Assistants VPN

Présentation du VPN

L'ASA crée un réseau privé virtuel en établissant une connexion sécurisée sur un réseau TCP/IP (tel qu'Internet) que les utilisateurs voient comme une connexion privée. Il peut créer des connexions utilisateur unique à réseau local (LAN) et des connexions de réseau local (LAN) à réseau local (LAN).

La connexion sécurisée est appelée tunnel, et l'ASA utilise des protocoles de tunnellisation pour négocier les paramètres de sécurité, créer et gérer des tunnels, encapsuler des paquets, les transmettre ou les recevoir par le tunnel, et les désencapsuler. L'ASA fonctionne comme un point terminal de tunnel bidirectionnel : il peut recevoir des paquets simples, les encapsuler 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, les désencapsuler et les envoyer à leur destination finale.

L'assistant VPN vous permet de configurer les connexions de base entre les réseaux locaux et d'accès à distance et d'affecter des clés prépartagées ou des certificats numériques pour l'authentification. Utilisez ASDM pour modifier et configurer les fonctionnalités avancées.

Les quatre assistants VPN décrits dans cette section sont les suivants :

- Assistant VPN Secure Client, à la page 4

  Le module VPN AnyConnect de Cisco Secure Client fournit des connexions SSL ou IPsec (IKEv2) sécurisées à l'ASA pour les utilisateurs distants avec une tunnellisation VPN complète vers les ressources de l'entreprise. Sans client déjà installé, les utilisateurs distants saisissent dans leur navigateur l'adresse IP d'une interface configurée pour accepter les connexions VPN sans client. L'ASA télécharge le client correspondant au système d'exploitation de l'ordinateur distant. Après le téléchargement, le client s'installe et se configure, établit une connexion sécurisée et reste ou se désinstalle (selon la configuration de l'ASA) lorsque la connexion s'interrompt. Dans le cas d'un client déjà installé, lorsque l'utilisateur s'authentifie, l'ASA vérifie la version du client et le met à niveau au besoin.

  L'assistant VPN Secure Client ne sera disponible que dans les contextes d'utilisateur lorsque l'ASA est en mode multi-contexte. Le stockage et la classe de ressources pour le contexte requis doivent être configurés à partir du contexte du système.

Le stockage par contexte est requis pour avoir les fichiers de paquet et de profil Cisco Secure Client. La classe de ressource est requise pour l'attribution de licence pour chaque contexte. La licence utilisée est Secure Client Premium.

Remarque Le reste de la configuration pour cet assistant reste la même que celle d'un contexte unique.

- Assistant d'accès à distance IPsec IKEv2, à la page 12

  IKEv2 permet aux clients VPN d'autres fournisseurs de se connecter aux appareils de sécurité adaptables Cisco. Cela améliore la sécurité et est conforme aux exigences d'accès à distance IPsec définies dans les mandats du gouvernement américain et du secteur public.

  L'assistant d'accès à distance IPSec IKEv2 ne sera disponible que dans les contextes d'utilisateur lorsque l'ASA est en mode multi-contexte. La classe de ressource pour le contexte requis doit être configurée à partir du contexte système pour l'attribution de licence. La licence utilisée est Secure Client Premium.

Remarque Le reste de la configuration pour cet assistant reste la même que celle d'un contexte unique.

- Assistant d'accès à distance IPsec IKEv1, à la page 7
- Assistant VPN de site à site IPsec, à la page 2

  Pour les connexions de réseau local à réseau local utilisant l'adressage IPv4 et IPv6, l'ASA prend en charge les tunnels VPN si les deux homologues sont ASA et si les deux réseaux internes ont des schémas d'adressage correspondants (IPv4 ou IPv6). Cela est également vrai si les deux réseaux internes homologues sont IPv6 et si le réseau externe est IPv6.

Assistant VPN de site à site IPsec

Un tunnel entre deux périphériques ASA s'appelle un tunnel de site à site et est bidirectionnel. Un tunnel VPN de site à site protège les données à l'aide du protocole IPsec.

Identification de l'appareil homologue.

- Peer IP Address (Adresse IP homologue) : configurez l'adresse IP de l'autre site (périphérique homologue).
- VPN Access Interface (Interface d'accès VPN) : sélectionnez l'interface à utiliser pour le tunnel de site à site.
- Crypto Map Type (Type de carte de chiffrement) : spécifiez le type de cartes qui sera utilisé pour cet homologue, statique ou dynamique.

Trafic à protéger

Cette étape vous permet d'identifier le réseau local et le réseau distant. Ces réseaux protègent le trafic à l'aide du chiffrement IPsec.

