Controlador sem fio de acesso convergido (5760/3850/3650) Integração de cliente BYOD com ACLs FQDN

Contents

Introduction

Este documento descreve um exemplo de configuração para o uso de listas de acesso (ACLs) baseadas em DNS, lista de domínios totalmente qualificados (FQDN) para permitir o acesso a listas de domínio específicas durante a autenticação da Web/estado de provisionamento BYOD (Bring Your Own Device) do cliente em controladores de acesso convergente.

Prerequisites

Requirements

Este documento pressupõe que você já sabe como configurar a CWA (Central Web Authentication, Autenticação da Web Central) básica, isso é apenas uma adição para demonstrar o uso de listas de domínio FQDN para facilitar o BYOD. Exemplos de configuração de BYOD do CWA e do ISE são referenciados no final deste documento.

Componentes Utilizados

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

Software Cisco WLC 5760 versão 3.7.4

Fluxo de processo ACL baseado em DNS

Quando o Identity Services Engine (ISE) retornar o nome da ACL de redirecionamento (nome da ACL usada para determinar qual tráfego será redirecionado para o ISE e qual não será) e o nome

da lista de domínios FQDN (nome da ACL que é mapeada para a lista de URL FQDN no controlador para ter acesso antes da autenticação), o fluxo será como tal:

1. O Wireless LAN Controller (WLC) enviará o payload capwap ao ponto de acesso (AP) para ativar o rastreamento de DNS para os URLs.
2. O AP snoops para a consulta DNS do cliente. Se o nome de domínio corresponder ao URL permitido, o AP encaminhará a solicitação ao servidor DNS, aguardará a resposta do servidor DNS e analisará a resposta DNS e a encaminhará com apenas o primeiro endereço IP resolvido.Se o nome de domínio não corresponder, a resposta DNS será encaminhada como está (sem modificação) de volta ao cliente.
3. Caso o nome de domínio corresponda, o primeiro endereço IP resolvido será enviado para a WLC no payload do capwap. A WLC atualiza implicitamente a ACL mapeada para a lista de domínios FQDN com o endereço IP resolvido que obteve do AP usando a seguinte abordagem: O endereço IP resolvido será adicionado como um endereço de destino em cada regra da ACL mapeada para a lista de domínios FQDN.Cada regra de ACL é revertida de permitir para negar e vice-versa, então a ACL será aplicada ao cliente. **Note**: Com esse mecanismo, não podemos mapear a lista de domínios para a ACL de redirecionamento CWA, pois reverter as regras de ACL de redirecionamento resultará na alteração para permitir, o que significa que o tráfego deve ser redirecionado para o ISE. Portanto, a lista de domínios FQDN será mapeada para uma ACL separada "permit ip any any" na parte de configuração.Para esclarecer esse ponto, suponha que o administrador de rede tenha configurado a lista de domínios FQDN com o url cisco.com na lista e mapeado essa lista de domínios para a seguinte ACL:

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

   Ao solicitar o cisco.com, o AP resolve o nome de domínio cisco.com para o endereço IP 72.163.4.161 e o envia ao controlador, a ACL será modificada para ser como abaixo e será aplicada ao cliente:

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Quando o cliente envia uma solicitação HTTP "GET": O cliente será redirecionado caso a ACL permita o tráfego.Com o endereço IP negado, o tráfego http será permitido.
5. Quando o aplicativo é baixado no cliente e o provisionamento é concluído, o servidor ISE envia a sessão CoA terminada para o WLC.
6. Quando o cliente for desautenticado da WLC, o AP removerá o sinalizador de espionagem por cliente e desativará o rastreamento.

Configurar

Configuração de WLC

1. Criar ACL de redirecionamento:
   Essa ACL é usada para definir qual tráfego não deve ser redirecionado para ISE (negado na

ACL) e qual tráfego deve ser redirecionado (permitido na 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 acesso 10.48.39.228 está o endereço IP do servidor ISE.

