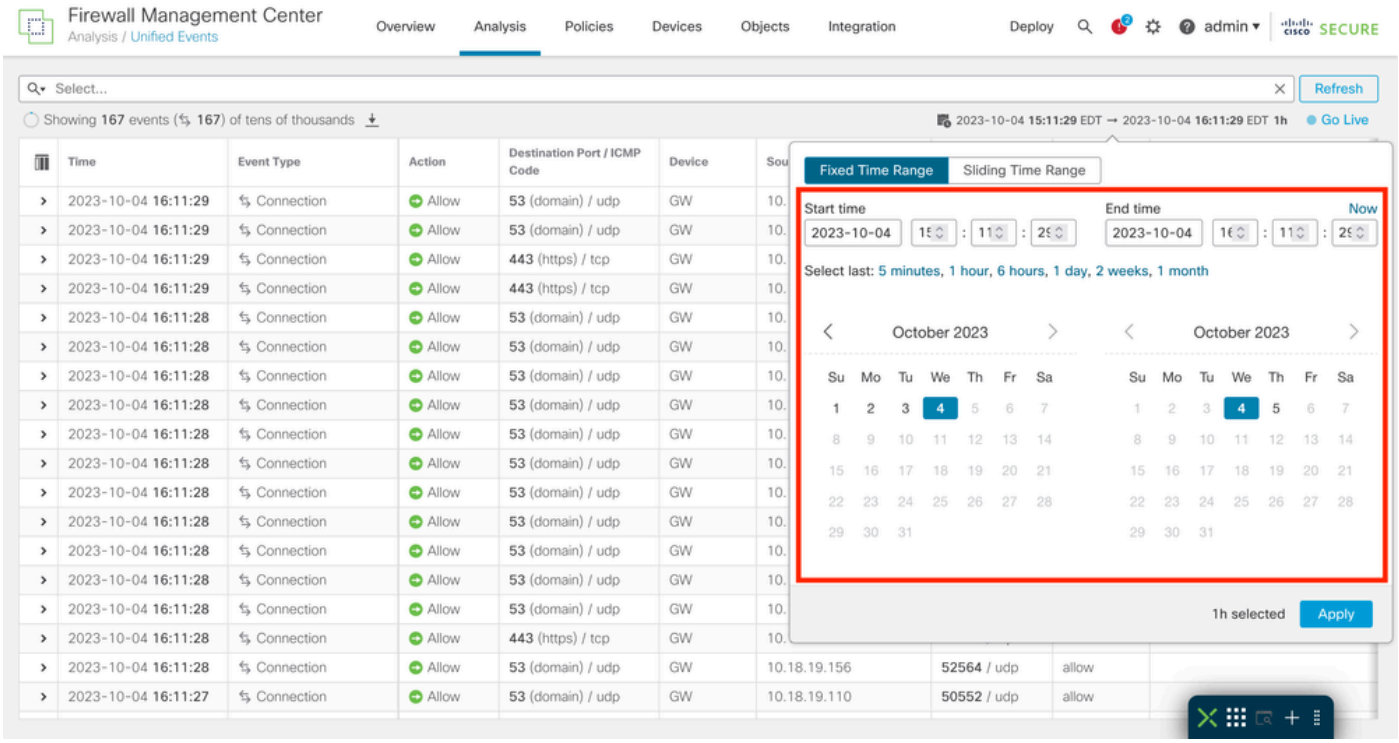

# Janela de Tempo

É mais fácil restringir eventos relevantes, com base em uma hora específica, modificando a janela de tempo.

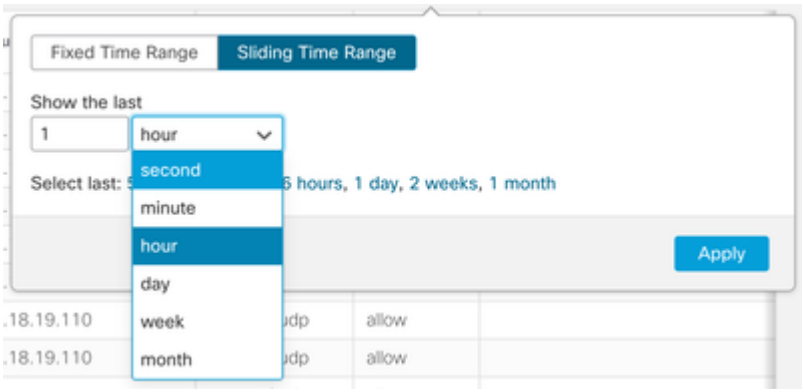
Etapa 1. Para modificar o quadro de eventos da janela, clique em um intervalo de datas.



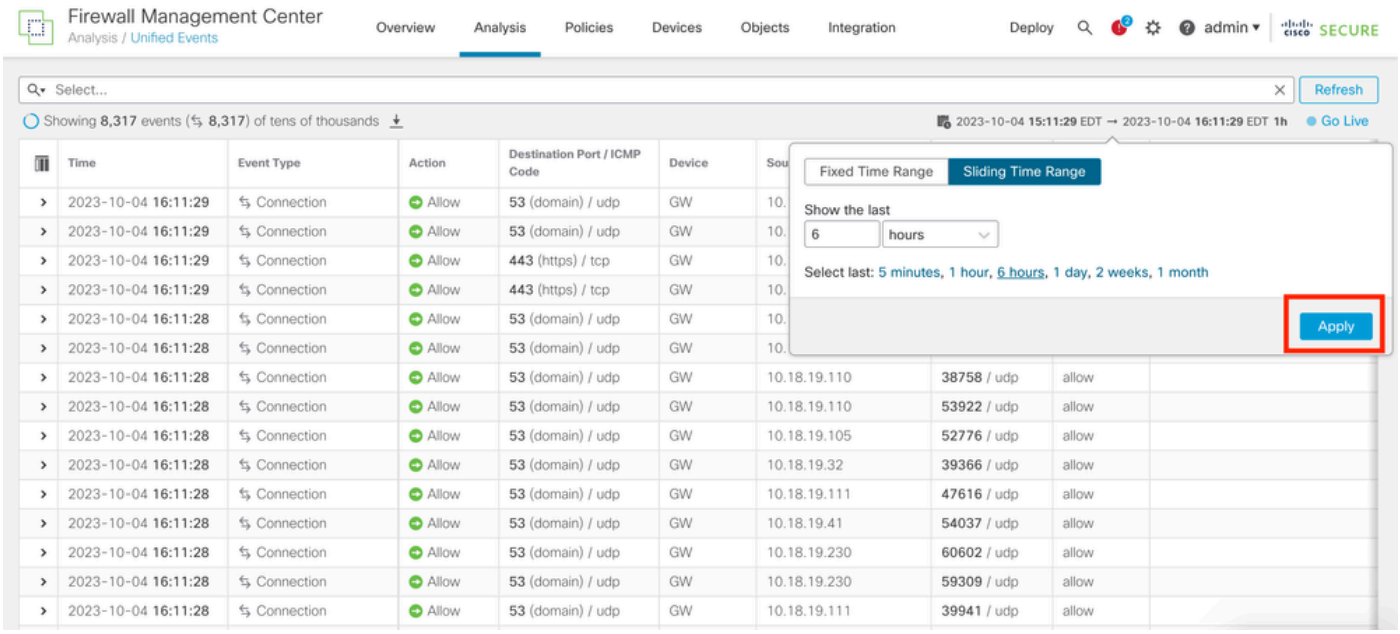

Etapa 2. Selecione o intervalo de tempo na janela pop-up.




Etapa 3. (Opcional) Use Intervalo de tempo deslizante para mostrar eventos de um horário específico para o seu horário atual.



