ASA 8.0 : Configurer l'authentification RADIUS pour les utilisateurs WebVPN

Contenu

Introduction

Ce document explique comment configurer l'appliance de sécurité adaptable Cisco (ASA) pour utiliser un serveur de Service RADIUS (Remote Authentication Dial-In User Service) pour l'authentification des utilisateurs WebVPN. Le serveur de RAYON dans cet exemple est un serveur du serveur de contrôle d'accès de Cisco (ACS), version 4.1 que cette configuration est exécutée avec Adaptive Security Device Manager (ASDM) 6.0(2) sur une ASA qui exécute la version de logiciel 8.0(2).

Remarque: Dans ce RAYON d'exemple l'authentification est configurée pour des utilisateurs WebVPN, mais cette configuration peut être aussi bien utilisée pour d'autres types d'Accès à distance VPN. Affectez simplement le Groupe de serveurs AAA au profil désiré de connexion (groupe de tunnel) comme affiché.

Conditions préalables

- Une configuration de base de webvpn est exigée.
- Cisco ACS doit avoir des utilisateurs configurés pour l'authentification de l'utilisateur. Référez-vous à ajouter une section de base de compte utilisateur de pour en savoir plus de gestion des utilisateurs.

Configurez le serveur ACS

Dans cette section, vous êtes présenté avec les informations pour configurer l'authentification de RAYON sur l'ACS et l'ASA.

Terminez-vous ces étapes afin de configurer le serveur ACS pour communiquer avec l'ASA.

1. Choisissez la **configuration réseau du** menu de gauche de l'écran ACS.
2. Choisissez **ajoutent l'entrée** sous des **clients d'AAA**.
3. Fournissez les informations de client :**Adresse Internet de client d'AAA** — un nom de votre choix**Adresse IP de client d'AAA** — l'adresse dont les dispositifs de sécurité entrent en contact avec l'ACS**Secret partagé** — un secret clé configuré sur l'ACS et sur les dispositifs de sécurité
4. Dans l'**authentifier utilisant** déroulant choisissez le **RAYON (Cisco VPN 3000/ASA/PIX 7.x+)**.
5. Clic **Submit+Apply**.

Configuration de client d'AAA d'exemple

Configurez les dispositifs de sécurité

ASDM

Terminez-vous ces étapes dans l'ASDM afin de configurer l'ASA pour communiquer avec le serveur ACS et pour authentifier des clients de webvpn.

1. Choisissez la **configuration > l'Accès à distance VPN > AAA installé > des Groupes de serveurs AAA**.
2. Cliquez sur Add à côté des Groupes de serveurs AAA.
3. Dans la fenêtre qui apparaît, spécifiez un nom pour le nouveau Groupe de serveurs AAA et choisissez le **RAYON** comme protocole. Cliquez sur OK une fois terminé.
4. Soyez sûr que votre nouveau groupe est sélectionné dans le volet supérieur et cliquez sur Add à la droite du volet inférieur.
5. Fournissez les informations du serveur :**Nom d'interface** — l'interface que l'ASA doit employer pour atteindre le serveur ACS**Nom du serveur ou adresse IP** — l'adresse que l'ASA doit employer pour atteindre le serveur ACS**Clé secrète de serveur** — le clé configuré secret partagé pour l'ASA sur le serveur ACS**Configuration du serveur d'AAA d'exemple sur l'ASA**
6. Une fois que vous avez configuré le Groupe de serveurs AAA et le serveur, naviguez vers la configuration > l'Accès à distance VPN > VPN SSL sans client Access > profils de connexion afin de configurer le webvpn pour utiliser la nouvelle configuration d'AAA.**Remarque:** Quoique cet exemple utilise le webvpn, vous pouvez placer n'importe quel profil de connexion d'Accès à distance (groupe de tunnel) pour utiliser cette installation d'AAA.
7. Choisissez le profil pour lequel vous voulez configurer l'AAA, et cliquez sur Edit.
8. Sous l'**authentification** choisissez le groupe de serveurs de RAYON que vous avez créé plus tôt. Cliquez sur OK une fois terminé.

Interface de ligne de commande

Terminez-vous ces étapes dans l'interface de ligne de commande (CLI) afin de configurer l'ASA pour communiquer avec le serveur ACS et pour authentifier des clients de webvpn.

```
ciscoasa#configure terminal !--- Configure the AAA Server group. ciscoasa(config)# aaa-server
RAD_SRV_GRP protocol RADIUS ciscoasa(config-aaa-server-group)# exit !--- Configure the AAA
```

```
Server. ciscoasa(config)# aaa-server RAD_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-
server-host)# key secretkey ciscoasa(config-aaa-server-host)# exit !--- Configure the tunnel
group to use the new AAA setup. ciscoasa(config)# tunnel-group ExampleGroup1 general-attributes
ciscoasa(config-tunnel-general)# authentication-server-group RAD_SRV_GRP
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Test avec l'ASDM

Vérifiez votre configuration RADIUS avec la touche "TEST" sur l'écran de configuration de Groupes de serveurs AAA. Une fois que vous fournissez un nom d'utilisateur et mot de passe, ce bouton te permet pour envoyer une demande de test d'authentification au serveur ACS.

1. Choisissez la **configuration > l'Accès à distance VPN > AAA installé > des Groupes de serveurs AAA**.
2. Sélectionnez votre Groupe de serveurs AAA désiré dans le volet supérieur.
3. Sélectionnez le serveur d'AAA que vous voulez examiner dans le volet inférieur.
4. Cliquez sur la touche "TEST" à la droite du volet inférieur.
5. Dans la fenêtre qui apparaît, cliquez sur la case d'option d'**authentification**, et fournissez les qualifications avec lesquelles vous voulez tester. Cliquez sur OK une fois terminé.
6. Après que l'ASA contacte le serveur d'AAA, un message de succès ou échec apparaît.

Test avec le CLI

Vous pouvez employer la commande de **test** sur la ligne de commande afin de tester votre installation d'AAA. Une demande de test est envoyée au serveur d'AAA, et le résultat apparaît sur la ligne de commande.

```
ciscoasa#test aaa-server authentication RAD_SVR_GRP host 192.168.1.2 username kate password
cisco123 INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds)
INFO: Authentication Successful
```

Dépannez

La commande de **debug radius** peut vous aider à dépanner des problèmes d'authentification dans ce scénario. Ces élimination des imperfections de session de RAYON de commandes enables aussi bien que décoder de paquet RADIUS. Dans chaque sortie de débogage présentée, le premier paquet décodé est le paquet envoyé de l'ASA au serveur ACS. Le deuxième paquet est la réponse du serveur ACS.

Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Quand l'authentification est réussie, le serveur de RAYON envoie un message d'Access-**recevoir**.

```
ciscoasa#debug radius !--- First Packet. Authentication Request. ciscoassa#radius mkreq: 0x88
alloc_rip 0xd5627ae4 new request 0x88 --> 52 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x88 id 52 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) -------------------------------------- Raw packet data (length =
62)..... 01 34 00 3e 18 71 56 d7 c4 ad e2 73 30 a9 2e cf | .4.>.qV....s0... 5c 65 3a eb 01 06 6b
61 74 65 02 12 0e c1 28 b7 | \e:...kate....(. 87 26 ed be 7b 2c 7a 06 7c a3 73 19 04 06 c0 a8 |
```

```
.&..{,z.|.s..... 01 01 05 06 00 00 00 34 3d 06 00 00 00 05 | .......4=..... Parsed packet
data..... Radius: Code = 1 (0x01) Radius: Identifier = 52 (0x34) Radius: Length = 62 (0x003E)
Radius: Vector: 187156D7C4ADE27330A92ECF5C653AEB Radius: Type = 1 (0x01) User-Name Radius:
Length = 6 (0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 0e c1 28 b7 87 26 ed be 7b 2c 7a 06
7c a3 73 19 | ..(..&..{,z.|.s. Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x34 Radius: Type = 61 (0x3D) NAS-Port-Type Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id
52 rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer
0x0 : reqauth: 18 71 56 d7 c4 ad e2 73 30 a9 2e cf 5c 65 3a eb : info 0x88 session_id 0x88
request_id 0x34 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type
1 !--- Second Packet. Authentication Response. RADIUS packet decode (response) ----------------
---------------------- Raw packet data (length = 50)..... 02 34 00 32 35 a1 88 2f 8a bf 2a 14 c5
31 78 59 | .4.25../..*..1xY 60 31 35 89 08 06 ff ff ff ff 19 18 43 41 43 53 | `15.........CACS
3a 30 2f 32 61 36 2f 63 30 61 38 30 31 30 31 2f | :0/2a6/c0a80101/ 35 32 | 52 Parsed packet
data..... Radius: Code = 2 (0x02) Radius: Identifier = 52 (0x34) Radius: Length = 50 (0x0032)
Radius: Vector: 35A1882F8ABF2A14C531785960313589 Radius: Type = 8 (0x08) Framed-IP-Address
Radius: Length = 6 (0x06) Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF) Radius: Type
= 25 (0x19) Class Radius: Length = 24 (0x18) Radius: Value (String) = 43 41 43 53 3a 30 2f 32 61
36 2f 63 30 61 38 30 | CACS:0/2a6/c0a80 31 30 31 2f 35 32 | 101/52 rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination RADIUS_DELETE remove_req 0xd5627ae4 session 0x88 id 52
free_rip 0xd5627ae4 radius: send queue empty
```

Quand l'authentification échoue, le serveur ACS envoie un message d'Access-anomalie.

```
ciscoasa#debug radius !--- First Packet. Authentication Request. ciscoasa# radius mkreq: 0x85
alloc_rip 0xd5627ae4 new request 0x85 --> 49 (0xd5627ae4) got user '' got password add_req
0xd5627ae4 session 0x85 id 49 RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode
(authentication request) ------------------------------------ Raw packet data (length =
62)..... 01 31 00 3e 88 21 46 07 34 5d d2 a3 a0 59 1e ff | .1.>.!F.4]...Y.. cc 15 2a 1b 01 06 6b
61 74 65 02 12 60 eb 05 32 | ..*...kate..`..2 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 04 06 c0 a8 |
.ix.....K..7.... 01 01 05 06 00 00 00 31 3d 06 00 00 00 05 | .......1=..... Parsed packet
data..... Radius: Code = 1 (0x01) Radius: Identifier = 49 (0x31) Radius: Length = 62 (0x003E)
Radius: Vector: 88214607345DD2A3A0591EFFCC152A1B Radius: Type = 1 (0x01) User-Name Radius:
Length = 6 (0x06) Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-
Password Radius: Length = 18 (0x12) Radius: Value (String) = 60 eb 05 32 87 69 78 a3 ce d3 80 d8
4b 0d c3 37 | `..2.ix.....K..7 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x31 Radius: Type = 61 (0x3D) NAS-Port-Type Radius:
Length = 6 (0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id
49 rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer
0x0 : reqauth: 88 21 46 07 34 5d d2 a3 a0 59 1e ff cc 15 2a 1b : info 0x85 session_id 0x85
request_id 0x31 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type
1 !--- Second packet. Authentication Response. RADIUS packet decode (response) ----------------
---------------------- Raw packet data (length = 32)..... 03 31 00 20 70 98 50 af 39 cc b9 ba df
a7 bd ff | .1. p.P.9....... 06 af fb 02 12 0c 52 65 6a 65 63 74 65 64 0a 0d | ......Rejected..
Parsed packet data..... Radius: Code = 3 (0x03) Radius: Identifier = 49 (0x31) Radius: Length =
32 (0x0020) Radius: Vector: 709850AF39CCB9BADFA7BDFF06AFFB02 Radius: Type = 18 (0x12) Reply-
Message Radius: Length = 12 (0x0C) Radius: Value (String) = 52 65 6a 65 63 74 65 64 0a 0d |
Rejected.. rad_procpkt: REJECT RADIUS_DELETE remove_req 0xd5627ae4 session 0x85 id 49 free_rip
0xd5627ae4 radius: send queue empty
```

Informations connexes

- Service RADIUS (Remote Authentication Dial-In User Service)
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems