

ISEでのIPアクセス制限の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ISE 3.1以前の動作](#)

[設定](#)

[ISE 3.2の動作](#)

[設定](#)

[ISE 3.2 P4以降での動作](#)

[設定](#)

[ISE GUI/CLIの回復](#)

[トラブルシューティング](#)

[ISEファイアウォールルールの確認](#)

[デバッグログの確認](#)

[関連情報](#)

はじめに

このドキュメントでは、ISE 3.1、3.2、および3.3でIPアクセス制限を設定するために使用できるオプションについて説明します。

前提条件

要件

Cisco Identity Service Engine(ISE)に関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ISE バージョン 3.1
- Cisco ISE バージョン 3.2
- Cisco ISE バージョン 3.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

IPアクセス制限機能を使用すると、管理者は、どのIPアドレスまたは範囲がISE管理ポータルおよびサービスにアクセスできるかを制御できます。

この機能は、次のようなさまざまなISEインターフェイスおよびサービスに適用されます。

- 管理ポータルアクセスおよびCLI
- ERS APIアクセス
- ゲストおよびスポンサーポータルへのアクセス
- My Devicesポータルへのアクセス

有効にすると、ISEは指定されたIPアドレスまたは範囲からの接続のみを許可します。指定されていないIPからISE管理インターフェイスにアクセスしようとする、ブロックされます。

誤ってロックアウトが発生した場合、ISEには、IPアクセス制限をバイパスできる「セーフモード」起動オプションが用意されています。これにより、管理者はアクセスを回復し、設定ミスを修正できます。

ISE 3.1以前の動作

Administration > Admin Access > Settings > Accessに移動します。次のオプションがあります。

- セッション
- IPアクセス
- MnTアクセス

設定

- **Allow only listed IP addresses to connect** を選択します。
- をクリックします。Add

∨ Access Restriction

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

∨ Configure IP List for Access Restriction

IP List

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

No data available

IPアクセスの設定

- ISE 3.1では、AdminとサーUser ビスの間で選択するオプションがありません。IPアクセス制限を有効にすると、次のものに対する接続がブロックされます。
 - GUI
 - CLI を使う場合 :
 - SNMP
 - SSH
- ダイアログボックスが開き、IPアドレス (IPv4またはIPv6) をCIDR形式で入力できます。
- IPを設定したら、CIDR形式でマスクを設定します。



