Autenticação da Web central com um exemplo de configuração do interruptor e do Identity Services Engine

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Configurar
Visão geral
Crie o ACL baixável
Crie o perfil da autorização
Crie uma regra da autenticação
Crie uma regra da autorização
Permita a renovação IP (opcional)
Configuração de switch (trecho)
Configuração de switch (completa)
Configuração de proxy HTTP
Observação importante sobre o interruptor SVI
Observação importante sobre o redirecionamento em https
Resultado final
Verificar
Troubleshooting
Informações Relacionadas

Introdução

Este documento descreve como configurar a autenticação da Web central com os clientes prendidos conectados ao Switches com a ajuda do Identity Services Engine (ISE).

O conceito da autenticação da Web central é oposto à autenticação da Web local, que é a autenticação da Web usual no interruptor própria. Nesse sistema, em cima da falha dot1x/mab, o interruptor Failover ao perfil do webauth e reorientará o tráfego do cliente a um página da web no interruptor.

A autenticação da Web central oferece a possibilidade ter um dispositivo central que atue como um portal da web (no th é o exemplo, o ISE). A diferença principal comparada à autenticação da Web local usual é que está deslocada para mergulhar 2 junto com a autenticação mac/dot1x. O conceito igualmente difere que o servidor Radius (ISE neste exemplo) retorna os atributos especiais que indicam ao interruptor que uma reorientação da Web deve ocorrer. Esta solução tem a vantagem para eliminar todo o atraso que seja necessário para que a autenticação da Web retroceda. Globalmente, se o MAC address da estação do cliente não está sabido pelo servidor Radius (mas por outros critérios pode igualmente ser usado), os atributos da reorientação dos

retornos do server, e o interruptor autoriza a estação (através do [MAB] do desvio da autenticação de MAC) mas coloca uma lista de acessos para reorientar o tráfego de web ao portal. Uma vez que o usuário entra no portal do convidado, é possível através de CoA (mudança da autorização) saltar a porta de switch de modo que uma autenticação nova MAB da camada 2 ocorra. O ISE pode então recordar que era um usuário do webauth e para aplicar atributos da camada 2 (como CAMIONETE dinâmica atribuição) ao usuário. Um componente de ActiveX pode igualmente forçar o PC cliente a refrescar seu endereço IP de Um ou Mais Servidores Cisco ICM NT.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Identity Services Engine (ISE)
- Configuração de switch do ® do Cisco IOS

Componentes Utilizados

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

- Cisco Identity Services Engine (ISE), liberação 1.1.1
- Cisco Catalyst 3560 Series Switch que executa a versão de software 12.2.55SE3

  Note: O procedimento é similar ou idêntico para outros modelos de Catalyst switch. Você pode usar estas etapas em todos os Cisco IOS Software Release para o catalizador salvo indicação em contrário.

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.

Configurar

Visão geral

A configuração ISE é composta destas cinco etapas:

1. Crie o Access Control List carregável (ACL).
2. Crie o perfil da autorização.
3. Crie uma regra da autenticação.
4. Crie uma regra da autorização.
5. Permita a renovação IP (opcional).

Crie o ACL baixável

Esta não é uma etapa imperativa. A reorientação ACL enviada para trás com o perfil central do

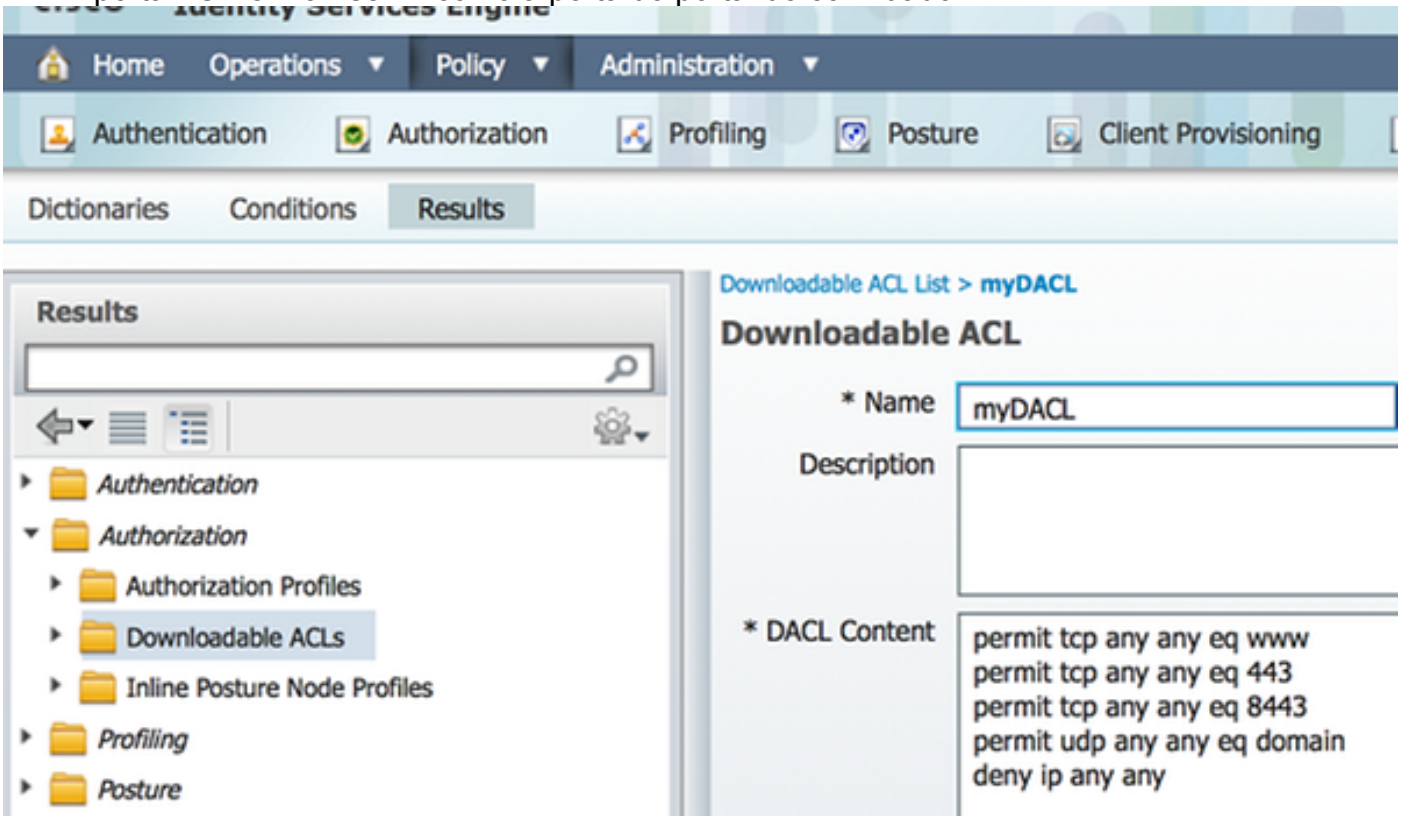
webauth determina que tráfego (HTTP ou HTTPS) é reorientado ao ISE. O ACL baixável permite que você defina que tráfego é permitido. Você deve tipicamente permitir o DNS, o HTTP, e os 8443 e negar o resto. Se não, o interruptor reorienta o tráfego de HTTP mas permite outros protocolos.

Termine estas etapas a fim criar o ACL baixável:

1. Clique a **política**, e clique **elementos da política**.
2. Clique **resultados**.
3. Expanda a **autorização**, e clique **ACL carregável**.
4. Clique o **botão Add** a fim criar um ACL baixável novo.
5. **No campo de nome**, dê entrada com um nome para o DACL. Este exemplo usa o *myDACL*.

Esta imagem mostra o índice típico DACL, que reserva:

- DNS - resolva o hostname do portal ISE
- HTTP e HTTPS - permita a reorientação
- A porta TCP 8443 - servir como a porta do portal do convidado



