

Configuration de la restriction d'accès IP dans ISE

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Comportement dans ISE 3.1 et versions antérieures](#)

[Configurer](#)

[Comportement dans ISE 3.2](#)

[Configurer](#)

[Comportement dans ISE 3.2 P4 et versions ultérieures](#)

[Configurer](#)

[Récupérer l'interface utilisateur graphique/CLI ISE](#)

[Dépannage](#)

[Vérifier les règles de pare-feu ISE](#)

[Vérifier les journaux de débogage](#)

[Informations connexes](#)

Introduction

Ce document décrit les options disponibles pour configurer la restriction d'accès IP dans ISE 3.1, 3.2 et 3.3.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base de Cisco Identity Service Engine

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

La fonctionnalité de restriction d'accès IP permet aux administrateurs de contrôler les adresses IP ou les plages qui peuvent accéder au portail et aux services d'administration ISE.

Cette fonctionnalité s'applique à divers services et interfaces ISE, notamment :

- Accès au portail admin et CLI
- Accès à l'API ERS
- Accès au portail invité et sponsor
- Accès au portail Mes périphériques

Lorsqu'elle est activée, ISE autorise uniquement les connexions à partir des plages ou adresses IP spécifiées. Toute tentative d'accès aux interfaces d'administration ISE à partir d'IP non spécifiées est bloquée.

En cas de verrouillage accidentel, ISE fournit une option de démarrage « en mode sans échec » qui peut contourner les restrictions d'accès IP. Cela permet aux administrateurs de récupérer l'accès et de corriger les erreurs de configuration.

Comportement dans ISE 3.1 et versions antérieures

Accédez à Administration>Admin Access>Settings>Access. Vous disposez des options suivantes :

- Session
- Accès IP
- Accès MnT

Configurer

- Sélectionnez « Autoriser uniquement les adresses IP répertoriées à se connecter »
- Cliquez sur Ajouter.

∨ Access Restriction

- Allow all IP addresses to connect
- Allow only listed IP addresses to connect

∨ Configure IP List for Access Restriction

IP List

- + Add**
-  Edit
-  Delete

<input type="checkbox"/>	IP	▼	MASK
--------------------------	----	---	------

No data available

Configuration d'accès IP

- Dans ISE 3.1, vous n'avez pas la possibilité de sélectionner entre les services « Admin » et « User », ce qui permet à la restriction d'accès IP de bloquer les connexions vers :
 - IUG
 - CLI
 - SNMP
 - SSH
- Une boîte de dialogue s'ouvre et vous permet d'entrer les adresses IP, IPv4 ou IPv6, au format CIDR.
- Une fois l'adresse IP configurée, définissez le masque au format CIDR.

restriction

in
d



Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address



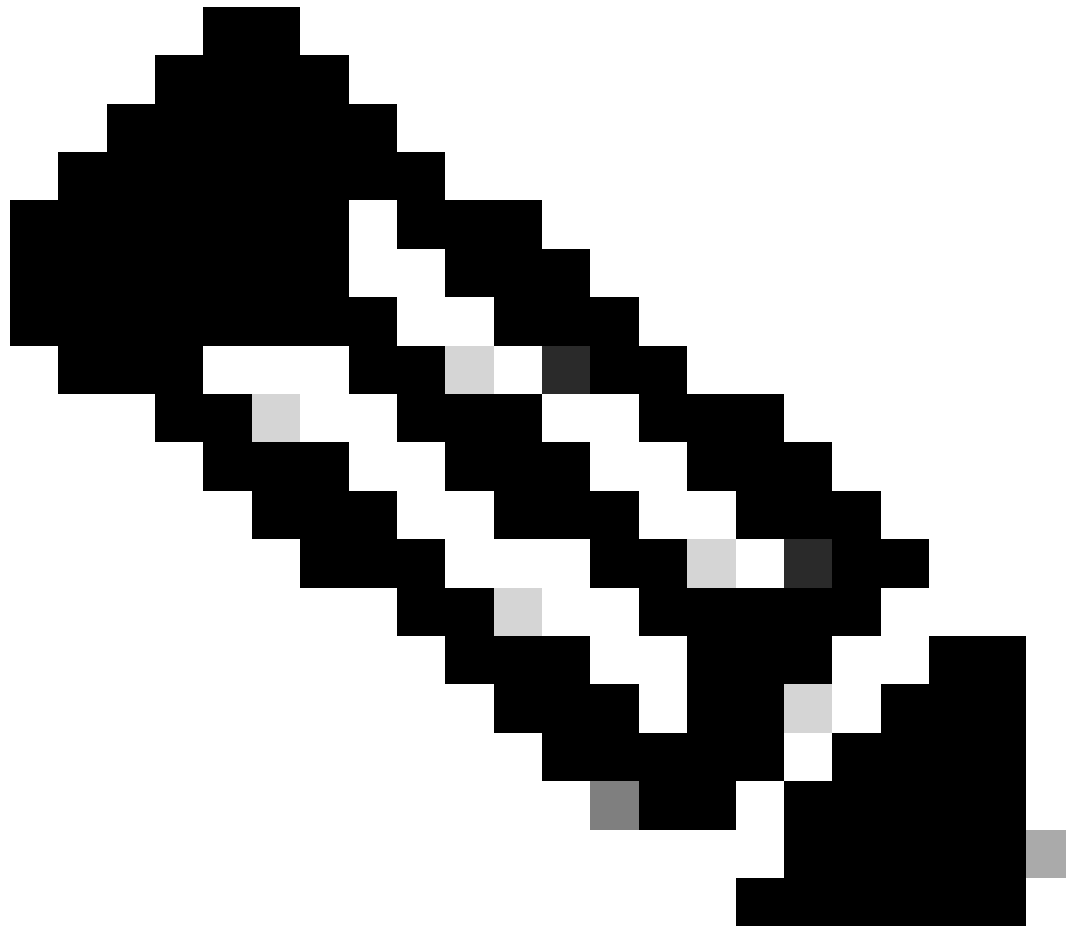
Netmask in CIDR format

32

Cancel

OK

Modifier le CIDR IP

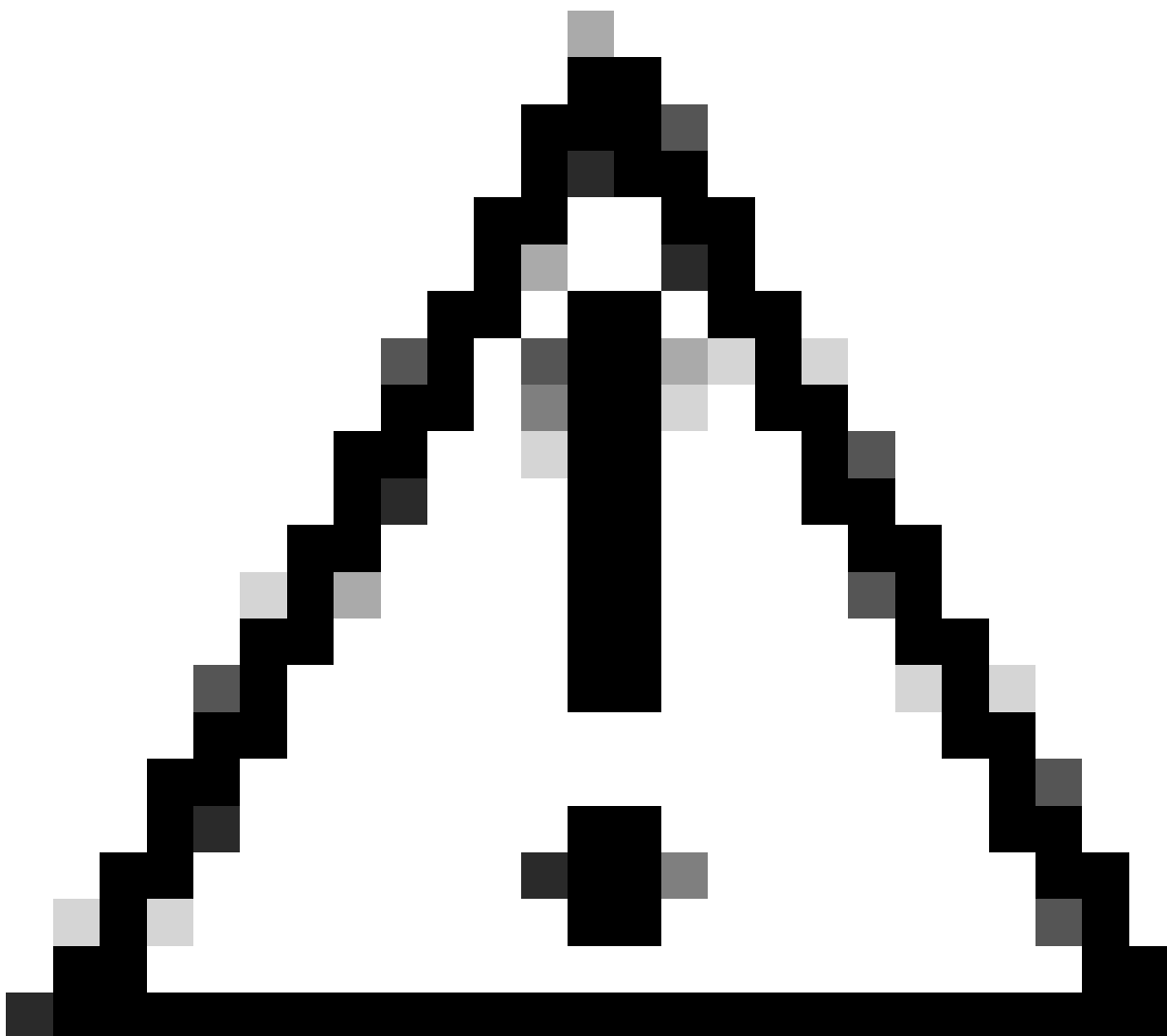


Remarque : le format CIDR (Classless Inter-Domain Routing) IP est une méthode de représentation des adresses IP et de leur préfixe de routage associé.

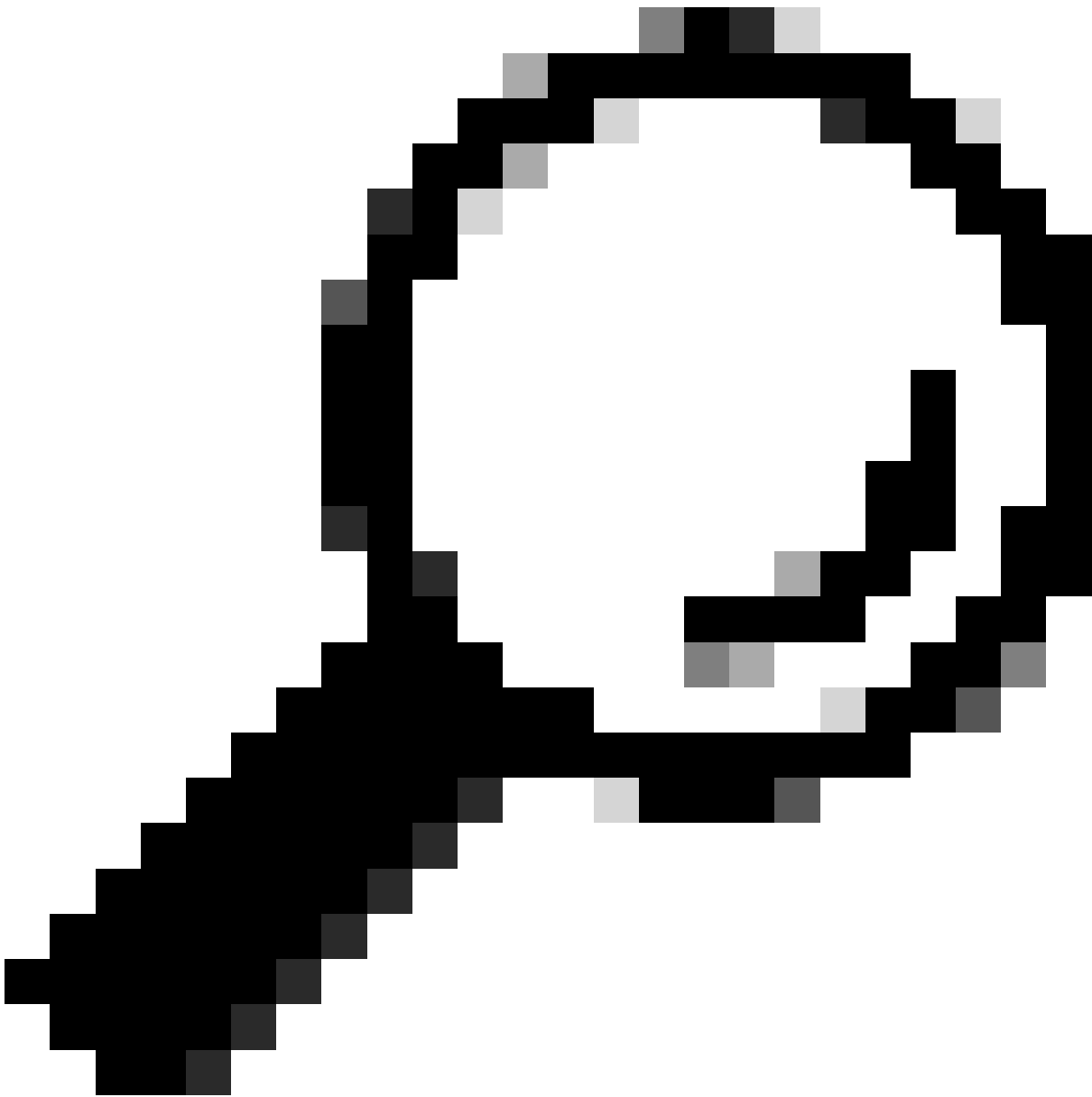
Exemple :

