

# ISE を使用した FirePOWER 6.1 pxGrid 修復の設定

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[Firepower を設定して下さい](#)

[ISE の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

この資料に Identity Services Engine ( ISE ) で Firepower 6.1 pxGrid 治療を設定する方法を記述されています。 ISE エンドポイント保護サービス ( EPS ) と Firepower 6.1+ ISE 治療モジュールがネットワークアクセスレイヤの攻撃者の quarantine/ブラックリストに載せることを自動化するのに使用することができます。

## 前提条件

### 要件

Cisco では、次の項目について基本的な知識があることを推奨しています。

- Cisco ISE
- Cisco Firepower

### 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くものです。

- Cisco ISE バージョン 2.0 パッチ 4
- Cisco Firepower 6.1.0
- バーチャル ワイヤレス LAN コントローラ ( vWLC ) 8.3.102.0

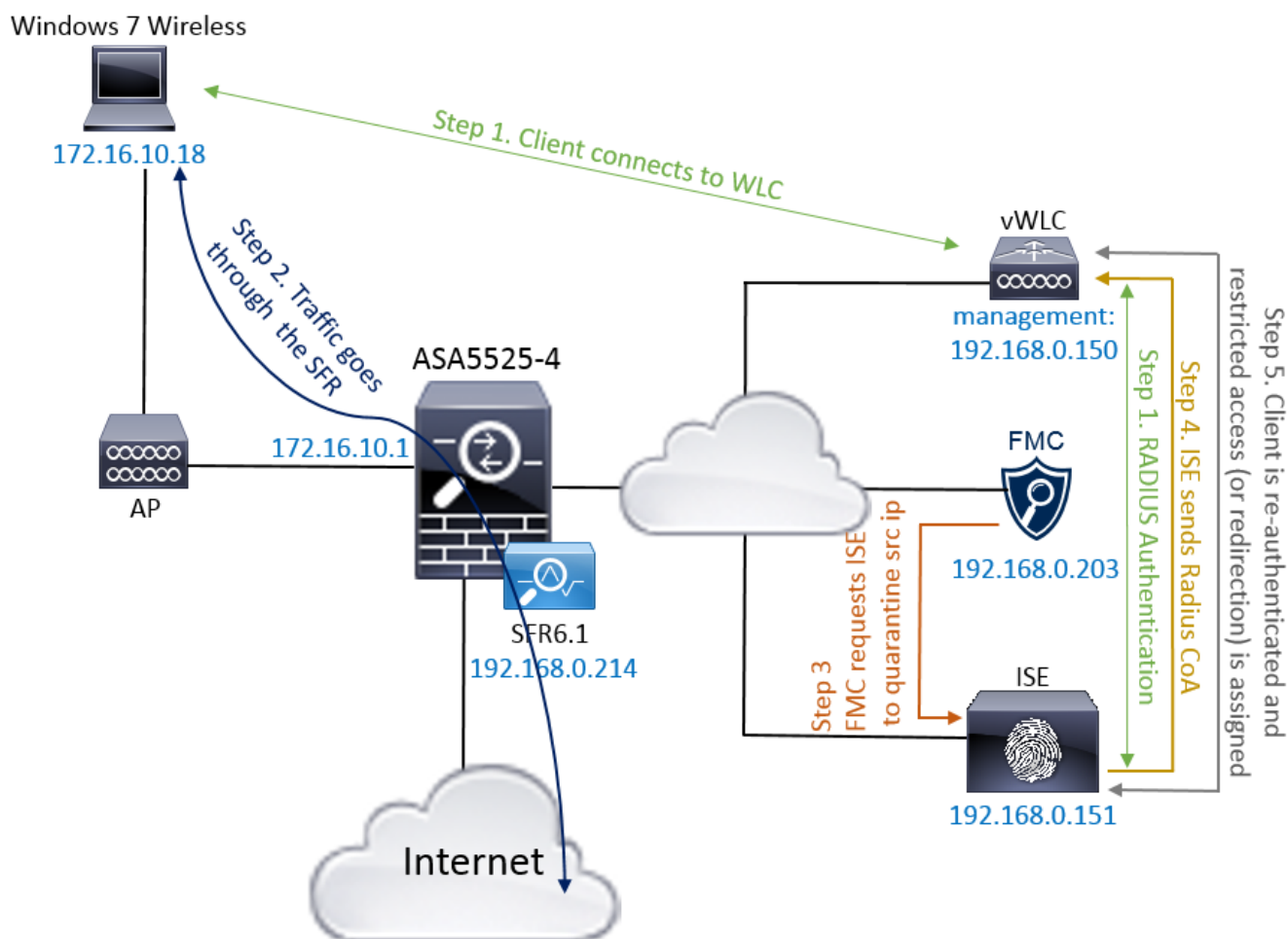
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

