

Configurazione di Firepower 6.1 pxGrid Remediation con ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurare Firepower](#)

[Configurare ISE](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare il monitoraggio e l'aggiornamento di Firepower 6.1 pxGrid con Identity Services Engine (ISE). Il modulo di correzione ISE Firepower 6.1+ può essere utilizzato con ISE Endpoint Protection Service (EPS) per automatizzare la quarantena o la creazione di una blacklist degli aggressori sul layer di accesso alla rete.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Cisco ISE
- Cisco Firepower

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Patch 4 per Cisco ISE versione 2.0
- Cisco Firepower 6.1.0
- Controller LAN wireless virtuale (vWLC) 8.3.102.0

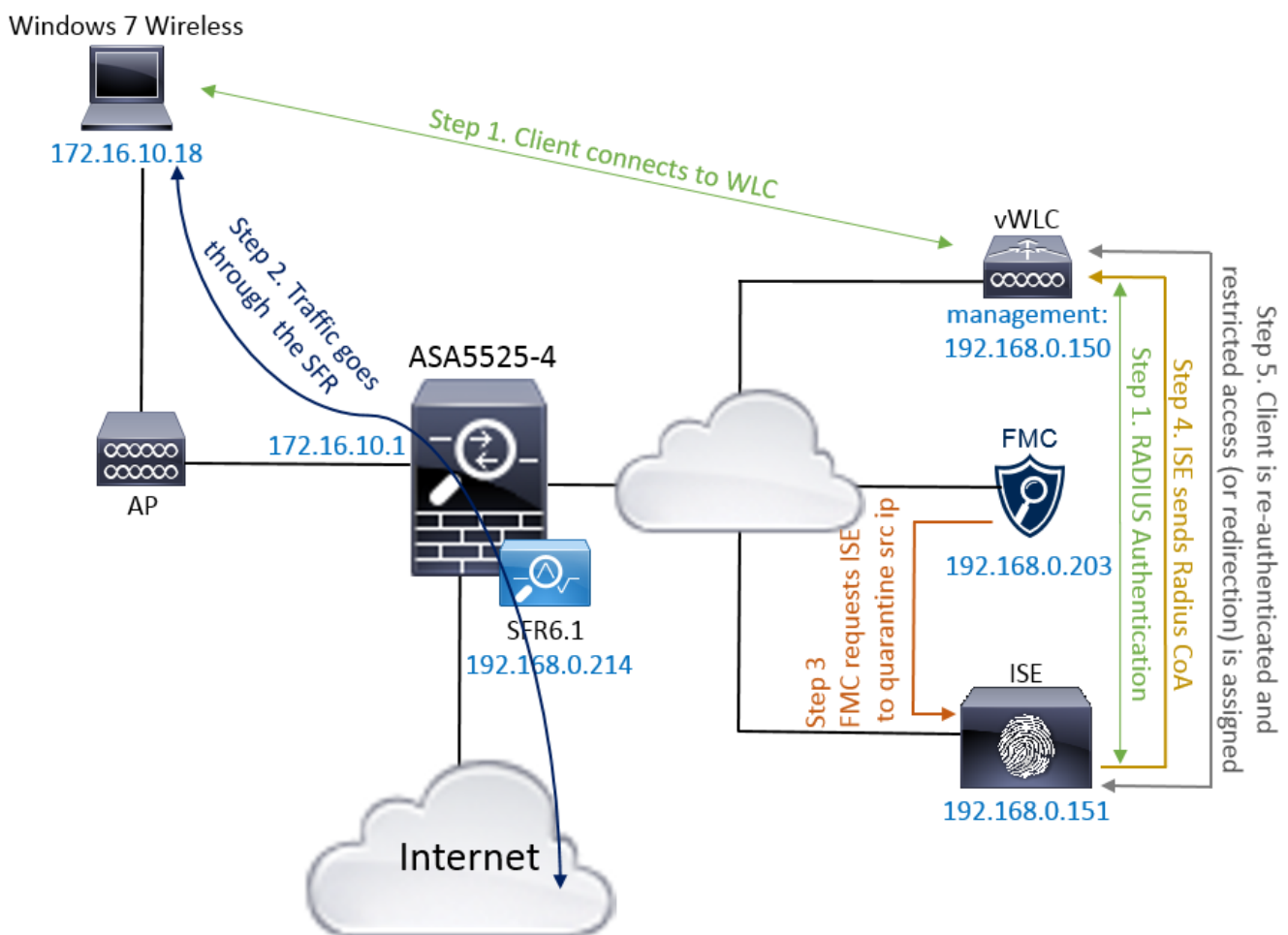
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questo articolo non viene trattata la configurazione iniziale dell'integrazione di ISE con Firepower, l'integrazione di ISE con Active Directory (AD) e l'integrazione di Firepower con AD. Per queste informazioni, passare alla sezione dei riferimenti. Il modulo di monitoraggio e aggiornamento di Firepower 6.1 consente al sistema Firepower di utilizzare le funzionalità EPS di ISE (quarantena, rimozione della quarantena, chiusura della porta) come monitoraggio e aggiornamento quando viene rispettata la regola di correlazione.

