

# Utilice el marco MITER para ver y actuar ante las amenazas potenciales en FMC seguro

## Contenido

---

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Ventajas del marco MITER](#)

[Ver el marco de MITER en su política de intrusiones](#)

[Ver eventos de intrusión](#)

---

## Introducción

Este documento describe cómo utilizar la estructura MITER para ver y actuar sobre las amenazas potenciales en un Firepower Management Center (FMC) seguro.

## Antecedentes

El marco MITER ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) es una amplia base de conocimientos y metodología que proporciona información sobre las tácticas, técnicas y procedimientos (TTP) distribuidos por los agentes de amenazas con el objetivo de dañar los sistemas. ATT&CK se compila en matrices que representan sistemas operativos o una plataforma en particular. Cada etapa de un ataque, conocida como "táctica", se asigna a los métodos específicos utilizados para lograr esas etapas, conocidas como "técnicas".

Cada técnica del marco de ATT&CK va acompañada de información sobre la técnica, procedimientos asociados, defensas probables y detecciones, y ejemplos reales. El marco de MITER ATT&CK también incorpora grupos para hacer referencia a grupos de amenazas, grupos de actividad o agentes de amenazas en función del conjunto de tácticas y técnicas que emplean. Mediante el uso de Grupos, el marco de trabajo ayuda a categorizar y documentar comportamientos.

Para obtener más información sobre MITER, consulte <https://attack.mitre.org>.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de Snort
- FMC seguro
- Firepower Threat Defense (FTD) seguro

## Componentes Utilizados

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

- Este documento se aplica a todas las plataformas Firepower
- FTD seguro con software versión 7.3.0
- Secure Firepower Management Center Virtual (FMC) con software versión 7.3.0

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.

## Ventajas del marco MITER

- Las Tácticas, Técnicas y Procedimientos (TTP) MITER se agregan a los eventos de intrusión que permiten a los administradores actuar sobre el tráfico basado en el marco MITER ATT&CK (Técnicas de Tácticas Adversarias y Conocimiento Común). Esto permite a los administradores ver y gestionar el tráfico con mayor granularidad, y pueden agrupar reglas por tipo de vulnerabilidad, sistema de destino o categoría de amenaza.
- Puede organizar las reglas de intrusión según el marco de MITER ATT&CK. Esto le permite personalizar las políticas en función de tácticas y técnicas específicas de los atacantes.

## Ver el marco de MITER en su política de intrusiones

La estructura MITER le permite navegar a través de las reglas de intrusión. MITRE es solo otra categoría de grupos de reglas y forma parte de los grupos de reglas Talos. Se admite la exploración de reglas para varios niveles de grupos de reglas, lo que proporciona más flexibilidad y una agrupación lógica de las reglas.

1. Seleccione [Políticas > Intrusion](#).
2. Asegúrese de seleccionar la [Intrusion Políticas](#) pestaña.
3. Haga clic [Snort 3 Version](#) junto a la política de intrusiones que desea ver o editar. Cierre la guía de ayuda de Snort que aparece.
4. Haga clic en la [Group Overrides](#) capa.

La [Group Overrides](#) capa muestra todas las categorías de grupos de reglas en una estructura jerárquica. Puede pasar al último grupo de reglas de hoja de cada grupo de reglas.

< Policies / Intrusion / MITRE\_ATTACK

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description MITRE\_ATTACK

Base Policy → **Group Overrides** → Recommendations **Not in use** → Rule Overrides | Summary

Group Overrides ?

2 items Overrid... x v +

MITRE (1 group) 1

ATT&CK Framework (1 group) 1

Search through all Rule Groups

MITRE 1 Groups

Group Name Security Level

ATT&CK Framework mixed

MITRE ATT&CK is a globally-accessible knowledge base of adversary tactics and techn...

6. En Group Overrides, asegúrese de que **All** se elige en la lista desplegable, de modo que todos los grupos de reglas de la directiva de intrusiones estén visibles en el panel izquierdo.

