Controller wireless ad accesso convergente (5760/3850/3650) BYOD: caricamento del client con ACL FQDN

Sommario

Introduzione

In questo documento viene descritto un esempio di configurazione per l'utilizzo di elenchi di accesso basati su DNS (ACL) e di elenchi di domini con nome di dominio completo (FQDN) per consentire l'accesso a elenchi di domini specifici durante l'autenticazione Web/lo stato di provisioning BYOD (Bring Your Own Device) del client sui controller di accesso convergenti.

Prerequisiti

Requisiti

In questo documento si presume che l'utente sappia già configurare l'autenticazione Web centrale di base (CWA). Si tratta solo di un'aggiunta per dimostrare l'utilizzo degli elenchi di domini FQDN per semplificare l'autenticazione BYOD. Gli esempi di configurazione CWA e ISE BYOD sono menzionati alla fine di questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
Software Cisco Identity Services Engine release 1.4

Software Cisco WLC 5760 release 3.7.4

Flusso di processo ACL basato su DNS

Dopo la restituzione da parte di Identity Services Engine (ISE) del nome ACL di reindirizzamento

(nome dell'ACL utilizzato per determinare quale traffico deve essere reindirizzato a ISE e quale no) e del nome dell'elenco di domini FQDN (nome dell'ACL mappato all'elenco di URL FQDN sul controller a cui deve essere consentito l'accesso prima dell'autenticazione), il flusso sarà il seguente:

1. Il controller WLC (Wireless LAN Controller) invierà il payload capwap al punto di accesso (AP) per abilitare lo snooping DNS per gli URL.
2. AP snoops per la query DNS dal client. Se il nome di dominio corrisponde all'URL consentito, il punto di accesso inoltrerà la richiesta al server DNS, attenderà la risposta dal server DNS e analizzerà la risposta DNS e la inoltrerà solo con il primo indirizzo IP risolto.Se il nome di dominio non corrisponde, la risposta DNS viene inoltrata senza modifiche al client.
3. Se il nome di dominio corrisponde, il primo indirizzo IP risolto viene inviato al WLC nel payload capwap. WLC aggiorna in modo implicito l'ACL mappato all'elenco di domini FQDN con l'indirizzo IP risolto ottenuto dall'access point utilizzando il seguente approccio: L'indirizzo IP risolto verrà aggiunto come indirizzo di destinazione in ogni regola dell'ACL mappata all'elenco di domini FQDN.Ogni regola dell'ACL viene annullata e quindi negata e viceversa, l'ACL viene applicato al client. **Nota:** Con questo meccanismo non è possibile mappare l'elenco dei domini all'ACL di reindirizzamento CWA, in quanto l'inversione delle regole ACL di reindirizzamento causerà la loro modifica per consentire, il che significa che il traffico deve essere reindirizzato all'ISE. Pertanto, l'elenco dei domini FQDN verrà mappato su un ACL "allow ip any" separato nella parte di configurazione.Per chiarire questo punto, si supponga che l'amministratore di rete abbia configurato l'elenco di domini FQDN con cisco.com URL nell'elenco e abbia mappato tale elenco di domini al seguente ACL:

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

   Quando il client richiede cisco.com, AP risolve il nome di dominio cisco.com nell'indirizzo IP 72.163.4.161 e lo invia al controller, l'ACL verrà modificato come indicato di seguito e applicato al client:

   ```
   ip access-list extended FQDN_ACL
   deny ip any host 72.163.4.161
   ```
4. Quando il client invia la richiesta HTTP "GET": Il client verrà reindirizzato qualora l'ACL autorizzi il traffico.Se l'indirizzo IP è negato, il traffico http sarà consentito.
5. Una volta scaricata l'app sul client e completato il provisioning, il server ISE invia il messaggio di terminazione della sessione CoA al WLC.
6. Dopo aver deautenticato il client dal WLC, l'AP rimuove il flag per lo snooping per client e disabilita lo snooping.

Configurazione

Configurazione WLC

1. Creare un ACL di reindirizzamento:
   Questo ACL è usato per definire il traffico da non reindirizzare all'ISE (accesso negato) e il

traffico da reindirizzare (accesso consentito nell'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
```

Nell'elenco degli accessi 10.48.39.228 è l'indirizzo IP del server ISE.

2. Configurare l'elenco di domini FQDN:Questo elenco contiene i nomi di dominio a cui il client può accedere prima del provisioning o dell'autenticazione CWA.
```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```
3. Configurare un elenco degli accessi con allow ip any any da combinare con l'URL_LIST: Ènecessario eseguire il mapping di questo ACL all'elenco di domini FQDN perché è necessario applicare un elenco di accessi IP effettivo al client (non è possibile applicare un elenco di domini FQDN autonomo).

```
ip access-list extended FQDN_ACL
permit ip any any
```
4. Mappare l'elenco dei domini URL_LIST all'FQDN_ACL:

```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```
5. Configurare il SSID CWA di caricamento:
Questo SSID verrà utilizzato per l'autenticazione Web centrale del client e il provisioning del client. I valori FQDN_ACL e REDIRECT_ACL verranno applicati a questo SSID da 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
```

In questa configurazione SSID l'elenco dei metodi **MACFILTER** è l'elenco dei metodi che punta al gruppo del raggio ISE e **rad-acct** è l'elenco dei metodi di accounting che punta allo stesso gruppo del raggio ISE.

Riepilogo della configurazione dell'elenco di metodi utilizzata nell'esempio:

```
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
```

Configurazione di ISE

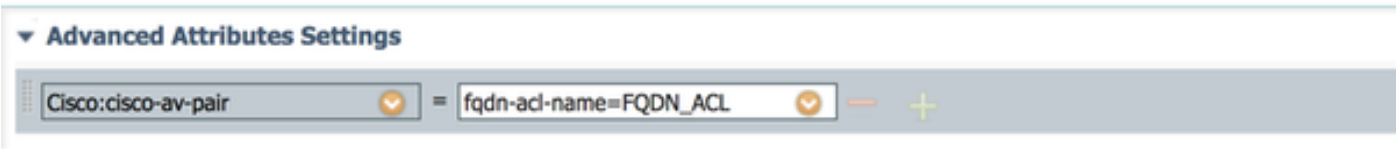
In questa sezione si presume che l'utente abbia familiarità con la parte di configurazione CWA ISE e che la configurazione ISE sia pressoché la stessa con le modifiche seguenti.

Il risultato dell'autenticazione MAB (Authentication Bypass) dell'indirizzo Mac CWA wireless deve restituire gli attributi seguenti insieme all'URL di reindirizzamento di CWA:

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

Dove FQDN_ACL è il nome dell'elenco degli accessi IP mappato all'elenco dei domini e REDIRECT_ACL è il normale elenco degli accessi di reindirizzamento CWA.

Pertanto, il risultato dell'autenticazione MAB CWA deve essere configurato come indicato di seguito:



Verifica

Per verificare che l'elenco dei domini FQDN sia applicato al client, utilizzare il comando seguente:

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

Esempio di output del comando che mostra i nomi di dominio consentiti:

```
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
```

Riferimenti

[Esempio di autenticazione Web centralizzata su WLC e ISE]

[Progettazione dell'infrastruttura wireless BYOD]

[Configurazione di ISE 2.1 per Chromebook Onboarding]