使用ISE配置Firepower 6.1 pxGrid補救

目錄

簡介

本文檔介紹如何使用身份服務引擎(ISE)配置Firepower 6.1 pxGrid補救。 Firepower 6.1+ ISE補救模組可與ISE端點保護服務(EPS)配合使用，自動在網路訪問層對攻擊者進行排隊/黑名單。

必要條件

需求

思科建議您瞭解以下主題的基本知識：

- Cisco ISE
- Cisco Firepower

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本2.0補丁4
- Cisco Firepower 6.1.0
- 虛擬無線LAN控制器(vWLC)8.3.102.0

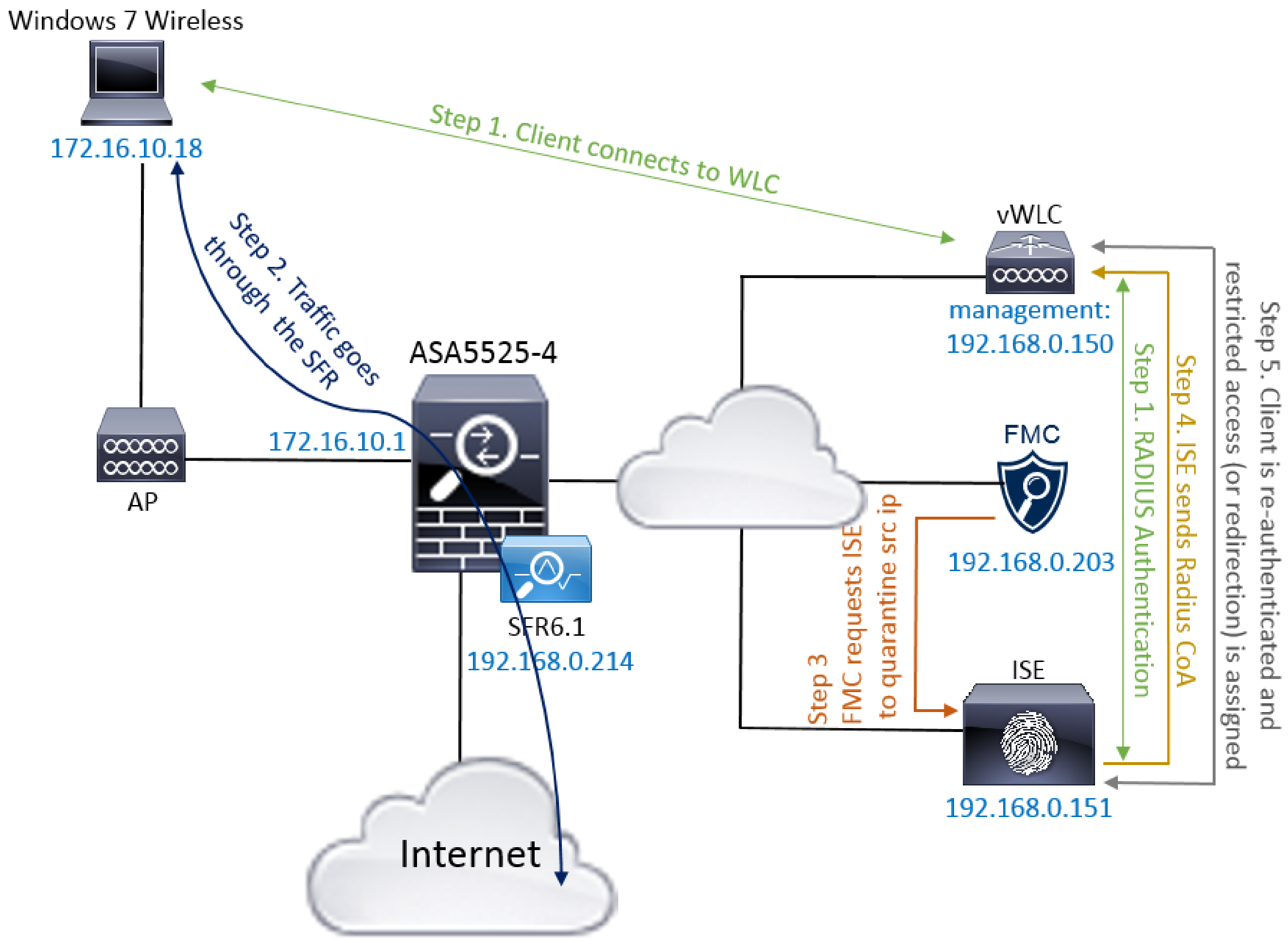
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

本文不涉及ISE與Firepower整合的初始配置、ISE與Active Directory(AD)的整合、Firepower與AD的整合。有關此資訊，請導航到參考部分。Firepower 6.1補救模組允許Firepower系統在匹配關聯規則時使用ISE EPS功能（隔離、取消隔離、埠關閉）作為補救。

附註：埠關閉不可用於無線部署。

網路圖表


Windows 7 Wireless
172.16.10.18
Step 1. Client connects to WLC
Step 2. Traffic goes through the SFR
AP
172.16.10.1
ASA5525-4
SFR6.1
192.168.0.214
Internet
vWLC
management:
192.168.0.150
FMC
192.168.0.203
ISE
192.168.0.151
Step 3 FMC requests ISE to quarantine src ip
Step 1. RADIUS Authentication
Step 4. ISE sends Radius CoA
Step 5. Client is re-authenticated and restricted access (or redirection) is assigned