# 設定

この技術情報は Firepower で ISE 統合の初期設定を、Active Directory ( AD ) の ISE 統合、AD の Firepower 統合カバーしません。References セクションへのこの情報ナビゲートに関しては。 相関 ルールが一致する場合の治療として ISE EPS 機能 ( 検疫、unquarantine、ポート シャットダウン ) を使用する Firepower 6.1 治療モジュール割り当て Firepower システム。

注: ポート シャットダウンはワイヤレス配備に利用できません。

## ネットワーク図



### フロー説明:

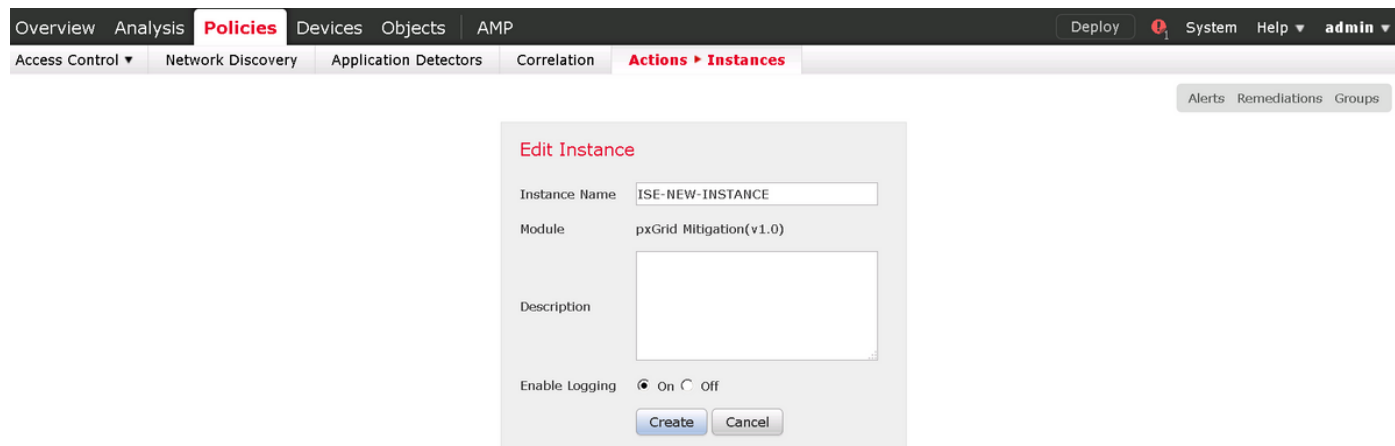
1. クライアントはネットワークに接続し、ISE と認証を受け、ネットワークに無制限のアクセスを認める許可プロファイルの承認規則を見つけます。
2. クライアントからのトラフィックは Firepower デバイスをそれからフローします。
3. ユーザは悪意のあるアクティビティを行い始め、pxGrid によって ISE 治療をするためにそれから Firepower Management Center ( FMC ) を誘発する相関 ルールを見つけます。
4. ISE はエンド ポイントに EPSStatus 検疫を割り当て、ネットワーク アクセス デバイスへの許可の半径変更を誘発します ( WLC かスイッチ ) 。
5. クライアントは制限された アクセス ( 変更 SGT かポータルまたは拒否アクセスへのリダイレクト ) を割り当てる別の承認ポリシーを見つけます。

注: ネットワーク アクセス デバイス ( NAD ) はエンド ポイントに IP アドレスをマップするのに使用されている IP アドレス情報をそれに与えるために説明する ISE に RADIUS を送信するために設定する必要があります。

## Firepower を設定して下さい

ステップ 1. pxGrid 軽減例を設定して下さい。

ポリシー > 操作 > 例にナビゲートし、イメージに示すように pxGrid 軽減例を追加して下さい。



Overview Analysis **Policies** Devices Objects AMP Deploy System Help admin

Access Control Network Discovery Application Detectors Correlation **Actions ▶ Instances** Alerts Remediations Groups

**Edit Instance**

Instance Name: ISE-NEW-INSTANCE

Module: pxGrid Mitigation(v1.0)

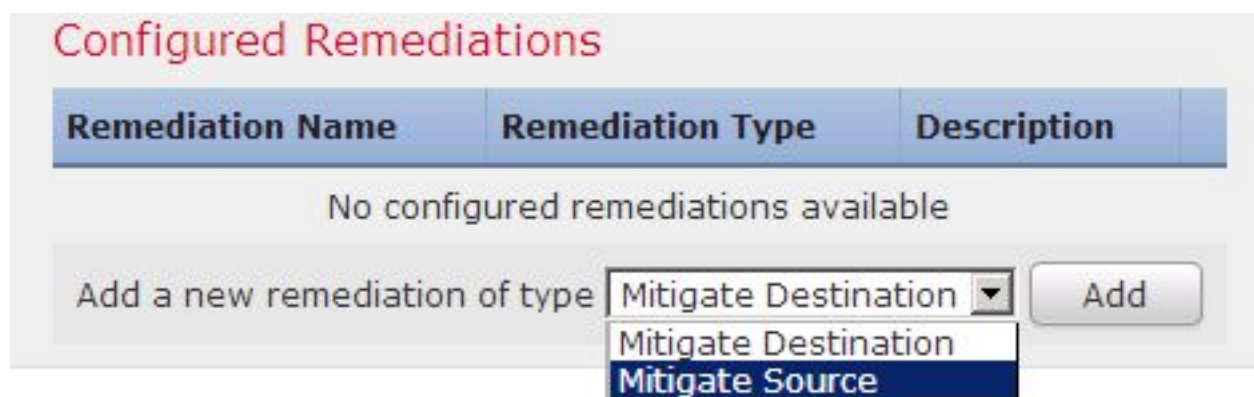
Description:

Enable Logging:  On  Off

Create Cancel

ステップ 2. 治療を設定して下さい。

利用可能な 2 つの型があります: 宛先を軽減し、ソースを軽減して下さい。このソース例で軽減は使用されます。治療型を選択し、イメージに示すように『Add』をクリックして下さい:



**Configured Remediations**

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type: **Mitigate Source** Add

イメージに示すように治療に軽減操作を割り当てて下さい:

## Edit Remediation

Remediation Name

Remediation Type

Mitigate Source

Description

Mitigation Action

Whitelist

(an optional list of networks )

ステップ 3. 関連ルールを設定して下さい。

ナビゲートし、ルール関連ルールをあります起こる治療のためのトリガーはポリシー > 関連 > ルール管理に『Create』をクリックします。関連ルールは複数の状態が含まれている場合があります。この関連ルール例で PingDC は不正侵入イベントが発生し、宛先 IP アドレスが 192.168.0.121 なら場合見つかります。カスタム不正侵入ルール一致する ICMP エコー応答はイメージに示すようにテストの為に設定されます:

Overview Analysis **Policies** Devices Objects AMP Deploy System Help admin

Access Control Network Discovery Application Detectors **Correlation** Actions

Alerts Remediations Groups

**Policy Management** Rule Management White List Traffic Profiles

**Rule Information** Add Connection Tracker Add User Qualification Add Host Profile Qualification

Rule Name: PingDC  
 Rule Description:  
 Rule Group: Ungrouped

Select the type of event for this rule  
 If an intrusion event occurs and it meets the following conditions:

Add condition Add complex condition

Destination IP is 192.168.0.121

**Rule Options** Add Inactive Period

Snooze: If this rule generates an event, snooze for 0 hours  
 Inactive Periods: There are no defined inactive periods. To add an inactive period, click "Add Inactive Period".

ステップ 4. 関連ポリシーを設定して下さい。

ポリシー > 関連 > ポリシー管理へのナビゲートはおよびポリシーを『Create』をクリックし、ポリシーにルールを追加し、イメージに示すようにそれへの応答を割り当てます:

Overview Analysis **Policies** Devices Objects AMP Deploy System Help admin

Access Control Network Discovery Application Detectors **Correlation** Actions

Alerts Remediations Groups

**Policy Management** Rule Management White List Traffic Profiles

**Correlation Policy Information** You have unsaved changes Save Cancel

Policy Name: ise\_corellation\_policy  
 Policy Description:  
 Default Priority: None

**Policy Rules** Add Rules

Rule	Responses	Priority
PingDC	QUARANTINE-SOURCE (Remediation)	Default

イメージに示すように関連ポリシーを有効に して下さい:

Overview Analysis **Policies** Devices Objects AMP Deploy System Help admin

Access Control Network Discovery Application Detectors **Correlation** Actions

Alerts Remediations Groups

**Policy Management** Rule Management White List Traffic Profiles

Create Policy

Name: ise\_corellation\_policy Sort by: State

## ISE の設定

ステップ 1. 承認ポリシーを設定して下さい。

ポリシー > 許可にナビゲートし、治療が起こった後見つかる新しい承認ポリシーを追加して下さい。使用セッション: EPSStatus は状態として検疫に匹敵します。その結果使用することができる複数のオプションがあります:

- 割り当てアクセスは異なる SGT を割り当て、（ネットワークデバイスのアクセス制御制限を適用して下さい）
- アクセスを拒否して下さい（ユーザはネットワークから蹴り、再度接続できないはずです）
- **ブラックリスト** ポータルへのリダイレクト（このシナリオカスタム ホットスポット ポータルでこのために設定されます）

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	AssignSGTBlockOnFP	if Session:EPSSStatus EQUALS Quarantine	then MaliciousUser AND PermitAccess
<input checked="" type="checkbox"/>	BlockOnISE	if Session:EPSSStatus EQUALS Quarantine	then DenyAccess
<input checked="" type="checkbox"/>	BlockOnISE_copy	if Session:EPSSStatus EQUALS Quarantine	then blacklist_redirect

## カスタム門脈設定

この例では、ホットスポット ポータルは**ブラックリスト**で設定されます。カスタム テキストが付いている Acceptable Use Policy (AUP) ページだけあり、AUP を受け入れる可能性がありません（これはジヤバスクリプトとされます）。これを実現させるために、最初にジヤバスクリプトを使用可能にし、次に門脈カスタマイゼーション設定に AUP ボタンおよび制御を隠すコードを貼り付ける必要があります。

ステップ 1. イネーブル ジヤバスクリプト。

**Administration > システム > Admin Access > 設定へのナビゲート > 門脈カスタマイゼーション。** HTML およびジヤバスクリプトの門脈カスタマイゼーションを『Enable』を選択し、『SAVE』をクリックして下さい。

Portal Customization

Enable Portal Customization with HTML

Enable Portal Customization with HTML and JavaScript

Save

ステップ 2. ホットスポット ポータルを作成して下さい。

**ゲスト アクセスへのナビゲートは >> ゲスト ポータル設定し、『Create』** をクリックしましたり、そしてホットスポット型を選択します。

Guest Portals

Choose one of the three pre-defined portal types, which you can edit, customize, and authorize for guest access.

Create Edit Duplicate Delete

ステップ 3. 門脈カスタマイゼーションを設定して下さい。

門脈ページ カスタマイゼーションにナビゲートし、ユーザに適切な警告を提供するためにタイトルおよび内容を変更して下さい。

オプション内容 2 にスクロールし、HTML ソースを『toggle』をクリックし、スクリプト内部を貼り付けて下さい:

```
<script> (function(){ jQuery('.cisco-ise-aup-text').hide(); jQuery('.cisco-ise-aup-controls').hide(); setTimeout(function(){ jQuery('#portal-session-timeout-popup-screen, #portal-session-timeout-popup-popup, #portal-session-timeout-popup').remove(); }, 100); })(); </script>
```

Untoggle HTML ソースをクリックして下さい。

### Optional Content 2

(text or HTML) Click Preview to test HTML rendering.

