

Gebeurtenissen bewaken met Unified Event Viewer op FMC GUI

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[verkennen](#)

[Voorbeeld van de pagina Unified Event](#)

[Gebeurtenissen bekijken](#)

[Kolommen personaliseren](#)

[Kolomset opslaan](#)

[Zoeken naar gebeurtenissen](#)

[Zoekopdracht opslaan](#)

[tijdsvenster](#)

[Ga live](#)

[Gebeurtenissen downloaden als door komma's gescheiden waarden \(CSV\)](#)

[Gerelateerde informatie](#)

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:

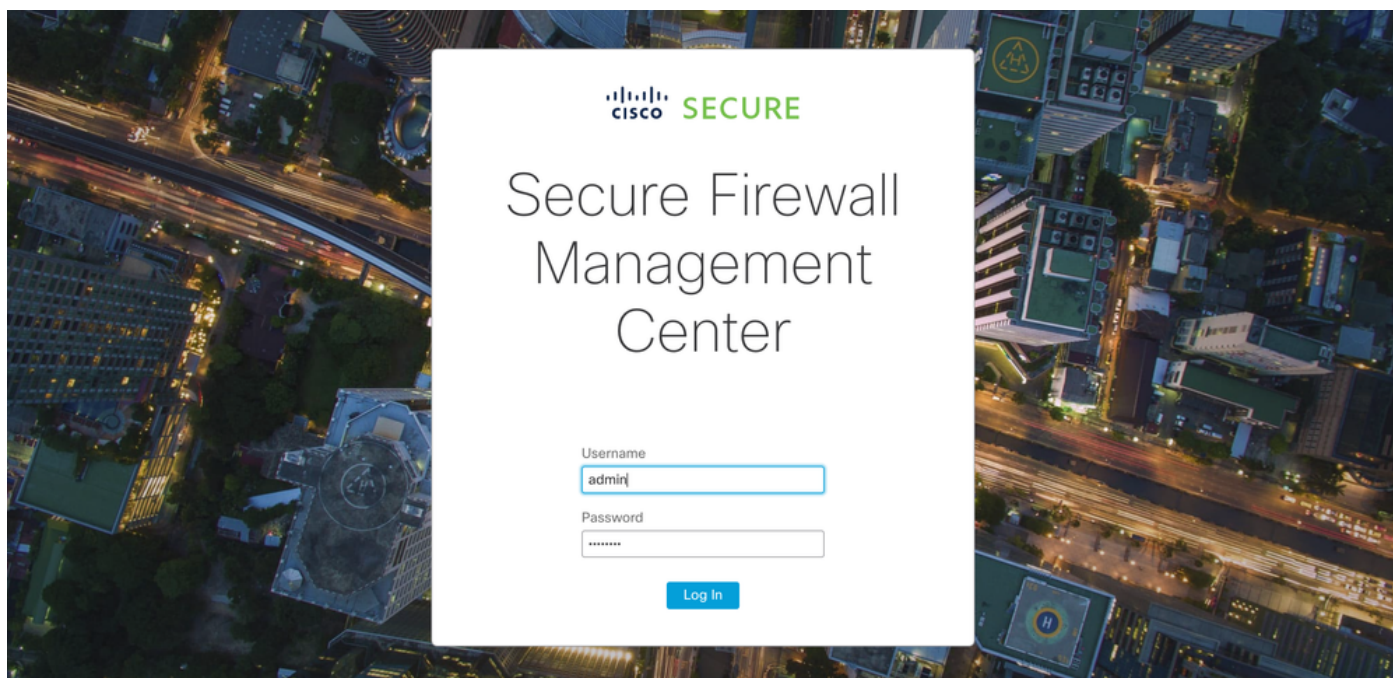
- Secure Firewall Management Center voor VMware v7.2.5

