VPN de site à site

Un réseau privé virtuel (VPN) est une connexion réseau qui établit un tunnel sécurisé entre des pairs distants en utilisant une source publique, comme Internet ou un autre réseau. Les VPN utilisent des tunnels pour encapsuler les paquets de données dans les paquets IP normaux pour les acheminer sur les réseaux IP. Ils utilisent le chiffrement pour assurer la confidentialité et l'authentification pour assurer l'intégrité des données.

- Principes de base du VPN, à la page 1
- Gestion des VPN de site à site, à la page 10
- Supervision du VPN de site à site, à la page 28
- Exemples de VPN de site à site, à la page 28

Principes de base du VPN

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

Les technologies VPN basées sur IPsec utilisent les normes de protocole ISAKMP ou IKE (Internet Security Association and Key Management Protocol) et les normes de tunnellisation 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.

Un périphérique dans un VPN 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.

Une fois la connexion VPN de site à site établie, les hôtes derrière la passerelle locale peuvent se connecter aux hôtes derrière la passerelle distante par le tunnel VPN sécurisé. Une connexion comprend les adresses IP et les noms d'hôte des deux passerelles, les sous-réseaux derrière elles et la méthode que les deux passerelles utilisent pour s'authentifier l'une auprès de l'autre.

protocole IKE (Internet Key Exchange)

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec.

La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion.

Une politique IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation IKE entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité qui protègent les négociations IKE ultérieures. Pour IKE version 1 (IKEv1), les politiques IKE contiennent un seul ensemble d'algorithmes et un groupe de modules. Contrairement à IKEv1, dans une politique IKEv2, vous pouvez sélectionner plusieurs algorithmes et groupes de modules parmi lesquels les homologues peuvent choisir pendant la négociation de la phase 1. Il est possible de créer une seule politique IKE, bien que vous puissiez souhaiter que différentes politiques accordent une priorité plus élevée aux options les plus souhaitées. Pour les VPN de site à site, vous pouvez créer une politique IKE.

Pour définir une politique IKE, spécifiez :

- Une priorité unique (de 1 à 65 543, 1 étant la priorité la plus élevée).
- Une méthode de chiffrement pour la négociation IKE, afin de protéger les données et de garantir la confidentialité.
- Une méthode HMAC (hachage de codes d'authentification de message) (appelée algorithme d'intégrité dans IKEv2) pour s'assurer de l'identité de l'expéditeur et pour s'assurer que le message n'a pas été modifié pendant le transfert.
- Pour IKEv2, une fonction pseudo-aléatoire (PRF) distincte est utilisée comme algorithme pour extraire le contenu de la clé et les opérations de hachage nécessaires pour le chiffrement du tunnel IKEv2. Les options sont les mêmes que celles utilisées pour l'algorithme de hachage.
- Un groupe Diffie-Hellman pour déterminer la force de l'algorithme de détermination de la clé de chiffrement. Le périphérique utilise cet algorithme pour déduire les clés de chiffrement et de hachage.
- Une méthode d'authentification pour garantir l'identité des homologues.
- Une limite de temps pendant laquelle le périphérique utilise une clé de chiffrement avant de la remplacer.

Lorsque la négociation IKE commence, l'homologue qui commence la négociation envoie toutes ses politiques activées à l'homologue distant, et l'homologue distant 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 (intégrité et PRF pour IKEv2), d'authentification et de Diffie-Hellman, et une durée de vie d'association inférieure ou égale à la durée de vie indiquée dans la politique envoyée. Si les durées de vie ne sont pas identiques, la durée de vie la plus courte, obtenue de l'homologue distant, s'applique. Par défaut, une politique IKE simple qui utilise DES est la seule politique activée. Vous pouvez activer d'autres

politiques IKE avec des priorités plus élevées pour négocier des normes de chiffrement plus strictes, mais la politique DES devrait garantir la réussite de la négociation.

Dans quelle mesure une connexion VPN doit-elle être sécurisée?

Étant donné qu'un tunnel VPN traverse généralement un réseau public, très probablement Internet, vous devez chiffrer la connexion pour protéger le trafic. Vous définissez le chiffrement et les autres techniques de sécurité à appliquer à l'aide des politiques IKE et des propositions IPsec.

Si votre licence vous permet d'appliquer un chiffrement renforcé, vous pouvez choisir parmi un large éventail d'algorithmes de chiffrement et de hachage et de groupes Diffie-Hellman. Cependant, en règle générale, plus le chiffrement que vous appliquez au tunnel est fort, plus les performances du système sont mauvaises. Trouvez un équilibre entre sécurité et performance qui offre une protection suffisante sans compromettre l'efficacité.

Nous ne pouvons pas fournir de conseils précis sur les options à choisir. Si vous agissez au sein d'une grande entreprise ou d'une autre organisation, vous devez peut-être vous conformer à des normes déjà définies. Sinon, prenez le temps d'étudier les options.

Les rubriques suivantes expliquent les options disponibles.

Choix de l'algorithme de chiffrement à utiliser

Au moment de décider quels algorithmes de chiffrement utiliser pour la politique IKE ou la proposition IPsec, votre choix se limite aux algorithmes pris en charge par les périphériques du VPN.

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

Pour les propositions IPsec, l'algorithme est utilisé par le protocole ESP (Encapsulating Security Protocol), qui fournit des services d'authentification, de chiffrement et d'anti-relecture. ESP est un protocole IP de type 50. Dans les propositions IKEv1 IPsec, le nom de l'algorithme commence par ESP-.

Si votre licence de périphérique est admissible au chiffrement fort, vous pouvez choisir parmi les algorithmes de chiffrement suivants. Si vous n'êtes pas autorisé à utiliser le chiffrement renforcé, vous pouvez sélectionner DES uniquement.

Remarque Si vous êtes qualifié pour un chiffrement renforcé, avant de passer de la licence d'évaluation à une licence Smart, vérifiez et mettez à jour vos algorithmes de chiffrement pour un chiffrement plus fort afin que la configuration VPN fonctionne correctement. Choisissez des algorithmes basés sur AES. DES n'est pas pris en charge si vous êtes inscrit avec un compte prenant en charge le chiffrement renforcé. Après l'enregistrement, vous ne pouvez pas déployer les modifications avant d'avoir supprimé toutes les utilisations de DES.

- AES-GCM : (IKEv2 uniquement) Le chiffrement avancé standard en mode Galois/compteur est un mode de fonctionnement de chiffrement par bloc qui assure la confidentialité et l'authentification de l'origine des données, et qui offre une sécurité supérieure à l'AES. AES-GCM offre trois forces de clé différentes : les clés de 128, 192 et 256 bits. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances. GCM est un mode AES nécessaire pour prendre en charge NSA Suite B. NSA Suite B est un ensemble d'algorithmes cryptographiques que les périphériques doivent prendre en charge pour répondre aux normes fédérales en matière de force cryptographique. .

- AES : Advanced Encryption Standard est un algorithme de chiffrement symétrique qui offre une sécurité supérieure à DES et qui est plus efficace que le 3DES du point de vue informatique. AES offre trois puissances de clé différentes : les clés de 128, 192 et 256 bits. Une clé plus longue offre une sécurité plus élevée, mais une réduction des performances.
- DES, la norme de chiffrement des données, qui chiffre à l'aide de clés de 56 bits, est un algorithme de blocage de clé secrète symétrique. Si votre compte de licence ne répond pas aux exigences du contrôle des exportations, ceci est votre seule possibilité.
- Null, ESP-Null : ne pas l'utiliser. Un algorithme de chiffrement nul permet une authentification sans chiffrement. Cette fonction n'est pas prise en charge sur la plupart des plateformes.

Décider des algorithmes de hachage à utiliser

Dans les politiques IKE, l'algorithme de hachage crée un condensé du message, qui est utilisé pour assurer l'intégrité du message. Dans IKEv2, l'algorithme de hachage est séparé en deux options, une pour l'algorithme d'intégrité et une pour la fonction pseudo-aléatoire (PRF).

Dans les propositions IPsec, l'algorithme de hachage est utilisé par le protocole ESP (Encapsulating Security Protocol) pour l'authentification. Dans les propositions IKEv2 IPsec, cela s'appelle le hachage d'intégrité. Dans les propositions IKEv1 IPsec, le nom de l'algorithme est précédé de ESP-, et il y a également un suffixe -HMAC (qui signifie « code d'authentification de la méthode de hachage »).

Pour IKEv2, vous pouvez configurer plusieurs algorithmes de hachage. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

Vous pouvez choisir parmi les algorithmes de hachage suivants.

- SHA (Secure Hash Algorithm) : la norme SHA (SHA1) produit un condensé de 160 bits.

  Les options SHA-2 suivantes, qui sont encore plus sécurisées, sont disponibles pour les configurations IKEv2. Choisissez l'une de ces spécifications si vous souhaitez mettre en œuvre la spécification de chiffrement de la suite B de NSA.

  - SHA256 : spécifie l'algorithme de hachage sécurisé SHA2 avec le condensé 256 bits.
  - SHA384 : spécifie l'algorithme de hachage sécurisé SHA 2 avec le condensé de 384 bits.
  - SHA512 : spécifie l'algorithme Secure Hash SHA2 avec le condensé 512 bits.

- Null ou aucun (NULL, ESP-NONE) : (propositions IPsec uniquement.) un algorithme de hachage nul; cela est généralement utilisé à des fins de test uniquement. Cependant, vous devez choisir l'algorithme d'intégrité nulle si vous sélectionnez l'une des options AES-GCM comme algorithme de chiffrement. Même si vous choisissez une option non nulle, le hachage d'intégrité est ignoré pour ces normes de chiffrement.

Choix du groupe de module Diffie-Hellman à utiliser

Vous pouvez utiliser les algorithmes de dérivation de clé Diffie-Hellman suivants pour générer des clés d'association de sécurité IPsec. Chaque groupe a un module de taille différent. Un module plus élevé offre une sécurité élevée, mais nécessite plus de temps de traitement. Vous devez avoir un groupe de module correspondant sur les deux homologues.

Si vous sélectionnez le chiffrement AES, pour prendre en charge les grandes tailles de clés requises par AES, vous devez utiliser le groupe Diffie-Hellman (DH) 5 ou supérieur. Les politiques IKEv1 ne prennent pas en charge tous les groupes répertoriés ci-dessous.

Pour mettre en œuvre la spécification de cryptographie B de NSA, utilisez IKEv2 et sélectionnez l'une des options ECDH (elliptique courbe Diffie-Hellman) : 19, 20 ou 21. Les options de courbe elliptique et les groupes qui utilisent un module de 2048 bits sont moins exposés aux attaques telles que Logjam.

Pour IKEv2, vous pouvez configurer plusieurs groupes. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue dans cet ordre. Pour IKEv1, vous ne pouvez sélectionner qu'une seule option.

- 14 : Groupe Diffie-Hellman 14 : groupe MODP (exponentiel modulaire) 2048 bits. Considérées comme une bonne protection pour les clés de 192 bits.
- 15 : Groupe Diffie-Hellman 15 : groupe MODP 3 072 bits.
- 16 : Groupe Diffie-Hellman 16 : groupe MODP 4096 bits.
- 19 : Groupe Diffie-Hellman 19 : Courbe elliptique 256 bits modulo un nombre premier (ECP) du National Institue of Standards and Technology (NIST).
- 20 : Groupe Diffie-Hellman 20 : Groupe ECP NIST 384 bits.
- 21 : Groupe Diffie-Hellman 21 : Groupe ECP NIST 521 bits.
- 31 : Groupe Diffie-Hellman 31 : Courbe 25519 256 bits, groupe EC.

Choix de la méthode d'authentification à utiliser

Vous pouvez utiliser les méthodes suivantes pour authentifier les homologues dans une connexion VPN de site à site.

Clés prépartagées

Les clés prépartagées sont des chaînes de clés secrètes configurées sur chaque homologue de la connexion. Ces clés sont utilisées par IKE pendant la phase d'authentification. Pour IKEv1, vous devez configurer la même clé prépartagée sur chaque homologue. Pour IKEv2, vous pouvez configurer des clés uniques sur chaque homologue.

Les clés prépartagées ne sont pas aussi évolutives que les certificats. Si vous devez configurer un grand nombre de connexions VPN de site à site, utilisez la méthode des certificats plutôt que la méthode de la clé prépartagée.

Certificats

Les certificats numériques utilisent des paires de clés RSA pour signer et chiffrer les messages de gestion des clés IKE. Lorsque vous configurez chaque extrémité de la connexion VPN site-à-site, vous sélectionnez le certificat d'identité du périphérique local, afin que l'homologue distant puisse authentifier l'homologue local.

Pour utiliser la méthode du certificat, vous devez effectuer les opérations suivantes :

1. Enregistrez votre homologue local auprès d'une autorité de certification (CA) et obtenez un certificat d'identité d'appareil. Chargez ce certificat sur le périphérique. Pour en savoir plus, consultez Charger les certificats d'identité interne et d'autorité de certification interne.

Si vous êtes également responsable de l'homologue distant, enregistrez également cet homologue. Bien qu'il soit pratique d'utiliser la même autorité de certification pour les homologues, il n'est pas obligatoire.

Vous ne pouvez pas utiliser un certificat autosigné pour établir une connexion VPN. Vous devez inscrire le périphérique auprès d'une autorité de certification.

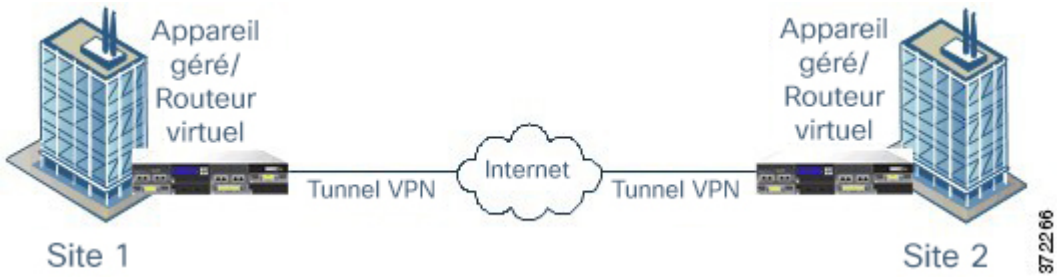
Si vous utilisez une autorité de certification Windows pour créer des certificats pour les points terminaux VPN de site à site, vous devez utiliser un certificat qui spécifie le système terminal de sécurité IP pour l'extension des politiques d'application. Vous pouvez le trouver dans la boîte de dialogue des propriétés du certificat, sous l'onglet Extensions (sur le serveur Windows CA). La valeur par défaut pour cette extension est IP security IKE intermédiaire, qui ne fonctionne pas pour un VPN de site à site configuré à l'aide de Firepower Device Manager.

2. Chargez le certificat d'autorité de certification de confiance qui a été utilisé pour signer le certificat d'identité de l'homologue local. Si vous avez utilisé une autorité de certification intermédiaire, chargez la chaîne complète, y compris les certificats racine et intermédiaire. Pour en savoir plus, consultez Téléchargement des certificats de l'autorité de certification de confiance.
3. Si l'homologue distant était inscrit auprès d'une autorité de certification différente, chargez également le certificat d'autorité de certification de confiance utilisé pour signer le certificat d'identité de l'homologue distant. Obtenez le certificat de l'organisation qui contrôle l'homologue distant. S'ils ont utilisé une autorité de certification intermédiaire, chargez la chaîne complète, y compris les certificats racine et intermédiaire.
4. Lorsque vous configurez la connexion VPN de site à site, sélectionnez la méthode de certificat, puis sélectionnez le certificat d'identité de l'homologue local. Chaque extrémité de la connexion spécifie le certificat pour l'extrémité locale de la connexion; vous ne spécifiez pas le certificat pour l'homologue distant.

Topologies VPN

Vous pouvez configurer uniquement les connexions VPN point à point en utilisant Firepower Device Manager. Bien que toutes les connexions soient point à point, vous pouvez vous connecter à des VPN plus importants en étoile ou en maillage en définissant chacun des tunnels auxquels votre périphérique participe.

Le diagramme suivant présente une topologie VPN point à point typique. Dans une topologie VPN point à point, deux points terminaux communiquent directement l'un avec l'autre. Vous configurez les deux points terminaux en tant qu'périphériques homologues, et l'un ou l'autre des périphériques peut démarrer la connexion sécurisée.



Établissement de connexions VPN de site à site avec des homologues à adresse dynamique

Vous pouvez créer des connexions VPN de site à site avec des homologues même lorsque vous ne connaissez pas l'adresse IP de l'homologue. Cela peut être utile dans les situations suivantes :

- Si l'homologue obtient son adresse à l'aide de DHCP, vous ne pouvez pas dépendre du point terminal distant d'une adresse IP statique spécifique.
- Lorsque vous souhaitez autoriser un nombre indéterminé d'homologues distants à établir une connexion avec le périphérique, qui servira de concentrateur dans une topologie en étoile.

Lorsque vous devez établir une connexion sécurisée avec un homologue B dont l'adresse est attribuée dynamiquement, vous devez vous assurer que l'extrémité de la connexion, A, dispose d'une adresse IP statique. Ensuite, lorsque vous créez la connexion sur A, spécifiez que l'adresse de l'homologue est dynamique. Toutefois, lorsque vous configurez la connexion sur l'homologue B, veillez à saisir l'adresse IP de A comme adresse d'homologue distant.

Lorsque le système établit des connexions VPN de site à site, toutes les connexions pour lesquelles l'homologue possède une adresse dynamique seront de réponse uniquement. C'est-à-dire que l'homologue distant doit être celui qui amorce la connexion. Lorsque l'homologue distant tente d'établir la connexion, votre périphérique valide la connexion à l'aide de la clé prépartagée ou du certificat, selon la méthode que vous avez définie dans la connexion.

Étant donné que la connexion VPN est établie uniquement après que l'homologue distant a lancé la connexion, tout trafic sortant correspondant aux règles de contrôle d'accès qui autorisent le trafic dans le tunnel VPN sera abandonné jusqu'à ce que cette connexion soit établie. Cela garantit que les données ne quittent pas votre réseau sans le chiffrement et la protection VPN appropriés.

Virtual Tunnel Interfaces et VPN basé sur le routage

Traditionnellement, vous configurez une connexion VPN de site à site en définissant les réseaux locaux et distants spécifiques qui seront chiffrés sur le tunnel VPN. Ceux-ci sont définis dans une carte cryptographique qui fait partie du profil de connexion VPN. Ce type de VPN de site à site est appelé basé sur les politiques.

Vous pouvez également configurer un VPN de site à site basé sur le routage. Dans ce cas, vous créez une interface de tunnel virtuel (VTI), qui est une interface virtuelle associée à une interface physique spécifique, généralement l'interface externe. Ensuite, vous utilisez la table de routage, avec des routes statiques et dynamiques, pour diriger le trafic souhaité vers le VTI. Tout trafic acheminé par le VTI (sortant) est chiffré sur le tunnel VPN que vous configurez pour le VTI.

Avec le VPN de site à site basé sur le routage, vous gérez les réseaux protégés dans une connexion VPN donnée en modifiant simplement la table de routage, sans modifier le profil de la connexion VPN. Vous n'avez pas besoin de suivre les réseaux distants et de mettre à jour le profil de connexion VPN pour prendre en compte ces modifications. Cela simplifie la gestion du VPN pour les fournisseurs de services infonuagiques et les grandes entreprises.

En outre, vous pouvez créer des règles de contrôle d'accès pour le VTI afin d'affiner les types de trafic autorisés dans le tunnel. Par exemple, vous pouvez appliquer l'inspection de prévention des intrusions et le filtrage des URL et des applications.

Aperçu du processus de configuration des VPN basés sur le routage

En tant qu'aperçu, le processus de configuration d'un VPN de site à site basé sur le routage comprend les étapes suivantes :

Procédure

Étape 1 Créez la politique IKEv1/2 et la proposition IPsec pour le terminal local.

Étape 2 Créez une interface de tunnel virtuel (VTI) associée à l'interface physique qui fait face à l'homologue distant.

Étape 3 Créez le profil de connexion VPN de site à site qui utilise le VTI, la politique IKE et la proposition IPsec.

Étape 4 Créez les mêmes propositions IKE et IPsec sur l'homologue distant, et un VTI distant, et le profil de connexion VPN de site à site qui spécifie ce VTI local comme point terminal distant (du point de vue de l'homologue distant).

Étape 5 Créez des routes et des règles de contrôle d'accès sur les deux homologues pour envoyer le trafic approprié dans le tunnel.

Assurez-vous que les routes et le contrôle d'accès sur chaque terminal sont en miroir, pour permettre au trafic de circuler dans les deux sens.

Les routes statiques auraient ces caractéristiques générales :

- **Interface** : nom de l'interface de tunnel virtuel (VTI).
- **Networks**(réseaux) : objets réseau qui définissent les réseaux distants protégés par le terminal distant.
- **Gateway** (Passerelle) : objet réseau qui définit l'adresse IP du point terminal distant du tunnel VPN.

Lignes directrices pour les interfaces de tunnel virtuel et VPN basé sur le routage

Directives IPv6

Les interfaces de tunnel virtuel prennent uniquement en charge les adresses IPv4. Vous ne pouvez pas configurer une adresse IPv6 sur un VTI.

Directives supplémentaires

- Vous pouvez créer un maximum de 1 024 VTI.
- Vous ne pouvez pas configurer l'injection de route inverse, statique ou dynamique, sur un VPN basé sur le routage VTI. (Vous pouvez configurer l'injection de route inverse à l'aide de l'API Firewall Threat Defense uniquement.)
- Vous ne pouvez pas configurer une adresse d'homologue dynamique lorsque vous sélectionnez un VTI comme interface locale.
- Vous ne pouvez pas configurer d'homologues de sauvegarde à distance lorsque vous sélectionnez un VTI comme interface locale.

- Vous ne pouvez pas créer de VTI pour une interface source qui est affectée à un routeur virtuel personnalisé. Lorsque vous utilisez des routeurs virtuels, vous pouvez configurer des VTI sur les interfaces du routeur virtuel global uniquement.
- Les associations de sécurité IKE et IPsec seront rachetées en permanence, quel que soit le trafic de données dans le tunnel. Cela garantit que les tunnels VTI sont toujours actifs.
- Vous ne pouvez pas configurer à la fois IKEv1 et IKEv2 sur un profil de connexion basé sur le routage : vous ne devez configurer qu'une seule version IKE.
- Les configurations du VTI et de la carte de chiffrement peuvent coexister sur la même interface physique, à condition que l'adresse homologue configurée dans la carte de chiffrement et la destination du tunnel pour le VTI soient différentes.
- Seul le protocole de routage BGP est pris en charge sur le VTI.
- Si le système met fin aux clients IKEv2 VTI IOS, désactivez la demande config-exchange sur IOS, car le système ne peut pas récupérer les attributs mode-CFG pour la session initiée par un client VTI IOS.
- Les VPN de site à site basés sur le routage sont configurés comme bidirectionnels, ce qui signifie que l'un ou l'autre des points terminaux du tunnel VPN peut lancer la connexion. Après avoir créé le profil de connexion, vous pouvez modifier ce point terminal pour qu'il soit soit le seul initiateur (INITIATE_ONLY) ou exclusivement le répondeur (RESPOND_ONLY). Assurez-vous de modifier le terminal distant pour utiliser le type de connexion complémentaire. Pour apporter cette modification, vous devez accéder à l'explorateur d'API et utiliser GET /devices/default/s2sconnectionprofiles pour trouver le profil de connexion. Vous pouvez ensuite copier/coller le contenu du corps dans la méthode PUT /devices/default/s2sconnectionprofiles/{objId}, mettre à jour **connectionType** pour préciser le type souhaité et exécuter la méthode.

Décharge de flux IPsec

Vous pouvez configurer des modèles de périphérique de prise en charge pour utiliser le déchargement de flux IPsec. Après la configuration initiale d'une association de sécurité (SA), d'un VPN de site à site ou d'un VPN d'accès à distance IPsec, les connexions IPsec sont déchargées vers le FPGA (field programmable gate RAID) dans le périphérique, ce qui devrait améliorer les performances du périphérique.

Les opérations déchargées sont spécifiquement liées au traitement de pré déchiffrement et de déchiffrement à l'entrée, et au traitement de pré chiffrement et de chiffrement à la sortie. Le logiciel système gère le flux interne pour appliquer vos politiques de sécurité.

Le déchargement de flux IPsec est activé par défaut et s'applique aux types de périphériques suivants :

- Secure Firewall 3100

Limites du déchargement de flux IPsec

Les flux IPsec suivants ne sont pas déchargés :

- Tunnels IKEv1. Seuls les tunnels IKEv2 seront déchargés. IKEv2 prend en charge les chiffrements plus forts.
- Flux pour lesquels une régénération basée sur le volume est configurée.
- Flux pour lesquels la compression est configurée.

- Flux des modes de transport. Seuls les flux en mode tunnel seront déchargés.
- Format AH. Seul le format ESP/NAT-T sera pris en charge.
- Les flux dont la post-fragmentation est configurée.
- Flux qui ont une taille de fenêtre d'anti-relecture autre que 64 bits et l'anti-relecture n'est pas désactivée.
- Les flux pour lesquels le filtre de pare-feu est activé.

Configurer le déchargement de flux IPsec

Le déchargement de flux IPSec est activé par défaut sur les plateformes matérielles qui prennent en charge la fonctionnalité. Pour modifier la configuration, utilisez FlexConfig pour implémenter la commande **flow-offload-ipsec**. Consultez le document de référence sur les commandes ASA pour des informations détaillées sur la commande.

Gestion des VPN de site à site

Un réseau privé virtuel (VPN) est une connexion réseau qui établit un tunnel sécurisé entre des pairs distants en utilisant une source publique, comme Internet ou un autre réseau. Les VPN utilisent des tunnels pour encapsuler les paquets de données dans les paquets IP normaux pour les acheminer sur les réseaux IP. Ils utilisent le chiffrement pour assurer la confidentialité et l'authentification pour assurer l'intégrité des données.

Vous pouvez créer des connexions VPN avec des périphériques homologues. Toutes les connexions sont point à point, mais vous pouvez lier le périphérique à des VPN plus importants en étoile ou maillés en configurant toutes les connexions pertinentes.

Avant de commencer

Les éléments suivants déterminent le type et le nombre de connexions VPN de site à site que vous pouvez recréer :

- Les connexions VPN utilisent le chiffrement pour sécuriser la confidentialité du réseau. Les algorithmes de chiffrement que vous pouvez utiliser varient selon que votre licence de base autorise le chiffrement renforcé. Ceci est contrôlé par le fait que vous ayez sélectionné l'option d'autoriser les fonctionnalités d'exportation contrôlée sur l'appareil lorsque vous vous êtes enregistré auprès du gestionnaire de licences Smart Cisco. Si vous utilisez la licence d'évaluation, ou si vous n'avez pas activé la fonctionnalité contrôlée à l'exportation, vous ne pouvez pas utiliser le chiffrement renforcé.
- Vous ne pouvez pas créer plus de 20 profils IPsec uniques. Le caractère unique est déterminé par la combinaison des propositions et des certificats IKEv1/v2, du type de connexion et du groupe DH et de la durée de vie SA. Vous pouvez réutiliser les profils existants. Ainsi, si vous utilisez les mêmes paramètres pour toutes vos connexions VPN de site à site, vous avez un profil IPsec unique. Une fois que vous avez atteint la limite de 20 profils IPsec uniques, vous ne pouvez pas créer de nouvelles connexions VPN de site à site, sauf si vous utilisez la même combinaison d'attributs que vous avez utilisée pour un profil de connexion existant.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis cliquez sur **View Configuration** (Afficher la configuration) dans le groupe VPN de site à site.

Cela ouvre la page VPN de site à site, qui répertorie toutes les connexions que vous avez configurées.

Étape 2 Effectuez l'une des actions suivantes.

- Pour créer une nouvelle connexion VPN de site à site, cliquez sur le bouton +. Consultez Configuration d'une connexion VPN de site à site, à la page 11.

  S'il n'y a aucune connexion pour le moment, vous pouvez également cliquer sur le bouton **Create Site-to-Site Connection** (Créer une connexion de site à site .

- Pour modifier une connexion existante, cliquez sur l'icône de modification ( ) de la connexion. Consultez Configuration d'une connexion VPN de site à site, à la page 11.

- Pour copier un résumé de la configuration de la connexion dans le presse-papier, cliquez sur l'icône de copie ( ) de la connexion. Vous pouvez coller ces informations dans un document et l'envoyer à l'administrateur du périphérique distant pour l'aider à configurer l'autre extrémité de la connexion.

- Pour supprimer une connexion dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la connexion.

Configuration d'une connexion VPN de site à site

Vous pouvez créer une connexion VPN point à point pour lier votre périphérique à un autre périphérique, en supposant que vous ayez la collaboration et l'autorisation du propriétaire du périphérique distant. Bien que toutes les connexions soient point à point, vous pouvez vous connecter à des VPN plus importants en étoile ou en maillage en définissant chacun des tunnels auxquels votre périphérique participe.

Avant de commencer

Vous pouvez créer une seule connexion VPN par combinaison réseau local/réseau distant. Cependant, vous pouvez créer plusieurs connexions pour un réseau local si le réseau distant est unique dans chaque profil de connexion.

Si les réseaux distants se chevauchent, veillez à créer d'abord le profil de connexion le plus restreint. Le système créera les tunnels dans l'ordre dans lequel vous créez les profils de connexion, et non dans l'ordre dans lequel ils sont affichés (qui est simplement alphabétique).

Par exemple, si vous souhaitez qu'un tunnel de 192.16.0.0/16 à 10.91.0.0/16 aille au point de terminaison distant A, mais que le tunnel 192.16.0.0/24 vers le reste de 10.0.0.0/8 passe par le point de terminaison distant B, vous devez créer le profil de connexion pour A avant de créer celui pour B.

Procédure

Étape 1 Cliquez sur **Device (périphérique)**, puis sur **View Configuration (Afficher la configuration)** dans le groupe VPN de site à site.

Étape 2 Effectuez l'une des actions suivantes :

- Pour créer une nouvelle connexion VPN de site à site, cliquez sur le bouton +.

  S'il n'y a aucune connexion pour le moment, vous pouvez également cliquer sur le bouton **Create Site-to-Site Connection** (Créer une connexion de site à site .

- Pour modifier une connexion existante, cliquez sur l'icône de modification ( ) de la connexion.

Pour supprimer une connexion dont vous n'avez plus besoin, cliquez sur l'icône de suppression ( ) de la connexion.

Étape 3 Définissez les points terminaux de la connexion VPN point à point.

- **Nom du profil de connexion** : le nom de cette connexion, jusqu'à 64 caractères sans espaces. Par exemple, MainOffice. Vous ne pouvez pas utiliser une adresse IP comme nom.
- **Type** : comment vous identifierez le trafic qui doit être envoyé par le tunnel VPN. Sélectionnez l'une des options suivantes :
  - **Basé sur le routage (VTI)** : vous utiliserez la table de routage, principalement les routes statiques, pour définir les réseaux locaux et distants qui doivent participer au tunnel. Si vous sélectionnez cette option, vous devez sélectionner une interface de tunnel virtuel (VTI) comme interface d'accès au VPN local. Vous devez également utiliser une adresse IP statique pour l'extrémité distante du tunnel. Assurez-vous de configurer les routes statiques et les règles de contrôle d'accès appropriées pour le VTI après avoir créé le profil de connexion VPN.
  - **Basé sur les politiques** : vous préciserez les réseaux locaux et distants directement dans le profil de connexion VPN de site à site. Il s'agit de l'approche classique pour définir le trafic qui doit être protégé par le tunnel VPN.
- **Site local** : ces options définissent le point terminal local.
  - **Interface d'accès VPN locale** : sélectionnez l'interface à laquelle l'homologue distant peut se connecter. Il s'agit généralement de l'interface externe. L'interface ne peut pas faire partie d'un groupe de pont. Si vous configurez des homologues de secours pour les connexions basées sur des politiques, veillez à sélectionner toutes les interfaces par lesquelles les homologues peuvent se connecter. Pour les connexions basées sur le routage, vous ne pouvez sélectionner qu'une seule interface.
  - **Réseau local** :(basé sur les politiques uniquement) Cliquez + et sélectionnez les objets réseau qui identifient les réseaux locaux qui doivent participer à la connexion VPN. Les utilisateurs de ces réseaux pourront atteindre les réseaux distants par la connexion.

Remarque
Vous pouvez utiliser des adresses IPv4 ou IPv6 pour ces réseaux, mais vous devez avoir un type d'adresse correspondant de chaque côté de la connexion. Par exemple, la connexion VPN pour un réseau IPv4

local doit avoir au moins un réseau IPv4 distant. Vous pouvez combiner IPv4 et IPv6 des deux côtés d'une connexion unique. Les réseaux protégés pour les points terminaux ne peuvent pas se chevaucher.

- **Site distant** : ces options définissent le terminal distant.
  - **Static**(Statique)/**Dynamic**(Dynamique) : si l'adresse IP de l'homologue distant est définie de manière statique ou dynamique (par exemple, par DHCP). Si vous sélectionnez **Static** (Statique), saisissez également l'adresse IP de l'homologue distant. Si vous sélectionnez **Dynamic** (Dynamique), seul l'homologue distant pourra établir cette connexion VPN.

    Pour le VPN basé sur le routage, vous pouvez sélectionner **Static** (Statique) uniquement.
  - **Adresse IP distante** (adressage statique uniquement.) : Saisissez l'adresse IP de l'interface de l'homologue du VPN distant qui accueillera la connexion VPN.
  - **Homologues de sauvegarde à distance** : (facultatif, connexions basées sur des politiques uniquement.) Cliquez sur **Add Peer** (Ajouter un homologue) pour ajouter une sauvegarde pour le point terminal distant. Si l'homologue distant principal n'est pas disponible, le système tentera de rétablir la connexion VPN en utilisant l'un des homologues de secours. Vous pouvez ajouter plusieurs sauvegardes.

    Lorsque vous configurez chaque homologue de sauvegarde, vous pouvez configurer les clés et les certificats prépartagés à utiliser avec cet homologue. Utilisez la même technique que vous avez configurée pour l'homologue distant principal. Laissez ce paramètre vide pour utiliser les valeurs configurées pour le profil de connexion.

    Après avoir configuré le premier homologue de sauvegarde, vous pouvez en ajouter un autre en cliquant sur **Add Another Peer (Ajouter un autre homologue)**, supprimer un homologue ou cliquer sur **Edit (Modifier)** pour changer les paramètres d'un homologue.

    Si un homologue de secours est accessible par une interface différente de celle de l'homologue principal, veillez à sélectionner l'interface requise sous **Local VPN Access Interface** (Interface d'accès VPN locale).
  - **Réseau distant** :(basé sur les politiques uniquement) Cliquez **+** et sélectionnez les objets réseau qui identifient les réseaux distants qui doivent participer à la connexion VPN. Les utilisateurs de ces réseaux pourront atteindre les réseaux locaux par le biais de la connexion.

Étape 4 Cliquez sur **Next** (suivant).

Étape 5 Définissez la configuration de confidentialité pour le VPN.

Remarque
Votre licence détermine les protocoles de chiffrement que vous pouvez sélectionner. Vous devez être admissible au chiffrement renforcé, c'est-à-dire satisfaire aux contrôles des exportations, pour pouvoir choisir d'autres options que les plus basiques.ions, pour choisir tout, sauf les options les plus simples.

- **Version IKE 2**, **Version IKE 1** : choisissez les versions IKE à utiliser lors des négociations d'Internet Key Exchange (IKE). Pour les connexions basées sur des politiques, vous pouvez sélectionner l'une ou les deux; pour celles basées sur le routage, vous ne pouvez sélectionner qu'une seule. Lorsque le périphérique tente de négocier une connexion avec l'autre homologue, il utilise les versions que vous autorisez et que l'autre homologue accepte. Si vous autorisez les deux versions, le périphérique revient automatiquement à l'autre version si les négociations échouent avec la version initialement choisie. IKEv2 est toujours essayé en premier s'il est configuré. Les deux homologues doivent prendre en charge IKEv2 pour l'utiliser dans une négociation.

- **Politique IKE** : Internet Key Exchange (IKE) est un protocole de gestion de clés utilisé pour authentifier les homologues IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec (SA). Il s'agit d'une politique globale : les objets que vous activez sont appliqués à tous les VPN. Cliquez sur **Edit** (Modifier) pour examiner les politiques actuellement activées globalement par version IKE, puis pour activer et créer de nouvelles politiques. Pour en savoir plus, consultez Configuration de la politique IKE globale, à la page 17.
- **Proposition IPsec** : la proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec. Cliquez sur **Edit** (Modifier)r et sélectionnez les propositions pour chaque version IKE. Sélectionnez toutes les propositions que vous souhaitez autoriser. Cliquez sur **Set Default** (Définir par défaut) pour simplement sélectionner les valeurs par défaut du système, qui varient en fonction de votre conformité aux règles d'exportation. Le système négocie avec l'homologue, en commençant par le groupe le plus fort vers le plus faible jusqu'à ce qu'une correspondance soit trouvée. Pour en savoir plus, consultez Configuration des propositions IPsec, à la page 22.
- **Authentication Type** (type d'authentification) : comment vous souhaitez authentifier les homologues dans la connexion VPN, soit **par clé manuelle prépartagée**, soit **par certificat**. Vous devez également remplir les champs suivants en fonction de votre sélection. Pour IKEv1, votre sélection doit correspondre à la méthode d'authentification sélectionnée dans l'objet de politique IKEv1 configuré pour la connexion. Pour des informations détaillées sur les options, consultez Choix de la méthode d'authentification à utiliser, à la page 5.
  - (IKEv2) **Local Preshared Key** (Clé prépartagée locale), **Remote Peer Preshared Key** (Clé prépartagée d'homologue distant) : les clés définies sur ce périphérique et sur le périphérique distant pour la connexion VPN. Ces clés peuvent être différentes dans IKEv2. La clé peut comporter entre 1 et 127 caractères alphanumériques.
  - (IKEv1) **Clé prépartagée** : la clé qui est définie sur les périphériques locaux et distants. La clé peut comporter entre 1 et 127 caractères alphanumériques.
  - **Certificate** (Certificat) : le certificat d'identité du périphérique pour l'homologue local. Il doit s'agir d'un certificat obtenu auprès d'une autorité de certification (CA) ; vous ne pouvez pas utiliser de certificat autosigné. Si vous n'avez pas chargé le certificat, cliquez sur le lien **Create New Object** (Créer un nouvel objet). Vous devez également télécharger le certificat racine et tous les certificats d'autorité de certification intermédiaires de confiance utilisés pour signer le certificat d'identité. Assurez-vous de définir le champ **Validation Usage** (utilisation de validation) pour le certificat chargé de manière à inclure **IPsec Client**. Si vous ne les avez pas encore chargés, vous pouvez le faire après avoir terminé cet assistant.
- **IPsec Settings** (Paramètres IPsec) : la durée de vie de l'association de sécurité. Une fois la durée de vie atteinte, le système renégocie l'association de sécurité. Lorsque le système reçoit une demande de négociation de l'homologue, il utilise la plus petite des durées de vie proposées par l'homologue ou configurées localement comme durée de vie des nouvelles associations de sécurité. Il existe deux durées de vie : une durée de vie « temporelle » et une durée de vie « en fonction du volume de trafic ». L'association de sécurité expire lorsque la première de ces deux durées de vie est atteinte.
  - **Lifetime Duration** (Durée de vie) : le nombre de secondes pendant lesquelles une association de sécurité peut rester active avant d'expirer. La plage est comprise entre 120 et 214783647 secondes. La valeur globale par défaut est de 28 800 secondes (huit heures).
  - **Lifetime Size** (Taille de durée de vie) : le volume de trafic (en kilo-octets) qui peut passer entre les homologues à l'aide d'une association de sécurité donnée avant son expiration. La plage est de 10 à 2147483647 kilo-octets, ou le champ est vide. La valeur par défaut est de 4 608 000 kilo-octets.

Laissez le champ vide pour supprimer la limite basée sur la taille et utiliser uniquement la durée comme limite.

- **NAT Exempt**(exemption de NAT) : (basé sur les politiques uniquement) Indique s'il faut exempter le trafic VPN des politiques de NAT sur l'interface d'accès VPN locale. Si vous ne souhaitez pas que les règles NAT s'appliquent au réseau local, sélectionnez l'interface qui héberge le réseau local. Cette option ne fonctionne que si le réseau local se trouve derrière une interface de routage unique (et non un membre d'un groupe de ponts). Si le réseau local se trouve derrière plusieurs interfaces de routage ou un ou plusieurs membres de groupes de pont, vous devez créer manuellement les règles d'exemption NAT. Pour plus d'informations sur la création manuelle des règles requises, consultez Exemption du trafic VPN de site à site de la NAT, à la page 28.
- **Diffie-Hellman Group for Perfect Forward Secrecy** (Groupe Diffie-Hellman pour la confidentialité de transmission parfaite) : indique s'il faut utiliser la Confidentialité de transmission parfaite (PFS) pour générer et utiliser une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange du déchiffrement ultérieur, même si l'échange en entier a été enregistré et que l'agresseur a obtenu les clés prépartagées ou privées utilisées par les terminaux. Pour activer la Confidentialité de transmission parfaite, sélectionnez l'algorithme de dérivation de clé Diffie-Hellman à utiliser pour générer la clé de session PFS dans la liste Modulus Group (groupe de module). Si vous activez IKEv1 et IKEv2, les options sont limitées à celles qu'IKEv1 prend en charge. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 4.

Étape 6 Cliquez sur **Next** (suivant).

Étape 7 Passez en revue le résumé et cliquez sur **Finish** (Terminer).

Les renseignements récapitulatifs sont copiés dans le presse-papiers. Vous pouvez coller ces renseignements dans un document et les utiliser pour vous aider à configurer l'homologue distant ou les envoyer à la personne responsable de la configuration de cet homologue.

Vous devez effectuer des étapes supplémentaires pour autoriser le trafic dans le tunnel VPN, comme expliqué dans Autoriser le trafic via le VPN de site à site, à la page 16.

Après avoir déployé la configuration, connectez-vous à la console d'interface en ligne de commande du périphérique et utilisez la commande **show ipsec sa** pour vérifier que les points terminaux établissent une association de sécurité. Consultez Vérification des connexions VPN de site à site, à la page 25.

Configuration d'une interface de tunnel virtuel

Vous pouvez utiliser une Virtual Tunnel Interface (Interface de tunnel virtuel) (VTI) uniquement dans un profil de connexion VPN de site à site basé sur le routage. Une VTI est associée à une interface physique, par laquelle la connexion VPN est établie avec l'homologue distant. En utilisant une interface virtuelle, vous pouvez simplifier la connexion VPN site à site et contrôler le trafic à l'aide de routes statiques et dynamiques, plutôt que de préciser les réseaux locaux et distants du VPN dans le profil de connexion.

Procédure

Étape 1 Cliquez sur **Device**(Périphérique), cliquez sur le lien dans le résumé des **Interfaces**, puis cliquez sur Virtual Tunnel Interfaces (Interfaces de tunnel virtuel).

Étape 2 Effectuez l'une des actions suivantes :

- Cliquez sur + ou sur **Create Virtual Tunnel Interface (Créer une interface de tunnel virtuel)** pour créer une nouvelle interface.
- Cliquez sur l'icône de modification ( ) pour une interface existante.

Si vous n'avez plus besoin d'une interface, cliquez sur l'icône de suppression ( ) pour la supprimer. Vous devez d'abord supprimer tout profil de connexion site à site qui utilise l'interface, avant de pouvoir la supprimer.

Étape 3 Configurez les options suivantes :

- **Name** (Nom) : le nom de l'interface, jusqu'à 48 caractères. Si vous modifiez le nom d'une interface existante, il est automatiquement mis à jour dans toutes les politiques et tous les objets qui l'incluent. Vous ne pouvez pas utiliser de lettres majuscules dans le nom.
- **Status** (État) : cliquez sur le curseur pour le mettre en position Enabled (Activé) .
- **Description** : (facultatif.) La description peut contenir jusqu'à 200 caractères sur une seule ligne (sans retour chariot).
- **Tunnel ID** (ID du tunnel) : un nombre de 0 à 10 413. Ce numéro est ajouté au mot Tunnel pour former le nom matériel de l'interface. Vous devez choisir un numéro que vous n'avez pas déjà utilisé pour une autre VTI. Par exemple, saisissez 1 pour créer l'interface Tunnel1.
- **Tunnel Source** (Source du tunnel) : sélectionnez l'interface associée à cette VTI. La source du tunnel est l'interface par laquelle le VPN site à site défini sur l'interface de tunnel virtuel se connectera au point de terminaison distant. Sélectionnez une interface qui peut atteindre le point de terminaison distant, par exemple l'interface outside. L'interface source peut être une interface physique, une sous-interface ou un EtherChannel, et elle doit avoir un nom. L'interface ne peut pas être membre d'une interface virtuelle de pont (BVI).
- **IP Address and Subnet Mask (Adresse IP et masque de sous-réseau)** : l'adresse IPv4 et le masque de sous-réseau associé. Par exemple, 192.168.1.1/24 ou /255.255.255.0. Cette adresse n'a pas besoin d'être sur le même sous-réseau que l'adresse de l'interface source du tunnel. Toutefois, si vous configurez un VPN d'accès à distance (RA) sur l'interface source, l'adresse IP de la VTI ne peut pas se trouver dans le pool d'adresses configuré pour le VPN RA.

Étape 4 Cliquez sur **OK**.

Autoriser le trafic via le VPN de site à site

Vous pouvez utiliser l'une des techniques suivantes pour activer la circulation du trafic dans le tunnel VPN de site à site.

- Configurez la commande **sysopt connection permit-vpn**, qui exempte le trafic qui correspond à la connexion VPN de la politique de contrôle d'accès. La valeur par défaut pour cette commande est **no sysopt connection permit-vpn**, ce qui signifie que le trafic VPN doit également être autorisé par la politique de contrôle d'accès.

  Il s'agit de la méthode la plus sécurisée pour autoriser le trafic dans le VPN, car les utilisateurs externes ne peuvent pas falsifier des adresses IP dans le réseau protégé distant. L'inconvénient est que le trafic

VPN ne sera pas inspecté, ce qui signifie que la protection contre les intrusions et les fichiers, le filtrage des URL ou d'autres fonctions avancées ne seront pas appliqués au trafic. Cela signifie également qu'aucun événement de connexion ne sera généré pour le trafic, et donc les tableaux de bord statistiques ne refléteront pas les connexions VPN.

La méthode préférée pour configurer cette commande est de créer un profil de connexion VPN d'accès à distance dans lequel vous sélectionnez l'option **Bypass Access Control** (contournement du contrôle d'accès) pour le trafic déchiffré. Si vous ne souhaitez pas configurer le VPN d'accès à distance ou si vous ne pouvez pas configurer le VPN d'accès à distance, vous pouvez utiliser FlexConfig pour configurer la commande.

