Configurar a remediação do pxGrid de FirePOWER 6.1 com ISE

Índice

Introdução

Este documento descreve como configurar a remediação do pxGrid de FirePOWER 6.1 com Identity Services Engine (ISE). O módulo da remediação de FirePOWER 6.1+ ISE pode ser usado com serviço de proteção do valor-limite ISE (EP) para automatizar o qurantine/põr dos atacantes na camada de acesso de rede.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico destes assuntos:

- Cisco ISE
- Cisco FirePOWER

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Correção de programa 4 da versão 2.0 de Cisco ISE
- Cisco FirePOWER 6.1.0
- Controlador virtual do Wireless LAN (vWLC) 8.3.102.0

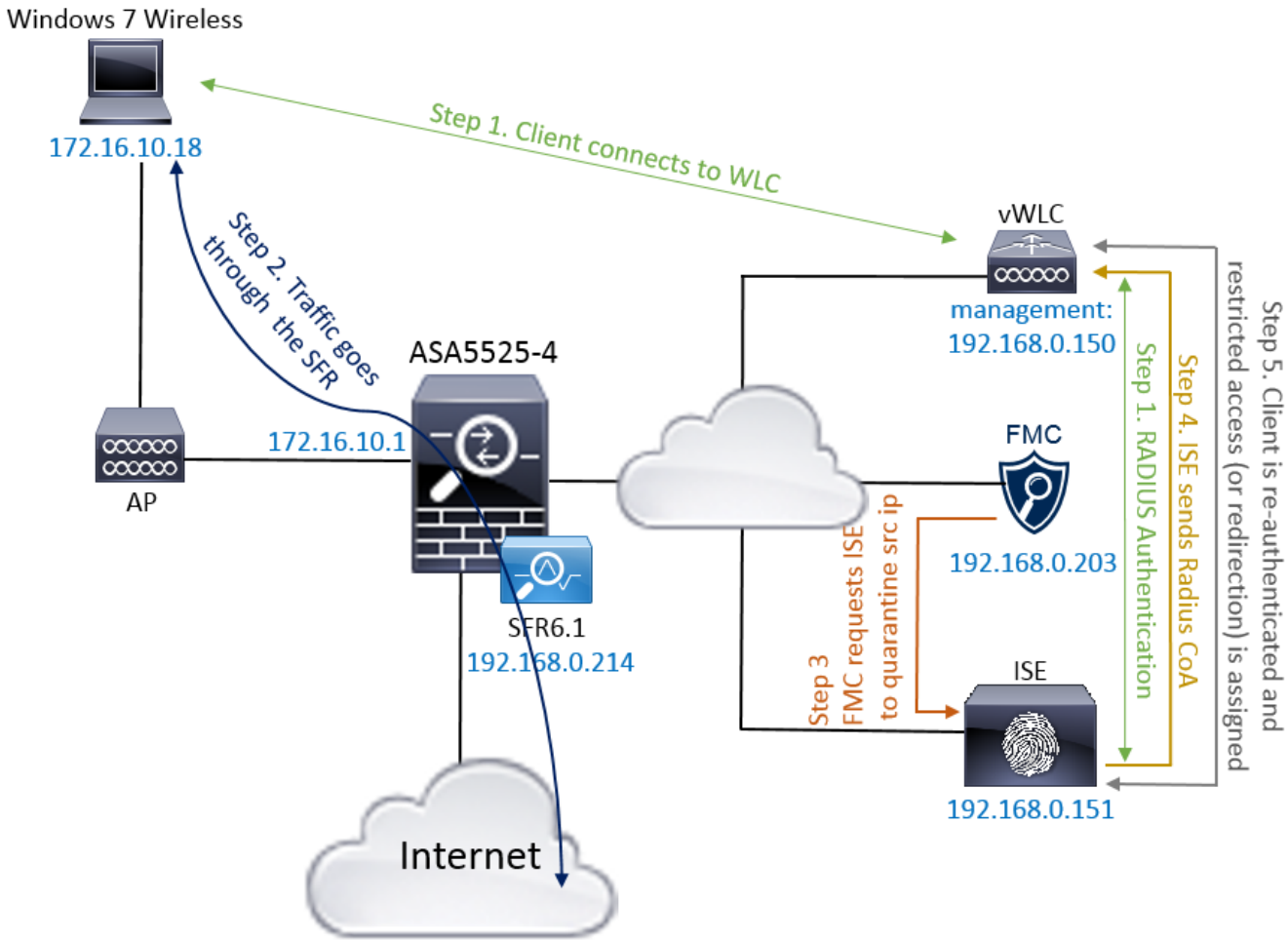
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Este artigo não cobre a configuração inicial da integração ISE com FirePOWER, integração ISE com diretório ativo (AD), integração de FirePOWER com AD. Para esta informação navegue à seção de referências. O módulo da remediação de FirePOWER 6.1 permite que o sistema de FirePOWER use capacidades ISE EP (quarentena, unquarantine, parada de porta) como uma remediação quando a regra da correlação é combinada.

