VPN IPsec de LAN à LAN

Un VPN de LAN à LAN connecte des réseaux dans différents emplacements géographiques.

Vous pouvez créer des connexions IPsec de LAN à LAN avec des homologues Cisco et des homologues tiers conformes à toutes les normes pertinentes. Ces homologues peuvent avoir n'importe quelle combinaison d'adresses IPv4 et IPv6 internes et externes.

L'ASA ne permet pas au trafic d'origine locale autre que le message ping de passer par le tunnel VPN.

Ce chapitre décrit comment établir une connexion VPN de LAN à LAN.

Résumé de la configuration

Cette section fournit un résumé de l'exemple de configuration LAN-à-LAN décrit dans ce chapitre. Les sections ultérieures fournissent des instructions détaillées.

```
hostname(config)# interface ethernet0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)# group 2
hostname(config-ikev1-policy)# lifetime 43200
hostname(config)# crypto ikev1 enable outside
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)# # encryption aes
hostname(config-ikev2-policy)# group 2
hostname(config-ikev12-policy)# prf sha
```

```
hostname(config-ikev2-policy)# lifetime 43200
hostname(config)# crypto ikev2 enable outside
hostname(config)#  crypto ipsec ikev1 transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)# protocol esp encryption aes
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1 pre-shared-key 44kkaol59636jnfx
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set ikev1 transform-set FirstSet
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)# crypto map abcmap interface outside
hostname(config)# write memory
```

Configurer le VPN de site à site en mode de contexte multiple

Suivez ces étapes pour permettre la prise en charge de site à site en mode multi-contexte. En effectuant ces étapes, vous pouvez voir comment l'affectation des ressources se décompose.

Procédure

Étape 1 Pour configurer le VPN en mode multi-contexte, configurez une classe de ressources et choisissez les licences VPN dans le cadre des ressources autorisées. La « configuration d'une classe pour la gestion des ressources » présente ces étapes de configuration. Voici un exemple de configuration :

```
class ctx1
 limit-resource VPN Burst Other 100
 limit-resource VPN Other 1000
```

Étape 2 Configurez un contexte et faites-en membre de la classe configurée qui autorise les licences VPN. Voici un exemple de configuration :

```
context context1
 member ctx1
 allocate-interface GigabitEthernet3/0.2
 allocate-interface GigabitEthernet3/1.2
 allocate-interface Management0/0
 config-url disk0:/sm_s2s_ik1_ip4_no_webvpn.txt
 join-failover-group 1
```

Étape 3 Configurez les profils de connexion, les politiques, les cartes de chiffrement, etc., comme vous le feriez avec une configuration VPN de site à site en mode contexte unique.

Interfaces de configuration

Un ASA comporte au moins deux interfaces, appelées ici outside et inside. En règle générale, l'interface externe est connectée à l'Internet public, tandis que l'interface interne est connectée à un réseau privé et est protégée contre tout accès public.

Pour commencer, configurez et activez deux interfaces sur l'ASA. Attribuez ensuite un nom, une adresse IP et un masque de sous-réseau. Vous pouvez également configurer son niveau de sécurité, sa vitesse et son fonctionnement en duplex sur l'appareil de sécurité.

Remarque L'adresse de l'interface externe de l'ASA (pour IPv4 et IPv6) ne peut pas chevaucher l'espace d'adresse du côté privé.

Procédure

Étape 1 Pour passer en mode de configuration d'interface, en mode de configuration globale, saisissez la commande **interface** avec le nom par défaut de l'interface à configurer. Dans l'exemple suivant, l'interface est ethernet0.

```
hostname(config)# interface ethernet0/0
hostname(config-if)#
```

Étape 2 Pour définir l'adresse IP et le masque de sous-réseau de l'interface, saisissez la commande **ip address**. Dans l'exemple suivant, l'adresse IP est 10.10.4.100 et le masque de sous-réseau est 255.255.0.0.

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

Étape 3 Pour nommer l'interface, entrez la commande **nameif**, maximum de 48 caractères. Vous ne pourrez pas modifier ce nom ultérieurement. Dans l'exemple suivant, le nom de l'interface ethernet0 est externe.

```
hostname(config-if)# nameif outside
hostname(config-if)##
```

Étape 4 Pour activer l'interface, saisissez la version **no** de la commande **shutdown**. Par défaut, les interfaces sont désactivées.

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

Étape 5 Pour enregistrer vos modifications, entrez la commande **write memory** :

```
hostname(config-if)# write memory
hostname(config-if)#
```

Étape 6 Pour configurer une deuxième interface, utilisez la même procédure.

Configurer la politique ISAKMP et activer ISAKMP sur l'interface externe

ISAKMP est le protocole de négociation qui permet à deux hôtes de s'accorder sur la façon de créer une association de sécurité IPsec (SA). Il fournit un cadre commun pour convenir du format des attributs SA. Cela inclut la négociation avec l'homologue au sujet de la SA et la modification ou la suppression de la SA. ISAKMP sépare la négociation en deux étapes : la phase 1 et la phase 2. La phase 1 crée le premier tunnel, qui protège les messages de négociation ISAKMP ultérieurs. La phase 2 crée le tunnel qui protège les données.

IKE utilise ISAKMP pour configurer la SA pour l'utilisation d'IPsec. IKE crée les clés cryptographiques utilisées pour authentifier les homologues.

L'ASA prend en charge IKEv1 pour les connexions de l'ancien client VPN Cisco et IKEv2 pour le client VPN AnyConnect.

Pour définir les termes des négociations ISAKMP, vous créez une politique IKE, qui comprend les éléments suivants :

- Le type d'authentification requis pour l'homologue IKEv1, soit signature RSA à l'aide de certificats, soit clé prépartagée (PSK).
- Une méthode de chiffrement pour protéger les données et garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Un groupe Diffie-Hellman pour déterminer la force de l'algorithme de détermination de la clé de chiffrement. L'ASA utilise cet algorithme pour dériver les clés de chiffrement et de hachage.
- Pour IKEv2, une fonction pseudo-aléatoire (PRF) distincte est utilisée comme algorithme pour dériver le matériel de clé et effectuer les opérations de hachage nécessaires au chiffrement du tunnel IKEv2.
- Une limite de temps pendant laquelle le périphérique utilise une clé de chiffrement avant de la remplacer.

Avec les politiques IKEv1, pour chaque paramètre, vous définissez une valeur. Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'authentification pour une seule politique. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Cela vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les combinaisons autorisées au lieu d'avoir besoin d'envoyer chaque combinaison autorisée individuellement, comme avec IKEv1.

Les sections suivantes fournissent des procédures pour créer des politiques IKEv1 et IKEv2 et les activer sur une interface :

- Configurer les politiques ISAKMP pour les connexions IKEv1, à la page 4
- Configurer les politiques ISAKMP pour les connexions IKEv2, à la page 6

Configurer les politiques ISAKMP pour les connexions IKEv1

Pour configurer les politiques ISAKMP pour les connexions IKEv1, utilisez la commande de priorité **crypto ikev1 policy** pour passer en mode de configuration de politique IKEv1 où vous pouvez configurer les paramètres IKEv1.

Procédure

Étape 1 Entrez en mode de configuration de politique IPsec IKEv1. Par exemple :

```
hostname(config)# crypto ikev1 policy 1
hostname(config-ikev1-policy)#
```

Étape 2 Définissez la méthode d'authentification. L'exemple suivant configure une clé prépartagée :

```
hostname(config-ikev1-policy)# authentication pre-share
hostname(config-ikev1-policy)#
```

Étape 3 Choisissez la méthode de chiffrement. L'exemple suivant configure l' :

```
hostname(config-ikev1-policy)# encryption aes
hostname(config-ikev1-policy)#
```

Étape 4 Définissez la méthode HMAC. L'exemple suivant configure SHA-1 :

```
hostname(config-ikev1-policy)# hash sha
hostname(config-ikev1-policy)#
```

Étape 5 Définissez le groupe Diffie-Hellman. L'exemple suivant configure le groupe 14 :

```
hostname(config-ikev1-policy)# group 14
hostname(config-ikev1-policy)#
```

Étape 6 Définissez la durée de vie de la clé de chiffrement. L'exemple suivant configure 43 200 secondes (12 heures) :

```
hostname(config-ikev1-policy)# lifetime 43200
hostname(config-ikev1-policy)#
```

Étape 7 Activez IKEv1 sur l'interface nommée outside en mode contexte unique ou multiple :

```
hostname(config)# crypto ikev1 enable outside
hostname(config)#
```

Étape 8 Pour enregistrer vos modifications, entrez la commande **write memory** :

```
hostname(config)# write memory
hostname(config)#
```

Configurer les politiques ISAKMP pour les connexions IKEv2

Pour configurer les politiques ISAKMP pour les connexions IKEv2, utilisez la commande de priorité **crypto ikev2 policy** pour passer en mode de configuration de politique IKEv2 où vous pouvez configurer les paramètres IKEv2.

Procédure

Étape 1 Entrez en mode de configuration de politique IPsec IKEv2. Par exemple :

```
hostname(config)# crypto ikev2 policy 1
hostname(config-ikev2-policy)#
```

Étape 2 Choisissez la méthode de chiffrement. L'exemple suivant configure AES :

```
hostname(config-ikev2-policy)# encryption aes
hostname(config-ikev2-policy)#
```

Étape 3 Définissez le groupe Diffie-Hellman. L'exemple suivant configure le groupe 15 :

```
hostname(config-ikev2-policy)# group 15
hostname(config-ikev2-policy)#
```

Étape 4 Définissez la fonction pseudo-aléatoire (PRF) utilisée comme algorithme pour générer le matériel de clé et les opérations de hachage nécessaires au chiffrement du tunnel IKEv2. L'exemple suivant configure SHA-1 (une variante de HMAC) :

```
hostname(config-ikev12-policy)# prf sha
hostname(config-ikev2-policy)#
```

Étape 5 Définissez la durée de vie de la clé de chiffrement. L'exemple suivant configure 43 200 secondes (12 heures) :

```
hostname(config-ikev2-policy)# lifetime seconds 43200
hostname(config-ikev2-policy)#
```

Étape 6 Activez IKEv2 sur l'interface nommée outside :

```
hostname(config)# crypto ikev2 enable outside
hostname(config)#
```

Étape 7 Pour enregistrer vos modifications, entrez la commande **write memory** :

```
hostname(config)# write memory
hostname(config)#
```

Plusieurs échanges de clés pour IKEv2

IKEv2 utilise des groupes Diffie-Hellman (DH) pour établir un secret partagé entre un initiateur et un répondeur. IKEv2 prend en charge les échanges de clés supplémentaires pour sécuriser la communication IPsec contre

les attaques d'ordinateurs quantiques. Chaque échange utilise des groupes DH différents. Le secret partagé calculé pour la configuration SA est une combinaison de toutes les clés dérivées de chaque échange. Une SA IKE est établie après les multiples échanges de clés entre les homologues IKE.

L'ASA utilise sept nouveaux types de transformation pour les échanges de clés multiples :

- Échange de clé supplémentaire : valeur IANA 6
- Échange de clé supplémentaire : valeur IANA 7
- Échange de clé supplémentaire : valeur IANA 8
- Échange de clé supplémentaire : valeur IANA 9
- Échange de clé supplémentaire : valeur IANA 10
- Échange de clé supplémentaire : valeur IANA 11
- Échange de clé supplémentaire : valeur IANA 12

Vous pouvez configurer un maximum de sept échanges de clés multiples. Pour chaque échange de clés supplémentaire que vous configurez, vous devez préciser les groupes DH. L'ASA chiffre les échanges de clés intermédiaires à l'aide des clés dérivées de l'échange précédent. Si les homologues entre l'initiateur et le répondeur ne s'accordent pas avec un groupe DH, la négociation échoue et une notification d'erreur **NO_PROPOSAL_CHOSEN** est envoyée à l'initiateur. Vous pouvez également configurer la transformation comme nulle. Ce faisant, l'échange de clés n'a pas lieu.

Pour un initiateur, si la méthode d'échange de clés est configurée à **aucune** pour un échange de clés supplémentaire *n* :

- Le répondeur peut choisir la méthode d'échange de clés comme **none** pour l'échange de clés supplémentaire *n*.
- L'échange de clés supplémentaire est optionnel.

Pour une négociation de proposition réussie, toutes les transformations de la proposition de l'initiateur doivent correspondre aux transformations du répondeur.

Dans l'exemple suivant pour un initiateur :

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 5
key-exchange-method none
```

Le répondeur doit avoir un échange de clé supplémentaire 5 pour que la proposition corresponde.

Si l'homologue ne prend pas en charge l'échange de clé supplémentaire, l'un des événements suivants se produit :

- Si l'initiateur a une autre proposition IKEv2 qui correspond à la proposition du répondeur, une SA IKEv2 est établie.
- L'homologue traite tout type de transformation d'échange de clés supplémentaire dans le message d'échange IKE_SA_INIT comme un type inconnu et ignore ces propositions. La négociation échoue et une notification d'erreur **NO_PROPOSAL_CHOSEN** est envoyée à l'initiateur.

Pour en savoir plus sur cette fonctionnalité, consultez la RFC 9242.

Lignes directrices et limites relatives aux échanges de clés multiples, IKEv2

- Vous pouvez avoir un maximum de sept échanges de clés multiples.
- Vous ne pouvez pas utiliser le même groupe DH dans les échanges de clés suivants.

Pour cette fonctionnalité, l'ASA ne prend pas en charge :

- IKEv1
- Combinaison d'un échange de clés classique et d'un échange de clés fondé sur un algorithme post-quantique.
- VPN d'accès à distance. Seuls les VPN de site à site prennent en charge les échanges de clés multiples IKEv2.
- Mise en grappes

Vérifier les configurations d'échanges de clés multiples IKEv2

Utilisez les commandes show suivantes pour afficher ou vérifier les configurations d'échanges de clés multiples IKEv2 :

- **show running-config crypto ikev2**

```
crypto ikev2 policy 1
encryption aes
integrity sha256
group 14
prf sha256
lifetime seconds 120
additional-key-exchange 1
key-exchange-method 21 31
additional-key-exchange 2
key-exchange-method 20 21
...
```

- **show crypto ikev2 sa detail**

```
IKEv2 SAs:
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id Local Remote fvrf/ivrf Status Role
41567725 192.168.15.1/500 192.168.15.2/500 READY INITIATOR
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:14, Auth sign: PSK, Auth verify: PSK
Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6: 15
AKE7: 14
Life/Active Time: 120/5 sec
Session-id: 4
Status Description: Negotiation done
Local spi: 6BB6B7BFA0BAADF4 Remote spi: 7030C7xxx xxxxxxE9DBDE77EB
Local id: 192.168.15.1
Remote id: 192.168.15.2
Local req mess id: 9 Remote req mess id: 0
Local next mess id: 9 Remote next mess id: 0
Local req queued: 9 Remote req queued: 0
Local window: 1 Remote window: 1
DPD configured for 10 seconds, retry 2
NAT-T is not detected
IKEv2 Fragmentation Configured MTU: 576 bytes, Overhead: 28 bytes, Effective MTU: 548
```

```
bytes
Parent SA Extended Status:
Delete in progress: FALSE
Marked for delete: FALSE
Child sa: local selector 20.0.0.0/0 - 20.0.0.255/65535
remote selector 30.0.0.0/0 - 30.0.0.255/65535
ESP spi in/out: 0x4a7d5da2/0x56a28fa8
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Créer un ensemble de transformation IKEv1

Un ensemble de transformation IKEv1 combine une méthode de chiffrement et une méthode d'authentification. Lors de la négociation de l'association de sécurité IPsec avec ISAKMP, les homologues conviennent d'utiliser un ensemble de transformation particulier pour protéger un flux de données particulier. L'ensemble de transformation doit être le même pour les deux homologues.

Un ensemble de transformation protège les flux de données pour l'ACL spécifiée dans l'entrée de carte de chiffrement associée. Vous pouvez créer des ensembles de transformations dans la configuration ASA, puis spécifier un maximum de 11 parmi ceux-ci dans une carte de chiffrement ou une entrée de carte de chiffrement dynamique.

Le tableau ci-dessous répertorie les méthodes de chiffrement et d'authentification valides.

Tableau 1 : Méthodes de chiffrement et d'authentification valides

Méthodes de chiffrement valides	Méthodes d'authentification valides
	esp-sha-hmac (par défaut)
esp-aes (chiffrement 128 bits) (par défaut)	
esp-aes-192	
esp-aes-256	
esp-null	

Le mode tunnel est la méthode habituelle pour mettre en œuvre IPsec entre deux ASAs connectés sur un réseau non fiable, tel qu'Internet. Le mode tunnel est la configuration par défaut et ne nécessite aucune configuration.

Pour configurer un ensemble de transformations, effectuez les tâches de site à site suivantes en mode contexte unique ou multiple :

Procédure

Étape 1 En mode de configuration globale, entrez la commande **crypto ipsec ikev1 transform-set** . L'exemple suivant configure un ensemble de transformation avec le nom FirstSet, le chiffrement esp-aes, , et l'authentification esp-sha-hmac . La syntaxe est la suivante :

esp-sha-hmac (par défaut)

crypto ipsec ikev1 transform-set *transform-set-nameencryption-method authentication-method*

```
hostname(config)#
crypto ipsec transform-set FirstSet esp-aes esp-sha-hmac
hostname(config)#
```

Étape 2 Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```

Créer une proposition IKEv2

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'authentification, et plusieurs algorithmes d'intégrité pour une seule politique. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Cela vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les combinaisons autorisées au lieu d'avoir besoin d'envoyer chaque combinaison autorisée individuellement, comme avec IKEv1.

Le tableau ci-dessous répertorie les méthodes de chiffrement et d'authentification IKEv2 valides.

Tableau 2 : Méthodes de chiffrement et d'intégrité IKEv2 valides

Méthodes de chiffrement valides	Méthodes d'intégrité valides
	sha (par défaut)
aes (par défaut) - AES avec une clé de 128 bits.	
aes-192	
aes-256	

Pour configurer une proposition IKEv2, effectuez les tâches suivantes en mode contexte unique ou multiple :

Procédure

Étape 1 En mode de configuration globale, utilisez la commande **crypto ipsec ikev2 ipsec-proposal** pour passer en mode de configuration de proposition ipsec où vous pouvez spécifier plusieurs types de chiffrement et d'intégrité pour la proposition. Dans cet exemple, secure est le nom de la proposition :

```
hostname(config)# crypto ipsec ikev2 ipsec-proposal secure
hostname(config-ipsec-proposal)#
```

Étape 2 Saisissez ensuite un protocole et des types de chiffrement. ESP est le seul protocole pris en charge. Par exemple :

```
hostname(config-ipsec-proposal)# protocol esp encryption aes

hostname(config-ipsec-proposal)#
```

Étape 3 Saisissez un type d'intégrité. Par exemple :

```
hostname(config-ipsec-proposal)# protocol esp integrity sha-1
hostname(config-ipsec-proposal)#
```

Étape 4 Enregistrez vos modifications.

Configurer une ACL

L'ASA utilise des listes de contrôle d'accès pour contrôler l'accès au réseau. Par défaut, l'appareil de sécurité adaptatif refuse tout le trafic. Vous devez configurer une liste de contrôle d'accès qui autorise le trafic. Pour en savoir plus, consultez « Renseignements sur les listes de contrôle d'accès » dans le guide de configuration sur les opérations générales.

Les listes de contrôle d'accès que vous configurez pour ces connexions de contrôle VPN de réseau local (LAN) à réseau local (LAN) sont basées sur les adresses IP source et de destination traduite et, éventuellement, sur les ports. Configurez des listes de contrôle d'accès qui sont symétriques des deux côtés de la connexion.

Une liste de contrôle d'accès pour le trafic VPN utilise l'adresse traduite.

Remarque Pour plus d'informations sur la configuration d'une liste de contrôle d'accès avec un filtre VPN, consultez Préciser un réseau VLAN pour l'accès à distance ou appliquer une règle de contrôle d'accès unifiée à la stratégie de groupe.

Procédure

Étape 1 Entrez la commande **access-list extended**.

access-list *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask*

L'exemple suivant configure une liste de contrôle d'accès nommée l2l_list qui permet au trafic des adresses IP du réseau 192.168.0.0 d'accéder au réseau 150.150.0.0.

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0 150.150.0.0
 255.255.0.0
hostname(config)#
```

Étape 2 Configurez une liste de contrôle d'accès pour l'ASA de l'autre côté de la connexion qui reflète l'ACL.

Les sous-réseaux qui sont définis dans une liste de contrôle d'accès dans une carte de chiffrement ou dans deux listes de contrôle d'accès de chiffrement différentes qui sont associées à la même carte de chiffrement ne doivent pas se chevaucher.

Dans l'exemple suivant, l'invite pour l'homologue est hostname2.

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0 192.168.0.0
 255.255.0.0
hostname(config)#
```

Définition d'un groupe de tunnels

Un groupe de tunnels est un ensemble d'enregistrements qui contiennent des politiques de connexion de tunnel. Vous configurez un groupe de tunnels pour identifier les serveurs AAA, préciser les paramètres de connexion et définir une stratégie de groupe par défaut. L'ASA stocke les groupes de tunnels en interne.

Il existe deux groupes de tunnels par défaut dans l'ASA : DefaultRAGroup, qui est le groupe de tunnels d'accès à distance IPsec par défaut, et DefaultL2Lgroup, qui est le groupe de tunnels IPsec de LAN à LAN par défaut. Vous pouvez les modifier, mais pas les supprimer.

La principale différence entre les versions IKE 1 et 2 réside dans la méthode d'authentification qu'elles autorisent. IKEv1 n'autorise qu'un seul type d'authentification aux deux extrémités du VPN (c'est-à-dire clé prépartagée ou certificat). Cependant, IKEv2 permet la configuration de méthodes d'authentification asymétriques (c'est-à-dire authentification par clé prépartagée pour l'initiateur, mais authentification par certificat pour le répondeur) à l'aide d'interfaces de ligne de commande d'authentification locales et distantes distinctes. Par conséquent, avec IKEv2, vous avez une authentification asymétrique, dans laquelle un côté s'authentifie avec un identifiant et l'autre côté utilise un autre identifiant (une clé prépartagée ou un certificat).

Vous pouvez également créer un ou plusieurs nouveaux groupes de tunnels en fonction de votre environnement. L'ASA utilise ces groupes pour configurer les paramètres de tunnel par défaut pour les groupes de tunnels d'accès à distance et de LAN à LAN lorsqu'aucun groupe de tunnels spécifique n'est identifié lors de la négociation du tunnel.

Pour établir une connexion de base de LAN à LAN, vous devez définir deux attributs pour un groupe de tunnels :

- Définissez le type de connexion sur IPsec de LAN à LAN.
- Configurez une méthode d'authentification pour l'adresse IP (c'est-à-dire une clé prépartagée pour IKEv1 et IKEv2).

Procédure

Étape 1 Pour définir le type de connexion sur IPsec de LAN à LAN, entrez la commande **tunnel-group**.

La syntaxe est **tunnel-group** *nom* **type***type*, où nom est le nom que vous attribuez au groupe de tunnels, et type est le type de tunnel. Les types de tunnels tels que vous les saisissez dans l'interface de ligne de commande sont les suivants :

- **remote-access** (accès à distance IPsec, SSL et SSL sans client)
- **ipsec-l2l** (IPsec de LAN à LAN)

Dans l'exemple suivant, le nom du groupe de tunnels est l'adresse IP de l'homologue de LAN à LAN, 10.10.4.108.

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec-l2l
hostname(config)#
```

Remarque
Les groupes de tunnels de LAN à LAN dont les noms ne sont pas des adresses IP peuvent être utilisés uniquement si la méthode d'authentification du tunnel est Digital Certificates (Certificats numériques) et/ou si l'homologue est configuré pour utiliser le Aggressive Mode (Mode agressif).

Étape 2 Pour définir la méthode d'authentification afin d'utiliser une clé prépartagée, passez en mode ipsec-attributes, puis saisissez la commande **ikev1pre-shared-key** pour créer la clé prépartagée. Vous devez utiliser la même clé prépartagée sur les deux ASA pour cette connexion de LAN à LAN.

La clé est une chaîne alphanumérique de 1 à 128 caractères.

Dans l'exemple suivant, la clé prépartagée IKEv1 est 44kkaol59636jnfx :

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-tunnel-ipsec)# ikev1-pre-shared-key 44kkaol59636jnfx
```

Étape 3 Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```

Pour vérifier que le tunnel est opérationnel et en cours d'exécution, utilisez la commande **show vpn-sessiondb summary**, **show vpn-sessiondb detail l2l**, ou **show crypto ipsec sa**.

Créer une carte de chiffrement et l'appliquer à une interface

Les entrées de carte de chiffrement regroupent les différents éléments des associations de sécurité IPsec, notamment les suivants :

- Quel trafic IPsec doit protéger, que vous définissez dans une liste de contrôle d'accès.

- Où envoyer le trafic protégé par IPsec, en identifiant l'homologue.
- La sécurité IPsec qui s'applique à ce trafic, laquelle est précisée par un ensemble de transformation.
- L'adresse locale pour le trafic IPsec, que vous identifiez en appliquant la carte de chiffrement à une interface.

Pour qu'IPsec réussisse, les deux homologues doivent avoir des entrées de carte de chiffrement avec des configurations compatibles. Pour que deux entrées de carte de chiffrement soient compatibles, elles doivent, au minimum, répondre aux critères suivants :

- Les entrées de la carte de chiffrement doivent contenir des listes de contrôle d'accès de chiffrement compatibles (par exemple, listes de contrôle d'accès d'image miroir). Si l'homologue qui répond utilise des cartes de chiffrement dynamiques, les entrées de la liste de contrôle d'accès de chiffrement de l'ASA doivent être « autorisées » par la liste de contrôle d'accès crypto de l'homologue.
- Les entrées de la carte de chiffrement doivent chacune identifier l'autre homologue (sauf si l'homologue répondeur utilise une carte de chiffrement dynamique).
- Les entrées de carte de chiffrement doivent avoir au moins un ensemble de transformation en commun.

Si vous créez plusieurs entrées de carte de chiffrement pour une interface donnée, utilisez le numéro de séquence (seq-num) de chaque entrée pour les classer : plus le numéro de séquence est faible, plus la priorité est élevée. Sur l'interface à laquelle la carte de chiffrement est appliquée, l'ASA évalue d'abord le trafic en fonction des entrées des cartes de priorité plus élevée.

Si l'injection de route inverse (RRI) est appliquée à une carte de chiffrement, cette carte doit être propre à une seule interface de l'ASA. En d'autres termes, la même carte de chiffrement ne peut pas être appliquée à plusieurs interfaces. Si plus d'une carte de chiffrement est appliquée à plusieurs interfaces, les routes risquent de ne pas être supprimées correctement. Si plusieurs interfaces nécessitent une carte de chiffrement, chacune doit utiliser une carte définie de manière unique.

Créez plusieurs entrées de carte de chiffrement pour une interface donnée si l'une des conditions suivantes s'applique :

- Chaque homologue gère différents flux de données.
- Vous souhaitez appliquer une sécurité IPsec différente à différents types de trafic (vers le même ou des homologues distincts), par exemple, si vous souhaitez que le trafic entre un ensemble de sous-réseaux soit authentifié et que le trafic entre un autre ensemble de sous-réseaux soit à la fois authentifié et chiffré. Dans ce cas, définissez les différents types de trafic dans deux listes de contrôle d'accès distinctes et créez une entrée de carte de chiffrement distincte pour chaque liste de contrôle d'accès de chiffrement.

Application d'une carte de chiffrement sur plusieurs interfaces

Dans un environnement à double FSI, vous pouvez appliquer une carte de chiffrement aux interfaces externes et de secours de l'ASA. L'option d'origine uniquement n'est pas disponible lorsque vous utilisez cette configuration. Vous devez utiliser Virtual Tunnel Interface (VTI) si vous avez besoin de cette redondance.

