Acesso de convidado com fio com âncora e estrangeiro como WLC 5760

Contents

Introduction

Este documento aborda a implantação do recurso de acesso de convidado com fio no Cisco 5760 Wireless LAN Controller que atua como âncora estrangeiro e no controlador de LAN sem fio Cisco 5760 que atua como âncora de convidado na zona desmilitarizada (DMZ) com o software versão 03.03.2.SE. Atualmente, existem soluções para fornecer acesso de convidado através de redes com e sem fio no Cisco 5508 Wireless LAN Controller. O recurso funciona de maneira semelhante no switch Cisco Catalyst 3650, que atua como um controlador externo.

Em redes corporativas, normalmente é necessário fornecer acesso à rede para seus convidados no campus. Os requisitos de acesso para convidados incluem o fornecimento de conectividade à Internet ou outros recursos empresariais seletivos para convidados com e sem fio de forma consistente e gerenciável. O mesmo controlador de LAN sem fio pode ser usado para fornecer acesso a ambos os tipos de convidados no campus. Por razões de segurança, um grande número de administradores de rede corporativa segregam o acesso de convidado a um controlador DMZ por tunelamento. A solução de acesso de convidado também é usada como um método de fallback para clientes convidados que falham nos métodos de autenticação dot1x e MAC Authentication Bypass (MAB).

O usuário convidado se conecta à porta com fio designada em um switch de camada de acesso para acesso e, opcionalmente, pode ser feito para passar pelos modos Web Consent ou Web Authentication, dependendo dos requisitos de segurança (detalhes em seções posteriores). Quando a autenticação de convidado for bem-sucedida, o acesso será fornecido aos recursos de rede e o controlador de convidado gerenciará o tráfego do cliente. A âncora externa é o switch principal no qual o cliente se conecta para acesso à rede. Inicia solicitações de túnel. A âncora do convidado é o switch onde o cliente fica ancorado. Além do Cisco 5500 Series WLAN Controller, o

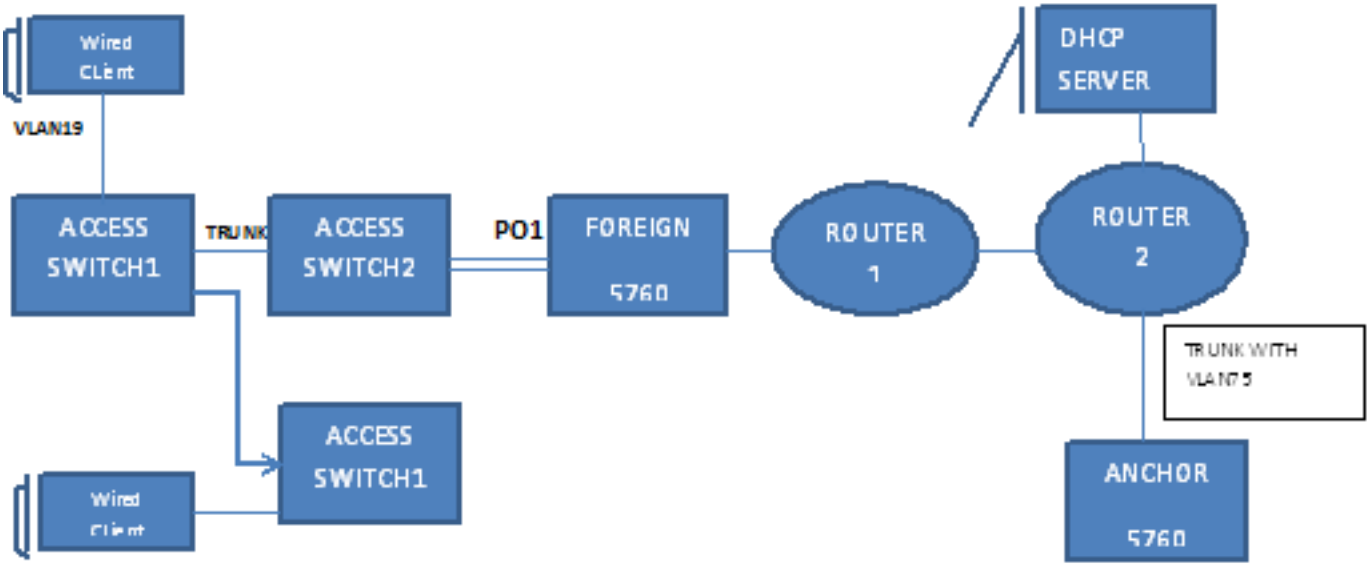
Cisco 5760 Wireless LAN Controller pode ser usado como âncora de convidado. Antes que o recurso de acesso de convidado possa ser implantado, deve haver um túnel de mobilidade estabelecido entre a âncora externa e os switches de âncora de convidado. O recurso de acesso de convidado funciona para os modelos MC (Âncora Estrangeira) > MC (Âncora de Convidado) e MA (Âncora Estrangeira) >> MC (Âncora de Convidado). Os troncos de switch de âncora externa conectam o tráfego de convidado com fio ao controlador de âncora do convidado e várias âncoras de convidado podem ser configuradas para o balanceamento de carga. O cliente está ancorado em um controlador de âncora DMZ. Também é responsável por tratar a atribuição de endereço IP DHCP, bem como a autenticação do cliente. Após a conclusão da autenticação, o cliente pode acessar a rede.

Cenário de implantação

O documento aborda casos de uso comuns em que os clientes com fio se conectam a switches de acesso para acesso à rede. Dois modos de acesso são explicados em exemplos diferentes. Em todos os métodos, o recurso de acesso de convidado com fio pode atuar como um método de fallback para autenticação. Geralmente, esse é um caso de uso quando um usuário convidado traz um dispositivo final desconhecido para a rede. Como o dispositivo final não tem o suplicante de ponto final, ele falhará no modo dot1x de autenticação. Da mesma forma, a autenticação MAB também falharia, pois o endereço MAC do dispositivo final seria desconhecido do servidor de autenticação. Vale observar que nessas implementações, os dispositivos finais corporativos obteriam acesso com êxito, pois teriam um suplicante dot1x ou seus endereços MAC no servidor de autenticação para validação. Isso permite flexibilidade na implantação, pois o administrador não precisa restringir e vincular portas especificamente para acesso de convidado.

Topologia

Este diagrama mostra a topologia usada no cenário de implantação:



OPENAUTH

Configuração de âncora de convidado

1. Ative o rastreamento de dispositivo IP (IPDT) e o rastreamento de DHCP em VLAN(s) cliente(s), neste caso a VLAN 75. A VLAN do cliente precisa ser criada na âncora do convidado.
```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```
2. Crie a VLAN 75 e a interface L3 VLAN.
```
vlan 75
interface Vlan75
ip address 75.1.1.1 255.255.255.0
ip helper-address 192.168.1.1
ip dhcp pool DHCP_75
network 75.1.1.0 255.255.255.0
default-router 75.1.1.1
lease 0 0 10
update arp
```
3. Crie uma LAN de convidado que especifique a VLAN do cliente com o próprio 5760 que atua como âncora de mobilidade. Para o openmode, o comando **no security web-auth** é necessário.
```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor
no security web-auth
no shutdown
```

Configuração externa

1. Ative o DHCP e a criação da VLAN. Como observado, a VLAN do cliente não precisa ser configurada no estrangeiro.
```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```
2. O switch detecta o endereço MAC do cliente de entrada no canal de porta configurado com "access-Session port-control auto" e aplica a política de assinante OPENAUTH. A política OPENAUTH conforme descrito aqui deve ser criada primeiro.
```
policy-map type control subscriber OPENAUTH
event session-started match-all
1 class always do-until-failure
2 activate service-template SERV-TEMP3-OPENAUTH
3 authorize

interface Po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
service-policy type control subscriber OPENAUTH
ip dhcp snooping trust
end
```
3. O aprendizado do endereço MAC deve ser configurado no estrangeiro para VLAN.
```
mac address-table learning vlan 19
```
4. A política OPENAUTH é chamada sequencialmente, que nesse caso aponta para um

serviço. O modelo denominado "SERV-TEMP3 OPENAUTH" é definido aqui:

```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH
```

5. O modelo de serviço contém uma referência ao tipo e nome do túnel. A VLAN 75 do cliente só precisa existir na âncora do convidado, pois é responsável por tratar o tráfego do cliente.

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor 9.7.104.62
no security web-auth
no shutdown
```

6. A solicitação de túnel é iniciada da âncora externa para a âncora do convidado para o cliente com fio e um tunneladdbem-sucedido indica que o processo de criação do túnel está concluído. No ACCESS-SWITCH1, um cliente com fio se conecta à porta Ethernet definida para o modo de acesso pelo administrador da rede. É a porta GigabitEthernet1/0/11 neste exemplo.

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

WEBAUTH

Configuração de âncora de convidado

1. Ative o rastreamento IPDT e DHCP na(s) VLAN(s) cliente(s), neste caso a VLAN 75. A VLAN do cliente precisa ser criada na âncora do convidado.

```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```

2. Crie a VLAN 75 e a interface L3 VLAN.

```
vlan 75
interface Vlan75
ip address 75.1.1.1 255.255.255.0
ip helper-address 192.168.1.1
ip dhcp pool DHCP_75
network 75.1.1.0 255.255.255.0
default-router 75.1.1.1
lease 0 0 10
update arp
```

3. Crie uma LAN de convidado que especifique a VLAN do cliente com o próprio 5760 atuando como âncora de mobilidade. Para o openmode, o comando **no security web-auth** é necessário.

```
guest-lan GUEST_LAN_WEBAUTH 3
client vlan VLAN0075
mobility anchor
security web-auth authentication-list default
security web-auth parameter-map webparalocal
no shutdown
```

Configuração externa

1. Habilite o DHCP e a criação de uma VLAN. Como observado, a VLAN do cliente não precisa ser configurada no estrangeiro.

```
ip dhcp relay information trust-all
```

```
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```

2. O switch detecta o endereço MAC do cliente de entrada no canal de porta configurado com "access-Session port-control auto" e aplica a política de assinante WEBAUTH. A política WEBAUTH conforme descrita aqui deve ser criada primeiro.

```
policy-map type control subscriber WEBAUTH
event session-started match-all
1 class always do-until-failure
2 activate service-template SERV-TEMP3-WEBAUTH
3 authorize

interface po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
service-policy type control subscriber WEBAUTH
ip dhcp snooping trust
end
```

3. O aprendizado MAC deve ser configurado no estrangeiro para VLAN.

```
mac address-table learning vlan 19
```

4. Configure o raio e o mapa de parâmetros.

```
aaa new-model
aaa group server radius rad-grp
server Radius1

dot1x system-auth-control
aaa authentication dot1x default group rad-grp



radius server Radius1
address ipv4 172.19.45.194 auth-port 1812 acct-port 1813
timeout 60
retransmit 3
key radius

parameter-map type webauth webparalocal
type webauth
timeout init-state sec 5000
```

5. A política WEBAUTH é chamada sequencialmente, que nesse caso aponta para um serviço. O modelo chamado SERV-TEMP3 WEBAUTH conforme definido aqui.

```
service-template SERV-TEMP3-WEBAUTH
tunnel type capwap name GUEST_LAN_WEBAUTH
```

6. O modelo de serviço contém uma referência ao tipo e nome do túnel. A VLAN 75 do cliente só precisa existir na âncora do convidado, pois é responsável por tratar o tráfego do cliente.

```
guest-lan GUEST_LAN_WEBAUTH 3
client vlan 75
mobility anchor 9.7.104.62
security web-auth authentication-list default
security web-auth parameter-map webparalocal
no shutdown
```

7. A solicitação de túnel é iniciada da âncora externa para a âncora do convidado para o cliente com fio e um "tunneladdsuccessfully" indica que o processo de criação do túnel foi concluído. No ACCESS-SWITCH1, um cliente com fio se conecta à porta Ethernet definida para o modo de acesso pelo administrador da rede. É a porta GigabitEthernet1/0/11 neste exemplo.

