IKEv2 avec l'authentification agile de client vpn et de certificat du Windows 7 IKEv2 sur FlexVPN

Contenu

Introduction

FlexVPN est la nouvelle version 2 d'échange de clés Internet (IKE) (infrastructure IKEv2)-based le VPN sur le Cisco IOS® et est censé pour être une solution VPN unifiée. Ce document décrit comment configurer le client IKEv2 qui est construit dans le Windows 7 afin de connecter un headend de Cisco IOS à l'utilisation d'un Autorité de certification (CA).

> Remarque: L'appliance de sécurité adaptable (ASA) prend en charge maintenant les connexions IKEv2 avec le client intégré de Windows 7 en date de la version 9.3(2).

> Remarque: Les protocoles SUITE-B ne fonctionnent pas parce que le headend IOS ne prend en charge pas SUITE-B avec IKEv1, ou le client vpn agile du Windows 7 IKEv2 ne prend en charge pas actuellement SUITE-B avec IKEv2.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Client vpn de fonction intégrée de Windows 7
- Version du logiciel Cisco IOS 15.2(2)T
- Autorité de certification - OpenSSL CA

Composants utilisés

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

- Client vpn de fonction intégrée de Windows 7
- Logiciel Release15.2(2)T de Cisco IOS
- Autorité de certification - OpenSSL CA

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

Aperçu

Il y a quatre étapes principales dans la configuration du client IKEv2 intégré de Windows 7 afin de connecter un headend de Cisco IOS à l'utilisation d'un CA :

1. Configurez le CA

   Le CA devrait te permettre pour inclure l'utilisation principale étendue exigée (EKU) dans le certificat. Par exemple, sur le serveur IKEv2, le « serveur EKU authentique » est prié, alors que le certificat client a besoin de « client EKU authentique. » Les déploiements locaux peuvent se servir :Serveur du Cisco IOS CA - des Certificats Auto-signés ne peuvent pas être utilisés en raison de la bogue CSCuc82575.Serveur d'OpenSSL CAServeur de Microsoft CA - Généralement c'est l'option préférée parce qu'il peut être configuré pour signer le certificat exactement comme désiré.

2. Configurez le headend de Cisco IOS

Obtenez un certificatConfigurez IKEv2

3. Configurez le client de fonction intégrée de Windows 7
4. Obtenez le certificat client

Chacune de ces étapes principales est expliquée en détail dans les parties suivantes.

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

Configurez l'autorité de certification

Ce document ne fournit pas les étapes détaillées sur la façon dont installer un CA. Cependant, les étapes dans cette section t'affichent comment configurer le CA ainsi il peut délivrer des Certificats pour ce genre de déploiement.

OpenSSL

OpenSSL CA est basé sur le fichier de « config ». Le fichier de « config » pour le serveur d'OpenSSL devrait avoir :

```
[ extCSR ]
keyUsage            = nonRepudiation, digitalSignature, keyEncipherment, dataEncipherment
extendedKeyUsage    = serverAuth, clientAuth
```

Serveur du Cisco IOS CA

Si vous utilisez un serveur du Cisco IOS CA, assurez-vous que vous utilisez la version logicielle de Cisco IOS la plus récente, qui assigne l'EKU.

```
IOS-CA# show run | section crypto pki
crypto pki server IOS-CA
 issuer-name cn=IOS-CA.cisco.com,ou=TAC,o=cisco
 grant auto
  eku server-auth client-auth
```

Configurez le Headend de Cisco IOS

Obtenez un certificat

Le certificat doit avoir les champs EKU réglés à la « authentification de serveur » pour le Cisco IOS et la « authentification client » pour le client. Typiquement, le même CA est utilisé pour signer les les deux les Certificats de client et serveur. Dans ce cas, la « authentification de serveur » et la « authentification client » sont vues sur le certificat et le certificat client de serveur respectivement, qui est acceptable.

Si le CA délivre les Certificats dans les normes de cryptographie à clé publique (PKCS) #12 formatent sur le serveur IKEv2 aux clients et le serveur, et si le Liste des révocations de certificat (CRL) n'est pas accessible ou disponible, ils doivent être configurés :

```
crypto pki trustpoint FlexRootCA
   revocation-check none
```

Sélectionnez cette commande afin d'importer le certificat PKCS#12 :

```
copy ftp://user:***@OpenSSLServer/p12/ikev2.p12*  flash:/
crypto pki import FlexRootCA pkcs12 flash:/ikev2.p12 password <password>
!! Note: ikev2.p12 is a pkcs12 format certificate that has CA Certificate bundled in it.
```

Si un automatique de serveur du Cisco IOS CA accorde des Certificats, le serveur IKEv2 doit être configuré avec l'URL de serveur CA afin de recevoir un certificat suivant les indications de cet exemple :

```
crypto pki trustpoint IKEv2
enrollment url http://<CA_Sever_IP>:80
subject-name cn=ikev2.cisco.com,ou=TAC,o=cisco
revocation-check none
```

Quand le point de confiance est configuré, vous avez besoin :

