

Exemplo de configuração do ponto quente da versão 1.3 ISE

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Topologia e fluxo](#)

[Configurar](#)

[WLC](#)

[ISE](#)

[Verificar](#)

[Postura adicional](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

A versão 1.3 do Cisco Identity Services Engine (ISE) tem um novo tipo de convidado Ponto quente chamado portal. Este tipo de portal permite que você forneça o acesso do convidado à rede e não força o usuário a fornecer nenhuma credenciais. Este documento descreve como configurar e pesquisar defeitos esta funcionalidade.

Pré-requisitos

Requisitos

Cisco recomenda que você tem a experiência com configuração ISE e conhecimento básico destes assuntos:

- Disposições ISE e fluxos do convidado
- Configuração dos controladores do Wireless LAN (WLC)

[Componentes Utilizados](#)

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

- Microsoft Windows 7

- Versão 7.6 e mais recente de Cisco WLC
- Software ISE, versão 1.3 e mais recente

Topologia e fluxo

Esta encenação é para os usuários convidado que aceitam a política de uso aceitável (AUP) e seja dada somente então o acesso ao Internet (ou algum outro acesso limitado).

Etapa 1. Associados do usuário convidado ao Service Set Identifier (SSID): Ponto quente. Esta é uma rede aberta com o MAC que filtra com o ISE para a autenticação. Esta autenticação combina a segunda regra da autorização no ISE e o perfil da autorização reorienta ao ponto quente. O ISE retorna uma aceitação de acesso do RAIO com dois pares Cisco AV:

- URL-reorientar-ACL (que o tráfego deve ser reorientado, e o nome do Access Control List (ACL) definido localmente no WLC)
- URL-reorientar (onde reorientar esse tráfego ao ISE)

Etapa 2. Um usuário convidado é reorientado ao ISE, aceita o AUP, e fornece opcionalmente um código de acesso secreto.

Etapa 3. O ISE envia uma mudança do RAIO da Admin-restauração da autorização (CoA) ao WLC. O WLC autentica novamente o usuário quando envia a solicitação de acesso do RAIO. O ISE responde com a aceitação de acesso e Airespace ACL definidos localmente no WLC, que fornece o acesso ao Internet somente.

Note: A Admin-restauração CoA é específica para a funcionalidade do ponto quente e é descrita na identificação de bug Cisco [CSCus46754](#). O comportamento para a versão 1.2 ISE com um portal do convidado era diferente; um CoA autentica novamente ou Terminate foi enviada.

Etapa 4. Um usuário convidado deseja o acesso à rede. O administrador de rede está certo que o usuário aceitou o AUP. O usuário convidado pode ser reorientado à URL original, a uma URL estático-configurada, ou a uma página do sucesso. Todas as páginas indicadas pelo ISE podem ser personalizadas.

A integração com uma verificação opcional da postura é apresentada na última seção.

Configurar

WLC

1. Adicionar o servidor Radius novo para a autenticação e a contabilidade. Navegue à **Segurança > ao AAA > ao raio > à autenticação** a fim permitir CoA do RAIO (RFC 3576).

Há uma configuração similar para explicar. Igualmente recomenda-se configurar o WLC para

enviar o SSID no atributo da estação chamada ID, que permite que o ISE configure as regras flexíveis baseadas no SSID:

2. Sob os WLAN catalogue, crie o ponto quente do Wireless LAN (WLAN) e configurar a relação correta. Ajuste a Segurança Layer2 a **nenhuns** com filtração MAC. Em server da Segurança/Authentication, Authorization, and Accounting (AAA), selecione o endereço IP de Um ou Mais Servidores Cisco ICM NT ISE para a autenticação e a contabilidade (a contabilidade é opcional). No guia avançada, permita a **ultrapassagem AAA** e ajuste o estado do Network Admission Control (NAC) ao RAIO NAC (apoio CoA).
3. Navegue à **Segurança > às listas de controle de acesso > às listas de controle de acesso** e crie duas Listas de acesso:

HotspotRedirect, que permite o tráfego que não deve ser reorientado e reorienta todo tráfego restanteInternet, que é negado para redes corporativas e permitido para todo o outro

Está aqui um exemplo de HotspotRedirect ACL (necessidade de excluir o tráfego para/desde o ISE da reorientação):

ISE

1. Navegue ao **acesso do convidado > configuram > portais do convidado**, e criam um tipo portal novo, portal do convidado do ponto quente:
2. Escolha o nome portal que será provido no perfil da autorização. A fim personalizar o portal dos ajustes portais do comportamento e do fluxo, permita o AUP, e um código secreto (opcional):

Diversas mais opções podem ser permitidas sob a personalização portal da página; todas as páginas apresentadas podem ser personalizadas.

3. Navegue à **política > aos resultados > à autorização > ao perfil da autorização** a fim configurar perfis da autorização.

Ponto quente (com reorientação ao nome portal do ponto quente e ao ACL HotspotRedirect):

Internet (com Airespace o ACL iguala o Internet):

4. A fim verificar as regras da autorização, navegue à **política > à autorização**. Na versão 1.3 ISE à revelia para o acesso falhado do desvio da autenticação de MAC (MAB) (MAC address não encontrado), a autenticação é continuada (não rejeitado). Isto é muito útil para portais do convidado porque não há nenhuma necessidade de mudar qualquer coisa nas regras da autenticação padrão.

Para a primeira autenticação MAB, a segunda regra é combinada (o valor-limite não está ainda em qualquer grupo da identidade). Então o usuário é reorientado a um webportal (ponto quente), aceita o AUP, e datilografa opcionalmente o código de acesso secreto correto. O ISE envia um CoA do RAIO e o WLC executa a reautenticação. Para a segunda autenticação, a primeira regra é combinada junto com o perfil PermitInternet da autorização e retorna o nome ACL que é aplicado no WLC (esta vez, o valor-limite está já no grupo de GuestEndpoints).

À revelia, os convidados que aceitam o AUP são postos no grupo da identidade de GuestEndpoints. O grupo da identidade que é atribuído para aqueles valores-limite é configurado sob a configuração portal do convidado, que pode ser diferente para cada portal.

5. Adicionar o WLC como um dispositivo do acesso de rede da **administração > dos recursos de rede > dos dispositivos de rede**.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

1. Depois que os usuários convidado associam com o ponto quente SSID e datilografam uma URL, estão reorientados ao AUP:
2. Se o código de acesso foi configurado sob o portal do convidado, a seguir exige-se. Se o usuário fornece um código incorreto, exibições de erros:
3. Está aqui a tela que indica se o código correto é dado entrada:
4. Uma vez que o código correto é dado entrada, o WLC executa a reautenticação e apresenta o Internet ACL anexado à sessão.

Postura adicional

Se há uma necessidade de fornecer o acesso aos usuários convidado, mas somente quando satisfazem uma política específica (postura) como atualizações anti-vírus frescas e atualizações de Microsoft Windows, a seguir pode ser realizada com estas regras:

A regra do ponto quente não fornecerá o acesso ao Internet, mas executa pelo contrário a reorientação a um serviço da postura. Então o agente da Web pode ser empurrado para a estação (o abastecimento do cliente ordena) e executar verificações da política (regras da postura). A conformidade do relatório é enviada pelo agente da Web ao ISE. Depois que a estação é complacente, o ISE envia um outro CoA reauthenticate, que provoque uma atualização da autorização no WLC. A regra de HotSpot_Compliant é encontrada então e o acesso ao Internet é fornecido.

A configuração da postura com NAC ou agente da Web é muito similar como na versão 1.2 ISE e é fora do espaço para este documento (veja a seção Informação Relacionada para mais informação).

Troubleshooting

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

O ISE deve apresentar:

Está aqui o fluxo:

- O usuário convidado encontra a segunda regra da autorização e é reorientado ao ponto quente (“autenticação sucedida”).
- Depois que o usuário aceita o AUP, o ISE envia a Admin-restauração CoA, que é confirmada pelo WLC (“autorização dinâmica sucedida”).
- O WLC executa a reautenticação, e o nome ACL é retornado (“Autorizar-Somente sucedeu”).

Isto pode igualmente ser verificado se você navega às **operações > aos relatórios > ao ISE relata > relatórios do acesso do convidado > de aceitação AUP estado:**

Informações Relacionadas

- [Serviços da postura no manual de configuração de Cisco ISE](#)
- [Guia de administradores de Cisco ISE 1.3](#)
- [Autenticação da Web central no exemplo de configuração WLC e ISE](#)
- [Autenticação da Web central com FlexConnect AP em um WLC com exemplo de configuração ISE](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)