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

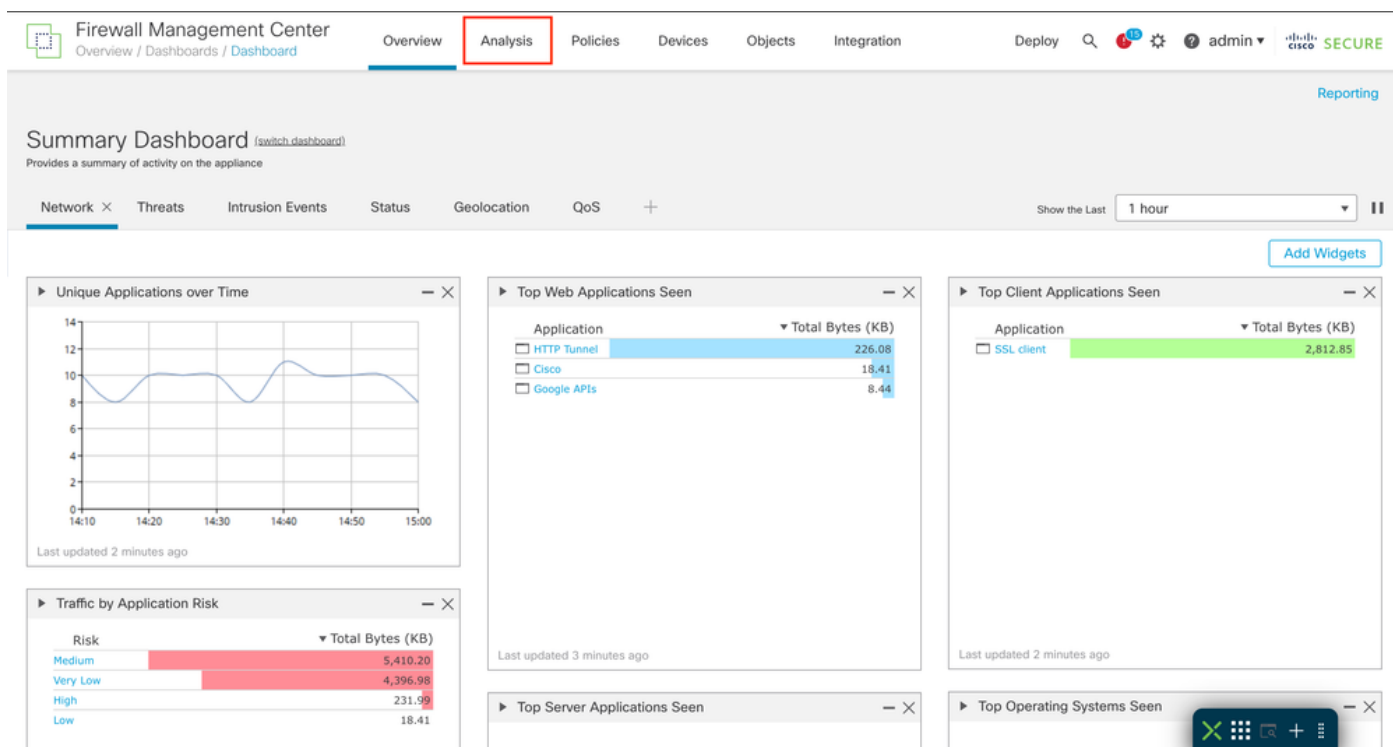
opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

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.

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
12
10
8
6
4
2
0

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

Voorbeeld van de pagina Unified Event

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

Gebeurtenissen bekijken

Stap 1. Klik op het > icoon.

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

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

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

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: ApplD

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

Kolommen personaliseren

Stap 1. Klik op het icoon .

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

Stap 2. Selecteer de gewenste gebeurtenisvelden op de tabel.

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 App
		OW		10.18.19.111	10.1.8.107	55046 / udp	53 (domain) / udp	
		OW		10.18.19.105	10.1.20.51	44563 / udp	53 (domain) / udp	
		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) / udp	
		OW		10.18.19.105	10.1.20.51	42318 / udp	53 (domain) / udp	
		OW		10.18.19.110	10.1.9.38	38758 / udp	53 (domain) / udp	
		OW		10.18.19.110	10.1.8.101	53922 / udp	53 (domain) / udp	
		OW		10.18.19.105	10.27.20.51	52776 / udp	53 (domain) / udp	
		OW		10.18.19.32	208.67.220.220	39366 / udp	53 (domain) / udp	
		OW		10.18.19.111	10.1.8.101	47616 / udp	53 (domain) / udp	
		OW		10.18.19.41	208.67.220.220	54037 / udp	53 (domain) / udp	
		OW		10.18.19.230	173.37.87.157	60602 / udp	53 (domain) / udp	
		OW		10.18.19.230	173.37.87.157	59309 / udp	53 (domain) / udp	
		OW		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

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

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

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

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

Stap 5. Klik op Toepassen.

Saved Column Sets

Select...

Filter columns

Select none

Select default

☒ Event Type

☒ Action

☒ Destination Port / ICMP Code

☒ Source IP

☒ Device

Revert

6 selected

Apply

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

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

admin

Go Live

Select...

Refresh

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

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

	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	

Kolomset opslaan

Stap 1. Klik op Opgeslagen kolomsets.

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	

Revert 11 selected Apply

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

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

Revert 11 selected Apply

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

Saved Column Sets

Select...

2 saved column sets

Rule match ✓

Time Event Type Action Reason Source IP Destination IP S

Saved Column Set 1

Time Event Type Action Reason Source IP Destination IP S

+ Create column set from current selection

☐ NetFlow **Source** Autonomous System

☐ NetFlow **Source** Prefix

Revert 6 selected Apply

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

Firewall Management Center
Analysis / Unified Events

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

Select... Refresh

Showing 10,000 events (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

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

Rename Delete Overwrite

Revert 11 selected Apply

Zoeken naar gebeurtenissen

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

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

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

Firewall Management Center
Analysis / Unified Events

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

Q source Refresh

Selected: 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**

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

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

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

Q Source IP X Select...

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

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔍

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

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

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔍

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

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

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔍

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



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.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Analysis' tab is selected. The search bar at the top has a magnifying glass icon highlighted with a red box. Below the search bar, the search criteria are 'Destination Port / ICMP Code' with the value '8910' and 'Source IP' with the values '10.18.19.111' and '10.18.19.105'. The search results table shows the following data:

Source IP	Device	Access Control Rule
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow

Stap 2. Klik op Zoekopdracht opslaan.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Analysis' tab is selected. The search bar at the top has a magnifying glass icon highlighted with a red box. Below the search bar, the search criteria are 'Destination Port / ICMP Code' with the value '8910' and 'Source IP' with the values '10.18.19.111' and '10.18.19.105'. The search results table shows the following data:

Source IP	Device	Access Control Rule
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow
10.18.19.105	GW	allow

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

Firewall Management Center
Analysis / Unified Events

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

Source IP 10.18.19.111 x 10.18.19.105 x Destination Port / ICMP Code 8910 x Select... Refresh

Saved searches

Find saved search

1 saved search

Saved search

Saved search 1 ✓

10.18.19.111/10.18.19.105 | 8910

+ Save search

Saved search

Apply search Overwrite

1 Filter Condition

Action = !Allow

Device	Source IP	Source Port / ICMP Type	Access Control Rule
--------	-----------	-------------------------	---------------------

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

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.

Firewall Management Center
Analysis / Unified Events

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

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

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 16:11:28	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

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.

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

Zodra het is ingeschakeld, wordt het woord Live weergegeven.

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



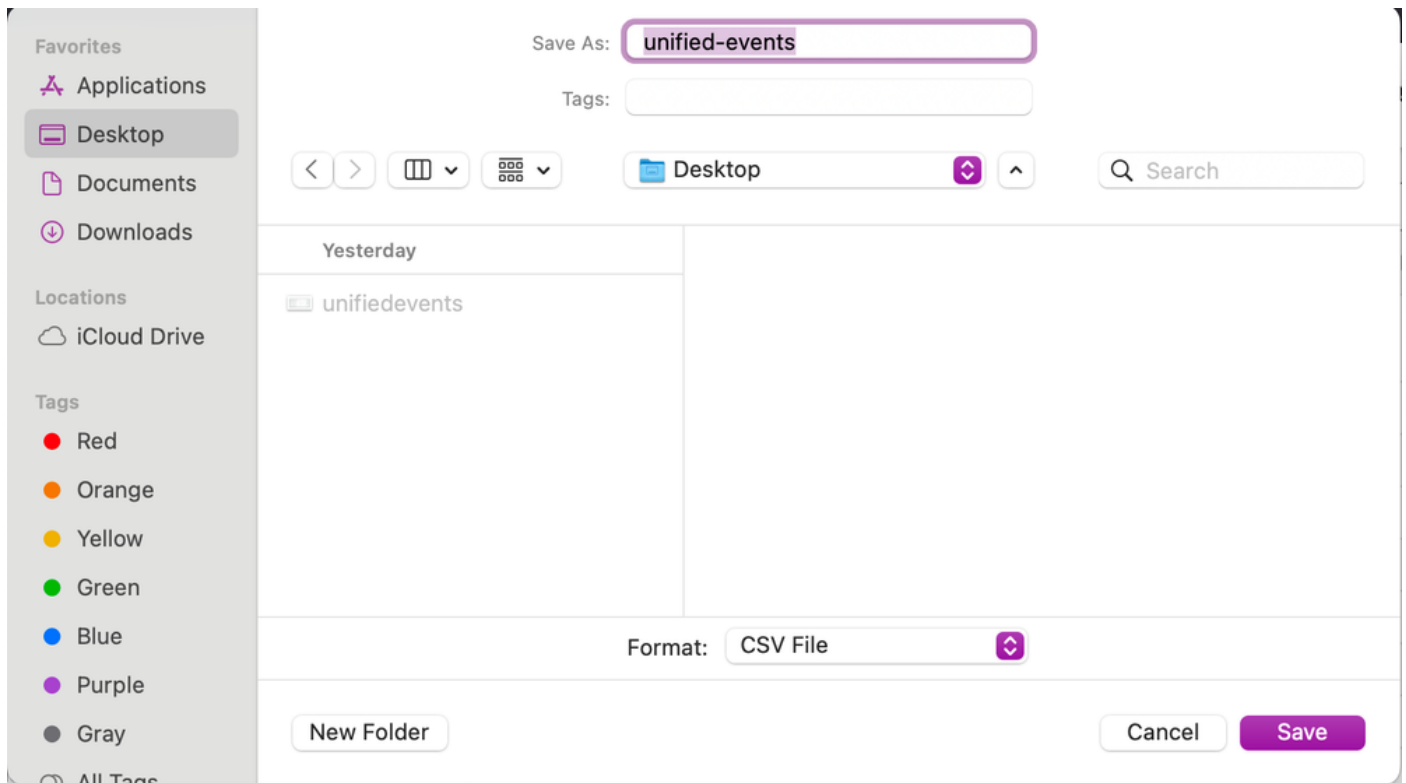
Let op: wanneer Live is ingeschakeld, is het niet mogelijk om het tijdvenster te wijzigen. Om het tijdvenster te wijzigen, schakelt u eerst de optie Live uit door er opnieuw op te klikken.

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.

Destination Port / ICMP Code 8910		Source IP 10.18.19.111		10.18.19.105		Select...		Refresh	
Showing all 144 events (1/144)				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			

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.