流說明：

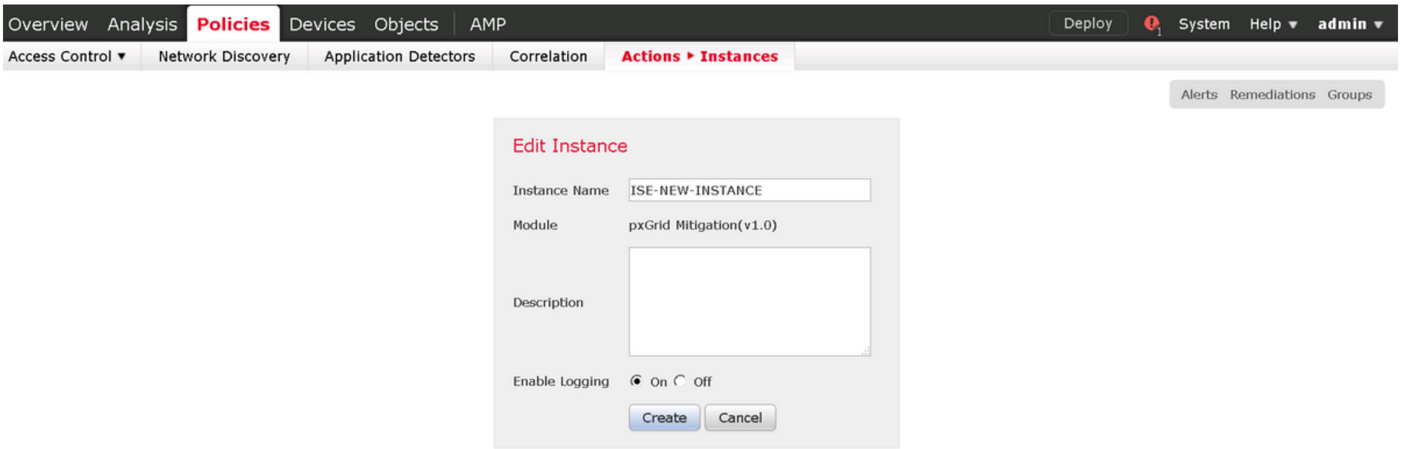
1. 客戶端連線到網路，使用ISE進行身份驗證並使用授權配置檔案訪問授權規則，授權配置檔案授予對網路的無限制訪問許可權。
2. 來自客戶端的流量隨後通過Firepower裝置。
3. 使用者開始執行惡意活動並點選關聯規則，該規則進而觸發Firepower管理中心(FMC)通過pxGrid執行ISE補救。
4. ISE將EPSSstatus Quarantine分配給終端並觸發RADIUS授權更改到網路接入裝置（WLC或交換機）。
5. 客戶端點選另一個授權策略，該策略分配受限訪問（更改SGT或重定向到門戶或拒絕訪問）。

附註：網路接入裝置(NAD)應配置為向ISE傳送RADIUS記帳，以便為其提供用於將IP地址對映到終端的IP地址資訊。

配置Firepower

步驟1.配置pxGrid緩解例項。

導覽至**Policies > Actions > Instances**，然後新增pxGrid緩解例項，如下圖所示。



Edit Instance

Instance Name: ISE-NEW-INSTANCE

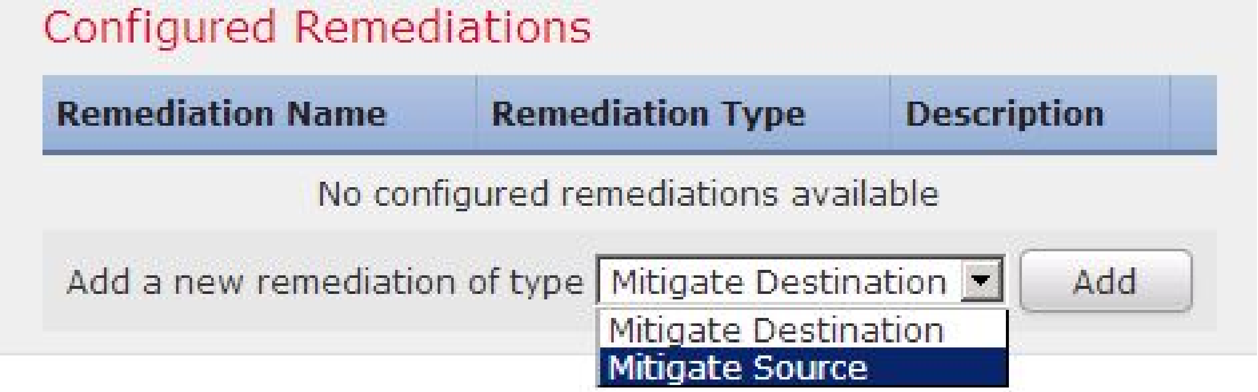
Module: pxGrid Mitigation(v1.0)

Description:

Enable Logging: ● On ○ Off

步驟2.配置補救。

有兩種型別可用：緩解目的地和緩解源。在此示例中，使用源緩解。選擇修正型別，然後按一下**Add**，如下圖所示：

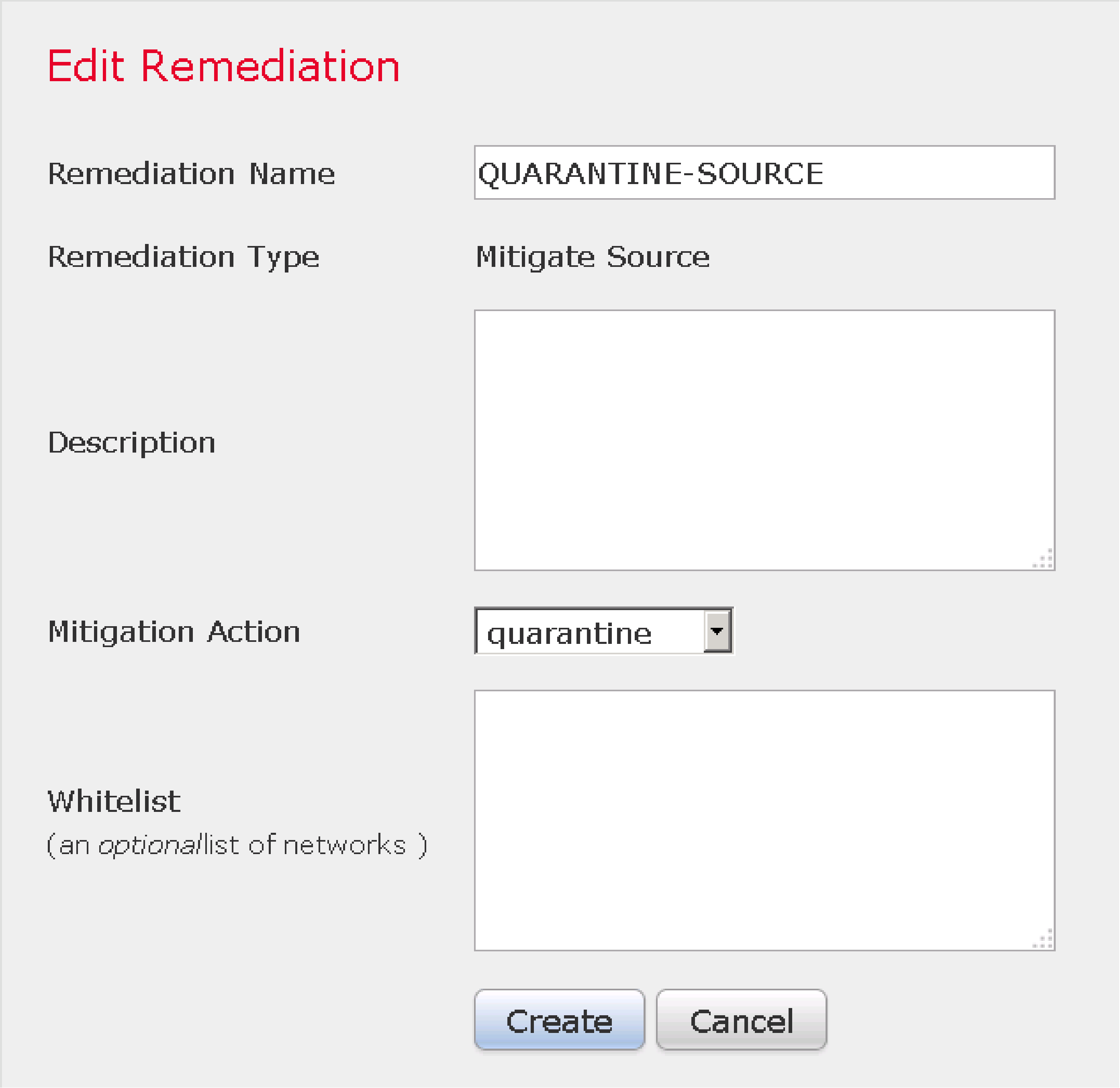


Configured Remediations

Remediation Name	Remediation Type	Description
No configured remediations available		

