Dépannage des problèmes courants d’interconnexion de réseaux LAN à LAN et d’accès à distance au protocole IPsec du VPN

Table des matières

Introduction

Informations générales

Conditions préalables

La configuration de VPN IPsec ne fonctionne pas

Les clients VPN ne peuvent pas se connecter avec ASA

Le client interrompt fréquemment la connexion à la première tentative ou la connexion VPN sécurisée est interrompue par le pair. Reason 433" ou "Connexion VPN sécurisée interrompue par l'homologue Reason 433:(Reason Not Specified by Peer)"

Les utilisateur de l'accès à distance et d'EZVPN se connectent au VPN mais ne peuvent pas accéder aux ressources externes

Impossible d'accéder aux serveurs dans DMZ

Impossible de se connecter m=Plus de trois utilisateurs de client VPN

Impossible de lancer la session ou une application et transfert lent après l'établissement du tunnel

Impossible d'initier un tunnel VPN depuis ASA

Impossible de faire circuler le trafic à travers le tunnel VPN

Configurer un homologue de sauvegarde pour un tunnel VPN sur la même carte de chiffrement

Désactiver/Redémarrer un tunnel VPN

Certains tunnels ne sont pas chiffrés.

Erreur : – %ASA-5-713904 : Groupe = DefaultRAGroup, IP = x.x.x.x, ...Mode de transaction v2 non pris en charge.Tunnel terminé

Erreur : – %ASA-6-722036 : Groupe client-groupe Utilisateur xxxx IP x.x.x.x Transmission d'un grand paquet 1220 (seuil 1206)

Message d'erreur lorsque la QoS est activée à une extrémité du tunnel VPN

AVERTISSEMENT : Entrée de carte de chiffrement incomplète

Erreur : – %ASA-4-400024 : IDS:2151 Grand paquet ICMP provenant de l'interface externe

Erreur : – %ASA-4-402119 : IPSEC : Réception d'un paquet de protocole (SPI=spi, sequence number= seq_num) de Remote_IP (username) vers Local_IP ayant échoué à la vérification de la fonctionnalité anti-relecture

Message d'erreur - %ASA-4-407001 : Refuser le trafic pour local-host interface_name:inside_address, limite de licence dépassée

Error Message - %VPN_HW-4-PACKET_ERROR:

Message d'erreur : Command rejected: Supprimer la connexion de chiffrement entre VLAN XXXX et XXXX, d'abord

Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Paquet abandonné - Option d'échelle de fenêtre non valide pour la session x.x.x.x:27331 à x.x.x.x:23 [Initiator(flag 0, factor 0) Responder (flag 1, factor 2)]

%ASA-5-305013 : Règles NAT asymétriques jumelées pour l'aval et l'amont. Mettez

à jour les flux liés à ce problème

%ASA-5-713068 : Message de notification inhabituel reçu : notify_type

%ASA-5-720012 : (VPN secondaire) n'a pas pu mettre à jour les données d'exécution du basculement pour les capacités IPSec sur l'installation de réserve (ou) %ASA-6-720012 : (unité VPN) n'a pas pu mettre à jour les données d'exécution du basculement pour les capacités IPSec sur l'installation de réserve

Erreur : – %ASA-3-713063 : Adresse de pair IKE non configurée pour la destination 0.0.0.0

Erreur : %ASA-3-752006 : Tunnel Manager n'a pas pu envoyer un message KEY_ACQUIRE

Erreur : %ASA-4-402116 : IPSEC : Réception d'un paquet ESP (SPI= 0x99554D4E, numéro d'ordre= 0x9E) de XX.XX.XX.XX (user= XX.XX.XX.XX) vers YY.YY.YY.YY

Échec de lancement de l'installateur VA de 64 bits pour activer l'adaptateur virtuel, en raison de l'erreur 0xffffffff

Le client VPN Cisco ne fonctionne pas avec la carte de données sous Windows 7

Alerte : « La fonctionnalité VPN pourrait ne pas fonctionner du tout ».

Erreur de remplissage d'IPSec

Le tunnel VPN est déconnecté toutes les 18 heures

Le flux de trafic n'est pas maintenu après la renégociation du tunnel LAN à LAN

Le message d'erreur déclare que la bande passante a atteint pour la fonctionnalité de chiffrement

Problème : Échec du trafic de chiffrement sortant dans le tunnel IPsec, même si le trafic de déchiffrement entrant fonctionne

Divers

Informations connexes

Introduction

Ce document décrit les solutions les plus courantes pour les problèmes VPN IPsec.

Informations générales

Les solutions décrites dans ce document proviennent directement des demandes de service que l'équipe d'assistance technique Cisco a résolues. La plupart de ces solutions sont mises en oeuvre avant le dépannage approfondi d'une connexion VPN IPsec. Ce document fournit un résumé des procédures courantes à essayer avant de commencer à dépanner une connexion.

Les exemples de configuration présentés dans ce document sont destinés à être utilisés sur des routeurs et des dispositifs de sécurité. Presque tous les concepts sont applicables au VPN 3000. Référez-vous à Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage pour une explication des commandes de débogage courantes utilisées pour dépanner les problèmes IPsec sur le logiciel Cisco IOS®.

Remarque : SA ne transmet pas le trafic de multidiffusion sur les tunnels VPN IPsec.

Avertissement : beaucoup des solutions présentées dans ce document peuvent mener à une perte provisoire de toute connectivité VPN IPsec sur un périphérique. Il est recommandé d'implémenter ces solutions avec prudence et conformément à votre politique de contrôle des modifications.

Conditions préalables

Exigences

Cisco recommande de connaître la configuration VPN IPsec sur ces périphériques Cisco :

- Routeurs Cisco IOS®
- Dispositif de sécurité de la gamme Cisco ASA 5500

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco IOS®
- Dispositif de sécurité de la gamme Cisco ASA 5500

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Reportez-vous aux conventions des conseils techniques Cisco pour plus d’information sur les conventions utilisées dans ce document.

La configuration de VPN IPsec ne fonctionne pas

Problème

- Une solution VPN IPsec récemment configurée ou modifiée ne fonctionne pas.
- Une configuration actuelle de VPN IPsec ne fonctionne plus.

Solutions

Cette section contient des solutions pour les problèmes de VPN IPsec les plus courants. Bien qu'elles ne soient pas répertoriées dans un ordre particulier, ces solutions peuvent être utilisées comme liste de contrôle pour vérifier avant de vous engager dans une résolution approfondie. Toutes ces solutions proviennent directement des demandes de service du TAC et ont résolu de nombreux problèmes.

- Activer NAT-Traversal (problème #1 de VPN RA)
- Tester correctement la connectivité
- Activer ISAKMP
- Activer/Désactiver PFS
- Effacer des associations de sécurité anciennes ou existantes (tunnels)
- Vérifier la durée de vie d'ISAKMP
- Activer ou désactiver les Keepalives d'ISAKMP
- Ressaisir ou récupérer les clés pré-partagées
- Clé pré-partagée non correspondante
- Supprimer et ré-appliquer des cartes de chiffrement
- Vérification de la présence des commandes Sysopt (/ASA uniquement)
- Vérifier l'identité d'ISAKMP
- Vérifier le délai d'attente d'inactivité/de session

- Vérifier que les listes de contrôle d’accès sont correctes et liées à la crypto-carte
- Vérifier les stratégies ISAKMP
- Vérification du routage
- Vérifier que Transform-Set est correct
- Vérifier les numéros et le nom de la séquence de la carte de chiffrement
- Vérifier que l'adresse IP de l'homologue est correcte
- Vérifier le groupe de tunnels et les noms de groupe
- Désactiver XAUTH pour des homologues L2L
- Réserve VPN en voie d'épuisement
- Problèmes de latence pour le trafic du client VPN

Remarque : Certaines commandes de ces sections sont déplacées vers une deuxième ligne pour des raisons d'espace.

Activer NAT-Traversal (problème #1 de VPN RA)

La fonction NAT-Traversal (ou NAT-T) permet au trafic VPN de traverser des périphériques NAT ou PAT, tels que le routeur SOHO de Linksys. Si NAT-T n'est pas activé, les utilisateurs du client VPN semblent souvent se connecter à l'ASA sans problème, mais ils ne peuvent pas accéder à un réseau interne derrière l'appliance de sécurité. Si NAT-T dans le périphérique NAT/PAT n'est pas activé, vous pouvez recevoir le message d'erreur regular translation creation failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.694 dans l'ASA.

Si vous ne pouvez pas effectuer de connexions simultanées à partir de la même adresse IP, la connexion VPN sécurisée s'est arrêtée localement par le client. Raison 412 : Le message d'erreur L'homologue distant ne répond plus apparaît. Activez NAT-T dans le périphérique VPN de tête de réseau pour résoudre cette erreur.

Remarque : Avec le logiciel Cisco IOS® version 12.2(13)T et ultérieure, NAT-T est activé par défaut dans Cisco IOS®.

La commande suivante active NAT-T sur le dispositif de sécurité Cisco. Le 20 dans cet exemple est la durée de keepalive (par défaut).

ASA

<#root>

```
securityappliance(config)#

crypto isakmp nat-traversal 20
```

Les clients doivent être modifiés pour que cela fonctionne correctement. Dans Client VPN Cisco, accédez à Entrées de connexion et cliquez sur Modifier. Une nouvelle fenêtre s'ouvre et vous devez sélectionner l'onglet Transport. Sous cet onglet, cliquez sur Activer la tunnellisation transparente et sur la case d'option IPSec sur UDP (NAT/PAT). Cliquez ensuite sur Enregistrer et testez la connexion.

Il est important d'autoriser l'UDP 4500 pour les ports NAT-T, UDP 500 et ESP par la configuration d'une liste de contrôle d'accès, car l'ASA agit comme un périphérique NAT. Référez-vous àConfiguration d'un tunnel IPsec à travers un pare-feu avec NATpour plus d'informations sur la configuration ACL dans ASA.

Tester correctement la connectivité

La connectivité VPN est testée à partir des périphériques situés derrière le terminal de cryptage. De nombreux utilisateurs testent la connectivité VPN en exécutant la commande ping à partir du point d'extrémité de cryptage. Bien que la commande ping fonctionne généralement à cette fin, il est important d'envoyer votre requête ping à partir de l'interface correcte. Si la commande ping provient d'une source incorrecte, il peut apparaître que la connexion VPN a échoué lorsqu'elle fonctionne correctement. En voici un exemple :

ACL de chiffrement routeur A

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

ACL de chiffrement routeur B

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

Dans cet exemple, le ping doit provenir de l'intérieur du réseau derrière l'un des routeurs. Les ACL de chiffrement sont uniquement configurées pour chiffrer le trafic avec ces adresses source. Les données Apingprovenant des interfaces externes de l'un des routeurs ne sont pas chiffrées. Utilisez les options étendues de la commande ping en mode d'exécution privilégié pour envoyer une requête ping à partir de l'interface interne d'un routeur :

<#root>

```
routerA#

ping

Protocol [ip]:

Target IP address: 192.168.200.10

Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:

Extended commands [n]: y


Source address or interface: 192.168.100.1

Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:

Packet sent with a source address of 192.168.100.1

!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

Imaginez que les routeurs de ce schéma soient remplacés par des appareils de sécurité ASA. La commande utilisée pour tester la connectivité peut également provenir de l'interface interne avec

le mot clé insidekeyword :

<#root>

```
securityappliance#
```

ping inside 192.168.200.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Il n'est pas recommandé de cibler l'interface interne d'un dispositif de sécurité avec votreping. Si vous devez cibler l'interface interne avec la commande ping, vous devez activer management-access sur cette interface, sinon l'appliance ne répond pas"

<#root>

```
securityappliance(config)#
```

management-access inside

En cas de problème de connectivité, même la phase 1 du VPN ne fonctionne pas. Sur l'ASA, si la connectivité échoue, le résultat de l'ASA est similaire à cet exemple, qui indique une configuration d'homologue de chiffrement incorrecte possible ou une configuration de proposition ISAKMP incorrecte :

<#root>

```
Router#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG2
```

L'état peut être de MM_WAIT_MSG2 à MM_WAIT_MSG5, ce qui indique l'échec de l'échange d'état concerné en mode principal (MM). La sortie de l'association de sécurité de chiffrement peut

être activée lorsque la phase 1 est active ; comme dans cet exemple :

<#root>

```
Router#

show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Activer ISAKMP

S'il n'y a aucune indication qu'un tunnel VPN IPsec fonctionne comme prévu, il est possible que l'ISAKMP ne soit pas activé. Assurez-vous d'avoir activé ISAKMP sur vos périphériques. Utilisez l'une de ces commandes pour activer ISAKMP :

Cisco IOS®

<#root>

```
router(config)#

crypto isakmp enable
```

Cisco ASA (remplacé à l'extérieur par l'interface souhaitée) :

<#root>

```
securityappliance(config)#

crypto isakmp enable outside
```

Vous pouvez également recevoir cette erreur lorsque vous activez ISAKMP sur l'interface externe :

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

La cause de l'erreur peut être liée au client derrière l'ASA reçoit PAT vers le port UDP 500 avant qu'ISAKMP puisse être activé sur l'interface. Une fois la traduction PAT supprimée (clear xlate), l'ISAKMP peut être activé. Vérifiez que les numéros de port UDP 500 et 4500 sont réservés pour la négociation des connexions ISAKMP avec l'homologue. Lorsque ISAKMP n'est pas activé sur l'interface, le client VPN affiche un message d'erreur similaire à celui-ci :

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

Pour résoudre cette erreur, activez l'ISAKMP sur l'interface de chiffrement de la passerelle VPN.

Activer/Désactiver PFS

Dans les négociations IPsec, Perfect Forward Secrecy (PFS) s'assure que chaque nouvelle clé cryptographique n'est liée à aucune clé précédente. Activez ou désactivez PFS sur les deux homologues de tunnel ; sinon, le tunnel IPsec de LAN à LAN (L2L) n'est pas établi dans le routeur ASA / Cisco IOS®. Le protocole PFS (Perfect Forward Secrecy) est un protocole propriétaire de Cisco et n'est pas pris en charge sur les périphériques tiers.

ASA:

PFS est désactivé par défaut et pour activer PFS, exécutez la commande pfsavec le mot clé enable en mode de configuration group-policy. Pour désactiver PFS, entrez le mot clé disable.

<#root>

```
hostname(config-group-policy)#

pfs {enable | disable}
```

Pour supprimer l'attribut PFS de la configuration, exécutez la forme no de cette commande. Une

stratégie de groupe peut hériter d'une valeur pour PFS d'une autre stratégie de groupe. Exécutez la forme no de cette commande pour empêcher le transfert d'une valeur.

<#root>

```
hostname(config-group-policy)#
```

no pfs

Routeur Cisco IOS®

- Pour spécifier qu'IPsec doit demander PFS quand de nouvelles associations de sécurité sont demandées pour l'entrée de crypto-carte, exécutez la commande set pfsen mode de configuration de crypto-carte.
- Pour spécifier qu'IPsec doit exiger PFS lorsqu'il reçoit des demandes pour de nouvelles associations de sécurité, exécutez la commande set pfsen mode de configuration crypto map.
- Pour spécifier qu'IPsec ne doit pas demander PFS, exécutez la forme no de cette commande. Par défaut, PFS n'est pas demandé si un groupe n'est pas spécifié avec cette commande et group1 est utilisé comme valeur par défaut.

```
set pfs [group1 | group2]
no set pfs
```

Pour la commande set pfs :

- group1 — Spécifie qu'IPsec doit utiliser le groupe modulaire de nombres premiers 768 bits Diffie-Hellman quand le nouvel échange Diffie-Hellman est exécuté.
- group2 : indique qu'IPsec doit utiliser le groupe de modules premiers Diffie-Hellman 1024 bits lorsque le nouvel échange Diffie-Hellman est effectué.

Exemple :

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

```
set pfs group2
```

Effacer les associations de sécurité anciennes ou actuelles (tunnels)

Si ce message d'erreur s'affiche sur le routeur Cisco IOS®®, l'association de sécurité a expiré ou a été effacée. Le périphérique final du tunnel distant ne sait pas qu'il utilise l'association de sécurité expirée pour envoyer un paquet (et non un paquet d'établissement d'association de sécurité). Lorsqu'une nouvelle association de sécurité est établie, la communication reprend. Par conséquent, initiez le trafic à travers le tunnel pour créer une nouvelle association de sécurité et rétablir le tunnel.

<#root>

```
%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x  has no SA
```

Si vous effacez les associations de sécurité ISAKMP (Phase 1) et IPsec (Phase 2), c'est souvent la meilleure solution pour résoudre les problèmes VPN IPsec. Si vous effacez les SA, vous pouvez résoudre une grande variété de messages d'erreur et de comportements sans dépannage approfondi. Bien que cette technique puisse être facilement utilisée dans n'importe quelle situation, il est recommandé d'effacer d'abord les SA après avoir modifié ou ajouté une configuration VPN IPsec actuelle. En outre, bien qu'il soit possible d'effacer uniquement des associations de sécurité spécifiques, vous pouvez tirer parti de l'effacement global des associations de sécurité sur le périphérique. Une fois les associations de sécurité effacées, il peut être nécessaire d'envoyer du trafic à travers le tunnel pour les rétablir.



Avertissement : À moins de spécifier quelles associations de sécurité doivent être effacées, les commandes mentionnées ici peuvent effacer toutes les associations de sécurité sur le périphérique. Procédez avec prudence si d'autres tunnels VPN IPsec sont en service.

---

1. Afficher les associations de sécurité avant de les effacer
    1. Cisco IOS®

        <#root>

```
router#
show crypto isakmp sa
router#
show crypto ipsec sa
```

---

2. Appareils de sécurité Cisco ASA

<#root>

```
securityappliance#
show crypto isakmp sa
securityappliance#
show crypto ipsec sa
```

---

2. Effacez les associations de sécurité car chaque commande peut être saisie comme indiqué en gras ou avec les options affichées.

A. Cisco IOS®

1. ISAKMP (phase I)

<#root>

```
router#
clear crypto isakmp
 ?
  <0 - 32766>  connection id of SA
  <cr>
```

IPsec (phase II)

<#root>

```
router#
clear crypto sa
 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
```

```
<cr>
```

---

2. Appareils de sécurité Cisco ASA

    1. ISAKMP (phase I)

    <#root>

    ```
    securityappliance#
    ```

    clear crypto isakmp sa

    ---

    2. IPsec (phase II)

    <#root>

    ```
    security appliance#
    ```

    clear crypto ipsec sa

    ```
     ?

      counters  Clear IPsec SA counters
      entry     Clear IPsec SAs by entry
      map       Clear IPsec SAs by map
      peer      Clear IPsec SA by peer
      <cr>
    ```

Vérifier la durée de vie d'ISAKMP

Si les utilisateurs sont fréquemment déconnectés à travers le tunnel L2L, ce problème peut être configuré à vie dans ISAKMP SA. Si une différence se produit dans la durée de vie ISAKMP, vous pouvez recevoir le message %ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Échec lors de la tentative de nouvelle clé de phase 1 en raison du message d'erreur de collision dans /ASA. La valeur par défaut est 86 400 secondes ou 24 heures. En règle générale, une durée de vie plus courte fournit des négociations ISAKMP plus sécurisées (jusqu'à un certain point), cependant, avec des durées de vie plus courtes, l'appliance de sécurité configure les futures SA IPsec plus rapidement.

Une correspondance est établie lorsque les deux stratégies de deux homologues contiennent les mêmes valeurs de paramètre de chiffrement, de hachage, d'authentification et Diffie-Hellman, et

lorsque la stratégie de l'homologue distant spécifie une durée de vie inférieure ou égale à la durée de vie de la stratégie comparée. Si les durées de vie ne sont pas identiques, la durée de vie la plus courte (à partir de la stratégie de l'homologue distant) est utilisée et aucune correspondance acceptable n'est trouvée, l'IKE refuse la négociation et l'association de sécurité IKE n'est pas établie.

- Spécifiez la durée de vie de la SA: Cet exemple définit une durée de vie de 4 heures (14400 secondes) et la valeur par défaut est 86400 secondes (24 heures).

ASA:

<#root>

```
hostname(config)#

isakmp policy 2 lifetime  14400
```

Routeur Cisco IOS® :

<#root>

```
R2(config)#

crypto isakmp policy 10

R2(config-isakmp)#

lifetime 86400
```

Si la durée de vie maximale configurée est dépassée, vous recevez ce message d'erreur quand la connexion VPN est terminée :

Connexion VPN sécurisée arrêtée localement par le client. Raison 426 : Durée de vie maximale configurée dépassée.

Pour résoudre cette erreur, définissez la valeur de durée de vie sur zéro (0). Pour définir la durée de vie d'une association de sécurité IKE à l'infini, le VPN doit toujours être connecté et ne se

termine pas :

```
hostname(config)#isakmp policy 2 lifetime 0
```

Vous pouvez également désactiver re-xauth dans la stratégie de groupe pour résoudre le problème.

Activer ou désactiver les Keepalives d'ISAKMP

Si vous configurez des keepalives ISAKMP, cela permet d'empêcher l'abandon sporadique de LAN à LAN ou de VPN d'accès à distance. Cela inclut les clients VPN, les tunnels et les tunnels abandonnés après une période d'inactivité. Cette fonctionnalité permet aux points d'extrémité du tunnel de surveiller la présence continue d'un homologue distant et de signaler sa propre présence à cet homologue. Si l'homologue ne répond plus, le périphérique supprime la connexion. Pour que les keepalives ISAKMP fonctionnent, les deux terminaux VPN doivent les prendre en charge.

Configurez les keepalives ISAKMP dans Cisco IOS® en exécutant cette commande :

<#root>

```
router(config)#

crypto isakmp keepalive 15
```

Exécutez ces commandes pour configurer les keepalives ISAKMP sur les dispositifs de sécurité ASA :

Cisco ASA pour le groupe de tunnels nommé 10.165.205.222 :

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes
```

```
securityappliance(config-tunnel-ipsec)#

isakmp keepalive
   threshold 15 retry 10
```

Dans certaines situations, il est nécessaire de désactiver cette fonctionnalité pour résoudre le problème. Par exemple, si le client VPN est derrière un pare-feu qui empêche les paquets DPD. Avec Cisco ASA, pour le groupe de tunnels nommé 10.165.205.222 - Désactivez le traitement IKE keepalive, qui est activé par défaut :

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive



disable
```

Désactiver Keepalive pour un client Cisco VPN 4.x

1. Accédez à%System Root% > Program Files > Cisco Systems > VPN Client > Profiles sur le PC client qui rencontre le problème pour désactiver IKE keepalive, et modifiez le fichier PCF, le cas échéant, pour la connexion.
2. Remplacez la valeur de ForceKeepAlives=0(default) par ForceKeepAlives=1. Les Keepalive sont des produits propriétaires Cisco et ne sont pas pris en charge par des périphériques tiers.

