Gebeurtenissen bewaken met Unified Event Viewer op FMC GUI

Inhoud

Inleiding

Dit document beschrijft het gebruik van Unified Event Viewer op een grafische gebruikersinterface (GUI) in Firewall Management Center (FMC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot FMC met bevoegdheden voor Beheer of Beveiligingsanalist
- FMC-versie gelijk aan of hoger dan v7.0

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

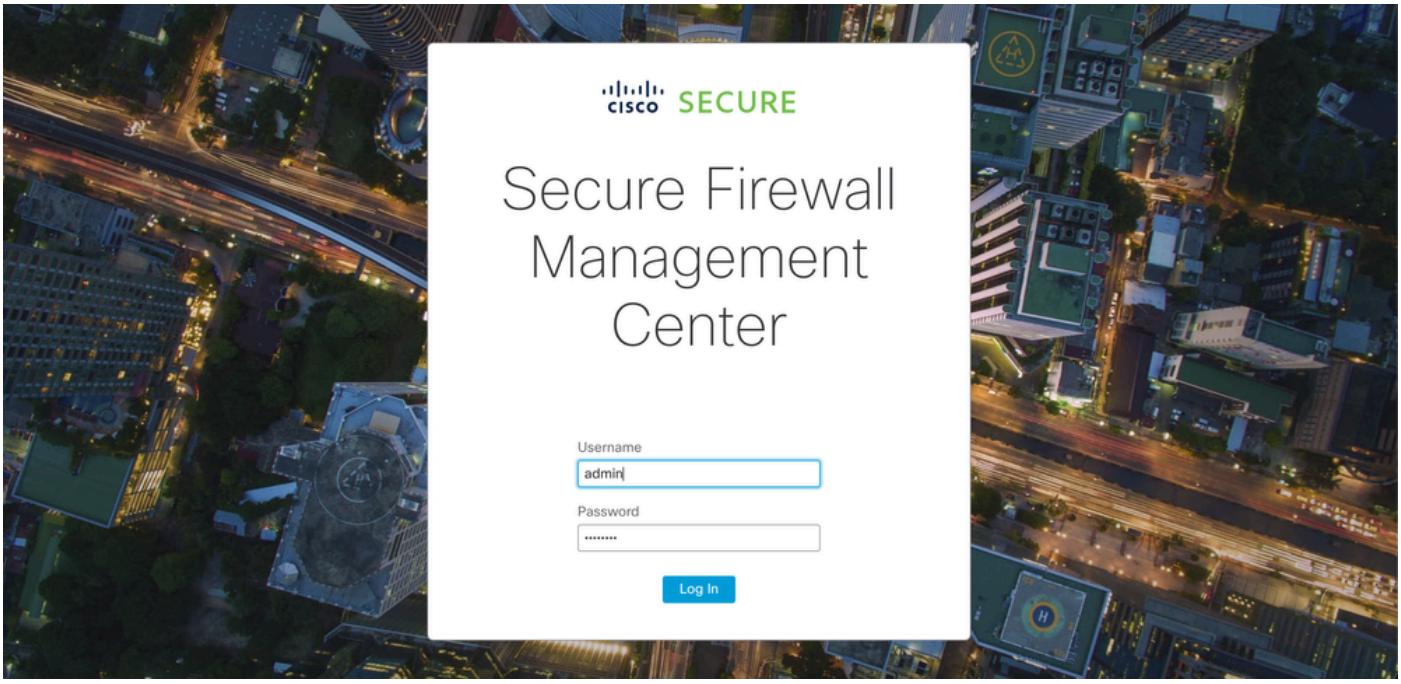
- Secure Firewall Management Center voor VMware v7.2.5

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

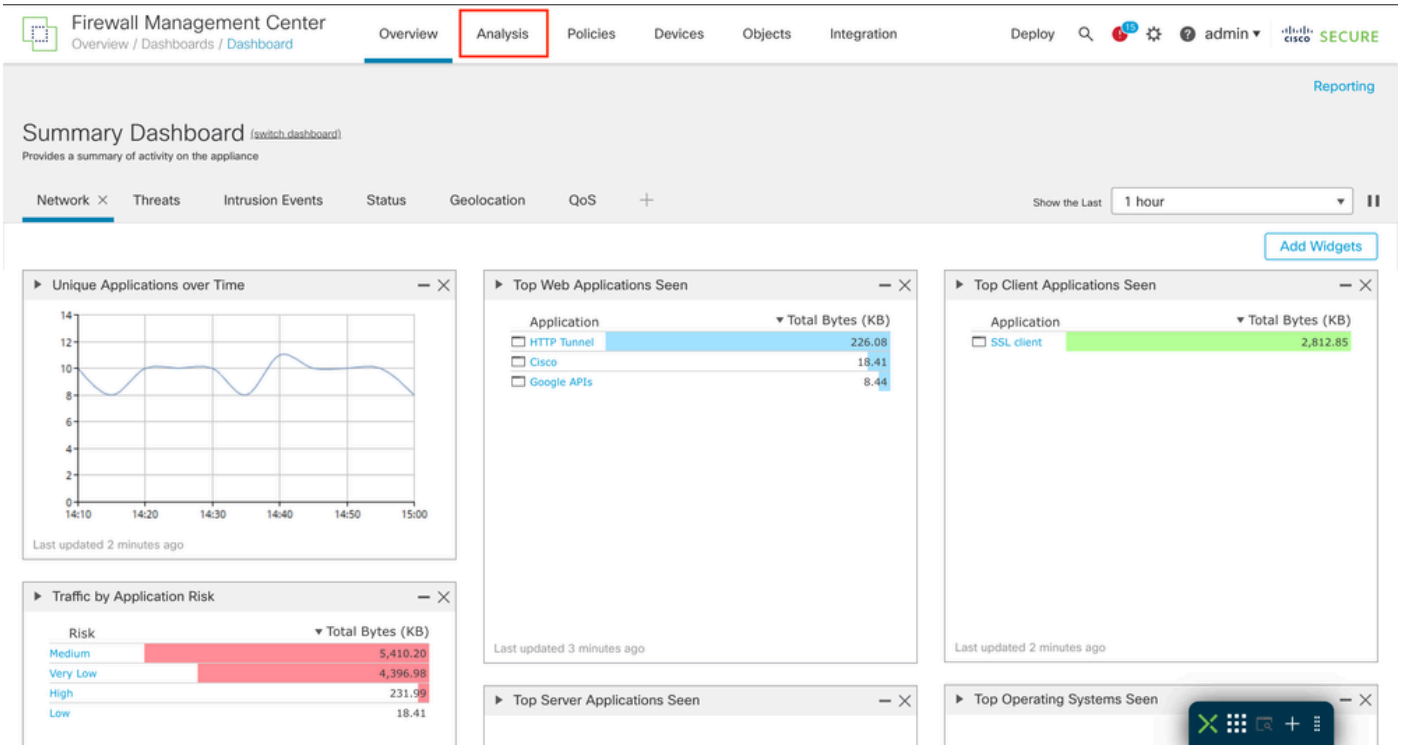
opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

verkennen

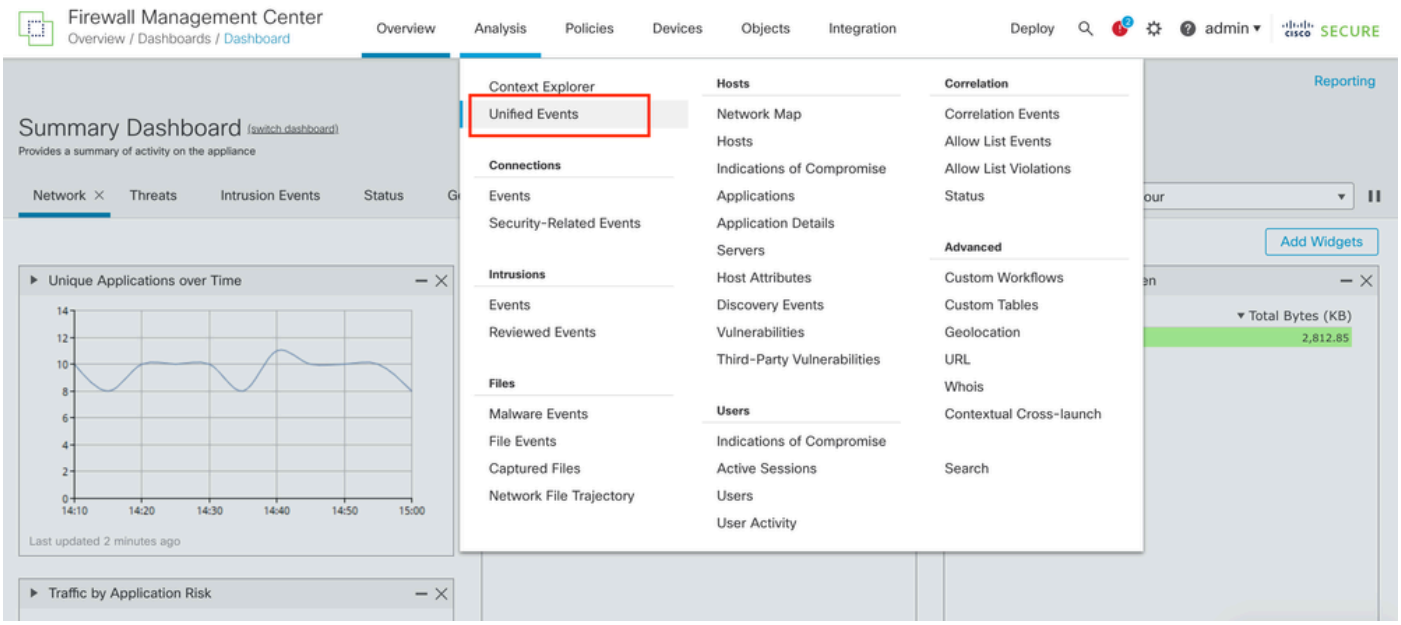
Stap 1. Log in op de FMC GUI.



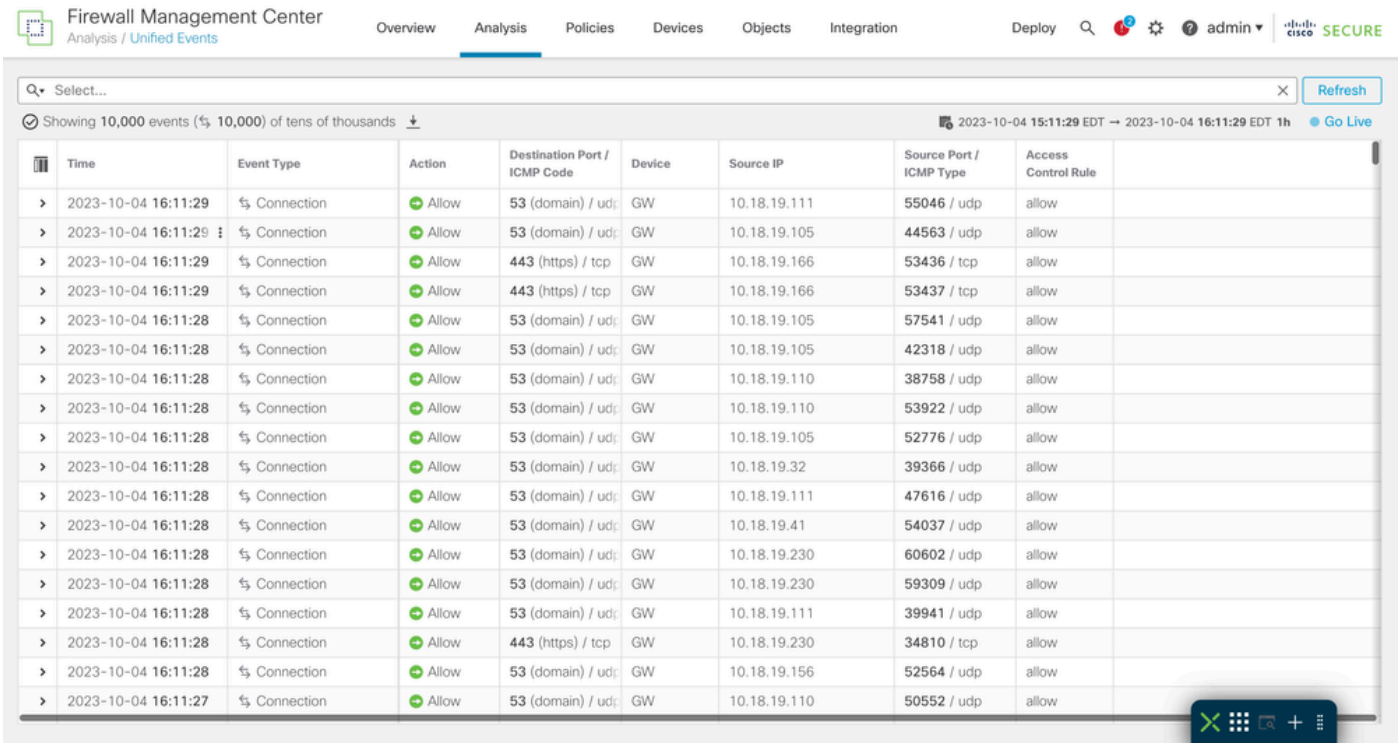
Stap 2. Navigeer naar het tabblad Analyse.



Stap 3. Klik in het vervolgkeuzemenu op Unified Events.

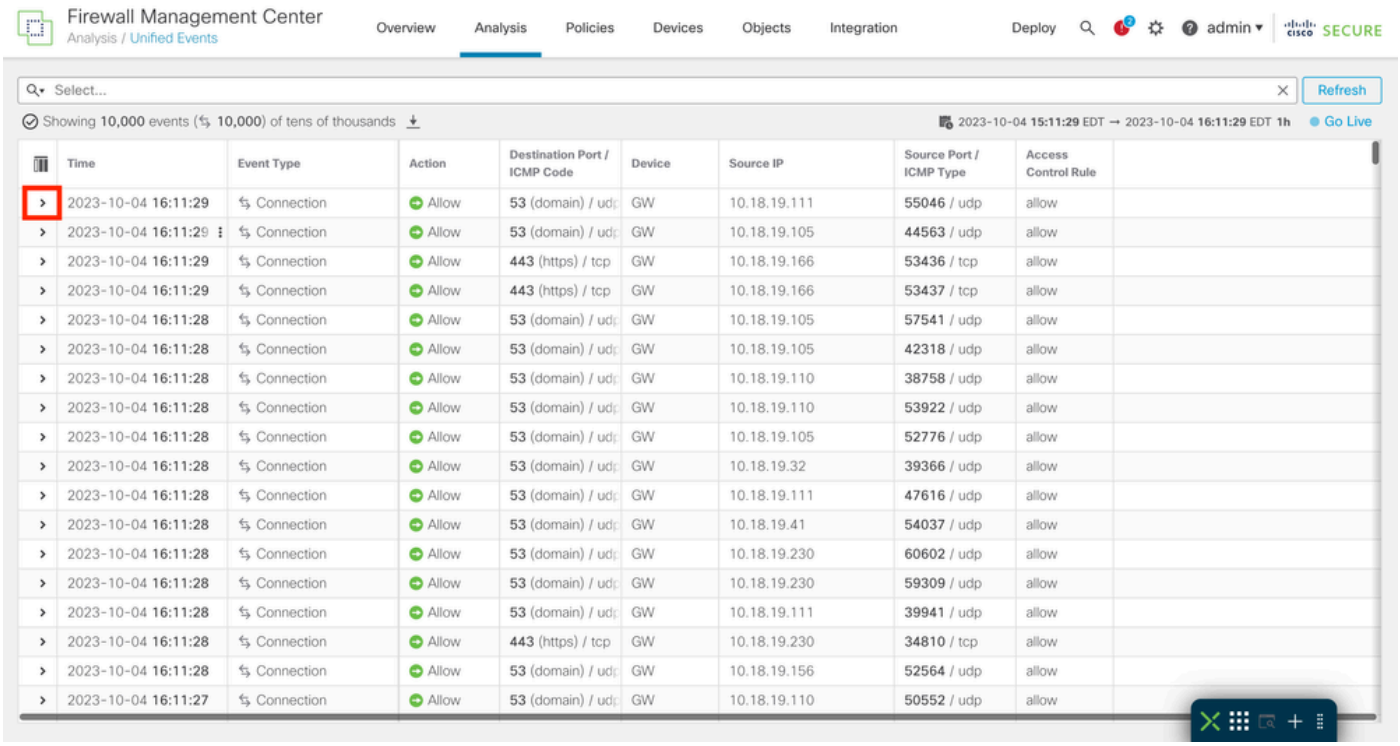


Voorbeeld van de pagina Unified Event

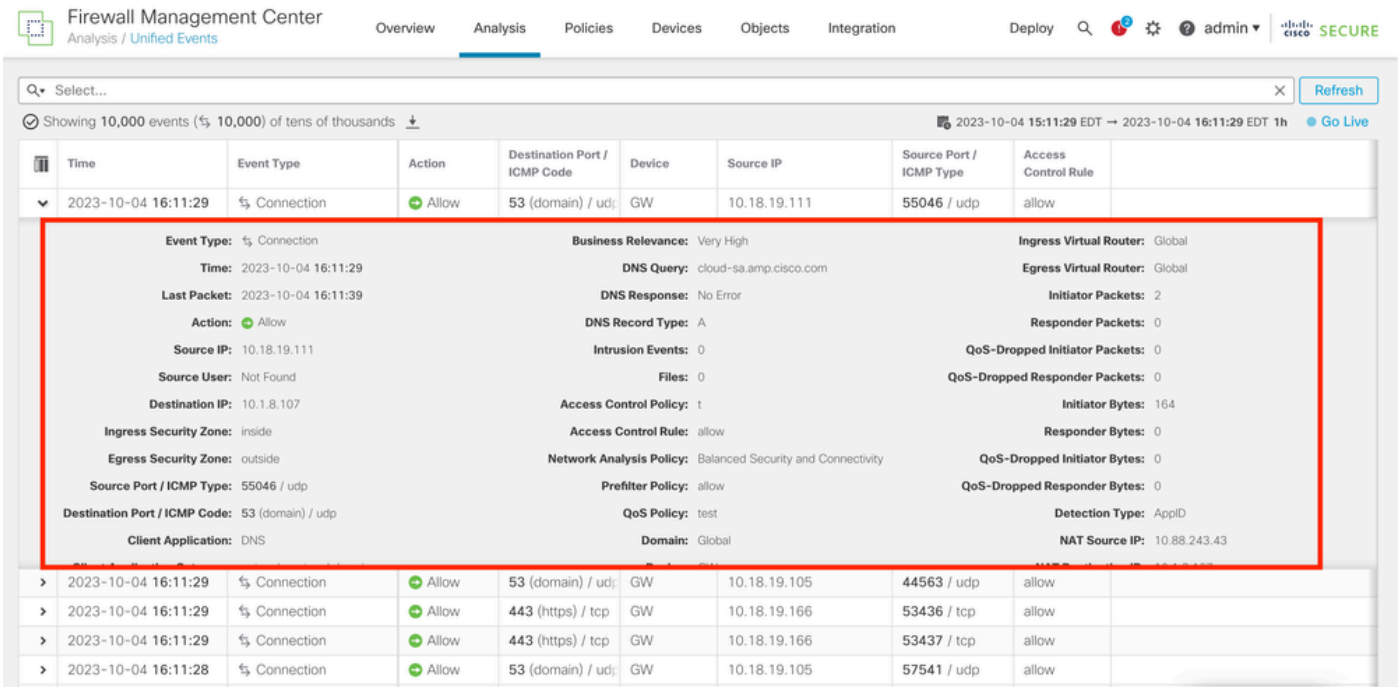


Gebeurtenissen bekijken

Stap 1. Klik op het > icoon.

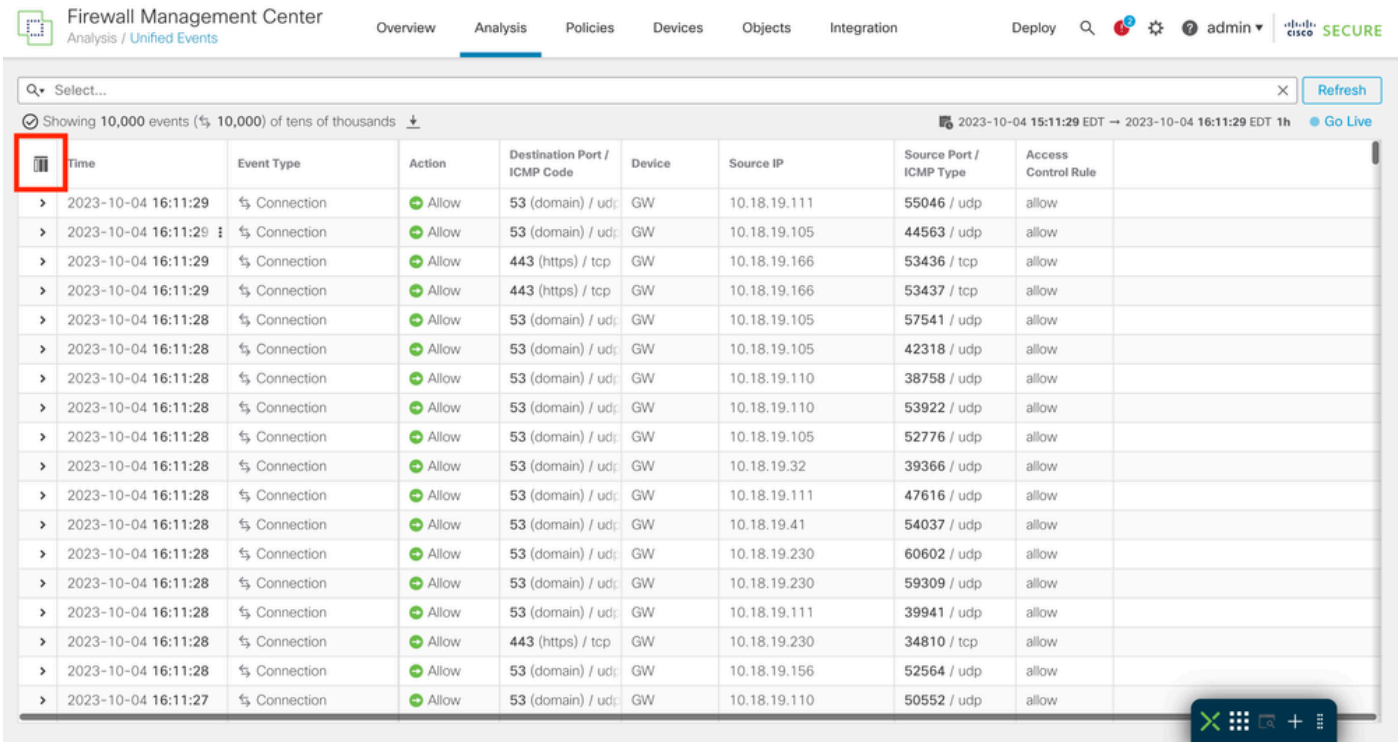


Stap 2. De gedetailleerde informatie van het evenement wordt getoond.

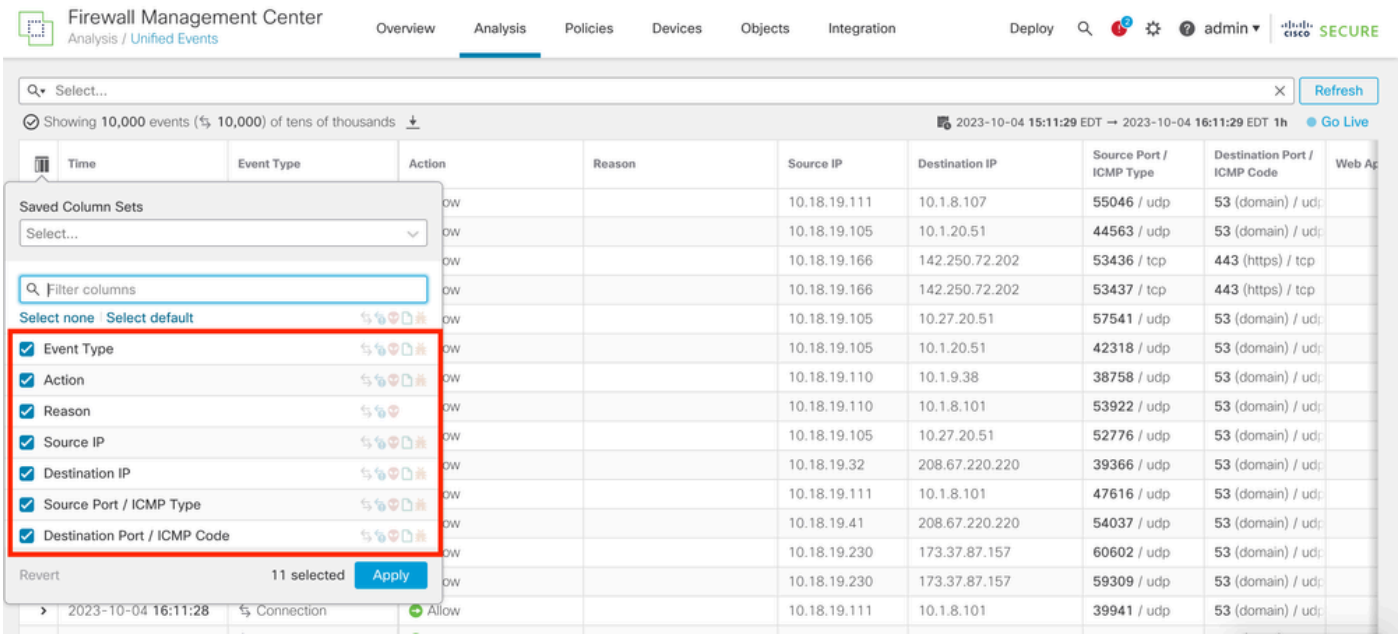


Kolommen personaliseren

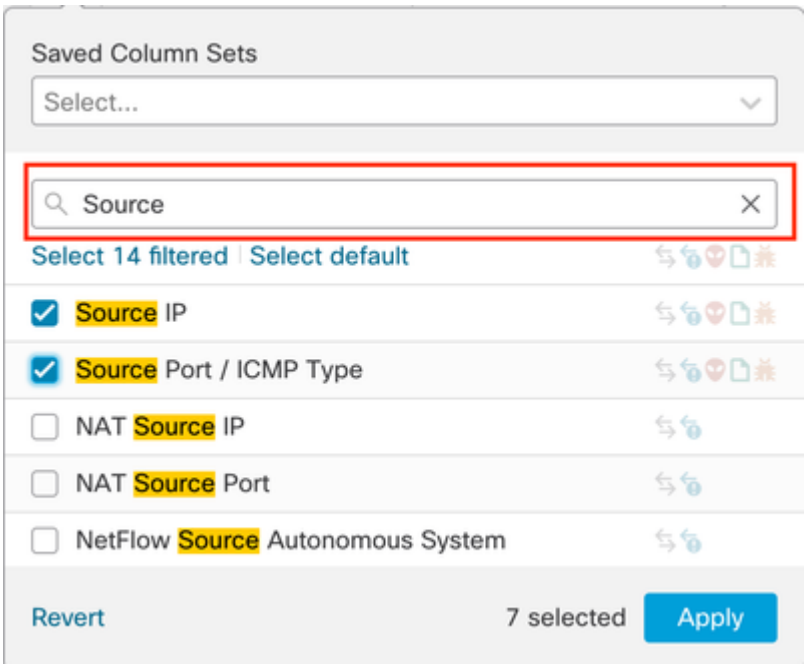
Stap 1. Klik op het icoon .



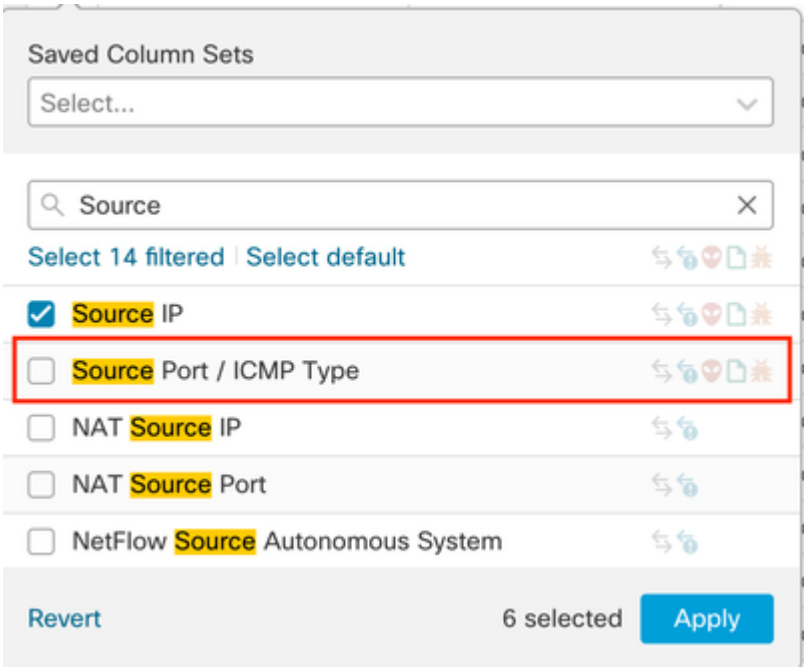
Stap 2. Selecteer de gewenste gebeurtenisvelden op de tabel.



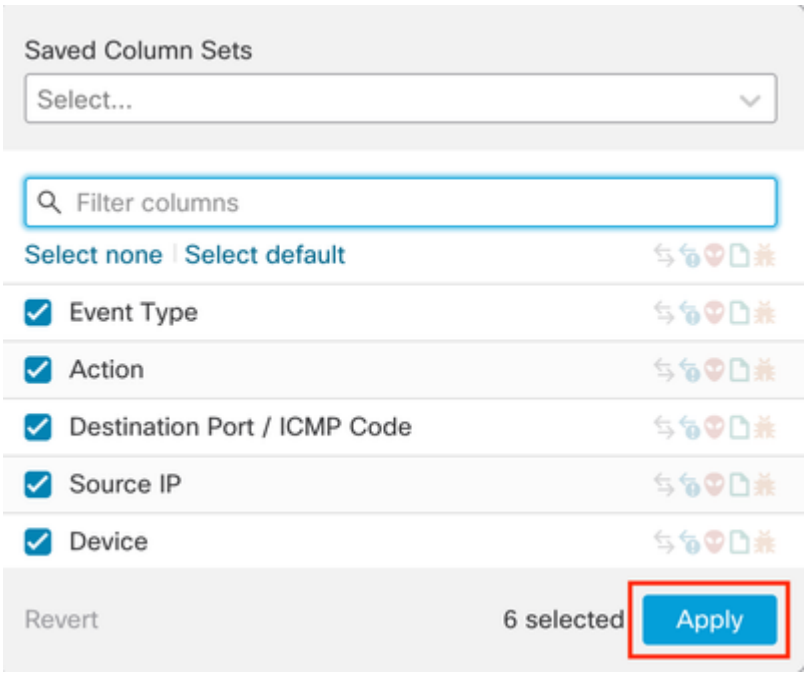
Stap 3. (Optioneel) Zoek naar het veld om de navigatie te vergemakkelijken.



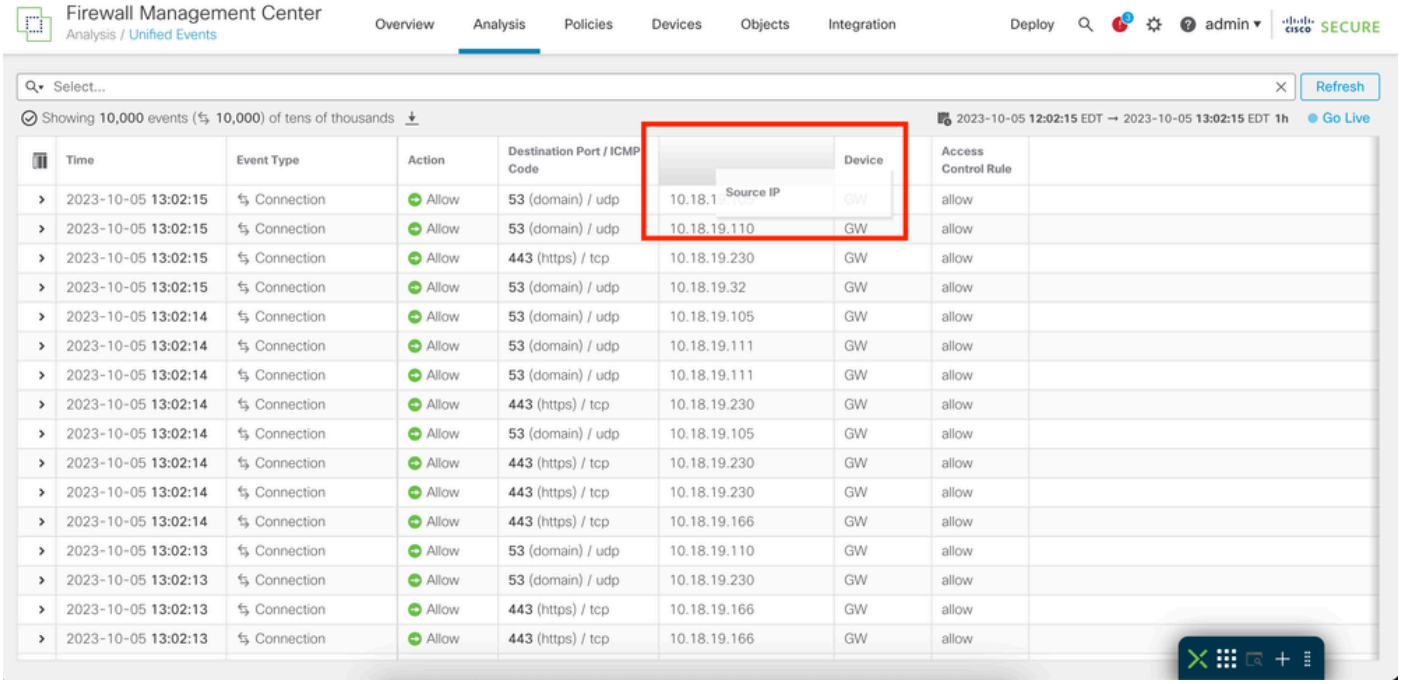
Stap 4. Klik op een gebeurtenisveld om uit te schakelen of in te schakelen.



Stap 5. Klik op Toepassen.

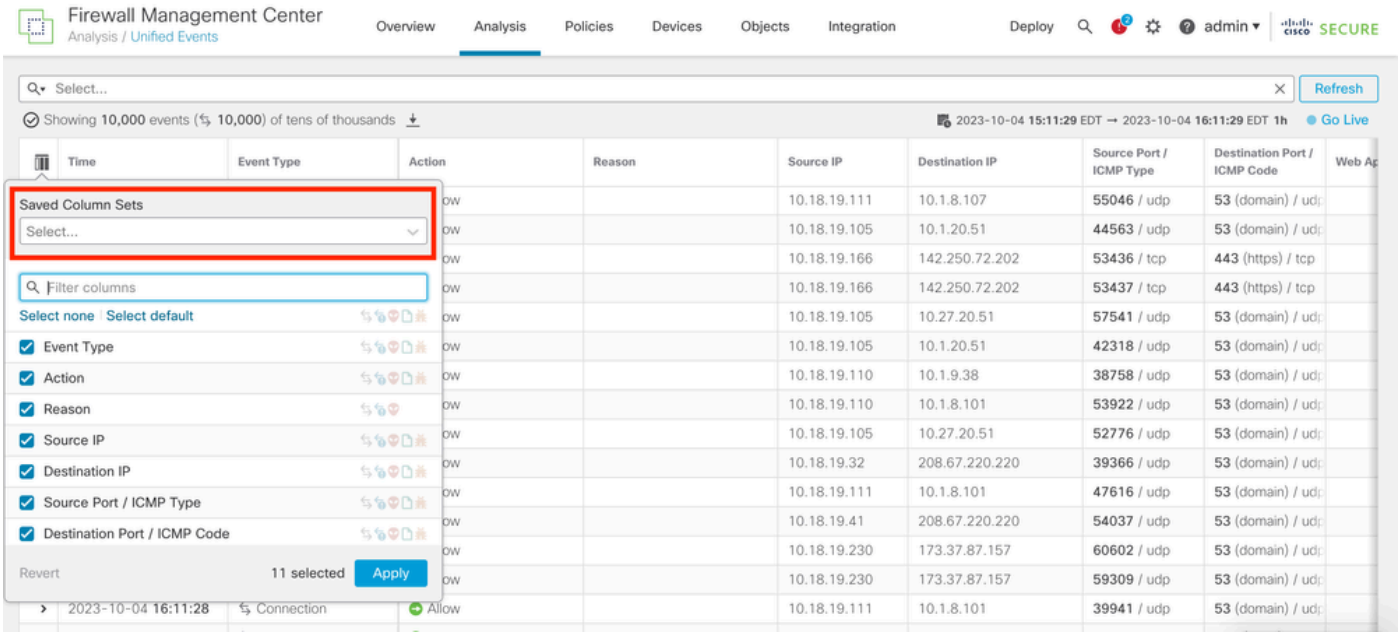


Stap 6. (Optioneel) U kunt de kolommen verplaatsen door ze naar een andere locatie te slepen.

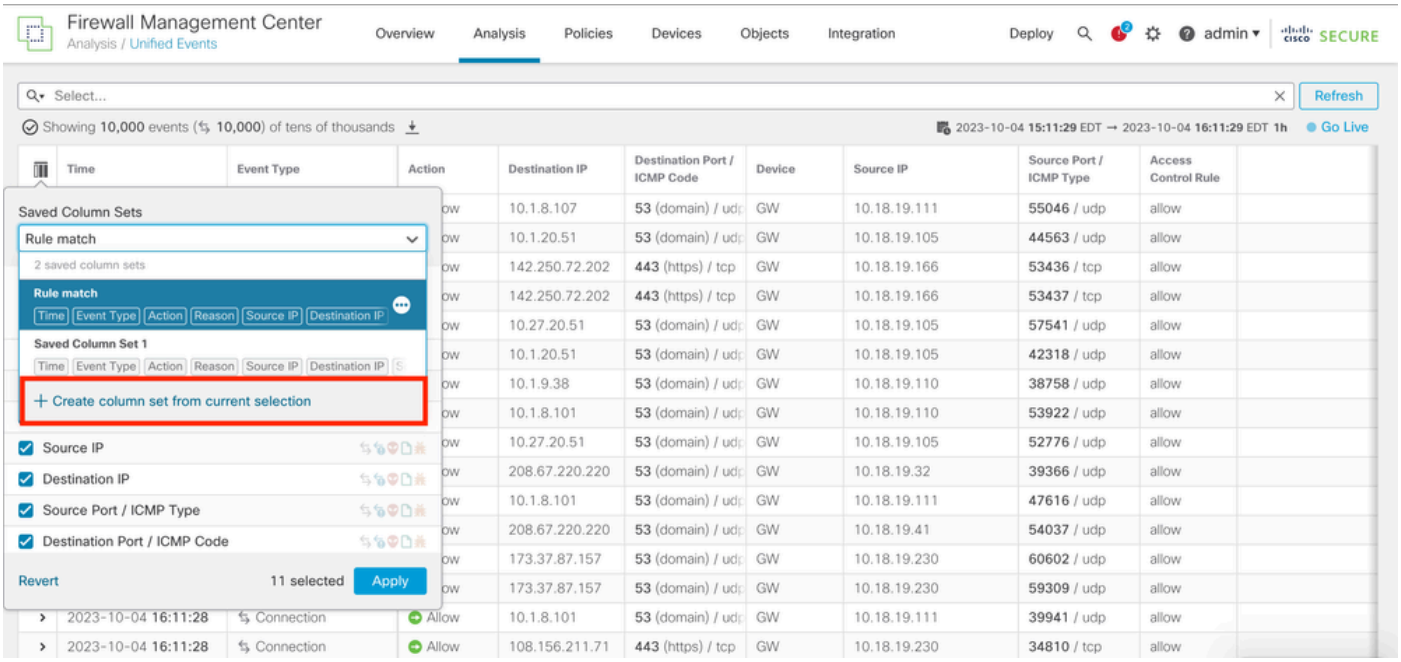


Kolomset opslaan

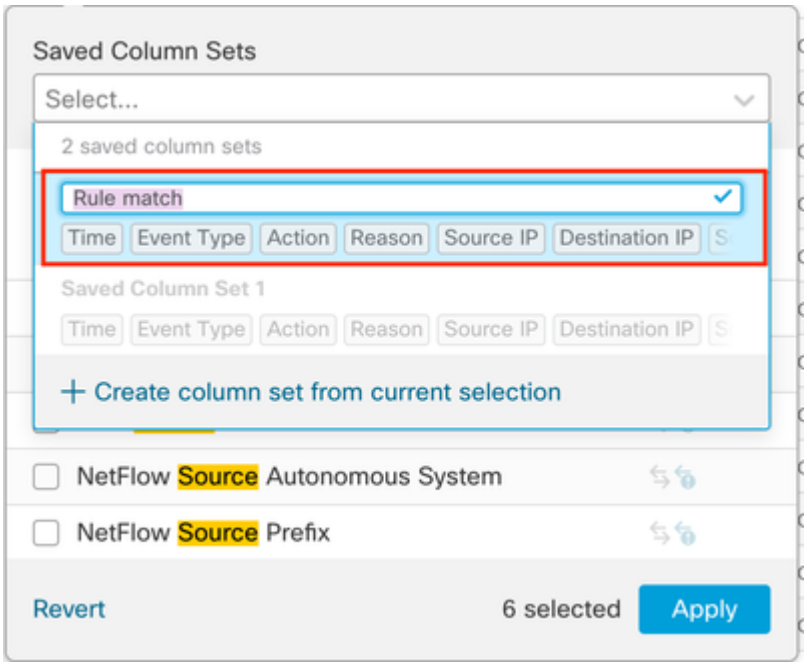
Stap 1. Klik op Opgeslagen kolomsets.



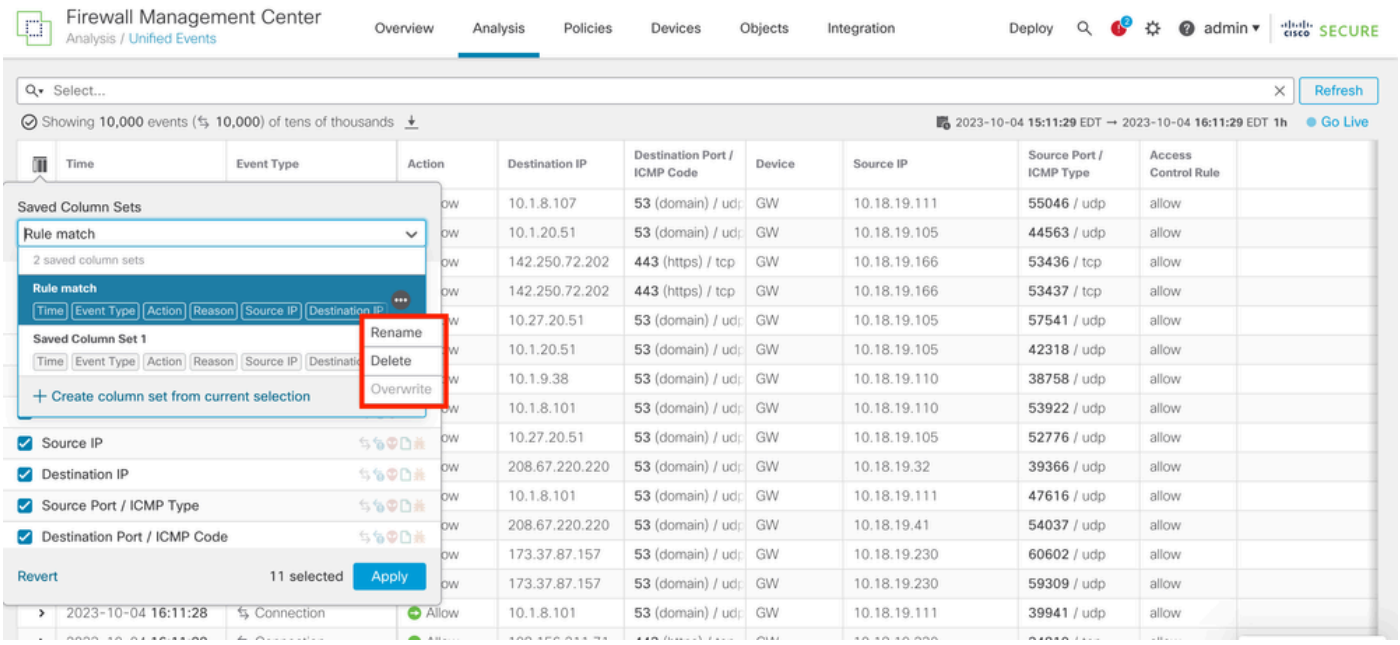
Stap 2. Klik op Kolomset maken uit de huidige selectie.



Stap 3. (Optioneel) Wijzig de naam van de kolomset.

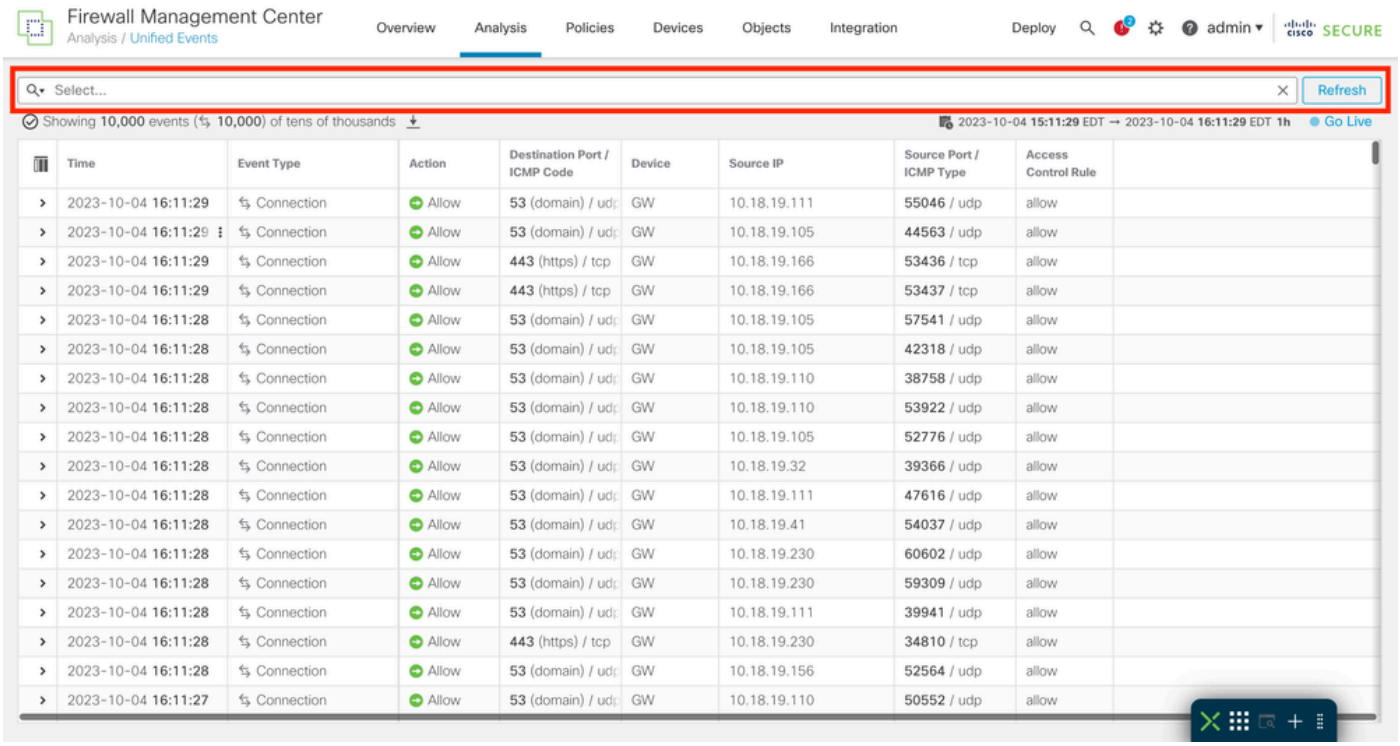


Stap 4. U kunt een bestaande set bewerken door op de ellipsis (...) te klikken.

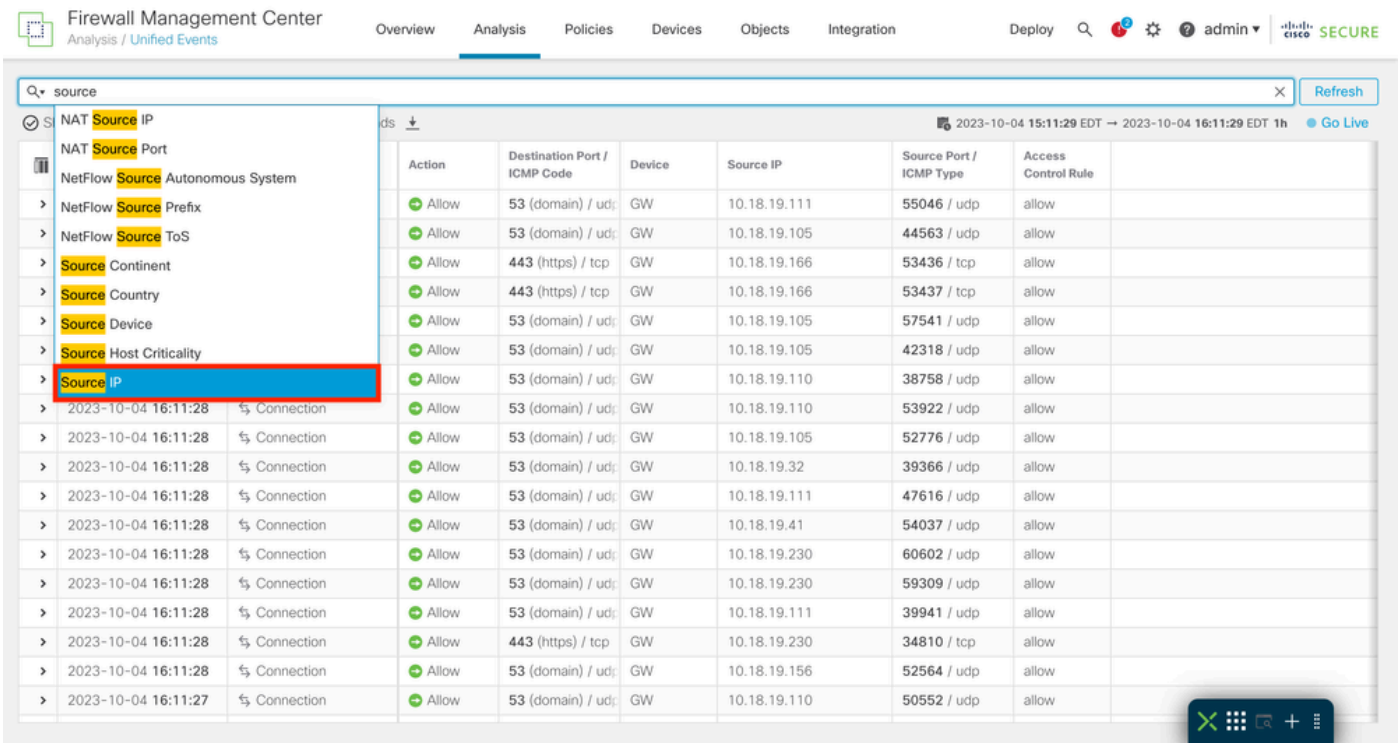


Zoeken naar gebeurtenissen

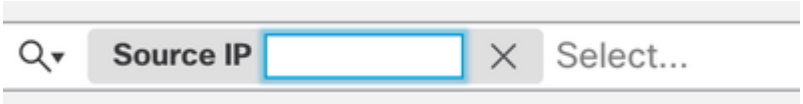
Stap 1. Om te beginnen met zoeken naar specifieke gebeurtenissen, klik op Selecteren.



Stap 2. Selecteer het veld waar u het filter wilt toepassen.

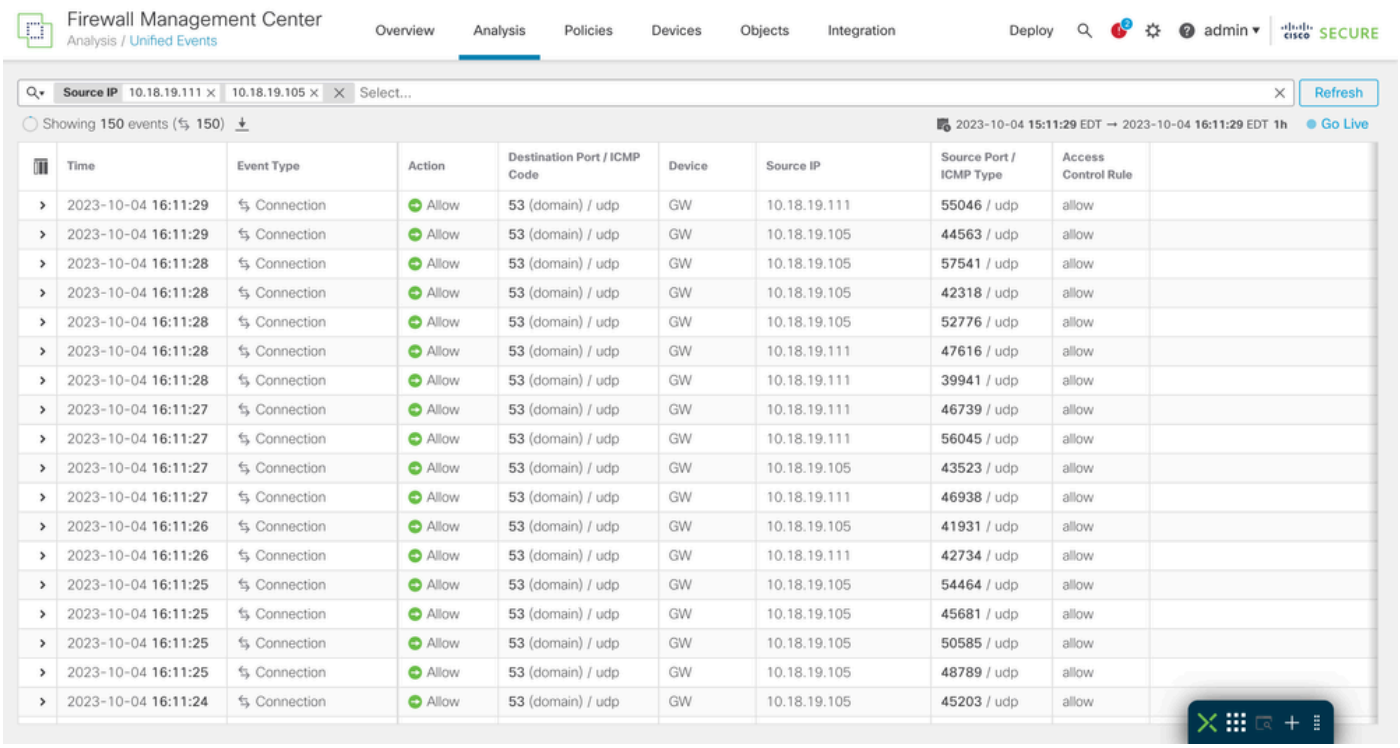


Stap 3. Schrijf de waarden die u als filter wilt gebruiken.

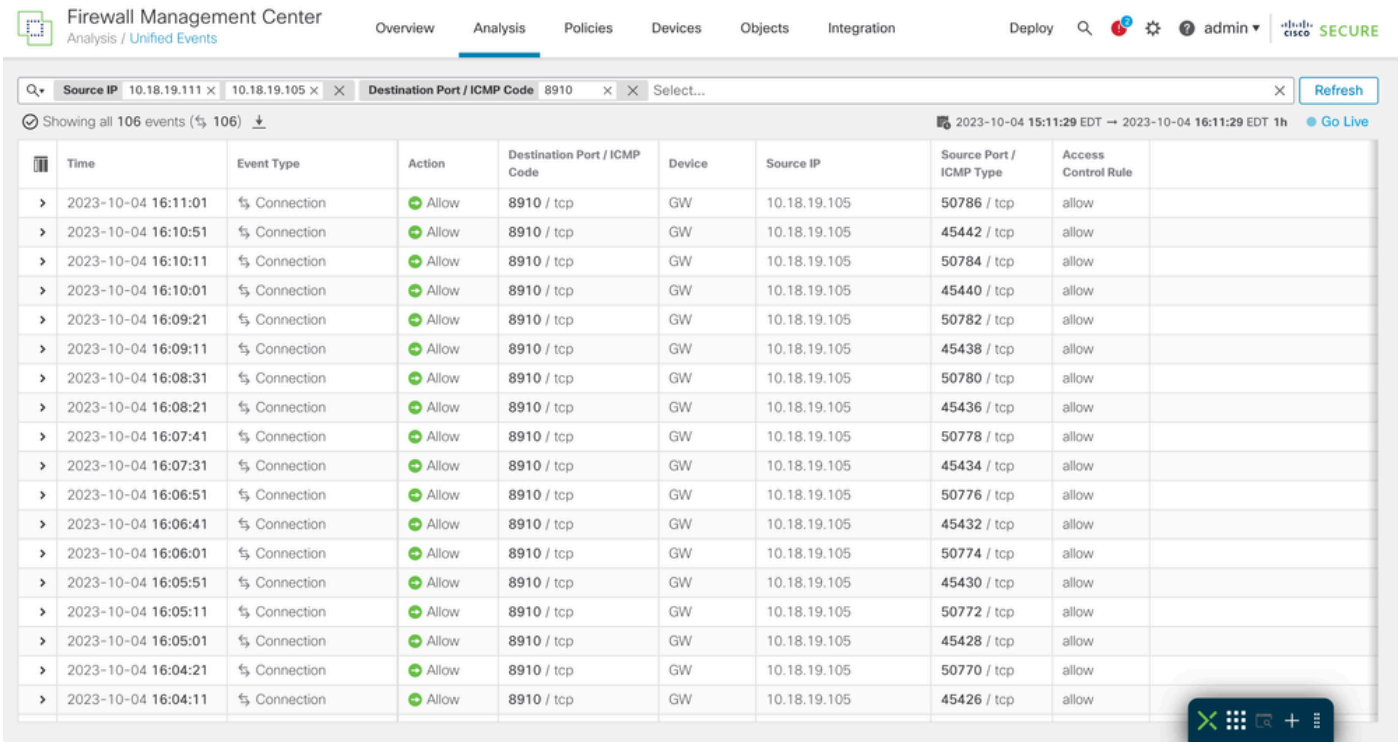


Stap 4. Klik op Toepassen, om het filter te configureren.

Stap 5. (Optioneel) U kunt meerdere waarden aan elk filter toevoegen.



Stap 6. (Optioneel) Voeg zoveel filters toe als je nodig hebt.

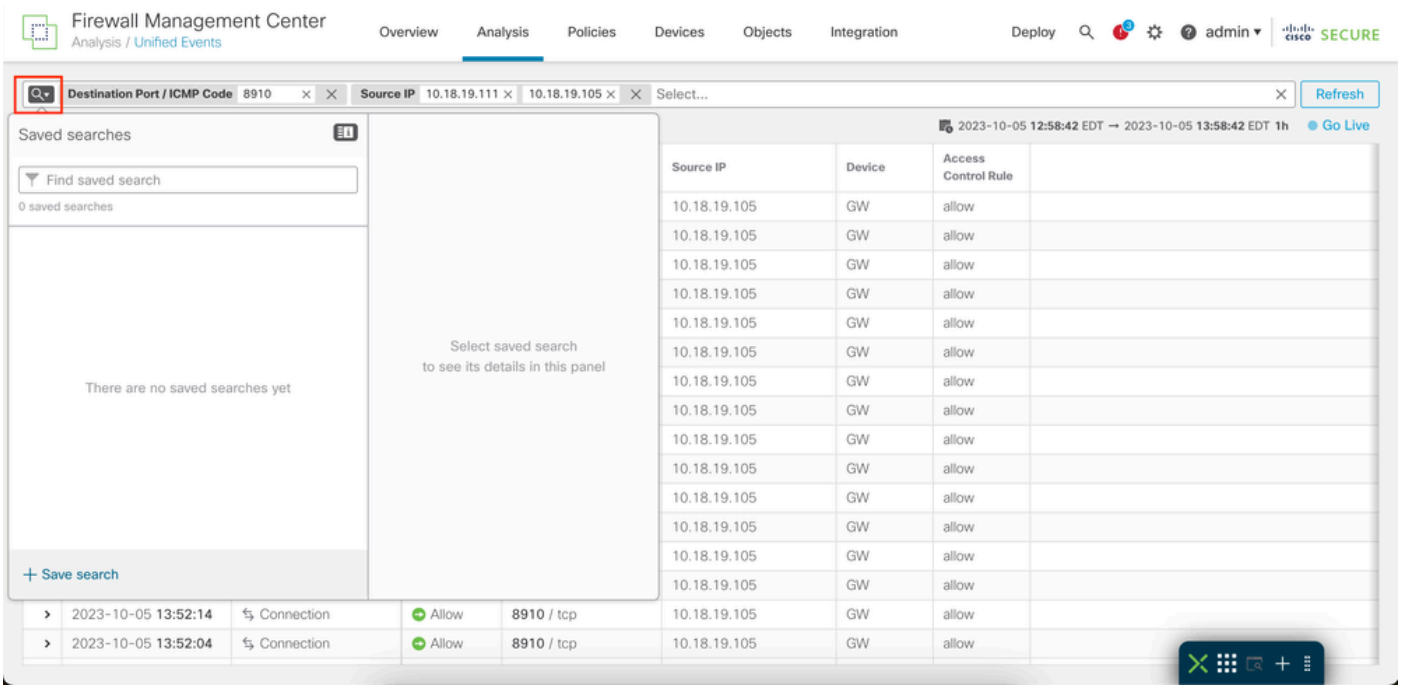


Tip: U kunt operatoren (>,<,!, enzovoort) gebruiken bij het schrijven van de waarden.

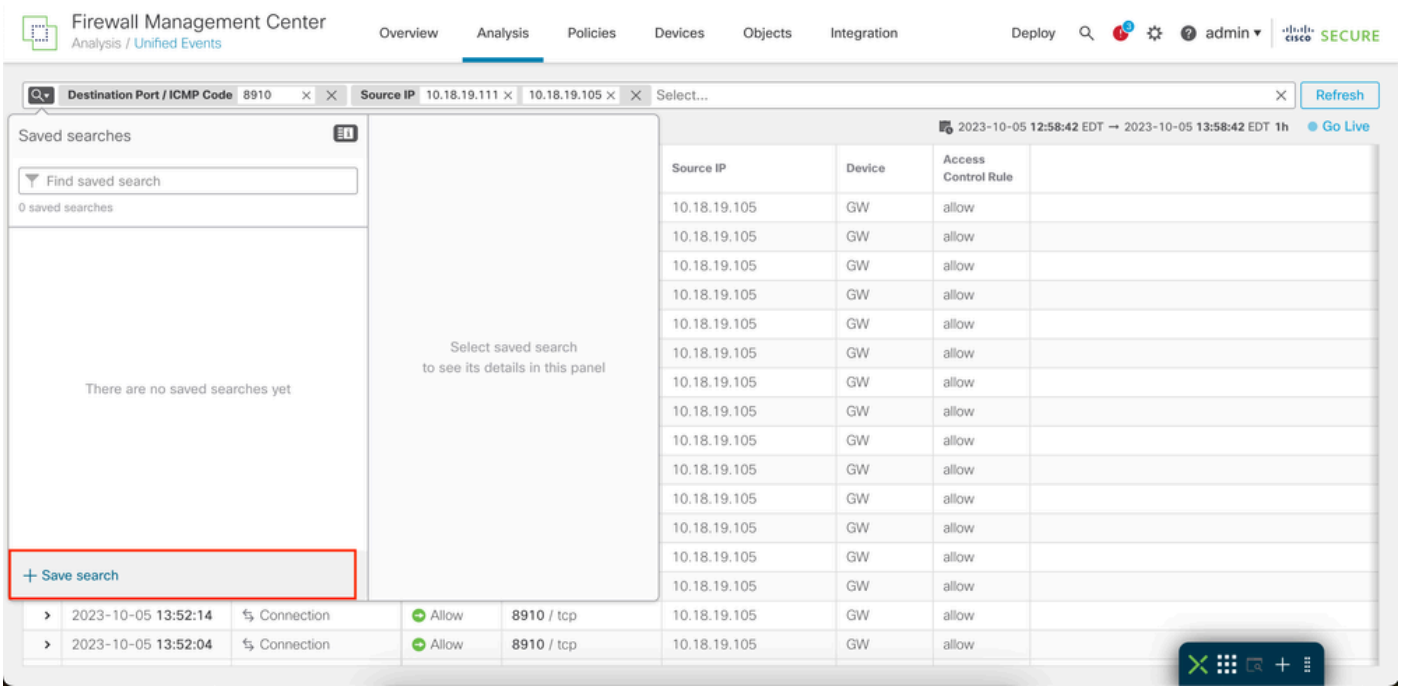
Zoekopdracht opslaan

Het is mogelijk om zoekopdrachten op te slaan, zodat u de filters die u hebt gemaakt opnieuw kunt gebruiken.

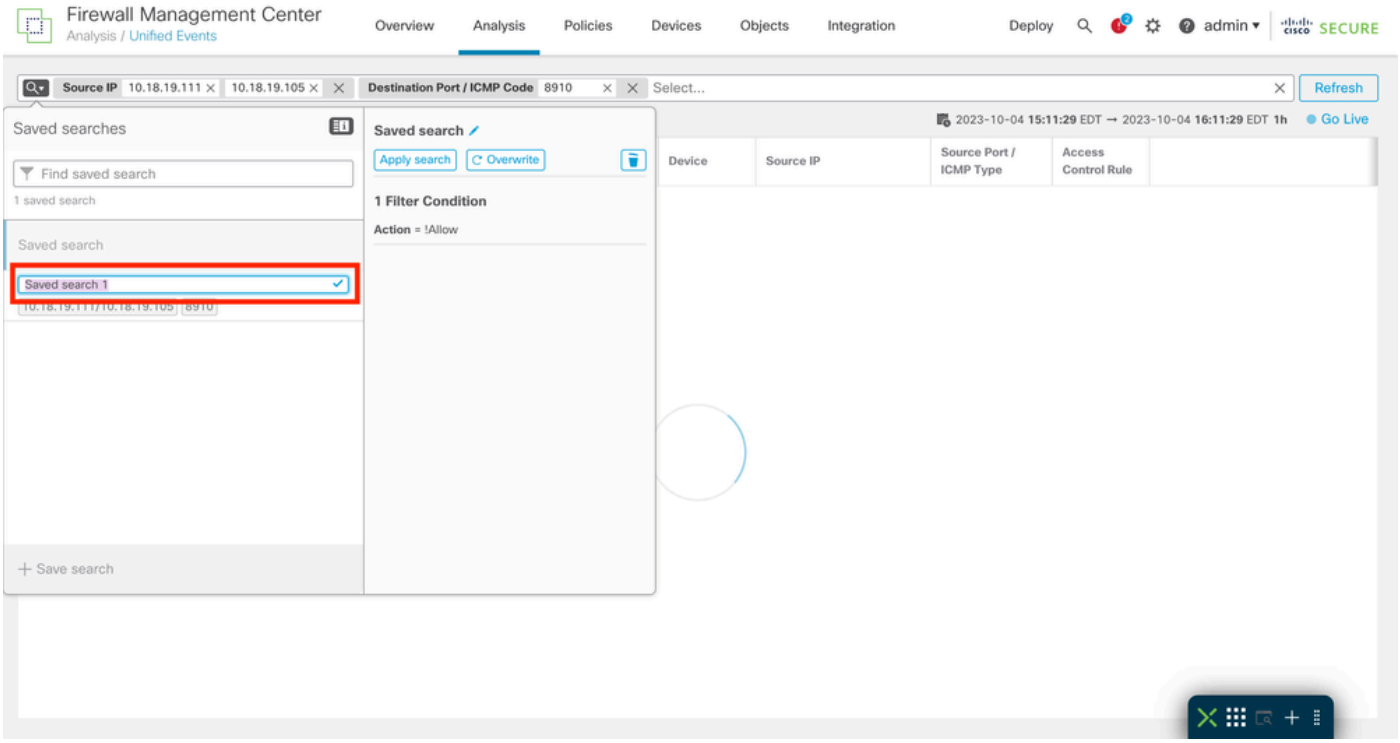
Stap 1. Klik op het pictogram van het vergrootglas.



Stap 2. Klik op Zoekopdracht opslaan.



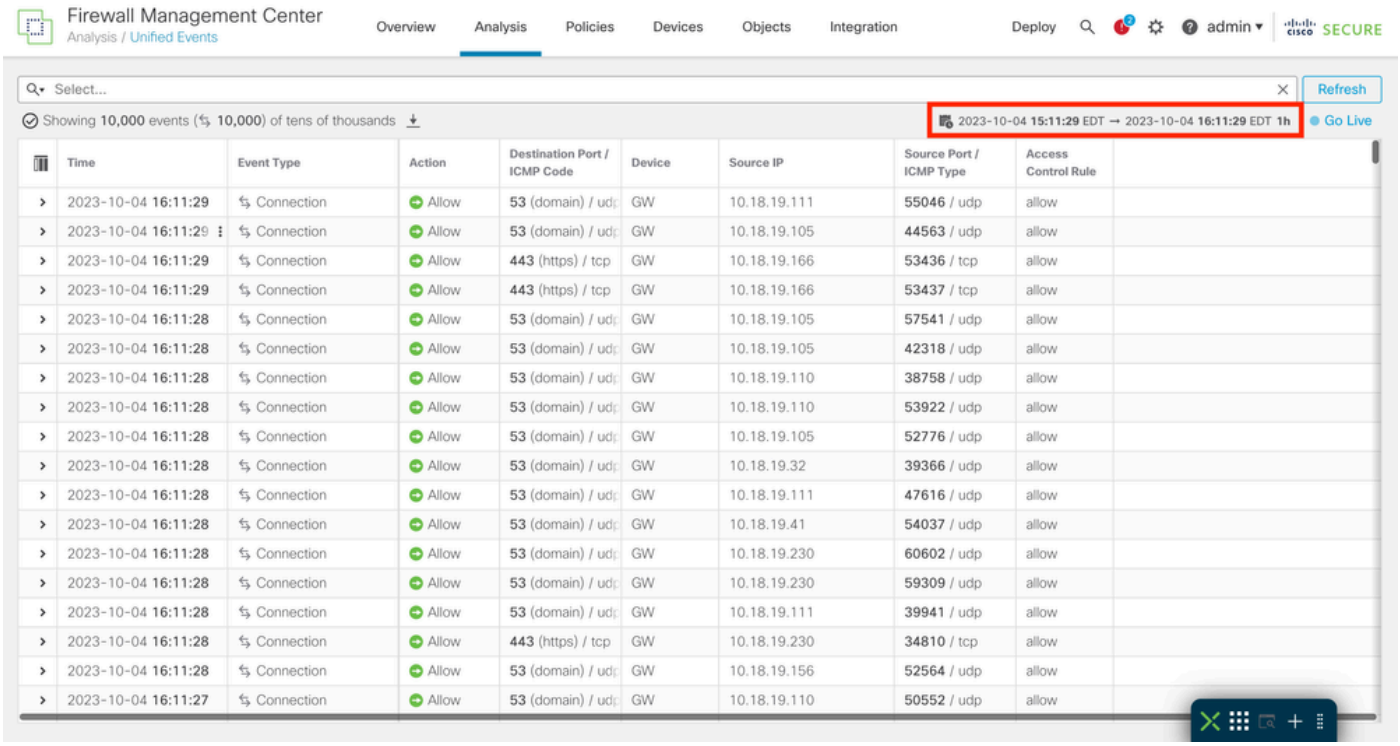
Stap 3. (Optioneel) Wijzig de naam van de zoekopdracht.



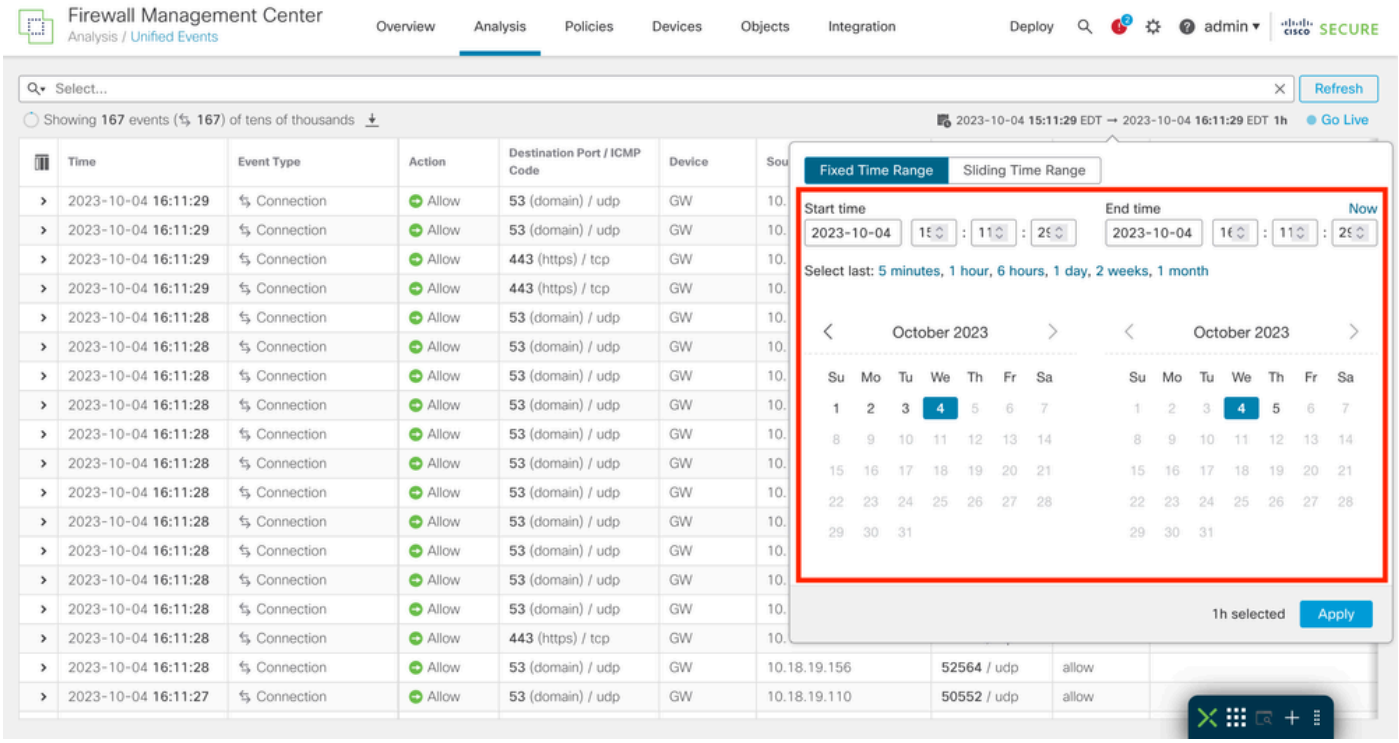
tijdsvenster

Het is gemakkelijker om relevante gebeurtenissen te beperken, op basis van een specifieke tijd, door het tijdsvenster te wijzigen.

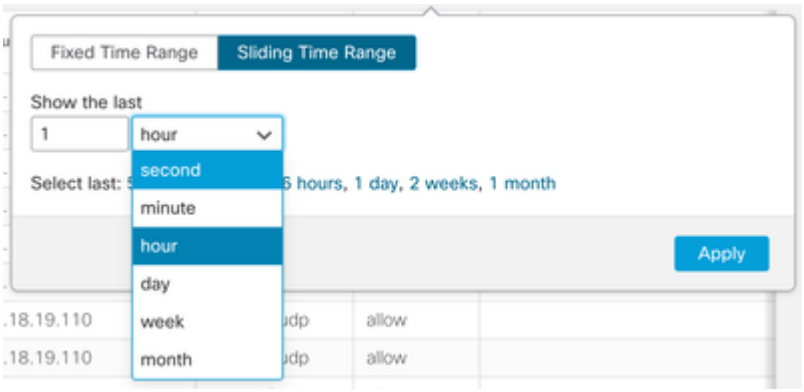
Stap 1. Als u het vensterkader van gebeurtenissen wilt wijzigen, klikt u op Datumbereik.



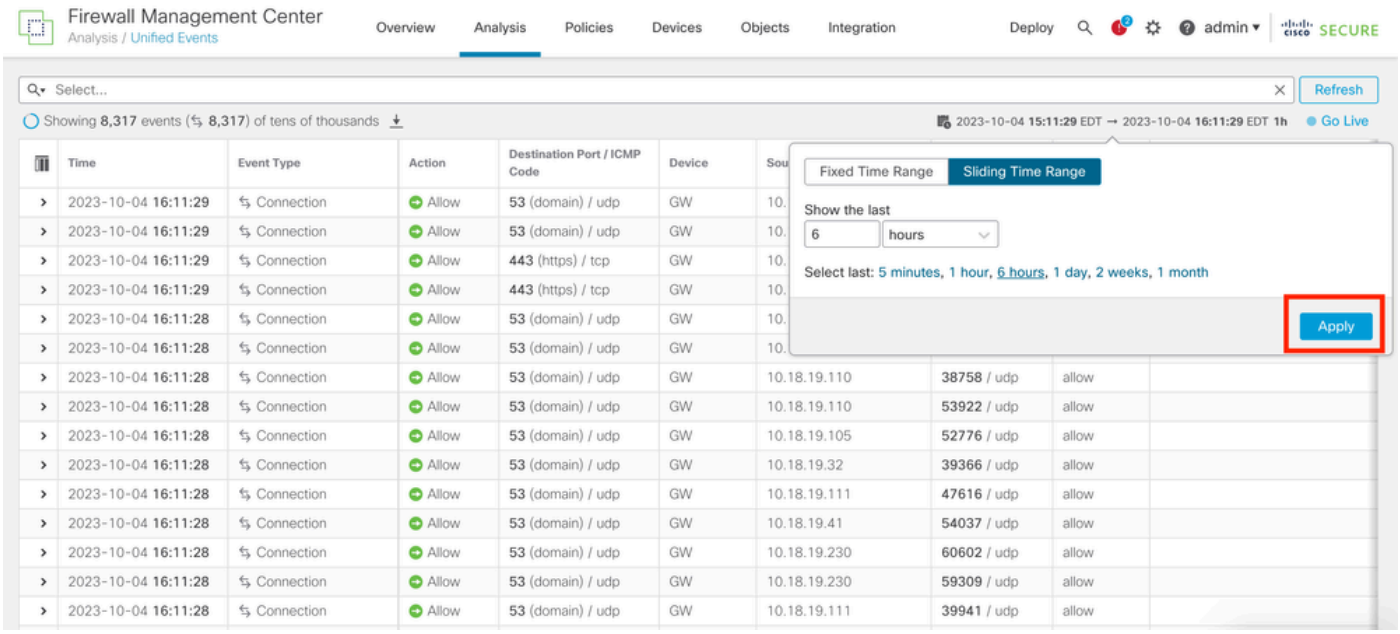
Stap 2. Selecteer het tijdbereik in het pop-upvenster.