- Local Networks (Réseaux locaux) : identifiez l'hôte utilisé dans le tunnel IPsec.
- Remote Networks (Réseaux distants) : identifiez les réseaux utilisés dans le tunnel IPsec.

Sécurité

Cette étape vous permet de configurer les méthodes d'authentification auprès du périphérique homologue. Vous pouvez soit choisir la configuration simple et fournir une clé prépartagée. Ou vous pouvez choisir une configuration personnalisée pour des options plus avancées, comme suit :

- IKE Version (Version IKE) : cochez la case IKEv1 ou IKEv2 selon la version que vous souhaitez utiliser.
- Méthodes d'authentification IKE version 1
    - Pre-shared Key (Clé prépartagée : l'utilisation d'une clé prépartagée est un moyen rapide et facile de configurer la communication avec un nombre limité d'homologues distants et un réseau stable. Cela peut entraîner des problèmes d'évolutivité dans un grand réseau, car chaque homologue IPsec nécessite des informations de configuration pour chaque homologue avec lequel il établit des connexions sécurisées.

      Chaque paire d'homologues IPsec doit échanger des clés prépartagées pour établir des tunnels sécurisés. Utilisez une méthode sécurisée pour échanger la clé prépartagée avec l'administrateur du site distant.
    - Device Certificate (Certificat de périphérique) : cliquez sur cette option pour utiliser des certificats pour l'authentification entre l'ASA local et l'homologue IPsec distant.

      Vous pouvez gérer efficacement les clés de sécurité utilisées pour établir un tunnel IPsec avec des certificats numériques. Un certificat numérique contient des informations qui identifient un utilisateur ou un périphérique, tel qu'un nom, un numéro de série, une entreprise, un service ou une adresse IP. Un certificat numérique contient également une copie de la clé publique.

      Lorsque deux homologues veulent communiquer, ils échangent des certificats et signent numériquement des données pour s'authentifier mutuellement. Lorsque vous ajoutez un nouvel homologue au réseau, il s'enregistre auprès d'une autorité de certification, et aucun des autres homologues ne nécessite de configuration supplémentaire.
- Méthodes d'authentification IKE version 2
    - Local Pre-shared Key (Clé prépartagée locale) : spécifiez les méthodes d'authentification et les algorithmes de chiffrement IPsec IKEv2.
    - Local Device Certificate (Certificat de périphérique local) : authentifie l'accès VPN au moyen du périphérique de sécurité.
    - Remote Peer Pre-shared Key (Clé prépartagée de l'homologue distant) : saisissez une clé prépartagée pour l'authentification entre l'ASA local et l'homologue IPsec distant.
    - Remote Peer Certificate Authentication (Authentification du certificat de l'homologue distant) : lorsque cette option est cochée, le périphérique homologue est autorisé à utiliser le certificat pour s'authentifier auprès de ce périphérique.

- Encryption Algorithms (Algorithmes de chiffrement) : cet onglet vous permet de choisir les types d'algorithmes de chiffrement utilisés pour protéger les données.
  - IKE Policy (Politique IKE) : spécifiez les méthodes d'authentification IKEv1/IKEv2.
  - IPsec Proposal (Proposition IPsec) : spécifiez les algorithmes de chiffrement IPsec.
- Confidentialité de transmission parfaite
  - Enable Perfect Forwarding Secrecy (PFS) (Activer la confidentialité persistante [PFS]) : spécifiez s'il faut utiliser la confidentialité persistante et la taille des nombres à utiliser pour générer les clés IPsec de phase :2. PFS est un concept cryptographique dans lequel chaque nouvelle clé n'est liée à aucune clé précédente. Dans les négociations IPsec, les clés de phase 2 sont basées sur les clés de phase 1, sauf si le protocole PFS est activé. PFS utilise des techniques Diffie-Hellman pour générer les clés.

    PFS garantit qu'une clé de session dérivée d'un ensemble de clés publiques et privées à long terme ne sera pas compromise si l'une des clés privées est compromise à l'avenir.

    Le protocole PFS doit être activé des deux côtés de la connexion.
  - Groupe Diffie-Hellman : sélectionnez l'identifiant du groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre. La valeur par défaut est Group 14 (Diffie-Hellman 2048 bits).

Exemption NAT

- Exempter l'hôte/le réseau côté ASA de la traduction d'adresses : utiliser la liste déroulante pour choisir un hôte ou un réseau à exclure de la traduction d'adresses.

Assistant VPN Secure Client

Utilisez cet assistant pour configurer l'ASA afin qu'il accepte les connexions VPN du module VPN AnyConnect du client AnyConnect. Cet assistant configure les protocoles IPsec (IKEv2) ou SSL VPN pour un accès complet au réseau. L'ASA télécharge automatiquement le module VPN AnyConnect du client VPN Cisco Secure Client sur le périphérique de l'utilisateur final lorsqu'une connexion VPN est établie.

Identification du profil de connexion

L'identification du profil de connexion est utilisée pour identifier l'ASA auprès des utilisateurs de l'accès à distance :

- Connection Profile Name (Nom du profil de connexion) : fournissez un nom que les utilisateurs d'accès à distance utiliseront pour les connexions VPN.
- VPN Access Interface (Interface d'accès VPN) : choisissez une interface à laquelle les utilisateurs d'accès à distance accéderont pour les connexions VPN.

Protocoles VPN

Précisez le protocole VPN autorisé pour ce profil de connexion.

La valeur par défaut est SSL Secure Client. Si vous activez IPsec comme protocole de tunnel VPN pour le profil de connexion, vous devez également créer et déployer un profil client avec IPsec activé à l'aide de l'éditeur de profils d'ASDM, puis déployer le profil.

Si vous prédéployez le Secure Client au lieu d'utiliser le lancement Web, la première connexion client utilise SSL et reçoit le profil client de l'ASA pendant la session. Pour les connexions ultérieures, le client utilise le protocole spécifié dans le profil, soit SSL ou IPsec. Si vous prédéployez le profil avec IPsec précisé pour le client, la première connexion client utilise IPsec. Pour en savoir plus sur le prédéploiement d'un profil client avec IPsec activé, consultez le *guide d'administration AnyConnect Secure Mobility Client.*

- SSL
- IPsec (IKE v2)
- Device Certificate (Certificat de périphérique) : identifie l'ASA auprès des clients d'accès à distance. Certaines fonctionnalités Secure Client (comme la fonctionnalité permanente et IPsec/IKEv2) nécessitent un certificat de périphérique valide sur l'ASA.
- Manage (Gérer) : choisir **Manage** (Gérer) ouvre la fenêtre Manage Identity Certificates (Gérer les certificats d'identité).
  - Add (Ajouter) : choisissez **Add** (Ajouter) pour ajouter un certificat d'identité et ses détails.
  - Show Details (Afficher les détails) : si vous choisissez un certificat particulier et cliquez sur **Show Details** (Afficher les détails), la fenêtre Certificate Details (Détails du certificat) apparaît et indique à qui le certificat a été délivré et par qui il a été délivré, ainsi que des détails sur son numéro de série, son utilisation, les points de confiance associés, sa période de validité, etc.
  - Delete (Supprimer) : mettez en surbrillance le certificat que vous souhaitez supprimer et cliquez sur **Delete** (Supprimer).
  - Export (Exporter) : mettez le certificat en surbrillance et cliquez sur **Export** (Exporter) pour exporter le certificat vers un fichier avec ou sans phrase secrète de chiffrement.
  - Enroll ASA SSL VPN with Entrust (Inscrire ASA SSL VPN avec Entrust) : permet à votre appareil ASA SSL VPN d'être rapidement opérationnel avec un certificat numérique SSL Advantage d'Entrust.

Images du client

ASA peut charger automatiquement le dernier ensemble Secure Client sur le périphérique client lorsqu'il accède au réseau de l'entreprise. Vous pouvez utiliser une expression régulière pour faire correspondre l'agent utilisateur d'un navigateur à une image. Vous pouvez également réduire le temps de configuration de la connexion en déplaçant l'image utilisée par le système d'exploitation le plus courant qui figure en haut de la liste.

Méthodes d'authentification

Précisez les informations d'authentification sur cet écran.

- AAA server group (Groupe de serveurs AAA) : activez cette option pour permettre à l'ASA de communiquer avec un groupe de serveurs AAA distant afin d'authentifier l'utilisateur. Sélectionnez un groupe de serveurs AAA dans la liste des groupes préconfigurés ou cliquez sur **New** (Nouveau) pour créer un nouveau groupe.

- Local User Database Details (Détails de la base de données des utilisateurs locaux) : ajoutez de nouveaux utilisateurs à la base de données locale stockée sur l'ASA.
  - Username (Nom d'utilisateur) : créez un nom d'utilisateur pour l'utilisateur.
  - Password (Mot de passe) : créez un mot de passe pour l'utilisateur.
  - Confirm Password (Confirmer le mot de passe) : saisissez de nouveau le même mot de passe pour le confirmer.
  - Add/Delete (Ajouter/Supprimer) : ajoutez ou supprimez l'utilisateur de la base de données locale.

Attribution d'adresses client

Indiquez une plage d'adresses IP aux utilisateurs Secure Client distants.

