Cliente wireless convirgido Onboarding do controlador do acesso 5760/3850/3650) de BYOD (com FQDN ACL

Índice

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[O DNS baseou o fluxo de processo ACL](#)
[Configurar](#)
[Configuração de WLC](#)
[Configuração ISE](#)
[Verificar](#)
[Referências](#)

Introdução

Este documento descreve um exemplo de configuração para o uso das Listas de acesso baseadas DNS (ACL), lista de domínios do nome de domínio totalmente qualificado (FQDN) permitir o acesso às listas de domínios específicas durante o estado da autenticação da Web/do abastecimento Bring Your Own Device do cliente (BYOD) em controladores convirgidos do acesso.

Pré-requisitos

Requisitos

Este documento supõe que você já sabe configurar a autenticação da Web central básica (CWA), isto é apenas uma adição para demonstrar o uso de listas de domínios FQDN ao faciltate BYOD. Os exemplos de configuração CWA e ISE BYOD são providos na extremidade deste documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:
Software Release 1.4 do Cisco Identity Services Engine

Software Release 3.7.4 de Cisco WLC 5760

O DNS baseou o fluxo de processo ACL

Em cima do Identity Services Engine (ISE) que retorna o nome do nome da reorientação ACL que tráfego deve ser reorientada ao ISE e qual não) e da lista de domínios FQDN (nome do ACL

usado para determinar (nome do ACL que é traçado à lista URL FQDN no controlador a ser permitido o acesso antes da autenticação), o fluxo será como esta'n:

1. O controlador do Wireless LAN (WLC) enviará o payload do capwap ao Access Point (AP) para permitir a espião DNS para as URL.
2. Espiões AP para a pergunta DNS do cliente. Se o Domain Name combina a URL permitida, o AP enviará o pedido ao servidor DNS, esperará a resposta do servidor DNS e analisará gramaticalmente a resposta de DNS e enviá-la-á com somente o primeiro endereço IP de Um ou Mais Servidores Cisco ICM NT resolvido.Se o Domain Name não combina, a seguir a resposta de DNS está enviada como é (sem alteração) de volta ao cliente.
3. Caso que o Domain Name combina, o primeiro endereço IP de Um ou Mais Servidores Cisco ICM NT resolved estará enviado ao WLC no payload do capwap. O WLC atualiza implicitamente o ACL traçado à lista de domínios FQDN com o endereço IP de Um ou Mais Servidores Cisco ICM NT que resolved obteve do AP usando a seguinte aproximação: O endereço IP de Um ou Mais Servidores Cisco ICM NT resolved será adicionado como um endereço de destino em cada regra de ACL traçada à lista de domínios FQDN.Cada regra de ACL obtém invertida da licença para negar e vice-versa então a vontade ACL obtém aplicada ao cliente. **Note**: Com este mecanismo nós não podemos traçar a lista de domínios a CWA reorientamos o ACL, porque inverter as regras ACL da reorientação resultará nas mudar para permitir que significa que o tráfego deve ser reorientado ao ISE. Consequentemente a lista de domínios FQDN será traçada a uma “licença separada IP todo o qualquer” ACL na divisória da configuração.Para esclarecer esse ponto, supõe que a rede admin configurou a lista de domínios FQDN com cisco.com URL na lista, e traçou essa lista de domínios ao seguinte ACL:

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

   Em cima do cliente que pede cisco.com, o Domain Name cisco.com das resoluções AP ao endereço IP 72.163.4.161 e envia-o ao contoller, o ACL será alterado para ser como abaixo e obtém aplicado ao cliente:

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Quando o cliente enviar o pedido HTTP “GET”: O cliente obterá reorientado caso que o ACL permite o tráfego.Com endereço IP de Um ou Mais Servidores Cisco ICM NT negado o tráfego HTTP será permitido.
5. Uma vez que o App está transferido no cliente e o abastecimento está completo, o server ISE envia a sessão CoA termina ao WLC.
6. Uma vez que o cliente de-é autenticado do WLC, o AP removerá a bandeira para a espião pelo cliente e desabilitará a espião.

Configurar

Configuração de WLC

1. Create reorienta o ACL:
   Este ACL é usado para definir que tráfego não deve ser reorientado ao ISE (negado no ACL) e que tráfego deve ser reorientado (permitido no ACL).

```
ip access-list extended REDIRECT_ACL
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny udp any any eq domain
deny udp any eq domain any
deny ip any host 10.48.39.228
deny ip host 10.48.39.228 any
permit tcp any any eq www
permit tcp any any eq 443
```

   Nesta lista de acessos 10.48.39.228 é o endereço IP do servidor ISE.