Remarque Cette méthode ne s'applique pas aux connexions VPN basées sur le routage configurées sur une Virtual Tunnel Interface (interface de tunnel virtuel) (VTI). Vous devez toujours configurer les règles de contrôle d'accès pour les VPN basés sur le routage.

- Créez des règles de contrôle d'accès pour autoriser les connexions à partir du réseau distant. Cette méthode garantit que le trafic VPN est inspecté et que des services avancés peuvent être appliqués aux connexions. L'inconvénient est que des utilisateurs externes ont alors la possibilité de falsifier les adresses IP et d'accéder ainsi à votre réseau interne.

Configuration de la politique IKE globale

L'Internet Key Exchange (IKE ou l'échange de clé Internet) est un protocole de gestion de clés utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec.

La négociation IKE comprend deux phases. La phase 1 négocie une association de sécurité entre deux homologues IKE, ce qui permet aux homologues de communiquer de manière sécurisée pendant la phase 2. Pendant la négociation de la phase 2, IKE établit les associations de sécurité pour d'autres applications, telles qu'IPsec. Les deux phases utilisent des propositions lorsqu'elles négocient une connexion. Une proposition IKE est un ensemble d'algorithmes que deux homologues utilisent pour sécuriser la négociation entre eux. La négociation IKE commence lorsque chaque homologue s'accorde sur une politique IKE commune (partagée). Cette politique énonce les paramètres de sécurité utilisés pour protéger les négociations IKE ultérieures.

Les objets de politique IKE définissent les propositions IKE pour ces négociations. Les objets que vous activez sont ceux utilisés lorsque les homologues négocient une connexion VPN : vous ne pouvez pas spécifier différentes politiques IKE par connexion. La priorité relative de chaque objet détermine quelles politiques sont essayées en premier, le nombre le plus bas correspondant à la priorité la plus élevée. La connexion n'est pas établie si la négociation ne parvient pas à trouver une politique que les deux homologues puissent prendre en charge.

Pour définir la politique IKE globale, vous sélectionnez les objets à activer pour chaque version IKE. Si les objets prédéfinis ne satisfont pas vos exigences, créez de nouvelles politiques pour appliquer votre politique de sécurité.

La procédure suivante explique comment configurer la politique globale à l'aide de la page Objets. Vous pouvez également activer, désactiver et créer des politiques lors de la modification d'une connexion VPN en cliquant sur **Edit** (Modifier) dans les paramètres de politique IKE.

Remarque Vous pouvez activer jusqu'à 20 politiques IKE.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **IKE Policies** (Politiques IKE) dans la table des matières.

Les politiques pour IKEv1 et IKEv2 sont affichées dans des listes distinctes.

Étape 2 Activez les politiques IKE que vous souhaitez autoriser pour chaque version IKE.

a) Sélectionnez **IKEv1** ou **IKEv2** au-dessus de la table d'objets pour afficher les politiques de cette version.

b) Cliquez sur la bascule **State** (État) pour activer les objets appropriés et désactiver ceux qui ne répondent pas à vos besoins.

Si certaines de vos exigences de sécurité ne sont pas reflétées dans les objets existants, définissez-en de nouveaux pour les mettre en œuvre. Pour plus de détails, consultez les rubriques suivantes :

- Configuration des politiques IKEv1, à la page 18
- Configuration des politiques IKEv2, à la page 20

c) Vérifiez que les priorités relatives correspondent à vos besoins.

Si vous devez modifier la priorité d'une politique, modifiez-la. S'il s'agit d'une politique système prédéfinie, vous devez créer votre propre version de la politique pour modifier la priorité.

La priorité est relative et non absolue. Par exemple, la priorité 80 est supérieure à 160. Si 80 est l'objet ayant la priorité la plus élevée que vous activez, cela devient votre politique de premier choix. Si vous activez ensuite une politique de priorité 25, elle devient votre politique de premier choix.

d) Si vous utilisez les deux versions IKE, répétez le processus pour l'autre version.

Configuration des politiques IKEv1

Les objets de politique Internet Key Exchange (IKE), version 1 contiennent les paramètres requis pour les politiques IKEv1 lors de la définition des connexions VPN. IKE est un protocole de gestion de clés qui facilite la gestion des communications basées sur IPsec. Il est utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec (SA).

Il existe plusieurs politiques IKEv1 prédéfinies. Si certaines répondent à vos besoins, activez-les simplement en cliquant sur le bouton à bascule **State** (État). Vous pouvez également créer des politiques pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de politique IKEv1 lors de la modification des paramètres IKEv1 dans une connexion VPN en cliquant sur le lien **Create New IKE Policy** (Créer une nouvelle politique IKE) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **IKE Policies** (Politiques IKE) dans la table des matières.

Étape 2 Sélectionnez **IKEv1** au-dessus de la table d'objets pour afficher les politiques IKEv1.

Étape 3 Si l'une des politiques définies par le système répond à vos besoins, cliquez sur la bascule **State** (État) pour les activer.

Utilisez également la bascule **State** (État) pour désactiver les politiques indésirables. La priorité relative de chaque objet détermine lesquelles de ces politiques sont essayées en premier, le nombre le plus bas étant une priorité la plus élevée.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 5 Configurez les propriétés IKEv1.

- **Priority**(Priorité) : Priorité : priorité relative de la politique IKE, de 1 à 65 535. La priorité détermine l'ordre de la politique IKE par rapport aux deux homologues négociateurs lors de la tentative de trouver une association de sécurité (SA) commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de priorité la plus élevée, il essaie d'utiliser les paramètres définis dans la prochaine priorité la plus basse. Plus le numéro de priorité est faible, plus la priorité est élevée.
- **Name** (Nom) : Le nom de l'objet, jusqu'à 128 caractères.
- **State**(État) : État : indique si la politique IKE est activée ou désactivée. Cliquez sur le bouton à bascule pour modifier l'état. Seules les politiques activées sont utilisées pendant les négociations IKE.
- **Authentification** : la méthode d'authentification à utiliser entre les deux homologues. Pour obtenir plus de renseignements, consultez Choix de la méthode d'authentification à utiliser, à la page 5.
  - **Clé prépartagée** : utilisez la clé prépartagée définie sur chaque périphérique. Ces clés permettent de partager une clé secrète entre deux homologues et d'être utilisée par IKE pendant la phase d'authentification. Si l'homologue n'est pas configuré avec la même clé prépartagée, le SA IKE ne peut pas être établi.
  - **Certificat)** : utilisez les certificats d'identité d'appareil pour les homologues pour s'identifier. Vous devez obtenir ces certificats en inscrivant chaque homologue dans une autorité de certification. Vous devez également télécharger la racine de l'autorité de certification et les certificats intermédiaires de l'autorité de certification de confiance utilisés pour signer les certificats d'identité chez chaque homologue. Les homologues peuvent être inscrits dans la même autorité de certification ou dans une autre autorité de certification. Vous ne pouvez pas utiliser de certificats autosignés pour l'un ou l'autre des homologues.
- **Chiffrement** : l'algorithme de chiffrement utilisé pour établir l'association de sécurité (SA) de phase 1 en vue de protéger les négociations de la phase 2. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 3.

- **Groupe Diffie-Hellman** : le groupe Diffie-Hellman à utiliser pour obtenir un secret partagé entre les deux homologues IPsec sans le transmettre l'un à l'autre.. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 4.
- **Hachage** : l'algorithme de hachage pour créer un condensé de message, qui est utilisé pour assurer l'intégrité du message. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 4.
- **Lifetime** (Durée de vie) :Durée de vie : la durée de vie de l'association de sécurité (SA), en secondes, de 120 à 2 147 483 647 ou vide. Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En règle générale, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE seront sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes. La valeur par défaut est 86 400. Pour spécifier une durée de vie illimitée, ne saisissez aucune valeur (laissez le champ vide).

Étape 6 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des politiques IKEv2

Les objets de politique Internet Key Exchange (IKE) version 2 contiennent les paramètres requis pour les politiques IKEv2 lors de la définition des connexions VPN. IKE est un protocole de gestion de clés qui facilite la gestion des communications basées sur IPsec. Il est utilisé pour authentifier les pairs IPsec, négocier et distribuer les clés de chiffrement IPsec et établir automatiquement des associations de sécurité IPsec (SA).

Il existe plusieurs politiques IKEv2 prédéfinies. Si certaines répondent à vos besoins, activez-les simplement en cliquant sur le bouton à bascule **State** (État). Vous pouvez également créer des politiques pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer une politique IKEv2 lors de la modification des paramètres IKE dans une connexion VPN de site à site en cliquant sur le lien **Create New IKEv2 Policy** (Créer une nouvelle politique IKEv2) affiché dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects (objets)**, puis sélectionnez **Politiques IKE** dans la table des matières.

Étape 2 Sélectionnez **IKEv2** au-dessus de la table d'objets pour afficher les politiques IKEv2.

Étape 3 Si l'une des politiques définies par le système répond à vos besoins, cliquez sur la bascule **State** (État) pour les activer.

Utilisez également la bascule **State** (État) pour désactiver les politiques indésirables. La priorité relative de chaque objet détermine lesquelles de ces politiques sont essayées en premier, le nombre le plus bas étant une priorité la plus élevée.

Étape 4 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification () de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille () de l'objet.

Étape 5 Configurez les propriétés IKEv2.

- **Priority**(Priorité) : Priorité : priorité relative de la politique IKE, de 1 à 65 535. La priorité détermine l'ordre de la politique IKE par rapport aux deux homologues négociateurs lors de la tentative de trouver une association de sécurité (SA) commune. Si l'homologue IPsec distant ne prend pas en charge les paramètres sélectionnés dans votre politique de priorité la plus élevée, il essaie d'utiliser les paramètres définis dans la prochaine priorité la plus basse. Plus le numéro de priorité est faible, plus la priorité est élevée.
- **Name** (Nom) : Le nom de l'objet, jusqu'à 128 caractères.
- **State**(État) : État : indique si la politique IKE est activée ou désactivée. Cliquez sur le bouton à bascule pour modifier l'état. Seules les politiques activées sont utilisées pendant les négociations IKE.
- **Chiffrement** : l'algorithme de chiffrement utilisé pour établir l'association de sécurité (SA) de phase 1 en vue de protéger les négociations de la phase 2. Sélectionnez tous les algorithmes que vous souhaitez autoriser, bien que vous ne puissiez pas inclure les options de mode mixte (AES-GCM) et de mode normal dans la même politique. (Le mode normal exige que vous sélectionniez un hachage d'intégrité, tandis que le mode mixte interdit une sélection de hachage d'intégrité distincte.) Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 3.
- **Groupe Diffie-Hellman** : le groupe Diffie-Hellman à utiliser pour obtenir un secret partagé entre les deux homologues IPsec sans le transmettre l'un à l'autre.. Un module plus élevé offre une sécurité supérieure, mais nécessite plus de temps de traitement. Les deux homologues doivent avoir un groupe de module correspondant. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par le groupe le plus fort vers le plus faible jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Choix du groupe de module Diffie-Hellman à utiliser, à la page 4.
- **Integrity Hash** (hachage d'intégrité) : la partie intégrité de l'algorithme de hachage pour la création d'un condensé de message, qui est utilisée pour assurer l'intégrité du message. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Le hachage d'intégrité n'est pas utilisé avec les options de chiffrement AES-GCM. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 4.
- **Pseudo-Random Function (PRF) Hash** (hachage de la fonction pseudo-aléatoire (PRF)) : la partie fonction pseudo-aléatoire (PRF) de l'algorithme de hachage, qui est utilisée comme algorithme pour dériver le matériel de clé et les opérations de hachage requises pour le chiffrement du tunnel IKEv2. Dans IKEv1, les algorithmes d'intégrité et de PRF ne sont pas séparés, mais dans IKEv2, vous pouvez spécifier des algorithmes différents pour ces éléments. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 4.

- **Lifetime** (Durée de vie) :Durée de vie : la durée de vie de l'association de sécurité (SA), en secondes, de 120 à 2 147 483 647 ou vide. Lorsque la durée de vie est dépassée, l'association de sécurité expire et doit être renégociée entre les deux homologues. En règle générale, plus la durée de vie est courte (jusqu'à un certain point), plus vos négociations IKE seront sécurisées. Cependant, avec des durées de vie plus longues, les futures associations de sécurité IPsec peuvent être configurées plus rapidement qu'avec des durées de vie plus courtes. La valeur par défaut est 86 400. Pour spécifier une durée de vie illimitée, ne saisissez aucune valeur (laissez le champ vide).

Étape 6 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des propositions IPsec

IPsec est l'une des méthodes les plus sécurisées de configuration d'un VPN. La fonctionnalité IPsec de Cisco IOS fournit le chiffrement de données réseau au niveau des paquets IP et offre une solution de sécurité robuste basée sur des normes. Grâce à IPsec, les données sont transmises sur un réseau public par l'intermédiaire de tunnels. Un tunnel est un chemin de communication logique et sécurisé entre deux homologues. Le trafic qui entre dans un tunnel IPsec est sécurisé par une combinaison d'algorithmes et de protocoles de sécurité appelée ensemble de transformations. Pendant la négociation d'association de sécurité (SA) d'IPsec, les homologues recherchent un ensemble de transformations identique sur les deux homologues.

Il existe des objets de proposition IPsec distincts selon la version IKE, IKEv1 ou IKEv2 :

- Lorsque vous créez une proposition IKEv1, vous sélectionnez le mode de fonctionnement d'IPsec et définissez les types de chiffrement et d'authentification requis. Vous pouvez sélectionner une seule option pour les algorithmes. Si vous souhaitez prendre en charge plusieurs combinaisons dans un VPN, créez et sélectionnez plusieurs objets Proposition IKEv1 IPsec.
- Lorsque vous créez une proposition IKEv2 IPsec, vous pouvez sélectionner tous les algorithmes de chiffrement et de hachage autorisés dans un VPN. Le système classe les paramètres du plus sécurisé au moins sécurisé et négocie avec l'homologue jusqu'à ce qu'une correspondance soit trouvée. Cela vous permet d'envoyer potentiellement une seule proposition pour transmettre toutes les combinaisons autorisées au lieu d'avoir besoin d'envoyer chaque combinaison autorisée individuellement, comme avec IKEv1.

Le protocole ESP (Encapsulating Security Protocol) est utilisé pour les propositions d'IPsec IKEv1 et IKEv2. Il fournit des services d'authentification, de chiffrement et d'antirelecture. ESP est un protocole IP de type 50.

Remarque Nous vous recommandons d'utiliser à la fois le chiffrement et l'authentification sur les tunnels IPsec.

Les rubriques suivantes expliquent comment configurer les propositions IPsec pour chaque version d'IKE :

Configuration des propositions IPsec pour IKEv1

Utilisez les objets IKEv1 IPsec Proposal (proposition IPsec IKEv1) pour configurer la proposition IPsec utilisée lors des négociations de la phase 2 d'IKE. La proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec.

Il existe plusieurs propositions IKEv1 IPsec prédéfinies. Vous pouvez également créer de nouvelles propositions pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets IKEv1 IPsec Proposals (propositions IKEv1 IPsec) tout en modifiant les paramètres IKEv1 IPsec dans une connexion VPN, en cliquant sur le lien **Create New IPsec Proposal** (Créer une nouvelle proposition IPsec) affiché dans la liste des objets.

Procédure

Étape 1 Sélectionnez **Objects** (Objets), puis sélectionnez **IPsec Proposals** (propositions IPsec) dans la table des matières.

Étape 2 Sélectionnez **IKEv1** au-dessus de la table des objets pour afficher les propositions IKEv1 IPsec.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Configurez les propriétés de la proposition IPsec IKEv1.

- **Name (Nom)**—Le nom de l'objet, jusqu'à 128 caractères.
- **Mode** : le mode dans lequel fonctionne le tunnel IPSec.
  - Le mode **Tunnel** encapsule l'ensemble du paquet IP. L'en-tête IPSec est ajouté entre l'en-tête IP d'origine et le nouvel en-tête IP. Il s'agit du paramètre par défaut. Utilisez le mode tunnel lorsque le pare-feu protège le trafic vers et en provenance des hôtes situés derrière le pare-feu. Le mode tunnel est la façon dont le protocole IPSec standard est mis en œuvre entre deux pare-feu (ou autres passerelles de sécurité) qui sont connectés sur un réseau non fiable, comme Internet.
  - Le mode **Transport** encapsule uniquement les protocoles des couches supérieures d'un paquet IP. L'en-tête IPSec est inséré entre l'en-tête IP et l'en-tête de protocole de la couche supérieure (comme TCP). Le mode de transport nécessite que les hôtes source et de destination prennent en charge IPSec et ne peut être utilisé que lorsque l'homologue de destination du tunnel est la destination finale du paquet IP. Le mode de transport est généralement utilisé uniquement pour la protection d'un protocole de tunnellisation de couche 2 ou de couche 3 comme GRE, L2TP et DLSW.
- **ESP Encryption** (Chiffrement ESP) : algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 3.
- **ESP Hash (Hachage ESP)** : algorithme de hachage ou d'intégrité à utiliser pour l'authentification. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 4.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Configuration des propositions IPsec pour IKEv2

Les objets Proposition IPsec IKEv2 configurent la proposition IPsec utilisée lors des négociations de la phase 2 d'IKE. La proposition IPsec définit la combinaison de protocoles et d'algorithmes de sécurité qui sécurisent le trafic dans un tunnel IPsec.

Il existe plusieurs propositions IKEv2 IPsec prédéfinies. Vous pouvez également créer de nouvelles propositions pour mettre en œuvre d'autres combinaisons de paramètres de sécurité. Vous ne pouvez pas modifier ou supprimer des objets définis par le système.

La procédure suivante explique comment créer et modifier des objets directement à partir de la page des objets (Objects). Vous pouvez également créer des objets de propositions IKEv2 IPsec tout en modifiant les paramètres IKEv2 IPsec dans une connexion VPN en cliquant sur le lien **Créer une nouvelle proposition IPsec** dans la liste d'objets.

Procédure

Étape 1 Sélectionnez **Objects** (objets), puis **IPsec Proposals** (propositions IPsec) dans la table des matières.

Étape 2 Sélectionnez **IKEv2** au-dessus de la table des objets pour afficher les propositions IPsec IKEv2.

Étape 3 Effectuez l'une des opérations suivantes :

- Pour créer un objet, cliquez sur le bouton +.
- Pour modifier un objet, cliquez sur l'icône de modification ( ) de l'objet.

Pour supprimer un objet non référencé, cliquez sur l'icône de la corbeille ( ) de l'objet.

Étape 4 Configurez les propriétés de la proposition IPsec IKEv2.

- **Nom**—Le nom de l'objet, jusqu'à 128 caractères.
- **Chiffrement** : l'algorithme de chiffrement Encapsulating Security Protocol (ESP) pour cette proposition. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Choix de l'algorithme de chiffrement à utiliser, à la page 3.
- **Hachage d'intégrité** : l'algorithme de hachage ou d'intégrité à utiliser pour l'authentification. Sélectionnez tous les algorithmes que vous souhaitez autoriser. Le système négocie avec l'homologue, en commençant par l'algorithme le plus fort vers l'algorithme le plus faible, jusqu'à ce qu'une correspondance soit trouvée. Pour obtenir une explication des options, consultez Décider des algorithmes de hachage à utiliser, à la page 4.

  Remarque
  Cependant, vous devez choisir l'algorithme d'intégrité nulle si vous sélectionnez l'une des options AES-GCM/GMAC comme algorithme de chiffrement. Même si vous choisissez une option non nulle, le hachage d'intégrité est ignoré pour ces normes de chiffrement.

Étape 5 Cliquez sur **OK** pour enregistrer les modifications.

Vérification des connexions VPN de site à site

Après avoir configuré une connexion VPN de site à site et déployé la configuration sur le périphérique, vérifiez que le système établit l'association de sécurité avec le périphérique distant.

Si la connexion ne peut pas être établie, utilisez la commande **ping interface** *interface_name remote_ip_address* de l'interface de ligne de commande du périphérique pour vous assurer qu'il existe un chemin dans l'interface VPN vers le périphérique distant. S'il n'y a aucune connexion par l'intermédiaire de l'interface configurée, vous pouvez ignorer le mot-clé **interface** *interface_name* et déterminer si la connectivité se fait par l'intermédiaire d'une interface différente. Vous avez peut-être sélectionné la mauvaise interface pour la connexion : vous devez sélectionner l'interface qui fait face au périphérique distant, et non l'interface qui fait face au réseau protégé.

S'il existe un chemin réseau, vérifiez les versions et les clés IKE configurées et prises en charge par les deux points terminaux, et ajustez la connexion VPN au besoin. Assurez-vous qu'aucune règle de contrôle d'accès ou de NAT ne bloque la connexion.

Procédure

Étape 1 Connectez-vous à l'interface de ligne de commande du périphérique comme expliqué dans Connexion avec l'interface de ligne de commande (CLI).

Étape 2 Utilisez la commande **show ipsec sa** pour vérifier que l'association de sécurité IPsec est établie.

Vous devriez voir que la connexion VPN est établie entre votre périphérique (l'**adresse locale**) et l'homologue distant (**current_peer**). Le nombre de paquets (pkts) devrait augmenter à mesure que vous envoyez du trafic par la connexion. La liste d'accès doit afficher les réseaux locaux et distants pour la connexion.

Par exemple, la sortie suivante montre une connexion IKEv2.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 69, #pkts encrypt: 69, #pkts digest: 69
      #pkts decaps: 69, #pkts decrypt: 69, #pkts verify: 69
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 69, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/500, remote crypto endpt.: 192.168.4.6/500
      path mtu 1500, ipsec overhead 55(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: CD22739C
      current inbound spi : 52D2F1E4
```

```
    inbound esp sas:
      spi: 0x52D2F1E4 (1389556196)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4285434/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xCD22739C (3441587100)
         SA State: active
         transform: esp-aes-gcm-256 esp-null-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 19, IKEv2, }
         slot: 0, conn_id: 62738432, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (4055034/28730)
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

La sortie suivante montre une connexion IKEv1.

```
> show ipsec sa
interface: site-a-outside
    Crypto map tag: s2sCryptoMap, seq num: 1, local addr: 192.168.2.15

      access-list |s2sAcl|0730e31c-1e5f-11e7-899f-27f6e1030344
extended permit ip 192.168.1.0 255.255.255.0 192.168.3.0 255.255.255.0
      local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
      current_peer: 192.168.4.6


      #pkts encaps: 10, #pkts encrypt: 10, #pkts digest: 10
      #pkts decaps: 10, #pkts decrypt: 10, #pkts verify: 10
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 10, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 192.168.2.15/0, remote crypto endpt.: 192.168.4.6/0
      path mtu 1500, ipsec overhead 74(44), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 077D72C9
      current inbound spi : AC146DEC

    inbound esp sas:
      spi: 0xAC146DEC (2887020012)
         SA State: active
         transform: esp-aes-256 esp-sha-hmac no compression
         in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
         slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
         sa timing: remaining key lifetime (kB/sec): (3914999/28567)
         IV size: 16 bytes
         replay detection support: Y
```

```
        Anti replay bitmap:
         0x00000000 0x000007FF
    outbound esp sas:
      spi: 0x077D72C9 (125661897)
        SA State: active
        transform: esp-aes-256 esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, PFS Group 5, IKEv1, }
        slot: 0, conn_id: 143065088, crypto-map: s2sCryptoMap
        sa timing: remaining key lifetime (kB/sec): (3914999/28567)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Étape 3 Utilisez la commande **show isakmp sa** pour vérifier les associations de sécurité IKE.

Vous pouvez utiliser la commande sans le mot-clé **sa** (ou utiliser le mot-clé **stats** à la place) pour afficher les statistiques IKE.

Par exemple, la sortie suivante affiche une association de sécurité IKEv2.

```
> show isakmp sa

There are no IKEv1 SAs

IKEv2 SAs:

Session-id:15317, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local             Remote            Status   Role
592216161 192.168.2.15/500  192.168.4.6/500   READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:21, Auth sign: PSK, Auth verify: PSK
      Life/Active Time: 86400/12 sec
Child sa: local selector  192.168.1.0/0 - 192.168.1.255/65535
          remote selector 192.168.3.0/0 - 192.168.3.255/65535
          ESP spi in/out: 0x52d2f1e4/0xcd22739c
```

Le résultat suivant montre une association de sécurité IKEv1.

```
> show isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 192.168.4.6
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
```

Supervision du VPN de site à site

Pour superviser et dépanner les connexions VPN de site à site, ouvrez la console d'interface en ligne de commande ou connectez-vous à l'interface de ligne de commande du périphérique et utilisez les commandes suivantes.

- **show ipsec sa** affiche les sessions VPN (associations de sécurité). Vous pouvez réinitialiser ces statistiques à l'aide de la commande **clear ipsec sa counters**.
- **show ipsec** *keyword* affiche les données et les statistiques opérationnelles IPsec. Saisissez **show ipsec ?** pour afficher les mots-clés disponibles.
- **show isakmp** affiche les données et les statistiques opérationnelles d'ISAKMP.

Exemples de VPN de site à site

Voici des exemples de configuration d'un VPN de site à site.

Exemption du trafic VPN de site à site de la NAT

Lorsque vous avez une connexion VPN de site à site définie sur une interface, et que vous avez également des règles NAT pour cette interface, vous pouvez éventuellement exempter le trafic sur le VPN des règles NAT. Vous souhaiterez peut-être le faire si l'extrémité distante de la connexion VPN peut gérer vos adresses internes.

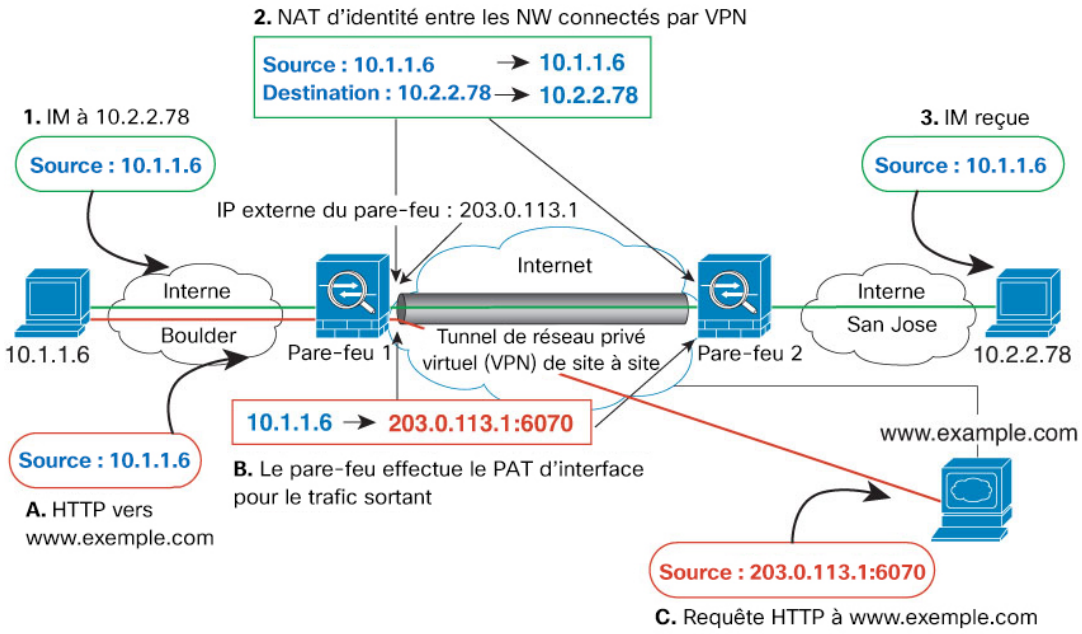
Lorsque vous créez la connexion VPN, vous pouvez sélectionner l'option d'**exemption de NAT** pour créer les règles automatiquement. Cependant, cela ne fonctionne que si votre réseau local protégé est connecté par l'intermédiaire d'une interface à routage unique (et non un membre d'un groupe de ponts). Si, au contraire, les réseaux locaux de la connexion se trouvent derrière au moins deux interfaces de routage ou un ou plusieurs membres de groupes de ponts, vous devez configurer manuellement les règles d'exemption NAT.

Pour exempter le trafic VPN des règles NAT, vous créez une règle NAT manuelle d'identité pour le trafic local lorsque la destination est le réseau distant. Ensuite, appliquez la NAT au trafic lorsque la destination est autre chose (par exemple, Internet). Si vous avez plusieurs interfaces pour le réseau local, créez des règles pour chaque interface. Tenez également compte des suggestions suivantes :

- S'il y a plusieurs réseaux locaux dans la connexion, créez un groupe d'objets réseau pour contenir les objets qui définissent les réseaux.
- Si vous incluez à la fois des réseaux IPv4 et IPv6 dans le VPN, créez des règles NAT d'identité distinctes pour chacun.

Considérez l'exemple suivant, qui montre un tunnel de site à site connectant les bureaux de Bouder et de San José. Pour le trafic que vous souhaitez diriger vers Internet (par exemple, de la section 10.1.1.6 à Boulder vers www.exemple.com), vous avez besoin d'une adresse IP publique fournie par la NAT pour accéder à Internet. L'exemple ci-dessous utilise les règles PAT d'interface. Cependant, pour le trafic que vous souhaitez acheminer par le tunnel VPN (par exemple, de la version 10.1.1.6 à Boulder au 10.2.2.78 à San Jose), vous ne souhaitez pas effectuer la NAT; vous devez exclure ce trafic en créant une règle NAT d'identité. La NAT d'identité traduit simplement une adresse en la même adresse.

Illustration 1 : PAT d'interface et NAT d'identité pour le VPN de site à site



L'exemple suivant explique la configuration de Firewall1 (Boulder). Cet exemple suppose que l'interface interne est un groupe de ponts. Vous devez donc écrire les règles pour chaque interface membre. Le processus est le même si vous avez une ou plusieurs interfaces internes routées.

Remarque Cet exemple suppose qu'il s'agit d'un protocole IPv4 uniquement. Si le VPN comprend également des réseaux IPv6, créez des règles parallèles pour IPv6. Notez que vous ne pouvez pas implémenter l'interface PAT pour IPv6, vous devez donc créer un objet hôte avec une adresse IPv6 unique à utiliser pour la PAT.

Procédure

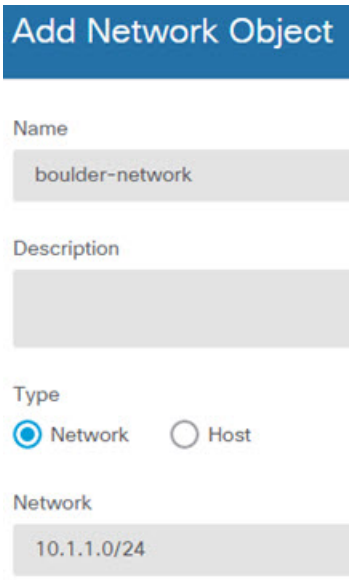
Étape 1 Créez les objets pour définir les différents réseaux.

a) Choisissez **Objects** (Objets).

b) Sélectionnez **Network** (Réseau) dans la table des matières et cliquez sur +.

c) Repérez le réseau interne Boulder.

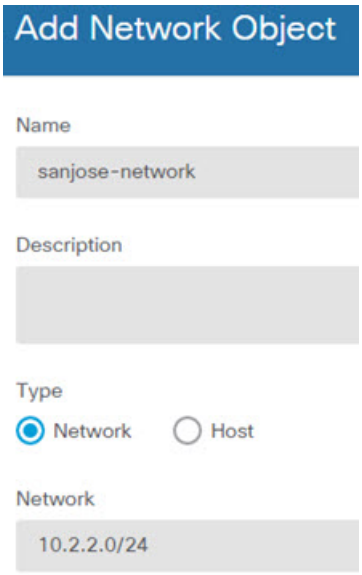
Nommez l'objet réseau (par exemple, boulder-network), sélectionnez **Network** (Réseau) et saisissez l'adresse réseau, 10.1.1.0/24.



d) Cliquez sur **OK**.

e) Cliquez sur + et définissez le réseau interne de San Jose.

Nommez l'objet réseau (par exemple, sanjose-network), sélectionnez **Network** (Réseau), et saisissez l'adresse réseau 10.2.2.0/24.



f) Cliquez sur **OK**.

Étape 2 Configurer la NAT d'identité manuelle pour le réseau Boulder lorsqu'il passe par le VPN vers San Jose sur le Firewall1 (Boulder).

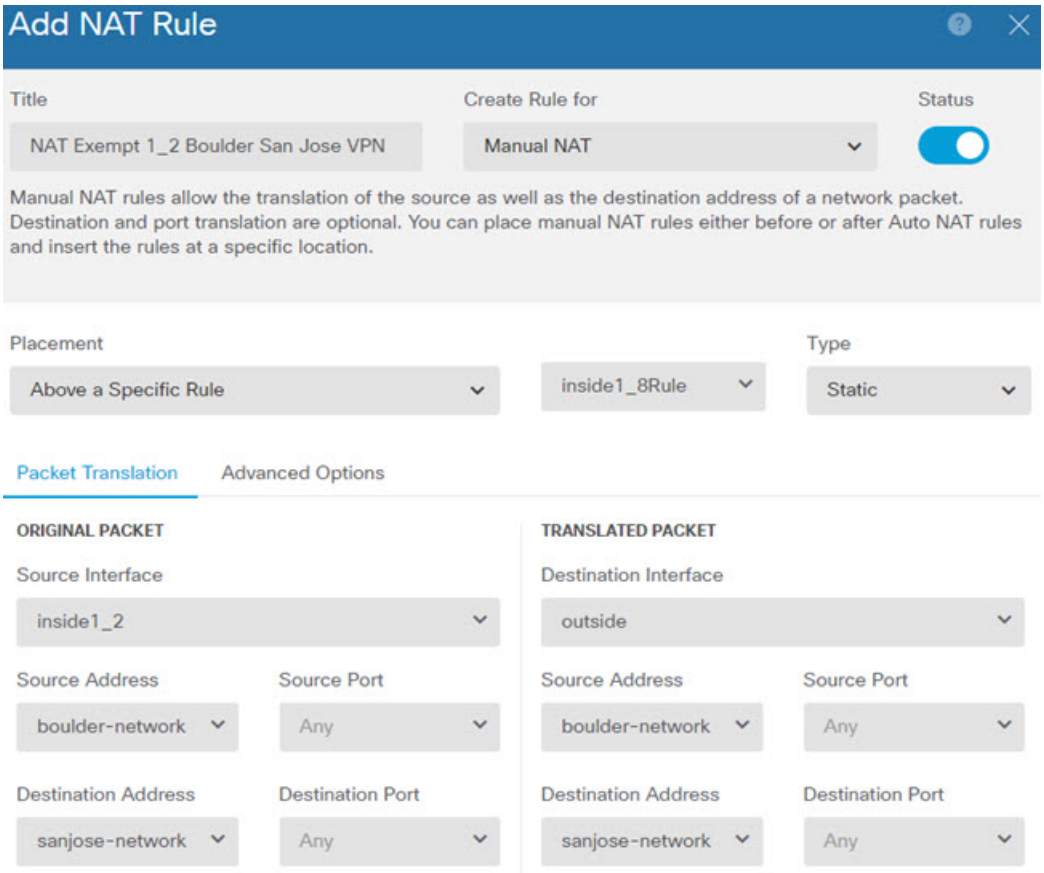
a) Sélectionnez **Policies (Politiques)** > **NAT**.

b) Cliquez sur le bouton +.

c) Configurez les propriétés suivantes :

- **Titre** = NAT Exempt 1_2 Boulder San Jose VPN (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Placement** (Emplacement) = **Above a Specific Rule** (Au-dessus d'une règle spécifique), et sélectionnez la première règle dans la section NAT manuelle avant NAT automatique. Vous voulez vous assurer que cette règle précède toutes les règles PAT d'interface générales pour l'interface de destination. Sinon, la règle pourrait ne pas être appliquée au bon trafic.
- **Type** = Statique.
- **Interface source** = inside1_2.
- **Interface de destination** = externe.
- **Adresse source d'origine** = objet boulder-network.
- **Adresse source traduite** = objet boulder-network.
- **Adresse de destination d'origine** = objet sanjose-network.
- **Adresse de destination traduite** = objet sanjose-network.

Remarque
Comme vous ne souhaitez pas traduire l'adresse de destination, vous devez configurer la NAT d'identité en utilisant la même adresse pour les adresses de destination originale et traduite. Laissez tous les champs de port vides. Cette règle configure la NAT d'identité pour la source et la destination.



d) Dans l'onglet **Advanced** (Avancé), sélectionnez **Do not proxy ARP on Destination interface** (Désactiver le mandataire ARP sur l'interface de destination).
e) Cliquez sur **OK**.
f) Répétez le processus pour créer des règles équivalentes pour chacune des autres interfaces internes.

Étape 3 Configurez manuellement l'interface dynamique PAT lors de la connexion à Internet pour le réseau interne Boulder sur Firewall1 (Boulder).

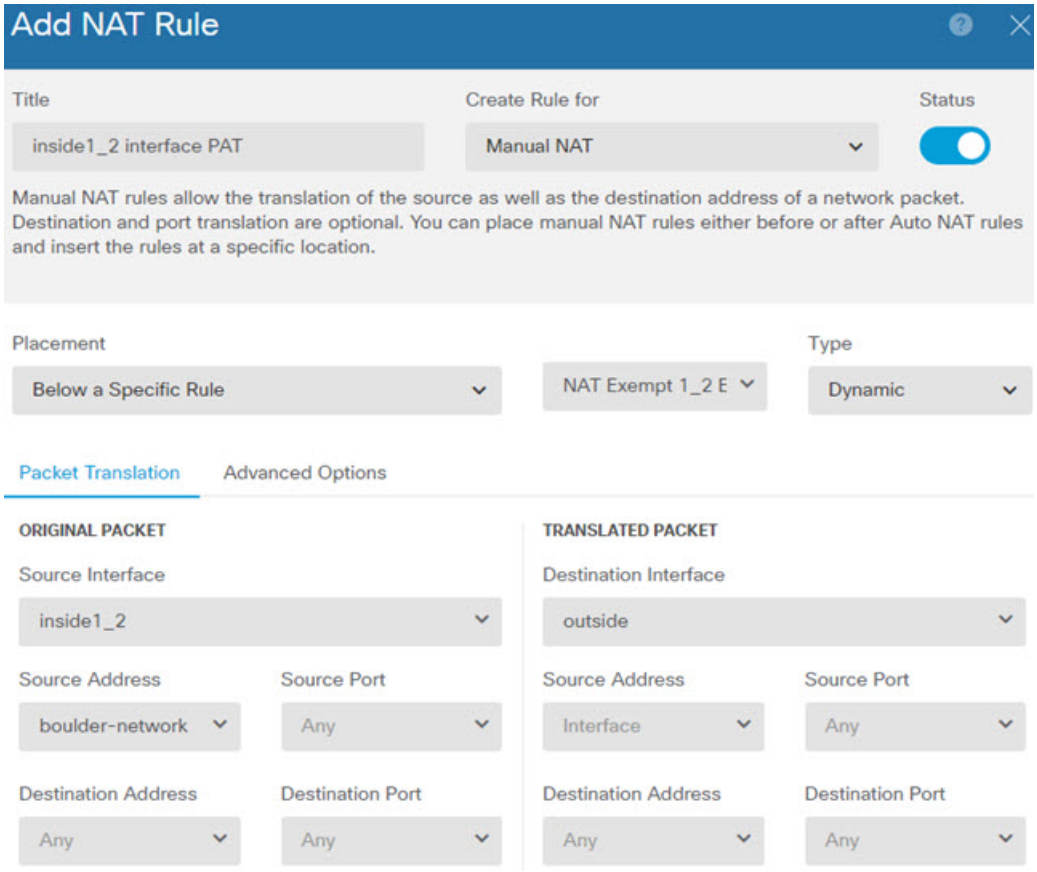
Remarque
Remarque : Il existe peut-être déjà des règles PAT d'interface dynamique pour les interfaces internes, couvrant tout trafic IPv4, car celles-ci sont créées par défaut lors de la configuration initiale. Cependant, la configuration est affichée ici par souci d'exhaustivité. Avant de suivre ces étapes, vérifiez si une règle existe déjà qui couvre l'interface interne et le réseau, et ignorez cette étape si c'est le cas.

a) Cliquez sur le bouton +.
b) Configurez les propriétés suivantes :

- **Title** (Titre) = interface PAT inside1_2 (ou un autre nom de votre choix).
- **Create Rule For** (créer une règle pour) = Manual NAT (NAT manuelle).
- **Placement** (Emplacement) = **Below a Specific Rule** (Ci-dessous une règle spécifique), et sélectionnez la première règle dans la section NAT manuelle avant NAT automatique. Étant donné que cette règle s'applique à toute adresse de destination, la règle qui utilise sanjose-network comme destination doit précéder cette règle, sinon la règle sanjose-network ne sera jamais mise en correspondance. La

procédure par défaut est de placer les nouvelles règles NAT manuelles à la fin de la section « NAT Rules Before Auto NAT ».

- **Type** = Dynamique.
- **Interface source** = inside1_2.
- **Interface de destination** = externe.
- **Adresse source d'origine** = objet boulder-network.
- **Adresse source traduite** = **Interface**. Cette option configure l'interface PAT à l'aide de l'interface de destination.
- **Adresse de destination d'origine** = n'importe laquelle.
- **Adresse de destination traduite** = n'importe laquelle.



c) Cliquez sur **OK**.

d) Répétez le processus pour créer des règles équivalentes pour chacune des autres interfaces internes.

Étape 4 Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement.

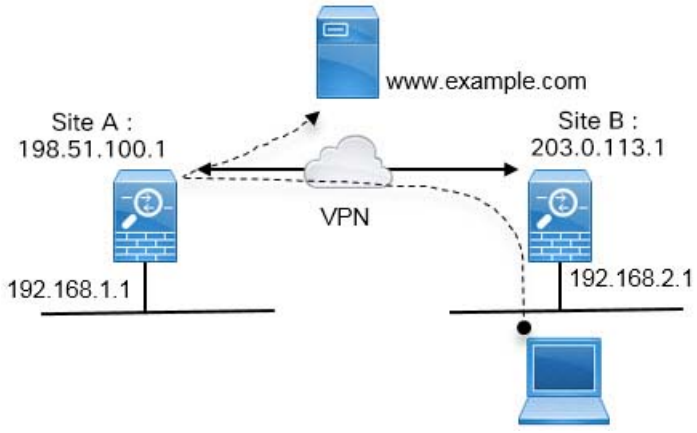
Étape 5 Si vous gérez également Firewall2 (San Jose), vous pouvez configurer des règles similaires pour ce périphérique.

- La règle de la NAT d'identité manuelle serait pour sanjose-network lorsque la destination est boulder-network. Créez de nouveaux objets d'interface pour Firewall2 , à l'intérieur et à l'extérieur des réseaux.
- La règle PAT de l'interface dynamique manuelle serait pour sanjose-network lorsque la destination est « any » (Toute).

Comment fournir un accès Internet sur l'interface externe pour les utilisateurs d'un VPN site à site externe (hairpinning)

Dans un VPN de site à site, vous pouvez souhaiter que les utilisateurs des réseaux distants accèdent à Internet par l'intermédiaire de votre périphérique. Cependant, comme les utilisateurs distants accèdent à votre périphérique sur la même interface qui fait face à Internet (l'interface externe), vous devez faire revenir le trafic Internet directement sur l'interface externe. Cette technique est appelée hairpinning.

Le graphique suivant présente un exemple. Il existe un tunnel VPN de site à site configuré entre 198.51.100.1 (sur le site principal, site A) et 203.0.113.1 (site distant, site B). Tout le trafic d'utilisateur à partir du réseau interne du site distant, 192.168.2.0/24, passe par le VPN. Ainsi, lorsqu'un utilisateur de ce réseau souhaite accéder à un serveur sur Internet, tel que www.exemple.com, la connexion passe d'abord par le VPN, puis est acheminée vers l'Internet à partir de l'interface 198.51.100.1.



La procédure suivante explique comment configurer ce service. Vous devez configurer les deux points terminaux du tunnel VPN.

Avant de commencer

Cette procédure suppose que vous utilisiez le paramètre par défaut pour autoriser le trafic VPN, ce qui applique le trafic VPN à la stratégie de contrôle d'accès. Dans la configuration en cours, cela est représenté par la commande **no sysopt connection permit-vpn**. Si vous avez plutôt activé **sysopt connection permit-vpn** par le**biais de FlexConfig ou en sélectionnant l'option de politique de contournement du contrôle d'accès pour le trafic déchiffré** dans les profils de connexion VPN d'accès à distance, les étapes de configuration des règles de contrôle d'accès ne sont pas nécessaires.

Procédure

Étape 1 (Site A, site principal.) Configurez la connexion VPN de site à site vers le site distant B.

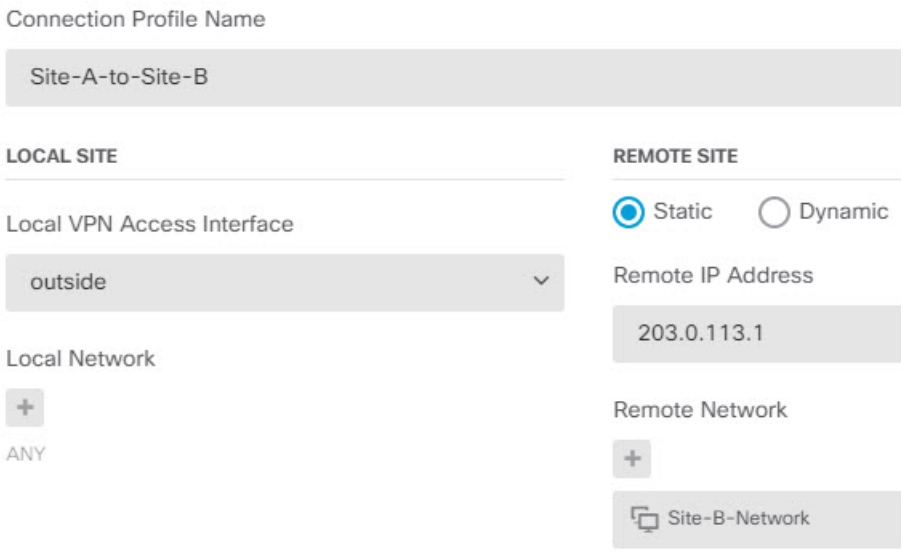
a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe Connexion VPN de site à site.

b) Cliquez sur + pour ajouter une nouvelle connexion.

c) Définissez les points terminaux comme suit, puis cliquez sur **Next** (Suivant) :

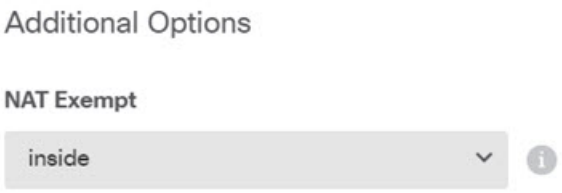
- **Connection Profile Name** (Nom du profil de connexion) : donnez à la connexion un nom significatif, par exemple Site-A-vers-Site-B.
- **Local VPN Access Interface** (Interface d'accès VPN locale) : sélectionnez l'interface externe.
- **Local Network** (Réseau local) : conservez la valeur par défaut, Any (Tout).
- **Remote IP Address** (Adresse IP distante) : saisissez l'adresse IP de l'interface externe de l'homologue distant. Dans cet exemple, 203.0.113.1.
- **Remote Network** (Réseau distant) : cliquez sur +, puis sélectionnez l'objet réseau qui définit le réseau protégé de l'homologue distant. Dans cet exemple, 192.168.2.0/24. Vous pouvez cliquer sur **Create New Network** (Créer un nouvel objet réseau) pour créer l'objet maintenant.

Le graphique suivant montre à quoi la première étape doit ressembler.



d) Définissez la configuration de confidentialité, puis cliquez sur **Next** (Suivant).

- **Politique IKE** : les paramètres IKE n'ont aucune incidence sur le hairpinning. Sélectionnez simplement les versions, les politiques et les propositions IKE qui correspondent à vos besoins de sécurité. Notez les clés prépartagées locales et distantes que vous saisissez : vous en aurez besoin lors de la configuration de l'homologue distant.
- **Exemption**de NAT : sélectionnez l'interface interne.



- **Diffie Hellman Group for Perfect Forward Secrecy** (Groupe Diffie Hellman pour la confidentialité persistante) : ce paramètre n'a aucune incidence sur le hairpinning. Configurez-le comme bon vous semble.

e) Cliquez sur **Terminer**.

Le résumé de la connexion est copié dans le presse-papiers. Vous pouvez le coller dans un fichier texte ou tout autre document pour vous aider à configurer l'homologue distant.

Étape 2 (Site A, site principal.) Configurez la règle NAT pour traduire toutes les connexions sortant de l'interface externe en ports sur l'adresse IP externe (PAT de l'interface).

Lorsque vous avez terminé la configuration initiale du périphérique, le système crée une règle NAT nommée InsideOutsideNatRule. Cette règle applique la PAT d'interface au trafic IPv4 de toute interface qui quitte le périphérique par l'intermédiaire de l'interface externe. Comme l'interface externe est incluse dans l'interface source « Any », la règle dont vous avez besoin existe déjà, sauf si vous l'avez modifiée ou supprimée.

La procédure suivante explique comment créer la règle dont vous avez besoin.

a) Cliquez sur **Policies (Politiques)** > **NAT**.
b) Effectuez l'une des opérations suivantes :

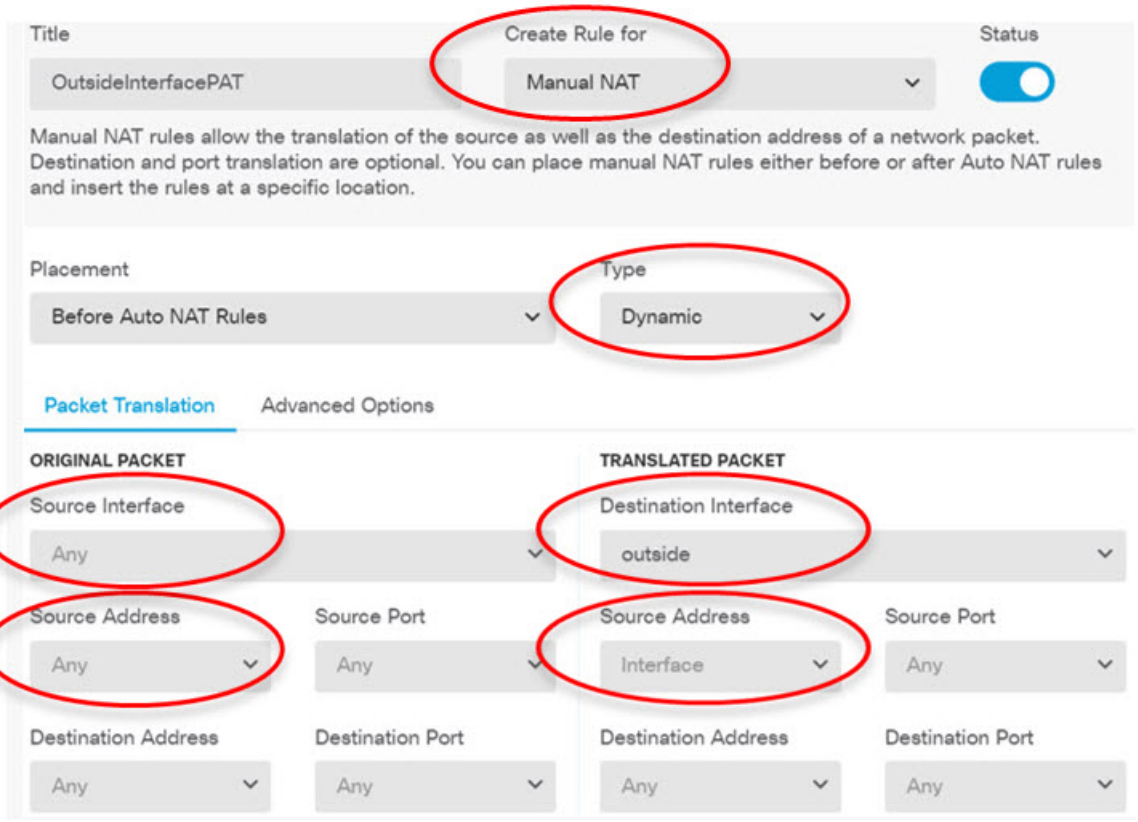
- Pour modifier la règle InsideOutsideNatRule, passez le curseur sur la colonne **Action** et cliquez sur l'icône de modification ( ).
- Pour créer une nouvelle règle, cliquez sur le bouton **+**.

c) Configurez une règle avec les propriétés suivantes :

- **Title** (Titre) : pour une nouvelle règle, saisissez un nom significatif, sans espaces. Par exemple, OutsideInterfacePAT.
- **Create Rule For** (Créer une règle pour) : **Manual NAT** (NAT manuelle).
- **Placement** : **Before Auto NAT Rules (Avant les règles de NAT automatique)** (valeur par défaut).
- **Type** :**Dynamic** (Dynamique).
- **Original Packet** (Paquet d'origine) : pour **Source Address** (Adresse source), sélectionnez Any (tout) ou any-ipv4. Pour **Source Interface** (Interface source), veillez à sélectionner Any (tout) (qui est la valeur par défaut). Pour toutes les autres options de Original Packet (Paquet d'origine), conservez la valeur par défaut, Any (tout).

- **Translated Packet** (Paquet traduit) : pour **Destination Interface** (Interface de destination), sélectionnez externe. Pour **Translated Address** (Adresse traduite), sélectionnez **Interface**. Pour toutes les autres options de Translated Packet (Paquet traduit), conservez la valeur par défaut, Any (tout).

Le graphique suivant montre le cas simple où vous sélectionnez Any (tout) pour l'adresse source.



d) Cliquez sur **OK**.

Étape 3 (Site A, site principal.) Configurez une règle de contrôle d'accès pour autoriser l'accès au réseau protégé sur le site B.

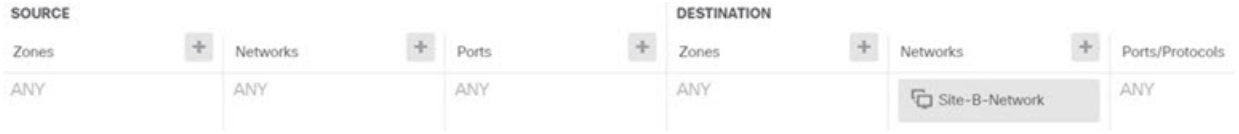
La simple création d'une connexion VPN n'autorise pas automatiquement le trafic sur le VPN. Vous devez vous assurer que votre stratégie de contrôle d'accès autorise le trafic vers le réseau distant.

La procédure suivante montre comment ajouter une règle spécifiquement pour le réseau distant. Le fait que vous ayez besoin d'une règle supplémentaire dépend de vos règles existantes.

a) Cliquez sur **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.
b) Cliquez sur + pour créer une nouvelle règle.
c) Configurez une règle avec les propriétés suivantes :

- **Order** (Ordre) : sélectionnez une position dans la politique avant toute autre règle qui pourrait correspondre à ces connexions et les bloquer. La valeur par défaut consiste à ajouter la règle à la fin de la politique. Si vous devez repositionner la règle ultérieurement, vous pouvez modifier cette option ou simplement faire glisser et déposer la règle dans le bon emplacement dans le tableau.
- **Titre** : saisissez un nom significatif sans espaces. Par exemple, Site-B-Network.

- **Action** : **Autoriser**. Vous pouvez sélectionner Trust (Confiance) si vous ne souhaitez pas que ce trafic soit inspecté pour détecter des violations de protocole ou des intrusions.
- Onglet **Source/Destination** : pour **Destination** > **Network (Réseau)**, sélectionnez le même objet que vous avez utilisé dans le profil de connexion VPN pour le réseau distant. Laissez la valeur par défaut, Any, (tout), pour toutes les autres options de source et de destination.



- Onglets **Application**, **URL** et **Users** (Utilisateurs) : laissez les paramètres par défaut sur ces onglets, c'est-à-dire qu'aucune option n'est sélectionnée.
- Onglets **Intrusion**, **File** (Fichiers) : vous pouvez, au besoin, sélectionner des politiques de prévention des intrusions ou des politiques de fichiers afin d'inspecter les menaces ou les logiciels malveillants.
- Onglet**Logging (journalisation**) : vous pouvez éventuellement activer la journalisation des connexions.

d) Cliquez sur **OK**.

Étape 4 (Site A, site principal.) Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

b) Cliquez sur le bouton **Deploy Now** (déployer maintenant).

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement. Si vous laissez la fenêtre ouverte, elle indiquera qu'il n'y a aucune modification en attente après un déploiement réussi.

Étape 5 (Site B, site distant.) Connectez-vous au périphérique du site distant et configurez la connexion VPN de site à site pour le site A.

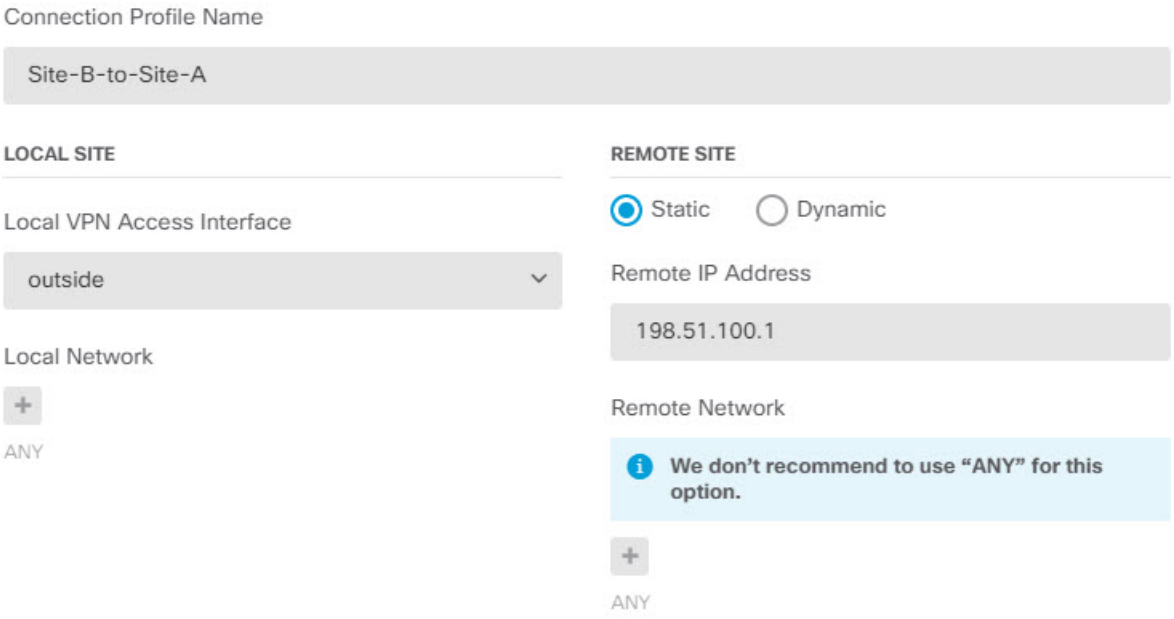
Utilisez le résumé de connexion obtenu à partir de la configuration du périphérique du site A pour vous aider à configurer le côté du site B de la connexion.

a) Cliquez sur **Device** (Périphérique), puis sur **View Configuration** (Afficher la configuration) dans le groupe Connexion VPN de site à site.
b) Cliquez sur **+** pour ajouter une nouvelle connexion.
c) Définissez les points terminaux comme suit, puis cliquez sur **Next** (Suivant) :

- **Connection Profile Name** (Nom du profil de connexion) : donnez à la connexion un nom significatif, par exemple Site-B-vers-Site-A.
- **Local VPN Access Interface** (Interface d'accès VPN locale) : sélectionnez l'interface externe.
- **Local Network** (Réseau local) : cliquez sur **+**, puis sélectionnez l'objet réseau qui définit le réseau protégé local. Dans cet exemple, 192.168.2.0/24. Vous pouvez cliquer sur **Create New Network** (Créer un nouvel objet réseau) pour créer l'objet maintenant.

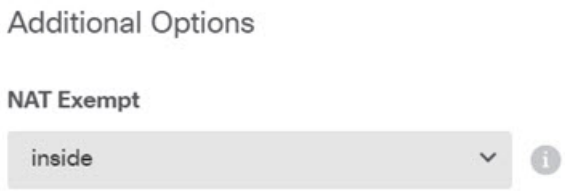
- **Remote IP Address** (Adresse IP distante) : saisissez l'adresse IP de l'interface externe du site principal. Dans cet exemple, 198.51.100.1.
- **distant Network** (Réseau distant) : conservez la valeur par défaut, Any (Tout). Ignorez l'avertissement ; il n'est pas pertinent pour ce scénario d'utilisation.

Le graphique suivant montre à quoi la première étape doit ressembler.



d) Définissez la configuration de confidentialité, puis cliquez sur **Next** (Suivant).

- **Politique IKE** : les paramètres IKE n'ont aucune incidence sur le hairpinning. Configurez les mêmes options ou des options compatibles que celles de la fin de la connexion VPN du site A. Vous devez configurer correctement les clés prépartagées : inversez les clés locales et distantes (pour IKEv2) comme configuré sur le périphérique du site A. Pour IKEv1, il n'y a qu'une seule clé, qui doit être la même sur les deux homologues.
- **NAT Exempt** (Exemption NAT) : sélectionnez l'interface interne.



- **Diffie Hellman Group for Perfect Forward Secrecy** (Groupe Diffie Hellman pour la confidentialité persistante) : ce paramètre n'a aucune incidence sur le hairpinning.. Faire correspondre le paramètre utilisé à la fin de la connexion VPN du site A.

e) Cliquez sur **Terminer**.

Étape 6 (Site B, site distant.) Supprimez toutes les règles NAT pour le réseau protégé afin que tout le trafic sortant du site doive passer par le tunnel VPN.

L'exécution de la NAT sur ce périphérique est inutile, car c'est le périphérique du site A qui effectuera la traduction d'adresses. Mais veuillez examiner votre situation spécifique. Si vous avez plusieurs réseaux internes et qu'ils ne prennent pas tous part à cette connexion VPN, ne supprimez pas les règles NAT dont vous avez besoin pour ces réseaux.

a) Cliquez sur **Policies (Politiques)** > **NAT**.
b) Effectuez l'une des opérations suivantes :

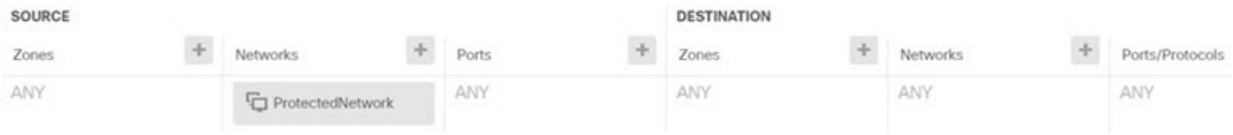
- Pour supprimer des règles, passez le curseur sur la colonne Action et cliquez sur l'icône de suppression ( ).
- Pour modifier les règles afin qu'elles ne s'appliquent plus au réseau protégé, passez le curseur sur la colonne Action et cliquez sur l'icône de modification ( ).

Étape 7 (Site B, site distant.) Configurez une règle de contrôle d'accès pour autoriser l'accès du réseau protégé à Internet.

L'exemple suivant permet le trafic du réseau protégé vers n'importe quelle destination. Vous pouvez l'ajuster selon vos besoins précis. Vous pouvez également faire précéder la règle de règles de blocage pour filtrer le trafic indésirable. Une autre option consiste à configurer les règles de blocage sur l'appareil du site A.

a) Cliquez sur **Policies (Politiques)** > **Access Control (Contrôle d'accès)**.
b) Cliquez sur **+** pour créer une nouvelle règle.
c) Configurez une règle avec les propriétés suivantes :

- **Order** (Ordre) : sélectionnez une position dans la politique avant toute autre règle qui pourrait correspondre à ces connexions et les bloquer. La valeur par défaut consiste à ajouter la règle à la fin de la politique. Si vous devez repositionner la règle ultérieurement, vous pouvez modifier cette option ou simplement faire glisser et déposer la règle dans le bon emplacement dans le tableau.
- **Titre** : saisissez un nom significatif sans espaces. Par exemple, Protected-Network-to-Any.
- **Action** : **Autoriser**. Vous pouvez sélectionner Trust (Confiance) si vous ne souhaitez pas que ce trafic soit inspecté pour détecter des violations de protocole ou des intrusions.
- Onglet **Source/Destination** : pour **Source** > **Network (Réseau)**, sélectionnez le même objet que vous avez utilisé dans le profil de connexion VPN pour le réseau local. Laissez la valeur par défaut, Any, (tout), pour toutes les autres options de source et de destination.



- Onglets **Application**, **URL** et **Users** (Utilisateurs) : laissez les paramètres par défaut sur ces onglets, c'est-à-dire qu'aucune option n'est sélectionnée.
- Onglets **Intrusion**, **File** (Fichiers) : vous pouvez, au besoin, sélectionner des politiques de prévention des intrusions ou des politiques de fichiers afin d'inspecter les menaces ou les logiciels malveillants.
- Onglet **Logging (journalisation**) : vous pouvez éventuellement activer la journalisation des connexions.

d) Cliquez sur **OK**.

Étape 8 (Site B, site distant.) Validez vos modifications.

a) Cliquez sur l'icône **Deploy Changes** (déployer les modifications) dans le coin supérieur droit de la page Web.

b) Cliquez sur le bouton **Deploy Now** (déployer maintenant) et attendez la fin du déploiement.

Vous pouvez attendre la fin du déploiement ou cliquer sur **OK** et vérifier la liste des tâches ou l'historique du déploiement ultérieurement. Si vous laissez la fenêtre ouverte, elle indiquera qu'il n'y a aucune modification en attente après un déploiement réussi.

Sécuriser le trafic de réseaux dans plusieurs routeurs virtuels sur un VPN de site à site

Si vous configurez plusieurs routeurs virtuels sur un périphérique, vous devez configurer le VPN de site à site dans le routeur virtuel global. Vous ne pouvez pas configurer le VPN de site à site sur une interface affectée à un routeur virtuel personnalisé.

Comme les tables de routage pour les routeurs virtuels sont distinctes, vous devez créer des routes statiques si vous devez sécuriser les connexions des réseaux hébergés dans des routeurs virtuels personnalisés sur le VPN de site à site. Vous devez également mettre à jour la connexion VPN de site à site pour inclure ces réseaux supplémentaires.

Prenons l'exemple suivant. Dans ce cas, le VPN de site à site est défini sur l'interface externe à l'adresse 172.16.3.1. Ce VPN peut inclure le réseau interne 192.168.2.0/24 sans configuration supplémentaire, car l'interface interne fait également partie du routeur virtuel global. Mais, pour fournir des services VPN de site à site au réseau 192.168.1.0/24, qui fait partie du routeur virtuel VR1, vous devez configurer des routes statiques dans les deux sens, et ajouter le réseau à la configuration VPN de site à site.

Avant de commencer

Cet exemple suppose que vous ayez déjà configuré le VPN de site à site entre le réseau local 192.168.2.0/24 et le réseau externe 172.16.20.0/24, défini les routeurs virtuels et configuré et affecté les interfaces aux routeurs virtuels appropriés.

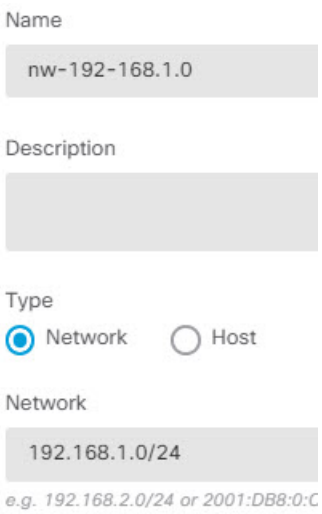
Procédure

Étape 1 Configurez la fuite de route du routeur virtuel global vers VR1.

Cette fuite de route permet aux points terminaux protégés par l'extrémité externe (distant) du VPN de site à site d'accéder au réseau 192.168.1.0/24 dans le routeur virtuel VR1.

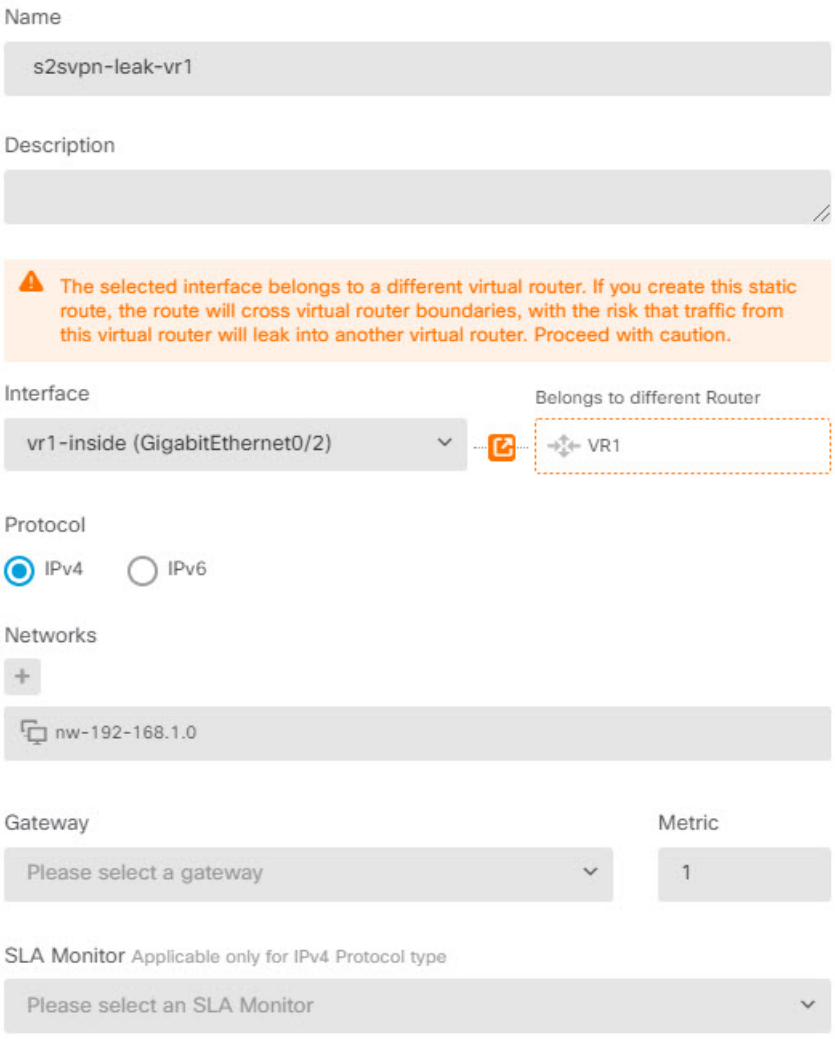
a) Choisissez **Device (Périphérique)** > **Routing (Routage)** > **View Configuration (Afficher la configuration)**.
b) Cliquez sur l'icône d'affichage ( ) du routeur virtuel global.
c) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel global, cliquez sur **+** et configurez la route :

- **Nom** : n'importe quel nom suffit, tel que **s2svpn-leak-vr1**.
- **Interface** : sélectionnez **vr1-inside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez un objet qui définit le réseau 192.168.1.0/24. Cliquez sur **Create New Network** (Créer un nouveau réseau) pour créer l'objet maintenant, si nécessaire.



- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



d) Cliquez sur **OK**.

Étape 2 Configurez la fuite de route de VR1 vers le routeur virtuel global :

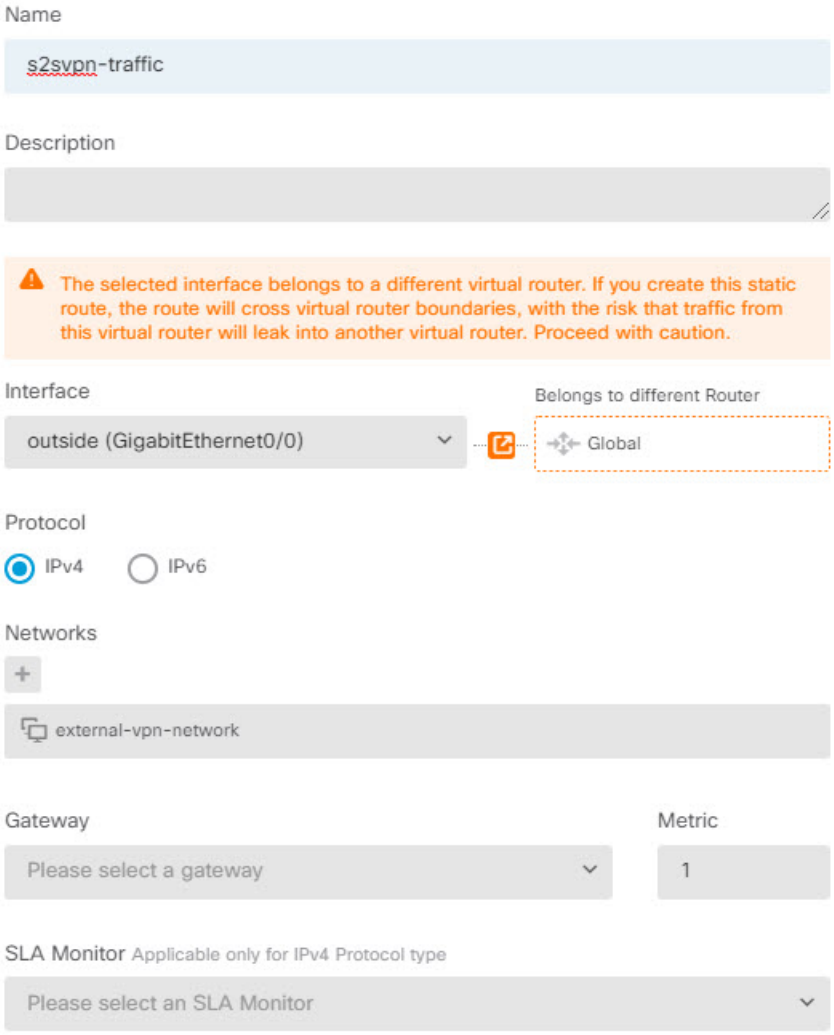
Cette route permet aux points terminaux sur le réseau 192.168.1.0/24 d'établir des connexions qui traverseront le tunnel VPN de site à site. Pour cet exemple, le point terminal distant protège le réseau 172.16.20.0/24.

a) Choisissez **VR1** dans la liste déroulante des routeurs virtuels pour passer à la configuration VR1.
b) Dans l'onglet **Static Routing** (Routage statique) du routeur virtuel VR1, cliquez sur + et configurezla route :

- **Nom** : n'importe quel nom suffit, tel que **s2svpn-traffic**.
- **Interface** : sélectionnez **outside**.
- **Protocole** : sélectionnez **IPv4**.
- **Réseaux** : sélectionnez l'objet que vous avez créé pour les réseaux protégés du point terminal distant, par exemple, **externe-vpn-network**.

- **Gateway** (passerelle) : laissez ce champ vide. Lors de la fuite d'une route vers un autre routeur virtuel, ne sélectionnez pas la passerelle.

La boîte de dialogue doit ressembler à ce qui suit :



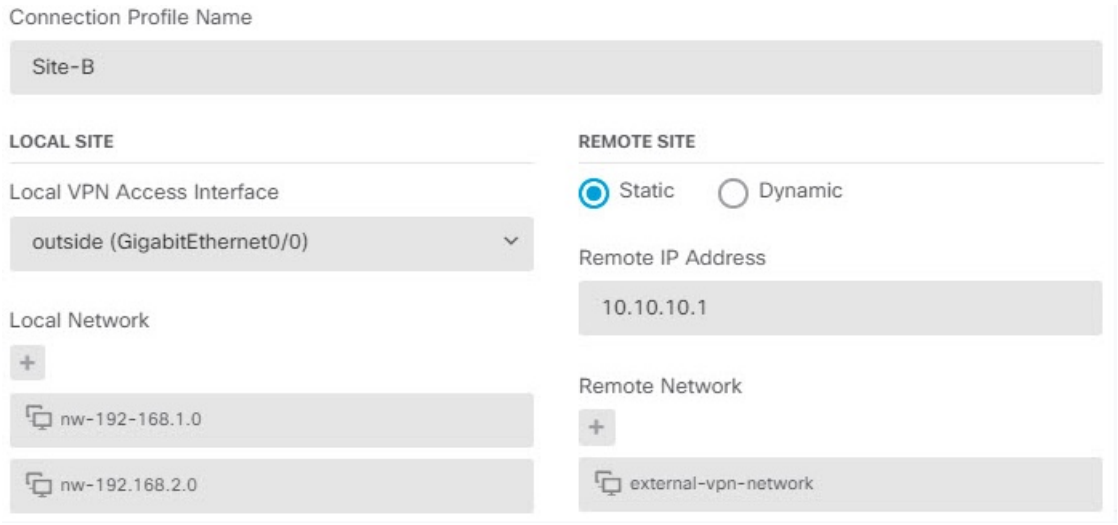
c) Cliquez sur **OK**.

Étape 3 Ajoutez le réseau 192.168.1.0/24 au profil de connexion VPN de site à site :

a) Choisissez **Device (Périphérique)** > **Site-to-Site VPN (VPN de site à site)** > **View Configuration (Afficher la configuration)**.

b) Cliquez sur l'icône de modification ( ) du profil de connexion.

c) Sur la première page de l'assistant, cliquez sur **+** sous **Local Network (Réseau local)**, puis ajoutez l'objet correspondant au réseau 192.168.1.0/24.



d) Achevez l'assistant.

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.