Установившийся Контроллер беспроводной локальной сети Доступа (5760/3850/3650) BYOD клиент Онбоардинг с ACL FQDN

Содержание

Введение

Этот документ описывает пример конфигурации для использования DNS Базирующиеся списки доступа (ACL), список доменов Полного доменного имени (FQDN)
для предоставления доступа к определенным спискам доменов во время состояния инициализации BYOD Web-аутентификации/Клиента на Установившихся Контроллерах доступа.

Предварительные условия

Требования

Этот документ предполагает, что вы уже знаете, как настроить основную Центральную веб-аутентификацию (CWA), это - просто добавление для демонстрации использования списков доменов FQDN для упрощения BYOD. На CWA и ISE примеры конфигурации BYOD ссылаются в конце этого документа.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:
Выпуск ПО платформы Cisco Identity Services Engine 1.4

Выпуск ПО Cisco WLC 5760 3.7.4

DNS базирующийся поток процессов ACL

На платформу Identity Services Engine (ISE), возвращая название ACL перенаправления (название ACL использовало определять, какой трафик должен быть перенаправлен к ISE и который не будет) и название списка доменов FQDN (название ACL , который сопоставлен со Списком URL - адресов FQDN на контроллере, который будет позволен для доступа перед аутентификацией), поток будет как таков:

1. Контроллер беспроводной локальной сети (WLC) передаст capwap информационное наполнение к точке доступа (AP) для включения DNS, snooping для URL.
2. AP snooping для запроса DNS от клиента. Если доменное имя совпадет с позволенным URL, то AP перешлет запрос на сервер DNS, будет ждать ответа от сервера DNS и проанализирует DNS - ответ и передаст его с только первым решенным IP-адресом.Если доменное имя не совпадает, то DNS - ответ передан, как (без модификации) назад клиенту.
3. В случае, если доменное имя совпадает, первый решенный IP-адрес будет передаваться WLC в capwap информационном наполнении. WLC неявно обновляет ACL, сопоставленный со списком доменов FQDN с решенным IP-адресом, который это получило от AP с помощью следующего подхода: Решенный IP-адрес будет добавлен как адрес назначения (DA) на каждом правиле ACL, сопоставленного со списком доменов FQDN.Каждое правило ACL инвертировано от разрешения для запрета, и наоборот затем ACL будет применяться к клиент. **Примечание:** С этим механизмом мы не можем сопоставить список доменов с ACL перенаправления CWA, потому что инвертирование правил списка прав доступа (ACL) перенаправления закончится в изменение их для разрешения, что означает, что трафик должен быть перенаправлен к ISE. Therfore FQDN список доменов будет сопоставлен с отдельным ACL "permit ip any any" в части конфигурации.Для прояснения той мысли предположите, что сеть admin настроила список доменов FQDN с URL cisco.com в списке и сопоставила тот список доменов со следующим ACL:
   ```
   ip access-list extended FQDN_ACLpermit ip any any
   ```
   На клиента, запрашивающего cisco.com, cisco.com доменного имени решений AP к IP-адресу 72.163.4.161 и, передают его к contoller, ACL будет модифицироваться, чтобы быть как ниже и применен к клиент:
   ```
   ip access-list extended FQDN_ACLdeny ip any host 72.163.4.161
   ```
4. Когда клиент отправляет запрос "GET" HTTP: Клиент будет перенаправлен в случае, если ACL разрешает трафик.С запрещенным IP-адресом будет позволен трафик HTTP.
5. Как только Приложение загружено на клиенте, и инициализация завершена, сервер ISE передает сеанс CoA, оконечный к WLC.
6. Как только клиент является de-authenticated от WLC, AP удалит флаг для отслеживания на клиента и отключит отслеживание.

Настройка

Настройка WLC

1. Создайте ACL перенаправления:
   Этот ACL используется для определения, какой трафик не должен быть перенаправлен к ISE (запрещенный в ACL) и какой трафик должен быть

перенаправлен (Разрешенный в ACL).
`ip access-list extended REDIRECT_ACLdeny udp any eq bootps anydeny udp any any eq bootpcdeny udp any eq bootpc anydeny udp any any eq domaindeny udp any eq domain anydeny ip any host 10.48.39.228deny ip host 10.48.39.228 anypermit tcp any any eq wwwpermit tcp any any eq 443` В этом списке доступа 10.48.39.228 IP-адрес сервера ISE.

2. Настройте список доменов FQDN:Этот список содержит доменные имена, к которым клиент может обратиться прежде, чем настроить или аутентификация CWA.`passthru-domain-list URLS_LISTmatch play.google.*.*match cisco.com`
3. Настройте список доступа с permit ip any any, который будет объединен с URLS_LIST: Этот ACL необходим, чтобы быть сопоставленным со списком доменов FQDN, потому что мы должны применить фактический список доступа IP к клиенту (мы не можем применить автономный список доменов FQDN).
   `ip access-list extended FQDN_ACLpermit ip any any`
4. Сопоставьте список доменов URLS_LIST с FQDN_ACL:
   `access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST`
5. Настройте Onboarding CWA SSID:
   Этот SSID будет использоваться для клиентской центральной веб-аутентификации и клиентской инициализации, FQDN_ACL и REDIRECT_ACL будут применены к этому SSID 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` В этой конфигурации SSID список методов **MACFILTER** является списком методов, указывающим на группу радиуса ISE, и **рад-acct** является списком метода учета, который указывает той же группе радиуса ISE.

   Сводка конфигурации списка методов использовала в данном примере:
   `aaa group server radius ISEGroup server name ISE1aaa authorization network MACFILTER group ISEGroup aaa accounting network rad-acct start-stop group ISEGroupradius server ISE1 address ipv4 10.48.39.228 auth-port 1812 acct-port 1813 key 7 112A1016141D5A5E57aaa server radius dynamic-author client 10.48.39.228 server-key 7 123A0C0411045D5679 auth-type any`

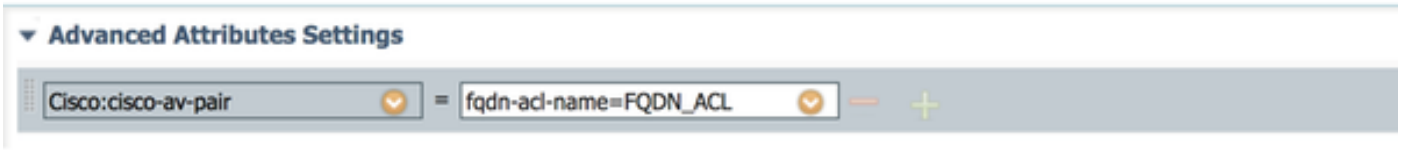
Конфигурация ISE

Этот раздел предполагает, что вы - familar с частью конфигурации ISE CWA, конфигурация ISE является почти тем же со следующими модификациями.

Беспроводной Обход Аутентификации с использованием MAC-адреса CWA (MAB) результат аутентификации должен возвратить следующие атрибуты наряду с URL перенаправления CWA:

`cisco-av-pair = fqdn-acl-name=FQDN_ACLcisco-av-pair = url-redirect-acl=REDIRECT_ACL`
Где FQDN_ACL является названием списка доступа IP, который сопоставлен со списком доменов, и REDIRECT_ACL является обычным списком доступа перенаправления CWA.

Thefore CWA результат аутентификации MAB должен быть настроен как в ниже:



Проверка

Проверить, что список доменов FQDN применен к клиентскому использованию ниже команды:

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

Пример выходных данных команды, показывая разрешил доменные имена:

```
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 PushedServer 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_ACLMethod status list: empty
```

Ссылки

[Центральная веб-аутентификация на WLC и примере конфигурации ISE]

[Дизайн беспроводной инфраструктуры BYOD]

[Настройте ISE 2.1 для Chromebook Onboarding]