Corrección del pxGrid de FirePOWER 6.1 de la configuración con el ISE

Contenido

Introducción

Este documento describe cómo configurar la corrección del pxGrid de FirePOWER 6.1 con el Identity Services Engine (ISE). El módulo de la corrección de FirePOWER 6.1+ ISE se puede utilizar con el servicio de protección del punto final ISE (EP) para automatizar el qurantine/poner de los atacantes en la capa de acceso a la red.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento básico de estos temas:

- Cisco ISE
- Cisco FirePOWER

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Corrección 4 de la versión 2.0 de Cisco ISE
- Cisco FirePOWER 6.1.0
- Regulador virtual del Wireless LAN (vWLC) 8.3.102.0

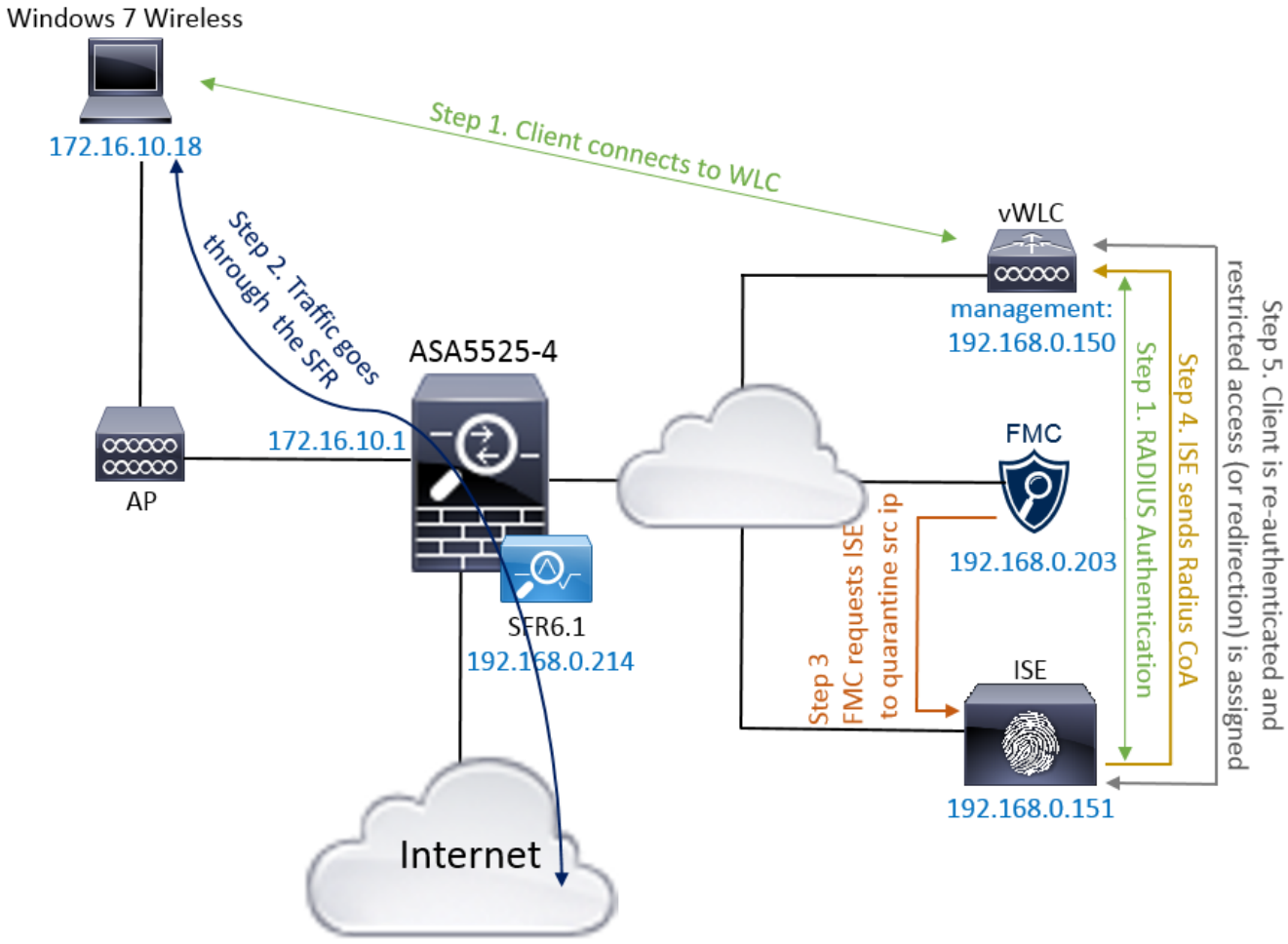
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Este artículo no cubre la configuración inicial de la integración ISE con FirePOWER, integración ISE con el Active Directory (AD), integración de FirePOWER con el AD. Para esta información navegue a la sección de referencias. El módulo de la corrección de FirePOWER 6.1 permite que el sistema de FirePOWER utilice las capacidades ISE EP (cuarentena, unquarantine, cierre de puerto) como corrección cuando se corresponde con la regla de la correlación.

Note: El cierre de puerto no está disponible para las implementaciones sin hilos.

Diagrama de la red



La descripción del flujo:

1. Un cliente conecta con una red, autentica con el ISE y golpea una regla de la autorización con un perfil de la autorización que conceda el acceso sin restricciones a la red.
2. El tráfico del cliente entonces atraviesa un dispositivo de FirePOWER.
3. El usuario comienza a realizar una actividad maliciosa y golpea una regla de la correlación que a su vez accione el centro de administración de FirePOWER (FMC) para hacer la corrección ISE vía el pxGrid.
4. El ISE asigna una cuarentena de EPSStatus al punto final y acciona el cambio RADIUS de la autorización a un dispositivo de acceso a la red (WLC o Switch).

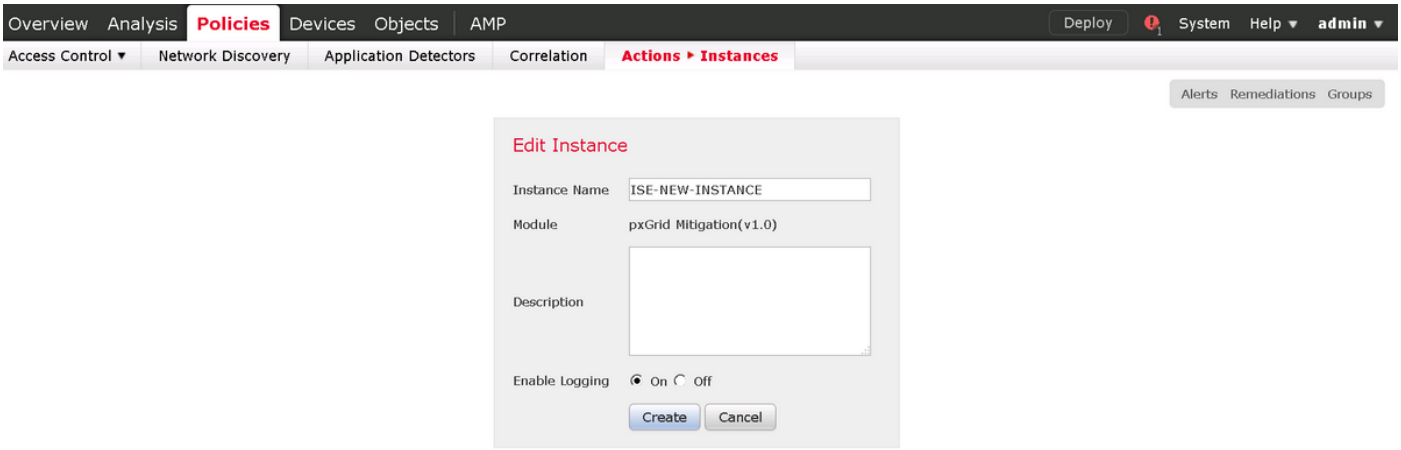
5. El cliente golpea otra directiva de la autorización que asigne un acceso restringido (los cambios SGT o reorientan al portal o niegan el acceso).

Note: El dispositivo de acceso a la red (NAD) se debe configurar para enviar el RADIUS que considera al ISE para proveer de él la información del IP Address que se utiliza para asociar el IP Address a un punto final.