7. Haga clic **MITRE** en el panel izquierdo.



Nota: En este ejemplo, se selecciona MITRE, pero, en función de sus requisitos específicos, puede elegir el grupo de reglas Categorías de regla o cualquier otro grupo de reglas y los grupos de reglas subsiguientes bajo él. Todos los grupos de reglas utilizan la estructura MITER.

Base Policy: Balanced Security and Connectivity Mode: Prevention

Description test\_policy

Base Policy → **Group Overrides** → Recommendations **Not in use** → Rule Overrides | Summary

Group Overrides ?

101 items **All** x v +

MITRE (1 group) 1

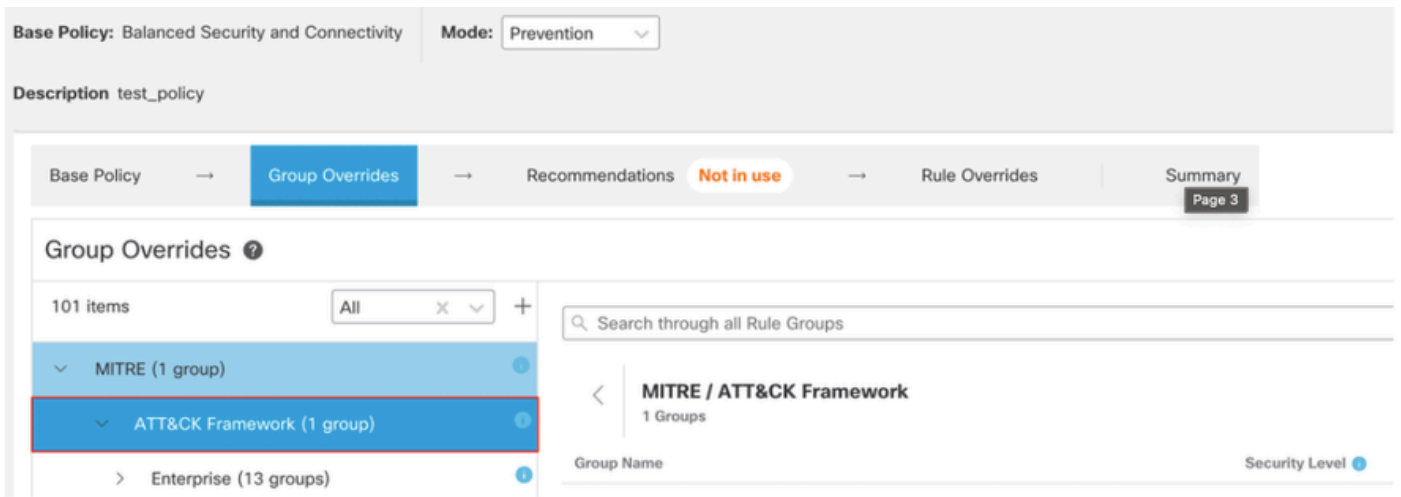
Rule Categories (9 groups) 1

Search through all Rule Groups

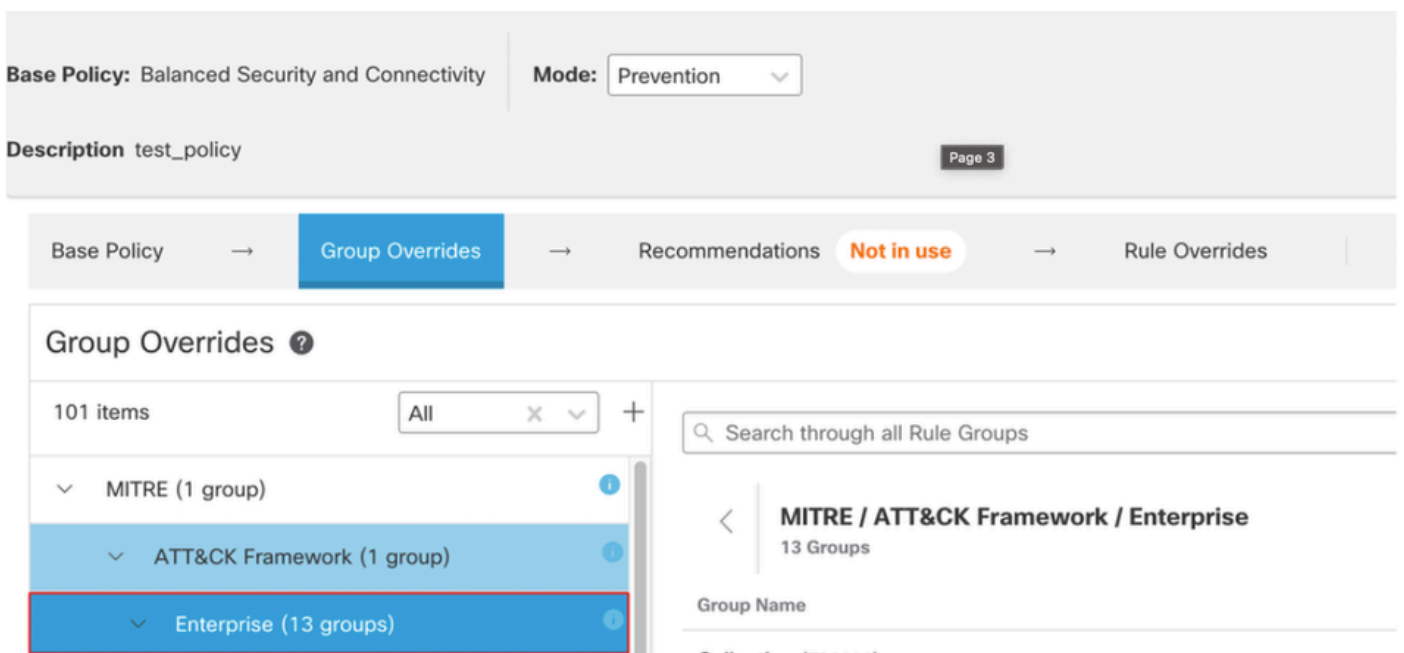
Rule Groups

To optimize intrusion policy configuration, you can configure the various rule group categories enable or disable groups and increase or decrease security levels, thus enriching intrusion eve