# 確認

設定が適切に機能することを確認するために、この項に記載する情報を活用してください。

## Firepower

起こる治療のためのトリガーは関連ポリシー/ルールのヒットです。分析 > 関連 > 関連イベントにナビゲートし、関連イベントが起こったことを確認して下さい。

Time	Impact	Inline Result	Source IP	Source Country	Destination IP	Destination Country	Security Intelligence Category	Source User	Destination User	Source Port / ICMP Type	Destination Port / ICMP Code
2017-02-16 13:27:51	Hit	Hit	172.16.10.19		192.168.0.121					8 (Echo Request) / icmp	0 / icmp

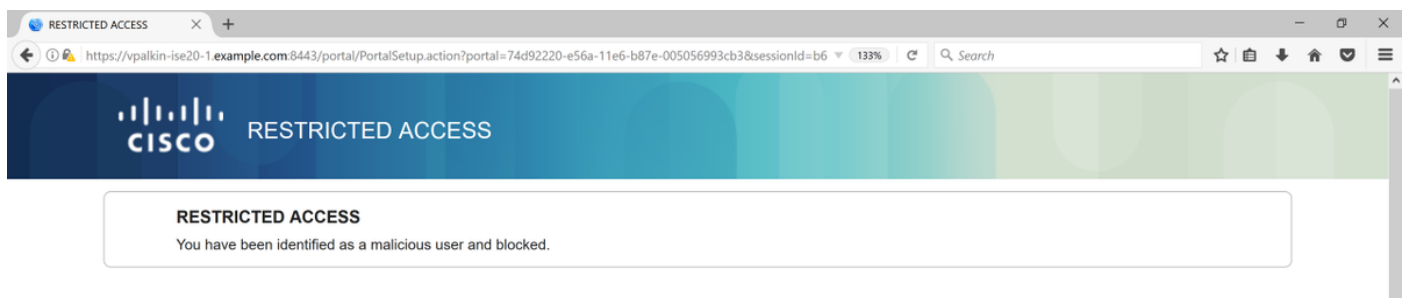
## ISE

ISE はそれから Radius を誘発する必要があります: CoA はユーザを、これらのイベント確認された作動中である場合もあります > RADIUS Livelog 再認証し。

2017-02-16 13:26:22.894	Success		alice	E4:B3:18:69:EB:8C	Windows10-Workst...	Default >> Dot1X >> D..	Default >> AssignSGT...	MaliciousUser,PermitAcc...	vWLC
2017-02-16 13:26:21.040	Success			E4:B3:18:69:EB:8C					vWLC
2017-02-16 13:25:29.036	Success		alice	E4:B3:18:69:EB:8C	Windows10-Workst...	Default >> Dot1X >> D..	Default >> Standard R...	PermitAccess,Administra...	vWLC

この例では、ISE はエンドポイントに異なる SGT MaliciousUser を割り当てました。拒否アクセス許可プロファイルの場合にはユーザは無線接続を失い、再度接続できません。

ブラックリスト ポータルとの治療。治療承認規則がポータルにリダイレクトするために設定される場合攻撃者観点からこのようになる必要があります:



## トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

このイメージに示すように分析 > 関連 > ステータスにナビゲートして下さい。



Time	Remediation Name	Policy	Rule	Result Message
2017-02-16 14:26:19	QUARANTINE-SOURCE	ise_correlation_policy	PingDC	Successful completion of remediation

結果メッセージは治療の正常な完了か特定のエラーメッセージを返す必要があります。syslogを確認して下さい: システム > モニタリング > Syslog およびフィルタは pxgrid と出力しました。同じログは /var/log/messages で確認することができます。

## 関連情報

- <https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200319-Troubleshoot-ISE-and-FirePOWER-Integrati.html>
- <https://communities.cisco.com/docs/DOC-68284>
- <https://communities.cisco.com/docs/DOC-68285>
- <https://communities.cisco.com/thread/64870?start=0&tstart=0>
- [http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin\\_guide/b\\_ise\\_admin\\_guide\\_20.html](http://www.cisco.com/c/en/us/td/docs/security/ise/2-0/admin_guide/b_ise_admin_guide_20.html)
- <http://www.cisco.com/c/en/us/td/docs/security/firepower/610/configuration/guide/fpmc-config-guide-v61.html>