Ressaisir ou récupérer les clés pré-partagées

Dans de nombreux cas, une simple erreur typographique peut être à blâmer quand un tunnel VPN

IPsec ne fonctionne pas. Par exemple, sur le dispositif de sécurité, les clés pré-partagées deviennent masquées une fois qu'elles sont saisies. Cet obscurcissement empêche de voir si une clé est incorrecte. Assurez-vous que vous avez correctement entré les clés pré-partagées sur chaque point d'extrémité VPN.

Dans le VPN d'accès à distance, vérifiez que le nom du groupe et la ou les clés pré-partagées valides sont entrés dans le client CiscoVPN. Vous pouvez rencontrer cette erreur si le nom du groupe ou la ou les clés pré-partagées ne correspondent pas entre le client VPN et le périphérique de tête de réseau.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```



Avertissement : Si vous supprimez des commandes liées au chiffrement, vous pouvez désactiver un ou tous vos tunnels VPN. Utilisez ces commandes avec prudence et reportez-vous à la stratégie de contrôle des modifications de votre organisation avant de supprimer les commandes liées au chiffrement.

Exécutez ces commandes pour supprimer et ressaisir la clé pré-partagée keysecretkeypour l'homologue10.0.0.1ou le groupvpngroupdans Cisco IOS® :

VPN Cisco de LAN-à-LAN:

<#root>

```
router(config)#

no crypto isakmp key secretkey
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

VPN Cisco d'accès à distance:

<#root>

```
router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

Exécutez ces commandes pour supprimer et ressaisir la clé pré-partagée secretkeypour l'homologue10.0.0.1sur les dispositifs de sécurité /ASA :

Cisco 6.x :

<#root>

```
(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco /ASA 7.x et versions ultérieures :

<#root>

```
securityappliance(config)#

tunnel-group 10.0.0.1
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key

securityappliance(config-tunnel-ipsec)#

ikev1




pre-shared-key
   secretkey
```

Clé pré-partagée non correspondante

L'initialisation du tunnel VPN est déconnectée. Ce problème se produit en raison d'une clé pré-partagée non concordante au cours des négociations de la phase I. Le message MM_WAIT_MSG_6dans la commande show crypto isakmp indique une clé pré-partagée non concordante comme indiqué dans cet exemple :

<#root>

```
ASA#

show crypto isakmp sa


Active SA: 1
Rekey SA: 0 (A tunnel reports 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :

MM_WAIT_MSG_6
```

Pour résoudre ce problème, saisissez à nouveau la clé prépartagée dans les deux appliances. la clé pré-partagée doit être unique et correspondre. Pour plus d'informations, reportez-vous à la section Saisir à nouveau ou récupérer des clés prépartagées.

Supprimer et ré-appliquer des cartes de chiffrement

Lorsque vous effacez les associations de sécurité, et qu'il ne résout pas le problème VPN IPsec, supprimez et réappliquez la crypto-carte appropriée pour résoudre une grande variété de problèmes qui incluent des abandons intermittents du tunnel VPN et des défaillances de certains sites VPN.



Avertissement : Si vous supprimez une crypto-carte d'une interface, elle supprime tous les tunnels IPsec associés à cette crypto-carte. Procédez avec prudence, reportez-vous à ces étapes et tenez compte de la politique de contrôle des modifications de votre organisation avant d'aller de l'avant.

Exécutez ces commandes pour supprimer et remplacer une carte de chiffrement dans Cisco IOS® :

Commencez en supprimant la carte de chiffrement de l'interface. Exécutez la forme no de la commande crypto map :

<#root>

```
router(config-if)#

no crypto map mymap
```

Continuez à exécuter le formulaire pour supprimer une carte de chiffrement complète :

<#root>

```
router(config)#

no crypto map mymap 10
```

Remplacez la crypto-carte sur l’interface Ethernet0/0 pour l’homologue10.0.0.1. Cet exemple montre la configuration minimale requise pour la crypto-carte :

<#root>

```
router(config)#

crypto map mymap 10 ipsec-isakmp

router(config-crypto-map)#

match address 101

router(config-crypto-map)#

set transform-set mySET

router(config-crypto-map)#

set peer 10.0.0.1

router(config-crypto-map)#

exit

router(config)#

interface ethernet0/0

router(config-if)#

crypto map mymap
```

Exécutez ces commandes pour supprimer et remplacer une carte de chiffrement sur l'ASA. Commencez en supprimant la carte de chiffrement de l'interface. Exécutez la forme no de la commande crypto map :

<#root>

```
securityappliance(config)#

no crypto map mymap interface outside
```

Continuez à exécuter la forme pour supprimer les autres commandes de crypto-carte :

<#root>

```
securityappliance(config)#

no crypto map mymap 10 match
   address 101

securityappliance(config)#

no crypto map mymap set
   transform-set mySET

securityappliance(config)#

no crypto map mymap set
   peer 10.0.0.1
```

Remplacez la crypto-carte pour peer10.0.0.1. Cet exemple montre la configuration minimale requise pour la crypto-carte :

<#root>

```
securityappliance(config)#

crypto map mymap 10 ipsec-isakmp

securityappliance(config)#

crypto map mymap 10
   match address 101

securityappliance(config)#

crypto map mymap 10 set
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

Si vous supprimez et réappliquez la crypto-carte, cela résout également le problème de connectivité si l'adresse IP de la tête de réseau a été modifiée.

Vérification de la présence des commandes Sysopt (ASA uniquement)

Les commandes sysopt connection permit-ipsecandsysopt connection permit-vpnallow paquets d'un tunnel IPsec et leurs données utiles pour contourner les ACL d'interface sur l'appliance de sécurité. Les tunnels IPsec qui se terminent sur le dispositif de sécurité sont susceptibles d'échouer si l'une de ces commandes n'est pas activée.

- Dans le logiciel du dispositif de sécurité version 7.0 et antérieure, la commande sysopt appropriée pour cette situation est sysopt connection permit-ipsec.
- Dans le logiciel du dispositif de sécurité version 7.1(1) et ultérieure, la commande sysopt appropriée pour cette situation est sysopt connection permit-vpn.
- Dans 6.x, cette fonctionnalité est désactivée par défaut. Avec /ASA 7.0(1) et versions ultérieures, cette fonctionnalité est activée par défaut. Exécutez ces commandes show pour déterminer si la commande sysoptpertinente est activée sur votre périphérique :

Cisco ASA:

<#root>

```
securityappliance#

show running-config all sysopt

no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret

sysopt connection permit-vpn

!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

Exécutez cette commande pour activer la commande correcte pour votre périphérique :

Cisco ASA:

<#root>

```
securityappliance(config)#
```

sysopt connection permit-vpn

Si vous ne voulez pas exécuter la commande sysopt connection, autorisez explicitement le trafic requis de la source à la destination. Par exemple, de Remote vers Local LAN du périphérique distant et « UDP port 500 » pour l'interface externe du périphérique distant vers l'interface externe du périphérique local, dans l'ACL externe.

Vérifier l'identité d'ISAKMP

Les échecs de négociation IKE dans les VPN IPsec résultent souvent d'une incapacité d'un homologue à reconnaître l'identité de son partenaire, c'est ainsi. Lorsque deux homologues utilisent IKE pour établir des associations de sécurité IPsec, chaque homologue envoie son identité ISAKMP à l'homologue distant. Ils envoient leur adresse IP ou leur nom d'hôte selon la façon dont l'identité ISAKMP de chacun est paramétrée. Par défaut, l'identité ISAKMP de l'unité de pare-feu est définie sur l'adresse IP.

En règle générale, définissez l'appliance de sécurité et les identités de ses homologues de la même manière pour éviter un échec de négociation IKE. Pour définir l'ID de phase 2 à envoyer à l'homologue, exécutez la commande isakmp identitycommand en mode de configuration globale :

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

OU:

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

OU:

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

Si le tunnel VPN ne démarre pas après un changement de configuration d'ASA avec l'outil de migration de configuration ASA ; ces messages apparaissent dans le journal :

[IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x,Stale PeerTblEntry found, removing! (saisie périmée PeerTblEntry retrouvée, retrait en cours!)

[IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match! (Échec de retrait du pair de la table de corrélation, aucune correspondance!)

[IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete() : Aucun SPI pour déterminer la SA de phase 2!

[IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match! (Échec de retrait du pair de la table de corrélation, aucune correspondance!)

Vérifier le délai d'attente d'inactivité/de session

Si le délai d'inactivité est défini sur 30 minutes (valeur par défaut), il abandonne le tunnel au bout de 30 minutes si aucun trafic ne passe. Le client VPN est déconnecté après 30 minutes, quel que soit le paramètre de délai d'inactivité, et reçoit l'erreur PEER_DELETE-IKE_DELETE_UNSPECIFIED.

Configurez idle timeoutandsession timeoutasnone pour que le tunnel soit toujours actif, et que le tunnel ne soit jamais abandonné même lorsque des périphériques tiers sont utilisés.

ASA

Exécutez la commande vpn-idle-timeout en mode de configuration group-policy ou en mode de configuration username pour configurer le délai d'attente utilisateur :

<#root>

```
hostname(config)#

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-idle-timeout none
```

Configurez une durée maximale pour les connexions VPN avec la commande vpn-session-timeout en mode de configuration de stratégie de groupe ou en mode de configuration de nom d'utilisateur :

<#root>

```
hostname(config)#

group-policy DfltGrpPolicy attributes

hostname(config-group-policy)#

vpn-session-timeout none
```

Quand vous avez tunnel-all configuré, vous n'avez pas besoin de configurer idle-timeout parce que, même si vous configurez VPN-idle timeout, il ne fonctionne pas comme tous les processus de trafic à travers le tunnel (puisque tunnel-all est configuré).

Par conséquent, le trafic (ou même le trafic généré par le PC) ne laisse pas le délai d'inactivité se produire.

Routeur Cisco IOS®

Exécutez la commande crypto ipsec security-association idle-time en mode de configuration globale ou en mode de configuration crypto map pour configurer le minuteur d'inactivité de l'association de sécurité IPsec. Par défaut, les temporisateurs de SA IPsec sont désactivés:

<#root>

crypto ipsec security-association idle-time

seconds

Le temps est mesuré en secondes, ce qui permet à un homologue inactif de maintenir une SA. Les valeurs valides pour l'argument seconds sont comprises entre 60 et 86 400.

Vérifier que les listes de contrôle d’accès sont correctes et liées à la carte de chiffrement

Dans une configuration VPN IPsec classique, deux listes d'accès sont utilisées. L'une permet d'exempter le trafic destiné au tunnel VPN à partir du processus NAT, l'autre définit le trafic à crypter. cela inclut une ACL de chiffrement dans une configuration de LAN à LAN ou une ACL de tunnel partagé dans une configuration d'accès à distance. Lorsque ces listes de contrôle d'accès sont mal configurées ou manquées, le trafic circule dans une direction à travers le tunnel VPN, ou n'est pas envoyé à travers le tunnel.

Assurez-vous que vous liez la ACL de chiffrement avec la carte de chiffrement en exécutant la commande crypto map match address en mode de configuration globale. Vérifiez que vous avez configuré toutes les listes d'accès pour terminer vos configurations VPN IPsec et que ces listes d'accès définissent le trafic correct. Cette liste contient des éléments à valider lorsque vous suspectez qu'une liste de contrôle d'accès est la cause de problèmes avec votre VPN IPsec.

Confirmez votre exemption NAT et les ACL de chiffrement spécifient le trafic correct. Si vous avez plusieurs tunnels VPN et plusieurs ACL de chiffrement, assurez-vous que ces ACL ne se chevauchent pas. Vérifiez également que votre périphérique est configuré pour utiliser la liste de contrôle d'accès d'exemption NAT. Sur un routeur, cela signifie que vous exécutez la commande route-map. Sur l'ASA, vous exécutez la commande enat (0). Une liste de contrôle d'accès d'exemption NAT est requise pour les configurations de LAN-à-LAN et les configurations d'accès à distance.

Dans l'exemple suivant, un routeur Cisco IOS® est configuré pour exempter le trafic envoyé entre192.168.100.0 /24 et192.168.200.0 /24ou192.168.1.0 /24de la NAT. Le trafic destiné à n'importe où ailleurs est soumis à la surcharge NAT :

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
```

```
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

Les listes de contrôle d’accès d’exemption NAT fonctionnent uniquement avec l’adresse IP ou les réseaux IP, tels que les exemples mentionnés (access-list noNAT), et doivent être identiques aux listes de contrôle d’accès de la crypto-carte. Les listes de contrôle d'accès d'exemption NAT ne fonctionnent pas avec les numéros de port (par exemple, 23, 25, etc.). Dans un environnement VOIP, où les appels vocaux entre les réseaux sont communiqués via le VPN, les appels vocaux ne fonctionnent pas si les listes de contrôle d'accès NAT 0 ne sont pas correctement configurées. Avant le dépannage, il est recommandé de vérifier l'état de la connectivité VPN, car le problème peut être dû à une mauvaise configuration des listes de contrôle d'accès exemptées NAT.

Vous pouvez recevoir le message d'erreur comme indiqué s'il y a une mauvaise configuration dans les ACL d'exemption NAT (nat 0).

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

Exemple incorrect :

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

eq 25

Si l'exemption NAT (nat 0) ne fonctionne pas correctement, essayez de la supprimer et exécutez la commande NAT 0. Assurez-vous que vos listes de contrôle d’accès ne sont pas en arrière et qu’elles sont du bon type. Les listes de contrôle d’accès d’exemption NAT et de chiffrement pour les configurations LAN à LAN doivent être écrites du point de vue du périphérique sur lequel la liste de contrôle d’accès est configurée. Par conséquent, les listes de contrôle d’accès doivent se refléter. Dans cet exemple, un tunnel LAN à LAN est configuré entre192.168.100.0 /24

et192.168.200.0 /24.

ACL de chiffrement routeur A:

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

ACL de chiffrement routeur B:

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

Bien qu'il ne soit pas illustré, le même concept s'applique aux appareils de sécurité ASA. Dans ASA, les ACL de tunnel partagé pour les configurations d'accès à distance doivent être des listes d'accès standard qui autorisent le trafic vers le réseau où les clients VPN ont besoin d'un accès. Les routeurs Cisco IOS® peuvent utiliser une liste de contrôle d’accès étendue pour les tunnels partagés. Dans la liste de contrôle d'accès étendue, l'utilisation de « any » à la source dans la liste de contrôle d'accès du tunnel partagé est similaire à la désactivation du tunnel partagé. Utilisez uniquement les réseaux sources dans la liste de contrôle d’accès étendue pour le tunnel partagé.

Exemple correct :

<#root>

```
access-list 140 permit ip
```

10.1.0.0 0.0.255.255

```
 10.18.0.0 0.0.255.255
```

Exemple incorrect :

<#root>

```
access-list 140 permit ip
```

```
any

 10.18.0.0 0.0.255.255
```

Cisco IOS®

<#root>

```
router(config)#

access-list 10 permit ip 192.168.100.0

router(config)#

crypto isakmp client configuration group MYGROUP

router(config-isakmp-group)#

acl 10
```

Cisco ASA

<#root>

```
securityappliance(config)#

access-list 10 standard
   permit 192.168.100.0 255.255.255.0

securityappliance(config)#

group-policy MYPOLICY internal

securityappliance(config)#

group-policy MYPOLICY attributes

securityappliance(config-group-policy)#

split-tunnel-policy
   tunnelspecified

securityappliance(config-group-policy)#
```

```
split-tunnel-network-list
   value 10
```

Configuration d'exemption dans la version ASA 8.3 pour le tunnel VPN de site à site :

Un VPN site à site doit être établi entre HOASA et BOASA avec les deux ASA avec la version 8.3. La configuration d'exemption NAT sur HOASA ressemble à ceci :

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

Vérifier les stratégies ISAKMP

Si le tunnel IPsec n'est pas UP, vérifiez si les stratégies ISAKMP correspondent aux homologues distants. Cette stratégie ISAKMP s'applique à la fois au VPN IPsec de site-à-site (L2L) et au VPN IPsec d'accès à distance. Si les clients VPN Cisco ou le VPN site à site ne peuvent pas établir le tunnel avec le périphérique distant, vérifiez que les deux homologues contiennent les mêmes valeurs de paramètre de cryptage, de hachage, d'authentification et Diffie-Hellman. Vérifiez que la stratégie d'homologue distant spécifie une durée de vie inférieure ou égale à la durée de vie dans la stratégie que l'initiateur a envoyée. Si les durées de vie ne sont pas identiques, le dispositif de sécurité utilise la durée de vie plus courte. Si aucune correspondance acceptable n'existe, ISAKMP refuse la négociation et la SA n'est pas établie.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

Voici un exemple de message de journal détaillé :

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

Ce message apparaît généralement en raison d'une erreur de correspondance dans les stratégies ISAKMP ou d'une instruction NAT 0 manquée. En outre, ce message apparaît :

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

Ce message indique que les messages de phase 2 sont dans la file d'attente une fois la phase 1 terminée. Ce message d'erreur est dû à l'une des raisons suivantes :

- Non correspondance de phase sur l'un des homologues
- La liste de contrôle d’accès empêche les homologues de terminer la phase 1

Ce message arrive généralement après **`l'échec de la suppression de l'homologue de la table d'homologues, aucun`** message d'erreur **`match !`**. Si le client VPN Cisco ne parvient pas à connecter le périphérique de tête de réseau, le problème peut être la non-correspondance de la stratégie ISAKMP. Le périphérique de tête de réseau doit correspondre à l'une des propositions IKE du client VPN Cisco. Pour la stratégie ISAKMP et l'ensemble de transformation IPsec utilisés sur l'ASA, le client VPN Cisco ne peut pas utiliser une stratégie avec une combinaison de DES et SHA. Si vous utilisez DES, vous devez utiliser MD5 pour l'algorithme de hachage, ou vous pouvez utiliser d'autres combinaisons telles que 3DES avec SHA et 3DES avec MD5.

Vérification du routage

Assurez-vous que vos périphériques de cryptage, tels que les routeurs et les dispositifs de sécurité ASA, disposent des informations de routage appropriées pour envoyer le trafic sur votre tunnel VPN. S’il existe d’autres routeurs derrière votre périphérique de passerelle, vérifiez qu’ils peuvent atteindre le tunnel et quels sont les réseaux situés de l’autre côté. Un composant clé du routage dans un déploiement VPN est l’injection de routage inverse (RRI). Le RRI place des entrées dynamiques pour des réseaux distants ou des clients VPN dans la table de routage d'une passerelle VPN. Ces routes sont utiles pour le périphérique sur lequel elles sont installées et pour d’autres périphériques sur le réseau, car les routes installées par RRI peuvent être redistribuées via des protocoles de routage tels que EIGRP ou OSPF.

Dans une configuration de réseau local à réseau local, il est important que chaque point d’extrémité dispose d’une ou de plusieurs routes vers les réseaux où il doit chiffrer le trafic. Dans

cet exemple, le routeur A doit disposer de routes vers les réseaux situés derrière le routeur B, via10.89.129.2. Le routeur B doit disposer d'une route similaire vers192.168.100.0 /24. La première façon de s'assurer que chaque routeur connaît la ou les routes appropriées consiste à configurer des routes statiques pour chaque réseau de destination. Par exemple, Router A peut avoir ces instructions de route configurées :

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

Si le routeur A a été remplacé par un ASA, la configuration peut ressembler à ceci :

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

S'il existe un grand nombre de réseaux derrière chaque point d'extrémité, la configuration des routes statiques devient difficile à gérer. Au lieu de cela, il est recommandé d'utiliser l'injection de route inverse. RRI place les routes de la table de routage pour tous les réseaux distants répertoriés dans la liste de contrôle d'accès de chiffrement. Par exemple, l'ACL de chiffrement et la carte de chiffrement de Router A peuvent ressembler à ceci :

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

reverse-route

```
 set transform-set mySET
 match address 110
```

Si le routeur A a été remplacé par ASA, la configuration peut ressembler à ceci :

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET

crypto map mymap 10 set reverse-route
```

Dans une configuration d'accès à distance, des changements de routage ne sont pas toujours nécessaires. Cependant, si d'autres routeurs existent derrière le routeur de passerelle VPN ou l'appareil de sécurité, ces routeurs doivent apprendre le chemin vers les clients VPN. Dans cet exemple, imaginez que les clients VPN reçoivent des adresses dans la plage 10.0.0.0 /24lorsqu'ils se connectent.

Si aucun protocole de routage n'est en service entre la passerelle et l'autre routeur, des routes statiques peuvent être utilisées sur des routeurs tels que Router 2 :

<#root>

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

Si un protocole de routage tel qu'EIGRP ou OSPF est en service entre la passerelle et d'autres routeurs, il est recommandé d'utiliser le Reverse Route Injection comme décrit. Le RRI ajoute automatiquement des routes pour le client VPN à la table de routage de la passerelle. Ces routes peuvent alors être distribuées aux autres routeurs dans le réseau.

Routeur Cisco IOS® :

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET


reverse-route


crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Appliance de sécurité Cisco ASA :

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET

crypto dynamic-map dynMAP 10 set reverse-route


crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Le problème de routage se produit si le pool d'adresses IP attribuées aux clients VPN chevauche les réseaux internes du périphérique de tête de réseau. Pour plus d'informations, référez-vous à la section Chevauchement de réseaux privés .

Vérifiez que Transform-Set est correct

Assurez-vous que les algorithmes de hachage et de chiffrement IPsec utilisés par le jeu de transformation aux deux extrémités sont identiques. Référez-vous à la section Références des commandes du guide de configuration du dispositif de sécurité Cisco pour plus d'informations. Pour la stratégie ISAKMP et l'ensemble de transformation IPsec utilisés sur l'ASA, le client VPN Cisco ne peut pas utiliser une stratégie avec une combinaison de DES et SHA. Si vous utilisez le DES, vous devez utiliser le MD5 pour l'algorithme de hachage, ou vous pouvez utiliser les autres combinaisons, 3DES avec SHA et 3DES avec MD5.

Vérifier que le numéro de séquence, le nom et la carte de chiffrement sont appliqués à l'interface appropriée au début/à la fin du tunnel IPsec

Si des homologues statiques et dynamiques sont configurés sur la même crypto-carte, l'ordre des entrées de la crypto-carte est critique. Le numéro de séquence de l'entrée de crypto-carte

dynamique doit être supérieur à toutes les autres entrées de crypto-carte statique. Si les entrées statiques sont numérotées plus haut que les entrées dynamiques, les connexions avec ces homologues échouent et les débogages comme indiqué s'affichent :

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Une seule carte de chiffrement dynamique est autorisée pour chaque interface de l'appliance de sécurité. Ceci est un exemple de crypto-carte correctement numérotée qui contient une entrée statique et une entrée dynamique. L'entrée dynamique a le numéro de séquence le plus élevé et il reste de la place pour ajouter des entrées statiques supplémentaires :

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe
```

Les noms de cartes de chiffrement sont sensibles à la casse. Ce message d'erreur peut également être vu lorsque la séquence de crypto-carte dynamique est incorrecte, ce qui entraîne l'homologue à atteindre la mauvaise crypto-carte. Cela est également dû à une liste d'accès de chiffrement incompatible qui définit le trafic : `%ASA-3-713042 : L'initiateur IKE ne parvient pas à trouver la stratégie :`

Dans un scénario où plusieurs tunnels VPN se terminent dans la même interface, créez une carte de chiffrement portant le même nom (une seule carte de chiffrement est autorisée par interface), mais avec un numéro de séquence différent. Cela est vrai pour le routeur et ASA. Référez-vous àASA : Ajouter un nouveau tunnel ou un accès distant à un VPN L2L existant - Cisco pour plus d'informations sur la configuration de crypto-carte pour les scénarios VPN L2L et d'accès distant.

Vérifier que l'adresse IP homologue est correcte

Créer et gérer la base de données des enregistrements spécifiques à la connexion pour IPsec. Pour une configuration VPN IPsec LAN-to-LAN (L2L) d'appliance de sécurité ASA, spécifiez

<name>du groupe de tunnels comme adresse IP de l'homologue distant (extrémité du tunnel distant) dans la commande tunnel-group <name> type ipsec-l2l. L'adresse IP de l'homologue doit correspondre au nom du groupe de tunnels et aux commandes Crypto map set address. Lorsque vous configurez le VPN avec l'ASDM, il génère automatiquement le nom du groupe de tunnels avec l'adresse IP homologue correcte. Si l'adresse IP de l'homologue n'est pas configurée correctement, les journaux peuvent contenir ce message, qui peut être résolu par une configuration correcte de l'adresse IP de l'homologue :

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

Lorsque l'adresse IP de l'homologue n'a pas été configurée correctement sur la configuration de chiffrement ASA, l'ASA ne peut pas établir le tunnel VPN et se bloque uniquement dans l'étape MM_WAIT_MSG4. Pour résoudre ce problème, corrigez l'adresse IP de l'homologue dans la configuration. Voici la sortie de la commande show crypto isakmp lorsque le tunnel VPN se bloque à l'état MM_WAIT_MSG4 :

<#root>

```
hostname#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

Vérifier le groupe de tunnels et les noms de groupe

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

Ce message apparaît lorsqu'un tunnel est abandonné parce que le tunnel autorisé spécifié dans la stratégie de groupe est différent du tunnel autorisé dans la configuration du groupe de tunnels.

<#root>

```
group-policy hf_group_policy attributes
```

```
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines read:

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

Activez IPSec dans la stratégie de groupe par défaut pour appliquer les protocoles existants dans la stratégie de groupe par défaut.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

Désactiver XAUTH pour des homologues L2L

Si un tunnel LAN-à-LAN et un tunnel VPN d'accès à distance sont configurés sur la même crypto-carte, l'homologue LAN-à-LAN est invité à fournir des informations XAUTH, et le tunnel LAN-à-LAN échoue avec CONF_XAUTH dans le résultat de la commande show crypto isakmp . Voici un exemple de la sortie SA :

<#root>

```
Router#

show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

Ce problème ne s'applique qu'à Cisco IOS® où ASA n'est pas affecté par ce problème car il utilise des groupes de tunnels. Exécutez la commande no-xauthkeyword lorsque vous entrez la clé ISAKMP, de sorte que le périphérique n'invite pas l'homologue à entrer des informations XAUTH (nom d'utilisateur et mot de passe). Ce mot clé désactive XAUTH pour les homologues IPsec statiques. Exécutez une commande similaire à celle-ci sur le périphérique pour lequel L2L et RA VPN sont configurés sur la même crypto-carte :

<#root>

```
router(config)#

crypto isakmp key cisco123 address
   172.22.1.164 no-xauth
```

Dans le scénario où l'ASA agit en tant que serveur Easy VPN, le client Easy VPN ne peut pas se connecter à la tête de réseau en raison d'un problème Xauth. Désactivez l'authentification de l'utilisateur dans l'ASA pour résoudre le problème :

<#root>

```
ASA(config)#

tunnel-group example-group type ipsec-ra

ASA(config)#

tunnel-group example-group ipsec-attributes

ASA(config-tunnel-ipsec)#

isakmp ikev1-user-authentication none
```

Référez-vous à la section Divers de ce document pour plus d'informations sur la commande isakmp ikev1-user-authenticationcommand.

Pool VPN épuisé

Quand la plage des adresses IP attribuées à la réserve VPN n'est pas suffisante, vous pouvez étendre l'offre des adresses IP de deux manières :

1. Supprimez la plage existante et définissez la nouvelle plage :

<#root>

```
CiscoASA(config)#

no ip local pool testvpnpool 10.76.41.1-10.76.41.254
```

```
CiscoASA(config)#
ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

---

2. Lorsque des sous-réseaux discontinus doivent être ajoutés au pool VPN, vous pouvez définir deux pools VPN distincts, puis les spécifier sous les « attributs du groupe de tunnels ». Voici un exemple :

```
<#root>
CiscoASA(config)#
ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254
CiscoASA(config)#
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

L'ordre dans lequel vous spécifiez les pools est important, car l'ASA alloue les adresses de ces pools dans l'ordre dans lequel les pools apparaissent dans cette commande. Les paramètres des pools d'adresses dans la commande group policy address pools remplacent toujours les paramètres du pool local dans la commande tunnel-group address-pool.

Problèmes de latence pour le trafic du client VPN

En cas de problèmes de latence sur une connexion VPN, vérifiez les conditions suivantes pour résoudre ce problème :

1. Vérifiez si le MSS du paquet peut être réduit plus loin.
2. Si IPsec/tcp est utilisé à la place d'IPsec/udp, alors configurepreserve-vpn-flow.

3. Réinstallez Cisco ASA .

Les clients VPN ne peuvent pas se connecter avec ASA

Problème

Les clients VPN Cisco ne peuvent pas s'authentifier lorsque Xauth est utilisé avec le serveur Radius.

Solution

Parfois, Xauth expire, vous pouvez augmenter la valeur de délai d'attente pour le serveur AAA pour résoudre ce problème. Exemple :

<#root>

```
Hostname(config)#

aaa-server test protocol radius


hostname(config-aaa-server-group)#

aaa-server test host 10.2.3.4


hostname(config-aaa-server-host)#

timeout 10
```

Problème

Les clients VPN Cisco ne peuvent pas authentifier quand le X-auth est utilisé avec le serveur Radius.

Solution

Assurez-vous d'abord que l'authentification fonctionne correctement. Pour réduire le problème, vérifiez d'abord l'authentification avec la base de données locale sur ASA.

```
tunnel-group tggroup general-attributes
              authentication-server-group none
              authentication-server-group LOCAL
        exit
```

Si cela fonctionne, le problème est lié à la configuration du serveur Radius. Vérifiez la Connectivité du serveur Radius à partir du ASA . Si la requête ping s'exécute sans problème, vérifiez la configuration relative à Radius sur ASA et la configuration de la base de données sur le serveur Radius. Vous pouvez exécuter la commande debug radius pour dépanner les problèmes liés au radius. Pour obtenir un exemple de sortie de débogage radiusoutput, référez-vous à cet exemple de sortie. Avant d'utiliser la commande debugsur l'ASA, référez-vous à cette documentationMessage d'avertissement.

Le client interrompt fréquemment la connexion à la première tentative ou la connexion VPN sécurisée est interrompue par le pair. Reason 433" ou "Connexion VPN sécurisée interrompue par l'homologue Reason 433:(Reason Not Specified by Peer)"

Problème

Les utilisateurs du client VPN Cisco reçoivent cette erreur lorsqu'ils tentent de se connecter au périphérique VPN de tête de réseau.

- Le client VPN interrompt fréquemment la connexion à la première tentative.
- Connexion VPN de sécurité terminée par la raison homologue 433.
- Connexion VPN sécurisée terminée par l'homologue Raison 433 : (Raison non spécifiée par l'homologue).
- Tentative d'attribution d'une adresse IP réseau ou de diffusion, suppression (x.x.x.x) du pool.

Solution 1

Ce problème peut être lié à l'affectation du pool d'adresses IP soit par l'intermédiaire d'ASA, du

serveur Radius, du serveur DHCP, soit par l'intermédiaire du serveur Radius qui agit en tant que serveur DHCP. Exécutez la commande debug crypto pour vérifier que le masque de réseau et les adresses IP sont corrects. Vérifiez également que le pool n'inclut pas l'adresse réseau et l'adresse de diffusion. Les serveurs Radius doivent attribuer les adresses IP appropriées aux clients.

Solution 2

Ce problème se produit également en raison de l'échec de l'authentification étendue. Vous devez vérifier le serveur AAA pour éliminer cette erreur. Vérifiez le mot de passe d'authentification du serveur sur le serveur et le client. Le rechargement du serveur AAA peut résoudre ce problème.

Solution 3

Un autre solution pour cette question est de désactiver la configuration de détection des menaces. Lorsqu'il y a plusieurs retransmissions pour différentes associations de sécurité (SA) incomplètes, l'ASA avec la fonctionnalité de détection des menaces activée pense qu'une attaque d'analyse s'est produite et les ports VPN sont marqués comme le principal contrevenant. Désactivez la fonction de détection des menaces, car cela peut entraîner des problèmes de surcharge sur le traitement de l'ASA. Exécutez ces commandes pour désactiver la détection des menaces :

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

Cela peut être utilisé comme solution de contournement pour vérifier si cela résout le problème. Assurez-vous de désactiver la détection des menaces sur Cisco ASA car cela compromet plusieurs fonctions de sécurité telles que la limitation des tentatives d'analyse, le déni de service avec SPI non valide, les paquets qui échouent à l'inspection de l'application et les sessions incomplètes.

Solution 4

Ce problème se produit également lorsqu'un jeu de transformation n'est pas correctement configuré et qu'une configuration correcte du jeu de transformation résout le problème.

Les utilisateur de l'accès à distance et d'EZVPN se connectent au VPN mais ne peuvent pas accéder aux ressources externes

Problème

- Les utilisateurs d'accès à distance n'ont pas de connectivité Internet une fois connectés au VPN.
- Les utilisateurs de l'accès à distance ne peuvent pas accéder à des ressources situées derrière d'autres VPN sur le même périphérique.
- Les utilisateurs de l'accès à distance peuvent seulement accéder au réseau local.

Solutions

Essayez ces solutions pour résoudre le problème :

- Impossible d'accéder aux serveurs dans DMZ
- Les clients VPN sont incapables de résoudre le DNS
- Transmission tunnel partagée — Impossible d'accéder à l'Internet ou aux réseaux exclus
- Accès au LAN local
- Réseaux privés en superposition

Impossible d'accéder aux serveurs dans DMZ

Une fois que le client VPN est établi, le tunnel IPsec avec le périphérique tête de réseau VPN (routeur ASA/Cisco IOS®), les utilisateurs du client VPN peuvent accéder aux ressources du réseau INSIDE (10.10.10.0/24), cependant. ils ne peuvent pas accéder au réseau DMZ (10.1.1.0/24).

Diagramme

Vérifiez que le tunnel partagé, AUCUNE configuration NAT n'est ajoutée au périphérique de tête de réseau pour accéder aux ressources du réseau DMZ.

Configuration ASA

Cette configuration montre comment configurer l'exemption NAT pour le réseau DMZ afin de permettre aux utilisateurs VPN d'accéder au réseau DMZ :

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

Une fois que vous avez ajouté une nouvelle entrée pour la configuration NAT, effacez la traduction NAT.

```
Clear xlate
Clear local
```

Vérifier

Si le tunnel est établi, accédez à Cisco VPN Client et choisissez Status > Route Details pour valider que les routes sécurisées sont affichées pour les réseaux DMZ et INSIDE.

Référez-vous àASA : Add a New Tunnel or Remote Access to an Existing L2L VPN - Cisco décrit les étapes requises pour ajouter un nouveau tunnel VPN ou un VPN d'accès à distance à une configuration de VPN L2L qui existe déjà. Vous pouvez également faire référence àASA : Allow Split Tunneling for VPN Clients on the ASA Configuration Exemple pour obtenir des instructions détaillées sur la façon d'autoriser les clients VPN à accéder à Internet tout en utilisant un tunnel vers un appareil de sécurité adaptatif (ASA) de la gamme Cisco 5500.

Les clients VPN sont incapables de résoudre le DNS

Une fois le tunnel établi, si les clients VPN ne peuvent pas résoudre le DNS, le problème peut être lié à la configuration du serveur DNS dans le périphérique de tête de réseau (ASA). Vérifiez la connectivité entre les clients VPN et le serveur DNS. Les configurations du serveur DNS doivent être configurées sous la stratégie de groupe et appliquées sous la stratégie de groupe dans les attributs généraux du groupe de tunnels :

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a

group-policy vpn3000 internal
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com

!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.

tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

Les clients VPN ne peuvent pas se connecter aux serveurs internes par nom

Le client VPN ne peut pas envoyer de requête ping aux hôtes ou serveurs du réseau interne distant ou de tête de réseau par nom. Vous devez activer la configuration split-dns sur l'ASA pour résoudre ce problème.

Transmission tunnel partagée — Impossible d'accéder à l'Internet ou aux réseaux exclus

Le tunnel partagé permet aux clients IPsec d'accès à distance de diriger conditionnellement des paquets sur le tunnel IPsec sous forme chiffrée ou vers une interface réseau sous forme de texte clair déchiffré, où ils sont routés vers leur destination finale.

Split-tunnel sont désactivés par défaut, ce qui vous permet de voir l'exécution de la commande tunnelalltraffic.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

L'option excludepecified est prise en charge uniquement pour les clients VPN Cisco, pas pour les clients EZVPN.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

Reportez-vous à ces documents pour des exemples de configuration détaillée de split-tunnel :

- ASA: Permettre le split tunneling pour des clients VPN sur l'exemple de configuration de l'ASA
- Exemple de configuration d'un routeur autorisant les clients VPN à se connecter à IPsec et à Internet via la transmission tunnel partagée

---

Solution D'Épingle À Cheveux

Cette fonctionnalité est utile pour le trafic VPN qui entre dans une interface, mais qui est ensuite routé à partir de la même interface. Par exemple, dans un réseau VPN Hub and Spoke où le dispositif de sécurité est le concentrateur et les réseaux VPN distants sont des rayons. Le trafic de communication satellite à satellite doit être acheminé vers l'appliance de sécurité, puis à nouveau vers l'autre satellite. Exécutez la configuration same-security-traffic pour permettre au trafic d'entrer et de sortir de la même interface :

<#root>

```
securityappliance(config)#

same-security-traffic permit intra-interface
```

Accès au LAN local

Les utilisateurs d'accès à distance se connectent au VPN et peuvent se connecter aux réseaux locaux uniquement. Pour un exemple de configuration plus détaillé, référez-vous àASA : Permettre l'accès au LAN local pour des clients VPN.

Réseaux privés en superposition

Problème

Si vous ne pouvez pas accéder au réseau interne après l'établissement du tunnel, vérifiez l'adresse IP attribuée au client VPN qui chevauche le réseau interne derrière le périphérique de tête de réseau.

Solution

Vérifiez que les adresses IP du pool attribuées aux clients VPN, le réseau interne du périphérique de tête de réseau et le réseau interne du client VPN se trouvent dans des réseaux différents. Vous pouvez affecter le même réseau principal à différents sous-réseaux, mais des problèmes de routage se produisent parfois. Pour plus d'exemples, consultez la sectionDiagramme etExemple de l'impossibilité d'accéder aux serveurs dans DMZ.

Impossible de se connecter m=Plus de trois utilisateurs de client VPN

Problème

Seuls trois clients VPN peuvent se connecter à ASA/ et la connexion du quatrième client échoue. Lors de la panne, ce message d'erreur est affiché :

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

Solutions

Dans la plupart des cas, ce problème est lié à un paramètre de connexion simultanée dans la stratégie de groupe et à la limite maximale de session. Essayez ces solutions pour résoudre le problème :

- Configurer des procédures de connexion simultanées
- Configuration de l'ASA avec CLI

- Configurer Configurer

Configurer des procédures de connexion simultanées

Si la case Hériter dans ASDM est cochée, seul le nombre par défaut de connexions simultanées est autorisé pour l'utilisateur. La valeur par défaut pour les connexions simultanées est 3. Pour résoudre ce problème, augmentez la valeur pour les connexions simultanées.

1. Lancez ASDM, puis accédez à Configuration > VPN > Group Policy.
2. Choisissez le groupe approprié et cliquez sur le bouton Modifier.
3. Une fois dans l'onglet Général, annulez la case à cocher Hériter pourConnexions simultanées sous Paramètres de connexion. Choisissez une valeur Appropriée dans le champ.

La valeur minimale de ce champ est 0, ce qui désactive les connexions et empêche l'accès des utilisateurs. Lorsque vous vous connectez avec le même compte d'utilisateur à partir d'un autre PC, la session en cours (la connexion établie à partir d'un autre PC avec le même compte d'utilisateur) est interrompue et la nouvelle session est établie. Il s'agit du comportement par défaut et il est indépendant des connexions simultanées VPN.

Configuration de l'ASA avec CLI

Complétez ces étapes pour configurer le nombre souhaité de connexions simultanées. Dans cet exemple, 20 a été choisi comme valeur désirée:

<#root>

```
ciscoasa(config)#

group-policy Bryan attributes

ciscoasa(config-group-policy)#

vpn-simultaneous-logins 20
```

Pour en savoir plus sur cette commande, reportez-vous au Guide de référence des commandes

des dispositifs de sécurité Cisco. Exécutez la commande vpn-sessiondb max-session-limit en mode de configuration globale pour limiter les sessions VPN à une valeur inférieure à celle autorisée par l'appliance de sécurité. Exécutez la version de cette commande pour supprimer la limite de session et exécutez à nouveau la commande pour remplacer le paramètre actuel :

```
vpn-sessiondb max-session-limit {session-limit}
```

Cet exemple montre comment paramétrer une limite de session VPN maximale à 450 :

<#root>

```
hostname#

vpn-sessiondb max-session-limit 450
```

Configurer

Message d'erreur :

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Solution

Complétez ces étapes pour configurer le nombre souhaité de connexions simultanées. Vous pouvez également définir les connexions simultanées sur 5 pour cette association de sécurité. Choisissez Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins, et changez le nombre de connexions à 5.

Impossible de lancer la session ou une application et transfert lent après l'établissement du tunnel

Problème

Après l'établissement du tunnel IPsec, l'application ou la session ne se lance pas à travers le tunnel.

Solutions

Exécutez la commande ping pour vérifier le réseau ou pour déterminer si le serveur d'applications est accessible depuis votre réseau. Il peut s'agir d'un problème de taille de segment maximale (MSS) pour les paquets transitoires qui traversent un routeur ou un périphérique /ASA, en particulier les segments TCP avec le bit SYN défini.

Routeur Cisco IOS® : modifiez la valeur MSS dans l'interface externe (interface d'extrémité de tunnel) du routeur

Exécutez ces commandes pour modifier la valeur MSS dans l'interface externe (interface d'extrémité de tunnel) du routeur :

<#root>

```
Router>

enable


Router#

configure terminal

Router(config)#

interface ethernet0/1



Router(config-if)#ip tcp adjust-mss 1300

Router(config-if)#

end
```

Ces messages affichent le résultat du débogage pour TCP MSS :

<#root>

```
Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

Le MSS est réglé sur 1300 sur le routeur tel que configuré. Pour plus d'informations, référez-vous àASA et Cisco IOS® : fragmentation de VPN.

ASA : reportez-vous à la documentation /ASA

Il y a une incapacité à accéder correctement à Internet ou un transfert lent par le tunnel parce qu'il présente un message d'erreur de taille MTU et des problèmes de MSS. Reportez-vous à ce document pour résoudre le problème :

- ASA et Cisco IOS® : Fragmentation VPN

Impossible d'initier un tunnel VPN depuis ASA

Problème

Vous ne pouvez pas initier le tunnel VPN à partir de l'interface ASA et après l'établissement du tunnel. Le client distant/VPN ne peut pas envoyer de requête ping à l'interface interne de l'ASA sur le tunnel VPN. Par exemple, le client VPN ne peut pas initier une connexion SSH ou HTTP aux ASA à l'intérieur de l'interface sur un tunnel VPN.

Solution

L'interface interne ne peut pas recevoir de requête ping de l'autre extrémité du tunnel à moins que

la commande management-access soit configurée en mode de configuration globale.

```
<#root>

ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access

management-access inside
```

Cette commande aide également à l'initiation ssh ou à la connexion http pour l'interface interne de l'ASA via un tunnel VPN. Ces informations sont également valables pour les interfaces DMZ. Par exemple, si vous voulez envoyer une requête ping à l'interface DMZ de /ASA ou si vous voulez lancer un tunnel à partir de l'interface DMZ, alors l'exécution de la commande management-access DMZest requise.

```
<#root>

ASA-02(config)#

management-access DMZ
```

Si le client VPN ne peut pas se connecter, assurez-vous que les ports ESP et UDP sont ouverts. Cependant, si ces ports ne sont pas ouverts, essayez de vous connecter sur TCP 10000 en sélectionnant ce port sous l'entrée de connexion du client VPN. Cliquez avec le bouton droit sur Modifier > Onglet Transport > IPsec sur TCP.

Impossible de faire circuler le trafic à travers le tunnel VPN

Problème

Vous ne pouvez pas faire passer le trafic à travers un tunnel VPN.

Solution

Ce problème peut également se produire lorsque des paquets ESP sont bloqués. Pour résoudre ce problème, reconfigurez le tunnel VPN. Il peut également se produire lorsque les données ne sont pas chiffrées, mais seulement déchiffrées sur le tunnel VPN, comme indiqué dans ce résultat :

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y



 #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393


      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #send errors: 0, #recv errors: 0
```

Pour résoudre ce problème, vérifiez les conditions suivantes :

1. Si les listes d'accès de chiffrement correspondent au site distant et que les listes d'accès NAT 0 sont correctes.
2. Si le routage est correct et que le trafic atteint l'extérieur de l'interface, ce qui passe à l'intérieur, l'exemple de sortie montre que le déchiffrement est terminé, mais que le chiffrement n'a pas lieu.
3. Si la commande sysopt permit connection-vpn est configurée sur l'ASA. Si elle n'est pas configurée, configurez cette commande car elle exempte le trafic crypté/VPN vers l'ASA de la vérification de la liste de contrôle d'accès de l'interface.

Configurer un homologue de sauvegarde pour un tunnel VPN sur la même carte de chiffrement

Problème

Vous voulez utiliser plusieurs homologues de secours pour un seul tunnel vpn.

Solution

La configuration de plusieurs homologues équivaut à la mise à disposition d'une liste de secours. Pour chaque tunnel, le dispositif de sécurité essaye de négocier avec le premier homologue de la liste. Si cet homologue ne répond pas, le dispositif de sécurité descend dans la liste jusqu'à ce qu'un homologue réponde ou qu'il n'y ait plus d'homologues dans la liste. L'ASA a déjà configuré une carte de chiffrement comme homologue principal. L'homologue secondaire peut être ajouté après l'homologue principal. Cet exemple de configuration montre l'homologue primaire en tant que X.X.X.X et l'homologue de secours en tant que Y.Y.Y.Y :

<#root>

```
ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

Désactiver/Redémarrer un tunnel VPN

Problème

Pour désactiver temporairement le tunnel VPN et redémarrer le service, suivez la procédure décrite dans cette section.

Solution

Exécutez la commande d'interface crypto map en mode de configuration globale pour supprimer une carte de chiffrement précédemment définie définie sur une interface. Exécutez la forme de cette commande pour supprimer l'ensemble de crypto-cartes de l'interface.

<#root>

```
hostname(config)#

no crypto map

 map-name

interface

 interface-name
```

Cette commande supprime une crypto-carte définie sur n'importe quelle interface active du dispositif de sécurité et change le tunnel VPN IPsec en inactif dans l'interface. Pour redémarrer le tunnel IPsec sur une interface, vous devez assigner une carte de chiffrement à une interface avant que celle-ci puisse fournir des services IPsec.

<#root>

```
hostname(config)#

crypto map

 map-name

interface

 interface-name
```

Certains tunnels ne sont pas chiffrés.

Problème

Quand un nombre énorme de tunnels sont configurés sur la passerelle VPN, quelques tunnels ne passent pas le trafic. L'ASA ne reçoit pas les paquets chiffrés pour ces tunnels.

Solution

Cette question se produit parce que l'ASA ne passe pas les paquets chiffrés par les tunnels. Des règles en double de cryptage sont créées dans le tableau ASP .

Erreur : – %ASA-5-713904 : Groupe = DefaultRAGroup, IP = x.x.x.x, ... Mode de transaction v2 non pris en charge.Tunnel terminé

Problème

Le message d'erreur %ASA-5-713904: **`Group = DefaultRAGroup, IP = 192.0.2.0,... unsupported Transaction Mode v2 version.Tunnel`** terminatederror s'affiche.

Solution

La raison du message d'erreur Transaction Mode v2 est qu'ASA prend uniquement en charge la configuration du mode IKE v6 et non l'ancienne version du mode v2. Utilisez la configuration du mode IKE v6 pour résoudre cette erreur.

Erreur : – %ASA-6-722036 : Groupe client-groupe Utilisateur xxxx IP x.x.x.x Transmission d'un grand paquet 1220 (seuil 1206)

Problème

Le message d'erreur %ASA-6-722036: **`Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206) error message s'affiche dans les messages du journal de l'ASA.`** Que signifie ce message de journal et comment ceci peut être résolu ?

Solution

Ce message indique qu'un paquet volumineux a été envoyé au client. La source du paquet ne connaissait pas le MTU du client. Cela peut être dû à la compression de données non compressibles. Vous pouvez désactiver la compression SVC avec la commande vc compression none, qui résout le problème.

Message d'erreur lorsque la QoS est activée à une extrémité du

tunnel VPN

Problème

Si vous avez activé QoS à une extrémité du tunnel VPN, vous pouvez recevoir ce message d'erreur :

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

Solution

Ce message est normalement généré lorsqu'une extrémité du tunnel exécute la QoS. Cela se produit lorsqu'un paquet est détecté comme étant dans le désordre. Vous pouvez désactiver QoS pour arrêter cela, mais il peut être ignoré tant que le trafic peut traverser le tunnel.

AVERTISSEMENT : Entrée de carte de chiffrement incomplète

Problème

Lorsque vous exécutez la commande crypto map mymap 20 ipsec-isakmpcommand, vous pouvez recevoir cette erreur : **`WARNING : entrée crypto map incomplète`**

Exemple :

<#root>

```
ciscoasa(config)#
```

`crypto map mymap 20 ipsec-isakmp`

`WARNING: crypto map entry incomplete`

Solution

Il s'agit d'une alerte normale lorsque vous définissez une nouvelle crypto-carte ; nous vous rappelons que des paramètres tels que access-list (match address), transform set et peer address doivent être configurés avant de pouvoir fonctionner correctement. Il est également standard de voir la première ligne que vous tapez pour définir la crypto-carte, et elle ne s'affiche pas dans la configuration.

Erreur : – %ASA-4-400024 : IDS:2151 Grand paquet ICMP provenant de l'interface externe

Problème

Impossible de passer un grand paquet ping à travers le tunnel vpn. Quand nous essayons de passer de grands paquets ping, nous obtenons l'erreur %ASA-4-400024: **`IDS:2151 Grand paquet ICMP de à sur l'interface externe.`**

Solution

Désactivez les signatures 2150 et 2151 pour résoudre ce problème. Une fois les signatures désactivées, la commande ping fonctionne correctement. Exécutez ces commandes pour désactiver les signatures :

- ASA(config)#ip audit signature 2151 disable
- ASA(config)#ip audit signature 2150 disable

Erreur : – %ASA-4-402119 : IPSEC : Réception d'un paquet de protocole (SPI=spi, sequence number= seq_num) de Remote_IP (username) vers Local_IP ayant échoué à la vérification de la fonctionnalité anti-relecture

Problème

J'ai reçu cette erreur dans les messages du journal de l'ASA :

Erreur : - %|ASA-4-402119 : IPSEC : Réception d'un paquet de protocole (SPI=spi, sequence number= seq_num) de remote_IP (username) vers local_IP qui n'a pas pu être vérifié.

Solution

Pour résoudre cette erreur, exécutez la commande crypto ipsec security-association replay window-size pour modifier la taille de la fenêtre.

<#root>

```
hostname(config)#
```

crypto ipsec security-association replay window-size 1024

Cisco vous recommande d'utiliser la taille de fenêtre 1024 complète pour éliminer tout problème d'anti-relecture.

Message d'erreur - %ASA-4-407001 : Refuser le trafic pour local-host interface_name:inside_address, limite de licence dépassée

Problème

Peu d'hôtes ne peuvent pas se connecter à Internet ; ce message d'erreur apparaît dans le journal système : Message d'erreur - %ASA-4-407001 : Refuser le trafic pour local-host interface_name:inside_address, limite de licence dépassée

---

Solution

Ce message d'erreur est reçu lorsque le nombre d'utilisateurs dépasse la limite d'utilisateurs pour la licence utilisée. Cette erreur peut être résolue en mettant à niveau la licence à un nombre plus élevé d'utilisateurs. La licence utilisateur peut inclure 50, 100 ou un nombre illimité d'utilisateurs si nécessaire.

Error Message - %VPN_HW-4-PACKET_ERROR:

Problème

Le message d'erreur - %VPN_HW-4-PACKET_ERROR : error message indique que le paquet ESP avec HMAC reçu par le routeur ne correspond pas. Cette erreur peut être causée par les problèmes suivants :

- Module H/W VPN défectueux
- Paquet ESP corrompu

Solution

Pour résoudre ce message d'erreur :

- Ignorez les messages d'erreur à moins qu'il y ait interruption du trafic.
- S'il y a interruption du trafic, remplacez le module.

Message d'erreur : Command rejected: Supprimer la connexion de chiffrement entre VLAN XXXX et XXXX, d'abord

Problème

Ce message d'erreur apparaît quand vous essayez d'ajouter un VLAN autorisé sur le port d'agrégation d'un commutateur : Command rejected: supprimez d'abord la connexion de chiffrement entre VLAN XXXX et VLAN XXXX. L'agrégation de périphérie WAN ne peut pas être modifiée pour autoriser des VLAN supplémentaires. Si vous ne pouvez pas ajouter de VLAN dans le SPAtrunk VPN IPSEC. Cette commande est rejetée car elle aboutit à un VLAN d'interface connecté par chiffrement qui appartient à la liste des VLAN autorisés, ce qui constitue une violation potentielle de la sécurité IPSec.



Remarque : Ce comportement s'applique à tous les ports trunk.

Solution

Au lieu de la commande no switchport trunk allowed vlan (vlanlist), exécutez la commande switchport trunk allow vlan nonecommand ou la commande « switchport trunk allowed vlan remove (vlanlist) ».

Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Paquet abandonné - Option d'échelle de fenêtre non valide pour la session x.x.x.x:27331 à x.x.x.x:23 [Initiator(flag 0, factor 0) Responder (flag 1, factor 2)]

Problème

Cette erreur se produit quand vous essayez de vous connecter au telnet à partir d'un périphérique sur l'extrémité lointaine d'un tunnel VPN ou à partir du routeur lui-même : Message d'erreur - % FW-3-RESPONDER_WND_SCALE_INI+NO_SCALE : Paquet abandonné - Option d'échelle de fenêtre non valide pour la session x.x.x.x:27331 à x.x.x.x:23 pediaK[Initiator(flag 0, factor 0) Responder (flag 1, factor2)]

Solution

La licence utilisateur peut inclure 50, 100 ou un nombre illimité d'utilisateurs si nécessaire. La fonction d'échelle de fenêtre a été ajoutée afin de permettre la transmission rapide de données sur les réseaux de graisse longue (LFN). Il s’agit généralement de connexions à bande passante élevée et à latence élevée. Les réseaux dotés de connexions par satellite sont un exemple de réseau local à bande étroite, car les liaisons par satellite présentent toujours des délais de propagation élevés avec une bande passante généralement élevée. Pour activer la fonction d'échelle de fenêtre pour prendre en charge les LFN, la taille de fenêtre TCP doit être supérieure à 65 535. Ce message d'erreur peut être résolu si vous augmentez la taille de fenêtre TCP pour qu'elle soit supérieure à 65 535.

%ASA-5-305013 : Règles NAT asymétriques jumelées pour l'aval et l'amont. Mettez à jour les flux liés à ce problème

Problème

Ce message d'erreur apparaît une fois que le tunnel VPN est soulevé : %ASA-5-305013 : Correspondances de règles NAT asymétriques pour le transfert et le retour. Mettez à jour ces flux de problèmes.

Solution

Pour résoudre ce problème lorsqu'il ne se trouve pas sur la même interface que l'hôte avec NAT, utilisez l'adresse mappée au lieu de l'adresse réelle pour vous connecter à l'hôte. En outre, activez la commande inspectsi l'application intègre l'adresse IP.

%ASA-5-713068 : Message de notification inhabituel reçu : notify_type

Problème

Ce message d'erreur apparaît si le tunnel VPN n'apparaît pas : %ASA-5-713068 : Message de notification inhabituel reçu : notify_type

---

Solution

Ce message se produit en raison d'une mauvaise configuration (lorsque les stratégies ou les ACL ne sont pas configurées de la même manière sur les homologues). Une fois que les stratégies et les ACL sont mises en correspondance, le tunnel s'active sans aucun problème.

%ASA-5-720012 : (VPN secondaire) n'a pas pu mettre à jour les données d'exécution du basculement pour les capacités IPSec sur l'installation de réserve (ou) %ASA-6-720012 : (unité VPN) n'a pas pu mettre à jour les données d'exécution du basculement pour les capacités IPSec sur l'installation de réserve

Problème

L'un des messages d'erreur suivants s'affiche lorsque vous tentez de mettre à niveau l'appliance de sécurité adaptatif Cisco (ASA) :

- **%ASA-5-720012 : (VPN-Secondaire) Impossible de mettre à jour les données de délai d'exécution de basculement IPSec sur l'équipement de réserve.**
- **%ASA-6-720012 : (L'unité VPN) n'a pas pu mettre à jour les données de délai d'exécution de basculement IPsec sur l'équipement de réserve.**

Solution

Ces messages d'erreur sont des erreurs informatives et n'ont pas d'impact sur la fonctionnalité de l'ASA ou du VPN. Elles apparaissent lorsque le sous-système de basculement VPN ne peut pas mettre à jour les données d'exécution IPsec, car le tunnel IPsec associé a été supprimé sur l'unité en veille. Pour résoudre ces problèmes, exécutez la commande wr standby sur l'unité active.

Erreur : – %ASA-3-713063 : Adresse de pair IKE non configurée pour la destination 0.0.0.0

Problème

Le %ASA-3-713063 : Le message d'erreur IKE Peer address not configured for destination 0.0.0.0 s'affiche et le tunnel ne s'affiche pas.

Solution

Ce message apparaît quand l'adresse de pair IKE n'est pas configurée pour un tunnel L2L . L'erreur peut être résolue si vous modifiez le numéro de séquence de la crypto-carte, puis supprimez et réappliquez la crypto-carte.

Erreur : %ASA-3-752006 : Tunnel Manager n'a pas pu envoyer un message KEY_ACQUIRE

Problème

Le %ASA-3-752006 : Le gestionnaire de tunnels n'a pas pu envoyer un message de saisie de clé KEY_ACQUIRE. Mauvaise configuration probable de la crypto-carte ou du groupe de tunnels. le message d'erreur est obtenu sur Cisco ASA.

Solution

Ce message d'erreur peut être causé par par une mauvaise configuration de la carte de chiffrement ou du groupe de tunnels. Assurez-vous que les deux sont configurés correctement. Pour plus d'informations sur ce message d'erreur, reportez-vous à Erreur 752006.

Voici certaines des actions correctives :

- Supprimez la liste de contrôle d’accès de chiffrement associée à la carte dynamique.
- Retirez la configuration IKE liée à v2 inutilisée, le cas échéant.
- Vérifiez que la liste de contrôle d’accès cryptographique correspond correctement.
- Supprimez toutes les entrées de la liste de contrôle d’accès dupliquées.

Erreur : %ASA-4-402116 : IPSEC : Réception d'un paquet ESP (SPI= 0x99554D4E, numéro d'ordre= 0x9E) de XX.XX.XX.XX (user= XX.XX.XX.XX) vers YY.YY.YY.YY

Dans une installation tunnel LAN à LAN VPN, cette erreur est reçue sur une extrémité ASA :

Le paquet interne décapsulé ne correspond pas à la stratégie négociée dans l’association de sécurité.

Le paquet spécifie sa destination à 10.32.77.67, sa source à 10.105.30.1 et son protocole à icmp.

La SA spécifie son proxy local comme 10.32.77.67/255.255.255.255/ip/0 et son remote_proxy comme 10.105.42.192/255.255.255.224/ip/0.

Solution

Vous devez vérifier les listes d'accès de trafic uniques définies aux deux extrémités du tunnel VPN. Les deux doivent correspondre comme images miroir exactes.

Échec de lancement de l'installateur VA de 64 bits pour activer l'adaptateur virtuel, en raison de l'erreur 0xffffffff

Problème

Pour lancer l'installateur 64-bit VA afin d'activer l'adaptateur virtuel dû au message d'erreur de connexion 0xffffffff est reçu quand AnyConnect ne parvient pas à établir une connexion.

Solution

Pour résoudre ce problème, procédez comme suit :

1. Accédez à Système > Gestion des communications Internet > Paramètres de communication Internet et assurez-vous que la case Désactiver les mises à jour automatiques des certificats racine est désactivée.
2. Si elle est désactivée, désactivez toute la partie Modèle d'administration de l'objet de stratégie de groupe affecté à l'ordinateur affecté et testez à nouveau. Référez-vous à Désactiver la mise à jour automatique des certificats racine pour plus d'informations.

Le client VPN Cisco ne fonctionne pas avec la carte de données sous Windows 7

Problème

Le client VPN Cisco ne fonctionne pas avec la carte de données sous Windows 7.

Solution

Le client VPN Cisco installé sur Windows 7 ne fonctionne pas avec les connexions 3G car les cartes de données ne sont pas prises en charge sur les clients VPN installés sur les ordinateurs Windows 7.

Alerte : « La fonctionnalité VPN pourrait ne pas fonctionner du tout ».

Problème

Lors des tentatives d'activation d'ISAKMP sur l'interface externe d'ASA, ce message d'alerte est reçu :

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

L'accès à ASA via SSH et HTTPS est arrêté et d'autres clients SSL sont également affectés.

Solution

Ce problème est dû aux mémoires requises par différents modules tels que le module de connexion (logger) et de chiffrement (crypto). Assurez-vous que vous n'avez pas la commande logging queue 0. La taille de la file d'attente est définie sur 8192 et l'allocation de mémoire augmente. Sur les plates-formes telles que ASA5505 et ASA5510, cette allocation de mémoire tend à réduire la mémoire des autres modules.

Erreur de remplissage d'IPSec

Problème

Ce message d'erreur est reçu :

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

Solution

Le problème se produit parce que le VPN IPSec négocie sans algorithme de hachage. Le hachage des paquets assure le contrôle d'intégrité du canal ESP. Par conséquent, sans hachage, les paquets malformés sont acceptés sans être détectés par le Cisco ASA et celui-ci tente de les décrypter. Cependant, comme ces paquets sont mal formés, l'ASA détecte des défauts lors du déchiffrement des paquets. Ceci entraîne les messages d'erreur de remplissage qui sont observés. Il est recommandé d'inclure un algorithme de hachage dans l'ensemble de transformation pour le VPN et de s'assurer que la liaison entre les homologues présente une malformation de paquet minimale.

Le tunnel VPN est déconnecté toutes les 18 heures

Problème

Le tunnel VPN est déconnecté toutes les 18 heures, même si la durée de vie est définie sur 24 heures.

Solution

La durée de vie est la durée maximale pendant laquelle l'association de sécurité peut être utilisée pour une nouvelle clé. La valeur que vous écrivez dans la configuration, car la durée de vie est différente de la période de réintroduction d'une clé de SA. Il est nécessaire de négocier une nouvelle SA (ou paire SA dans le cas d'IPsec) avant l'expiration de la SA actuelle. La durée de la nouvelle clé doit être inférieure à la durée de vie pour permettre plusieurs tentatives en cas d'échec de la première tentative de nouvelle clé.

Les documents RFC ne précisent pas comment calculer le délai de nouvelle saisie. Ceci est laissé à votre discrétion, par conséquent, l'heure varie avec la plate-forme. Quelques implantation peuvent employer un facteur aléatoire pour calculer le temporisateur de réintroduction d'une clé. Par exemple, si l'ASA initie le tunnel, il est normal qu'il effectue une nouvelle saisie à 64800 secondes = 75 % de 86400. Si le routeur démarre, l'ASA peut attendre plus longtemps pour accorder plus de temps à l'homologue pour initier la nouvelle saisie. Il est donc normal que la

session VPN soit déconnectée toutes les 18 heures pour utiliser une autre clé pour la négociation VPN.

Le flux de trafic n'est pas maintenu après la renégociation du tunnel LAN à LAN

Problème

Le flux de trafic n'est pas maintenu après que le tunnel LAN à LAN soit renégocié.

Solution

L'ASA surveille chaque connexion qui passe et conserve une entrée dans sa table d'état conformément à la fonctionnalité d'inspection d'application. Les détails du trafic crypté qui transitent par le VPN sont conservés sous la forme d'une base de données d'association de sécurité (SA). Des connexions de réseau local aux connexions de réseau privé virtuel local, deux flux de trafic différents sont mis à jour. L'un est le trafic chiffré entre les passerelles VPN. L'autre est la circulation entre la ressource de réseau derrière la passerelle VPN et l'utilisateur derrière l'autre extrémité.

Quand la commexion VPN se termine, les détails d'écoulement pour cette SA particulière sont supprimés. Cependant, l'entrée du tableau d'état mis à jour par l'ASA pour cette connexion TCP devient éventée en raison de l'absence d'activité, qui entrave le téléchargement. Cela signifie que l'ASA conserve toujours la connexion TCP pour ce flux particulier pendant que l'application utilisateur se termine. Les connexions TCP deviennent incohérentes et finissent par expirer après l'expiration du délai d'inactivité TCP. Ce problème a été résolu avec l'introduction d'une fonctionnalité appelée Flux tunnel IPSec persistants. Une nouvelle commande, sysopt connection preserve-vpn-flows, a été intégrée à Cisco ASA pour conserver les informations de la table d'état lors de la renégociation du tunnel VPN.

Par défaut, cette commande est désactivée. Pour ce faire, Cisco ASA conserve les informations de la table d'état TCP lorsque le VPN L2L se rétablit de l'interruption et rétablit le tunnel.

Le message d'erreur déclare que la bande passante a atteint

pour la fonctionnalité de chiffrement

Problème

Ce message d'erreur est reçu sur le routeur de série 2900 :

Erreur : 20 mars 10:51:29 : %CERM-4-TX_BW_LIMIT : La limite maximale de bande passante de 8 500 Kbits/s est atteinte pour la fonctionnalité Crypto avec la licence du package technologique securityk9.

Solution

C'est un problème connu qui se produit en raison des instructions strictes émises par le gouvernement des États-Unis. Conformément à la licence securityk9, elle ne peut autoriser un cryptage de charge utile que jusqu'à des débits proches de 90 Mbits/s et elle limite le nombre de tunnels/sessions TLS cryptés au périphérique. Pour plus d'informations sur les restrictions d'exportation de chiffrement, référez-vous à Licence SEC et HSEC Cisco ISR G2.

Pour les périphériques Cisco, il est calculé comme étant inférieur à 85 Mbits/s de trafic unidirectionnel entrant ou sortant du routeur ISR G2 avec un total bidirectionnel de 170 Mbits/s. Cette exigence s'applique aux plates-formes Cisco 1900, 2900 et 3900 ISR G2. Cette commande permet d'afficher les limitations suivantes :

<#root>

```
Router#

show platform cerm-information

Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)          85000                  85000
 Rx Bandwidth(in kbps)          85000                  85000
 Number of tunnels                225                    225
 Number of TLS sessions          1000                   1000
---Output truncated----
```

Pour éviter ce problème, achetez une licence HSECK9. Une licence de fonction « hseck9 » fournit une fonctionnalité de cryptage de charge utile améliorée avec un nombre accru de tunnels VPN et des sessions vocales sécurisées. Pour plus d'informations sur la licence du routeur Cisco ISR, reportez-vous à Activation logicielle.

Problème : Échec du trafic de chiffrement sortant dans le tunnel IPsec, même si le trafic de déchiffrement entrant fonctionne

Solution

Ce problème a été observé sur une connexion IPsec après plusieurs clés, cependant, la condition de déclenchement n'est pas claire. La présence de ce problème peut être établie si vous vérifiez le résultat de la commande show asp dropcommand et si le compteur de contexte VPN expiré augmente pour chaque paquet sortant envoyé.

Divers

Un message AG_INIT_EXCH apparaît dans la sortie des commandes « show crypto isakmp sa » et « debug »

Si le tunnel n'est pas initié, le message AG_INIT_EXCHmessage apparaît dans la sortie de la commande show crypto isakmp et dans la sortie debugoutput aussi. La raison peut être liée à une non-correspondance des politiques ISAKMP ou si le port udp 500 est bloqué.

Le message de débogage « Received an IPC message during invalid state » apparaît

Il s'agit d'un message d'information et n'est en rien lié à la déconnexion du tunnel VPN.

Informations connexes

- ASA et Cisco IOS® : Fragmentation VPN
- Dispositifs de sécurité de la gamme Cisco ASA 5500

- Négociation IPSec/Protocoles IKE
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.