Présentation du VPN

Une connexion de réseau privé virtuel (VPN) établit un tunnel sécurisé entre les points terminaux sur un réseau public comme Internet.

Ce chapitre s'applique aux VPN d'accès à distance et de site à site sur les périphériques Cisco Secure Firewall Threat Defense. Il décrit les normes IPsec (Internet Protocol Security), ISAKMP ou IKE (Internet Security Association and Key Management Protocol) et SSL qui sont utilisées pour créer des VPN de site à site et d'accès à distance.

Types de VPN

centre de gestion prend en charge les types de connexions VPN suivants :

- VPN d'accès à distance sur les périphériques défense contre les menaces .

  Les VPN d'accès à distance sont des connexions ou tunnels sécurisés et chiffrés, entre les utilisateurs distants et le réseau privé de votre entreprise. La connexion se compose d'un périphérique VPN, qui est un poste de travail ou un appareil mobile avec des fonctionnalités de client VPN, et d'un périphérique de tête de réseau VPN, ou passerelle sécurisée, en périphérie du réseau privé d'entreprise.

  Cisco Secure Firewall Threat Defense peuvent être configurés pour prendre en charge les VPN d'accès à distance sur SSL ou IPsec IKEv2 par l' centre de gestion. Fonctionnant comme des passerelles sécurisées à ce titre, ils authentifient les utilisateurs distants, autorisent l'accès et chiffrent les données pour fournir des connexions sécurisées à votre réseau. Aucun autre type d'appareil, géré par centre de gestion, ne prend en charge les connexions VPN d'accès à distance.

  Les passerelles sécuriséesCisco Secure Firewall Threat Defense prennent en charge le client de tunnel complet Secure Client. Ce client est tenu de fournir des connexions SSL IPsec IKEv2 sécurisées aux utilisateurs distants. Ce client offre aux utilisateurs distants les avantages d'un client sans que les

administrateurs réseau n'aient à installer et à configurer les clients sur les ordinateurs distants, car il peut être déployé sur la plateforme client lors de la connectivité. C'est le seul client pris en charge sur les périphériques de point terminal.

- VPN de site à site sur des périphériques défense contre les menaces .

  Un VPN de site à site connecte des réseaux dans différents emplacements géographiques. Vous pouvez créer des connexions IPsec de site à site entre des périphériques gérés, et entre des périphériques gérés et d'autres homologues de Cisco ou de tiers, qui sont conformes à toutes les normes pertinentes. Ces homologues peuvent avoir n'importe quelle combinaison d'adresses IPv4 et IPv6 internes et externes. Les tunnels de site à site sont conçus à l'aide de la suite de protocoles Internet Protocol Security (IPsec) et IKEv1 ou IKEv2. Une fois la connexion VPN établie, les hôtes derrière la passerelle locale peuvent se connecter aux hôtes derrière la passerelle distante grâce au tunnel VPN sécurisé.

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

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 à l'homologue distant, et ce dernier recherche une correspondance avec ses propres politiques, par ordre de priorité. Il existe une correspondance entre les politiques IKE, si elles ont les mêmes valeurs de chiffrement, de hachage (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 politique de durée de vie la plus courte (de l'homologue distant) s'applique. Par défaut, Cisco Secure Firewall Management Center déploie une politique IKEv1 à la priorité la plus basse pour tous les terminaux VPN afin d'assurer le succès de la négociation.

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 de protocoles et d'algorithmes de sécurité.

Une politique de proposition IPsec définit les paramètres requis pour les tunnels IPsec. Une proposition IPsec est un ensemble d'une ou de plusieurs cartes cryptographiques qui sont appliquées aux interfaces VPN sur les périphériques. Une carte de chiffrement combine tous les composants requis pour configurer les associations de sécurité IPsec, notamment :

- Une proposition (ou ensemble de transformations) est une combinaison de protocoles de sécurité et d'algorithmes qui sécurisent le trafic dans un tunnel IPsec. Pendant la négociation d'association de sécurité (SA) d'IPsec, les homologues recherchent une proposition identique sur les deux homologues. Une fois trouvé, il est appliqué pour créer un SA qui protège les flux de données dans la liste d'accès pour cette carte de chiffrement, protégeant le trafic dans le VPN. Il existe des propositions d'IPsec distinctes pour IKEv1 et IKEv2. Dans les propositions IKEv1 (ou ensembles de transformations), pour chaque paramètre, vous définissez une valeur. Pour les propositions IKEv2, vous pouvez configurer plusieurs algorithmes de chiffrement et d'intégration pour une seule proposition.
- Une carte de chiffrement combine tous les composants requis pour configurer les associations de sécurité (SA) IPsec, y compris les règles IPsec, les propositions, les homologues distants et d'autres paramètres nécessaires pour définir une SA IPsec. Lorsque deux homologues tentent d'établir une SA, ils doivent chacun avoir au moins une entrée de carte de chiffrement compatible.

  Les politiques de carte de chiffrement dynamique sont utilisées dans les VPN de site à site lorsqu'un homologue distant inconnu tente de démarrer une association de sécurité IPsec avec le concentrateur local. Le concentrateur ne peut pas être l'initiateur de la négociation d'association de sécurité. Les politiques de chiffrement dynamiques permettent aux homologues distants d'échanger du trafic IPsec avec un concentrateur local même si le concentrateur ne connaît pas l'identité de l'homologue distant. Une politique de carte de chiffrement dynamique crée essentiellement une entrée de carte de chiffrement sans que tous les paramètres soient configurés. Les paramètres manquants sont ultérieurement configurés dynamiquement (à la suite d'une négociation IPsec) pour correspondre aux exigences d'un homologue distant.

  Les politiques de carte de chiffrement dynamique s'appliquent aux topologies en étoile et VPN point à point. Pour appliquer des politiques de carte de chiffrement dynamique, spécifiez une adresse IP dynamique pour l'un des homologues dans la topologie et assurez-vous que la carte de chiffrement dynamique est activée sur cette topologie. Notez que dans une topologie VPN à maillage complet, vous ne pouvez appliquer que des politiques de carte de chiffrement statique.

Remarque La carte de chiffrement dynamique IKEv2 simultanée n'est pas prise en charge pour la même interface pour à la fois les VPN d'accès à distance et les VPN de site à site sur Firepower Threat Defense (FTD).

Flux de paquets VPN

Sur un périphérique défense contre les menaces , par défaut, aucun trafic n'est autorisé à passer par le contrôle d'accès sans autorisation explicite. Le trafic du tunnel VPN n'est pas non plus relayé vers les points terminaux avant d'être passé par Snort. Les paquets du tunnel entrants sont déchiffrés avant d'être envoyés au processus Snort. Snort traite les paquets sortants avant le chiffrement.

Le contrôle d'accès, qui identifie les réseaux protégés pour chaque nœud d'extrémité d'un tunnel VPN, détermine quel trafic est autorisé à passer par le périphérique défense contre les menaces et à atteindre les points terminaux. Pour le trafic VPN d'accès à distance, un filtre de politique de groupe ou une règle de contrôle d'accès doit être configuré pour permettre le flux de trafic VPN.

De plus, le système n'envoie pas le trafic du tunnel vers la source publique lorsque le tunnel est en panne.

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.

Licences VPN

Il n’y a pas de licence spécifique pour l’activation du VPN Cisco Secure Firewall Threat Defense, il est disponible par défaut.

Le centre de gestion détermine s’il faut autoriser ou bloquer l’utilisation d’un chiffrement fort sur le périphérique défense contre les menaces en fonction des attributs fournis par le serveur de licences Smart.

Cela est contrôlé si vous avez sélectionné ou non la fonctionnalité contrôlée à l'exportation sur le périphérique lors de votre inscription au gestionnaire de licences Cisco Smart. 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.

Si vous avez créé vos configurations VPN avec une licence d’évaluation et mis à niveau votre licence d’évaluation à une licence Smart avec fonctionnalité contrôlée à l'exportation, vérifiez et mettez à jour vos algorithmes de chiffrement pour un chiffrement plus fort et pour que les VPN fonctionnent correctement. Les chiffrements basés sur DES ne sont plus pris en charge.

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.

Respect des exigences en matière de certification de la sécurité

De nombreux paramètres VPN comportent des options qui vous permettent de vous conformer aux diverses normes de certification de sécurité. Passez en revue vos exigences de certification et les options disponibles pour planifier votre configuration VPN.

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. Ceci est généralement utilisé à des fins de test uniquement. Cependant, il ne fonctionne pas du tout sur de nombreuses plateformes, y compris virtuelles et Firepower 2100.

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

Les clés prépartagées et les certificats numériques sont les méthodes d'authentification disponibles pour les VPN.

Les connexions VPN de site à site, IKEv1 et IKEv2 peuvent utiliser les deux options.

L'accès à distance, qui utilise uniquement SSL et IPsec, IKEv2, prend uniquement en charge l'authentification par certificat numérique.

Les clés prépartagées permettent de partager une clé secrète entre deux homologues et de l'utiliser par IKE pendant la phase d'authentification. La même clé partagée doit être configurée sur chaque homologue, sinon IKE SA ne peut pas être établi.

Les certificats numériques utilisent des paires de clés RSA pour signer et chiffrer les messages de gestion des clés IKE. Les certificats assurent la non-répudiation des communications entre deux pairs, ce qui signifie qu'il est possible de prouver que la communication a effectivement eu lieu. Lorsque vous utilisez cette méthode d'authentification, vous avez besoin d'une infrastructure à clé publique (PKI) définie où les homologues peuvent obtenir des certificats numériques auprès d'une autorité de certification (AC). Les autorités de certification gèrent les demandes de certificats et délivrent des certificats aux périphériques du réseau participants, ce qui assure une gestion centralisée des clés pour tous les périphériques participants.

Les clés prépartagées n'évoluent pas facilement. L'utilisation d'une autorité de certification améliore la facilité de gestion et l'évolutivité de votre réseau IPsec. Grâce à une autorité de certification, vous n'avez pas besoin de configurer des clés entre tous les périphériques de chiffrement. Au lieu de cela, chaque périphérique participant est enregistré auprès de l'autorité de certification et demande un certificat à cette dernière. Chaque périphérique, qui possède son propre certificat et la clé publique de l'autorité de certification, peut authentifier tous les autres périphériques dans le domaine d'une autorité de certification donnée.

Clés prépartagées

La clé pré-partagée vous permet de partager une clé secrète entre deux homologues. IKE utilise la clé lors de la phase d'authentification. Vous devez configurer la même clé partagée sur chaque homologue, sinon l'ASA IKE ne peut pas être établi.

Pour configurer les clés prépartagées, choisissez si vous souhaitez utiliser une clé générée manuellement ou automatiquement, puis spécifiez la clé dans les options IKEv1/IKEv2. Ensuite, lorsque vous déployez votre configuration, la clé est configurée sur tous les périphériques de la topologie.

Infrastructure de l'infrastructure PKI et certificats numériques

Infrastructure de clé publique

Une PKI fournit une gestion centralisée des clés pour les périphériques réseau participants. Il s'agit d'un ensemble défini de politiques, de procédures et de rôles qui prennent en charge *le chiffrement à clé publique* en générant, en vérifiant et en révoquant *des certificats de clé publique,* communément appelés *certificats numériques*.

En cryptographie à clé publique, chaque extrémité d'une connexion est dotée d'une paire de clés composée d'une clé publique et d'une clé privée. Les paires de clés sont utilisées par les points terminaux VPN pour signer et chiffrer les messages. Les clés agissent comme des compléments, et tout ce qui est chiffré avec l'une des clés peut être déchiffré avec l'autre, sécurisant les données circulant sur la connexion.

Générez une paire de clés RSA, RSA, ECDSA ou EDDSA à usage général, utilisée à la fois pour la signature et le chiffrement, ou générez des paires de clés distinctes pour chaque objectif. Des clés de signature et de chiffrement distinctes aident à réduire l'exposition des clés. SSL utilise une clé pour le chiffrement mais pas la signature, cependant, IKE utilise une clé pour la signature mais pas le chiffrement. En utilisant des clés distinctes pour chacune, l'exposition des clés est réduite au minimum.

Certificats numériques ou certificats d'identification

Lorsque vous utilisez les certificats numériques comme méthode d'authentification pour les connexions VPN, les homologues sont configurés pour obtenir des certificats numériques d'une autorité de certification (CA). Les autorités de certification sont des autorités de confiance qui « signent » des certificats pour vérifier leur authenticité, garantissant ainsi l'identité du périphérique ou de l'utilisateur.

Les serveurs d'autorité de certification gèrent les demandes de certificats publics d'une autorité de certification et délivrent des certificats aux périphériques du réseau participants dans le cadre d'une infrastructure à clé publique (PKI). Cette activité s'appelle inscription de certificats. Ces certificats numériques, également appelés certificats d'identité, contiennent :

- L'identification numérique du propriétaire aux fins d'authentification, comme le nom, le numéro de série de l'entreprise, le service ou l'adresse IP.
- Clé publique nécessaire pour envoyer et recevoir des données chiffrées au propriétaire du certificat.
- La signature numérique sécurisée de l'autorité de certification.

Les certificats assurent également la non-répudiation de la communication entre deux homologues, ce qui signifie que cela prouve que la communication a réellement eu lieu.

Inscription de certificat

L'utilisation d'une PKI améliore la facilité de gestion et l'évolutivité de votre VPN, car vous n'avez pas à configurer des clés prépartagées entre tous les périphériques de chiffrement. Au lieu de cela, vous *inscrivez* individuellement chaque périphérique participant auprès d'un serveur d'autorité de certification, qui est explicitement approuvé pour valider les identités et créer un certificat d'identité pour le périphérique. Lorsque cela a été fait, chaque homologue participant envoie son certificat d'identité à l'autre homologue pour valider son identité et établir des sessions chiffrées avec les clés publiques contenues dans les certificats. Consultez Objets d'Inscription du certificat pour en savoir plus sur l'inscription de défense contre les menaces .

Certificats d'autorité de certification

Afin de valider le certificat d'un homologue, chaque périphérique participant doit récupérer le certificat de l'autorité de certification sur le serveur. Un certificat d'autorité de certification est utilisé pour signer les autres certificats. Il est autosigné et appelé certificat racine. Ce certificat contient la clé publique de l'autorité de certification, utilisée pour déchiffrer et valider la signature numérique de l'autorité de certification ainsi que le contenu du certificat de l'homologue reçu. Le certificat de l'autorité de certification peut être obtenu en :

- Utilisant le protocole SCEP (Simple Certificate Enrollment Protocol) ou l'inscription sur le transport sécurisé (EST) pour récupérer le certificat de l'autorité de certification auprès du serveur de l'autorité de certification
- Copiant manuellement le certificat de l'autorité de certification à partir d'un autre périphérique participant

Point de confiance

Une fois l'inscription terminée, un point de confiance est créé sur le périphérique géré. Il s'agit de la représentation objet d'une autorité de certification et des certificats associés. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres spécifiques à l'autorité de certification et une association avec un seul certificat d'identité inscrit.

Fichier PKCS#12

Un fichier PKCS#12, ou PFX, contient le certificat du serveur, tous les certificats intermédiaires et la clé privée en un seul fichier chiffré. Ce type de fichier peut être importé directement dans un périphérique pour créer un point de confiance.

Vérification de la révocation

Une autorité de certification peut également révoquer les certificats d'homologues qui ne font plus partie de votre réseau. Les certificats révoqués sont soit gérés par un serveur OCSP (Online Certificate Status Protocol), soit répertoriés dans une liste de révocation de certificats (CRL) stockée sur un serveur LDAP. Un homologue peut les vérifier avant d'accepter un certificat d'un autre homologue.