Note: A parada de porta não está disponível para disposições wireless.

Diagrama de Rede



A descrição do fluxo:

1. Um cliente conecta a uma rede, autentica com ISE e bate uma regra da autorização com um perfil da autorização que conceda o acesso irrestrito à rede.
2. O tráfego do cliente corre através então de um dispositivo de FirePOWER.
3. O usuário começa executar uma atividade mal-intencionada e bate uma regra da correlação que provoque por sua vez o centro de gerenciamento de FirePOWER (FMC) para fazer a remediação ISE através do pxGrid.
4. O ISE atribui uma quarentena de EPSStatus ao valor-limite e provoca a mudança do RAIO da autorização a um dispositivo do acesso de rede (WLC ou interruptor).

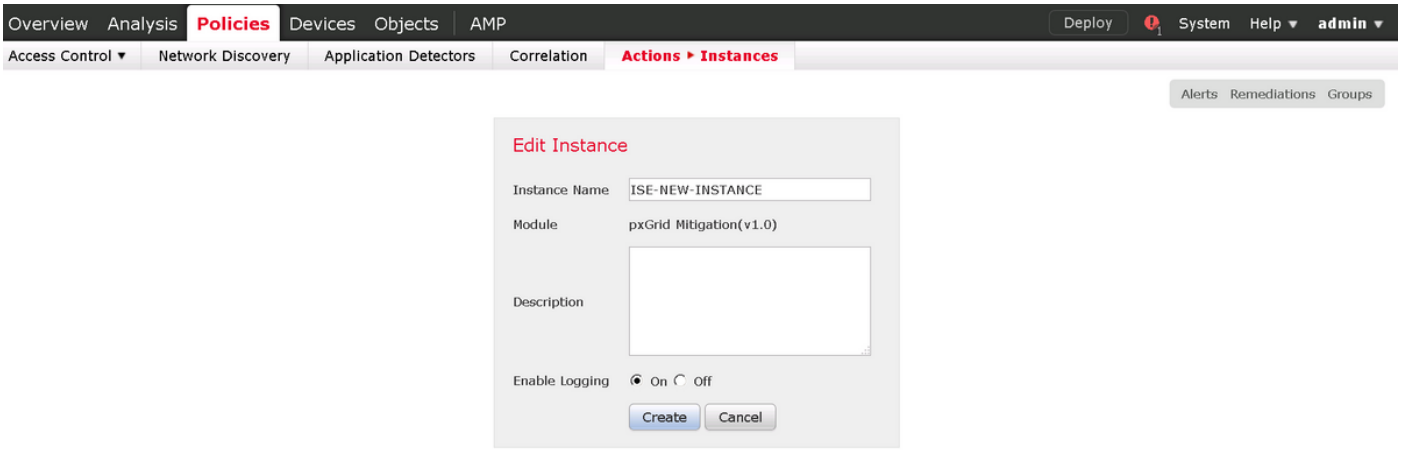
5. O cliente bate uma outra política da autorização que atribua um acesso restrito (as mudanças SGT ou reorientam ao portal ou negam o acesso).

