

Supervisión de eventos mediante el visor de eventos unificado en la GUI de FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Explorar](#)

[Ejemplo de la página Evento de Unified](#)

[Revisar eventos](#)

[Personalizar columnas](#)

[Guardar conjunto de columnas](#)

[Búsqueda de eventos](#)

[Guardar búsqueda](#)

[Ventana de tiempo](#)

[Puesta en marcha](#)

[Descargar eventos como valores separados por comas \(CSV\)](#)

[Información Relacionada](#)

Introducción

Este documento describe el uso de Unified Event Viewer en una interfaz gráfica de usuario (GUI) en Firewall Management Center (FMC).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso a FMC con privilegios de administrador o analista de seguridad
- FMC con versión igual o superior a v7.0

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

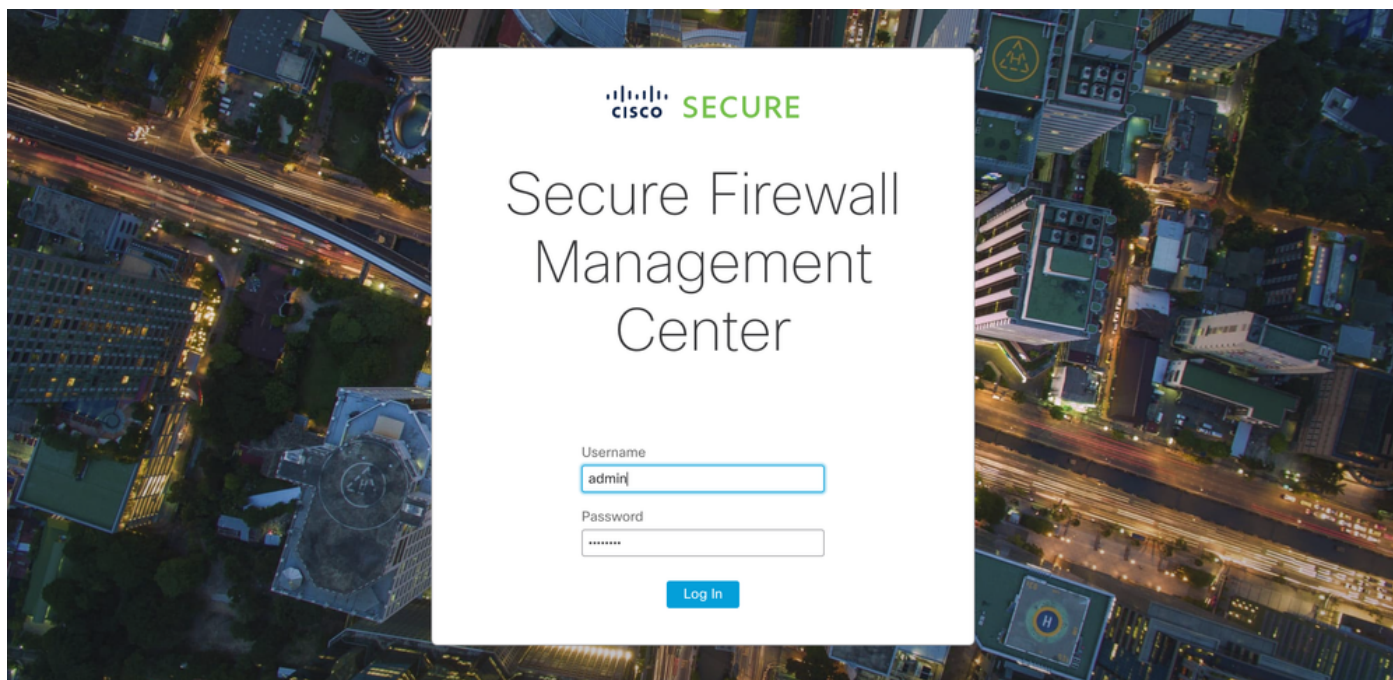
- Secure Firewall Management Center para VMware v7.2.5

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

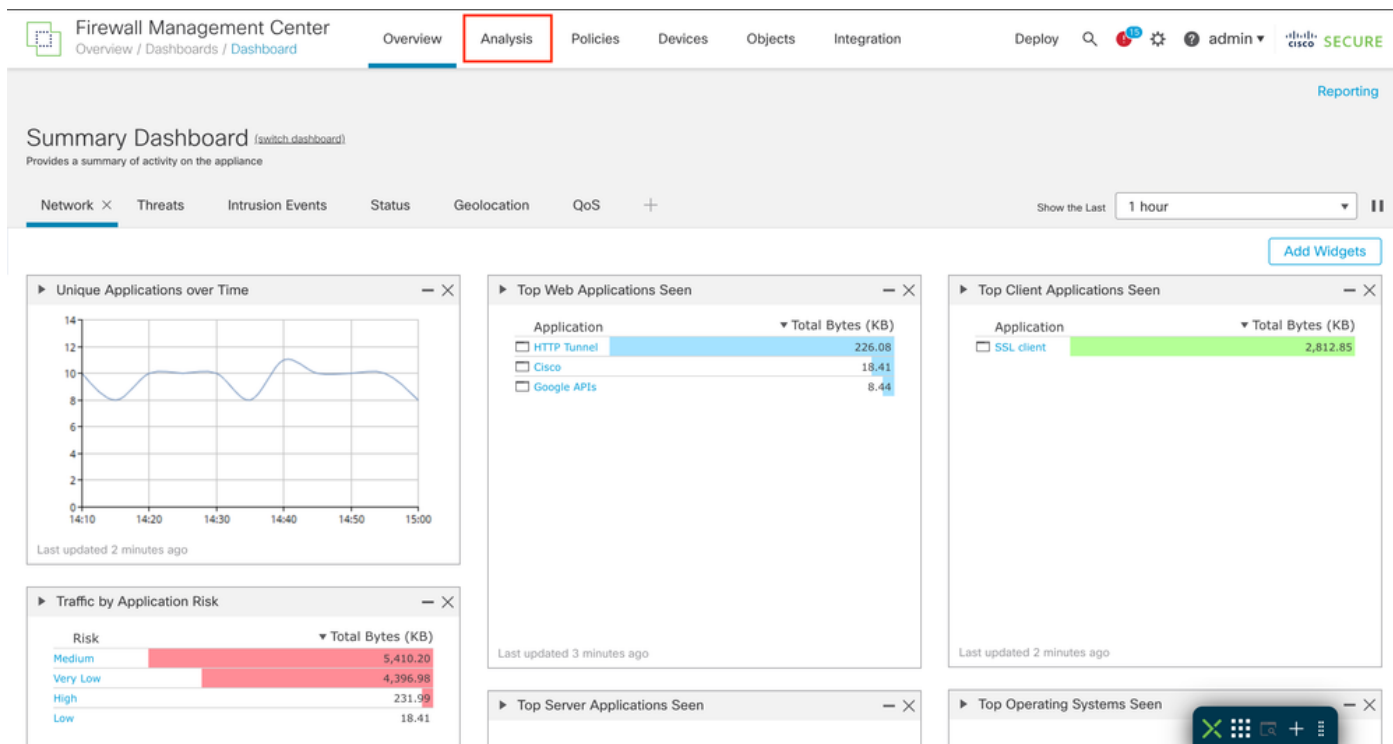
de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Explorar

Paso 1. Inicie sesión en la GUI de FMC.



Paso 2. Acceda a la pestaña Análisis.



Paso 3. En el menú desplegable, haga clic en 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

Unique Applications over Time

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

Ejemplo de la página Evento de Unified

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

Revisar eventos

Paso 1. Haga clic en el icono >.

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

Paso 2. Se muestra la información detallada del evento.

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

Personalizar columnas

Paso 1. Haga clic en el icono

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

Paso 2. Seleccione los campos de eventos que desea incluir en la tabla.

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

Paso 3. (Opcional) Busque el campo para facilitar la navegación.

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

Paso 4. Haga clic en un campo de evento para desactivar o activar.

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

Paso 5. Haga clic en Aplicar.

Saved Column Sets

Select...

Filter columns

Select none | Select default

- ☒ Event Type
- ☒ Action
- ☒ Destination Port / ICMP Code
- ☒ Source IP
- ☒ Device

Revert 6 selected **Apply**

Paso 6. (Opcional) Puede cambiar la posición de las columnas arrastrando cada una de ellas a una ubicación diferente.

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy Search Settings Admin admin

Showing 10,000 events (of tens of thousands)

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

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

Guardar conjunto de columnas

Paso 1. Haga clic en Conjuntos de Columnas Guardados.

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	

2023-10-04 16:11:28 Connection Allow

Paso 2. Haga clic en Crear juego de columnas de la selección actual.

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

2023-10-04 16:11:28 Connection Allow

2023-10-04 16:11:28 Connection Allow

Paso 3. (Opcional) Cambie el nombre del juego de columnas.

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

Paso 4. Puede editar un juego existente haciendo clic en los puntos suspensivos (...).

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

2023-10-04 16:11:28 Connection Allow

Búsqueda de eventos

Paso 1. Para comenzar a buscar eventos específicos, haga clic en Seleccionar.

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

Paso 2. Seleccione el campo al que desea aplicar el filtro.

Firewall Management Center
Analysis / Unified Events

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

Q source Refresh

Selected: NAT Source IP

Available fields:

- 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

Paso 3. Escriba los valores que se utilizarán como filtro.

Q Source IP X Select...

Paso 4. Haga clic en Apply, para configurar el filtro.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔒

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

Paso 5. (Opcional) Puede agregar varios valores a cada filtro.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔒

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

Paso 6. (Opcional) Agregue tantos filtros como necesite.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

🔍

🔧

🔔

admin

🔒

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



Guardar búsqueda

Paso 1. Haga clic en el icono de lupa.

Paso 2. Haga clic en Guardar búsqueda.

