IKE

Configurer le protocole d'échange de clés de chiffrement (IKE)

IKE, également appelé ISAKMP, est le protocole de négociation qui permet à deux hôtes de se mettre d'accord sur la façon de créer une association de sécurité IPsec. Pour configurer l'ASA pour les réseaux privés virtuels, vous définissez des paramètres IKE globaux qui s'appliquent à l'échelle du système et vous créez également des politiques IKE que les homologues négocient pour établir une connexion VPN.

Procédure

Étape 1 Activer IKE, à la page 1.

Étape 2 Définir les Paramètres IKE pour le VPN de site à site, à la page 2.

Étape 3 Configurer les Politiques IKE, à la page 8.

Activer IKE

Procédure

Étape 1 Pour activer IKE pour les connexions VPN :

a) Dans ASDM, choisissez Configuration (**Configuration) > Remote Access VPN (VPN d'accès à distance) > Network (Client) Access (Accès réseau [client]) > Secure Client Connection Profiles (Profils de connexion Secure Client/AnyConnect**).

b) Dans la zone Access Interfaces (Interfaces d'accès), cochez **Allow Access** (Autoriser l'accès) sous IPsec (IKEv2) Access (Accès IPsec [IKEv2]) pour les interfaces sur lesquelles vous utiliserez IKE.

Étape 2 Pour activer IKE pour le VPN de site à site :

a) Dans ASDM, choisissez Configuration (**Configuration) > Site-to-Site VPN (VPN de site à site) > Connection Profiles (Profils de connexion)**.
b) Sélectionnez les interfaces sur lesquelles vous souhaitez utiliser IKEv1 et IKEv2.

Paramètres IKE pour le VPN de site à site

Dans ASDM, choisissez **Configuration > Site-to-Site VPN > Advanced > IKE Parameters** (Configuration > VPN de site à site > Avancé > Paramètres IKE).

Transparence NAT

- Activer IPsec sur NAT-T

  IPsec sur NAT-T permet aux homologues IPsec d'établir des connexions d'accès à distance et de réseau local (LAN) par l'intermédiaire d'un périphérique NAT. Il le fait en encapsulant le trafic IPsec dans des datagrammes UDP, en utilisant le port 4500, fournissant ainsi 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. Cette fonction est activée par défaut.

  - 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.
  - Lorsque NAT-T et IPsec sur UDP sont activés, NAT-T prévaut.
  - Lorsque cette option est activée, IPsec sur TCP prévaut sur toutes les autres méthodes de connexion.

  La mise en œuvre de l'ASA de NAT-T prend en charge les homologues IPsec derrière un seul périphérique NAT/PAT comme suit :

  - Une connexion de réseau local (LAN) à réseau local (LAN).
  - Il s'agit d'une connexion de réseau local (LAN) ou de plusieurs clients d'accès à distance, mais pas d'un mélange des deux.

  Pour utiliser NAT-T, vous devez :

  - Créez une liste de contrôle d'accès pour l'interface que vous utiliserez afin d'ouvrir le port 4500 (Configuration > Firewall > Access Rules [Configuration > Pare-feu > Règles d'accès]).
  - Activez IPsec sur NAT-T dans ce volet.
  - Dans le paramètre Fragmentation Policy (Politique de fragmentation) du volet Configuration > Site-to-Site VPN > Advanced > IPsec Prefragmentation Policies (Configuration > VPN de site à site > Avancé > Politiques de préfragmentation IPsec), modifiez l'interface que vous utiliserez pour activer la préfragmentation IPsec. Lorsque cela est configuré, il est toujours acceptable de laisser le trafic passer par les périphériques NAT qui ne prennent pas en charge la fragmentation IP; ils n'affectent pas le fonctionnement des périphériques NAT qui le font.

- Activez IPsec sur TCP

  IPsec sur TCP permet à un client VPN d'évoluer dans un environnement dans lequel l'ESP ou IKE standard ne peut pas fonctionner ou ne peut fonctionner qu'avec modification des règles de pare-feu existantes. IPsec sur TCP encapsule les protocoles IKE et IPsec dans un paquet TCP et permet la

tunnellisation sécurisée à travers les périphériques et les pare-feu NAT et PAT. Par défaut, cette fonction est désactivée.

Remarque Cette fonctionnalité ne fonctionne pas avec les pare-feu basés sur des proxys.

IPsec sur TCP fonctionne avec les clients d'accès à distance. Il fonctionne sur toutes les interfaces physiques et VLAN. Il s'agit d'une fonctionnalité de client pour ASA uniquement. 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.
- Lorsque cette option est activée, IPsec sur TCP prévaut sur toutes les autres méthodes de connexion.

Vous activez IPsec sur TCP sur l'ASA et sur le client auquel il se connecte.

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 fonctionnera plus. Par conséquent, vous ne pouvez plus utiliser de navigateur pour gérer l'ASA au moyen de l'interface compatible avec IKE. Pour résoudre ce problème, reconfigurez la gestion HTTP/HTTPS sur différents ports.

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.

Identité envoyée aux homologues

Choisissez l'**identité** que les homologues utiliseront pour s'identifier pendant les négociations IKE :

Address	Utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
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	L'homologue distant utilise la **chaîne d'identifiant de clé** que vous spécifiez pour rechercher la clé prépartagée.
Automatic	Détermine la négociation IKE par type de connexion : • Adresse IP pour la clé prépartagée • Cert DN pour l'authentification par certificat.

Contrôle de session

- Désactiver les connexions entrantes en mode progressif

  Les négociations IKE de phase 1 peuvent utiliser le mode principal ou le mode progressif. Les deux fournissent les mêmes services, mais le mode progressif ne nécessite que deux échanges entre les homologues, au lieu de trois. Le mode agressif est plus rapide, mais ne fournit pas de protection d'identité pour les parties qui communiquent. Il est donc nécessaire qu'ils échangent des informations d'identification avant d'établir une SA sécurisée dans laquelle chiffrer les informations. Par défaut, cette fonction est désactivée.

- Alerter les homologues avant la déconnexion
  - Les sessions client ou de réseau local (LAN) peuvent être abandonnées pour plusieurs raisons, telles que : l'arrêt ou le redémarrage de l'ASA, le délai d'inactivité de la session, le temps de connexion maximal dépassé ou l'arrêt de l'administrateur.
  - L'ASA peut notifier les homologues admissibles (dans les configurations de réseau local [LAN] à réseau local [LAN]) des sessions qui sont sur le point d'être déconnectées et leur transmettre la raison. 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.
  - Ce volet vous permet d'activer la fonctionnalité pour que l'ASA envoie ces alertes et transmette la raison de la déconnexion.

  Les clients et homologues admissibles sont les suivants :
  - Appareils de sécurité avec Alerts (Alertes) activé.
  - Clients VPN exécutant la version 4.0 ou ultérieure (aucune configuration requise).

- Attendre que toutes les sessions actives se terminent volontairement avant le redémarrage

  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.

- Nombre de SA autorisées dans la négociation pour IKEv1

  Limite le nombre maximal de SA qui peuvent être en négociation à tout moment.