```
interface GigabitEthernet1/0/11
switchport access vlan 19
```

```
switchport mode access
```

Configurar o OPENAUTH e o WEBAUTH em paralelo

Para ter duas LANs de convidado e atribuí-las a diferentes clientes, você deve baseá-las nas VLANs nas quais os clientes são aprendidos.

Configuração de âncora de convidado

1. Habilite o rastreamento IPDT e DHCP na(s) VLAN(s) do cliente, neste caso a VLAN 75. A VLAN do cliente precisa ser criada na âncora do convidado.
```
ip device tracking
ip dhcp relay information trust-all
ip dhcp snooping vlan 75
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
```
2. Crie a VLAN 75 e a interface L3 VLAN.
```
vlan 75
interface Vlan75
ip address 75.1.1.1 255.255.255.0
ip helper-address 192.168.1.1
ip dhcp pool DHCP_75
network 75.1.1.0 255.255.255.0
default-router 75.1.1.1
lease 0 0 10
update arp
```
3. Crie uma LAN de convidado que especifique a VLAN do cliente com o próprio 5760 que atua como âncora de mobilidade. Para o openmode, o comando **no security web-auth** é necessário.
```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor
no security web-auth
no shutdown


guest-lan GUEST_LAN_WEBAUTH 4
client vlan VLAN0075
mobility anchor
security web-auth authentication-list joseph
security web-auth parameter-map webparalocal
no shutdown
```

Configuração externa

1. Habilite o DHCP e a criação de uma VLAN. Como observado, a VLAN do cliente não precisa ser configurada no estrangeiro.
```
ip dhcp relay information trust-all
ip dhcp snooping information option allow-untrusted
ip dhcp snooping
ip device tracking
```
2. O switch detecta o endereço MAC do cliente de entrada no canal de porta configurado com "access-Session port-control auto" e aplica a política de assinante DOUBLEAUTH. O mapa de classe mac1 contém os endereços MAC adicionados para OPENAUTH. Tudo o resto é a WEBAUTH usando o segundo mapa de classe "sempre" com o evento "match-first". A

política DOUBLEAUTH conforme descrito aqui deve ser criada primeiro.

```
policy-map type control subscriber DOUBLEAUTH
event session-started match-first
 1 class vlan19 do-until-failure
 2 activate service-template SERV-TEMP3-OPENAUTH
3 authorize
 2 class vlan18 do-until-failure
 2 activate service-template SERV-TEMP4-WEBAUTH
 3 authorize


interface po1
switchport trunk allowed vlan 19,137
switchport mode trunk
ip arp inspection trust
access-session port-control auto
 service-policy type control subscriber DOUBLEAUTH
ip dhcp snooping trust
end
```

3. O aprendizado MAC deve ser configurado no exterior para as VLANs 18 e 19.

```
mac address-table learning vlan 18 19
```

4. Os mapas de classe da VLAN 19 e da VLAN18 contêm os critérios de correspondência da VLAN com base nos quais você vai diferenciar em qual LAN de convidado o cliente pertence. Ele é definido aqui:

```
class-map type control subscriber match-any vlan18
 match vlan 18

class-map type control subscriber match-any vlan19
 match vlan 19
```

5. A política OPENAUTH é chamada sequencialmente, que nesse caso aponta para um serviço. O modelo denominado SERV-TEMP3 OPENAUTH, conforme definido aqui.

```
service-template SERV-TEMP3-OPENAUTH
tunnel type capwap name GUEST_LAN_OPENAUTH

service-template SERV-TEMP4-WEBAUTH
tunnel type capwap name GUEST_LAN_WEBAUTH
```

6. O modelo de serviço contém uma referência ao tipo e nome do túnel. A VLAN 75 do cliente só precisa existir na âncora do convidado, pois é responsável por tratar o tráfego do cliente.

```
guest-lan GUEST_LAN_OPENAUTH 3
client vlan 75
mobility anchor 9.7.104.62
no security web-auth
no shutdown


guest-lan GUEST_LAN_WEBAUTH 4
client vlan VLAN0075
mobility anchor 9.7.104.62
security web-auth authentication-list joseph
security web-auth parameter-map webparalocal
no shutdown
```

7. A solicitação de túnel é iniciada da âncora externa para a âncora do convidado para o cliente com fio e um "tunneladdsuccessfully" indica que o processo de criação do túnel foi concluído. Nos ACCESS-SWITCHs há vários clientes com fio que se conectam à VLAN 18 ou à VLAN 19, que podem ser atribuídos às LANs convidadas de acordo. É a porta GigabitEthernet1/0/11 neste exemplo.

```
interface GigabitEthernet1/0/11
switchport access vlan 19
switchport mode access
```

Exemplo de O/P do comando WEBAUTH

Externo

```
FOREIGN#show wir client summary
Number of Local Clients : 2
MAC Address    AP Name                          WLAN State              Protocol
--------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                              3    UP                 Ethernet
0021.ccbb.ac7d N/A                              4   UP                Ethernet

ANCHOR#show mac address-table
        Mac Address Table
-------------------------------------------

Vlan   Mac Address    Type       Ports
----   -----------    --------   -----
19   0021.ccbc.44f9   DYNAMIC     Po1
19   0021.ccbb.ac7d   DYNAMIC     Po1

FOREIGN#show access-session mac 0021.ccbc.44f9 details
          Interface: Port-channel1
              IIF-ID: 0x83D880000003D4
        MAC Address: 0021.ccbc.44f9
        IPv6 Address: Unknown
        IPv4 Address: Unknown
          User-Name: 0021.ccbc.44f9
        Device-type: Un-Classified Device
             Status: Unauthorized
             Domain: DATA
     Oper host mode: multi-auth
    Oper control dir: both
    Session timeout: N/A
  Common Session ID: 090C895F000012A70412D338
    Acct Session ID: Unknown
             Handle: 0x1A00023F
     Current Policy: OPENAUTH
      Session Flags: Session Pushed


Local Policies:
      Service Template: SERV-TEMP3-OPENAUTH (priority 150)

Tunnel Profile Name: GUEST_LAN_OPENAUTH
        Tunnel State: 2

Method status list:
      Method           State
      webauth         Authc Success
```

Âncora

```
#show wir client summary
Number of Local Clients : 1
MAC Address    AP Name                          WLAN State              Protocol
--------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                              3    WEBAUTH_PEND       Ethernet
0021.ccbb.ac7d N/A                              4   WEBAUTH_PEND       Ethernet
```

```
ANCHOR#show wir client summary
Number of Local Clients : 2
MAC Address    AP Name                          WLAN State              Protocol
------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                               3    UP                 Ethernet
0021.ccbb.ac7d N/A                               4   UP                 Ethernet

ANCHOR#show mac address-table
         Mac Address Table
-------------------------------------------
Vlan   Mac Address       Type       Ports
----   -----------       --------   -----
19   0021.ccbc.44f9   DYNAMIC     Po1
18   0021.ccbb.ac7d   DYNAMIC     Po1

ANCHOR#show wir client summary
Number of Local Clients : 1

MAC Address   AP Name                          WLAN State              Protocol
------------------------------------------------------------------------------
0021.ccbc.44f9 N/A                               3   UP                  Ethernet
0021.ccbb.ac7d N/A                               4   UP                  Ethernet

ANCHOR#show access-session mac 0021.ccbc.44f9

Interface   MAC Address   Method Domain Status Fg Session ID
-----------------------------------------------------------------------
Ca1         0021.ccbc.44f9 webauth DATA   Auth     090C895F000012A70412D338

ANCHOR#show access-session mac 0021.ccbc.44f9 details
           Interface: Capwap1
             IIF-ID: 0x6DAE4000000248
        MAC Address: 0021.ccbc.44f9
       IPv6 Address: Unknown
       IPv4 Address: 75.1.1.11
          User-Name: 0021.ccbc.44f9
             Status: Authorized
             Domain: DATA
      Oper host mode: multi-auth
   Oper control dir: both
    Session timeout: N/A
  Common Session ID: 090C895F000012A70412D338
    Acct Session ID: Unknown
             Handle: 0x4000023A
     Current Policy: (No Policy)

Method status list:
      Method           State
      webauth         Authc Success
```