Nota: L'arresto della porta non è disponibile per le distribuzioni wireless.

Esempio di rete



Descrizione del flusso:

1. Un client si connette a una rete, esegue l'autenticazione con ISE e rileva una regola di autorizzazione con un profilo di autorizzazione che concede l'accesso illimitato alla rete.
2. Il traffico proveniente dal client passa quindi attraverso un dispositivo Firepower.
3. L'utente inizia a eseguire un'attività dannosa e incontra una regola di correlazione che a sua volta attiva Firepower Management Center (FMC) per eseguire il monitoraggio e l'aggiornamento di ISE tramite pxGrid.
4. ISE assegna una quarantena EPSStatus all'endpoint e attiva la modifica di autorizzazione

RADIUS a un dispositivo di accesso alla rete (WLC o switch).

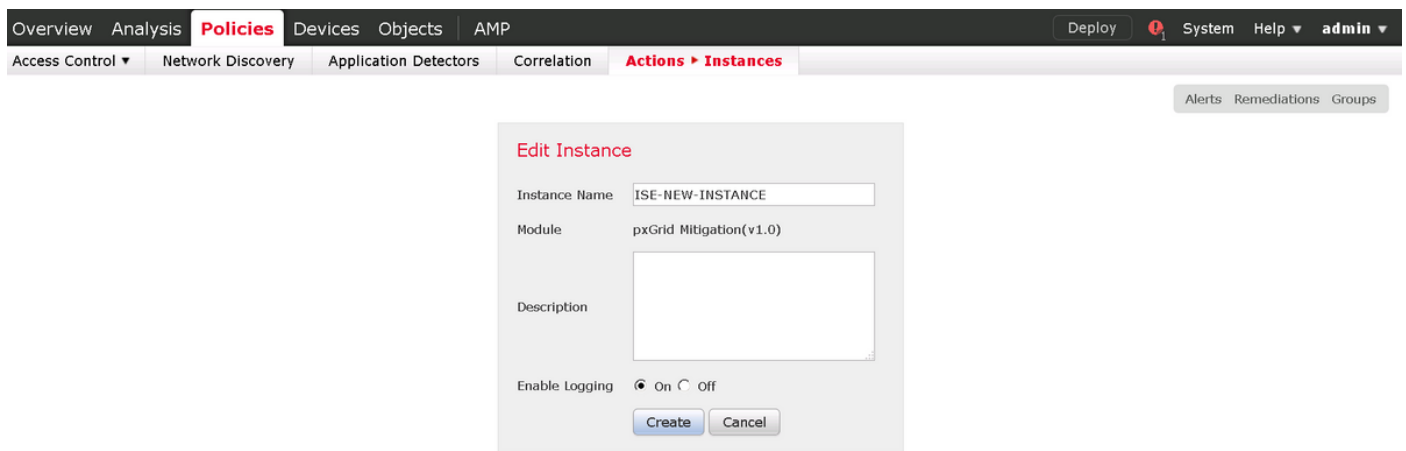
5. Il client ha riscontrato un altro criterio di autorizzazione che assegna un accesso limitato (modifica il protocollo SGT o reindirizza al portale o nega l'accesso).

Nota: Il dispositivo NAD (Network Access Device) deve essere configurato per inviare l'accounting RADIUS ad ISE in modo da fornire informazioni sull'indirizzo IP da utilizzare per mappare l'indirizzo IP a un endpoint.

Configurare Firepower

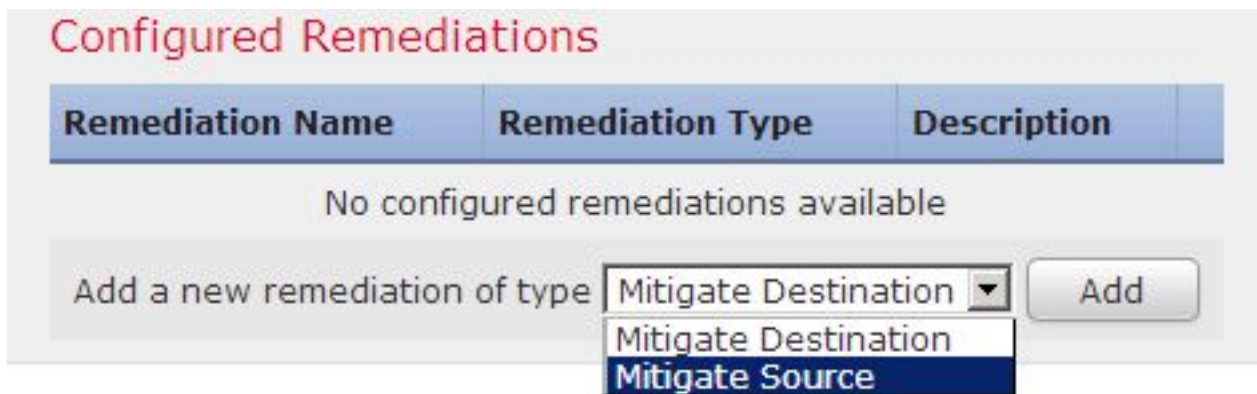
Passaggio 1. Configurare un'istanza di mitigazione pxGrid.

Passare a **Criteri > Azioni > Istanze** e aggiungere l'istanza di mitigazione pxGrid come mostrato nell'immagine.



Passaggio 2. Configurare una risoluzione.

Sono disponibili due tipi: Mitiga destinazione e Mitiga origine. In questo esempio viene utilizzata la mitigazione dell'origine. Scegliere il tipo di monitoraggio e aggiornamento e fare clic su **Aggiungi**, come mostrato nell'immagine:



Assegnare l'azione di mitigazione al rimedio come mostrato nell'immagine:

Edit Remediation

Remediation Name

QUARANTINE-SOURCE

Remediation Type

Mitigate Source

Description

Mitigation Action

quarantine

Whitelist

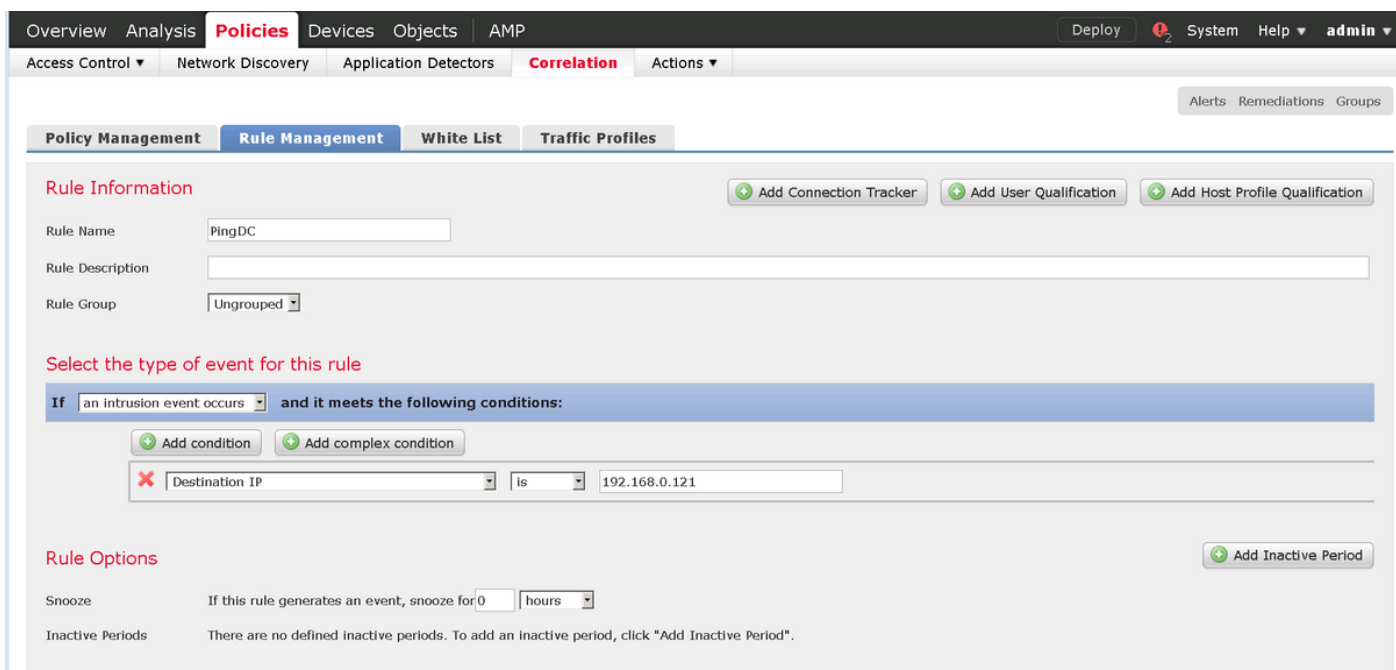
(an optional list of networks)

Create

Cancel

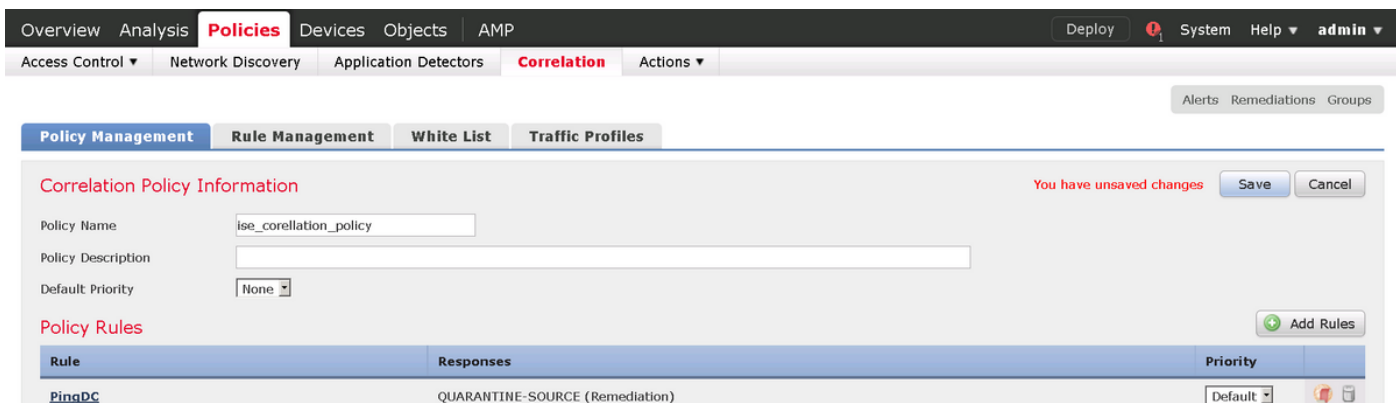
Passaggio 3. Configurare una regola di correlazione.

