Configuration d'un tunnel IKEv2 site à site entre deux ASA à l'aide d'échanges de clés multiples IKEv2

Table des matières

- Conditions préalables
  - Exigences
  - Composants utilisés
  - Limites
  - Licences
- Informations générales
  - Besoin d'échanges de clés supplémentaires
- Configurer
  - Diagramme du réseau
  - Configuration ASA
    - Configurer les interfaces ASA
    - Configurez la stratégie IKEv2 avec l'échange de clés multiples et activez IKEv2 sur l'interface externe
    - Configuration du groupe de tunnels
    - Configuration du trafic intéressant et ACL de chiffrement
    - Configuration d'une NAT d'identité (facultatif)
    - Configuration de la proposition IPSec IKEv2
    - Configurer une carte de chiffrement et la lier à l'interface
  - Configuration finale ASA locale
  - Configuration finale d'ASA distant
- Vérifier
- Dépannage

Introduction

Ce document décrit comment configurer une connexion VPN de site à site IKEv2 entre deux Cisco ASA utilisant des échanges de clés multiples IKEv2.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil de sécurité adaptatif Cisco (ASA)
- Concepts généraux d'IKEv2

Composants utilisés

Les informations contenues dans ce document sont basées sur les Cisco ASA exécutant la version 9.20.1.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Limites

L'échange de clés multiples IKEv2 présente les limitations suivantes :

- Pris en charge sur l'interface CLI ASA uniquement
- Pris en charge sur les périphériques multicontextes et haute disponibilité
- Non pris en charge sur les périphériques en cluster

Licences

Les conditions de licence sont les mêmes que pour le VPN site à site sur les ASA.

Informations générales

Besoin d'échanges de clés supplémentaires

L'arrivée des gros ordinateurs quantiques présente un risque important pour les systèmes de sécurité, en particulier ceux qui utilisent la cryptographie à clé publique. Les méthodes cryptographiques que l'on pensait très difficiles pour les ordinateurs ordinaires peuvent être facilement brisées par les ordinateurs quantiques. Il est donc nécessaire de passer à de nouvelles méthodes de résistance quantique, également appelées algorithmes de cryptographie post-quantique (PQC). L'objectif est d'améliorer la sécurité des communications IPsec en utilisant plusieurs échanges de clés. Cela implique de combiner un échange de clés traditionnel avec un

échange post-quantique. Cette approche garantit que l'échange qui en résulte est au moins aussi puissant que l'échange de clés traditionnel, offrant ainsi une couche de sécurité supplémentaire.

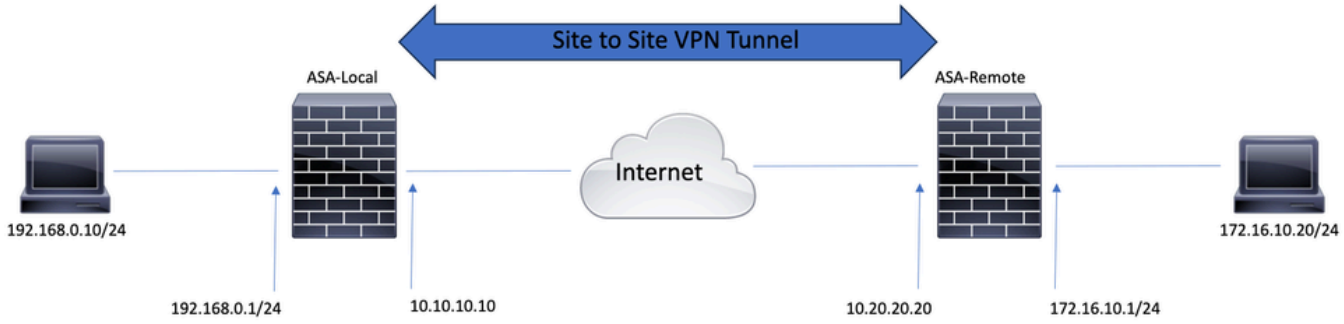
L'objectif est d'améliorer IKEv2 en ajoutant la prise en charge de plusieurs échanges de clés. Ces échanges de clés supplémentaires peuvent gérer des algorithmes qui sont à l'abri des menaces quantiques. Pour échanger des informations sur ces clés supplémentaires, un nouveau type de message appelé Échange intermédiaire est introduit. Ces échanges de clés sont négociés à l'aide de la méthode IKEv2 normale, via la charge utile SA.

Configurer

Cette section décrit les configurations ASA.

Diagramme du réseau

Le présent document utilise cette configuration de réseau :



Configuration ASA

Configurer les interfaces ASA

Si les interfaces ASA ne sont pas configurées, assurez-vous de configurer au moins les adresses IP, les noms d'interface et les niveaux de sécurité :

```
interface GigabitEthernet0/0
nameif outside
```

```
security-level 0
ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
```



Remarque : Assurez-vous qu'il existe une connectivité aux réseaux internes et externes, en particulier à l'homologue distant utilisé pour établir un tunnel VPN site à site. Vous pouvez utiliser un message ping pour vérifier la connectivité de base.

Configurez la stratégie IKEv2 avec l'échange de clés multiples et activez IKEv2 sur l'interface externe

Afin de configurer les stratégies IKEv2 pour ces connexions, entrez ces commandes :

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

D'autres transformations d'échange de clés peuvent être configurées sous `crypto ikev2 policy` à l'aide de la commande `additional-key-exchange` . Un total de sept transformations d'échange supplémentaires peut être configuré. Dans cet exemple, deux transformations d'échange supplémentaires ont été configurées (à l'aide des groupes DH 21 et 31).

```
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```

La stratégie IKEv2 finale ressemble à ceci :

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
```

```
prf sha256
lifetime seconds 86400
additional-key-exchange 1
 key-exchange-method 21
additional-key-exchange 2
 key-exchange-method 31
```



Remarque : Une correspondance de stratégie IKEv2 existe lorsque les deux stratégies des deux homologues contiennent les mêmes valeurs d'authentification, de chiffrement, de hachage, de paramètre Diffie-Hellman et de paramètre d'échange de clé supplémentaire.

Vous devez activer IKEv2 sur l'interface qui termine le tunnel VPN. Il s'agit généralement de l'interface externe (ou Internet). Afin d'activer IKEv2, entrez la commande `crypto ikev2 enable outside` en mode de configuration globale.

Configuration du groupe de tunnels

Pour un tunnel de site à site, le type de profil de connexion est IPSec-l2l. Afin de configurer la clé prépartagée IKEv2, entrez ces commandes :

```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

Configuration du trafic intéressant et ACL de chiffrement

L'ASA utilise des listes de contrôle d'accès (ACL) afin de différencier le trafic qui doit être protégé par cryptage IPSec du trafic qui ne nécessite pas de protection. Il protège les paquets sortants qui correspondent à un moteur de contrôle des applications (ACE) et veille à ce que les paquets entrants qui correspondent à un permis ACE soient protégés.

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
```

access-list asa-vpn extended permit ip object-group local-network object-group remote-network

---



Remarque : L'homologue VPN doit avoir la même liste de contrôle d'accès dans un format en miroir.

Configuration d'une NAT d'identité (facultatif)

Généralement, une NAT d'identité est nécessaire afin d'empêcher le trafic intéressant d'atteindre la NAT dynamique. La NAT d'identité qui est configurée dans ce cas est :

nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup

Configuration de la proposition IPSec IKEv2

La proposition IPSec IKEv2 est utilisée pour définir un ensemble d'algorithmes de chiffrement et d'intégrité afin de protéger le trafic de données. Cette proposition doit correspondre aux deux homologues VPN afin de créer une SA IPSec avec succès. Les commandes utilisées dans ce cas sont les suivantes :

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

Configurer une carte de chiffrement et la lier à l’interface

Une crypto-carte combine toutes les configurations requises et doit nécessairement contenir :

- Une liste d’accès correspondant au trafic qui doit être chiffré (communément appelée ACL de chiffrement)
- L’identification des homologues;
- Au moins une proposition IPSec IKEv2

La configuration utilisée ici est la suivante :

```
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
```

La dernière partie consiste à appliquer cette crypto-carte à l'interface externe (publique) à l'aide de la commande `crypto map outside_map interface outside`.

Configuration finale ASA locale

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.255.0
!
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
!
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0
!
access-list asa-vpn extended permit ip object-group local-network object-group remote-network
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
!
```

```
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```

Configuration finale d'ASA distant

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.20.20.20 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 172.16.10.1 255.255.255.0
!
crypto ikev2 policy 10
encryption aes-256
integrity sha256
group 20
prf sha256
lifetime seconds 86400
additional-key-exchange 1
key-exchange-method 21
additional-key-exchange 2
key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.10.10.10 type ipsec-l2l
tunnel-group 10.10.10.10 ipsec-attributes
ikev2 remote-authentication pre-shared-key cisco
ikev2 local-authentication pre-shared-key cisco
!
object-group network local-network
network-object 172.16.10.0 255.255.255.0
!
object-group network remote-network
network-object 192.168.0.0 255.255.255.0
!
access-list asa-vpn extended permit ip object-group local-network object-group remote-network
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
protocol esp encryption aes-256
protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.10.10.10
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
```

crypto map outside_map interface outside

Remarque : La liste de contrôle d’accès est au format miroir et les clés prépartagées sont identiques aux deux extrémités.

Vérifier

Avant de vérifier si le tunnel est actif et s'il passe le trafic, vous devez vous assurer que le trafic intéressant est envoyé aux ASA.

Remarque : Le traceur de paquets a été utilisé afin de simuler le flux de trafic. Cela peut être fait en utilisant la commande packet-tracer ; packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11 détaillé sur le Local-ASA.

Afin de valider les échanges de clés supplémentaires, vous pouvez utiliser la commande show crypto ikev2 sa. Comme le montre le résultat, vous pouvez vérifier les paramètres AKE afin de valider les algorithmes d'échange sélectionnés.

<#root>

Local-ASA# show crypto ikev2 sa

IKEv2 SAs:

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

Tunnel-id Local Remote fvrf/ivrf Status Role
246015 10.10.10.10/500 10.20.20.20/500 READY INITIATOR
Encr: AES-CBC, keysize: 256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Additional Key Exchange Group:

AKE1: 21 AKE2: 31

```
      Life/Active Time: 86400/7 sec
Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 172.16.10.0/0 - 172.16.10.255/65535
          ESP spi in/out: 0xf41ca3b5/0xda0e693b
```

Dépannage

Les débogages mentionnés peuvent être utilisés pour dépanner le tunnel IKEv2 :

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
```



Remarque : Si vous souhaitez dépanner un seul tunnel (ce qui doit être le cas si le périphérique est en production), vous devez activer les débogages conditionnellement en utilisant la commande debug crypto condition peer X.X.X.X.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.