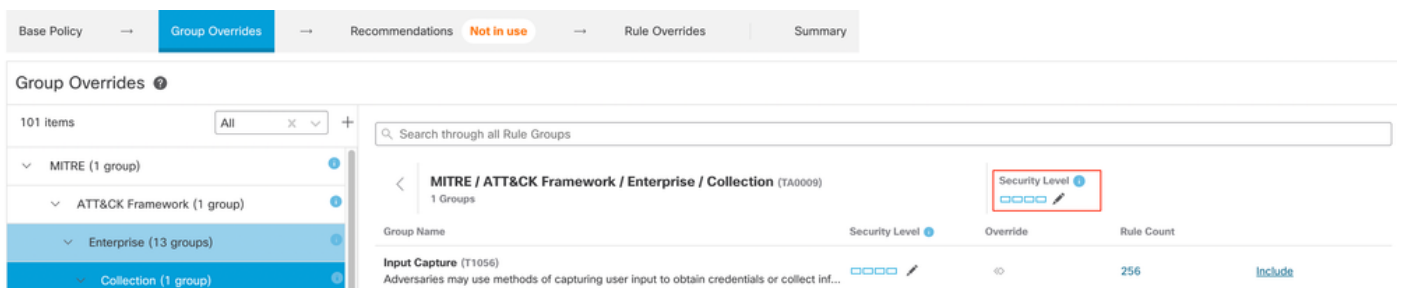
8. En MITRE, haga clic en **ATT&CK Marco conceptual** para expandirlo.



9. En ATT&CK Framework, haga clic en Empresa para expandirla.



10. Haga clic Edit () junto al nivel de seguridad del grupo de reglas para realizar cambios masivos en el nivel de seguridad de todos los grupos de reglas asociados en el Enterprise categoría de grupo de reglas.



Editar grupo de reglas de seguridad

11. Por ejemplo, seleccione el nivel de seguridad 3 en la Edit Security Level ventana y haga clic en Save.

# Edit Security Level



Higher security with more detections for administrators who are willing to tolerate some network latency and low level of false positives, in an effort to catch more attacks.