Passare a **Criteri > Correlazione > Gestione regole** e fare clic su **Crea regola di correlazione** è il trigger per la correzione da eseguire. La regola di correlazione può contenere diverse condizioni. Nell'esempio, la regola di correlazione **PingDC** viene trovata se si verifica un evento di intrusione e l'indirizzo IP di destinazione è 192.168.0.121. La regola di intrusione personalizzata che corrisponde alla risposta echo icmp è configurata per lo scopo del test, come mostrato nell'immagine:

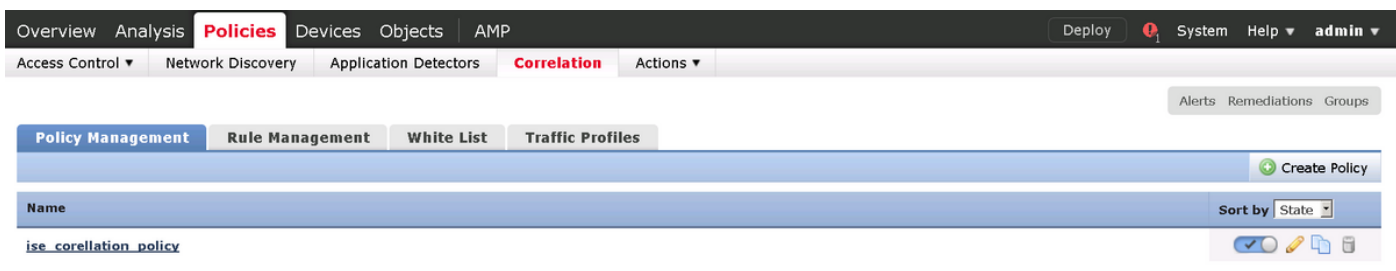


Passaggio 4. Configurare un criterio di correlazione.

Passare a **Criteri > Correlazione > Gestione criteri** e fare clic su **Crea criterio**, aggiungere la regola al criterio e assegnare la risposta come mostrato nell'immagine:



Abilitare il criterio di correlazione come mostrato nell'immagine:



Configurare ISE

Passaggio 1. Configurare i criteri di autorizzazione.

Passare a **Criterio > Autorizzazione** e aggiungere un nuovo criterio di autorizzazione che verrà attivato dopo l'esecuzione del monitoraggio e aggiornamento. Usa **sessione: EPSStatus** **equivale a Quarantena** come condizione. Di conseguenza è possibile utilizzare diverse opzioni:

- Consenti accesso e assegna SGT diverso (applica la restrizione del controllo di accesso ai dispositivi di rete)
- Nega accesso (l'utente deve essere escluso dalla rete e non deve essere in grado di riconnettersi)
- Reindirizzare a un portale di **blacklist** (in questo scenario il portale di hotspot personalizzato è configurato a questo scopo)

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

Configurazione personalizzata del portale

In questo esempio, il portale degli hotspot è configurato come **lista nera**. Esiste solo una pagina Acceptable Use Policy (AUP) con testo personalizzato e non è possibile accettare l'AUP (questa operazione viene eseguita con JavaScript). A tale scopo, è innanzitutto necessario attivare JavaScript e quindi incollare un codice che nasconda i pulsanti e i controlli AUP nella configurazione di personalizzazione del portale.

Passaggio 1. Abilitare JavaScript.

