Cliente inalámbrico convergido Onboarding del regulador del acceso (5760/3850/3650) BYOD con FQDN ACL

Contenido

Introducción

Este documento describe un ejemplo de configuración para el uso de las Listas de acceso basadas DNS (ACL), nombre de dominio completo (FQDN) lista de dominio de permitir el acceso a las listas específicas del dominio durante la autenticación Web/el estado de disposición de Bring Your Own Device del cliente (BYOD) en los reguladores convergidos del acceso.

Prerequisites

Requisitos

Este documento asume que usted sabe ya configurar la autenticación Web central básica (CWA), esto es apenas una adición para demostrar el uso de las listas del dominio FQDN al faciltate BYOD. Los ejemplos de configuración CWA y ISE BYOD se refieren en el extremo de este documento.

Componentes Utilizados

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

Software Release 3.7.4 del WLC 5760 de Cisco

El DNS basó el flujo del proceso ACL

Sobre el Identity Services Engine (ISE) que vuelve el nombre de la reorientación ACL (nombre del

ACL usado para determinar qué tráfico debe ser reorientado al ISE y cuál no) y el nombre FQDN lista de dominio (nombre del ACL que se asocia a la lista url FQDN en el regulador que se tendrá en cuenta el acceso antes de la autenticación), el flujo estará como tal:

1. El regulador del Wireless LAN (WLC) enviará el payload del capwap al Access Point (AP) para habilitar el snooping DNS para los URL.
2. Fisgones AP para la interrogación DNS del cliente. Si el Domain Name hace juego el URL permitido, el AP transmitirá a la petición el servidor DNS, esperará la respuesta del servidor DNS y analizará la respuesta de DNS y la remitirá con solamente la primera dirección IP resuelta.Si el Domain Name no hace juego, después se remite la respuesta de DNS como está (sin la modificación) de nuevo al cliente.
3. En caso de que el Domain Name haga juego, la primera dirección IP resuelta será enviada al WLC en el payload del capwap. El WLC pone al día implícito el ACL asociado al FQDN lista de dominio con la dirección IP resuelta que consiguió del AP usando el acercamiento siguiente: La dirección IP resuelta será agregada como dirección destino en cada regla de ACL asociada al FQDN lista de dominio.Cada regla de ACL consigue invertida del permiso de negar y vice versa entonces la voluntad ACL consigue aplicada al cliente. **Note**: Con este mecanismo no podemos asociar lista de dominio a CWA reorientamos el ACL, porque la inversión de las reglas ACL de la reorientación resultará en el cambio de ellas para permitir que significa que el tráfico se debe reorientar al ISE. Por lo tanto el FQDN lista de dominio será asociado a un “IP separado del permiso cualquier cualquier” ACL en la partición de la configuración.Para aclarar esa punta, asuma que la red admin ha configurado el FQDN lista de dominio con el URL de cisco.com en la lista, y que ha asociado eso lista de dominio al ACL siguiente:

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

   Sobre el cliente que pide cisco.com, el Domain Name cisco.com de las resoluciones AP a la dirección IP 72.163.4.161 y lo envía al contoller, el ACL será modificado para estar como abajo y consigue aplicado al cliente:

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Cuando el cliente envía la petición HTTP “GET”: El cliente conseguirá reorientado en caso de que el ACL permita el tráfico.Con la dirección IP negada el tráfico HTTP será permitido.
5. Una vez que el App se descarga en el cliente y el aprovisionamiento es completo, el servidor ISE envía la sesión CoA termina al WLC.
6. Una vez que de-autentican al cliente del WLC, el AP quitará el indicador para el snooping por el cliente y inhabilitará el snooping.

Configurar

Configuración del WLC

1. Create reorienta el ACL:

Este ACL se utiliza para definir qué tráfico no se debe reorientar al ISE (negado en el ACL) y qué tráfico debe ser reorientado (permitido en el 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 es el dirección IP del servidor ISE.

2. Configure el FQDN lista de dominio:Esta lista contiene los Domain Name que el cliente puede acceder antes de disposición o de la autenticación CWA.

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

3. Configure una lista de acceso con el IP del permiso cualquier ser combinado con el URLS_LIST:
   Este ACL es necesario ser asociado al FQDN lista de dominio porque debemos aplicar una lista de acceso real IP al cliente (no podemos aplicar el FQDN independiente lista de dominio).

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

4. Asocie el URLS_LIST lista de dominio al FQDN_ACL:

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

5. Configure el Onboarding CWA SSID:
   Este SSID será utilizado para la autenticación Web central del cliente y el aprovisionamiento del cliente, el FQDN_ACL y REDIRECT_ACL serán aplicados a este SSID por el 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 de la configuración **MACFILTER** SSID es la lista de métodos que señala al grupo del radio ISE y el **rad-acct** es la lista del método de contabilidad esas puntas al mismo grupo del radio ISE.

Resumen de configuración de la lista de métodos usado 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 ISE

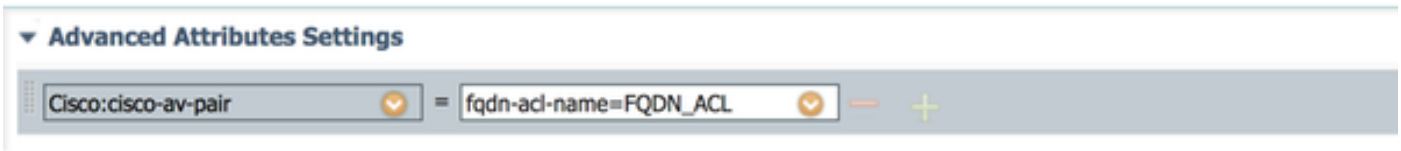
Esta sección asume que usted es familiar con la pieza de la configuración CWA ISE, configuración ISE es casi lo mismo con las modificaciones siguientes.

El resultado inalámbrico de la autenticación de puente de la autenticación del MAC address CWA (MAB) debe volver los atributos siguientes junto con el CWA reorienta el URL:

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

Donde está el nombre FQDN_ACL de la lista de acceso por IP que se asocia al lista de dominio y REDIRECT_ACL es el CWA normal reorienta la lista de acceso.

El resultado de la autenticación de Thefore CWA MAB se debe configurar como adentro abajo:



Verificación

Para verificar que el FQDN lista de dominio esté aplicado al comando abajo del uso del cliente:

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

Ejemplo de las salidas de comando que muestran los 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
```

Referencias

[Autenticación Web central en el ejemplo de configuración del WLC y ISE]

[Diseño de la infraestructura de red inalámbrica BYOD]

[2.1 de la configuración ISE para Chromebook Onboarding]