Lorsque vous utilisez une carte de chiffrement sur plusieurs interfaces :

- Vous devez avoir un protocole de routage ou un suivi de route.
- Assurez-vous que le côté distant utilise également des protocoles de routage.
- Vous devez choisir avec soin plusieurs interfaces pour une même carte de chiffrement, car l'ASA permet une connexion provenant d'un site distant sur l'interface dont la route est la moins privilégiée.

Pour créer une carte de chiffrement et l'appliquer à l'interface externe en mode de configuration globale, effectuez les étapes suivantes en mode de contexte unique ou multiple :

Procédure

Étape 1 Pour attribuer une ACL à une entrée de carte de chiffrement, saisissez la commande **crypto map match address**.

La syntaxe est **crypto map** map-name seq-num **match address** aclname. Dans l'exemple suivant, le nom de la carte est abcmap, le numéro de séquence est 1 et le nom de l'ACL est **l2l_list**.

```
hostname(config)# crypto map abcmap 1 match address l2l_list
hostname(config)#
```

Étape 2 Pour identifier le ou les homologues de la connexion IPsec, saisissez la commande **crypto map set peer** .

La syntaxe est **crypto map** map-name seq-num **set peer** {ip_address1 | hostname1} [... ip_address10 | hostname10]. Dans l'exemple suivant, le nom d'homologue est 10.10.4.108.

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

Étape 3 Pour spécifier un ensemble de transformation IKEv1 pour une entrée de carte de chiffrement, saisissez la commande **crypto map ikev1 set transform-set** .

La syntaxe est **crypto map** map-name seq-num **ikev1 set transform-set** transform-set-name. Dans l'exemple suivant, le nom de l'ensemble de transformation est FirstSet.

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

Étape 4 Pour préciser une proposition IKEv2 pour une entrée de carte crypto, saisissez la commande crypto map ikev2 set ipsec-proposal :

La syntaxe est **crypto map** map-name seq-num set **ikev2 ipsec-proposal proposal-name**. Dans l'exemple suivant, le nom de la proposition est secure.

La commande **crypto map** vous permet de spécifier plusieurs propositions IPsec pour un seul index de carte. Dans ce cas, plusieurs propositions sont transmises à l'homologue IKEv2 dans le cadre de la négociation, et l'ordre des propositions est déterminé par l'administrateur lors de l'ordonnancement de l'entrée de carte de chiffrement.

Remarque
Si des algorithmes en mode combiné (AES-GCM/GMAC) et en mode normal (tous les autres) existent dans la proposition IPsec, vous ne pouvez pas envoyer une seule proposition à l'homologue. Vous devez avoir au moins deux propositions dans ce cas, une pour le mode combiné et une pour les algorithmes en mode normal.

```
hostname(config)# crypto map abcmap 1 set ikev2 ipsec-proposal secure
hostname(config)#
```

Appliquer les cartes de chiffrement aux interfaces

Vous devez appliquer un ensemble de cartes de chiffrement à chaque interface par laquelle le trafic IPsec passe. L'ASA prend en charge IPsec sur toutes les interfaces. L'application de l'ensemble de cartes de chiffrement à une interface demande à l'ASA d'évaluer tout le trafic de l'interface par rapport à l'ensemble de cartes de chiffrement et d'utiliser la politique précisée lors des négociations de connexion ou d'association de sécurité.

La liaison d'une carte de chiffrement à une interface initialise également les structures de données d'exécution, telles que la base de données des associations de sécurité et la base de données des politiques de sécurité. Lorsque vous modifiez ultérieurement une carte de chiffrement de quelque manière que ce soit, l'ASA applique automatiquement les modifications à la configuration en cours. Il supprime les connexions existantes et les rétablit après avoir appliqué la nouvelle carte de chiffrement.

Pour appliquer la carte de chiffrement configurée à l'interface externe, procédez comme suit :

Procédure

Étape 1 Entrez la commande **crypto map interface**. La syntaxe est **crypto map** map-name **interface** interface-name.

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

Étape 2 Enregistrez vos modifications.

```
hostname(config)# write memory
hostname(config)#
```

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.