Virtual Tunnel Interface

Ce chapitre décrit comment configurer un tunnel VTI.

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

ASA prend en charge une interface logique appelée Virtual Tunnel Interface (VTI). 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. Vous pouvez utiliser des routes dynamiques ou statiques. Le trafic sortant du VTI est chiffré et envoyé à l'homologue, et la SA associée déchiffre le trafic d'entrée vers le VTI.

Avec une interface VTI, il n'est plus nécessaire de configurer des listes d'accès aux cartes de chiffrement statiques et de les mapper aux interfaces. Vous n'avez plus à suivre tous les sous-réseaux distants et à les inclure dans la liste d'accès de la carte de chiffrement. Les déploiements deviennent plus simples, et le fait de disposer d'une VTI statique qui prend en charge un VPN fondé sur le routage avec un protocole de routage dynamique répond également à de nombreuses exigences d'un nuage privé virtuel.

VTI statique

Vous pouvez utiliser des configurations VTI statiques pour une connectivité de site à site dans laquelle un tunnel est toujours actif entre deux sites. Pour un VTI statique, vous devez définir une interface physique comme source de tunnel. Vous pouvez associer un maximum de 1 024 VTI par périphérique. Pour créer une interface VTI statique, consultez Ajouter une interface VTI, à la page 8.

VTI dynamique

Le VTI dynamique fournit une connectivité hautement sécurisée et évolutive pour les VPN de site à site. Le VTI dynamique facilite la configuration des homologues pour les déploiements en étoile dans les grandes entreprises. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Le VTI dynamique remplace les cartes de chiffrement dynamiques et la méthode dynamique

en étoile pour l'établissement des tunnels. Dans le centre de gestion, le VTI dynamique prend uniquement en charge la topologie concentrateur-étoile.

Le VTI dynamique utilise un modèle virtuel pour l'instanciation et la gestion dynamiques des interfaces IPsec. Le modèle virtuel génère dynamiquement l'interface d'accès virtuelle qui est 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. Le VTI dynamique prend également en charge les sites distants dynamiques DHCP. Pour créer une interface VTI dynamique, consultez Ajouter une interface VTI dynamique :, à la page 10.

Comment un ASA crée un tunnel VTI dynamique pour une session VPN

1. Créez un modèle virtuel sur l'ASA).

   Vous pouvez utiliser ce modèle pour plusieurs sessions VPN.
2. Associez ce modèle à un groupe de tunnels. Vous pouvez associer un modèle virtuel à plusieurs groupes de tunnels.
3. Le site distant initie une demande de tunnel auprès du concentrateur.
4. Le concentrateur authentifie le en étoile.
5. L'ASA utilise le modèle virtuel pour créer dynamiquement une interface d'accès virtuelle sur le concentrateur pour la session VPN avec le site distant.
6. Le concentrateur établit un tunnel VTI dynamique avec le site distant à l'aide de l'interface d'accès virtuelle.
7. Configurez l' de commande ikev2 route set interface afin d'annoncer l'adresse IP de l'interface VTI au moyen des échanges IKEv2. Cette option permet la joignabilité en monodiffusion entre les interfaces VTI afin que BGP ou la surveillance des chemins fonctionne à travers le tunnel.
8. À la fin de la session VPN, le tunnel se déconnecte et le concentrateur supprime l'interface d'accès virtuelle correspondante.

Lignes directrices pour les interfaces Virtual Tunnel Interfaces

Mode contexte et mise en grappe

- Pris en charge en mode unique uniquement.
- Aucune prise en charge de mise en grappe.

Mode pare-feu

Pris en charge en mode routé uniquement.

Prise en charge de BGP IPv4 et IPv6

Prend en charge le routage BGP IPv4 et IPv6 sur un VTI.

Prise en charge d'EIGRP

Prend en charge le routage EIGRP IPv4 et IPv6 sur un VTI.

Prise en charge d'OSPF IPv4 et IPv6

Prend en charge le routage OSPF IPv4 et IPv6 sur un VTI.

Prise en charge d'IPv6

- Vous pouvez configurer des VTI dotés d'adresses IPv6.
- La source et la destination du tunnel d'un VTI peuvent toutes deux avoir des adresses IPv6.
- Les combinaisons suivantes d'adresse IP de VTI (ou de version IP des réseaux internes) sur des versions d'IP publique sont prises en charge :
  - IPv6 sur IPv6
  - IPv4 sur IPv6
  - IPv4 sur IPv4
  - IPv6 sur IPv4
- Seules les adresses IPv6 statiques sont prises en charge comme source et destination du tunnel.
- L'interface source du tunnel peut avoir des adresses IPv6, et vous pouvez préciser laquelle utiliser comme point de terminaison du tunnel. Si vous ne précisez rien, la première adresse IPv6 globale de la liste est utilisée par défaut comme point de terminaison du tunnel.
- Vous pouvez préciser le mode de tunnel comme IPv6. Lorsque ce mode est précisé, le trafic IPv6 peut être acheminé par tunnel par le VTI. Cependant, pour un même VTI, le mode de tunnel peut être soit IPv4, soit IPv6.

Directives de configuration générale

- Si vous utilisez des cartes de chiffrement dynamiques et des VTI dynamiques dans vos VPN LAN-à-LAN, seuls les tunnels VTI dynamiques seront établis. 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 LAN-à-LAN 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. La terminaison des tunnels GRE sur un ASA n'est pas prise en charge.
- Vous pouvez utiliser des routes IPv4 statiques, BGP, OSPF ou EIGRP pour le trafic qui utilise l'interface de tunnel.
- Pour les VTI statiques et dynamiques, assurez-vous de ne pas utiliser l'interface borrow IP comme adresse IP source du tunnel pour une interface VTI.
- La MTU pour les VTI est définie automatiquement en fonction de l'interface physique sous-jacente. Cependant, si vous modifiez la MTU de l'interface physique après l'activation du VTI, vous devez désactiver et réactiver le VTI pour utiliser le nouveau paramètre de MTU.

- Pour le VTI dynamique, l'interface d'accès virtuel hérite de la MTU de l'interface source du tunnel configurée. Si vous ne précisez pas l'interface source du tunnel, l'interface d'accès virtuel hérite de la MTU de l'interface source sur laquelle l'ASA accepte la demande de session VPN.
- 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.
  - Même si une plateforme prend en charge plus de 1 024 interfaces, le nombre de VTI est limité au nombre de VLAN configurables sur cette plateforme. Par exemple, si un modèle prend en charge 500 VLAN, le nombre de tunnels correspond à 500 moins le nombre d'interfaces physiques configurées.
- Le VTI prend en charge les versions IKEv1 et IKEv2 et utilise IPsec pour envoyer et recevoir des données entre la source et la destination du tunnel.
- 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 seront rachetées 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 site à site, vous pouvez utiliser des noms autres que des adresses IP si la méthode d'authentification du tunnel repose sur des certificats numériques et/ou si l'homologue est configuré en mode agressif.
- Les configurations du VTI et de la carte de chiffrement peuvent coexister sur la même interface physique, à condition que l'adresse homologue configurée dans la carte de chiffrement et la destination du tunnel pour le VTI soient différentes.
- Les règles d'accès peuvent être appliquées sur une interface VTI pour contrôler le trafic via VTI.
- Le ping ICMP est pris en charge entre interfaces VTI.
- Si l'équipement homologue d'un tunnel VPN site à site IKEv2 envoie des charges utiles de requête de configuration IKEv2, l'ASA ne peut pas établir de tunnel IKEv2 avec cet équipement. Vous devez désactiver la requête config-exchange sur l'équipement homologue pour permettre à l'ASA d'établir un tunnel VPN avec celui-ci.
- Les VTI dynamiques prennent en charge la haute disponibilité (HA) et IKEv2.

Paramètres d'usine

- Par défaut, tout le trafic passant par VTI est chiffré.
- Par défaut, le niveau de sécurité pour les interfaces VTI est 0. Ce niveau de sécurité ne peut pas être modifié.

Limitations des VTI

L'ASA rejette les trames et paquets contenant des Security Group Tags (SGT) après le déchiffrement du VTI.

Le VTI dynamique ne prend pas en charge :

- ECMP et VRF
- Mise en grappes
- IKEv1
- Qualité de service

Pour les VTI dynamiques, si aucune source de tunnel n'est spécifiée, IKEv2 est activé sur toutes les interfaces de l'équipement, sauf celles dédiées à la gestion (management-only) et au basculement (failover).

Créer un tunnel VTI

Pour configurer un tunnel VTI, créez une proposition IPsec (ensemble de transformation). Vous devrez créer un profil IPsec qui fait référence à la proposition IPsec, suivi d'une interface VTI avec le profil IPsec. Configurez l'homologue distant avec des paramètres de proposition IPsec et de profil IPsec identiques. La négociation SA commencera lorsque tous les paramètres de tunnel seront configurés.

Remarque Pour l'ASA qui fait partie des deux domaines VTI du VPN et qui a une contiguïté de BGP sur l'interface physique :

Lorsqu'un changement d'état est déclenché en raison de la vérification de l'intégrité de l'interface, les routes de l'interface physique seront supprimées jusqu'à ce que la contiguïté BGP soit rétablie avec le nouvel homologue actif. Ce comportement ne s'applique pas aux interfaces logiques VTI.

Des listes de contrôle d'accès peuvent être appliquées à une interface VTI pour contrôler le trafic qui passe par le VTI. Pour autoriser tous les paquets provenant d'un tunnel IPsec sans vérifier les ACL des interfaces source et destination, saisissez la commande sysopt connection permit-vpn en mode de configuration globale.

Vous pouvez utiliser la commande suivante pour activer le trafic IPsec dans l'ASA sans vérifier les listes de contrôle d'accès :

hostname(config)# sysopt connection permit-vpn

Lorsqu'une interface externe et une interface VTI ont toutes deux un niveau de sécurité de 0, si une ACL est appliquée à l'interface VTI, elle ne sera pas atteinte si same-security-traffic n'est pas configuré.

Pour configurer cette fonctionnalité, utilisez la commande **same-security-traffic** en mode de configuration globale avec son argument **intra-interface** .

Procédure

Étape 1 Ajouter une proposition IPsec (ensembles de transformations)

Étape 2 Ajouter un profil IPsec.

Étape 3 Ajouter un tunnel VTI

Ajouter une proposition IPsec (ensembles de transformations)

Un ensemble de transformation est nécessaire pour sécuriser le trafic dans un tunnel VTI. Utilisé comme partie intégrante du profil IPsec, il s'agit d'un ensemble de protocoles et d'algorithmes de sécurité qui protège le trafic du VPN.

Avant de commencer

- Vous pouvez utiliser soit une clé prépartagée, soit des certificats pour authentifier la session IKE associée à un VTI. IKEv2 permet des méthodes d'authentification et des clés dissymétriques. Pour IKEv1 et IKEv2, vous devez configurer la clé prépartagée dans le groupe de tunnels utilisé pour le VTI.
- Pour l'authentification fondée sur des certificats au moyen d'IKEv1, vous devez préciser le point de confiance à utiliser du côté de l'initiateur. Pour le répondeur, vous devez configurer le point de confiance dans la commande tunnel-group. Pour IKEv2, vous devez configurer, dans la commande tunnel-group, le point de confiance à utiliser pour l'authentification, tant pour l'initiateur que pour le répondeur.

Procédure

Étape 1 Choisissez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec [ensembles de transformation])**.

Étape 2 Configurez IKEv1 ou IKEv2 pour établir l'association de sécurité.

- Configurez IKEv1.

a) Dans le panneau des propositions IKEv1 IPsec (ensembles Transform), cliquez sur **Add** (Ajouter).
b) Saisissez le **Set Name** (Nom de l'ensemble).
c) Conservez la sélection par défaut de la case **Tunnel**.
d) Sélectionnez **ESP Encryption** (Chiffrement ESP) et **ESP Authentication** (Authentification ESP).
e) Cliquez sur **OK**.

- Configurez IKEv2.

a) Dans le panneau des propositions IKEv2 IPsec, cliquez sur **Add** (Ajouter).
b) Saisissez **Name** (Nom), et **Encryption** (Chiffrement).
c) Choisissez **Integrity Hash** (Hachage d'intégrité).
d) Cliquez sur **OK**.

Ajouter un profil IPsec

Un profil IPsec contient les protocoles et les algorithmes de sécurité requis dans l'ensemble de proposition ou de transformation IPsec auquel il fait référence. Cela garantit un chemin de communication logique et sécurisé entre deux homologues VPN VTI de site à site.

Procédure

Étape 1 Choisissez **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec [ensembles de transformation])**.

Étape 2 Dans le panneau **IPsec Profile** (Profil IPsec), cliquez sur **Add** (Ajouter).

Étape 3 Saisissez le **Name** (Nom) du profil IPsec.

Étape 4 Saisissez la **proposition IKE v1 IPsec** ou la **proposition IKE v2 IPsec** créée pour le profil IPsec. Vous pouvez choisir un ensemble de transformation IKEv1 ou une proposition IKEv2 IPsec.

Étape 5 Si vous avez besoin d'une extrémité du tunnel VTI pour agir uniquement en tant que répondeur, cochez la case **Responder only** (Répondeur uniquement.

- Vous pouvez configurer une extrémité du tunnel VTI pour qu'elle fonctionne uniquement en tant que répondeur. L'extrémité configurée en mode répondeur uniquement n'initie ni le tunnel ni le renouvellement de clés.
- Si vous utilisez IKEv2, définissez une durée de vie de l'association de sécurité supérieure à la valeur de durée de vie définie dans le profil IPsec à l'extrémité initiatrice. Cela vise à faciliter un renouvellement de clés réussi par l'extrémité initiatrice et à garantir que les tunnels restent opérationnels.
- Si la configuration du renouvellement de clés à l'extrémité initiatrice est inconnue, supprimez le mode répondeur uniquement afin de rendre l'établissement de la SA bidirectionnel, ou configurez une durée de vie IPsec infinie à l'extrémité en mode répondeur uniquement afin d'éviter l'expiration.

Étape 6 (Facultatif) Cochez la case **Enable security association lifetime** (Activer la durée de vie de l'association de sécurité) et saisissez les valeurs de durée de l'association de sécurité en **kilo-octets** et **en secondes**.

Étape 7 (Facultatif) Cochez la case des **PFS Settings** (Paramètres PFS) pour activer PFS, puis sélectionnez le groupe Diffie-Hellman requis.

La confidentialité de transmission parfaite (PFS) génère une clé de session unique pour chaque échange chiffré. La clé de session unique protège l'échange contre tout déchiffrement ultérieur. Pour configurer PFS, vous devez sélectionner l'algorithme de dérivation de clé Diffie-Hellman à utiliser lors de la génération de la clé de session PFS. Les algorithmes de dérivation de clé génèrent des clés d'association de sécurité IPsec. Chaque groupe a un module de taille différent. Un module plus élevé offre une sécurité élevée, mais nécessite plus de temps de traitement. Vous devez avoir des groupes Diffie-Hellman correspondants sur les deux homologues.

Cela détermine la robustesse de l'algorithme de dérivation de la clé de chiffrement. L'ASA utilise cet algorithme pour dériver les clés de chiffrement et de hachage.

Étape 8 (Facultatif) Cochez la case **Enable sending certificate** (Activer l'envoi du certificat) et sélectionnez un **Trustpoint** (Point de confiance) qui définit le certificat à utiliser lors de l'initialisation d'une connexion de tunnel VTI. Cochez la case **Chain** (Chaîne), le cas échéant.

Étape 9 Cochez la case **Enable Reverse Route Injection** (Activer l'injection de route inverse) pour activer l'injection de route inverse (RRI) pour ce profil IPsec.

La RRI renseigne la table de routage d'un routeur interne exécutant des protocoles de routage dynamiques tels qu'OSPF, EIGRP sur ASA, ou RIP pour les clients VPN d'accès à distance ou les sessions LAN à LAN. La RRI est effectuée lors de la configuration et est considérée comme statique, restant en place jusqu'à ce que la configuration soit modifiée ou soit supprimée. L'ASA ajoute automatiquement des routes statiques à la table de routage et communique ces routes à son réseau privé ou aux routeurs de frontière à l'aide d'OSPF. N'activez pas RRI si vous spécifiez une source/destination (0.0.0.0/0.0.0.0) comme réseau protégé, car cela aura une incidence sur le trafic qui utilise votre route par défaut.

Étape 10 Cochez la case **Dynamic** (Dynamique) pour définir la route inverse comme dynamique.

Étape 11 Cliquez sur **OK**.

Étape 12 Dans le panneau principal **IPsec Proposals (Transform Sets) (Propositions IPsec [Ensembles de transformation])**, cliquez sur **Apply** (Appliquer).

Étape 13 Dans la boîte de dialogue **Preview CLI Commands** (Aperçu des commandes CLI), cliquez sur **Send** (Envoyer).

Ajouter une interface VTI

Pour créer une nouvelle interface VTI et établir un tunnel VTI, procédez comme suit :

Remarque Implémentez l'IP SLA pour vous assurer que le tunnel reste opérationnel lorsqu'un routeur dans le tunnel actif n'est pas disponible. Consultez la section Configurer le suivi de route statique dans le Guide de configuration des opérations générales ASA dans http://www.cisco.com/go/asa-config.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez **Add (Ajouter)** > **VTI Interface (Interface VTI)**. La fenêtre **Add VTI Interface** (Ajouter une interface VTI) s'affiche.

Étape 3 Dans l'onglet **General** (Général) :

a) Saisissez l'**ID VTI**. La plage est de 0 à 10 413. Jusqu'à 10413 interfaces VTI sont prises en charge.

b) Saisissez l'**Interface Name** (Nom de l'interface).

c) Assurez-vous que la case **Enable Interface** (Activer l'interface) est cochée.

d) Choisissez **IPv4** ou **IPv6** dans la liste déroulante **Path Monitoring** (Surveillance du chemin d'accès) et saisissez l'adresse IP de l'homologue.

e) Saisissez le **coût**. La plage est de 1 à 65 535.

Le coût détermine la priorité pour équilibrer la charge du trafic sur plusieurs VTI. Ce serveur a la priorité la plus élevée.

f) Pour configurer l'adresse IP :

Cliquez sur le bouton radio **Address** (Adresse) pour configurer une adresse IP et le masque de sous-réseau.

Ou

Cliquez sur le bouton radio **Unnumbered** (Non numéroté) pour choisir une interface dans la liste déroulante **IP Unnumbered** (IP non numérotée) afin d'emprunter son adresse IP. Vous pouvez choisir une interface de boucle ou une interface physique dans la liste.

Étape 4 Dans l'onglet **Advanced** (Avancé) :

a) Saisissez l'**adresse IP de destination**.

b) Choisissez l'interface source du tunnel dans la liste déroulante **Source Interface** (Interface source).

Vous pouvez sélectionner une interface de boucle ou une interface physique.

c) Sélectionnez la stratégie IPsec dans le champ **Tunnel Protection with IPsec Policy** (Protection du tunnel avec stratégie IPsec).
d) Sélectionnez le profil IPsec dans le champ **Tunnel Protection with IPsec Profile** (Protection du tunnel avec profil IPsec).
e) Cochez la case **Enable Tunnel Mode IPv4 IPsec** (Activer le mode tunnel IPsec IPv4).

Étape 5 Cliquez sur **OK**.

Étape 6 Dans le panneau **Interfaces**, cliquez sur **Apply** (Appliquer).

Étape 7 Dans la boîte de dialogue **Preview CLI Commands** (Aperçu des commandes CLI), cliquez sur **Send** (Envoyer).

Après le chargement de la configuration mise à jour, le nouveau VTI apparaît dans la liste des interfaces. Ce nouveau VTI peut être utilisé pour créer un VPN de site à site IPsec.

Exemple

Exemple de configuration d'un tunnel VTI (avec IKEv2) entre l'ASA et un périphérique IOS :

```
ASA :

crypto ikev2 policy 1
 encryption aes-gcm-256
 integrity null
 group 21
 prf sha512
 lifetime seconds 86400
!
crypto ipsec ikev2 ipsec-proposal gcm256
 protocol esp encryption aes-gcm-256
 protocol esp integrity null
!
crypto ipsec profile asa-vti
 set ikev2 ipsec-proposal gcm256
!
interface Tunnel 100
 nameif vti
 ip address 10.10.10.1 255.255.255.254
 tunnel source interface [asa-source-nameif]
 tunnel destination [router-ip-address]
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile asa-vti
!
tunnel-group [router-ip-address] ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
crypto ikev2 enable [asa-interface-name]


IOS :
```

```
!
crypto ikev2 proposal asa-vti
 encryption aes-gcm-256
 prf sha512
 group 21
!
crypto ikev2 policy asa-vti
 match address local [router-ip-address]
 proposal asa-vti
!
crypto ikev2 profile asa-vti
 match identity remote address [asa-ip-address] 255.255.255.255
 authentication local pre-share key cisco
 authentication remote pre-share key cisco
 no config-exchange request
!
crypto ipsec transform-set gcm256 esp-gcm 256
!
crypto ipsec profile asa-vti
 set ikev2-profile asa-vti
 set transform-set gcm256
!
interface tunnel 100
 ip address 10.10.10.0 255.255.255.254
 tunnel mode ipsec ipv4
 tunnel source [router-interface]
 tunnel destination [asa-ip-address]
 tunnel protection ipsec profile asa-vti
!
```

Ajouter une interface VTI dynamique :

Pour créer un modèle virtuel pour le VTI dynamique :

Remarque Implémentez l'IP SLA pour vous assurer que le tunnel reste opérationnel lorsqu'un routeur dans le tunnel actif n'est pas disponible. Consultez « Configure Static Route Tracking » (Configurer le suivi de route statique) dans le Guide de configuration des opérations générales ASA dans http://www.cisco.com/go/asa-config.

Avant de commencer

Assurez-vous d'avoir configuré un profil IPsec et une interface IP non numérotée.

Procédure

Étape 1 Choisissez **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces**.

Étape 2 Choisissez **Add (Ajouter)** > **DVTI Interface (Interface DVTI)**. La fenêtre **Add DVTI Interface** (Ajouter une interface DVTI) s'affiche.

Étape 3 Dans l'onglet **General** (Général) :

a) Saisissez l'**ID DVTI**. Cet ID peut être n'importe quelle valeur comprise entre 1 et 10413. Jusqu'à 1 024 interfaces VTI sont prises en charge par périphérique.

b) Saisissez l'**Interface Name** (Nom de l'interface).

c) Cochez la case **Enable Interface** (Activer l'interface).

d) Choisissez une interface dans la liste déroulante **IP Unnumbered**.

Le modèle virtuel hérite de l'adresse IP de l'interface sélectionnée. Veillez à utiliser une adresse IP différente de l'adresse IP source du tunnel. Vous pouvez choisir n'importe quelle interface physique ou une adresse de boucle avec retour configurée sur le périphérique.

e) Saisissez une description pour le VTI dynamique dans le champ **Description**.

Étape 4 Dans l'onglet **Advanced** (Avancé) :

a) Choisissez une interface source du tunnel dans la liste déroulante **Source Interface** (Interface source). L'adresse IP de cette interface sera l'adresse IP de destination pour le site distant. Vous pouvez sélectionner uniquement les interfaces physiques et de boucle dans la liste.

b) Cochez la case **Enable IPv6 Source Address** (Activer l'adresse source IPv6) pour accepter les demandes de session VPN uniquement à partir de l'interface configurée avec l'adresse IP source du tunnel. Si vous n'activez pas cette option, l'ASA accepte les demandes de session VPN de n'importe quelle interface.

L'interface d'accès virtuel hérite également de la MTU de l'interface source du tunnel configurée. Si vous n'activez pas l'option ci-dessus, l'interface d'accès virtuel hérite de la MTU de l'interface source à partir de laquelle l'ASA accepte la demande de session VPN.

c) Choisissez le profil IPsec dans la liste déroulante **Tunnel Protection with IPsec Profile** (Protection du tunnel avec profil IPsec).

d) Cochez la case **Enable Tunnel Mode IP Overlay for IPSec (Activer la superposition IP en mode tunnel pour IPsec)** et sélectionnez le bouton radio **IPv4** ou **IPv6** pour activer le mode de tunnel IPsec.

Étape 5 Dans l'onglet **IPv6** :

a) Cliquez sur le bouton de navigation **IPv6 Address Unnumbered** (Adresse IPv6 non numérotée) et choisissez une adresse IPv6 dans la liste.

Toutes les interfaces d'accès virtuelles clonées à partir du modèle virtuel auront la même adresse IP.

b) Cliquez sur **OK**.

Étape 6 Dans la boîte de dialogue **Preview CLI Commands** (Aperçu des commandes CLI), vous pouvez afficher les commandes de modèle virtuel.

Étape 7 Cliquez sur **Send** (envoyer).

Prochaine étape

Associez ce modèle à un groupe de tunnels. Pour en savoir plus, consultez Groupes de tunnels de site à site.

Historique des fonctionnalités de Virtual Tunnel Interface

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de Dynamic Virtual Tunnel Interface	9.19(1)	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. Le VTI dynamique facilite la configuration des homologues pour les déploiements en étoile dans les grandes entreprises. Un seul VTI dynamique peut remplacer plusieurs configurations de VTI statique sur le concentrateur. Vous pouvez ajouter de nouveaux satellites à un concentrateur sans modifier la configuration du concentrateur. Écrans nouveaux/modifiés : **Configuration > Device Setup > Interface Settings > Interfaces > Add > DVTI Interface**
Prise en charge du routage OSPF IPv4 et IPv6	9.19(1)	Prend en charge le protocole de routage OSPF IPv4 et IPv6 sur un VTI.
Prise en charge d'EIGRP	9.19(1)	Prend en charge le protocole de routage EIGRP IPv4 et IPv6 sur un VTI.
Prise en charge de l'interface loopback pour les VTI statiques et dynamiques	9.19(1)	Vous pouvez désormais définir une interface de bouclage comme interface source pour un VTI. La possibilité d'hériter de l'adresse IP d'une interface de bouclage au lieu d'une adresse IP configurée de manière statique a également été ajoutée. 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. Écrans nouveaux/modifiés : **Configuration (configuration)** > **Device Setup (configuration de l'appareil)** > **Interface Settings (paramètres de l'interface)** > **Interfaces** > **Add VTI Interface (ajouter une interface VTI)** > **Advanced (avancé)**.
Prise en charge de l'ID de tunnel local	9.17(1)	L'ASA prend en charge un ID de tunnel local unique qui permet à l'ASA d'avoir plusieurs tunnels IPsec derrière une NAT pour se connecter à Cisco Umbrella Secure Internet Gateway (SIG). L'identité locale est utilisée pour configurer une identité unique par tunnel IKEv2, au lieu d'une identité globale pour tous les tunnels.
Prise en charge d'IPv6 sur VTI statique	9.16(1)	L'ASA prend en charge les adresses IPv6 dans les configurations Virtual Tunnel Interfaces (VTI). Une interface source de tunnel VTI peut avoir une adresse IPv6, que vous pouvez configurer pour l'utiliser comme terminal du tunnel. Si l'interface source du tunnel a plusieurs adresses IPv6, vous pouvez spécifier l'adresse à utiliser, sinon la première adresse globale IPv6 de la liste est utilisée par défaut. Le mode du tunnel peut être IPv4 ou IPv6, mais il doit être identique au type d'adresse IP configuré sur VTI pour que le tunnel soit actif. Une adresse IPv6 peut être attribuée à l'interface source ou de destination du tunnel dans un VTI.

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de 1024 interfaces VTI par périphérique	9.16(1)	Le nombre de VTI maximum à configurer sur un périphérique est passé de 100 à 1 024. Même si une plateforme prend en charge plus de 1 024 interfaces, le nombre de VTI est limité au nombre de VLAN configurables sur cette plateforme. Par exemple, l'ASA 5510 prend en charge 100 VLAN, le nombre de tunnels serait donc de 100 moins le nombre d'interfaces physiques configurées. Écrans nouveaux ou modifiés : aucun
Prise en charge du serveur relais DHCP sur VTI	9.14(1)	L'ASA permet de configurer les interfaces VTI comme interfaces de connexion du serveur relais DHCP. Nous avons modifié l'écran suivant pour spécifier une interface VTI pour le relais DHCP : **Configuration** > **Device Management (Gestion des périphériques)** > **DHCP** > **DHCP Relay (Relais DHCP)** > **DHCP Relay Interface Servers (Serveurs d'interface de relais DHCP)**
Prise en charge d'IKEv2, de l'authentification par certificat et de l'ACL dans VTI	9.8(1)	Virtual Tunnel Interface (VTI) prend désormais en charge BGP (VTI statique). Vous pouvez désormais utiliser IKEv2 en modes autonome et à haute disponibilité. Vous pouvez utiliser l'authentification par certificat en configurant un point de confiance dans le profil IPsec. Vous pouvez également appliquer des listes d'accès sur le VTI à l'aide des commandes access-group pour filtrer le trafic d'entrée. Nous avons introduit des options pour sélectionner le point de confiance pour l'authentification par certificat dans l'écran suivant : **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec (ensembles de transformation))** > **IPsec Profile (Profil IPsec)** > **Add (Ajouter)**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
Prise en charge de Virtual Tunnel Interface (VTI)	9.7(1)	L'ASA est enrichi d'une nouvelle interface logique appelée Virtual Tunnel Interface (VTI), utilisée pour représenter un tunnel VPN vers un homologue. Ces interfaces prennent en charge le VPN basé sur le routage avec des profils IPsec associés à chaque extrémité du tunnel. Avec une interface VTI, vous n'avez plus besoin de configurer des listes d'accès aux cartes de chiffrement statiques et de les mapper aux interfaces. Nous avons introduit les écrans suivants : **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec (ensembles de transformation))** > **IPsec Profile (Profil IPsec)** **Configuration** > **Site-to-Site VPN (VPN de site à site)** > **Advanced (Avancé)** > **IPsec Proposals (Transform Sets) (Propositions IPsec (ensembles de transformation))** > **IPsec Profile (Profil IPsec)** > **Add (Ajouter)** > **Add IPsec Profile (Ajouter un profil IPsec)** **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add (Ajouter)** > **VTI Interface (Interface VTI)** **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add (Ajouter)** > **VTI Interface (Interface VTI)** > **General (Général)** **Configuration** > **Device Setup (Configuration du périphérique)** > **Interface Settings (Paramètres d'interface)** > **Interfaces** > **Add (Ajouter)** > **VTI Interface (Interface VTI)** > **Advanced (Avancé)**

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.