Selezionare **Amministrazione > Sistema > Accesso amministratore > Impostazioni > Personalizzazione portale**. Scegliere **Abilita personalizzazione portale con HTML e JavaScript** e fare clic su **Salva**.

Administration > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Identity Mapping

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore **Admin Access** Settings

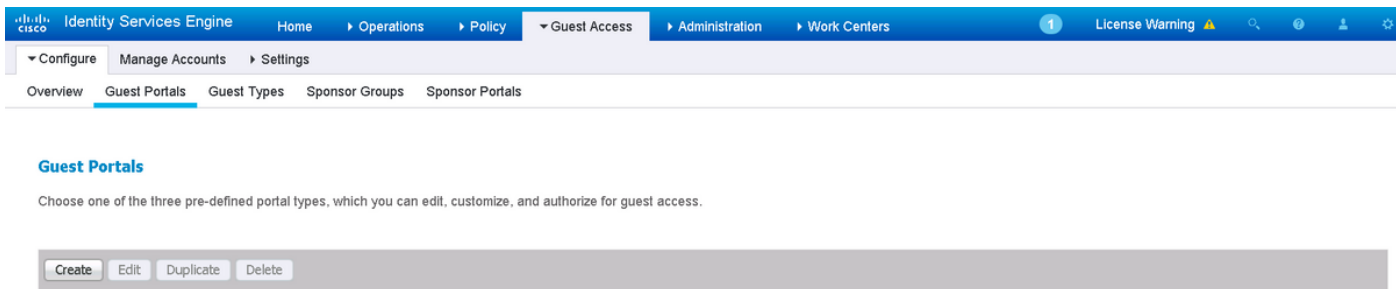
Portal Customization

Enable Portal Customization with HTML

Enable Portal Customization with HTML and JavaScript

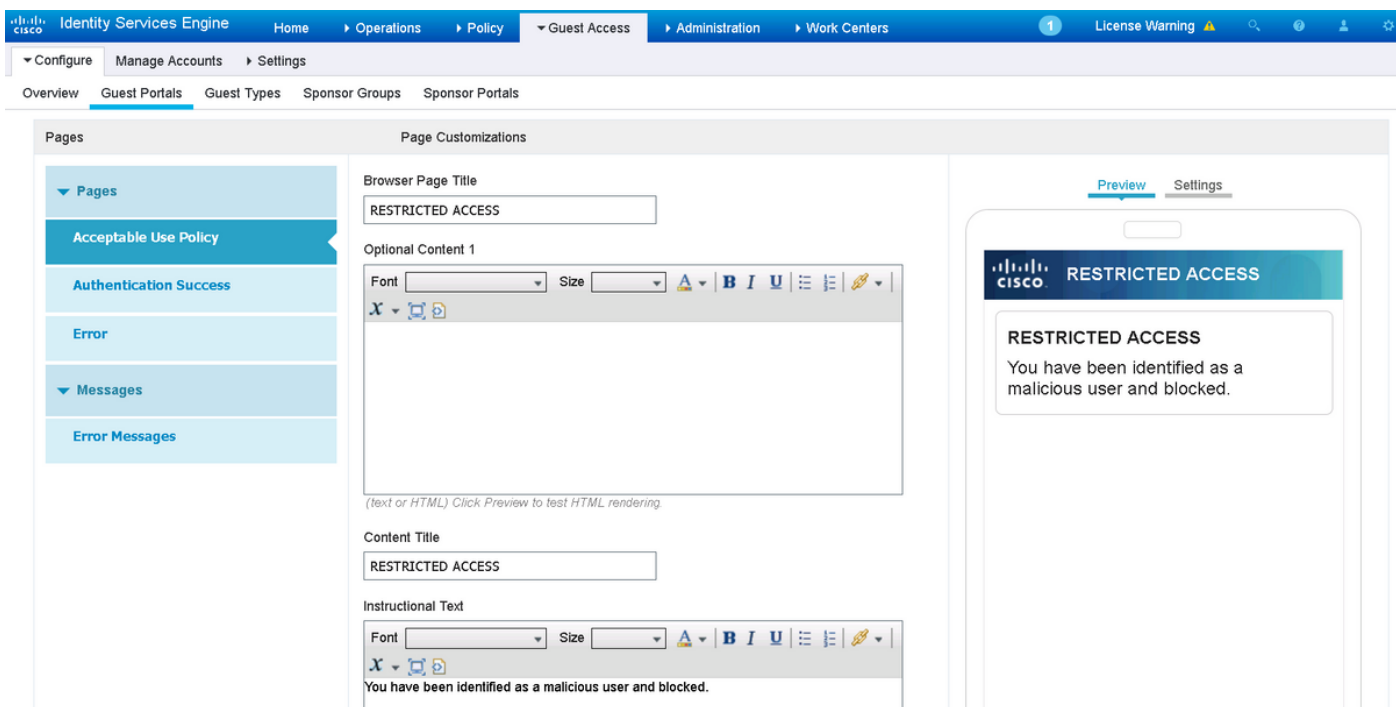
Passaggio 2. Creare un portale hotspot.

Passare a **Accesso guest > Configura > Portali guest** e fare clic su **Crea**, quindi scegliere il tipo di hotspot.



Passaggio 3. Configurare la personalizzazione del portale.

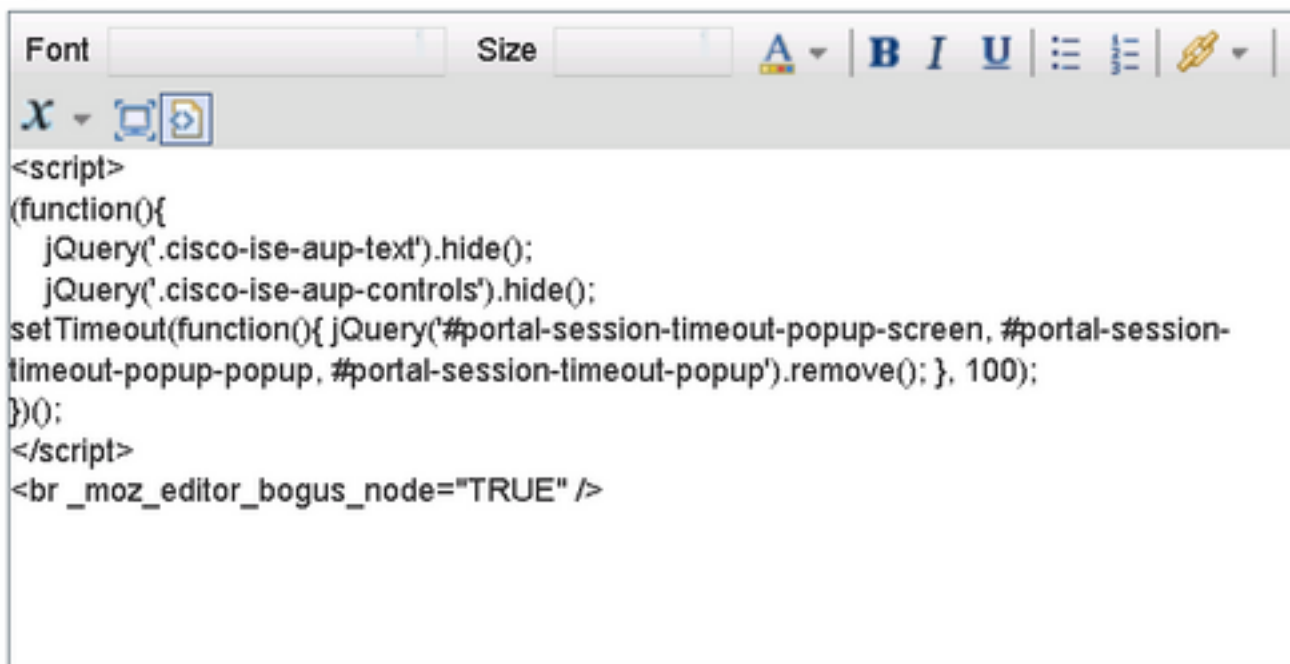
Passare a **Personalizzazione pagina portale** e modificare i titoli e il contenuto per inviare un messaggio di avviso appropriato all'utente.



