Exemple de configuration de FlexVPN avec chiffrement de nouvelle génération

Contenu

Introduction

Ce document décrit comment configurer un FlexVPN entre deux routeurs qui prennent en charge l'ensemble d'algorithmes Cisco NGE (Next-Generation Encryption).

Cryptage nouvelle génération

La cryptographie NGE de Cisco sécurise les informations qui circulent sur des réseaux utilisant quatre algorithmes cryptographiques configurables, bien établis et de domaine public :

- Chiffrement basé sur la norme AES (Advanced Encryption Standard), qui utilise des clés 128 bits ou 256 bits
- Signatures numériques avec l'algorithme ECDSA (Elliptic Curve Digital Signature Algorithm) qui utilisent des courbes avec des modules prime de 256 bits et 384 bits
- Échange de clés utilisant la méthode Diffie-Hellman (ECDH) de courbe elliptique
- Hachage (empreintes digitales) basé sur l'algorithme de hachage sécurisé 2 (SHA-2)

L'Agence nationale de sécurité (NSA) déclare que ces quatre algorithmes combinés fournissent une assurance adéquate des informations classifiées. La cryptographie NSA Suite B pour IPsec a été publiée en tant que norme dans la RFC 6379 et a été acceptée dans le secteur.

Suite B-GCM-128

Conformément à la RFC 6379, ces algorithmes sont requis pour la suite Suite-B-GCM-128.

Cette suite fournit une protection et une confidentialité d'intégrité ESP (Encapsulating Security Payload) avec AES-GCM 128 bits (voir RFC4106). Cette suite doit être utilisée lorsque la protection de l'intégrité ESP et le chiffrement sont tous deux nécessaires.

ESP
Cryptage AES avec clés 128 bits et ICV (Integrity Check Value) 16 octets en mode Galois/Counter (GCM) (RFC4106)
Intégrité NULL

IKEv2
Cryptage AES avec clés 128 bits en mode de chaînage par bloc de chiffrement (CBC) (RFC3602)
Fonction pseudo-aléatoire HMAC-SHA-256 (RFC4868)
Integrity HMAC-SHA-256-128 (RFC4868)
Diffie-Hellman, groupe ECP aléatoire 256 bits (RFC5903)

Pour plus d'informations sur Suite B et NGE, consultez le site Encryption Next-Generation.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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

- Matériel : Routeurs à services intégrés (ISR) de 2e génération (G2) qui exécutent la licence de sécurité.
- le logiciel Cisco IOS: Logiciel Cisco IOS® Version 15.2.3T2. Toute version du logiciel Cisco IOS Version M ou 15.1.2T ou ultérieure peut être utilisée car c'est à ce moment que GCM a été introduit.

Pour plus d'informations, reportez-vous au Navigateur de fonctions.

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.

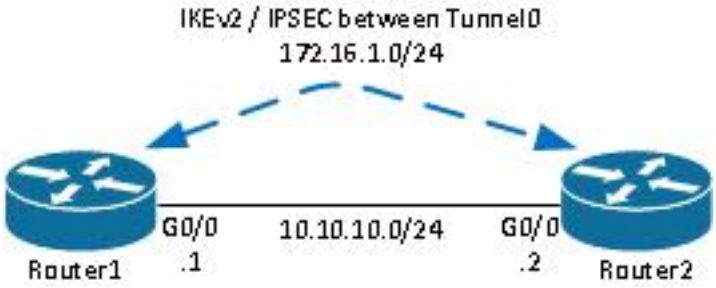
Autorité de certification

Actuellement, la plate-forme logicielle Cisco IOS ne prend pas en charge un serveur d'autorité de certification local qui exécute ECDH, qui est requis pour la suite B. Un serveur AC tiers doit être implémenté. Cet exemple utilise une autorité de certification Microsoft basée sur l'ICP Suite B

Configuration

Topologie du réseau

Ce guide est basé sur cette topologie illustrée. Les adresses IP doivent être modifiées en fonction de vos besoins.



Remarques :

La configuration se compose de deux routeurs directement connectés, qui 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. Cette configuration ne détaille que le chiffrement utilisé. Le routage IKEv2 ou un protocole de routage doit être implémenté sur le VPN IPSec.

Étapes requises pour permettre au routeur d'utiliser l'algorithme de signature numérique de courbe elliptique

1. Créez le nom de domaine et le nom d'hôte, qui sont des conditions préalables à la création d'une paire de clés EC.

```
ip domain-name cisco.com
hostname Router1
crypto key generate ec keysize 256 label Router1.cisco.com
```

   Note: Sauf si vous exécutez une version avec le correctif pour l'ID de bogue Cisco CSCue59994, le routeur ne vous permettra pas d'inscrire un certificat avec une taille de clé inférieure à 768.
2. Créez un point de confiance local afin d'obtenir un certificat de l'autorité de certification.

```
crypto pki trustpoint ecdh
 enrollment terminal
```

```
 revocation-check none
 eckeypair Router1.cisco.com
```

Note: Comme l'autorité de certification était hors ligne, les vérifications de révocation ont été désactivées. Les contrôles de révocation doivent être activés pour une sécurité maximale dans un environnement de production.

3. Authentifiez le point de confiance (il obtient une copie du certificat de l'autorité de certification qui contient la clé publique).

```
crypto pki authenticate ecdh
```

4. Entrez le certificat codé en base 64 de l'autorité de certification à l'invite. Entrez **quit**, puis **yes** to accept.

5. Inscrivez le routeur à l'ICP sur l'AC.

```
crypto pki enrol ecdh
```

6. Le résultat affiché est utilisé afin d'envoyer une demande de certificat à l'AC. Pour l'autorité de certification Microsoft, connectez-vous à l'interface Web de l'autorité de certification et sélectionnez **Soumettre une demande de certificat**.

7. Importez le certificat reçu de l'autorité de certification dans le routeur. Entrez **quit** une fois le certificat importé.

```
crypto pki import ecdh certificate
```

Configuration

La configuration fournie ici concerne Router1. Le routeur 2 nécessite un miroir de la configuration dans lequel seules les adresses IP de l'interface de tunnel sont uniques.

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

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

2. Configurez la proposition IKEv2 pour la suite B.

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

Note: IKEv2 Smart Defaults implémente un certain nombre d'algorithmes préconfigurés dans

la proposition IKEv2 par défaut. Comme aes-cbc-128 et sha256 sont requis pour la suite B-GCM-128, vous devez supprimer aes-cbc-256, sha384 et sha512 dans ces algorithmes. La raison en est qu'IKEv2 choisit l'algorithme le plus puissant lorsqu'il a le choix. Pour une sécurité maximale, utilisez aes-cbc-256 et sha512. Cependant, cela n'est pas nécessaire pour la Suite-B-GCM-128. Afin d'afficher la proposition IKEv2 configurée, entrez la commande **show crypto ikev2**.

3. Configurez le profil IKEv2 pour qu'il corresponde à la carte de certificat et utilisez ECDSA avec le point de confiance défini précédemment.

```
crypto ikev2 profile default
 match certificate certmap
 identity local dn
 authentication remote ecdsa-sig
 authentication local ecdsa-sig
 pki trustpoint ecdh
```

4. Configurez la transformation IPSec pour utiliser GCM.

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

5. Configurez le profil IPSec avec les paramètres configurés précédemment.

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

6. Configurez l'interface de tunnel.

```
interface Tunnel0
 ip address 172.16.1.1 255.255.255.0
 tunnel source Gigabit0/0 tunnel destination 10.10.10.2
 tunnel protection ipsec profile default
```

Vérifier la connexion

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Vérifiez que les clés ECDSA ont été générées avec succès.

```
Router1#show crypto key mypubkey ec
% Key pair was generated at: 04:05:07 JST Jul 6 2012
Key name: Router1.cisco.com
Key type: EC KEYS
 Storage Device: private-config
 Usage: Signature Key
 Key is not exportable.
 Key Data&colon;
 30593013 06072A86 48CE3D02 0106082A 8648CE3D 03010703 4200048F 2B0B5B5E
```

```
(...omitted...)
```

2. Vérifiez que le certificat a bien été importé et que ECDH est utilisé.

```
Router1#show crypto pki certificates verbose ecdh
Certificate
 Status: Available
 Version: 3
 Certificate Serial Number (hex): 6156E3D5000000000009
(...omitted...)
```

3. Vérifiez que la SA IKEv2 a été créée et utilise les algorithmes Suite B.

```
Router1#show crypto ikev2 sa
 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: SHA256, DH Grp:19, Auth sign: ECDSA, Auth verify:
ECDSA
     Life/Active Time: 86400/20 sec
```

4. Vérifiez que la SA IKEv2 a été créée et utilise les algorithmes Suite B.

```
Router1#show crypto ipsec sa

interface: Tunnel0
   Crypto map tag: Tunnel0-head-0, local addr 10.10.10.1

(...omitted...)

    local crypto endpt.: 10.10.10.1, remote crypto endpt.: 10.10.10.2
    plaintext mtu 1466, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
    current outbound spi: 0xAC5845E1(2891466209)
    PFS (Y/N): N, DH group: none

    inbound esp sas:
     spi: 0xAEF7FD9C(2935487900)
       transform: esp-gcm ,
       in use settings ={Transport, }
       conn id: 6, flow_id: SW:6, sibling_flags 80000000, crypto map: Tunnel0-head-0
       sa timing: remaining key lifetime (k/sec): (4341883/3471)
       IV size: 8 bytes
       replay detection support: N
       Status: ACTIVE(ACTIVE)
```

Note: Dans cette sortie, contrairement à la version 1 d'Internet Key Exchange (IKEv1), la valeur de groupe Diffie-Hellman (DH) de secret avant parfait (PFS) s'affiche comme **PFS (Y/N) : N, groupe DH : aucun** lors de la première négociation de tunnel, mais après une nouvelle clé, les valeurs de droite s'affichent. Ce n'est pas un bogue, même si le comportement est décrit dans l'ID de bogue Cisco CSCug67056. La différence entre IKEv1 et IKEv2 réside dans le fait que, dans ce dernier cas, les associations de sécurité d'enfants (SA) sont créées dans le cadre de l'échange AUTH lui-même. Le groupe DH configuré sous

la carte de chiffrement est utilisé uniquement pendant la reclé. Par conséquent, vous voyez **PFS (O/N) : N, groupe DH : aucun** jusqu'à la première clé. Mais avec IKEv1, vous voyez un comportement différent parce que la création de l'association de sécurité enfant se produit pendant le mode rapide et que le message CREATE_CHILD_SA a une disposition pour transporter la charge utile Key Exchange qui spécifie les paramètres DH pour dériver un nouveau secret partagé.

Dépannage

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

Conclusion

Les algorithmes cryptographiques efficaces et puissants définis dans NGE garantissent à long terme que les données sont fournies et conservées de manière confidentielle et intègre à un coût de traitement réduit. NGE peut être facilement implémenté avec FlexVPN, qui fournit la cryptographie standard Suite B.

Pour plus d'informations sur la mise en oeuvre de la suite B par Cisco, consultez le site Encryption Next-Generation.