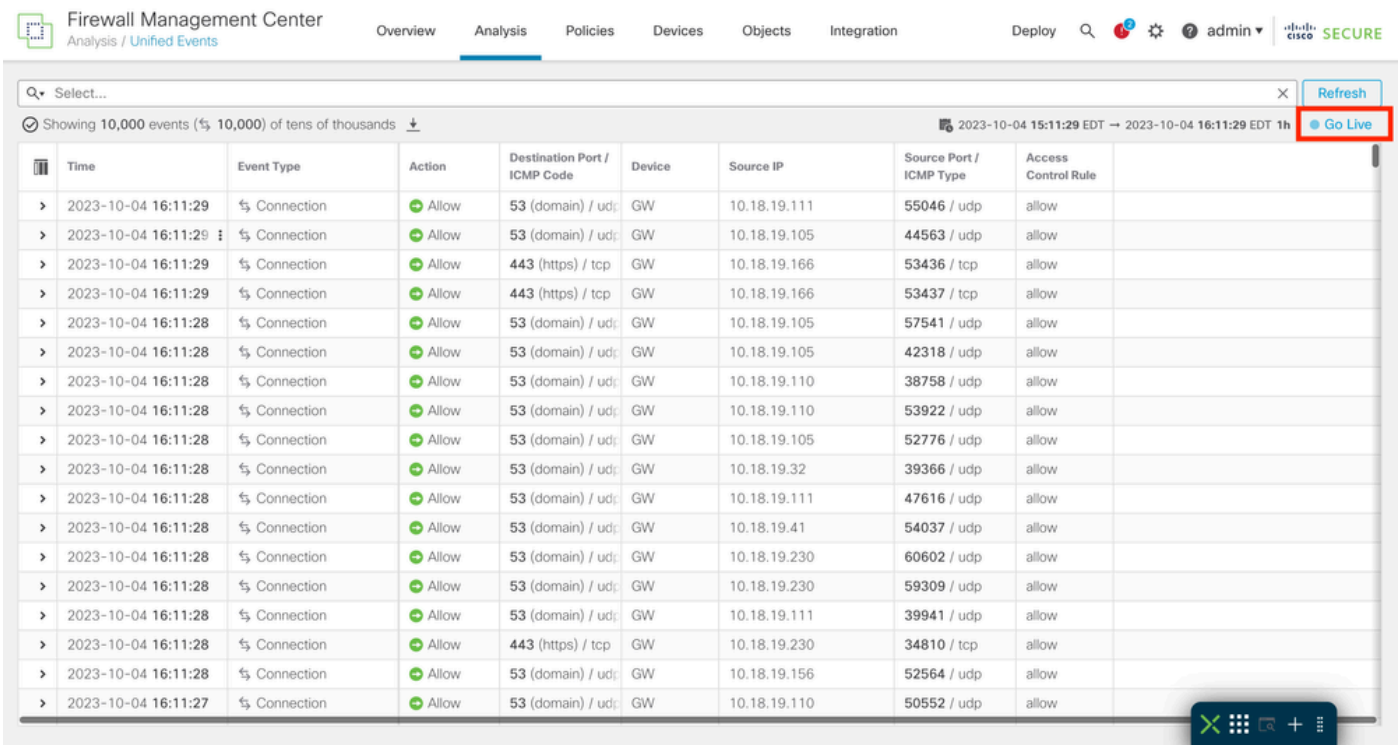

Etapa 4. Clique em Apply para filtrar os eventos no intervalo de tempo configurado.



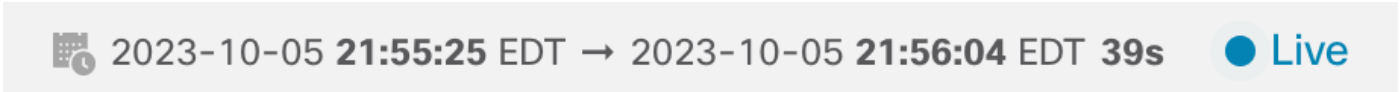

## Lançamento

Você pode ativar o recurso de ativação para mostrar eventos em tempo real. Os eventos aparecem à medida que são gerados.

Para habilitar, clique em Go Live.



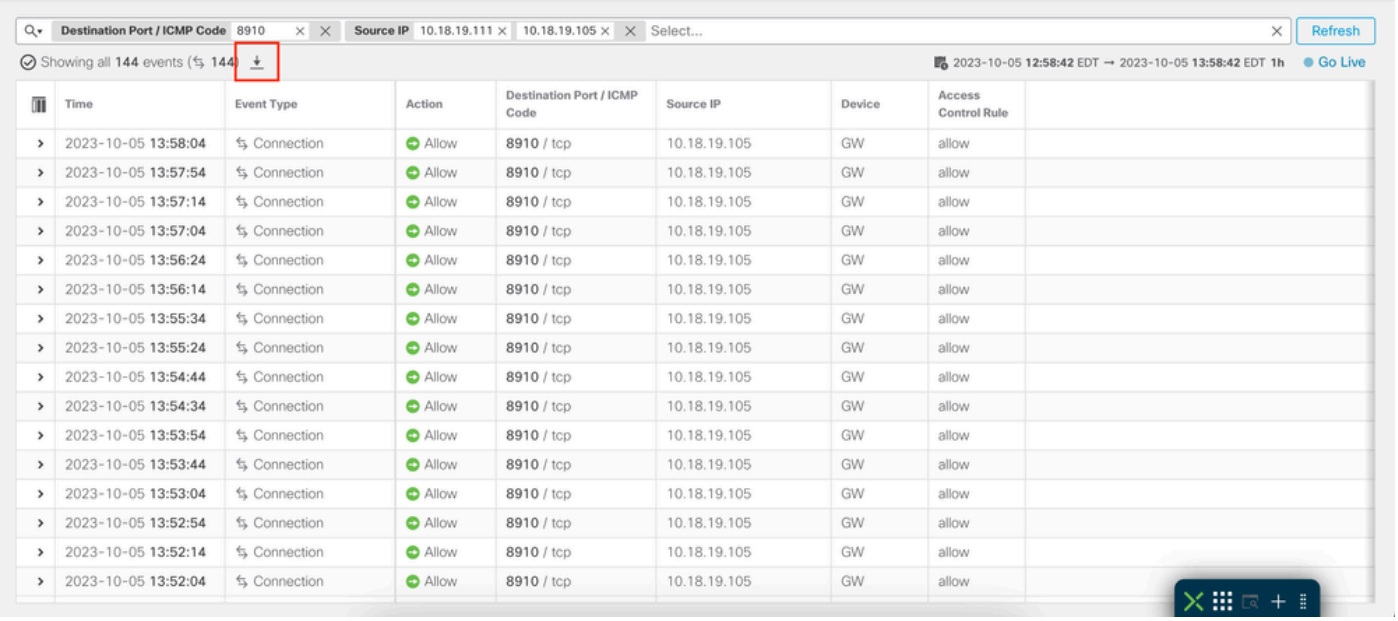

Depois de ativada, ela exibe a palavra Live.



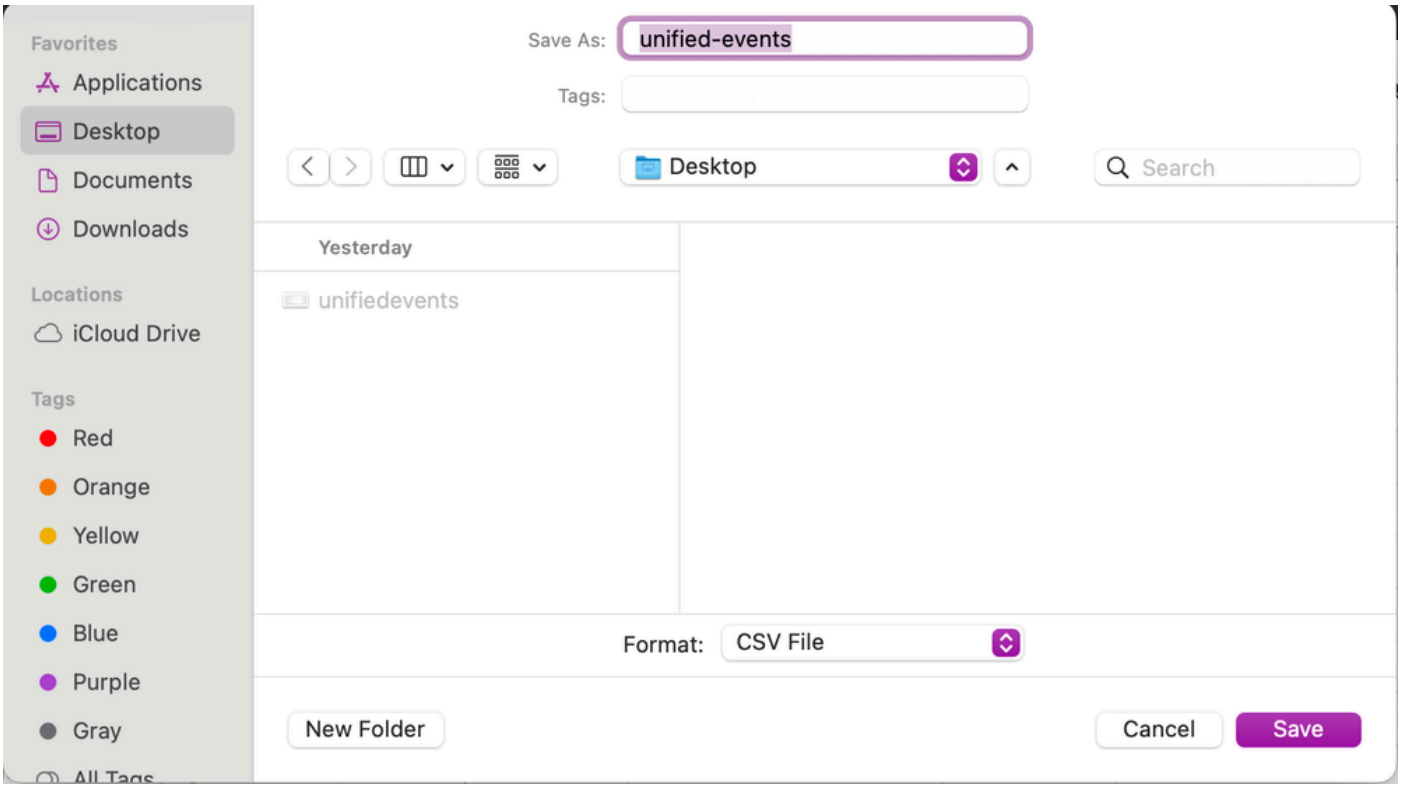
Caution: Quando a opção Ao vivo está habilitada, não é possível modificar a janela de tempo. Para modificar a janela de tempo, primeiro desative a opção Ao vivo clicando nela novamente.

## Baixar Eventos como Valores separados por vírgula (CSV)

Etapa 1. Clique no ícone de download para gerar um arquivo contendo os eventos atualmente exibidos na página.




Etapa 2. Selecione a pasta de download, o nome e clique em Save.




Etapa 3. Verificar o arquivo CSV.

| 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 |

# Informações Relacionadas

- Trabalhando com o Visualizador de Eventos Unificado
- Cisco Secure Firewall - Visualizador de eventos unificado: Dicas e truques
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.