Scorrere fino a **Contenuto opzione 2**, fare clic su **Attiva/disattiva origine HTML** e incollare lo script all'interno:

Fare clic su **Disattiva origine HTML**.

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.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare le informazioni contenute in questa sezione.

Firepower


Il trigger per il rimedio da realizzare è un colpo di correlazione politica / regola. Passare ad **Analisi > Correlazione > Eventi di correlazione** e verificare che si sia verificato un evento di correlazione.



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 13:26:22.894	✓	🔒	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		

ISE

ISE deve quindi attivare Radius: CoA e riautenticare l'utente, questi eventi possono essere verificati in **Operazione > RADIUS LiveLog**.

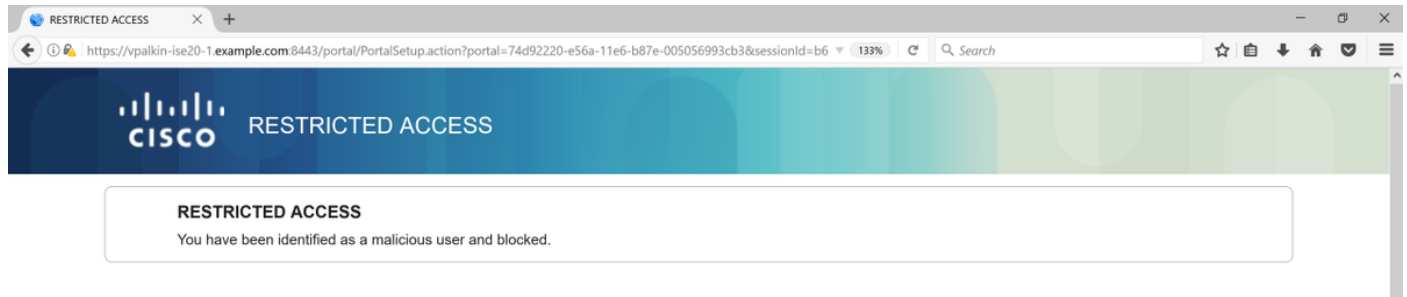


Time	Source IP	Destination IP	Source User	Destination User	Source Port	Destination Port	Source Country	Destination Country	Source Port / ICMP Type	Destination Port / ICMP Code
2017-02-16 13:26:22.894	172.16.10.19	192.168.0.121	alice							
2017-02-16 13:26:21.040	172.16.10.19	192.168.0.121								
2017-02-16 13:25:29.036	172.16.10.19	192.168.0.121	alice							

Nell'esempio, ISE ha assegnato un SGT **MaliciousUser** diverso all'endpoint. Nel caso del profilo di autorizzazione **Nega accesso**, l'utente perde la connessione wireless e non può connettersi di nuovo.

Monitoraggio e aggiornamento con il portale delle liste nere. Se la regola di autorizzazione di

monitoraggio e aggiornamento è configurata per il reindirizzamento al portale, dal punto di vista dell'autore dell'attacco dovrebbe avere il seguente aspetto:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Passare ad **Analisi > Correlazione > Stato**, come mostrato in questa immagine.



Il messaggio di risultato deve restituire il **completamento corretto della correzione** o un messaggio di errore specifico. Verificare syslog: **Sistema > Monitoraggio > Syslog** e filtro dell'output con **pxgrid**. Gli stessi registri possono essere verificati in **/var/log/messages**.

Informazioni correlate

- <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>