Políticas ISE baseadas em exemplos de configuração SSID

Índice

Introdução

Este documento descreve como configurar políticas da autorização no Cisco Identity Services Engine (ISE) para distinguir entre os service set identifier diferentes (SSID). É muito comum para que uma organização tenha SSID múltiplos em sua rede Wireless para várias finalidades. Uma das finalidades as mais comuns é ter um SSID corporativo para os empregados e um convidado SSID para visitantes à organização.

Este guia supõe aquele:

1. O controlador do Wireless LAN (WLC) estabelece-se e trabalha para todos os SSID envolvidos.
2. A autenticação trabalha em todos os SSID envolvidos contra o ISE.

Outros documentos nesta série

- Autenticação da Web central com um exemplo de configuração do interruptor e do Identity Services Engine
- Autenticação da Web central no exemplo de configuração WLC e ISE
- O convidado ISE esclarece o exemplo da configuração de autenticação RADIUS/802.1x
- Postura Inline VPN usando o iPEP ISE e ASA

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Liberação 7.3.101.0 do controlador do Wireless LAN
- Liberação 1.1.2.145 do Identity Services Engine

As versões anterior igualmente têm both of these características.

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.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Configurações

Este documento utiliza as seguintes configurações:

- Método 1: Airespace-WLAN-identificação
- Método 2: Chamar-Estação-ID

Somente um método de configuração deve ser usado em um momento. Se ambas as configurações são executadas simultaneamente, a quantidade processou por aumentos ISE e afeta a legibilidade da regra. Este revisões de documento as vantagens e desvantagem de cada método de configuração.

Método 1: Airespace-WLAN-identificação

Cada Wireless Local Area Network (WLAN) criado no WLC tem um ID de WLAN. O ID de WLAN é indicado na página de sumário WLAN.

Quando um cliente conecta ao SSID, a requisição RADIUS ao ISE contém o atributo Airespace-WLAN-ID. Este atributo simples é usado para fazer decisões de política no ISE. Uma desvantagem a este atributo é se o ID de WLAN não combina em um SSID espalhado através dos controladores múltiplos. Se isto descreve seu desenvolvimento, continue ao método 2.

Neste caso, a Airespace-WLAN-identificação é usada como uma circunstância. Pode ser usada como uma condição simples (por si só) ou em uma condição composta (conjuntamente com um outro atributo) para conseguir o resultado desejado. Este capas de documento ambos os casos

do uso. Com os dois SSID acima, estas duas regras podem ser criadas.

A) Os usuários convidado devem entrar ao convidado SSID.

B) Os usuários corporativos devem estar no grupo “usuários de domínio” do diretório ativo (AD) e devem entrar ao SSID corporativo.

Ordene A

Ordene A tem apenas uma exigência, assim que você pode construir uma condição simples (baseada nos valores acima):

1. No ISE, vão à **política > aos elementos > às condições > à autorização da política > as condições simples** e criam uma condição nova.
2. No campo de nome, dê entrada com um nome da circunstância
3. No campo de descrição, incorpore uma descrição (opcional).
4. Da lista de drop-down do atributo, escolha **Airespace > Airespace-Wlan-Id--[1]**.
5. Da lista de drop-down do operador, escolha **iguais.**
6. Da lista de drop-down de valor, escolha **2.**
7. Clique em Salvar.

Ordene B

A regra B tem duas exigências, assim que você pode construir uma condição composta (baseada nos valores acima):

1. No ISE, vão à **política > aos elementos > às condições > à autorização da política > as condições compostas** e criam uma condição nova.
2. No campo de nome, dê entrada com um nome da circunstância.
3. No campo de descrição, incorpore uma descrição (opcional).
4. Escolha **criam a condição nova (opção avançada)**.
5. Da lista de drop-down do atributo, escolha **Airespace > Airespace-Wlan-Id--[1]**.
6. Da lista de drop-down do operador, escolha **iguais.**
7. Da lista de drop-down de valor, escolha **1.**
8. Clique a engrenagem à direita e escolha-a **adicionam o atributo/valor**.
9. Da lista de drop-down do atributo, escolha **AD1 > grupos externos**.
10. Da lista de drop-down do operador, escolha **iguais.**
11. Da lista de drop-down de valor, selecione o grupo exigido. Neste exemplo, é ajustada aos usuários de domínio.
12. Clique em Salvar.

Nota: Durante todo este documento nós usamos os perfis simples da autorização configurados sob a política > os elementos da política > os resultados > a autorização > os perfis da autorização. São ajustados para permitir o acesso, mas podidos ser adaptados para caber as necessidades do seu desenvolvimento.

Agora que nós temos as circunstâncias, nós podemos aplicá-las a uma política da autorização. Vá à **política > à autorização**. Determine onde introduzir a regra na lista ou editar sua regra existente.

Regra do convidado

1. Clique a seta para baixo à direita de uma regra existente e escolha a **inserção uma regra nova**.
2. Dê entrada com um nome para sua regra do convidado e deixe aos grupos da identidade o conjunto de campo a alguns.
3. Sob circunstâncias, clique o sinal de adição e clique a **condição existente seleta da biblioteca**.
4. Sob o nome de circunstância, escolha a **condição simples > o GuestSSID**.
5. Sob permissões, escolha o perfil apropriado da autorização para seus usuários convidado.
6. Clique em Concluído.

Regra corporativa

1. Clique a seta para baixo à direita de uma regra existente e escolha a **inserção uma regra nova**.
2. Dê entrada com um nome para sua regra corporativa e deixe aos grupos da identidade o conjunto de campo a alguns.
3. Sob circunstâncias, clique o sinal de adição e clique a **condição existente seleta da biblioteca**.
4. Sob o nome de circunstância, escolha a **condição composta > o CorporateSSID**.
5. Sob permissões, escolha o perfil apropriado da autorização para seus usuários corporativos.
6. Clique em Concluído.

Nota: Até que você clique a salvaguarda na parte inferior da lista da política, nenhuma mudança feita nesta tela estará aplicada a seu desenvolvimento.

Método 2: Chamar-Estação-ID

O WLC pode ser configurado para enviar o nome SSID no atributo do RAIO CHAMAR-ESTAÇÃO-ID, que por sua vez pode ser usado como uma condição no ISE. A vantagem deste atributo é que se pode se usar apesar do que o ID de WLAN é ajustado no WLC. À revelia, o WLC não envia o SSID no atributo Chamar-Estação-ID. Para permitir esta característica no WLC, ir à **Segurança > ao AAA > ao RAIO > à autenticação** e ajustar o tipo do ID de estação do atendimento ao MAC address AP: SSID. Isto ajusta o formato do Chamar-Estação-ID a *<MAC do AP que o usuário está conectando o to>: <SSID Name>*.

Você pode ver que nome SSID está indo ser enviado da página de sumário WLAN.

Desde que o atributo Chamar-Estação-identificação igualmente contém o MAC address do AP, uma expressão regular (REGEX) é usada para combinar o nome SSID na política ISE. O operador “combina” na configuração da circunstância pode ler um REGEX do campo de valor.

Exemplos REGEX

“Começa com” — por exemplo, use o valor REGEX do **^ (Acme). *** — esta circunstância é configurada como o CERTIFICADO: A organização COMBINA o “Acme” (algum fósforo com uma circunstância que comece com “Acme”).

“Termina com” — por exemplo, use o valor REGEX de. *** (mktg) $** — esta circunstância é configurada como o CERTIFICADO: A organização COMBINA o “mktg” (algum fósforo com uma circunstância essa extremidades com “mktg”).

“Contém” — por exemplo, use o valor REGEX de .*(1234).* — esta circunstância é configurado como o CERTIFICADO: A organização COMBINA '1234' (algum fósforo com uma circunstância

que contenha "1234", tal como Eng1234, 1234Dev, e Corp1234Mktg).

“Não começa com” — por exemplo, use o valor REGEX do **^ (?! LDAP). *** — esta circunstância é configurada como o CERTIFICADO: A organização COMBINA o “LDAP” (algum fósforo com uma condição que não comece com o “LDAP”, como o usLDAP ou o CorpLDAPmktg).

O Chamar-Estação-ID termina com o nome SSID, assim que o REGEX a usar-se neste exemplo é**. * (: <SSID NAME>) $**. Mantenha isto na mente como você atravessa a configuração.

Com os dois SSID acima, você pode criar duas regras com estas exigências:

A) Os usuários convidado devem entrar ao convidado SSID.

B) Os usuários corporativos devem estar no grupo “usuários de domínio” AD e devem entrar ao SSID corporativo.

