

Monitore eventos usando o Unified Event Viewer na GUI do FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Explorar](#)

[Exemplo da página de eventos unificados](#)

[Revisar eventos](#)

[Personalizar Colunas](#)

[Salvar Conjunto de Colunas](#)

[Pesquisa de evento](#)

[Salvar pesquisa](#)

[Janela de Tempo](#)

[Lançamento](#)

[Baixar eventos como valores separados por vírgula \(CSV\)](#)

[Informações Relacionadas](#)

Introdução

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

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

Componentes Utilizados

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

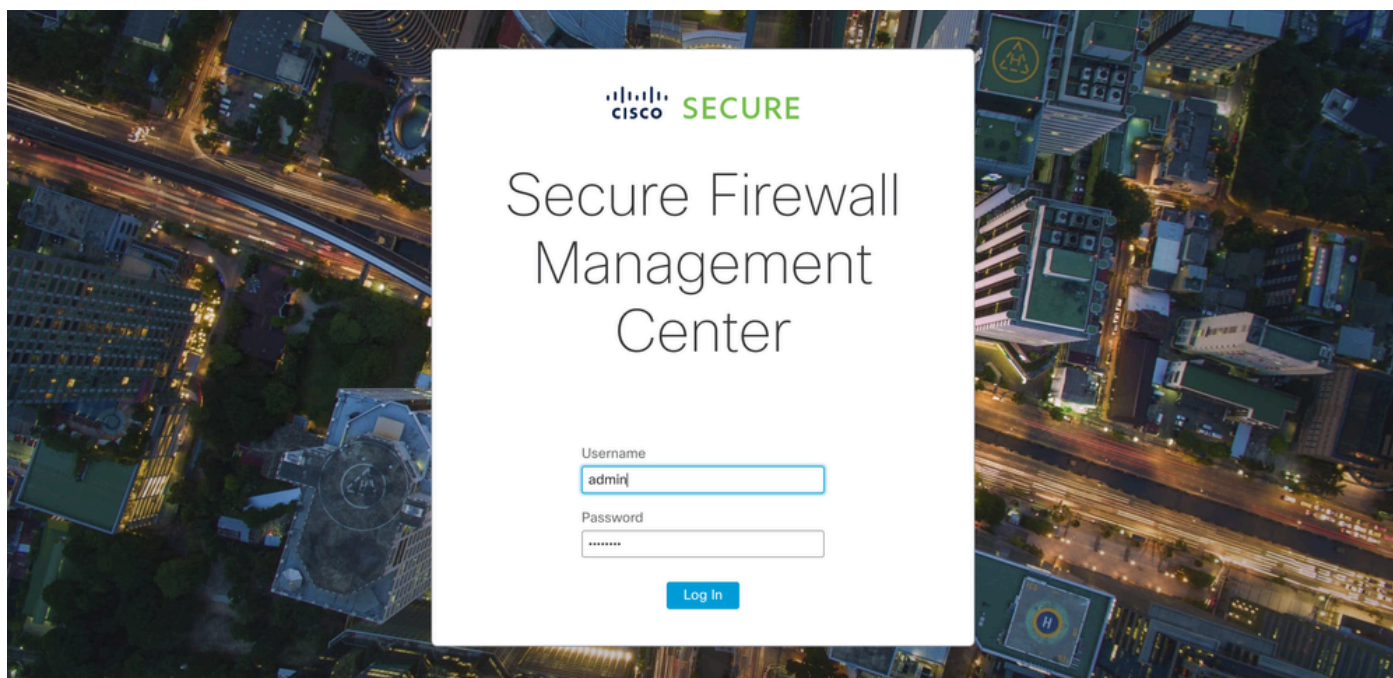
- Secure Firewall Management Center para VMware v7.2.5

