IPsec et ISAKMP

À propos de la tunnelisation, d'IPsec et d'ISAKMP

Ce sujet décrit les normes IPsec (Internet Protocol Security) et ISAKMP (Internet Security Association and Key Management Protocol) utilisées pour créer des réseaux privés virtuels (VPN).

La tunnellisation permet d'utiliser un réseau TCP/IP public, comme Internet, pour créer des connexions sécurisées entre des utilisateurs distants et un réseau privé d'entreprise. Chaque connexion sécurisée s'appelle un tunnel.

L'ASA utilise les normes de tunnellisation ISAKMP et IPsec pour créer et gérer les tunnels. ISAKMP et IPsec accomplissent les tâches suivantes :

- Négocier les paramètres du tunnel.
- Établir des tunnels.
- Authentifier les utilisateurs et les données.
- Gérer les clés de sécurité.
- Chiffrer et déchiffrer les données.
- Gérer le transfert de données dans le tunnel.
- Gérer le transfert de données entrant et sortant en tant que point terminal de tunnel ou routeur.

L'ASA fonctionne comme un point terminal de tunnel bidirectionnel. Il peut recevoir des paquets simples du réseau privé, les encapsuler, créer un tunnel et les envoyer à l'autre extrémité du tunnel où ils sont désencapsulés et envoyés à leur destination finale. Il peut également recevoir des paquets encapsulés du réseau public, les désencapsuler et les envoyer à leur destination finale sur le réseau privé.

Présentation d'IPsec

L'ASA utilise IPsec pour les connexions VPN de site à site et offre la possibilité d'utiliser IPsec pour les connexions VPN client à réseau local. Dans la terminologie IPsec, un *homologue* est un client d'accès à distance ou une autre passerelle sécurisée. Pour les deux types de connexion, l'ASA prend officiellement en charge uniquement les homologues Cisco. Comme nous respectons les normes de l'industrie VPN, les ASA peuvent fonctionner avec des homologues d'autres fournisseurs ; toutefois, nous ne les prenons pas en charge.

Lors de l'établissement du tunnel, les deux homologues négocient des associations de sécurité (SA) qui régissent l'authentification, le chiffrement, l'encapsulation et la gestion des clés. Ces négociations comportent deux phases : la première pour établir le tunnel (l'IKE SA) et la seconde pour régir le trafic dans le tunnel (l'IPsec SA).

Un VPN de LAN à LAN connecte des réseaux dans différents emplacements géographiques. Dans les connexions IPsec de site à site, l'ASA peut fonctionner comme initiateur ou répondeur. Dans les connexions client IPsec à réseau local, l'ASA fonctionne uniquement comme répondeur. Les initiateurs proposent des SA ; les répondeurs acceptent, rejettent ou font des contre-propositions, tout cela conformément aux paramètres SA configurés. Pour établir une connexion, les deux entités doivent convenir des SA.

Comprendre les tunnels IPsec

Les tunnels IPsec sont des ensembles de SA que l'ASA établit entre les homologues. Les SA précisent les protocoles et les algorithmes à appliquer aux données sensibles et précisent également le matériel de clé que les homologues utilisent. Les SA IPsec contrôlent la transmission réelle du trafic utilisateur. Les SA sont unidirectionnelles, mais sont généralement établies en paires (entrantes et sortantes).

Les homologues négocient les paramètres à utiliser pour chaque SA. Chaque SA comprend les éléments suivants :

- Ensembles de transformation IKEv1 ou propositions IKEv2
- cartes de chiffrement
- ACL
- Groupes de tunnels
- Politiques de préfragmentation

Survol d'ISAKMP et d'IKE

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. Cette association de sécurité comprend la négociation avec l'homologue au sujet de la SA, ainsi que 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 les éléments de clé et effectuer les opérations de hachage nécessaires au chiffrement du tunnel IKEv2, entre autres.
- Une limite de temps pendant laquelle l'ASA utilise une clé de chiffrement avant de la remplacer.

Avec les politiques IKEv1, vous définissez une valeur pour chaque paramètre. Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'authentification, et plusieurs algorithmes d'intégrité pour une seule politique. L'ASA classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue selon cet ordre. Cet ordonnancement vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les transformations autorisées, au lieu d'envoyer chaque combinaison autorisée comme avec IKEv1.

L'ASA ne prend pas en charge les associations de sécurité multiples (SA) IKEv2. L'ASA accepte actuellement le trafic IPsec entrant uniquement sur la première SA trouvée. Si du trafic IPsec est reçu sur une autre SA, il est abandonné avec le motif `vpn-overlap-conflict`. Plusieurs SA IPsec peuvent résulter de tunnels dupliqués entre deux homologues, ou d'une tunnellisation dissymétrique.

Comprendre les ensembles de transformations IKEv1 et les propositions IKEv2

Un ensemble de transformation IKEv1 ou une proposition IKEv2 est une combinaison de protocoles de sécurité et d'algorithmes qui définissent la façon dont l'ASA protège les données. Pendant les négociations d'une SA IPsec, les homologues doivent identifier un ensemble de transformation ou une proposition identique aux deux extrémités. L'ASA applique ensuite l'ensemble de transformation ou la proposition correspondante afin de créer une SA qui protège les flux de données de l'ACL associée à cette carte de chiffrement.

Avec les ensembles de transformation IKEv1, vous définissez une valeur pour chaque paramètre. Pour les propositions IKEv2, vous pouvez configurer plusieurs types de chiffrement et d'authentification ainsi que plusieurs algorithmes d'intégrité pour une seule proposition. L'ASA classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue selon 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.

L'ASA supprime le tunnel si vous modifiez la définition de l'ensemble de transformation ou de la proposition utilisée pour créer sa SA. Consultez la section Effacer les associations de sécurité, à la page 43 pour obtenir de plus amples renseignements.

Remarque Si vous effacez ou supprimez le seul élément d'un ensemble de transformation ou d'une proposition, l'ASA supprime automatiquement les références de carte de chiffrement qui y sont associées.

À propos de la carte de chiffrement IKEv2 multi-homologues

À partir de la version 9.14(1), ASA IKEv2 prend en charge la carte de chiffrement multi-homologues : lorsqu'un homologue d'un tunnel tombe en panne, IKEv2 tente d'établir le tunnel avec l'homologue suivant dans la liste. Vous pouvez configurer une carte de chiffrement avec un maximum de 10 adresses homologues. Cette prise en charge des homologues multiples par IKEv2 est particulièrement utile lorsque vous migrez depuis IKEv1 avec des cartes de chiffrement multi-homologues.

IKEv2 prend en charge uniquement les cartes de chiffrement bidirectionnelles. Par conséquent, les homologues multiples sont également configurés sur des cartes de chiffrement bidirectionnelles, et celles-ci servent aussi à accepter la demande des homologues qui initient le tunnel.

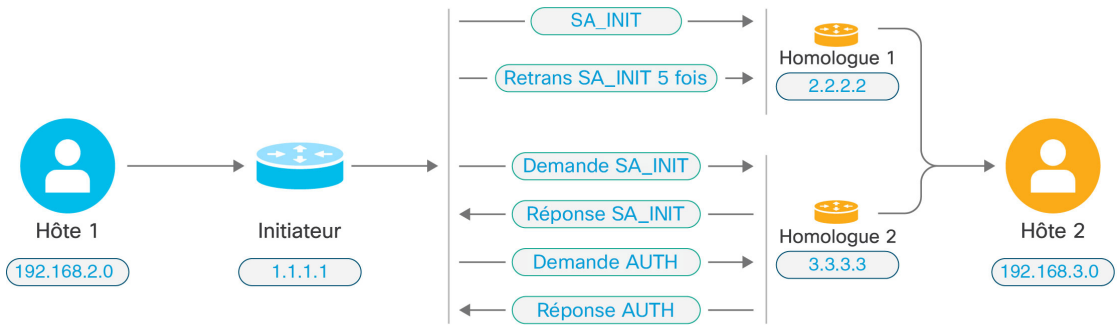
Comportement de l'initiateur IKEv2

IKEv2 initie une session avec un homologue, par exemple Peer1. Si Peer1 est inaccessible après 5 retransmissions SA_INIT, une retransmission finale est envoyée. Cette activité prend environ 2 minutes.

Lorsque Peer1 tombe en panne, le message SA_INIT est envoyé à Peer2. Si Peer2 est également inaccessible, l'établissement de la session est lancé avec Peer3 après 2 minutes.

Une fois que tous les homologues de la liste d'homologues de la carte de chiffrement ont été essayés, IKEv2 relance la session à partir de Peer1 jusqu'à ce qu'une SA soit établie avec l'un des homologues. La figure suivante illustre ce comportement.

Illustration 1 : Flux de processus de l'initiateur



Remarque Un trafic continu est nécessaire pour initier l'IKE SA afin que chaque tentative échouée fasse passer à l'homologue suivant et qu'un homologue accessible finisse par établir la SA. En cas d'interruption du trafic, un déclenchement manuel est nécessaire pour initier l'IKE SA avec l'homologue suivant.

Comportement du répondeur IKEv2

Si le périphérique répondeur de l'IKE SA est configuré avec plusieurs homologues dans la carte de chiffrement, chaque fois qu'une IKE SA est tentée, l'adresse de l'initiateur de l'IKE SA est validée par rapport à celle de l'homologue actif courant dans la carte crypto.

Par exemple, si l'homologue actif courant dans la carte de chiffrement, utilisée comme répondeur, est le premier homologue, l'IKE SA est initiée à partir de l'adresse IP de Peer1. De même, si l'homologue actif

actuel dans la carte de chiffrement, utilisée comme répondeur, est le deuxième homologue, l'IKE SA est initiée à partir de l'adresse IP de Peer2.

Remarque Le parcours des homologues n'est pas pris en charge du côté répondeur dans une topologie IKEv2 multi-homologues.

Réinitialisation de l'index d'homologue lors des modifications de la carte de chiffrement

Toute modification de la carte de chiffrement réinitialise l'index d'homologue à zéro, et l'initiation du tunnel recommence à partir du premier homologue de la liste. Le tableau suivant présente la transition de l'index multi-homologues dans des conditions particulières :

Tableau 1 : Transition de l'index multi-homologues avant la SA

Conditions antérieures à SA	Index d'homologue déplacé Oui/Non/Réinitialiser
Homologue inaccessible	Oui
Incompatibilité de proposition de phase 1	Oui
Incompatibilité de proposition de phase 2	Oui
Accusé de réception DPD non reçu	Oui
Incompatibilité des sélecteurs de trafic pendant la phase d'authentification	Oui
Échec de l'‘authentification	Oui
Échec du renouvellement en raison d'un homologue inaccessible	Réinitialiser

Tableau 2 : Transition de l'index multi-homologues après la SA

Conditions après SA	Index d'homologue déplacé Oui/Non/Réinitialiser
Échec du renouvellement en raison d'une incompatibilité de proposition	Réinitialiser
Incompatibilité des sélecteurs de trafic lors du renouvellement	Réinitialiser
Modification de la carte de chiffrement	Réinitialiser
Basculement HA	Non
Effacer le chiffrement IKEv2 SA	Réinitialiser
Effacer ipsec sa	Réinitialiser

Conditions après SA	Index d'homologue déplacé Oui/Non/Réinitialiser
Délai d'expiration IKEv2 SA	Réinitialiser

Lignes directrices relatives à IKEv2 multi-homologues

Protocoles IKEv1 et IKEv2

Si une carte de chiffrement est configurée avec les deux versions IKE et plusieurs homologues, une tentative de SA est effectuée sur chaque homologue avec les deux versions avant de passer au suivant.

Par exemple, si une carte de chiffrement est configurée avec deux homologues, soit P1 et P2, le tunnel est initié vers P1 avec IKEv2, puis vers P1 avec IKEv1, puis vers P2 avec IKEv2, et ainsi de suite.

Haute disponibilité

Une carte de chiffrement avec plusieurs homologues initie des tunnels vers le périphérique répondeur qui se trouve en haute disponibilité. Elle passe au périphérique répondeur suivant lorsque le premier périphérique n'est pas accessible.

Un périphérique initiateur amorce des tunnels vers le périphérique répondeur. Si le périphérique actif tombe en panne, le périphérique en veille tente d'établir le tunnel à partir de l'adresse IP de Peer1, indépendamment du fait que la carte de chiffrement soit passée à l'adresse IP de Peer2 sur le périphérique actif.

Grappe centralisée

Une carte de chiffrement avec plusieurs homologues peut lancer des tunnels vers le périphérique répondeur qui se trouve dans un déploiement de grappe centralisée. Si le premier périphérique est inaccessible, il tente de passer au périphérique du répondeur suivant.

Un périphérique initiateur amorce des tunnels vers le périphérique répondeur. Chaque nœud de la grappe passe à Peer2 si Peer1 n'est pas accessible.

Grappe distribuée

La mise en grappe distribuée n'est pas prise en charge lorsqu'une carte de chiffrement IKEv2 multi-homologues est configurée.

Mode contexte multiple

En mode contexte multiple, le comportement multi-homologues est propre à chaque contexte.

Commandes de débogage

Si l'établissement du tunnel échoue, activez ces commandes pour analyser davantage le problème.

- **debug crypto ikev2 platform 255**
- **debug crypto ikev2 protocol 255**
- **debug crypto ike-common 255**

L'exemple suivant montre un journal de débogage propre à IKEv2 multi-homologues, qui affiche la transition des homologues.

```
Sep 13 10:08:58 [IKE COMMON DEBUG]Failed to initiate ikev2 SA with peer 192.168.2.2,
initiate to next peer 192.168.2.3 configured in the multiple peer list of the crypto map.
```

Licences pour les VPN IPsec

Remarque Cette fonctionnalité n'est pas disponible sur les modèles sans chiffrement de charge utile.

Le VPN d'accès à distance IPsec utilisant IKEv2 nécessite une licence AnyConnect Plus ou Apex, disponible séparément. Le VPN d'accès à distance IPsec utilisant IKEv1 et le VPN de site à site IPsec utilisant IKEv1 ou IKEv2 utilise la licence Autre VPN fournie avec la licence Essentials. Consultez les licences pour fonctionnalités de la gamme Cisco ASA pour connaître les valeurs maximales par modèle.

Lignes directrices relatives aux VPN IPsec

Directives relatives au mode contextuel

Pris en charge en mode contexte unique ou multiple. Une licence AnyConnect Apex est requise pour le VPN d'accès à distance en mode multi-contexte. Bien que l'ASA ne reconnaisse pas spécifiquement une licence AnyConnect Apex, elle applique les caractéristiques d'une licence Apex, telles que AnyConnect Premium sous licence jusqu'à la limite de la plateforme, Secure Client (services client sécurisés) pour la mobilité, Secure Client (services client sécurisés) pour le téléphone VPN Cisco et l'évaluation avancée des points terminaux.

Directives sur le mode pare-feu

Pris en charge uniquement en mode de pare-feu routé. Le mode pare-feu transparent n'est pas pris en charge.

Directives en matière de basculement

- Les sessions VPN IPsec sont répliquées uniquement dans les configurations de basculement actif/veille.
- Lorsqu'un basculement se produit, le numéro de séquence ESP augmente de 25 millions pour empêcher un faux positif anti-rejeu.

Directives supplémentaires

Lorsque vous configurez IKE, le système réserve automatiquement les ports RADIUS UDP 1645 et 1646. Cette réservation est indiquée dans le journal système 713903, où les numéros de port sont affichés comme 27910 et 28166. Cette réservation garantit que les ports ne sont pas utilisés pour les traductions PAT.

Configurer ISAKMP

Configurer les politiques IKEv1 et IKEv2

IKEv1 et IKEv2 prennent chacune en charge un maximum de 20 politiques IKE, chacune avec un ensemble de valeurs différent. Attribuez une priorité unique à chaque politique que vous créez. Plus le numéro de priorité est faible, plus la priorité est élevée.

Lorsque la négociation IKE commence, l'homologue qui initie la négociation envoie toutes ses politiques à l'homologue distant, et l'homologue distant recherche une correspondance. L'homologue distant vérifie toutes les politiques de l'homologue par rapport à chacune de ses politiques configurées dans l'ordre de priorité (priorité la plus élevée en premier) jusqu'à ce qu'il trouve une correspondance.

Une correspondance existe lorsque les deux politiques des deux homologues contiennent les mêmes valeurs de chiffrement, de hachage, d'authentification et de paramètres Diffie-Hellman. Pour IKEv1, la politique d'homologue distante doit également spécifier une durée de vie inférieure ou égale à la durée de vie de la politique envoyée par l'initiateur. Si les durées de vie ne sont pas identiques, l'ASA utilise la durée de vie la plus courte. Pour IKEv2, la durée de vie n'est pas négociée mais gérée localement par chaque homologue, ce qui permet de la configurer indépendamment. S'il n'existe aucune correspondance acceptable, IKE refuse la négociation et la SA n'est pas établie.

Il existe un compromis implicite entre la sécurité et les performances lorsque vous choisissez une valeur spécifique pour chaque paramètre. Le niveau de sécurité fourni par les valeurs par défaut est adéquat pour les exigences de sécurité de la plupart des entreprises. Si vous interopérez avec un homologue qui ne prend en charge qu'une seule des valeurs d'un paramètre, votre choix se limite à cette valeur.

Vous devez inclure la priorité dans chacune des commandes ISAKMP. Le numéro de priorité identifie de manière unique la politique et détermine la priorité de la politique dans les négociations IKE.

Procédure

Étape 1 Pour créer une politique IKE, entrez la commande **crypto** *ikev1* | *ikev2* policy à partir du mode de configuration globale en mode contexte unique ou multiple. L'invite affiche le mode de configuration de politique IKE.

Exemple :

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

Remarque
Les nouvelles configurations ASA n'ont pas de politique IKEv1 ou IKEv2 par défaut.

Étape 2 Spécifiez l'algorithme de chiffrement. La valeur par défaut est AES-128.

encryption [aes | aes-192 | aes-256]

Exemple :

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

Étape 3 Précisez l'algorithme de hachage. La valeur par défaut est SHA-1.

hash[**sha**]

Exemple :

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

Étape 4 Spécifiez la méthode d'authentification. La valeur par défaut est les clés prépartagées.

authentication[**pre-shared**]**rsa-sig**]

Exemple :

```
hostname(config-ikev1-policy)# authentication rsa-sig
```

Étape 5 Précisez l'identifiant de groupe Diffie-Hellman. La valeur par défaut est Group 14.

group [14]

Exemple :

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

Étape 6 Précisez la durée de vie de la SA. La valeur par défaut est 86 400 secondes (24 heures).

lifetime *seconds*

Exemple :

Cet exemple définit une durée de vie de 4 heures (14 400 secondes) :

```
hostname(config-ikev1-policy)# lifetime 14400
```

Étape 7 Précisez les paramètres supplémentaires à l'aide des mots-clés de politique IKEv1 et IKEv2 et leurs valeurs fournies dans Valeurs et mots-clés de la politique IKE, à la page 9. Si vous ne spécifiez pas de valeur pour un paramètre de politique donné, la valeur par défaut s'applique.

Valeurs et mots-clés de la politique IKE

	Mot-clé	Signification	Description
authentication	**rsa-sig**	Un certificat numérique avec des clés générées par l'algorithme de signatures RSA	Spécifie la méthode d'authentification utilisée par l'ASA pour établir l'identité de chaque homologue IPsec.
	pre-share (pré-partage)(par défaut)	Clés prépartagées	Les clés prépartagées n'évoluent pas facilement avec un réseau en croissance, mais sont plus faciles à configurer dans un petit réseau.
encryption	**AES**(par défaut)	AES avec une clé de 128 bits	Spécifie l'algorithme de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. La valeur par défaut est une clé de 128 bits.

	Mot-clé	Signification	Description
hash	**sha** (par défaut)	SHA-1 (variante HMAC)	Spécifie l'algorithme de hachage utilisé pour assurer l'intégrité des données. Il garantit qu'un paquet provient bien de la source indiquée et qu'il n'a pas été modifié en cours de transit.
group	**14** (par défaut)	Groupe 14 (2 048 bits)	Spécifie l'identifiant du groupe Diffie-Hellman, que les deux homologues IPsec utilisent pour dériver un secret partagé sans se le transmettre. Plus le numéro de groupe Diffie-Hellman est faible, moins il faut de temps CPU pour s'exécuter. Plus le numéro de groupe Diffie-Hellman est élevé, plus la sécurité est élevée. Le groupe par défaut est DH Group 14.
lifetime	**integer value** (valeur entière) (86 400 = par défaut)	120 à 2 147 483 647 secondes	Spécifie la durée de vie de la SA. La valeur par défaut est 86 400 secondes ou 24 heures. En règle générale, une durée de vie plus courte permet des négociations ISAKMP plus sécurisées (jusqu'à un certain point). Cependant, avec des durées de vie plus courtes, l'ASA configure les futures SA IPsec plus rapidement.

	Mot-clé	Signification	Description
integrity	sha (par défaut)	SHA-1 (variante HMAC)	Spécifie l'algorithme de hachage utilisé pour assurer l'intégrité des données. Il garantit qu'un paquet provient d'où il provient et qu'il n'a pas été modifié en cours de transit.
	sha256	SHA 2, condensé de 256 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 256 bits.
	sha384	SHA 2, condensé de 384 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
	sha512	SHA 2, condensé de 512 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 512 bits.
	null (nul)		Lorsque AES-GCM est spécifié comme algorithme de chiffrement, un administrateur peut choisir NULL comme algorithme d'intégrité IKEv2.
encryption	aes (par défaut)	AES	Spécifie l'algorithme de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. La valeur par défaut est AES 128 bits.
	aes aes-192 aes-256		La norme de chiffrement avancé prend en charge les longueurs de clé de 128, 192 et 256 bits.

	Mot-clé	Signification	Description
	aes-gcm **aes-gcm-192** **aes-gcm-256** **null**	Options de l'algorithme AES-GCM à utiliser pour le chiffrement IKEv2	La norme de chiffrement avancé prend en charge les longueurs de clé de 128, 192 et 256 bits.
policy_index			Accède au sous-mode de politique IKEv2.
prf	sha (par défaut)	SHA-1 (variante HMAC)	Spécifie la fonction pseudo-aléatoire (PRF) — l'algorithme utilisé pour générer le matériel de dérivation de clés.
	sha256	SHA 2, condensé de 256 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 256 bits.
	sha384	SHA 2, condensé de 384 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
	sha512	SHA 2, condensé de 512 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 512 bits.
priority			Étend le mode de politique pour prendre en charge les fonctionnalités IPsec V3 supplémentaires et intègre les paramètres AES-GCM et ECDH à la prise en charge de la suite B.
group	**14 19 20 21 24**	Groupe 14 (2 048 bits)	Spécifie l'identifiant du groupe Diffie-Hellman, que les deux homologues IPsec utilisent pour dériver un secret partagé sans se le transmettre. Plus le numéro de groupe Diffie-Hellman est faible, moins il faut de temps CPU pour s'exécuter. Plus le numéro de groupe Diffie-Hellman est élevé, plus la sécurité est élevée. La valeur par défaut est le groupe (DH) 14
lifetime	**integer value** (valeur entière) (86 400 = par défaut)	120 à 2 147 483 647 secondes	Spécifie la durée de vie de la SA. La valeur par défaut est 86 400 secondes ou 24 heures. En règle générale, une durée de vie plus courte permet des négociations ISAKMP plus sécurisées (jusqu'à un certain point). Cependant, avec des durées de vie plus courtes, l'ASA configure les futures SA IPsec plus rapidement.

Activer IKE sur l'interface externe.

Vous devez activer IKE sur l'interface qui termine le tunnel VPN. Il s'agit généralement de l'interface externe. Pour activer IKEv1 ou IKEv2, utilisez la commande crypto [**ikev1** | **ikev2**] **enable** *interface-name* en mode de configuration globale, que ce soit en mode contexte unique ou multiple.

Par exemple :

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

Activer ou désactiver le mode agressif IKEv1

Les négociations IKEv1 de phase 1 peuvent utiliser le mode principal ou le mode agressif. Tous deux fournissent les mêmes services, mais le mode agressif ne nécessite que deux échanges entre les homologues pour un total de trois messages, plutôt que trois échanges pour un total de six messages. Le mode agressif est plus rapide, mais ne fournit pas de protection d'identité pour les parties qui communiquent. Par conséquent, les homologues doivent échanger des informations d'identification avant d'établir une SA sécurisée. Le mode agressif est activé par défaut.

Remarque La désactivation du mode agressif empêche les clients VPN de Cisco d'utiliser l'authentification par clé prépartagée pour établir des tunnels vers l'ASA. Cependant, ils peuvent utiliser l'authentification basée sur les certificats (c'est-à-dire ASA ou RSA) pour établir les tunnels.

Pour activer le mode agressif pour les négociations de la phase 1 du protocole IKEv1, entrez la commande suivante en mode contexte unique ou multiple :

```
hostname(config)# crypto map <map-name> seq-num set ikev1 phase1-mode aggressive <group-name>
```

Pour désactiver le mode agressif, entrez la commande suivante en mode contexte unique ou multiple :

```
hostname(config)# crypto ikev1 am-disable
```

Si vous avez désactivé le mode agressif et que vous souhaitez le réactiver, utilisez la forme no de la commande. Par exemple :

```
hostname(config)#  no crypto ikev1 am-disable
```

Configurer une méthode d'ID pour les homologues ISAKMP IKEv1 et IKEv2

Au cours des négociations de phase I ISAKMP IKEv1 ou IKEv2, les homologues doivent s'identifier les uns aux autres. Vous pouvez choisir la méthode d'identification parmi les options suivantes.

Address	Utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
Automatic (par défaut)	Détermine la négociation ISAKMP par type de connexion : • Adresse IP pour la clé prépartagée • Nom distinctif du certificat pour l'authentification par certificat.
Hostname	Utilise le nom de domaine complet des hôtes échangeant les informations d'identité ISAKMP (par défaut). Ce nom comprend le nom d'hôte et le nom de domaine.
Key ID *key_id_string*	Spécifie la chaîne utilisée par l'homologue distant pour rechercher la clé prépartagée.

L'ASA utilise l'ID de phase I à envoyer à l'homologue. Cela est vrai pour tous les scénarios VPN, à l'exception des connexions IKEv1 LAN à LAN en mode principal qui s'authentifient au moyen de clés prépartagées.

Pour modifier la méthode d'identification des homologues, saisissez la commande suivante en mode monocontexte ou multicontexte :

crypto isakmp identity {*address* | *hostname* | **key-id** *id-string* | **auto**}

Par exemple, la commande suivante définit la méthode d'identification de l'homologue sur hostname :

```
hostname(config)# crypto isakmp identity hostname
```

Notification INVALID_SELECTORS

Si un système IPsec reçoit un paquet entrant sur une SA et que les champs d'en-tête du paquet ne sont pas cohérents avec les sélecteurs de la SA, il DOIT rejeter le paquet. L'entrée du journal d'audit pour cet événement comprend la date et l'heure actuelles, le SPI, le ou les protocoles IPsec, la source et la destination du paquet, toutes les autres valeurs de champ du paquet qui sont disponibles et les valeurs de sélecteur de l'entrée de SA correspondante. Le système génère et envoie une notification IKE de INVALID_SELECTORS à l'expéditeur (homologue IPsec), indiquant que le paquet reçu a été rejeté en raison d'un échec des vérifications du sélecteur.

L'ASA met déjà en œuvre la journalisation de cet événement dans CTM à l'aide du journal système existant affiché ci-dessous :

```
%ASA-4-751027: IKEv2 Received INVALID_SELECTORS Notification from peer: <peer IP>. Peer
received a packet (SPI=<spi>) from <local_IP>. The decapsulated inner packet didn't match
 the negotiated policy in the SA. Packet destination <pkt_daddr>, port <pkt_dest_port>,
source <pkt_saddr>, port <pkt_src_port>, protocol <pkt_prot>
```

Un administrateur peut maintenant activer ou désactiver l'envoi d'une notification IKEv2 à l'homologue lorsqu'un paquet entrant est reçu sur une SA qui ne correspond pas aux sélecteurs de trafic de cette SA. Si elles sont activées, les messages de notification IKEv2 sont limités en fréquence à un message de notification par SA toutes les cinq secondes. La notification IKEv2 est envoyée dans un échange d'informations IKEv2 avec l'homologue.

Configurer la clé prépartagée IKEv2 en format hexadécimal

Vous pouvez configurer les clés prépartagées IKEv2 en hexadécimal en ajoutant le mot-clé *hex* aux commandes de clé prépartagée locale et distante.

```
ikev2 local-authentication pre-shared-key [ 0 | 8 | hex ] <string>
ikev2 remote-authentication pre-shared-key [ 0 | 8 | hex ] <string>
```

Activer ou désactiver l'envoi de la notification IKE

Un administrateur peut activer ou désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant est reçu sur une connexion VPN IPsec IKEv2 qui ne correspond pas aux sélecteurs de trafic pour cette connexion. L'envoi de cette notification est désactivé par défaut. Envoi de notifications IKE INVALID_SELECTORS lorsque l'autorisation d'un nom d'utilisateur à partir du certificat ASDM est activée ou désactivée via la CLI suivante :

[**no**]**crypto ikev2 notify invalid-selectors**

Lors de l'authentification par certificat, le CN du certificat est le nom d'utilisateur, et l'autorisation est effectuée sur le serveur LOCAL. Si l'attribut « service-type » est récupéré, il est traité comme décrit précédemment.

Configurer les options de fragmentation IKEv2

Sur l'ASA, la fragmentation IKEv2 peut être activée ou désactivée, la MTU utilisée lors de la fragmentation des paquets IKEv2 peut être précisée et une méthode de fragmentation préférée peut être configurée par l'administrateur à l'aide de la commande suivante :

[**no**] **crypto ikev2 fragmentation** [**mtu** <*mtu-size*>] | [**preferred-method** [**ietf** | **cisco**]]

Par défaut, toutes les méthodes de fragmentation IKEv2 sont activées, la MTU est de 576 pour IPv4 ou de 1280 pour IPv6, et la méthode préférée est la norme IETF RFC-7383.

Précisez la [**mtu** <*mtu-size*>] en tenant compte des considérations suivantes :

- La valeur MTU utilisée doit inclure l'en-tête IP (IPv4/IPv6) et la taille d'en-tête UDP.
- Si elle n'est pas précisée par l'administrateur, la MTU par défaut est de 576 pour IPv4 ou de 1 280 pour IPv6.
- Une fois précisée, la même MTU sera utilisée pour IPv4 et IPv6.
- La plage valide est de 68 à 1 500.

Remarque Vous devez prendre en compte le surdébit ESP lors de la configuration de la MTU. La taille des paquets augmente après le chiffrement en raison du surdébit ESP ajouté à la MTU pendant le chiffrement. Si vous obtenez l'erreur « paquet trop volumineux », veillez à vérifier la taille de la MTU et à configurer une MTU inférieure.

L'une des méthodes de fragmentation suivantes prises en charge peut être configurée comme méthode de fragmentation préférée pour IKEv2 [**preferred-method** [**ietf** | **cisco**]] :

- Fragmentation IKEv2 basée sur la norme IETF RFC-7383.
  - Cette méthode sera utilisée lorsque les deux homologues précisent la prise en charge et la préférence durant la négociation.
  - À l'aide de cette méthode, le chiffrement est effectué après la fragmentation, ce qui assure une protection individuelle pour chaque message de fragment IKEv2.
- Fragmentation propriétaire Cisco.
  - Cette méthode sera utilisée s'il s'agit de la seule méthode fournie par un homologue, tel que le Secure Client (services client sécurisés), ou si les deux homologues précisent la prise en charge et les préférences pendant la négociation.
  - À l'aide de cette méthode, la fragmentation est effectuée après le chiffrement. L'homologue de réception ne peut pas déchiffrer ou authentifier le message tant que tous les fragments ne sont pas reçus.
  - Cette méthode n'est pas interopérable avec des homologues non Cisco.

La commande **show running-config crypto ikev2** affiche la configuration actuelle et **show crypto ikev2 sa detail** affiche la MTU appliquée si la fragmentation a été utilisée pour la SA.

Avant de commencer

- Le chemin de découverte de MTU n'est pas pris en charge, la MTU doit être configurée manuellement pour correspondre aux besoins du réseau.
- Cette configuration est globale et aura une incidence sur les futurs SA établies après son application. Les anciennes SA ne seront pas touchées. Le même comportement s'applique lorsque la fragmentation est désactivée.
- Un maximum de 100 fragments peut être reçu.

Exemples

- Pour désactiver la fragmentation IKEv2 :

```
no crypto ikev2 fragmentation
```

- Pour rétablir l'opération par défaut :

```
crypto ikev2 fragmentation
```

ou

```
crypto ikev2 fragmentation mtu 576
preferred-method ietf
```

- Pour modifier la valeur MTU à 600 :

```
crypto ikev2 fragmentation mtu 600
```

- Pour restaurer la valeur MTU par défaut :

```
 no crypto ikev2 fragmentation mtu 576
```

- Pour définir Cisco comme méthode de fragmentation préférée :

```
crypto ikev2 fragmentation preferred-method cisco
```

- Pour restaurer la méthode de fragmentation préférée dans IETF :

```
no crypto ikev2 fragmentation preferred-method cisco
```

ou

```
 crypto ikev2 fragmentation preferred-method ietf
```

Authentification AAA avec autorisation

```
aaa authentication http console LOCAL
aaa authorization http console radius
```

L'authentification AAA est effectuée sur le serveur LOCAL à l'aide du nom d'utilisateur et du mot de passe saisis par l'utilisateur. Une autorisation supplémentaire est effectuée sur le serveur *radius* en utilisant le même nom d'utilisateur. L'attribut *service-type*, s'il est récupéré, est traité comme décrit précédemment.

Activer IPsec sur NAT-T

NAT-T permet aux homologues IPsec d'établir une connexion par l'intermédiaire d'un périphérique NAT. Il le fait en encapsulant le trafic IPsec dans des datagrammes UDP, en utilisant le port 4500, qui fournit aux périphériques NAT des informations de port. NAT-T détecte automatiquement tous les périphériques NAT et encapsule le trafic IPsec uniquement lorsque cela est nécessaire.

Remarque En raison d'une limitation de Secure Client (services client sécurisés), vous devez activer NAT-T pour que Secure Client (services client sécurisés) se connecte avec succès à l'aide de IKEv2. Cette exigence s'applique même si le client ne se trouve pas derrière un périphérique NAT-T.

L'ASA peut prendre en charge simultanément IPsec standard, IPsec sur TCP, NAT-T et IPsec sur UDP, selon le client avec lequel il échange des données.

La ventilation suivante montre les connexions pour chaque option activée.

Options	Fonction activée	Position du client	Fonction utilisée
Option 1	Si NAT-T est activé	et le client se trouve derrière la NAT, alors	NAT-T est utilisé
		et qu'aucune NAT n'existe, alors	L'IPsec natif (ESP) est utilisé
Option 2	Si IPsec sur UDP est activé	et le client se trouve derrière la NAT, alors	IPsec sur UDP est utilisé
		et qu'aucune NAT n'existe, alors	IPsec sur UDP est utilisé
Option 3	Si NAT-T et IPsec sur UDP sont activés	et le client se trouve derrière la NAT, alors	NAT-T est utilisé
		et qu'aucune NAT n'existe, alors	IPsec sur UDP est utilisé

Remarque Lorsque IPsec sur TCP est activé, il prévaut sur toutes les autres méthodes de connexion.

Lorsque vous activez NAT-T, l'ASA ouvre automatiquement le port 4500 sur toutes les interfaces compatibles avec IPsec.

L'ASA prend en charge plusieurs homologues IPsec derrière un seul périphérique NAT/PAT fonctionnant dans des déploiements LAN à LAN ou d'accès à distance, mais pas simultanément pour les deux types sur le même équipement NAT/PAT. Dans un environnement mixte, les tunnels d'accès à distance échouent dans la négociation, ar tous les homologues semblent provenir de la même adresse IP publique, celle du périphérique NAT. De plus, les tunnels d'accès à distance échouent dans un environnement mixte, car ils utilisent souvent le même nom que le groupe de tunnels LAN à LAN (c'est-à-dire l'adresse IP du périphérique NAT). Cette correspondance peut provoquer des échecs de négociation entre plusieurs homologues dans un environnement mixte de site à site et d'accès à distance d'homologues derrière le périphérique NAT.

Pour utiliser NAT-T, effectuez les étapes suivantes de site à site en mode contexte unique ou multiple :

Procédure

Étape 1 Entrez la commande suivante pour activer IPsec sur NAT-T globalement sur l'ASA :

crypto isakmp nat-traversal *natkeepalive*

La plage pour l'argument natkeepalive est de 10 à 3600 secondes. La valeur par défaut est de 20 secondes.

Exemple :

Entrez la commande suivante pour activer NAT-T et définir la valeur keepalive à une heure :

```
hostname(config)# crypto isakmp nat-traversal 3600
```

Étape 2 Sélectionnez l'option before-encryption pour la politique de fragmentation IPsec en entrant cette commande :

```
hostname(config)# crypto ipsec fragmentation before-encryption
```

Cette option permet au trafic de traverser des périphériques NAT qui ne prennent pas en charge la fragmentation IP. Cela n'affecte pas le fonctionnement des périphériques NAT qui prennent en charge la fragmentation IP.

Activer IPsec avec IKEv1 sur TCP

IPsec sur TCP encapsule les protocoles IKEv1 et IPsec dans un paquet de type TCP et permet la tunnellisation sécurisée au travers des périphériques NAT et PAT ainsi que des pare-feu. Par défaut, cette fonction est désactivée. IPsec/IKEv1 sur TCP permet à un client VPN Cisco de fonctionner dans un environnement où l'ESP standard ou IKEv1 ne peut pas fonctionner, ou ne peut fonctionner qu'au prix d'une modification des règles de pare-feu existantes.

Remarque Cette fonctionnalité ne fonctionne pas avec les pare-feu basés sur un proxy.

IPsec sur TCP fonctionne avec les clients d'accès à distance. Vous activez IPsec sur TCP sur l'ASA et sur le client auquel il se connecte. Sur l'ASA, il est activé de façon globale et fonctionne sur toutes les interfaces où IKEv1 est activé. Il ne fonctionne pas pour les connexions LAN à LAN.

L'ASA peut prendre en charge simultanément IPsec standard, IPsec sur TCP, NAT-Traversal et IPsec sur UDP, selon le client avec lequel il échange des données. IPsec sur TCP, s'il est activé, prévaut sur toutes les autres méthodes de connexion.

Vous pouvez activer IPsec sur TCP pour un maximum de 10 ports que vous spécifiez. Si vous saisissez un port bien connu, par exemple le port 80 (HTTP) ou le port 443 (HTTPS), le système affiche un avertissement indiquant que le protocole associé à ce port ne fonctionne plus sur l'interface publique. Par conséquent, vous ne pouvez plus utiliser de navigateur pour gérer l'ASA au moyen de l'interface publique. Pour résoudre ce problème, reconfigurez la gestion HTTP/HTTPS sur différents ports.

Le port par défaut est 10 000.

Vous devez configurer les ports TCP sur le client ainsi que sur l'ASA. La configuration du client doit inclure au moins un des ports que vous avez définis pour l'ASA.

Pour activer globalement IPsec sur TCP pour IKEv1 sur l'ASA, saisissez la commande suivante en mode monocontexte ou multicontexte :

crypto ikev1 ipsec-over-tcp [port *port 1...port0]*

Cet exemple active IPsec sur TCP sur le port 45 :

```
hostname(config)# crypto ikev1 ipsec-over-tcp port 45
```

Configurer la correspondance de groupe de certificats pour IKEv1

Les groupes de tunnels définissent les conditions de connexion et les autorisations des utilisateurs. La correspondance de groupe de certificats vous permet d'associer un utilisateur à un groupe de tunnels en utilisant soit le DN du sujet, soit le DN de l'émetteur du certificat utilisateur.

Remarque La correspondance de groupe de certificats s'applique uniquement aux connexions IKEv1 et IKEv2 LAN à LAN. Les connexions d'accès à distance IKEv2 prennent en charge la sélection de groupe dans une liste déroulante configurée dans les webvpn-attributes du tunnel-group et dans le mode de configuration webvpn pour certificate-group-map, et ainsi de suite.

Pour faire correspondre les utilisateurs aux groupes de tunnels en fonction de ces champs du certificat, vous devez d'abord créer des règles qui définissent un critère de correspondance, puis associer chaque règle au groupe de tunnels souhaité.

Pour créer une correspondance de certificats, utilisez la commande **use the crypto ca certificate map**. Pour définir un groupe de tunnels, utilisez la commande tunnel-group.

Vous devez également configurer une politique de correspondance de groupe de certificats, en précisant si la correspondance du groupe doit être établie à partir des règles, du champ de l'unité organisationnelle (OU) ou d'un groupe par défaut pour tous les utilisateurs de certificats. Vous pouvez utiliser une ou toutes ces méthodes.

Procédure

Étape 1 Pour configurer la politique et les règles selon lesquelles les sessions ISAKMP fondées sur des certificats sont associées à des groupes de tunnels, et pour associer les entrées de correspondance de certificats aux groupes de tunnels, saisissez la commande tunnel-group-map en mode monocontexte ou multicontexte.

tunnel-group-map enable {*rules* | *ou* | *ike-id* | *peer ip*}

tunnel-group-map [*rule-index*] **enable** *policy*

politique	Spécifie la politique utilisée pour dériver le nom du groupe de tunnels à partir du certificat. La politique peut être l'une des suivantes : *ike-id* : indique que si un groupe de tunnels n'est pas déterminé selon une recherche de règle ou tiré de l'OU, les sessions ISAKMP fondées sur des certificats sont alors associées à un groupe de tunnels en fonction du contenu de l'ID ISAKMP de phase1. *ou* : indique que si un groupe de tunnels n'est pas déterminé selon une recherche de règle, il faut alors utiliser la valeur de l'OU dans le nom distinctif (DN) du sujet. *peer-ip* : indique que si un groupe de tunnels n'est pas déterminé selon une recherche de règle ni tiré des méthodes OU ou ike-id, il faut alors utiliser l'adresse IP de l'homologue. *rules* : indique que les sessions ISAKMP fondées sur des certificats sont associées à un groupe de tunnels selon les associations de correspondance de certificats configurées par cette commande.
index de règle	(Facultatif) fait référence aux paramètres spécifiés par la commande **crypto ca certificate map**. Les valeurs sont comprises entre 1 et 65 535.

Tenez compte des éléments suivants :

- Vous pouvez appeler cette commande plusieurs fois tant que chaque appel est unique et que vous ne faites pas référence à un index de correspondance plus d'une fois.
- Les règles ne peuvent pas dépasser 255 caractères.
- Vous pouvez affecter plusieurs règles au même groupe. Pour ce faire, ajoutez d'abord la priorité de la règle et le groupe. Vous définissez ensuite autant de critères que nécessaires pour chaque groupe. Lorsque plusieurs règles sont affectées au même groupe, la première règle dont la condition est vérifiée est appliquée.
- En créant une règle unique, vous pouvez exiger que tous les critères soient satisfaits avant d'affecter un utilisateur à un groupe de tunnels spécifique. Exiger la mise en correspondance de tous les critères équivaut à une opération ET logique. Sinon, créez une règle pour chaque critère si vous souhaitez exiger qu'une seule correspondance avant d'affecter un utilisateur à un groupe de tunnels spécifique. L'exigence d'un seul critère pour la mise en correspondance équivaut à une opération OU logique.

Étape 2 Précisez un groupe de tunnels par défaut à utiliser lorsque la configuration ne spécifie pas de groupe de tunnels.

La syntaxe est **tunnel-group-map** [*rule-index*] **default-group***tunnel-group-name* où *rule-index* est la priorité de la règle, et le nom du groupe de tunnels doit correspondre à un groupe de tunnels qui existe déjà.

Exemples

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats avec un groupe de tunnels en fonction du contenu de l'ID ISAKMP phase1 :

```
hostname(config)# tunnel-group-map enable ike-id
```

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats vers un groupe de tunnels en fonction de l'adresse IP de l'homologue :

```
hostname(config)# tunnel-group-map enable peer-ip
```

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats en fonction de l'unité d'organisation (OU) dans le nom distinctif (DN) du sujet :

```
hostname(config)# tunnel-group-map enable ou
```

L'exemple suivant permet le mappage des sessions ISAKMP basées sur des certificats en fonction des règles établies :

```
hostname(config)# tunnel-group-map enable rules
```

Configurer IPsec

Cette section décrit les procédures requises pour configurer l'ASA lors de l'utilisation d'IPsec pour mettre en œuvre un VPN.

Définir les cartes de chiffrement

Les cartes de chiffrement définissent la politique IPsec à négocier dans la SA IPsec. Elles comprennent les éléments suivants :

- ACL pour identifier les paquets que la connexion IPsec autorise et protège.
- Identification des homologues.
- Adresse locale pour le trafic IPsec. (Voir Appliquer les cartes de chiffrement aux interfaces, à la page 29 pour plus de détails.)
- Jusqu'à 11 ensembles de transformation IKEv1 ou propositions IKEv2, avec lesquels tenter de faire correspondre les paramètres de sécurité homologues.

Un *ensemble de cartes de chiffrement* se compose d'une ou de plusieurs cartes de chiffrement qui ont le même nom de carte. Vous créez un ensemble de cartes de chiffrement lorsque vous créez sa première carte de chiffrement. La tâche de site à site suivante crée ou ajoute une carte de chiffrement en mode contexte unique ou multiple :

crypto map *map-name seq-num* **match address** *access-list-name*

Utilisez le nom de liste d'accès pour spécifier l'ID d'ACL, sous forme de chaîne ou d'entier d'une longueur maximale de 241 caractères.

Astuces Utilisez toutes les lettres majuscules pour identifier plus facilement l'ID d'ACL dans votre configuration.

Vous pouvez continuer à entrer cette commande pour ajouter des cartes de chiffrement à l'ensemble de cartes de chiffrement. Dans l'exemple suivant, *mymap* est le nom de l'ensemble de cartes de chiffrement auquel vous pourriez ajouter des cartes de chiffrement :

crypto map mymap 10 match address 101

Le *numéro de séquence* (*seq-num*) affiché dans la syntaxe ci-dessus distingue une carte de chiffrement d'une autre carte portant le même nom. Le numéro de séquence attribué à une carte de chiffrement détermine également sa priorité par rapport aux autres cartes de chiffrement d'un ensemble de cartes de chiffrement. Plus le numéro de séquence est bas, plus la priorité est élevée. Après avoir affecté un ensemble de cartes de chiffrement à une interface, l'ASA évalue tout le trafic IP passant par l'interface par rapport aux cartes de chiffrement de l'ensemble, en commençant par la carte de chiffrement ayant le numéro de séquence le plus bas.

[no] crypto map *map_name map_index* **set pfs [group14 | group15 | group16 | group19 | group20 | group21]**

Spécifie le groupe ECDH utilisé pour la confidentialité de transmission parfaite (PFS) pour la carte de chiffrement. Empêche de configurer les options group14 et group24 pour une carte de chiffrement (lors de l'utilisation d'une politique IKEv1).

[no] crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

Active l'injection de route inverse (RRI) pour toute connexion basée sur cette entrée de carte de chiffrement. Si dynamic n'est pas spécifié, la RRI est effectuée lors de la configuration et est considérée comme statique, restant en place jusqu'à ce que la configuration soit modifiée ou supprimée. En outre, chaque fois qu'une route RRI est configurée avec la même destination pour laquelle une route statique existe déjà, la route statique existante est supprimée et la route RRI est installée. L'ASA ajoute automatiquement des routes statiques à la table de routage et communique ces routes à son réseau privé ou aux routeurs de frontière à l'aide d'OSPF. N'activez pas RRI si vous spécifiez une source/destination (0.0.0.0/0.0.0.0) comme réseau protégé, car cela aura une incidence sur le trafic qui utilise votre route par défaut.

Remarque Utilisez un réseau spécifique pour RRI, car cela ne fonctionnera pas si vous choisissez le réseau protégé comme « any ».

Si dynamic est spécifié, les routes sont créées lors de l'établissement réussi des associations de sécurité (SA) IPsec et supprimées après la suppression des SA IPsec.

Vous ne pouvez pas configurer une carte de chiffrement dynamique portant le même nom qu'une carte de chiffrement statique, et vice versa, même si l'une des cartes de chiffrement n'est pas actuellement utilisée.

Remarque La RRI dynamique est prise en charge sur les cartes de chiffrement statiques basées sur IKEv2 uniquement.

[no] crypto map *name priority* **set validate-icmp-errors**

OU

[**no**]**crypto dynamic-map** *name priority* **set validate-icmp-errors**

Spécifie si les messages d'erreur ICMP entrants sont validés pour la carte de chiffrement ou de chiffrement dynamique.

[no] crypto map <name> <priority> set df-bit [clear-df | copy-df | set-df}

OU

[no] crypto map dynamic-map <name> <priority> set df-bit [clear-df | copy-df | set-df]

Configure la politique existante de ne pas fragmenter (DF) (à un niveau d'association de sécurité) pour la carte de chiffrement ou de chiffrement dynamique.

- *clear-df* : ignore le bit DF.
- *copy-df* : maintient le bit DF.
- *set-df* : définit et utilise le bit DF.

[no] crypto map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

OU

[no] crypto dynamic-map <name> <priority> set tfc-packets [burst <length | auto] [payload-size <bytes | auto> [timeout <seconds | auto>

Un administrateur peut activer des paquets factices de confidentialité de flux de trafic (TFC) à des longueurs et à des intervalles aléatoires sur une association de sécurité IPsec. Vous devez avoir une proposition IKEv2 IPsec définie avant d'activer TFC.

Remarque L'activation des paquets de confidentialité du flux de trafic empêche le délai d'expiration d'inactivité du VPN.

L'ACL attribuée à une carte de chiffrement se compose de toutes les ACE ayant le même nom d'ACL, comme indiqué dans la syntaxe de commande suivante :

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

Vous créez une ACL lorsque vous créez sa première ACE. La syntaxe de commande suivante crée ou ajoute à une ACL :

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

Dans l'exemple suivant, l'ASA applique les protections IPsec attribuées à la carte de chiffrement à tout le trafic circulant du sous-réseau 10.0.0.0 vers le sous-réseau 10.1.1.0 :

access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0

La carte de chiffrement qui correspond au paquet détermine les paramètres de sécurité utilisés dans les négociations d'une SA. Si l'ASA local amorce la négociation, il utilise la politique spécifiée dans la carte de chiffrement statique pour créer l'offre à envoyer à l'homologue spécifié. Si l'homologue amorce la négociation, l'ASA tente de faire correspondre la politique à une carte de chiffrement statique et, en cas d'échec, tente de la faire correspondre à l'une des cartes de chiffrement dynamiques de l'ensemble de cartes de chiffrement, afin de décider s'il accepte ou refuse l'offre de l'homologue.

Pour que deux homologues réussissent à établir une SA, ils doivent avoir au moins une carte de chiffrement compatible. Pour être compatible, une carte de chiffrement doit respecter les critères suivants :

- La carte de chiffrement doit 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, l'ASA doit également contenir des listes de contrôle d'accès de chiffrement compatibles comme condition requise pour appliquer IPsec.

- Chaque carte de chiffrement identifie l'autre homologue (sauf si l'homologue qui répond utilise des cartes de chiffrement dynamiques).
- Les cartes de chiffrement ont au moins un ensemble de transformation ou une proposition en commun.

Vous ne pouvez appliquer qu'un seul ensemble de cartes de chiffrement à une seule interface. Créez plusieurs cartes de chiffrement pour une interface particulière sur l'ASA si l'une des conditions suivantes existe :

- Vous souhaitez que des homologues spécifiques gèrent différents flux de données.
- Vous souhaitez que différentes sécurités IPsec s'appliquent à différents types de trafic.

Par exemple, créez une carte de chiffrement et attribuez une liste de contrôle d'accès pour identifier le trafic entre deux sous-réseaux et attribuez un ensemble de transformation IKEv1 ou une proposition IKEv2. Créez une autre carte de chiffrement avec une liste de contrôle d'accès différente pour identifier le trafic entre deux autres sous-réseaux et appliquez un ensemble de transformation ou une proposition avec des paramètres VPN différents.

Si vous créez plusieurs cartes de chiffrement pour une interface, spécifiez un numéro de séquence (seq-num) pour chaque entrée de carte afin de déterminer sa priorité dans l'ensemble de cartes de chiffrement.

Chaque ACE contient une instruction d'autorisation ou de refus. Le tableau suivant explique les significations particulières des ACE permit et deny dans les listes de contrôle d'accès appliquées aux cartes de chiffrement.

Résultat de l'évaluation de la carte de chiffrement	**Intervention**
Critère de correspondance dans une commande ACE contenant une déclaration d'autorisation	Interrompt l'évaluation du paquet par rapport aux ACE restantes dans l'ensemble de cartes de chiffrement, puis évalue les paramètres de sécurité du paquet par rapport à ceux des ensembles de transformation IKEv1 ou des propositions IKEv2 attribués à la carte de chiffrement. Après avoir fait correspondre les paramètres de sécurité à ceux d'un ensemble ou d'une proposition de transformation, l'ASA applique les paramètres IPsec associés. En règle générale, pour le trafic sortant, cela signifie qu'il chiffre, authentifie et achemine le paquet.
Critère de correspondance dans une ACE contenant une instruction de refus	Interrompt l'évaluation du paquet par rapport aux ACE restantes dans la carte de chiffrement en cours d'évaluation, puis reprend l'évaluation par rapport aux ACE de la carte de chiffrement suivante, selon le numéro de séquence suivant qui lui est attribué.
Échec de la correspondance de toutes les ACE d'autorisation testées dans l'ensemble de cartes de chiffrement	Acheminez le paquet sans le chiffrer.

Les ACE contenant des instructions de refus filtrent le trafic sortant qui ne nécessite pas de protection IPsec (par exemple, le trafic de protocole de routage). Par conséquent, insérez des instructions de refus initiales pour filtrer le trafic sortant qui ne doit pas être évalué en fonction des instructions d'autorisation dans une liste de contrôle d'accès de chiffrement.

Pour un paquet entrant chiffré, l'appareil de sécurité utilise l'adresse source et le SPI ESP pour déterminer les paramètres de déchiffrement. Après que l'appareil de sécurité a déchiffré le paquet, il compare l'en-tête interne du paquet déchiffré aux ACE permit de l'ACL associée à la SA du paquet. Si l'en-tête interne ne

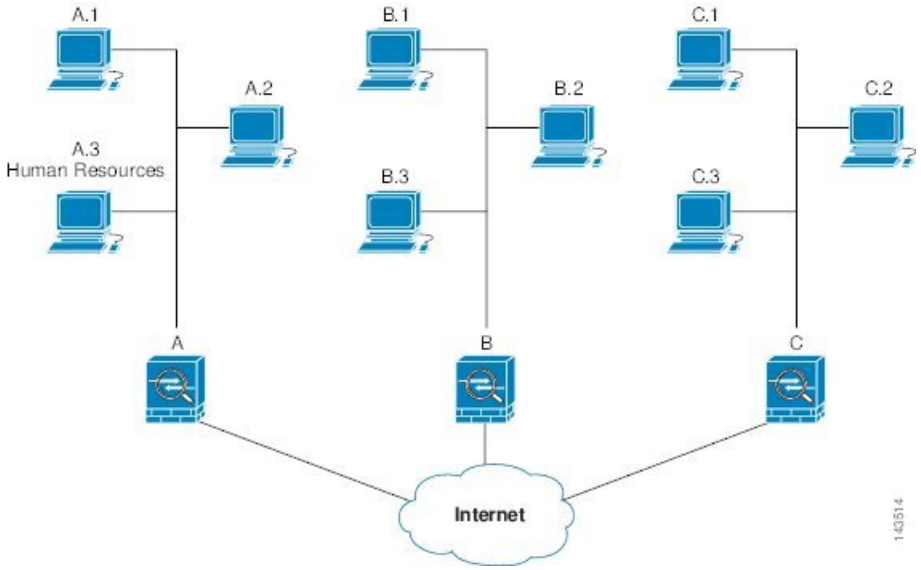
correspond pas au proxy, l'appareil de sécurité abandonne le paquet. Si l'en-tête interne correspond au proxy, l'appareil de sécurité achemine le paquet.

Lors de la comparaison de l'en-tête interne d'un paquet entrant qui n'a pas été chiffré, l'appareil de sécurité ignore toutes les règles de refus, car elles empêcheraient l'établissement d'une SA de phase 2.

Remarque Pour acheminer le trafic entrant non chiffré en texte clair, insérez les ACE de refus avant les ACE d'autorisation. L'ASA ne peut pas transmettre plus de 28 ACE dans une liste d'accès de tunnellisation fractionnée.

Exemple de cartes de chiffrement LAN à LAN

L'objectif de la configuration des appareils de sécurité A, B et C dans cet exemple de réseau LAN à LAN est de permettre la tunnellisation de tout le trafic provenant de l'un des hôtes et destiné à l'un des autres hôtes. Cependant, comme le trafic de l'hôte A.3 contient des données sensibles du service des ressources humaines, il nécessite un chiffrement renforcé et un renouvellement plus fréquent que l'autre trafic. Vous voudrez donc attribuer un ensemble de transformation spécial pour le trafic de l'hôte A.3.



La notation d'adresse simple indiquée dans cette figure et utilisée dans l'explication suivante est une expression conceptuelle. Un exemple avec des adresses IP réelles suit l'explication.

Pour configurer l'appareil de sécurité A pour le trafic sortant, vous créez deux cartes de chiffrement, l'une pour le trafic de l'hôte A.3 et l'autre pour le trafic des autres hôtes du réseau A, comme illustré dans l'exemple suivant :

```
Crypto Map Seq_No_1
    deny packets from A.3 to B
    deny packets from A.3 to C
    permit packets from A to B
    permit packets from A to C
Crypto Map Seq_No_2
    permit packets from A.3 to B
    permit packets from A.3 to C
```

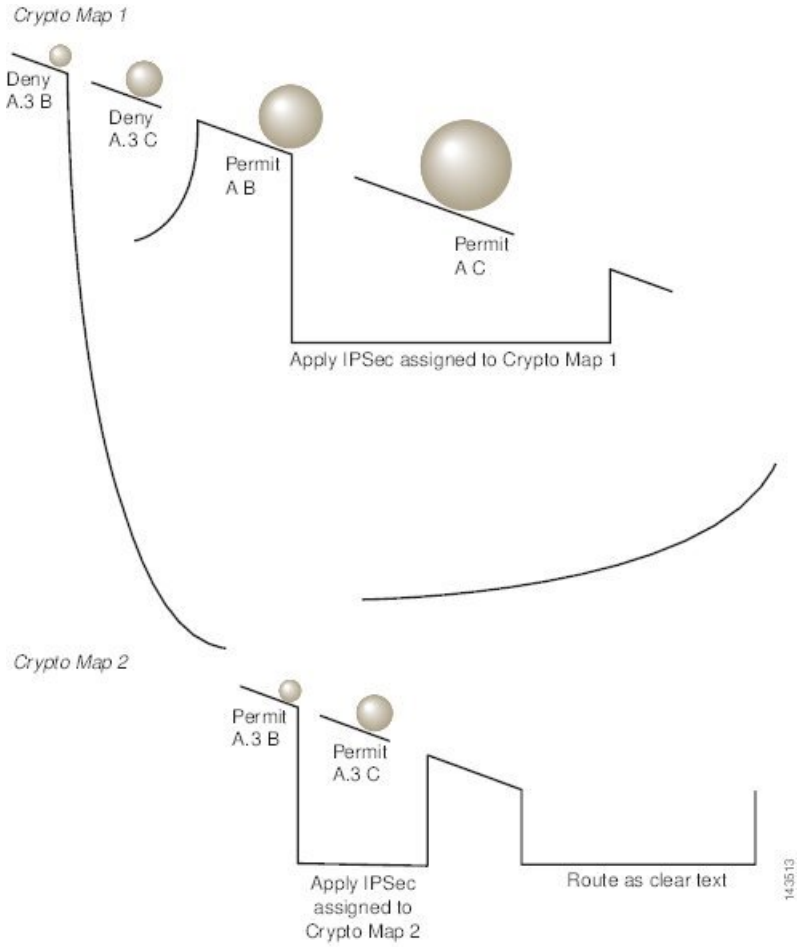
Après avoir créé les listes de contrôle d'accès, vous attribuez un ensemble de transformation à chaque carte de chiffrement pour appliquer l'IPsec requis à chaque paquet correspondant.

Les ACL en cascade consistent à insérer des ACE de refus pour contourner l'évaluation par rapport à une ACL et reprendre l'évaluation par rapport à une ACL suivante dans l'ensemble de cartes de chiffrement. Comme vous pouvez associer chaque carte de chiffrement à des paramètres IPsec différents, vous pouvez utiliser les ACE de refus pour exclure le trafic spécial d'une évaluation plus approfondie dans la carte de chiffrement correspondante et faire correspondre le trafic spécial pour permettre aux instructions d'une autre carte de chiffrement de fournir ou d'exiger une sécurité différente. Le numéro de séquence attribué à l'ACL de chiffrement détermine sa position dans la séquence d'évaluation au sein de l'ensemble de cartes de chiffrement.

L'illustration suivante montre les ACL en cascade créées à partir des ACE conceptuelles dans cet exemple. La signification de chaque symbole est définie comme suit :

	Carte de chiffrement dans un ensemble de cartes de chiffrement.
	(Espace sur une ligne droite) Quitter une carte de chiffrement lorsqu'un paquet correspond à une entrée ACE.
	Paquet qui correspond à la description d'une ACE. Chaque cercle de taille différente représente un paquet distinct correspondant à l'ACE concernée dans la figure. Les différences de taille représentent simplement les différences dans la source et la destination de chaque paquet.
	Redirection vers la carte de chiffrement suivante dans l'ensemble de cartes de chiffrement.
	Réponse lorsqu'un paquet correspond à une ACE ou ne parvient pas à correspondre à toutes les ACE autorisées dans un ensemble de cartes de chiffrement.

Illustration 2 : ACL en cascade dans un ensemble de cartes de chiffrement



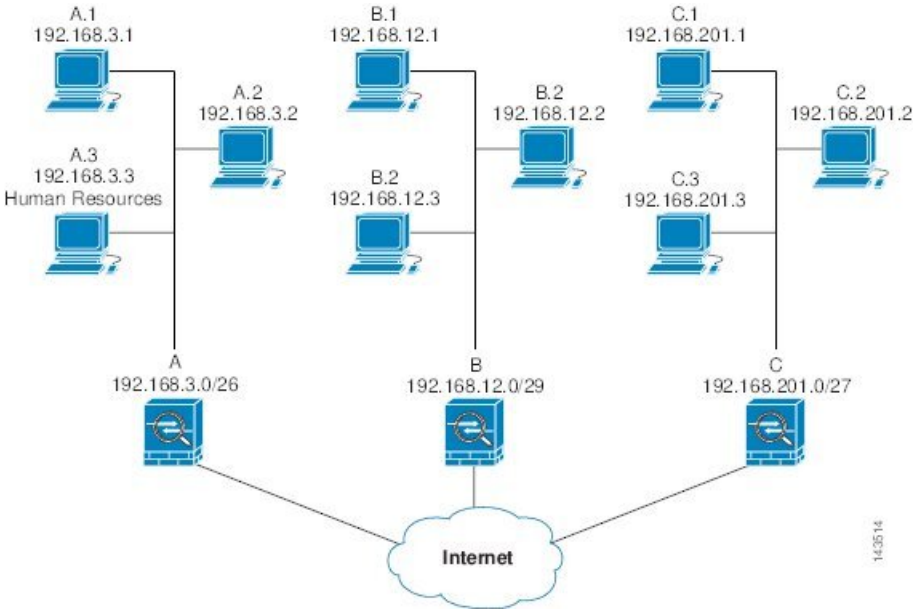
L'appareil de sécurité A évalue un paquet provenant de l'hôte A.3 jusqu'à ce qu'il corresponde à une ACE permit, puis tente d'appliquer la sécurité IPsec associée à la carte de chiffrement. Chaque fois que le paquet correspond à une ACE deny, l'ASA ignore les ACE restantes dans la carte de chiffrement et reprend l'évaluation avec la carte de chiffrement suivante, selon le numéro de séquence qui lui est attribué. Ainsi, dans l'exemple, si l'appareil de sécurité A reçoit un paquet provenant de l'hôte A.3, il le fait correspondre à une ACE deny dans la première carte de chiffrement, puis reprend l'évaluation de ce paquet avec la carte de chiffrement suivante. Lorsqu'il fait correspondre le paquet à l'ACE permit de cette carte de chiffrement, il applique la sécurité IPsec associée (chiffrement renforcé et renouvellement fréquent).

Pour terminer la configuration ASA dans le réseau d'exemple, nous attribuons des cartes de chiffrement miroir aux ASA B et C. Toutefois, comme les ASA ignorent les ACE deny lors de l'évaluation du trafic entrant chiffré, nous pouvons omettre les équivalents miroir des ACE deny A.3 B et deny A.3 C, et donc aussi les équivalents miroir de la Crypto Map 2. La configuration des ACL en cascade dans les ASA B et C est donc inutile.

Le tableau suivant présente les listes de contrôle d'accès attribuées aux cartes de chiffrement configurées pour les trois ASA, A, B et C :

appareil de sécurité A		appareil de sécurité B		appareil de sécurité C	
Carte de chiffrement **Séquence** **Non.**	**Modèle ACE**	**Carte de chiffrement** **Séquence** **Non.**	**Modèle ACE**	**Carte de chiffrement** **Séquence** **Non.**	**Modèle ACE**
1	deny A.3 B	1	permit B A	1	permit C A
	deny A.3 C				
	permit A B				
	permit A C		permit B C		permit C B
2	permit A.3 B				
	permit A.3 C				

L'illustration suivante fait correspondre les adresses conceptuelles présentées précédemment aux adresses IP réelles.



Les ACE réelles affichées dans le tableau suivant garantissent que tous les paquets IPsec soumis à l'évaluation dans ce réseau reçoivent les paramètres IPsec appropriés.

Appareil de sécurité	Crypto-carte Séquence Non.	Modèle ACE	ACE réelles
A	1	deny A.3 B	deny 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		deny A.3 C	deny 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
		permit A B	permit 192.168.3.0 255.255.255.192 192.168.12.0 255.255.255.248
		permit A C	permit 192.168.3.0 255.255.255.192 192.168.201.0 255.255.255.224
	2	permit A.3 B	permit 192.168.3.3 255.255.255.192 192.168.12.0 255.255.255.248
		permit A.3 C	permit 192.168.3.3 255.255.255.192 192.168.201.0 255.255.255.224
B	Non nécessaire	permit B A	permit 192.168.12.0 255.255.255.248 192.168.3.0 255.255.255.192
		permit B C	permit 192.168.12.0 255.255.255.248 192.168.201.0 255.255.255.224
C	Non nécessaire	permit C A	permit 192.168.201.0 255.255.255.224 192.168.3.0 255.255.255.192
		permit C B	permit 192.168.201.0 255.255.255.224 192.168.12.0 255.255.255.248

Vous pouvez appliquer le même raisonnement affiché dans l'exemple de réseau pour utiliser les ACL en cascade afin d'affecter différents paramètres de sécurité à différents hôtes ou sous-réseaux protégés par un ASA.

Remarque Par défaut, l'ASA ne prend pas en charge le trafic IPsec destiné à la même interface que celle par laquelle il entre. Les appellations de ce type de trafic incluent « demi-tour », « hub-and-spoke » et « hairpinning ». Cependant, vous pouvez configurer IPsec pour prendre en charge le trafic en demi-tour en ajoutant une entrée ACE qui autorise le trafic vers et depuis le réseau. Par exemple, pour prendre en charge le trafic en demi-tour sur l'appareil de sécurité B, ajoutez une entrée ACE conceptuelle « permit B B » à ACL1. L'ACE réelle serait la suivante :**permit 192.168.12.0 255.255.255.248 192.168.12.0 255.255.255.248**

Définir les clés de l'infrastructure à clé publique (PKI)

Vous devez définir l'infrastructure à clé publique (PKI) pour qu'un administrateur puisse choisir les algorithmes ECDSA de la suite B lors de la génération ou de la mise à zéro d'une paire de clés :

Avant de commencer

Si vous configurez une carte de chiffrement pour utiliser un point de confiance RSA ou ECDSA pour l'authentification, vous devez d'abord générer l'ensemble de clés. Vous pouvez ensuite créer le point de confiance et le référencer dans la configuration du groupe de tunnels.

Procédure

Étape 1 Choisissez l'algorithme ECDSA Suite B lors de la génération d'une paire de clés :

crypto key generate [rsa [general-keys | label <name> | modules [512 | 768 | 1024 | 2048 | 4096] | noconfirm | usage-keys] | ecdsa [label <name> | elliptic-curve [256 | 384 | 521] | noconfirm]]

Étape 2 Choisissez l'algorithme ECDSA Suite B lors de la réinitialisation d'une paire de clés :

crypto key zeroize [rsa | ecdsa] [default | label <name> | noconfirm]

Appliquer les cartes de chiffrement aux interfaces

Vous devez attribuer 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'affectation de l'ensemble de cartes de chiffrement à une interface demande à l'ASA d'évaluer tout le trafic par rapport à l'ensemble de cartes de chiffrement et d'utiliser la politique précisée lors de la connexion ou de la négociation de la SA.

L'affectation d'une carte de chiffrement à une interface initialise également les structures de données d'exécution, telles que la base de données SA et la base de données des politiques de sécurité. La réaffectation d'une carte de chiffrement modifiée à l'interface resynchronise les structures de données d'exécution avec la configuration de la carte de chiffrement. De plus, l'ajout de nouveaux homologues par l'utilisation de nouveaux numéros de séquence et la réaffectation de la carte de chiffrement ne supprime pas les connexions existantes.

Utiliser les listes de contrôle d'interface

Par défaut, l'ASA permet aux paquets IPsec de contourner les listes de contrôle d'interface. Si vous souhaitez appliquer les listes de contrôle d'interface au trafic IPsec, utilisez la forme **no** de la commande **sysopt connection permit-vpn**.

La liste de contrôle d'accès de carte de chiffrement liée à l'interface sortante autorise ou refuse les paquets IPsec dans le tunnel VPN. IPsec authentifie et déchiffre les paquets qui arrivent d'un tunnel IPsec et les soumet à une évaluation par rapport à l'ACL associée au tunnel.

Les listes de contrôle d'accès définissent le trafic IP à protéger. Par exemple, vous pouvez créer des listes de contrôle d'accès pour protéger tout le trafic IP entre deux sous-réseaux ou deux hôtes. (Ces listes de contrôle d'accès sont similaires aux listes de contrôle d'accès utilisées avec la commande **access-group**. Cependant, avec la commande **access-group**, l'ACL détermine le trafic à transférer ou à bloquer au niveau d'une interface.)

Avant l'affectation aux cartes de chiffrement, les listes de contrôle d'accès ne sont pas spécifiques à IPsec. Chaque carte de chiffrement fait référence aux listes de contrôle d'accès et détermine les propriétés IPsec à appliquer à un paquet s'il correspond à une autorisation dans l'une des listes de contrôle d'accès.

Les ACL attribuées aux cartes de chiffrement IPsec ont quatre fonctions principales :

- Sélectionner le trafic sortant à protéger par IPsec (autoriser = protéger).
- Déclencher une négociation ISAKMP pour les données circulant sans SA établie.
- Traiter le trafic entrant pour filtrer et ignorer le trafic qui aurait dû être protégé par IPsec.

- Déterminer s'il faut accepter les demandes de SA IPsec lors du traitement de la négociation IKE de l'homologue. (La négociation s'applique uniquement aux entrées **ipsec-isakmp crypto map**.) L'homologue doit permettre un flux de données associé à une entrée de commande **ipsec-isakmp crypto map** afin d'assurer l'acceptation pendant la négociation.

Remarque Si vous supprimez le seul élément d'une ACL, l'ASA supprime également la carte de chiffrement associée.

Si vous modifiez une ACL actuellement référencée par une ou plusieurs cartes de chiffrement, utilisez la commande **crypto map interface** pour réinitialiser la base de données SA d'exécution. Consultez la commande **crypto map** pour obtenir plus d'informations.

Nous vous recommandons que, pour chaque ACL de chiffrement spécifiée pour une carte de chiffrement statique que vous définissez sur l'homologue local, vous définissiez une ACL de chiffrement « image miroir » sur l'homologue distant. Les cartes de chiffrement doivent également prendre en charge des transformations communes et faire référence à l'autre système en tant qu'homologue. Cela garantit un traitement correct d'IPsec par les deux homologues.

Remarque Chaque carte de chiffrement statique doit définir une ACL et un homologue IPsec. Si l'un des deux éléments manque, la carte de chiffrement est incomplète et l'ASA abandonne tout trafic qu'il n'a pas déjà mis en correspondance avec une carte de chiffrement antérieure complète. Utilisez la commande **show conf** pour vous assurer que chaque carte de chiffrement est complète. Pour corriger une carte de chiffrement incomplète, supprimez-la, ajoutez les entrées manquantes, puis réappliquez-la.

L'ACL de chiffrement ne prend pas en charge les entrées en double ou qui se chevauchent.

Nous déconseillons l'utilisation du mot-clé **any** pour spécifier les adresses de source ou de destination dans les ACL cryptographiques, car elles causent des problèmes. Nous vous déconseillons fortement l'instruction de commande **permit any any**, car elle fait ce qui suit :

- Protège tout le trafic sortant, y compris tout le trafic protégé envoyé à l'homologue spécifié dans le crypto map correspondant.
- Nécessite une protection pour tout le trafic entrant.

Dans ce scénario, l'ASA abandonne secrètement tous les paquets entrants qui ne disposent pas de protection IPsec.

Assurez-vous de définir les paquets à protéger. Si vous utilisez le mot-clé **any** dans une instruction **permit**, préfacez-le d'une série d'instructions **deny** pour filtrer le trafic qui, autrement, correspondrait à cette instruction **permit** que vous ne souhaitez pas protéger.

Remarque Le trafic traversant déchiffré est autorisé à partir du client malgré la présence d'un groupe d'accès sur l'interface externe, qui appelle une liste de contrôle d'accès deny ip any any, alors que **no sysopt connection permit-vpn** est configuré.

Les utilisateurs qui souhaitent contrôler l'accès au réseau protégé via un VPN de site à site ou d'accès à distance en utilisant la commande **no sysopt permit** en conjonction avec une liste de contrôle d'accès (ACL) sur l'interface externe ne réussissent pas.

Dans cette situation, lorsque l'accès de gestion interne est activé, l'ACL n'est pas appliquée et les utilisateurs peuvent toujours se connecter à l'appareil de sécurité à l'aide de SSH. Le trafic vers les hôtes sur le réseau interne est bloqué correctement par la liste de contrôle d'accès, mais le trafic traversant déchiffré vers l'interface interne n'est pas bloqué.

Les commandes **ssh** et **http** ont une priorité plus élevée que les ACL. En d'autres termes, pour refuser le trafic SSH, Telnet ou ICMP vers le périphérique à partir de la session VPN, utilisez les commandes **ssh**, **telnet** et **icmp** , auxquelles l'ensemble local d'adresses IP refusé doit être ajouté.

Que le trafic soit entrant ou sortant, l'ASA évalue le trafic en fonction des ACL attribuées à une interface. Suivez ces étapes pour affecter IPsec à une interface :

Procédure

Étape 1 Créez les ACL à utiliser pour IPsec.

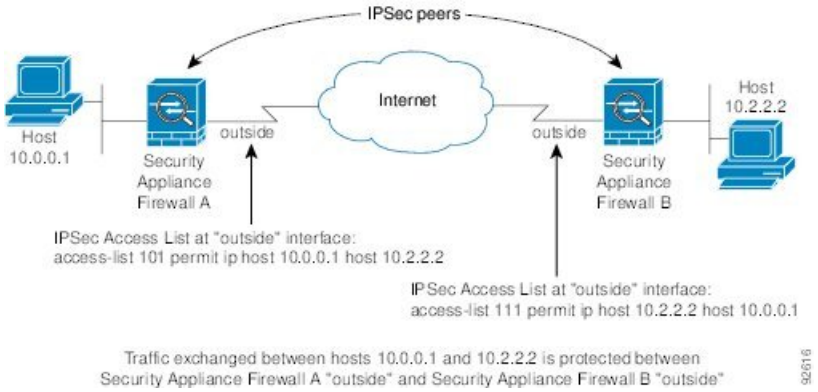
Étape 2 Mappez les listes à une ou plusieurs cartes de chiffrement, en utilisant le même nom de carte de chiffrement.

Étape 3 Mappez les ensembles de transformation IKEv1 ou les propositions IKEv2 aux cartes de chiffrement pour appliquer IPsec aux flux de données.

Étape 4 Appliquez les cartes de chiffrement collectivement en tant qu'ensemble de cartes de chiffrement en attribuant le nom de carte de chiffrement qu'elles partagent à l'interface.

Exemple

Dans cet exemple, la protection IPsec s'applique au trafic entre l'hôte 10.0.0.1 et l'hôte 10.2.2.2, car les données quittent l'interface externe sur l'ASA A vers l'hôte 10.2.2.2.



L'ASA A évalue le trafic de l'hôte 10.0.0.1 à l'hôte 10.2.2.2, comme suit :

- source = hôte 10.0.0.1
- dest = hôte 10.2.2.2

L'ASA A évalue également le trafic de l'hôte 10.2.2.2 à l'hôte 10.0.0.1, comme suit :

- source = hôte 10.2.2.2
- dest = hôte 10.0.0.1

La première instruction permit qui correspond au paquet évalué détermine la portée de la SA IPsec.

Modifier la durée de vie des SA IPsec

Vous pouvez modifier les valeurs de durée de vie globale que l'ASA utilise lors de la négociation de nouvelles SA IPsec. Vous pouvez remplacer ces valeurs de durée de vie globale pour une carte de chiffrement particulière.

Les SA IPsec utilisent une clé secrète partagée et dérivée. La clé fait partie intégrale de la SA ; les clés expirent ensemble pour exiger l'actualisation de la clé. Chaque SA a deux durées de vie : temporelle et en fonction du volume du trafic. Une SA expire après la durée de vie respective et les négociations commencent pour une nouvelle. Les durées de vie par défaut sont de 28 800 secondes (8 heures) et de 4 608 000 kilooctets (10 mA par seconde pendant une heure).

Si vous modifiez une durée de vie globale, l'ASA abandonne le tunnel. Il utilise la nouvelle valeur lors de la négociation des SA établies ultérieurement.

Lorsqu'une carte de chiffrement n'a pas de valeurs de durée de vie configurées et que l'ASA demande un nouveau SA, il insère les valeurs de durée de vie globale utilisées dans la SA existante dans la demande envoyée à l'homologue. Lorsqu'un homologue reçoit une demande de négociation, il utilise la plus petite des durées de vie proposées par l'homologue ou configurées localement comme durée de vie des nouvelles SA.

Les homologues négocient un nouveau SA avant de dépasser le seuil de durée de vie de la SA existante pour s'assurer qu'un nouveau SA est prêt à l'expiration de la SA existante. Les homologues négocient une nouvelle SA lorsqu'il reste environ 5 à 15 % de la durée de vie de la SA existante.

Remarque Nous vous recommandons de configurer différents temporisateurs d'association de sécurité de chaque côté du tunnel IKEv2 de site à site pour éviter la collision de renouvellement.

Modifier le routage VPN

Par défaut, des recherches d'adjacence par paquet sont effectuées pour les paquets ESP externes ; aucune recherche n'est effectuée pour les paquets envoyés via le tunnel IPsec.

Dans certaines topologies de réseau, lorsqu'une mise à jour de routage a modifié le chemin du paquet interne, mais que le tunnel IPsec local est toujours actif, les paquets qui passent par le tunnel peuvent ne pas être acheminés correctement et ne pas atteindre leur destination.

Pour éviter cela, activez les recherches de routage par paquet pour les paquets internes IPsec.

Avant de commencer

Pour éviter tout impact sur les performances de ces recherches, cette fonctionnalité est désactivée par défaut. Activez-le uniquement lorsque cela est nécessaire.

Procédure

Activez les recherches de routage par paquet pour les paquets internes IPsec.

[**no**] [**crypto**] **ipsec inner-routing-lookup**

Remarque
Une fois configurée, cette commande s'applique uniquement aux tunnels qui ne sont pas fondés sur une VTI.

Exemple

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
 crypto ipsec ikev2 ipsec-proposal GCM
 protocol esp encryption aes-gcm
 protocol esp integrity null
 crypto ipsec inner-routing-lookup
```

Créer des cartes de chiffrement statiques

Pour créer une configuration IPsec de base à l'aide d'une carte de chiffrement statique, procédez comme suit :

Procédure

Étape 1 Pour créer une ACL afin de définir le trafic à protéger, saisissez la commande suivante :

access-list *access-list-name* **{deny | permit} ip** *source source-netmask destination destination-netmask*

L'argument *access-list-name* précise l'identifiant de l'ACL, sous la forme d'une chaîne ou d'un entier d'une longueur maximale de 241 caractères. Les *destination-netmask* et *source-netmask* spécifient une adresse réseau IPv4 et un masque de sous-réseau. Dans cet exemple, le mot-clé **permit** fait en sorte que tout trafic correspondant aux conditions spécifiées soit protégé par chiffrement.

Exemple :

```
hostname(config)# access-list 101 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

Étape 2 Pour configurer un ensemble de transformation IKEv1 qui définit la protection du trafic, saisissez la commande suivante :

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

Le chiffrement spécifie quelle méthode de chiffrement protège les flux de données IPsec :

- esp-aes : utilise AES avec une clé de 128 bits.
- esp-aes-192 : utilise AES avec une clé de 192 bits.
- esp-aes-256 : utilise AES avec une clé de 256 bits.
- esp-null : pas de chiffrement.

L'authentification spécifie la méthode d'authentification pour protéger les flux de données IPsec :

- esp-sha-hmac : utilise SHA/HMAC-160 comme algorithme de hachage.
- esp-none : aucune authentification HMAC.

Exemple :

Dans cet exemple, myset1, myset2 et aes_set sont les noms des ensembles de transformation.

```
hostname(config)# crypto ipsec ikev1 transform-set myset1 esp-aes esp-sha-hmac
hostname(config)#
hostname(config)# crypto ipsec ikev1 transform-set aes_set esp-md5-hmac esp-aes-256
```

Étape 3 Pour configurer une proposition IKEv2 qui définit également la protection du trafic, saisissez la commande suivante :

crypto ipsec ikev2 ipsec-proposal [*proposal tag*]

La balise de proposition est le nom de la proposition IKEv2 IPsec, une chaîne de 1 à 64 caractères.

Créez la proposition et passez en mode de configuration ipsec proposal, où vous pouvez spécifier plusieurs types de chiffrement et d'intégrité pour la proposition.

Exemple :

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

Dans cet exemple, secure est le nom de la proposition. Saisissez un protocole et les types de chiffrement :

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

Exemple :

Cette commande choisit l'algorithme AES-GCM ou AES-GMAC à utiliser :

[**no**] **protocol esp encryption** [**aes| aes-192 | aes-256 | aes-gcm| aes-gcm-192 | aes-gcm-256| null]**

Si SHA-2 ou null est choisi, vous devez choisir l'algorithme à utiliser comme algorithme d'intégrité IPsec. Vous devez choisir l'algorithme d'intégrité null si AES-GCM/GMAC est configuré comme algorithme de chiffrement :

[**no**] **protocol esp integrity** [**sha-1** | **sha-256** | **sha-384** | **sha-512** | **null**]

Remarque
Vous devez choisir l'algorithme d'intégrité nulle si AES-GCM/GMAC a été configuré comme algorithme de chiffrement. SHA-256 peut être utilisé pour l'intégrité et PRF pour établir des tunnels IKEv2, mais il peut également être utilisé pour la protection de l'intégrité ESP.

Étape 4 (Facultatif) Un administrateur peut activer le vieillissement de la PMTU du chemin et définir l'intervalle auquel la valeur PMTU est réinitialisée à sa valeur d'origine.

[**no**] **crypto ipsec security-association pmtu-aging** *reset-interval*

Étape 5 Pour créer une carte cryptographique, effectuez les étapes site à site suivantes en mode monocontexte ou multicontexte :

a) Attribuez une ACL à une carte de chiffrement :

crypto map *map-name seq-num* **match address** *access-list-name*

Un ensemble de cartes de chiffrement est un ensemble d'entrées de cartes de chiffrement, chacune avec un numéro de séquence différent (*seq-num)*, mais le même *nom de carte*. Utilisez l'argument *access-list-name* pour préciser l'identifiant de l'ACL, sous la forme d'une chaîne ou d'un entier d'une longueur maximale de 241 caractères. Dans l'exemple suivant, mymap est le nom de l'ensemble de cartes de chiffrement. Le numéro de séquence 10 de l'ensemble de cartes de chiffrement est utilisé pour classer plusieurs entrées au sein d'un même ensemble. Plus le numéro de séquence est bas, plus la priorité est élevée.

Exemple :

Dans cet exemple, l'ACL nommée 101 est affectée à la carte de chiffrement mymap.

```
crypto map mymap 10 match address 101
```

b) Précisez l'homologue vers lequel le trafic protégé par IPsec peut être acheminé :

crypto map *map_name sequence number***set peer** *ip_address1 [ip_address2] [...]*

Exemple :

```
crypto map mymap 10 set peer 192.168.1.100
```

L'ASA configure une SA avec l'homologue auquel est attribuée l'adresse IP 192.168.1.100.

Remarque
À partir de la version 9.14(1), l'ASA prend en charge plusieurs homologues dans la carte de chiffrement IKEv2. Vous pouvez ajouter un maximum de 10 homologues à la liste.

c) Précisez quels ensembles de transformation IKEv1 ou propositions IKEv2 sont autorisés pour cette carte de chiffrement. Répertoriez plusieurs ensembles de transformation ou propositions par ordre de priorité (priorité la plus élevée en premier). Vous pouvez spécifier jusqu'à 11 ensembles de transformation ou propositions dans une carte de chiffrement à l'aide de l'une ou l'autre de ces deux commandes :

crypto map *map-name seq-num* **set ikev1 transform-set** *transform-set-name1 [transform-set-name2*, *…transform-set-name11*]

OU

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2, … proposal-name11*]

Proposal-name1 et *proposal-name11* spécifient un ou plusieurs noms des propositions IPsec pour IKEv2. Chaque entrée de carte de chiffrement prend en charge jusqu'à 11 propositions.

Exemple :

Dans cet exemple pour IKEv1, lorsque le trafic correspond à l'ACL 101, la SA peut utiliser myset1 (première priorité) ou myset2 (seconde priorité), selon l'ensemble de transformation qui correspond aux ensembles de transformation de l'homologue.

```
crypto map mymap 10 set ikev1 transform-set myset1 myset2
```

d) (Optionnel) Pour IKEv2, spécifiez le **mode** pour appliquer le chiffrement et l'authentification ESP au tunnel. Cela permet de déterminer quelle partie du paquet IP d'origine a été appliquée à l'ESP.

crypto map *map-name seq-num* **set ikev2 mode** [**transport | tunnel | transport-require**]

- **Mode tunnel** : (par défaut) le mode d'encapsulation est réglé sur Mode tunnel. Le mode tunnel applique le chiffrement et l'authentification ESP à l'ensemble du paquet IP d'origine (en-tête IP et données), masquant ainsi les adresses source et destination finales. Le datagramme IP d'origine entier est chiffré et devient la charge utile d'un nouveau paquet IP.

  Ce mode permet à un périphérique réseau, comme un routeur, de servir de serveur mandataire IPsec. C'est-à-dire que le routeur effectue le chiffrement au nom des hôtes. Le routeur source chiffre les paquets et les transfère dans le tunnel IPsec. Le routeur de destination déchiffre le datagramme IP d'origine et le transmet au système de destination.

  Le principal avantage du mode de tunnel est qu'il n'est pas nécessaire de modifier les systèmes d'extrémité pour profiter des avantages d'IPsec. Le mode tunnel offre également une protection contre l'analyse du trafic; Avec le mode tunnel, un attaquant ne peut déterminer que les points terminaux du tunnel, et non la source et la destination réelles des paquets acheminés dans le tunnel, même s'ils sont identiques aux points terminaux du tunnel.

- **Mode transport** : le mode d'encapsulation est le mode transport avec option de repli en mode tunnel, si l'homologue ne le prend pas en charge. En mode transport, seules les données utiles IP sont chiffrées, et les en-têtes IP d'origine demeurent inchangés.

  Ce mode présente l'avantage d'ajouter seulement quelques octets à chaque paquet et de permettre aux périphériques du réseau public de voir la source et la destination finales du paquet. Le mode de transport vous permet d'activer le traitement spécial (par exemple, QoS) sur le réseau intermédiaire en fonction des informations contenues dans l'en-tête IP. Cependant, l'en-tête de couche 4 est chiffré, ce qui limite l'examen du paquet.

- **Transport requis** : le mode d'encapsulation est réglé au mode transport uniquement, le retour au mode tunnel n'est pas autorisé.

Où le mode d'encapsulation **tunnel** est le mode par défaut. Le mode d'encapsulation **transport** est le mode transport avec option de repli en mode tunnel si l'homologue ne le prend pas en charge, et le mode d'encapsulation **transport-require** impose uniquement le mode transport.

Remarque
Le mode transport n'est pas recommandé pour les VPN d'accès à distance.

Des exemples de négociation du mode d'encapsulation sont les suivants :

- Si l'initiateur propose le mode transport et que le répondeur répond en mode tunnel, l'initiateur passera en mode tunnel.
- Si l'initiateur propose le mode tunnel et que le répondeur répond en mode transport, le répondeur passera en mode tunnel.
- Si l'initiateur propose le mode tunnel et que le répondeur est en mode transport-require, le message NO PROPOSAL CHOSEN sera envoyé par le répondeur.
- De même, si l'initiateur est en mode transport-require et que le répondeur est en mode tunnel, le message NO PROPOSAL CHOSEN sera envoyé par le répondeur.

e) (Facultatif) Précisez une durée de vie de SA pour la carte de chiffrement si vous souhaitez remplacer la durée de vie globale.

crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

Map-name spécifie le nom de l'ensemble de cartes de chiffrement. *Seq-num* spécifie le numéro que vous attribuez à l'entrée de carte de chiffrement. Vous pouvez définir les deux durées de vie en fonction du temps ou des données transmises. Cependant, la durée de vie des données transmises s'applique uniquement au VPN de site à site et ne s'applique pas au VPN d'accès à distance.

Exemple :

Cet exemple raccourcit la durée de vie de la carte de chiffrement mymap 10 à 2 700 secondes (45 minutes). La durée de vie du volume du trafic n'est pas modifiée.

```
crypto map mymap 10 set security-association lifetime seconds 2700
```

f) (Facultatif) Précisez qu'IPsec exige la Perfect Forward Secrecy (PFS) lors de la demande d'une nouvelle SA pour cette carte de chiffrement, ou qu'il exige la PFS dans les demandes reçues de l'homologue :

crypto map *map_name seq-num* **set pfs** [**group14** | **group15** | **group16** | **group19** | **group20** | **group21**]

Exemple :

Cet exemple exige la PFS lors de la négociation d'une nouvelle SA pour la carte de chiffrement mymap 10. L'ASA utilise le groupe de module premier Diffie-Hellman de 2 048 bits dans la nouvelle SA.

```
crypto map mymap 10 set pfs group14
```

g) (Facultatif) Activez l'injection de route inverse (RRI) pour toute connexion basée sur cette entrée de carte de chiffrement.

crypto map *map_name seq-num* **set reverse-route** [**dynamic**]

Si dynamic n'est pas spécifié, la RRI est effectuée lors de la configuration et est considérée comme statique, restant en place jusqu'à ce que la configuration soit modifiée ou supprimée. L'ASA ajoute automatiquement des routes statiques à la table de routage et communique ces routes à son réseau privé ou aux routeurs de frontière à l'aide d'OSPF. N'activez pas RRI si vous spécifiez une source/destination (0.0.0.0/0.0.0.0) comme réseau protégé, car cela aura une incidence sur le trafic qui utilise votre route par défaut.

Si dynamic est spécifié, les routes sont créées lors de l'établissement réussi des associations de sécurité (SA) IPsec et supprimées après la suppression des SA IPsec.

Remarque
La RRI dynamique est prise en charge sur les cartes de chiffrement statiques basées sur IKEv2 uniquement.

Exemple :

```
crypto map mymap 10 set reverse-route dynamic
```

Étape 6 Appliquez un ensemble de cartes de chiffrement à une interface pour évaluer le trafic IPsec :

crypto map *map-name* **interface** *interface-name*

Map-name spécifie le nom de l'ensemble de cartes de chiffrement. *Interface-name* spécifie le nom de l'interface sur laquelle activer ou désactiver la négociation ISAKMP IKEv1.

Exemple :

Dans cet exemple, l'ASA évalue le trafic passant par l'interface externe en fonction de la carte de chiffrement mymap afin de déterminer s'il doit être protégé.

```
crypto map mymap interface outside
```

Créer des cartes de chiffrement dynamiques

Une carte de chiffrement dynamique est une carte de chiffrement sans que tous les paramètres soient configurés. Elle agit comme un modèle de politique où les paramètres manquants sont ensuite appris dynamiquement, à la suite d'une négociation IPsec, pour correspondre aux exigences de l'homologue. L'ASA applique une carte de chiffrement dynamique pour permettre à un homologue de négocier un tunnel si son adresse IP n'est pas déjà identifiée dans une carte de chiffrement statique. Cela se produit avec les types d'homologues suivants :

- Homologues avec des adresses IP publiques attribuées dynamiquement.

  Les homologues de site à site et d'accès à distance peuvent utiliser DHCP pour obtenir une adresse IP publique. L'ASA utilise cette adresse uniquement pour amorcer le tunnel.

- Homologues avec des adresses IP privées attribuées dynamiquement.

  Les homologues demandant des tunnels d'accès à distance ont généralement des adresses IP privées attribuées par la tête de réseau. En général, les tunnels de site à site ont un ensemble prédéfini de réseaux privés utilisés pour configurer des cartes statiques et, par conséquent, pour établir des SA IPsec.

En tant qu'administrateur configurant des cartes de chiffrement statiques, vous ne connaissez peut-être pas les adresses IP attribuées dynamiquement (par DHCP ou toute autre méthode), et vous pourriez ne pas connaître les adresses IP privées d'autres clients, quelle que soit la façon dont elles ont été attribuées. Les clients VPN n'ont généralement pas d'adresses IP statiques ; ils nécessitent une carte de chiffrement dynamique pour permettre la négociation IPsec. Par exemple, la tête de réseau attribue l'adresse IP à un client VPN Cisco lors de la négociation IKE, que le client utilise ensuite pour négocier les SA IPsec.

Remarque Une carte de chiffrement dynamique ne nécessite que le paramètre **transform-set**.

Les cartes de chiffrement dynamiques peuvent faciliter la configuration IPsec, et nous les recommandons pour une utilisation dans les réseaux où les homologues ne sont pas toujours prédéfinis. Utilisez des cartes de chiffrement dynamiques pour les clients VPN Cisco (comme les utilisateurs mobiles) et les routeurs qui obtiennent des adresses IP attribuées dynamiquement.

Astuces Faites preuve de prudence lorsque vous utilisez le mot-clé **any** dans les entrées **permit** des cartes de chiffrement dynamiques. Si le trafic couvert par une telle entrée **permit** (d'autorisation) peut inclure du trafic de multidiffusion ou de diffusion, insérez des entrées **deny** (de refus) pour la plage d'adresses appropriée dans la liste de contrôle d'accès. N'oubliez pas d'insérer des entrées **deny** (de refus) pour le trafic de diffusion en réseau et en sous-réseau, et pour tout autre trafic qu'IPsec ne doit pas protéger.

Les cartes de chiffrement dynamiques fonctionnent uniquement pour négocier les SA avec les homologues distants qui amorcent la connexion. L'ASA ne peut pas utiliser de cartes de chiffrement dynamiques pour établir des connexions à un homologue distant. Avec une carte de chiffrement dynamique, si le trafic sortant correspond à une entrée d'autorisation dans une liste de contrôle d'accès et que la SA correspondante n'existe pas encore, l'ASA abandonne le trafic.

Un ensemble de cartes de chiffrement peut inclure une carte de chiffrement dynamique. Les ensembles de cartes de chiffrement dynamiques doivent être les cartes de chiffrement de priorité la plus basse dans l'ensemble de cartes de chiffrement (c'est-à-dire qu'ils doivent avoir les numéros de séquence les plus élevés) pour que l'ASA évalue les autres cartes de chiffrement en premier. Il examine l'ensemble de cartes de chiffrement dynamiques uniquement lorsque les autres entrées de carte (statiques) ne correspondent pas.

Comme pour les ensembles de cartes de chiffrement statiques, un ensemble de cartes de chiffrement dynamiques se compose de toutes les cartes de chiffrement dynamiques ayant le même nom de carte dynamique. Le dynamic-seq-num différencie les cartes de chiffrement dynamiques dans un ensemble. Si vous configurez une carte de chiffrement dynamique, insérez une ACL permit pour identifier le flux de données de l'homologue IPsec pour l'ACL de chiffrement. Sinon, l'ASA accepte toute identité de flux de données proposée par l'homologue.

Mise en garde N'affectez pas de routes par défaut au module pour le trafic à tunneliser vers une interface ASA configurée avec un ensemble de cartes de chiffrement dynamiques. Pour identifier le trafic qui doit être tunnellisé, ajoutez les listes de contrôle d'accès à la carte de chiffrement dynamique. Faites attention à identifier les ensembles d'adresses appropriés lors de la configuration des listes de contrôle d'accès associées aux tunnels d'accès à distance. Utilisez l'injection de route inverse pour installer les routes uniquement une fois que le tunnel est opérationnel.

Créez une entrée de carte de chiffrement dynamique en mode contexte unique ou multiple. Vous pouvez combiner des entrées de carte statiques et dynamiques dans un seul ensemble de cartes de chiffrement.

Procédure

Étape 1 (Facultatif) Attribuez une liste de contrôle d'accès à une carte de chiffrement dynamique :

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *access-list-name*

Cela détermine quel trafic doit être protégé et non protégé. *Dynamic-map-name* spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique.

Exemple :

Dans cet exemple, l'ACL 101 est affecté à la carte de chiffrement dynamique dyn1. Le numéro de séquence de carte est 10.

```
crypto dynamic-map dyn1 10 match address 101
```

Étape 2 Précisez quels ensembles de transformation IKEv1 ou propositions IKEv2 sont autorisés pour cette carte de chiffrement dynamique. Énumérez plusieurs ensembles de transformations ou propositions en ordre de priorité (la priorité la plus élevée en premier) en utilisant la commande pour les ensembles de transformation IKEv1 ou les propositions IKEv2 :

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1*, [*transform-set-name2*, ...*transform-set-name9*]

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev2 ipsec-proposal** *proposal-name1* [*proposal-name2, … proposal-name11*]

Dynamic-map-name spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique. Le *transform-set-name* est le nom de l'ensemble de transformation en cours de création ou de modification. Le *nom de la proposition* spécifie un ou plusieurs noms des propositions IPsec pour IKEv2.

Exemple :

Dans cet exemple pour IKEv1, lorsque le trafic correspond à l'ACL 101, la SA peut utiliser myset1 (première priorité) ou myset2 (seconde priorité), selon l'ensemble de transformation qui correspond aux ensembles de transformation de l'homologue.

```
crypto dynamic-map dyn 10 set ikev1 transform-set myset1 myset2
```

Étape 3 (Facultatif) Précisez la durée de vie de la SA pour l'entrée de carte de chiffrement dynamique si vous souhaitez remplacer la valeur de durée de vie globale :

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

Dynamic-map-name spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique. Vous pouvez définir les deux durées de vie en fonction du temps ou des données transmises. Cependant, la durée de vie des données transmises s'applique uniquement au VPN de site à site et ne s'applique pas au VPN d'accès à distance.

Exemple :

Cet exemple raccourcit la durée de vie de la carte de chiffrement dynamique dyn1 10 à 2 700 secondes (45 minutes). La durée de vie en volume de trafic n'est pas modifiée.

```
crypto dynamic-map dyn1 10 set security-association lifetime seconds 2700
```

Étape 4 (Facultatif) Précisez qu'IPsec demande PFS lors de la demande de nouveaux SA pour cette carte de chiffrement dynamique, ou devrait exiger PFS dans les demandes reçues de l'homologue :

crypto dynamic-map *dynamic-map-name dynamic-seq-num***set pfs** [**group14** | **group15** | **group16** | **group19** | **group20** | **group21**]

Dynamic-map-name spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante. *Dynamic-seq-num* spécifie le numéro de séquence qui correspond à l'entrée de carte de chiffrement dynamique.

Exemple :

```
crypto dynamic-map dyn1 10 set pfs group14
```

Étape 5 Ajoutez l'ensemble de cartes de chiffrement dynamique dans un ensemble de cartes de chiffrement statiques.

Veillez à définir les cartes de chiffrement qui référencent des cartes dynamiques comme entrées de priorité la plus basse (numéros de séquence les plus élevés) dans un ensemble de cartes de chiffrement.

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

Map-name spécifie le nom de l'ensemble de cartes de chiffrement. *Dynamic-map-name* spécifie le nom de l'entrée de carte de chiffrement qui fait référence à une carte de chiffrement dynamique préexistante.

Exemple :

```
crypto map  mymap 200 ipsec-isakmp dynamic dyn1
```

Configurer la redondance de site à site

Vous pouvez définir plusieurs homologues IKEv1 en utilisant des cartes de chiffrement pour assurer la redondance. Cette configuration est utile pour les VPN de site à site. Cette fonctionnalité n'est pas prise en charge avec IKEv2.

Si un homologue échoue, l'ASA établit un tunnel vers l'homologue suivant associé à la carte de chiffrement. Il envoie des données à l'homologue avec lequel il a négocié avec succès, et cet homologue devient l'homologue actif. L'homologue actif est l'homologue que l'ASA continue d'essayer en premier pour les négociations de suivi jusqu'à ce qu'une négociation échoue. À ce stade, l'ASA passe à l'homologue suivant. L'ASA revient au premier homologue lorsque tous les homologues associés à la carte de chiffrement ont échoué.

Gestion des VPN IPsec

Affichage d'une configuration IPsec

Il s'agit des commandes que vous pouvez saisir en mode contexte unique ou multiple pour afficher les informations sur votre configuration IPsec.

Tableau 3 : Commandes pour afficher les informations de configuration IPsec

show running-configuration crypto	Affiche l'ensemble de la configuration du chiffrement, y compris IPsec, les cartes de chiffrement, les cartes de chiffrement dynamiques et ISAKMP.
show running-config crypto ipsec	Affiche la configuration IPsec complète.
show running-config crypto isakmp	Affiche la configuration ISAKMP complète.
show running-config crypto map	Affiche la configuration complète de la carte de chiffrement.
show running-config crypto dynamic-map	Affiche la configuration de la carte de chiffrement dynamique.

show all crypto map	Affiche tous les paramètres de configuration, y compris ceux avec des valeurs par défaut.
show crypto ikev2 sa detail	Affiche la prise en charge de l'algorithme Suite B dans les statistiques de chiffrement.
show crypto ipsec sa	Affiche la prise en charge de l'algorithme Suite B et la sortie IPsec ESPv3 en mode contexte unique ou multiple.
show ipsec stats	Affiche les informations sur le sous-système IPsec en mode contexte unique ou multiple. Les statistiques ESPv3 sont affichées dans les paquets TFC et les erreurs ICMP valides et non valides reçues.

Attendre la fin des sessions actives avant de redémarrer

Vous pouvez planifier un redémarrage de l'ASA qui ne se produira qu'une fois que toutes les sessions actives auront pris fin volontairement. Par défaut, cette fonction est désactivée.

Utilisez la commande **reload** pour redémarrer l'ASA. Si vous définissez la commande **reload-wait**, vous pouvez utiliser la commande **reload quick** pour outrepasser le paramètre **reload-wait**. Les commandes **reload** et **reload-wait** sont disponibles en mode d'exécution privilégié ; aucune des deux n'inclut le préfixe **isakmp**.

Procédure

Pour faire en sorte que l'ASA attende la fin volontaire de toutes les sessions actives avant de redémarrer, effectuez la tâche de site à site suivante en mode monocontexte ou multicontexte :

crypto isakmp reload-wait

Exemple :

```
hostname(config)# crypto isakmp reload-wait
```

Alerter les homologues avant la déconnexion

Les sessions d'accès à distance ou LAN-à-LAN peuvent être interrompues pour plusieurs raisons, comme l'arrêt ou le redémarrage de l'ASA, le délai d'inactivité de la session, le dépassement de la durée maximale de connexion ou une interruption par l'administrateur.

L'ASA peut avertir les homologues admissibles, dans les configurations LAN-à-LAN ou les clients VPN, des sessions sur le point d'être déconnectées. L'homologue ou le client qui reçoit l'alerte décode la raison et l'affiche dans le journal des événements ou dans une fenêtre contextuelle. Par défaut, cette fonction est désactivée.

Les clients et homologues admissibles sont les suivants :

- périphériques de sécurité avec alertes activées

- Clients VPN Cisco exécutant le logiciel version 4.0 ou ultérieure, sans configuration requise

Pour activer la notification de déconnexion aux homologues IPsec, entrez la commande **crypto isakmp disconnect-notify** en mode contexte unique ou multiple.

Effacer les associations de sécurité

Certaines modifications de configuration ne prennent effet que pendant la négociation des SA suivantes. Si vous souhaitez que les nouveaux paramètres prennent effet immédiatement, effacez les SA existantes pour les rétablir avec la configuration modifiée. Si l'ASA traite activement le trafic IPsec, effacez uniquement la partie de la base de données SA affectée par les modifications de configuration. Réservez l'effacement de la base de données SA complète pour les modifications à grande échelle ou lorsque l'ASA traite une petite quantité de trafic IPsec.

Le tableau suivant répertorie les commandes que vous pouvez saisir pour effacer et réinitialiser les SA IPsec en mode contexte unique ou multiple.

Tableau 4 : Commandes pour effacer et réinitialiser les SA IPsec

clear configure crypto	Supprime une configuration complète de chiffrement, y compris IPsec, les cartes de chiffrement, les cartes de chiffrement dynamiques et ISAKMP.
clear configure crypto ca trustpoint	Supprime tous les points de confiance.
clear configure crypto dynamic-map	Supprime toutes les cartes de chiffrement dynamiques. Inclut des mots-clés permettant de supprimer des cartes de chiffrement dynamiques spécifiques.
clear configure crypto map	Supprime toutes les cartes de chiffrement. Inclut des mots-clés permettant de supprimer des cartes de chiffrement spécifiques.
clear configure crypto isakmp	Supprime l'ensemble de la configuration ISAKMP.
clear configure crypto isakmp policy	Supprime toutes les politiques ISAKMP ou une politique spécifique.
clear crypto isakmp sa	Supprime l'ensemble de la base de données des SA ISAKMP.

Effacer les configurations de cartes de chiffrement

La commande **clear configure crypto** comprend des arguments qui vous permettent de supprimer des éléments de la configuration cryptographique, notamment IPsec, les cartes de chiffrement, les cartes de chiffrement dynamiques, les points de confiance d'autorité de certification, tous les certificats, les configurations de mappage de certificats et ISAKMP.

Sachez que si vous saisissez la commande **clear configure crypto** sans arguments, vous supprimez l'ensemble de la configuration crypto, y compris tous les certificats.

Pour en savoir plus, consultez la commande **clear configure crypto** dans la *Référence des commandes de la série Cisco Secure Firewall ASA*.

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.