Edit IP CIDR

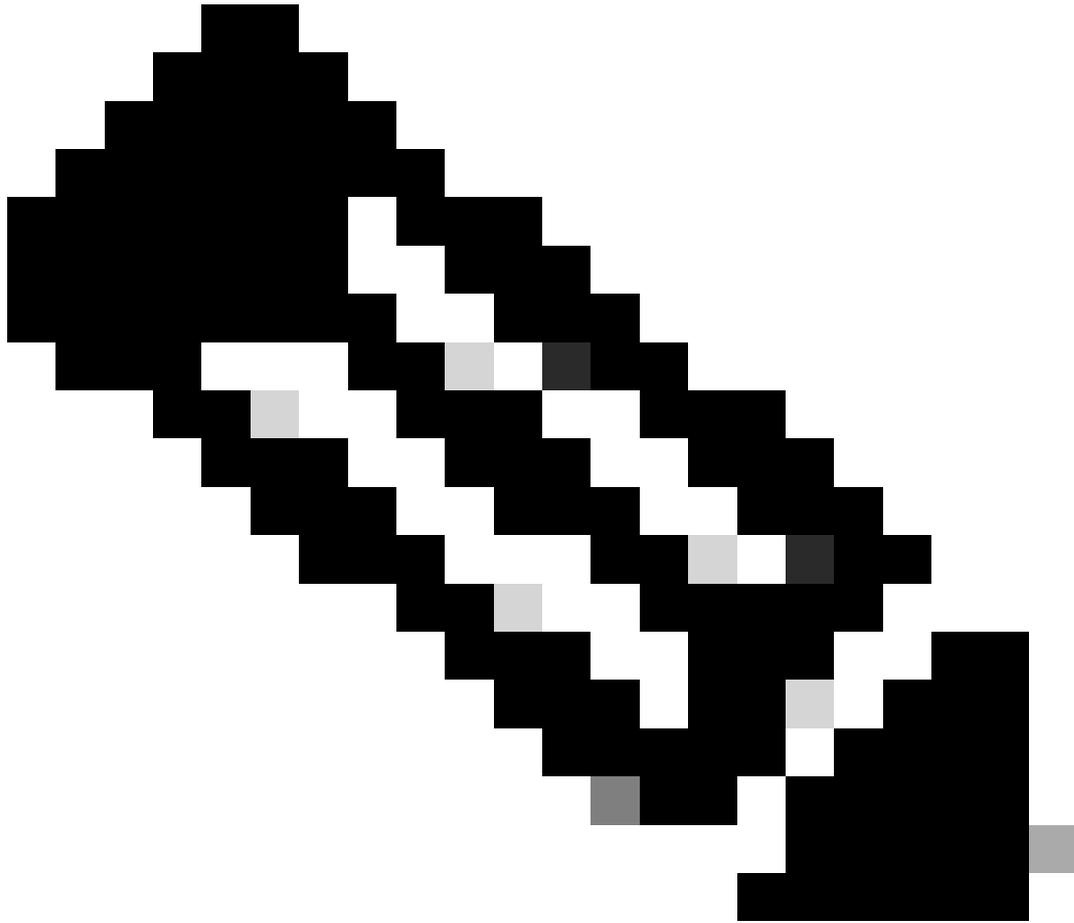
IP Address/Subnet in CIDR format

IP Address

Netmask in CIDR format

Cancel

OK

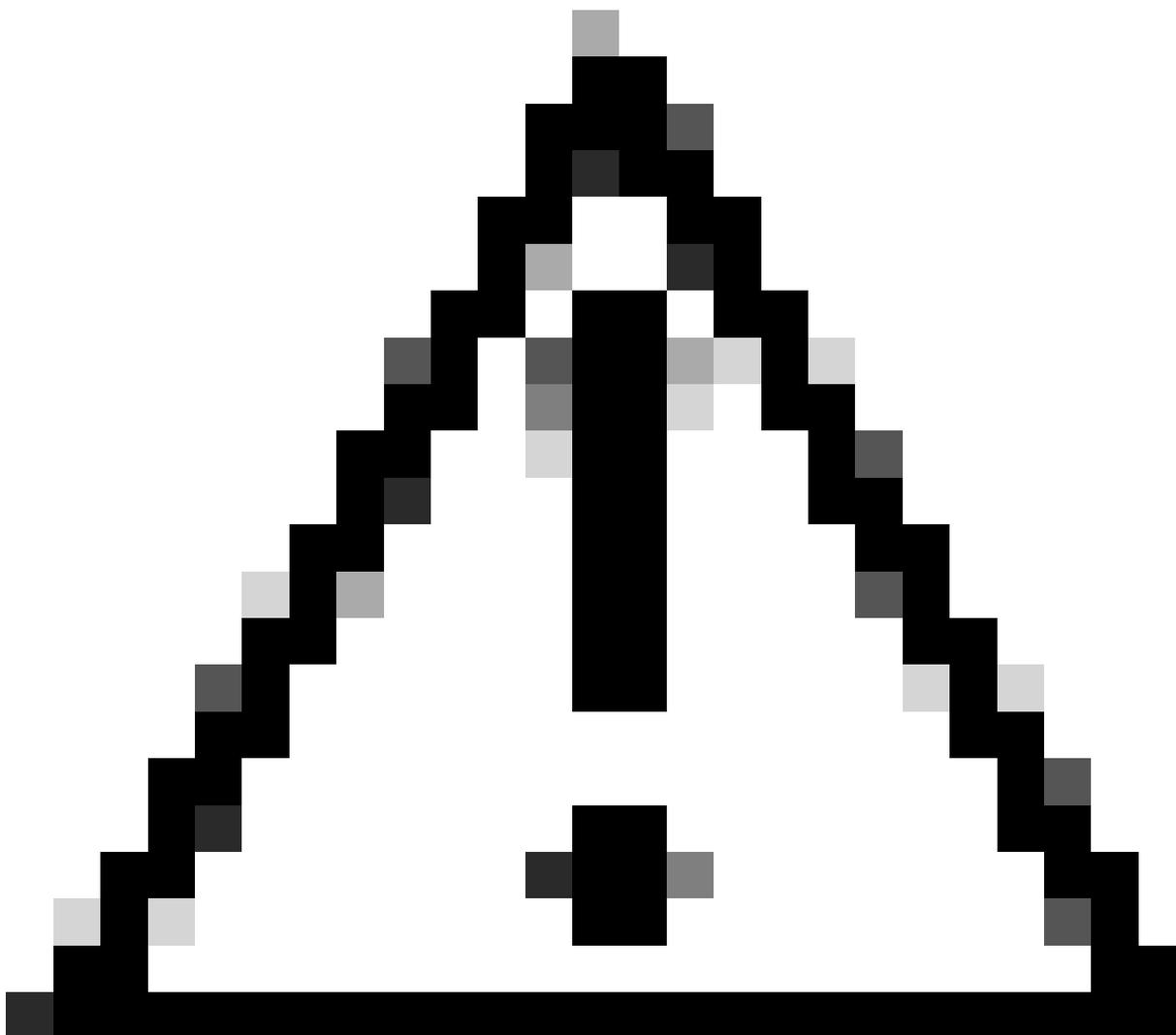


注:IP Classless Inter-Domain Routing(CIDR)形式は、IPアドレスとそれに関連付けられているルーティングプレフィクスを表す方法です。