↶ Revert to default

Cancel

Save

Nivel de seguridad

12. En Enterprise, haga clic **Initial Access** para expandirlo.

13. En **Initial Access**, haga clic en **Exploit Public-Facing Application**, que es el último grupo de hojas.

Group Name	Security Level	Override	Rule Count	
<b>Drive-by Compromise</b> (T1189) Adversaries may gain access to a system through a user visiting a website over the nor...	□□□□	⊖	8783	<a href="#">Include</a>
<b>Exploit Public-Facing Application</b> (T1190) Adversaries may attempt to take advantage of a weakness in an Internet-facing comput...	□□□□	⊖	11976	<a href="#">Include</a>
<b>External Remote Services</b> (T1133) Adversaries may leverage external-facing remote services to initially access and/or per...	□□□□	⊖	443	<a href="#">Include</a>
<b>Phishing</b> (T1566) Adversaries may send phishing messages to gain access to victim systems. All forms o...	□□□□	⊖	304	<a href="#">Include</a>
<b>Valid Accounts</b> (T1078) Adversaries may obtain and abuse credentials of existing accounts as a means of gaini...	□□□□			

Grupo de acceso inicial

14. Haga clic en el botón **View Rules in Rule Overrides** para ver las distintas reglas, detalles de reglas, acciones de regla, etc. de las distintas reglas.

This group does not contain any children.

0 Groups / Group contains 8783 rules

[View Rules in Rule Overrides](#)

Reglas de anulaciones de reglas

15. Haga clic en el botón **Recommendations** y, a continuación, haga clic **Start** para empezar a utilizar las reglas recomendadas por Cisco. Puede utilizar las recomendaciones de reglas de intrusión para identificar las vulnerabilidades asociadas con los activos de host detectados en la red. Para más información.

The screenshot shows a navigation bar with the following items: 'Base Policy', 'Group Overrides', 'Recommendations' (highlighted with a red box and a 'Not in use' status), 'Rule Overrides', and 'Summary'. Below the navigation bar, the main content area is titled 'Cisco Recommended Rules' and contains a section titled 'Start using recommendations' with the text: 'You can use Cisco Recommended Rules to target vulnerabilities associated with host assets detected in the network'. A blue 'Start' button is located at the bottom of this section.

Recomendaciones

# Cisco Recommended Rules



Security Level (Click to select)

Accept Recommendation to Disable Rules

**Higher Efficiency**– Keeps existing rules that match potential vulnerabilities on discovered hosts and disables rules for vulnerabilities not found on the network.

Protected Networks

Add +

Cancel

Generate

Generate and Apply

16. Haga clic en el botón `Summary` para obtener una vista integral de los cambios actuales de la política. Puede ver la distribución de reglas de la directiva, las invalidaciones de grupos, las invalidaciones de reglas, etc.

Resumen de políticas

## Ver eventos de intrusión

Puede ver las técnicas y grupos de reglas de MITER ATT&CK en los eventos de intrusión en el Visor de eventos clásico y el Visor de eventos unificado. Talos proporciona asignaciones de

reglas de Snort (GID:SID) a técnicas y grupos de reglas MITER AT&CK. Estas asignaciones se instalan como parte del paquete de seguridad ligero (LSP).

Antes de comenzar, deben implementarse las directivas de control de acceso e intrusiones para detectar y registrar los eventos desencadenados por las reglas de Snort.

1. Haga clic en **Analysis > Intrusions > Events**.

2. Haga clic en el botón **Table View of Events** como se muestra en la imagen.

Events By Priority and Classification (switch workflow) 2022-07-19 09:05:58 - 2022-07-19 11:17:05

No Search Constraints (Edit Search)

Drilldown of Event, Priority, and Classification **Table View of Events** Packets

Jump to...

	Time	Priority	Impact	Inline Result	Reason	Source IP	Source Country	Destination IP
▼	2022-07-19 11:17:10	high	2	Would block	Interface in Passive or Tap mode	192.168.0.227		146.112.255.69
▼	2022-07-19 11:17:06	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.4.106
▼	2022-07-19 11:17:06	medium	3	Would block	Interface in Passive or Tap mode	54.68.177.240	USA	192.168.7.214
▼	2022-07-19 11:17:05	medium	2	Would block	Interface in Passive or Tap mode	192.168.3.254		192.168.7.241

Events

3. En el **MITRE ATT&CK** encabezado de columna, puede ver las técnicas para un evento de intrusión.

Access Control Policy	Access Control Rule	Network Analysis Policy	MITRE ATT&CK	Rule Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy	1 Technique	1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group
AC_with_security_intelligence_file_file	TestRuleFile	Simple NAP Policy		1 Group

Encabezado de columna inglete

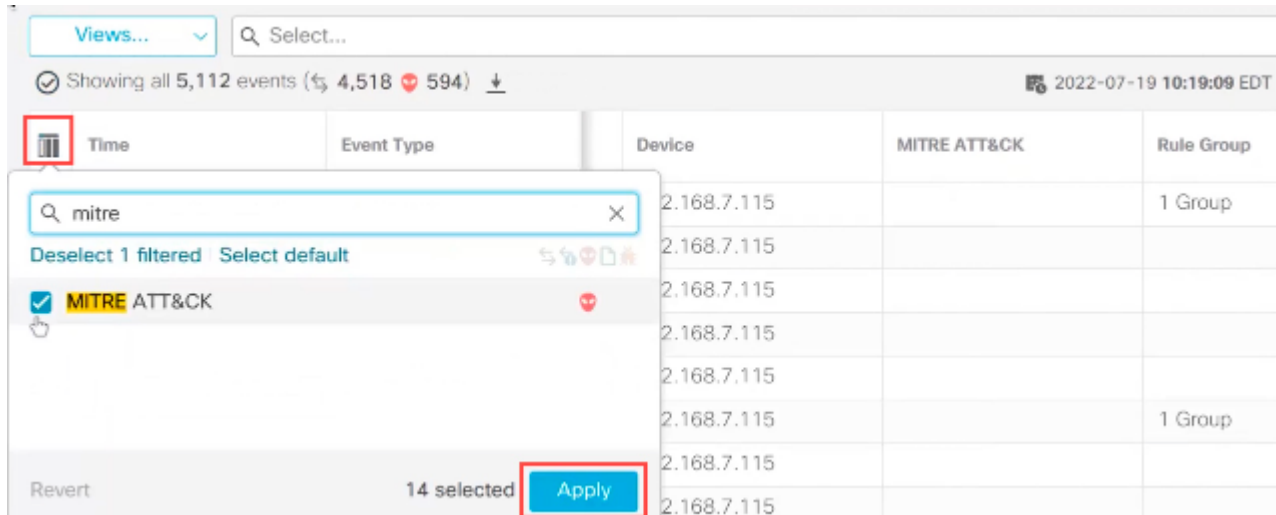
4. Haga clic en **1 Technique** para ver las Técnicas ATT&CK de MITER, como se muestra en esta figura. En este ejemplo, **Exploit Public-Facing Application** es la técnica.

MITRE ATT&CK Techniques

- Enterprise
  - Initial Access
    - Exploit Public-Facing Application

Close

5. Haga clic en **Close**.
6. Haga clic en **Analysis > Unified Events**.
7. Puede hacer clic en el icono selector de columna para activar las columnas **MITRE ATT&CK** **Rule Group**.



