Autenticação com base na porta com um exemplo de configuração do REGAÇO e ACS 5.2

Índice

Introdução

Este documento descreve como configurar um Access point de pouco peso (REGAÇO) enquanto um suplicante do 802.1x a fim autenticar contra um servidor Radius tal como um Access Control Server (ACS) 5.2.

Pré-requisitos

Requisitos

Certifique-se de que você cumpre estas exigências antes que você tente esta configuração:

- Tenha o conhecimento básico do controlador do Wireless LAN (WLC) e de regaços.

- Tenha o conhecimento funcional do servidor AAA.
- Tenha o conhecimento completo das redes Wireless e das edições de segurança Wireless.

Componentes Utilizados

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

- Cisco 5508 WLC que executa a versão de firmware 7.0.220.0
- REGAÇO do Cisco 3502 Series
- Cisco Secure ACS que executa a versão 5.2
- Cisco 3560 Series Switch

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.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Os regaços têm os Certificados X.509 instalados fábrica - assinados por uma chave privada - que são queimados no dispositivo na altura da fabricação. Os regaços usam este certificado a fim autenticar com o WLC no processo da junta. Este método descreve uma outra maneira de autenticar regaços. Com software WLC, você pode configurar a autenticação do 802.1x entre um Access Point (AP) do Cisco Aironet e um switch Cisco. Nesta instância, o AP atua como o suplicante do 802.1x e é autenticado pelo interruptor contra um servidor Radius (ACS) esse os usos EAP-FAST com abastecimento anônimo PAC. Uma vez que é configurado para a autenticação do 802.1x, o interruptor não permite que nenhum tráfego a não ser o tráfego do 802.1x passe através da porta até que o dispositivo conectado à porta autentique com sucesso. Um AP pode ser autenticado ou antes que se junte a um WLC ou depois que se juntou a um WLC, neste caso você configura o 802.1x no interruptor depois que o REGAÇO se junta ao WLC.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Estes são os detalhes de configuração dos componentes usados neste diagrama:

- O endereço IP de Um ou Mais Servidores Cisco ICM NT do server ACS (RAIO) é 192.168.150.24.

- O Gerenciamento e o endereço da relação do gerenciador AP do WLC são 192.168.75.44.
- Os servidores DHCP endereçam 192.168.150.25.
- O REGAÇO é colocado em VLAN 253.
- VLAN 253: 192.168.153.x/24. Gateway: 192.168.153.10
- VLAN 75: 192.168.75.x/24. Gateway: 192.168.75.1

Hipóteses

- O Switches é configurado para toda a camada 3 VLAN.
- O servidor DHCP é atribuído um escopo de DHCP.
- A Conectividade da camada 3 existe entre todos os dispositivos na rede.
- O REGAÇO é juntado já ao WLC.
- Cada VLAN tem uma máscara de /24.
- O ACS 5.2 tem um certificado assinado do auto instalado.

Passos de configuração

Esta configuração é dividida em três categorias:

1. Configurar o REGAÇO.
2. Configurar o interruptor.
3. Configurar o servidor Radius.

Configurar o REGAÇO

Suposições:

O REGAÇO é registrado já ao WLC usando a opção 43, DNS, ou IP estaticamente configurado da interface de gerenciamento WLC.

Conclua estes passos:

1. Vão ao **Sem fio** > aos **Access point** > **todos os AP** a fim verificar o registro do REGAÇO no WLC.
2. Você pode configurar as credenciais do 802.1x (isto é, username/senha) para todos os regaços em duas maneiras:**Globalmente**Para um REGAÇO já juntado, você pode ajustar as credenciais globalmente assim que cada REGAÇO que junta-se ao WLC herdará aquelas credenciais.**Individualmente**Configurar perfis do 802.1x pelo AP. Em nosso exemplo, nós configuraremos credenciais pelo AP.Vão ao **Sem fio** > **todos os AP**, e selecionam o AP interessado.Adicionar o nome de usuário e senha nos campos das **credenciais do suplicante do 802.1x**.**Nota:** As credenciais do início de uma sessão são usadas ao telnet, ao SSH, ou ao console dentro ao AP.
3. Configurar a Alta disponibilidade da seção, e o clique **aplica-se**.**Nota:** Uma vez que salvar, estas credenciais são retidas através do WLC e das repartições AP. As credenciais mudam somente quando o REGAÇO se junta a um WLC novo. O REGAÇO supõe o nome de usuário e senha que foi configurado no WLC novo.Se o AP não se juntou a um WLC ainda, você deve consolar dentro ao REGAÇO a fim ajustar as credenciais. Emita este comando CLI no modo enable:*<password> da* **senha do** *<username>* **username do dot1x de**

LAP#lwapp ap ou*<password> da* **senha do** *<username>* **username do dot1x de LAP#capwap ap Nota:** Este comando está disponível somente para os AP que executam a imagem de recuperação.O nome de usuário padrão e a senha para o REGAÇO são `Cisco` e `Cisco` respectivamente.

Configurar o interruptor

O interruptor atua como um autenticador para o REGAÇO e autentica o REGAÇO contra um servidor Radius. Se o interruptor não tem o software complacente, promova o interruptor. No interruptor CLI, emita estes comandos a fim permitir a autenticação do 802.1x em uma porta de switch:

```
switch#configure terminal switch(config)#dot1x system-auth-control switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco !--- Configures the RADIUS server
with shared secret and enables switch to send !--- 802.1x information to the RADIUS server for
authentication. switch(config)#ip radius source-interface vlan 253 !--- We are sourcing RADIUS
packets from VLAN 253 with NAS IP: 192.168.153.10. switch(config)interface gigabitEthernet 0/11
switch(config-if)switchport mode access switch(config-if)switchport access vlan 253
switch(config-if)mls qos trust dscp switch(config-if)spanning-tree portfast !--- gig0/11 is the
port number on which the AP is connected. switch(config-if)dot1x pae authenticator !---
Configures dot1x authentication. switch(config-if)dot1x port-control auto !--- With this
command, the switch initiates the 802.1x authentication.
```

Nota: Se você tem outros AP no mesmo interruptor e você não os quer usar o 802.1x, você pode deixar a porta un-configurada para o 802.1x ou emitir este comando:

```
switch(config-if)authentication port-control force-authorized
```

Configurar o servidor Radius

O REGAÇO é autenticado com EAP-FAST. Certifique-se de que o servidor Radius você usa apoios este método de EAP se você não está usando Cisco ACS 5.2.

A configuração de servidor RADIUS é dividida em quatro etapas:

1. Configurar recursos de rede.
2. Configurar usuários.
3. Defina elementos da política.
4. Aplique políticas de acesso.

O ACS 5.x é um ACS com base em política. Ou seja o ACS 5.x usa um modelo baseado em regras da política em vez do modelo grupo-baseado usado nas versões 4.x.

O modelo baseado em regras da política ACS 5.x fornece um controle de acesso mais poderoso e mais flexível comparado à aproximação grupo-baseada mais velha.

No modelo grupo-baseado mais velho, um grupo define a política porque contém e amarra junto três tipos de informação:

- **Informação de identidade** - Esta informação pode ser baseada na sociedade em grupos AD ou LDAP ou em uma atribuição estática para usuários internos ACS.

- **Outras limitações ou circunstâncias** - Restrições de tempo, limitações do dispositivo, e assim por diante.
- **Permissões** - Níveis de privilégio do ® VLAN ou de Cisco IOS.

O modelo da política ACS 5.x é baseado em regras do formulário:

Se a circunstância resulta então

Por exemplo, nós usamos a informação descrita para o modelo grupo-baseado:

Se identidade-condição, autorização-perfil da limitação-condição então.

Em consequência, isto dá-nos a flexibilidade limitar as circunstâncias sob que é permitido ao usuário alcançar a rede e também que nível da autorização é permitido quando as circunstâncias específicas são estadas conformes.

Configurar recursos de rede

Nesta seção, nós configuramos o cliente de AAA para o interruptor no servidor Radius.

Este procedimento explica como adicionar o interruptor como um cliente de AAA no servidor Radius de modo que o interruptor possa passar as credenciais do usuário do REGAÇO ao servidor Radius.

Conclua estes passos:

1. Do ACS GUI, clique **recursos de rede**.
2. Clique **grupos de dispositivo de rede**.
3. Vá ao **lugar > criam** (na parte inferior).
4. Adicionar os campos requerido e o clique **submete-se**.
5. O indicador refresca:
6. **O tipo de dispositivo do** clique **> cria**.
7. Clique em Submit. Uma vez que terminado, o indicador refresca:
8. Vá aos **recursos de rede >** aos **dispositivos de rede e aos clientes de AAA**.
9. O clique **cria**, e preenche os detalhes como descritos aqui:
10. Clique em Submit. O indicador refresca:

Configurar usuários

Nesta seção, você verá como criar um usuário no ACS configurado previamente. Você atribuirá o usuário a um grupo chamado do “usuários REGAÇO”.

Conclua estes passos:

1. Vá aos **usuários e a identidade armazena > grupos da identidade > cria**.
2. Clique em Submit.
3. Crie **3502e** e atribua-o para agrupar do “usuários REGAÇO”.
4. Vá aos **usuários e a identidade armazena > identidade agrupa > usuários > cria**.
5. Você verá a informação atualizadas:

Defina elementos da política

Verifique que o **acesso da licença** está ajustado.

Aplique políticas de acesso

Nesta seção, você selecionará EAP-FAST porque o método de autenticação usado para regaços a fim autenticar. Você criará então as regras baseadas nas etapas precedentes.

Conclua estes passos:

1. Vai às **políticas de acesso** > ao **acesso presta serviços de manutenção** > o **acesso de rede padrão > edita: De "acesso rede padrão"**.
2. Certifique-se de você ter permitido o **abastecimento EAP-FAST** e **anônimo da Em-faixa PAC**.
3. Clique em Submit.
4. Verifique o grupo da identidade que você selecionou. Neste exemplo, os **usuários internos do** uso (que foi criado no ACS) e salvar as mudanças.
5. Vão às **políticas de acesso** > ao **acesso prestam serviços de manutenção** > o **acesso** > a **autorização de rede padrão** a fim verificar o perfil da autorização.Você pode personalizar sob que circunstâncias você permitirá a um acesso de usuário à rede e que perfil da autorização (atributos) você passará autenticado uma vez. Esta granularidade está somente disponível em ACS 5.x. Neste exemplo, o **lugar**, o **tipo de dispositivo**, o **protocolo**, o **grupo da identidade**, e o **método de autenticação de EAP** são selecionados.
6. **APROVAÇÃO do** clique, e **mudanças da salvaguarda**.
7. A próxima etapa é criar uma regra. Se nenhuma regra é definida, o REGAÇO está permitido o acesso sem nenhumas circunstâncias.
8. O clique **cria > Rule-1**. Esta regra é para usuários no grupo do "usuários REGAÇO".
9. **Mudanças da salvaguarda do** clique. Se você quer os usuários que não combinam as circunstâncias a ser negadas, edite a regra de padrão dizer que "negue o acesso".
10. A última etapa é definir regras de seleção do serviço. Use esta página para configurar uma política simples ou baseado em regras a fim determinar que serviço a se aplicar às requisições recebidas. Por exemplo:

Verificar

Uma vez que o 802.1x é permitido na porta de switch, todo o tráfego a não ser que o tráfego do 802.1x seja obstruído através da porta. O REGAÇO, que é registrado já ao WLC, obtém dissociado. Somente depois que uma autenticação bem sucedida do 802.1x é o outro tráfego permitido passar completamente. O registro bem-sucedido do REGAÇO ao WLC depois que o 802.1x é permitido no interruptor indica que a autenticação do REGAÇO é bem sucedida.

Console AP:

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
```

```
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false *Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface
GigabitEthernet0 authenticated [EAP-FAST] *Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN:
Interface GigabitEthernet0 assigned DHCP address 192.168.153.106, mask 255.255.255.0, hostname
3502e !--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN *Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan wmmAC
status is FALSEged state to CFG *Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0,
changed state to down *Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed
state to reset *Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP *Jan 29
09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller 5508-3 *Jan 29 09:11:39.013:
%CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake. Wireless client traffic will be blocked
until DTLS tunnel is established. *Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0,
changed state to up *Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to down *Jan 29
09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset *Jan 29
09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up *Jan 29 09:11:39.060:
%LINK-3-UPDOWN: Interface Dot11Radio0, changed state to down *Jan 29 09:11:39.069: %LINK-5-
CHANGED: Interface Dot11Radio0, changed state to reset *Jan 29 09:11:39.085: %LINK-3-UPDOWN:
Interface Dot11Radio0, changed state to up *Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID
goa added to the slot[1]DTLS keys are plumbed successfully. *Jan 29 09:11:39.151: %CAPWAP-5-
DATA_DTLS_ESTABLISHED: Data DTLS tunnel established. *Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS
Signature is loaded and enabled !--- AP joins the 5508-3 WLC.
```

Logs ACS:

1. Veja as contagens da batida:Se você está verificando logs dentro de 15 minutos da autenticação, certifique-se de você refrescar a contagem da batida. Na mesma página, na parte inferior você tem uma aba da **contagem da batida**.
2. **A monitoração do** clique **e os relatórios** e uma janela pop-up nova aparecem. **Autenticações do** clique **– RAIO – Hoje**. Você pode igualmente clicar **detalhes** a fim verificar que regra de seleção do serviço era aplicada.

Troubleshooting

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

Informações Relacionadas

- Cisco Secure Access Control System
- Suporte Técnico e Documentação - Cisco Systems