authentification basée sur port avec l'exemple d'une configuration de RECOUVREMENT et ACS 5.2

Contenu

Introduction

Ce document décrit comment configurer un point d'accès léger (LAP) pendant qu'un suppliant de 802.1x afin d'authentifier contre un serveur de RAYON tel qu'un serveur de contrôle d'accès (ACS) 5.2.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant que vous tentiez cette configuration :

- Ayez la connaissance de base du contrôleur LAN Sans fil (WLC) et des recouvrements.

- Ayez la connaissance fonctionnelle du serveur d'AAA.
- Ayez la connaissance complète des réseaux Sans fil et des problèmes de sécurité Sans fil.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco 5508 WLC qui exécute la version de microprogramme 7.0.220.0
- RECOUVREMENT de gamme Cisco 3502
- Cisco Secure ACS qui exécute la version 5.2
- Commutateur de gamme Cisco 3560

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Les recouvrements ont installé les Certificats en usine X.509 - signés par une clé privée - qui sont gravés dans le périphérique au moment de la fabrication. Les recouvrements emploient ce certificat afin d'authentifier avec le WLC au processus de jonction. Cette méthode décrit une autre manière d'authentifier des recouvrements. Avec le logiciel WLC, vous pouvez configurer l'authentification de 802.1x entre un Point d'accès de Cisco Aironet (AP) et Cisco commutent. Dans ce cas, AP agit en tant que suppliant de 802.1x et est authentifié par le commutateur contre un serveur de RAYON (ACS) cet EAP-FAST d'utilisations avec le ravitaillement anonyme PAC. Une fois qu'il est configuré pour l'authentification de 802.1x, le commutateur ne permet à aucun trafic autre que le trafic de 802.1x pour traverser le port jusqu'à ce que le périphérique connecté au port authentifie avec succès. AP peut être authentifié ou avant qu'il joigne un WLC ou après qu'il a joint un WLC, dans ce cas vous configurent le 802.1x sur le commutateur après que le RECOUVREMENT joigne le WLC.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Voici les détails de configuration des composants utilisés dans ce diagramme :

- L'adresse IP du serveur ACS (RAYON) est 192.168.150.24.
- L'adresse d'interface de Gestion et d'AP-gestionnaire du WLC est 192.168.75.44.
- L'adresse 192.168.150.25 de serveurs DHCP.
- Le RECOUVREMENT est placé dans VLAN 253.
- VLAN 253 : 192.168.153.x/24. Passerelle : 192.168.153.10
- VLAN 75 : 192.168.75.x/24. Passerelle : 192.168.75.1

Suppositions

- Des Commutateurs sont configurés pour toute la couche 3 VLAN.
- Le serveur DHCP est assigné une portée de DHCP.
- La Connectivité de la couche 3 existe entre tous les périphériques dans le réseau.
- Le RECOUVREMENT est déjà joint au WLC.
- Chaque VLAN a un masque de /24.
- ACS 5.2 a un certificat signé d'individu installé.

Étapes de configuration

Cette configuration est divisée en trois catégories :

1. Configurez le RECOUVREMENT.
2. Configurez le commutateur.
3. Configurez le serveur de RAYON.

Configurez le RECOUVREMENT

Suppositions :

Le RECOUVREMENT est déjà enregistré au WLC utilisant l'option 43, les DN, ou l'IP statiquement configuré d'interface de gestion WLC.

Procédez comme suit :

1. Allez au **Wireless > Access Points > All APs** afin de vérifier l'enregistrement de RECOUVREMENT sur le WLC.
2. Vous pouvez configurer les qualifications de 802.1x (c'est-à-dire, nom d'utilisateur/mot de passe) pour tous les recouvrements de deux manières :**Globalement**Pour un RECOUVREMENT déjà joint, vous pouvez placer les qualifications globalement ainsi chaque RECOUVREMENT joignant le WLC héritera de ces qualifications.**Individuellement**Configurez les profils de 802.1x par AP. Dans notre exemple, nous configurerons des qualifications par AP.Allez à la **radio > tous les aps**, et sélectionnez AP intéressé.Ajoutez le nom d'utilisateur et mot de passe dans les domaines de **qualifications de suppliant de 802.1x**.**Note**: Des qualifications de procédure de connexion sont utilisées au telnet, au SSH, ou à la console dedans à AP.
3. Configurez la section facilement disponible, et cliquez sur Apply.**Note**: Une fois qu'enregistrées, ces qualifications sont retenues à travers le WLC et les réinitialisations AP. Les qualifications changent seulement quand le RECOUVREMENT joint un nouveau WLC. Le RECOUVREMENT assume le nom d'utilisateur et mot de passe qui ont été configurés sur

le nouveau WLC.Si AP n'a pas joint un WLC encore, vous devez consoler dedans au RECOUVREMENT afin de placer les qualifications. Émettez cette commande CLI dans le mode enable :*<password> de* ***mot de passe de*** *<username> de* ***nom d'utilisateur de dot1x de LAP#lwapp AP*** ou*<password> de* ***mot de passe de*** *<username> de* ***nom d'utilisateur de dot1x de LAP#capwap AP*** **Note**: Cette commande est disponible seulement pour les aps qui exécutent l'image de reprise.Le nom d'utilisateur et mot de passe par défaut pour le RECOUVREMENT est `Cisco` et `Cisco` respectivement.

Configurez le commutateur

Le commutateur agit en tant qu'authentificateur pour le RECOUVREMENT et authentifie le RECOUVREMENT contre un serveur de RAYON. Si le commutateur n'a pas le logiciel conforme, améliorez le commutateur. Dans le commutateur CLI, émettez ces commandes afin d'activer l'authentification de 802.1x sur un port de commutateur :

```
switch#configure terminal
switch(config)#dot1x system-auth-control
switch(config)#aaa new-model
!--- Enables 802.1x on the Switch. switch(config)#aaa authentication dot1x default group radius
switch(config)#radius server host 192.168.150.24 key cisco
!--- Configures the RADIUS server with shared secret and enables switch to send !--- 802.1x
information to the RADIUS server for authentication. switch(config)#ip radius source-interface
vlan 253
!--- We are sourcing RADIUS packets from VLAN 253 with NAS IP: 192.168.153.10.
switch(config)interface gigabitEthernet 0/11 switch(config-if)switchport mode access
switch(config-if)switchport access vlan 253 switch(config-if)mls qos trust dscp switch(config-
if)spanning-tree portfast !--- gig0/11 is the port number on which the AP is connected.
switch(config-if)dot1x pae authenticator !--- Configures dot1x authentication. switch(config-
if)dot1x port-control auto !--- With this command, the switch initiates the 802.1x
authentication.
```

Note: Si vous avez d'autres aps sur le même commutateur et vous ne voulez pas qu'ils utilisent le 802.1x, vous pouvez quitter le port ONU-configuré pour le 802.1x ou émettre cette commande :

```
switch(config-if)authentication port-control force-authorized
```

Configurez le serveur de RAYON

Le RECOUVREMENT est authentifié avec l'EAP-FAST. Assurez-vous que le serveur de RAYON vous utilisent des supports cette méthode d'EAP si vous n'utilisez pas Cisco ACS 5.2.

La configuration du serveur RADIUS est divisée en quatre étapes :

1. Ressources en configure network.
2. Configurez les utilisateurs.
3. Définissez les éléments de stratégie.
4. Appliquez les stratégies d'accès.

ACS 5.x est un ACS basé sur la politique. En d'autres termes, ACS 5.x utilise un modèle basé sur les règles de stratégie au lieu du modèle basé sur groupe utilisé dans les versions 4.x.

Le modèle basé sur les règles de stratégie ACS 5.x fournit un contrôle d'accès plus puissant et plus flexible comparé à l'approche basée sur groupe plus ancienne.

Dans le modèle basé sur groupe plus ancien, un groupe définit la stratégie parce qu'elle contient et attache ensemble trois types d'informations :

- **Les informations d'identité** - Ces informations peuvent être basées sur l'adhésion dans des groupes d'AD ou de LDAP ou une affectation statique pour les utilisateurs internes ACS.
- **D'autres restrictions ou conditions** - Restrictions temporelles, restrictions de périphérique, et ainsi de suite.
- **Autorisations** - Niveaux de privilège VLAN ou de Cisco IOS®.

Le modèle de stratégie ACS 5.x est basé sur des règles de la forme :

Si la condition résultent alors

Par exemple, nous utilisons les informations décrites pour le modèle basé sur groupe :

S'identité-état, autorisation-profil de restriction-état puis.

En conséquence, ceci nous donne la flexibilité de limiter les conditions dans lesquelles l'utilisateur est permis pour accéder au réseau et aussi quel niveau d'autorisation est permis quand des conditions spécifiques sont remplies.

Ressources en configure network

Dans cette section, nous configurons le client d'AAA pour le commutateur sur le serveur de RAYON.

Cette procédure explique comment ajouter le commutateur en tant que client d'AAA sur le serveur de RAYON de sorte que le commutateur puisse passer les identifiants utilisateurs du RECOUVREMENT au serveur de RAYON.

Procédez comme suit :

1. Du GUI ACS, **ressources de réseau en** clic.
2. **Groupes de périphériques réseau de** clic.
3. Allez à l'**emplacement > créent** (au bas).
4. Ajoutez les champs requis et cliquez sur Submit.
5. La fenêtre régénère :
6. **Le type de périphérique de** clic **> créent**.
7. Cliquez sur **Submit**. Une fois que terminée, la fenêtre régénère :
8. Allez aux **ressources de réseau >** aux **périphériques de réseau et aux clients d'AAA**.
9. Le clic **créent**, et complètent les détails comme représenté ici :
10. Cliquez sur **Submit**. La fenêtre régénère :

Configurer des utilisateurs

Dans cette section, vous verrez comment créer un utilisateur sur l'ACS configuré précédemment. Vous affecterez l'utilisateur à un groupe appelé les « utilisateurs de RECOUVREMENT ».

Procédez comme suit :

1. Allez aux **utilisateurs et l'identité enregistre** > des **groupes d'identité** > **créent**.
2. Cliquez sur **Submit**.
3. Créez **3502e** et assignez-le pour grouper des « utilisateurs de RECOUVREMENT ».
4. Allez aux **utilisateurs et l'identité enregistre** > **identité groupe** > des **utilisateurs** > **créent**.
5. Vous verrez les informations mises à jour :

Définissez les éléments de stratégie

Vérifiez que l'**autorisation Access** est placée.

Appliquez les stratégies d'Access

Dans cette section, vous sélectionnerez l'EAP-FAST car la méthode d'authentification utilisée pour des recouvrements afin d'authentifier. Vous créerez alors des règles basées sur les étapes précédentes.

Procédez comme suit :

1. Allez à **Access les stratégies** > les **services d'accès** > l'**accès au réseau de par défaut** > **éditent : « Accès au réseau par défaut »**.
2. Veillez-vous pour avoir activé l'**EAP-FAST** et le **ravitaillement anonyme PAC d'intrabande**.
3. Cliquez sur **Submit**.
4. Vérifiez le groupe d'identité que vous avez sélectionné. Dans cet exemple, les **utilisateurs internes d'**utilisation (qui a été créé sur l'ACS) et sauvegardent les modifications.
5. Allez à **Access les stratégies** > les **services d'accès** > l'**accès au réseau** > l'**autorisation de par défaut** afin de vérifier le profil d'autorisation.Vous pouvez personnaliser dans quelles conditions vous permettrez à un accès client au réseau et quelles profil d'autorisation (attributs) vous passerez une fois authentifié. Cette finesse est seulement disponible dans ACS 5.x. Dans cet exemple, l'**emplacement**, le **type de périphérique**, le **Protocol**, le **groupe d'identité**, et la **méthode d'authentification EAP** sont sélectionnés.
6. Cliquez sur OK, et **sauvegardez les modifications**.
7. L'étape suivante est de créer une règle. Si aucune règle n'est définie, on ne permet le RECOUVREMENT l'accès sans aucune condition.
8. Le clic **créent** > **Rule-1**. Cette règle est pour des utilisateurs dans le groupe « utilisateurs de RECOUVREMENT ».
9. **Modifications de sauvegarde de** clic. Si vous voulez des utilisateurs n'appariant pas les conditions à refuser, éditez la règle par défaut de dire que « refusez Access ».
10. La dernière étape est de définir des règles de sélection de service. Employez cette page pour configurer une stratégie simple ou basée sur les règles afin de déterminer quel service à s'appliquer aux demandes en entrée. Exemple :

Vérifiez

Une fois que le 802.1x est activé sur le port de commutateur, tout le trafic excepté le trafic de 802.1x est bloqué par le port. Le RECOUVREMENT, qui est déjà enregistré au WLC, obtient dissocié. Seulement après qu'une authentification réussie de 802.1x est l'autre trafic permis pour

traverser. L'enregistrement réussi du RECOUVREMENT au WLC après que le 802.1x soit activé sur le commutateur indique que l'authentification de RECOUVREMENT est réussie.

Console AP :

```
*Jan 29 09:10:24.048: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5246
*Jan 29 09:10:27.049: %DTLS-5-SEND_ALERT: Send FATAL : Close notify Alert to
   192.168.75.44:5247
!--- AP disconnects upon adding dot1x information in the gig0/11. *Jan 29 09:10:30.104: %WIDS-5-
DISABLED: IDS Signature is removed and disabled. *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP
changed state to DISCOVERY *Jan 29 09:10:30.107: %CAPWAP-5-CHANGED: CAPWAP changed state to
DISCOVERY *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
administratively down *Jan 29 09:10:30.176: %LINK-5-CHANGED: Interface Dot11Radio1, changed
state to administratively down *Jan 29 09:10:30.186: %LINK-5-CHANGED: Interface Dot11Radio0,
changed state to reset *Jan 29 09:10:30.201: %LINK-3-UPDOWN: Interface Dot11Radio1, changed
state to up *Jan 29 09:10:30.211: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:10:30.220: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to reset Translating
"CISCO-CAPWAP-CONTROLLER"...domain server (192.168.150.25) *Jan 29 09:10:36.203: status of
voice_diag_test from WLC is false
*Jan 29 09:11:05.927: %DOT1X_SHIM-6-AUTH_OK: Interface GigabitEthernet0 authenticated [EAP-FAST]
*Jan 29 09:11:08.947: %DHCP-6-ADDRESS_ASSIGN: Interface GigabitEthernet0 assigned DHCP address
192.168.153.106, mask 255.255.255.0, hostname 3502e
!--- Authentication is successful and the AP gets an IP. Translating "CISCO-CAPWAP-
CONTROLLER.Wlab"...domain server (192.168.150.25) *Jan 29 09:11:37.000: %CAPWAP-5-DTLSREQSEND:
DTLS connection request sent peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.000:
%CAPWAP-5-CHANGED: CAPWAP changed state to *Jan 29 09:11:37.575: %CAPWAP-5-DTLSREQSUCC: DTLS
connection created successfully peer_ip: 192.168.75.44 peer_port: 5246 *Jan 29 09:11:37.578:
%CAPWAP-5-SENDJOIN: sending Join Request to 192.168.75.44 *Jan 29 09:11:37.578: %CAPWAP-5-
CHANGED: CAPWAP changed state to JOIN

*Jan 29 09:11:37.748: %CAPWAP-5-CHANGED: CAPWAP chan
wmmAC status is FALSEged state to CFG
*Jan 29 09:11:38.890: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:38.900: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:38.900: %CAPWAP-5-CHANGED: CAPWAP changed state to UP
*Jan 29 09:11:38.956: %CAPWAP-5-JOINEDCONTROLLER: AP has joined controller
   5508-3
*Jan 29 09:11:39.013: %CAPWAP-5-DATA_DTLS_START: Starting Data DTLS handshake.
   Wireless client traffic will be blocked until DTLS tunnel is established.
*Jan 29 09:11:39.013: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.016: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[0]
*Jan 29 09:11:39.028: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to
   down
*Jan 29 09:11:39.038: %LINK-5-CHANGED: Interface Dot11Radio1, changed state to
   reset
*Jan 29 09:11:39.054: %LINK-3-UPDOWN: Interface Dot11Radio1, changed state to up
*Jan 29 09:11:39.060: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to
   down
*Jan 29 09:11:39.069: %LINK-5-CHANGED: Interface Dot11Radio0, changed state to
   reset
*Jan 29 09:11:39.085: %LINK-3-UPDOWN: Interface Dot11Radio0, changed state to up
*Jan 29 09:11:39.135: %LWAPP-3-CLIENTEVENTLOG: SSID goa added to the slot[1]DTLS
   keys are plumbed successfully.
*Jan 29 09:11:39.151: %CAPWAP-5-DATA_DTLS_ESTABLISHED: Data DTLS tunnel
   established.
*Jan 29 09:11:39.161: %WIDS-5-ENABLED: IDS Signature is loaded and enabled
!--- AP joins the 5508-3 WLC.
```

Logs ACS :

1. Visualisez les nombres de hits :Si vous vérifiez des logs dans un délai de 15 minutes d'authentification, veillez-vous pour régénérer le nombre de hits. À la même page, au bas vous avez un onglet de **nombre de hits**.
2. **La surveillance de** clic **et les états** et une nouvelle fenêtre externe apparaît. **Authentifications de** clic **– RAYON – Aujourd'hui**. Vous pouvez également cliquer sur les **détails** afin de vérifier qui entretiennent la règle de sélection étaient appliqués.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Système de contrôle d'accès sécurisé Cisco
- Support et documentation techniques - Cisco Systems