Configurez le SSID et les VLAN sur des aps autonomes

Contenu

Introduction

Ce document explique comment configurer les points d'accès autonome (aps) pour :

- Réseaux locaux virtuels (VLAN)
- Ouvrez l'authentification
- 802.1x avec le Service RADIUS (Remote Authentication Dial-In User Service) interne
- 802.1x avec le RAYON externe
- Clé pré-partagée (PSK)
- Authentification d'adresse MAC
- Authentification Web (rayon interne)
- Intercommunication de Web

Conditions préalables

Conditions requises

Cisco vous recommande ont une connaissance de base de ces thèmes :

- 802.1x
- PSK
- RAYON
- Authentification Web

Composants utilisés

Les informations dans ce document sont basées sur la version 15.3(3)JBB AP 3700.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

> **Conseil** : Ces exemples s'applique également à AP en mode autonome à l'intérieur d'ASA 5506, la différence est celui au lieu de configurent le port de commutateur où AP est connecté, la configuration est appliqués à la yole 1/9 de l'ASA.

Configurez

> Remarque: Les identifiants d'ensemble de services (SSID) qui appartiennent au même VLAN ne peuvent pas être appliqués à une radio en même temps. Les exemples de configuration du SSID avec le même VLAN n'ont pas été activés en même temps sur même AP.

Configurez le VLAN-commutateur et l'AP

Configurez les VLAN requis sur AP et commutez. Ce sont les VLAN utilisés dans cet exemple :

- VLAN 2401 (indigène)
- VLAN 2402
- VLAN 2403

Configurez les aps et les VLAN

Configurez les Gigabit Ethernet d'interface

```
# conf t

# interface gig 0.2401
# encapsulation dot1q 2401 native

# interface gig 0.2402
# encapsulation dot1q 2402
# bridge-group 242

# interface gig 0.2403
```

```
# encapsulation dot1q 2403
# bridge-group 243
```

Configurez l'interface 802.11a par radio

```
# interface dot11radio 1.2401
# encapsulation dot1q 2401 native

# interface dot11radio 1.2402
# encapsulation dot1q 2402
# bridge-group 242

# interface dot11radio 1.2403
# encapsulation dot1q 2403
# bridge-group 243
```

> Remarque: 802.11b transmettent par radio (interface dot11radio 0) ne sont pas configurés, car ils utilisent le VLAN indigène d'AP.

Configurez le commutateur VLAN

```
# conf t
# vlan 2401-2403
```

Configurez l'interface où AP est connecté :

```
# conf t
# interface <port-id-where-AP-is-connected>
# switchport trunk encapsulation dot1q
# switchport mode trunk
# switchport trunk native vlan 2401
# switchport trunk allowed vlan 2401-2403
# spanning-tree portfast trunk
```

Authentification ouverte SSID - Le VLAN indigène d'AP

Ce SSID n'a pas la Sécurité, il est annoncé (visible aux clients) et les clients sans fil qui joint le WLAN sont assignés au VLAN indigène.

Étape 1. Configurez le SSID.

```
# dot11 ssid OPEN
# authentication open
# guest-mode
```

Étape 2. Assignez le SSID à la radio 802.11b.

```
# interface dot11radio 0
# ssid OPEN
```

802.1x SSID - RAYON interne

Ce SSID utilise AP comme serveur de RAYON. Rendez-vous compte qu'AP car les supports de serveur de RAYON seulement SAUTENT, EAP-FAST et authentification MAC.

Étape 1. Enable AP comme serveur de rayon.

L'IP address de Server(NAS) d'accès au réseau est le BVI d'AP, car cette adresse IP est celle qui envoie la demande d'authentification elle-même. En outre, créez un nom d'utilisateur et mot de passe.

```
# aaa new-model
# radius-server local
# nas <a.b.c.d> key 0 <shared-key>
# user <username> password 0 <password>
```

Étape 2. Configurez le serveur de RAYON auquel AP envoie la demande d'authentification, comme il est RAYON local, l'adresse IP est celui assigné à l'interface de Vitrual de la passerelle d'AP (BVI).

```
# radius server <radius-server-name>
# address ipv4 <a.b.c.d> auth-port 1812 acct-port 1813
# timeout 10
# retransmit 3
# key 0 <shared-key>
```

Étape 3. Affectez ce serveur de RAYON à un groupe de rayon.

```
# aaa group server radius <radius-group>
# server name <radius-server-name>
```

Étape 4. Assignez ce groupe de rayon à une méthode d'authentification.

```
# aaa authentication login <eap-method-name> group <radius-group>
```

Étape 5. Créez le SSID, assignez-le à VLAN 2402.

```
#  dot11 ssid internal-radius
#  vlan 2402
#  authentication open eap <eap-method-name>
#  authentication network-eap <eap-method-name>
#  authentication key-management wpa version 2
#  mbssid guest-mode
```

Étape 6. Assignez le ssid à l'interface 802.11a et spécifiez le mode de chiffrement.

```
# interface dot11radio 1
# mbssid
# encryption vlan 2402 mode ciphers aes-ccm
# ssid internal-radius
```

802.1x SSID - RAYON externe

La configuration est presque identique que le RAYON interne.

Étape 1. Configurez l'**aaa new-model.**

Étape 2, au lieu de l'IP address d'AP, utilisent l'adresse IP externe de RAYON.

SSID - PSK

Ce SSID utilise la Sécurité WPA2/PSK et les utilisateurs sur ce SSID sont assignés à VLAN 2402.

Étape 1. Configurez le SSID.

```
# conf t
# dot11 ssid PSK-ex
# authentication open
# authentication key-management wpa version 2
# wpa-psk ascii 0 <password>
# mbssid guest-mode
# vlan 2402
```

Étape 2. Assignez le SSID à l'interface par radio et configurez le mode de chiffrement.

```
# interface dot11radio 1
# encryption vlan 2402 mode ciphers aes-ccm
# ssid PSK-ex
```

SSID - Authentification d'adresse MAC

Ce SSID authentifie les clients sans fil basés sur leur adresse MAC. Il utilise l'adresse MAC comme nom d'utilisateur/mot de passe. Dans cet exemple AP agit en tant que RAYON local, ainsi AP enregistre la liste d'adresse MAC. La même configuration peut être appliquée avec le serveur RADIUS externe.

Étape 1. Enable AP comme serveur de RAYON. L'IP address de NAS est le BVI d'AP. Créez l'entrée pour le client avec l'aaaabbbbcccc d'adresse MAC.

```
# aaa new-model
# radius-server local
# nas <a.b.c.d> key 0 <shared-key>
# user aaaabbbbcccc password 0 aaaabbbbcccc mac-auth-only
```

Étape 2. Configurez le serveur de RAYON auquel AP envoie la demande d'authentification (c'est AP lui-même).

```
# radius server <radius-server-name>
# address ipv4 <a.b.c.d> auth-port 1812 acct-port 1813
# timeout 10
# retransmit 3
# key 0 <shared-key>
```

Étape 3. Affectez ce serveur de RAYON à un groupe de rayon.

```
# aaa group server radius <radius-group>
# server name <radius-server-name>
```

Étape 4. Assignez ce groupe de rayon à une méthode d'authentification.

```
# aaa authentication login <mac-method> group <radius-group>
```

Étape 5. Créez le SSID, cet exemple l'assigne à VLAN 2402.

```
#  dot11 ssid mac-auth
#  vlan 2402
#  authentication open mac-address <mac-method>
#  mbssid guest-mode
```

Étape 6. Assignez le SSID à l'interface 802.11a.

```
# interface dot11radio 1
# mbssid
# ssid mac-auth
```

SSID - Authentification de Web interne

Des utilisateurs qui se connectent à ce SSID sont réorientés à un portail d'authentification Web pour entrer un nom d'utilisateur valide/mot de passe, si l'authentification est réussie, ils ont accès au réseau. Dans cet exemple, les utilisateurs sont enregistrés sur le serveur local de RAYON.

Dans cet exemple, le SSID est assigné à VLAN 2403.

Étape 1. Enable AP comme serveur de RAYON. L'IP address de NAS est le BVI d'AP.

```
# aaa new-model
# radius-server local
# nas <a.b.c.d> key 0 <shared-key>
```

Étape 2. Configurez le serveur de RAYON auquel AP envoie la demande d'authentification (c'est AP lui-même).

```
# radius server <radius-name>
# address ipv4 <a.b.c.d> auth-port 1812 acct-port 1813
# timeout 10
# retransmit 3
# key 0 <shared-key>
```

Étape 3. Affectez ce serveur de rayon à un groupe de rayon.

```
# aaa group server radius <radius-group>
# server name <radius-name>
```

Étape 4. Assignez ce groupe de rayon à une méthode d'authentification.

```
# aaa authentication login <web-method> group <radius-group>
```

Étape 5. Créez les stratégies d'admission.

```
# ip admission name webauth-pol proxy http
# ip admission name webauth-pol method-list authentication <web-method>
```

Étape 6. Configurez le SSID.

```
# conf t
# dot11 ssid webauth-autonomous
# authentication open
```

```
# web-auth
# vlan 2403
# mbssid guest-mode
```

Étape 7. Assignez le SSID à l'interface.

```
# conf t
# int dot11radio 1
# ssid webauth-autonomous
```

Étape 8. Assignez la stratégie à la bonne sous-interface.

```
# conf t
# int dot11radio 1.2403
# ip admission webauth-pol
```

> Remarque: Si le SSID travaille à l'indigène, alors la stratégie est appliquée directement à l'interface, pas à la sous-interface (dot11radio 0 ou dot11radio 1).

Étape 9. Créez le nom d'utilisateur/mot de passe pour les utilisateurs d'invité.

```
# conf t
# dot11 guest
# username <username> lifetime 35000 password <password>
```

SSID - Intercommunication de Web

Quand un client se connecte à un SSID à la configuration d'intercommunication de Web, elle sera réorientée à un portail web pour recevoir les termes et les conditions de l'utilisation de réseau, sinon, l'utilisateur ne pourront pas utiliser le service.

Cet exemple assigne le SSID au VLAN indigène.

Étape 1. Créez la stratégie d'admission.

```
# config t
# ip admission name web-passth consent
```

Étape 2. Spécifiez le message à afficher quand les clients se connectent à ce SSID.

```
# ip admission consent-banner text %
                                    ======= WELCOME ======
                                   Message to be displayed to clients
                                                          .........
                                                          .........
                                                          .........
                                                          .........
                                                          .........
%
```

Étape 3. Créez le SSID.

```
# dot11 ssid webpassth-autonomous
# web-auth
# authentication open
```

```
# guest-mode
```

Étape 4. Assignez le SSID et la stratégie d'admission à la radio

```
# interface dot11radio { 0 | 1 }
# ssid webpassth-autonomous
# ip admission web-passth
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

show dot11 associations

Ceci affiche le MAC address, l'ipv4 et l'ipv6 addres, le nom du SSID des clients sans fil connectés.

```
ap# show dot11 associations

802.11 Client Stations on Dot11Radio0:

SSID [webpassth-autonomous] :

MAC Address    IP address      IPV6 address                            Device        Name
Parent         State
c4b3.01d8.5c9d 172.16.0.122    ::                                      unknown       -
self           Assoc
```

show dot11 associations aaaa.bbbb.cccc

Ceci affiche plus de coordonnées du client sans fil spécifié dans le MAC address comme RSSI, SNR, des débits de données l'a pris en charge et d'autres.

```
ap# show dot11 associations c4b3.01d8.5c9d

Address : c4b3.01d8.5c9d Name : NONE
IP Address : 172.16.0.122 IPv6 Address : ::
Gateway Address : 0.0.0.0
Netmask Address : 0.0.0.0 Interface : Dot11Radio 0
Bridge-group : 1
reap_flags_1 : 0x0 ip_learn_type : 0x0 transient_static_ip : 0x0
Device : unknown Software Version : NONE
CCX Version : NONE Client MFP : Off

State : Assoc Parent : self
SSID : webpassth-autonomous
VLAN : 0
Hops to Infra : 1 Association Id : 1
Clients Associated: 0 Repeaters associated: 0
Tunnel Address : 0.0.0.0
Key Mgmt type : NONE Encryption : Off
Current Rate : m15b2 Capability : WMM ShortHdr ShortSlot
Supported Rates : 1.0 2.0 5.5 11.0 6.0 9.0 12.0 18.0 24.0 36.0 48.0 54.0 m0-2 m1-2 m2-2 m3-2 m4-
2 m5-2 m6-2 m7-2 m8-2 m9-2 m10-2 m11-2 m12-2 m13-2 m14-2 m15-2
Voice Rates : disabled Bandwidth : 20 MHz
Signal Strength : -30 dBm Connected for : 447 seconds
Signal to Noise : 56 dB Activity Timeout : 56 seconds
Power-save : On Last Activity : 4 seconds ago
```

```
Apsd DE AC(s) : NONE

Packets Input : 1035 Packets Output : 893
Bytes Input : 151853 Bytes Output : 661627
Duplicates Rcvd : 1 Data Retries : 93
Decrypt Failed : 0 RTS Retries : 0
MIC Failed : 0 MIC Missing : 0
Packets Redirected: 0 Redirect Filtered: 0
IP source guard failed : 0 PPPoE passthrough failed : 0
DAI failed : IP mismatch : 0 src MAC mismatch : 0 target MAC mismatch : 0
Existing IP failed : 0 New IP failed : 0
11w Status       : Off
```

webauth-sessions de l'exposition dot11

Ceci affiche le MAC address, l'ipv4 addres pour l'intercommunication d'authentification Web ou de Web et le nom d'utilisateur si le SSID est configuré pour l'authentification Web.

```
ap# show dot11 webauth-sessions
c4b3.01d8.5c9d 172.16.0.122  connected
```

show dot11 bssid

Ceci affiche les BSSID associés aux WLAN par interface par radio.

```
ap# show dot11 bssid

Interface      BSSID         Guest  SSID
Dot11Radio0   00c8.8b1b.49f0  Yes  webpassth-autonomous
Dot11Radio1   00c8.8b04.ffb0  Yes  PSK-ex
Dot11Radio1   00c8.8b04.ffb1  Yes  mac-auth
```

show bridge bavard

Ceci affiche la relation entre les sous-interfaces et les groupes de passerelle.

```
ap# show bridge verbose

Total of 300 station blocks, 297 free
Codes: P - permanent, S - self


Flood ports (BG 1)           RX count    TX count
Dot11Radio0                         0           0
Dot11Radio1.2401                    0           7
GigabitEthernet0.2401              31         225


Flood ports (BG 242)         RX count    TX count
Dot11Radio1.2402                    0           0
GigabitEthernet0.2402               0           0


Flood ports (BG 243)         RX count    TX count
Dot11Radio1.2403                    0           0
GigabitEthernet0.2403               0           0
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

clear dot11 client aaa.bbbb.cccc

Cette commande aide à démonter un client sans fil du réseau.

nom d'utilisateur clair de webauth-utilisateur du webauth dot11

Cette commande aide à supprimer la session d'authentification Web de l'utilisateur spécifié.

Exécutez ces commandes de débogage afin de vérifier la procédure d'authentification du client :

```
ap# show bridge verbose

Total of 300 station blocks, 297 free
Codes: P - permanent, S - self


Flood ports (BG 1)           RX count    TX count
Dot11Radio0                         0           0
Dot11Radio1.2401                    0           7
GigabitEthernet0.2401              31         225


Flood ports (BG 242)         RX count    TX count
Dot11Radio1.2402                    0           0
GigabitEthernet0.2402               0           0


Flood ports (BG 243)         RX count    TX count
Dot11Radio1.2403                    0           0
GigabitEthernet0.2403               0           0
```

PSK

```
ap# show bridge verbose

Total of 300 station blocks, 297 free
Codes: P - permanent, S - self


Flood ports (BG 1)           RX count    TX count
Dot11Radio0                         0           0
Dot11Radio1.2401                    0           7
GigabitEthernet0.2401              31         225


Flood ports (BG 242)         RX count    TX count
Dot11Radio1.2402                    0           0
GigabitEthernet0.2402               0           0


Flood ports (BG 243)         RX count    TX count
Dot11Radio1.2403                    0           0
GigabitEthernet0.2403               0           0
```

802.1x

```
ap# show bridge verbose

Total of 300 station blocks, 297 free
```

```
Codes: P - permanent, S - self


Flood ports (BG 1)           RX count    TX count
Dot11Radio0                         0           0
Dot11Radio1.2401                    0           7
GigabitEthernet0.2401              31         225


Flood ports (BG 242)         RX count    TX count
Dot11Radio1.2402                    0           0
GigabitEthernet0.2402               0           0


Flood ports (BG 243)         RX count    TX count
Dot11Radio1.2403                    0           0
GigabitEthernet0.2403               0           0
```

Authentification MAC

```
ap# show bridge verbose

Total of 300 station blocks, 297 free
Codes: P - permanent, S - self


Flood ports (BG 1)           RX count    TX count
Dot11Radio0                         0           0
Dot11Radio1.2401                    0           7
GigabitEthernet0.2401              31         225


Flood ports (BG 242)         RX count    TX count
Dot11Radio1.2402                    0           0
GigabitEthernet0.2402               0           0


Flood ports (BG 243)         RX count    TX count
Dot11Radio1.2403                    0           0
GigabitEthernet0.2403               0           0
```