Configurar o Sem fio CWA ISE e o ponto quente flui com AireOS e próxima geração WLC

Índice

Introdução

Este documento descreve como configurar três casos do uso do convidado no Identity Services Engine (ISE) com Cisco AireOS e controladores seguintes do Wireless LAN de Generation(NGWC) (WLC).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controladores de LAN do Cisco Wireless (unificados e acesso convirgido)
- Identity Services Engine (ISE)

Componentes Utilizados

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

- Versão 2.1 do Cisco Identity Services Engine
- Controlador de LAN 5508 8.0.121.0 sendo executado do Cisco Wireless
- Catalizador wireless do controlador da próxima geração (NGWC) 3850(WS-C3850-24P) 03.06.04.E sendo executado

Configurar

Diagrama de Rede

As etapas cobertas neste documento descrevem a configuração típica no acesso unificado e convirgido WLC para apoiar todo o fluxo do convidado com ISE.

Configurar unificou 5508 WLC

Apesar do exemplo do uso configurado no ISE, da perspectiva WLC todo começa com um ponto final Wireless que conecte a um SSID aberto com a filtração MAC permitida (mais a ultrapassagem AAA e o RAIO NAC) esses pontos ao ISE como a autenticação e o servidor de contabilidade. Isto assegura-se de que o ISE possa dinamicamente empurrar os atributos necessários para o WLC para a aplicação bem sucedida de uma reorientação para o portal do convidado do ISE.

Configuração global

1. Adicionar o ISE globalmente como uma autenticação e um servidor de contabilidade.

   - Navegue à **Segurança > ao AAA > à autenticação** e clique **novo**

   - Incorpore o IP de servidor ISE e o segredo compartilhado
   - Assegure-se de que o status de servidor e o **apoio para o RFC 3676** (mudança do apoio da autorização ou CoA) sejam ambos grupo ao **permitido**.
   - Sob o timeout de servidor à revelia AireOS os WLC terão 2 segundos. Segundo as

características de rede (latência, ISE e WLC em lugar diferentes, etc.) pode ser benéfico aumentar o timeout de servidor pelo menos aos segundos 5 para evitar eventos desnecessários do Failover.
- Clique em Apply.
- Se há os Nós dos serviços da política múltipla (PSN) a configurar continuam criar entradas de servidor adicionais.

Note: Este exemplo da configuração específica inclui 2 exemplos ISE

- Navegue à **Segurança > ao AAA > ao RAIO > à contabilidade** e clique **novo**
- Incorpore o IP de servidor ISE e o segredo compartilhado
- Assegure-se de que o status de servidor esteja ajustado ao permitido
- Aumente o timeout de servidor caso necessário (o padrão é 2 segundos).

2. Configuração da reserva.

No ambiente unificado uma vez que o timeout de servidor é provocado o WLC move-se para o servidor configurado seguinte. Em seguida na linha do WLAN. Se não outro está disponível então o WLC seleciona seguinte na lista global dos server. Quando os servidores múltiplos forem configurados no SSID (preliminar, secundário, etc.) uma vez que que o Failover ocorre o WLC continua à revelia a enviar o tráfego da autenticação e (ou) da contabilidade permanentemente ao exemplo secundário mesmo se o servidor primário é para trás em linha.

A fim abrandar este comportamento permita a reserva. Navegue à **Segurança > ao AAA > ao RAIO > à reserva.** O comportamento padrão está. A única maneira de recuperar de um evento do server-para baixo exige a intervenção admin (salte globalmente o status administrativo do server).

Para permitir a reserva você tem duas opções:

- **Passivo** - No modo passivo, se um server não responde ao pedido de autenticação WLC, o WLC move o server para a fila inativa e ajusta um temporizador (intervalo na opção do segundo). Quando o temporizador expira, o WLC move o server para a fila ativa independentemente do status real dos server. Se o pedido de autenticação conduz a um evento do intervalo (que significa que o server é ainda para baixo) que a entrada de servidor está movida outra vez para a fila inativa e o temporizador retrocede dentro outra vez. Se o server responde com sucesso para trás, permanece na fila ativa. Os valores configurável aqui vão 180 a 3600 segundos.

- **Ativo -** No modo ativo, quando um server não responde ao pedido de autenticação WLC, o WLC marca o server como inoperante, a seguir move o server para o pool NON-ativo do server e começa-o enviar mensagens da ponta de prova periodicamente até que esse server responda. Se o server responde, a seguir o WLC move o servidor inoperante para o pool ativo e para-o de enviar mensagens da ponta de prova.

Neste modo o WLC exige-o incorporar um username e um intervalo da ponta de prova aos segundos (180 3600).

Note: A ponta de prova WLC não exige uma autenticação bem sucedida. De qualquer maneira, um bem sucedido ou as autenticações falha são considerados uma resposta de servidor que seja bastante para promover o server à fila ativa.

Configurar o Service Set Identifier (SSID) do convidado:

- Navegue à aba WLAN e crie abaixo o clique novo da opção **vão**:

- Dê entrada com o nome de perfil e o nome SSID. Clique em Apply.
- Sob o tab geral selecione a relação ou o grupo de interface a ser usados (convidado VLAN).

- Sob a **Segurança > a camada 2 > a Segurança da camada 2** seleta **nenhuns** e permite a caixa de seleção de **filtração do Mac**.

- Sob autenticação ajustada e servidores de contabilidade da aba dos **servidores AAA permitiu** e selecionam seus preliminar e servidores secundários.

- **Atualização provisória**: Esta é uma configuração opcional que não adicione nenhuns benefícios a este fluxo. Se você prefere a permitir, o WLC eu devo executar 8.x ou um código mais alto:

Deficiente: A característica é desabilitada completamente.

Permitido com 0 intervalos: O WLC envia atualizações da contabilidade ao ISE cada vez que há uma mudança na entrada móvel de Block(MSCB) do controle de estação do cliente (IE. O IPv4 ou a atribuição de endereço ou a mudança do IPv6, o evento vagueando do cliente, etc.) nenhumas atualizações periódicas adicionais são mandados.

Permitido com um intervalo provisório configurado: Neste modo o WLC envia notificações ao ISE em cima das mudanças da entrada MSCB do cliente e igualmente envia notificações periódicas adicionais da contabilidade no intervalo configurado (apesar de algumas mudanças).

- Sob o guia avançada permita **permitem a ultrapassagem AAA** e sob o **estado NAC** selecione o **RAIO NAC**. Isto assegura-se de que o WLC aplique todos os pares de valor de atributo (AVP) que vierem do ISE.
- Navegue ao tab geral SSID e ajuste o estado SSID ao **permitido**

- **Aplique as** mudanças.

Configurar a reorientação ACL

Este ACL é provido pelo ISE e determina que tráfego obtém reorientado e que tráfego será permitido completamente.

- Vá à **ABA de segurança >** às **listas de controle de acesso** e clique **novo**
- Este é um exemplo do ACL

Este ACL deve permitir o acesso a e dos serviços DNS e dos Nós ISE sobre a porta TCP 8443. Há um implícito nega na parte inferior que significa que o resto do tráfego obtém reorientado ao portal URL do convidado do ISE.

O HTTPS reorienta

Esta característica é apoiada em versões 8.0.x de AireOS e levanta mas é desligada à revelia. Para permitir o apoio HTTPS vá ao **Gerenciamento** WLC > ao **HTTP-HTTPS > ao redirecionamento em https** e ajuste-o **permitido** ou aplique-o este comando no CLI:

```
(Cisco Controller) >config network web-auth https-redirect enable
```

Os avisos do certificado após o HTTPS reorientam são permitidos

Depois que https-reoriente é permitido, o usuário pode experimentar edições da confiança do certificado durante a reorientação. Isto é visto mesmo se há um certificado acorrentado válido no controlador e mesmo se este certificado é assinado por um Certificate Authority confiado 3ª parte. A razão é que o certificado instalado no WLC está emitido a seu hostname ou endereço IP de Um ou Mais Servidores Cisco ICM NT da interface virtual. Quando o cliente tentar https: //cisco.com, o navegador espera o certificado ser emitido a cisco.com. Contudo, porque o WLC a poder interceptar o GET emitido pelo cliente, precisa primeiramente de estabelecer a sessão HTTPS para que o WLC apresenta seu certificado da interface virtual durante a fase da saudação de SSL. Isto faz com que o navegador indique um aviso porque o certificado apresentado durante a saudação de SSL não foi emitido ao site que original o cliente está tentando alcançar (IE. cisco.com opôs ao hostname da interface virtual do WLC). Você pôde ver Mensagens de Erro diferentes do certificado em navegadores diferentes mas em todos relacionar-se ao mesmo problema.

Failover agressivo

Esta característica é permitida à revelia em AireOS WLC. Quando o Failover agressivo é permitido, o WLC marca o servidor AAA enquanto sem resposta e ele se move para o servidor AAA configurado seguinte depois que um evento do intervalo do raio afeta um cliente.

Quando a característica está desabilitada o WLC falha sobre ao server seguinte somente se o evento do intervalo do RAIO ocorre com pelo menos 3 sessões cliente. Esta característica pode ser desabilitada por este comando (nenhuma repartição é exigida para este comando):

```
(Cisco Controller) >config radius aggressive-failover disable
```

Para verificar o status atual da característica:

```
(Cisco Controller) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

Desvio prisioneiro

Os valores-limite que apoiam um assistente de rede prisioneiro (PODEM) mecanismo descobrir um cativo-portal e auto-lançamento que uma página do fazer logon faz geralmente esta através de um pseudo--navegador em um indicador controlado quando outros valores-limite lançarem um navegador inteiramente capaz para provocar este. Para os valores-limite onde a LATA lança um pseudo--navegador, isto pode quebrar o fluxo quando reorientado a um portal do cativo ISE. Isto afeta tipicamente dispositivos de IOS de Apple e tem especialmente efeitos negativos nos fluxos

que exigem o registro do dispositivo, o VLAN DHCP-Rlease, a verificação da conformidade, etc.

Segundo a complexidade do fluxo no uso pode-se recomendar permitir o desvio prisioneiro. Em tal encenação, o WLC ignora o mecanismo de descoberta portal da LATA e o cliente precisa de abrir um navegador para iniciar o processo da reorientação.

Verifique o estado da característica:

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..................... Disabled
Web Auth Redirect Ports ................... 80,3128
Web Auth Proxy Redirect  .................. Disable
Web Auth Captive-Bypass   ................. Disabled
Web Auth Secure Web  ...................... Enable
Web Auth Secure Redirection  .............. Enable
```

Para permitir este tipo da característica este comando:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.
```

O WLC alerta o usuário que para que as mudanças tomem a efeito um restauração-sistema (reinício) são precisadas.

Neste momento um **sumário da rede da mostra** mostra a característica como permitida, mas para que as mudanças tomem a efeito o WLC precisam de ser reiniciadas.

Configurar convirgiu 3850 NGWC

Configuração global

1. **Adicionar o ISE globalmente como uma autenticação e um servidor de contabilidade**
   - Navegue ao **> segurança > ao RAIO > aos server da configuração** e clique **novo**
   - Incorpore o **endereço IP do servidor** ISE, o **segredo compartilhado**, o **timeout de servidor** e o **contagem de novas tentativas** que reflete suas condições ambientais.
   - Assegure-se de que o **apoio para o RFC 3570** (apoio CoA) esteja permitido.
   - Repita o processo para adicionar uma entrada do servidor secundário.
2. **Crie o grupo de servidor do ISE**
   - Navegue ao **> segurança > aos grupos de servidor da configuração** e clique **novo**
   - Atribua um nome ao grupo e incorpore um valor de **período inoperante aos** minutos. Este é o tempo que o controlador mantém o server na fila inativa antes que esteja promovido outra vez à lista do servidor ativo.
   - Da lista disponível dos server adicionar-los à coluna de servidores atribuída.
3. **Permita globalmente o dot1x**
   - Navegue à **configuração > ao AAA > às listas de método > ao general** e permita o **controle do**

AUTH do sistema do dot1x

4. Configurar listas de método

- Navegue à **configuração** > ao **AAA** > às **listas de método** > à **autenticação** e crie uma lista de método nova. Neste caso é tipo dot1x e grupo ISE_Group (grupo criado na etapa precedente). Então a batida **aplica-se**

- Faça o mesmos para explicar (**configuração > AAA > listas de método > contabilidade**) e a autorização (**configuração > AAA > listas de método > autorização**). Devem olhar como este

5. **Crie o método do MAC-filtro da autorização**.

Isto é chamado dos ajustes SSID mais atrasado.

- Navegue a **Configuration> AAA > listas de método > autorização** e clique **novo**.
- Dê entrada com o **nome da lista de método**. Escolheu o **tipo = o grupo da rede** e do **tipo de grupo**.
- Adicionar ISE_Group aos grupos de servidor atribuídos campo.

Configuração SSID

1. **Crie o convidado SSID**

- Navegue à **configuração > ao Sem fio > aos WLAN** e clique **novo**
- Dê entrada com o ID de WLAN, o SSID e o nome de perfil e o clique aplica-se.
- Uma vez nos ajustes SSID sob a relação/grupo de interface selecione a relação da camada 3 do convidado VLAN.

- Sob a **Segurança** > a **camada 2** seletas **nenhuns** e ao lado da **filtração do Mac** dão entrada com o nome que da lista de método do filtro do Mac você configurou previamente (MacFilterMethod).
- Sob a **Segurança** > a aba do **servidor AAA** selecione a autenticação apropriada e as lista dos métodos de contabilidade (ISE_Method).

- Sob o **guia avançada** permita **permitem a ultrapassagem AAA** e o **estado NAC.** O resto dos ajustes deve ser ajustado conforme as exigências de cada desenvolvimento (timeout de sessão, exclusão do cliente, apoio para extensões Aironet, etc.).

- Navegue ao tab geral ajustam o estado ao permitido. Então a batida **aplica-se.**

Reoriente a configuração ACL

Este ACL é provido pelo ISE mais tarde na aceitação de acesso em resposta ao pedido inicial MAB. O NGWC usa-o para determinar que tráfego a reorientar e que tráfego deve ser permitido completamente.

- Navegue ao **> segurança da configuração > ao ACL > às listas de controle de acesso** e o clique **adiciona novo**.
- Selecione prolongado e dê entrada com o nome ACL.
- Esta imagem mostra que um exemplo de um típico reorienta o ACL:

Note: A linha 10 é opcional. Isto é adicionado geralmente pesquisando defeitos propõe. Este ACL deve permitir o acesso ao DHCP, serviços DNS e igualmente à porta de server TCP ISE 8443(Deny ACE). O tráfego HTTP e HTTPS obtém reorientado (licença ACE).

Configuração do comando line interface(cli)

Toda a configuração discutida em etapas precedentes pode igualmente ser aplicada com o CLI.

802.1x permitido globalmente

```
dot1x system-auth-control
```

Configuração de AAA global

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 14.36.157.210 server-key *****
 client 14.36.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 14.36.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
 address ipv4 14.36.157.21 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
!
aaa group server radius ISE_Group
 server name ISE2
 server name ISE1
 deadtime 10
 mac-delimiter colon
!
```

Configuração de Wlan

```
 wlan Guest 1 Guest
 aaa-override
```

```
 accounting-list ISE_Method
 client vlan VLAN0301
 mac-filtering MacFilterMethod
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE_Method
 no security ft over-the-ds
 session-timeout 28800
 no shutdown
```

Reoriente o exemplo de ACL

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
    10 deny icmp any any
    20 deny udp any any eq bootps
    30 deny udp any any eq bootpc
    40 deny udp any any eq domain
    50 deny tcp any host 14.36.157.210 eq 8443
    60 deny tcp any host 14.36.157.21 eq 8443
    70 permit tcp any any eq www
    80 permit tcp any any eq 443
```

Apoio HTTP e HTTPS

```
3850#show run | inc http
ip http server
ip http secure-server
```

Note: Se você aplica um ACL para restringir o acesso ao WLC sobre o HTTP, afeta a reorientação.

Configurar o ISE

Esta seção descreve a configuração exigida no ISE para apoiar todos os exemplos dos usos discutida neste documento.

Tarefas de configuração comuns ISE

1. Entre ao ISE e navegue à **administração > aos recursos de rede > aos dispositivos de rede** e o clique **adiciona**
2. Dê entrada com o **nome** associado ao WLC e ao **endereço IP de Um ou Mais Servidores Cisco ICM NT do** dispositivo.
3. Verifique a caixa dos **ajustes da autenticação RADIUS** e datilografe o **segredo compartilhado** configurado no lado WLC. Clique então **submetem-se**.

4. Navegue à **política > à autenticação** e sob o clique **MAB edite** e assegure isso sob o **uso:**

Os valores-limite internos a opção se o **usuário não é encontrado** são ajustados **para continuar** (deve estar lá à revelia).

Use o caso 1: CWA com autenticação do convidado em cada conexão do usuário

Vista geral do fluxo

1. O usuário Wireless conecta ao convidado SSID.
2. O WLC autentica o valor-limite baseado em seu MAC address usando o ISE como o servidor AAA.
3. O ISE retorna para trás e aceitação de acesso com dois pares de valor de atributo (AVP): URL-reoriente e URL-reorientar-ACL. Uma vez que o WLC aplica este AVP à sessão do valor-limite, as transições da estação ao DHCP-exigido e uma vez que agarra um endereço IP de Um ou Mais Servidores Cisco ICM NT fica em CENTRAL_WEB_AUTH. Nesta etapa o WLC está pronto para começar reorientar o tráfego HTTP/https do cliente.
4. O utilizador final abre o navegador da Web e uma vez que o tráfego HTTP ou HTTPS é gerado, o WLC reorienta o usuário ao portal do convidado ISE.
5. Uma vez que o usuário obtém ao portal do convidado alerta para incorporar as credenciais do convidado (patrocinador-criadas neste caso).
6. Em cima da validação das credenciais o ISE indica a página AUP e uma vez que o cliente aceita, um tipo dinâmico Re-authenticate CoA é mandado ao WLC.
7. Os re-processos WLC a autenticação de filtração MAC sem emitir uma de-autenticação à estação móvel. Isto deve ser sem emenda ao valor-limite.
8. Uma vez que o evento da reautenticação acontece o ISE reavalia políticas da autorização e esta vez o valor-limite é dado um acesso da licença desde que havia um evento bem sucedido precedente da autenticação do convidado.

Este processo repete-se cada vez que o usuário conecta ao SSID.

Configuração

1. Navegue ao ISE e navegue aos **centros de trabalho > ao acesso do convidado > configuram > portais do convidado >** selecionam o **portal patrocinado do convidado** (ou crie um tipo portal novo Patrocinar-convidado).
2. Sob o **registro do dispositivo do convidado os** ajustes desmarcam todas as opções e clicam a **salvaguarda**.

3. Navegue à **política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização**. Clique em Add.

4. Este perfil é abaixado para o WLC a Reorientar-**URL** e o Reorientar-URL-**ACL** em resposta ao pedido inicial do desvio da autenticação do Mac (MAB).

- Uma vez o **AUTH centralizado** seleto verificado da **Web da reorientação da Web (CWA, MDM, NSP, CPP)**, então datilografa o nome da reorientação ACL sob o campo **ACL** e sob o **valor** seleciona o **convidado patrocinado Portal(default)** (ou algum outro portal específico criado em etapas precedentes).

O perfil deve olhar similar esse nesta imagem. Clique então a **salvaguarda**.

Os detalhes do atributo na parte inferior da página o valor de atributo Pairs(AVPs) como são sejam empurrados para o WLC

5. Navegue à **política > à autorização** e introduza uma regra nova. Esta regra é essa que provoca o processo da reorientação em resposta ao pedido inicial da autenticação de MAC do WLC. (Neste caso chamado **Wireless_Guest_Redirect**).

6. Sob **circunstâncias** escolha a **condição existente seleta da biblioteca**, a seguir sob a **circunstância composta** seleta de **nome de condição**. Selecione uma condição composta predefinida chamada **Wireless_MAB**.

> **Note**: Esta circunstância consiste em 2 atributos RADIUS esperados no formulário originado pedido do acesso o WLC (IEEE 802.11 de NAS-Port-Type= <present em todo o requests> e tipo de serviço = atendimento wireless Check< que refere um pedido específico para um bypass> da autenticação do Mac)

7. Sob resultados, **padrão** seleto > **CWA_Redirect** (perfil da autorização criado na etapa precedente). Clique então **feito** e **salvaguarda**

8. Navegue ao fim da regra de **CWA_Redirect** e clique a seta ao lado de **editam**. Selecione então a **duplicata acima**.

9. Altere o nome porque esta é a política essa os fósforos do valor-limite a sessão é autenticar novamente uma vez que em cima do CoA do ISE (neste caso Wireless_Guest_Access).

10. Ao lado da condição composta de **Wireless_MAB** clique **+** símbolo para expandir as condições e para o fim do clique da condição de **Wireless_MAB adicionar o atributo/valor**.

11. Sob “o atributo seleto” escolheu o **acesso de rede > o fluxo do convidado dos iguais de UseCase**

12. Sob **permissões** selecione **PermitAccess**. Clique então **feito** e **salvaguarda**

As duas políticas devem olhar similares a esta:

Use o caso 2: CWA com o registro do dispositivo que reforça a autenticação do convidado uma vez por dia.

Vista geral do fluxo

1. O usuário Wireless conecta ao convidado SSID.
2. O WLC autentica o valor-limite baseado em seu MAC address usando o ISE como o servidor AAA.
3. O ISE retorna para trás e aceitação de acesso com dois pares de valor de atributo (AVP) (URL-reoriente e URL-reorientar-ACL).
4. Uma vez que o WLC aplica este AVP à sessão do valor-limite, as transições da estação ao DHCP-exigido e uma vez que agarra um endereço IP de Um ou Mais Servidores Cisco ICM NT fica em CENTRAL_WEB_AUTH. Nesta etapa o WLC está pronto para começar

reorientar o tráfego HTTP/https do cliente.
5. O utilizador final abre o navegador da Web e uma vez que o tráfego HTTP ou HTTPS é gerado, o WLC reorienta o usuário ao portal do convidado ISE.
6. Uma vez que o usuário obtém ao portal do convidado, obtém alertado para incorporar credenciais patrocinador-criadas.
7. Em cima da validação das credenciais o ISE adiciona este valor-limite a um grupo (PRE-configurado) específico da identidade do valor-limite (registro do dispositivo).
8. A página AUP é indicada e uma vez que o cliente aceita, um tipo dinâmico CoA autenticar novamente. É mandado ao WLC.
9. O re-processo WLC a autenticação de filtração MAC sem emitir uma de-autenticação à estação móvel. Isto deve ser sem emenda ao valor-limite.
10. Uma vez que o re evento da autenticação acontece o ISE reavalia políticas da autorização. Esta vez desde que o valor-limite é membro do grupo direito ISE da identidade do valor-limite retorna um acesso aceita sem limitações.
11. Desde que o valor-limite esteve registrado na etapa 6, cada vez que aquele o usuário volta, está permitido na rede até que esteja removida manualmente do ISE, ou uma política da remoção do valor-limite executa o nivelamento dos valores-limite que encontram os critérios.

Neste cenário de laboratório, a autenticação é reforçada uma vez por dia. O disparador da reautenticação é a política da remoção do valor-limite que remove todos os valores-limite da identidade usada do valor-limite agrupa cada dia.

> **Note**: É possível reforçar o evento da autenticação do convidado baseado no tempo transcorrido desde a última aceitação AUP. Esta pode ser uma opção se você precisa de reforçar mais frequentemente o fazer logon do convidado que uma vez por dia (no exemplo cada 4 horas).

Configuração

1. No ISE navegue aos **centros de trabalho > ao acesso do convidado > configuram > portais do convidado >** selecionam o **portal patrocinado do convidado** (ou crie um tipo portal novo Patrocinar-convidado).
2. Sob ajustes do **registro do dispositivo do convidado** verifique que a opção **registra automaticamente o convidado que os dispositivos** são verificados. Click **Save**.

3. Navegue ao **centro de trabalho > ao acesso do convidado > configuram > tipos do convidado** ou apenas clicam sobre o atalho especificado sob ajustes do registro do dispositivo do convidado no portal.

4. Quando o usuário do patrocinador cria uma conta do convidado, atribui-lhe um tipo do convidado. Cada tipo individual do convidado pode ter um valor-limite registrado que pertença a uma identidade diferente Group.To do valor-limite atribua o grupo que da identidade do valor-limite o dispositivo deve ser adicionado a, selecione o tipo do convidado os usos do patrocinador para estes usuários convidado (este caso do uso é baseado no semanário (padrão)).

5. Uma vez no tipo do convidado, sob **opções do início de uma sessão** selecione o grupo do valor-limite do **grupo da identidade do valor-limite do** menu de gota para baixo **para o registro do dispositivo do convidado**

6. Navegue à **política > aos elementos da política > aos resultados > à autorização > aos perfis da**

autorização. Clique em Add.

7. Este perfil é abaixado para o WLC a Reorientar-**URL** e o Reorientar-URL-**ACL** em resposta ao pedido inicial do desvio da autenticação do Mac (MAB).

- Uma vez o **AUTH centralizado** seleto verificado da **Web da reorientação da Web (CWA, MDM, NSP, CPP)**, então datilografa o nome da reorientação ACL sob o campo **ACL** e sob o **valor** seleciona o portal criado para este fluxo (**CWA_DeviceRegistration**).

8. Navegue à **política > à autorização** e introduza uma regra nova. Esta regra é essa que provoca o processo da reorientação em resposta ao pedido inicial da autenticação de MAC do WLC. (Neste caso chamado **Wireless_Guest_Redirect**).

9. Sob **circunstâncias** escolheu a **condição existente seleta da biblioteca**, a seguir sob a **circunstância composta** seleta de **nome de condição**. Selecione uma condição composta predefinida chamada **Wireless_MAB**.

10. Sob resultados, **padrão** seleto **> CWA_DeviceRegistration** (perfil da autorização criado na etapa precedente). Clique então **feito** e **salvaguarda**

11. Duplique a política acima, altere seu nome porque esta é a política que o valor-limite bate depois que retorna do evento da reautenticação (chamado Wireless_Guest_Access).

12. Sob o **grupo da identidade detalha a** caixa, **grupo** seleto da **identidade do valor-limite** e selecionam o grupo que você proveu sob o convidado Type(GuestEndpoints).

13. Sob resultados selecione **PermitAccess**. Clique **feito** e **salvar as** mudanças.

14. Crie e o política da remoção do valor-limite que cancela o grupo de GuestEndpoint diário.

- Navegue à **administração >** ao **Gerenciamento de identidades >** aos **ajustes >** à **remoção do valor-limite**
- Sob regras da **remoção** deve haver uma à revelia esse supressão de GuestEndpoints dos disparadores se o tempo transcorrido é maior de 30 dias.
- Altere a política existente para GuestEndpoints ou crie um novo (caso que o padrão foi removido). Note que as políticas da remoção executam cada dia um o horário definido.

Neste caso a circunstância é membros de GuestEndpoints com dias decorridos menos de 1 dia

Use o caso 3: Portal de HostSpot

Vista geral do fluxo

1. O usuário Wireless conecta ao convidado SSID.
2. O WLC autentica o valor-limite baseado em seu MAC address usando o ISE como o servidor AAA.
3. O ISE retorna para trás uma aceitação de acesso com dois pares de valor de atributo (AVP): URL-reoriente e URL-reorientar-ACL.
4. Uma vez que o WLC aplica este AVP à sessão do valor-limite, as transições da estação ao DHCP-exigido e uma vez que agarra um endereço IP de Um ou Mais Servidores Cisco ICM NT fica em CENTRAL_WEB_AUTH. Nesta etapa o WLC está pronto para reorientar o tráfego HTTP/https do cliente.

5. O utilizador final abre o navegador da Web e uma vez que o tráfego HTTP ou HTTPS é gerado, o WLC reorienta o usuário ao portal do ponto quente ISE.
6. Uma vez no portal o usuário é alertado aceitar uma política de uso aceitável.
7. O ISE adiciona o MAC address do valor-limite (ID de ponto final) no grupo da identidade do ponto final configurado.
8. A política presta serviços de manutenção ao nó (PSN) esse processos que o pedido emite um tipo dinâmico Admin-**restauração** CoA ao WLC.
9. Uma vez que o WLC termina processar o CoA entrante, emite uma de-autenticação ao cliente (a conexão é perda pelo tempo onde toma para que o cliente volte).
10. Uma vez que o cliente reconecta, uma sessão nova não está criada tão lá é nenhuma continuidade da sessão no lado ISE. Significa que a autenticação está processada como uma linha nova.
11. Desde que o valor-limite é adicionado ao grupo da identidade do ponto final configurado, e há uma política da autorização que verifique se o valor-limite é parte de esse grupo, a autenticação nova combina esta política. O resultado é acesso direto à rede de convidado.
12. O usuário não deve ter que aceitar outra vez o AUP a menos que o objeto da identidade do valor-limite for removido do base de dados ISE em consequência de uma política da remoção do valor-limite.

Configuração

1. Crie um grupo novo da identidade do valor-limite para mover estes dispositivos para em cima do registro. Navegue aos **centros de trabalho > ao acesso > à identidade do convidado agrupa > grupos da identidade do valor-limite** e clicam .

- Dê entrada com um nome do grupo (neste caso HotSpot_Endpoints). Adicionar uma descrição e nenhum grupo de pai é precisado.

2. Navegue aos **centros de trabalho > ao acesso do convidado > configuram > portais do convidado > portal** seleto do **ponto quente (padrão**).

3. Expanda ajustes portais e sob o grupo seleto de **HostSpot_Endpoints do** grupo da identidade do valor-limite sob o **grupo da identidade do valor-limite.** Isto envia os dispositivos registrados ao grupo especificado.

4. **Salvar as** mudanças.

5. Crie o perfil da autorização que chama o portal do ponto quente em cima da autenticação MAB originada pelo WLC.

- Navegue aos **elementos da política > da política > aos resultados > à autorização > aos perfis da autorização** e crie um (HotSpotRedirect).
- Uma vez a **reorientação da Web (CWA, MDM, NSP, CPP)** é **ponto ativo** seleto verificado, a seguir datilografa o nome da reorientação ACL no campo ACL (Guest_Redirect) e como um portal correto seleto do valor (**portal do ponto quente (padrão)**).

6. Crie a política da autorização que provoca o resultado de HotSpotRedirect em cima do pedido inicial MAB do WLC.

- Navegue à **política > à autorização** e introduza uma regra nova. Esta regra é essa que

provoca o processo da reorientação em resposta ao pedido inicial da autenticação de MAC do WLC. (Neste caso chamado **Wireless_HotSpot_Redirect**).
- Sob **circunstâncias** escolha a **condição existente seleta da biblioteca**, a seguir sob a **circunstância composta** seleta de **nome de condição**
- Sob resultados, **padrão** seleto **> HotSpotRedirect** (perfil da autorização criado na etapa precedente). Clique então **feito** e **salvaguarda**

7. Crie a segunda política da autorização.

- Duplique a política acima, altere seu nome porque esta é a política que o valor-limite bate depois que retorna do evento da reautenticação (chamado Wireless_HotSpot_Access).
- Sob o **grupo da identidade detalha a** caixa, o **grupo** seleto da **identidade do valor-limite** e então o grupo que você criou mais cedo (**HotSpot_Endpoints**).
- Sob resultados selecione **PermitAccess**. Clique **feito** e **salvar as** mudanças.

8. Configurar a política da remoção que cancela valores-limite com um tempo transcorrido maior do que os dias 5.

- Navegue à **administração > ao Gerenciamento de identidades > aos ajustes > à remoção do valor-limite** e sob a remoção as regras criam um novo.
- Sob a caixa dos **detalhes do grupo da identidade** selecione o **grupo > o HotSpot_Endpoints da identidade do valor-limite**
- Sob o clique das **circunstâncias crie a condição nova (opção avançada)**.
- Sob o atributo seleto escolha *ENDPOINTPURGE:* Dias de *ElapsedDays GREATERTHAN* 5

Verificar

Use o caso 1

1. O usuário conecta ao convidado SSID.
2. Abre o navegador e assim que o tráfego de HTTP for gerado, o portal do convidado é indicado.
3. Uma vez que o usuário convidado autentica e aceita o AUP, uma página do sucesso está indicada.
4. Um CoA autenticar novamente é mandado (transparente ao cliente).
5. A sessão do valor-limite é autenticar novamente com acesso direto à rede.
6. Toda a conexão subsequente do convidado tem que passar a autenticação do convidado antes de aceder à rede.

Fluxo dos logs vivos do RAIO ISE:

Use o caso 2

1. O usuário conecta ao convidado SSID.
2. Abre o navegador e assim que o tráfego de HTTP for gerado, o portal do convidado é indicado.
3. Uma vez que o usuário convidado autentica e aceita o AUP, o dispositivo está registrado.
4. Uma página do sucesso é indicada e um CoA autenticar novamente é mandado (transparente ao cliente).
5. A sessão do valor-limite é autenticar novamente com acesso direto à rede.

6. Toda a conexão subsequente 9s do ventania permitiu sem reforçar a autenticação do convidado enquanto o valor-limite está ainda no grupo da identidade do ponto final configurado.

Fluxo dos logs vivos do RAIO ISE:

Use o caso 3

1. O usuário conecta ao convidado SSID.
2. Abre o navegador e assim que o tráfego de HTTP for gerado, uma página AUP é indicada.
3. Uma vez que o usuário convidado aceita o AUP, o dispositivo está registrado.
4. Uma página do sucesso é indicada e um CoA da Admin-restauração é mandado (transparente ao cliente).
5. O valor-limite reconecta com o acesso direto à rede.
6. Toda a conexão subsequente do ventania é permitida sem reforçar a aceitação AUP (a menos que é configurado de outra maneira) para enquanto o valor-limite permanece no grupo da identidade do ponto final configurado.

Switching local de FlexConnect em AireOS

Quando o switching local de FlexConnect é configurado a rede Admin precisa de assegurar aquela:

- Reoriente o ACL é configurado como um FlexConnect ACL.
- Reoriente o ACL foi aplicado como uma política de qualquer maneira com O AP próprio sob a aba de **FlexConnect > WebAuthentication externo ACL > políticas >** seleto reorientam o ACL e o clique **aplicam-se**

Ou adicionando a política o ACL ao grupo de FlexConnect pertence a (o **Sem fio > os grupos de FlexConnect >** selecionam o grupo correto **>** o **mapeamento > as políticas ACL** selecionam a reorientação ACL e o clique adicionam)

A adição da política ACL provoca o WLC para abaixar o ACL configurado para os membros AP do grupo de FlexConnect. A falha fazer isto conduz a uma Web reorienta a edição.

Encenação da Estrangeiro-âncora

Na auto-âncora (estrangeira – Encenações da âncora) é importante destacar os seguintes fatos:

- Reoriente o ACL precisa de ser definido no estrangeiro e na âncora WLC. Mesmo quando é reforçado somente na âncora.
- A autenticação da camada 2 é segurada sempre pelo WLC estrangeiro. Isto é crítico durante fases de concepção (também para pesquisar defeitos) como toda a autenticação RADIUS e o tráfego explicando ocorre entre o ISE e o WLC estrangeiro.

- A reorientação AVP é aplicada uma vez à sessão cliente que o WLC estrangeiro atualiza a sessão cliente na âncora através de uma mensagem da entrega da mobilidade.
- Neste momento a âncora WLC começa reforçar a reorientação usando o Reorientar-ACL que PRE-foi configurado.
- A contabilidade deve completamente ser desligada na âncora WLC SSID para evitar as

atualizações explicando que vão para o ISE (que provê o mesmo evento da autenticação) que vem ambos da âncora e estrangeiro.
- Os ACL baseados URL não são apoiados em encenações da Estrangeiro-âncora.

Troubleshooting

Estados quebrados comuns em AireOS e no acesso convirgido WLC

1. **O cliente é incapaz de juntar-se ao convidado SSID**

Da “um **cliente mostra detalhou xx: xx: xx: xx: xx: xx**” revelam que o cliente está colado no **COMEÇO**. Geralmente este é um indicador do WLC que é incapaz de aplicar um atributo que o servidor AAA retorna.

Verifique que o nome da reorientação ACL empurrou por fósforos ISE exatamente o nome do ACL predefinido no WLC.

O mesmo princípio aplica-se a todo o outro atributo que você configurou o ISE para abaixar para o WLC (VLAN ID, nomes da relação, Airespace-ACL, etc.). O cliente deve então transição ao DHCP e então ao CENTRAL_WEB_AUTH.

2. **Reoriente AVP são aplicados à sessão de cliente mas reorientam não está trabalhando**

Verifique que o estado do gerente da política do cliente é CENTRAL_WEB_AUTH com um endereço IP válido de acordo com a interface dinâmica configurada para o SSID e igualmente que a reorientação ACL e URL-reoriente atributos são aplicados à sessão de cliente.

Reoriente o ACL

Em AIreOS WLC a reorientação ACL deve explicitamente permitir o tráfego que não deve ser reorientado, como o DNS e o ISE na porta TCP 8443 nos ambos sentidos e o deny ip any any implícito provoca o resto do tráfego a ser reorientado.

No acesso convirgido a lógica é o oposto. Negue desvios ACE reorientam quando a licença ACE provocar a reorientação. Eis porque recomenda-se permitir explicitamente a porta TCP 80 e 443.

Verifique o acesso ao ISE sobre a porta 8443 do convidado VLAN. Se tudo olha bom da perspectiva da configuração a maneira a mais fácil de mover-se para a frente é agarrar uma captação atrás do adaptador Wireless do cliente e verificar aonde a reorientação quebra.

- O resoultion DNS acontece?
- O reconhecimento de sentido TCP 3 é terminado contra a página pedida?
- O WLC retorna uma ação da reorientação depois que o cliente inicia o GET?
- O reconhecimento de sentido TCP 3 contra o ISE sobre 8443 é terminado?

3. **O cliente é incapaz de alcançar a rede após o ISE empurrou uma alteração de VLAN no fim do fluxo do convidado**

Uma vez que o cliente agarrou um endereço IP de Um ou Mais Servidores Cisco ICM NT no início do fluxo (reoriente pre o estado), se uma alteração de VLAN está abaixada depois que a autenticação do convidado acontece (CoA do cargo autenticar novamente), a única maneira de forçar uma liberação DHCP/renova no convidado que o fluxo (sem agente da postura) é através de um Java applet que nos dispositivos móveis não trabalha.

Isto deixa o cliente preto-furado em VLAN X com um endereço IP de Um ou Mais Servidores Cisco ICM NT do VLAN Y. Isto deve ser considerado ao planejar a solução.

4. **O ISE mostra "o erro interno HTTP 500, mensagem não encontrada da sessão do raio" no convidado que o navegador de cliente durante reorienta**

Este é geralmente um indicador da perda de sessão no ISE (a sessão foi terminada). A maioria de motivo comum para este está explicando configurou na âncora WLC quando a Estrangeiro-âncora foi distribuída. Para fixar este desabilitação que explica na âncora e deixar a autenticação e explicar estrangeiros do punho.

5. **As disconexões do cliente e permanecem desligado ou conectam a um SSID diferente após ter aceitado o AUP no portal do ponto quente do ISE.**

Isto pode ser esperado no ponto quente devido à mudança dinâmica da autorização (CoA) envolvida neste fluxo (CoA Admin restaurado) esse causas o WLC emitir um deauth à estação wireless. A maioria dos pontos finais Wireless não tem nenhuma edições a vir para trás ao SSID depois que a de-autenticação acontece, mas em alguns casos o cliente conecta a um outro SSID preferido em resposta ao de-authenitcate evento. Nada pode ser feito do ISE ou do WLC para impedir isto como incumbe o cliente Wireless a colar ao SSID original, ou para conectá-lo a um outro SSID (preferido) disponível.

Neste caso o usuário Wireless deve manualmente conectar de volta ao ponto quente SSID.

AireOS WLC

(Cisco Controller) >debug client <MAC addr>

Debugar grupos do cliente PARA DEBUGAR um grupo de componentes envolvidos em mudanças da máquina de estado do cliente.

(Cisco Controller) >debug client <MAC addr>

Debugar componentes AAA

(Cisco Controller) >debug client <MAC addr>

Este pode ser recursos do impacto segundo a quantidade de usuários que conectam com MAB ou dot1x SSID. Estes componentes no nível de debug gravam transações AAA entre o WLC e o ISE e imprimem os pacotes de informação de RADIUS na tela.

Isto é crítico se você que o ISE não pode entregar os atributos previstos, ou se o WLC não os processa corretamente.

O Web-AUTH reorienta

(Cisco Controller) >debug client <MAC addr>

Isto pode ser usado para verificar que o WLC está provocando com sucesso a reorientação. Este é um exemplo de como a reorientação deve olhar como de debuga:

(Cisco Controller) >debug client <MAC addr>

NGWC

Debugar grupos do cliente PARA DEBUGAR um grupo de componentes envolvidos em mudanças da máquina de estado do cliente.

(Cisco Controller) >debug client <MAC addr>

Este componente imprime os pacotes de informação de RADIUS (autenticação e contabilidade) na tela. Isto é acessível quando você precisa de verificar que o ISE entrega os AVP direitos e para verificar igualmente que o CoA está sendo enviado e processado corretamente.

(Cisco Controller) >debug client <MAC addr>

Isto todas as transições AAA (autenticação, autorização e contabilidade) onde os clientes Wireless são involvidos. Isto é crítico para verificar que o WLC analisa gramaticalmente corretamente os AVP e os aplica à sessão cliente.

(Cisco Controller) >debug client <MAC addr>

Isto pode permitido quando você suspeita uma edição da reorientação no NGWC.

(Cisco Controller) >debug client <MAC addr>

ISE

Logs vivos do RAIO

Verifique que o pedido inicial MAB esteve processado corretamente no ISE e esse ISE empurra para trás os atributos previstos. Navegue às **operações > ao RAIO > logs vivos** e filtre a saída usando o cliente MAC sob o **ID de ponto final**. Uma vez que o evento da autenticação é encontrado, clique sobre detalhes e verifique então os resultados empurrados como parte da aceitação.

Tcpdump

Esta característica pode ser usada quando um olhar mais profundo na troca do pacote de informação de RADIUS entre o ISE e o WLC é precisado. Esta maneira você pode mostrar que o ISE envia os atributos corretos na aceitação de acesso sem ter que permitir debuga no lado WLC. Para começar uma captação usando TCDDump para navegar às **operações > pesquise defeitos > ferramentas > tcpdump >General das ferramentas de diagnóstico.**

Este é um exemplo de um fluxo correto capturado com o tcpdump

Estão aqui os AVP enviados em resposta ao pedido inicial MAB (segundo pacote no tiro de tela acima).

(Cisco Controller) >debug client <MAC addr>

O valor-limite debuga:

Se você precisa de mergulhar mais profundo nos processos ISE que envolvem decisões de política, a seleção portal, a autenticação do convidado, o CoA que seguram, etc. a maneira a

mais fácil de aproximar isto são permitir **Endpoit debugam** em vez de ter que ajustar componentes completos ao nível de debug.

Para permitir isto, navegue às **operações > ao Troubleshooting > ao DiagnosticTools > ferramentas gerais > valor-limite debugam.**

Uma vez no valor-limite debugar a página, incorpore o MAC address do valor-limite e clique o começo quando pronto para recrear a edição.

Debugar foi parado uma vez clica sobre o link que identifica o ID de ponto final para transferir o resultado do debug.

Informações Relacionadas

O TAC recomendou construções de AireOS

Guia de configuração de controle do Cisco Wireless, liberação 8.0.

Guia do administrador do Cisco Identity Services Engine, 2.1 da liberação

Configuração sem fio universal NGWC com Identity Services Engine