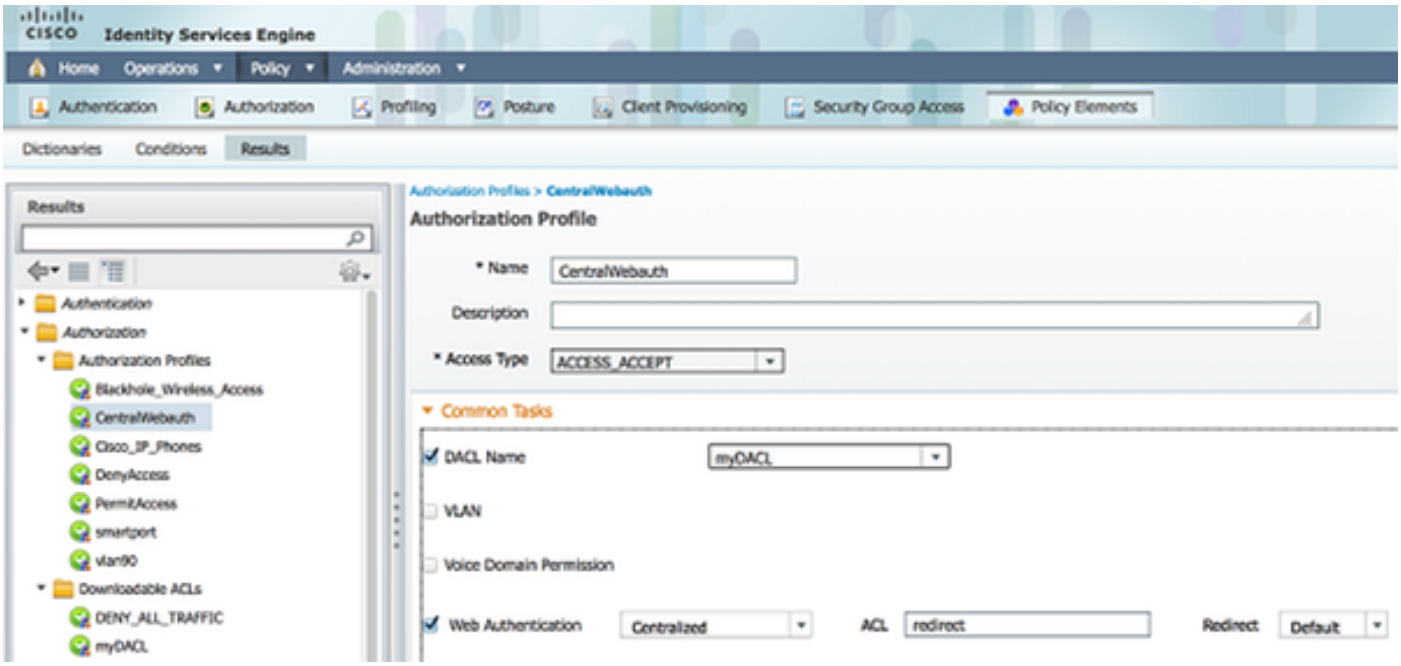
Crie o perfil da autorização

Termine estas etapas a fim criar o perfil da autorização:

1. Clique a **política**, e clique **elementos da política**.
2. Clique **resultados**.
3. Expanda a **autorização**, e clique 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-a **centralizado 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 os exemplos usam-se *reorientam*.
9. Escolha o **padrão da** lista de drop-down da reorientação.
10. Verifique a caixa de seleção do **nome DACL**, e escolha o **myDACL do** lsit da gota-para baixo se você decide usar um DACL em vez de uma porta estática ACL no interruptor.

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, a *reorientação* ACL neste exemplo provoca uma reorientação em cima do tráfego HTTP ou HTTPS do cliente a em qualquer lugar. O ACL é definido no interruptor mais tarde neste exemplo de configuração.

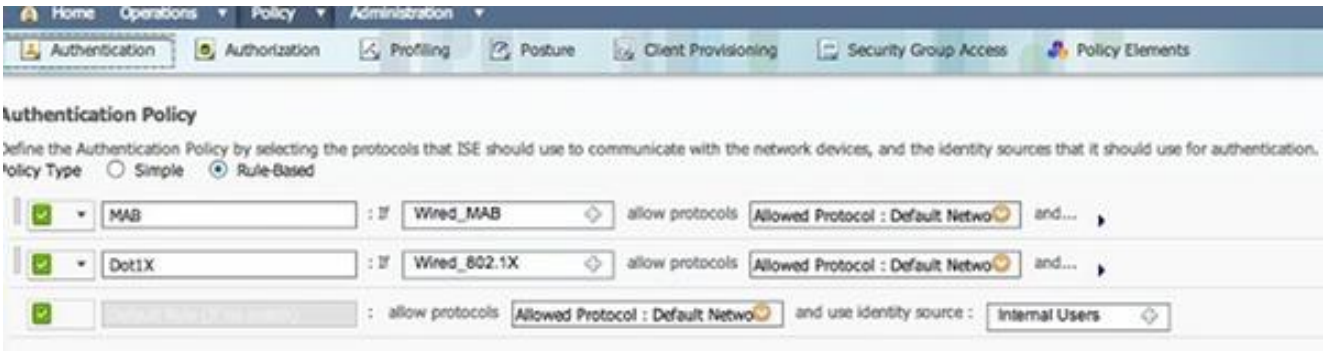


Crie uma regra da autenticação

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**.

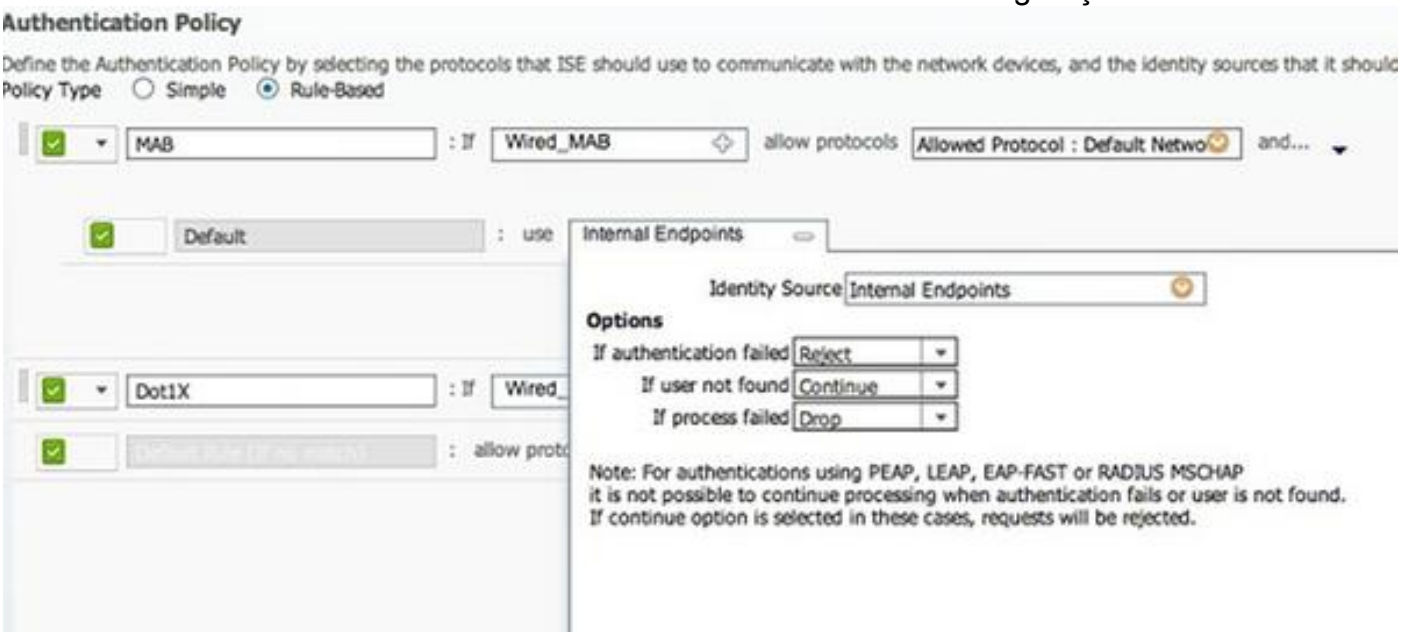
   Esta imagem mostra um exemplo de como configurar a regra da política de autenticação. Neste exemplo, uma regra está configurada que provoque quando o MAB é detectado.



2. Dê entrada com um nome para sua regra da autenticação. Este exemplo usa o *MAB*.
3. Selecione (**+**) o ícone positivo no se campo da circunstância.

4. Escolha a **condição composta**, e escolha **Wired_MAB**.
5. Clique a seta encontrada ao lado de **e…** a fim expandir mais a regra.
6. Clique **+** ícone no campo de fonte da identidade, e escolha **valores-limite internos**.
7. 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 obstruído dentro, atravessa o MAB; 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 nesta imagem 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.

   Note: É muito importante que esta regra nova vem antes da regra *não conhecida MAC*.
9. Dê entrada com um nome para a regra nova. Este exemplo usa o Estar-um-*CONVIDADO*.
10. Escolha uma circunstância que combine seus usuários convidado.

    Este exemplo usa *InternalUser: IdentityGroup iguala o convidado* porque todos os usuários convidado são limitados ao grupo do *convidado* (ou a um outro grupo que você configurou em seus ajustes do patrocinador).
11. Escolha **PermitAccess na** caixa do resultado (situada à direita da palavra *então*).

    Quando o usuário é autorizado na página de login, o ISE reinicia uma autenticação da camada 2 na porta de switch, e um MAB novo ocorre. Nesta encenação, a diferença é que uma bandeira invisível está ajustada para que o ISE recorde que era um usuário convidado-autenticado. Esta regra é *ò AUTH*, e a circunstância é *acesso de rede: UseCase iguala GuestFlow*. Esta circunstância é estada conforme quando o usuário autentica através do webauth, e a porta de switch está ajustada outra vez para um MAB novo. Você pode atribuir todos os atributos que você gostar. Este exemplo atribui um perfil *vlan90* de modo que o usuário seja atribuído o VLAN 90 em sua segunda autenticação MAB.
12. Clique as **ações** (situadas no fim da regra do Estar-um-CONVIDADO), e escolha a **regra nova da inserção acima**.
13. Inscreva o **ò AUTH no** campo de nome.
14. No campo da circunstância, clique (**+**) o ícone positivo, e escolha-o criar uma condição nova.
15. Escolha o **acesso de rede**, e clique **UseCase**.
16. Escolha **iguais** como o operador.
17. Escolha **GuestFlow** como o operando direito.
18. 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 (vlan90) 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.

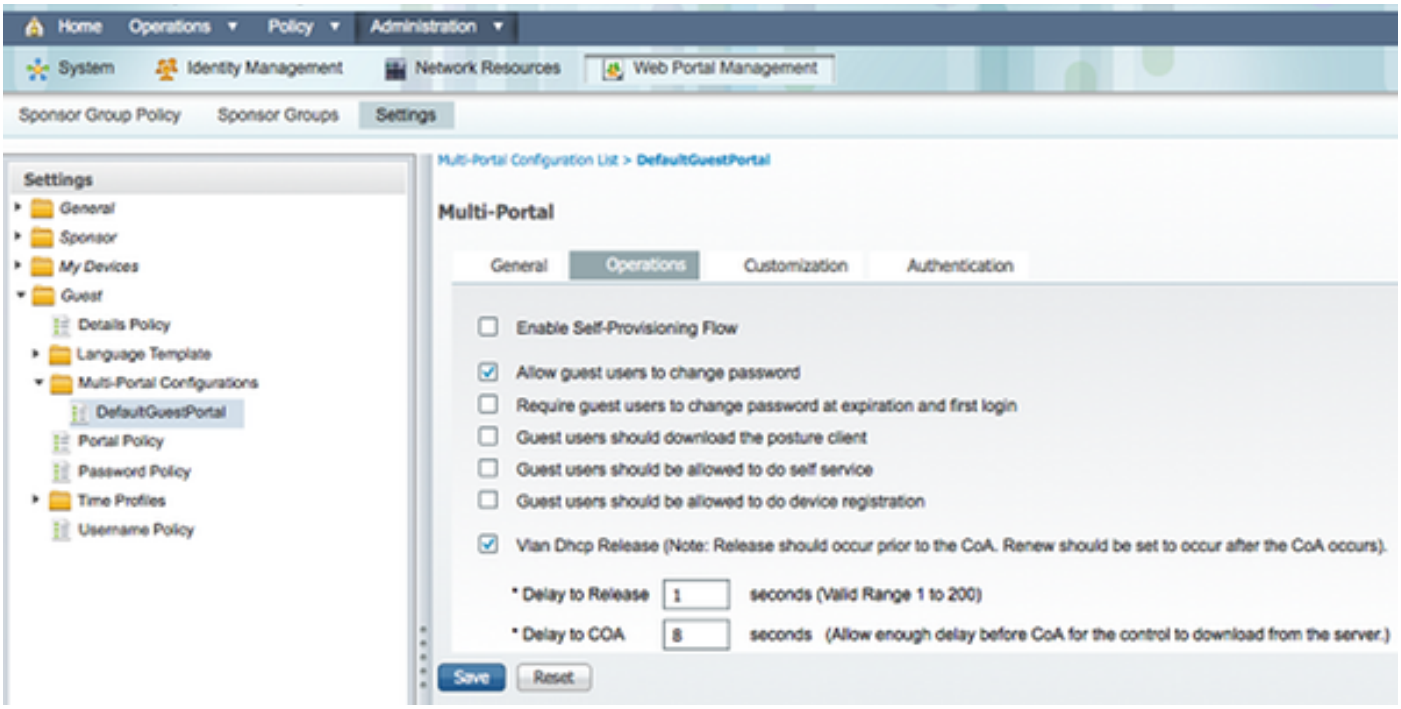
Permita a renovação IP (opcional)

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 o **Gerenciamento do convidado**.
2. Clique **ajustes**.
3. Expanda o **convidado**, e expanda 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 **Vlan DHCP Releasecheck**. **Note**: Esta opção trabalha somente para clientes do Windows.



