Configurez la correction de pxGrid de FirePOWER 6.1 avec ISE

Contenu

Introduction

Ce document décrit comment configurer la correction de pxGrid de FirePOWER 6.1 avec le Cisco Identity Services Engine (ISE). Le module de correction de FirePOWER 6.1+ ISE peut être utilisé avec le service de protection de point final ISE (ENV) pour automatiser le qurantine/mettre des attaquants sur la liste noire sur la couche d'accès au réseau.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE
- Cisco FirePOWER

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 4 de version 2.0 de Cisco ISE
- Cisco FirePOWER 6.1.0
- Contrôleur LAN Sans fil virtuel (vWLC) 8.3.102.0

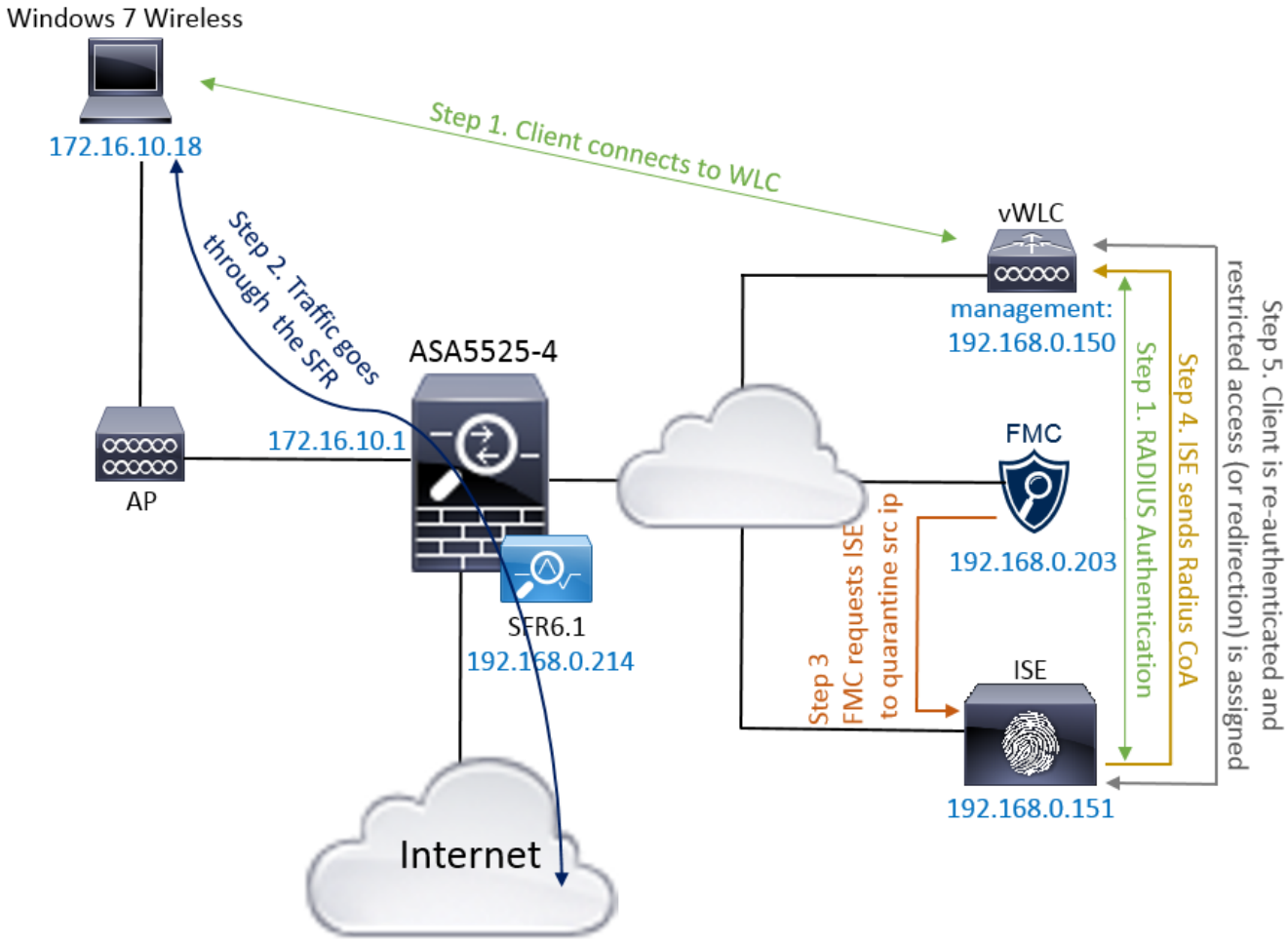
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Cet article ne couvre pas la configuration initiale de l'intégration ISE de FirePOWER, intégration ISE avec le Répertoire actif (AD), intégration de FirePOWER avec l'AD. Pour ces informations naviguez vers la section de références. Le module de correction de FirePOWER 6.1 permet au système de FirePOWER pour utiliser des capacités ISE ENV (quarantaine, unquarantine, arrêt de port) comme correction quand la règle de corrélation est appariée.

Note: L'arrêt de port n'est pas disponible pour des déploiements Sans fil.

Diagramme du réseau



La description d'écoulement :

1. Un client se connecte à un réseau, authentifie avec ISE et frappe une règle d'autorisation avec un profil d'autorisation qui accorde l'accès sans restriction au réseau.
2. Le trafic du client traverse alors un périphérique de FirePOWER.
3. Les débuts d'utilisateur pour exercer une action malveillante et frappe une règle de corrélation qui déclenche consécutivement le centre de Gestion de FirePOWER (FMC) pour faire la correction ISE par l'intermédiaire du pxGrid.
4. ISE assigne une quarantaine d'EPSStatus au point final et déclenche la modification de RADIUS de l'autorisation à un périphérique d'accès au réseau (WLC ou commutateur).

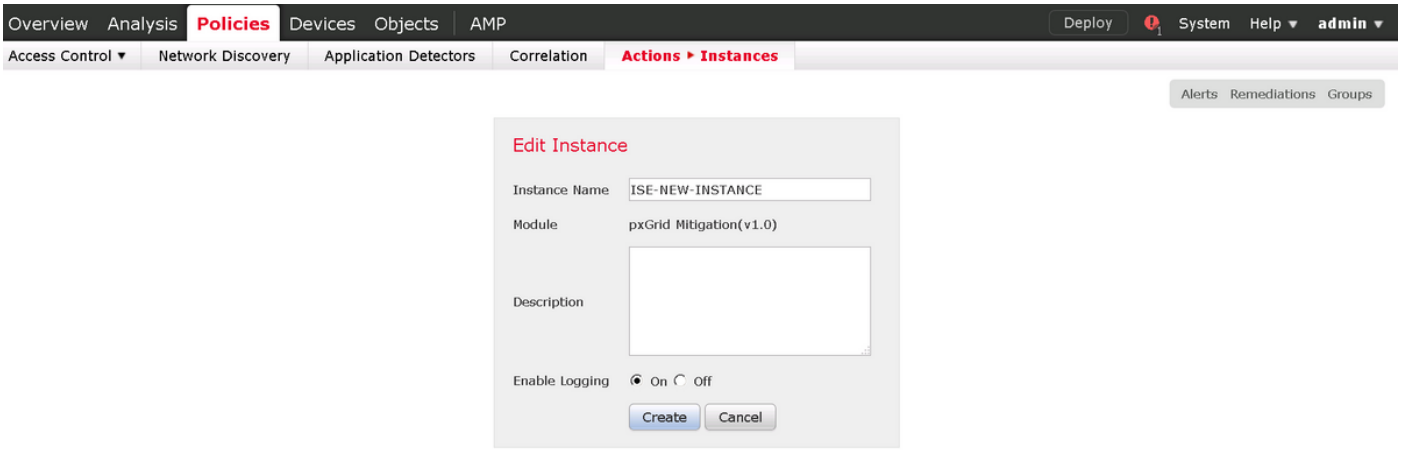
5. Le client frappe une autre stratégie d'autorisation qui assigne un accès restreint (les modifications SGT ou les redirect to portaiux ou refuse l'accès).

Note: Le périphérique d'accès au réseau (NAD) devrait être configuré pour envoyer RADIUS rendant compte à ISE afin de lui fournir les informations d'IP address qui sont utilisées pour tracer l'IP address à un point final.

Configurez FirePOWER

Étape 1. Configurez un exemple de réduction de pxGrid.

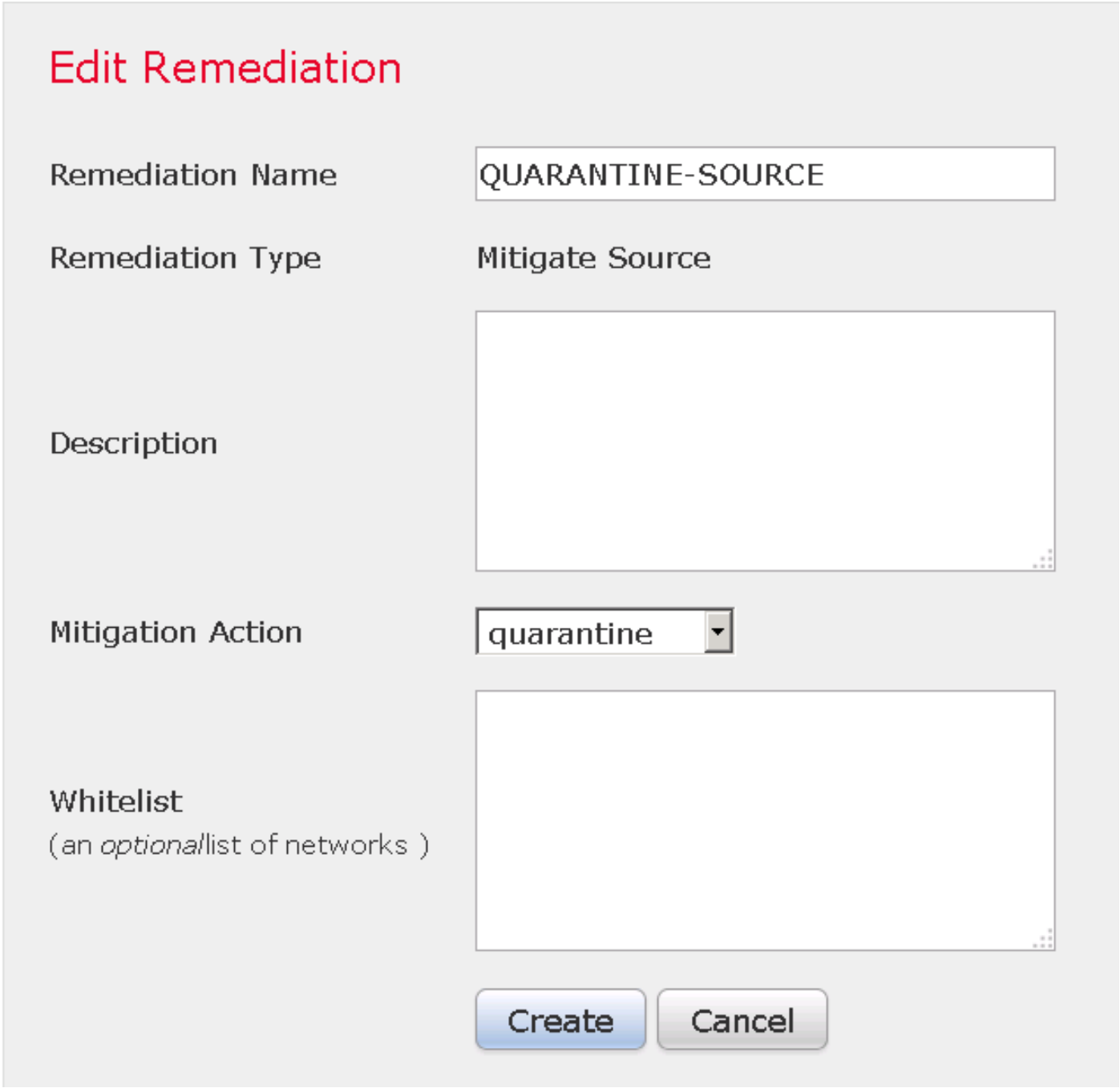
Naviguez vers des **stratégies > des actions > des exemples** et ajoutez l'exemple de réduction de pxGrid suivant les indications de l'image.



Étape 2. Configurez une correction.

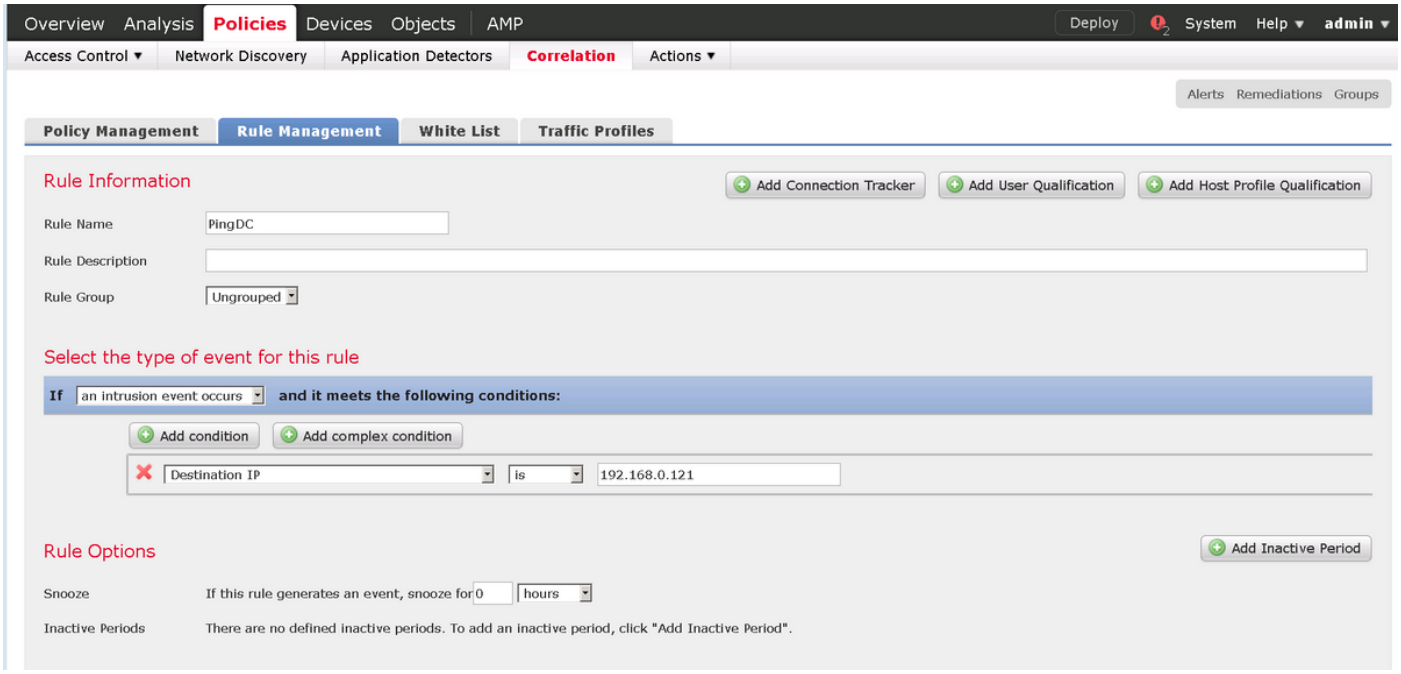
Il y a deux types disponibles : Atténuez la destination et atténuez la source. Dans cette source d'exemple la réduction est utilisée. Choisissez le type de correction et cliquez sur Add **suivant les indications de l'image :**

Assignez l'action de réduction à la correction suivant les indications de l'image :



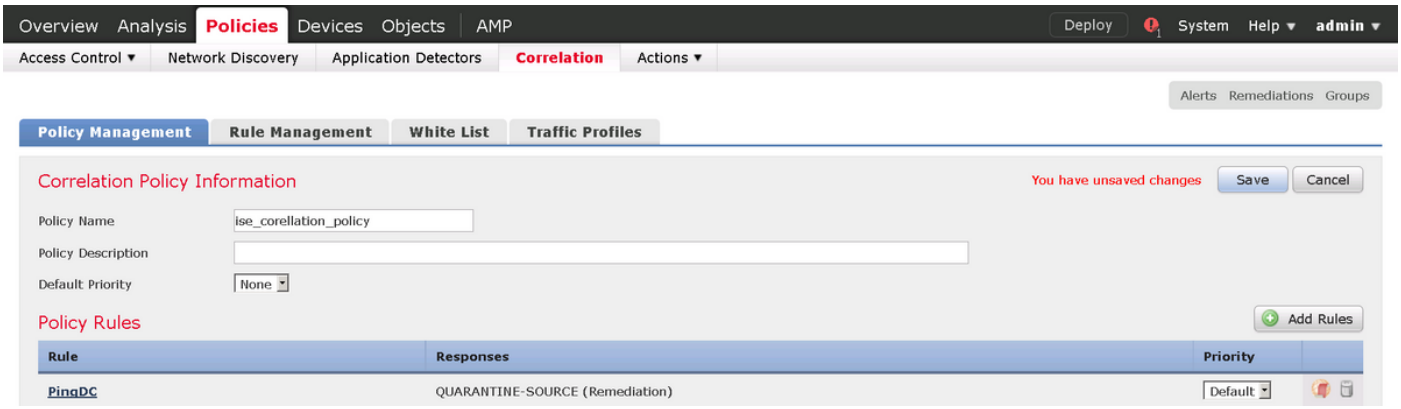
Étape 3. Configurez une règle de corrélation.

Naviguez vers les **stratégies > la Gestion de corrélation > de règle** et le clic **créent la** règle de corrélation de **règle** est le déclencheur pour que la correction se produise. La règle de corrélation peut contenir plusieurs conditions. Dans cette règle de corrélation d'exemple **PingDC** est frappé si l'événement d'intrusion se produit et IP address de destination est 192.168.0.121. La réponse d'écho assortie d'ICMP de règle faite sur commande d'intrusion est configurée afin du test suivant les indications de l'image :

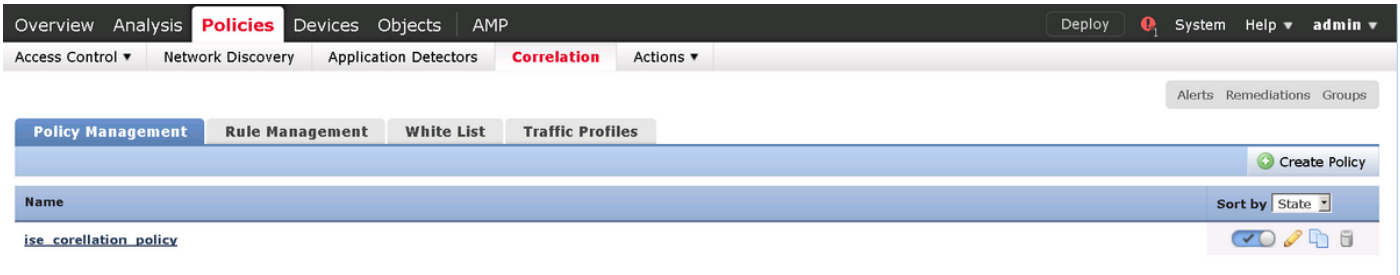


Étape 4. Configurez une stratégie de corrélation.

Naviguez vers des **stratégies > la corrélation > la Gestion des stratégies** et le clic **créent la stratégie**, ajoutent la règle à la stratégie et assignent la réponse à lui suivant les indications de l'image :



Activez la stratégie de corrélation suivant les indications de l'image :

