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 « Secure VPN Connection terminated by Peer 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 de connecter 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 le tunnel VPN depuis ASA

Impossible de faire circuler le trafic à travers le tunnel VPN

Configurer l'homologue de sauvegarde pour le tunnel VPN sur la même crypto-carte

Désactiver/Redémarrer un tunnel VPN

Certains tunnels ne sont pas chiffrés.

Erreur : - %ASA-5-713904 : Groupe = DefaultRAGroup, IP = x.x.x.x, ...version v2 du mode de transaction non prise en charge.Fin du tunnel.

Erreur : - %ASA-6-722036 : Groupe client-groupe Utilisateur xxxx IP x.x.x.x Transmission du paquet volumineux 1220 (seuil 1206)

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

AVERTISSEMENT : entrée de crypto-carte incomplète

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

Erreur : - %ASA-4-402119 : IPSEC : a reçu un paquet de protocole (SPI=spi, numéro de séquence= num_séquence) de remote_IP (nom d'utilisateur) vers local_IP qui n'a pas pu être vérifié.

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 : Commande rejetée : supprimez d'abord la connexion de chiffrement entre VLAN XXXX et XXXX.

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 [Initiator(flag 0, factor 0) Responder (flag 1, factor 2)]

%ASA-5-305013 : Les règles NAT asymétriques correspondent pour le transfert et le retour . Mettez à jour les flux liés à ce problème

%ASA-5-713068 : message de notification non routinier reçu : notify_type

%ASA-5-720012 : (VPN-Secondary) échec de la mise à jour des données

d'exécution du basculement IPSec sur l'unité en veille (ou) %ASA-6-720012 : (VPN-unit) échec de la mise à jour des données d'exécution du basculement IPSec sur l'unité en veille

Erreur : - %ASA-3-713063 : adresse homologue IKE non configurée pour la destination 0.0.0.0

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

Erreur : %ASA-4-402116 : IPSEC : a reçu un paquet ESP (SPI= 0x99554D4E, numéro de séquence= 0x9E) de XX.XX.XX.XX (utilisateur= 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 sur Windows 7

Alerte : "La fonctionnalité VPN peut ne pas fonctionner du tout"

Erreur de remplissage d'IPSec

Le tunnel VPN se déconnecte après 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 : le trafic de chiffrement sortant dans un tunnel IPsec échoue, même si le trafic de déchiffrement entrant fonctionne.

Divers

Informations connexes

Introduction

Ce document décrit les solutions les plus courantes aux problèmes de VPN IPsec.

Informations générales

Les solutions décrites ici proviennent directement de demandes de service que l'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.

Bien que les exemples de configuration de ce document soient destinés à être utilisés sur des routeurs et des dispositifs de sécurité, presque tous ces concepts sont également applicables au VPN 3000 .

Référez-vous à Dépannage de la sécurité IP - Présentation et utilisation des commandes de débogage pour une explication des commandes de débogage courantes qui sont utilisées pour dépanner les problèmes IPsec sur le logiciel Cisco IOS® et .

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

Avertissement : de nombreuses solutions présentées dans ce document peuvent entraîner une

perte temporaire de toute connectivité VPN IPsec sur un périphérique.

Il est recommandé de mettre en application ces solutions avec prudence et selon votre politique de contrôle de modification.

Conditions préalables

Exigences

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

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

Composants utilisés

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

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

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 des éléments à vérifier ou à essayer avant d'entreprendre une

correction 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
- Vérifiez que les commandes sysopt sont présentes (/ASA uniquement)
- Vérifier l'identité d'ISAKMP
- Vérifier le délai d'attente d'inactivité/de session
- Vérifiez si les ACL sont exacts et liés à la carte de chiffrement.
- Vérifier les stratégies ISAKMP
- Vérifier que le routage est correct
- Vérifier que le jeu de transformation 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 des commandes de ces sections ont été ramenées à 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 qu'un 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 sont incapables d'accéder au réseau interne derrière l'appliance de sécurité.

Si vous n'activez pas la NAT-T dans le périphérique NAT/PAT, vous pouvez recevoir le message d'erreur **`failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.69.4`** dans l'ASA.

De même, si vous ne parvenez pas à vous connecter simultanément à partir de la même adresse IP, **`la connexion VPN sécurisée est interrompue localement par le client. Raison 412 : L'homologue distant ne répond plus.Un`** message d'erreur s'affiche.

Activez NAT-T dans le périphérique VPN de tête de réseau afin de 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®.

Voici la commande pour activer NAT-T sur un dispositif de sécurité Cisco. Le vingt (20) dans cet exemple est le temps keepalive (par défaut).

ASA

<#root>

securityappliance(config)#

crypto isakmp nat-traversal 20

Les clients ont aussi besoin d'être modifiés afin que cela fonctionne.

Dans Client VPN Cisco, accédez à Entrées de connexion et cliquez sur Modifier. Il ouvre une nouvelle fenêtre dans laquelle vous devez choisir l'onglet Transport.

Sous cet onglet, cliquez sur le bouton radio Enable Transparent Tunneling et IPSec over 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 afin d'en savoir plus sur la configuration de l'ACL dans ASA.

Tester correctement la connectivité

Idéalement, la connectivité VPN est testée à partir des périphériques situés derrière les périphériques d'extrémité qui effectuent le chiffrement, mais de nombreux utilisateurs testent la connectivité VPN à l'aide de la commande ping sur les périphériques qui effectuent le chiffrement.

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 alors qu'elle fonctionne réellement. 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 cette situation, le ping doit provenir du réseau interne derrière l'un des routeurs. Cela est nécessaire, parce que les ACL de chiffrement sont seulement configurés pour crypter le trafic avec ces adresses sources.

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 ont été remplacés par des appliances de sécurité ASA. Le cryptage utilisé 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 yourping.

Si vous devez cibler l'interface interne avec yourping, vous devez activer l'accès à la gestion sur cette interface, sinon l'appliance ne répond pas.

<#root>

```
securityappliance(config)#
```

management-access inside

En cas de problème de connectivité, même la première 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 et/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 SA Crypto quand la phase 1 fonctionne est semblable à 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, il est possible qu'ISAKMP n'ait pas été activé. Soyez sûr que vous avez activé ISAKMP sur vos périphériques.

Utilisez l'une de ces commandes pour activer ISAKMP sur vos périphériques :

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 obtenir cette erreur quand 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 que le Client derrière ASA obtient PAT au port udp 500 avant que isakmp puisse être activé sur l'interface. Une fois que cette traduction PAT retirée (clear xlate), 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.

Quand ISAKMP n'est pas activé sur l'interface, le client VPN affiche un message d'erreur semblable à ce message :

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

Afin de résoudre cette erreur, activerISAKMO sur l'interface de chiffrage de la passerelle VPN .

Activer/Désactiver PFS

Dans des négociations IPsec, le Perfect Forward Secrecy (PFS) assure que chacune nouvelle clé cryptographique est indépendante de toute clé précédente.

Activez ou désactivez PFS sur les deux homologues de tunnel ; sinon, le tunnel IPsec LAN à LAN (L2L) n'est pas établi dans le routeur ASA / Cisco IOS®.

Perfect Forward Secrecy (PFS) est une fonctionnalité propriétaire de Cisco et n'est pas prise en charge sur des périphériques fournis par un autre constructeur.

ASA :

PFS est désactivé par défaut. Afin d'activer PFS, utilisez la commande pfscommand avec le mot clé enable en mode de configuration de stratégie de groupe. Afin de désactiver PFS, saisissez le mot clé disable.

<#root>

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

pfs {enable | disable}

Afin de supprimer l'attribut PFS de la configuration, entrez la forme no de cette commande.

Une stratégie de groupe peut hériter d'une valeur pour PFS d'une autre stratégie de groupe.

