Autenticação da Web central com FlexConnect AP em um WLC com exemplo de configuração ISE

Índice

Introdução

Este documento descreve como configurar a autenticação da Web central com Access point de FlexConnect (AP) em um controlador do Wireless LAN (WLC) com Identity Services Engine (ISE) no modo do switching local.

Nota importante: Neste tempo, a autenticação local no FlexAPs não é apoiada para esta encenação.

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

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco Identity Services Engine (ISE), liberação 1.2.1
- Software do controlador do Wireless LAN, versão de liberação - 7.4.100.0

Configurar

Há uns métodos múltiplos para configurar a autenticação da Web central no controlador do Wireless LAN (WLC). O primeiro método é a autenticação da Web local em que o WLC reorienta o tráfego de HTTP a um interno ou a um servidor interno onde o usuário seja alertado autenticar. O WLC então busca as credenciais (enviadas para trás através de um pedido HTTP GET no caso de um servidor interno) e faz uma autenticação RADIUS. No caso de um usuário convidado, um servidor interno (tal como o server do motor do serviço da identidade (ISE) ou do convidado NAC (NG)) é exigido enquanto o portal fornece características tais como se registrar e auto-abastecimento do dispositivo. Este processo inclui estas etapas:

1. Os associados do usuário à autenticação da Web SSID.
2. O usuário abre seu navegador.
3. O WLC reorienta ao portal do convidado (tal como o ISE ou os NG) assim que uma URL for incorporada.
4. O usuário autentica no portal.
5. O portal do convidado reorienta de volta ao WLC com as credenciais incorporadas.
6. O WLC autentica o usuário convidado através do RAIO.
7. O WLC reorienta de volta à URL original.

Este processo inclui muita reorientação. A aproximação nova é usar a autenticação da Web central que trabalha com ISE (versões mais tarde de 1.1) e WLC (versões mais tarde de 7.2). Este processo inclui estas etapas:

1. Os associados do usuário à autenticação da Web SSID.
2. O usuário abre seu navegador.
3. O WLC reorienta ao portal do convidado.
4. O usuário autentica no portal.
5. O ISE envia uma mudança do RAIO da autorização (CoA - porta 1700 UDP) indicar ao controlador que o usuário é válido e empurra eventualmente atributos RADIUS tais como o Access Control List (ACL).
6. O usuário é alertado experimentar de novo a URL original.

Esta seção descreve as etapas necessárias configurar a autenticação da Web central no WLC e no ISE.

Diagrama de Rede

Essa configuração utiliza esta configuração de rede:

Configuração de WLC

A configuração WLC é relativamente simples. Um “truque? é usado (mesmos que no Switches) para obter a autenticação dinâmica URL do ISE. (Desde que usa o CoA, uma sessão precisa de ser criada como o ID de sessão é parte da URL.) O SSID é configurado para usar o MAC que filtra, e o ISE é configurado para retornar uma mensagem da aceitação de acesso mesmo se o MAC address não é encontrado de modo que envie a reorientação URL para todos os usuários.

Além, o Network Admission Control (NAC) do RAIO e a ultrapassagem AAA devem ser permitidos. O RAIO NAC permite que o ISE envie um pedido CoA que indique o usuário está autenticado agora e pode alcançar a rede. É usado igualmente para a avaliação da postura em que o ISE muda o perfil de usuário baseado no resultado da postura.

1. Assegure-se de que o servidor Radius tenha o RFC3576 (CoA) permitido, que é o padrão.

2. Crie um WLAN novo. Este exemplo cria um *CWAFlex* nomeado WLAN novo e atribui-o a vlan33. (Nota que não terá muito efeito desde que o Access point reage do modo do switching local.)

3. Na ABA de segurança, permita o MAC que filtra como a Segurança da camada 2.

4. Na aba da camada 3, assegure-se de que a Segurança esteja desabilitada. (Se a autenticação da Web é permitida na camada 3, a autenticação da Web local é permitida, autenticação da Web não central.)

5. Nos servidores AAA catalogue, selecione o server ISE como o servidor Radius para o WLAN. Opcionalmente, você pode selecioná-lo para explicar a fim ter mais informação detalhada no ISE.

6. No guia avançada, assegure permitem a ultrapassagem AAA é verificado e o raio NAC é selecionado para o estado NAC.

7. Crie uma reorientação ACL.

   ThisACL é provido na mensagem da aceitação de acesso do theISE e define que tráfego deve ser reorientado (negado pelo theACL) assim como que tráfego não deve ser reorientado (permitido pelo theACL). Basicamente, o DNS e o tráfego para/desde o theISE

precisam de ser permitidos. Nota: Uma edição com FlexConnect AP é que você deve criar um FlexConnect ACL separa de seu ACL normal. Esta edição é documentada no Bug da Cisco CSCue68065 e fixada na liberação 7.5. Em WLC 7.5 e mais atrasado, somente um FlexACL é exigido, e nenhum padrão ACL é precisado. O WLC espera que a reorientação ACL retornada pelo ISE é um ACL normal. Contudo, assegurá-lo trabalha, você precisa o mesmo ACL aplicado que o FlexConnect ACL.
Este exemplo mostra como criar um FlexConnect ACL nomeado *flexred*:

Crie regras para permitir o tráfego DNS assim como o tráfego para o ISE e para negar o resto.

Se você quer a segurança máxima, você pode permitir somente a porta 8443 para o ISE. (Se posturing, você deve adicionar portas típicas da postura, tais como 8905,8906,8909,8910.)

(Somente no código antes da versão 7.5 devido a CSCue68065) escolha a **Segurança > as listas de controle de acesso** para criar um ACL idêntico com o mesmo nome.

Prepare o FlexConnect específico AP. Note que para um desenvolvimento maior, você usaria tipicamente grupos de FlexConnect e não executaria estes artigos em uma base por-AP para motivos de escalabilidade.

Clique o **Sem fio**, e selecione o Access point específico.Clique a aba de **FlexConnect**, e clique **Webauthentication externo ACL**. (Antes da versão 7.4, esta opção foi nomeada *políticas da Web*.)

Adicionar o ACL (nomeado *flexred n*este exemplo) à área de políticas da Web. Isto PRE-impulsos o ACL ao Access point. Não é aplicado ainda, mas o índice ACL é dado ao AP de modo que possa se aplicar quando necessário.

A configuração WLC está agora completa.

Configuração ISE

Crie o perfil da autorização

Termine estas etapas a fim criar o perfil da autorização:

1. Clique a **política**, e clique então **elementos da política**.
2. Clique **resultados**.
3. Expanda a **autorização**, e clique então o **perfil da autorização**.
4. Clique o **botão Add** a fim criar um perfil novo da autorização para o webauth central.
5. **No campo de nome**, dê entrada com um nome para o perfil. Este exemplo usa *CentralWebauth*.
6. Escolha **ACCESS_ACCEPT da** lista de drop-down do tipo de acesso.
7. Verifique a caixa de verificação da **autenticação da Web**, e escolha o **AUTH centralizado da Web da** lista de drop-down.
8. No campo ACL, dê entrada com o nome do ACL no WLC que define o tráfego que será reorientado. Este os exemplos usam-se *flexred*.
9. Escolha o **padrão da** lista de drop-down da reorientação.

O atributo da reorientação define se o ISE vê o portal de web padrão ou um portal da web feito sob encomenda que o ISE admin criou. Por exemplo, o ACL *flexred n*este exemplo provoca uma reorientação em cima do tráfego de HTTP do cliente a em qualquer lugar.

Crie uma regra da autenticação

Termine estas etapas a fim usar o perfil da autenticação para criar a regra da autenticação:

1. Sob o menu da política, clique a **autenticação**. Esta imagem mostra um exemplo de como configurar a regra da política de autenticação. Neste exemplo, uma regra está configurada que provoque quando a filtração MAC é detectada.

2. Dê entrada com um nome para sua regra da autenticação. Este exemplo usa o *Sem fio mab*.
3. Selecione (**+**) o ícone positivo no se campo da circunstância.
4. Escolha a **condição composta**, e escolha então **Wireless_MAB**.
5. Escolha de “o acesso rede padrão” como o protocolo permitido.
6. Clique a seta encontrada ao lado de **e…** a fim expandir mais a regra.
7. Clique **+** ícone no campo de fonte da identidade, e escolha **valores-limite internos**.
8. Escolha **continuam do** se lista de drop-down não encontrada do usuário.

Esta opção permite que um dispositivo seja autenticado (através do webauth) mesmo se seu MAC address não é sabido. Os clientes do dot1x podem ainda autenticar com suas credenciais e não devem ser estados relacionados com esta configuração.

Crie uma regra da autorização

Há agora diversas regras a configurar na política da autorização. Quando o PC é associado, atravessará a filtração do Mac; supõe-se que o MAC address não está sabido, assim que o webauth e o ACL são retornados. Esta regra *não conhecida MAC* é mostrada na imagem abaixo e configurada nesta seção.

Termine estas etapas a fim criar a regra da autorização:

1. Crie uma regra nova, e dê entrada com um nome. Este exemplo usa o *MAC não conhecido*.
2. Clique (**+**) o ícone positivo no campo da circunstância, e escolha-o criar uma condição nova.
3. Expanda a lista de drop-down da **expressão**.
4. Escolha o **acesso de rede**, e expanda-o.
5. Clique **AuthenticationStatus**, e escolha o operador dos **iguais**.
6. Escolha **UnknownUser no** campo à direita.
7. Na página geral da autorização, escolha **CentralWebauth** (perfil da autorização) no campo à direita da palavra **então**.Esta etapa permite que o ISE continue mesmo que o usuário (ou o MAC) não sejam sabidos.Os usuários desconhecidos são apresentados agora com a página de login. Contudo, uma vez que incorporam suas credenciais, são apresentados outra vez com um pedido de autenticação no ISE; consequentemente, uma outra regra deve ser configurada com uma circunstância que seja estada conforme se o usuário é um usuário convidado. Neste exemplo, *se o convidado dos iguais de UseridentityGroup* é usado, e nele é suposto que todos os convidados pertencem a este grupo.
8. Clique as ações abotoam-se ficado situado no fim da regra *não conhecida MAC*, e escolhem-se introduzir uma regra nova acima.**Nota:** É muito importante que esta regra nova vem antes da regra *não conhecida MAC*.
9. Inscreva o **ò AUTH no** campo de nome.
10. Selecione um grupo da identidade como a circunstância. Este exemplo escolheu o **convidado**.

11. No campo da circunstância, clique (**+**) o ícone positivo, e escolha-o criar uma condição nova.

12. Escolha o **acesso de rede**, e clique **UseCase**.

13. Escolha **iguais** como o operador.

14. Escolha **GuestFlow** como o operando direito. Isto significa que você travará os usuários que apenas entraram no Web page e voltam depois que uma mudança da autorização (o fluxo do convidado parte da regra) e somente se pertencem ao grupo da identidade do convidado.

15. Na página da autorização, clique (**+**) o ícone positivo (situado ao lado de *então*) a fim escolher um resultado para sua regra.

    Neste exemplo, um perfil preconfigured (vlan34) é atribuído; esta configuração não é mostrada neste documento.

    Você pode escolher uma opção do **acesso da licença** ou para criar um perfil feito sob encomenda a fim retornar o VLAN ou os atributos esse você gosta.

Nota importante: Em ISE Version1.3, segundo o tipo de autenticação da Web, do “o exemplo do uso do fluxo convidado” não pôde ser encontrado anymore. A regra da

autorização teria que então conter o grupo de utilizadores do convidado como a única condição possível.

Permita a renovação IP (opcional)

Se você atribui um VLAN, a etapa final é para que o PC cliente renove seu endereço IP de Um ou Mais Servidores Cisco ICM NT. Esta etapa é conseguida pelo portal do convidado para clientes do Windows. Se você não ajustou um VLAN para a*?a* regra do *AUTH* mais adiantado, você pode saltar esta etapa.

Note que em FlexConnect AP, o VLAN precisa de preexistir no AP próprio. Consequentemente, se não faz, você pode criar um mapeamento no AP próprio VLAN-ACL ou no grupo do cabo flexível onde você não aplica nenhum ACL para o VLAN novo você quer criar. Isso cria realmente um VLAN (sem o ACL nele).

Se você atribuiu um VLAN, termine estas etapas a fim permitir a renovação IP:

1. Clique a **administração**, e clique então o **Gerenciamento do convidado**.
2. Clique **ajustes**.
3. Expanda o **convidado**, e expanda então a **configuração do Multi-portal**.
4. Clique **DefaultGuestPortal** ou o nome de um portal que feito sob encomenda você pode ter criado.
5. Clique a caixa de verificação da **liberação de Vlan DHCP**.**Nota:** Esta opção trabalha somente para clientes do Windows.

Fluxo de tráfego

Pode parecer difícil compreender que tráfego é enviado onde nesta encenação. Está aqui uma revisão rápida:

- O cliente envia o pedido da associação sobre o ar para o SSID.
- O WLC segura a autenticação de filtração MAC com ISE (onde recebe os atributos da reorientação).
- O cliente recebe somente uma resposta do assoc depois que a filtração MAC está completa.
- O cliente submete uma requisição DHCP e aquele é comutado **LOCALMENTE pelo** obain do Access point um endereço IP de Um ou Mais Servidores Cisco ICM NT do local remoto.
- No estado de Central_webauth, o tráfego marcado para nega na reorientação ACL (assim que HTTP tipicamente) é comutado **CENTRALMENTE**. Assim não é o AP que faz a reorientação mas o WLC; por exemplo, quando o cliente pede todo o Web site, o AP envia este ao WLC encapsulado em CAPWAP e nas paródias WLC que o endereço IP de Um ou Mais Servidores Cisco ICM NT do Web site e reorienta para o ISE.
- O cliente é reorientado ao ISE reorienta a URL. Isto é comutado **LOCALMENTE** outra vez (porque bate na licença no cabo flexível reorienta o ACL).
- Uma vez no estado de CORRIDA, o tráfego é comutado localmente.

Verificar

Uma vez que o usuário é associado ao SSID, a autorização está indicada na página ISE.

Da parte inferior acima, você pode ver a autenticação de filtração do MAC address que retorna os atributos CWA. Está em seguida o início de uma sessão portal com nome de usuário. O ISE envia então um CoA ao WLC e a última autenticação é uma autenticação de filtração do Mac da camada 2 no lado WLC, mas o ISE recorda o cliente e o username e aplica o VLAN que necessário nós configuramos neste exemplo.

Quando todo o endereço é aberto no cliente, o navegador está reorientado ao ISE. Assegure-se de que o Domain Name System (DNS) esteja configurado corretamente.

O acesso de rede é concedido depois que o usuário aceita as políticas.

No controlador, no estado do gerente da política e em mudanças de estado do RAIO NAC de *POSTURE_REQD A SER EXECUTADO*.