

Configure Firepower 6.1 pxGrid Remediation with ISE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configure Firepower](#)

[Configure ISE](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes how to configure Firepower 6.1 pxGrid remediation with Identity Services Engine (ISE). Firepower 6.1+ ISE remediation module can be used with ISE Endpoint Protection Service (EPS) to automate quarantine/blacklisting of attackers on the network access layer.

Prerequisites

Requirements

Cisco recommends that you have basic knowledge of these topics:

- Cisco ISE
- Cisco Firepower

Components Used

The information in this document is based on these software and hardware versions:

- Cisco ISE version 2.0 Patch 4
- Cisco Firepower 6.1.0
- Virtual Wireless LAN Controller (vWLC) 8.3.102.0

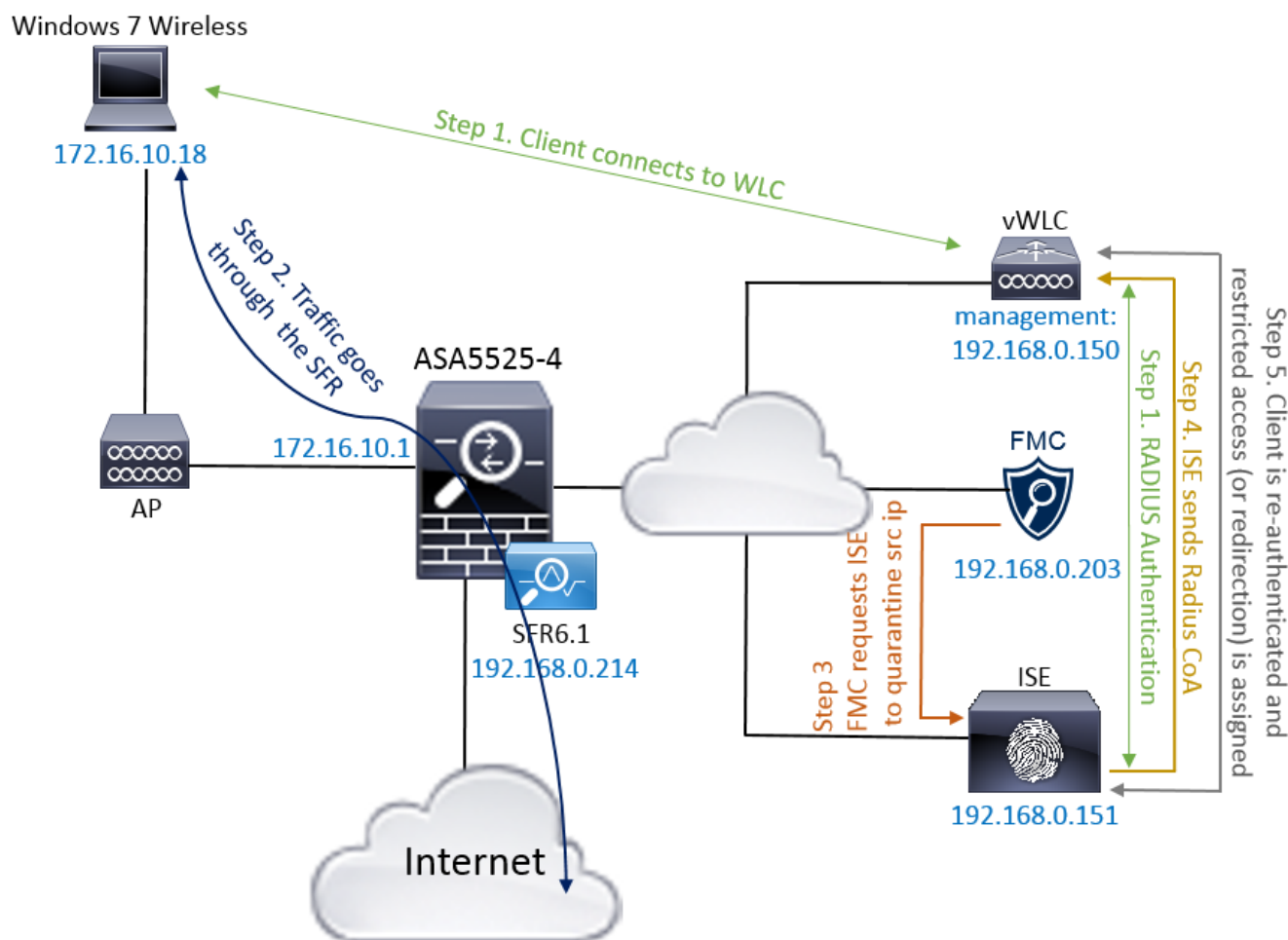
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

This article does not cover initial configuration of ISE integration with Firepower, ISE integration with Active Directory (AD), Firepower integration with AD. For this information navigate to references section. Firepower 6.1 Remediation module allows Firepower system to use ISE EPS capabilities (quarantine, unquarantine, port shutdown) as a remediation when correlation rule is matched.

Note: Port shutdown is not available for wireless deployments.

Network Diagram



The flow description:

1. A client connects to a network, authenticates with ISE and hits an authorization rule with an authorization profile which grants unrestricted access to the network.
2. Traffic from the client then flows through a Firepower device.
3. User starts to perform a malicious activity and hits a correlation rule which in turn triggers Firepower Management Center (FMC) to do ISE remediation via pxGrid.
4. ISE assigns a EPSStatus Quarantine to the endpoint and triggers RADIUS Change of Authorization to a network access device (WLC or Switch).
5. The client hits another authorization policy which assigns a restricted access (changes SGT or redirects to portal or denies access).

Note: Network Access Device (NAD) should be configured to send RADIUS Accounting to ISE in order to provide it with ip address information which is used to map ip address to an

endpoint.

Configure Firepower

Step 1. Configure a pxGrid Mitigation Instance.

Navigate to **Policies > Actions > Instances** and add pxGrid Mitigation Instance as shown in the image.

The screenshot shows the 'Edit Instance' dialog box in the Firepower management console. The dialog is titled 'Edit Instance' and contains the following fields:

- Instance Name:** ISE-NEW-INSTANCE
- Module:** pxGrid Mitigation(v1.0)
- Description:** (Empty text area)
- Enable Logging:** ☒ On ☐ Off

At the bottom of the dialog are two buttons: 'Create' and 'Cancel'.

Step 2. Configure a Remediation.

There are two types available: Mitigate Destination and Mitigate Source. In this example Source mitigation is used. Choose remediation type and click **Add** as shown in the image:

The screenshot shows the 'Configured Remediations' section in the Firepower management console. It features a table with the following headers:

Remediation Name	Remediation Type	Description
------------------	------------------	-------------

Below the table, it states 'No configured remediations available'. At the bottom, there is a form to 'Add a new remediation of type' with a dropdown menu showing 'Mitigate Destination' and 'Mitigate Source'. The 'Add' button is to the right of the dropdown.

Assign Mitigation Action to the Remediation as shown in the image:

Edit Remediation

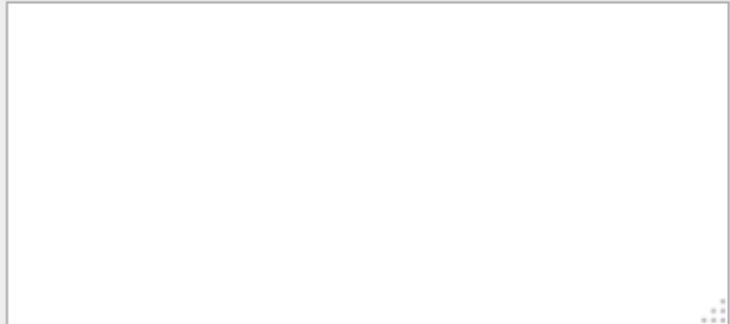
Remediation Name

QUARANTINE-SOURCE

Remediation Type

Mitigate Source

Description

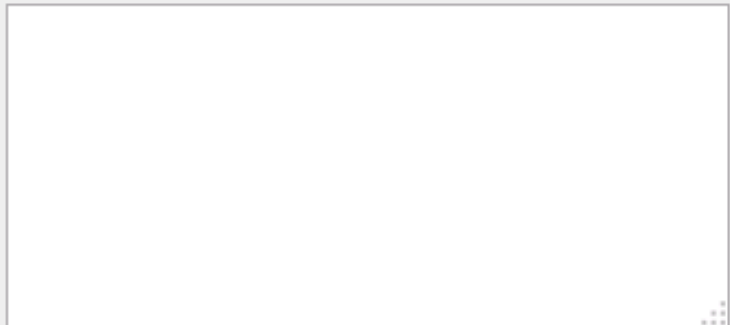


Mitigation Action

quarantine

Whitelist

(an *optional* list of networks)



Create

Cancel

Step 3. Configure a Correlation rule.

Navigate to **Policies > Correlation > Rule Management** and click **Create Rule** Correlation rule is the trigger for the remediation to happen. Correlation rule can contain several conditions. In this example Correlation Rule **PingDC** is hit if intrusion event occurs and destination ip address is 192.168.0.121. Custom intrusion rule matching icmp echo reply is configured for the purpose of the test as shown in the image:

Overview Analysis **Policies** Devices Objects AMP Deploy 2 System Help admin

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

Alerts Remediations Groups

Policy Management Rule Management White List Traffic Profiles

Rule Information

Rule Name: PingDC

Rule Description:

Rule Group: Ungrouped

Buttons: Add Connection Tracker Add User Qualification Add Host Profile Qualification

Select the type of event for this rule

If an intrusion event occurs and it meets the following conditions:

Buttons: Add condition Add complex condition

Condition: Destination IP is 192.168.0.121

Rule Options

Buttons: 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".

Step 4. Configure a Correlation policy.

Navigate to **Policies > Correlation > Policy Management** and click **Create Policy**, add rule to the policy and assign response to it as shown in the image:

Overview Analysis **Policies** Devices Objects AMP Deploy 1 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

Policy Name: ise_corellation_policy

Policy Description:

Default Priority: None

Buttons: Save Cancel

Policy Rules

Buttons: Add Rules

Rule	Responses	Priority
PingDC	QUARANTINE-SOURCE (Remediation)	Default

Enable the correlation policy as shown in the image:

Overview Analysis **Policies** Devices Objects AMP Deploy 1 System Help admin

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

Alerts Remediations Groups

Policy Management Rule Management White List Traffic Profiles

Buttons: Create Policy

Name	Sort by
ise_corellation_policy	State

Buttons: [Icons]

Configure ISE

Step 1. Configure Authorization Policy.

Navigate to **Policy > Authorization** and add a new authorization policy which will be hit after Remediation takes place. Use **Session: EPSStatus EQUALS Quarantine** as the condition. There are several options which can be used as a result:

- Permit Access and assign Different SGT (enforce access control restriction on network devices)
- Deny Access (user should be kicked out of the network and should not be able to connect again)
- Redirect to a **blacklist** portal (in this scenario custom hotspot portal is configured for this purpose)

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

First Matched Rule Applies

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

Custom Portal Configuration

In this example, the hotspot portal is configured as a **blacklist**. There is only an Acceptable Use Policy (AUP) page with custom text and there is no possibility to accept the AUP (this is done with JavaScript). In order to achieve this, you first need to enable JavaScript and then paste a code that hides AUP button and controls in portal customization configuration.

Step 1. Enable JavaScript.

Navigate to **Administration > System > Admin Access > Settings > Portal Customization**. Choose **Enable Portal Customization with HTML and JavaScript** and click **Save**.

Portal Customization

☐ Enable Portal Customization with HTML

☒ Enable Portal Customization with HTML and JavaScript

[Save](#)

Step 2. Create a Hotspot Portal.

Navigate to **Guest Access > Configure > Guest Portals** and click **Create**, then choose Hotspot type.