Entrez la forme no de cette commande afin d'empêcher le transfert d'une valeur.

<#root>

hostname(config-group-policy)#

no pfs

Routeur Cisco IOS® :

Afin de spécifier qu'IPsec doit demander PFS quand de nouvelles associations de sécurité sont demandées pour cette entrée de crypto-carte, utilisez la commande set pfsen mode de configuration de crypto-carte.

Afin de spécifier qu'IPsec nécessite PFS quand il reçoit des demandes pour de nouvelles associations de sécurité, utilisez la commande set pfsen mode de configuration de crypto-carte.

Afin de spécifier qu'IPsec ne doit pas demander le PFS, utilisez la forme no de cette commande. Par défaut, PFS n'est pas demandé. Si aucun groupe n'est spécifié avec cette commande, group1 est utilisé 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®®, le problème est que l'association de sécurité a expiré ou a été effacée.

Le périphérique de tunnel distant ne sait pas qu'il utilise la SA qui a expirée pour envoyer un paquet (pas un paquet d'établissement de SA).

Quand une nouvelle SA a été établie, la communication reprend, initiant ainsi le trafic intéressant à travers le tunnel pour créer une nouvelle SA 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 (SA) ISAKMP (phase I) et IPsec (phase II), la meilleure solution et la plus simple est de résoudre les problèmes IPsec des VPN.

Si vous effacez des SA, vous pouvez fréquemment résoudre une grande variété de messages d'erreur et de comportements étranges sans nécessité de dépanner.

Tandis que cette technique peut facilement être utilisée dans n'importe quelle situation, c'est presque toujours une condition d'effacer des SA après avoir fait des changements ou des ajouts dans la configuration VPN IPsec actuelle.

De plus, alors qu'il est possible d'effacer uniquement des associations de sécurité spécifiques, le plus grand avantage peut venir du moment où vous effacer l'ensemble des SA sur le périphérique.

Une fois que les associations de sécurité ont été effacées, il peut être nécessaire d'envoyer le trafic à travers le tunnel pour les rétablir.

Avertissement : sauf si vous spécifiez les associations de sécurité à effacer, les commandes répertoriées 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

    a. Cisco IOS®

    <#root>

    ```
    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa
    ```

    b. Appareils de sécurité Cisco ASA

<#root>

securityappliance#

show crypto isakmp sa

securityappliance#

show crypto ipsec sa

2. Effacez les associations de sécurité. Chaque commande peut être saisie comme indiqué en gras ou avec les options montrées avec elles.

    a. Cisco IOS®

        a. ISAKMP (phase I)

<#root>

router#

clear crypto isakmp

?
<0 - 32766> connection id of SA
<cr>

        b. 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>

    b. Appareils de sécurité Cisco ASA

        a. ISAKMP (phase I)

<#root>

securityappliance#

```
clear crypto isakmp sa
```

b. 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, le problème peut être la durée de vie moindre configurée dans la SA ISAKMP.

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, Failure during phase 1 rekey try due to collisionerror 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 point), mais, avec des durées de vie plus courtes, le dispositif de sécurité installe plus rapidement les futures SA IPsec.

Une correspondance est établie quand les stratégies des deux homologues contiennent des valeurs identiques de cryptage, de hachage, d'authentification et de paramètre Diffie-Hellman, et quand la stratégie de l'homologue distant spécifie une durée de vie inférieure ou égale à la durée de vie dans la stratégie comparée.

Si les durées de vie ne sont pas identiques, la durée de vie plus courte — provenant de la stratégie de l'homologue distant — est utilisée. Si aucune correspondance acceptable n'est trouvée, l'IKE refuse la négociation et la SA IKE n'est pas établie.

Spécifiez la durée de vie de la SA. Cet exemple définit une durée de vie de 4 heures (14 400 secondes). La valeur par défaut est 86 400 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 :

Secure VPN Connection terminated locally by the Client. Raison 426 : La Durée De Vie Maximale Configurée A Été Dépassée.

