Exemple de configuration de FlexVPN entre un routeur et un ASA avec chiffrement de nouvelle génération

Contenu

Introduction

Ce document décrit comment configurer un VPN entre un routeur avec FlexVPN et un appareil de sécurité adaptatif (ASA) prenant en charge les algorithmes de chiffrement nouvelle génération (NGE) de Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- Internet Key Exchange version 2 (IKEv2)
- IPsec
- ASA

- Cryptographie de nouvelle génération

Components Used

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

- **Matériel :** Routeur de 2ème génération IOS qui exécute la licence de sécurité.
- **le logiciel Cisco IOS:** Version du logiciel Cisco IOS® 15.2-3.T2. Toute version de M ou T pour les versions ultérieures à la version 15.1.2T du logiciel Cisco IOS® peut être utilisée car elle est incluse avec l'introduction du mode compteur Galois (GCM).
- **Matériel :** ASA prenant en charge NGE.**Remarque :** Seules les plates-formes multicoeurs prennent en charge la norme AES (Advanced Encryption Standard) GCM.
- **le logiciel Cisco IOS:** Logiciel ASA version 9.0 ou ultérieure prenant en charge NGE.
- OpenSSL.

Pour plus d'informations, reportez-vous à Cisco Feature Navigator.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Créer dynamiquement des associations de sécurité IPSec

L'interface IPSec recommandée sur IOS est une interface de tunnel virtuel (VTI), qui crée une interface GRE (Generic Routing Encapsulation) protégée par IPsec. Pour une VTI, le sélecteur de trafic (quel trafic doit être protégé par les associations de sécurité IPSec (SA)) est constitué du trafic GRE de la source du tunnel à la destination du tunnel. Comme l'ASA n'implémente pas les interfaces GRE, mais crée plutôt des SA IPSec basées sur le trafic défini dans une liste de contrôle d'accès (ACL), nous devons activer une méthode qui permet au routeur de répondre à l'initiation IKEv2 avec un miroir des sélecteurs de trafic proposés. L'utilisation de l'interface DVTI (Dynamic Virtual Tunnel Interface) sur le routeur FlexVPN permet à ce périphérique de répondre au sélecteur de trafic présenté avec un miroir du sélecteur de trafic présenté.

Cet exemple chiffre le trafic entre les deux réseaux internes. Lorsque l'ASA présente les sélecteurs de trafic du réseau interne ASA au réseau interne IOS, `192.168.1.0/24` à `172.16.10.0/24`, l'interface DVTI répond avec un miroir des sélecteurs de trafic, qui est `172.16.10.0/24` à `192.168.1.0/24`.

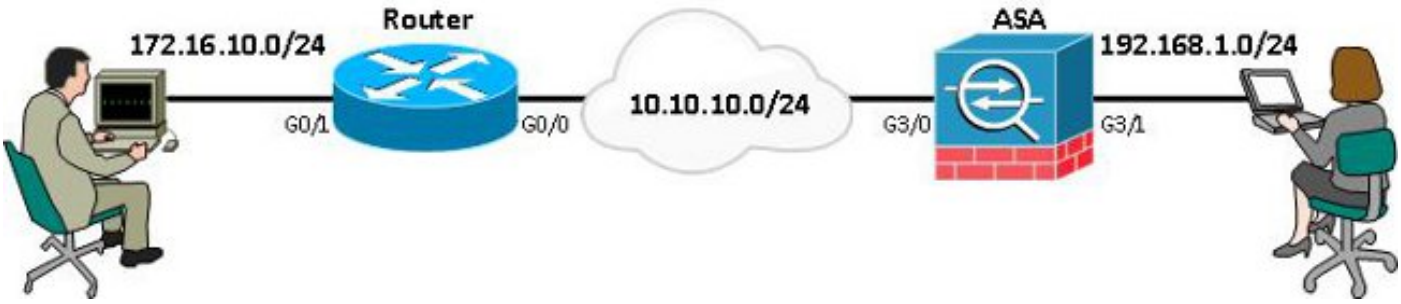
Autorité de certification

Actuellement, IOS et ASA ne prennent pas en charge un serveur d'autorité de certification local avec des certificats ECDSA (Elliptic Curve Digital Signature Algorithm), requis pour Suite-B. Un serveur CA tiers doit donc être mis en oeuvre. Par exemple, utilisez OpenSSL pour agir en tant qu'autorité de certification.

Configuration

Topologie du réseau

Ce guide est basé sur la topologie illustrée dans ce schéma. Vous devez modifier les adresses IP en conséquence.



Remarque : la configuration inclut une connexion directe du routeur et de l'ASA. Ils peuvent être séparés par de nombreux sauts. Si oui, assurez-vous qu'il existe une route pour accéder à l'adresse IP de l'homologue. La configuration suivante ne détaille que le chiffrement utilisé.

Étapes requises pour permettre au routeur d'utiliser l'ECDSA

Autorité de certification

1. Créez une **paire de clés de courbe elliptique.**
   ```
   openssl ecparam -out ca.key -name secp256r1 -genkey
   ```
2. Créez un **certificat auto-signé de courbe elliptique**.
   ```
   openssl req -x509 -new -key ca.key -out ca.pem -outform PEM -days 3650
   ```

FlexVPN

1. Créez **domain-name** et **hostname**, qui sont des conditions préalables pour créer une paire de clés de courbe elliptique (EC).
   ```
   ip domain-name cisco.com
   hostname Router1
   crypto key generate ec keysize 256 label router1.cisco.com
   ```
2. Créez un **point de confiance** local afin d'obtenir un certificat de l'autorité de certification.
   ```
   crypto pki trustpoint ec_ca
    enrollment terminal
    subject-name cn=router1.cisco.com
    revocation-check none
    eckeypair router1.cisco.com
    hash sha256
   ```
   Remarque : étant donné que l'autorité de certification est hors connexion, la vérification de révocation est désactivée ; le contrôle de révocation doit être activé pour une sécurité maximale dans un environnement de production.
3. Authentifiez le **point de confiance**. Cette commande obtient une copie du certificat de l'autorité de certification, qui contient la clé publique.
   ```
   crypto pki authenticate ec_ca
   ```
4. Vous êtes alors invité à saisir le certificat codé en base 64 de l'autorité de certification. Il s'agit du fichier ca.pem, qui a été créé avec OpenSSL. Pour afficher ce fichier, ouvrez-le

dans un éditeur ou avec la commande OpenSSL **openssl x509 -in ca.pem**. Entrez **quit** lorsque vous collez ceci. Tapez ensuite **yes** à accepter.

5. Inscrivez le routeur à l'infrastructure à clé publique (PKI) de l'autorité de certification.
```
crypto pki enrol ec_ca
```
6. La sortie que vous recevez doit être utilisée pour envoyer une demande de certificat à l'AC. Ceci peut être enregistré sous forme de fichier texte (flex.csr) et signé avec la commande OpenSSL.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in flex.csr -out flex.pem
```
7. Importez le certificat, qui est contenu dans le fichier flex.pem, généré à partir de l'autorité de certification, dans le routeur après avoir entré cette commande. Ensuite, entrez **quit** lorsque vous avez terminé.
```
crypto pki import ec_ca certificate
```

ASA

1. Créez **domain-name** et **hostname**, qui sont des conditions préalables pour créer une paire de clés EC.
```
domain-name cisco.com
hostname ASA1
crypto key generate ecdsa label asa1.cisco.com elliptic-curve 256
```
2. Créez un **point de confiance** local afin d'obtenir un certificat de l'autorité de certification.
```
crypto ca trustpoint ec_ca
 enrollment terminal
 subject-name cn=asa1.cisco.com
 revocation-check none
 keypair asa1.cisco.com
```
Remarque : étant donné que l'autorité de certification est hors connexion, la vérification de révocation est désactivée ; le contrôle de révocation doit être activé pour une sécurité maximale dans un environnement de production.
3. Authentifiez le **point de confiance**. Cette commande obtient une copie du certificat de l'autorité de certification, qui contient la clé publique.
```
crypto ca authenticate ec_ca
```
4. Vous êtes alors invité à saisir le certificat codé en base 64 de l'autorité de certification. Il s'agit du fichier ca.pem, qui a été créé avec OpenSSL. Pour afficher ce fichier, ouvrez-le dans un éditeur ou avec la commande OpenSSL **openssl x509 -in ca.pem**. Entrez **quit** lorsque vous collez ce fichier, puis tapez **yes** pour accepter.
5. Inscrivez l'ASA à l'ICP sur l'AC.
```
crypto ca enrol ec_ca
```
6. La sortie que vous recevez doit être utilisée pour soumettre une demande de certificat à l'AC. Il peut être enregistré sous forme de fichier texte (asa.csr), puis signé avec la commande OpenSSL.
```
openssl ca -keyfile ca.key -cert ca.pem -md sha256 -in asa.csr -out asa.pem
```
7. Importez le certificat, qui est contenu dans le fichier sous la forme a.pem, généré à partir de l'autorité de certification dans le routeur après l'entrée de cette commande. Puis **entrez** quit une fois terminé.
```
crypto ca import ec_ca certificate
```

Configuration

FlexVPN

Créez une carte de certificat correspondant au certificat du périphérique homologue.

```
crypto pki certificate map certmap 10
 subject-name co cisco.com
```

Entrez les commandes suivantes pour la proposition IKEv2 de configuration de la suite B :

Remarque : pour une sécurité maximale, configurez avec la commande **de hachage aes-cbc-256 avec sha512**.

```
crypto ikev2 proposal default
 encryption aes-cbc-128
 integrity sha256
 group 19
```

Associez le profil IKEv2 à la carte de certificat et utilisez ECDSA avec le **trustpoint** précédemment défini.

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ec_ca
 virtual-template 1
```

Configurez le jeu de transformation IPSec pour qu'il utilise le mode Compteur Galois (GCM).

```
crypto ipsec transform-set ESP_GCM esp-gcm
 mode transport
```

Configurez le profil IPSec avec les paramètres précédemment configurés.

```
crypto ipsec profile default
 set transform-set ESP_GCM
 set pfs group19
 set ikev2-profile default
```

Configurez l'interface de tunnel :

```
interface Virtual-Template1 type tunnel
 ip unnumbered GigabitEthernet0/0
 tunnel source GigabitEthernet0/0
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile default
```

Voici la configuration de l'interface :

```
interface GigabitEthernet0/0
 ip address 10.10.10.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 172.16.10.1 255.255.255.0
```

ASA

Utilisez cette configuration d'interface :

```
interface GigabitEthernet3/0
 nameif outside
 security-level 0
 ip address 10.10.10.2 255.255.255.0
interface GigabitEthernet3/1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
```

Entrez cette commande de liste d'accès afin de définir le trafic à chiffrer :

```
access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0 255.255.255.0
```

Entrez cette commande de proposition IPSec avec NGE :

```
crypto ipsec ikev2 ipsec-proposal prop1
 protocol esp encryption aes-gcm
 protocol esp integrity null
```

Commandes de carte de chiffrement :

```
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 10.10.10.1
crypto map mymap 10 set ikev2 ipsec-proposal prop1
crypto map mymap 10 set trustpoint ec_ca
crypto map mymap interface outside
```

Cette commande configure la stratégie IKEv2 avec NGE :

```
crypto ikev2 policy 10
 encryption aes
 integrity sha256
 group 19
 prf sha256
 lifetime seconds 86400
crypto ikev2 enable outside
```

Groupe de tunnels configuré pour les commandes homologues :

```
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 peer-id-validate cert
 ikev2 remote-authentication certificate
 ikev2 local-authentication certificate ec_ca
```

Vérification de la connexion

Vérifiez que les clés ECDSA ont été générées avec succès.

```
Router1#show crypto key mypubkey ec router1.cisco.com
% Key pair was generated at: 21:28:26 UTC Feb 19 2013
Key name: router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
```

```
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
<...omitted...>

ASA-1(config)#show crypto key mypubkey ecdsa
Key pair was generated at: 21:11:24 UTC Feb 19 2013
Key name: asa1.cisco.com
 Usage: General Purpose Key
 EC Size (bits): 256
 Key Data&colon;
<...omitted...>
```

Vérifiez que le certificat a bien été importé et que l'ECDSA est utilisé.

```
Router1#show crypto pki certificates verbose
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 0137
  Certificate Usage: General Purpose
  Issuer:
<...omitted...>
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    EC Public Key:  (256 bit)
  Signature Algorithm: SHA256 with ECDSA


ASA-1(config)#show crypto ca certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 00a293f1fe4bd49189
  Certificate Usage: General Purpose
  Public Key Type: ECDSA (256 bits)
  Signature Algorithm: SHA256 with ECDSA Encryption
 <...omitted...>
```

Vérifiez que l'association de sécurité IKEv2 est correctement créée et utilise les algorithmes NGE configurés.

```
Router1#show crypto ikev2 sa  detailed
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.10.10.1/500        10.10.10.2/500        none/none            READY
      Encr: AES-CBC, keysize: 128, Hash: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      Life/Active Time: 86400/94 sec


ASA-1#show crypto ikev2 sa detail

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                 Local                 Remote     Status         Role
268364957        10.10.10.2/500        10.10.10.1/500      READY    INITIATOR
      Encr: AES-CBC, keysize: 128, Hash: SHA384, DH Grp:19, Auth sign: ECDSA,
        Auth verify: ECDSA
      <...omitted...>
```

```
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 172.16.10.0/0 - 172.16.10.255/65535
          ESP spi in/out: 0xe847d8/0x12bce4d
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Vérifiez que l'association de sécurité IPSec est correctement créée et utilise les algorithmes NGE configurés.

Remarque : FlexVPN peut arrêter les connexions IPSec des clients non IOS qui prennent en charge les protocoles IKEv2 et IPSec.

```
Router1#show crypto ipsec sa

interface: Virtual-Access1
    Crypto map tag: Virtual-Access1-head-0, local addr 10.10.10.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
   current_peer 10.10.10.2 port 500
     PERMIT, flags={origin_is_acl,}
<...omitted...>

     inbound esp sas:
      spi: 0x12BCE4D(19648077)
        transform: esp-gcm ,
        in use settings ={Tunnel, }

ASA-1#show crypto ipsec sa detail
interface: outside
    Crypto map tag: mymap, seq num: 10, local addr: 10.10.10.2

      access-list 100 extended permit ip 192.168.1.0 255.255.255.0 172.16.10.0
        255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (172.16.10.0/255.255.255.0/0/0)
      current_peer: 10.10.10.1
<...omitted...>


    inbound esp sas:
      spi: 0x00E847D8 (15222744)
         transform: esp-aes-gcm esp-null-hmac no compression
         in use settings ={L2L, Tunnel, IKEv2, }
```

Pour plus d'informations sur la mise en oeuvre de la suite B par Cisco, reportez-vous au Livre blanc sur le chiffrement de nouvelle génération.

Reportez-vous à la page Solution de chiffrement nouvelle génération pour en savoir plus sur la mise en oeuvre du chiffrement nouvelle génération par Cisco.

Informations connexes

- Livre blanc sur le chiffrement de nouvelle génération
- Page Solution de cryptage nouvelle génération
- Secure Shell (SSH)

- Négociation IPSec/Protocoles IKE
- Débogues ASA IKEv2 pour VPN site à site avec PSKs TechNote
- Dépannage des débogages ASA IPSec et IKE (IKEv1 Main Mode)
- Débogues IOS IPSec et IKE - IKEv1 Main Mode Trouver TechNote
- Débogues ASA IPSec et IKE - IKEv1 Aggressive Mode TechNote
- Support et documentation techniques - Cisco Systems