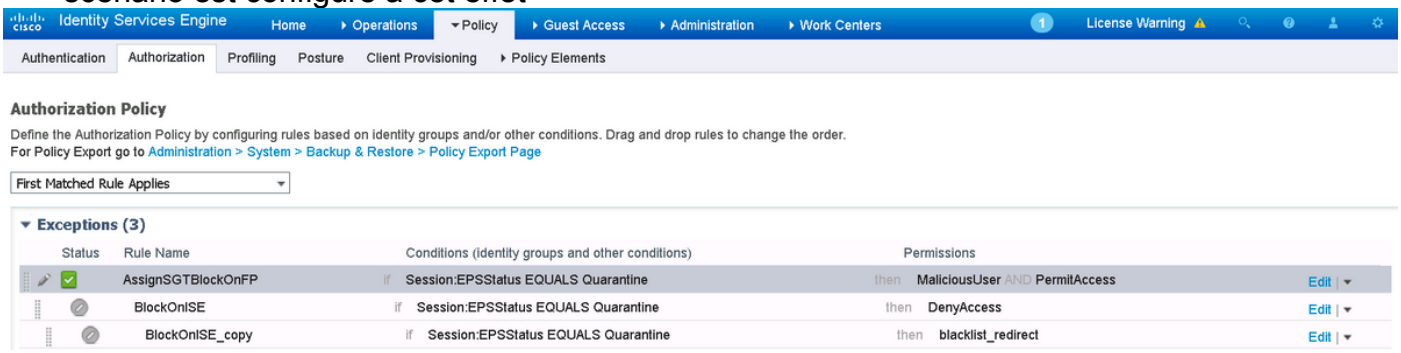


Configurez ISE

Étape 1. Configurez la stratégie d'autorisation.

Naviguez vers la **stratégie > l'autorisation** et ajoutez une nouvelle stratégie d'autorisation qui sera frappée après la correction a lieu. **Session d'**utilisation **: Quarantaine d'ÉGAUX d'EPSStatus** comme condition. Il y a plusieurs options qui peuvent être utilisées en conséquence :

- Permettez Access et assignez SGT différent (imposez la restriction de contrôle d'accès sur des périphériques de réseau)
- Refusez Access (l'utilisateur devrait être donné un coup de pied hors du réseau et ne devrait pas pouvoir se connecter de nouveau)
- Redirect to un portail de **liste noire** (dans ce portail fait sur commande de point névralgique de scénario est configuré à cet effet

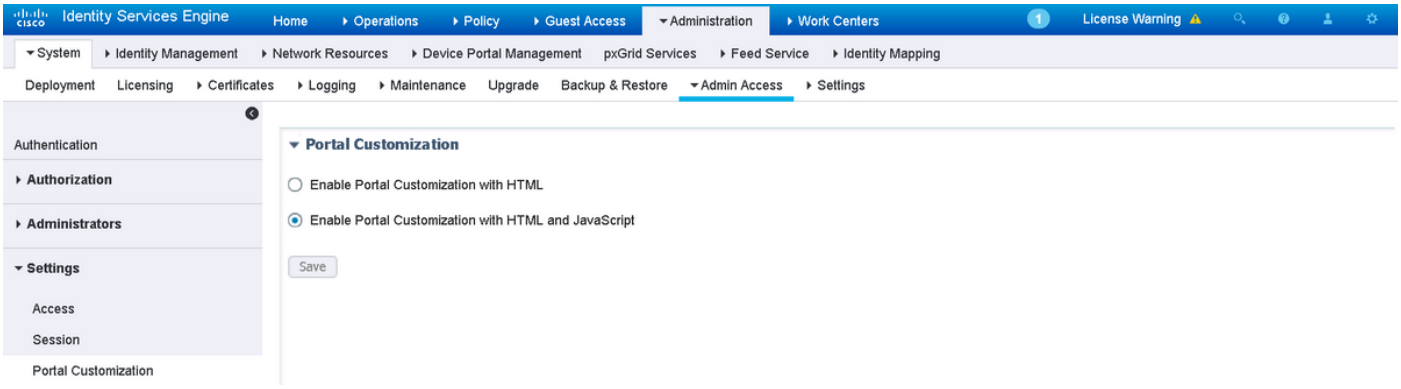


Configuration portaile faite sur commande

Dans cet exemple, le portail de point névralgique est configuré comme **liste noire**. Il y a seulement une page de la Politique d'Utilisation Acceptable (AUP) avec le texte fait sur commande et il n'y a aucune possibilité pour recevoir l'AUP (ceci est fait avec le Javascript). Afin de réaliser ceci, vous le premier besoin d'activer le Javascript et puis de coller un code qui masque le bouton et les contrôles AUP dans la configuration portaile de personnalisation.