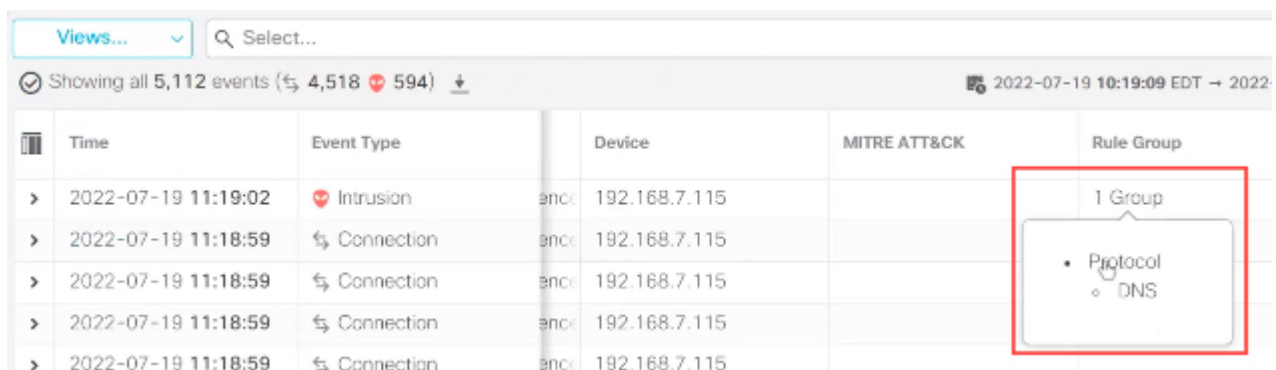
Habilitar el ataque de inglete

8. Como se muestra en el ejemplo, el evento de intrusión fue activado por un evento asignado a un grupo de reglas. Haga clic en **1 Group** en la **Rule Group** columna.



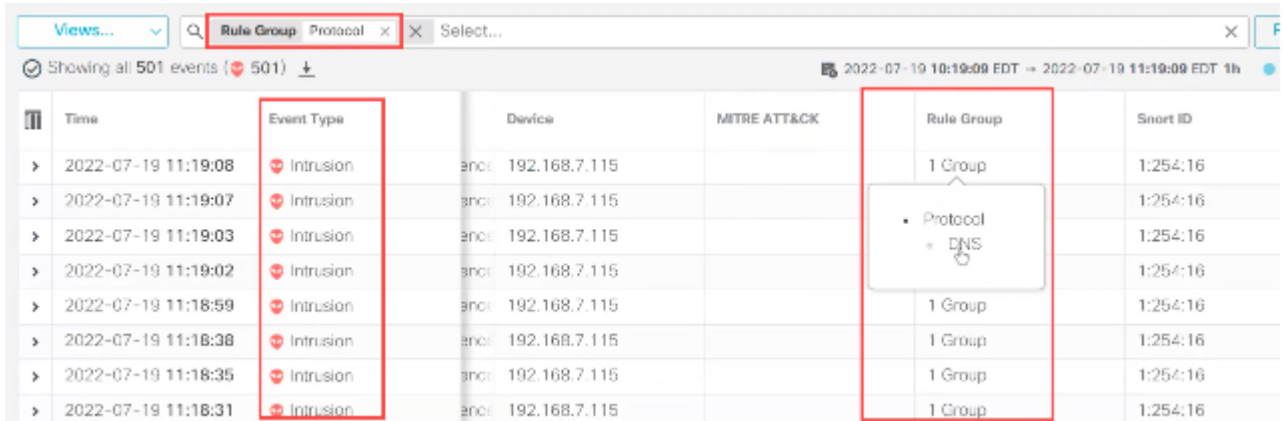
Grupo de reglas

9. Por ejemplo, puede ver **Protocolo**, que es el grupo de reglas principal, y el grupo de reglas **DNS** que se encuentra debajo.



Ver protocolo

10. Puede hacer clic **Protocolo** para buscar todos los eventos de intrusión que tienen al menos un grupo de reglas, es decir, **Protocol > DNS** . Se muestran los resultados de la búsqueda, como se muestra en el ejemplo siguiente.



The screenshot shows a security event viewer interface with a search filter 'Protocol > DNS' applied. The table displays several intrusion events. A dropdown menu is open over the 'Rule Group' column, showing 'Protocol > DNS' as the selected filter.

Time	Event Type	Device	MITRE ATT&CK	Rule Group	Smart ID
2022-07-19 11:19:08	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:07	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:03	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:19:02	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:59	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:38	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:35	Intrusion	enc: 192.168.7.115		1 Group	1:254:16
2022-07-19 11:18:31	Intrusion	enc: 192.168.7.115		1 Group	1:254:16

Protocolo de grupo de reglas

## 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).