Note: O dispositivo do acesso de rede (NAD) deve ser configurado para enviar o RAIO que explica ao ISE a fim fornecê-lo a informação do endereço IP de Um ou Mais Servidores Cisco ICM NT que é usada para traçar o endereço IP de Um ou Mais Servidores Cisco ICM NT a um valor-limite.

Configurar FirePOWER

Etapa 1. Configurar um exemplo da mitigação do pxGrid.

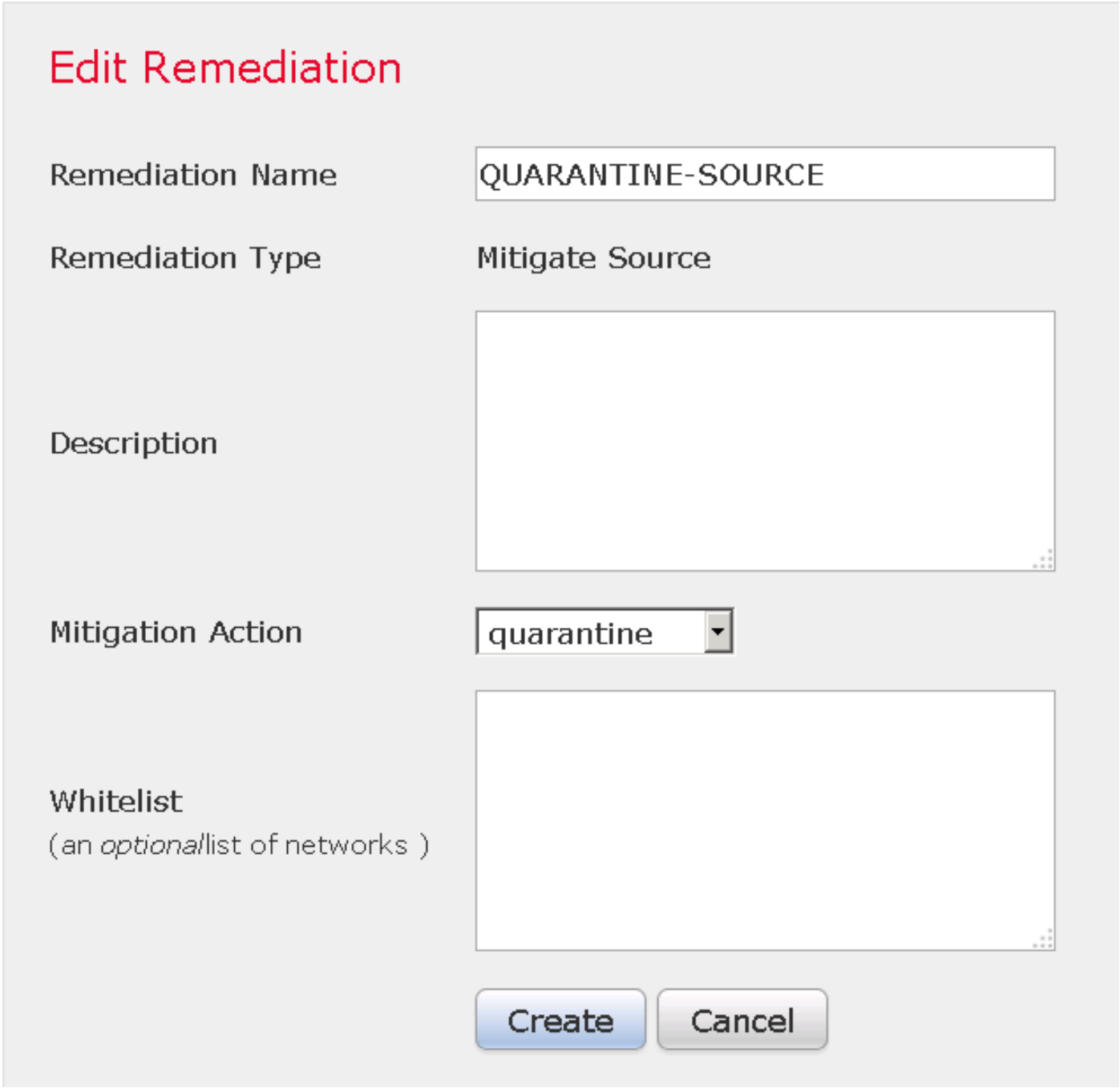
Navegue às **políticas > às ações > aos exemplos** e adicionar o exemplo da mitigação do pxGrid segundo as indicações da imagem.



