

# FlexVPN avec l'exemple de la deuxième génération de configuration de chiffrement

## Contenu

[Introduction](#)

[Cryptage de la deuxième génération](#)

[Suite Suite-B-GCM-128](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Autorité de certification](#)

[Configurez](#)

[Topologie du réseau](#)

[Étape nécessaire pour permettre au routeur d'utiliser l'algorithme elliptique de signature numérique de curve](#)

[Configuration](#)

[Vérifiez la connexion](#)

[Dépannez](#)

[Conclusion](#)

## Introduction

Ce document décrit comment configurer un FlexVPN entre deux Routeurs qui prennent en charge Cisco le cryptage que de la deuxième génération (NGE) a placé des algorithmes.

## Cryptage de la deuxième génération

Le chiffrement de Cisco NGE sécurise les informations qui voyagent au-dessus des réseaux qui utilisent quatre configurables, bien établi, et des algorithmes de chiffrement de public domain :

- Cryptage basé sur le Norme AES (Advanced Encryption Standard), qui utilise les clés 128-bit ou 256-bit
- Signatures numériques avec l'algorithme elliptique de signature numérique de curve (ECDSA) que cette utilisation courbe avec les modules 256-bit et 384-bit principaux
- Échange clé qui utilise la méthode elliptique de Diffie-Hellman de curve (ECDH)
- Hachage (empreintes digital numériques) basé sur le Secure Hash Algorithm 2 (SHA-2)

L'agence de Sécurité nationale (NSA) déclare que ces quatre algorithmes fournissent en association l'assurance adéquate de l'information pour information les informations classifiées. Le chiffrement de la suite B NSA pour IPsec a été édité comme norme dans RFC 6379 et a gagné l'acceptation dans le secteur.

## Suite Suite-B-GCM-128

Selon RFC 6379, ces algorithmes sont exigés pour la suite Suite-B-GCM-128.

Cette suite fournit à la protection et à la confidentialité d'intégrité de Protocole ESP (Encapsulating Security Payload) 128-bit AES-GCM (voir le [RFC4106](#)). Cette suite devrait être utilisée quand la protection et le cryptage chacun des deux d'intégrité de l'ESP sont nécessaires.

### L'ESP

Cryptage AES avec les clés 128-bit et la valeur du contrôle d'intégrité 16-octet (ICV) en mode de Galois/compteur (GCM) (RFC4106)

NULL d'intégrité

### IKEv2

Cryptage AES avec les clés 128-bit dans le bloc de chiffrement enchaînant le mode (CBC) (RFC3602)

Fonction pseudo-aléatoire HMAC-SHA-256 (RFC4868)

Intégrité HMAC-SHA-256-128 (RFC4868)

Groupe aléatoire ECP du groupe 256-bit de Diffie-Hellman (RFC5903)

Plus d'informations sur la suite B et NGE peuvent être trouvées au [cryptage de la deuxième génération](#).

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- FlexVPN
- Version 2 (IKEv2) d'échange de clés Internet (IKE)
- IPsec

### Composants utilisés

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

- Matériel : Ce de la génération 2 (G2) des Integrated Services Router (ISR) exécuté le permis de Sécurité.
- Logiciel : Version de logiciel 15.2.3T2 de Cisco IOS®. N'importe quelle release de version du logiciel Cisco IOS M ou 15.1.2T ou plus tard peut être utilisée puisque c'est quand GCM a été introduit.

Pour des détails, référez-vous au navigateur de caractéristique.

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.

## Autorité de certification

Actuellement, le logiciel de Cisco IOS ne prend en charge pas un serveur local d'Autorité de certification (CA) qui exécute ECDH, qui est exigé pour la suite B. Un serveur du tiers CA doit être mis en application. Cet exemple utilise Microsoft CA basé sur le [PKI de la suite B](#)

## Configurez

### [Topologie du réseau](#)

Ce guide est basé sur cette topologie illustrée. Des adresses IP devraient être modifiées pour satisfaire à vos exigences.

Remarques :

L'installation se compose de deux Routeurs directement connectés, qui pourraient être séparés par beaucoup de sauts. Si oui, assurez-vous qu'il y a une artère à obtenir à l'adresse IP de pair. Cette configuration détaille seulement le cryptage utilisé. Le routage IKEv2 ou un protocole de routage devrait être mis en application au-dessus de l'IPSec VPN.

## Étape nécessaire pour permettre au routeur d'utiliser l'algorithme elliptique de signature numérique de curve

1. Créez le nom de domaine et l'adresse Internet, qui sont des conditions préalables pour créer un keypair EC.

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

Remarque: À moins que vous exécutiez une version avec la difficulté pour l'ID de bogue Cisco [CSCue59994](#), le routeur ne te permettra pas pour s'inscrire un certificat avec un keysize moins de 768.

2. Créez un point de confiance local afin de gagner un certificat du CA.

```
crypto pki trustpoint ecdh
  enrollment terminal
  revocation-check none
  eckeypair Router1.cisco.com
```

Remarque: Puisque le CA était hors ligne, des contrôles de révocation ont été désactivés. Des contrôles de révocation devraient être activés pour la sécurité maximale dans un environnement de production.

3. Authentifiez le point de confiance (ceci obtient une copie du certificat de Ca qui contient la clé publique).

```
crypto pki authenticate ecdh
```

4. Entrez dans le certificat encodé de la base 64 du CA à la demande. Entrez **quitté** et puis entrez **oui** pour recevoir.

5. Inscrivez-vous le routeur dans le PKI sur le CA.

```
crypto pki enrol ecdh
```

6. La sortie affichée est utilisée afin de soumettre une demande de certificat au CA. Pour Microsoft CA, connectez à l'interface web du CA et choisi **soumettez une demande de certificat**.

7. Importez le certificat reçu du CA dans le routeur. Entrez **quitté** une fois que le certificat est importé.

```
crypto pki import ecdh certificate
```

## Configuration

La configuration fournie ici est pour Router1. Le Router2 exige un miroir de la configuration où seulement les adresses IP sur l'interface de tunnel sont seules.

1. Créez une carte de certificat pour appairer le certificat du périphérique de pair.

```
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
```

Remarque: Les par défaut IKEv2 intelligents implémente un certain nombre d'algorithmes préconfigurés dans la proposition du par défaut IKEv2. Puisqu'aes-cbc-128 et sha256 sont exigés pour la suite Suite-B-GCM-128, vous devez retirer aes-cbc-256, sha384, et sha512 dans ces algorithmes. La raison pour ceci est qu'IKEv2 choisit l'algorithme le plus fort une fois présenté avec un choix. Pour la sécurité maximale, l'utilisation aes-cbc-256 et le sha512. Cependant, ceci n'est pas exigé pour Suite-B-GCM-128. Afin de visualiser la proposition IKEv2 configurée, sélectionnez la **crypto** commande de la **proposition ikev2 d'exposition**.

3. Configurez le profil IKEv2 pour appairer la carte de certificat et pour utiliser ECDSA avec le point de confiance défini plus tôt.

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

4. Configurez l'IPSec transformant pour utiliser GCM.

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

```
mode transport
```

## 5. Configurez le profil IPsec avec les paramètres configurés plus tôt.

```
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
```

# Vérifiez la connexion

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

```
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 été avec succès importé et qu'ECDH soit utilisé.

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

### 3. Vérifiez qu'IKEv2 SA a été avec succès créé et utilisez les algorithmes de la 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 qu'IKEv2 SA a été avec succès créé et utilisez les algorithmes de la 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)
```

Remarque: Dans cette sortie, à la différence de dans la version 1 (IKEv1) d'échange de clés Internet (IKE), la valeur de groupe de Protocole DH (Diffie-Hellman) de perfect forward secrecy (PFS) affiche comme **PFS (Y/N) : N, groupe CAD : aucun** pendant la première négociation de tunnel, mais après qu'un rekey se produise, les bonnes valeurs n'affiche. Ce n'est pas une bogue quoique le comportement soit décrit dans l'ID de bogue Cisco [CSCug67056](#). La différence entre IKEv1 et IKEv2 est que, dans ce dernier, les associations de sécurité d'enfant (SAS) sont créées en tant qu'élément de l'échange AUTHENTIQUE lui-même. Le groupe configuré CAD sous le crypto map est utilisé seulement pendant le rekey. Par conséquent, vous voyez le **PFS (Y/N) : N, groupe CAD : aucun** jusqu'au premier rekey. Mais avec IKEv1, vous voyez un comportement différent parce que la création d'enfant SA se produit pendant le mode rapide et le message CREATE\_CHILD\_SA prévoit porter la charge utile de Key Exchange qui spécifie les paramètres CAD pour dériver un nouveau secret partagé.

## Dépannez

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

## Conclusion

Les algorithmes de chiffrement efficaces et forts définis dans NGE fournissent l'assurance à long terme que des données confidentiellement et l'intégrité sont fournies et mises à jour à un coût réduit pour traiter. NGE peut facilement être mis en application avec FlexVPN, qui fournit le chiffrement de norme de la suite B.

Les informations supplémentaires sur l'implémentation de Cisco de la suite B peuvent être trouvées au [cryptage de la deuxième génération](#).