1. Authentifiez le CA avec cette commande :

   ```
   crypto pki authenticate FlexRootCA
   ```

2. Inscrivez-vous le serveur IKEv2 avec le CA avec cette commande :

   ```
   crypto pki enroll FlexRootCA
   ```

Afin de voir si le certificat contient toutes les options exigées, utilisez cette **commande show** :

```
ikev2#show crypto pki cert verbose
Certificate
  <snip>
 Issuer:
   <snip>
 Subject:
   Name: ikev2.cisco.com
   ou=TAC
   o=Cisco
   c=BE
  cn=ikev2.cisco.com
<snip>
 Subject Key Info:
   Public Key Algorithm: rsaEncryption
   RSA Public Key: (1024 bit)
 Signature Algorithm: MD5 with RSA Encryption
 Fingerprint MD5: 3FB01AE4 E36DF9D8 47F3C206 05F287C6

 Fingerprint SHA1: DEE6C4D1 00CDD2D5 C0976274 203D2E74 2BC49BE8
 X509v3 extensions:
  X509v3 Key Usage: F0000000
      Digital Signature
     Non Repudiation
     Key Encipherment
     Data Encipherment
   X509v3 Subject Key ID: CBCE6E9F F508927C E97040FD F49B52D1 D5919D45
   X509v3 Authority Key ID: 4B86A079 A5738694 85721D0D 7A75892F 0CDAC723
   Authority Info Access:
  Extended Key Usage:
        Client Auth
        Server Auth
 Associated Trustpoints: FlexRootCA
 Key Label: FlexRootCA
```

Configurez IKEv2

C'est un exemple de la configuration IKEv2 :

```
!! IP Pool for IKEv2 Clients

ip local pool mypool 172.16.0.101 172.16.0.250


!! Certificate MAP to match Remote Certificates, in our case the Windows 7 Clients

crypto pki certificate map win7_map 10
  subject-name co ou = tac

!! One of the proposals that Windows 7 Built-In Client Likes

crypto ikev2 proposal win7
  encryption aes-cbc-256
  integrity sha1
  group 2

!! IKEv2 policy to store a proposal

crypto ikev2 policy win7
  proposal win7

!! IKEv2 Local Authorization Policy. Split-Tunneling does not work, as was
!! the case in good old l2tp over IPSec.

crypto ikev2 authorization policy win7_author
  pool mypool

!! IKEv2 Profile

crypto ikev2 profile win7-rsa
  match certificate win7_map
  identity local fqdn ikev2.cisco.com
  authentication local rsa-sig
  authentication remote rsa-sig
  pki trustpoint FlexRootCA
  aaa authorization group cert list win7 win7_author
  virtual-template 1


!! One of the IPSec Transform Sets that Windows 7 likes

crypto ipsec transform-set aes256-sha1 esp-aes 256 esp-sha-hmac


!! IPSec Profile that calls IKEv2 Profile

crypto ipsec profile win7_ikev2
  set transform-set aes256-sha1
  set ikev2-profile win7-rsa


!! dVTI interface - A termination point for IKEv2 Clients

interface Virtual-Template1 type tunnel
  ip unnumbered Loopback0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile win7_ikev2
```

L'ip unnumbered du virtual-template devrait être quelque chose local-address d'exceptthe utilisé pour la connexion d'IPsec. [Si vous utilisez un client matériel, vous permuteriez les informations de routage par l'intermédiaire du noeud de la configuration IKEv2 et créeriez une question

récursive de routage sur le client matériel.]

Configurez le client de fonction intégrée de Windows 7

Cette procédure décrit comment configurer le client de fonction intégrée de Windows 7.

1. Naviguez vers le **réseau et centre de partager**, et cliquez sur **installent une nouvelle connexion ou réseau**.

2. **Utilisation de** clic **ma connexion Internet (VNP)**. Ceci te permet pour installer une connexion VPN négociée au-dessus d'une connexion Internet en cours.

3. Écrivez le nom de domaine complet (FQDN) ou l'adresse IP du serveur IKEv2, et donnez-lui un nom de destination pour l'identifier localement.

   Remarque: Le FQDN doit apparier le nom commun (NC) du certificat d'identité de routeur. Arrêters la connexion de Windows 7 avec une erreur 13801 si elle détecte une non-concordance.
   Puisque des paramètres supplémentaires doivent être placés, le contrôle **ne se connectent pas maintenant ; juste réglé le ainsi je peux me connecter plus tard**, et clique sur Next :

4. Ne complétez pas les champs **(facultatifs) de nom d'utilisateur**, de **mot de passe** et de **domaine** parce que l'authentification de certificat doit être utilisée. Cliquez sur **Create**.

   Remarque: Fermez la fenêtre résultante. **N'essayez pas de se connecter.**
5. Naviguez de nouveau au **réseau et centre de partager**, et cliquez sur les **configurations d'adaptateur de modification**.

6. Choisissez le FlexVPN-IOS logique d'adaptateur, qui est le résultat de toutes les mesures prises à ce point. Cliquez sur ses propriétés. Ce sont les propriétés du profil de création récente de connexion appelé le FlexVPN-IOS :

   Sur l'onglet Sécurité, le type de VPN devrait être IKEv2.Dans la section d'authentification, choisissez les **Certificats d'ordinateur d'utilisation**.

   Le profil FlexVPN-IOS est maintenant prêt à être connecté après que vous ayez importé un

certifcate à la mémoire de certificat d'ordinateur.

Obtenez le certificat client

Le certificat client exige ces facteurs :

- Le certificat client a un EKU de la « authentification client ». En outre, le CA donne un certificat PKCS#12 :

```
Client's PKCS12 Certificate will go into Local Machine Personal Certificate Store
```

- Certificat de CA :

```
CA Certificate goes into Local Machine Trusted Root Certificate Authorities Store
```

Importants détails

- « L'intermédiaire d'IKE d'IPSec » (OID = 1.3.6.1.5.5.8.2.2) devrait être utilisée comme EKU si chacun des deux déclarations s'appliquent :

  Le serveur IKEv2 est un serveur de Windows 2008.Il y a plus d'un certificat d'authentification de serveur en service pour les connexions IKEv2. Si c'est vrai, ou placez la « authentification de serveur » EKU et « l'intermédiaire d'IKE d'IPSec » EKU sur un certificat, ou distribuent ces EKUs parmi les Certificats. Assurez-vous qu'au moins un certificat contient « l'intermédiaire » EKU d'IKE d'IPSec.

  Référez-vous dépannage derrière IKEv2 VPN Connectionsfor plus d'informations.

- Dans un déploiement de FlexVPN, n'utilisez pas « l'intermédiaire d'IKE d'IPSec » dans EKU. Si vous faites, le client IKEv2 ne prend pas le certificat de serveur IKEv2. En conséquence, ils ne peuvent pas répondre à CERTREQ d'IOS dans le message de réponse IKE_SA_INIT et ainsi pour se connecter à un ID de 13806 erreurs.

- Tandis que le nom alternatif soumis (SAN) n'est pas exigé, il est acceptable si les Certificats ont un.

- Sur la mémoire de certificat client de Windows 7, assurez-vous que la mémoire Ordinateur-faite confiance d'autorités de certificat racine a le moins nombre de Certificats possibles. S'il a plus de 50 environ, le Cisco IOS pourrait pour lire la charge utile entière de Cert_Req, qui contient le nom unique de certificat (DN) de tout le CAs connu de la case de Windows 7. En conséquence, la négociation échoue et vous voyez la minuterie de connexion sur le client.

Vérifiez

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

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

```
ikev2#show crypto ikev2 session detail
IPv4 Crypto IKEv2 Session
```

Session-id:4, **Status:UP-ACTIVE**, IKE count:1, **CHILD count:1**

Tunnel-id Local Remote fvrf/ivrf Status
1 10.0.3.1/4500 192.168.56.1/4500 none/none READY
Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:2, Auth sign: RSA,
Auth verify: RSA
Life/Active Time: 86400/17 sec
CE id: 1004, Session-id: 4
Status Description: Negotiation done
Local spi: A40828A826160328 Remote spi: C004B7103936B430
Local id: ikev2.cisco.com
Remote id: ou=TAC,o=Cisco,c=BE,cn=Win7
Local req msg id: 0 Remote req msg id: 2
Local next msg id: 0 Remote next msg id: 2
Local req queued: 0 Remote req queued: 2
Local window: 5 Remote window: 1 DPD configured for 0 seconds,
retry 0
NAT-T is not detected
Cisco Trust Security SGT is disabled

ikev2#**show crypto ipsec sa peer 192.168.56.1**

interface: **Virtual-Access1**

Crypto map tag: Virtual-Access1-head-0, local addr 10.0.3.1
protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.0.104/255.255.255.255/0/0)
current_peer 192.168.56.1 port 4500
PERMIT, flags={origin_is_acl,}
#pkts encaps:5, #pkts encaps:5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 55, #pkts decrypt: 55, #pkts verify: 55
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.0.3.1, remote crypto endpt.: 192.168.56.1
path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
current outbound spi: 0x3C3D299(63165081)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0xE461ED10(3831622928)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 7, flow_id: SW:7, sibling_flags 80000040, crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4257423/0)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0x3C3D299(63165081)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 8, flow_id: SW:8, sibling_flags 80000040, crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4257431/0)

```
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```

Dépannez

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

Informations connexes

- Debugs ASA IKEv2 pour le site à site VPN avec PSKs TechNote
- ASA IPsec et IKE met au point (mode IKEv1 principal) dépannage de TechNote
- IOS IPSec et IKE met au point - Mode IKEv1 principal dépannant TechNote
- ASA IPSec et IKE met au point - IKEv1 mode agressif TechNote
- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Téléchargements logiciels de Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500
- Cisco IOS Firewall
- Logiciel Cisco IOS
- Secure Shell (SSH)
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems