VPN de site à site

À propos du VPN de site à site

Le VPN site à site Cisco Secure Firewall Threat Defense prend en charge les fonctions suivantes :

- Protocoles IPsec IKEv1 et IKEv2.
- Certificats et Clés prépartagées ou manuelles pour l'authentification.
- IPv4 et IPv6 Toutes les combinaisons d’éléments internes et externes sont prises en charge.
- Les topologies VPN de site à site IPsec IKEv2 fournissent des paramètres de configuration conformes aux certifications de sécurité.
- Interfaces statiques et dynamiques.
- Environnements à haute disponibilité pour centre de gestion et défense contre les menaces .
- Le VPN est alerté lorsque le tunnel tombe en panne.

- Statistiques de tunnellisation disponibles à l'aide de l'interface de ligne de commande unifiée défense contre les menaces .
- Configuration de secours homologues Kev1 et IKEv2 pour l'extranet point à point et VPN en étoile.
- Périphérique extranet comme concentrateur dans les déploiements en étoile.
- Adresse IP dynamique pour un jumelage de point terminal géré avec un périphérique extranet dans les déploiements « point à point ».
- Adresse IP dynamique pour le périphérique extranet comme point terminal.
- Hub comme extranet dans les déploiements « en étoile ».

Topologie VPN

Pour créer une nouvelle topologie VPN de site à site, vous devez préciser un nom unique, un type de topologie, choisir la version IKE qui est utilisée pour IPsec IKEv1 ou IKEv2, ou les deux. En outre, pour déterminer votre méthode d'authentification. Une fois la configuration terminée, vous déployez la topologie sur les périphériques défense contre les menaces . Cisco Secure Firewall Management Center configure les VPN de site à site sur les périphériques défense contre les menaces .

Vous pouvez choisir parmi trois types de topologies, contenant un ou plusieurs tunnels VPN :

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

IPsec et IKE

Dans Cisco Secure Firewall Management Center, les VPN de site à site sont configurés en fonction des politiques IKE et des propositions IPsec qui sont affectées aux topologies VPN. Les politiques et les propositions sont des ensembles de paramètres qui définissent les caractéristiques d'un VPN de site à site, tels que les protocoles de sécurité et les algorithmes utilisés pour sécuriser le trafic dans un tunnel IPsec. Plusieurs types de politiques peuvent être nécessaires pour définir une image de configuration complète qui peut être affectée à une topologie VPN.

Authentification

Pour l'authentification des connexions VPN, configurez une clé prépartagée dans la topologie ou un point de confiance sur chaque périphérique. Les clés prépartagées permettent de partager une clé secrète, utilisée pendant la phase d'authentification IKE, entre deux homologues. 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.

Périphériques extranet

Chaque type de topologie peut inclure des périphériques extranet, des périphériques que vous ne gérez pas dans centre de gestion. Notamment :

- les périphériques Cisco pris en charge par Cisco Secure Firewall Management Center, mais dont votre entreprise n'est pas responsable. Tels que des réseaux en étoile dans des réseaux gérés par d'autres organisations au sein de votre entreprise, ou une connexion au réseau d'un fournisseur de services ou d'un partenaire.
- Périphériques autres que Cisco Vous ne pouvez pas utiliser Cisco Secure Firewall Management Center pour créer et déployer des configurations sur des périphériques autres que ceux de Cisco.

Ajouter des périphériques autres que ceux de Cisco, ou des périphériques Cisco non gérés par Cisco Secure Firewall Management Center, à une topologie VPN en tant que périphériques « extranet ». Précisez également l'adresse IP de chaque périphérique distant.

Directives et limites du VPN site à site Cisco Secure Firewall Threat Defense

- Le VPN de site à site prend en charge les interfaces de zone ECMP.
- Vous devez configurer tous les nœuds dans une topologie avec une ACL de chiffrement ou un réseau protégé. Vous ne pouvez pas configurer une topologie avec une liste de contrôle d'accès de chiffrement sur un nœud et un réseau protégé sur un autre.
- Vous pouvez configurer une connexion VPN sur plusieurs domaines en utilisant un homologue extranet pour le point terminal qui ne fait pas partie du domaine actuel.
- Vous pouvez sauvegarder les VPN Défense contre les menaces à l'aide de la commande centre de gestion.
- IKEv1 ne prend pas en charge les périphériques conformes CC/UCAPL. Nous vous recommandons d'utiliser IKEv2 pour ces périphériques.
- Vous ne pouvez pas déplacer une topologie VPN entre des domaines.
- Le VPN ne prend pas en charge les objets réseau avec une option de « plage ».
- Les VPN Défense contre les menaces ne prennent actuellement pas en charge l'exportation au format PDF et la comparaison des politiques.
- Il n'y a pas d'option de modification par tunnel ou par appareil pour les VPN défense contre les menaces , vous pouvez modifier uniquement l'ensemble de la topologie.
- centre de gestion ne vérifie pas le contrôle de l'adresse d'interface de périphérique pour le mode de transport lorsque vous sélectionnez une ACL de chiffrement.
- Il n'y a pas de prise en charge pour la génération automatique d'ACE miroir. La génération d'ACE miroir pour l'homologue est un processus manuel de chaque côté.
- Avec la liste de contrôle d'accès chiffrée, centre de gestion prend uniquement en charge le VPN point à point et ne prend pas en charge les événements d'intégrité du tunnel.
- Chaque fois que les ports IKE 500/4500 sont utilisés ou qu'il y a des traductions PAT actives, vous ne pouvez pas configurer un VPN de site à site sur les mêmes ports, car il ne parvient pas à démarrer le service sur ces ports.
- L'état du tunnel n'est pas mis à jour en temps réel, mais à un intervalle de cinq minutes dans centre de gestion.
- Vous ne pouvez pas utiliser le caractère « » (guillemets doubles) dans les clés prépartagées. Si vous avez utilisé « » dans une clé pré-partagée, assurez-vous de modifier le caractère.

Types de topologies VPN de site à site

Topologie de VPN de site à site	Description	Autres renseignements
VPN basé sur le routage	Sécurise le trafic de façon dynamique entre les homologues en fonction du routage sur les interfaces de tunnel virtuelles (VTI).	Créer un VPN de site à site basé sur le routage, à la page 27
VPN basé sur des politiques	Configure un trafic sécurisé entre homologues au sein d'un réseau sur la base d'une politique statique utilisant des réseaux protégés.	Configurer un VPN de site à site basé sur une politique, à la page 5
Topologie du service d’accès sécurisé en périphérie (SASE)	Configure un tunnel IPsec IKEv2 à partir d’un périphérique de défense contre les menaces vers une passerelle Internet sécurisée Umbrella (SIG). Ce tunnel achemine tout le trafic Internet à Cisco Umbrella SIG pour l’inspection et le filtrage.	Configurer un tunnel SASE pour Umbrella, à la page 50

Exigences et prérequis pour les VPN de site à site

Prise en charge des modèles

Défense contre les menaces

Domaines pris en charge

Domaine enfant

Rôles utilisateur

Admin

Gérer un VPN de site à site

La page VPN de site à site fournit un instantané des tunnels VPN de site à site. Vous pouvez afficher l’état des tunnels et les filtrer en fonction du périphérique, de la topologie ou du type de tunnel. La page répertorie 20 topologies par page et vous pouvez naviguer entre les pages pour afficher plus de détails sur la topologie. Vous pouvez cliquer sur chaque topologie VPN pour la développer et afficher les détails des points terminaux.

Avant de commencer

Pour l'authentification de certificats de votre VPN de site à site, vous devez préparer les périphériques en attribuant des points de confiance, comme décrit dans la section Certificats.

Procédure

Sélectionnez **Devices > VPN > Site To Site** pour gérer vos configurations et vos déploiements de VPN de site à site Firepower Threat Defense.

La page répertorie les topologies des VPN de site à site et indique l'état des tunnels à l'aide de codes de couleur :

- Actif (vert) : tunnel IPsec actif.
- Inconnu (orange) : aucun événement d'établissement de tunnel n'a encore été reçu du périphérique.
- Désactivé (rouge) : aucun tunnel IPsec actif.
- Déploiement en attente : la topologie n'a pas encore été déployée sur le périphérique.

Choisissez l'une des opérations suivantes :

- **Refresh** (actualiser) : pour afficher l'état mis à jour des VPN.
- **Add** (ajouter) : pour créer de nouveaux VPN de site à site basés sur la politique ou le routage.
- **Edit** (modifier) : modifiez les paramètres d'une topologie VPN existante.

  Remarque Vous ne pouvez pas modifier le type de topologie après l'avoir enregistré pour la première fois. Pour modifier le type de topologie, supprimez-la et créez-en une nouvelle.

  Deux utilisateurs ne doivent pas modifier la même topologie simultanément; cependant, l'interface Web n'interdit pas la modification simultanée.

- **Delete** (supprimer) : pour supprimer un déploiement VPN, cliquez sur **Supprimer** ( ).
- Deploy—Choose (déployer, choisir) **Deploy (déployer)** > **Deployment (déploiement)**; voir Déployer les modifications de configuration.

  Remarque Certains paramètres VPN ne sont validés que lors du déploiement. Assurez-vous de vérifier que votre déploiement a réussi.

Configurer un VPN de site à site basé sur une politique

Procédure

Étape 1 Sélectionner **Périphériques > Site à site**. Cliquez ensuite sur **+ VPN de site à site** ou modifiez une topologie VPN répertoriée.

Étape 2 Saisissez un **nom de topologie** unique. Nous vous recommandons de nommer votre topologie pour indiquer qu'il s'agit d'un VPN défense contre les menaces , ainsi que son type de topologie.

Étape 3 Cliquez sur **Policy Based (Crypto Map)** (Basé sur la politique (Carte de chiffrement) pour configurer un VPN de site à site.

Étape 4 Choisir la **topologie de réseau** pour ce VPN.

Étape 5 Choisissez les versions IKE à utiliser pendant les négociations IKE. **IKEv1** ou **IKEv2**.

La valeur par défaut est IKEv2. Sélectionner l'une ou l'autre des options ou les deux, le cas échéant; sélectionnez IKEv1 si un périphérique de la topologie ne prend pas en charge IKEv2.

Vous pouvez également configurer un homologue de sauvegarde pour les VPN extranet point à point. Pour obtenir plus de renseignements, consultez Options de point terminal VPN Défense contre les menaces, à la page 7.

Étape 6 Obligatoire : Ajoutez des points terminaux pour ce déploiement VPN en cliquant sur **Ajouter** (+) pour chaque nœud de la topologie.

Configurez chaque champ de point terminal comme décrit dans Options de point terminal VPN Défense contre les menaces, à la page 7.

- Pour Point à point, configurez le **nœud A** et le **nœud B**.
- Pour Hub and Spoke, configurer un **nœud** de concentrateur et des **nœuds en étoile**
- Pour un maillage complet, configurer plusieurs **nœuds**

Étape 7 (Facultatif) Spécifiez des options IKE autres que celles par défaut pour ce déploiement, comme décrit dans la section Options IKE VPN Défense contre les menaces, à la page 10

Étape 8 (Facultatif) Spécifiez des options IPsec autres que celles par défaut pour ce déploiement, comme décrit dans Options IPsec VPN Défense contre les menaces, à la page 13

Étape 9 (Facultatif) Précisez des options avancées autres que celles par défaut pour ce déploiement, comme décrit dans Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 16.

Étape 10 Cliquez sur **Save** (enregistrer).
Les points terminaux sont ajoutés à votre configuration.

Prochaine étape

Déployer les changements de configuration.

Remarque Certains paramètres VPN ne sont validés que lors du déploiement. Assurez-vous de vérifier que votre déploiement a réussi.

Si vous recevez une alerte que votre tunnel VPN est inactif même lorsque la session VPN est active, suivez les instructions de dépannage VPN pour vérifier et vous assurer que votre VPN est actif.

Options de point terminal VPN Défense contre les menaces

Chemin de navigation

Périphériques > Site à site. Cliquez ensuite sur **+ VPN de site à site** ou modifiez une topologie VPN répertoriée. Cliquez sur l'onglet **Point terminal**.

Champs

Périphérique

Choisissez un nœud de point terminal pour votre déploiement :

- Un périphérique défense contre les menaces géré par ce centre de gestion
- Un conteneur défense contre les menaces à haute disponibilité géré par ce centre de gestion
- Un périphérique **extranet**, tout périphérique (Cisco ou tiers) non géré par ce centre de gestion.

Nom de l'appareil

Pour les périphériques extranet uniquement, attribuez un nom à ce périphérique. Nous vous recommandons de le nommer de manière à ce qu'il puisse être identifié comme périphérique non géré.

Interface

Si vous avez choisi un périphérique géré comme point terminal, choisissez une interface sur ce périphérique géré.

Pour les déploiements « point à point », vous pouvez également configurer un point terminal avec une interface dynamique. Un point terminal doté d'une interface dynamique ne peut être jumelé qu'avec un périphérique extranet et ne peut pas être jumelé avec un point terminal, qui a un périphérique géré.

Vous pouvez configurer les interfaces de périphériques dans **Devices** > **Device Management** > **Add/Edit device** > **Interfaces** (Périphériques > Gestion des périphériques > Ajouter/Modifier un périphérique > interfaces).

Adresse IP

- Si vous choisissez un périphérique extranet, un périphérique **non** géré par centre de gestion, spécifiez une adresse IP pour le point terminal.

  Pour un périphérique extranet, sélectionnez **Statique** et spécifiez une adresse IP, ou sélectionnez **Dynamique** pour autoriser les périphériques extranet dynamiques.

- Si vous avez choisi un périphérique géré comme point terminal, choisissez une adresse IPv4 unique ou plusieurs adresses IPv6 dans la liste déroulante. Ces adresses IP sont déjà affectées à cette interface sur le périphérique géré.
- Tous les points terminaux d'une topologie doivent avoir le même schéma d'adressage IP. Les tunnels IPv4 peuvent acheminer le trafic IPv6 et inversement. Les réseaux protégés définissent le schéma d'adressage utilisé par le trafic en tunnel.
- Si le périphérique géré est un conteneur à haute disponibilité, choisissez dans une liste d'interfaces.

Cette adresse IP est privée

Cochez la case si le point terminal se trouve derrière un pare-feu avec traduction d'adresses réseau (NAT).

Remarque Utilisez cette option uniquement lorsque l'homologue est géré par le même centre de gestion et n'utilisez pas cette option si l'homologue est un périphérique extranet.

Adresse IP publique

Si vous avez coché la case **Cette adresse IP est privée**, spécifiez une adresse IP publique pour le pare-feu. Si le point terminal est un répondeur, spécifiez cette valeur.

Type de connexion

Précisez la négociation autorisée comme étant bidirectionnelle, avec réponse seulement ou avec origine seulement. Les combinaisons prises en charge pour le type de connexion sont les suivantes :

Tableau 1 : Associations de types de connexion prises en charge

Nœud distant	Nœud central
Origine seulement	Avec réponse seulement
Bidirectionnel	Avec réponse seulement
Bidirectionnel	Bidirectionnel

Carte de certificat

Choisissez un objet de correspondance de certificat préconfiguré ou cliquez sur **Ajouter** (+) pour ajouter un objet de correspondance de certificat. La carte de certificats définit les informations nécessaires dans le certificat client reçu pour être valide pour la connectivité VPN. Consultez Objets carte de certificat pour en savoir plus.

Réseaux protégés

Mise en garde Topologie en étoile : pour éviter une perte de trafic pour une carte de chiffrement dynamique, veillez à ne pas sélectionner le réseau protégé *Tout* pour les deux points terminaux.

Si le réseau protégé est configuré comme *tout*, sur les deux terminaux, la liste de contrôle d'accès de chiffrement qui fonctionne sur le tunnel n'est pas générée.

Définit les réseaux protégés par ce point terminal VPN. Sélectionnez les réseaux dans la liste des sous-réseaux et des adresses IP qui définissent les réseaux protégés par ce point terminal. Cliquez sur **Ajouter** (+) pour effectuer une sélection parmi les objets réseau disponibles ou ajouter de nouveaux objets réseau. Consultez Création d'objets réseau. Les listes de contrôle d'accès sont générées à partir des choix effectués ici.

- **Sous-réseau/adresse IP (réseau)** : les points terminaux VPN ne peuvent pas avoir la même adresse IP et les réseaux protégés dans une paire de points terminaux VPN ne peuvent pas se chevaucher. Si les réseaux protégés d'un terminal contiennent des entrées IPv4 ou IPv6, le réseau protégé de l'autre terminal doit avoir au moins une entrée du même type (IPv4 ou IPv6). Si ce n'est pas le cas, l'adresse IP de l'autre point terminal doit être du même type et ne pas se chevaucher avec les entrées du réseau protégé. (Utilisez les blocs d'adresses CIDR /32 pour IPv4 et les blocs d'adresses CIDR /128 pour IPv6.) Si ces deux vérifications échouent, la paire de points terminaux n'est pas valide.

Remarque Par défaut, **l'injection de route inverse** est activée dans Cisco Secure Firewall Management Center.

Le sous-réseau/l'adresse IP (réseau) demeure la sélection par défaut.

Lorsque vous avez sélectionné Réseaux protégés comme *Tout* et observé l'abandon du trafic de routage par défaut, désactivez l'injection de routage inverse. Choisissez **VPN > Site à site** > Modifier un VPN > **IPsec** > **Activer l'injection de route inverse**. Déployez les modifications de configuration pour supprimer la route inverse définie (injection de route inverse) de la configuration de la carte de chiffrement et supprimez la route inverse annoncée par le VPN qui entraîne l'abandon du trafic du tunnel inverse.

- **Liste d'accès (étendue)** : une liste d'accès étendue permet de contrôler le type de trafic qui sera accepté par ce point terminal, comme le trafic GRE ou OSPF. Le trafic peut être limité par l'adresse ou le port. Cliquez sur **Ajouter** (+) pour ajouter des objets de liste de contrôle d'accès.

Remarque La liste de contrôle d'accès est prise en charge uniquement dans la topologie point à point.

Paramètres avancés

Enable Dynamic Reverse Route Injection : L'injection de routage inverse (RRI) permet d'insérer automatiquement des routes dans le processus de routage pour les réseaux et les hôtes protégés par un point de terminaison de tunnel distant. Les routes RRI dynamiques sont créées uniquement lors de l'établissement réussi d'associations de sécurité IPsec (SA).

Remarque

- La RRI dynamique est prise en charge uniquement sur IKEv2, et non prise en charge sur IKEv1 ou IKEv1 + IKEv2.
- L'adresse RRI dynamique n'est pas prise en charge sur l'homologue d'origine uniquement, la topologie à maillage complet et l'homologue extranet.
- Dans le mode point à point, un RRI dynamique peut être activé pour un seul homologue.
- Dans le réseau en étoile, le RRI dynamique ne peut être activé que pour un des points terminaux.
- RRI dynamique ne peut pas être combiné avec une carte de chiffrement dynamique.

Send Local Identity to Peers (envoyer l'identité locale aux homologues) : sélectionnez cette option pour envoyer des informations d'identité locale au périphérique homologue. Sélectionnez l'une des **configurations d'identité locale** suivantes dans la liste et configurez l'identité locale :

- **IP address** : utilisez l'adresse IP de l'interface pour l'identité.
- **Auto** : utilisez l'adresse IP pour la clé pré-partagée et le DN du certificat pour les connexions basées sur des certificats.

- **Email ID** (ID de courriel) : précisez l'ID de courriel à utiliser pour l'identité. L'identifiant de courriel peut comporter jusqu'à 127 caractères.
- **Hostname** (nom d'hôte) : utilisez le nom d'hôte complet.
- **Key ID** (ID de clé) : spécifiez l'ID de clé à utiliser pour l'identité. L'ID de clé doit comporter moins de 65 caractères.

L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels. L'identité unique permet à défense contre les menaces d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à Cisco Umbrella Secure Internet Gateway (SIG).

Pour en savoir plus sur la configuration d'un ID de tunnel unique sur Umbrella, consultez **le Guide de l'utilisateur de Cisco Umbrella SIG**.

VPN Filter (filtre VPN) : sélectionnez une liste d'accès étendue dans la liste ou cliquez sur **Add** (ajouter) pour créer un nouvel objet de liste d'accès étendue afin de filtrer le trafic VPN de site à site.

Le filtre VPN offre plus de sécurité et filtre les données VPN de site à site à l'aide d'une liste d'accès étendue. L'objet de liste d'accès étendue sélectionné pour le filtre VPN vous permet de filtrer le trafic pré chiffré avant d'entrer dans le tunnel VPN et le trafic déchiffré qui sort du tunnel VPN. L'option **sysopt permit-vpn**, lorsqu'elle est activée, contourne les règles de politique de contrôle d'accès pour le trafic provenant du tunnel VPN. Lorsque l'option **sysopt permit-vpn** est activée, le filtre VPN aide à identifier et à filtrer le trafic VPN de site à site.

Remarque Le filtre VPN est pris en charge uniquement dans les topologies point à point et en étoile. Elle n'est pas prise en charge sur la topologie maillée.

Pour la topologie en étoile, vous pouvez choisir de remplacer le filtre VPN du concentrateur sur les points terminaux en étoile au cas où un filtre VPN différent devrait être activé sur un tunnel spécifique.

Sélectionnez l'option **Remplacer le filtre VPN sur le concentrateur** pour remplacer le filtre VPN du concentrateur sur les satellites. Sélectionnez l'objet de liste d'accès étendu **Remote VPN Filter** (Filtre VPN à distance) ou créez une liste d'accès à remplacer.

Remarque Pour un périphérique extranet en étoile, seule la fonction **Remplacer le filtre VPN du concentrateur** est disponible.

Pour plus d'informations sur sysopt permit-VPN, consultez Options avancées de tunnel de VPN de site à site Défense contre les menaces, à la page 18.

Options IKE VPN Défense contre les menaces

Pour les versions d'IKE que vous avez choisies pour cette topologie, spécifiez les **paramètres IKEv1/IKEv2**.

Remarque Les paramètres de cette boîte de dialogue s'appliquent à la topologie entière, à tous les tunnels et à tous les périphériques gérés.

Chemin de navigation

Périphériques > **Site à site**. Cliquez ensuite sur **+ VPN de site à site** ou modifiez une topologie VPN répertoriée. Cliquez sur l'onglet **IKE**.

Champs

Politique

Choisissez les objets de politique IKEv1 ou IKEv2 requis dans la liste prédéfinie ou créez de nouveaux objets à utiliser. Vous pouvez choisir plusieurs politiques IKEv1 et IKEv2. IKEv1 et IKEv2 prennent 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 de plus amples renseignements, consultez Politiques IKE Défense contre les menaces.

Type d'authentification

Le VPN de site à site prend en charge deux méthodes d'authentification, par clé prépartagée et par certificat. Pour obtenir une explication des deux méthodes, consultez Choix de la méthode d'authentification à utiliser.

Remarque Dans une topologie VPN qui prend en charge IKEv1, la **méthode d'authentification** spécifiée dans l'objet de politique IKEv1 choisi devient la valeur par défaut dans le paramètre de type d'**authentification** IKEv1. Ces valeurs doivent correspondre, sinon, votre configuration produira une erreur.

- **Clé automatique prépartagée** : Le centre de gestion définit automatiquement la clé pré-partagée pour ce VPN. Spécifiez la **Longueur de clé pré-partagée**, le nombre de caractères de la clé, 1 à 27.

  Le caractère « » (guillemets doubles) n'est pas pris en charge dans les clés prépartagées. Si vous avez utilisé « » dans une clé prépartagée, assurez-vous de modifier le caractère après la mise à niveau vers Cisco Secure Firewall Threat Defense 6.30 ou une version ultérieure.

- **Clé manuelle pré-partagée** : attribuez manuellement la clé pré-partagée pour ce VPN. Spécifiez la **clé**, puis saisissez-la à nouveau pour **Confirmer la clé**.

  Lorsque vous choisissez cette option pour IKEv2, la case à cocher **Enforce hex-based pre-shared key only** (Appliquer uniquement les clés pré-partagées basées sur des caractères hexadécimaux) s'affiche, cochez si vous le souhaitez. Si cette option est appliquée, vous devez saisir une valeur hexadécimale valide pour la clé, un nombre pair de 2 à 256 caractères, en utilisant les chiffres de 0 à 9 ou AF.

- **Certificat** : lorsque vous utilisez des certificats comme méthode d'authentification pour les connexions VPN, les homologues obtiennent des certificats numériques d'un serveur d'autorité de certification de votre infrastructure PKI et les échangent pour s'authentifier mutuellement.

  Dans le champ **Certificate** (certificat), sélectionnez un objet d'inscription de certificat préconfiguré. Cet objet d'inscription génère un point de confiance (Trustpoint) du même nom sur le périphérique géré. L'objet d'inscription de certificat doit être associé et installé sur le périphérique. Le processus d'inscription est achevé, puis un point de confiance est créé.

  Un point de confiance est la représentation d'une autorité de certification ou d'une paire d'identités. Un point de confiance comprend l'identité de l'autorité de certification, des paramètres de

configuration propres à l'autorité de certification et une association avec un certificat d'identité inscrit.

Avant de sélectionner cette option, tenez compte des éléments suivants :

- Assurez-vous d'avoir inscrit un objet d'inscription de certificat sur tous les points d'extrémité de la topologie. Un objet d'inscription de certificat contient les informations du serveur de l'autorité de certification (CA) et les paramètres d'inscription nécessaires à la création de demandes de signature de certificat (CSR) et à l'obtention de certificats d'identité auprès de l'autorité de certification spécifiée. Les objets d'inscription de certificat sont utilisés pour inscrire les appareils gérés dans votre infrastructure PKI et pour créer des points de confiance (objets CA) sur les appareils qui prennent en charge les connexions VPN. Pour obtenir des instructions sur la création d'un objet d'inscription de certificat, consultez Ajout d'objets d'Inscription du certificat et pour des instructions sur l'inscription de l'objet sur les points terminaux, consultez l'une des ressources suivantes, le cas échéant :
  - Installation d'un certificat à l'aide de l'inscription autosignée
  - Installation d'un certificat à l'aide de l'inscription EST
  - Installation d'un certificat à l'aide de l'inscription SCEP
  - Installation d'un certificat à l'aide de l'inscription manuelle
  - Installation d'un certificat à l'aide d'un fichier PKCS12

Remarque Pour une topologie VPN de site à site, assurez-vous que le même objet de certificat d'inscription est inscrit sur tous les points terminaux de la topologie. Pour en savoir plus, consultez le tableau ci-dessous.

- Consultez le tableau suivant pour comprendre les exigences d'inscription pour différents scénarios. Certains scénarios nécessitent que vous remplaciez l'objet d'inscription de certificat pour des périphériques spécifiques. Consultez Gestion des mises en priorité d'objets pour comprendre comment remplacer des objets.

Types d'inscription de certificat	Le certificat d'identité du périphérique pour tous les points terminaux provient de la même autorité de certification		Le certificat d'identité du périphérique pour tous les points terminaux provient de différentes autorités de certification
	Les paramètres spécifiques au périphérique NE SONT PAS spécifiés dans l'objet d'inscription du certificat	Les paramètres spécifiques au périphérique sont spécifiés dans l'objet d'inscription du certificat	
Manuel	Aucun remplacement requis	Remplacement requis	Remplacement requis
(HNE)	Aucun remplacement requis	Remplacement requis	Remplacement requis

Types d'inscription de certificat	Le certificat d'identité du périphérique pour tous les points terminaux provient de la même autorité de certification		Le certificat d'identité du périphérique pour tous les points terminaux provient de différentes autorités de certification
	Les paramètres spécifiques au périphérique NE SONT PAS spécifiés dans l'objet d'inscription du certificat	Les paramètres spécifiques au périphérique sont spécifiés dans l'objet d'inscription du certificat	
SCEP	Aucun remplacement requis	Remplacement requis	Remplacement requis
PKCS	Remplacement requis	Remplacement requis	Remplacement requis
Autosigné	Sans objet	Sans objet	Sans objet

- Comprenez les limites des certificats VPN mentionnées dans Lignes directrices et limites des certificats VPN Cisco Secure Firewall Threat Defense.

Remarque Si vous utilisez une autorité de certification (CA) Windows, l'extension des politiques d'application par défaut est **intermédiaire IKE de sécurité**. Si vous utilisez ce paramètre par défaut, vous devez sélectionner l'option **Ignore IPsec Key Usage** (Ignorer l'utilisation des clés IPsec) dans la section Advanced Settings (Paramètres avancés), sous l'onglet **Key** (Clé) de la boîte de dialogue **PKI Certificate Enrollment** (Inscription de certificats PKI) pour l'objet que vous sélectionnez. Sinon, les points terminaux ne peuvent pas établir la connexion VPN de site à site.

Options IPsec VPN Défense contre les menaces

Remarque Les paramètres de cette boîte de dialogue s'appliquent à la topologie entière, à tous les tunnels et à tous les périphériques gérés.

Type de carte de chiffrement

Une carte de chiffrement combine tous les composants requis pour configurer les associations de sécurité IPsec. Lorsque deux homologues tentent d'établir une SA, ils doivent chacun avoir au moins une entrée de carte de chiffrement compatible. La négociation de sécurité IPsec utilise les propositions définies dans l'entrée de la carte de chiffrement pour protéger les flux de données spécifiés par les règles IPsec de cette carte de chiffrement. Choisissez statique ou dynamique pour la carte de chiffrement de ce déploiement :

- **Statique** : utilisez une carte de chiffrement statique dans une topologie de VPN point à point ou à maillage complet.

- **Dynamique** : les cartes de chiffrement dynamiques créent essentiellement une entrée de carte de chiffrement sans tous les paramètres 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 ces politiques, 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. Dans une topologie VPN à maillage complet, vous ne pouvez appliquer que des politiques de carte de chiffrement statique.

Mode IKEv2

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

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

  Le principal avantage du mode tunnel est qu'il n'est pas nécessaire de modifier les systèmes d'extrémité pour profiter des avantages d'IPsec. Ce mode permet à un périphérique réseau, comme un routeur, de servir de serveur mandataire IPsec. C'est-à-dire que le routeur effectue le chiffrement au nom des hôtes. Le routeur source chiffre les paquets et les transfère dans le tunnel IPsec. Le routeur de destination déchiffre le datagramme IP d'origine et le transmet au système de destination. Le mode tunnel offre également une protection contre l'analyse du trafic; Avec le mode tunnel, un attaquant ne peut déterminer que les points terminaux du tunnel, et non la source et la destination réelles des paquets acheminés dans le tunnel, même s'ils sont identiques aux points terminaux du tunnel.

- **Transport préféré** : le mode d'encapsulation est réglé au mode de transport avec une option pour revenir au mode tunnel si l'homologue ne le prend pas en charge. En mode transport, seule les données utiles IP sont chiffrées et les en-têtes IP d'origine demeurent inchangés. Par conséquent, l'administrateur doit sélectionner un réseau protégé qui correspond à l'adresse IP de l'interface VPN.

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

- **Transport requis** : le mode d'encapsulation est réglé au mode de transport uniquement, le retour au mode tunnel est autorisé. Si les points terminaux ne peuvent pas négocier avec succès le mode de transport, car un point terminal ne le prend pas en charge, la connexion VPN n'est pas établie.

Propositions

Cliquez sur **Edit** (✎) pour préciser les propositions pour la méthode IKEv1 ou IKEv2 de votre choix. Sélectionnez parmi les objets de propositions **IKEv1 IPsec Proposals** ou **IKEv2 IPsec Proposals** disponibles, ou créez puis sélectionnez-en un nouveau. Consultez Configurer des objets de proposition IKEv1 IPsec et Configurer des objets de proposition IKEv2 IPsec pour en savoir plus.

Activer l’application de la force dans les associations de sécurité (SA)

L’activation de cette option garantit que l’algorithme de chiffrement utilisé par l’association de sécurité IPsec enfant n’est pas plus fort (en termes de nombre de bits dans la clé) que l’association de sécurité IKE parent.

Activer le RRI

La fonction Reverse Route Injection (RRI) permet d’insérer automatiquement des routes statiques dans le processus de routage pour les réseaux et les hôtes protégés par un point terminal de tunnel distant.

Activer la confidentialité parfaite de transmission

L'utilisation ou non du Perfect Forward Secrecy (PFS) pour générer et utiliser une clé de session unique pour chaque échange crypté. 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. Si vous sélectionnez cette option, sélectionnez également l’algorithme de dérivation de clé Diffie-Hellman à utiliser lors de la génération de la clé de session PFS dans la liste Module (groupe de modules).

Groupe de modules

Le groupe Diffie-Hellman à utiliser pour dériver un secret partagé entre les deux homologues IPsec sans se transmettre. 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 une explication complète des options, consultez Choix du groupe de module Diffie-Hellman à utiliser.

Durée de vie

Le nombre de secondes qu’une association de sécurité existe avant d’expirer. La valeur par défaut est de 28,800 secondes.

Taille de la durée de vie

Le volume de trafic (en kilo-octets) qui peut passer entre les homologues IPsec à l’aide d’une association de sécurité donnée avant son expiration. La valeur par défaut est de 4 608 000 kilo-octets. Des données infinies ne sont pas autorisées.

Paramètres ESPv3

Valider les messages d’erreur ICMP entrants

Choisissez de valider ou non les messages d’erreur ICMP reçus par l’intermédiaire d’un tunnel IPsec et destinés à un hôte intérieur sur le réseau privé.

Activer la politique « Do Not Fragment » (ne pas fragmenter)

Définissez comment le sous-système IPsec gère les paquets volumineux dont le bit « Ne pas fragmenter » (DF) est défini dans l’en-tête IP.

Politique

- Copy DF bit (copier le bit DF) : maintient le bit DF.
- Clear DF bit (effacer bit DF) : ignore le bit DF.
- Set DF bit (définir le bit DF) : définit et utilise le bit DF.

Activer les paquets Traffic Flow Confidentiality (TFC ou confidentialité du flux de données)

Activez les paquets TFC factices qui masquent le profil de trafic qui traverse le tunnel. Utilisez les paramètres **Burst** (Rafale), **Payload Size** (Taille de la charge utile) et **Timeout** (Expiration) pour générer des paquets de longueur aléatoire à des intervalles aléatoires sur le SA spécifié.

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

L'activation des paquets TFC empêche le tunnel VPN d'être inactif. Par conséquent, le délai d'inactivité VPN configuré dans la politique de groupe ne fonctionne pas comme prévu lorsque vous activez les paquets TFC.

Options de déploiement avancées de VPN de site à site Défense contre les menaces

Les sections suivantes décrivent les options avancées que vous pouvez spécifier dans votre déploiement VPN de site à site. Ces paramètres s'appliquent à la topologie entière, à tous les tunnels et à tous les périphériques gérés.

Options IKE avancées de VPN Défense contre les menaces

Avancé > IKE > Paramètres ISAKAMP

IKE Keepalive

Active ou désactive le maintien de l'activité IKE. Vous pouvez définir cette option sur EnableInfinite afin que le périphérique ne démarre jamais lui-même la surveillance Keepalive.

Seuil
Spécifie l'intervalle de confiance de maintien d'activité IKE. Cet intervalle est le nombre de secondes permettant à un homologue de passer au mode inactif avant de commencer la surveillance Keepalive. L'intervalle minimal et par défaut est de 10 secondes; l'intervalle maximal est de 3600 secondes.

Intervalle entre les tentatives
Spécifie le nombre de secondes à attendre entre les tentatives de maintien IKE. La valeur par défaut est de 2 secondes, la maximale est de 10 secondes.

Identité envoyée aux pairs :
Choisissez l'identité que les homologues utiliseront pour s'identifier pendant les négociations IKE :

- **autoOrDN**(par défaut) : détermine la négociation IKE par type de connexion : adresse IP pour la clé prépartagée ou Cert DN pour l'authentification de certificat (non pris en charge).
- **ipAddress** : utilise les adresses IP des hôtes qui échangent des informations d'identité ISAKMP.
- **hostname** : utilise le nom de domaine complet des hôtes échangeant les informations d'identité ISAKMP. Ce nom comprend le nom d'hôte et le nom de domaine.

Remarque Activez ou désactivez cette option pour toutes vos connexions VPN.

Activer le mode agressif
Sélectionnez cette méthode de négociation pour l'échange d'informations de clé si l'adresse IP est inconnue et que la résolution DNS n'est peut-être pas disponible sur les périphériques. La négociation est basée sur le nom d'hôte et le nom de domaine.

Activer la notification pour la déconnexion du tunnel
Permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur une SA (Security Association, association de sécurité) ne correspond pas aux sélecteurs de trafic de cette SA. Cette notification est désactivée par défaut.

Avancé > IKE > Paramètres de l'association de sécurité (SA) IKEv2

Davantage de contrôles de session sont disponibles pour IKE v2, ce qui limite le nombre de SA ouvertes. Par défaut, il n'y a pas de limite au nombre de SA ouvertes.

Contestation des témoins
s'il faut envoyer des défis liés aux témoins aux périphériques homologues en réponse aux paquets de lancement de la SA, qui peuvent aider à déjouer les attaques par déni de service (DoS). La valeur par défaut est d'utiliser les défis liés aux témoins lorsque 50 % des SA disponibles sont en négociation. Sélectionnez une des options :

- Personnalisé
- Jamais (par défaut)
- Toujours

Seuil pour contester les témoins entrants
Le pourcentage du total des associations de sécurité autorisées qui sont en cours de négociation. Cela déclenche la contestation des témoins pour les futures négociations d'un SA. La plage va de zéro à 100 %.

Nombre de SA autorisés en négociation
Limite le nombre maximal de SA qui peuvent être en négociation à tout moment. S'il est utilisé avec le Défi des témoins, configurez le seuil de défi pour les témoins sur une valeur inférieure à cette limite pour une vérification par recoupement efficace.

Nombre maximum de SA autorisées
Limite le nombre de connexions IKEv2 autorisées. La valeur par défaut est illimité.

Activer la notification pour la déconnexion du tunnel
Permet à un administrateur d'activer ou de désactiver l'envoi d'une notification IKE à l'homologue lorsqu'un paquet entrant reçu sur une SA ne correspond pas aux sélecteurs de trafic pour cette SA. L'envoi de cette notification est désactivé par défaut.

Options IPsec avancées de VPN Défense contre les menaces

Avancé > IPsec > Paramètres IPsec

Activer la fragmentation avant le chiffrement
Cette option permet au trafic de traverser des périphériques NAT qui ne prennent pas en charge la fragmentation IP. Il n'entame pas le fonctionnement des périphériques NAT qui prennent en charge la fragmentation IP.

Chronologie de l'unité de transmission maximale d'un chemin
Cochez cette case pour activer l'intervalle pour réinitialiser la PMTU d'une association de sécurité (SA).

Intervalle de valeur de réinitialisation
Saisissez le nombre de minutes pendant lesquelles la valeur de PMTU d'un SA est réinitialisée à sa valeur d'origine. La plage valide est de 10 à 30 minutes, la valeur par défaut est illimitée.

Options avancées de tunnel de VPN de site à site Défense contre les menaces

Chemin de navigation

Périphériques > site à site, puis cliquez sur **+ VPN de site à site**, ou modifiez une topologie VPN répertoriée. Cliquez sur l'onglet **Avancé**, puis sélectionnez **Tunnel** dans le volet de navigation.

Options de tunnel

Disponible uniquement pour les topologies en étoile et en étoile et à maillage complet. Cette section ne s'affiche pas pour les configurations point à point.

- **Activer la connectivité satellite à satellite via le concentrateur** : désactivé par défaut. Choisir ce champ permet aux périphériques à chaque extrémité des satellites d'étendre leur connexion via le nœud de concentrateur jusqu'à l'autre périphérique.

Paramètres NAT

- **Traversée des messages Keepalive** : choisissez d'activer ou non la traversée des messages Keepalive NAT. La traversée de la NAT Keepalive est utilisée pour la transmission de messages Keepalive lorsqu'un périphérique (le périphérique du milieu) est situé entre un concentrateur connecté au VPN et en étoile, et que cet appareil effectue une NAT sur le flux IPsec.

  Si vous sélectionnez cette option, configurez l'**intervalle**, en secondes, entre les signaux de maintien (keepalive) envoyés entre le périphérique en étoile et le périphérique du milieu pour indiquer que la session est active. La valeur peut être comprise entre 5 et 3 600 secondes. La valeur par défaut est de 20 secondes.

Contrôle d'accès pour le trafic VPN

- **Contourner la politique de contrôle d'accès pour le trafic déchiffré (sysopt permit-vpn)** – Par défaut, défense contre les menaces applique l'inspection de la politique de contrôle d'accès au trafic déchiffré. Activez cette option pour contourner l'inspection de la liste de contrôle d'accès (ACL). Le défense contre les menaces applique toujours l'ACL de filtrage VPN et l'ACL d'autorisation téléchargée depuis le serveur AAA au trafic VPN.

  Activez ou désactivez l'option pour toutes vos connexions VPN. Si vous désactivez cette option, assurez-vous que le trafic est autorisé par la politique de contrôle d'accès ou la politique de préfiltre.

Paramètres de carte de certificats

- **Utiliser la carte de certificats configurée dans les points terminaux pour déterminer le tunnel** : si cette option est activée (cochée), le tunnel est déterminé en faisant correspondre le contenu du certificat reçu aux objets de la carte de certificats configurés dans les nœuds des points terminaux.
- **Utiliser le champ certificat OU pour déterminer le tunnel** : indique que si un nœud n'est pas déterminé en fonction du mappage configuré (l'option ci-dessus) s'il est sélectionné, utilisez la valeur de l'unité organisationnelle (OU) dans le nom distinctif du sujet (DN) du certificat reçu pour déterminer le tunnel.
- **Utiliser l'identité IKE pour déterminer le tunnel** : Indique que si un nœud n'est pas déterminé en fonction d'une correspondance de règle ou issu de l'unité d'organisation (les options ci-dessus) si cette option est sélectionnée, les sessions IKE basées sur des certificats sont mappées à un tunnel en fonction de le contenu de l'ID IKE phase1.

- **Utiliser l'adresse IP de l'homologue pour déterminer le tunnel** : indique que si un tunnel n'est pas déterminé en fonction d'une règle de correspondance ou issu des méthodes d'ID d'unité d'organisation ou d'ID IKE (les options ci-dessus) si elles sont sélectionnées, il utilise l'adresse IP homologue établie.

A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel)

Centre de gestion prend en charge une interface logique routable appelée Virtual Tunnel Interface (VTI). Les VTI ne nécessitent pas un mappage statique des sessions IPsec vers une interface physique. Le point terminal de tunnel IPsec est associé à une interface virtuelle. Vous pouvez utiliser ces interfaces comme d'autres interfaces et appliquer des politiques de routage statique et dynamique.

Comme alternative au VPN basé sur les politiques, vous pouvez créer un tunnel VPN entre les homologues à l'aide des VTI. Les VTI prennent en charge le VPN basé sur le routage avec des profils IPsec associés à l'extrémité de chaque tunnel. Les VTI utilisent des routes statiques ou dynamiques. Le périphérique chiffre ou déchiffre le trafic en provenance ou à destination de l'interface du tunnel et le transmet en fonction de la table de routage. Les déploiements deviennent plus faciles, et le fait d'avoir une VTI qui prend en charge le VPN basé sur le routage avec un protocole de routage dynamique répond également à de nombreuses exigences d'un nuage privé virtuel. Centre de gestion vous permet de migrer facilement d'une configuration VPN basée sur une carte de chiffrement à une configuration VPN basée sur un VTI.

Vous pouvez configurer un VPN basé sur le routage avec une VTI statique ou dynamique à l'aide de l'assistant VPN de site à site. Le trafic est chiffré par voie de routage statique, BGP, OSPFv2/v3 ou EIGRP.

Vous pouvez créer une zone de sécurité routée, ajoutez des interfaces VTI, puis définir des règles de contrôle d'accès pour le contrôle du trafic décrypté sur le tunnel VTI.

Vous pouvez créer des VPN basés sur des VTI entre :

- Deux périphériques défense contre les menaces .
- Un défense contre les menaces et un nuage public.
- Un défense contre les menaces et un autre défense contre les menaces avec la redondance des fournisseurs de services.
- Un défense contre les menaces et tout autre périphérique avec des interfaces VTI.
- Un défense contre les menaces et un autre périphérique avec une configuration VPN basée sur les politiques.

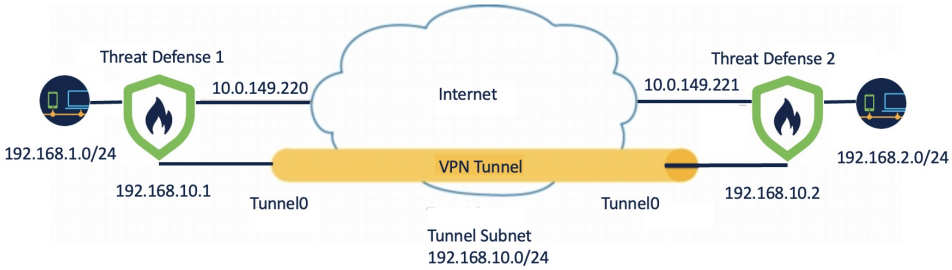
Il existe deux types d'interfaces VTI : la VTI statique et la VTI dynamique.

Pour plus de renseignements, consultez VTI statique, à la page 19 et VTI dynamique, à la page 21.

VTI statique

Le VTI statique utilise des interfaces de tunnel pour créer un tunnel permanent entre deux sites. Vous devez définir une interface physique comme source de tunnel pour un VTI statique. Vous pouvez associer un maximum de 1 024 VTI par périphérique. Pour créer une interface VTI statique dans le centre de gestion, consultez Ajouter une interface VTI, à la page 26.

La figure ci-dessous montre une topologie VPN utilisant des VTI statiques.



Dans Threat Defense 1 :

- L'adresse IP statique du VTI est 192.168.10.1
- La source du tunnel est 10.0.149.220
- La destination du tunnel est 10.0.149.221

À propos de Threat Defense 2 :

- L’adresse IP statique du VTI est 192.168.10.2
- La source du tunnel est 10.0.149.222
- La destination du tunnel est 10.0.149.220

Avantages

- Minimise et simplifie la configuration.

  Vous n’avez pas besoin de suivre tous les sous-réseaux distants pour obtenir une liste d’accès à une carte de chiffrement et configurer des listes d’accès ou des cartes de chiffrement complexes.

- Fournit une interface routable.

  Prend en charge les protocoles de routage IP tels que BGP, EIGRP et OSPFv2/v3 et les routes statiques.

- Prend en charge les tunnels VPN de secours
- Prend en charge l’équilibrage de la charge à l’aide d’ECMP.
- Prend en charge les routeurs virtuels.
- Fournit un contrôle d’accès différentiel pour le trafic VPN.

  Vous pouvez configurer un VTI avec une zone de sécurité et l’utiliser dans une politique de CA. Cette configuration :

  - Vous permet de classer et de différencier le trafic VPN du trafic en texte clair et d’autoriser le trafic VPN de manière sélective.
  - Fournit un contrôle d’accès différentiel pour le trafic VPN dans différents tunnels VPN.

VTI dynamique

Le VTI dynamique utilise un modèle virtuel pour l'instanciation et la gestion dynamiques des interfaces IPsec. Le modèle virtuel génère de manière dynamique une interface d'accès virtuelle unique pour chaque session VPN. Le VTI dynamique prend en charge plusieurs associations de sécurité IPsec et accepte plusieurs sélecteurs IPsec proposés par l'étoile.

Avantages

- Minimise et simplifie la configuration.

  Vous n'avez pas besoin de configurer des listes d'accès ou des cartes cryptographiques complexes.

- Simplifie la gestion
  - Gérez facilement la configuration des homologues pour les déploiements Hub and Spoke dans les grandes entreprises.
  - Utilisez un seul VTI dynamique pour plusieurs satellites, au lieu de configurer un seul VTI statique par satellite.
- Fournit une interface routable.

  Prend en charge les protocoles de routage IP tels que BGP, EIGRP et OSPFv2/v3 et les routes statiques.

- Simplifie l'évolutivité

  L'ajout de nouveaux satellites ne nécessite aucune configuration VPN supplémentaire sur le concentrateur. Vous devrez peut-être mettre à jour les configurations de NAT et de routage en fonction de la configuration.

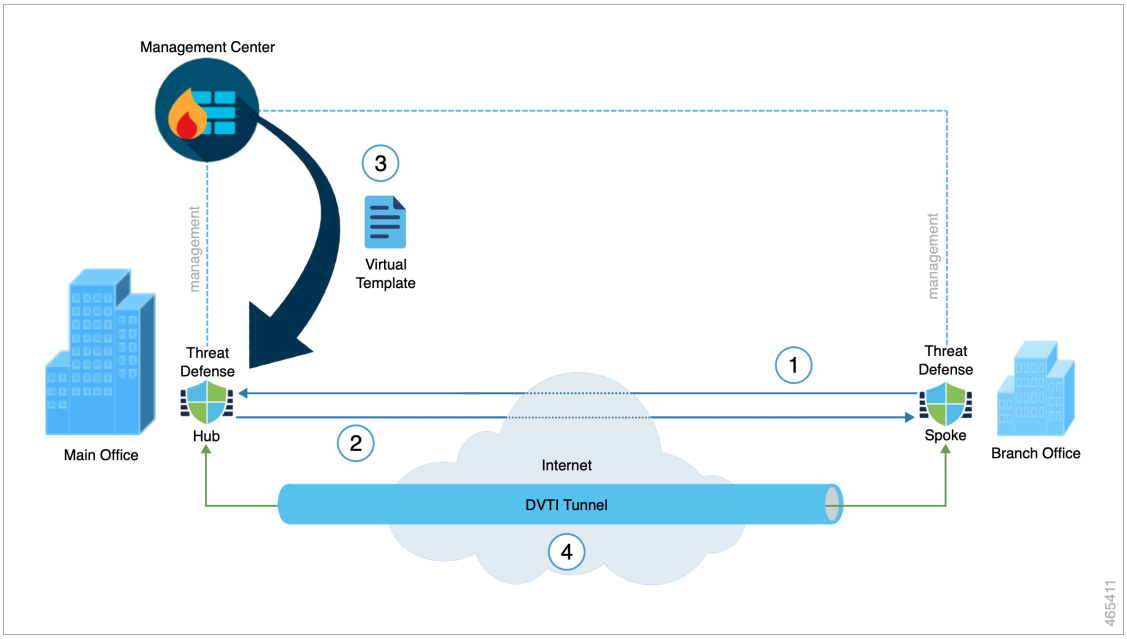
- Prise en charge des tunnels VPN de secours.
- Prend en charge les satellites dynamiques.

  Vous n'avez pas besoin de mettre à jour la configuration du concentrateur pour les modifications d'adresse IP DHCP en étoile.

- Conserve les adresses IP.
  - Utilise la fonctionnalité d'interface IP non numérotée pour emprunter l'adresse IP à partir d'une autre interface physique ou interface de boucle avec retour.
  - Toutes les interfaces d'accès virtuelles associées à un VTI dynamique utilisent la même adresse IP.
- Fournit un contrôle d'accès différentiel pour le trafic VPN.

  Vous pouvez configurer un VTI avec une zone de sécurité et l'utiliser dans une politique de CA. Cette configuration :
  - Vous permet de classer et de différencier le trafic VPN du trafic en texte clair et d'autoriser le trafic VPN de manière sélective.
  - Fournit un contrôle d'accès différentiel pour le trafic VPN dans différents tunnels VPN.

Comment Centre de gestion crée un tunnel VTI dynamique pour une session VPN



Lorsqu'un étoile lance une requête de tunnel auprès du concentrateur :

1. Le étoile initie un échange IKE avec le concentrateur pour une connexion VPN.
2. Le concentrateur authentifie le en étoile.
3. L' centre de gestion attribue un modèle virtuel dynamique sur le concentrateur pour le râteau.

   Le modèle virtuel génère dynamiquement une interface d'accès virtuelle sur le concentrateur. Cette interface est unique pour la session VPN avec le service en étoile.
4. Le concentrateur établit un tunnel VTI dynamique avec l'étoile en utilisant l'interface d'accès virtuel.
   1. Le concentrateur échange le trafic en étoile sur le tunnel à l'aide :
      - Du trafic spécifique proposé par les centres en étoile sur les échanges IKE.
      - Des protocoles BGP/OSPF/EIRGP sur le tunnel IPsec.
   2. À la fin de la session VPN, le tunnel se déconnecte et le concentrateur supprime l'interface d'accès virtuelle correspondante.

Pour créer une interface VTI dynamique dans le centre de gestion, consultez Ajouter une interface VTI, à la page 26.

Pour configurer un VPN de site à site basé sur le routage à l'aide de VTI dynamique, consultez Configurer le VTI dynamique pour un VPN de site à site basé sur le routage, à la page 41.

Directives et limites pour les interfaces de tunnel virtuel

Prise en charge d'IPv6

- Le VTI prend en charge IPv6.
- Vous pouvez utiliser une adresse IPv6 pour l'interface de source du tunnel et utiliser la même adresse que le point de terminaison du tunnel.
- centre de gestion prend en charge les combinaisons suivantes d'adresse IP VTI (ou de version IP pour les réseaux internes) par rapport aux versions IP publiques :
  - IPv6 sur IPv6
  - IPv4 sur IPv6
  - IPv4 sur IPv4
  - IPv6 sur IPv4
- VTI prend en charge les adresses IPv6 statiques et dynamiques comme source et destination du tunnel.
- L'interface de source du tunnel peut avoir des adresses IPv6 et vous pouvez en préciser l'adresse. Si vous ne spécifiez pas d'adresse, par défaut, le défense contre les menaces utilise la première adresse globale IPv6 de la liste comme point de terminaison du tunnel.

Prise en charge du protocole BGP IPv6

Le VTI prend en charge BGP IPv6.

Prise en charge d'EIGRP IPv4

Le VTI prend en charge le protocole EIGRP IPv4.

Prise en charge d'OSPFv2 et OSPFv3 IPv6/IPv4

Le VTI prend en charge OSPF IPv4 et IPv6.

Multi-instance et mise en grappe

- Le VTI est pris en charge en cas d'instances multiples.
- Les VTI ne sont pas pris en charge par la mise en grappe.

Mode pare-feu

Le VTI est pris en charge en mode routé uniquement.

Limites pour le VTI statique

- Seuls 20 profils IPSec uniques sont pris en charge.

- Dans le routage basé sur les politiques, vous pouvez configurer VTI uniquement comme interface de sortie.

Limites du VTI dynamique

- Le VTI dynamique ne prend pas en charge :
  - ECMP et VRF
  - Mise en grappes
  - IKEv1
  - Qualité de service
- Si un étoile a une adresse IP dynamique et qu'un concentrateur a un VTI dynamique derrière une NAT, l'état du tunnel sera inconnu.
- Pour un extranet dynamique, lorsque plusieurs satellites établissent une connexion, le tableau de bord de la surveillance de site à site n'affiche pas les tunnels individuels.
- Si vous configurez un concentrateur avec VTI dynamique derrière la NAT avec des satellites dynamiques, les données de surveillance VPN ne seront pas précises.

Directives générales de configuration pour le VTI statique et dynamique

- Si vous utilisez des cartes de chiffrement dynamiques et des VTI dynamiques dans vos VPN de site à site, seuls les tunnels VTI dynamiques apparaîtront. Ce comportement se produit car les cartes de chiffrement et les VTI dynamiques tentent d'utiliser le groupe de tunnels par défaut.

  Nous vous recommandons d'effectuer l'une des opérations suivantes :
  - Migrez vos VPN de site à site vers des VTI dynamiques.
  - Utiliser des cartes de chiffrement statiques avec leurs propres groupes de tunnels.
- Les VTI ne sont configurables qu'en mode IPsec.
- Le VTI dynamique prend uniquement en charge la topologie de concentrateur-en étoile dans le centre de gestion.
- Le VTI dynamique prend uniquement en charge les périphériques de défense contre les menaces à partir de la version 7.3.
- Nous vous recommandons de configurer un seul concentrateur pour une topologie en étoile basée sur le routage. Pour configurer une topologie avec plusieurs concentrateurs pour un ensemble de satellites, avec un concentrateur comme concentrateur de secours, configurez plusieurs topologies avec un seul concentrateur et le même ensemble de satellites. Pour en savoir plus, consultez Configurer plusieurs concentrateurs dans un VPN basé sur le routage, à la page 35.
- Vous pouvez utiliser des routes statiques, BGP, EIGRP IPv4 et OSPFv2/v3 pour le trafic utilisant l'interface du tunnel.
- Dans une configuration à haute disponibilité avec routage dynamique, le périphérique en veille ne peut pas accéder aux sous-réseaux connus par les tunnels VTI, car ces tunnels sont créés avec l'adresse IP active.

- Vous pouvez configurer un maximum de 1 024 VTI statiques et dynamiques sur un périphérique. Lors du calcul du nombre de VTI, tenez compte des éléments suivants :
  - Incluez les sous-interfaces Nameif pour dériver le nombre total de VTI qui peuvent être configurés sur le périphérique.
  - Vous ne pouvez pas configurer Nameif sur les interfaces membres d'un canal de port. Par conséquent, le nombre de tunnels est réduit par le nombre d'interfaces du canal de port principal principal seulement et non par aucune de ses interfaces membres.
  - Le nombre de VTI sur une plateforme est limité au nombre de VLAN configurables sur cette plateforme. Par exemple, Firepower 1120 prend en charge 512 VLAN, le nombre de tunnels est de 512 *moins* le nombre d'interfaces physiques configurées.
- Si vous configurez plus de 400 VTI sur un périphérique dans une configuration à haute disponibilité, vous devez configurer 45 secondes comme temps d'attente de l'unité pour le défense contre les menaces à haute disponibilité.
- La MTU pour les VTI est définie automatiquement en fonction de l'interface physique sous-jacente.
- Pour le VTI dynamique, l'interface d'accès virtuel hérite de la MTU de l'interface source du tunnel configurée. Si vous ne spécifiez pas l'interface de source du tunnel, l'interface d'accès virtuel hérite de la MTU de l'interface source de laquelle la défense contre les menaces accepte la demande de session VPN.
- Le VTI statique prend en charge les versions IKE v1, v2 et utilise IPsec pour envoyer et recevoir des données entre la source et la destination du tunnel.
- Le VTI dynamique prend uniquement en charge IKE version v2 et utilise IPsec pour envoyer et recevoir des données entre la source et la destination du tunnel.
- Pour les interfaces VTI statiques et dynamiques, assurez-vous de ne pas utiliser l'interface IP d'emprunt comme adresse IP source de tunnel pour une interface VTI.
- Lorsque vous configurez un VPN de site à site basé sur le routage à l'aide d'interfaces VTI statiques ou dynamiques, vérifiez que la valeur du saut TTL est supérieure à un si vous utilisez BGP.
- Si la NAT doit être appliquée, les paquets IKE et ESP sont encapsulés dans l'en-tête UDP.
- Les associations de sécurité IKE et IPsec sont rajustées en permanence, quel que soit le trafic de données dans le tunnel. Cela garantit que les tunnels VTI sont toujours actifs.
- Le nom du groupe de tunnels doit correspondre à ce que l'homologue envoie comme identité IKEv1 ou IKEv2.
- Pour IKEv1 dans les groupes de tunnels de réseau LAN à LAN, vous pouvez utiliser des noms qui ne sont pas des adresses IP si la méthode d'authentification du tunnel utilise des certificats numériques et/ou si l'homologue est configuré pour utiliser le mode dynamique.
- Les configurations du VTI et de la carte de chiffrement peuvent coexister sur la même interface physique si l'adresse homologue configurée dans la carte de chiffrement et la destination du tunnel pour le VTI sont différentes.
- Par défaut, tout le trafic envoyé par un VTI est chiffré.
- Les règles d'accès peuvent être appliquées sur une interface VTI pour contrôler le trafic via VTI.

- Vous pouvez associer des interfaces VTI aux zones ECMP et configurer des routes statiques ECMP pour réaliser ce qui suit :
  - Équilibrage de charge (actifs/VTI actifs) : la connexion peut passer par n'importe quel tunnel VTI parallèle.
  - Migration de connexion transparente : lorsqu'un tunnel VTI devient inaccessible, les flux sont migrés de manière transparente vers une autre interface VTI configurée dans la même zone.
  - Routage symétrique : flux de trafic vers l'avant à travers une interface VTI et configure le flux de trafic de retour à travers une autre interface VTI.

Pour en savoir plus sur la configuration d'ECMP, consultez Configurer un routage statique à coût égal.

Directives et limites des sauvegardes VTI

- La résilience de flux sur les basculements de tunnel n'est pas prise en charge. Par exemple, la connexion TCP en clair est perdue après le basculement du tunnel et vous devez relancer tout transfert FTP qui a eu lieu pendant le basculement.
- L'authentification de certificat n'est pas prise en charge dans le VTI de sauvegarde.

Sujets connexes

Directives et limites pour les interfaces de boucle avec retour
Créer un VPN de site à site basé sur le routage, à la page 27

Ajouter une interface VTI

Pour configurer un VPN de site à site basé sur le routage, vous devez créer une interface VTI sur les périphériques des deux nœuds du tunnel VTI.

Lorsque vous spécifiez le type de tunnel comme dynamique et que vous configurez les paramètres connexes, centre de gestion génère un modèle virtuel dynamique. Le modèle virtuel génère dynamiquement l'interface d'accès virtuelle qui est unique pour chaque session VPN.

Avant de commencer

Configurez une interface de boucle avec retour pour la redondance des tunnels VPN VTI statiques et dynamiques. Pour en savoir plus, consultez Configurer une interface de boucle avec retour.

Procédure

Étape 1 Choisissez **Devices**(périphériques) Device Management (gestion des périphériques).

Étape 2 Cliquez sur l'icône **Edit** (modifier) à côté du périphérique sur lequel vous souhaitez créer une interface VTI.

Étape 3 Choisissez **Add Interfaces > Virtual Tunnel Interface** (Ajouter des interfaces > interface de tunnel virtuelle).

Étape 4 Sélectionnez le **type de tunnel** comme **statique** ou **dynamique**.

Étape 5 Saisissez le nom et la description de l'interface. Par défaut, l'interface externe est activée.

Assurez-vous de spécifier un nom ne dépassant pas 28 caractères.

Étape 6 (Facultatif) Choisissez une zone de sécurité dans la liste déroulante **Security Zone** pour ajouter le VTI statique ou dynamique à cette zone.

Si vous souhaitez effectuer une inspection du trafic en fonction d'une zone de sécurité, ajoutez l'interface VTI à la zone de sécurité et configurez une règle de contrôle d'accès (AC). Pour autoriser le trafic VPN dans le tunnel, vous devez ajouter une règle AC avec cette zone de sécurité comme zone source.

Étape 7 Saisissez la priorité pour équilibrer la charge du trafic sur plusieurs VTI dans le champ **Priority**.

La valeur doit être comprise entre 0 et 65 535. Ce serveur a la priorité la plus élevée. Cette option ne s'applique pas au VTI dynamique.

Étape 8 Selon le type de tunnel, effectuez l'une des opérations suivantes :

- Pour un VTI dynamique, saisissez un ID unique compris entre 1 et 10 413 dans le champ **Template ID** (ID de modèle).
- Pour un VTI statique, utilisez un ID de tunnel unique compris entre 0 et 10 413 dans le champ **Tunnel ID** (ID de tunnel).

Étape 9 (Facultatif pour le VTI dynamique) Choisissez l'interface de source du tunnel dans la liste déroulante **Tunnel Source** (Source de tunnel).

Le tunnel VPN se termine à cette interface, une interface physique ou une interface de boucle avec retour. Choisissez l'adresse IP de l'interface dans la liste déroulante. Vous pouvez sélectionner l'adresse IP quel que soit le mode du tunnel IPsec. Dans le cas de plusieurs adresses IPv6, sélectionnez l'adresse que vous souhaitez utiliser comme point de terminaison du tunnel.

Étape 10 Sous **IPSec Tunnel Mode**(mode de tunnel IPSec), cliquez sur le bouton radio **IPv4** ou **IPv6** pour préciser le type de trafic sur le tunnel IPSec.

Étape 11 Sous **l'adresse IP** :

- **Configure IP** Configurer l'adresse IP) : saisissez l'adresse IPv4 ou IPv6 de l'interface VTI statique. Vous ne pouvez pas configurer d'adresse IP sur une interface VTI dynamique. Utilisez le champ **Borrow IP** (Emprunter une adresse IP) pour l'interface VTI dynamique.
- **Emprunter une adresse IP (IP non numérotée)** : Choisissez une interface physique ou une interface de boucle avec retour dans la liste déroulante, l'interface VTI hérite de cette adresse IP.

  Veillez à utiliser une adresse IP différente de l'adresse IP source du tunnel. Vous pouvez utiliser cette option pour une interface VTI statique ou dynamique.

  Cliquez sur **+** pour configurer une interface de boucle avec retour. L'interface de boucle avec retour permet de résoudre les échecs de chemin. Si une interface tombe en panne, vous pouvez accéder à toutes les interfaces grâce à l'adresse IP attribuée à l'interface de boucle avec retour.

Étape 12 Cliquez sur **OK**.

Étape 13 Cliquez sur **Save** (enregistrer).

Créer un VPN de site à site basé sur le routage

Vous pouvez configurer un VPN de site à site basé sur le routage pour les deux topologies suivantes :

- **Point à point** : Configurez les VTI sur les deux nœuds du tunnel et utilisez l'assistant pour configurer le VPN.
- **Hub and Spoke** (En étoile) : configurez les VTI sur le concentrateur et les satellites. Configurez le concentrateur avec un VTI dynamique et les satellites avec des VTI statiques.

Vous pouvez configurer un périphérique extranet comme concentrateur et des périphériques gérés comme satellites. Vous pouvez configurer plusieurs concentrateurs et satellites, ainsi que des concentrateurs et satellites de secours.

- Pour les concentrateurs et satellites extranet, vous pouvez configurer plusieurs adresses IP en tant que secours.
- Pour les satellites gérés, vous pouvez configurer une interface VTI statique de secours avec l'interface VTI principale.

Pour en savoir plus sur le VTI, consultez A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel), à la page 19.

Remarque Toutes les références à VTI signifient VTI statique et VTI dynamique, sauf si elles sont mentionnées.

Procédure

Étape 1 Choisissez **Devices (périphériques) > site à site** .

Étape 2 Cliquez sur **VPN de site à site**

Étape 3 Saisissez un nom pour la topologie VPN dans le champ **Topology Name** (nom de la topologie).

Étape 4 Choisissez **Route Based (VTI)** (basé sur le routage) et effectuez l'une des opérations suivantes :

- Sélectionnez **point à point** comme topologie du réseau. Pour configurer des points terminaux pour une topologie **point à point** basée sur le routage, consultez Configurer les points terminaux pour une topologie point à point, à la page 29.
- Sélectionnez **Hub and Spoke** (concentrateur et satellites) comme topologie de réseau. Pour configurer les points terminaux pour une topologie **Hub and Spoke** basée sur le routage, consultez Configurer les points terminaux pour une topologie en étoile, à la page 31.

Étape 5 (Facultatif) Spécifiez les options **IKE** pour le déploiement, comme décrit dans Options IKE VPN Défense contre les menaces, à la page 10.

Étape 6 (Facultatif) Spécifiez les options **IPsec** pour le déploiement, comme décrit dans Options IPsec VPN Défense contre les menaces, à la page 13.

Étape 7 (Facultatif) Spécifiez les options **avancées** pour le déploiement, comme décrit dans Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 16.

Étape 8 Cliquez sur **Save** (enregistrer).

Prochaine étape

Après avoir configuré les interfaces et le tunnel VTI sur les deux périphériques, vous devez configurer :

- Une politique de routage pour acheminer le trafic VTI entre les périphériques sur le tunnel VTI. Pour en savoir plus, consultez Configurer les politiques de routage et d'AC pour VTI, à la page 41.
- Une règle de contrôle d'accès pour autoriser le trafic chiffré. Sélectionnez **Policies (politiques)** > **Access Control (contrôle d'accès)**.

Configurer les points terminaux pour une topologie point à point

Configurez les paramètres suivants afin de configurer les points terminaux pour un VPN de site à site basé sur le routage pour les nœuds de topologie **point à point** :

Avant de commencer

Configurez les paramètres de base pour une topologie point à point dans un VPN basé sur le routage, comme décrit dans Créer un VPN de site à site basé sur le routage, à la page 27, puis cliquez sur l'onglet **Endpoints** (Points terminaux).

Procédure

Étape 1 Sous le **nœud A**, dans le menu déroulant **Device** (périphérique), sélectionnez le nom du périphérique enregistré (défense contre les menaces) ou de l' extranet comme premier point terminal de votre tunnel VTI.

Pour un homologue extranet, spécifiez les paramètres suivants :

1. Précisez le nom du périphérique.
2. Saisissez l'adresse IP de gestion ISE dans le champ **IEndpoint IP address** (Adresse IP de point terminal). Si vous configurez un VTI de secours, ajoutez une virgule et spécifiez l'adresse IP de secours.
3. Cliquez sur **OK**.

Après avoir configuré les paramètres ci-dessus pour le concentrateur extranet, spécifiez la clé prépartagée pour l' extranet dans l'onglet **IKE**.

Remarque Le VPC AWS a **AES-GCM-NULL-SHA-LATEST** comme politique par défaut. Si l'homologue distant se connecte au VPC AWS, sélectionnez **AES-GCM-NULL-SHA-LATEST** dans la liste déroulante **Policy** pour établir la connexion VPN sans modifier la valeur par défaut dans AWS.

Étape 2 Pour un périphérique enregistré, vous pouvez spécifier l'interface VTI pour le nœud A dans la liste déroulante **Virtual Tunnel Interface**.

L'interface de tunnel sélectionnée est l'interface source pour le nœud A et la destination du tunnel pour le nœud B.

Si vous souhaitez créer une nouvelle interface sur le nœud A, cliquez sur l'icône + et configurez les champs comme décrit dans Ajouter une interface VTI, à la page 26.

Si vous souhaitez modifier la configuration d'un VTI existant, sélectionnez le VTI dans le champ déroulant **Virtual Tunnel Interface** (Interface de tunnel virtuel) et cliquez sur **Edit VTI** (Modifier VTI).

Étape 3 Si votre périphérique du nœud A se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private** (l'adresse IP de la source du tunnel est privée). Dans le champ **Tunnel Source Public IP Address** (adresses IP de la source du tunnel), saisissez l'adresse IP publique de la source du tunnel.

Étape 4 **Send Local Identity to Peers** (envoyer l'identité locale aux homologues) : sélectionnez cette option pour envoyer des informations d'identité locale au périphérique homologue. Sélectionnez l'une des **configurations d'identité locale** suivantes dans la liste et configurez l'identité locale :

- **IP address** : utilisez l'adresse IP de l'interface pour l'identité.
- **Auto** : utilisez l'adresse IP pour la clé pré-partagée et le DN du certificat pour les connexions basées sur des certificats.
- **Email ID** (ID de courriel) : précisez l'ID de courriel à utiliser pour l'identité. L'identifiant de courriel peut comporter jusqu'à 127 caractères.
- **Hostname** (nom d'hôte) : utilisez le nom d'hôte complet.
- **Key ID** (ID de clé) : spécifiez l'ID de clé à utiliser pour l'identité. L'ID de clé doit comporter moins de 65 caractères.

L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels. L'identité unique permet à défense contre les menaces d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à une passerelle Internet Secure Internet Gateway (SIG) de Cisco Umbrella.

Pour en savoir plus sur la configuration d'un ID de tunnel unique sur Umbrella, consultez **le Guide de l'utilisateur de Cisco Umbrella SIG**.

Étape 5 (Facultatif) Cliquez sur **Add Backup VTI** (ajouter un VTI de sauvegarde) pour spécifier un VTI supplémentaire comme interface de secours et configurer les paramètres.

Remarque Assurez-vous que les deux homologues de la topologie n'ont pas la même source de tunnel pour le VTI de secours. Un périphérique ne peut pas avoir deux VTI avec la même source et la même destination de tunnel; configurez donc une combinaison unique de source et de destination de tunnel.

Bien que l'interface de tunnel virtuel soit spécifiée sous le VTI de secours, la configuration de routage détermine quel tunnel être utilisé comme tunnel principal ou de secours.

Étape 6 Développez **Advanced Settings** (Paramètres avancés) pour définir des configurations supplémentaires pour le périphérique. Pour en savoir plus, consultez Configurations avancées pour une topologie point à point dans un VPN basé sur le routage, à la page 31.

Étape 7 Répétez la procédure ci-dessus pour le nœud B.

Étape 8 Cliquez sur **OK**.

Prochaine étape

- (Facultatif) Spécifiez les options **IKE** pour le déploiement, comme décrit dans le Options IKE VPN Défense contre les menaces, à la page 10.
- (Facultatif) Spécifiez les options **IPsec** pour le déploiement, comme décrit dans le Options IPsec VPN Défense contre les menaces, à la page 13.
- (Facultatif) Spécifiez les options **avancées** pour le déploiement, comme décrit dans le Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 16.
- Cliquez sur **Save** (enregistrer).

- Pour acheminer le trafic vers le VTI, choisissez **Devices > Device Management**(Périphériques > Gestion des périphériques), modifiez le périphérique de défense contre les menaces et cliquez sur l'onglet **Routing** (routage).

  Vous pouvez configurer les routes statiques ou utiliser BGP, OSPF v2/v3 ou EIGRP pour acheminer le trafic VPN.

- Pour autoriser le trafic VPN, choisissez **Policies > Access Control** (Politiques > Contrôle d'accès).. Ajoutez une règle spécifiant la zone de sécurité du VTI. Pour un VTI de secours, assurez-vous d'inclure le VTI de secours dans la même zone de sécurité que celle du VTI principal.

Configurations avancées pour une topologie point à point dans un VPN basé sur le routage

Configurez les configurations avancées suivantes pour une topologie point à point dans un VPN basé sur le routage :

Avant de commencer

Configurez les paramètres de base pour une topologie point à point dans un VPN basé sur le routage, comme décrit dans Configurer les points terminaux pour une topologie point à point, à la page 29 et développez **Advanced Settings**.

Procédure

Étape 1 Cochez la case **Send Virtual Tunnel Interface IP to peers** pour envoyer l'adresse IP du VTI au périphérique homologue.

Étape 2 Cochez la case **Allow received IKEv2 routes from the peers** (autoriser les routes IKEv2 entrantes à partir des homologues) pour autoriser les routes IKEv2 entrantes des satellites et des homologues.

Étape 3 Dans la liste déroulante **Connection type** (Type de connexion), choisissez l'une des options suivantes :

Réponse seulement : le périphérique ne peut répondre que lorsqu'un périphérique homologue initie une connexion. Il ne peut initier aucune connexion.

Bidirectionnel : le périphérique peut initier une connexion ou y répondre. Il s'agit de l'option par défaut.

Configurer les points terminaux pour une topologie en étoile

Vous pouvez créer un VPN de site à site basé sur le routage à l'aide de VTI dynamique uniquement pour les topologies en étoile. Le concentrateur ne peut utiliser qu'un VTI dynamique et les satellites ne peuvent utiliser que des interfaces VTI statiques. Vous pouvez également configurer un périphérique extranet comme concentrateur.

Configurez les paramètres suivants pour configurer les points terminaux pour un VPN de site à site basé sur le routage pour les nœuds de topologie en **concentrateur en étoile** :

Avant de commencer

Configurez les paramètres de base pour une topologie en étoile dans un VPN basé sur le routage comme décrit dans Créer un VPN de site à site basé sur le routage, à la page 27 et cliquez sur l'onglet **Endpoints** (Terminaux).

Procédure

Étape 1 Sous **Nœuds de concentrateur** :

a) Cliquez sur le signe plus (+) pour configurer le nœud de concentrateur dans la boîte de dialogue **Add Endpoint** (ajouter un point terminal).

b) Sélectionnez un concentrateur dans la liste déroulante **Devices** (Périphériques).

Remarque Un périphérique défense contre les menaces fonctionnant avec la version de logiciel 7.2 ne peut pas être configuré comme concentrateur. Il doit s'agir d'un extranet ou d'un périphérique fonctionnant avec la version logicielle 7.3 ou ultérieure.

Pour un concentrateur extranet, spécifiez les paramètres suivants :

1. Saisissez le nom du périphérique.
2. Entrez l'adresse IP principale. Si vous configurez un VTI de secours, ajoutez une virgule, puis spécifiez l'adresse IP de secours.
3. Cliquez sur **OK**.

Après avoir configuré les paramètres ci-dessus pour le concentrateur extranet, spécifiez la clé prépartagée pour l' extranet dans l'onglet **IKE**.

Remarque Le VPC AWS a **AES-GCM-NULL-SHA-LATEST** comme politique par défaut. Si l'homologue distant se connecte au VPC AWS, sélectionnez **AES-GCM-NULL-SHA-LATEST** dans la liste déroulante **Policy** pour établir la connexion VPN sans modifier la valeur par défaut dans AWS.

c) Choisissez un VTI dynamique dans la liste déroulante **Dynamic Virtual Tunnel Interface** (Interface de tunnel virtuel dynamique).

La configuration de la source du tunnel est obligatoire pour un VTI dynamique, car le centre de gestion a besoin de cette information pour déterminer la destination du tunnel en étoile.

Cliquez sur le signe plus **(+)** pour ajouter un nouveau VTI dynamique. Nous vous recommandons de configurer l'adresse IP d'emprunt pour l'interface dynamique à partir d'une interface de boucle avec retour.

Si vous souhaitez modifier un VTI dynamique existant, sélectionnez l'interface et cliquez sur **Edit VTI** (Modifier le VTI).

d) (Facultatif) Si votre périphérique de point terminal se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private (** l'adresse IP de la source du tunnel est privée) et configurez l'adresse IP de la source du tunnel dans le champ **Tunnel Source Public IP Address** (adresse IP publique de la source du tunnel).

e) Cliquez sur **Routing Policy** (Politique de routage) pour configurer la politique de routage du concentrateur.

f) Cliquez sur **AC Policy** (Politique de contrôle d'accès) pour configurer la politique de contrôle d'accès.

g) Développez **Advanced Settings** (Paramètres avancés) pour configurer des configurations supplémentaires sur le concentrateur. Pour en savoir plus, consultez Configurations avancées pour le concentrateur en étoile dans un VPN basé sur le routage, à la page 34.

h) Cliquez sur **OK**.

Étape 2 Sous **Nœuds en étoile** :

a) Cliquez sur le signe plus + pour configurer le satellite dans la boîte de dialogue **Add Endpoint** (Ajouter un point terminal).

b) Choisissez un satellite dans la liste déroulante **Device** (Périphérique).

Pour un extranet en étoile, spécifiez les paramètres suivants :

1. Saisissez le nom du périphérique.
2. Sous **Endpoint IP Address** (Adresse IP du point terminal), choisissez l'une des options suivantes :
   - **Statique** : saisissez l'adresse IP du périphérique et l'adresse IP de secours, le cas échéant.
   - **Dynamique** : choisissez cette option pour affecter de manière dynamique les adresses IP aux satellites extranet.
3. Cliquez sur **OK**.

c) Choisissez un VTI statique dans la liste déroulante **Static Virtual Tunnel Interface**.

Cliquez sur le signe plus **(+)** pour ajouter un nouveau VTI statique. L'adresse IP du tunnel du VTI statique est remplie automatiquement, assurez-vous que cette adresse IP est unique pour le satellite.

Si vous souhaitez modifier un VTI statique existant, sélectionnez l'interface et cliquez sur **Edit VTI** (Modifier le VTI).

d) (Facultatif) Si votre périphérique de point d'extrémité se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private** (l'adresse IP de la source du tunnel est privée). Le centre de gestion a besoin de l'adresse de l'interface source du tunnel pour configurer l'adresse IP de destination du tunnel sur les satellites. Dans le champ **Tunnel Source Public IP Address** (adresses IP de la source du tunnel), saisissez l'adresse IP publique de la source du tunnel.

e) (Facultatif) **Send Local Identity to Peers** (envoyer l'identité locale aux homologues) : Cochez cette case pour envoyer les informations d'identité locale au périphérique homologue. Choisissez un des paramètres suivants dans la liste déroulante **Local Identity Configuration** et configurez l'identité locale :

- **IP address** : utilisez l'adresse IP de l'interface pour l'identité.
- **Auto** : utilisez l'adresse IP pour la clé pré-partagée et le DN du certificat pour les connexions basées sur des certificats.
- **Email ID** (ID de courriel) : précisez l'ID de courriel à utiliser pour l'identité. L'identifiant de courriel peut comporter jusqu'à 127 caractères.
- **Hostname** (nom d'hôte) : utilisez le nom d'hôte complet.
- **Key ID** (ID de clé) : spécifiez l'ID de clé à utiliser pour l'identité. L'ID de clé doit comporter moins de 65 caractères.

L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels. L'identité unique permet à défense contre les menaces d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à la passerelle Internet Cisco Umbrella Secure (SIG).

Pour en savoir plus sur la configuration d'un ID de tunnel unique sur Umbrella, consultez *le Guide de l'utilisateur de Cisco Umbrella SIG*.

f) (Facultatif) Cliquez sur **Add Backup VTI** (Ajouter un VTI de sauvegarde) pour spécifier une interface VTI supplémentaire comme interface de secours.

Remarque Assurez-vous que les deux homologues de la topologie n'ont pas de VTI de secours configuré sur la même source de tunnel. Par exemple, si l'homologue A a deux VTI (principal et un de secours) configurés avec une seule interface de source de tunnel, disons 10.0.10.1/30, alors l'homologue B ne peut pas non plus avoir ses 2 VTI avec une seule interface de source de tunnel, disons 20.20.01/30.

Bien que l'interface du tunnel virtuel soit spécifiée sous le VTI de secours, la configuration du routage détermine quel tunnel doit être utilisé comme tunnel principal ou de secours.

g) Cliquez sur **Routing Policy** (Politique de routage) pour configurer la politique de routage du satellite.
h) Cliquez sur **AC Policy** (Politique de contrôle d'accès) pour configurer la politique de contrôle d'accès.
i) Développez les **paramètres avancés** pour configurer des configurations supplémentaires sur le satellite. Pour en savoir plus, consultez Configurations avancées pour le concentrateur en étoile dans un VPN basé sur le routage, à la page 34.
j) Cliquez sur **OK**.

Prochaine étape

- (Facultatif) Spécifiez les options **IKE** pour le déploiement, comme décrit dans le Options IKE VPN Défense contre les menaces, à la page 10.
- (Facultatif) Spécifiez les options **IPsec** pour le déploiement, comme décrit dans le Options IPsec VPN Défense contre les menaces, à la page 13.
- (Facultatif) Spécifiez les options **avancées** pour le déploiement, comme décrit dans le Options de déploiement avancées de VPN de site à site Défense contre les menaces, à la page 16.
- Cliquez sur **Save** (enregistrer).

Configurations avancées pour le concentrateur en étoile dans un VPN basé sur le routage

Configurez les configurations avancées suivantes pour un concentrateur en étoile dans un VPN basé sur le routage :

Avant de commencer

Configurez les paramètres de base pour un concentrateur en étoile dans un VPN basé sur le routage comme décrit dans Configurer les points terminaux pour une topologie en étoile, à la page 31 et développez **Advanced Settings** (Paramètres avancés).

Remarque Seul le champ **Connection Type** (type de connexion) s'applique au périphérique fonctionnant avec la version logicielle 7.2. Les autres champs ne s'appliquent pas à cette version du périphérique .

Procédure

Étape 1 Cochez la case **Send Virtual Tunnel Interface IP to peers** pour envoyer l'adresse IP du VTI au périphérique homologue.

Pour un concentrateur, vous devez cocher cette case si vous utilisez BGP comme protocole de routage. Cette configuration garantit que l'adresse IP des boucles avec retour est partagée dans la table de routage de BGP.

Pour un réseau en étoile, cette option est activée par défaut.

Étape 2 Ajoutez les **réseaux protégés** pour définir les réseaux protégés par le point terminal VPN. Cliquez sur **+** pour sélectionner un réseau protégé.

Pour un concentrateur, configurez les réseaux protégés derrière le concentrateur. Ces informations et le réseau protégé en étoile génèrent la liste d'accès en étoile.

Vous ne pouvez pas créer de route statique pour une interface d'accès virtuelle sur un concentrateur avec VTI dynamique. Le concentrateur crée et supprime ces interfaces de manière dynamique pendant l'établissement et la terminaison du tunnel.

Dans le cas d'un réseau en étoile, configurez le réseau protégé en étoile.

Pour activer le routage statique pour les satellites en étoile, après avoir configuré les points terminaux pour votre topologie, cliquez sur l'onglet **IPsec** et cochez la case **Enable Reverse Route Injection** (Activer l'injection de routes inversées).

Vous n'avez pas besoin de cette option si vous utilisez BGP, OSPF ou EIGRP.

Étape 3 Cochez la case **Allow received IKEv2 routes from the peers** (autoriser les routes IKEv2 entrantes à partir des homologues) pour autoriser les routes IKEv2 entrantes des satellites et des homologues.

Pour un concentrateur : lors d'un échange IKE, le concentrateur annonce les interfaces d'accès virtuelles créées dynamiquement aux satellites, et les satellites annoncent leurs adresses IP VTI au concentrateur.

Pour un réseau en étoile, cette option est activée par défaut.

Étape 4 Dans la liste déroulante **Connection Type** (type de connexion), choisissez l'une des options suivantes :

Réponse seulement : le périphérique ne peut répondre que lorsqu'un périphérique homologue initie une connexion. Il ne peut initier aucune connexion.

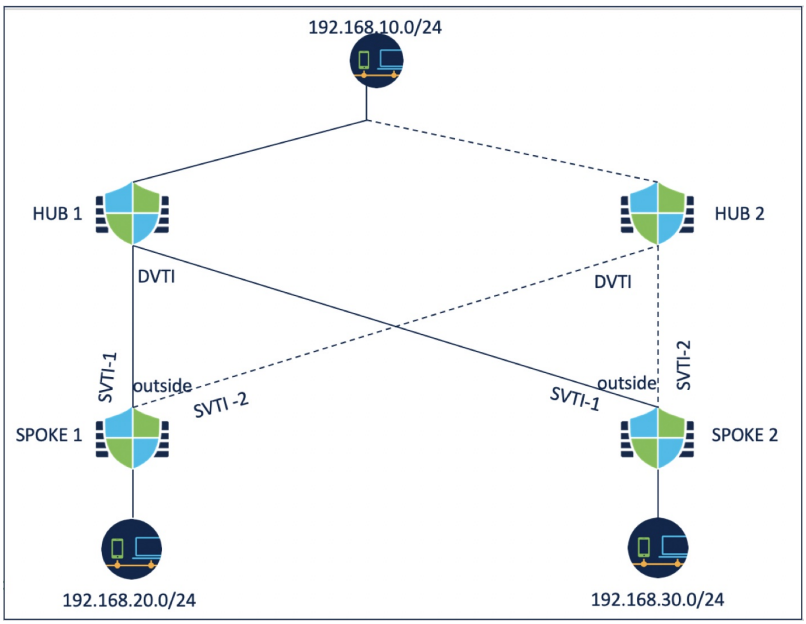
Bidirectionnel : le périphérique peut initier une connexion ou y répondre. Il s'agit de l'option par défaut.

Configurer plusieurs concentrateurs dans un VPN basé sur le routage

Vous pouvez configurer une topologie avec plusieurs concentrateurs pour un ensemble de satellites. En utilisant un concentrateur comme concentrateur de secours, vous pouvez configurer plusieurs topologies avec un seul concentrateur et le même ensemble de satellites.

Dans l'exemple suivant, deux concentrateurs sont connectés au même ensemble de satellites. Le concentrateur 1 est le concentrateur principal et le concentrateur 2 est le concentrateur secondaire. Pour configurer ce réseau dans la centre de gestion, vous devez configurer deux topologies de concentrateur en étoile basées sur le routage :

- Topologie 1 : le concentrateur 1 connecté au satellite 1 et au satellite 2.
- Topologie 2 : le concentrateur 2 connecté aux satellite 1 et au satellite 2.



Pour configurer la topologie 1 :

Procédure

Étape 1 Choisissez **Devices > Site To Site** (Périphériques > Site à site) et cliquez sur **+ Site To Site VPN** (+ VPN de site à site).

Étape 2 Saisissez un nom pour la topologie VPN dans le champ **Topology Name** (nom de la topologie).

Étape 3 Choisissez **Route Based (VTI) > Hub and Spoke > Endpoints** (Basé sur le routage (VTI) > concentrateur et étoile > points terminaux).

Étape 4 Sous **Nœuds de concentrateur** :

a) Cliquez sur le signe plus **(+)** pour ajouter le concentrateur.

b) Sélectionnez le concentrateur 1dans la liste déroulante **Devices** (Périphériques).

c) Choisissez un VTI dynamique dans la liste déroulante **Dynamic Virtual Tunnel Interface** (Interface de tunnel virtuel dynamique) ou cliquez sur le signe plus (**+)** pour ajouter un nouveau VTI dynamique.

Nous vous recommandons de configurer l'adresse IP d'emprunt pour l'interface dynamique à partir d'une interface de boucle avec retour.

d) (Facultatif) Si votre périphérique de point terminal se trouve derrière un périphérique NAT, cochez la case **Tunnel Source IP is Private (** l'adresse IP de la source du tunnel est privée) et configurez l'adresse IP de la source du tunnel dans le champ **Tunnel Source Public IP Address** (adresse IP publique de la source du tunnel).

e) Cliquez sur **Routing Policy** (Politique de routage) pour configurer la politique de routage du concentrateur. Vous pouvez configurer le routage dynamique à l'aide de BGP.

f) Développez **Advanced Settings** (Paramètres avancés). Vous pouvez configurer les paramètres avancés suivants pour que le concentrateur active le routage IKEv2, qui peut être utilisé si vous n'utilisez pas le routage dynamique.

- (Facultatif) Cochez la case **Send Virtual Tunnel Interface IP to the peers** (envoyer l'adresse IP de l'interface de tunnel virtuel aux homologues).

- Cochez la case **Allow incoming IKEv2 routes from the peers** (autoriser les routes IKEv2 entrantes des homologues) pour que le concentrateur accepte les routes des satellites et mette à jour la table de routage.
- Choisissez **Connection Type** (type de connexion) comme bidirectionnelle dans la liste déroulante.

g) Cliquez sur **OK**.

Étape 5 Sous **Nœuds en étoile** :

a) Cliquez sur le signe plus **(+)** pour ajouter un satellite.
b) Choisissez Spoke 1 dans la liste déroulante **Device** (Périphérique).
c) Choisissez SVTI-1 comme VTI statique pour le satellite dans la liste déroulante **Static Virtual Tunnel Interface** (Interface statique du tunnel virtuel) ou cliquez sur le signe plus + pour ajouter un nouveau VTI statique.

Choisissez l'interface externe comme source de tunnel de SVTI-1. L'adresse IP du tunnel du SVTI-1 est remplie automatiquement, assurez-vous que cette adresse IP est unique pour le satellite 1 à travers les pairs dans les deux topologies.

d) Développez **Advanced Settings** (Paramètres avancés). Si vous n'utilisez pas le routage dynamique, vous pouvez configurer ces paramètres pour activer le routage IKEv2 pour l'étoile.

- Cochez la case **Send Virtual Tunnel Interface IP to peers** pour envoyer l'adresse IP du VTI au périphérique homologue.
- Cochez la case **Allow incoming IKEv2 routes from the peers (** autoriser les routes IKEv2 entrantes des homologues) pour autoriser les routes IKEv2 entrantes des homologues.
- Choisissez **Connection Type** (type de connexion) comme bidirectionnelle dans la liste déroulante.

e) Cliquez sur **OK**.
f) Répétez les étapes 5a à 5e pour ajouter le satellite en étoile 2. Configurez SVTI-1 comme VTI statique de l'étoile 2.

Étape 6 Configurez les paramètres IKE et IPSec selon les besoins ou utilisez les valeurs par défaut.

Prochaine étape

1. Répétez les étapes 3 à 6 pour configurer la topologie 2 avec le concentrateur 2, les satellites en étoile 1 et 2.

   Configurez SVTI-2 en tant que VTI statique du satellite 1 et SVTI-2 en tant que VTI statique du satellite 2 (consultez l'illustration ci-dessus). La source du tunnel pour SVTI-2 doit être la même interface externe.

2. Pour chaque satellite en étoile, configurez la politique de routage. Pour en savoir plus, consultez Configurer le routage pour plusieurs concentrateurs dans un VPN basé sur le routage, à la page 37.

3. Vérifier la configuration et les états du tunnel. Pour en savoir plus, consultez Vérifier la configuration de plusieurs concentrateurs dans un VPN basé sur le routage, à la page 39.

Configurer le routage pour plusieurs concentrateurs dans un VPN basé sur le routage

La procédure suivante explique comment configurer le routage dynamique sur le concentrateur et les satellites en étoile, et comment configurer le routage basé sur les politiques sur les satellites en étoile.

Avant de commencer

Configurez la topologie 1 et 2 comme expliqué dans Configurer plusieurs concentrateurs dans un VPN basé sur le routage, à la page 35.

Procédure

Étape 1 Configurez le routage dynamique pour le concentrateur à l'aide de BGP.

a) Choisissez **Device > Device Management > Routing** (Périphérique > Gestion des périphériques > Routage).
b) Dans le volet gauche, choisissez **General Settings > BGP** (Paramètres généraux > BGP).
c) Cochez la case **Enable BGP** (activer BGP) et saisissez le **numéro de système autonome**.

   Vous pouvez configurer les autres champs selon vos besoins.

d) Cliquez sur **Save** (enregistrer).
e) Dans le volet gauche, choisissez **BGP > IPv4**.
f) Cochez la case **Enable IPv4** (activer IPv4).
g) Cliquez sur l'onglet **Neighbor** (voisin), cliquez sur **Add** (ajouter) et configurez les paramètres.

   1. **IP Address** (adresse IP) : saisissez l'adresse IP de l'interface du tunnel du satellite en étoile 1.
   2. **Remote AS** (AS distant) : numéro d'AS du satellite en étoile 1.
   3. Cochez la case **Enabled Address** (adresse activée).
   4. Cliquez sur **OK**.

   Répétez les étapes ci-dessus pour ajouter le satellite en étoile 2 en tant que voisin.

h) Cliquez sur **Save** (enregistrer).
i) Cliquez sur l'onglet **Networks** (réseaux), puis sur **Add** (ajouter) pour annoncer aux homologues le réseau derrière le concentrateur.

Étape 2 Configurez le routage dynamique pour les satellites en étoile à l'aide de BGP.

La configuration de BGP pour les satellites est similaire à celle du concentrateur, sauf pour les différences suivantes :

- Configurez les concentrateurs 1 et 2 comme voisins pour les deux satellites en étoile et utilisez l'adresse IP de l'interface de tunnel des concentrateurs.
- Lorsque vous configurez des réseaux, utilisez le réseau derrière chaque étoile.

Étape 3 Configurer le routage basé sur les politiques sur les satellites.

a) Dans le volet gauche, choisissez **Policy Based Routing** (routage basé sur les politiques) et cliquez sur **Add** (ajouter).
b) Choisissez **l'interface d'entrée** dans la liste déroulante.
c) Cliquez sur **Add** (ajouter) pour configurer une ACL de mise en correspondance.

   Par exemple, pour le réseau en étoile 1, le réseau source est 192.168.20.0/24 et le réseau de destination est 192.168.10.0/24.

d) Choisissez Egress Interfaces (interfaces de sortie) dans la liste déroulante **Send to** (envoyer à).

e) Choisissez l'ordre dans la liste déroulante **Ordre des interfaces**.
f) Sélectionnez les interfaces SVTI-1 et SVTI-2 comme interfaces de sortie.
g) Cliquez sur **Save** (enregistrer).

Si vous souhaitez utiliser les concentrateurs comme paire d'équilibrage de la charge, vous devez configurer ECMP.

Étape 4 Déployez les configurations sur les concentrateurs et les satellites en étoile.

Prochaine étape

Vérifier les configurations et les états des tunnels. Pour en savoir plus, consultez Vérifier la configuration de plusieurs concentrateurs dans un VPN basé sur le routage, à la page 39.

Vérifier la configuration de plusieurs concentrateurs dans un VPN basé sur le routage

Pour vérifier plusieurs configurations de concentrateurs et les états du tunnel :

- Après le déploiement, vérifiez l'état du tunnel.
- Utilisez les commandes show suivantes pour chaque point terminal afin de vérifier les configurations :
  - **show run route-map**
  - **show run access-list**
  - **show route-map**
  - **show route**

Acheminer le trafic par un tunnel VTI de secours

Cisco Secure Firewall Threat Defense prend en charge la configuration d'un tunnel de secours pour le VPN basé sur le routage (VTI). Lorsque le VTI principal ne peut pas acheminer le trafic, le trafic du VPN est acheminé par tunnellisation par le VTI de secours.

Vous pouvez déployer le tunnel VTI de secours dans les scénarios suivants :

- Les deux homologues ont une sauvegarde de la redondance du fournisseur de services.

  Dans ce cas, il y a deux interfaces physiques, servant de sources de tunnel pour les deux VTI des homologues.

- Un seul des homologues ayant une sauvegarde de la redondance du fournisseur de services.

  Dans ce cas, il n'y a de sauvegarde d'interface que d'un côté de l'homologue et de l'autre côté, il n'y a qu'une seule interface de source de tunnel.

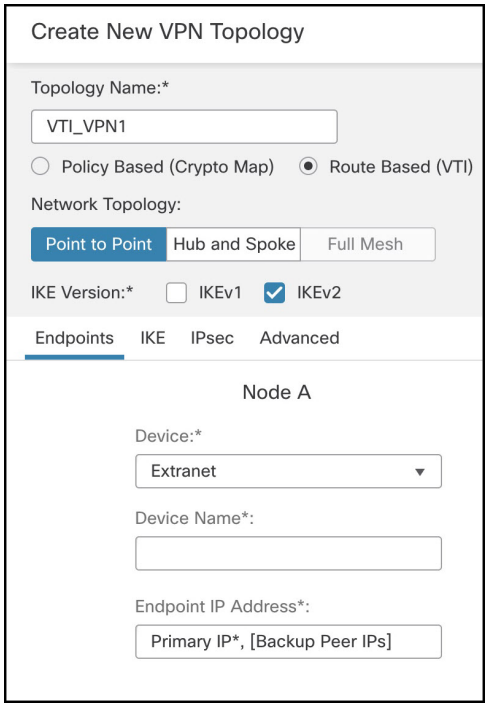
Étape	Faire ceci	Plus d'informations
1	Examinez les lignes directrices et les limites.	Directives et limites pour les interfaces de tunnel virtuel, à la page 23

Étape	Faire ceci	Plus d'informations
2	Créer l'interface VTI	Ajouter une interface VTI, à la page 26
3	Dans la boîte de dialogue **Add Endpoint** (Ajouter un point terminal) de l'assistant **Create New VPN Topology** (Créer une nouvelle typologie VPN), cliquez sur **Add Backup VTI** (Ajouter une VTI de secours) pour configurer l'interface de sauvegarde respective pour chaque homologue.	• Configurer les points terminaux pour une topologie point à point, à la page 29 • Configurer les points terminaux pour une topologie en étoile, à la page 31
4	Configurez la politique de routage.	• Sélectionnez **Devices (périphériques) > Device Management (gestion des périphériques)**, et modifiez le périphérique Threat Defense. • Cliquez sur **Routing** (Routage).
5	Configurez la politique de contrôle d'accès.	• Sélectionnez **Policies (politiques) > Access Control (contrôle d'accès)**.

Directives pour la configuration d'un tunnel VTI de secours

- Pour un homologue extranet, vous pouvez préciser l'adresse IP source du tunnel de l'interface de secours et configurer l'adresse IP de destination du tunnel sur l'homologue géré.

  Vous pouvez spécifier l'adresse IP homologue de secours dans le champ **Endpoint IP Address** (Adresse IP du point terminal) de l'assistant **Create New VPN Topology** (Créer une nouvelle topologie VPN).



- Après avoir configuré les interfaces de secours, configurez la politique de routage et la politique de contrôle d'accès pour le routage du trafic.

  Bien que les VTI principaux et de secours soient toujours disponibles, le trafic ne circule que dans le tunnel configuré dans la politique de routage. Pour de plus amples renseignements, voir Configurer les politiques de routage et d'AC pour VTI, à la page 41.

- Lorsque vous configurez un VTI de secours, assurez-vous d'inclure le tunnel de secours vers la même zone de sécurité que celle du VTI principal. Aucun paramètre spécifique n'est requis pour le VTI de secours dans la page de politique CA.

- Si vous configurez une voie de routage statique pour le tunnel de secours, configurez une voie de routage statique avec une métrique différente pour gérer le basculement du flux de trafic vers le tunnel de secours.

Configurer le VTI dynamique pour un VPN de site à site basé sur le routage

Pour configurer le VTI dynamique pour un VPN de site à site basé sur le routage dans le centre de gestion :

Étape	Faire ceci	Autres renseignements
1	Créez une interface VTI dynamique sur le concentrateur.	Ajouter une interface VTI, à la page 26
2	Créez des interfaces VTI statiques sur les satellites en étoile.	Ajouter une interface VTI, à la page 26
3	Créez un VPN de site à site basé sur le routage.	Créer un VPN de site à site basé sur le routage, à la page 27
4	Configurer la politique de routage et la politique de contrôle d'accès.	Configurer les points terminaux pour une topologie en étoile, à la page 31

Configurer les politiques de routage et d'AC pour VTI

Après avoir configuré les interfaces VTI et le tunnel VTI sur les deux périphériques, vous devez configurer :

- Une politique de routage pour acheminer le trafic VTI entre les périphériques sur le tunnel VTI.
- Une règle de contrôle d'accès pour autoriser le trafic chiffré.

Configuration du routage pour VTI

Pour les interfaces VTI, vous pouvez configurer des protocoles de routage statique ou de routage tels que BGP, EIGRP, OSPF/OSPFv3.

1. Sélectionnez **Devices (périphériques) > Device Management (gestion des périphériques)**, et modifiez le périphérique défense contre les menaces .
2. Cliquez sur **Routing** (Routage).

3. Configurez le routage statique, ou BGP, EIGRP, OSPF/OSPFv3.

Routage	Paramètres	Autres renseignements
Route statique	• **Interface** : sélectionnez l'interface VTI. Pour un tunnel de secours, sélectionnez l'interface VTI de secours. • **Réseau sélectionné** : réseau protégé de l'homologue distant. • **Passerelle** : adresse IP de l'interface du tunnel de l'homologue distant. Pour un tunnel de secours, sélectionnez l'adresse IP de l'interface du tunnel de secours de l'homologue distant. • **Mesure** : pour un tunnel de secours, configurez une mesure différente pour gérer le basculement du flux de trafic sur le tunnel de secours.	Ajouter une route statique

Routage	Paramètres	Autres renseignements

BGP	• Activez BGP sous **General Settings** (Paramètres généraux) > **BGP**, fournissez le numéro de système d'exploitation du périphérique local et ajoutez l'ID de routeur (si vous choisissez Manuel).
	• Sous **BGP**, activez IPv4 ou IPv6 et cliquez sur l'onglet **Neighbor** (Voisin) pour configurer les voisins.
	  • **Adresse IP** : adresse IP de l'interface VTI de l'homologue distant. Pour un tunnel de secours, ajoutez un voisin avec l'adresse IP de l'interface VTI de secours de l'homologue distant.
	  • **Système autonome à distance** : Numéro de système autonome de l'homologue distant.
	• Cliquez sur l'onglet **Redistribution**, sélectionnez le **Protocole source** comme connecté pour activer la redistribution des routes connectées.
		Configurer le protocole BGP

Routage	Paramètres	Autres renseignements
EIGRP	• Activez le protocole EIGRP, indiquez le numéro de système autonome du périphérique local et sélectionnez les réseaux ou les hôtes qui participent au processus de routage par protocole EIGRP. • Cliquez sur l'onglet **Neighbors** (Voisins) et définissez les voisins statiques pour le processus EIGRP. • Pour annoncer les adresses résumées d'une interface VTI, cliquez sur l'onglet **Summary Address** (adresses résumées), choisissez l'interface VTI dans la liste déroulante **Interface**. Dans la liste déroulante **Network** (réseau), choisissez le réseau à résumer. • Cliquez sur l'onglet **Interfaces** (interfaces) pour configurer les propriétés de routage EIGRP spécifiques à l'interface pour l'interface VTI. Pour activer le mode fractionné de l'EIGRP sur l'interface, cochez la case **Split Horizon** (Fractionner l'horizon). Vous pouvez également configurer le **Hold Time** (temps d'attente) annoncé par le périphérique dans les paquets Hello du protocole EIGRP.	
OSPF	• Cochez la case **Process 1** (processus 1) et choisissez le rôle OSPF. • Cliquez sur l'onglet **Interface** et choisissez une interface VTI.	Configurer le protocole OSPFv2
OSPFv3	• Cochez les cases **Processus 1** et **Activer le processus 1**, puis choisissez le rôle OSPFv3. • Cliquez sur l'onglet **Interface** et choisissez une interface VTI.	Configurer le protocole OSPFv3

Règle de politique de contrôle d'accès

Ajoutez une règle de contrôle d’accès à la politique de contrôle d’accès sur le périphérique pour autoriser le trafic chiffré entre les tunnels VTI avec les paramètres suivants :

1. Créez la règle avec l’action Allow (autoriser).
2. Sélectionnez la zone de sécurité VTI du périphérique local comme zone source et la zone de sécurité VTI de l’homologue distant comme zone de destination.
3. Sélectionnez la zone de sécurité VTI de l’homologue distant comme zone source et la zone de sécurité VTI du périphérique local comme zone de destination.

Pour plus d'informations sur la configuration d'une règle de contrôle d'accès, consultez Créer et modifier les règles de contrôle d’accès.

Déployer un tunnel SASE sur Umbrella

Cisco Umbrella est la plateforme en nuage de passerelle Internet sécurisée (SIG) de Cisco qui offre plusieurs niveaux de défense contre les menaces Internet. Umbrella intègre une passerelle Web sécurisée, la sécurité de la couche DNS et la fonctionnalité de contrôle d’accès de sécurité infonuagique (Cloud Access Security Broker ou CASB) pour protéger vos systèmes contre les menaces.

Vous pouvez établir un tunnel IPsec IKEv2 entre un périphérique de défense contre les menaces et Umbrella à l’aide du centre de gestion. Ce tunnel achemine tout le trafic Internet à Cisco Umbrella SIG pour l’inspection et le filtrage. Cette solution assure une gestion centralisée de la sécurité afin que les administrateurs réseau n’aient pas à gérer séparément les paramètres de sécurité de chaque bureau.

Pour configurer et déployer directement des tunnels Umbrella à partir d’un périphérique de défense contre les menaces, vous pouvez créer une topologie SASE à l’aide d’un assistant simple. La topologie SASE est un nouveau type de topologie VPN de site à site qui prend en charge :

- le VPN statique de site à site basé sur VTI.
- La topologie de réseau en étoile, où Umbrella est le centre et les périphériques de défense contre les menaces gérés sont les relais.
- L'authentification par clé partagée (PSK)
- défense contre les menaces déployés en mode haute disponibilité.
- Multi-instance : dans un déploiement multi-instance, vous ne pouvez intégrer qu’un seul compte Umbrella.

Pour une disponibilité élevée, vous pouvez configurer deux tunnels à partir d’un périphérique de défense contre les menaces et utiliser le deuxième tunnel comme tunnel de secours. Assurez-vous de configurer des ID de tunnel local différents pour chaque tunnel.

Pour faciliter la configuration, le centre de gestion configure les politiques IPsec et IKEv2 par défaut.

Configuration de la politique IKEv2 par défaut :

- Algorithmes d’intégrité : NULL
- Algorithmes de chiffrement : AES-GCM-256
- Algorithme PRF : SHA-256

- Groupe DH : 19, 20

Configuration de la politique IKEv2 IPsec par défaut :

- Hachage ESP : SHA-256
- Chiffrement ESP : AES-GCM-256

Sujets connexes

Déployer un tunnel SASE sur Umbrella, à la page 47

Directives et limites de configuration des tunnels SASE sur Umbrella

La topologie SASE prend en charge :

- Authentification basée sur la PSK uniquement
- IKEv2
- Haute disponibilité

Directives de configuration générale

- Le centre de gestion ne détecte pas les tunnels créés directement sur Umbrella ou par d'autres applications.
- Vous pouvez ajouter uniquement des périphériques gérés par centre de gestion en tant que points terminaux pour la topologie SASE. Vous ne pouvez pas ajouter de périphériques extranet.

  Pour les paires à haute disponibilité, les noms de ces dernières apparaissent dans la liste des points terminaux.
- Lorsque vous supprimez un tunnel de centre de gestion et s'il est impossible de le supprimer de Umbrella, vous devez le supprimer manuellement en vous connectant à Umbrella.
- Vous ne pouvez pas modifier ou supprimer une topologie SASE si le déploiement sur Umbrella est en cours. Vous pouvez afficher l'état de déploiement du tunnel dans :
  - La boîte de dialogue de l'assistant de configuration de Cisco Umbrella
  - La page Notifications sous les onglets Déploiements et Tâches
  - Le tableau de bord de la surveillance VPN de site à site
- Si vous cochez la case **Deploy configuration on threat defense node** (Déployer la configuration sur le nœud de défense contre les menaces) dans l'assistant, la configuration de la topologie Umbrella SASE est déployée sur défense contre les menaces uniquement après le déploiement des tunnels sur Umbrella.

  Le centre de gestion a besoin de l'ID de tunnel local pour déployer la configuration de Cisco Umbrella sur le défense contre les menaces . Umbrella génère l'ID de tunnel complet (*<prefix>@<umbrella generated ID>*-umbrella.com) uniquement après que centre de gestion a déployé le tunnel sur Umbrella.

- centre de gestion ne reconnaît pas les topologies avec le centre de données Umbrella en tant que concentrateur extranet, créées avant la version 7.3, en tant que topologies SASE. Vous devez créer de nouvelles topologies SASE dans la version 7.3 et supprimer la topologie existante.

Restrictions

La topologie SASE ne prend pas en charge :

- Mise en grappes
- L'authentification par certificat
- IKEv1

Déployer un tunnel SASE sur Umbrella

Cette section fournit des instructions pour déployer un tunnel SASE sur Umbrella à partir d'un périphérique défense contre les menaces à l'aide de la commande centre de gestion.

Étape	Faire ceci	Plus d'informations
1	Examinez les lignes directrices et les limites.	Directives et limites de configuration des tunnels SASE sur Umbrella, à la page 46
2	Assurez-vous de remplir les conditions préalables.	Conditions préalables à la configuration des tunnels SASE Umbrella, à la page 47
3	Configurez les paramètres de connexion de Cisco Umbrella.	• Configurer les paramètres de la connexion Cisco Umbrella • Cartographier les paramètres Umbrella du centre de gestion et les clés API de Cisco Umbrella, à la page 48
4	Configurez un tunnel SASE sur Umbrella.	Configurer un tunnel SASE pour Umbrella, à la page 50
5	Affichez l'état du tunnel SASE.	Afficher l'état du tunnel SASE, à la page 51

Conditions préalables à la configuration des tunnels SASE Umbrella

- Vous devez avoir un abonnement Cisco Umbrella Secure Internet Gateway (SIG) Essentials.
- Vous devez activer votre compte de licence Smart avec les fonctionnalités d'exportation contrôlée pour déployer des tunnels sur Umbrella à partir de centre de gestion. Si cette licence n'est pas activée, vous pouvez uniquement créer une topologie SASE. Vous ne pouvez pas déployer de tunnels sur Umbrella.
- Vous devez créer un compte auprès de Cisco Umbrella à l'adresse https://umbrella.cisco.com, vous connecter à Umbrella à l'adresse http://login.umbrella.com et obtenir les informations nécessaires pour établir la connexion à Cisco Umbrella.

- Vous devez enregistrer Cisco Umbrella avec centre de gestion et configurer la clé de gestion et le code secret de gestion dans les paramètres de Cisco Umbrella Connection. Le centre de gestion a besoin de la clé de gestion et du code secret de gestion pour récupérer les détails du centre de données à partir du nuage Cisco Umbrella. Vous devez également configurer l'identifiant de l'organisation, la clé du périphérique réseau, le code secret du périphérique réseau et le jeton du périphérique réseau actuel dans les paramètres de la connexion Cisco Umbrella.

  Pour obtenir plus de renseignements, consultez la section :

  - Configurer les paramètres de la connexion Cisco Umbrella
  - Cartographier les paramètres Umbrella du centre de gestion et les clés API de Cisco Umbrella, à la page 48

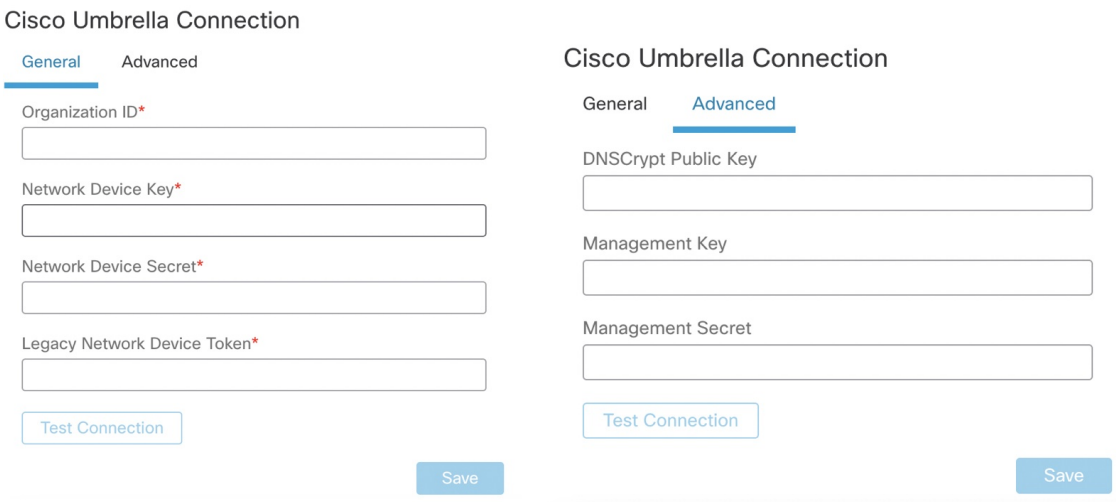
- Assurez-vous que le centre de données d'Umbrella est accessible à partir de défense contre les menaces .
- Vous pouvez déployer un tunnel uniquement entre Cisco Umbrella et défense contre les menaces pour les versions 7.1.0 ou ultérieures.

Cartographier les paramètres Umbrella du centre de gestion et les clés API de Cisco Umbrella

Pour enregistrer Cisco Umbrella auprès de centre de gestion et configurer les paramètres de Umbrella dans centre de gestion, vous devez effectuez ce qui suit :

1. Connectez-vous à Cisco Umbrella.
2. Choisissez **Admin » – Clés API > Clés existantes**.
3. Générez et copiez les clés API requises.
4. Utilisez les clés API pour configurer les paramètres de connexion de Cisco Umbrella dans centre de gestion.

La figure ci-dessous montre les paramètres que vous devez configurer dans Cisco Umbrella Connection dans centre de gestion. La clé publique DNScrypt est un paramètre facultatif.



La figure ci-dessous montre les clés API de Cisco Umbrella que vous devez utiliser pour enregistrer Cisco Umbrella auprès de centre de gestion.

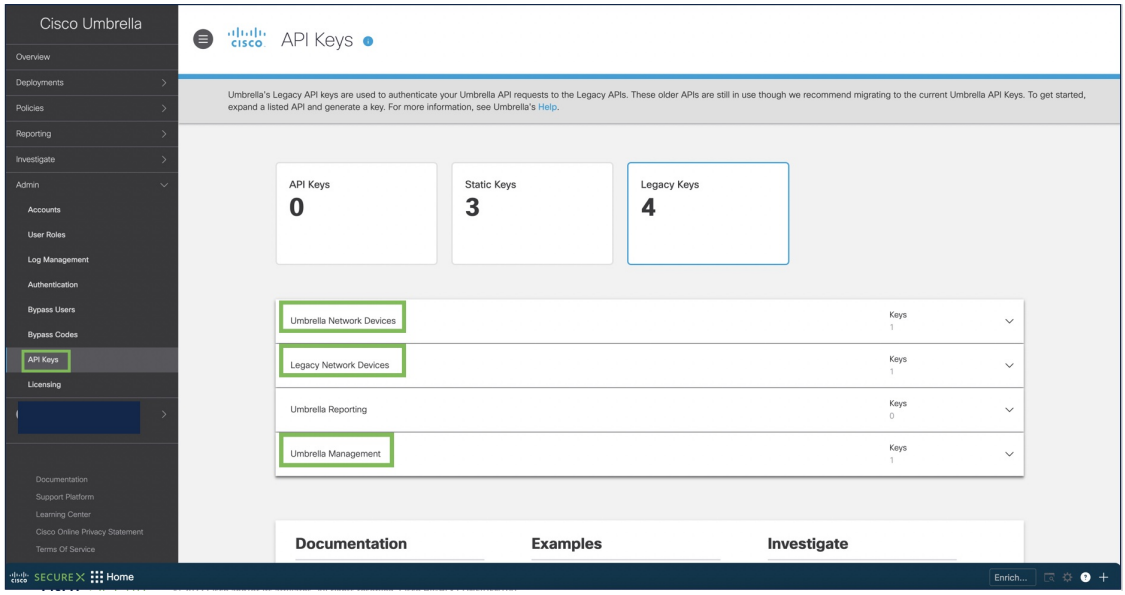


Tableau 2 : Mettre en correspondance les paramètres de Centre de gestion Umbrella et les clés API de Cisco Umbrella

Paramètres du centre de gestion	Clé API de Cisco Umbrella
Clé de l'appareil réseau Secret de l'appareil réseau	Périphériques de réseau Umbrella
Jeton d'appareil réseau existant	Périphériques réseau existants
Clé de gestion Secret de gestion	Gestion d'Umbrella

Configurer un tunnel SASE pour Umbrella

Avant de commencer

Assurez-vous de passer en revue les conditions préalables et les directives dans Conditions préalables à la configuration des tunnels SASE Umbrella, à la page 47 et Directives et limites de configuration des tunnels SASE sur Umbrella, à la page 46.

Procédure

Étape 1 Connectez-vous à votre centre de gestion, choisissez **Périphériques > Site à site**.

Étape 2 Cliquez sur **+ Topologie SASE** pour ouvrir l'assistant de topologie SASE.

Étape 3 Saisissez un **nom de topologie** unique.

Étape 4 **Clé pré-partagée** : cette clé est générée automatiquement en fonction des exigences de Umbrella PSK. Pour une topologie unique, la clé prépartagée est commune à tous les satellites de défense contre les menaces et à Umbrella.

L'appareil et Umbrella partagent cette clé secrète et IKEv2 l'utilise pour l'authentification. Si vous souhaitez configurer cette clé, elle doit comporter entre 16 et 64 caractères, inclure au moins une lettre majuscule, une lettre minuscule, un chiffre et ne comporter aucun caractère spécial. Chaque topologie doit avoir une clé prépartagée unique. Si une topologie comporte plusieurs tunnels, tous les tunnels ont la même clé prépartagée.

Étape 5 Choisissez un centre de données dans la liste déroulante **Centre de données Umbrella**. (Configurez le routage sur défense contre les menaces pour assurer l'accessibilité du contrôleur de domaine contextuel à partir du défense contre les menaces .)

Étape 6 Cliquez sur **Ajouter** pour ajouter un nœud défense contre les menaces .

a) Sélectionnez un défense contre les menaces dans la liste déroulante **Périphériques**.

Seuls les périphériques gérés par centre de gestion apparaissent dans la liste. Pour les paires à haute disponibilité, les noms de ces dernières apparaissent dans la liste des points terminaux.

b) Choisissez une interface statique VTI dans la liste déroulante **Interface VPN**.

Pour créer une nouvelle interface VTI statique, cliquez sur **+**. La boîte de dialogue **Add Virtual Tunnel Interface** (ajouter une interface de tunnel virtuel) s'affiche avec les configurations par défaut préremplies suivantes.

- Le type de tunnel est statique.
- Le nom est <*tunnel_source interface logical-name*>+ static_vti +<*tunnel ID*>. Par exemple, outside_static_vti_2.
- L'ID de tunnel est rempli automatiquement avec un ID unique.
- L'interface de la source du tunnel est remplie automatiquement avec une interface avec un préfixe « externe ».
- Mode de tunnel IPsec
- L'adresse IP provient de la plage d'adresses IP privées 169.254.xx/30.

c) Saisissez un préfixe pour l'ID de tunnel local dans le champ **Local Tunnel ID** (ID de tunnel local).

Le préfixe peut comporter un minimum de huit caractères et un maximum de 100 caractères. Umbrella génère l'ID de tunnel complet (<*prefix*>@<*umbrella generated ID*>-umbrella.com) une fois que le centre de gestion a déployé le tunnel sur Umbrella. Le centre de gestion récupère et met ensuite à jour l'ID de tunnel complet et le déploie sur le périphérique de défense contre les menaces. Chaque tunnel a un ID de tunnel local unique.

d) Cliquez sur **Save** (Enregistrer) pour ajouter le périphérique de point terminal à la topologie.

Vous pouvez ajouter plusieurs points terminaux dans une topologie SASE.

Étape 7 Cliquez sur **Next** (suivant) pour afficher le résumé de la configuration du tunnel Umbrella SASE.

- **Endpoints** (points terminaux) : affiche le récapitulatif des points terminaux configurés.
- **Encryption Settings** : affiche les politiques IKEv2 par défaut et les ensembles de transformations IKEv2 IPsec pour la topologie.

Étape 8 Cochez la case **Deploy configuration on threat defense nodes** (déploiement de la configuration sur les nœuds de défense contre les menaces) pour déclencher le déploiement des tunnels de réseau pour les nœuds de défense contre les menaces. Ce déploiement se produit après le déploiement des tunnels sur Umbrella. Un ID de tunnel local est requis pour le déploiement de la défense contre les menaces.

Étape 9 Cliquez sur **Save** (enregistrer).

Cette action :

1. Enregistre la topologie dans le centre de gestion.
2. Déclenche le déploiement des tunnels de réseau vers Umbrella.
3. Déclenche le déploiement des tunnels de réseau vers les périphériques de défense contre les menaces, si l'option est activée. Cette action valide et déploie toutes les configurations et toutes les politiques mises à jour, y compris les politiques non VPN, depuis le dernier déploiement sur le périphérique.
4. Ouvre la fenêtre de **configuration de Cisco Umbrella** et affiche l'état du déploiement du tunnel sur Umbrella. Pour en savoir plus, consultez Afficher l'état du tunnel SASE, à la page 51.

Prochaine étape

Pour le trafic intéressant destiné à circuler dans le tunnel SASE, configurez une politique PBR avec des critères de correspondance spécifiques pour envoyer le trafic par l'interface VTI.

Assurez-vous de configurer une politique PBR pour chaque point terminal de la topologie SASE.

Afficher l'état du tunnel SASE

Procédure

Étape 1 Choisissez **Devices (périphériques) > Site To Site (site à site)** .

Étape 2 Cliquez sur **+ SASE Topology** (Topologie SASE).

Étape 3 Saisissez un **nom de topologie** et une **clé pré-partagée** uniques , choisissez un centre de données, ajoutez un périphérique, puis cliquez sur **Next** (suivant).

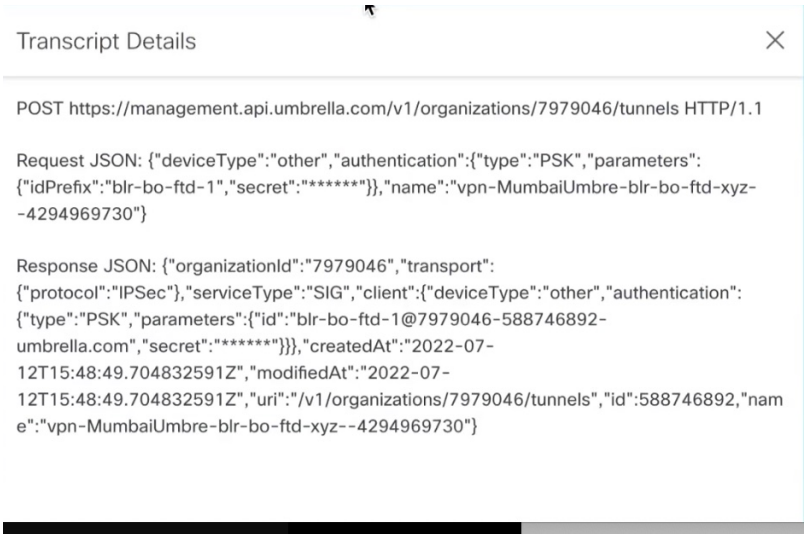
Étape 4 Affichez le résumé de la configuration du tunnel Umbrella SASE et cliquez sur **Save** (Enregistrer). La fenêtre de **Configuration Cisco Umbrella** s'affiche.

Vous pouvez afficher les détails de la topologie tels que le nom, le centre de données, l'adresse IP du centre de données et les heures de début et de fin du déploiement du tunnel.

Vous pouvez afficher l'état de déploiement des tunnels sur Umbrella. Les différents états de déploiement de tunnels sont les suivants :

- En attente : le centre de gestion n'a pas transféré la configuration vers Umbrella.
- Réussite : le centre de gestion a configuré avec succès un tunnel sur Umbrella.
- En cours : le centre de gestion déploie le tunnel sur Umbrella.
- Échec : le centre de gestion n'a pas pu configurer de tunnel sur Umbrella.

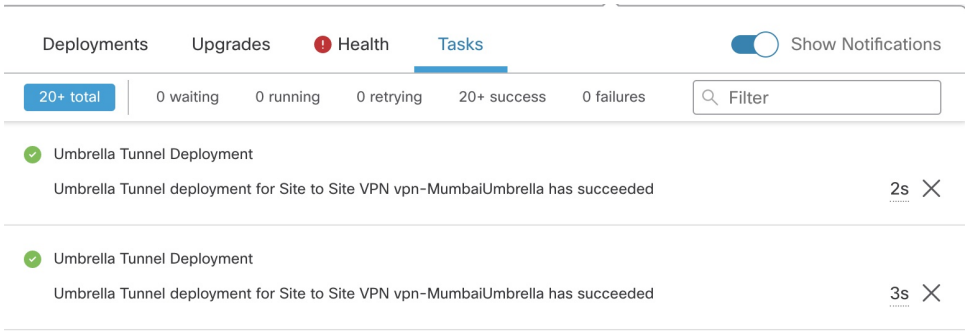
Si l'état apparaît comme en attente ou échec, utilisez la transcription pour dépanner la création du tunnel. Cliquez sur le bouton Transcript (Transcription) pour afficher les détails de la transcription tels que les API, la charge utile de la demande et la réponse reçue d'Umbrella.

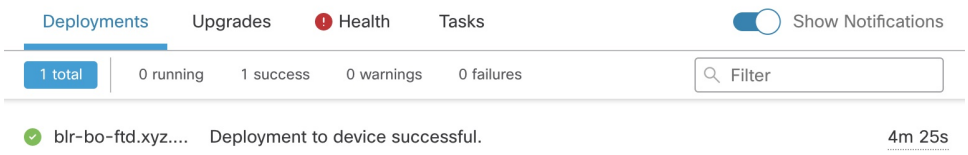


Étape 5 Cliquez sur **Umbrella Dashboard** (Tableau de bord Umbrella) pour afficher les tunnels de réseau dans Cisco Umbrella.

Étape 6 Affichez l'état de déploiement du tunnel Umbrella dans :

- La page **Notifications**, sous les onglets **Déploiements** et **Tâches**.





Surveillance des VPN de site à site

Le Cisco Secure Firewall Management Center fournit un instantané des tunnels VPN de site à site , y compris les tunnels de topologie SASE, pour déterminer l'état des tunnels VPN de site à site. Vous pouvez afficher la liste des tunnels entre les périphériques homologues et l'état de chaque tunnel : actif, inactif ou pas de données actives. Vous pouvez filtrer les données dans le tableau en fonction de la topologie, du périphérique et de l'état. Le tableau du tableau de bord de surveillance présente des données en direct et vous pouvez le configurer pour actualiser les données à un intervalle spécifié. Le tableau présente les topologies homologue à homologue, concentrateur en étoile et maillage complet pour les VPN par carte de chiffrement. Les informations sur le tunnel contiennent également les données pour les VPN basés sur le routage ou les interfaces de tunnel virtuel (VTI).

Vous pouvez utiliser ces données pour :

- Identifier les tunnels VPN présentant des problèmes et les dépanner.
- Vérifier la connectivité entre les périphériques homologues VPN de site à site.
- Surveiller l'intégrité des tunnels VPN pour fournir une connectivité VPN ininterrompue entre les sites.

Pour en savoir plus sur la configuration des VPN de site à site basés sur la carte de chiffrement, consultez Configurer un VPN de site à site basé sur une politique, à la page 5.

Pour plus d'informations sur les VTI, consultez A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel), à la page 19.

Lignes directrices et limites relatives à la licence

- Le tableau présente la liste des de site à site, y compris la topologie SASE, et les VPN qui sont déployés. Il n'affiche pas les tunnels qui sont créés et non déployés.
- Le tableau n'affiche pas les informations sur les tunnels de sauvegarde des VPN basés sur les politiques et des VTI de sauvegarde.
- Pour les déploiements en grappe, le tableau n'affiche pas le changement de directeur dans les données en temps réel. Il affiche uniquement les informations sur le directeur qui existent lors du déploiement du VPN. Le changement de directeur ne se reflète dans le tableau qu'après le redéploiement de l'AM du tunnel après le changement.

Tableau de bord de surveillance de VPN de site à site

Choisissez **Overview** > **Dashboards** > **Site to Site VPN** (Aperçu > Tableaux de bord > VPN de site à site) pour ouvrir le tableau de bord de surveillance de site à site.

Le tableau de bord de surveillance du VPN de site à site affiche les gadgets suivants pour les tunnels VPN de site à site :

- **État du tunnel)** : Tableau répertoriant l'état du tunnel des VPN de site à site , y compris les tunnels SASE pour Umbrella, configuré à l'aide de centre de gestion
- **Résumé du tunnel** : état agrégé des tunnels dans un graphique en anneau.
- **Topologie** : état des tunnels résumé par topologie.

État des tunnels VPN

Le tableau de bord de la surveillance de site à site répertorie les tunnels VPN dans les états suivants :

- **Inactif** : un tunnel VPN basé sur les politiques (basé sur la carte de chiffrement) est inactif si tous les tunnels IPSec sont en panne. Un tunnel VPN de topologie VTI et/ou SASE est en panne si le tunnel rencontre des problèmes de configuration ou de connectivité.
- **Actif** : dans la zone centre de gestion, les VPN de site à site basés sur les politiques sont configurés en fonction des politiques IKE et des propositions IPsec qui sont affectées aux topologies VPN. Un tunnel VPN basé sur des politiques est à l'état actif si centre de gestion identifie un trafic intéressant dans le tunnel après le déploiement. Un tunnel IKE ne fonctionne que si au moins un tunnel IPsec est actif.

  Les tunnels VPN basés sur le routage (VTI) et SASE n'ont pas besoin que le trafic intéressant soit à l'état actif. Ils ont l'état Actif s'ils sont configurés et déployés sans erreur.
- **No Active Data**(pas de données actives) : les tunnels VPN à topologie basée sur des politiques et SASE restent dans l'état No Active Data (pas de données actives) jusqu'à ce qu'un événement de flux de trafic se produise dans le tunnel pour la première fois. L'état Aucune donnée active répertorie également les VPN basés sur les politiques et basés sur le routage qui ont été déployés avec des erreurs.

Remarques importantes concernant les états des tunnels dans Centre de gestion

- Les états VPN dans centre de gestion sont basés sur les événements. Le centre de gestion ne lance pas les mises à jour d'état. Par conséquent, il peut y avoir des incompatibilités entre les états du tunnel dans le tableau de bord et défense contre les menaces . Vous pouvez afficher l'état correct sous l'onglet **CLI Details** (Détails de la CLI) du gadget **Tunnel Status** (état du tunnel).
- Lorsqu'un défense contre les menaces bascule sur un défense contre les menaces secondaire, il y a une incompatibilité entre les états des tunnels VPN dans centre de gestion et défense contre les menaces . Lorsque le périphérique repasse au périphérique principal, l'état correct du tunnel s'affiche.
- centre de gestion ne met pas à jour l'état du tunnel des périphériques défense contre les menaces de version antérieure à la version 7.3 après le redémarrage des périphériques. Nous vous recommandons de fermer le tunnel à l'aide de la commande **vpn-sessiondb logoff index** et de le réactiver à l'aide de Packet Tracer.

État du tunnel

Ce tableau répertorie les VPN de site à site, y compris le VPN de topologie SASE, configurés à l'aide de la commande centre de gestion. Survolez une topologie et cliquez sur View (Afficher) pour afficher les détails suivants à propos de la topologie :

- **Général** : affiche plus d'informations sur les nœuds, comme l'adresse IP et le nom d'interface.
- **Détails de la CLI** : affiche les sorties de la CLI pour les commandes suivantes :

- **show crypto ipsec sa peer** <*node A/B_ip_address*>: Affiche les associations de sécurité IPsec créées entre les nœuds A et B.
- **show vpn-sessiondb l2l filter ipaddress** <*node A/B_ip_address*>: Affiche des informations sur les sessions VPN.

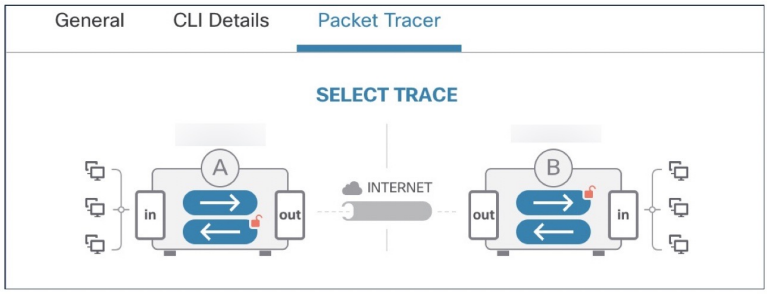
Pour un périphérique extranet, aucune sortie de commande ne s'affiche.

- **Packet Tracer** : utilisez Packet Tracer pour dépanner les tunnels VPN de défense contre les menaces.

Packet Tracer

Packet Tracer vous permet de dépanner les tunnels VPN entre deux périphériques de défense contre les menaces. Vous pouvez vérifier si la connexion VPN entre le périphérique A et le périphérique B est opérationnelle. Cet outil injecte un paquet dans le périphérique et suit le flux de paquets du port d'entrée aux ports de sortie. L'outil simule le trafic une fois que vous avez configuré les interfaces d'entrée des périphériques ainsi que les réseaux protégés. Packet Tracer évalue le paquet par rapport à des modules tels que les recherches de flux et de routage, les listes de contrôle d'accès, l'inspection de protocole, la NAT et la QoS.

Illustration 1 : Packet Tracer



Pour chaque périphérique, l'outil exécute une trace chiffrée et une trace déchiffrée (le paquet est traité comme un trafic VPN déchiffré). Vous pouvez exécuter quatre suivis différents entre les ports d'entrée et de sortie des périphériques. Cliquez sur les options individuelles de chiffrement et de déchiffrement pour activer ou désactiver la trace.

Lorsque vous exécutez la trace, l'outil l'exécute de manière séquentielle dans l'ordre suivant :

1. Trace chiffrée de A.
2. Trace déchiffrée de B.
3. Trace chiffrée de B.
4. Trace déchiffrée de A.

Une fois le suivi terminé, vous pouvez afficher la sortie du suivi avec les résultats de chaque module.

Remarque Vous ne pouvez pas exécuter de trace de déchiffrement pour les VPN basés sur le routage (VTI).

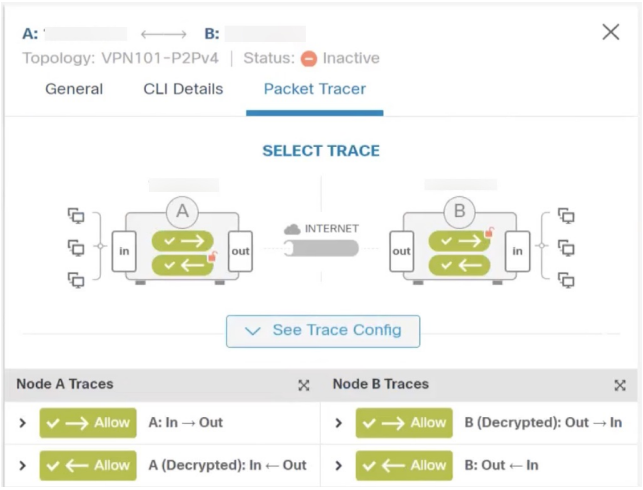
Pour exécuter Packet Tracer :

1. Cliquez sur **See Detailed Config** (afficher la configuration détaillée) pour afficher le nom de l'interface VPN, l'adresse IP de l'interface VPN, le nom de l'interface VTI et l'adresse IP de l'interface VTI.
2. (Facultatif) Choisissez le protocole souhaité dans la liste déroulante **Protocole**. Vous pouvez choisir ICMP/8/0, TCP ou UDP.

   ICMP/8/0 est l'option par défaut. Si vous choisissez ICMP/8/0, 8 indique le type ICMP comme demande Echo et 0 le code ICMP. Si vous choisissez TCP ou UDP, choisissez le port de destination dans la liste déroulante **Destination Port** (Port de destination). La valeur doit être comprise entre 0 et 65 535.
3. Choisissez l'interface d'entrée pour les deux périphériques sur lesquels tracer le paquet dans les listes déroulantes d'**interface d'entrée**. Packet Tracer ne prend pas en charge les interfaces de boucle avec retour.
4. Saisissez une adresse IP du même sous-réseau que l'interface d'entrée dans les champs **Protected Network IP Address** (adresse du réseau protégé).
5. Cliquez sur **Tracer maintenant**.

   Après avoir lancé le suivi, vous pouvez voir si le suivi a réussi ou non pour chaque module. Si le tunnel est en panne, le chemin s'affiche en rouge. Si le tunnel est actif, le chemin s'affiche en vert. Si un tunnel est en panne, cliquez sur **Re-trace** pour exécuter à nouveau l'outil. Pour un VPN basé sur la carte de chiffrement, lorsque le tunnel est inactif sans trafic intéressant, la trace initiale peut être rouge. Cliquez sur **Re-trace** pour exécuter à nouveau le traçage.

Illustration 2 : Packet Tracer après un suivi réussi



Nœuds extranet : vous pouvez lancer un suivi de paquets pour les tunnels VPN avec un nœud comme extranet. Pour un nœud extranet, vous ne pouvez pas choisir l'interface d'entrée. Les autres étapes de la trace des paquets sont les mêmes. Vous ne pouvez pas exécuter le suivi côté extranet.

Par exemple, si le nœud A est une défense gérée contre les menaces et le nœud B est un extranet :

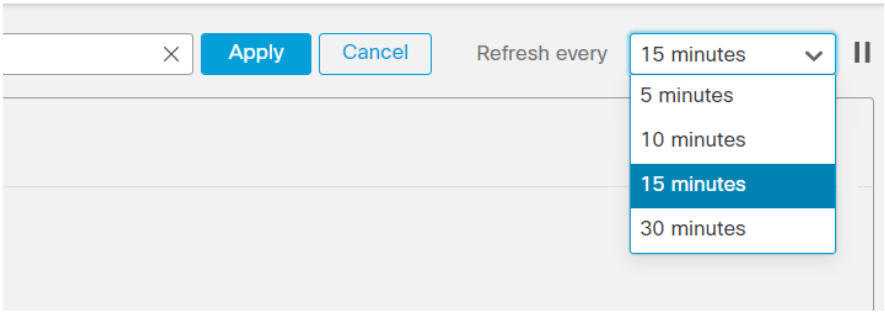
- Configurez l'interface d'entrée pour le nœud A.
- Configurez le réseau protégé pour les nœuds A et B.
- Cliquez sur **Tracer maintenant**. Les suivis s'affichent pour le nœud A et non pour le nœud B.

Actualisation automatique des données

Les données VPN de site à site dans le tableau sont actualisées régulièrement. Vous pouvez configurer l'intervalle d'actualisation des données de surveillance VPN à un intervalle spécifique ou désactiver l'actualisation automatique des données.

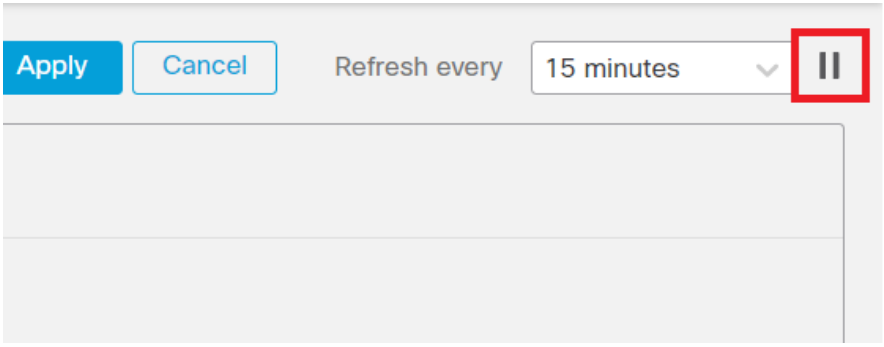
Cliquez sur la liste déroulante d'intervalle d'**actualisation** pour sélectionner parmi les intervalles disponibles et actualiser les données du tableau.

Illustration 3 : Actualiser les données du tunnel



Cliquez sur **Pause** (mettre en pause) pour interrompre l'actualisation automatique des données aussi longtemps que vous le souhaitez. Vous pouvez cliquer sur le même bouton pour reprendre l'actualisation des données du tunnel.

Illustration 4 : Suspendre l'actualisation périodique des données



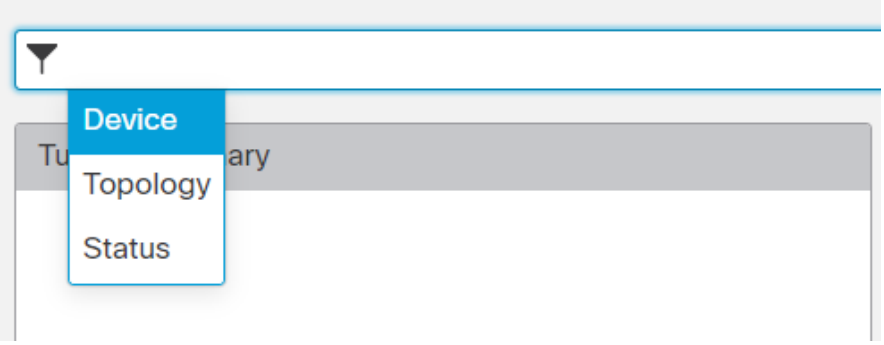
Filtrer et trier les données de surveillance VPN de site à site

Vous pouvez filtrer et afficher les données du tableau de surveillance VPN par topologie, périphérique et état.

Par exemple, vous pouvez afficher les tunnels qui sont à l'état inactif dans une topologie spécifique.

Cliquez dans la zone de filtre pour choisir les critères de filtre, puis spécifiez les valeurs à filtrer.

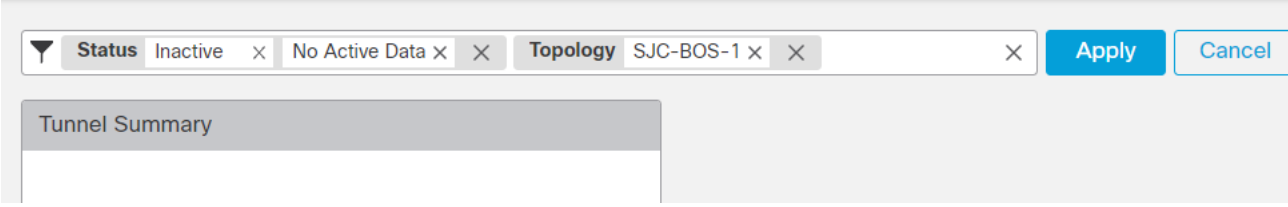
Illustration 5 : Filtrer les données du tunnel



Vous pouvez utiliser plusieurs critères de filtrage pour afficher les données en fonction de vos besoins.

Par exemple, vous pouvez choisir de n'afficher que les tunnels qui sont dans les états activé et désactivé et ignorer ceux dans l'état inconnu.

Illustration 6 : Exemple : filtrer les données du tunnel



Sort the data(trier les données) : pour trier les données en fonction d'une colonne, cliquez sur l'en-tête de la colonne.

Sujets connexes

À propos du VPN de site à site, à la page 1
A propos des Virtual Tunnel Interfaces (Interfaces de tunnel virtuel), à la page 19

Historique du VPN de site à site

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Topologie Umbrella SASE	7.3	N'importe lequel	Vous pouvez configurer une topologie SASE Umbrella et déployer des tunnels IPsec IKEv2 entre un périphérique de défense contre les menaces et Umbrella. Ce tunnel achemine tout le trafic Internet à la passerelle Internet sécurisée Umbrella (SIG) pour inspection et filtrage.
Prise en charge de l'interface dynamique du tunnel virtuel	7.3	N'importe lequel	Vous pouvez créer un VTI dynamique et l'utiliser pour configurer un VPN de site à site basé sur le routage dans une topologie en étoile.

Fonctionnalités	Version	Défense contre les menaces Minimum	Détails
Prise en charge d'EIGRP IPv4 pour le VTI	7.3	N'importe lequel	Les interfaces VTI statiques et dynamiques prennent en charge le protocole de routage EIGRP IPv4.
Prise en charge OSPFv2/v3 IPv4/v6 pour VTI	7.3	N'importe lequel	Les interfaces VTI statiques et dynamiques prennent en charge le protocole de routage OSPFv2/v3 IPv4/v6.
Packet Tracer dans le tableau de bord de surveillance VPN de site à site	7.3	N'importe lequel	Utilisez l'outil Packet Tracer dans le tableau de bord de la surveillance VPN de site à site pour dépanner les tunnels VPN de la défense contre les menaces. Écrans Nouveaux ou modifiés : **Présentation > Tableaux de bord > VPN de site à site**
Tableau de bord du VPN d'accès à distance	7.3	N'importe lequel	Utilisez le tableau de bord du VPN d'accès à distance pour surveiller les données en temps réel des sessions VPN d'accès à distance actives sur les périphériques. Écrans Nouveaux ou modifiés : **Présentation > Tableaux de bord > VPN d'accès à distance**
Déchargement de flux IPSec	7.2	N'importe lequel	Sur la Secure Firewall 3100, les flux IPsec sont déchargés par défaut. 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. Vous pouvez modifier la configuration à l'aide de FlexConfig et de la commande **flow-offload-ipsec**.

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.