- IPv4 Address Pools (Ensembles d'adresses IPv4) : les clients VPN SSL reçoivent de nouvelles adresses IP lorsqu'ils se connectent à l'ASA. Les connexions sans client ne nécessitent pas de nouvelles adresses IP. Les ensembles d'adresses définissent une plage d'adresses que les clients distants peuvent recevoir. Sélectionnez un ensemble d'adresses IP existant ou cliquez sur **New** (Nouveau) pour créer un nouvel ensemble.

  Si vous choisissez **New** (Nouveau), vous devrez fournir une adresse IP de début, une adresse IP de fin et un masque de sous-réseau.

- IPv6 Address Pool (Ensemble d'adresses IPv6) : sélectionnez un ensemble d'adresses IP existant ou cliquez sur **New** (Nouveau) pour créer un nouvel ensemble.

Remarque Les ensembles d'adresses IPv6 ne peuvent pas être créés pour les profils de connexion IKEv2.

Serveurs de résolution de noms réseau)

Précisez quels noms de domaine sont résolus pour l'utilisateur distant lors de l'accès au réseau interne.

- DNS Servers (Serveurs DNS) : saisissez l'adresse IP du serveur DNS.
- WINS Servers (Serveurs WINS) : saisissez l'adresse IP du serveur WINS.
- Domain Name (Nom de domaine) : saisissez le nom de domaine par défaut.

Exemption NAT

Si la traduction de réseau est activée sur l'ASA, le trafic VPN doit être exempt de cette traduction.

Déploiement Secure Client

Vous pouvez installer le programme Secure Client sur un périphérique client en utilisant l'une des deux méthodes suivantes :

- Web launch (Lancement Web) : le progiciel Secure Client s'installe automatiquement lors de l'accès à l'ASA à l'aide d'un navigateur Web.

Remarque Web launch (Lancement Web) n'est pas pris en charge en mode contexte multiple.

- Pre-deployment (Prédéploiement) : installez manuellement le progiciel Secure Client.

Allow Web Launch (Autoriser le lancement Web) est un paramètre global qui affecte toutes les connexions. Si cette option n'est pas cochée (non autorisée), les connexions SSL Secure Client et les connexions SSL sans client ne fonctionnent pas.

Pour le prédéploiement, l'ensemble de profils disk0:/test2_client_profile.xml contient un fichier .msi, et vous devez inclure ce profil client de l'ASA dans votre progiciel Secure Client afin d'assurer le bon fonctionnement des connexions IPsec.

Assistant d'accès à distance IPsec IKEv1

Remarque Le client VPN Cisco est en fin de vie et n'est plus pris en charge. Vous devez passer au client de Secure Client/AnyConnect.

Utilisez l'assistant d'accès à distance IKEv1 pour configurer l'accès à distance sécurisé pour les clients VPN, tels que les utilisateurs mobiles, et pour identifier l'interface qui se connecte à l'homologue IPsec distant.

- VPN Tunnel Interface (Interface de tunnel VPN) : choisissez l'interface à utiliser pour les clients d'accès à distance. Si l'ASA a plusieurs interfaces, arrêtez maintenant et configurez les interfaces sur l'ASA avant d'exécuter cet assistant.
- Enable inbound IPsec sessions to bypass interface access lists (Activer les sessions IPsec entrantes pour contourner les listes d'accès d'interface) : active les sessions entrantes authentifiées IPsec afin qu'elles soient toujours autorisées par l'ASA (c'est-à-dire sans vérifier les instructions des listes d'accès d'interface). Sachez que les sessions entrantes contournent uniquement les listes de contrôle d'accès de l'interface. Les stratégies de groupe configurées, les utilisateurs et les listes de contrôle d'accès téléchargées s'appliquent toujours.

Client d'accès à distance

Les utilisateurs d'accès à distance de différents types peuvent ouvrir des tunnels VPN vers cet ASA. Choisissez le type de client VPN pour ce tunnel.

- Type de client VPN
  - produit Easy VPN Remote.
  - Client Microsoft Windows utilisant L2TP sur IPsec : spécifiez le protocole d'authentification PPP. Les choix sont PAP, CHAP, MS-CHAP-V1, MS-CHAP-V2 et EAP-PROXY :

    Le PAP transmet un nom d'utilisateur et un mot de passe en clair lors de l'authentification et n'est pas sécurisé.

Avec le protocole CHAP, le client renvoie le [défi plus mot de passe] chiffré, avec un nom d'utilisateur en texte clair en réponse au défi du serveur. Le protocole CHAP est plus sécurisé que le protocole PAP, mais il ne chiffre pas les données.

MS-CHAP, version 1 : similaire à CHAP, mais plus sécurisé, car le serveur stocke et compare uniquement les mots de passe chiffrés plutôt que les mots de passe en clair comme dans CHAP.

MS-CHAP, version 2 : contient des améliorations de sécurité par rapport à MS-CHAP, version 1.

EAP-Proxy : active le protocole EAP qui permet à l'ASA de proxy le processus d'authentification PPP à un serveur d'authentification RADIUS externe.

Si un protocole n'est pas spécifié sur le client distant, ne le spécifiez pas.

- Précisez si le client enverra le nom du groupe de tunnels sous la forme d'un nom d'utilisateur@tunnelgroup.

Méthode d'authentification du client VPN et nom du groupe de tunnels

Utilisez le volet VPN Client Authentication Method and Name (Méthode d'authentification et nom du client VPN) pour configurer une méthode d'authentification et créer une politique de connexion (groupe de tunnels).

- Authentication Method (Méthode d'authentification) : l'homologue du site distant s'authentifie à l'aide d'une clé prépartagée ou d'un certificat.
  - Pre-shared Key (Clé prépartagée) : cliquez pour utiliser une clé prépartagée pour l'authentification entre l'ASA local et l'homologue IPsec distant.

    L'utilisation d'une clé prépartagée est un moyen rapide et facile d'établir la communication avec un nombre limité d'homologues distants et un réseau stable. Cela peut entraîner des problèmes d'évolutivité dans un grand réseau, car chaque homologue IPsec nécessite des informations de configuration pour chaque homologue avec lequel il établit des connexions sécurisées.

    Chaque paire d'homologues IPsec doit échanger des clés prépartagées pour établir des tunnels sécurisés. Utilisez une méthode sécurisée pour échanger la clé prépartagée avec l'administrateur du site distant.

  - re-shared Key (Clé prépartagée) : saisissez une chaîne alphanumérique comprise entre 1 et 128 caractères.

  - Certificate (Certificat) : cliquez pour utiliser des certificats pour l'authentification entre l'ASA local et l'homologue IPsec distant. Pour remplir cette section, vous devez vous être déjà inscrit auprès d'une autorité de certification et avoir téléchargé un ou plusieurs certificats sur l'ASA.

    Vous pouvez gérer efficacement les clés de sécurité utilisées pour établir un tunnel IPsec avec des certificats numériques. Un certificat numérique contient des informations qui identifient un utilisateur ou un périphérique, tel qu'un nom, un numéro de série, une entreprise, un service ou une adresse IP. Un certificat numérique contient également une copie de la clé publique.

    Pour utiliser des certificats numériques, chaque homologue s'inscrit auprès d'une autorité de certification (CA), qui est responsable d'émettre des certificats numériques. Une autorité de certification peut être un tiers de confiance ou une autorité de certification privée que vous établissez au sein de votre organisation.

    Lorsque deux homologues veulent communiquer, ils échangent des certificats et signent numériquement des données pour s'authentifier mutuellement. Lorsque vous ajoutez un nouvel

homologue au réseau, il s'enregistre auprès d'une autorité de certification, et aucun des autres homologues ne nécessite de configuration supplémentaire.

Algorithme de signature de certificat : affiche l'algorithme de signature des certificats numériques, rsa-sig pour RSA.

- Tunnel Group Name (Nom du groupe de tunnels) : saisissez un nom pour créer l'enregistrement qui contient les politiques de connexion de tunnel pour cette connexion IPsec. Une politique de connexion peut préciser les serveurs d'authentification, d'autorisation et de comptabilité, une Stratégie de groupe par défaut et des attributs IKE. Une politique de connexion que vous configurez avec cet assistant VPN spécifie une méthode d'authentification et utilise la stratégie de groupe par défaut de l'ASA.

Authentification du client

Utilisez le volet Client Authentication (authentification du client) pour choisir la méthode par laquelle l'ASA authentifie les utilisateurs distants. Sélectionnez l'une des options suivantes :

- Authenticate using the local user database (Authentifier à l'aide de la base de données d'utilisateurs locaux) : cliquez pour utiliser l'authentification interne à l'ASA. Utilisez cette méthode pour les environnements avec un nombre faible et stable d'utilisateurs. Le volet suivant vous permet de créer des comptes sur l'ASA pour les utilisateurs individuels.
- Authenticate using an AAA server group (Authentifier à l'aide d'un groupe de serveurs AAA) : cliquez pour utiliser un groupe de serveurs externe pour l'authentification des utilisateurs distants.
  - AAA Server Group Name (Nom du groupe de serveurs AAA) : choisissez un groupe de serveurs AAA configuré précédemment.
  - New... (Nouveau...) : cliquez pour configurer un nouveau groupe de serveurs AAA.