Add a new remediation of type: Mitigate Destination ▾

將緩解操作分配給補救，如下圖所示：

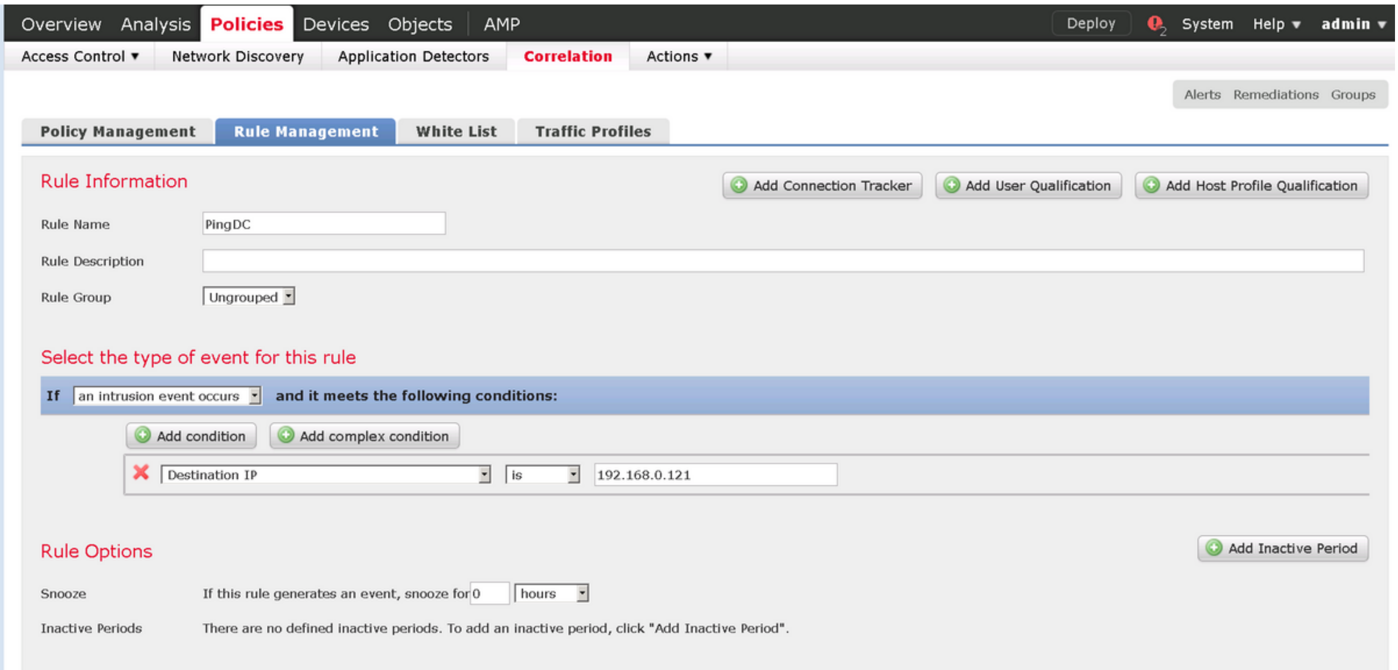


Edit Remediation

Remediation Name	QUARANTINE-SOURCE
Remediation Type	Mitigate Source
Description	
Mitigation Action	quarantine
Whitelist (an *optional*list of networks)	

步驟3.配置關聯規則。

導航到**Policies > Correlation > Rule Management**，然後按一下**Create Rule** Correlation rule是進行補救的觸發器。關聯規則可以包含多個條件。在此範例中，如果發生入侵事件，且目的地IP位址為192.168.0.121，則會命中Correlation Rule **PingDC**。為了測試的目的，已設定與icmp回應回覆相符的自訂入侵規則，如下圖所示：



Rule Information

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:

Destination IP is 192.168.0.121

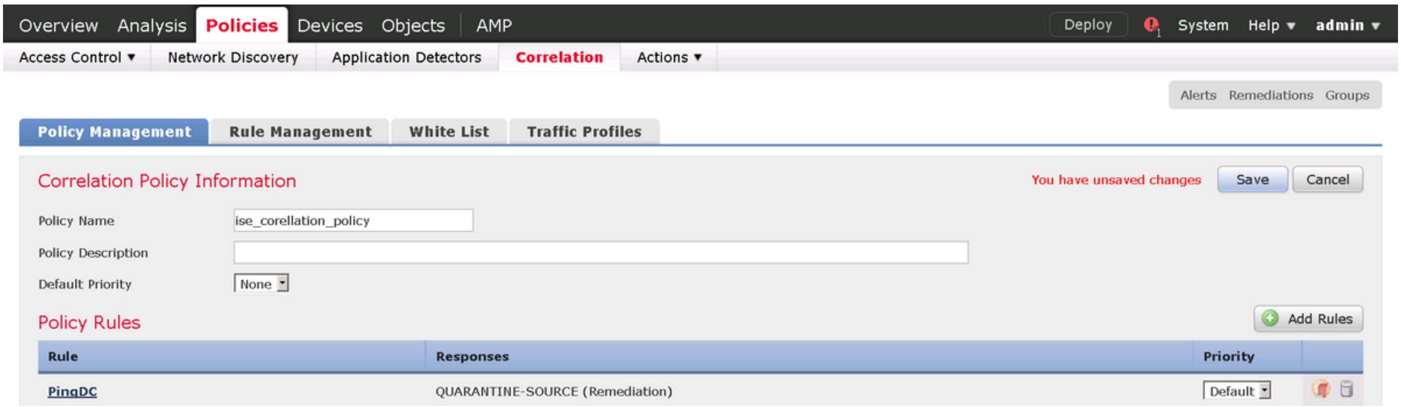
Rule Options

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".

步驟4.配置關聯策略。

導覽至**Policies > Correlation > Policy Management**，然後按一下**Create Policy**，將規則新增到策略並分配策略的響應，如下圖所示：



Correlation Policy Information

Policy Name: ise_corellation_policy

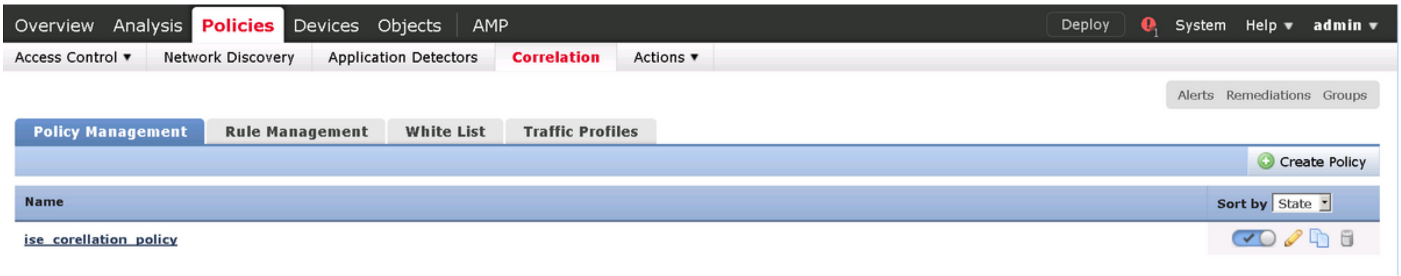
Policy Description:

Default Priority: None

Policy Rules

Rule	Responses	Priority
PingDC	QUARANTINE-SOURCE (Remediation)	Default

啟用關聯策略，如下圖所示：



Name
ise_corellation_policy

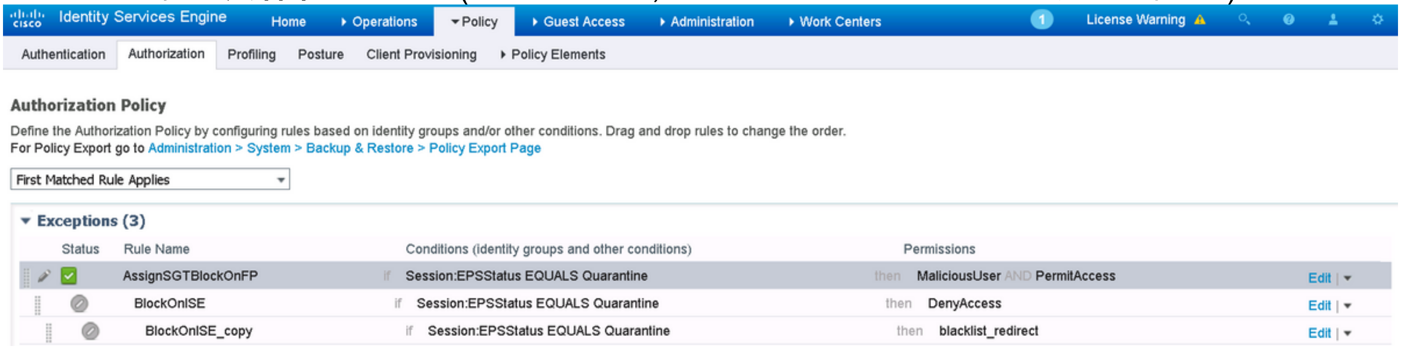
配置ISE

步驟1.配置授權策略。

導航到**Policy > Authorization**，然後新增新的授權策略，該策略將在補救發生後命中。使用**Session:EPSStatus等於Quarantine**作為條件。因此可使用多個選項：

- 允許訪問並分配不同的SGT（在網路裝置上實施訪問控制限制）

- 拒絕訪問（使用者應該被踢出網路，不能再次連線）
- 重新導向至**黑名單**入口網站（在此案例中，自定義熱點入口網站是為此用途配置的）



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

Exceptions (3)

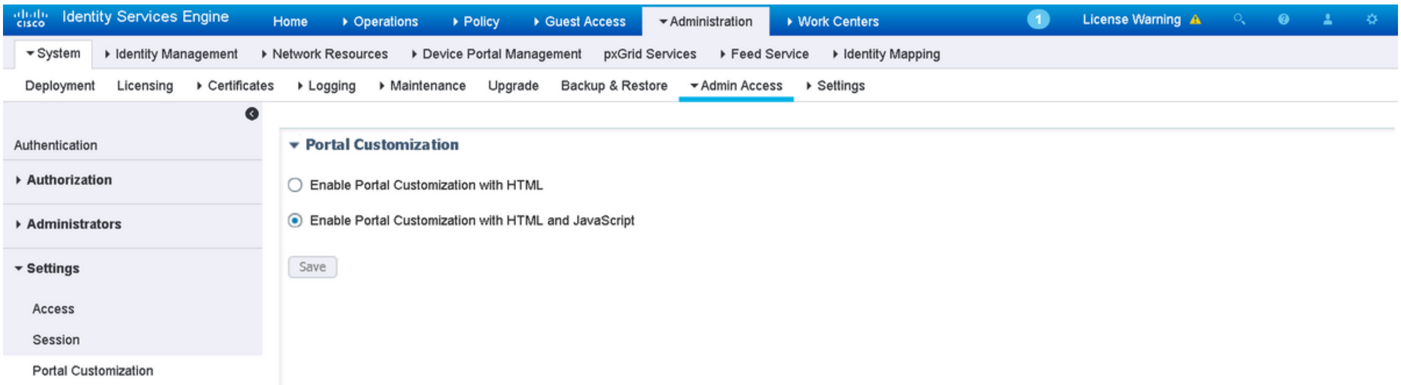
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	AssignSGTBlockOnFP	if	Session:EPSStatus EQUALS Quarantine	then	MaliciousUser AND PermitAccess	Edit | ▾
⊘	BlockOnISE	if	Session:EPSStatus EQUALS Quarantine	then	DenyAccess	Edit | ▾
⊘	BlockOnISE_copy	if	Session:EPSStatus EQUALS Quarantine	then	blacklist_redirect	Edit | ▾

自定義門戶配置

在本示例中，熱點門戶配置為**黑名單**。只有包含自定義文本的「可接受使用策略」(AUP)頁，並且不可能接受AUP（這通過JavaScript完成）。 為此，首先需要啟用JavaScript，然後貼上一個在門戶自定義配置中隱藏AUP按鈕和控制元件的代碼。

