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と、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」起動オプションがあります。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。

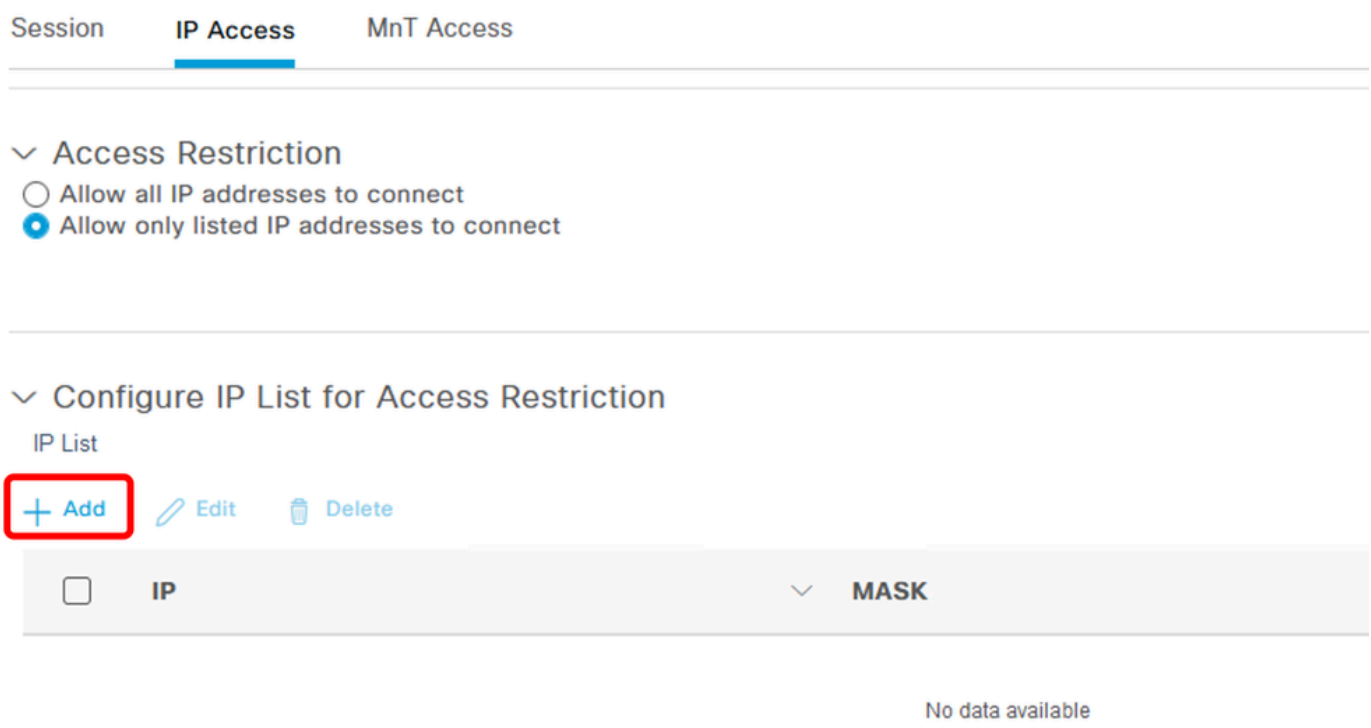
ISE 3.1以前の動作

Administration > Admin Access > Settings > Accessの順に移動します。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