2. Configure a lista de domínios FQDN:Esta lista contém os nomes de domínio que o cliente pode acessar antes do provisionamento ou da autenticação CWA.
```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```
3. Configure uma lista de acesso com permit ip any any para ser combinada com URLS_LIST: Essa ACL é necessária para ser mapeada para a lista de domínios FQDN porque devemos aplicar uma lista de acesso IP real ao cliente (não podemos aplicar a lista de domínios FQDN autônomos).

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

4. Mapeie a lista de domínios URLS_LIST para FQDN_ACL:

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

5. Configure o SSID do CWA de integração:
Este SSID será usado para a autenticação da Web central do cliente e o provisionamento do cliente , o FQDN_ACL e o 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 configuração de SSID, a lista de métodos **MACFILTER** é a lista de métodos que aponta para o grupo RADIUS do ISE e **rad-acct** é a lista de métodos de contabilidade que aponta para o mesmo grupo RADIUS do ISE.

Resumo da configuração da lista de métodos usada 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 do ISE

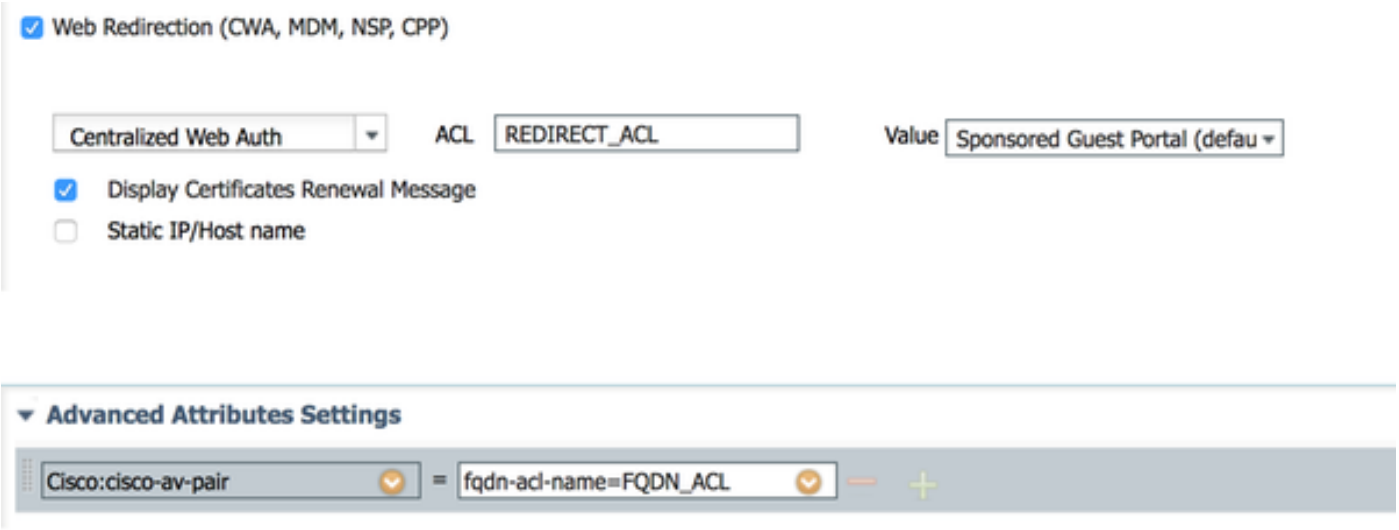
Esta seção supõe que você esteja familiarizado com a parte de configuração do CWA ISE, a configuração do ISE é praticamente a mesma com as seguintes modificações.

O resultado da autenticação do Wireless CWA Mac address Authentication Bypass (MAB) deve retornar os seguintes atributos junto com o URL de redirecionamento do CWA:

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

Onde FQDN_ACL é o nome da lista de acesso IP que é mapeada para a lista de domínios e REDIRECT_ACL é a lista de acesso de redirecionamento CWA normal.

O resultado da autenticação do CWA MAB deve ser configurado como abaixo:



Verificar

Para verificar se a lista de domínios FQDN é aplicada ao cliente, use o comando abaixo:

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

Exemplo de saídas de comando mostrando nomes de domínio 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

[Exemplo de autenticação da Web central no WLC e ISE]

[Projeto de infraestrutura sem fio BYOD]

[Configurar o ISE 2.1 para integração do catálogo]