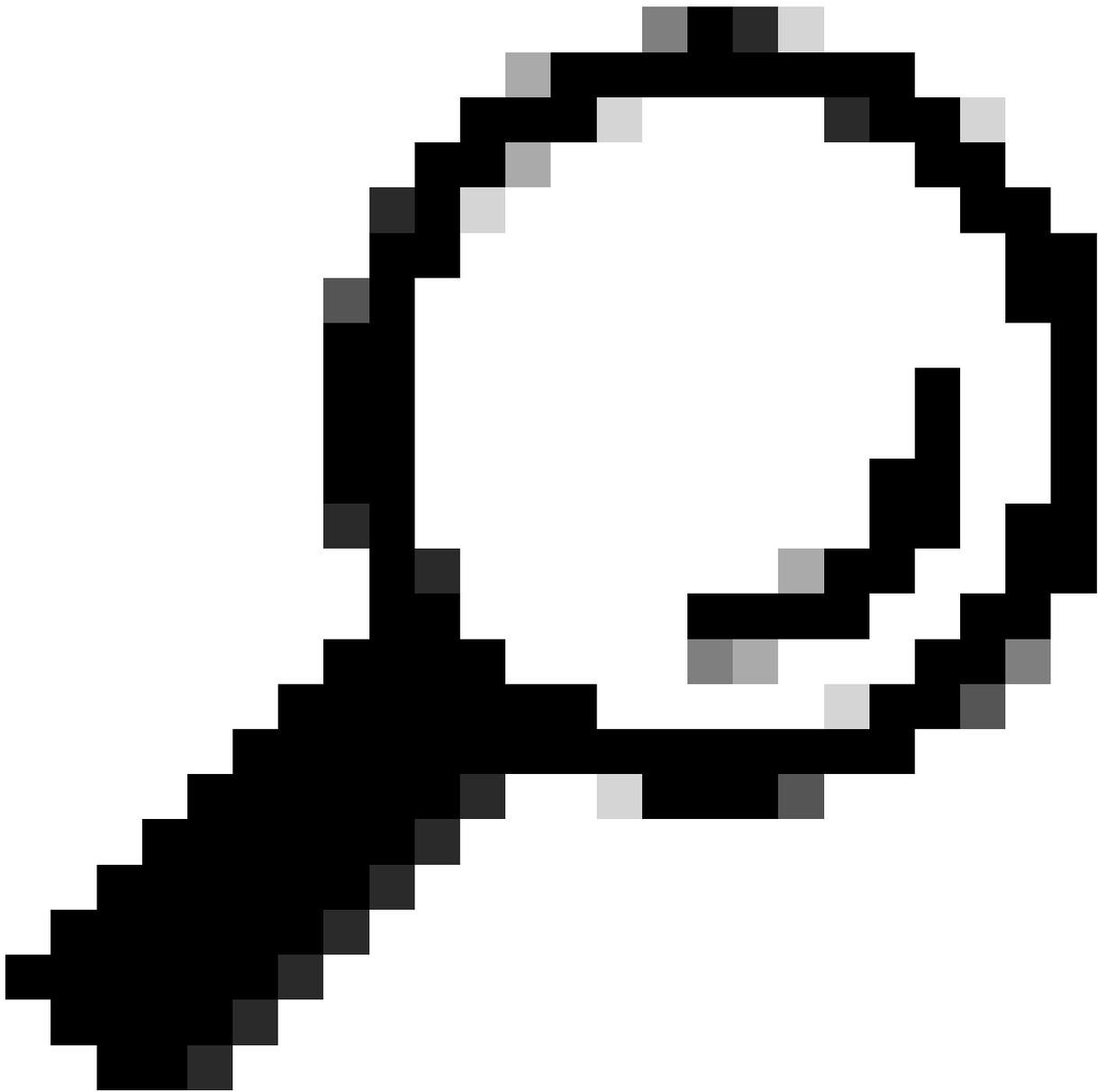
以下に例を挙げます。

IP:10.8.16.32

マスク : /32



注意:IP制限を設定する際は、正当な管理者アクセスが誤ってロックアウトされないように注意する必要があります。
IP制限を完全に実装する前に、IP制限設定を徹底的にテストすることをお勧めします。