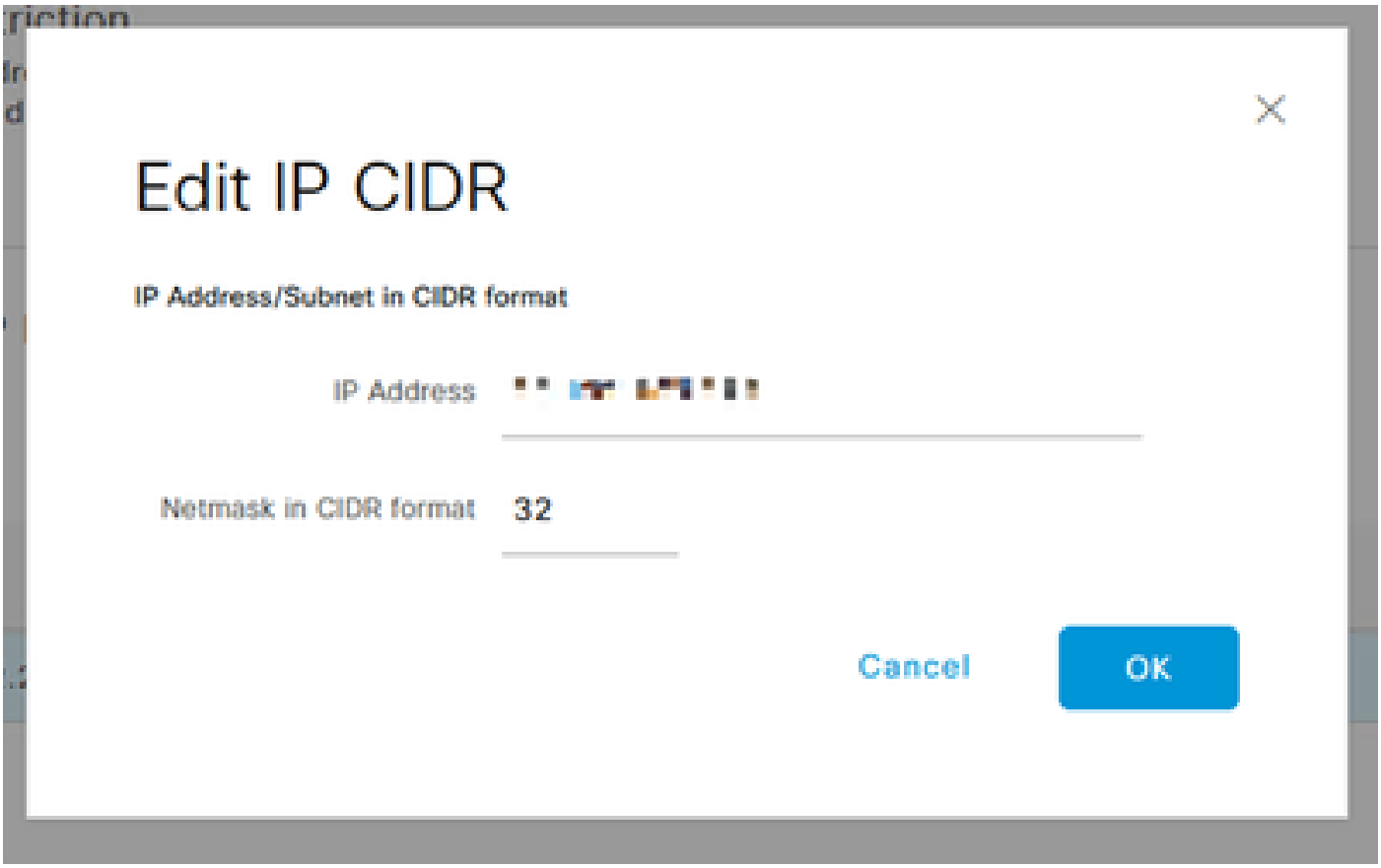
設定

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

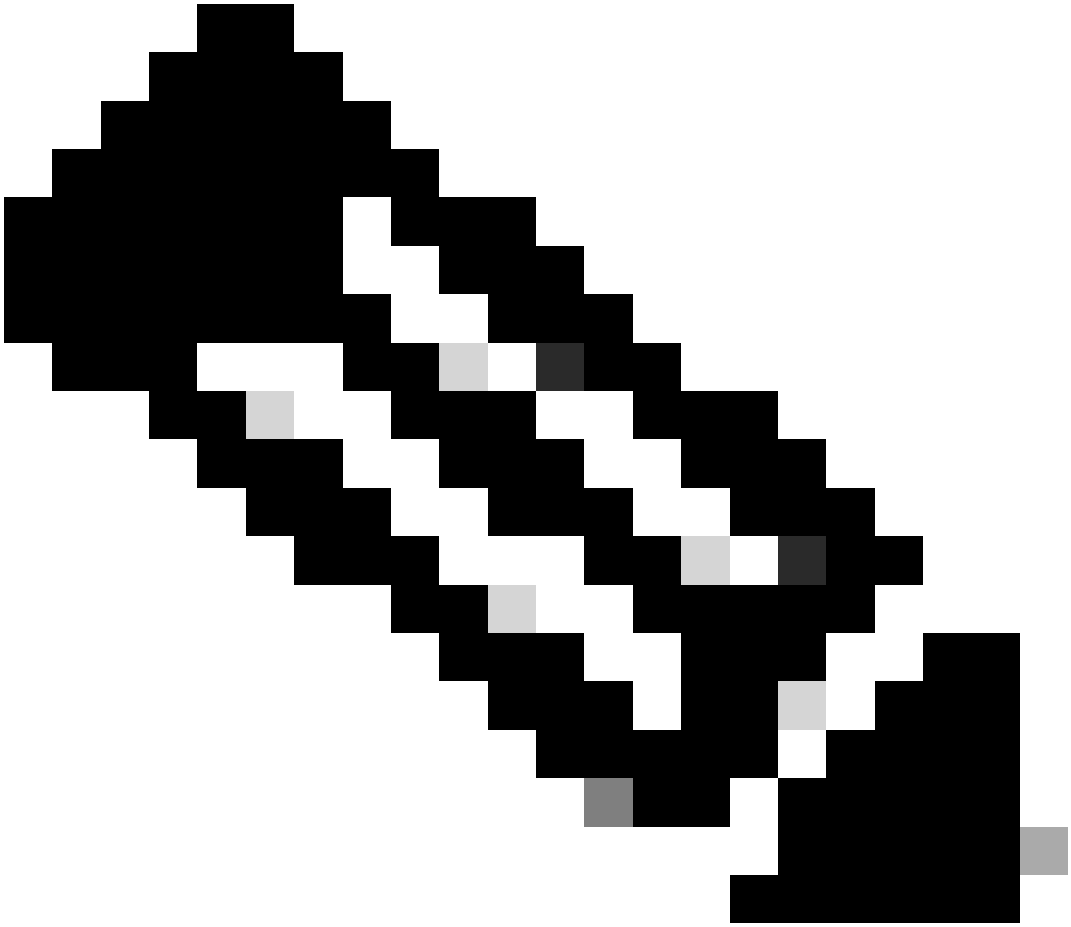


IPアクセスの設定

- ISE 3.1では、管理サービスとユーザサービスの間で選択するオプションがないため、IPアクセス制限を有効にすると次の接続先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、IPv4またはIPv6のIPアドレスを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
32
Cancel
OK