Stap 3. (Optioneel) Gebruik het schuiftijdbereik om gebeurtenissen van een specifieke tijd tot uw huidige tijd weer te geven.



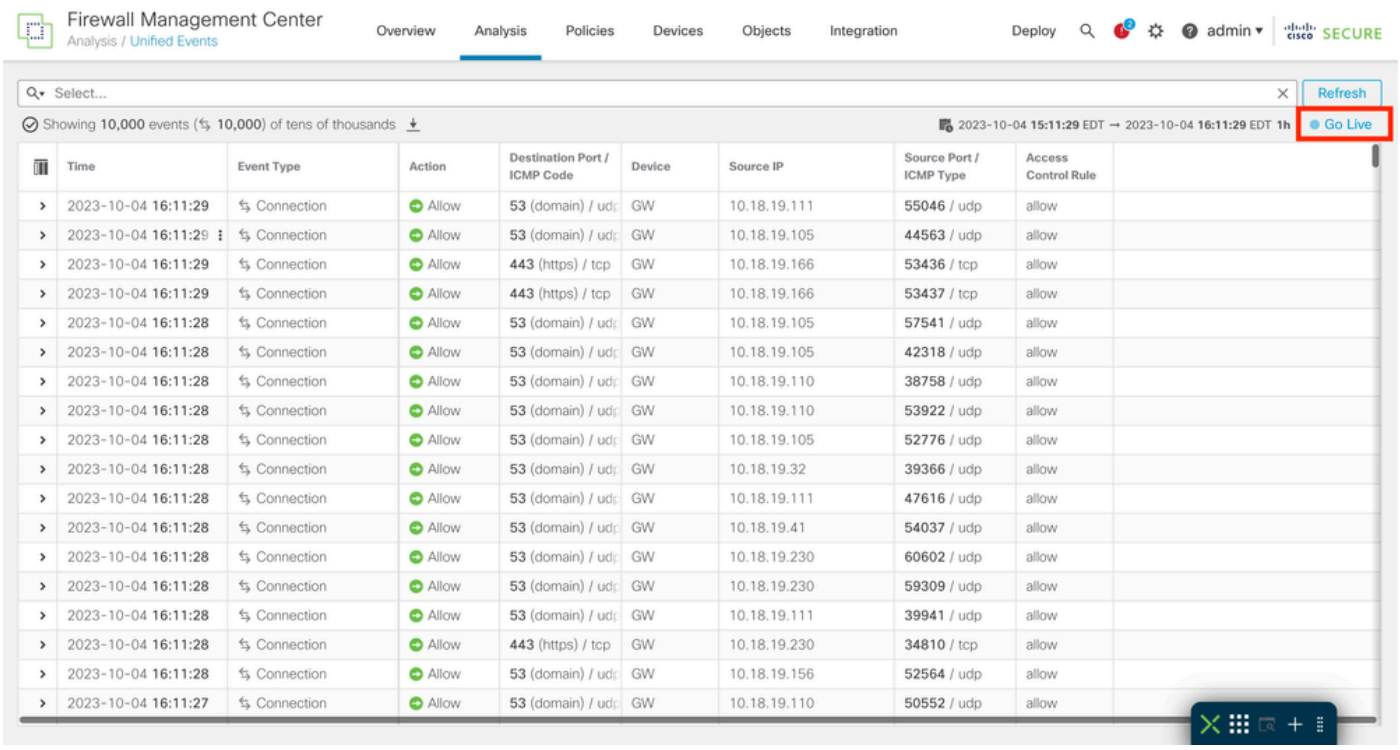
Stap 4. Klik op Toepassen om de gebeurtenissen in het geconfigureerde tijdbereik te filteren.



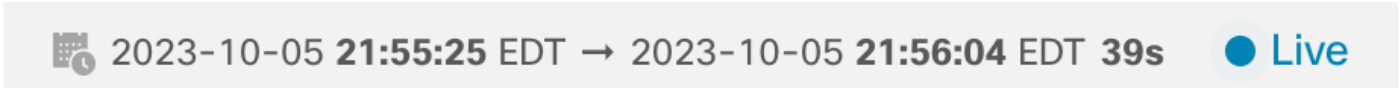
Ga live

U kunt de Go Live-functie inschakelen om gebeurtenissen in realtime weer te geven. De gebeurtenissen verschijnen zoals ze worden gegenereerd.

Om in te schakelen, klikt u op Go Live.



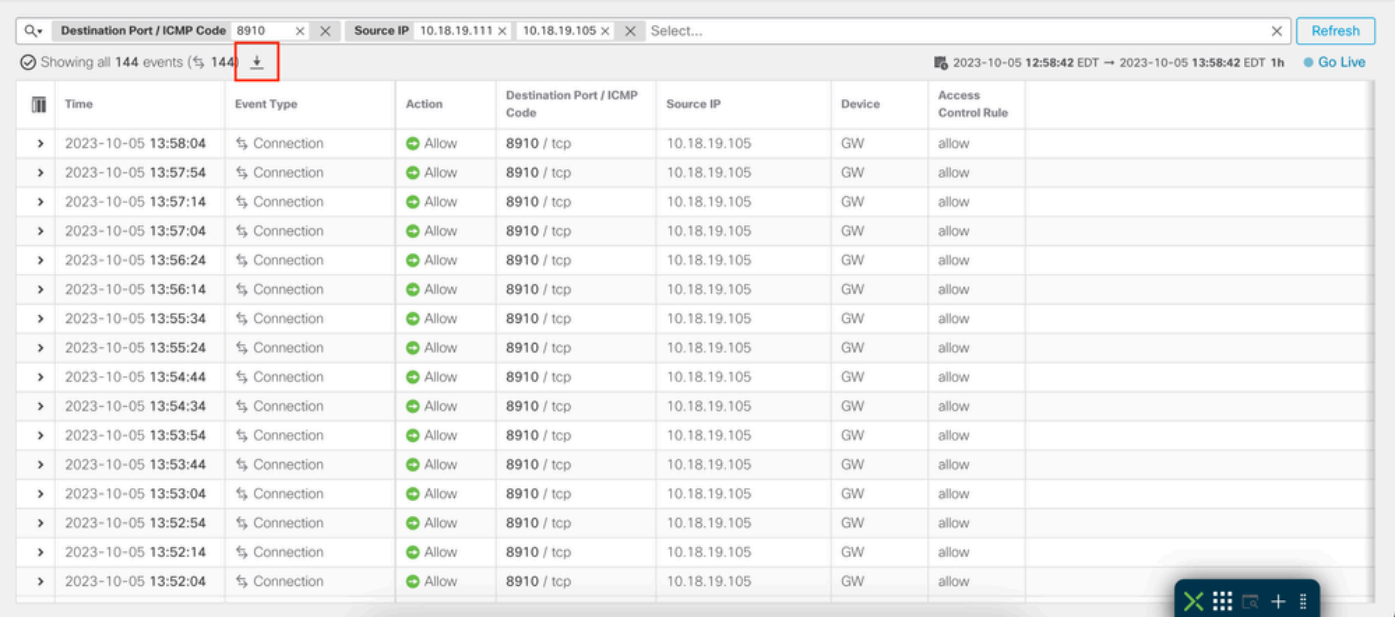
Zodra het is ingeschakeld, wordt het woord Live weergegeven.



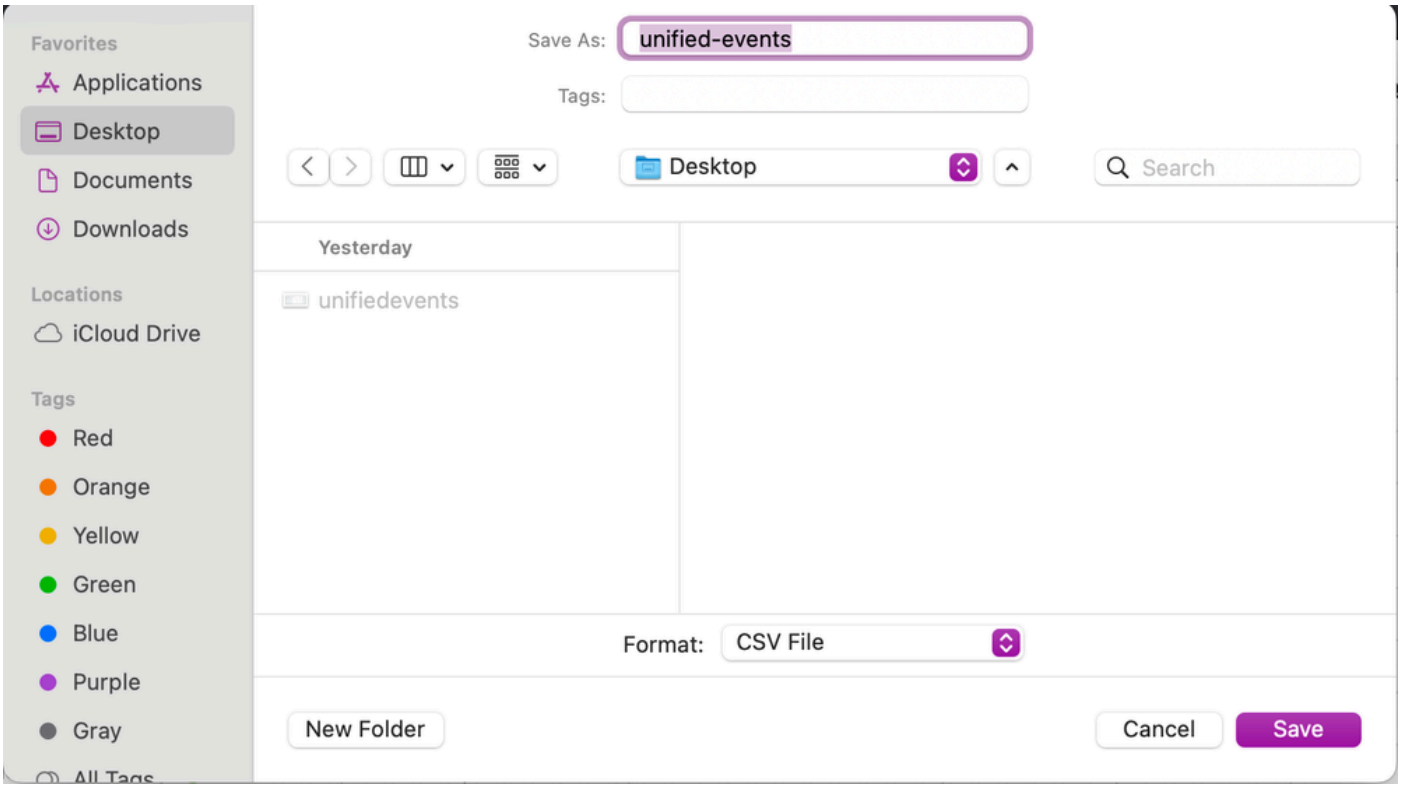
⚠ Let op: wanneer Live is ingeschakeld, is het niet mogelijk om het tijdvenster te wijzigen. Om het tijdvenster te wijzigen, schakelt u eerst de optie Live uit door er opnieuw op te klikken.

Downloaden van evenementen als Door komma's gescheiden waarden (CSV)

Stap 1. Klik op het downloadpictogram om een bestand te genereren met de gebeurtenissen die momenteel op de pagina worden weergegeven.



Stap 2. Selecteer de downloadmap, naam en klik op Opslaan.



Stap 3. Controleer het CSV-bestand.

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

Gerelateerde informatie

- Werken met de Unified Event Viewer
- Cisco Secure Firewall - Unified Events Viewer: tips en trucs
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.