步驟1.啟用JavaScript。

導航到**Administration > System > Admin Access> Settings > Portal Customization。選擇Enable Portal Customization with HTML and JavaScript**，然後按一下**Save**。



Portal Customization

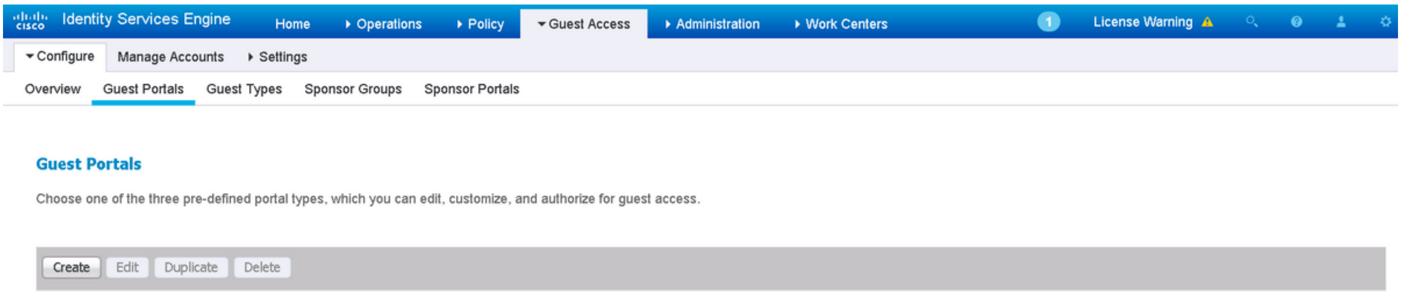
○ Enable Portal Customization with HTML

● Enable Portal Customization with HTML and JavaScript

Save

步驟2.建立熱點門戶。

導覽至**Guest Access > Configure > Guest Portals**，然後按一下**Create**，然後選擇熱點型別。

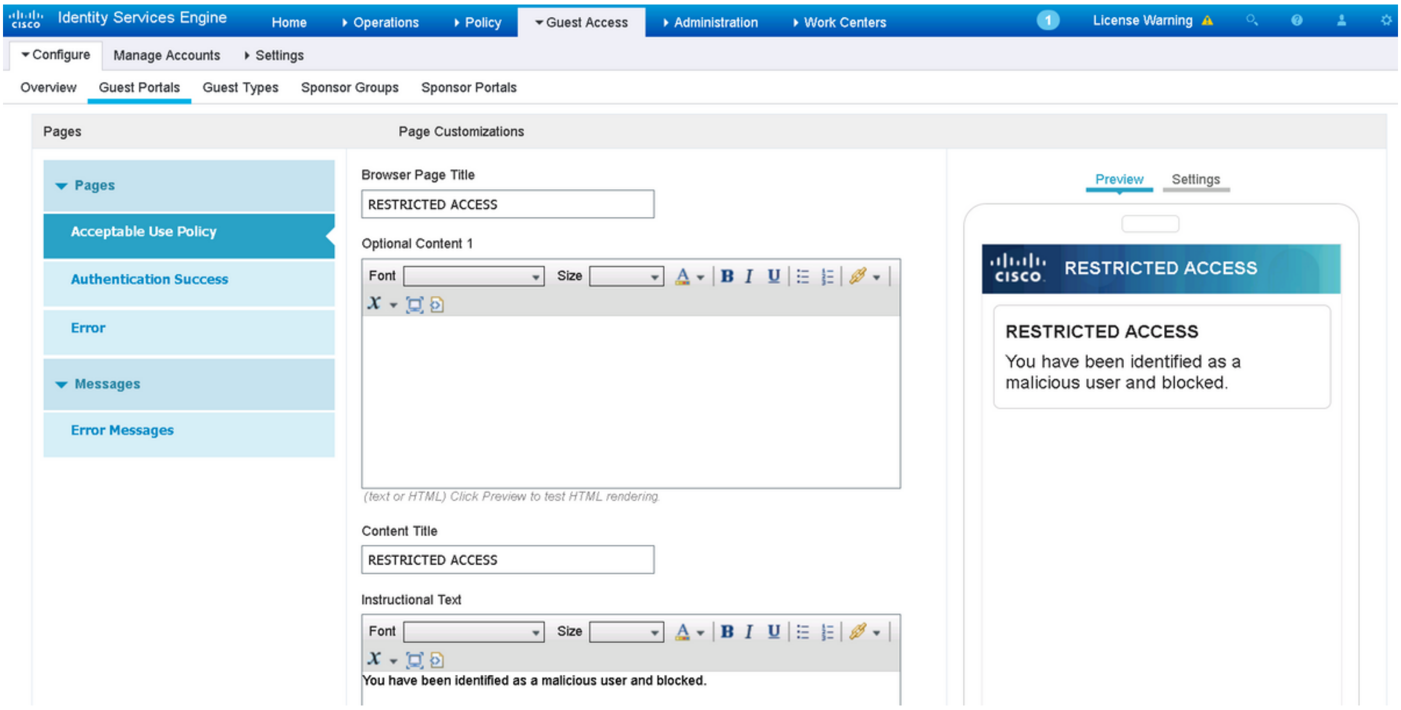


Guest Portals

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

步驟3.配置門戶自定義。

導航到**門戶頁面自定義**並更改標題和內容，為使用者提供適當的警告。



Browser Page Title: RESTRICTED ACCESS

Optional Content 1

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

Content Title: RESTRICTED ACCESS

Instructional Text: You have been identified as a malicious user and blocked.