IP : 10.8.16.32

Masque : /32



Attention : vous devez être prudent lors de la configuration des restrictions IP afin d'éviter de verrouiller accidentellement l'accès administrateur légitime. Cisco recommande de tester minutieusement toute configuration de restriction IP avant de l'implémenter complètement.



Conseil : pour les adresses IPv4 :

- Utilisez /32 pour des adresses IP spécifiques.
- Pour les sous-réseaux, utilisez une autre option. Exemple : 10.26.192.0/18

Comportement dans ISE 3.2

Accédez à Administration>Admin Access>Settings>Access. Vous disposez des options suivantes :

- Session
- Accès IP
- Accès MnT

Configurer

- Sélectionnez « Autoriser uniquement les adresses IP répertoriées à se connecter »
- Cliquez sur Ajouter.

Session **IP Access** MnT Access



∨ Access Restriction

Allow all IP addresses to connect

Allow only listed IP addresses to connect

∨ Configure IP List for Access Restriction

IP List

+ Add  Edit  Delete

<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input type="checkbox"/>	10.10.10.10	21	on	off
<input type="checkbox"/>	10.10.10.10	25	on	off

Configuration de l'accès IP

- Une boîte de dialogue s'ouvre et vous permet d'entrer les adresses IP, IPv4 ou IPv6, au format CIDR.
- Une fois l'adresse IP configurée, définissez le masque au format CIDR.
- Ces options sont disponibles pour la restriction d'accès IP
 - Services d'administration : GUI, CLI (SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid (désactivé dans le patch 2), MnT Analytics
 - Services utilisateur : invité, BYOD, posture, profilage
 - Services administrateur et utilisateur

✕

Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address

Netmask in CIDR format

Services and portals that receives incoming connection :

Admin Services ⓘ

User Services ⓘ

Admin and User Services

Cancel
Save

Modifier le CIDR IP

- Cliquez sur le bouton « Enregistrer »
- "ON" signifie que les services d'administration sont activés, "OFF" signifie que les services d'utilisateur sont désactivés.

▼ Configure IP List for Access Restriction

IP List

+ Add Edit Delete

	IP	MASK	Admin Services	User Services
<input checked="" type="checkbox"/>	10.10.10.10	21	on	off
<input type="checkbox"/>	10.10.10.10	25	on	off

Configuration de l'accès IP dans 3.2

Comportement dans ISE 3.2 P4 et versions ultérieures

Accédez à Administration>Admin Access>Settings>Access. Vous disposez des options suivantes

:

- Session
- Interface GUI&CLI d'administration : interface GUI d'ISE (TCP 443), interface CLI d'ISE (SSH TCP22) et SNMP.
- Services d'administration : API ERS, API ouverte, pxGrid, DataConnect.
- Services utilisateur : invité, BYOD, posture.
- MNT Access : avec cette option, ISE ne consomme pas les messages Syslog envoyés depuis des sources externes.

Configurer

- Sélectionnez « Autoriser uniquement les adresses IP répertoriées à se connecter »
- Cliquez sur Ajouter.

The screenshot shows the configuration page for 'Admin GUI & CLI'. At the top, there are tabs for 'Session', 'Admin GUI & CLI' (which is selected), 'Admin Services', 'User Services', and 'MnT Access'. Below the tabs, the section is titled 'Access Restriction for Admin GUI & CLI'. There are two radio button options: 'Allow all IP addresses to connect' (unselected) and 'Allow only listed IP addresses to connect' (selected). Below this, there is a section titled 'Configure IP List for Access Permission'. It features three buttons: '+ Add' (highlighted with a red box), 'Edit', and 'Delete'. Below the buttons is a table with two columns: 'IP' and 'MASK'. The table is currently empty, and the text 'No data available' is displayed at the bottom right of the table area.

Configuration de l'accès IP dans 3.3

- Une boîte de dialogue s'ouvre et vous permet d'entrer les adresses IP, IPv4 ou IPv6, au format CIDR.
- Une fois l'adresse IP configurée, définissez le masque au format CIDR.
- Cliquez sur Ajouter.

Récupérer l'interface utilisateur graphique/CLI ISE

- Se connecter avec la console
- Arrêter les services ISE à l'aide de l'application
- Démarrez les services ISE à l'aide de l'application start ise safe
- Supprimez la restriction d'accès IP de l'interface utilisateur graphique.

Dépannage

Effectuez une capture de paquets pour vérifier si ISE ne répond pas ou s'il abandonne le trafic.

No.	Time	Source	Destination	Protocol	Length	Info
181	2024-07-04 20:52:39.828119	10.0.193.197	10.4.17.115	TCP		59162 -> 22 [SYN, ECE, CW] Seq=0 Win=65535 Len=0 MSS=1119 WS=64 TS...
189	2024-07-04 20:52:39.985584	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 20:52:40.215829	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...

Vérifier les règles de pare-feu ISE

- Pour les versions 3.1 et inférieures, vous pouvez vérifier cela uniquement dans le show tech.
 - Vous pouvez prendre un show tech et le stocker dans le disque local en utilisant "show tech-support file <filename>"
 - Vous pouvez ensuite transférer le fichier vers un référentiel à l'aide de la commande "copy disk:<filename> ftp://<ip_address>/path". L'URL du référentiel change en fonction du type de référentiel que vous utilisez
 - Vous pouvez télécharger le fichier sur votre machine pour le lire et rechercher "Running iptables -nvL"
 - Les règles initiales du show tech ne sont pas incluses ci-dessous. En d'autres termes, vous trouverez ici les dernières règles ajoutées à la fonctionnalité de restriction show tech by IP Access.

```
<#root>
```

```
*****
```

```
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 segment x.x.x.x/x
```

```
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 segment x.x.x.x/x
```

```
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
```

- Pour les versions 3.2 et ultérieures, vous pouvez utiliser la commande "show firewall" pour vérifier les règles de pare-feu.
- Les versions 3.2 et ultérieures offrent un meilleur contrôle sur les services bloqués par la restriction d'accès IP.

```
<#root>
```

```
gjuarez0-311/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 from segment x.x.x.x/x
```

```
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 segment x.x.x.x/x
```

```
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 segment x.x.x.x/x
```

```
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 F

iptables rule permitting the HTTPS traffic from segment x.x.x.x/x

```
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 F

iptables rule permitting the Block List Portal traffic from segment x.x.x.x/x

```
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 F

iptables rule permitting the Sponsor Portal traffic from segment x.x.x.x/x

```
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
```

Vérifier les journaux de débogage



Avertissement : tout le trafic ne génère pas de journaux. La restriction d'accès IP peut bloquer le trafic au niveau de l'application et à l'aide du pare-feu interne Linux. Les protocoles SNMP, CLI et SSH sont bloqués au niveau du pare-feu, de sorte qu'aucun journal n'est généré.

-
- Activez le composant « Infrastructure » dans DEBUG à partir de l'interface utilisateur graphique.
 - Utiliser `show logging application ise-psc.log tail`

Les journaux suivants peuvent être consultés lorsque la restriction d'accès IP prend des mesures.

```
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
```

Informations connexes

- [Assistance technique de Cisco et téléchargements](#)
- [Guide d'administration ISE 3.1](#)
- [Guide d'administration ISE 3.2](#)
- [Guide d'administration ISE 3.3](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.