Configuración FirePOWER

Paso 1. Configure un caso de la mitigación del pxGrid.

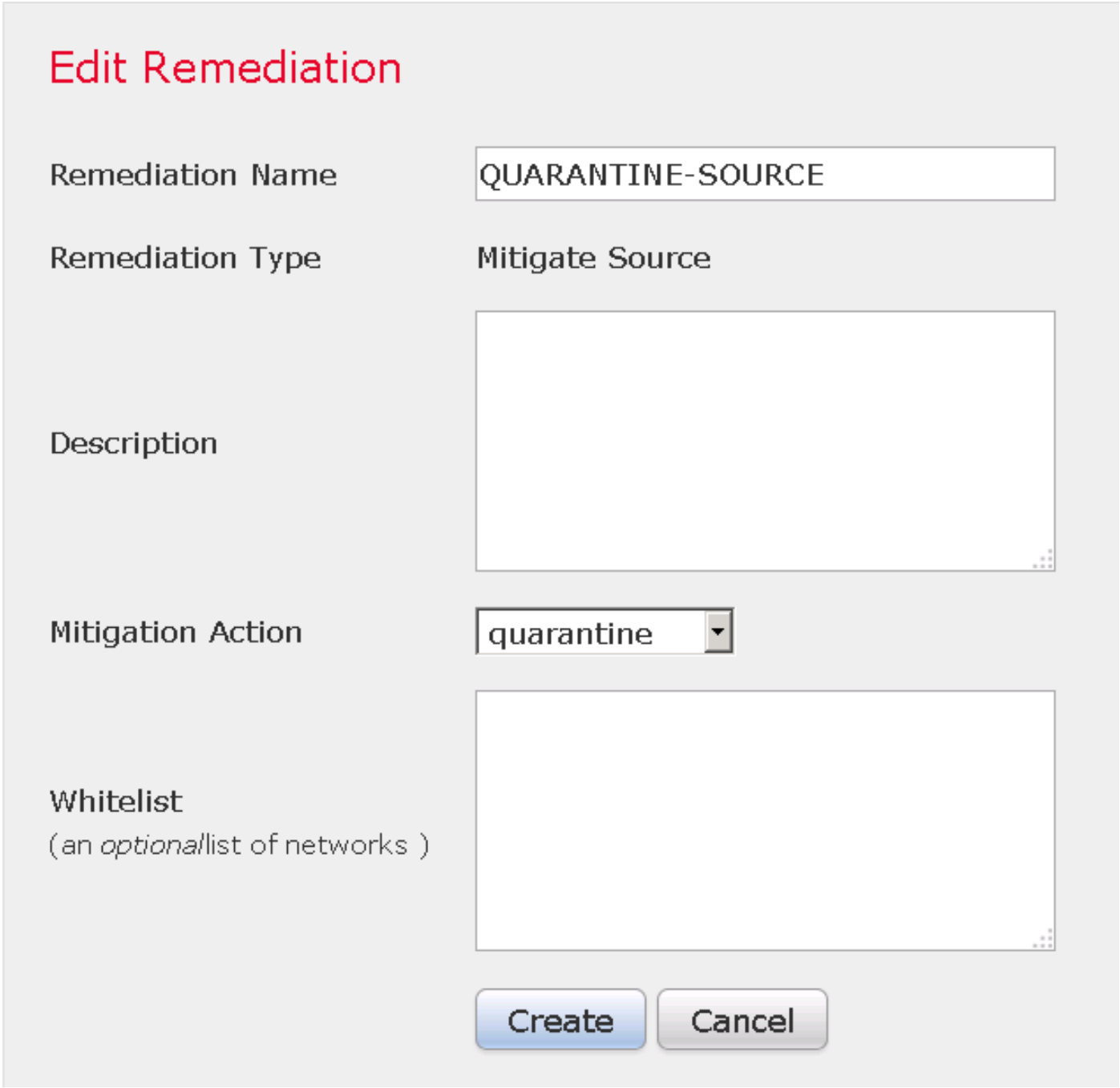
Navegue a las **directivas > a las acciones > a los casos** y agregue el caso de la mitigación del pxGrid tal y como se muestra en de la imagen.



Paso 2. Configure una corrección.

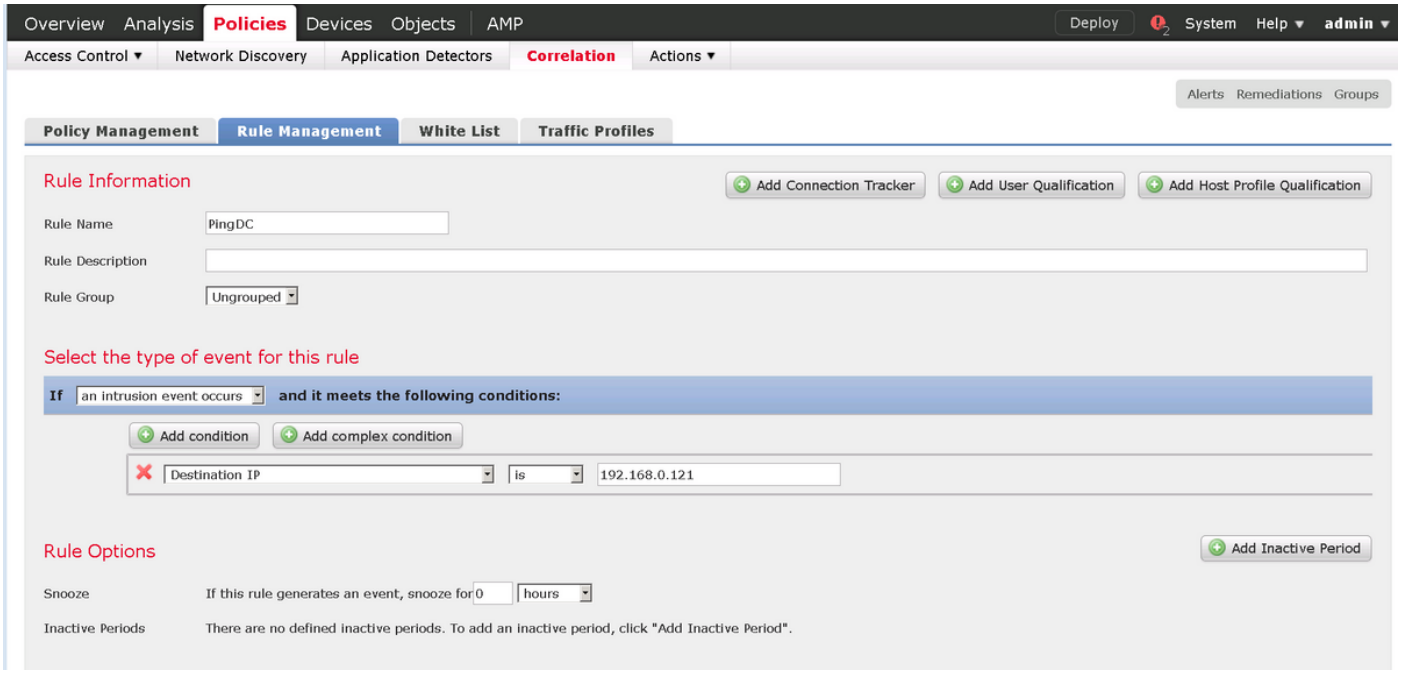
Hay dos tipos disponibles: Atenúe el destino y atenúe la fuente. En esta fuente del ejemplo se utiliza la mitigación. Elija el tipo de la corrección y el tecleo **agrega** tal y como se muestra en de la imagen:

Asigne la acción de la mitigación a la corrección tal y como se muestra en de la imagen:



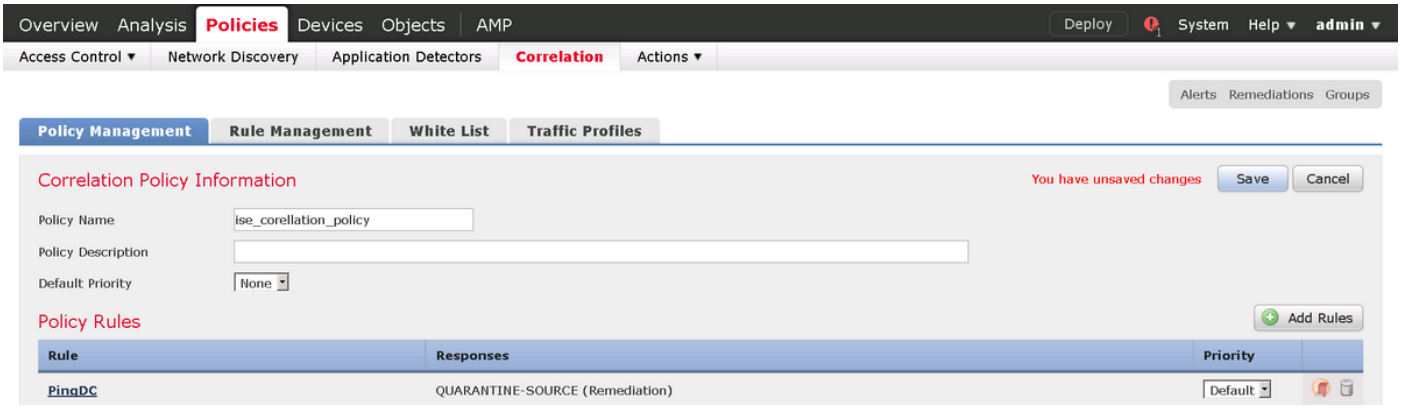
Paso 3. Configure una regla de la correlación.

Navegue a las **directivas > a la Administración de la correlación > de la regla** y el tecleo **crea la** regla de la correlación de la **regla** es el activador para que la corrección suceda. La regla de la correlación puede contener varias condiciones. En esta regla de la correlación del ejemplo se golpea **PingDC** si ocurre el evento de la intrusión y el IP Address de destino es 192.168.0.121. La regla de encargo de la intrusión que corresponde con la Respuesta de eco ICMP se configura con el fin de la prueba tal y como se muestra en de la imagen:

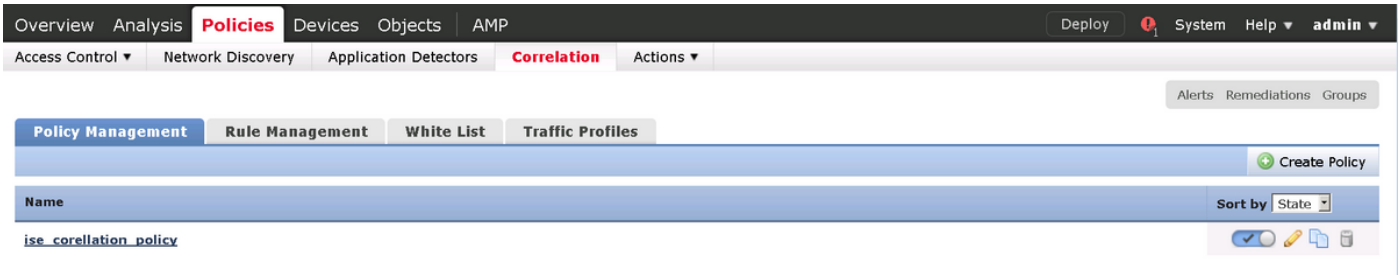


Paso 4. Configure una directiva de la correlación.

Navegue a las **directivas > a la correlación > a la Administración de políticas** y el tecleo **crea la directiva**, agrega la regla a la directiva y asigna la respuesta a él tal y como se muestra en de la imagen:



Habilite la directiva de la correlación tal y como se muestra en de la imagen:

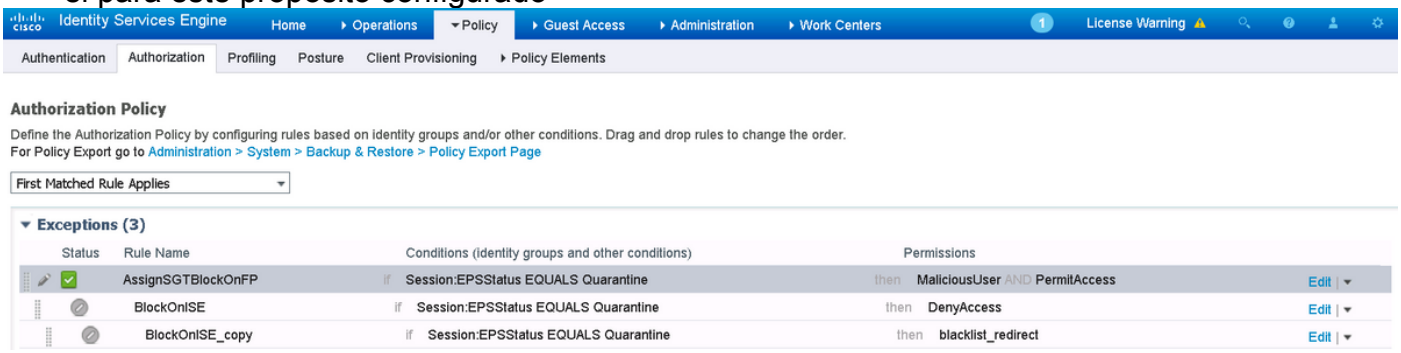


Configure el ISE

Paso 1. Directiva de la autorización de la configuración.

Navegue a la **directiva > a la autorización** y agregue una nueva directiva de la autorización que sea golpeada después de que ocurra la corrección. **Sesión del** uso: **EPSStatus IGUALA la cuarentena** como la condición. Hay varias opciones que se pueden utilizar como consecuencia:

- Permita el acceso y asigne diverso SGT (aplique la restricción del control de acceso en los dispositivos de red)
- Niegue el acceso (el usuario debe ser red golpeada con el pie de los y no debe poder conectar otra vez)
- Reoriente a un portal de la **lista negra** (en este portal de encargo del hotspot del escenario es el para este propósito configurado

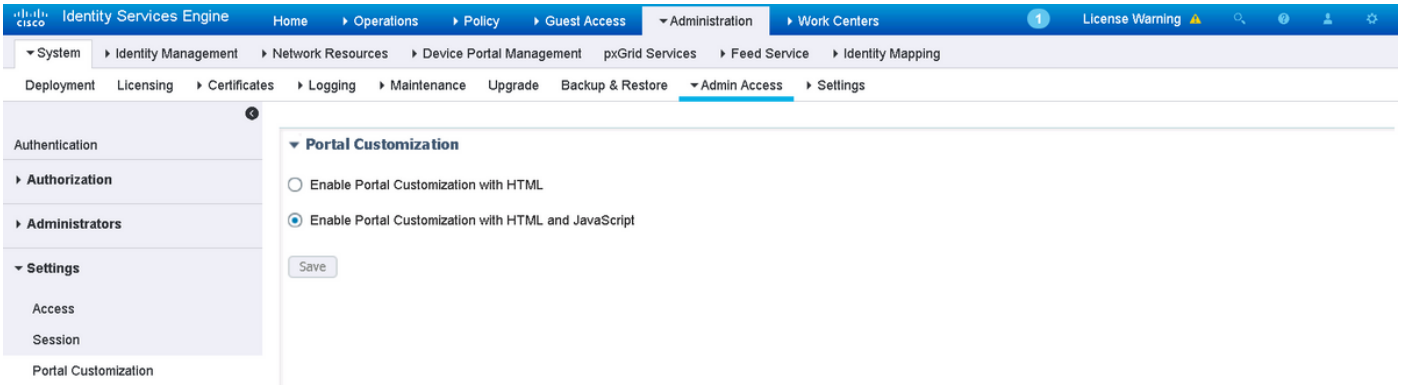


Configuración porta de encargo

En este ejemplo, el portal del hotspot se configura como **lista negra**. Hay solamente una página del Acceptable Use Policy (AUP) con el texto de encargo y no hay posibilidad para validar el AUP (esto se hace con el Javascript). Para alcanzar esto, usted primero necesita habilitar el Javascript y después pegar un código que oculte el botón y los controles AUP en la configuración porta del arreglo para requisitos particulares.

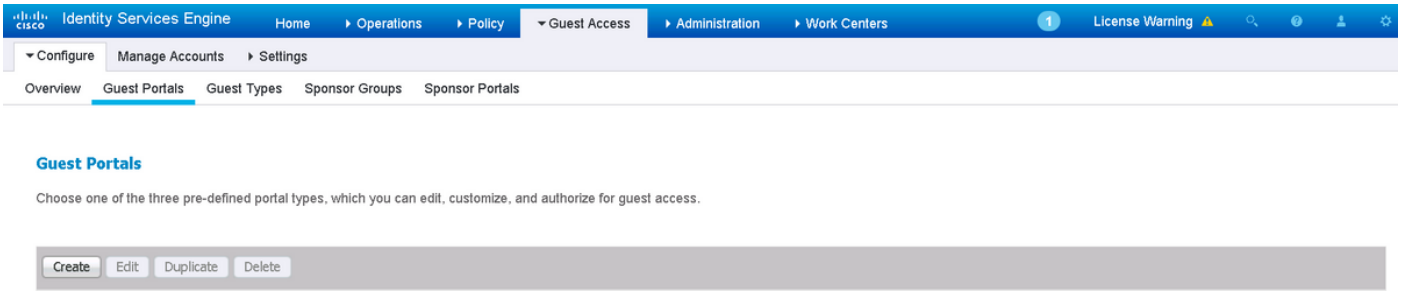
Paso 1. Javascript del permiso.

Navegue a la **administración > al sistema > a las configuraciones Admin Access> > arreglo para requisitos particulares porta.** Elija el **arreglo para requisitos particulares porta del permiso con el HTML y el Javascript** y haga clic la **salvaguardia**.



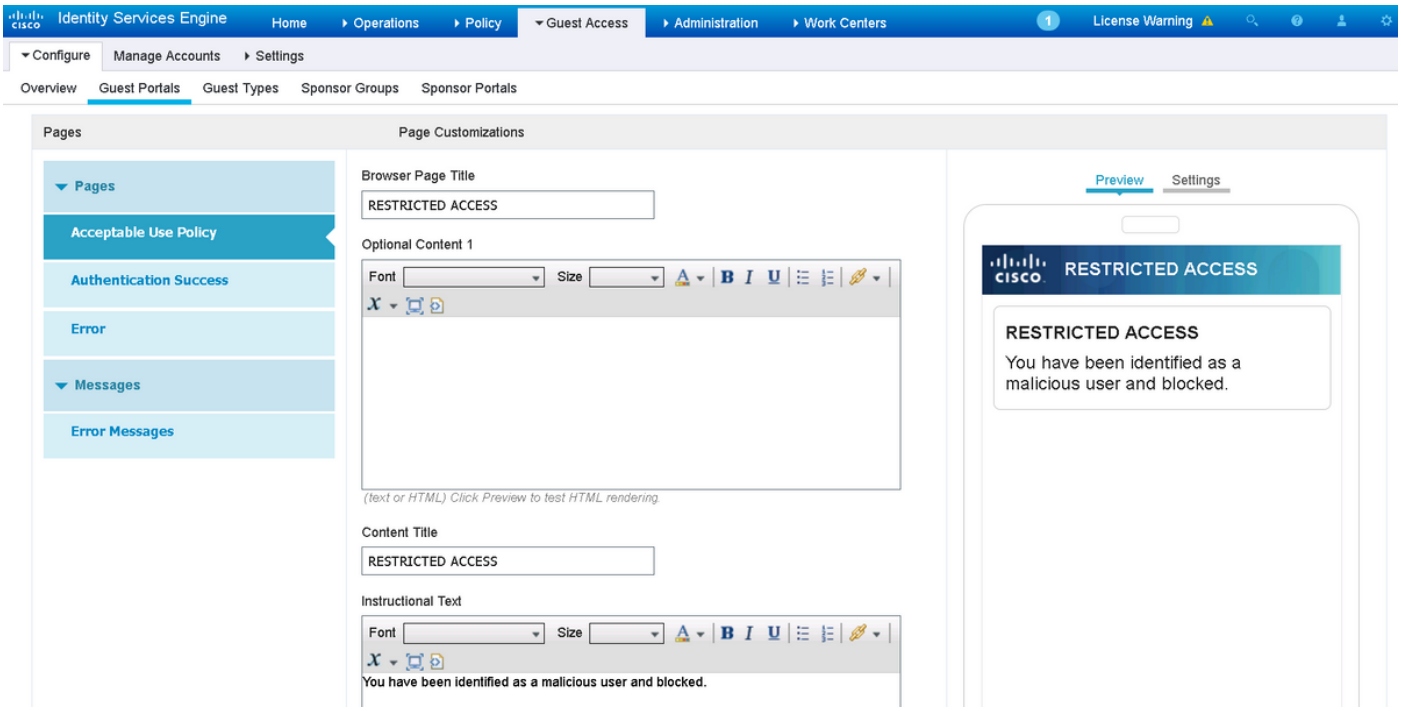
Paso 2. Cree un portal del hotspot.

Navegue al **acceso de invitado > a la configuración > a los portales del invitado** y el tecleo **crea**, después elige el tipo del hotspot.



Paso 3. Arreglo para requisitos particulares del portal de la configuración.

Navegue al **arreglo para requisitos particulares porta de la página** y cambie los títulos y el contenido para proporcionar una advertencia apropiada al usuario.



Navegue al **contenido 2 de la opción**, haga clic la **fuente de palanca HTML**, y pegue el interior del 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>
```

Haga clic la **fuente de Untoggle HTML.**

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.

Verificación

Utilice la información que se proporciona en esta sección para verificar que su configuración trabaja correctamente.

FirePOWER

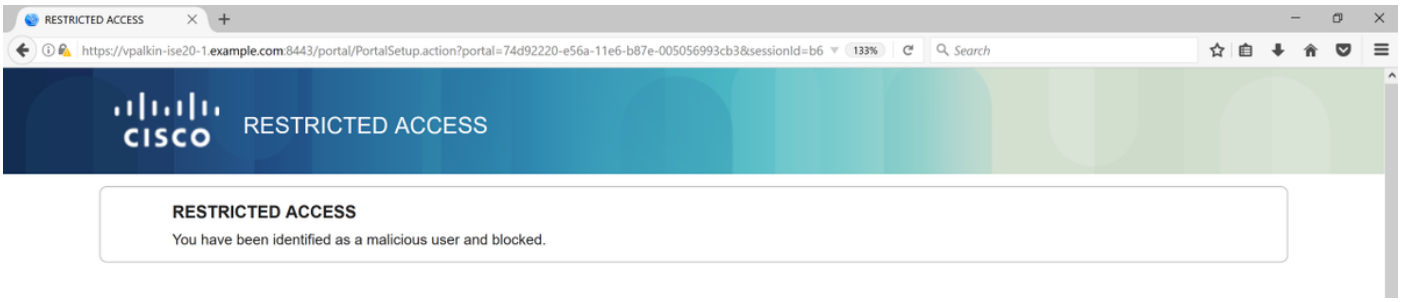
El activador para que la corrección suceda es un golpe de la directiva/de la regla de la correlación. Navegue al **análisis > a la correlación > a los eventos de la correlación** y verifique que sucedió el evento de la correlación.

ISE

El ISE debe entonces accionar el radio: El CoA y reautentifica al usuario, estos eventos puede ser en funcionamiento verificado **> RADIO Livelog.**

En este ejemplo, el ISE asignó diverso SGT **MaliciousUser al** punto final. En el caso de **niegue el** perfil de la autorización de **acceso que el** usuario pierde la conexión de red inalámbrica y que no puede conectar otra vez.

La corrección con el portal de la lista negra. Si la regla de la autorización de la corrección se configura para reorientar al portal, debe parecer esto de la perspectiva del atacante:



Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Navegue al **análisis > a la correlación > al estatus** tal y como se muestra en de esta imagen.

El mensaje del resultado debe volver la **terminación satisfactoria del** mensaje de la **corrección** o de error particular. Verifique el Syslog: **El sistema > la supervisión > el Syslog** y el filtro hicieron salir con el **pxgrid**. Los mismos registros se pueden verificar en **/var/log/messages.**

Información Relacionada

- 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