Etapa 2. Configurar uma remediação.

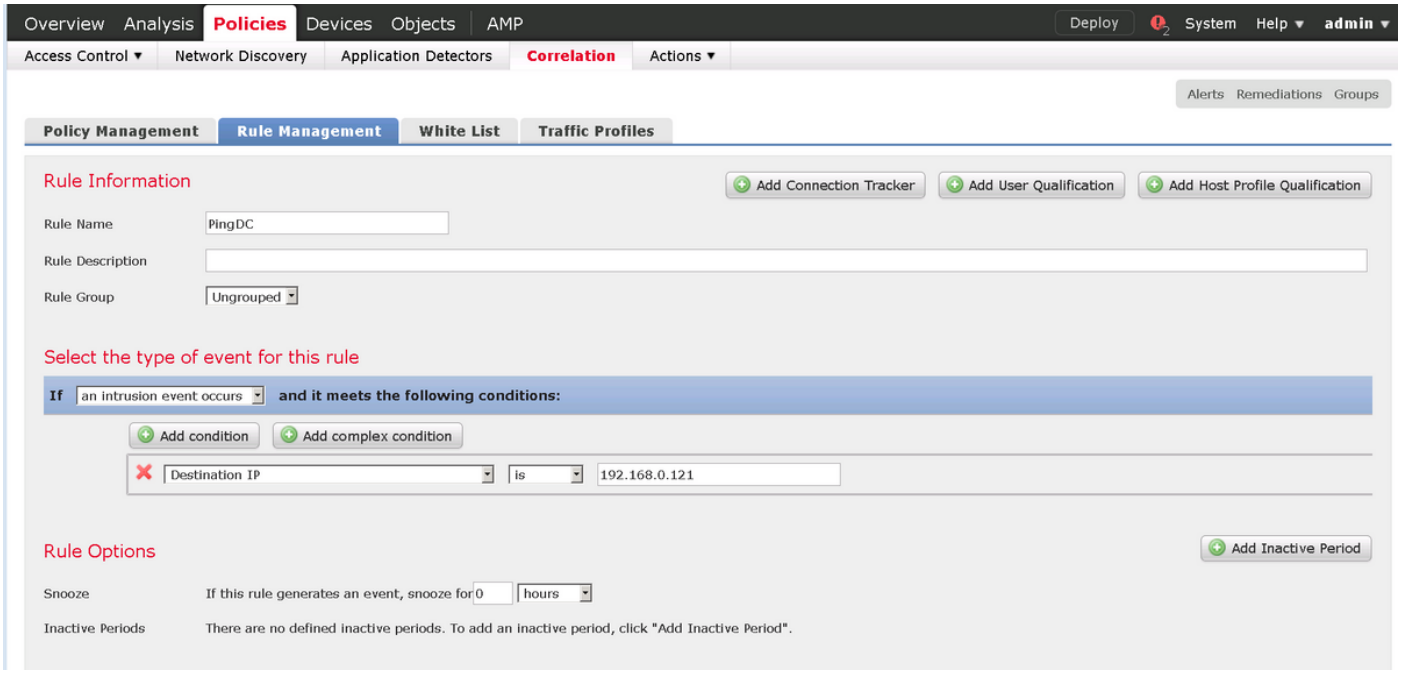
Há dois tipos disponíveis: Abrande o destino e abrande a fonte. Nesta fonte do exemplo a mitigação é usada. Escolha o tipo da remediação e o clique **adiciona** segundo as indicações da imagem:

Atribua a ação da mitigação à remediação segundo as indicações da imagem:



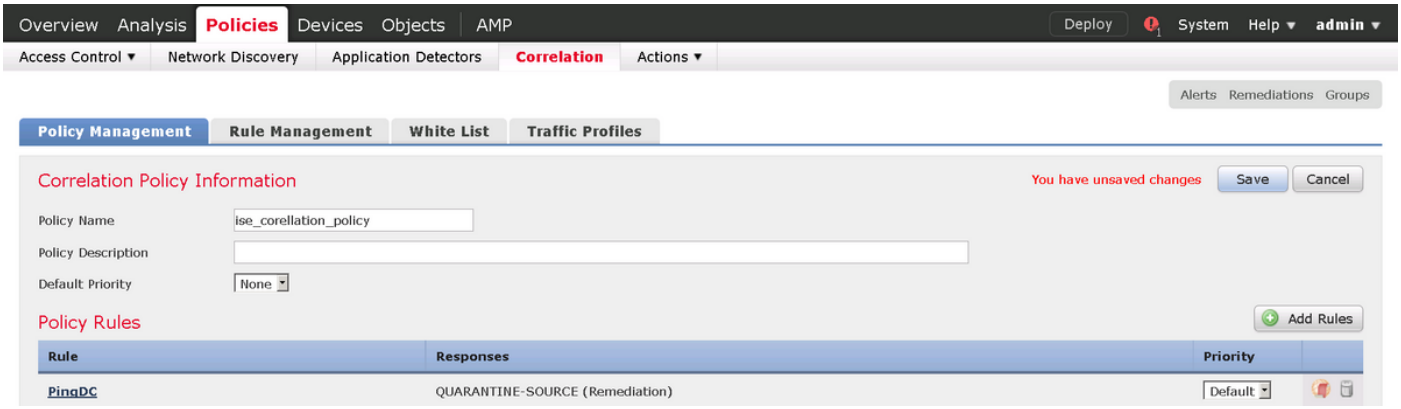
Etapa 3. Configurar uma regra da correlação.

Navegue às **políticas > ao Gerenciamento da correlação > da regra** e o clique **cria a** regra da correlação da **regra** é o disparador para que a remediação aconteça. A regra da correlação pode conter diversas circunstâncias. Nesta regra da correlação do exemplo **PingDC** está batido se o evento da intrusão ocorre e o endereço IP de destino é 192.168.0.121. A regra feita sob encomenda da intrusão que combina a resposta de eco ICMP é configurada com a finalidade do teste segundo as indicações da imagem:

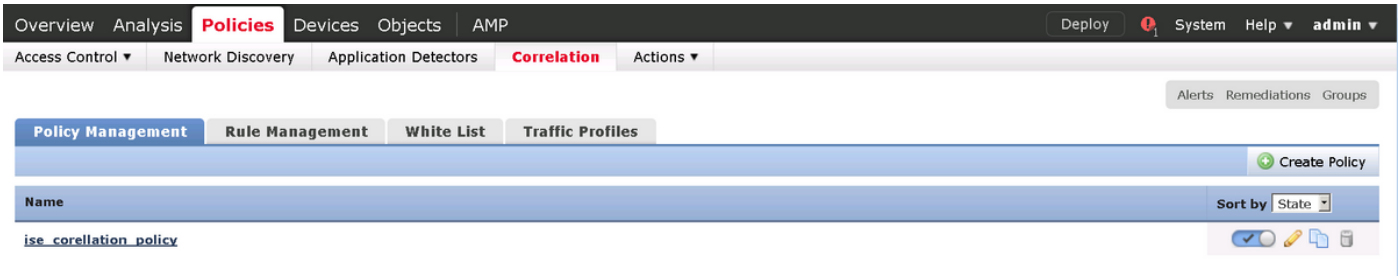


Etapa 4. Configurar uma política da correlação.

Navegue às **políticas > à correlação > ao Gerenciamento de políticas** e o clique **cria a política**, adiciona a regra à política e atribui a resposta a ele segundo as indicações da imagem:



Permita a política da correlação segundo as indicações da imagem:

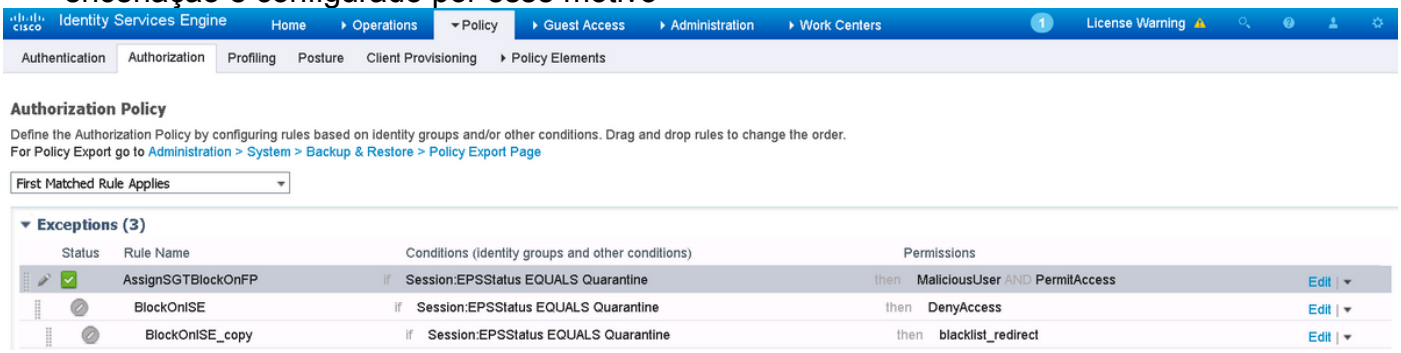


Configurar o ISE

Etapa 1. Configurar a política da autorização.

Navegue à **política > à autorização** e adicionar uma política nova da autorização que seja batida depois que a remediação ocorre. **Sessão do** uso: **EPSStatus IGUALA a quarentena** como a circunstância. Há diversas opções que podem ser usadas em consequência:

- Permita o acesso e atribua SGT diferente (reforce a limitação do controle de acesso em dispositivos de rede)
- Negue o acesso (o usuário deve ser retrocedido fora da rede e não deve poder conectar outra vez)
- Reoriente a um portal da **lista negra** (neste portal feito sob encomenda do ponto quente da encenação é configurado por esse motivo

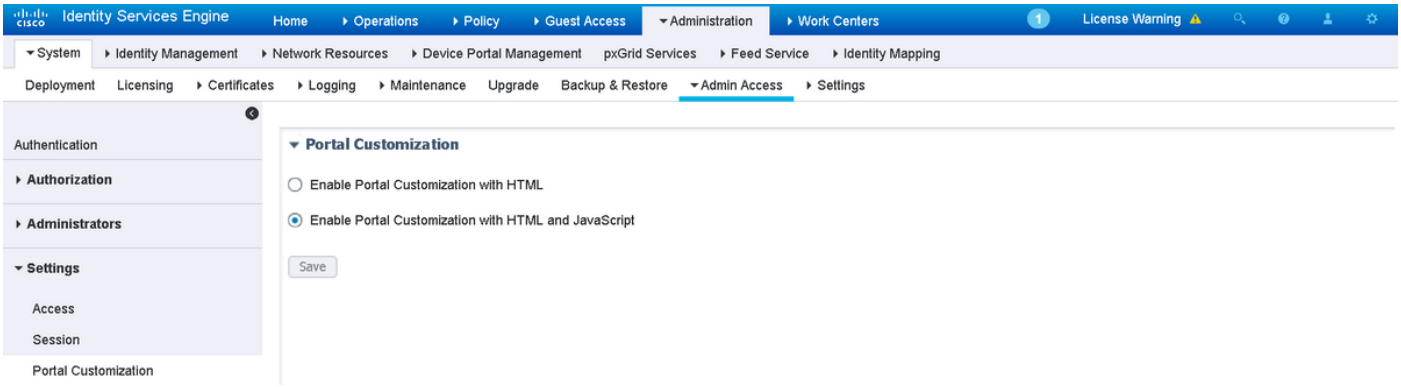


Configuração portal feita sob encomenda

Neste exemplo, o portal do ponto quente é configurado como uma **lista negra**. Há somente uma página da política de uso aceitável (AUP) com texto feito sob encomenda e não há nenhuma possibilidade para aceitar o AUP (este é feito com Javascript). A fim conseguir isto, você precisa primeiramente de permitir o Javascript e de colar então um código que esconda o botão e os controles AUP na configuração portal da personalização.

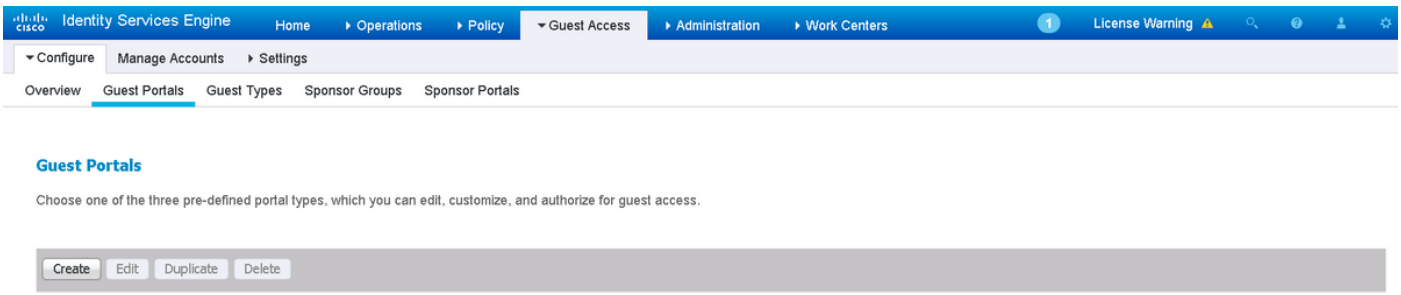
Etapa 1. Permita o Javascript.

Navegue à **administração > ao sistema > aos ajustes Admin Access> > personalização portal.** Escolha **permitem a personalização portal com HTML e Javascript** e clicam a **salvaguarda**.



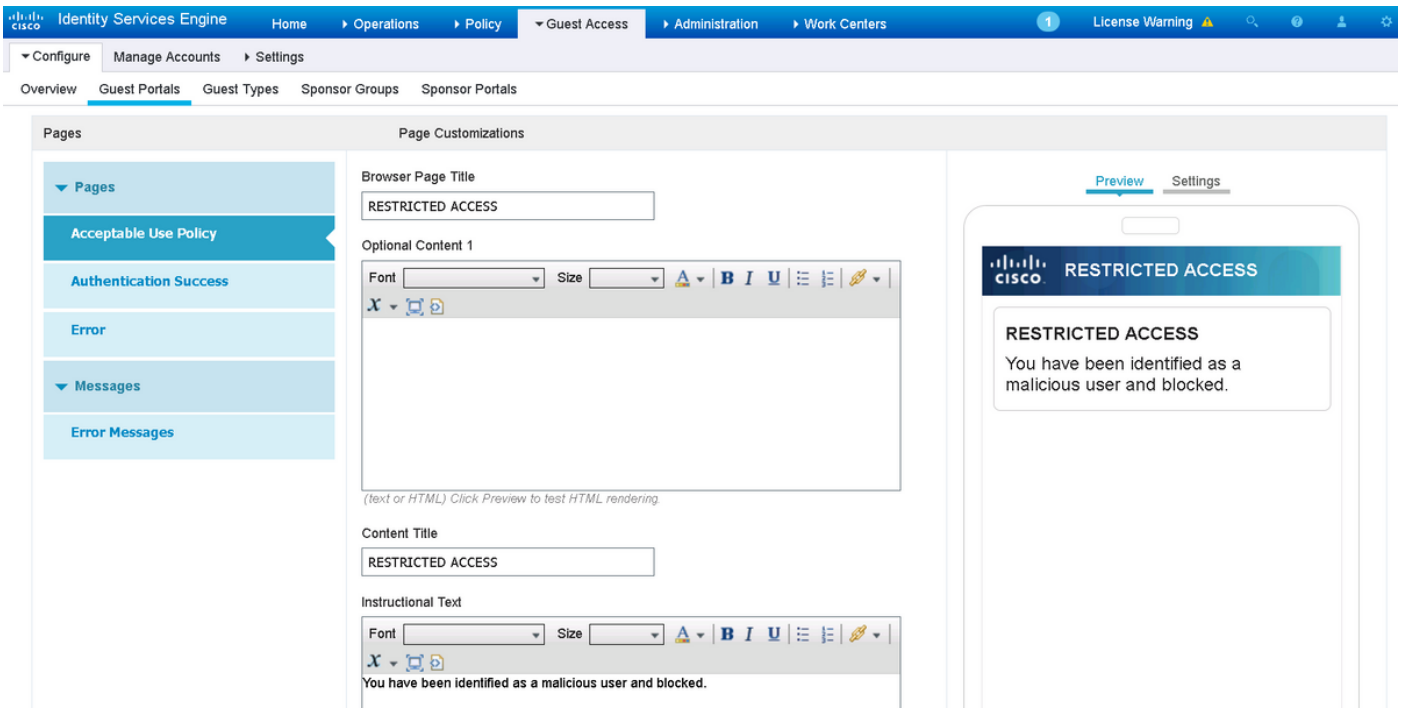
Etapa 2. Crie um portal do ponto quente.