ヒント: IPv4アドレスの場合:

- 特定のIPアドレスに/32を使用します。
- サブネットの場合は、他のオプションを使用します。例: 10.26.192.0/18

ISE 3.2の動作

次のオプションを使用しAdministration > Admin Access > Settings > Access. ぎるよう移動します。

- セッション
- IPアクセス
- MnTアクセス

設定

- 選択 **Allow only listed IP addresses to connect.**
- をクリックします。Add

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

IPアクセスの設定

- ダイアログボックスが開き、IPアドレス (IPv4またはIPv6) をCIDR形式で入力できます。
- IPを設定したら、CIDR形式でマスクを設定します。
- IPアクセスの制限には、次のオプションを使用できます。

- Admin Services:GUI、CLI(SSH)、SNMP、ERS、OpenAPI、UDN、API Gateway、PxGrid (パッチ2では無効)、MnT Analytics
- ユーザサービス : ゲスト、BYOD、ポスチャ、プロファイリング
- 管理サービスとユーザサービス

×

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

IP CIDRの編集

- Saveボタンをクリックします。
- ON Adminサービスが有効であることを意味し、OFF、ユーザサービスが無効であることを意味します。

Configure IP List for Access Restriction

IP List

+ Add Edit Delete

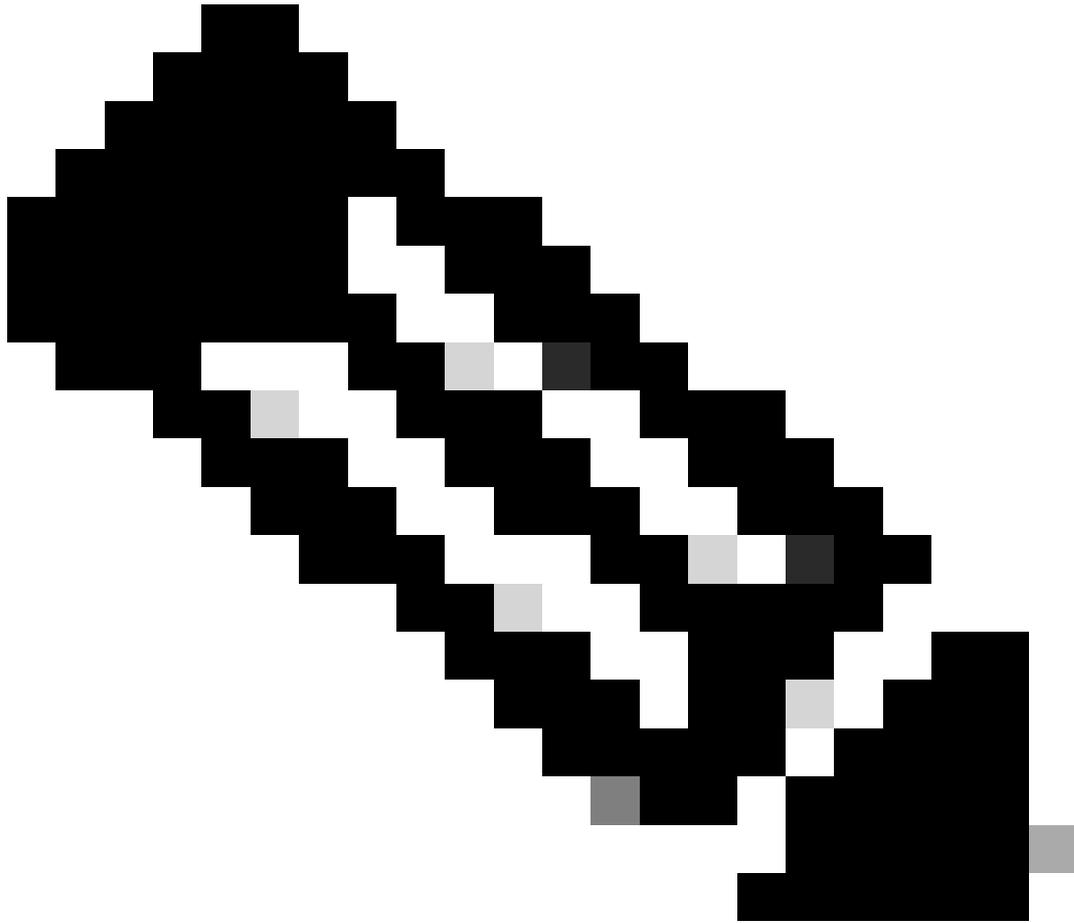
<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input checked="" type="checkbox"/>	10.10.10.10	21	on	off
<input type="checkbox"/>	10.10.10.10	25	on	off

3.2のIPアクセス設定

ISE 3.2 P4以降での動作

Administration > Admin Access > Settings > Accessに移動します。次のオプションを使用できます。

- セッション
- 管理GUIおよびCLI: ISE GUI(TCP 443)、ISE CLI(SSH TCP22)、およびSNMP。
- 管理サービス : ERS API、Open API、pxGrid、DataConnect
- ユーザサービス : ゲスト、BYOD、ポスチャ
- MNTアクセス : このオプションを使用すると、ISEは外部ソースから送信されるsyslogメッセージを消費しません。



注:pxGridおよびData Connectのアクセス制限はISE 3.3+に対してであり、ISE 3.2 P4+に対してではありません。

設定

- 選択 Allow only listed IP addresses to connect.
- クリック Add.

Access Restriction for Admin GUI & CLI

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

Configure IP List for Access Permission

+ Add
✎ Edit
🗑 Delete

<input type="checkbox"/>	IP	▼	MASK
No data available			

3.3のIPアクセス設定

- ダイアログボックスが開き、IPアドレス (IPv4またはIPv6) をCIDR形式で入力できます。
- IPを設定したら、CIDR形式でマスクを設定します。
- をクリックします。Add

ISE GUI/CLIの回復

- コンソールを使用してログインします。
- ISEサービスの停止 `application stop ise`
- ISEサービスの開始方法 `application start ise safe`
- GUIからIPアクセス制限を削除します。

トラブルシューティング

ISEが応答していないか、またはトラフィックをドロップしているかを確認するために、パケットキャプチャを実行します。

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 MS=64 TS...	
189	2024-07-04 20:52:39.985504	10.0.193.197	10.4.17.115	TCP	59162	[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	59162	[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	59162	[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	59162	[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	59162	[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	59162	[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	59162	[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
229	2024-07-04 20:52:41.096056	10.0.193.197	10.4.17.115	TCP	59162	[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	59162	[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	

ISEファイアウォールルールの確認

- 3.1以前の場合、これはshow techでのみチェックできます。
 - show techコマンドを実行して、localdiskに保存できます。 show tech-support file <filename>
 - その後、リポジトリにファイルを転送できます。 copy disk:/<filename> ftp://<ip_address>/path. リポジトリのURLは、使用しているリポジトリタイプに応じて変わります。
 - ファイルをマシンにダウンロードして、ファイルを読み取り、 **Running iptables -nvL**.
 - show techの初期ルールは含まれていません。つまり、show tech by IP Access restriction機能に最後のルールが追加されています。

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

- 3.2以降では、show firewallコマンドを使用してファイアウォールルールを確認できます。
- 3.2以降では、IPアクセス制限によってブロックされるサービスをより細かく制御できます。

gjuarez-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 Firewall 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 Firewall 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 Firewall 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

デバッグログの確認



警告：すべてのトラフィックでログが生成されるわけではありません。IPアクセス制限は、アプリケーションレベルでLinux内部ファイアウォールを使用してトラフィックをブロックできます。SNMP、CLI、SSHはファイアウォールレベルでブロックされるため、ログは生成されません。

-
- コンポーInfrastructure ネットをGUIからデバッグできるようにします。
 - コンポーAdmin-infra ネットがGUIからデバッグできるようにします。
 - コンポーNSF ネットがGUIからデバッグできるようにします。
 - `show logging application ise-psc.log tail`を使用します。

サンプルログエントリは、ISE管理者のwebUIアクセスが制限され、許可されるサブネットが198.18.133.0/24であるのに対し、ISE管理者のアクセス元が198.18.134.28の場合に表示されます。

```
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::- IpList -> 198.18.133.0/24/basicS
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::- Low ip address198.18.133.0
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::- High ip address198.18.133.255
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.nsf.impl.NetworkElement -:::- The ip address to check is v4 198.18.134.28
2024-07-18 02:27:55,508 DEBUG [admin-http-pool4][[]] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCache -:::- Checkin Ip In ipList returned Fin
```

関連情報

- [ISE 3.1管理ガイド](#)
- [ISE 3.2管理ガイド](#)
- [ISE 3.3管理ガイド](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。