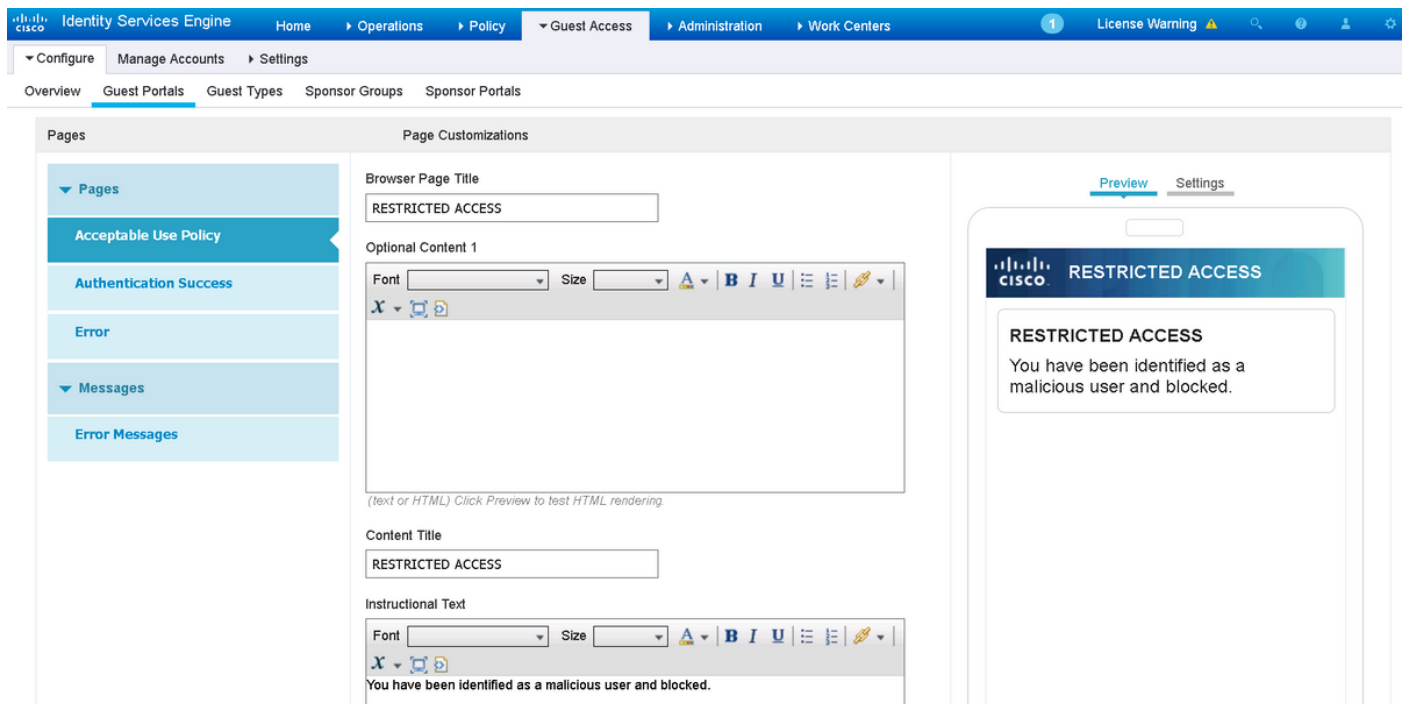
Guest Portals

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

[Create](#) [Edit](#) [Duplicate](#) [Delete](#)

Step 3. Configure Portal Customization.

Navigate to **Portal Page Customization** and change titles and content to provide an appropriate warning to the user.



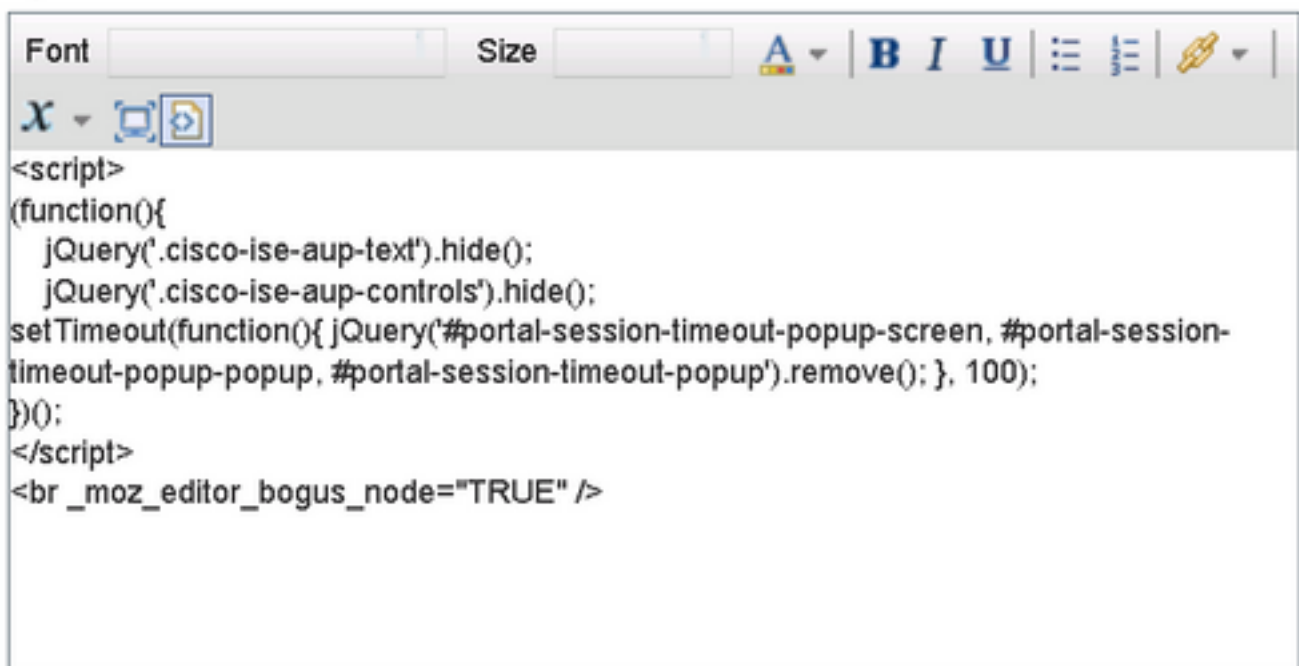
The screenshot shows the Cisco Identity Services Engine (ISE) Portal Page Customization interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. The 'Policy' section is expanded, showing 'Guest Access', 'Administration', and 'Work Centers'. The 'Guest Access' section is further expanded, showing 'Overview', 'Guest Portals', 'Guest Types', 'Sponsor Groups', and 'Sponsor Portals'. The 'Guest Portals' section is selected, and the 'Pages' tab is active. The 'Pages' section is expanded, showing 'Acceptable Use Policy', 'Authentication Success', 'Error', and 'Messages'. The 'Acceptable Use Policy' page is selected. The main area shows 'Page Customizations' for the 'Acceptable Use Policy' page. It includes fields for 'Browser Page Title' (RESTRICTED ACCESS), 'Optional Content 1' (with a rich text editor), 'Content Title' (RESTRICTED ACCESS), and 'Instructional Text' (with a rich text editor). A preview of the page is shown on the right, displaying the 'RESTRICTED ACCESS' warning message.

Scroll to **Option Content 2**, click **Toggle HTML Source**, and paste the script inside:

```
<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>
```

Click **Untoggle HTML Source**.

Optional Content 2



The screenshot shows the 'Optional Content 2' rich text editor. The editor has a toolbar with options for font, size, bold, italic, underline, list, and link. The main area displays the HTML source code for the content. The code is: `<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><br _moz_editor_bogus_node="TRUE" />`

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

Verify

Use the information that is provided in this section in order to verify that your configuration works properly.

Firepower

Trigger for the remediation to happen is a hit of correlation policy / rule. Navigate to **Analysis > Correlation > Correlation Events** and verify that correlation event happened.

Correlation Events

No Search Constraints (Edit Search)

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			172.16.10.19		192.168.0.121			8 (Echo Request) / icmp		0 / icmp	

ISE

ISE should then trigger Radius: CoA and re-authenticate the user, these events can be verified in **Operation > RADIUS LiveLog**.

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

In this example, ISE assigned different SGT **MaliciousUser** to the endpoint. In the case of **Deny Access** authorization profile the user loses wireless connection and is not able to connect again.

The remediation with blacklist portal. If remediation authorization rule is configured to redirect to the portal, it should look like this from the attacker perspective:

RESTRICTED ACCESS

You have been identified as a malicious user and blocked.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Navigate to **Analysis > Correlation > Status** as shown in this image.

Overview

Analysis

Policies

Devices

Objects

AMP

Deploy

System

Help

admin

Context Explorer

Connections

Intrusions

Files

Hosts

Users

Vulnerabilities

Correlation > Status

Custom

Lookup

Search

Bookmark This Page

Report Designer

View Bookmarks

Search

Remediation Status

Table View of Remediations

2017-02-16 14:25:00 - 2017-02-16 14:27:00

Static

No Search Constraints (Edit Search)

Jump to...

	Time	Remediation Name	Policy	Rule	Result Message
<input type="checkbox"/>	2017-02-16 14:26:19	QUARANTINE-SOURCE	ise_correlation_policy	PingDC	Successful completion of remediation

<< Page 1 of 1 >>

Displaying row 1 of 1 rows

View

Delete

View All

Delete All

Result message should return either **Successful completion of remediation** or particular error message. Verify syslog: **System > Monitoring > Syslog** and filter output with **pxgrid**. The same logs can be verified in **/var/log/messages**.

Related Information

- <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/firepower/610/configuration/guide/fpmc-config-guide-v61.html>