Afin de résoudre ce message d'erreur, définissez la valeur de durée de vie à zéro (0) afin de définir la durée de vie d'une association de sécurité IKE à l'infini. Le VPN est toujours connecté et ne se termine pas.

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

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

Activer ou désactiver les Keepalives d'ISAKMP

Si vous configurez les keepalives d'ISAKMP, cela aide à éviter des VPN LAN-à-LAN ou d'accès à distance sporadiquement abandonnés, ce qui inclut des clients VPN, des tunnels et les tunnels qui sont abandonnés après une période d'inactivité.

Cette fonctionnalité laisse le périphérique du tunnel surveiller la présence continue d'un homologue distant et enregistre sa propre présence auprès de cet homologue.

Si l'homologue ne répond plus, le périphérique supprime la connexion.

Pour que les keepalives d'ISAKMP fonctionnent, les deux périphériques VPN doivent les prendre en charge.

Configurez les keepalives ISAKMP dans Cisco IOS® avec cette commande :

<#root>

```
router(config)#
```

crypto isakmp keepalive 15

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

Cisco ASA pour le groupe de tunnels nommé10.165.205.222

<#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 afin de résoudre le problème, par exemple, si le client VPN est derrière un pare-feu qui bloque les paquets DPD.

Cisco ASA, pour le groupe de tunnels nommé10.165.205.222

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

Accédez à%System Root% > Program Files > Cisco Systems > VPN Client > Profiles sur le PC client qui rencontre le problème afin de désactiver IKE keepalive, et modifiez le fichier PCF, le cas

échéant, pour la connexion.

Remplacez ForceKeepAlives=0(par défaut) par ForceKeepAlives=1.

La fonctionnalité keepalive est propriétaire de Cisco et n'est pas prise en charge sur des périphériques fournis par un autre constructeur.

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. Soyez certain que vous avez saisi toutes les clés pré-partagées correctement sur chaque périphérique VPN.

Saisissez à nouveau une clé pour vous assurer qu'elle est correcte. Il s'agit d'une solution simple qui peut vous aider à éviter un dépannage approfondi.

Dans le VPN d'accès à distance, vérifiez que le nom de groupe valide et la clé pré-partagée sont saisis dans le client VPN Cisco.

Vous pouvez faire face à cette erreur si le nom du groupe ou la clé pré-partagée 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 risquez de 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.

Utilisez ces commandes pour supprimer et ressaisir la clé pré-partagée secretkeypour 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
```

Utilisez ces commandes pour supprimer et ressaisir la clé pré-partagée secretkey pour 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'initiation du tunnel VPN se déconnecte. Ce problème se produit en raison d'une clé pré-partagée non concordante au cours des négociations de phase I.

Le message MM_WAIT_MSG_6dans la commande show crypto isakmp sacommand indique une clé pré-partagée non correspondante, 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
```

Afin de résoudre ce problème, entrez à nouveau la clé pré-partagée 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 un problème VPN IPsec, supprimez et réappliquez la crypto-carte appropriée afin de résoudre une grande variété de problèmes qui incluent des abandons intermittents du tunnel VPN et l'échec de certains sites VPN

à apparaître.

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

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

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

```
<#root>

router(config-if)#

no crypto map mymap
```

Continuez à utiliser la forme pour supprimer une carte de chiffrement entière.

```
<#root>

router(config)#

no crypto map mymap 10
```

Remplacez la carte de chiffrement sur l'interface Ethernet0/0 pour l'homologue 10.0.0.1. Cet exemple montre la configuration minimale requise de la carte de chiffrement :

```
<#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
```

Utilisez ces commandes pour supprimer et remplacer une crypto-carte sur l'ASA :

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

<#root>

```
securityappliance(config)#

no crypto map mymap interface outside
```

Continuez à utiliser 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 carte de chiffrement pour l'homologue 10.0.0.1. Cet exemple montre la configuration minimale requise de la carte de chiffrement :

<#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 ré-appliquez la carte de chiffrement, cela résout également le problème de connectivité si l'adresse IP en tête de réseau a été changée.