Algorithmes de hachage, algorithmes de chiffrement et groupes de module Diffie-Hellman supprimés ou obsolètes

La prise en charge des chiffrements moins sécurisés a été supprimée. Nous vous recommandons de mettre à jour votre configuration VPN avant d'effectuer la mise à niveau à la version défense contre les menaces 6,70 vers la fonction DH et les algorithmes de chiffrement pris en charge pour vous assurer que le VPN fonctionne correctement.

Mettez à jour vos propositions IKE et politiques IPSec pour qu'elles correspondent à celles prises en charge dans défense contre les menaces 6.70, puis déployez les modifications de configuration.

Les chiffrements moins sécurisés suivants ont été supprimés ou sont obsolètes dans les versions ultérieures à défense contre les menaces 6.70 :

- **Le Diffie-Hellman GROUP 5** est obsolète pour IKEv1 et IKEv2.
- Les groupes Diffie-Hellman 2 et 24 ont été supprimés.
- **Les algorithmes de chiffrement** : 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256 ont été supprimés.

Remarque

DES continue d'être pris en charge en mode d'évaluation ou pour les utilisateurs qui ne satisfont pas les contrôles à l'exportation pour un chiffrement renforcé.

La valeur NULL est supprimée dans la politique IKEv2, mais prise en charge dans les ensembles de transformations IPsec IKEv1 et IKEv2.

Options de topologie VPN

Lorsque vous créez une topologie VPN, vous devez au minimum lui donner un nom unique, spécifier un type de topologie et sélectionner la version IKE. Vous avez le choix entre trois types de topologies, chacune contenant un groupe de tunnels VPN :

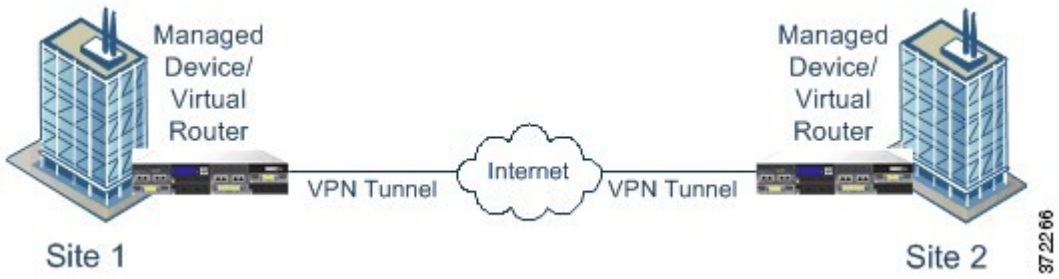
- Les topologies point à point (PTP) établissent un tunnel VPN entre deux points terminaux.
- Les topologies en étoile établissent un groupe de tunnels VPN connectant un point terminal de concentrateur à un groupe de points terminaux en étoile.
- Les topologies à maillage complet établissent un groupe de tunnels VPN parmi un ensemble de points terminaux.

Définissez une clé pré-partagée pour l'authentification VPN manuellement ou automatiquement, il n'y a pas de clé par défaut. Lorsque vous choisissez Automatic, Cisco Secure Firewall Management Center génère une clé prépartagée et l'affecte à tous les nœuds de la topologie.

Topologie VPN point à point

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.

Le diagramme suivant présente une topologie VPN point à point typique.

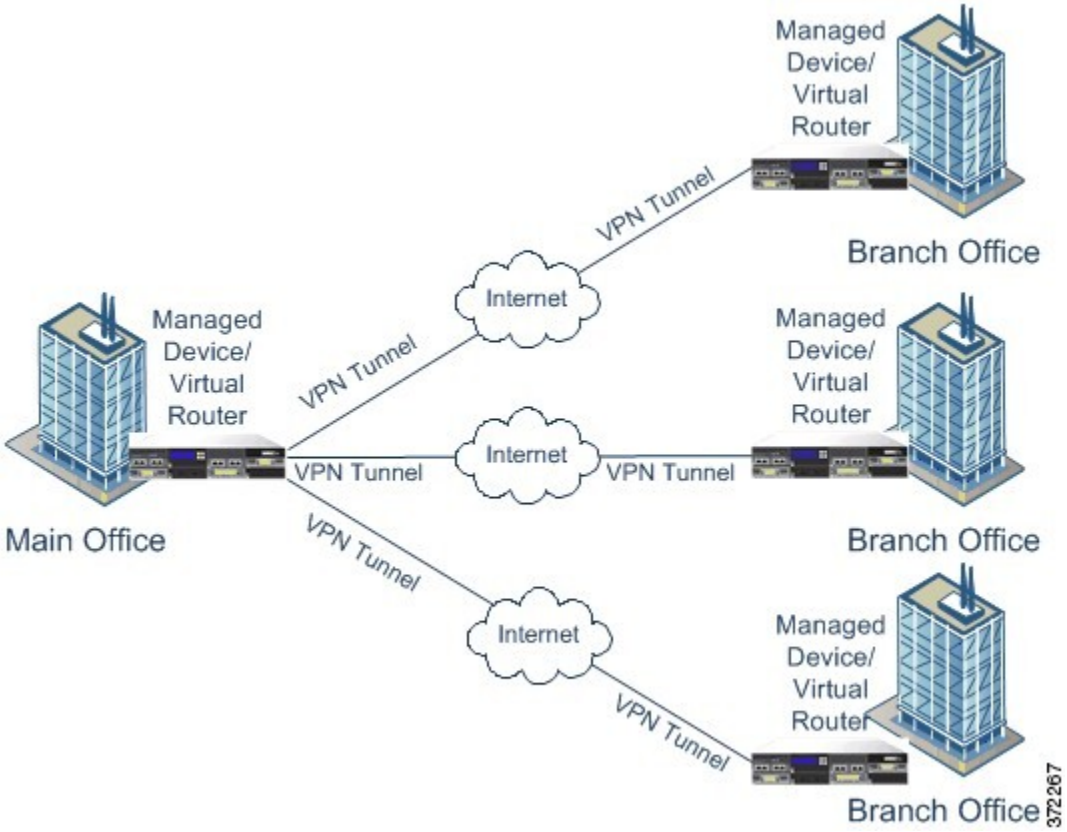


Topologie VPN de réseau en étoile

Dans une topologie VPN de concentrateur en étoile, un point terminal central (nœud de concentrateur) se connecte à plusieurs points terminaux distants (nœuds en étoile). Chaque connexion entre le nœud de concentrateur et un point terminal en étoile constitue un tunnel VPN distinct. Les hôtes derrière les nœuds en étoile peuvent communiquer entre eux par l'intermédiaire du nœud de concentrateur.

La topologie en étoile représente généralement un VPN qui connecte les emplacements du bureau principal et des sites distants d'une organisation à l'aide de connexions sécurisées sur Internet ou un autre réseau tiers. Ces déploiements offrent à tous les employés un accès contrôlé au réseau de l'entreprise. En règle générale, le nœud de concentrateur est situé au bureau principal. Les nœuds en étoile sont situés dans les sites distants et démarrent la majeure partie du trafic.

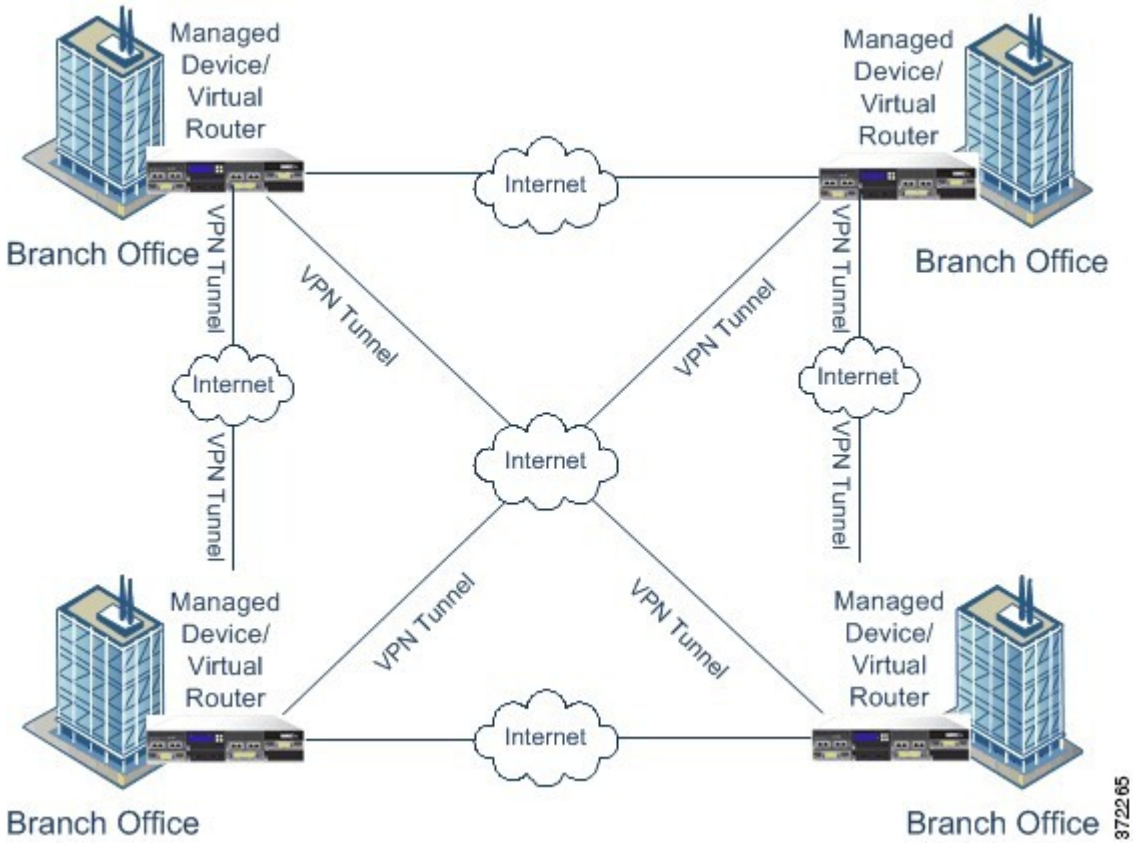
Le diagramme suivant présente une topologie VPN de concentrateur en étoile typique.



Topologie de VPN à maillage complet

Dans une topologie VPN à maillage complet, tous les points terminaux peuvent communiquer avec un autre point terminal par un tunnel VPN individuel. Cette topologie offre une redondance afin que, lorsqu'un point terminal tombe en panne, les autres points terminaux puissent toujours communiquer entre eux. Il représente généralement un VPN qui connecte un groupe de succursales centralisées. Le nombre de périphériques gérés activés par VPN que vous déployez dans cette configuration dépend du niveau de redondance dont vous avez besoin.

Le diagramme suivant présente une topologie typique de VPN à maillage complet.



Topologies implicites

En plus des trois topologies principales de VPN, d'autres topologies plus complexes peuvent être créées en combinant ces dernières. Cela comprend ce qui suit :

- Maillage partiel : réseau dans lequel certains périphériques sont organisés en une topologie à maillage complet, et d'autres périphériques forment une connexion en étoile ou point à point avec certains des périphériques entièrement maillés. Un maillage partiel n'offre pas le niveau de redondance d'une topologie à maillage complet, mais il est moins coûteux à mettre en œuvre. Les topologies de maillage partiel sont utilisées dans les réseaux périphériques qui se connectent à un réseau fédérateur à maillage complet.
- Réseau en étoile à plusieurs niveaux : réseau de topologies en étoile dans lequel un périphérique peut se comporter en tant que concentrateur dans une ou plusieurs topologies et en étoile dans d'autres topologies. Le trafic est autorisé des groupes en étoile vers leur concentrateur le plus immédiat.
- Une topologie en étoile jointe : une combinaison de deux topologies en étoile (en étoile, point à point ou à maillage complet) qui se connectent pour former un tunnel point à point. Par exemple, une topologie en étoile jointe pourrait comprendre deux topologies en étoile, les concentrateurs servant de périphériques homologues dans une topologie point à point.

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.