Configuração de switch (trecho)

Esta seção fornece um trecho da configuração de switch. Veja a [configuração de switch (completa)] para a configuração direta.

Esta amostra mostra uma configuração simples MAB.

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

O VLAN 100 é o VLAN que fornece a conectividade de rede completa. Uma porta padrão ACL (*webauth* Nomeado) é aplicada e definida como mostrado aqui:

```
ip access-list extended webauth
permit ip any any
```

Esta configuração de exemplo dá o acesso de rede completo mesmo se o usuário não é autenticado; consequentemente, você pôde querer restringir o acesso aos usuários não-autenticados.

Nesta configuração, o HTTP e o HTTPS que consultam não trabalham sem autenticação (pelo outro ACL) desde que o ISE é configurado para usar uma reorientação ACL (nomeada *reoriente*). Está aqui a definição no interruptor:

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

Esta lista de acessos deve ser definida no interruptor a fim definir em que tráfego o interruptor executará a reorientação. (Combina na *licença*.) Neste exemplo, em algum tráfego HTTP ou HTTPS que o cliente enviar disparadores a uma reorientação da Web. Este exemplo igualmente nega o endereço IP de Um ou Mais Servidores Cisco ICM NT ISE assim que o tráfego ao ISE vai ao ISE e não reorienta em um laço. (Nesta encenação, negue não obstrui o tráfego; apenas não reorienta o tráfego.) Se você usa portas de HTTP incomuns ou um proxy, você pode adicionar outras portas.

Uma outra possibilidade é permitir o acesso HTTP a alguns sites e reorientar outros sites. Por exemplo, se você define no ACL uma licença para servidores de Web internos somente, os clientes poderiam consultar a Web sem autenticar mas encontrariam a reorientação se tentam alcançar um servidor de Web interno.

A última etapa é permitir o CoA no interruptor. Se não, o ISE não pode forçar o interruptor a reauthenticate o cliente.

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

Este comando é exigido para que o interruptor reoriente baseado no tráfego de HTTP:

```
ip http server
```

Este comando é exigido para reorientar baseado no tráfego HTTPS:

```
ip http secure-server
```

Estes comandos são igualmente importantes:

```
radius-server vsa send authentication
radius-server vsa send accounting
```

Se o usuário não é autenticado ainda, o **num> do <interface int da sessão da autenticação da mostra** retorna esta saída:

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
```

```
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Note: Apesar de uma autenticação bem sucedida MAB, a reorientação ACL é colocada desde que o MAC address não foi sabido pelo ISE.

Configuração de switch (completa)

Esta seção alista a configuração de switch completa. Algumas relações e linhas de comando desnecessárias foram omitidas; consequentemente, esta configuração de exemplo deve ser usada para a referência somente e não deve ser copiada.

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
```

```
      mab      Authc Success
```

Configuração de proxy HTTP

Se você usa um proxy HTTP para seus clientes, significa que seus clientes:

- Use uma porta não convencional para o protocolo HTTP
- Envie todo seu tráfego a esse proxy

A fim mandar o interruptor escutar na porta não convencional (por exemplo, 8080), use estes comandos:

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Você igualmente precisa de configurar todos os clientes para manter-se usar seu proxy mas para não usar o proxy para o endereço IP de Um ou Mais Servidores Cisco ICM NT ISE. Todos os navegadores incluem uma característica que permita que você incorpore os nomes de host ou os endereços IP de Um ou Mais Servidores Cisco ICM NT que não devem usar o proxy. Se você não adiciona a exceção para o ISE, você encontra uma página da autenticação do laço.

Você igualmente precisa de alterar sua reorientação ACL para permitir na porta de proxy (8080 neste exemplo).

Observação importante sobre o interruptor SVI

Neste tempo, o interruptor precisa uma interface virtual do interruptor (SVI) a fim responder ao cliente e enviar a reorientação do portal da web ao cliente. Este SVI não tem que necessariamente estar no cliente subnet/VLAN. Contudo, se o interruptor não tem nenhum SVI no cliente subnet/VLAN, tem que usar alguns dos outros SVI e enviar o tráfego como definido na tabela de roteamento do cliente. Isto significa tipicamente que o tráfego está enviado a um outro gateway no núcleo da rede; este tráfego vem para trás ao switch de acesso dentro da sub-rede de cliente.

Dos Firewall o tráfego do bloco tipicamente e ao mesmo interruptor, como nesta encenação, assim que a reorientação não puderam trabalhar corretamente. As ações alternativas são permitir este comportamento no Firewall ou criar um SVI no switch de acesso na sub-rede de cliente.

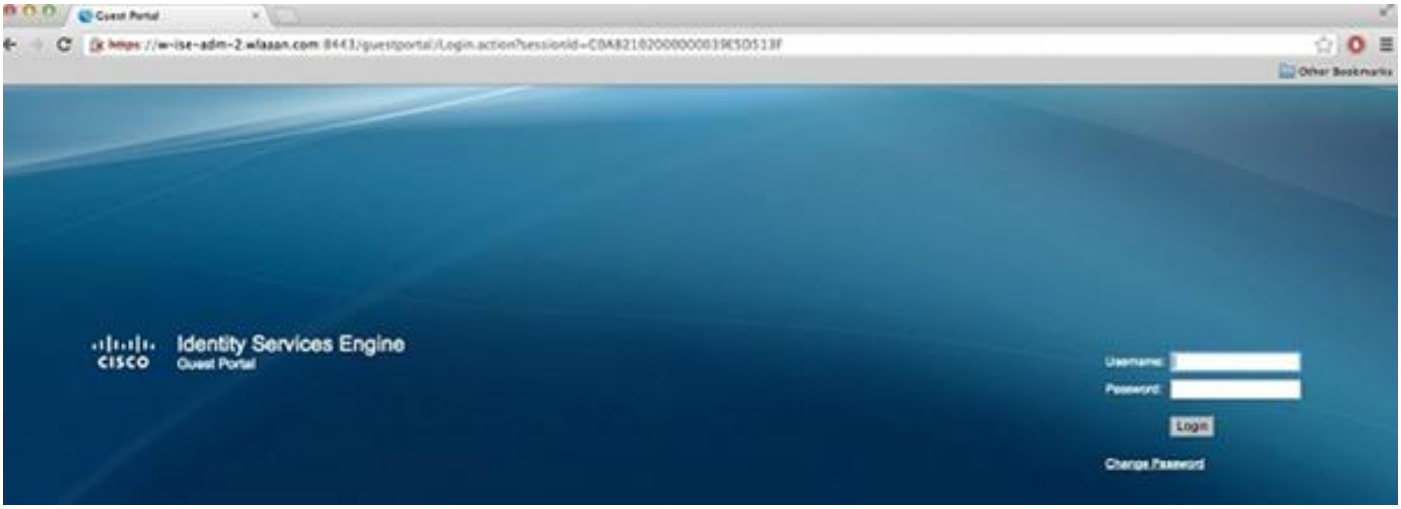
Observação importante sobre o redirecionamento em https

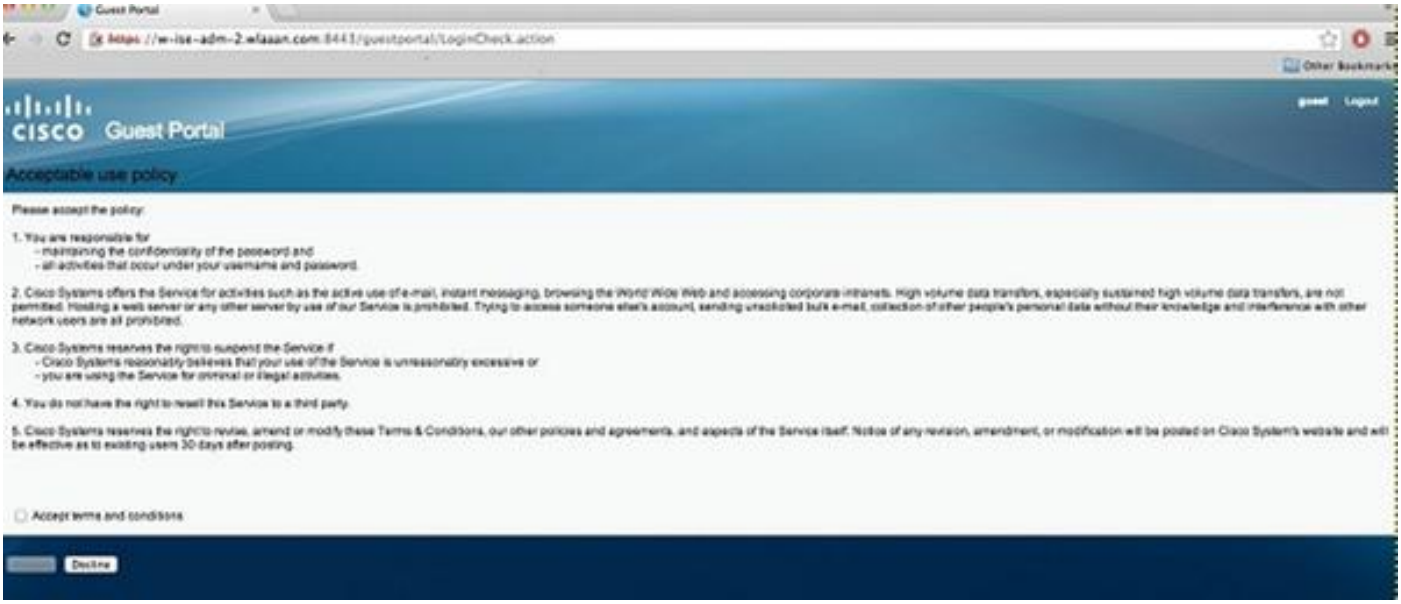
O Switches pode reorientar o tráfego HTTPS. Assim, se o cliente do convidado tem um homepage no HTTPS, a reorientação ocorre corretamente.

O conceito inteiro da reorientação é baseado no fato de que paródias de um dispositivo (neste caso, o interruptor) o endereço IP de Um ou Mais Servidores Cisco ICM NT do Web site. Contudo, uma questão principal elevara quando o interruptor intercepta e reorienta o tráfego HTTPS porque o interruptor pode apresentar somente seu próprio certificado no aperto de mão do Transport Layer Security (TLS). Desde que este não é o mesmo certificado que o Web site pediu originalmente, a maioria de major da edição dos navegadores alerta. Os navegadores seguram corretamente a reorientação e a apresentação de um outro certificado como um interesse de segurança. Não há nenhuma ação alternativa para esta, e não há nenhuma maneira para o interruptor ao spoof seu certificado original do Web site.

Resultado final

O PC cliente obstrui dentro e executa o MAB. O MAC address não é sabido, assim que o ISE empurra os atributos da reorientação de volta ao interruptor. O usuário tenta ir a um Web site e é reorientado.





Quando a autenticação da página de login é bem sucedida, o ISE salta o switchport através da mudança da autorização, que começa outra vez uma autenticação MAB da camada 2.

Contudo, o ISE sabe que é um cliente anterior do webauth e autoriza o cliente baseado nas credenciais do webauth (embora esta é uma autenticação da camada 2).

Nos logs da autenticação ISE, a autenticação MAB aparece na parte inferior do log. Embora fosse desconhecida, o MAC address foi autenticado e perfilado, e os atributos do webauth foram retornados. Em seguida, a autenticação ocorre com o username do usuário (isto é, os tipos de usuário suas credenciais na página de login). Imediatamente depois da autenticação, uma autenticação nova da camada 2 ocorre com o username como credenciais; esta etapa da autenticação é onde você pode retornar atribui tal VLAN dinâmico.

Mar 26,13 04:58:43.572 PM	✓		Nico	00:0F:80:49:5C:48	Nicoswitch	FastEthernet0/3	vlan90	Guest	NotApplicable	
Mar 26,13 04:58:43.445 PM	✓				Nicoswitch					Dynamic Author...
Mar 26,13 04:58:43.438 PM	✓		Nico	00:0F:80:49:5C:48				Guest		Guest Authentic...
Mar 26,13 04:58:37.900 PM	✓		#ACSACL#-IP-myDAC		celine					DACL Download...
Mar 26,13 04:58:36.995 PM	✓		00:1A:6C:78:56:0E	00:1A:6C:78:56:0E	celine	GigabitEthernet2/0/10	CentralWebauth		Pending	Authentication ...

Verificar

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

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Cisco Identity Services Engine
- Guia de referência de comando do Cisco Identity Services Engine
- Integração de ISE (Identity Services Engine) com Cisco WLC (controlador do Wireless LAN)
- Solicitações de Comentários (RFCs)

- Suporte Técnico e Documentação - Cisco Systems