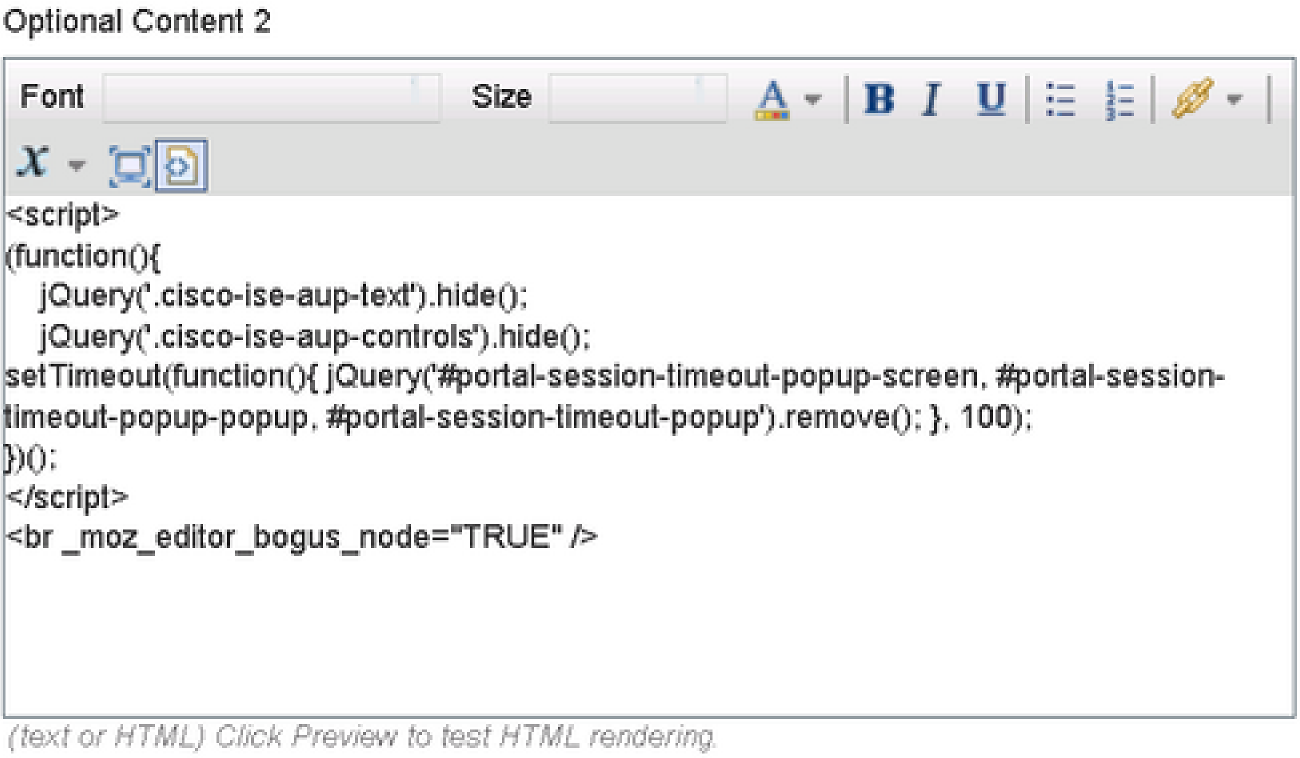
RESTRICTED ACCESS

RESTRICTED ACCESS

You have been identified as a malicious user and blocked.

滾動到**選項內容2**，按一下**切換HTML源**，然後將指令碼貼上到內部：

按一下**取消切換HTML源。**



Optional Content 2

```
<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" />
```

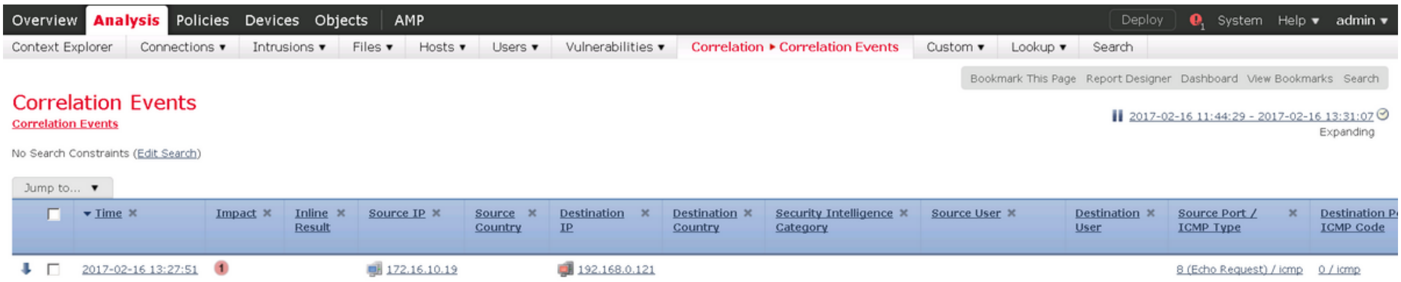
(text or HTML) Click Preview to test HTML rendering.

驗證

使用本節提供的資訊以驗證您的組態是否正常運作。

Firepower

觸發補救的是關聯策略/規則的命中。導覽至Analysis > Correlation > Correlation Events，然後驗證是否已發生關聯事件。



Correlation Events

Correlation Events

2017-02-16 11:44:29 - 2017-02-16 13:31:07

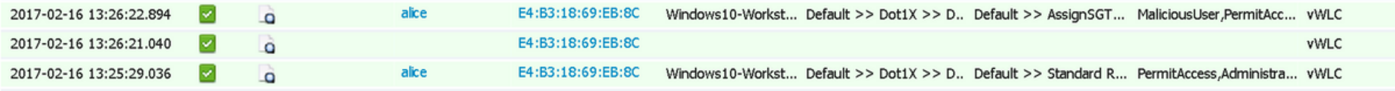
Expanding

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 P… ICMP Code
⬇	☐	2017-02-16 13:27:51	1		172.16.10.19		192.168.0.121					8 (Echo Request) / icmp	0 / icmp

ISE

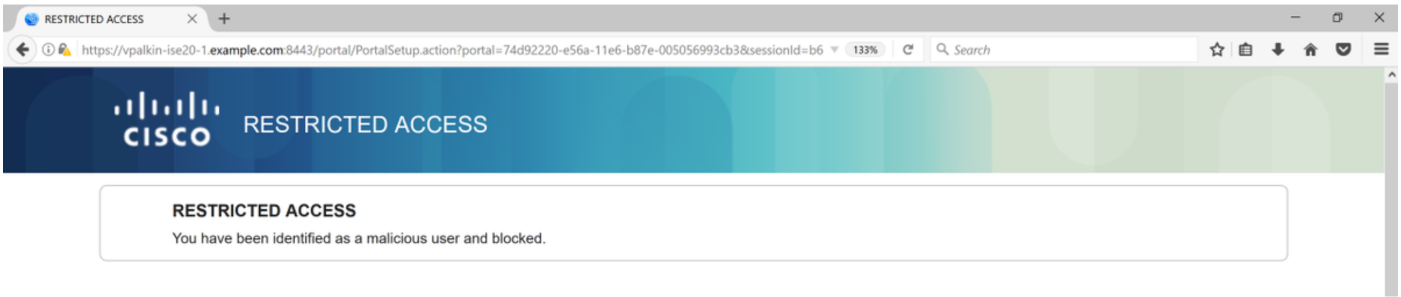
然後ISE應觸發Radius:CoA並重新驗證使用者，可以在**操作> RADIUS即時日誌**中驗證這些事件。



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

在本示例中，ISE為終端分配**了不**同的SGT MaliciousUser。在**Deny Access** authorization profile的情況下，使用者會丟失無線連線，並且無法再次連線。

使用黑名單門戶進行補救。如果補救授權規則配置為重定向到門戶，則從攻擊者的角度應如下所示：



RESTRICTED ACCESS
https://vpalkin-ise20-1.example.com:8443/portal/PortalSetup.action?portal=74d92220-e56a-11e6-b87e-005056993cb3&sessionId=b6
133%
Search
cisco
RESTRICTED ACCESS

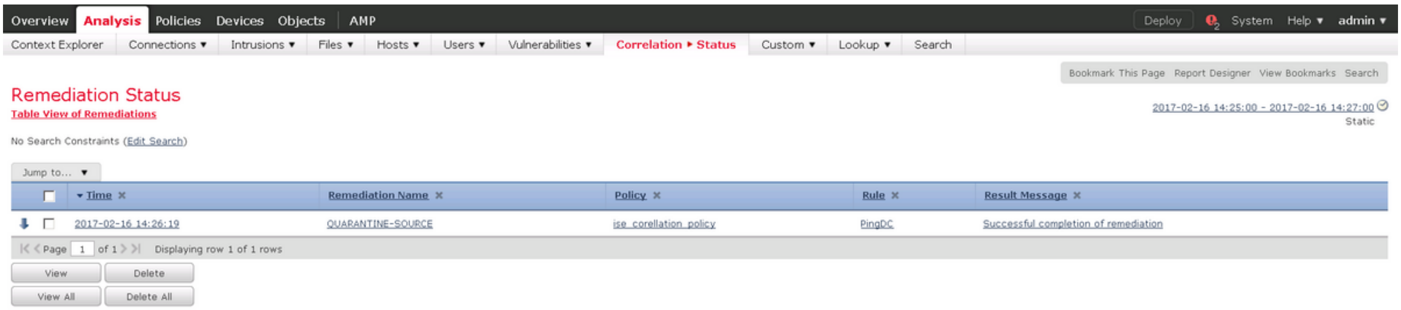
RESTRICTED ACCESS

You have been identified as a malicious user and blocked.

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

導覽至**Analysis > Correlation > Status**，如下圖所示。



Remediation Status

Table View of Remediations

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

Static

No Search Constraints (Edit Search)

	☐	Time	Remediation Name	Policy	Rule	Result Message
⬇	☐	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

結果消息應返回**Successful complete of remediation**或特定錯誤消息。驗證系統日誌：**System > Monitoring > Syslog**並使用pxgrid過濾**輸出**。可在**/var/log/messages中驗證相同的日誌。**

相關資訊

- 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