Controlador inalámbrico de acceso convergente (5760/3850/3650) Integración de cliente BYOD con ACL FQDN

Contenido

Introducción

Este documento describe un ejemplo de configuración para el uso de listas de acceso basadas en DNS (ACL), lista de dominios de nombre de dominio completo (FQDN) para permitir el acceso a listas de dominios específicas durante el estado de aprovisionamiento de autenticación web/uso de dispositivos propios de cliente (BYOD) en controladores de acceso convergentes.

Prerequisites

Requirements

Este documento supone que ya sabe configurar la autenticación web central básica (CWA), esto es solo una adición para demostrar el uso de listas de dominios FQDN para facilitar la BYOD. Al final de este documento se hace referencia a ejemplos de configuración de BYOD de CWA e ISE.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.
Versión 1.4 del software Cisco Identity Services Engine

Versión 3.7.4 del software Cisco WLC 5760

Flujo de proceso de ACL basado en DNS

Cuando Identity Services Engine (ISE) devuelva el nombre de ACL de redirección (nombre de ACL utilizado para determinar qué tráfico se redirigirá a ISE y cuál no) y el nombre de lista de

dominios FQDN (nombre de ACL asignado a la lista de URL de FQDN en el controlador al que se permitirá el acceso antes de la autenticación), el flujo será el siguiente:

1. El controlador de LAN inalámbrica (WLC) enviará la carga útil capwap al punto de acceso (AP) para habilitar la detección de DNS para las URL.
2. AP realiza snoops para la consulta DNS desde el cliente. Si el nombre de dominio coincide con la URL permitida, AP reenviará la solicitud al servidor DNS, esperará la respuesta del servidor DNS y analizará la respuesta DNS y la reenviará con sólo la primera dirección IP resuelta.Si el nombre de dominio no coincide, la respuesta DNS se reenvía tal como se reenvía (sin modificaciones) al cliente.
3. En caso de que el nombre de dominio coincida, la primera dirección IP resuelta será enviada al WLC en la carga útil capwap. El WLC actualiza implícitamente la ACL asignada a la lista de dominio FQDN con la dirección IP resuelta que obtuvo del AP usando el siguiente enfoque: La dirección IP resuelta se agregará como dirección de destino en cada regla de ACL asignada a la lista de dominios FQDN.Cada regla de ACL se revierte de permit a deny y viceversa, luego la ACL se aplicará al cliente. **Nota:** Con este mecanismo, no podemos asignar la lista de dominios a la ACL de redirección CWA, porque revertir las reglas de ACL de redirección resultará en cambiarlas para permitir lo que significa que el tráfico debe redirigirse a ISE. Por lo tanto, la lista de dominios FQDN se mapeará a una ACL separada "permit ip any any" en la parte de configuración.Para aclarar ese punto, asuma que el administrador de red ha configurado la lista de dominios FQDN con la url de cisco.com en la lista y ha asignado esa lista de dominios a la siguiente ACL:

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

   Cuando el cliente solicita cisco.com, AP resuelve el nombre de dominio cisco.com a la dirección IP 72.163.4.161 y lo envía al controlador, la ACL se modificará para que sea como se indica a continuación y se aplicará al cliente:

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Cuando el cliente envía una solicitud HTTP "GET": El cliente será redirigido en caso de que la ACL permita el tráfico.Con la dirección IP denegada, se permitirá el tráfico http.
5. Una vez que la Aplicación se descarga en el cliente y el aprovisionamiento se completa, el servidor ISE envía la sesión CoA terminada al WLC.
6. Una vez que el cliente se desautentica del WLC, el AP quitará el indicador para la indagación por cliente y desactivará la indagación.

Configurar

Configuración de WLC

1. Crear ACL de redirección:
   Esta ACL se utiliza para definir qué tráfico no se debe redirigir a ISE (denegado en la ACL) y qué tráfico se debe redirigir (permitido en la 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
```

En esta lista de acceso 10.48.39.228 se encuentra la dirección IP del servidor ISE.

2. Configure la lista de dominios FQDN:Esta lista contiene los nombres de dominio a los que el cliente puede acceder antes del aprovisionamiento o la autenticación de CWA.

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

3. Configure una lista de acceso con permit ip any any para que se combine con URLS_LIST: Esta ACL es necesaria para asignarse a la lista de dominios FQDN porque debemos aplicar una lista de acceso IP real al cliente (no podemos aplicar una lista de dominios FQDN independientes).

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

4. Asigne la lista de dominios URLS_LIST a FQDN_ACL:

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

5. Configure el SSID de CWA de incorporación:
   Este SSID se utilizará para la autenticación web central del cliente y el aprovisionamiento del cliente , el FQDN_ACL y REDIRECT_ACL serán aplicados a este SSID por 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
```

En esta lista de métodos **MACFILTER** de configuración SSID es la lista de métodos que apunta al grupo de RADIUS ISE y **rad-acct** es la lista de métodos de contabilidad que apunta al mismo grupo de RADIUS ISE.

Resumen de la configuración de lista de métodos utilizada en este ejemplo:

```
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
```

Configuración de ISE

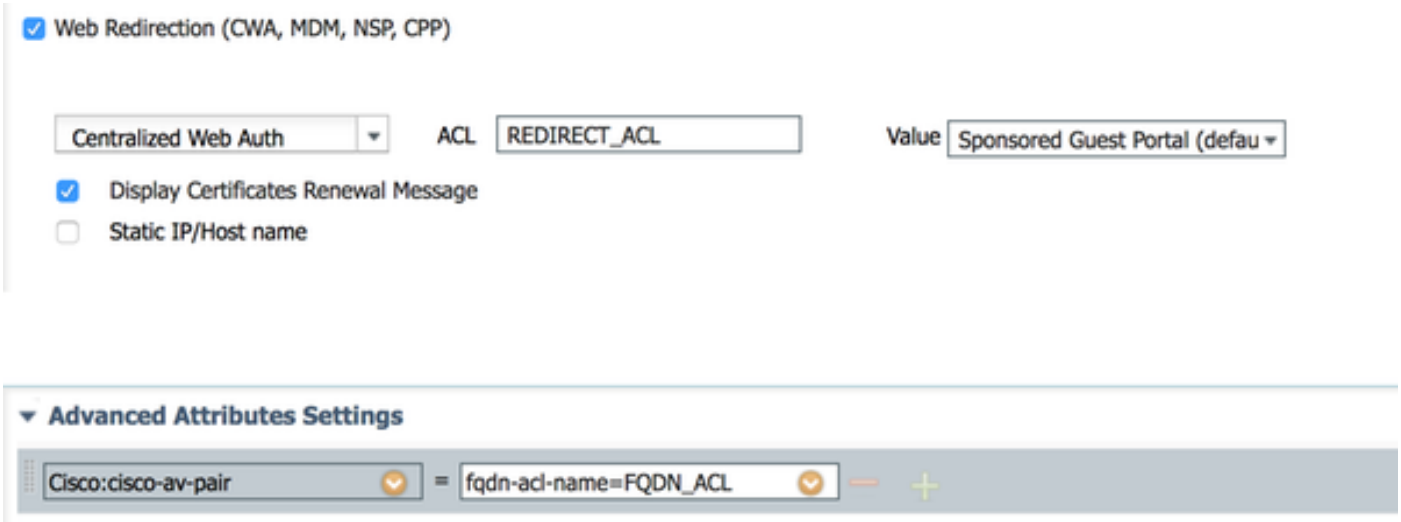
En esta sección se supone que está familiarizado con la parte de configuración de ISE de CWA, la configuración de ISE es prácticamente la misma con las siguientes modificaciones.

El resultado de la autenticación CWA MAC address Authentication Bypass (MAB) (Omisión de autenticación de dirección MAC) de Wireless debe devolver los siguientes atributos junto con la URL de redirección CWA:

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

Donde FQDN_ACL es el nombre de la lista de acceso IP asignada a la lista de dominios y REDIRECT_ACL es la lista de acceso de redirección de CWA normal.

Por lo tanto, el resultado de la autenticación de CWA MAB debe configurarse como se muestra a continuación:



Verificación

Para verificar que la lista de dominio FQDN se aplica al cliente, utilice el siguiente comando:

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

Ejemplo de resultados del comando que muestran nombres de dominio 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
```

Referencias

[Ejemplo de Configuración de Autenticación Web Central en el WLC y el ISE]

[Diseño de la infraestructura inalámbrica BYOD]

[Configuración de ISE 2.1 para la incorporación de Chromebook]