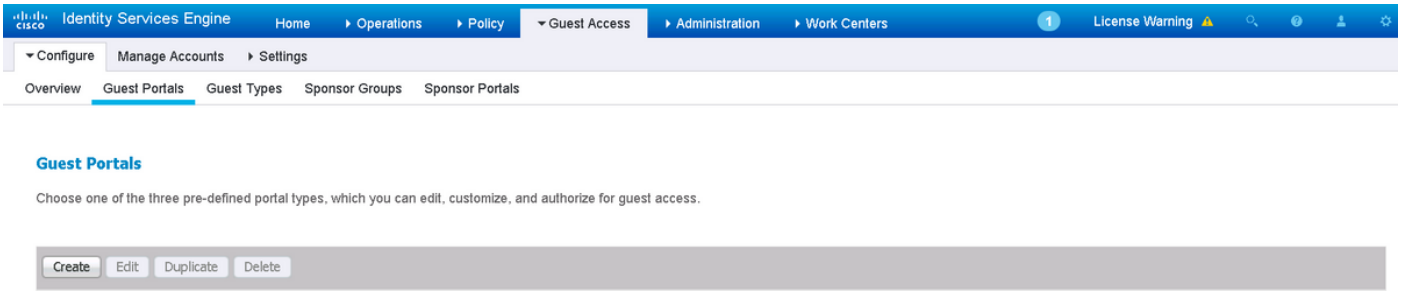
Étape 1. Javascript d'enable.

Naviguez vers des **configurations d'Access> de gestion > de système > d'admin > personnalisation portaile.** Choisissez Enable la **personnalisation portaile avec le HTML et le Javascript** et cliquez sur la **sauvegarde**.



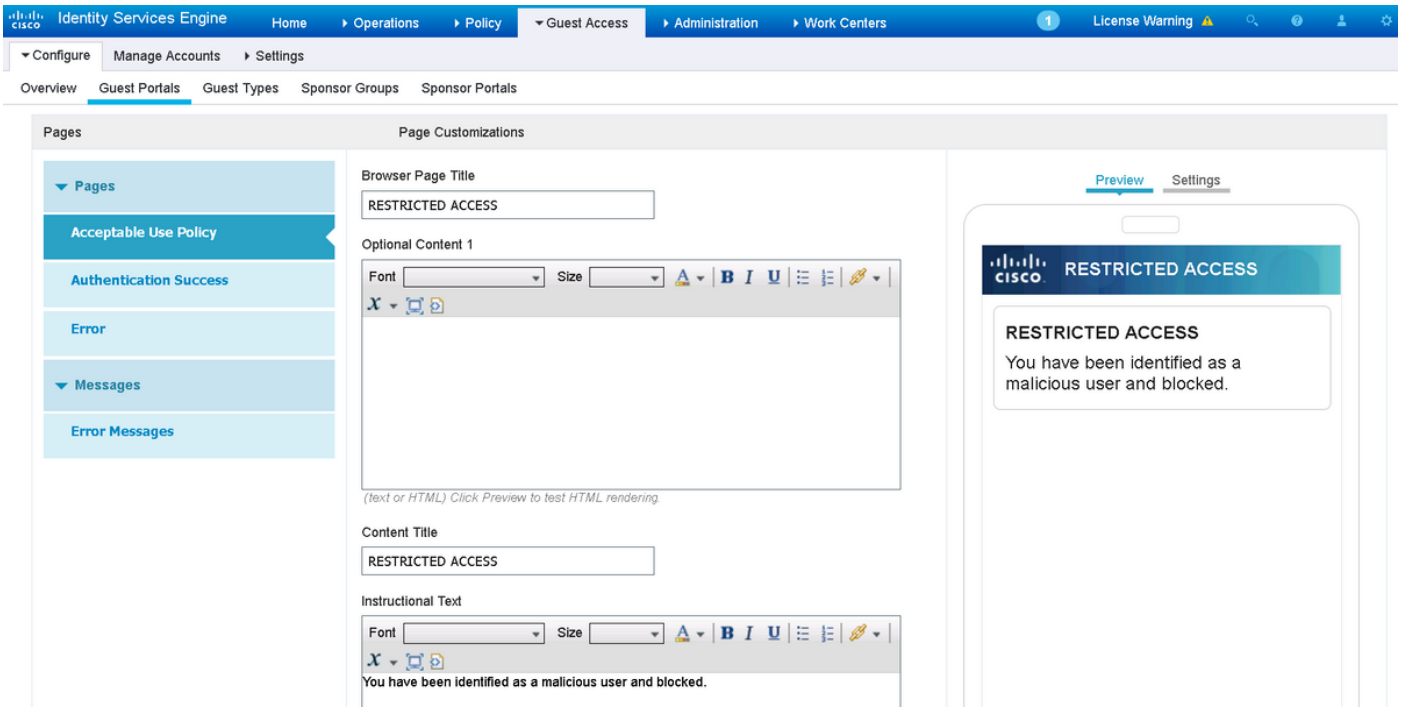
Étape 2. Créez un portail de point névralgique.