Paramètres spécifiques IKE v2

Davantage de contrôles de session sont disponibles pour IKE v2, ce qui limite le nombre de SA ouvertes. Par défaut, l'ASA ne limite pas le nombre de SA ouvertes :

- Cookie Challenge (Défi des témoins) : permet à l'ASA d'envoyer des défis liés aux témoins aux périphériques homologues en réponse aux paquets initiés par la SA.
  - % du seuil avant que les SA entrantes ne soient contestées par les témoins : le pourcentage du nombre total de SA autorisées pour l'ASA qui sont en négociation, ce qui déclenche la contestation des témoins pour les futures négociations d'une SA. La plage va de zéro à 100 %. La valeur par défaut est de 50 %.

- Nombre de SA autorisées dans la négociation : limite le nombre maximal de SA qui peuvent être en négociation à tout moment. S'il est utilisé avec le Cookie Challenge (Défi des témoins), configurez le seuil de défi pour les témoins sur une valeur inférieure à cette limite pour une vérification par recoupement efficace.
- Nombre maximal de SA autorisées : limite le nombre de connexions IKEv2 autorisées. Par défaut, la limite est le nombre maximal de connexions spécifiées par la licence.
- Notify Invalid Selector (Notification d'un sélecteur non valide) : permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur une SA ne correspond pas aux sélecteurs de trafic de cette SA. L'envoi de cette notification est désactivé par défaut.

Prévention des attaques DoS avec les paramètres spécifiques IKE v2

Vous pouvez empêcher les attaques par déni de service (DoS) pour les connexions IPsec IKEv2 en configurant Cookie Challenge (Défi des témoins), qui remet en question l'identité des associations de sécurité (SA) entrantes, ou en limitant le nombre de SA ouvertes. Par défaut, l'ASA ne limite pas le nombre de SA ouvertes et ne met jamais en cause les témoins. Vous pouvez également limiter le nombre de SA autorisées, ce qui empêche d'autres connexions de négocier afin de protéger contre les attaques de mémoire et/ou de CPU que la fonctionnalité Cookie Challenge (Défi des témoins) pourrait ne pas être en mesure de déjouer, et protège les connexions actuelles.

Avec une attaque DoS, un agresseur lance l'attaque lorsque l'appareil homologue envoie un paquet d'initialisation SA et que l'ASA envoie sa réponse, mais l'appareil homologue ne répond pas. Si le périphérique homologue le fait continuellement, toutes les requêtes SA autorisées sur l'ASA peuvent être utilisées jusqu'à ce qu'il arrête de répondre.

L'activation d'un pourcentage de seuil pour la contestation des témoins limite le nombre de négociations d'un SA ouvertes. Par exemple, avec le paramètre par défaut de 50 %, lorsque 50 % des SA autorisées sont en négociation (ouvertes), le témoin ASA conteste tous les paquets d'initialisation SA supplémentaires qui arrivent.

S'il est utilisé simultanément avec le **Number of SAs Allowed in Negotiation** ou le Nombre maximal de SA autorisées, configurez le seuil de contestation des témoins sur une valeur inférieure à ces paramètres pour une vérification par recoupement efficace.

Vous pouvez également limiter la durée de vie de tous les SA au niveau IPsec en choisissant Configuration > Site-to-Site VPN > Advanced > System Options (Configuration > VPN de site à site > Avancé > Options système).

À propos de la carte de chiffrement IKEv2 multi-homologues

À partir de la version 9.14(1), ASA IKEv2 prend en charge les cartes 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 de plusieurs homologues sur IKEv2 est utile, en particulier 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 sont utilisées pour accepter la demande des homologues qui initient le tunnel.

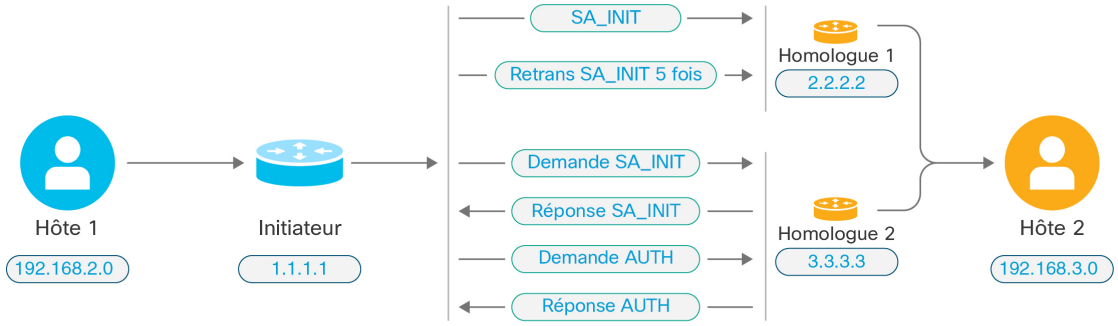
Comportement de l'initiateur IKEv2

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 épuisés, IKEv2 relance la session à partir de Peer1 jusqu'à ce qu'une SA soit établie avec l'un des homologues. La figure suivante décrit 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 de chiffrement,.

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

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

Lignes directrices relatives à l'homologue multiple IKEv2

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 Peer1, indépendamment du déplacement de la carte de chiffrement vers l'adresse IP 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 à homologues multiples IKEv2 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.
```

Politiques IKE

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > IKE Policies (Politiques IKE)

Utilisez ce volet pour ajouter, modifier ou supprimer des politiques IKEv1 et IKEv2.

Pour définir les conditions des négociations IKE, vous créez une ou plusieurs politiques IKE, qui comprennent les éléments suivants :

- Une priorité unique (de 1 à 65 543, 1 étant la priorité la plus élevée).
- Une méthode d'authentification pour garantir l'identité des homologues.
- Une méthode de chiffrement pour protéger les données et garantir la confidentialité.
- Une méthode HMAC 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 établir la force de l'algorithme de détermination de la clé de chiffrement. L'ASA utilise cet algorithme pour déduire les clés de chiffrement et de hachage.
- Une limite de temps pendant laquelle l'ASA utilise une clé de chiffrement avant de la remplacer.

Chaque négociation IKE est divisée en deux sections appelées Phase 1 et Phase 2. La phase 1 crée le premier tunnel, qui protège les messages de négociation IKE ultérieurs. La phase 2 crée le tunnel qui protège les données.

Pour IKEv1, vous ne pouvez activer qu'un seul paramètre pour chaque paramètre. Pour IKEv2, chaque proposition peut comporter plusieurs paramètres pour Encryption (Chiffrement), D-H Group (Groupe D-H), Integrity Hash (Hachage d'intégrité) et PRF Hash (Hachage PRF).

Si vous ne configurez aucune politique IKE, l'ASA utilise la politique par défaut, qui est toujours définie à la priorité la plus basse et qui contient la valeur par défaut pour chaque paramètre. Si vous ne spécifiez pas de valeur pour un paramètre spécifique, la valeur par défaut prend effet.

Lorsque la négociation IKE commence, l'homologue qui initie la négociation envoie toutes ses politiques à l'homologue distant, et ce dernier recherche une correspondance avec ses propres politiques, par ordre de priorité.

Il existe une correspondance entre les politiques IKE si elles ont les mêmes valeurs de chiffrement, de hachage, d'authentification et de Diffie-Hellman, ainsi qu'une durée de vie SA inférieure o Si les durées de vie ne sont pas identiques, la durée de vie la plus courte (de l'homologue distant) s'applique. Si aucune correspondance n'existe, IKE refuse la négociation et l'IKE SA n'est pas établie.

Champs

- IKEv1 Policies (Politiques IKEv1) : affiche les paramètres de chaque politique IKE configurée.
  - Priority # (Priorité #) : affiche la priorité de la politique.
  - Encryption (Chiffrement) : affiche la méthode de chiffrement.
  - Hash (Hachage) : affiche l'algorithme de hachage.
  - D-H Group (Groupe D-H) : affiche le groupe Diffie-Hellman.
  - Authentication (Authentification) : affiche la méthode d'authentification.
  - Lifetime (secs) (Durée de vie [s]) : affiche la durée de vie de la SA en secondes.
- IKEv2 Policies (Politiques IKEv2) : affiche les paramètres de chaque politique IKEv2 configurée.
  - Priority # (Priorité #) : affiche la priorité de la politique.
  - Encryption (Chiffrement) : affiche la méthode de chiffrement.
  - Integrity Hash (Hachage d'intégrité) : affiche l'algorithme de hachage.
  - PRF Hash (Hachage PRF) : affiche l'algorithme de hachage de la fonction pseudo-aléatoire (PRF).
  - D-H Group (Groupe D-H) : affiche le groupe Diffie-Hellman.
  - Lifetime (secs) (Durée de vie [s]) : affiche la durée de vie de la SA en secondes.

Créer ou modifier une politique IKEv1

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > IKE Policies (Politiques IKE) > Add/Edit IKE Policy (Ajouter/modifier une politique IKE)

Priority # (Priorité #) : saisissez un nombre pour définir une priorité pour la politique IKE. La plage est comprise entre 1 et 65 535, 1 étant la priorité la plus élevée.

Encryption (Chiffrement) : choisissez une méthode de chiffrement. Il s'agit d'une méthode de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. Les choix sont les suivants :

DES	DES-CBC 56 bits Moins sécurisée, mais plus rapide que les autres solutions. Il s'agit du paramètre par défaut.
3DES	Triple DES 168 bits
aes	AES-128 bits.
aes-192	AES-192 bits.
aes-256	AES 256 bits.

Hachage : choisissez l'algorithme de hachage qui garantit l'intégrité des données. Il garantit qu'un paquet provient de celui dont vous pensez qu'il provient et qu'il n'a pas été modifié en cours de transit.

sha	SHA-1	La valeur par défaut est SHA-1. MD5 a un condensé plus petit et est considéré comme légèrement plus rapide que SHA-1. Une attaque réussie (mais très difficile) contre MD5 s'est produite ; cependant, la variante de HMAC utilisée par IKE empêche cette attaque.
md5	MD5	

Authentification : choisissez la méthode d'authentification utilisée par l'ASA pour établir l'identité de chaque homologue IPsec. Les clés prépartagées n'évoluent pas facilement avec un réseau en croissance, mais sont plus faciles à configurer dans un petit réseau. Les choix sont les suivants :

pre-share	Clés prépartagées.
rsa-sig	Un certificat numérique avec des clés générées par l'algorithme de signatures RSA

Groupe Diffie-Hellman : choisissez le groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre.

1	Groupe 1 (768 bits)	, le groupe 2 (Diffie-Hellman 1 024 bits), nécessite moins de temps CPU pour s'exécuter, mais est moins sécurisé que le groupe 1 ou 5.
2	Groupe 2 (1 024 bits)	
5	Groupe 5 (1 536 bits)	
14	Groupe 14 (2 048 bits)	Le groupe Diffie-Hellman par défaut est le groupe 14 (Diffie-Hellman 2 048 bits)

Durée de vie (s) : cochez la case Illimité ou saisissez un entier pour la durée de vie de la SA. La valeur par défaut est 86 400 secondes (24 heures). Avec des durées de vie plus longues, l'ASA configure les futures associations de sécurité IPsec moins rapidement. La force de chiffrement est suffisamment élevée pour assurer

la sécurité sans utiliser des temps de renouvellement très rapides, de l'ordre de quelques minutes. Nous vous recommandons de conserver la valeur par défaut.

Mesure de temps : choisissez une mesure de temps. L'ASA accepte les valeurs suivantes :

120 secondes
2 à 1 440 minutes
1 à 24 heures
1 jour

Créer ou modifier une politique IKEv2

Configuration > Site-to-Site VPN > Advanced > IKE Policies > Add/Edit IKEv2 Policy (Configuration > VPN de site à site > Avancé > Politiques IKE > Ajouter/Modifier une politique IKEv2)

Priority # (Priorité #) : saisissez un nombre pour définir une priorité pour la politique IKEv2. La plage est comprise entre 1 et 65 535, 1 étant la priorité la plus élevée.

Encryption (Chiffrement) : choisissez une méthode de chiffrement. Il s'agit d'une méthode de chiffrement symétrique qui protège les données transmises entre deux homologues IPsec. Les choix sont les suivants :

DES	Spécifie le chiffrement DES-CBC 56 bits pour ESP.
3DES	(Par défaut) Spécifie l'algorithme de chiffrement triple DES pour ESP.
aes	Spécifie AES avec un chiffrement de clé de 128 bits pour ESP.
aes-192	Spécifie AES avec un chiffrement de clé de 192 bits pour ESP.
aes-256	Spécifie AES avec un chiffrement de clé de 256 bits pour ESP.
aes-gcm	Spécifie la prise en charge d'AES-GCM/GMAC 128 bits pour le chiffrement symétrique et l'intégrité.
aes-gcm-192	Spécifie la prise en charge d'AES-GCM/GMAC 192 bits pour le chiffrement symétrique et l'intégrité.
aes-gcm-256	Spécifie la prise en charge d'AES-GCM/GMAC 256 bits pour le chiffrement symétrique et l'intégrité.
NUL	Indique aucun chiffrement.

Groupe Diffie-Hellman : choisissez le groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre.

1	Groupe 1 (768 bits)	La valeur par défaut, le groupe 2 (Diffie-Hellman 1 024 bits), nécessite moins de temps CPU pour s'exécuter, mais est moins sécurisé que le groupe 2 ou 5.
2	Groupe 2 (1 024 bits)	
5	Groupe 5 (1 536 bits)	

14	Groupe 14	
19	Groupe 19	
20	Groupe 20	
21	Groupe 21	
24	Groupe 24	

Integrity Hash (Hachage d'intégrité) : choisissez l'algorithme de hachage qui garantit l'intégrité des données pour le protocole ESP. Il garantit qu'un paquet provient de celui dont vous pensez qu'il provient et qu'il n'a pas été modifié en cours de transit.

sha	SHA-1	La valeur par défaut est SHA 1. MD5 a un condensé plus petit et est considéré comme légèrement plus rapide que SHA-1. Une attaque réussie (mais très difficile) contre MD5 s'est produite ; cependant, la variante de HMAC utilisée par IKE empêche cette attaque.
md5	MD5	
sha256	SHA 2, condensé de 256 bits	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 256 bits.
sha384	**SHA 2, 384-bit digest**	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
sha512	**SHA 2, 512-bit digest**	Spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 512 bits.
null (nul)		Indique qu'AES-GCM ou AES-GMAC est configuré comme algorithme de chiffrement. Vous devez choisir l'algorithme d'intégrité nulle si AES-GCM a été configuré comme algorithme de chiffrement.

Fonction pseudo-aléatoire (PRF) : précisez la PRF utilisée pour la construction du matériel de saisie pour tous les algorithmes cryptographiques utilisés dans le SA.

sha	SHA-1	La valeur par défaut est SHA-1. MD5 a un condensé plus petit et est considéré comme légèrement plus rapide que SHA-1. Une attaque réussie (mais très difficile) contre MD5 s'est produite ; cependant, la variante de HMAC utilisée par IKE empêche cette attaque.
md5	MD5	
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.

Durée de vie (s) : cochez la case Illimité ou saisissez un entier pour la durée de vie de la SA. La valeur par défaut est 86 400 secondes (24 heures). Avec des durées de vie plus longues, l'ASA configure plus rapidement les futures associations de sécurité IPsec. La force de chiffrement est suffisamment élevée pour assurer la sécurité sans utiliser des temps de renouvellement très rapides, de l'ordre de quelques minutes. Nous vous recommandons de conserver la valeur par défaut.

L'ASA accepte les valeurs suivantes :

120 secondes
2 - 1 440 minutes
1 à 24 heures
1 jour

Configurer 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. L'ASA prend en charge les connexions IPsec de réseau local (LAN) à réseau local (LAN) avec les homologues Cisco (IPv4 ou IPv6) et avec les homologues tiers qui sont conformes à toutes les normes pertinentes.

Lors de l'établissement du tunnel, les deux homologues négocient des associations de sécurité 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.

L'ASA prend en charge ces attributs IPsec :

- Mode principal pour la négociation des associations de sécurité ISAKMP de phase 1 lors de l'utilisation de certificats numériques pour l'authentification
- Mode agressif pour négocier les associations de sécurité ISAKMP (SA) de phase 1 lors de l'utilisation de clés prépartagées pour l'authentification
- Algorithmes d'authentification :
  - ESP-MD5-HMAC-128
  - ESP-SHA1-HMAC-160
- Modes d'authentification
  - Clés prépartagées
  - Certificats numériques X.509
- Algorithmes de chiffrement :
  - AES-128, -192, et -256
  - 3DES-168
  - DES-56

- ESP-NULL

- Authentification étendue (XAuth)
- Configuration en mode (également connue sous le nom de méthode de configuration ISAKMP)
- Mode d'encapsulation de tunnel
- Compression d'IP (IPCOMP) à l'aide de LZS

Procédure

Étape 1 Configurer les Carte de chiffrement, à la page 14.

Étape 2 Configurer les Politiques de pré-fragmentation IPsec, à la page 23.

Étape 3 Configurer les Propositions IPsec (ensembles de transformations), à la page 25.

Carte de chiffrement

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > Crypto Maps (Cartes de chiffrement)

Ce volet affiche les cartes de chiffrement actuellement configurées, qui sont définies dans les règles IPsec. Ici, vous pouvez ajouter, modifier, supprimer et déplacer vers le haut, déplacer vers le bas, couper, copier et coller une règle IPsec.

Remarque Vous ne pouvez pas modifier, supprimer ou copier une règle implicite. L'ASA accepte implicitement la proposition de sélection du trafic des clients distants lorsqu'elle est configurée avec une politique de tunnel dynamique. Vous pouvez le remplacer en accordant une sélection de trafic spécifique.

Vous pouvez également **rechercher** (filtrer l'affichage des règles) en sélectionnant Interface, Source, Destination, Destination Service (Service de destination) ou Rule Query (Requête de règles), en sélectionnant is (est) ou contains (contient), puis en saisissant le paramètre de filtre. Cliquez sur... pour lancer une boîte de dialogue de navigation qui affiche toutes les entrées existantes que vous pouvez choisir. Utilisez **Diagram** (Diagramme) pour afficher les règles sous forme graphique.

Les règles IPsec spécifient les éléments suivants :

- Type : priorité : affiche le type de règle (statique ou dynamique) et sa priorité.
- Sélection de trafic
  - # : indique le numéro de la règle.
  - Source : indique les adresses IP qui sont soumises à cette règle lorsque le trafic est envoyé vers les adresses IP répertoriées dans la colonne Remote Côté Host/Network (Hôte/Réseau du côté distant). En mode détail (voir le bouton Show Detail (Afficher les détails)), une colonne d'adresses peut contenir un nom d'interface avec le mot any, tel que inside:any. any signifie que tout hôte sur l'interface interne est affecté par la règle.

- Destination : répertorie les adresses IP qui sont soumises à cette règle lorsque le trafic est envoyé à partir des adresses IP répertoriées dans la colonne Hôte/Réseau du côté de l'appareil de sécurité. En mode détail (voir le bouton Show Detail (Afficher les détails)), une colonne d'adresses peut contenir un nom d'interface avec le mot any, tel que outside:any. any signifie que tout hôte sur l'interface externe est affecté par la règle. Également en mode détail, une colonne d'adresses peut contenir des adresses IP entre crochets. Par exemple, [209.165.201.1-209.165.201.30]. Ces adresses sont des adresses traduites. Lorsqu'un hôte interne établit une connexion avec un hôte externe, l'ASA associe l'adresse de l'hôte interne à une adresse de l'ensemble. Après qu'un hôte ait créé une connexion sortante, l'ASA conserve ce mappage d'adresse. Cette structure de mappage d'adresses s'appelle un xlate et reste en mémoire pendant un certain temps.
- Service : spécifie le service et le protocole spécifiés par la règle (TCP, UDP, ICMP ou IP).
- Action : spécifie le type de règle IPsec (protéger ou ne pas protéger).

- Transform Set (Ensemble de transformation) : affiche l'ensemble de transformation pour la règle.
- Peer (Homologue) : identifie l'homologue IPsec.
- PFS : affiche les paramètres de confidentialité de transmission parfaite pour la règle.
- NAT-T Enabled (NAT-T activé) : indique si la traversée NAT est activée pour la politique.
- Reverse Route Enabled (Route inversée activée) : indique si l'injection de route inverse (RRI) est activée pour la politique. 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 soit 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.
  - Dynamic (Dynamique) : si la dynamique est spécifiée, les RRI sont créés lors de l'établissement réussi des associations de sécurité IPsec et supprimés après la suppression des SA IPsec.

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

- Connection Type (Type de connexion) : (significatif uniquement pour les politiques de tunnel statique.) Identifie le type de connexion pour cette politique comme bidirectionnel, d'origine uniquement ou de réponse uniquement).
- SA Lifetime (Durée de vie SA) : affiche la durée de vie SA pour la règle.
- CA Certificate (Certificat de l'autorité de certification) : affiche le certificat de l'autorité de certification de la politique. Cela s'applique uniquement aux connexions statiques.
- IKE Negotiation Mode (Mode de négociation IKE) : affiche si les négociations IKE utilisent le mode principal ou le mode agressif.
- Description : (facultatif) spécifie une brève description de cette règle. Pour une règle existante, il s'agit de la description que vous avez saisie lors de l'ajout de la règle. Une règle implicite comprend la description suivante : « Règle implicite ». Pour modifier la description de n'importe quelle règle, sauf d'une règle implicite, cliquez avec le bouton droit sur cette colonne et choisissez Edit Description (Modifier la description) ou double-cliquez sur la colonne.

- Enable Anti-replay window size (Activer la taille de la fenêtre anti-relecture) : définit la taille de la fenêtre anti-relecture entre 64 et 1 028 par incréments de 64. Un effet secondaire de la mise en file prioritaire dans une politique QoS hiérarchique avec régulation du trafic (voir « Actions de règles> Onglet QoS ») est le réordonnancement des paquets. Pour les paquets IPsec, les paquets en panne qui ne sont pas dans la fenêtre d'anti-relecture génèrent des messages d'avertissement syslog. Ces avertissements deviennent de fausses alarmes dans le cas de la mise en file d'attente prioritaire. La configuration de la taille du volet anti-relecture vous aide à éviter d'éventuelles fausses alarmes.
- Enable IPsec Inner Routing Lookup (Activer la recherche de routage interne IPsec) : par défaut, les recherches ne sont pas effectuées pour les paquets envoyés via le tunnel IPsec; les recherches d'adjacence par paquet sont effectuées uniquement pour les paquets ESP externes. 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 opérationnel, les paquets traversant 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.

Créer ou modifier une politique de tunnel de règle IPsec (carte de chiffrement) - Onglet Basic (Base)

Utilisez ce pour définir une nouvelle politique de tunnel pour une règle IPsec. Les valeurs que vous définissez ici s'affichent dans le tableau des règles IPsec après que vous avez cliqué sur **OK**. Toutes les règles sont activées par défaut dès qu'elles apparaissent dans le tableau des règles IPsec.

Le volet Tunnel Policy (Politique de tunnel) vous permet de définir une politique de tunnel utilisée pour négocier une association de sécurité (SA) IPsec (phase 2). ASDM enregistre vos modifications de configuration, mais ne les enregistre pas dans la configuration en cours tant que vous n'avez pas cliqué sur **Apply** (Appliquer).

Chaque politique de tunnel doit spécifier un ensemble de transformations et identifier l'interface de l'appareil de sécurité à laquelle elle s'applique. L'ensemble de transformation identifie les algorithmes de chiffrement et de hachage qui effectuent les opérations de chiffrement et de déchiffrement IPsec. Comme tous les homologues IPsec ne prennent pas en charge les mêmes algorithmes, vous pouvez spécifier un certain nombre de politiques et affecter une priorité à chacune. L'appareil de sécurité négocie ensuite avec l'homologue IPsec distant pour convenir d'un ensemble de transformations pris en charge par les deux homologues.

Les politiques de tunnel peuvent être *statiques* ou *dynamiques*. Une politique de tunnel statique identifie un ou plusieurs homologues IPsec distants ou sous-réseaux auxquels votre appareil de sécurité autorise les connexions IPsec. Une politique statique peut être utilisée si votre appareil de sécurité amorce la connexion ou reçoit une demande de connexion d'un hôte distant. Une politique statique vous oblige à saisir les informations nécessaires pour identifier les hôtes ou les réseaux autorisés.

Une politique de tunnel dynamique est utilisée lorsque vous ne pouvez pas ou ne souhaitez pas fournir d'informations sur les hôtes distants qui sont autorisés à établir une connexion avec l'appareil de sécurité. Si vous utilisez uniquement votre appareil de sécurité comme client VPN par rapport à un périphérique de site central VPN distant, vous n'avez pas besoin de configurer de politiques de tunnel dynamique. Les politiques de tunnel dynamique sont plus utiles pour permettre aux clients d'accès à distance d'établir une connexion à votre réseau par l'intermédiaire d'un appareil de sécurité agissant en tant qu'appareil de site central VPN. Une politique de tunnel dynamique est utile lorsque les clients d'accès à distance ont des adresses IP affectées dynamiquement ou lorsque vous ne souhaitez pas configurer des politiques distinctes pour un grand nombre de clients d'accès à distance.

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > Crypto Maps (Cartes de chiffrement) > Create / Edit IPsec Rule (Créer / Modifier une règle IPsec) > Tunnel Policy (Crypto Map) - Basic (Politique de tunnel (carte de chiffrement) - Base)

- Interface : choisissez le nom de l'interface à laquelle cette politique s'applique.
- Policy Type (Type de politique) : choisissez le type, statique ou dynamique, de cette politique de tunnel.
- Priority (Priorité) : saisissez la priorité de la politique.
- IKE Proposals (Transform Sets) (Propositions IKE (Ensembles de transformation)) : spécifie les propositions IPsec IKEv1 et IKEv2.
  - IKEv1 IPsec Proposal (Proposition IPsec IKEv1) : choisissez la proposition (ensemble de transformation) pour la politique et cliquez sur **Add** (Ajouter) pour la déplacer dans la liste des ensembles de transformation actifs. Cliquez sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour réorganiser l'ordre des propositions dans la zone de liste. Vous pouvez ajouter un maximum de 11 propositions à une entrée de carte de chiffrement ou à une entrée de carte de chiffrement dynamique.
  - IKEv2 IPsec Proposal (Proposition IPsec IKEv2) : choisissez la proposition (ensemble de transformation) pour la politique et cliquez sur **Add** (Ajouter) pour la déplacer dans la liste des ensembles de transformation actifs. Cliquez sur **Move Up** (Déplacer vers le haut) ou **Move Down** (Déplacer vers le bas) pour réorganiser l'ordre des propositions dans la zone de liste. Vous pouvez ajouter un maximum de 11 propositions à une entrée de carte de chiffrement ou à une entrée de carte de chiffrement dynamique.
- Peer Settings - Optional for Dynamic Crypto Map Entries (Paramètres homologues - Facultatif pour les entrées de carte de chiffrement dynamique) : configurez les paramètres homologues pour la politique.
  - Connection Type (Type de connexion) : (significatif uniquement pour les politiques de tunnel statique.) Choisissez bidirectionnel, origine uniquement ou réponse uniquement pour préciser le type de connexion de cette politique. Pour les connexions de réseau local (LAN à réseau local), choisissez bidirectionnel ou réponse uniquement (pas de source uniquement). Choisissez la réponse uniquement pour la redondance LAN-LAN. Originate Only (Générer uniquement), vous pouvez spécifier jusqu'à 10 homologues redondants. Pour unidirectionnel, vous pouvez spécifier l'origine uniquement ou la réponse uniquement, et aucun n'est activé par défaut.
  - IP Address of Peer to Be Added (Adresse IP de l'homologue à ajouter) : saisissez l'adresse IP de l'homologue IPsec que vous ajoutez. À partir de la version 9.14(1), l'ASA prend en charge plusieurs homologues dans IKEv2. Vous pouvez ajouter un maximum de 10 homologues à la carte de chiffrement.
- Enable Perfect Forwarding Secrecy (activer la confidentialité de transmission parfaite) : cochez cette option pour activer la confidentialité de transmission parfaite pour la politique. PFS est un concept cryptographique dans lequel chaque nouvelle clé n'est liée à aucune clé précédente. Dans les négociations IPsec, les clés de phase 2 sont basées sur les clés de phase 1, sauf si vous spécifiez la confidentialité de transmission parfaite.
- Diffie-Hellman Group (Groupe Diffie-Hellman) : lorsque vous activez PFS, vous devez également choisir un groupe Diffie-Hellman que l'ASA utilise pour générer des clés de session. Voici les différents choix proposés :
  - Groupe 1 (768 bits) = utilise la confidentialité de transmission parfaite et utilise le groupe Diffie-Hellman 1 pour générer des clés de session IPsec, où les numéros premiers et de génération sont de 768 bits. Cette option est plus sécurisée, mais nécessite plus de surdébit de traitement.
  - Groupe 2 (1 024 bits) = utilise la confidentialité de transmission parfaite et utilise le groupe Diffie-Hellman 2 pour générer des clés de session IPsec, où les numéros premiers et de génération

sont de 1 024 bits. Cette option est plus sécurisée que le groupe 1, mais nécessite un surdébit de traitement plus important.

- Groupe 5 (1 536 bits) : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 5 pour générer des clés de session IPsec, où les numéros du premiers et du générateur sont de 1 536 bits. Cette option est plus sécurisée que le groupe 2, mais nécessite un surdébit de traitement plus important.
- Groupe 14 (2 048 bits) : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 14 pour IKEv2.
- Groupe 19 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 19 pour IKEv2 afin de prendre en charge ECDH.
- Groupe 20 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 20 pour IKEv2 afin de prendre en charge ECDH.
- Groupe 21 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 21 pour IKEv2 afin de prendre en charge ECDH.
- Groupe 24 : utilisez la confidentialité de transmission parfaite et utilisez le groupe Diffie-Hellman 24 pour IKEv2.

Créer ou modifier une politique de tunnel de règle IPsec (carte de chiffrement) - Onglet Avancé

Configuration > Site-to-Site VPN > Advanced > Crypto Maps > Create / Edit IPsec Rule > Tunnel Policy (Crypto Map) - Advanced (Configuration > VPN de site à site > Avancé > Cartes de chiffrement > Créer / Modifier une règle IPsec > Stratégie de tunnel [carte de chiffrement] - Avancé)

- Enable NAT-T (Activer NAT-T) : active la traversée NAT (NAT-T) pour cette stratégie.
- Enable Reverse Route Injection (Activer l'injection de route inverse) : active l'injection de route inverse pour cette stratégie. L'injection de route inverse (RRI) est utilisée pour remplir la table de routage d'un routeur interne qui exécute des protocoles de routage dynamique tels que l'Open Shortest Path First (OSPF), le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) si vous utilisez ASA, ou le protocole d'information de routage (RIP) pour les clients VPN distants ou les sessions de réseau local (LAN) à LAN. 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 soit 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.
  - Dynamique : si dynamic est spécifié, les RRI sont créées lors de l'établissement réussi des associations de sécurité IPsec et supprimées après la suppression des SA IPsec. En règle générale, les routes RRI sont utilisées pour amorcer un tunnel s'il n'y en a pas et que le trafic doit être chiffré. Avec la prise en charge dynamique des RRI, aucune route n'est présente avant l'activation du tunnel. Par conséquent, un ASA avec une RRI dynamique configuré fonctionnerait généralement uniquement comme répondeur.

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

- Security Association Lifetime Settings (Paramètres de durée de vie de l'association de sécurité) : configure la durée d'une association de sécurité (SA). Ce paramètre spécifie comment mesurer la durée de vie des clés de SA IPsec, qui correspond à la durée de vie de la SA IPsec jusqu'à son expiration et doit être renégociée avec de nouvelles clés.
  - Time (Temps) : spécifie la durée de vie de la SA en heures (hh), minutes (mm) et en secondes (ss).
  - Traffic Volume (Volume du trafic) : définit la durée de vie de la SA en termes de kilo-octets de trafic. Saisissez le nombre de kilo-octets de données de charge utile après lequel la SA IPsec expire. Le minimum est de 100 Ko, la valeur par défaut est de 10 000 Ko, et le maximum est de 2 147 483 647 Ko.
- Static Type Only Settings (Paramètres de type statique uniquement) : spécifie les paramètres pour les politiques de tunnel statique.
  - Device Certificate (Certificat d'appareil) : choisissez le certificat à utiliser. Si vous choisissez autre chose que None (Use Preshared Keys) [None (Utiliser des clés prépartagées)], qui est la valeur par défaut. La case Send CA certificate chain (Envoyer la chaîne de certificats de l'autorité de certification) devient active lorsque vous choisissez autre chose que None.
  - Send CA certificate chain (Envoyer la chaîne de certificats de l'autorité de certification) : active la transmission de l'ensemble de la chaîne de points de confiance.
  - IKE Negotiation Mode (Mode de négociation IKE) : choisit le mode de négociation IKE, Main (Principal) ou Aggressive (Progressif). Ce paramètre définit le mode d'échange des informations de clé et de configuration des SA. Il définit le mode utilisé par l'initiateur de la négociation; le répondeur négocie automatiquement. Le mode agressif est plus rapide, utilise moins de paquets et moins d'échanges, mais il ne protège pas l'identité des parties qui communiquent. Le mode principal est plus lent, utilisant plus de paquets et plus d'échanges, mais il protège les identités des parties qui communiquent. Ce mode est plus sécurisé et il s'agit de la sélection par défaut. Si vous choisissez Aggressive (Mode agressif), la liste Diffie-Hellman Group (Groupe Diffie-Hellman) devient active.
  - Diffie-Hellman Group (Groupe Diffie-Hellman) : choisissez le groupe Diffie-Hellman à appliquer. Les choix sont les suivants : Groupe 1 (768 bits), Groupe 2 (1 024 bits) ou Groupe 5 (1 536 bits).
- ESP v3 : spécifiez si les messages d'erreur ICMP entrants sont validés pour les cartes de chiffrement statiques et dynamiques, définissez la stratégie par association de sécurité ou activez les paquets de flux de trafic :
  - Validate incoming ICMP error messages (Valider les messages d'erreur ICMP entrants) : choisissez s'il faut valider les messages d'erreur ICMP reçus dans un tunnel IPsec et destinés à un hôte intérieur sur le réseau privé.
  - Enable Do Not Fragment (DF) policy (Activer la stratégie Ne pas fragmenter [DF]) : définit comment le sous-système IPsec gère les paquets volumineux dont le bit « Ne pas fragmenter » (DF) est défini dans l'en-tête IP. Effectuez l'une des opérations suivantes :

    Clear DF bit (Effacer le bit DF) : ignore le bit DF.

    Copy DF bit (Copier le bit DF) : maintient le bit DF.

    Set DF bit (Définir le bit DF) : définit et utilise le bit DF.
  - Sélectionnez Enable Traffic Flow Confidentiality (TFC) packets (Activer les paquets TFC de confidentialité du flux de trafic) pour activer des paquets TFC factices qui masquent le profil de trafic qui traverse le tunnel.

Remarque Vous devez avoir une proposition IKEv2 IPsec définie dans l'onglet Tunnel Policy (Crypto Map) Basic (Base de la stratégie de tunnel [carte de chiffrement]) avant d'activer TFC.

Utilisez les paramètres Burst (Rafale), Payload Size (Taille de la charge utile) et Timeout (Expiration) pour générer des paquets de longueur aléatoire à des intervalles aléatoires sur la SA specifiée.

Créer ou modifier l'onglet Sélection du trafic de règle IPsec

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > Crypto Maps (Cartes de chiffrement) > Create / Edit IPsec Rule (Créer/modifier une règle IPsec) > Traffic Selection (Sélection du trafic)

Ce volet vous permet de définir le trafic à protéger (autoriser) ou à ne pas protéger (refuser).

- Action : précisez l'action que cette règle doit exécuter. Les sélections sont protect (protéger) et do not protect (ne pas protéger).
- Source : spécifiez l'adresse IP, le groupe d'objets réseau ou l'adresse IP de l'interface de l'hôte ou du réseau source. Une règle ne peut pas utiliser la même adresse comme source et destination. Cliquez sur ... pour lancer la boîte de dialogue Browse Source (Parcourir la source), qui contient les champs suivants :
  - Add/Edit (Ajouter/Modifier) : choisissez IP Address (Adresse IP) ou Network Object Group (Groupe d'objets réseau) pour ajouter d'autres adresses ou groupes source.
  - Delete (Supprimer) : cliquez pour supprimer une entrée.
  - Filter (Filtre) : saisissez une adresse IP pour filtrer les résultats affichés.
  - Name (Nom) : indique que les paramètres suivants précisent le nom de l'hôte ou du réseau source.
  - IP Address (Adresse IP) : indique que les paramètres suivants précisent l'interface, l'adresse IP et le masque de sous-réseau de l'hôte ou du réseau source.
  - Netmask (Masque réseau) : choisit un masque de sous-réseau standard à appliquer à l'adresse IP. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (Adresse IP).
  - Description : saisissez une description.
  - Selected Source (Source sélectionnée) : cliquez sur **Source** pour inclure l'entrée sélectionnée comme source.
- Destination : spécifiez l'adresse IP, le groupe d'objets réseau ou l'adresse IP de l'interface de l'hôte ou du réseau de destination. Une règle ne peut pas utiliser la même adresse comme source et comme destination. Cliquez ... pour lancer la boîte de dialogue Browse Destination (Parcourir la destination), qui contient les champs suivants :
  - Add/Edit (Ajouter/Modifier) : choisissez IP Address (Adresse IP) ou Network Object Group (Groupe d'objets réseau) pour ajouter d'autres adresses ou groupes de destination.
  - Delete (Supprimer) : cliquez pour supprimer une entrée.
  - Filter (Filtre) : saisissez une adresse IP pour filtrer les résultats affichés.

- Name (Nom) : indique que les paramètres suivants précisent le nom de l'hôte ou du réseau de destination.
- IP Address (Adresse IP) : indique que les paramètres suivants précisent l'interface, l'adresse IP et le masque de sous-réseau de l'hôte ou du réseau de destination.
- Netmask (Masque réseau) : choisit un masque de sous-réseau standard à appliquer à l'adresse IP. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (Adresse IP).
- Description : saisissez une description.
- Selected Destination (Destination sélectionnée) : cliquez sur **Destination** pour inclure l'entrée sélectionnée comme destination.

- Service : saisissez un service ou cliquez sur ... pour lancer la boîte de dialogue de navigation des services, où vous pouvez choisir dans une liste de services.
- Description : saisissez une description pour l'entrée de sélection du trafic.
- Plus d'options
  - nable Rule (Activer la règle) — Cliquez pour activer cette règle.
  - Source Service (Service source) : saisissez un service ou cliquez sur **...** pour lancer la boîte de dialogue de navigation des services, où vous pouvez choisir dans une liste de services.
  - Time Range (Plage temporelle) : définissez une plage temporelle pour laquelle cette règle s'applique.
  - Group (Groupe) : indique que les paramètres suivants précisent l'interface et le nom de groupe de l'hôte ou du réseau source.
  - Interface : choisissez le nom d'interface pour l'adresse IP. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (Adresse IP).
  - IP address (Adresse IP) : spécifie l'adresse IP de l'interface à laquelle cette politique s'applique. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option IP Address (adresse IP).
  - Destination : spécifiez l'adresse IP, le groupe d'objets réseau ou l'adresse IP de l'interface de l'hôte ou du réseau source ou de destination. Une règle ne peut pas utiliser la même adresse comme source et comme destination. Cliquez sur **...** pour l'un de ces champs afin de lancer la boîte de dialogue Browse (Parcourir), qui contient les champs suivants :
  - Name (nom) : choisissez le nom de l'interface à utiliser comme hôte ou réseau source ou de destination. Ce paramètre s'affiche lorsque vous choisissez le bouton d'option Name (Nom). Il s'agit du seul paramètre associé à cette option.
  - Interface : choisissez le nom d'interface pour l'adresse IP. Ce paramètre s'affiche lorsque vous cliquez sur le bouton d'option Group (Groupe).
  - Group (groupe) : choisissez le nom du groupe sur l'interface spécifiée pour l'hôte ou le réseau source ou de destination. Si la liste ne contient aucune entrée, vous pouvez saisir le nom d'un groupe existant. Ce paramètre s'affiche lorsque vous cliquez sur le bouton d'option Group (Groupe).

- **Protocol and Service** (Protocole et service) : spécifie les paramètres de protocole et de service pertinents pour cette règle.

Remarque Les règles IPsec « any-any » ne sont pas autorisées. Ce type de règle empêcherait le périphérique et son homologue de prendre en charge plusieurs tunnels de réseau local à réseau local.

- TCP : spécifie que cette règle s'applique aux connexions TCP. Cette sélection affiche également les zones de groupe Port source et Port de destination.
- UDP : spécifie que cette règle s'applique aux connexions UDP. Cette sélection affiche également les zones de groupe Port source et Port de destination.
- ICMP : spécifie que cette règle s'applique aux connexions ICMP. Cette sélection affiche également la zone de groupe Type ICMP.
- IP : spécifie que cette règle s'applique aux connexions IP. Cette sélection affiche également la zone de groupe IP Protocol (Protocole IP).
- Manage Service Groups (Gérer les groupes de services) : affiche le volet Manage Service Groups (Gérer les groupes de services), dans lequel vous pouvez ajouter, modifier ou supprimer un groupe de services/ports TCP/UDP.
- Source Port and Destination Port (Port source et Port de destination) : contiennent les paramètres de port TCP ou UDP, selon le bouton d'option que vous avez choisi dans la zone de groupe Protocol and Service (Protocole et service).
- Service : indique que vous spécifiez les paramètres d'un service individuel. Spécifie le nom du service et un opérateur booléen à utiliser lors de l'application du filtre.
- Boolean operator (unlabeled) (Opérateur booléen [sans étiquette]) : répertorie les conditions booléennes (equal [égal], not equal [différent], greater than [supérieur à], less than [inférieur à] ou range [plage]) à utiliser pour faire correspondre le service précisé dans la zone de service.
- Service (unlabeled) (Service [sans étiquette]) : identifie le service (comme https, ldaps ou any) à mettre en correspondance. Si vous avez spécifié l'opérateur de service de plage, ce paramètre devient deux zones, dans lesquelles vous saisissez le début et la fin de la plage.
- … : affiche une liste de services dans laquelle vous pouvez choisir le service à afficher dans la zone Service.
- Service Group (Groupe de services) : indique que vous précisez le nom d'un groupe de services pour le port source.
- Service (unlabeled) (Service [sans étiquette]) : choisissez le groupe de services à utiliser.
- ICMP Type (Type ICMP) : spécifie le type ICMP à utiliser. La valeur par défaut est any. Cliquez sur le bouton **...** pour afficher une liste des types disponibles.

- Options
  - Time Range (Plage temporelle) : spécifiez le nom d'une plage temporelle existante ou créez une nouvelle plage.
  - … : affiche le volet Add Time Range (Ajouter une plage temporelle), dans lequel vous pouvez définir une nouvelle plage temporelle.

