# Configuración de la restricción de acceso IP en ISE

## Contenido


Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Comportamiento en ISE 3.1 y versiones inferiores

- Configurar

Comportamiento en ISE 3.2

- Configurar

Comportamiento en ISE 3.2 P4 y versiones posteriores

- Configurar

Recuperar GUI/CLI de ISE

Resolución de problemas

- Comprobar las reglas del firewall ISE
- Comprobar registros de depuración

Información Relacionada


## Introducción

Este documento describe las opciones disponibles para configurar la restricción de acceso IP en ISE 3.1, 3.2 y 3.3.

## Prerequisites

### Requirements

Cisco recomienda que conozca Cisco Identity Service Engine (ISE).

### Componentes Utilizados

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

- Cisco ISE versión 3.1
- Cisco ISE versión 3.2
- Cisco ISE versión 3.3

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.

# Antecedentes

La función de restricción de acceso a IP permite a los administradores controlar qué rangos o direcciones IP pueden acceder al portal de administración y a los servicios de ISE.

Esta función se aplica a varias interfaces y servicios de ISE, entre los que se incluyen:

- Acceso al portal de administración y CLI
- Acceso a API ERS
- Acceso al portal de invitados y patrocinadores
- Acceso al portal Mis dispositivos

Cuando está habilitado, ISE solo permite conexiones de los rangos o direcciones IP especificados. Se bloquea cualquier intento de acceder a las interfaces de administración de ISE desde IP no especificadas.

En caso de bloqueo accidental, ISE proporciona una opción de inicio de 'modo seguro' que puede eludir las restricciones de acceso IP. Esto permite a los administradores recuperar el acceso y corregir cualquier configuración incorrecta.

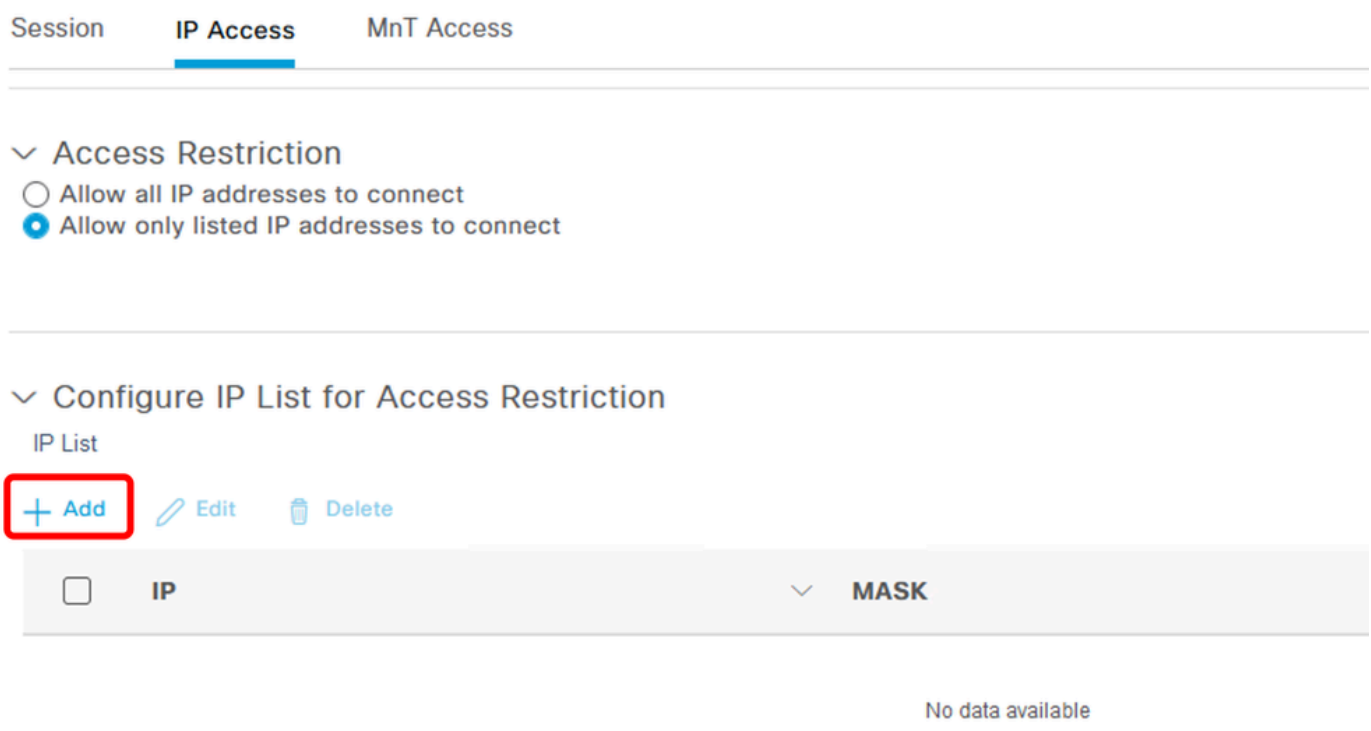
# Comportamiento en ISE 3.1 y versiones inferiores

Vaya a .Administration > Admin Access > Settings > Access Tiene estas opciones:

- Sesión
- Acceso IP
- Acceso MnT

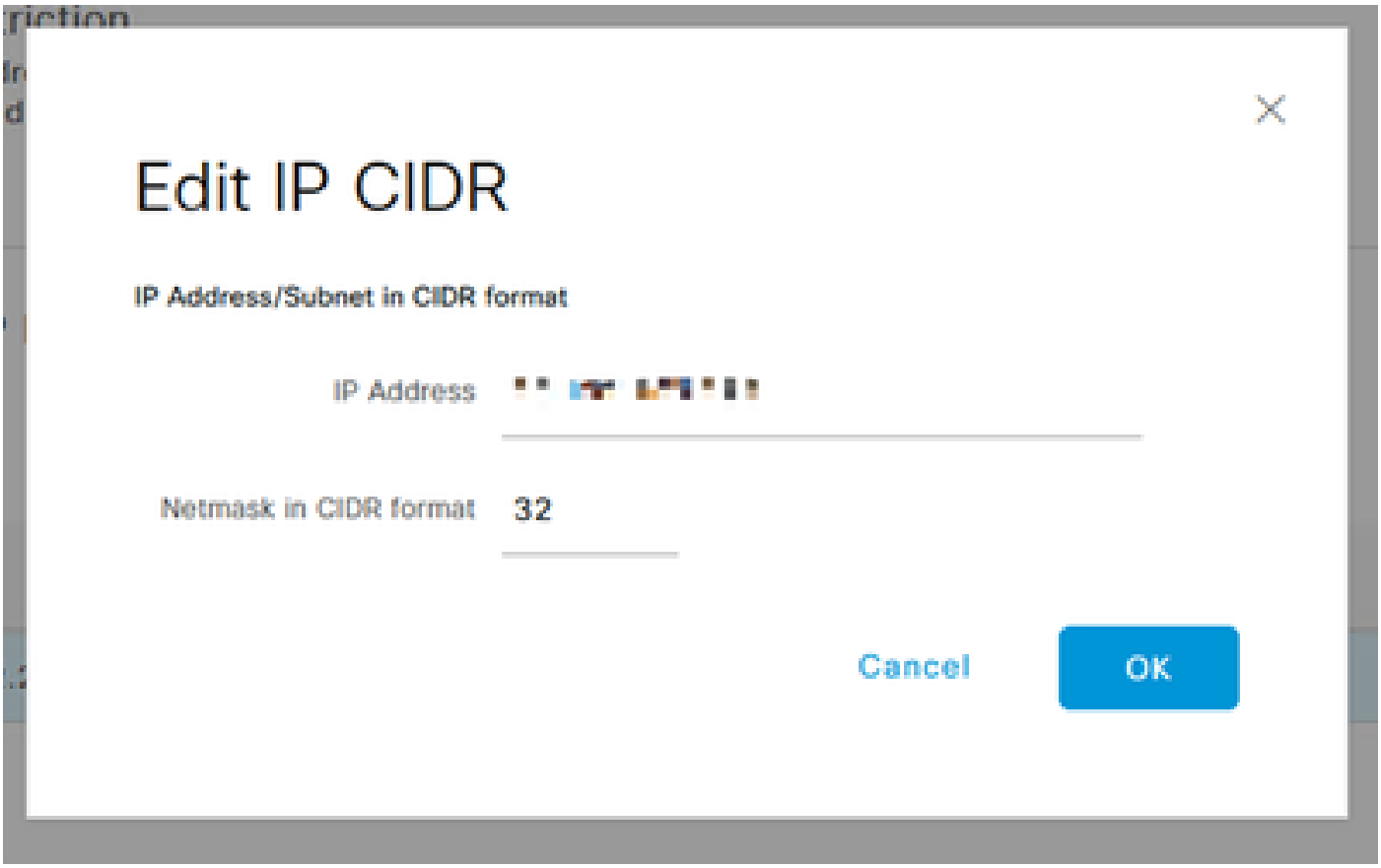
## Configurar

- Seleccione **Allow only listed IP addresses to connect** .
- Haga clic enAdd.