IP CIDRの編集

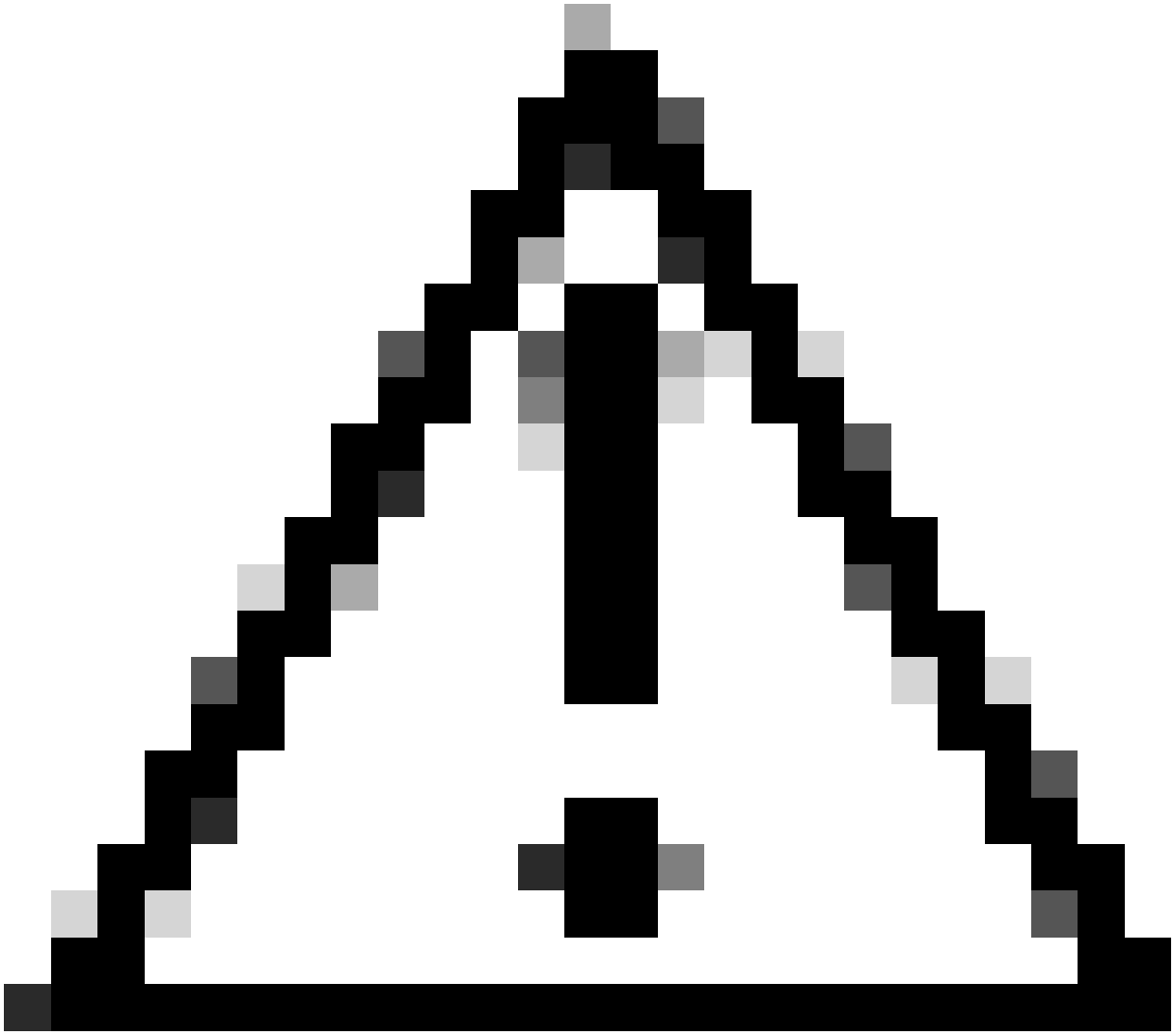


注:IP Classless Inter-Domain Routing(CIDR)形式は、IPアドレスとそれに関連付けられたルーティングプレフィックスを表す方法です。

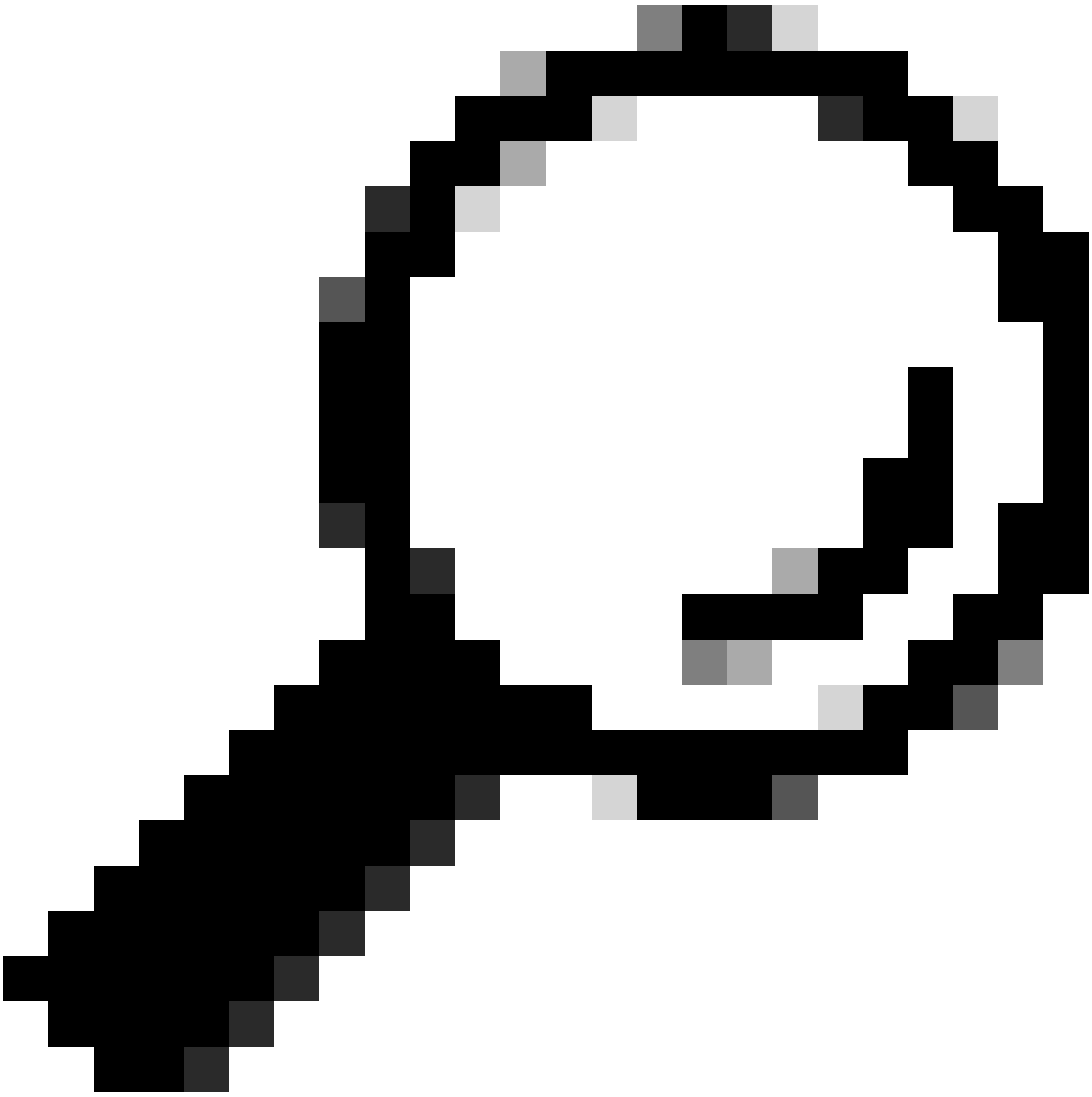
例：

IP:10.8.16.32

マスク： /32



注意:IP制限を設定する際には、正当な管理者アクセスを誤ってロックアウトしないように注意する必要があります。IP制限の設定を完全に実装する前に、その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