2. Configurar a lista de domínios FQDN:Esta lista contém os Domain Name que o cliente pode alcançar antes do abastecimento ou da autenticação CWA.

```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```

3. Configurar uma lista de acessos com a licença IP alguma ser combinado com o URLS_LIST:
   Este ACL é precisado de ser traçado à lista de domínios FQDN porque nós devemos aplicar uma lista de acesso real IP ao cliente (nós não podemos aplicar a lista de domínios autônoma FQDN).

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

4. Trace a lista de domínios URLS_LIST ao FQDN_ACL:

```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```

5. Configurar o Onboarding CWA SSID:
   Este SSID será usado para a autenticação da Web central do cliente e o abastecimento do cliente, o FQDN_ACL e REDIRECT_ACL serão aplicados a este SSID pelo ISE

```
wlan byod 2 byod
 aaa-override
 accounting-list rad-acct
 client vlan VLAN0200
 mac-filtering MACFILTER
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 no shutdown
```

   Nesta lista de método da configuração **MACFILTER** SSID é a lista de método que aponta ao grupo do raio ISE e o **rad-acct** é a lista do método de contabilidade esses pontos ao mesmo grupo do raio ISE.

   Sumário da configuração da lista de método usado neste exemplo:

```
aaa group server radius ISEGroup
 server name ISE1
```

```
aaa authorization network MACFILTER group ISEGroup

aaa accounting network rad-acct start-stop group ISEGroup

radius server ISE1
 address ipv4 10.48.39.228 auth-port 1812 acct-port 1813
 key 7 112A1016141D5A5E57

aaa server radius dynamic-author
 client 10.48.39.228 server-key 7 123A0C0411045D5679
 auth-type any
```

Configuração ISE

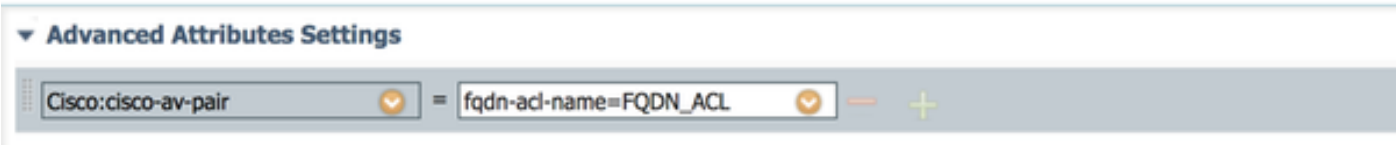
Esta seção supõe que você é familiar com a peça da configuração CWA ISE, configuração ISE é quase a mesma com as seguintes alterações.

O resultado wireless da autenticação do desvio da autenticação do MAC address CWA (MAB) deve retornar os seguintes atributos junto com o CWA reorienta a URL:

```
cisco-av-pair = fqdn-acl-name=FQDN_ACL
cisco-av-pair = url-redirect-acl=REDIRECT_ACL
```

Onde FQDN_ACL está o nome da lista de acesso IP que é traçada à lista de domínios e ao REDIRECT_ACL é o CWA normal reorienta a lista de acessos.

O resultado da autenticação de Thefore CWA MAB deve ser configurado como dentro abaixo:



Verificar

Para verificar que a lista de domínios FQDN está aplicada ao comando abaixo do uso do cliente:

```
show access-session mac <client_mac> details
```

O exemplo do comando outputs mostrar Domain Name permitidos:

```
5760-2#show access-session mac 60f4.45b2.407d details
            Interface:  Capwap7
               IIF-ID:  0x41BD400000002D
            Wlan SSID:  byod
       AP MAC Address:  f07f.0610.2e10
          MAC Address:  60f4.45b2.407d
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.200.151
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  0a30275b58610bdf0000004b
      Acct Session ID:  0x00000005
               Handle:  0x42000013
       Current Policy:  (No Policy)
        Session Flags:  Session Pushed

Server Policies:

             FQDN ACL: FQDN_ACL
         Domain Names: cisco.com play.google.*.*

         URL Redirect:  https://bru-
ise.wlaaan.com:8443/portal/gateway?sessionId=0a30275b58610bdf0000004b&portal=27963fb0-e96e-11e4-
a30a-005056bf01c9&action=cwa&token=fcc0772269e75991be7f1ca238cbb035
     URL Redirect ACL:  REDIRECT_ACL

Method status list: empty
```

Referências

[Autenticação da Web central no exemplo de configuração WLC e ISE]

[Projeto do infraestrutura Wireless BYOD]

[Configurar o 2.1 ISE para Chromebook Onboarding]