Autenticação da Web central no exemplo de configuração WLC e ISE

Índice

Introdução

Este documento descreve um exemplo de configuração que seja usado a fim terminar a autenticação da Web central (CWA) no controlador do Wireless LAN (WLC).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Release 1.2 do Cisco Identity Services Engine
- Liberação de software WLC 7.3.102.0 de Cisco

Configurar

O primeiro método de autenticação da Web é autenticação da Web local. Neste caso, 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 Identity Services Engine (ISE) ou do convidado NAC (NG)) é exigido porque o portal fornece características tais como se registrar e auto-abastecimento do dispositivo. O fluxo inclui estas etapas:

1. Os associados do usuário ao Service Set Identifier (SSID) da autenticação da Web.
2. O usuário abre o 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 fluxo inclui diversas reorientações. A aproximação nova é usar CWA. Este método trabalha com ISE (versões mais tarde de 1.1) e WLC (versões mais tarde de 7.2). O fluxo inclui estas etapas:

1. O usuário associa à autenticação da Web SSID, que é de fato open+macfiltering e nenhuma Segurança da camada 3.
2. O usuário abre o 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.

A instalação usada é:

Configuração de WLC

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

Além do que isto, o Network Admission Control (NAC) do RAIO e a ultrapassagem do Authentication, Authorization, and Accounting (AAA) devem ser permitidos. O RAIO NAC permite que o ISE envie um pedido CoA que indique que o usuário está autenticado agora e possa alcançar a rede. Está usado igualmente para a avaliação da postura, neste caso o ISE muda o perfil de usuário baseado no resultado da postura.

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

A etapa final é criar uma reorientação ACL. Este ACL é provido na aceitação de acesso do ISE e define que tráfego deve ser reorientado (negado pelo ACL) e que tráfego não deve ser reorientado (permitido pelo ACL). Aqui você apenas impede do tráfego da reorientação para o ISE. Você pôde querer ser mais específico e impedir somente o tráfego para/desde o ISE na porta 8443 (portal do convidado), mas ainda reorienta se um usuário tenta alcançar o ISE na porta 80/443.

> Nota: As versões anterior do software WLC como 7.2 ou 7.3 não o exigiram especificar o DNS mas umas versões de código mais novas exigem-no permitir o tráfego DNS no esse reorientam o ACL.

A configuração está agora completa no WLC.

Configuração ISE

Crie o perfil da autorização

No ISE, o perfil da autorização deve ser criado. Então, as políticas da authentication e autorização são configuradas. O WLC deve já ser configurado como um dispositivo de rede.

No perfil da autorização, dê entrada com o nome do ACL criado mais cedo no WLC.

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 **WLC_CWA**.
6. Escolha **ACCESS_ACCEPT da** lista de drop-down do tipo de acesso.

7. Verifique a caixa de verificação da **reorientação 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 interruptor que define o tráfego a ser reorientado. Este exemplo usa o **cwa_redirect**.

9. Escolha o **padrão da** lista de drop-down da reorientação. (Escolha algo a não ser o padrão se você usa um portal feito sob encomenda a não ser o padrão.)

Criam uma regra da autenticação

Assegure-se de que o ISE aceite todas as autenticações de MAC do WLC e certifique-se que levará a cabo a autenticação mesmo se o usuário não é encontrado.

Sob o menu da política, clique a **autenticação**.

A imagem seguinte mostra um exemplo de como configurar a regra da política de autenticação. Neste exemplo, uma regra está configurada que provoque quando o MAB é detectado.

- Dê entrada com um nome para sua regra da autenticação. Este exemplo usa o **MAB**, que já existe à revelia na versão 1.2 ISE.
- Selecione (**+**) o ícone positivo no se campo da circunstância.
- Escolha a **condição composta**, e escolha então **Wired_MAB OU Wireless_MAB**.
- Clique a seta encontrada ao lado de **e…** a fim expandir mais a regra.
- Clique **+** ícone no campo de fonte da identidade, e escolha **valores-limite internos**.
- Escolha **continuam do** se lista de drop-down não encontrada do usuário.

Crie uma política da autorização

Configurar a política da autorização. Um ponto importante a compreender é que há duas autenticações/autorizações:

- O primeiro é quando o usuário associa ao SSID e quando o perfil central da autenticação da Web está retornado (MAC address desconhecido, assim que você deve ajustar o usuário para a reorientação).
- O segundo é quando o usuário autentica no portal da web. Este combina a regra de padrão (usuários internos) nesta configuração (pode ser configurado a fim cumprir suas exigências). É importante que a peça da autorização não combina o perfil central da autenticação da Web outra vez. Se não, haverá um laço da reorientação. **O acesso de rede:** O atributo do **fluxo do convidado dos iguais de UseCase** pode ser usado a fim combinar esta segunda autenticação. O resultado olha como este:

  Nota: No ISE libere 1.3, dependente do tipo de autenticação da Web, “convidado que o

exemplo do uso do fluxo" não pôde ser batido anymore. A regra da autorização teria que então conter o grupo de utilizadores do convidado como a única condição possível.

Termine estas etapas a fim criar as regras da autorização segundo as indicações das imagens anterior:

1. Crie uma regra nova, e dê entrada com um nome. Este exemplo usa a **reorientação do convidado**.

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 **WLC_CWA** (perfil da autorização) no campo à direita da palavra **então**.

   Esta etapa permite que o ISE continue mesmo que o usuário (ou o MAC address) não sejam sabidos.

   Os usuários desconhecidos são apresentados agora com a página de login. Contudo, uma vez que incorporam suas credenciais, que é uma autenticação que suceda se as credenciais do cliente são válidas apesar do que você configurou na política da autenticação/autorização. Até à data das versões 1.1 e 1.2 ISE, as autenticações portais não seguem as regras da autenticação/autorização e sucedem se válidas. Assim, não há nenhuma necessidade de criar uma regra que permita o acesso em cima do início de uma sessão portal bem sucedido.

8. Clique as **ações** abotoam-se ficado situado no fim da regra da **reorientação do convidado**, e escolhem-se introduzir uma regra nova antes dela.

   Nota: É muito importante que esta regra nova vem antes da regra da **reorientação do convidado**.

9. Dê entrada com um nome para a regra nova. Este exemplo usa o **AUTH do portal do convidado**.

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

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

12. Escolha **iguais** como o operador.

13. Escolha **GuestFlow** como o operando direito. (Veja a nota, listada antes destas etapas, com respeito à liberação 1.3 ISE nesta circunstância.)

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

    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. Note que sobre **se GuestFlow**, você pode adicionar mais circunstâncias a fim retornar os vários perfis do authz baseados no grupo de usuário. Como mencionado na etapa 7, os fósforos **portais d**esta regra do **AUTH do convidado** em cima da segunda autenticação do MAC address iniciada após o início de uma sessão portal bem sucedido e após o ISE enviaram um CoA a fim reauthenticate o cliente. A diferença com esta segunda autenticação é que, em vez da vinda ao ISE com simplesmente seu MAC address, o ISE recorda o username dado no portal. Você pode fazer esta regra da autorização levar em consideração as credenciais incorporadas alguns milissegundos antes ao portal do convidado.

Nota: Se perfilando funções estão permitidos, valores-limite poderia ser introduzido automaticamente no base de dados, neste caso a condição do usuário desconhecido não combina. Neste caso, é melhor combinar pedidos de Wireless_MAB (condição incorporado). Se você usa a autenticação de MAC em seu controlador, você pode ou usar grupos do valor-limite para uma autorização mais específica, ou adicionar uma circunstância que combine o convidado SSID.

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.

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 criou.

5. Clique a caixa de verificação da **liberação VLAN DHCP**.

   Nota: Esta opção trabalha somente para clientes do Windows.

Encenação Âncora-estrangeira

Esta instalação pode igualmente trabalhar com a característica da auto-âncora dos WLC. A única captura é aquela desde que este método de autenticação da Web é a camada 2, você tem que estar ciente que será o WLC estrangeiro que faz todo o trabalho do RAIO. Somente o WLC estrangeiro contacta o ISE, e a obrigação da reorientação ACL esta presente igualmente no WLC estrangeiro.

Apenas como em outras encenações, o WLC estrangeiro mostra rapidamente o cliente para estar no estado de **CORRIDA**, que não é inteiramente verdadeiro. Significa simplesmente que o tráfego está enviado à âncora de lá. O estado de cliente real pode ser considerado na âncora onde deve indicar **CENTRAL_WEBAUTH_REQD**.

> Nota: A instalação âncora-estrangeira com autenticação da Web central (CWA) trabalha somente as liberações em 7.3 ou em mais atrasado.

> Nota: Devido à identificação de bug Cisco CSCuo56780 (mesmo nas versões que incluem reparos), você não pode executar a contabilidade na âncora e estrangeiro porque causa o perfilamento a se transformar impreciso devido a uma falta potencial do emperramento IP-à-MAC. Igualmente cria muitas edições com o ID de sessão para portais do convidado. Se você deseja configurar a contabilidade, a seguir configurar-la no controlador estrangeiro.

Verificar

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

Os detalhes do cliente no WLC mostram que a reorientação URL e ACL é aplicada.

Agora em que todo o endereço é aberto no cliente, o navegador é reorientado ao ISE. Assegure-se de que o Domain Name System (DNS) se estabeleça corretamente.

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

Segundo as indicações do exemplo ISE, a autenticação, a mudança da autorização, e o perfil aplicado são permitAccess.

O tiro de tela precedente é tomado da versão 1.1.x ISE onde cada única etapa da autenticação mostra claramente.

O tiro de tela seguinte é tomado da versão 1.2 ISE onde o ISE resume diversas autenticações executadas pelo mesmo cliente em uma linha. Embora mais prático na vida real, o tiro de tela da versão 1.1.x mostra mais claramente o que acontece exatamente para a claridade neste exemplo.

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

> Nota: A liberação em 7.3 ou em mais atrasado, o estado não é chamada **POSTURE_REQD** anymore, mas é chamada agora **CENTRAL_WEBAUTH_REQD**.

Troubleshooting

Termine estas etapas a fim pesquisar defeitos ou isolar um problema CWA:

1. Incorpore o **cliente debugar < o MAC address do** comando do **client> no** controlador e no monitor a fim determinar se o cliente alcança o estado **CENTRAL_WEBAUTH_REQD**. Um problema comum é observado quando o ISE retorna uma reorientação ACL que não exista (ou não é corretamente entrar) no WLC. Se este é o caso, a seguir o cliente deauthenticated uma vez que o estado **CENTRAL_WEBAUTH_REQD** é alcançado, que faz com que o processo comece outra vez.

2. Se o estado do cliente correto pode ser alcançado, a seguir navegue **para monitorar > clientes na** Web GUI WLC e para verificar que o corretos reorientam o ACL e a URL são aplicados para o cliente.

3. Verifique que o DNS correto está usado. O cliente deve ter a capacidade para resolver Web site do Internet e o hostname ISE. Você pode verificar este através do nslookup.

4. Verifique que todas as etapas das autenticações ocorrem no ISE:

   A autenticação de MAC deve ocorrer primeiramente, a que os atributos CWA são retornados.

   A autenticação de login portal ocorre.

   A autorização dinâmica ocorre.

   A autenticação final é uma autenticação de MAC que mostre o username do portal no ISE, a que os resultados finais da autorização são retornados (como o VLAN e o ACL finais).

Considerações especiais para ancorar encenações

Considere este o Bug da Cisco ID que limita a eficiência do processo CWA em uma encenação da mobilidade (especialmente ao explicar é configurado):

- CSCuo56780 - *Vulnerabilidade de negação de serviço do serviço de raio ISE*

- CSCul83594 - *O ID de sessão não está sincronizado através da mobilidade, se a rede está aberta*