- Please enter the description below (optional) (Veuillez saisir la description ci-dessous [facultatif]) : fournit un espace pour saisir une brève description de la règle.

Politiques de pré-fragmentation IPsec

Configuration > Site-to-Site VPN (VPN de site à site) > Advanced (Avancé) > IPsec Prefragmentation Policies (Politiques de préfragmentation IPsec)

La politique de préfragmentation IPsec spécifie comment traiter les paquets qui dépassent le paramètre d'unité de transmission maximale (MTU) lors de la tunnellisation du trafic via l'interface publique. Cette fonctionnalité permet de gérer les cas où un routeur ou un périphérique NAT entre l'ASA et le client rejette ou abandonne des fragments d'adresses IP. Par exemple, supposons qu'un client souhaite effectuer un FTP get à partir d'un serveur FTP derrière un ASA. Le serveur FTP transmet des paquets qui, encapsulés, dépasseraient la taille MTU de l'ASA sur l'interface publique. Les options sélectionnées déterminent la façon dont l'ASA traite ces paquets. La politique de préfragmentation s'applique à tout le trafic sortant de l'interface publique de l'ASA.

L'ASA encapsule tous les paquets tunnelisés. Après l'encapsulation, l'ASA fragmente les paquets qui dépassent le paramètre MTU avant de les transmettre par l'intermédiaire de l'interface publique. Il s'agit de la politique par défaut. Cette option fonctionne dans les situations où les paquets fragmentés sont autorisés à passer par le tunnel sans restriction. Pour l'exemple FTP, les paquets volumineux sont encapsulés puis fragmentés au niveau de la couche IP. Les périphériques intermédiaires peuvent abandonner des fragments ou simplement des fragments hors séquence. Les périphériques d'équilibrage de charge peuvent introduire des fragments hors séquence.

Lorsque vous activez la préfragmentation, l'ASA fragmente les paquets tunnelisés qui dépassent le paramètre MTU avant de les encapsuler. Si le bit DF sur ces paquets est défini, l'ASA efface le bit DF, fragmente les paquets, puis les encapsule. Cette action crée deux paquets IP indépendants non fragmentés quittant l'interface publique et transmet avec succès ces paquets au site homologue en transformant les fragments en paquets complets devant être réassemblés sur le site homologue. Dans notre exemple, l'ASA remplace la MTU et permet la fragmentation en effaçant le bit DF.

Remarque La modification de l'unité de transfert maximale (MTU) ou de l'option de préfragmentation sur une interface supprime toutes les connexions existantes. Par exemple, si 100 tunnels actifs se terminent sur l'interface publique et que vous modifiez la MTU ou l'option de préfragmentation sur l'interface externe, tous les tunnels actifs sur l'interface publique sont abandonnés.

Utilisez ce volet pour afficher ou **Edit** (Modifier) une politique de préfragmentation IPsec existante et une politique du bit Do Not Fragment (DF) pour une interface sélectionnée dans le volet parent.

Champs

- Interface : identifiant de l'interface. Vous ne pouvez pas modifier ce paramètre à l'aide de cette boîte de dialogue.
- Activer la préfragmentation IPsec : active ou désactive la préfragmentation IPsec. L'ASA fragmente les paquets tunnelisés qui dépassent le paramètre MTU avant de les encapsuler. Si le bit DF sur ces paquets est défini, l'ASA efface le bit DF, fragmente les paquets, puis les encapsule. Cette action crée deux paquets IP indépendants non fragmentés quittant l'interface publique et transmet avec succès ces paquets au site homologue en transformant les fragments en paquets complets devant être réassemblés sur le site homologue.

- Politique de paramètre du bit DF : politique du bit Do Not Fragment (DF) : Copy (Copier), Clear (Effacer) ou Set (Définir)

Configurer les options de fragmentation IKEv2

Sur l'ASA, la fragmentation IKEv2 peut être activée ou désactivée, la MTU (unité de transmission maximale) utilisée lors de la fragmentation des paquets IKEv2 peut être spécifiée, et une méthode de fragmentation préférée peut être configurée par l'administrateur sur l'écran suivant :

Configuration > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IKE parameters (Paramètres IKE)**

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 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 spécifiée par l'administrateur, l'unité de transfert maximale 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 :

- 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 Secure Client, 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.

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.

Procédure

Étape 1 Dans ASDM, accédez à **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IKE parameters (Paramètres IKE)**

Étape 2 Sélectionnez ou désélectionnez le champ **Enable fragmentation** (Activer la fragmentation).

Étape 3 Précisez la taille du champ **Fragmentation MTU** (MTU de fragmentation).

Étape 4 Précisez la **méthode de fragmentation préférée**.

Propositions IPsec (ensembles de transformations)

Configuration Site-to-Site VPN (VPN de site à site) Advanced (Avancé) IPsec Proposals (Transform Sets) (Propositions IPsec [ensembles de transformation]).

Une transformation est un ensemble d'opérations effectuées sur un flux de données pour assurer l'authentification des données, la confidentialité des données et la compression des données. Par exemple, une transformation est le protocole ESP avec chiffrement 3DES et l'algorithme d'authentification HMAC-MD5 (ESP-3DES-MD5).

Utilisez ce volet pour afficher, **Add** (Ajouter), **Edit** (Modifier) ou **Delete** (Supprimer) les ensembles de transformations IKEv1 et IKEv2 décrits ci-dessous. Chaque tableau affiche le nom et les détails des ensembles de transformation configurés.

Ensembles de transformations (propositions IPsec)

- **Mode** : mode d'application du chiffrement et de l'authentification ESP. Cela permet de déterminer quelle partie du paquet IP d'origine a été appliquée à l'ESP.
  - **Mode tunnel** : (par défaut) 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. L'intégralité du datagramme IP d'origine est chiffrée et devient la charge utile dans 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 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 de 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.

- **Chiffrement ESP** : algorithmes de chiffrement Encapsulating Security Protocol (ESP) pour les ensembles de transformations. ESP fournit des services de confidentialité des données, une authentification facultative des données et des services d'anti-relecture. ESP encapsule les données protégées.
- **Authentification ESP** : algorithmes d'authentification ESP pour l'ensemble de transformations.

Propositions IPsec IKEv2

- **Mode** : mode d'application du chiffrement et de l'authentification ESP. Cela permet de déterminer quelle partie du paquet IP d'origine a été appliquée à l'ESP.
  - **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 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.

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.

- **Chiffrement** : affiche l'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour la proposition IPsec IKEv2. ESP fournit des services de confidentialité des données, une authentification facultative des données et des services d'anti-relecture. ESP encapsule les données protégées.
- **Integrity Hash** (Hachage d'intégrité) : affiche l'algorithme de hachage qui garantit l'intégrité des données pour le protocole ESP. Il garantit qu'un paquet provient de l'expéditeur attendu et qu'aucune modification n'a été apportée en transit. Il garantit qu'un paquet provient de l'expéditeur attendu et qu'aucune modification n'a été apportée en transit. Vous devez choisir l'algorithme d'intégrité nulle si AES-GCM/GMAC a été configuré comme algorithme de chiffrement.

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.