Ordene A

Ordene A tem apenas uma exigência, assim que você pode construir uma condição simples (baseada nos valores acima):

1. No ISE, vão à **política > aos elementos > às condições > à autorização da política > as condições simples** e criam uma condição nova.
2. No campo de nome, dê entrada com um nome da circunstância.
3. No campo de descrição, incorpore uma descrição (opcional).
4. Da lista de drop-down do atributo, escolha o **raio - > Called-Station-ID--[30]**.
5. Da lista de drop-down do operador, escolha **fósforos.**
6. Da lista de drop-down de valor, escolha. *** (: Convidado) $**. Isto é diferenciando maiúsculas e minúsculas.
7. Clique em Salvar.

Regra B

A regra B tem duas exigências, assim que você pode construir uma condição composta (baseada nos valores acima):

1. No ISE, vão à **política > aos elementos > às condições > à autorização da política > as condições compostas** e criam uma condição nova.
2. No campo de nome, dê entrada com um nome da circunstância.
3. No campo de descrição, incorpore uma descrição (opcional).
4. Escolha **criam a condição nova (opção avançada)**.
5. Da lista de drop-down do atributo, escolha o **raio - > Called-Station-Id--[30]**.
6. Da lista de drop-down do operador, escolha **fósforos.**
7. Da lista de drop-down de valor, escolha**. * (:) $ corporativo**. Isto é diferenciando maiúsculas e minúsculas.
8. Clique a engrenagem à direita e escolha-a **adicionam o atributo/valor**.
9. Da lista de drop-down do atributo, escolha **AD1 > grupos externos**.
10. Da lista de drop-down do operador, escolha **iguais.**
11. Da lista de drop-down de valor, selecione o grupo exigido. Neste exemplo, é ajustada aos usuários de domínio.
12. Clique em Salvar.

Nota: Durante todo este documento, nós usamos os perfis simples da autorização configurados sob a política > os elementos da política > os resultados > a autorização > os perfis da autorização. São ajustados para permitir o acesso, mas podidos ser adaptados para caber as necessidades do seu desenvolvimento.

Agora que as circunstâncias são configuradas, aplique-as a uma política da autorização. Vá à **política > à autorização**. Introduza a regra na lista no lugar apropriado ou edite uma regra existente.

Regra do convidado

1. Clique a seta para baixo à direita de uma regra existente e escolha a **inserção uma regra nova**.
2. Dê entrada com um nome para sua regra do convidado e deixe aos grupos da identidade o conjunto de campo a alguns.
3. Sob circunstâncias, clique o sinal de adição e clique a **condição existente seleta da biblioteca**.
4. Sob o nome de circunstância, escolha a **condição simples > o GuestSSID**
5. Sob permissões, escolha o perfil apropriado da autorização para seus usuários convidado.
6. Clique em Concluído.

Regra corporativa

1. Clique a seta para baixo à direita de uma regra existente e escolha a **inserção uma regra nova**.
2. Dê entrada com um nome para sua regra corporativa e deixe aos grupos da identidade o conjunto de campo a alguns.
3. Sob circunstâncias, clique o sinal de adição e clique a **condição existente seleta da biblioteca**.
4. Sob o nome de circunstância, escolha a **condição composta > o CorporateSSID**.
5. Sob permissões, escolha o perfil apropriado da autorização para seus usuários corporativos.
6. Clique em Concluído.
7. Clique a **salvaguarda na** parte inferior da lista da política.

Nota: Até que você clique a salvaguarda na parte inferior da lista da política, nenhuma mudança feita nesta tela estará aplicada a seu desenvolvimento.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Para encontrar se a política foi criada corretamente e se certificar do ISE está recebendo os atributos apropriados, reveja o relatório detalhado da autenticação para passada ou a autenticação falha para o usuário. Escolha **operações > autenticações** e clique então o ícone dos **detalhes** para uma autenticação.

Primeiramente, verifique o sumário da autenticação. Isto mostra os princípios da autenticação quais incluem o que o perfil da autorização foi fornecido ao usuário.

Se a política está incorreta, os detalhes da autenticação mostrarão que Airespace-WLAN-identificação e que Chamar-Estação-identificação foi enviada do WLC. Ajuste suas regras em conformidade. A regra combinada política da autorização confirma mesmo se a autenticação está combinando sua regra pretendida.

Estas regras são desconfiguradas geralmente. Para revelar o problema de configuração, combine a regra contra o que é visto nos detalhes da autenticação. Se você não vê os atributos nos outros atributos colocam, certifique-se que o WLC está configurado corretamente.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems