Exemple de configuration de client de FlexVPN et d'Anyconnect IKEv2

Contenu

Introduction

Ce document décrit comment configurer le Client à mobilité sécurisé Cisco AnyConnect pour employer le Service RADIUS (Remote Authentication Dial-In User Service) et les attributs locaux d'autorisation afin d'authentifier contre la Microsoft Active Directory.

> Remarque: Actuellement, l'utilisation de la base de données locale des utilisateurs pour l'authentification ne fonctionne pas sur des périphériques de Cisco IOS®. C'est parce que le Cisco IOS ne fonctionne pas comme authentificateur d'EAP. La demande d'amélioration CSCui07025 a été classée d'ajouter le support.

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 :

- Version 15.2(T) ou ultérieures de Cisco IOS
- Version 3.0 ou ultérieures de Client à mobilité sécurisé Cisco AnyConnect
- Microsoft Active Directory

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.

Configurez

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

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

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- Configuration du concentrateur
- Configuration du serveur de Microsoft Active Directory
- Configuration du client

Configuration du concentrateur

1. Configurez le RAYON pour l'authentification seulement et définissez l'autorisation locale.

```
aaa new-model
aaa group server radius FlexVPN-AuthC-Server-Group-1
server-private 10.7.7.129 key Cisco123
aaa authentication login FlexVPN-AuthC-List-1 group
```

```
FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
```

La commande de **liste d'authentication login d'AAA** se rapporte au groupe d'Authentification, autorisation et comptabilité (AAA) (qui définit le serveur de RAYON). Les déclarer de commande de **liste d'aaa authorization network** qui ont localement défini des utilisateurs/groupes doivent être utilisés. La configuration sur le serveur de RAYON doit être changée pour permettre des demandes d'authentification de ce périphérique.

2. Configurez la stratégie locale d'autorisation.

```
ip local pool FlexVPN-Pool-1 10.8.8.100 10.8.8.200
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
pool FlexVPN-Pool-1
dns 10.7.7.129
netmask 255.255.255.0
def-domain example.com
```

La commande d'**ip local pool** est utilisée de définir les adresses IP qui sont assignées au client. Une stratégie d'autorisation est définie avec un nom d'utilisateur de *FlexVPN-Local-Policy-1*, et des attributs pour le client (serveurs DNS, netmask, liste de fractionnement, nom de domaine, et ainsi de suite) sont configurés ici.

3. Assurez que le serveur emploie un certificat (RSA-Sig) afin de s'authentifier.

Le Client à mobilité sécurisé Cisco AnyConnect a besoin de que le serveur s'authentifient utilisant un certificat (RSA-Sig). Le routeur doit avoir un certificat de *web server* (c'est-à-dire, un certificat avec la « authentification de serveur » dans l'extension étendue d'utilisation principale) d'un Autorité de certification (CA) de confiance.

Référez-vous aux étapes 1 à 4 dans ASA 8.x installent manuellement des Certificats de constructeur de tiers pour l'usage avec l'exemple de configuration de webvpn, et changent tous les exemples de *crypto Ca au crypto PKI*.

```
crypto pki trustpoint FlexVPN-TP-1
enrollment url
serial-number none
fqdn flex-hub.example.com
ip-address none
subject-name cn=flex-hub.example.com
revocation-check crl
rsakeypair FlexVPN-TP-1-Key 2048
```

4. Configurez les configurations pour cette connexion.`crypto ikev2 profile FlexVPN-IKEv2-Profile-1`

```
match identity remote key-id example.com
identity local dn
authentication remote eap query-identity
authentication local rsa-sig
pki trustpoint FlexVPN-TP-1
dpd 60 2 on-demand
aaa authentication eap FlexVPN-AuthC-List-1
aaa authorization group eap list FlexVPN-AuthZ-List-1
FlexVPN-Local-Policy-1
virtual-template 10
```

Les cryptos ontains du **profilec ikev2** la plupart des configurations appropriées pour cette

connexion : **clé-id distant de match identity** - Se rapporte à l'identité d'IKE utilisée par le client. Cette valeur de chaîne est configurée dans le profil d'AnyConnect XML.**dn local d'identité** - Définit l'identité d'IKE utilisée par le hub de FlexVPN. Cette valeur utilise la valeur du certificat utilisé.**distant d'authentification** - Déclarer que l'EAP devrait être utilisé pour l'authentification client.**les états locaux d'authentification** que des Certificats devraient être utilisés pour des gens du pays authentifient.**eap d'authentification d'AAA** - États pour utiliser la liste FlexVPN-AuthC-List-1 d'authentication login d'AAA quand l'EAP est utilisé pour l'authentification.**liste d'eap de groupe d'autorisation d'AAA** - États pour utiliser la liste FlexVPN-AuthZ-List-1 d'aaa authorization network avec le nom d'utilisateur de *FlexVPN-Local-Policy-1* pour des attributs d'autorisation.**virtual-template 10** - Définit quel modèle à l'utiliser quand une interface d'accès virtuel est copiée.

5. Configurez un profil IPSec qui joint de nouveau au profil IKEv2 défini dans l'étape 4.
   ```
   crypto ipsec profile FlexVPN-IPsec-Profile-1
   set ikev2-profile FlexVPN-IKEv2-Profile-1
   ```
   Remarque: Le Cisco IOS utilise des par défaut intelligents. En conséquence, un jeu de transformations n'a pas besoin d'être explicitement défini.

6. Configurez le modèle virtuel dont les interfaces d'accès virtuel sont copiées :
   ip unnumbered - Unnumber l'interface d'un acheminement d'*interface interne* ainsi d'ipv4 peut être activé sur l'interface.**ipv4 d'ipsec de tunnel mode -** Définit l'interface pour être un tunnel de type VTI.`interface Virtual-Template10 type tunnel`
   ```
   ip unnumbered GigabitEthernet0/0
   tunnel mode ipsec ipv4
   tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
   ```

7. Limitez la négociation à SHA-1. (Facultatif)

   Dû pour déserter CSCud96246 (clients enregistrés seulement), le client d'AnyConnect pourrait pour valider correctement le certificat de hub de FlexVPN. Cette question est due à IKEv2 négociant une fonction SHA-2 pour la fonction pseudo-aléatoire (PRF) tandis que le certificat de FlexVPN-hub a été signé utilisant SHA-1. Les limites ci-dessous de configuration la négociation à SHA-1 :

   ```
   crypto ikev2 proposal SHA1-only
   encryption aes-cbc-256
   integrity sha1
   group 5
   crypto ikev2 policy SHA1-only
   match fvrf any
   proposal SHA1-only
   ```

Configuration du serveur de Microsoft Active Directory

1. Dans le gestionnaire de Windows Server, développez les **rôles > la politique réseau et le serveur d'accès > le NMPS (gens du pays) > des clients RADIUS et des serveurs**, et cliquez sur les **clients RADIUS**.

   La nouvelle boîte de dialogue de client RADIUS apparaît.

2. Dans la nouvelle boîte de dialogue de client RADIUS, ajoutez le routeur Cisco IOS en tant que client RADIUS :
   Cliquez sur l'**enable cette** case de **client RADIUS**.Écrivez un nom dans la zone d'identification amicale. Cet exemple utilise le FlexVPN-*hub*.Écrivez l'adresse IP du routeur dans la zone adresse.Dans la zone secrète partagée, cliquez sur la case d'option **manuelle**, et écrivez le secret partagé dans le secret partagé et les domaines secrets partagés Confirm.**Remarque:** Le secret partagé doit apparier le secret partagé configuré sur le routeur.Cliquez sur **OK**.

3. Dans l'interface de gestionnaire du serveur, développez les **stratégies**, et choisissez les **politiques réseau**.

   La nouvelle boîte de dialogue de politique réseau apparaît.

4. Dans la nouvelle boîte de dialogue de politique réseau, ajoutez une nouvelle politique réseau :

   Écrivez un nom dans le domaine de nom de stratégie. Cet exemple utilise *FlexVPN*.Cliquez sur le **type de** case d'option de **serveur d'accès à distance**, et choisissez **non spécifié de la** liste déroulante.Cliquez sur **Next** (Suivant).Dans la nouvelle boîte de dialogue de politique réseau, cliquez sur Add **pour ajouter un nouvel état.**Dans la boîte de dialogue choisie de condition, sélectionnez l'état d'**ipv4 addres de NAS**, et cliquez sur Add.

   La boîte de dialogue d'ipv4 addres de NAS apparaît.

   Dans la boîte de dialogue d'ipv4 addres de NAS, entrez dans l'ipv4 addres du serveur d'accès à distance afin de limiter la politique réseau seulement aux demandes qui proviennent de ce routeur Cisco IOS.

   Cliquez sur **OK**.

   Dans la nouvelle boîte de dialogue de politique réseau, cliquez sur **Access a accordé la** case d'option afin de permettre l'accès client au réseau (si les qualifications fournies par l'utilisateur sont valides), et clique sur Next.

   Assurez seulement Microsoft : Le mot de passe sécurisé (EAP-MSCHAP v2) apparaît dans la région de types d'EAP afin de permettre EAP-MSCHAPv2 à utiliser comme moyen de communication entre le périphérique de Cisco IOS et le Répertoire actif, et clique sur Next.

Remarque: Laissez tout les « moins les options sécurisées de méthodes d'authentification décochées.

Continuez par l'assistant et appliquez n'importe quelles contraintes ou configurations supplémentaires comme définies par votre stratégie de sécurité d'organismes. En outre, assurez-vous que la stratégie est répertoriée d'abord dans la commande de traitement suivant les indications de cette image :

Configuration du client

1. Créez un profil XML dans un éditeur de texte, et nommez-le *flexvpn.xml.*

   Cet exemple utilise ce profil XML :

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/
AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">false
</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">true
</AutomaticCertSelection>
<ShowPreConnectMessage>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AllowLocalProxyConnections>true
</AllowLocalProxyConnections>
<AuthenticationTimeout>12</AuthenticationTimeout>
<AutoConnectOnStart UserControllable="true">false
</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">true
</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">false
</LocalLanAccess>
<ClearSmartcardPin UserControllable="true">false
</ClearSmartcardPin>
<AutoReconnect UserControllable="false">true
<AutoReconnectBehavior UserControllable="false">
DisconnectOnSuspend
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="true">false</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon
</WindowsLogonEnforcement>
<WindowsVPNEstablishment>LocalUsersOnly
</WindowsVPNEstablishment>
```

```
<AutomaticVPNPolicy>false</AutomaticVPNPolicy>
<PPPExclusion UserControllable="false">Disable
<PPPExclusionServerIP UserControllable="false">
</PPPExclusionServerIP>
</PPPExclusion>
<EnableScripting UserControllable="true">true
<TerminateScriptOnNextEvent>true
</TerminateScriptOnNextEvent>
<EnablePostSBLOnConnectScript>true
</EnablePostSBLOnConnectScript>
</EnableScripting>
<EnableAutomaticServerSelection UserControllable="false">false
<AutoServerSelectionImprovement>20
</AutoServerSelectionImprovement>
<AutoServerSelectionSuspendTime>4
</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false
</RetainVpnOnLogoff>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>FlexVPN Hub</HostName>
<HostAddress>flexvpn-hub.example.com</HostAddress>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>EAP-MSCHAPv2</AuthMethodDuringIKENegotiation>
<IKEIdentity>example.com</IKEIdentity>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

le **<HostName>** est une chaîne de texte qui apparaît dans le client.le **<HostAddress>** est le nom de domaine complet (FQDN) du hub de FlexVPN.le **<PrimaryProtocol>** configure la connexion pour utiliser IKEv2/IPsec plutôt que SSL (le par défaut dans AnyConnect).le **<**AuthMethodDuringIKENegotiation**>** configure la connexion pour utiliser MSCHAPv2 dans l'EAP. Cette valeur est exigée pour l'authentification contre la Microsoft Active Directory.le **<**IKEIdentity**>** définit la valeur de chaîne qui apparie le client à un profil de la particularité IKEv2 sur le hub (voir l'étape 4 ci-dessus).
Remarque: Le profil de client est quelque chose qui est seulement utilisé par le client. L'il est recommandé que un administrateur emploie l'éditeur de profil d'Anyconnect afin de créer le profil de client.

2. Sauvegardez le fichier flexvpn.xml au répertoire approprié comme répertorié dans cette table :

3. La fin et redémarrent le client d'AnyConnect.

4. Dans la boîte de dialogue de Client à mobilité sécurisé Cisco AnyConnect, choisissez le **hub de FlexVPN**, et le clic **se connectent**.

Le Cisco AnyConnect | La boîte de dialogue de hub de FlexVPN apparaît.

5. Écrivez un nom d'utilisateur et mot de passe, et cliquez sur OK.

Vérifiez

Afin de vérifier la connexion, utilisez la commande **distante de client-IP address de petit groupe de show crypto session**. Référez-vous au show crypto session pour plus d'informations sur cette commande.

> Remarque: L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Afin de dépanner la connexion, collecter et analyser des logs de DART du client et utiliser ces commandes de débogage sur le routeur : **paquet** et **debug crypto ikev2 du debug crypto ikev2 internes**.

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

Informations connexes

- Support et documentation techniques - Cisco Systems