Índice

Introdução

Este desenvolvimento das capas de documento dos recursos de acesso prendidos do convidado em um controlador do Wireless LAN de Cisco 5760 (WLC) que atue como uma âncora estrangeira e um Cisco 5760 WLC que atue como uma âncora do convidado na zona desmilitarizada (DMZ) com software de versão da versão 03.03.2.SE. A característica trabalha de forma semelhante em um Cisco Catalyst 3650 Switch que atue como um controlador estrangeiro.

Hoje, as soluções existem para a disposição do acesso do convidado através do Sem fio e das redes ligadas com fio em Cisco 5508 WLC. Nas redes de empreendimento, há tipicamente uma necessidade de fornecer o acesso de rede a seus convidados no terreno. As exigências do acesso do convidado incluem a disposição da conectividade de Internet ou de outros recursos seletivos da empresa aos convidados prendidos e wireless em uma maneira consistente e manejável. O mesmo WLC pode ser usado para fornecer o acesso a ambos os tipos de convidados no terreno. Por razões de segurança, um grande número administradores de rede de empreendimento segregam o acesso do convidado a um controlador DMZ através do Tunelamento. A solução de acesso do convidado é usada igualmente como um método da reserva para os clientes do convidado que falham o dot1x e os métodos de autenticação do desvio da autenticação de MAC (

O usuário convidado conecta à porta prendida designada em um switch de camada de acesso para o acesso e opcionalmente pôde ser feito para atravessar os modos do acordo ou da autenticação da Web da Web, dependentes dos requisitos de segurança (detalhes nas seções mais recente). Uma vez que a autenticação do convidado sucede, o acesso está fornecido aos recursos de rede e o controlador do convidado controla o tráfego do cliente. A âncora estrangeira é o interruptor preliminar onde o cliente conecta para o acesso de rede. Inicia requisições de túnel. A âncora do convidado é o interruptor aonde o cliente obtém realmente ancorado. Independentemente do controlador de WLAN do Cisco 5500 Series, Cisco 5760 WLC pode ser usado como uma âncora do convidado. Antes que os recursos de acesso do convidado possam ser distribuídos, devam haver um túnel da mobilidade estabelecido entre a âncora estrangeira e o Switches da âncora do convidado. Os recursos de acesso do convidado trabalham para MC

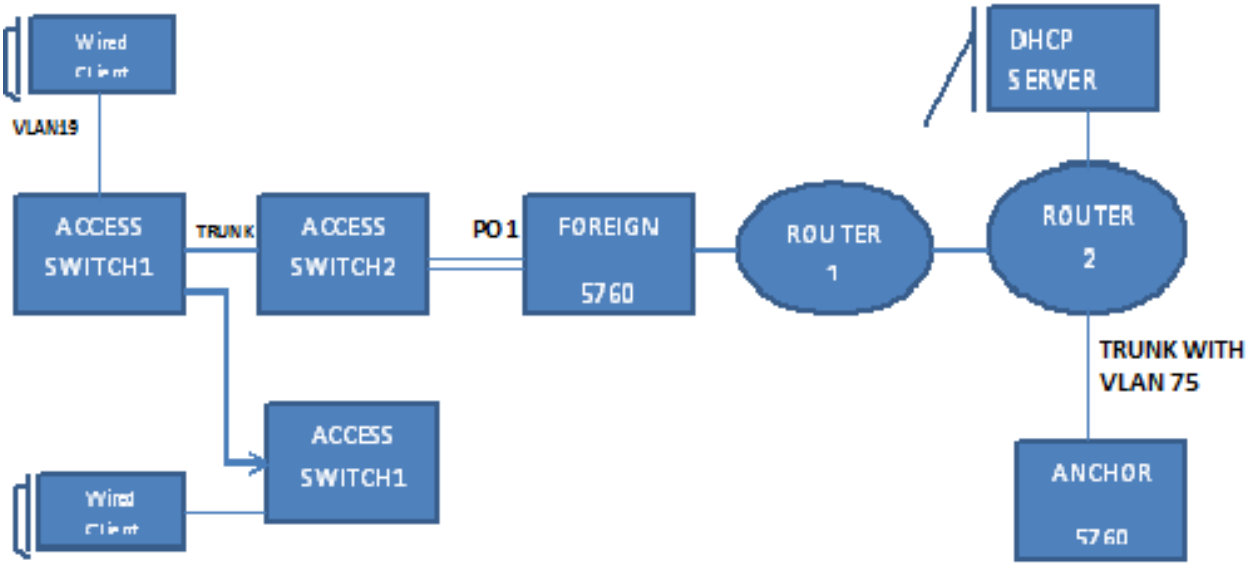
(âncora estrangeira) >> modelos MC (âncora do convidado) e MA (âncora estrangeira) >>MC (âncora do convidado). Os troncos estrangeiros do interruptor da âncora prenderam o tráfego do convidado ao controlador da âncora do convidado e as âncoras múltiplas do convidado podem ser configuradas para o Balanceamento de carga. O cliente é ancorado a um controlador da âncora DMZ. Igualmente segura a atribuição do endereço IP de Um ou Mais Servidores Cisco ICM NT DHCP assim como a autenticação do cliente. Depois que a autenticação termina, o cliente pode alcançar a rede.