Naviguez vers l'**accès invité > configurent > des portails d'invité** et le clic **créent**, puis choisissent le type de point névralgique.



Étape 3. Configurez la personnalisation portaile.

Naviguez vers la **personnalisation de page du portail** et changez les titres et le contenu pour fournir un avertissement approprié à l'utilisateur.



Le défilement au **contenu 2 d'option**, **source HTML à bascule de** clic, et collent l'intérieur de script :

```
<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>
```

Source HTML d'Untoggle de clic.

Optional Content 2

Font Size

```
<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

Vérifiez

Utilisez les informations qui sont fournies dans cette section afin de vérifier que votre configuration fonctionne correctement.

FirePOWER

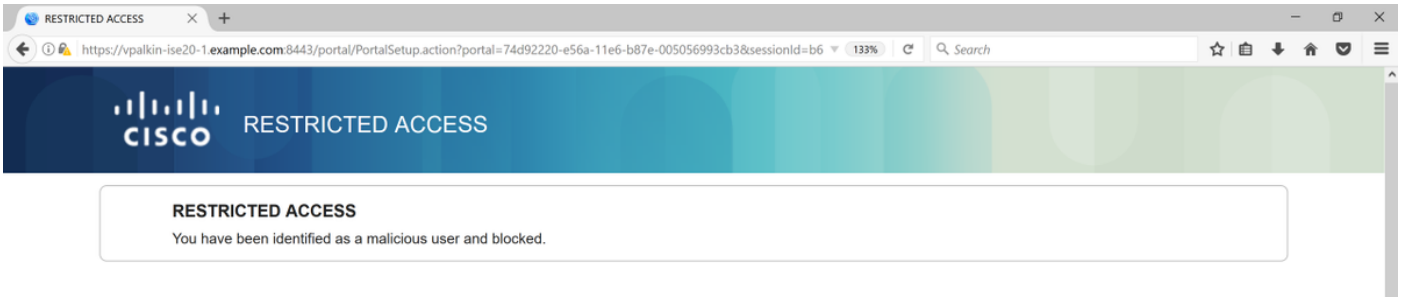
Le déclencheur pour que la correction se produise est un hit de stratégie/de règle de corrélation. Naviguez vers l'**analyse > la corrélation > les événements de corrélation** et vérifiez que l'événement de corrélation s'est produit.

ISE

ISE devrait alors déclencher Radius : Le CoA et authentifient à nouveau l'utilisateur, ces événements peut être en fonction vérifié **> RADIUS Livelog.**

Dans cet exemple, ISE a assigné SGT différent **MaliciousUser au** point final. Dans le cas de **refusez le** profil d'autorisation d'**Access que l'**utilisateur perd la connexion Sans fil et ne peut pas se connecter de nouveau.

La correction avec le portail de liste noire. Si la règle d'autorisation de correction est configurée au redirect to le portail, elle devrait ressembler à ceci du point de vue d'attaquant :



Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Naviguez vers l'**analyse > la corrélation > l'état** suivant les indications de cette image.

Le message de résultat devrait renvoyer la **réussite de la correction** ou le message d'erreur particulier. Vérifiez le Syslog : **Le système > la surveillance > le Syslog** et le filtre ont sorti avec le **pxgrid**. Les mêmes logs peuvent être vérifiés dans **/var/log/messages.**

Informations connexes

- 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