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

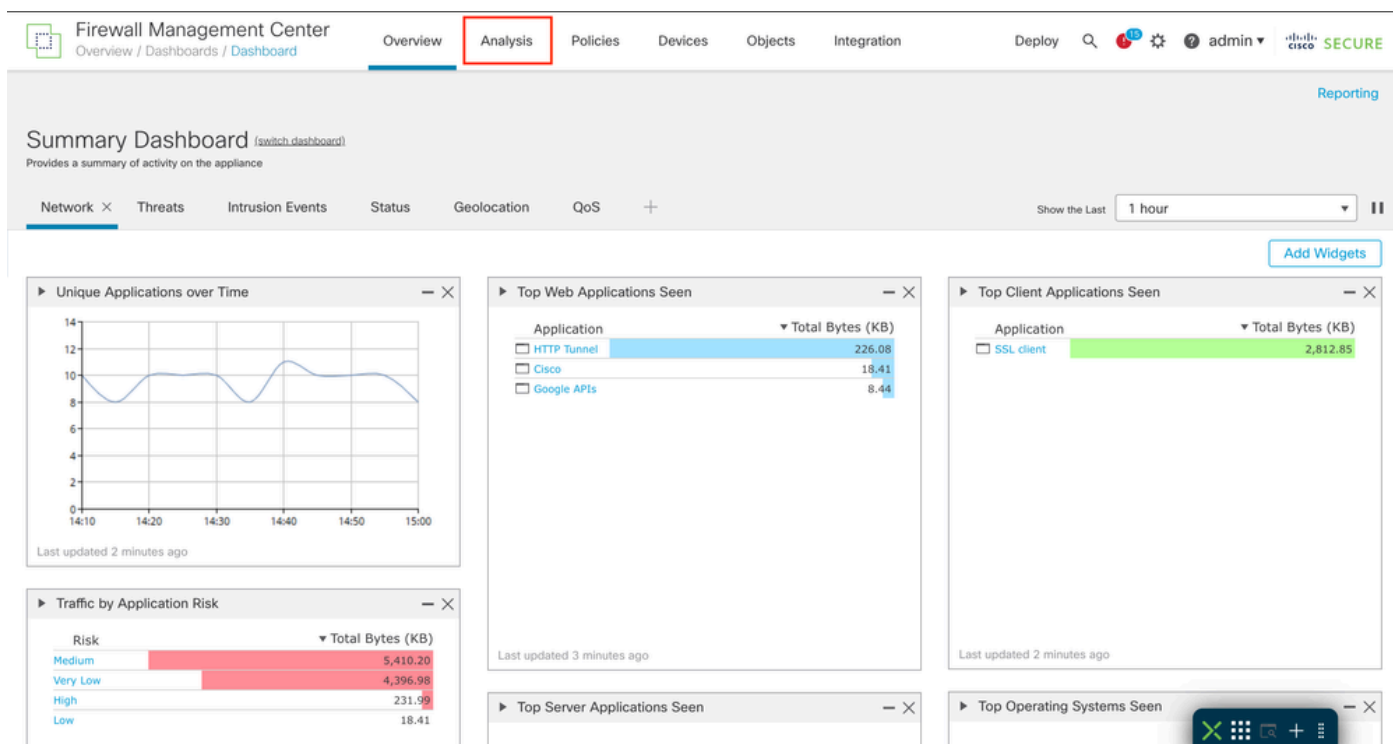
configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Explorar

Etapa 1. Fazer login na GUI do FMC.



Etapa 2. Navegue até a guia Análise.



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

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

Exemplo da página de eventos unificados

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

Etapa 1. Clique no ícone > .

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

Etapa 2. As informações detalhadas do evento são exibidas.

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 Colunas

Etapa 1. Clique no ícone

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

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

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	Reason	Source IP	Destination IP	Source Port / ICMP Type	Destination Port / ICMP Code	Web A
		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

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

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

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

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

Etapa 5. Clique em Apply.

Saved Column Sets

Select...

Filter columns

Select none | Select default

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

Revert 6 selected **Apply**

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

Firewall Management Center
Analysis / Unified Events

Overview Analysis Policies Devices Objects Integration Deploy Search Settings Admin Admin

Select... Refresh

Showing 10,000 events (of tens of thousands)

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

Salvar Conjunto de Colunas

Etapa 1. Clique em Conjuntos de Colunas Salvas.

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) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.105	10.1.20.51	44563 / udp	53 (domain) / udp	
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) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.105	10.1.20.51	42318 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.110	10.1.9.38	38758 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.110	10.1.8.101	53922 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.105	10.27.20.51	52776 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.32	208.67.220.220	39366 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.111	10.1.8.101	47616 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.41	208.67.220.220	54037 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.230	173.37.87.157	60602 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.230	173.37.87.157	59309 / udp	53 (domain) / udp	
2023-10-04 16:11:28	Connection	Allow		10.18.19.111	10.1.8.101	39941 / udp	53 (domain) / udp	

Revert 11 selected Apply

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

Firewall Management Center
Analysis / Unified Events

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

Q Select... Refresh

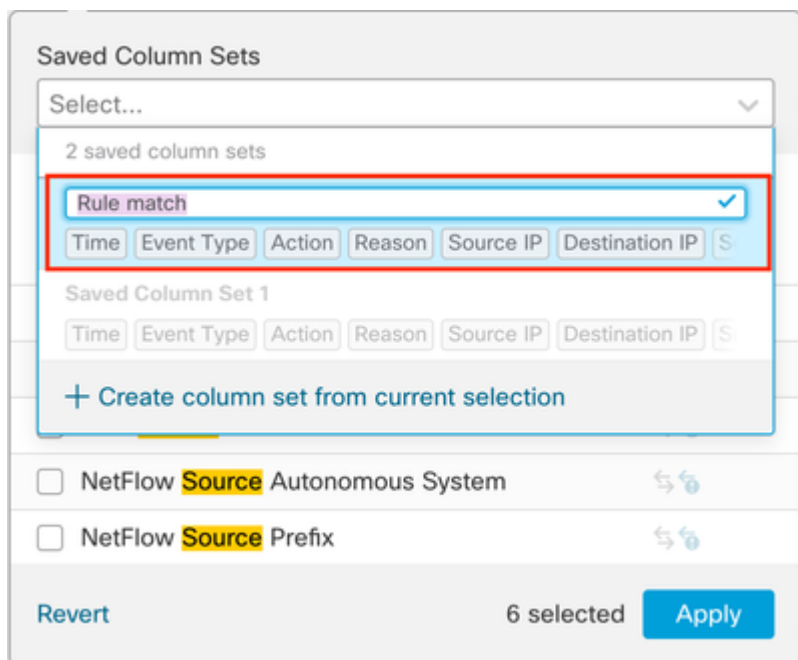
Showing 10,000 events (10,000) of tens of thousands

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) / udp	GW	10.18.19.111	55046 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.20.51	53 (domain) / udp	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) / udp	GW	10.18.19.105	57541 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.20.51	53 (domain) / udp	GW	10.18.19.105	42318 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.9.38	53 (domain) / udp	GW	10.18.19.110	38758 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.8.101	53 (domain) / udp	GW	10.18.19.110	53922 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.27.20.51	53 (domain) / udp	GW	10.18.19.105	52776 / udp	allow
2023-10-04 16:11:28	Connection	Allow	208.67.220.220	53 (domain) / udp	GW	10.18.19.32	39366 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.8.101	53 (domain) / udp	GW	10.18.19.111	47616 / udp	allow
2023-10-04 16:11:28	Connection	Allow	208.67.220.220	53 (domain) / udp	GW	10.18.19.41	54037 / udp	allow
2023-10-04 16:11:28	Connection	Allow	173.37.87.157	53 (domain) / udp	GW	10.18.19.230	60602 / udp	allow
2023-10-04 16:11:28	Connection	Allow	173.37.87.157	53 (domain) / udp	GW	10.18.19.230	59309 / udp	allow
2023-10-04 16:11:28	Connection	Allow	10.1.8.101	53 (domain) / udp	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

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



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

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 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

Source IP

Destination IP

Source Port / ICMP Type

Destination Port / ICMP Code

Revert 11 selected Apply

Pesquisa de evento

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

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

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

Firewall Management Center
Analysis / Unified Events

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

Q source 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

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

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

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

Q Source IP X Select...

Etapa 4. Clique em Apply para configurar o 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

Etapa 5. (Opcional) Você pode adicionar vários 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

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

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



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

Salvar pesquisa

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

Etapa 1. Clique no ícone de lupa.

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 main area displays a search bar with the text 'Destination Port / ICMP Code 8910' and 'Source IP 10.18.19.111 x 10.18.19.105 x'. Below the search bar, there is a 'Saved searches' panel on the left and a table of search results on the right. The 'Saved searches' panel shows '0 saved searches' and a '+ Save search' button. The table of search results has columns for 'Source IP', 'Device', and 'Access Control Rule'. The table contains 15 rows of data, all showing '10.18.19.105' as the Source IP, 'GW' as the Device, and 'allow' as the Access Control Rule.

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

Etapa 2. Clique em Save Search.

The screenshot shows the Firewall Management Center interface, similar to the previous one. The 'Saved searches' panel on the left now shows a '+ Save search' button, which is highlighted with a red box. The table of search results remains the same, showing 15 rows of 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

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

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

Janela de Tempo

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

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

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

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

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

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

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

Lançamento

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

Para habilitar, clique em Go Live.

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

Depois de ativada, ela exibe a palavra Live.