Cenário de distribuição

Este caixas de utilização comum das capas de documento onde os clientes prendidos conectam switch de acesso para o acesso de rede. Dois modos de acesso são explicados em exemplos diferentes. Em todos os métodos, os recursos de acesso prendidos do convidado podem atuar como um método de autenticação da reserva. Este é tipicamente um exemplo do uso quando um usuário convidado traz um dispositivo final que seja desconhecido à rede. Desde que o dispositivo final está faltando o suplicante do valor-limite, falha o modo de autenticação do dot1x. Similarmente, a autenticação MAB igualmente falha, porque o MAC address do dispositivo final é desconhecido ao server de autenticação. Note que em tais aplicações, os dispositivos finais corporativos obtêm com sucesso o acesso desde que têm um suplicante do dot1x ou seus endereços MAC no server de autenticação para a validação. Isto permite a flexibilidade no desenvolvimento, porque o administrador não precisa de restringir acima e amarrar especificamente portas para o acesso do convidado.

Topologia

Este diagrama mostra a topologia usada no cenário de distribuição.



OPENAUTH

Configuração da âncora do convidado

Conclua estes passos:

1. Permita a espião do seguimento (IPDT) e DHCP do dispositivo IP no cliente VLAN, neste caso VLAN75. O cliente VLAN precisa de ser criado na âncora do convidado.
2. Crie o VLAN 75 e a interface de VLAN da camada 3.
3. Crie um convidado LAN que especifique o cliente VLAN com os 5760 próprio que atua como a âncora da mobilidade.Para o openmode, **nenhum** comando do Web-**AUTH da Segurança** é exigido.

Configuração estrangeira

1. Permita o DHCP e crie um VLAN. Como notável, o cliente VLAN não precisa de estabelecer-se no estrangeiro.
2. O interruptor detecta o MAC address do cliente de entrada no canal de porta configurado com da “o porta-controle acesso-sessão auto” e aplica a política de assinante “OPENAUTH”. A política “OPENAUTH” como descrita aqui deve ser criada primeiramente: `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
   ```
3. Configurar a aprendizagem MAC no estrangeiro para o VLAN. `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
   ```
4. A política OPENAUTH é referida sequencialmente que aponta neste caso a um serviço, molde nomeado o "SERV-TEMP3OPENAUTH" como definido aqui: `service-template` **`SERV-TEMP3-OPENAUTH`**

   ```
   tunnel type capwap name GUEST_LAN_OPENAUTH
   ```
5. O molde do serviço contém uma referência ao tipo de túnel e ao nome. O cliente VLAN75 precisa somente de existir na âncora do convidado desde que segura 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 requisição de túnel é iniciada do estrangeiro à âncora do convidado para o cliente prendido e os “tunneladdsuccess” indicam que o processo do acúmulo do túnel terminou.No

ACCESS-SWITCH1 um cliente prendido conecta à porta Ethernet que é ajustada ao modo de acesso pelo administrador de rede. É o gigabitethernet 1/0/11 da porta neste exemplo:`interface GigabitEthernet1/0/11`

`switchport access vlan 19`

`switchport mode access`

`WEBAUTH`

WEBAUTH

Configuração da âncora do convidado

1. Permita a espião IPDT e DHCP no cliente VLAN, neste caso VLAN75. O cliente VLAN precisa de ser criado na âncora do convidado. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`
2. Crie o VLAN 75 e a interface de VLAN da camada 3. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`
3. Crie um convidado LAN que especifique o cliente VLAN com os 5760 próprio que atua como a âncora da mobilidade.Para o openmode, **nenhum** comando do Web-**AUTH da Segurança** é exigido.`interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`

Configuração estrangeira

1. Permita o DHCP e a criação do VLAN. Como notável, o cliente VLAN não precisa de estabelecer-se no estrangeiro. `interface GigabitEthernet1/0/11`

   `switchport access vlan 19`

   `switchport mode access`

   `WEBAUTH`
2. O interruptor detecta o MAC address do cliente de entrada no canal de porta configurado com da “o porta-controle acesso-sessão auto” e aplica a política de assinante “WEBAUTH”. A política “WEBAUTH” como descrita aqui deve ser criada primeiramente. `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
```

3. A aprendizagem MAC deve ser configurada no estrangeiro para o VLAN. `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
```

4. Configurar RADUIS e o mapa do parâmetro. `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
```

5. A política “WEBAUTH” é referida sequencialmente que aponta neste caso a um serviço, molde nomeado o "SERV-TEMP3WEBAUTH" como definido aqui: `service-template SERV-TEMP3-WEBAUTH`

```
tunnel type capwap name GUEST_LAN_WEBAUTH
```

6. O molde do serviço contém uma referência ao tipo de túnel e ao nome. O cliente VLAN75 precisa somente de existir na âncora do convidado desde que segura 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 requisição de túnel é iniciada do estrangeiro à âncora do convidado para o cliente prendido e os “tunneladdsuccess” indicam que o processo do acúmulo do túnel terminou.No ACCESS-SWITCH1 um cliente prendido conecta à porta Ethernet que é ajustada ao modo de acesso pelo administrador de rede. É o gigabitethernet 1/0/11 da porta neste exemplo:`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
```

Exemplo do comando O/P WEBAUTH

Estrangeiro

```
FOREIGN#sh 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              3   UP                Ethernet

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

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

FOREIGN#sh 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

```
#sh 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             3   WEBAUTH_PEND     Ethernet

ANCHOR#sh 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      3   UP                Ethernet

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

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


ANCHOR#sh 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      3   UP            Ethernet


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

Interface   MAC Address   Method Domain Status Fg Session ID
```

```
---------------------------------------------------------------------

Ca1         0021.ccbc.44f9 webauth DATA   Auth    090C895F000012A70412D338


ANCHOR#sh 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
```