Authentification de l'utilisateur ASA VPN contre le serveur de Windows 2008 NPS (Répertoire actif) avec l'exemple de configuration RADIUS

Contenu

Introduction

Ce document explique comment configurer une appliance de sécurité adaptable (ASA) pour communiquer avec un serveur de politique réseau de Microsoft Windows 2008 (NPS) avec le protocole RADIUS de sorte que le Client VPN Cisco/AnyConnect existant/utilisateurs WebVPN sans client soient authentifiés contre le Répertoire actif. NPS est l'un des rôles de serveur offerts par le serveur de Windows 2008. Il est équivalent au serveur Windows 2003, IAS (Service d'authentification Internet), qui est l'implémentation d'un serveur de RAYON pour fournir l'authentification d'utilisateur en accès entrant distante. De même, dans le serveur de Windows 2008, NPS est l'implémentation d'un serveur de RAYON. Fondamentalement, l'ASA est un client RADIUS à un serveur de RAYON NPS. L'ASA envoie des demandes d'authentification de RAYON au nom des utilisateurs VPN et NPS les authentifie contre le Répertoire actif.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- ASA qui exécute la version 9.1(4)
- Serveur R2 de Windows 2008 avec des services de Répertoire actif et le rôle NPS installés

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.

Configurez

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Configurations

Configuration ASDM

1. Choisissez le groupe de tunnels pour lequel l'authentification NPS est exigée.
2. Cliquez sur Edit et choisissez **de base**.
3. Dans la section d'authentification, le clic **gèrent**.
4. Dans la section de Groupes de serveurs AAA, cliquez sur Add.
5. Dans le domaine de Groupe de serveurs AAA, écrivez le nom du groupe de serveurs (par exemple, NPS).
6. De la liste déroulante de Protocol, choisissez le **RAYON**.
7. Cliquez sur **OK**.
8. Dans les serveurs dans la section de groupe sélectionné, choisissez le Groupe de serveurs AAA ajouté et cliquez sur Add.
9. Dans le nom du serveur ou le champ IP Address, entrez dans l'adresse IP du serveur.
10. Dans la zone de tri secrète de serveur, introduisez la clé secrète.
11. Quittez le port d'authentification de serveur et les champs de port de traçabilité de serveur à la valeur par défaut à moins que le serveur écoute sur un port différent.
12. Cliquez sur **OK**.
13. Cliquez sur **OK**.
14. De la liste déroulante de Groupe de serveurs AAA, choisissez le groupe (NPS dans cet exemple) ajouté dans les étapes précédentes.
15. Cliquez sur **OK**.

Configuration CLI

```
aaa-server NPS protocol radius
aaa-server NPS (inside) host 10.105.130.51
 key *****

tunnel-group TEST type remote-access
tunnel-group TEST general-attributes
 address-pool test
 authentication-server-group (inside) NPS
tunnel-group TEST webvpn-attributes
 group-alias TEST enable

ip local pool test 192.168.1.1-192.168.1.10 mask 255.255.255.0
```

Par défaut, l'ASA utilise le type d'authentification de Protocol d'authentification de mot de passe non chiffré (PAP). Ceci ne signifie pas que l'ASA envoie le mot de passe en texte brut quand elle envoie le paquet de DEMANDE RADIUS. En revanche, le mot de passe de plaintext est chiffré avec le secret partagé par RAYON.

Si la gestion des mots de passe est activée sous le groupe de tunnels, alors l'ASA emploie le type de l'authentification MSCHAP-v2 afin de chiffrer le mot de passe de plaintext. En pareil cas, assurez-vous que la case **capable de Microsoft CHAPv2** est signée la fenêtre de serveur d'AAA d'éditer configurée dans la section de configuration ASDM.

```
tunnel-group TEST general-attributes
address-pool test
authentication-server-group (inside) NPS
password-management
```

> Remarque: **L'authentication command d'AAA-serveur de test** utilise toujours le PAP. Seulement quand un utilisateur initie une connexion au groupe de tunnels avec la gestion des mots de passe activée fait l'utilisation MSCHAP-v2 ASA. En outre, de « l'option gestion des mots de passe [jours de mot de passe-expirer-dans-jours] » est seulement prise en charge avec le Protocole LDAP (Lightweight Directory Access Protocol). Le RAYON ne fournit pas cette caractéristique. Vous verrez le mot de passe expirer option quand le mot de passe est déjà expiré dans le Répertoire actif.

Serveur de Windows 2008 avec la configuration NPS

Le rôle de serveur NPS devrait être installé et s'exécutant sur le serveur de Windows 2008. Sinon, choisissez le **début > les outils d'administration > les rôles de serveur > ajoutent des services de rôle**. Choisissez le serveur de politique réseau et installez le logiciel. Une fois que le rôle de serveur NPS est installé, terminez-vous ces étapes afin de configurer le NPS pour recevoir et traiter des demandes d'authentification de RAYON de l'ASA :

1. Ajoutez l'ASA en tant que client RADIUS dans le serveur NPS. Choisissez les **outils d'administration > le serveur de politique réseau.**Cliquez avec le bouton droit les **clients RADIUS** et choisissez **nouveau**.Écrivez un nom amical, une adresse (IP ou DN), et un secret partagé configuré sur l'ASA.Cliquez sur l'onglet **Advanced**.De la liste déroulante de nom de constructeur, choisissez le **RADIUS Standard**.Cliquez sur **OK**.
2. Créez une nouvelle stratégie de demande de connexion pour des utilisateurs VPN. Le but de la stratégie de demande de connexion est de spécifier si les demandes des clients RADIUS doivent être traité localement ou expédié aux serveurs RADIUS distants. Sous NPS >

stratégies, cliquent avec le bouton droit des **stratégies de demande de connexion** et créent une nouvelle stratégie.Du type de liste déroulante de serveur d'accès à distance, choisissez **non spécifié**.Cliquez sur l'onglet de **conditions**.Cliquez sur **Add**.Écrivez l'adresse IP de l'ASA comme état « d'ipv4 addres de client ».Cliquez sur l'**onglet Settings**.Sous la demande de connexion d'expédition, choisissez l'**authentification**. Assurez que les demandes d'authentifier sur cette case d'option de serveur est choisies.Cliquez sur **OK**.

3. Ajoutez une politique réseau où vous pouvez spécifier quels utilisateurs sont permis pour authentifier.Par exemple, vous pouvez ajouter des groupes d'utilisateurs de Répertoire actif comme condition. Seulement ces utilisateurs qui appartiennent à un groupe spécifié de Windows sont authentifiés dans le cadre de cette stratégie.Sous NPS, choisissez les **stratégies**.Cliquez avec le bouton droit la **politique réseau** et créez une nouvelle stratégie.Assurez que la case d'option d'accès de Grant est choisie.Du type de liste déroulante de serveur d'accès à distance, choisissez **non spécifié**.Cliquez sur l'onglet de **conditions**.Cliquez sur **Add**.Écrivez l'adresse IP de l'ASA comme état d'ipv4 addres de client.Écrivez le groupe d'utilisateurs de Répertoire actif qui contient des utilisateurs VPN.Cliquez sur l'onglet de **contraintes**.Choisissez les **méthodes d'authentification**.Assurez que la case décryptée de l'authentification (PAP, SPAP) est cochée.Cliquez sur **OK**.

Passez l'attribut de stratégie de groupe (attribut 25) du serveur de RAYON NPS

Si la stratégie de groupe doit être assignée à l'utilisateur dynamiquement avec le serveur de RAYON NPS, l'attribut RADIUS de stratégie de groupe (attribut 25) peut être utilisé.

Terminez-vous ces étapes afin d'envoyer l'attribut RADIUS 25 pour l'affectation dynamique d'une stratégie de groupe à l'utilisateur.

1. Après que la politique réseau soit ajoutée, cliquez avec le bouton droit la politique réseau requise et cliquez sur l'**onglet Settings**.
2. Choisissez les **attributs RADIUS > la norme**. Cliquez sur **Add**. Laissez Access pour taper en tant que tous.
3. Dans les attributs enfermez dans une boîte, choisissez la **classe** et cliquez sur Add. Écrivez la valeur d'attribut, c.-à-d., le nom de la stratégie de groupe comme chaîne. Souvenez-vous qu'une stratégie de groupe avec ce nom doit être configurée dans l'ASA. C'est de sorte que l'ASA l'assigne à la session VPN après qu'elle reçoive cet attribut dans la réponse de RAYON.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

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

Debugs ASA

Debug radius tout d'enable sur l'ASA.

```
ciscoasa# test aaa-server authentication NPS host 10.105.130.51 username vpnuser password
INFO: Attempting Authentication test to IP address <10.105.130.51> (timeout: 12 seconds)
radius mkreq: 0x80000001
alloc_rip 0x787a6424
   new request 0x80000001 --> 8 (0x787a6424)
got user 'vpnuser'
got password
add_req 0x787a6424 session 0x80000001 id 8
RADIUS_REQUEST
radius.c: rad_mkpkt

RADIUS packet decode (authentication request)

--------------------------------------
Raw packet data (length = 65).....
01 08 00 41 c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f    |  ...A.....~m...
40 50 a8 36 01 09 76 70 6e 75 73 65 72 02 12 28    |  @P.6..vpnuser..(
c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43 04    |  .h.........Z.oC.
06 0a 69 82 de 05 06 00 00 00 00 3d 06 00 00 00    |  ..i........=....
05                                                 |  .

Parsed packet data.....
Radius: Code = 1 (0x01)
Radius: Identifier = 8 (0x08)
Radius: Length = 65 (0x0041)
Radius: Vector: C41BAB1AE37E6D12DA876F7F4050A836
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
76 70 6e 75 73 65 72                               |  vpnuser
Radius: Type = 2 (0x02) User-Password
Radius: Length = 18 (0x12)
Radius: Value (String) =
28 c3 68 fb 88 ad 1d f2 c3 b9 9a a9 5a fa 6f 43    |  (.h.........Z.oC
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.105.130.52 (0x0A6982DE)
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 61 (0x3D) NAS-Port-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x5
send pkt 10.105.130.51/1645
rip 0x787a6424 state 7 id 8
rad_vrfy() : response message verified
rip 0x787a6424
 : chall_state ''
 : state 0x7
 : reqauth:
    c4 1b ab 1a e3 7e 6d 12 da 87 6f 7f 40 50 a8 36
 : info 0x787a655c
    session_id 0x80000001
    request_id 0x8
    user 'vpnuser'
    response '***'
    app 0
    reason 0
    skey 'cisco'
    sip 10.105.130.51
    type 1

RADIUS packet decode (response)
```

```
-------------------------------------
Raw packet data (length = 78).....
02 08 00 4e e8 88 4b 76 20 b6 aa d3 0d 2b 94 37    |  ...N..Kv ....+.7
bf 9a 6c 4c 07 06 00 00 00 01 06 06 00 00 00 02    |  ..lL............
19 2e 9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a    |  .........7.....j
2c bf 00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf    |  ,.....<..n...@..
1e 3a 18 6f 05 81 00 00 00 00 00 00 00 03          |  .:.o..........

Parsed packet data.....
Radius: Code = 2 (0x02)
Radius: Identifier = 8 (0x08)
Radius: Length = 78 (0x004E)
Radius: Vector: E8884B7620B6AAD30D2B9437BF9A6C4C
Radius: Type = 7 (0x07) Framed-Protocol
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 6 (0x06) Service-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 25 (0x19) Class
Radius: Length = 46 (0x2E)
Radius: Value (String) =
9a 08 07 ad 00 00 01 37 00 01 02 00 0a 6a 2c bf    |  .......7.....j,.
00 00 00 00 3c 84 0f 6e f5 95 d3 40 01 cf 1e 3a    |  ....<..n...@...:
18 6f 05 81 00 00 00 00 00 00 00 03                |  .o..........
rad_procpkt: ACCEPT
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0x787a6424 session 0x80000001 id 8
free_rip 0x787a6424
radius: send queue empty
INFO: Authentication Successful
```

Dépannez

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

- Assurez que la Connectivité entre l'ASA et le serveur NPS est bonne.Appliquez les captures de paquet pour s'assurer que la demande d'authentification part de l'interface ASA (d'où le serveur est accessible). Confirmez que les périphériques dans le chemin ne bloquent pas le port UDP 1645 (port par défaut d'authentification de RAYON) afin de l'assurer atteint le serveur NPS. Plus d'informations sur des captures de paquet sur l'ASA peuvent être trouvées dans ASA/PIX/FWSM : Paquet capturant exemple utilisant CLI et ASDM configuration.
- Si l'authentification échoue toujours, regardez en cas le visualiseur sur les fenêtres NPS. Sous le visualisateur d'événements > les logs de Windows, choisissez la **Sécurité.** Recherchez les événements associés avec NPS autour de la période de la demande d'authentification.Une fois que vous ouvrez la manifestation Properties, vous devriez pouvoir voir la raison pour la panne suivant les indications de l'exemple. Dans cet exemple, le PAP n'a pas été choisi comme type d'authentification dans le cadre de la politique réseau. Par conséquent, la demande d'authentification échoue.
```
Log Name:      Security
Source:        Microsoft-Windows-Security-Auditing
Date:          2/10/2014 1:35:47 PM
Event ID:      6273
Task Category: Network Policy Server
Level:         Information
Keywords:      Audit Failure
User:          N/A
```

Computer: win2k8.skp.com
Description:
Network Policy Server denied access to a user.

Contact the Network Policy Server administrator for more information.

User:
   Security ID: SKP\vpnuser
   Account Name: vpnuser
   Account Domain: SKP
   Fully Qualified Account Name: skp.com/Users/vpnuser

Client Machine:
   Security ID: NULL SID
   Account Name: -
   Fully Qualified Account Name: -
   OS-Version: -
   Called Station Identifier: -
   Calling Station Identifier: -

NAS:
   NAS IPv4 Address: 10.105.130.69
   NAS IPv6 Address: -
   NAS Identifier: -
   NAS Port-Type: Virtual
   NAS Port: 0

RADIUS Client:
   Client Friendly Name: vpn
   Client IP Address: 10.105.130.69

Authentication Details:
   Connection Request Policy Name: vpn
   Network Policy Name: vpn
   Authentication Provider: Windows
   Authentication Server: win2k8.skp.com
   Authentication Type: PAP
   EAP Type: -
   Account Session Identifier: -
   Logging Results: Accounting information was written to the local log file.
   Reason Code: 66
   Reason: **The user attempted to use an authentication method that is not enabled on the matching network policy.**