

Monitoraggio degli eventi tramite il Visualizzatore eventi unificato sull'interfaccia utente di FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esplora](#)

[Esempio di pagina evento unificato](#)

[Eventi di revisione](#)

[Personalizza colonne](#)

[Salva set di colonne](#)

[Ricerca eventi](#)

[Salva ricerca](#)

[Finestra temporale](#)

[Vai in diretta](#)

[Scarica eventi come valori delimitati da virgole \(CSV\)](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto l'utilizzo del Visualizzatore eventi unificato su un'interfaccia utente grafica (GUI) in Firewall Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Accesso a FMC con privilegi di amministratore o analista della sicurezza
- FMC con versione uguale o superiore a v7.0

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

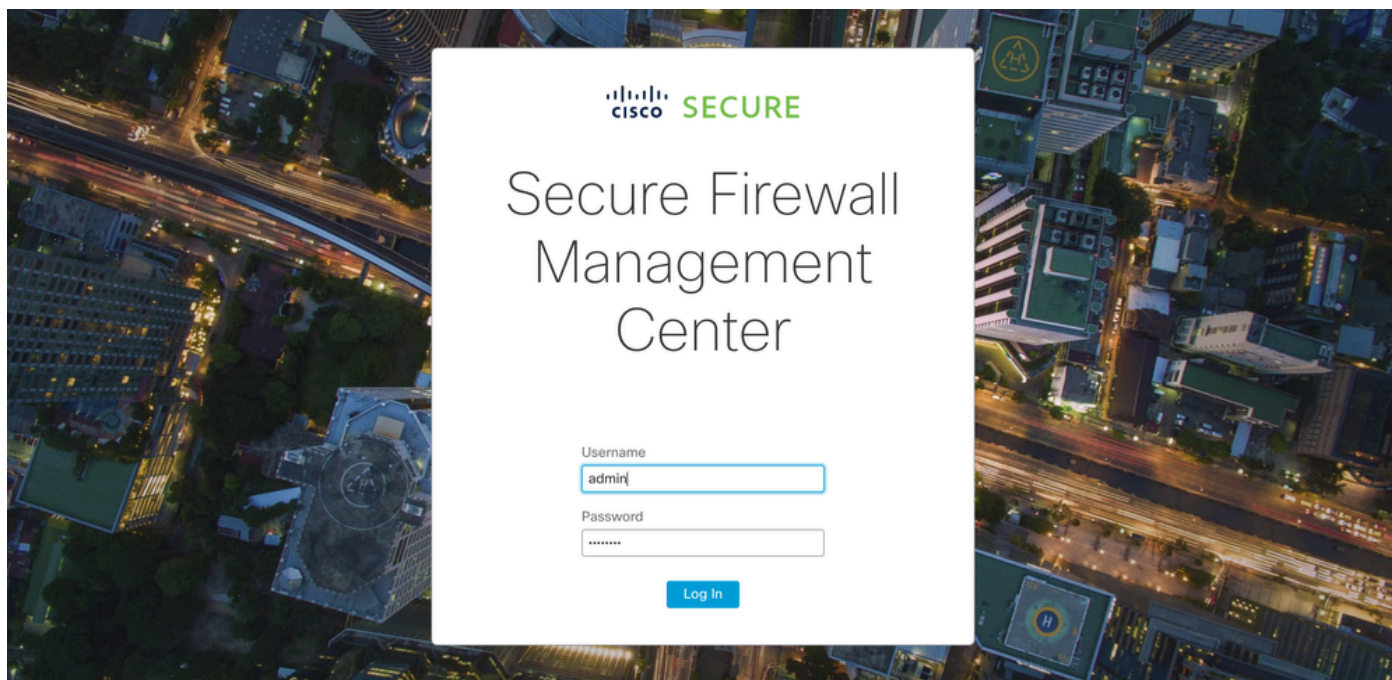
- Secure Firewall Management Center per VMware v7.2.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

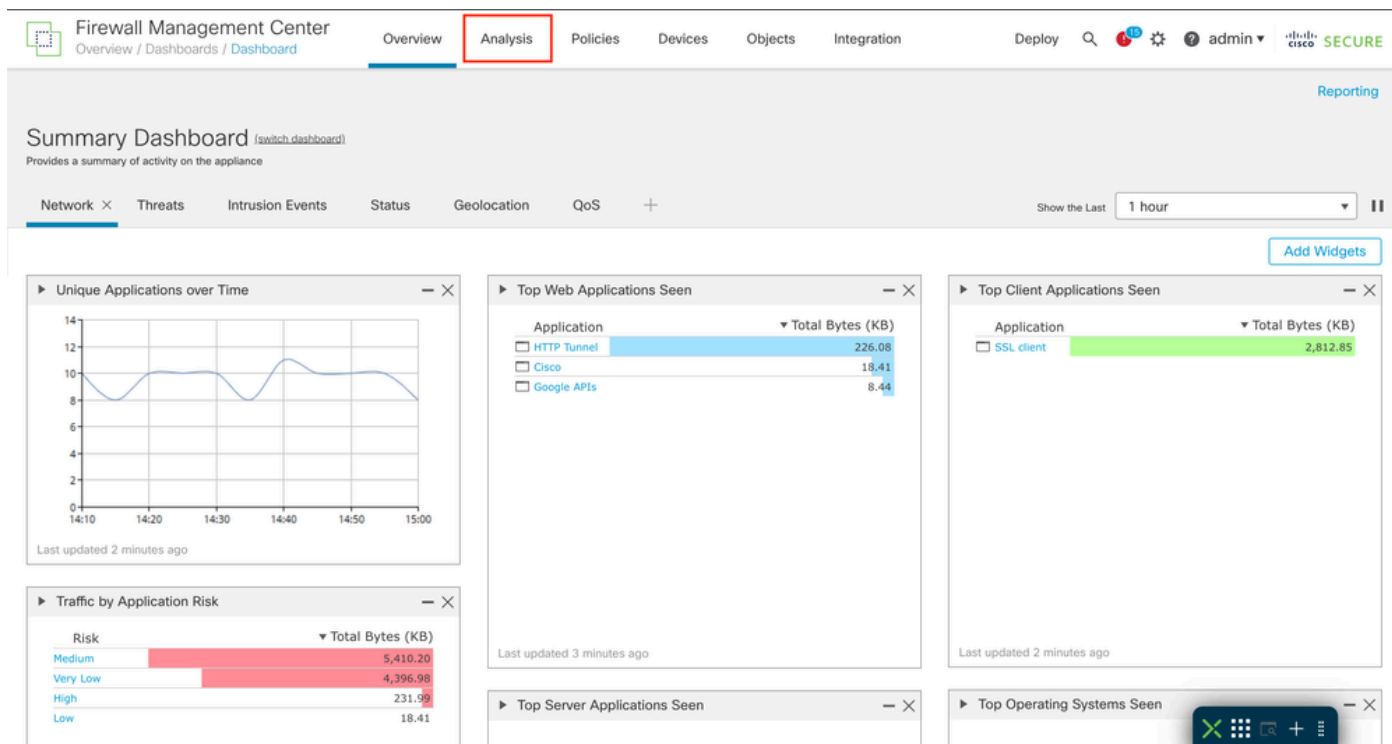
ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esplora

Passaggio 1. Accedere all'interfaccia utente di FMC.



Passaggio 2. Passare alla scheda Analisi.



Passaggio 3. Dal menu a discesa, fare clic su Unified Events (Eventi unificati).

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

Esempio di pagina evento unificato

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

Eventi di revisione

Passaggio 1. Fare clic sull'icona >.

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

Passaggio 2. Vengono visualizzate informazioni dettagliate sull'evento.

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

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

Personalizza colonne

Passaggio 1. Fare clic sull'icona .

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

Passaggio 2. Selezionare i campi evento che si desidera visualizzare nella tabella.

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 Ac
		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

Passaggio 3. (Facoltativo) Cercare il campo per semplificare la navigazione.

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

Passaggio 4. Fare clic su un campo evento per disabilitarlo o abilitarlo.

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

Passaggio 5. Fare clic su Apply (Applica).

Saved Column Sets

Select...

Q

Filter columns

Select none

Select default

☒

Event Type

☒

Action

☒

Destination Port / ICMP Code

☒

Source IP

☒

Device

Revert

6 selected

Apply

Passaggio 6. (Facoltativo) È possibile riposizionare le colonne trascinandole in una posizione diversa.

Firewall Management Center

Analysis / Unified Events

Overview

Analysis

Policies

Devices

Objects

Integration

Deploy

Q

admin

Go Live

Q

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

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	10.18.19.110	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

Salva set di colonne

Passaggio 1. Fare clic su Serie di colonne salvate.

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	

11 selected Apply

Passaggio 2. Fare clic su Crea serie di colonne dalla selezione corrente.

Firewall Management Center
Analysis / Unified Events

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

Q Select... Refresh

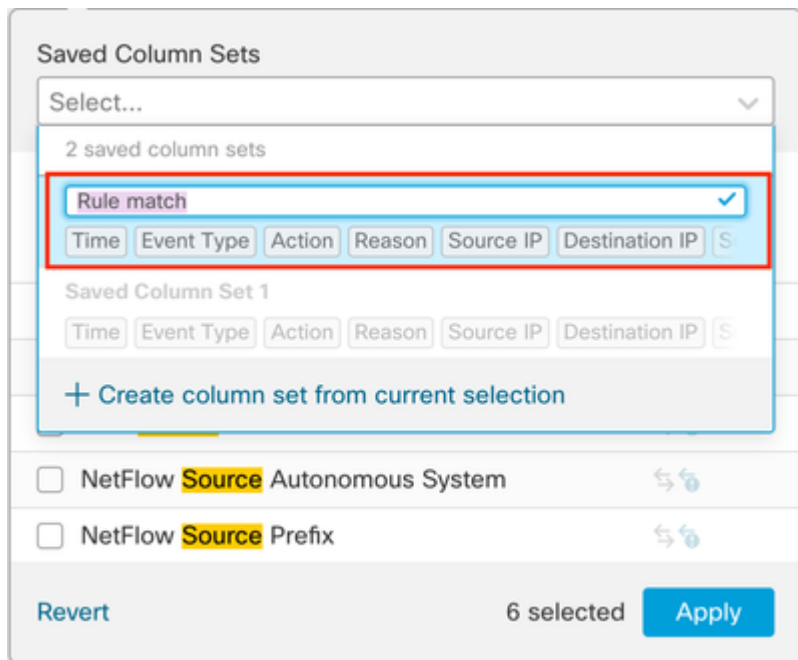
Showing 10,000 events (10,000) of tens of thousands

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

11 selected Apply

Passaggio 3. (Facoltativo) Modificare il nome della serie di colonne.



Passaggio 4. È possibile modificare un insieme esistente facendo clic sui puntini di sospensione (...).

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) / ud	GW	10.18.19.111	55046 / udp	allow
...	...	...	10.1.20.51	53 (domain) / ud	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) / ud	GW	10.18.19.105	57541 / udp	allow
...	...	...	10.1.20.51	53 (domain) / ud	GW	10.18.19.105	42318 / udp	allow
...	...	...	10.1.9.38	53 (domain) / ud	GW	10.18.19.110	38758 / udp	allow
...	...	...	10.1.8.101	53 (domain) / ud	GW	10.18.19.110	53922 / udp	allow
...	...	...	10.27.20.51	53 (domain) / ud	GW	10.18.19.105	52776 / udp	allow
...	...	...	208.67.220.220	53 (domain) / ud	GW	10.18.19.32	39366 / udp	allow
...	...	...	10.1.8.101	53 (domain) / ud	GW	10.18.19.111	47616 / udp	allow
...	...	...	208.67.220.220	53 (domain) / ud	GW	10.18.19.41	54037 / udp	allow
...	...	...	173.37.87.157	53 (domain) / ud	GW	10.18.19.230	60602 / udp	allow
...	...	...	173.37.87.157	53 (domain) / ud	GW	10.18.19.230	59309 / udp	allow
...	...	...	10.1.8.101	53 (domain) / ud	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

Ricerca eventi

Passaggio 1. Per iniziare la ricerca di eventi specifici, fare clic su Seleziona.

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

Passaggio 2. Selezionare il campo in cui si desidera applicare il 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 filters:

- 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

Passaggio 3. Scrivere i valori da utilizzare come filtro.

Q Source IP X Select...

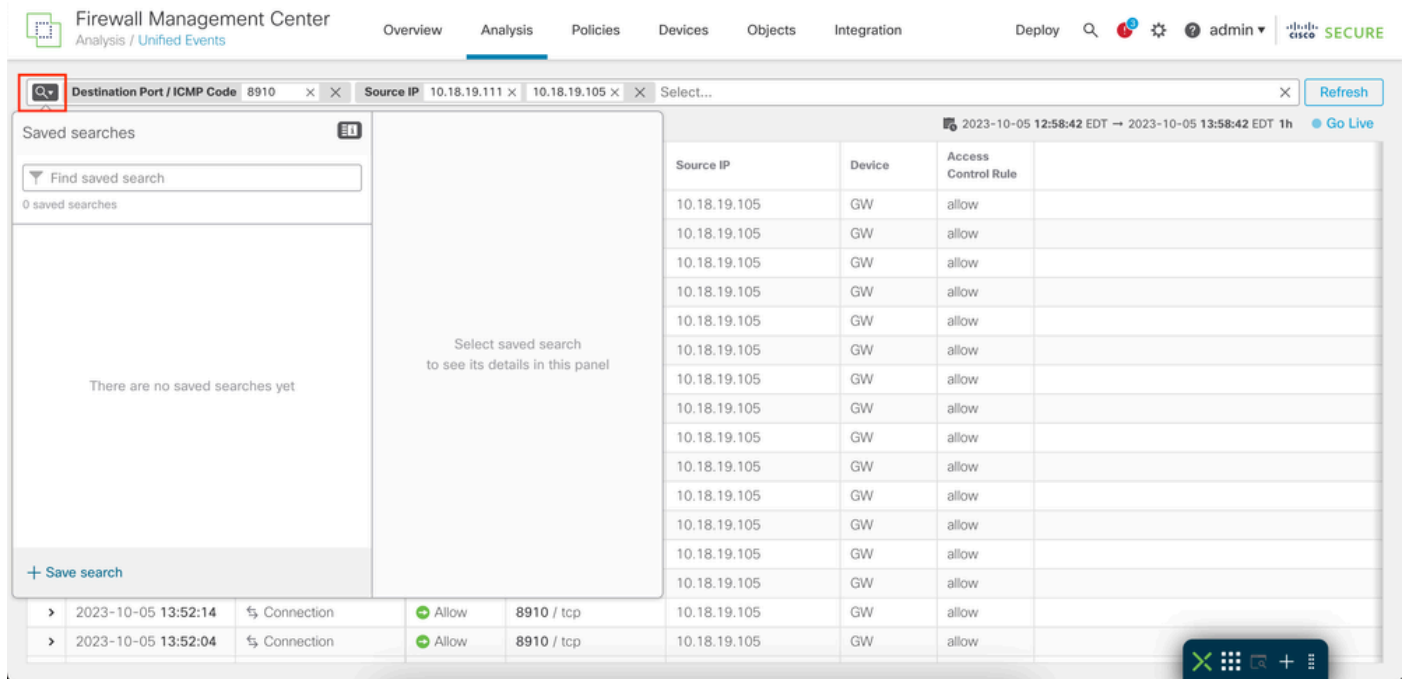
Passaggio 4. Fare clic su Apply (Applica) per configurare il filtro.

Suggerimento: È possibile utilizzare gli operatori (>,< , ! e così via) durante la scrittura dei valori.

Salva ricerca

È possibile salvare le ricerche in modo da poter riutilizzare i filtri creati.

Passaggio 1. Fare clic sull'icona della lente di ingrandimento.



Firewall Management Center
Analysis / Unified Events

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

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

2023-10-05 12:58:42 EDT → 2023-10-05 13:58:42 EDT 1h Go Live

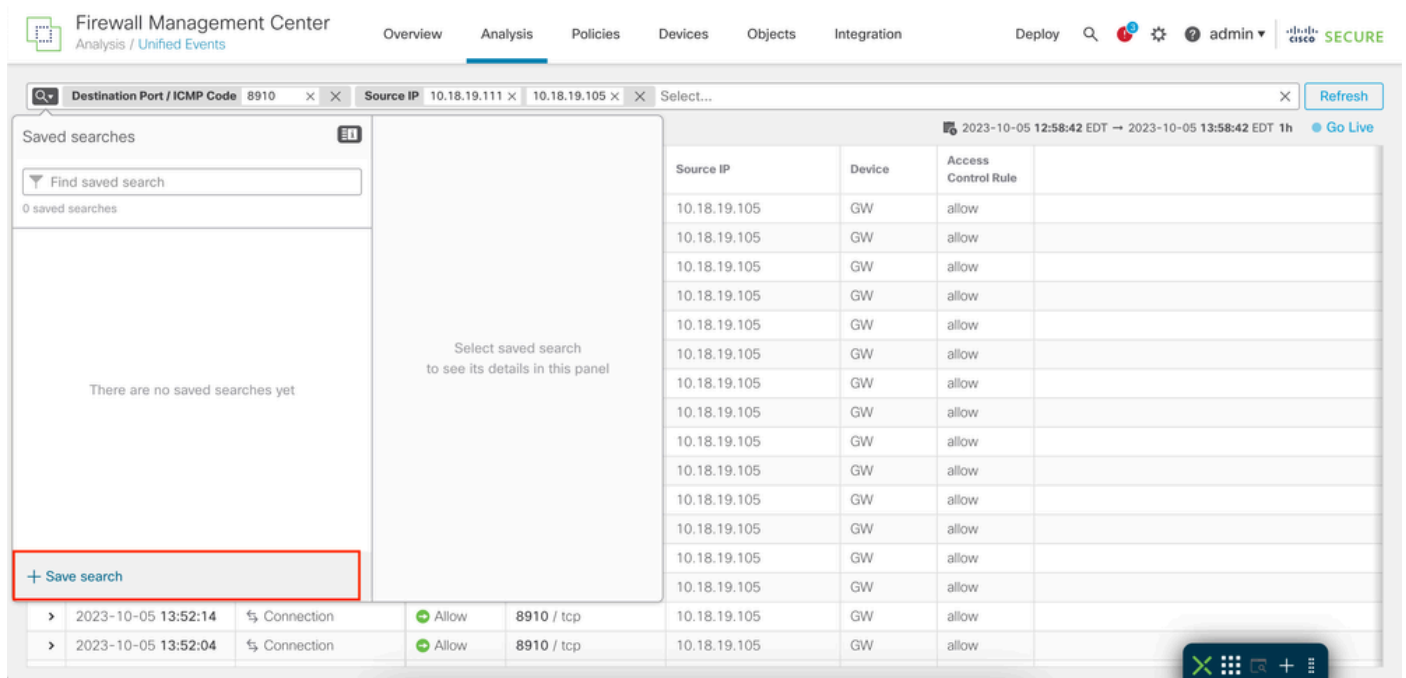
Source IP Device Access Control Rule

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

2023-10-05 13:52:14 Connection Allow 8910 / tcp

2023-10-05 13:52:04 Connection Allow 8910 / tcp

Passaggio 2. Fare clic su Salva ricerca.



Firewall Management Center
Analysis / Unified Events

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

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

2023-10-05 12:58:42 EDT → 2023-10-05 13:58:42 EDT 1h Go Live

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

2023-10-05 13:52:14 Connection Allow 8910 / tcp

2023-10-05 13:52:04 Connection Allow 8910 / tcp

+ Save search

Passaggio 3. (Facoltativo) Modificare il nome della ricerca.

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

Finestra temporale

È più semplice restringere gli eventi rilevanti in base a un tempo specifico modificando la finestra temporale.

Passaggio 1. Per modificare il frame della finestra degli eventi, fare clic su un intervallo di date.

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

Passaggio 2. Selezionare l'intervallo di tempo nella finestra popup.

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 16:11:29	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

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

Vai in diretta

È possibile attivare la funzione Go Live per visualizzare gli eventi in tempo reale. Gli eventi vengono visualizzati nel momento in cui vengono generati.

Per abilitarla, fai clic su 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

Una volta attivata, viene visualizzata la parola Live.

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



Attenzione: Quando Live è abilitato, non è possibile modificare la finestra temporale. Per modificare la finestra temporale, disattivate prima l'opzione Dal vivo facendovi nuovamente clic sopra.

Scarica eventi come Valori delimitati da virgole (CSV)

Passaggio 1. Fare clic sull'icona di download per generare un file contenente gli eventi attualmente visualizzati nella pagina.

Q

Destination Port / ICMP Code

8910

×

×

Source IP

10.18.19.111

×

10.18.19.105

×

Select...

×

Refresh

Showing all 144 events (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

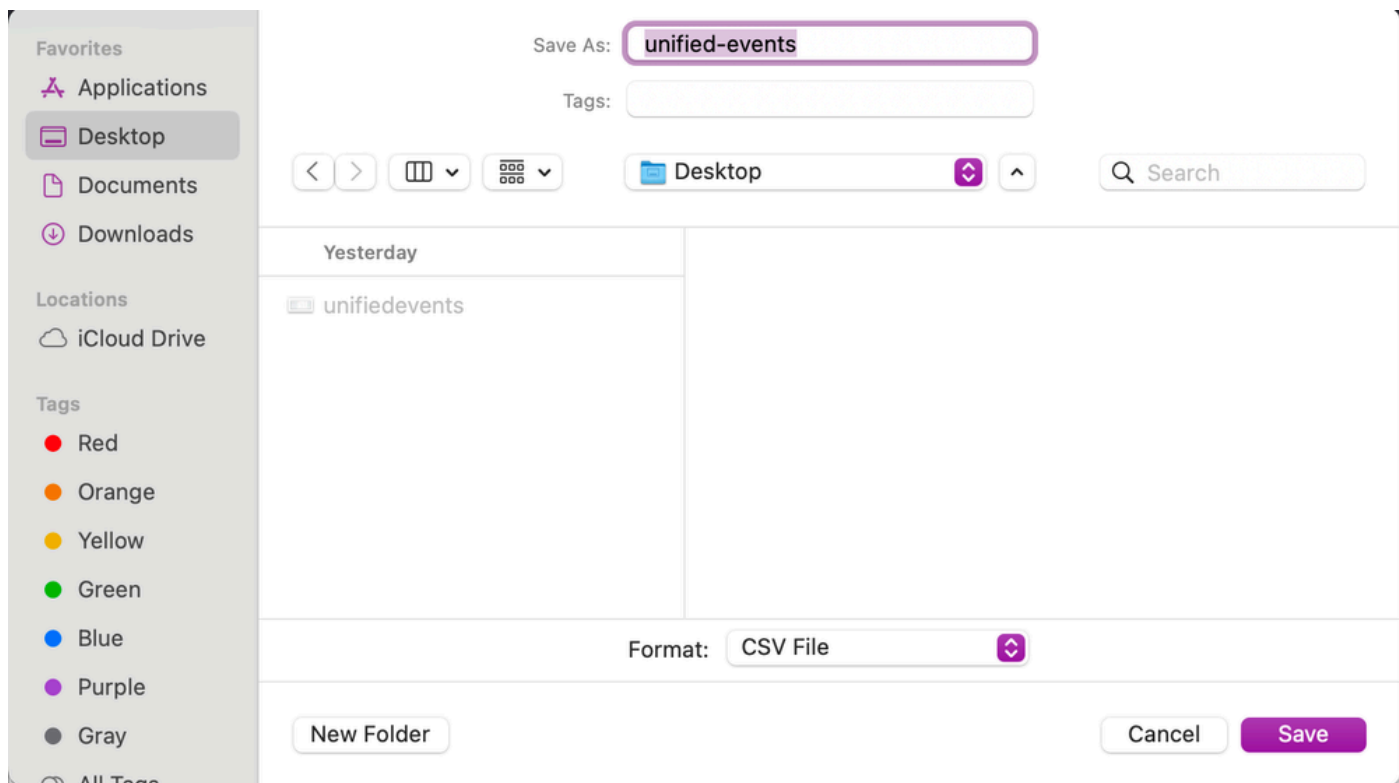
⌵

⌵

+

⌵

2. Selezionare la cartella di download, il nome e fare clic su Save (Salva).



Passaggio 3. Verificare il file 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

Informazioni correlate

- [Utilizzo del Visualizzatore eventi unificato](#)
- [Cisco Secure Firewall - Visualizzatore eventi unificato: Suggerimenti](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).