Paso 3. (Opcional) Cambie el nombre de la búsqueda.

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

Ventana de tiempo

Es más fácil restringir los eventos relevantes, basándose en una hora específica, modificando la ventana de tiempo.

Paso 1. Para modificar el marco de ventana de los eventos, haga clic en el rango de fechas.

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

Paso 2. Seleccione el rango de tiempo en la ventana emergente.

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	38758 / udp	allow
2023-10-04 16:11:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:29	Connection	Allow	443 (https) / tcp	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

Puesta en marcha

Puede activar la función Go Live para mostrar eventos en tiempo real. Los eventos aparecen a medida que se generan.

Para activarla, haga clic en Go Live (Activar).

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

Una vez habilitada, muestra la palabra Live.

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



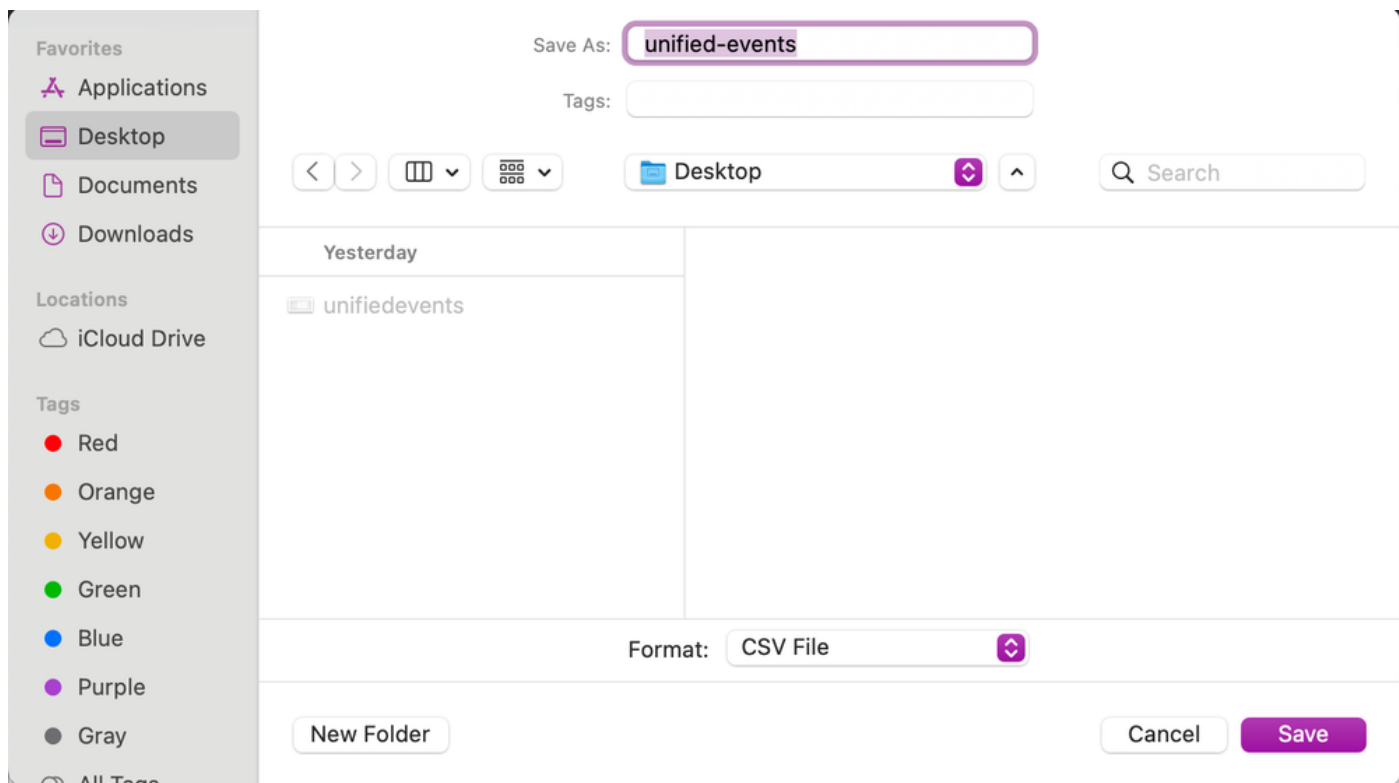
Precaución: Cuando Live está activado, no es posible modificar la ventana de tiempo. Para modificar la ventana de tiempo, primero inhabilite la opción Live haciendo clic en ella otra vez.

Descargar eventos como Valores separados por comas (CSV)

Paso 1. Haga clic en el icono de descarga para generar un archivo que contenga los eventos que se muestran actualmente en la página.

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

Paso 2. Seleccione la carpeta de descarga, nombre y haga clic en Guardar.



Paso 3. Verifique el archivo 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

Información Relacionada

- [Trabajo con el Visor de sucesos de Unified](#)
- [Cisco Secure Firewall - Visor de eventos unificado: Sugerencias y trucos](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).