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 entrant 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 ni à les inclure dans l'ACL 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 9.

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 établir les 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 12.

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

1. Créez un modèle virtuel sur l'ASA (**interface virtual-Template** *template_number* **type tunnel**).

   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 site distant.
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'option de 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.
- Pour les VTI statiques, vous pouvez configurer un maximum de 1 024 VTI 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 configurées 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 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.
- Pour les VTI dynamiques, le nombre maximal d'interfaces d'accès virtuelles créées dynamiquement peut être de 1 024 ou de la limite totale d'interfaces de la plateforme, selon la valeur la plus faible.
- 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 à laquelle le profil IPsec est associé. Configurez l'homologue distant avec des paramètres de proposition IPsec et de profil IPsec identiques. La négociation SA commencera lorsque tous les paramètres du tunnel seront configurés.

Remarque Pour l'ASA qui fait partie des deux domaines VPN VTI et qui présente une contiguïté 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 autoriser le trafic IPsec à travers l'ASA sans vérifier les ACL :

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** .

Pour en savoir plus, consultez Permettre le trafic intra-interface (hairpinning).

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

Ajoutez un ensemble de transformation IKEv1 ou une proposition IPsec IKEv2 pour établir l'association de sécurité.

Ajouter un ensemble de transformation IKEv1 :

crypto ipsec ikev1 transform-set {*transform-set-name* | *chiffrement* | *authentification*}

Exemple :

```
ciscoasa(config)#crypto ipsec ikev1 transform-set SET1 esp-aes esp-sha-hmac
```

Le chiffrement spécifie quelle méthode de chiffrement protège les flux de données IPsec :

- esp-aes : utilise AES avec une clé de 128 bits.
- esp-aes-192 : utilise AES avec une clé de 192 bits.
- esp-aes-256 : utilise AES avec une clé de 256 bits.
- esp-null : pas de chiffrement.

L'authentification spécifie la méthode d'authentification pour protéger les flux de données IPsec :

- esp-md5-hmac : utilise MD5/HMAC-128 comme algorithme de hachage.

- esp-sha-hmac : utilise SHA/HMAC-160 comme algorithme de hachage.
- esp-none : aucune authentification HMAC.

Ajouter une proposition IPsec IKEv2.

Remarque
Pour la plateforme IOS, utilisez la commande **no config-exchange request** dans le mode de configuration du profil IKEv2 pour désactiver les options d'échange de configuration. Consultez http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book/sec-cr-c2.html#wp3456426280 pour de plus amples renseignements.

- Précisez un nom pour la proposition IPsec :

  crypto ipsec ikev2 ipsec-proposal *nom de la proposition IPsec*

Exemple :

```
ciscoasa(config)#crypto ipsec ikev2 ipsec-proposal SET1
```

- Précisez les paramètres de sécurité en mode de configuration crypto IPsec ikev2 ipsec-proposal :

  protocol esp {encryption {aes | aes-192 | aes-256 | aes-gcm | aes-gcm-192 | aes-gcm-256 | null} | integrity {sha-1 | sha-256 | sha-384 | sha-512 | null}

Exemple :

```
ciscoasa(config-ipsec-proposal)#protocol esp encryption aes aes-192
```

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 Définissez un nom pour le profil :

crypto ipsec profile *nom*

Exemple :

```
ciscoasa(config)#crypto ipsec profile PROFILE1
```

Étape 2 Définissez la proposition IKEv1 ou IKEv2. Vous pouvez choisir un ensemble de transformation IKEv1 ou une proposition IKEv2 IPsec.

a) Définissez l'ensemble de transformation IKEv1.

- Pour définir la proposition IKEv1, saisissez la commande suivante dans le sous-mode de commande crypto ipsec profile :

  set ikev1 transform set *set_name*

Dans cet exemple, SET1 est l'ensemble de propositions IKEv1 créé précédemment.

```
ciscoasa(config-ipsec-profile)#set ikev1 transform-set SET1
```

b) Définissez la proposition IKEv2.

- Pour définir la proposition IKEv2, saisissez la commande suivante dans le sous-mode de commande de profil crypto ipsec :

  set ikev2 ipsec-proposal *IPsec_proposal_name*

  Dans cet exemple, SET1 est la proposition IKEv2 IPsec créée précédemment.

  ```
  ciscoasa(config-ipsec-profile)#set ikev2 ipsec-proposal SET1
  ```

Étape 3 (Facultatif) Précisez la durée de l'association de sécurité :

set security-association lifetime {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

Exemple :

```
ciscoasa(config-ipsec-profile)#set security-association lifetime
seconds 120 kilobytes 10000
```

Étape 4 (Facultatif) Configurez la fin du tunnel VTI pour qu'elle agisse uniquement en tant que répondeur :

responder-only

- 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 vous utilisez IKEv1, IOS doit toujours être en mode de répondeur uniquement, car IOS ne prend pas en charge le mode de canal continu. L'ASA devient l'initiateur de la session et du renouvellement de clés.
- 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 5 (Facultatif) Précisez le groupe de PFS. La confidentialité de transmission parfaite (PFS) génère une clé de session unique pour chaque échange chiffré. Cette 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.

set pfs { **group14** }

Exemple :

```
ciscoasa(config-ipsec-profile)# set pfs group14
```

Étape 6 (Facultatif) Précisez un point de confiance qui définit le certificat à utiliser lors de l'initialisation d'une connexion de tunnel VTI.

set trustpoint *nom*

Exemple :

```
ciscoasa(config-ipsec-profile)#set trustpoint TPVTI
```

Étape 7 (Facultatif) Activez l'injection de route inverse (RRI) pour ce profil IPsec et définissez la route inverse comme dynamique.

set reverse-route [dynamique]

Exemple :

```
ciscoasa(config-ipsec-profile)#set reverse-route dynamic
```

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 Créez une nouvelle interface de tunnel :

interface tunnel *tunnel_interface_number*

Précisez un ID de tunnel, dans une plage de 0 à 10 413. Jusqu'à 10 413 interfaces VTI sont prises en charge.

Exemple :

```
ciscoasa(config)#interface tunnel 100
```

Étape 2 Saisissez le nom de l'interface VTI.

Saisissez la commande suivante dans le sous-mode de commande **interface tunnel** :

nameif *interface name*

Exemple :

```
ciscoasa(config-if)#nameif vti
```

Étape 3 Saisissez l'adresse IP de l'interface VTI.

ip address *IP address mask*

Exemple :

```
ciscoasa(config-if)#ip address 192.168.1.10 255.255.255.254
```

Étape 4 Saisissez une adresse IPv4 ou IPv6 pour une interface dont hérite le modèle virtuel.

Vous pouvez choisir n'importe quelle interface physique ou une adresse de boucle avec retour configurée sur le périphérique. Toutes les interfaces d'accès virtuelles clonées à partir du modèle virtuel auront la même adresse IP.

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

Exemple :

```
ciscoasa(config-if)#ip unnumbered loopback1
```

Étape 5 Spécifiez l'interface source du tunnel.

tunnel source interface *interface_name*

L'interface source peut être une interface physique ou une interface de boucle.

Exemple :

```
ciscoasa(config-if)#tunnel source interface outside
```

Étape 6 Spécifiez l'adresse IP de destination du tunnel.

tunnel destination *ip_address*

Exemple :

```
ciscoasa(config-if)#tunnel destination 10.1.1.1
```

Étape 7 Configurez le tunnel avec le mode tunnel IPsec IPv4.

tunnel mode ipsec *ipv4*

Exemple :

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

Étape 8 Attribuez le profil IPsec au tunnel.

tunnel protection ipsec *IPsec profile*

Exemple :

```
ciscoasa(config-if)#tunnel protection ipsec Profile1
```

Étape 9 Attribuez un sélecteur de trafic pour l'interface VTI statique.

tunnel protection policy *acl_name*

La liste d'accès peut contenir un ou plusieurs sélecteurs de liste. Si vous ne configurez pas cette commande, l'interface VTI statique propose des sélecteurs any-any, ce qui est le comportement par défaut.

Exemple :

```
ciscoasa(config)# access-list Spoke-to-Hub extended permit ip 209.165.200.225 255.255.255.224
 any
ciscoasa(config-if)# tunnel protection ipsec policy Spoke-to-Hub
```

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 Créez un nouveau modèle virtuel :

interface virtual-Template *template_number* **type tunnel**

template_number est le numéro unique du modèle virtuel. La plage est comprise entre 1 et 10 413.

Le modèle d'interface ne doit pas être à l'état d'arrêt. Voici les paramètres obligatoires pour le modèle virtuel :

- Nom d'interface
- Mode de tunnel IPSec
- Profil IPsec du tunnel

Exemple :

```
ciscoasa(config)#interface virtual-Template 101 type tunnel
```

Étape 2 Précisez le nom de l'interface de modèle virtuel VTI dynamique.

Saisissez la commande suivante en mode de configuration **interface** :

nameif *interface_name*

L'ASA crée dynamiquement des interfaces d'accès virtuelles en tant que <*Virtual_Template_name*>_va<*n*>. Par exemple, si le nom du modèle virtuel est dVTI101, les interfaces d'accès virtuelles seront dVTI101_va1, dVTI101_va2, etc. Si vous souhaitez modifier un modèle virtuel, vous devez l'arrêter à l'aide de la commande **shutdown**.

Exemple :

```
ciscoasa(config-if)#nameif dVTI101
```

Étape 3 Configurez une adresse IPv4 ou IPv6 d'une interface dont le modèle virtuel hérite.

ip unnumbered *interface-name*

ipv6 unnumbered *interface-name*

Le modèle virtuel peut hériter de l'adresse IP de n'importe quelle interface physique ou d'une adresse de boucle configurée sur le périphérique. Toutes les interfaces d'accès virtuelles clonées à partir du modèle virtuel auront la même adresse IP.

Exemple :

```
ciscoasa(config-if)#ip unnumbered loopback1
```

Étape 4 (Facultatif) Précisez l'interface source du tunnel.

tunnel source interface *interface_name*

L'interface source peut être une interface physique ou une interface de boucle.

L'ASA accepte les demandes de session VPN uniquement de l'interface configurée comme adresse IP source du tunnel. Si vous ne spécifiez pas cette interface, l'ASA accepte les demandes de session VPN reçues de n'importe quelle interface. L'interface d'accès virtuel hérite 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 de laquelle l'ASA accepte la demande de session VPN.

Exemple :

```
ciscoasa(config-if)#tunnel source interface outside1
```

Étape 5 Précisez le mode de protection du tunnel comme IPv4 ou IPv6.

tunnel mode ipsec {**ipv4** | **ipv6**}

Exemple :

```
ciscoasa(config-if)#tunnel mode ipsec ipv4
```

Étape 6 Attribuez un profil IPsec au tunnel.

tunnel protection ipsec profile *ipsec_profile*

Ce profil IPsec configure les paramètres IPSec/IKE requis pour négocier l'échange.

Exemple :

```
ciscoasa(config-if)#tunnel protection ipsec profile Profile1
```

Étape 7 Associez le modèle virtuel à un groupe de tunnels.

tunnel-group *tunnel_group_name* **type** *type*

tunnel-group *tunnel_group_name* **ipsec-attributes**

virtual-template *template_number*

Vous pouvez associer le même modèle virtuel à plusieurs groupes de tunnels. L'ASA utilise le modèle virtuel pour créer des interfaces d'accès virtuelles individuelles pour chaque session VPN.

Exemple :

```
ciscoasa(config)#tunnel-group DVTI_spoke1 type ipsec-l2l
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#virtual-template 101
```

Étape 8 Activez le routage dynamique pour le groupe de tunnels.

tunnel-group *tunnel_group_name* **ipsec-attributes**

ikev2 route accept any

ikev2 route set interface

La commande **ikev2 route accept any** permet à l'ASA d'accepter toutes les adresses IP d'interface de tunnel reçues lors des échanges IKEv2. Par défaut, cette option est activée.

La commande **ikev2 route set interface** permet à l'ASA d'envoyer l'adresse IP de l'interface du tunnel pendant les échanges IKEv2. Cette option permet la connectivité en monodiffusion entre les interfaces VTI pour que BGP fonctionne sur le tunnel.

Le routage dynamique est activé pour les groupes de tunnels à l'aide de BGP/OSPF/EIGRP. Après avoir configuré le modèle virtuel, vous devez configurer une politique de routage pour acheminer le trafic VTI dynamique entre les périphériques sur le tunnel VTI. Vous devez également configurer une règle de contrôle d'accès pour autoriser le trafic chiffré.

Exemple :

```
ciscoasa(config)#tunnel-group DVTI_spoke1 ipsec-attributes
ciscoasa(config-tunnel-ipsec)#ikev2 route set interface
ciscoasa(config-tunnel-ipsec)#ikev2 route accept any
```

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. Commandes nouvelles/modifiées : **interface virtual-Template, ip unnumbered, ipv6 unnumbered, tunnel protection ipsec policy**
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. Commandes nouvelles/modifiées : **tunnel source interface**, **ip unnumbered**, **ipv6 unnumbered**

Nom de la caractéristique	Versions	Renseignements sur les fonctionnalités
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. Commandes nouvelles ou modifiées : **local-identity-from-cryptomap**
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. Commandes nouvelles/modifiées : **tunnel source interface**, **tunnel destination**, **tunnel mode**
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. Commandes nouvelles ou modifiées : aucune
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 les commandes suivantes : **dhcprelay server** *ip_address vti_ifc_name*.
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 la commande suivante dans le mode de configuration du profil IPsec : **set trustpoint**.
Prise en charge de l'interface de tunnel virtuel (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 commandes suivantes : **crypto ipsec profile, interface tunnel, responder-only, set ikev1 transform-set, set pfs, set security-association lifetime, tunnel destination, tunnel mode ipsec, tunnel protection ipsec profile, tunnel source interface**.

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.

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.

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.