Navegue ao **acesso do convidado > configuram > portais do convidado** e o clique **cria**, a seguir escolhe o tipo do ponto quente.



Etapa 3. Configurar a personalização portal.

Navegue à **personalização portal da página** e mude títulos e índice para fornecer um aviso apropriado ao usuário.



O rolo ao **índice 2 da opção**, **fonte de alavanca do** clique **HTML**, e cola o interior do 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>
```

Fonte de Untoggle HTML do clique.

Verificar

Use a informação que é fornecida nesta seção a fim verificar que sua configuração trabalha corretamente.

FirePOWER

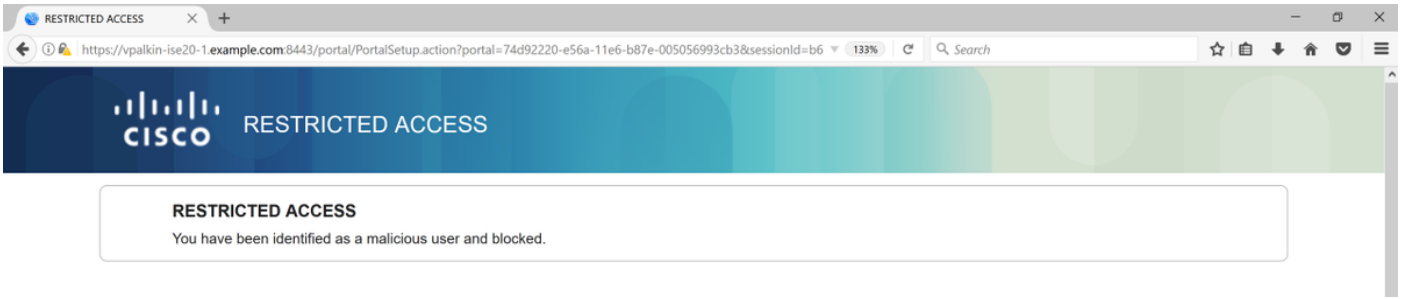
O disparador para que a remediação aconteça é uma batida da política/regra da correlação. Navegue à **análise > à correlação > aos eventos da correlação** e verifique que o evento da correlação aconteceu.

ISE

O ISE deve então provocar o raio: O CoA e autenticar novamente o usuário, estes eventos pode ser verificado na **operação > no RAIO Livelog.**

Neste exemplo, o ISE atribuiu SGT diferente **MaliciousUser ao** valor-limite. No caso de **negue o** perfil que da autorização de **acesso o** usuário perde a conexão Wireless e não pode conectar outra vez.

A remediação com portal da lista negra. Se a regra da autorização da remediação é configurada para reorientar ao portal, deve olhar como esta da perspectiva do atacante:



Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Navegue à **análise > à correlação > ao estado** segundo as indicações desta imagem.

A mensagem do resultado deve retornar a **conclusão bem sucedida da** mensagem da **remediação** ou de erro particular. Verifique o Syslog: **O sistema > a monitoração > o Syslog** e o filtro output com **pxgrid**. Os mesmos logs podem ser verificados em **/var/log/messages.**

Informações Relacionadas

- 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