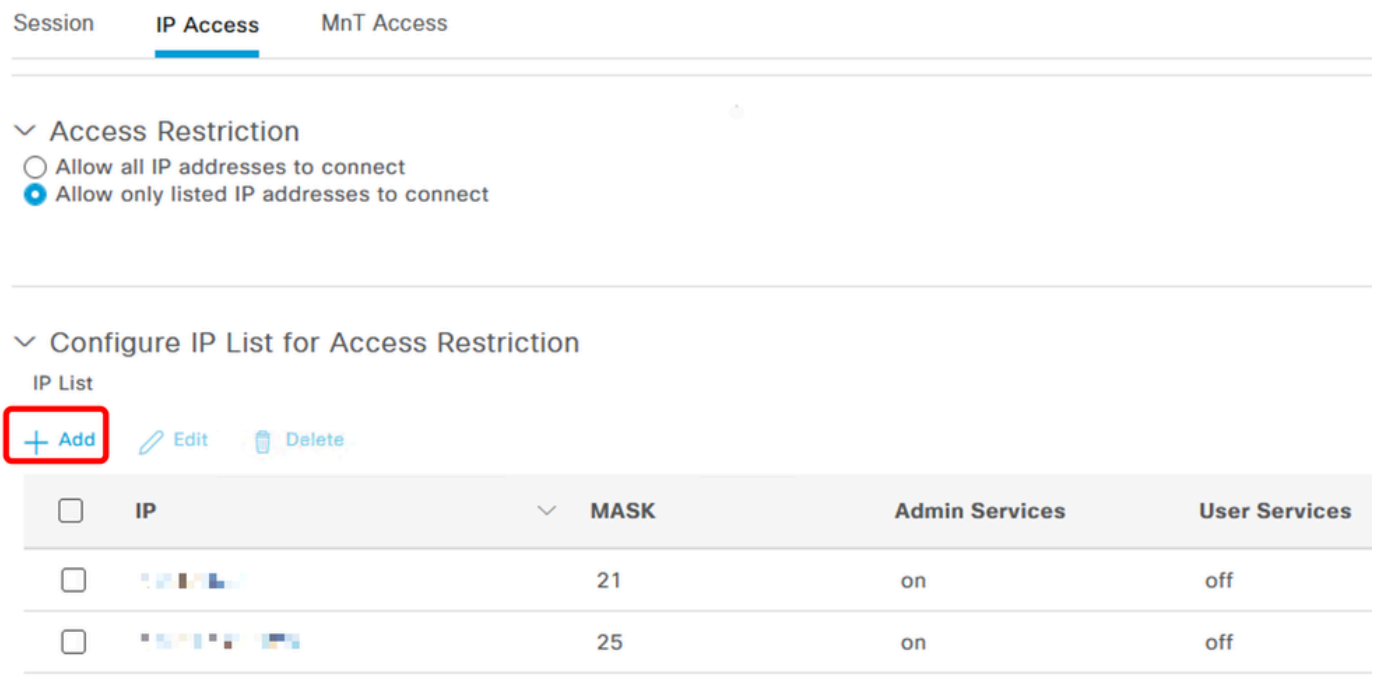
ISE 3.2の動作

Administration > Admin Access > Settings > Accessの順に選択します。次のオプションを使用できます。

- セッション
- IPアクセス
- MnTアクセス

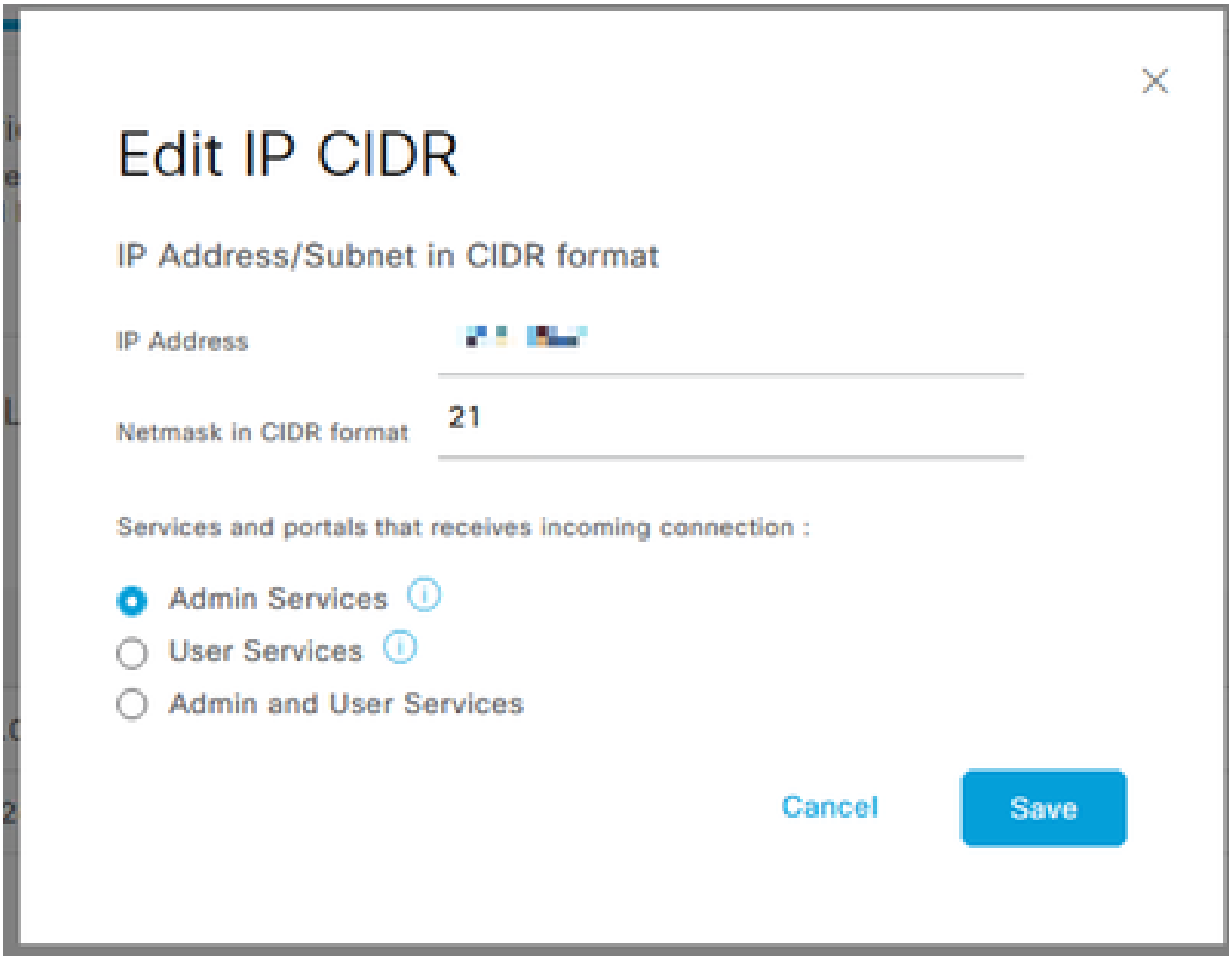
設定

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



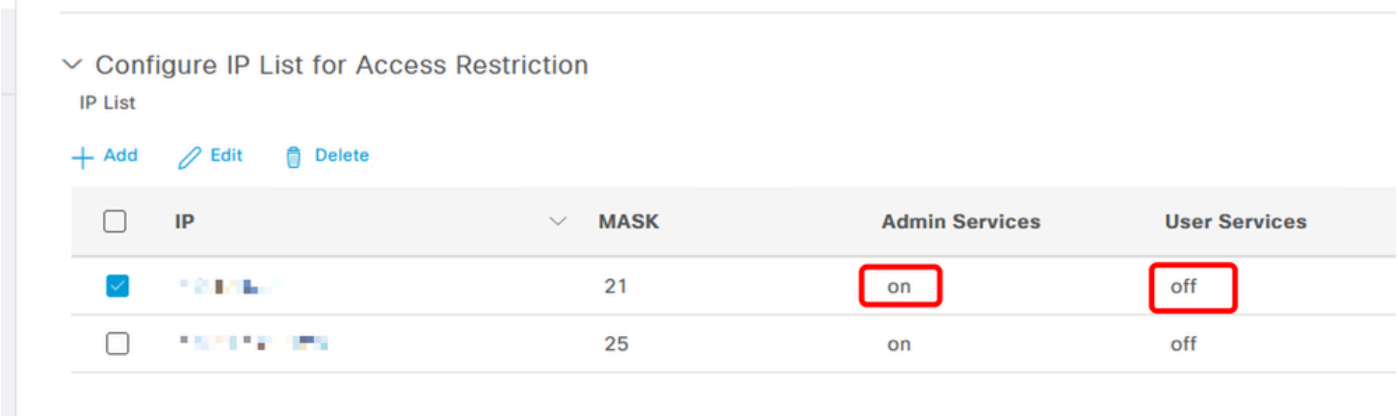
IPアクセスの設定

- ダイアログボックスが開き、IPv4またはIPv6のIPアドレスを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



IP CIDRの編集

- Saveボタンをクリックします。
- ONは管理サービスが有効になっていることを意味し、OFFはユーザサービスが無効になっていることを意味します。



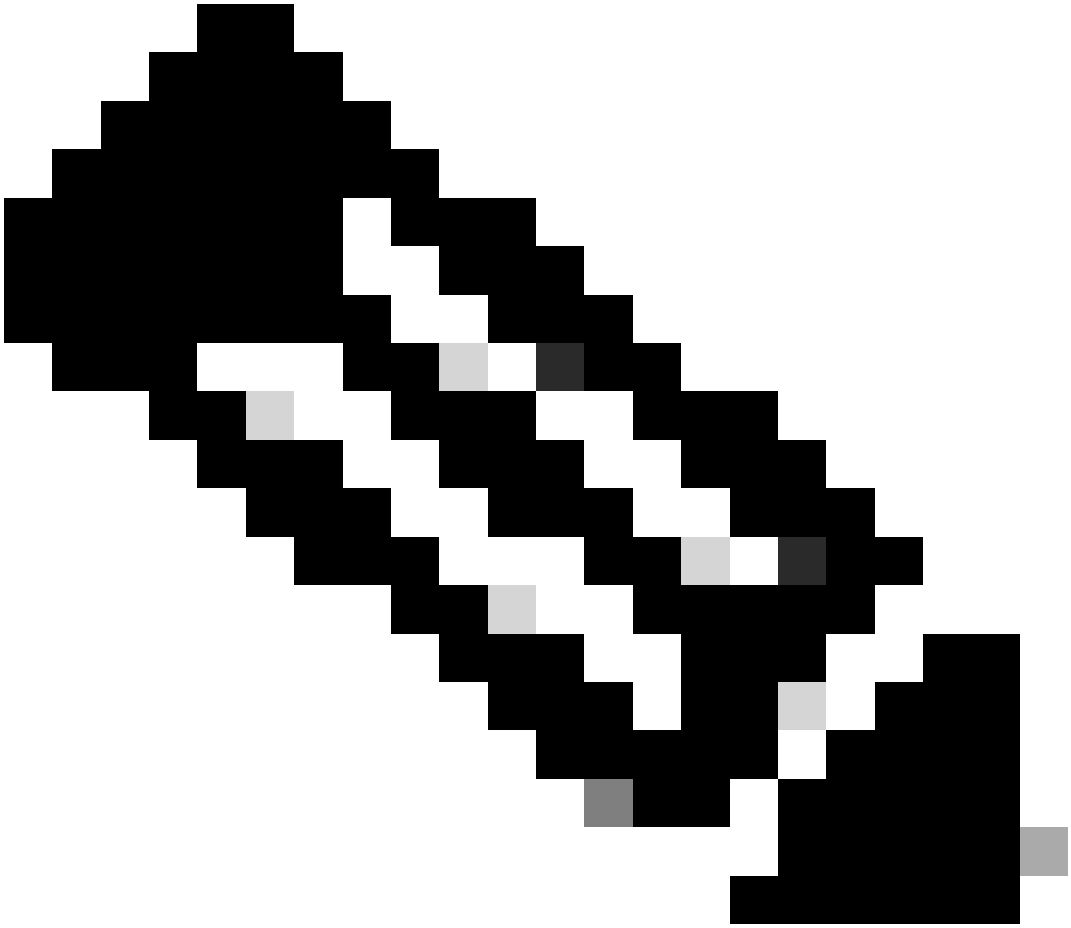
3.2のIPアクセス設定

ISE 3.2 P4以降での動作

Administration > Admin Access > Settings >

Accessの順に移動します。次のオプションを使用できます。

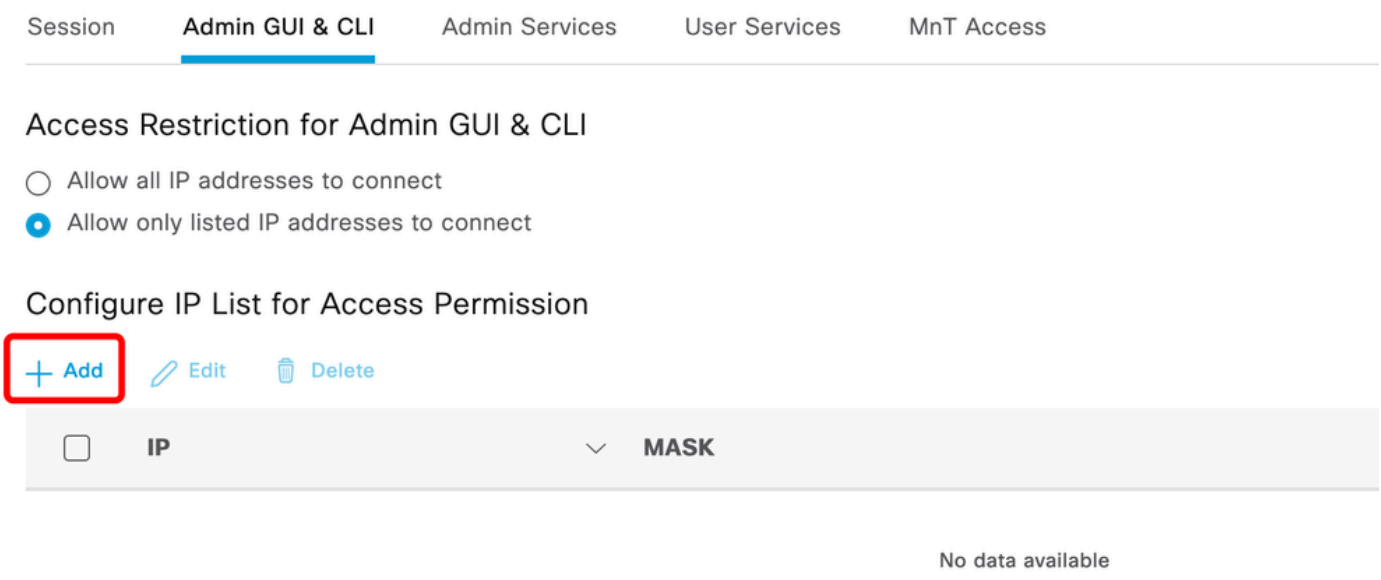
- セッション
- 管理GUIおよびCLI:ISE GUI(TCP 443)、ISE CLI(SSH TCP22)、およびSNMP。
- 管理サービス：ERS API、Open API、pxGrid、DataConnect
- ユーザサービス：ゲスト、BYOD、ポスチャ
- MNTアクセス：このオプションを使用すると、ISEは外部ソースから送信されるsyslogメッセージを消費しません。



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

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



3.3のIPアクセス設定

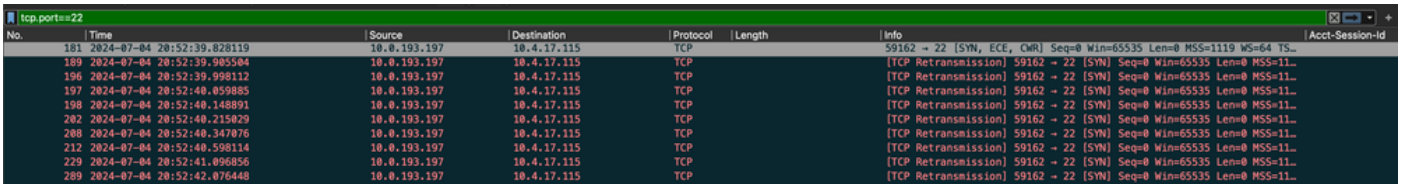
- ダイアログボックスが開き、IPv4またはIPv6のIPアドレスをCIDR形式で入力できます。
- IPを設定したら、CIDR形式でマスクを設定します。
- [Add] をクリックします。

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 アプリケーションSTOP ISE
- ISEサービスの開始方法 ise safeによるアプリケーションの起動
- 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取得します。



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-support file <filename>を使用して、show techを実行し、localdiskに保存できます。
  - 次に、copy disk:/<filename> ftp://<ip_address>/pathを使用して、ファイルをリポジトリに転送できます。 リポジトリのURLは、使用しているリポジトリタイプによって異なります。
  - このファイルを自分のマシンにダウンロードして、読み取ってRunning iptables -nvLを探す

ことができます。
- show techの最初のルールは含まれていません。つまり、show tech by IP Access restriction機能に最後に追加されたルールがあります。

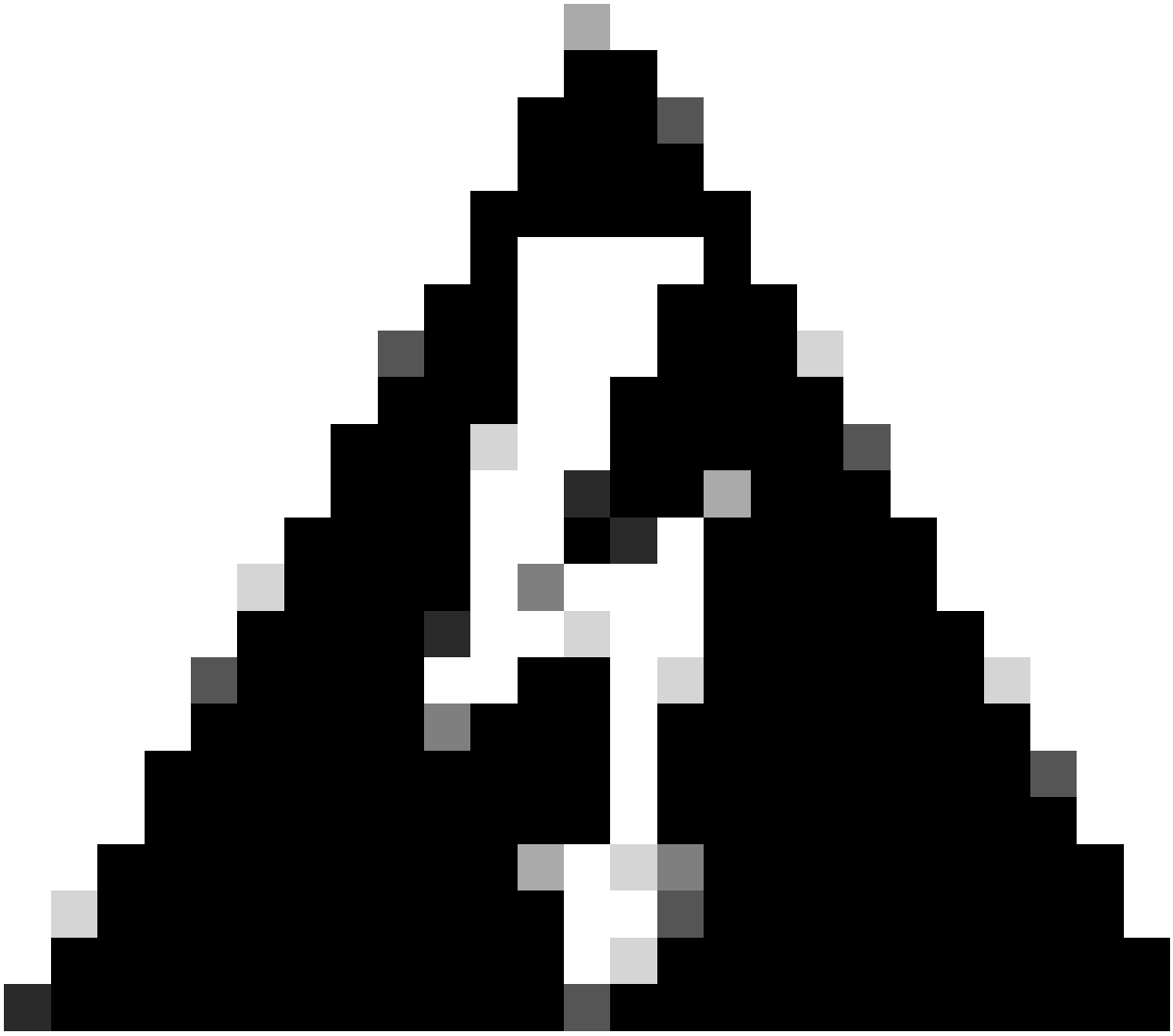
```
****************************************
Running iptables -nvL...
****************************************
.
.
Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0 tcp dpt:22 Firewall rule permitting the SSH traffic from 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
```

- 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。

```
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
```

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トラフィックをブロックし、Linux内部ファイアウォールを使用できます。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。

- GUIからデバッグするインフラストラクチャコンポーネントを有効にします。
- **Admin-infra**コンポーネントをGUIからデバッグできるようにします。
- GUIからデバッグする**NSF**コンポーネントを有効にします。
- 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管理は198.18.134.28からであることが確認できます。

```
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
```

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。