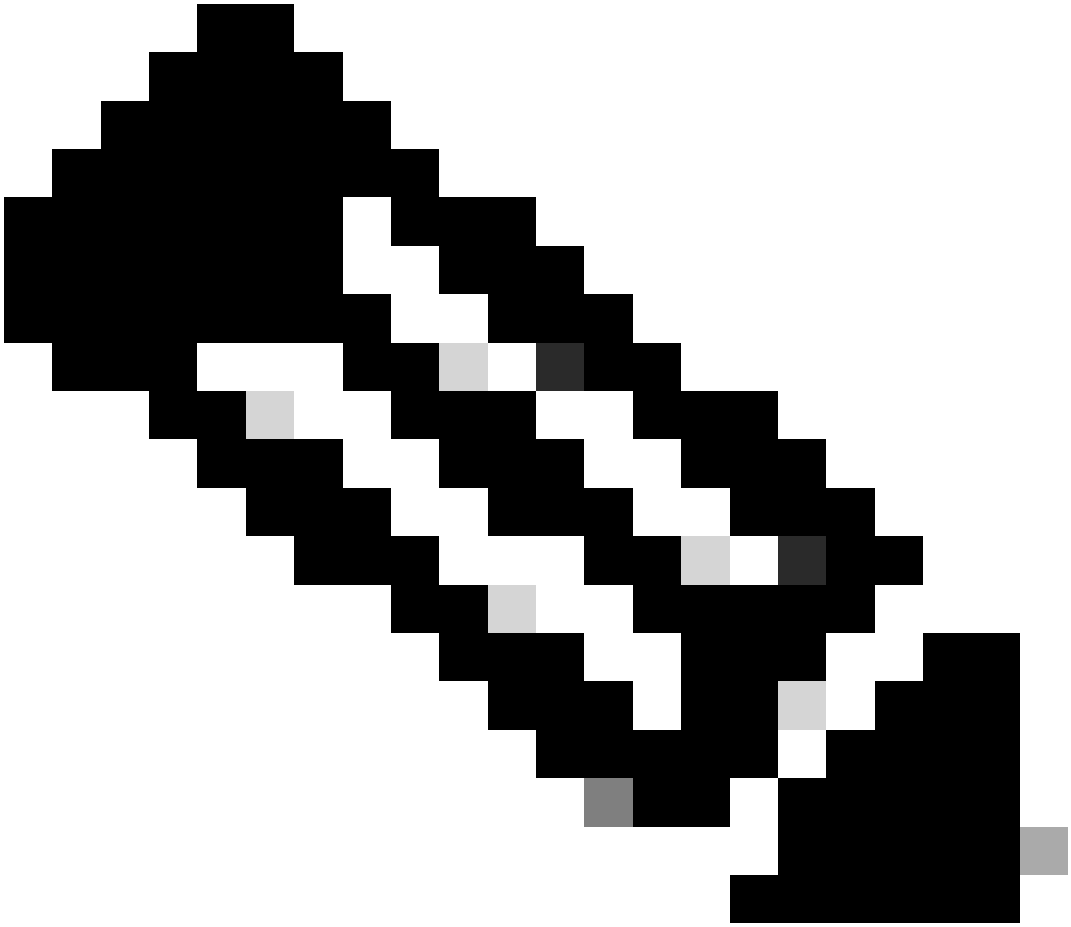



Configuración de acceso IP

- En ISE 3.1 no tiene la opción de seleccionar entre Admin y los User servicios, por lo que la activación de la restricción de acceso IP bloquea las conexiones a:
  - GUI
  - CLI
  - SNMP (Protocolo de administración de red simple)
  - SSH
- Se abre un cuadro de diálogo en el que se introducen las direcciones IP, IPv4 o IPv6, en formato CIDR.
- Una vez configurada la IP, establezca la máscara en formato CIDR.




Editar CIDR IP

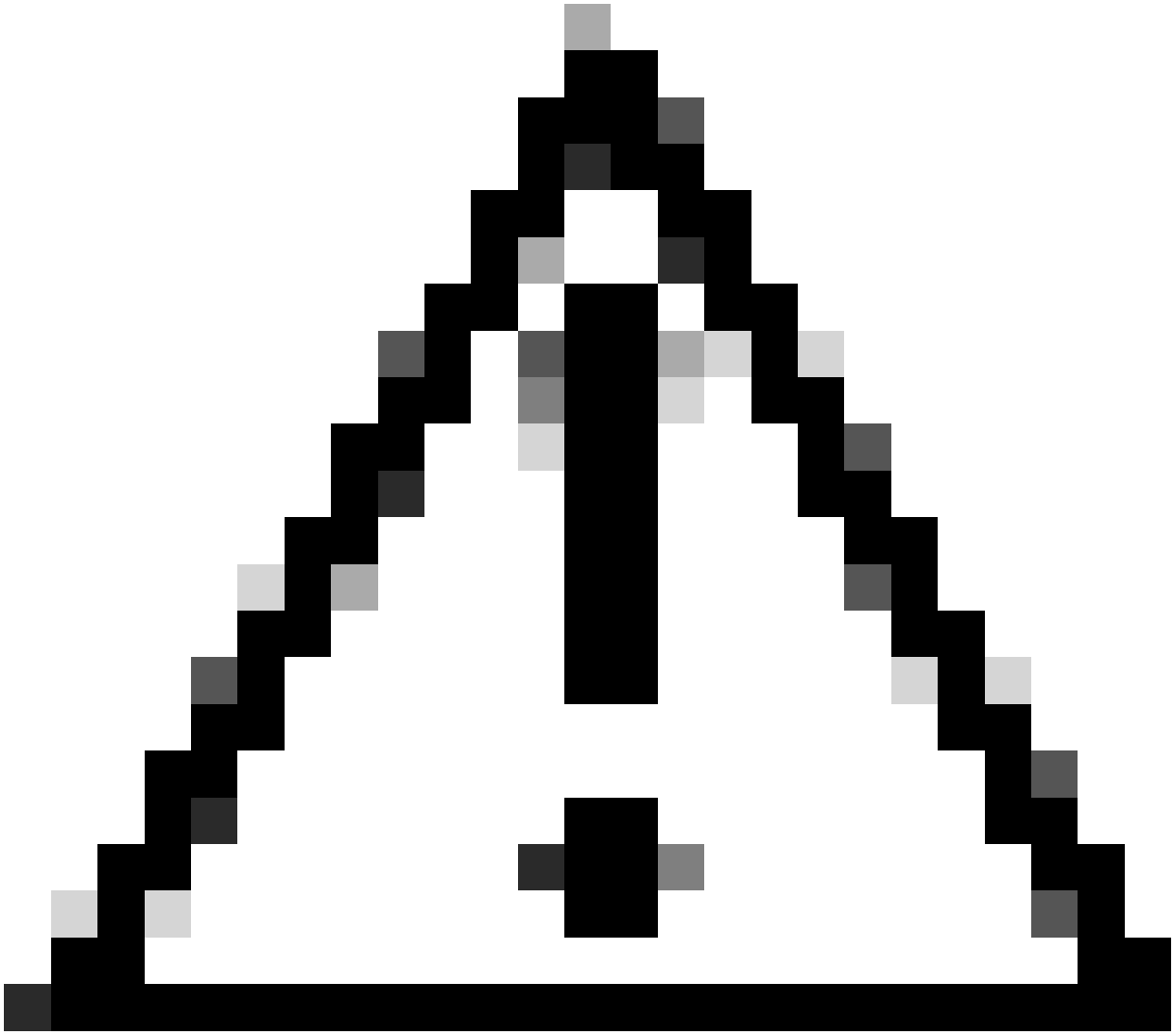


Nota: El formato de IP Classless Inter-Domain Routing (CIDR) es un método para representar direcciones IP y su prefijo de routing asociado.

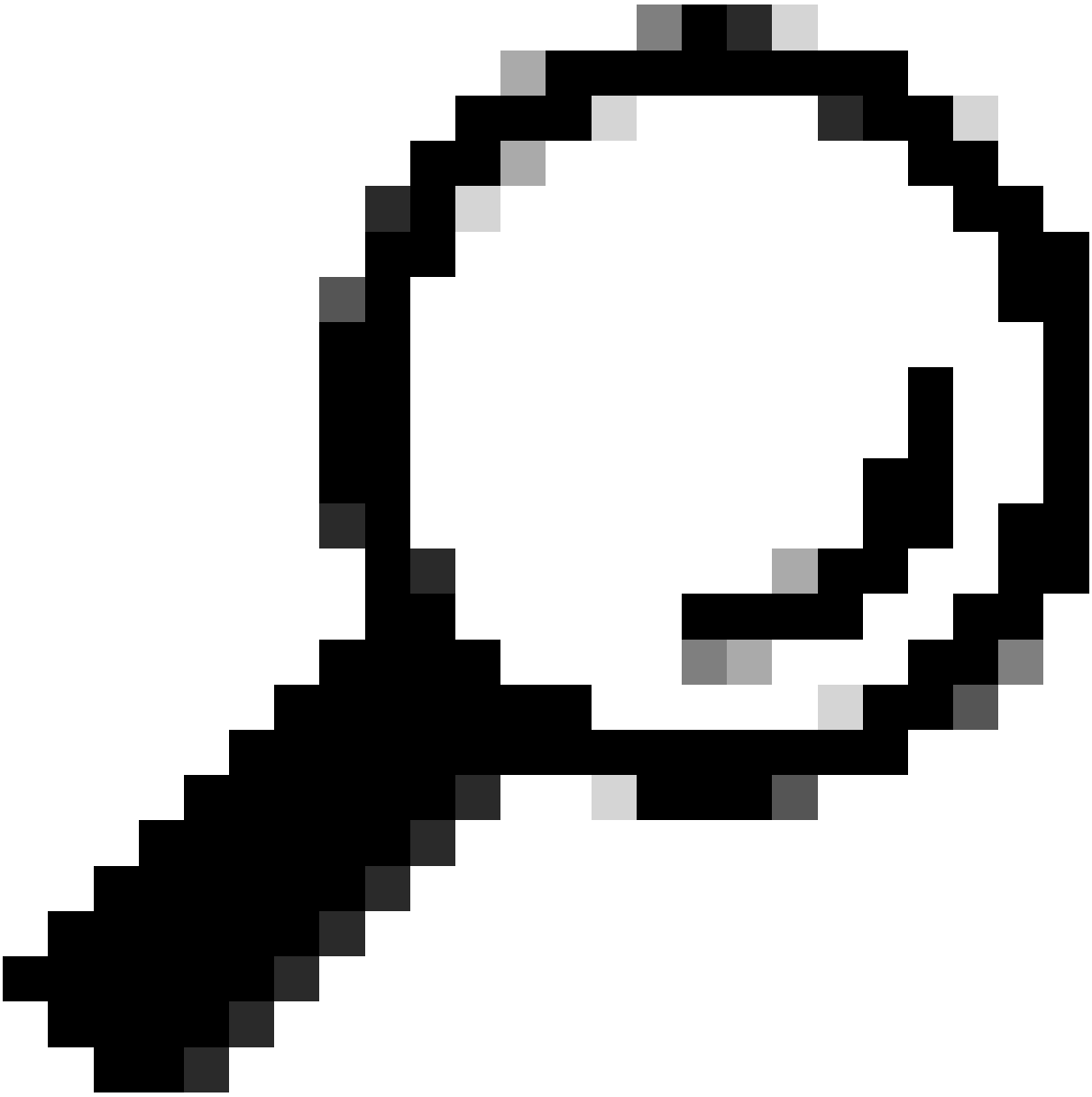
Ejemplo:

IP: 10.8.16.32

Máscara: /32



Precaución: Se debe tener cuidado al configurar las restricciones IP para evitar bloquear accidentalmente el acceso de administrador legítimo. Cisco recomienda probar exhaustivamente cualquier configuración de restricción de IP antes de implementarla por completo.



Consejo: Para direcciones IPv4:

- Utilice /32 para direcciones IP específicas.
- Para subredes, utilice cualquier otra opción. Ejemplo: 10.26.192.0/18

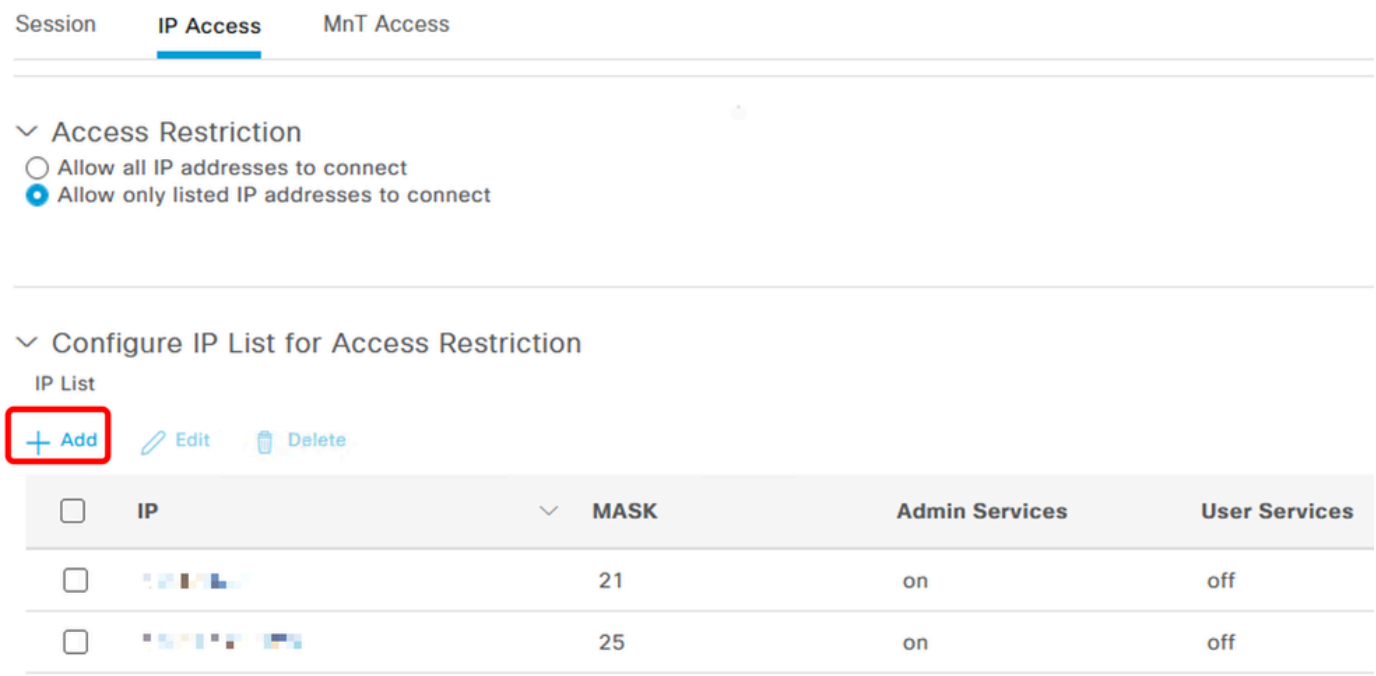
## Comportamiento en ISE 3.2

Navegue hasta Administration > Admin Access > Settings > Access. Tiene estas opciones disponibles:

- Sesión
- Acceso IP
- Acceso MnT

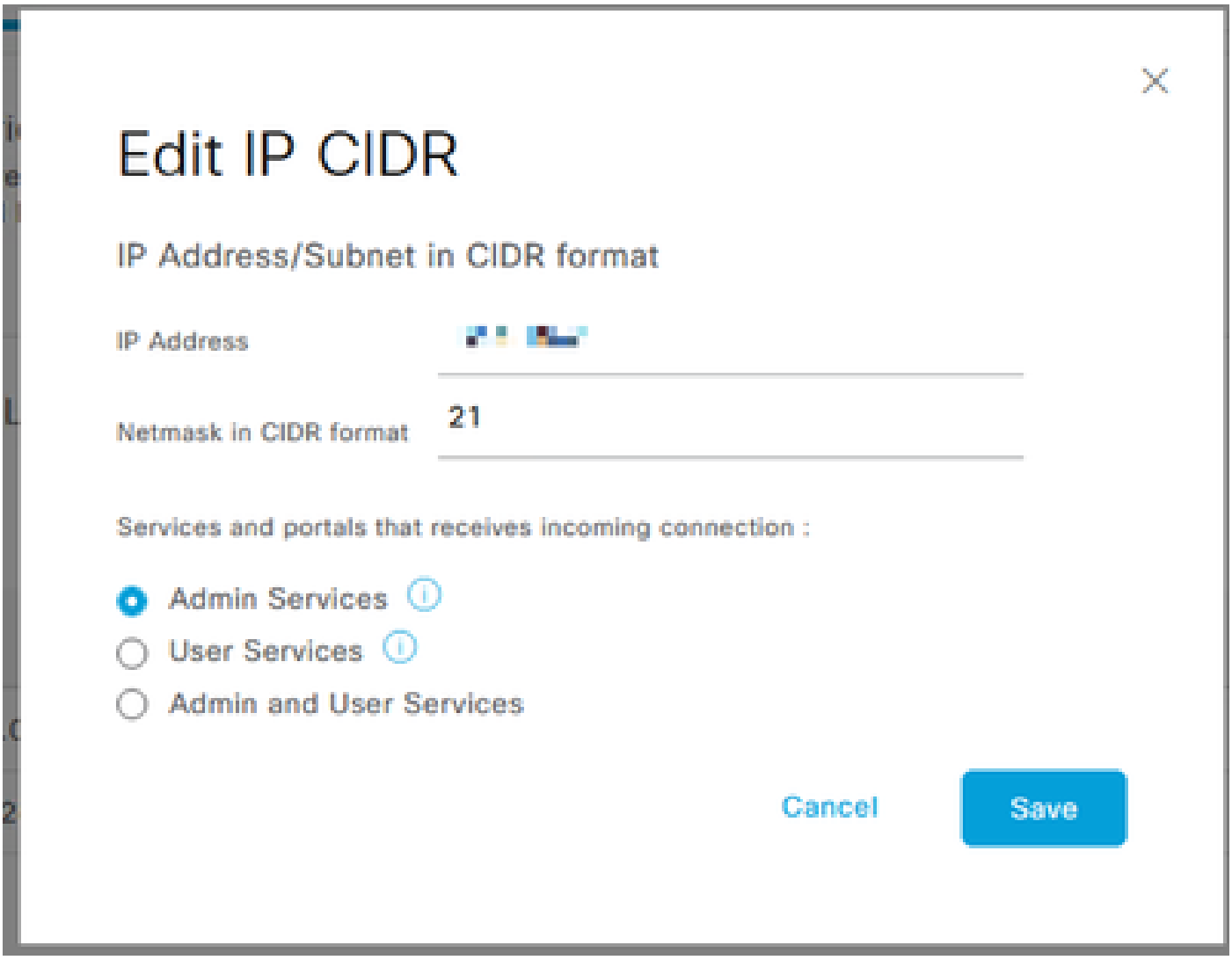
## Configurar

- Seleccionar **Allow only listed IP addresses to connect**.
- Haga clic en Add.



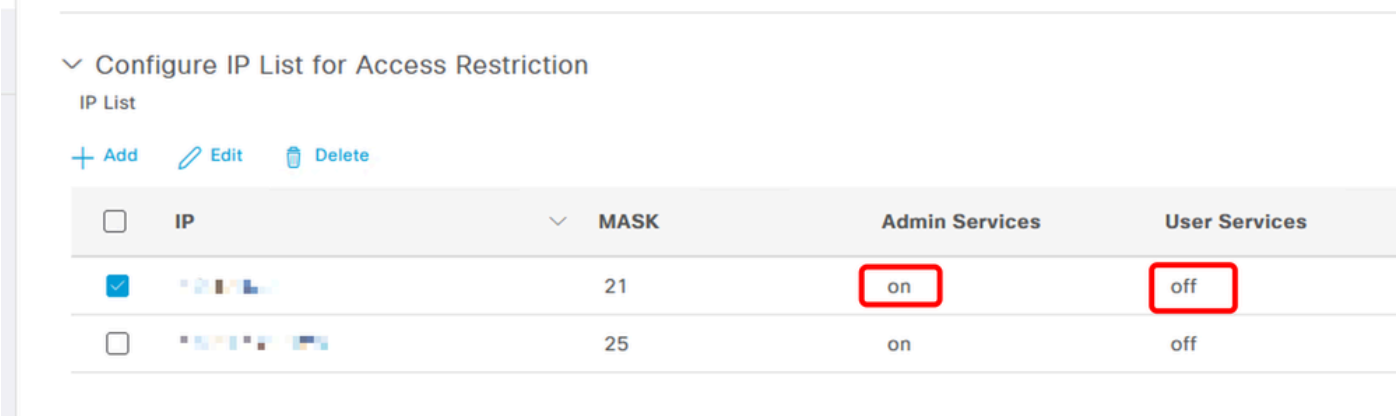

Configuración de acceso IP

- Se abre un cuadro de diálogo en el que se introducen las direcciones IP, IPv4 o IPv6, en formato CIDR.
- Una vez configurada la IP, establezca la máscara en formato CIDR.
- Estas opciones están disponibles para la restricción de acceso IP:
  - Servicios de administración: GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid (desactivado en el parche 2), MnT Analytics
  - Servicios para usuarios: Invitado, BYOD, estado, definición de perfiles
  - Servicios de administración y de usuario




Editar CIDR IP

- Haga clic en elSavebotón .
- ON significa que los servicios de administración están habilitados,OFFsignifica que los servicios de usuario están deshabilitados.



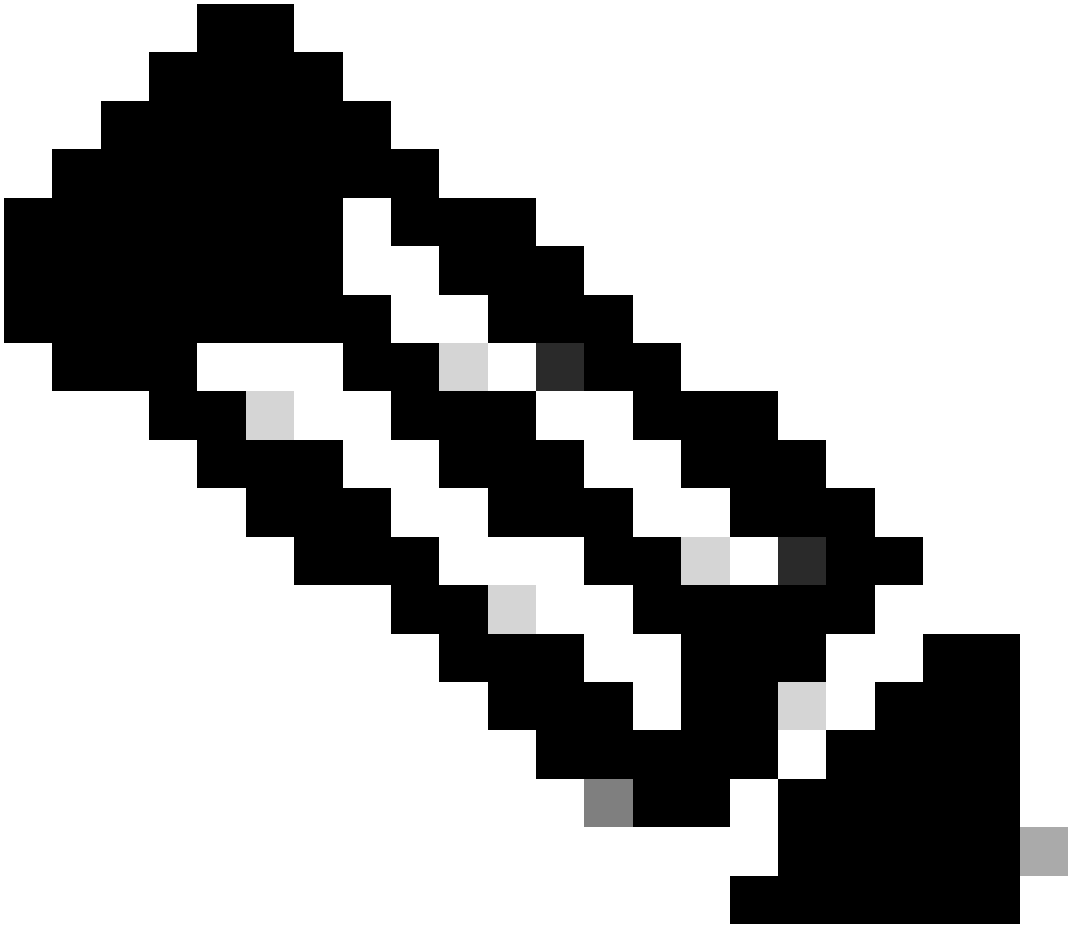

Configuración del acceso IP en 3.2

## Comportamiento en ISE 3.2 P4 y versiones posteriores

Vaya a .Administration > Admin Access > Settings > Access Tiene estas opciones disponibles:

- Sesión
- GUI y CLI de administración: GUI de ISE (TCP 443), CLI de ISE (SSH TCP22) y SNMP.
- Servicios de administración: API ERS, API abierta, pxGrid y DataConnect.
- Servicios para usuarios: Invitado, BYOD, estado.
- Acceso a MNT: Con esta opción, ISE no consume mensajes de Syslog enviados desde fuentes externas.

---

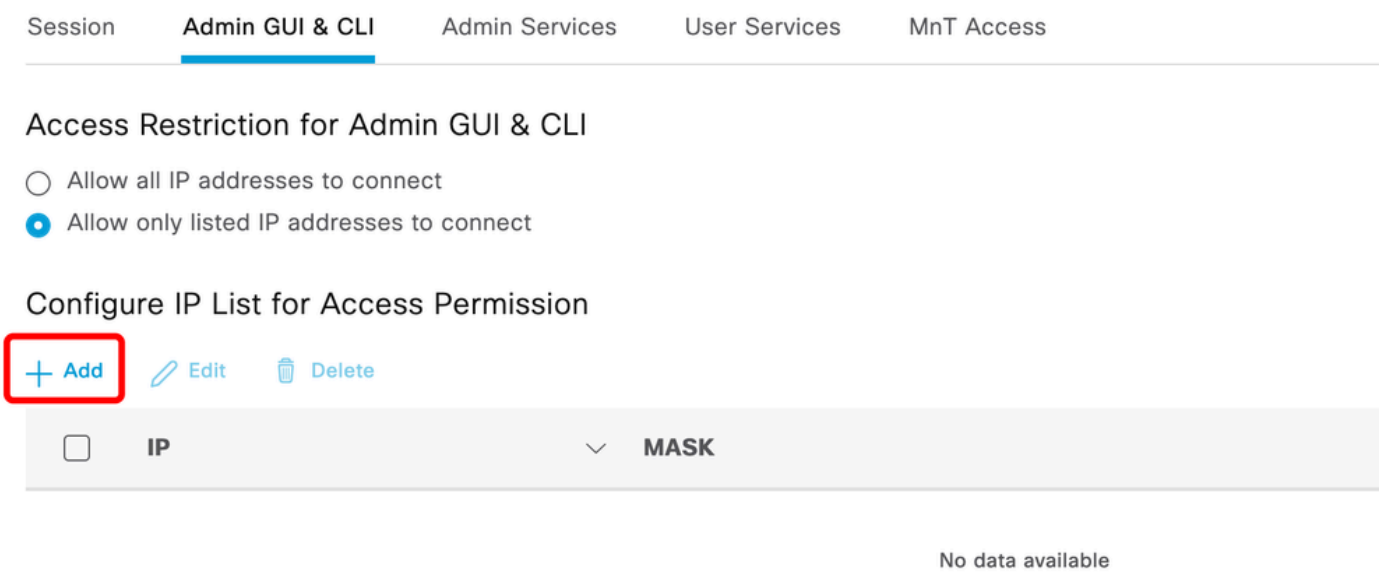


Nota: La restricción de acceso a pxGrid y Data Connect es para ISE 3.3+, pero no para ISE 3.2 P4+.

---

## Configurar

- Seleccionar Allow only listed IP addresses to connect.
- Haga clic en **Add**.




Configuración de acceso IP en 3.3

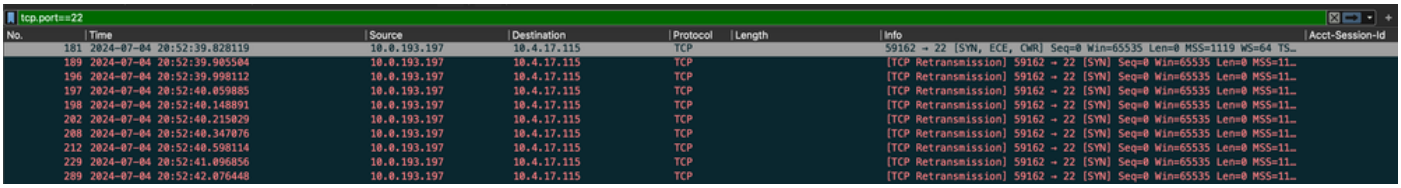
- Se abre un cuadro de diálogo en el que se introducen las direcciones IP, IPv4 o IPv6, en formato CIDR.
- Una vez configurada la IP, establezca la máscara en formato CIDR.
- Haga clic en Add.

# Recuperar GUI/CLI de ISE

- Inicie sesión con la consola.
- Detener los servicios de ISE mediante `application stop ise`
- Iniciar servicios ISE mediante `application start ise safe`
- Elimine la restricción de acceso IP de la GUI.

# Resolución de problemas

Realice una captura de paquetes para verificar si ISE no responde o si está descartando el tráfico.



| No. | Time | Source | Destination | Protocol | Length | Info | Acct-Session-Id |
|---|---|---|---|---|---|---|---|
| 181 | 2024-07-04 20:52:39.828119 | 10.0.193.197 | 10.4.17.115 | TCP | | 59162 → 22 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1119 WS=64 TS… | |
| 189 | 2024-07-04 20:52:39.905504 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 196 | 2024-07-04 20:52:39.998112 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 197 | 2024-07-04 20:52:40.059885 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 198 | 2024-07-04 20:52:40.148891 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 202 | 2024-07-04 20:52:40.215029 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 208 | 2024-07-04 20:52:40.347076 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 212 | 2024-07-04 20:52:40.598114 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 229 | 2024-07-04 20:52:41.096856 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |
| 289 | 2024-07-04 20:52:42.076448 | 10.0.193.197 | 10.4.17.115 | TCP | | [TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11… | |

## Comprobar las reglas del firewall ISE

- Para 3.1 y versiones inferiores, puede verificar esto solo en el show tech.
  - Puede tomar un show tech y almacenarlo en el disco local usando `show tech-support file`
  - A continuación, puede transferir el archivo a un repositorio mediante `copy disk:/`

    `ftp://`

/path

. La dirección URL del repositorio cambia en función del tipo de repositorio que esté utilizando.

- Puede descargar el archivo en su máquina para que pueda leerlo y buscar **Running iptables -nvL**.
- Las reglas iniciales del show tech no están incluidas aquí. En otras palabras, aquí puede encontrar las últimas reglas añadidas a la función show tech by IP Access restricted.

```
****************************************
Running iptables -nvL...
****************************************
.
.
Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0 tcp dpt:22 Firewall rule permitting the SSH traffic from s
461 32052 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
65 4048 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_161_udp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0 udp dpt:161 Firewall rule permitting the SNMP traffic from se
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

- Para la versión 3.2 y posteriores, puede utilizar el comando `show firewall` para verificar las reglas del firewall.
- Las versiones 3.2 y superiores proporcionan un mayor control sobre los servicios que están siendo bloqueados por la Restricción de acceso IP.

```
gjuarezo-311/admin#show firewall
.
.

Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
170 13492 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0 tcp dpt:22 Firewall rule permitting the SSH traffic
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
13 784 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_161_udp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0 udp dpt:161 Firewall rule permitting the SNMP traffic from se
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8910_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
```

```
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8910 Firewall rule permitting the PxGrid traffic from
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
90 5400 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8443_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8443 Firewall rule permitting the HTTPS traffic from
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8444_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8444 Firewall rule permitting the Block List Portal t
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8445_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0 tcp dpt:8445 Firewall rule permitting the Sponsor Portal traf
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

## Comprobar registros de depuración

Advertencia: No todo el tráfico genera registros. La restricción de acceso IP puede bloquear el tráfico en el nivel de aplicación y mediante el firewall interno de Linux. SNMP, CLI y SSH se bloquean en el nivel de firewall, por lo que no se generan registros.

- Habilite el Infrastructure componente para DEPURAR desde la GUI.
- Habilite el **Admin-infra** componente para DEPURAR desde la GUI.
- Habilite el **NSF** componente para DEPURAR desde la GUI.
- Utilice show logging application ise-psc.log tail.

Las entradas del registro de ejemplo pueden verse cuando el acceso a la interfaz de usuario web de administración de ISE está restringido, donde la subred permitida es 198.18.133.0/24 mientras que el administrador de ISE viene de 198.18.134.28.

```
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.nsf.impl.NetworkElement -::::- The ip a
```

```
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterC
```

## Información Relacionada

- Guía de administración de ISE 3.1
- Guía de administración de ISE 3.2
- Guía de administración de ISE 3.3
- Soporte técnico y descargas de Cisco

Acerca de esta traducción

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

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

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