Comptes utilisateurs

Utilisez le volet User Accounts (Comptes d'utilisateurs) pour ajouter de nouveaux utilisateurs à la base de données d'utilisateurs interne de l'ASA à des fins d'authentification.

Ensemble d'adresses

Utilisez le volet Address Pool (Ensemble d'adresses) pour configurer un ensemble d'adresses IP locales que l'ASA attribue aux clients VPN distants.

- Nom du groupe de tunnels : affiche le nom du profil de connexion (groupe de tunnels) auquel cet ensemble d'adresses s'applique. Vous définissez ce nom dans le volet VPN Client and Authentication Method (Client VPN et méthode d'authentification) (étape 3).
- Nom de l'ensemble : sélectionnez un identifiant descriptif pour l'ensemble d'adresses.
- New... (Nouveau...) : cliquez pour configurer un nouvel ensemble d'adresses.
- Adresse de début de plage : saisissez l'adresse IP de début dans l'ensemble d'adresses.
- Adresse de fin de plage : saisissez l'adresse IP de fin dans l'ensemble d'adresses.
- Masque de sous-réseau : (facultatif) choisissez le masque de sous-réseau pour ces adresses IP.

Attributs transmis au client (facultatif)

Utilisez le volet Attributes Pushed to Client (Attributs transmis au client) (facultatif) pour que l'ASA transmette des informations sur les serveurs DNS et WINS et le nom de domaine par défaut aux clients d'accès à distance.

- Groupe de tunnels : affiche le nom de la politique de connexion à laquelle l'ensemble d'adresses s'applique. Vous définissez ce nom dans le volet VPN Client Name and Authentication Method (Nom du client VPN et méthode d'authentification).
- Serveur DNS principal : saisissez l'adresse IP du serveur DNS principal.
- Serveur DNS secondaire : saisissez l'adresse IP du serveur DNS secondaire.
- Serveur WINS principal : saisissez l'adresse IP du serveur WINS principal.
- Serveur WINS secondaire : saisissez l'adresse IP du serveur WINS secondaire.
- Nom de domaine par défaut : saisissez le nom de domaine par défaut.

Politique IKE

IKE, également appelé protocole Internet Security Association and Key Management (ISAKMP), est le protocole de négociation qui permet à deux hôtes de se mettre d'accord sur la façon de créer une association de sécurité IPsec. Chaque négociation IKE est divisée en deux sections appelées Phase 1 et Phase 2. La phase 1 crée le premier tunnel, qui protège les messages de négociation IKE ultérieurs. La phase 2 crée le tunnel qui protège les données.

Utilisez le volet IKE Policy (Politique IKE) pour définir les conditions des négociations IKE de phase 1, qui comprennent une méthode de chiffrement pour protéger les données et assurer la confidentialité, une méthode d'authentification pour assurer l'identité des homologues et un groupe Diffie-Hellman pour établir la force de l'algorithme de détermination de la clé de chiffrement. L'ASA utilise cet algorithme pour déduire les clés de chiffrement et de hachage.

- Chiffrement : sélectionnez l'algorithme de chiffrement symétrique que l'ASA utilise pour établir le SA de phase 1 qui protège les négociations de phase 2. L'ASA prend en charge les algorithmes de chiffrement suivants :

Algorithme	Explication
DES	Standard de chiffrement des données. Utilise une clé de 56 bits.
3DES	Triple DES. Effectue le chiffrement à trois reprises à l'aide d'une clé de 56 bits.
AES-128	Standard de chiffrement avancé (AES). Utilise une clé de 128 bits.
AES-192	AES à l'aide d'une clé de 192 bits.
AES-256	AES à l'aide d'une clé de 256 bits.

  La valeur par défaut, 3DES, est plus sécurisée que DES, mais nécessite plus de traitement pour le chiffrement et le déchiffrement. De même, les options AES offrent une sécurité renforcée, mais nécessitent également un traitement renforcé.

- Authentification : choisissez l'algorithme de hachage utilisé pour l'authentification et assurer l'intégrité des données. La valeur par défaut est SHA. MD5 a un condensé plus petit et est considéré comme

légèrement plus rapide que SHA. Il y a eu une démonstration d'attaque réussie (mais très difficile) contre MD5. Cependant, la version du code d'authentification du message Keyed-Hash (HMAC) utilisée par l'ASA empêche cette attaque.

- Groupe Diffie-Hellman : choisissez l'identifiant du groupe Diffie-Hellman, que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre. Le groupe DH par défaut, groupe 14 (2 048 bits), est considéré comme plus sécurisé que les groupes 2 et 5.

Paramètres d'IPsec (facultatif)

Utilisez le volet IPsec Settings (Paramètres d'IPsec) (facultatif) pour identifier les hôtes ou les réseaux locaux qui ne nécessitent pas de traduction d'adresses. Par défaut, l'ASA cache les adresses IP réelles des hôtes internes et des réseaux des hôtes externes en utilisant la traduction d'adresses réseau (NAT) dynamique ou statique. La NAT réduit les risques d'attaque par des hôtes externes non fiables, mais peut être inappropriée pour ceux qui ont été authentifiés et protégés par VPN.

Par exemple, un hôte interne utilisant la NAT dynamique voit son adresse IP traduite en la faisant correspondre à une adresse sélectionnée au hasard dans un ensemble. Seule l'adresse traduite est visible à l'extérieur. Les clients VPN distants qui tentent d'atteindre ces hôtes en envoyant des données à leurs adresses IP réelles ne peuvent pas se connecter à ces hôtes, sauf si vous configurez une règle d'exemption NAT.

Remarque Si vous souhaitez que tous les hôtes et les réseaux soient exemptés de la NAT, ne configurez rien dans ce volet. Si vous avez même une entrée, tous les autres hôtes et réseaux sont soumis à la NAT.

- Interface : choisissez le nom de l'interface qui se connecte aux hôtes ou aux réseaux que vous avez sélectionnés.
- Réseaux exemptés : sélectionnez l'adresse IP de l'hôte ou du réseau que vous souhaitez exempter du réseau de l'interface choisie.
- Enable split tunneling (Activer la tunnellisation fractionnée) : sélectionnez cette option pour que le trafic des clients d'accès à distance destiné à l'Internet public soit envoyé non chiffré. La tunnellisation fractionnée entraîne le chiffrement du trafic vers les réseaux protégés, tandis que le trafic vers des réseaux non protégés n'est pas chiffré. Lorsque vous activez la tunnellisation fractionnée, l'ASA envoie une liste d'adresses IP au client VPN distant après l'authentification. Le client VPN distant chiffre le trafic vers les adresses IP qui se trouvent derrière l'ASA. Tout autre trafic circule non chiffré directement sur Internet, sans faire appel à l'ASA.
- Enable Perfect Forward Secrecy (PFS) (Activer la confidentialité de transmission parfaite [PFS]) : spécifiez s'il faut utiliser la confidentialité de transmission parfaite et la taille des nombres à utiliser dans la génération des clés IPsec de phase 2. PFS est un concept cryptographique dans lequel chaque nouvelle clé n'est liée à aucune clé précédente. Dans les négociations IPsec, les clés de phase 2 sont basées sur les clés de phase 1, sauf si le protocole PFS est activé. PFS utilise des techniques Diffie-Hellman pour générer les clés.

  PFS garantit qu'une clé de session dérivée d'un ensemble de clés publiques et privées à long terme ne sera pas compromise si l'une des clés privées est compromise à l'avenir.

  Le protocole PFS doit être activé des deux côtés de la connexion.

  - Groupe Diffie-Hellman : sélectionnez l'identifiant du groupe Diffie-Hellman que les deux homologues IPsec utilisent pour obtenir un secret partagé sans le transmettre l'un à l'autre. Le groupe DH par défaut, groupe 14 (2 048 bits), est considéré comme plus sécurisé que les groupes 2 et 5.

Résumé

Lorsque vous êtes satisfait de la configuration, cliquez sur **Finish** (Terminer). ASDM enregistre la configuration LAN à LAN. Après avoir cliqué sur **Finish** (Terminer), vous ne pouvez plus utiliser l'assistant VPN pour modifier cette configuration. Utilisez ASDM pour modifier et configurer les fonctionnalités avancées.

Assistant d'accès à distance IPsec IKEv2

Utilisez l'assistant d'accès à distance IKEv2 pour configurer l'accès à distance sécurisé pour les clients VPN, tels que les utilisateurs mobiles, et pour identifier l'interface qui se connecte à l'homologue IPsec distant.

Identification du profil de connexion

Saisissez un **nom de profil de connexion** et choisissez l'**interface d'accès VPN** qui sera utilisée pour l'accès à distance IPsec IKEv2.

- Nom du profil de connexion : saisissez un nom pour créer l'enregistrement qui contient les politiques de connexion de tunnel pour cette connexion IPsec. Une politique de connexion peut préciser les serveurs d'authentification, d'autorisation et de comptabilité, une Stratégie de groupe par défaut et des attributs IKE. Une politique de connexion que vous configurez avec cet assistant VPN spécifie une méthode d'authentification et utilise la stratégie de groupe par défaut de l'ASA.
- Interface d'accès VPN : choisissez l'interface qui établit un tunnel sécurisé avec l'homologue IPsec distant. Si l'ASA dispose de plusieurs interfaces, vous devez planifier la configuration VPN avant d'exécuter cet assistant, en identifiant l'interface à utiliser pour chaque homologue IPsec distant avec lequel vous prévoyez d'établir une connexion sécurisée.

Page d'authentification IPsec basée sur les normes (IKEv2)

Authentification d'homologue IKE : l'homologue du site distant s'authentifie à l'aide d'une clé prépartagée, d'un certificat ou de l'authentification d'homologue à l'aide du protocole EAP.

- Clé prépartagée : saisissez une chaîne alphanumérique comprise entre 1 et 128 caractères.

  L'utilisation d'une clé prépartagée est un moyen rapide et facile d'établir la communication avec un nombre limité d'homologues distants et un réseau stable. Cela peut entraîner des problèmes d'évolutivité dans un grand réseau, car chaque homologue IPsec nécessite des informations de configuration pour chaque homologue avec lequel il établit des connexions sécurisées.

  Chaque paire d'homologues IPsec doit échanger des clés prépartagées pour établir des tunnels sécurisés. Utilisez une méthode sécurisée pour échanger la clé prépartagée avec l'administrateur du site distant.

- Activer l'authentification des certificats : vous permet d'utiliser des certificats pour l'authentification si cette option est cochée.
- Activer l'authentification homologue à l'aide d'EAP : vous permet d'utiliser EAP pour l'authentification si cette option est cochée. Vous devez utiliser des certificats pour l'authentification locale si vous cochez cette case.
- Envoyer une demande d'identité EAP au client : vous permet d'envoyer une demande EAP d'authentification au client VPN d'accès à distance.

Mobike RRC

- Activer la vérification de la routabilité du retour pour mobike : activer la vérification de la routabilité du retour pour les modifications d'adresses IP dynamiques dans les associations de sécurité IKE/IPSEC sur lesquelles mobike est activé.

Authentification IKE

- Activez l'authentification locale et sélectionnez une clé prépartagée ou un certificat
  - Clé prépartagée : saisissez une chaîne alphanumérique comprise entre 1 et 128 :caractères.
  - Certificat : cliquez sur pour utiliser des certificats pour l'authentification entre l'ASA local et l'homologue IPsec distant. Pour remplir cette section, vous devez vous être déjà inscrit auprès d'une autorité de certification et avoir téléchargé un ou plusieurs certificats sur cette dernière.

    Vous pouvez gérer efficacement les clés de sécurité utilisées pour établir un tunnel IPsec avec des certificats numériques. Un certificat numérique contient des informations qui identifient un utilisateur ou un périphérique, tel qu'un nom, un numéro de série, une entreprise, un service ou une adresse IP. Un certificat numérique contient également une copie de la clé publique.

    Pour utiliser des certificats numériques, chaque homologue s'inscrit auprès d'une autorité de certification (CA), qui est responsable d'émettre des certificats numériques. Une autorité de certification peut être un tiers de confiance ou une autorité de certification privée que vous établissez au sein de votre organisation.

    Lorsque deux homologues veulent communiquer, ils échangent des certificats et signent numériquement des données pour s'authentifier mutuellement. Lorsque vous ajoutez un nouvel homologue au réseau, il s'enregistre auprès d'une autorité de certification, et aucun des autres homologues ne nécessite de configuration supplémentaire.

Méthodes d'authentification

Seule l'authentification Radius est prise en charge pour l'accès à distance IPsec IKEv2.

- Groupe de serveurs AAA : choisissez un groupe de serveurs AAA configuré précédemment.
- Nouveau : cliquez sur pour configurer un nouveau groupe de serveurs AAA.
- Détails du groupe de serveur AAA : utilisez cette zone pour modifier le groupe de serveur AAA si vous le souhaitez.

Attribution d'adresses client

Créez ou sélectionnez des ensembles d'adresses IPv4 et IPv6. Les clients d'accès à distance se verront attribuer des adresses issues de pools IPv4 ou IPv6. Les adresses IPv4 prévalent si les deux sont configurées. Consultez *Configuration des ensembles d'adresses IP locales* pour en savoir plus.

Serveurs de résolution de noms réseau

Précisez comment les noms de domaine sont résolus pour l'utilisateur distant lors de l'accès au réseau interne.

- Serveurs DNS : saisissez l'adresse IP des serveurs DNS.
- Serveurs WINS : saisissez l'adresse IP des serveurs WINS.
- Nom de domaine par défaut : saisissez le nom de domaine par défaut.

Exemption NAT

- Exempter le trafic VPN de la traduction d'adresses réseau : si la NAT est activée sur l'appareil de sécurité adaptable Cisco, cela doit être vérifié.

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.