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



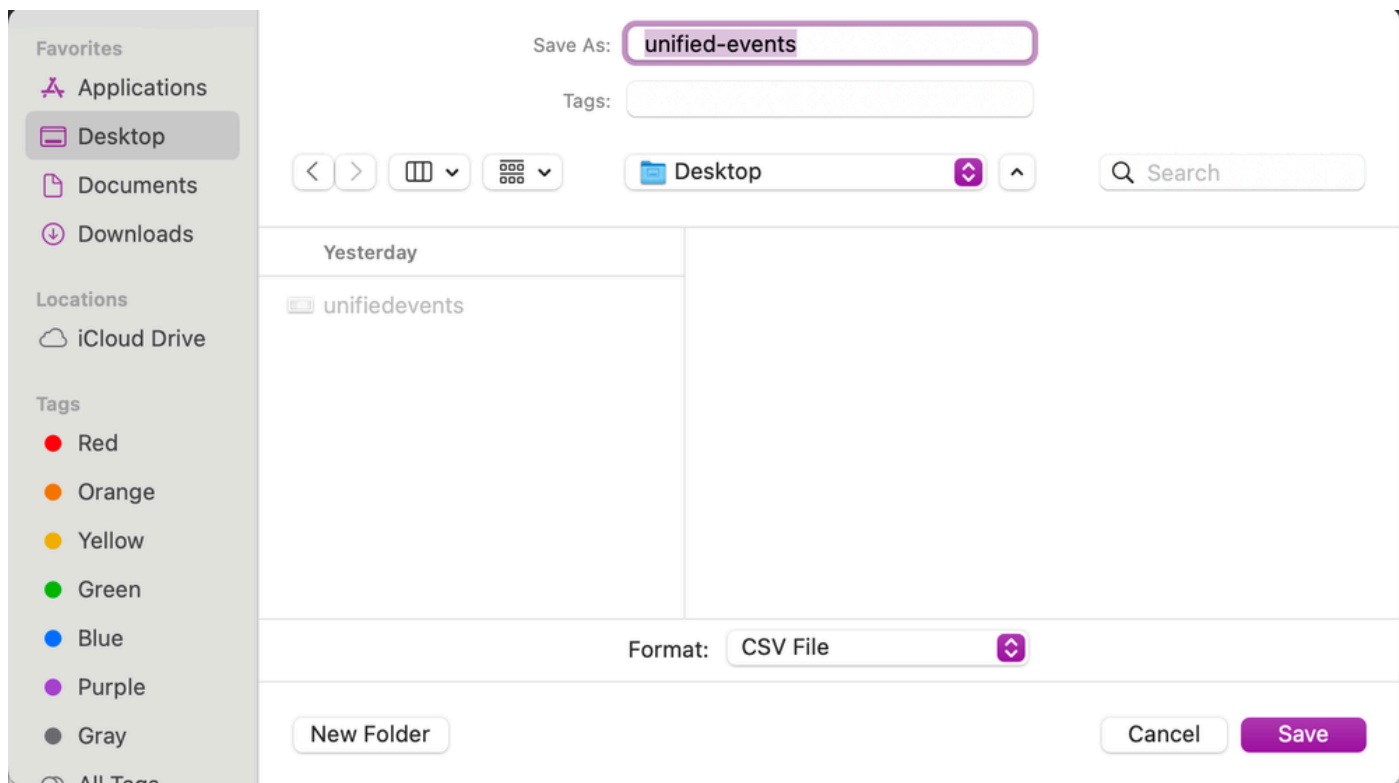
Caution: Quando a opção Ao vivo está habilitada, não é possível modificar a janela de tempo. Para modificar a janela de tempo, primeiro desative a opção Ao vivo clicando nela novamente.

Baixar Eventos como Valores separados por vírgula (CSV)

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

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

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



Etapa 3. Verificar o arquivo CSV.

Time	Event Type	Action	Destination Port / ICMP Code	Device	Source IP	Source Port / ICMP Type	Access Control Rule
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	37412 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	54766 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.166	54279 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	55185 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	46312 / udp	allow
2023-10-05 15:21:29	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	36785 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	57394 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	57395 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	38278 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	44865 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	58387 / udp	allow
2023-10-05 15:21:28	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	49873 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	51060 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	34103 / udp	allow
2023-10-05 15:21:27	Connection	Allow	53 (domain) / udp	GW	10.18.19.31	60020 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	43410 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	47406 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.105	43359 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	43336 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	42658 / udp	allow
2023-10-05 15:21:26	Connection	Allow	53 (domain) / udp	GW	10.18.19.156	52923 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.110	46485 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.201	52178 / udp	allow
2023-10-05 15:21:25	Connection	Allow	53 (domain) / udp	GW	10.18.19.111	55864 / udp	allow

Informações Relacionadas

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

Sobre esta tradução

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

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

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

Sobre esta tradução

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

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

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