Vérifier que les commandes sysopt sont présentes (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. Utilisez ces commandes show pour déterminer si la commande pertinente sysoptcommand 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)
```

Utilisez ces commandes afin d'activer la commande correcte sysoptpour votre périphérique :

Cisco ASA

<#root>

```
securityappliance(config)#
```

sysopt connection permit-vpn

Si vous ne souhaitez pas utiliser la commande sysopt connection, autorisez explicitement le trafic intéressant 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

Si le tunnel VPN IPsec a échoué dans la négociation IKE, l'échec peut être dû à l'échec ou à l'incapacité de son homologue à reconnaître l'identité de son homologue.

Quand 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, paramétrez le dispositif de sécurité et les identités de ses homologues de la même manière pour éviter un échec de la négociation IKE.

Afin de définir l'ID de phase 2 à envoyer à l'homologue, utilisez la commande isakmp identityen 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
```

Le tunnel VPN ne s'active pas après un changement de configuration de vers 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, PeerTblEntry périmé trouvé, suppression !

[IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x, échec de la suppression de l'homologue de la table de corrélateur, aucune correspondance !

[IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x, build_ipsec_delete() : aucun SPI pour identifier l'association de sécurité de phase 2 !

[IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x, échec de la suppression de l'homologue de la table de corrélateur, aucune correspondance !

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

Si le délai d'attente d'inactivité est défini à 30 minutes (par défaut), cela signifie qu'il supprime le tunnel après 30 minutes sans trafic passant par celui-ci.

Le client VPN est déconnecté après 30 minutes, quel que soit le paramètre de délai d'inactivité, et rencontre `l'`erreur **`PEER_DELETE-IKE_DELETE`**_UNSPECIFIED.

Configurez idle timeoutandsession timeoutaneafin de rendre le tunnel toujours up, et de sorte que le tunnel ne soit jamais abandonné même lorsque des périphériques tiers sont utilisés.

ASA

Entrez la commande vpn-idle-timeout en mode de configuration group-policy ou en mode de configuration username afin de 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 parce que tout le trafic passe par le tunnel (puisque tunnel-all est configuré).

Par conséquent, le trafic intéressant (ou même le trafic généré par le PC) est intéressant et ne laisse pas le délai d'inactivité entrer en action.

Routeur Cisco IOS®

Utilisez la commande crypto ipsec security-association idle-time en mode de configuration globale ou en mode de configuration crypto map afin de 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.

Vérifiez que les ACL sont exactes 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 liste d’accès définit le trafic à chiffrer ; elle inclut une liste de contrôle d’accès chiffrée dans

une configuration de réseau local à réseau local ou une liste de contrôle d’accès à tunnel partagé dans une configuration d’accès distant.

Lorsque ces listes de contrôle d'accès sont mal configurées ou manquées, le trafic circule peut-être dans une direction à travers le tunnel VPN, ou n'est pas envoyé à travers le tunnel.

Assurez-vous de lier la ACL de chiffrement avec la carte de chiffrement avec la commande crypto map match address en mode de configuration globale.

Assurez-vous d'avoir configuré toutes les listes d'accès nécessaires pour réaliser votre configuration VPN IPsec et que ces listes d'accès définissent le trafic voulu.

Cette liste contient les éléments simples à vérifier lorsque vous suspectez qu'une ACL est à l'origine des problèmes que vous rencontrez avec votre VPN IPsec.

Assurez-vous que votre exemption NAT et vos listes de contrôle d'accès de chiffrement spécifient le trafic voulu.

Si vous avez plusieurs tunnels VPN et ACL de chiffrement, assurez-vous que ces ACL ne se superposent pas.

Assurez-vous que votre périphérique est configuré pour utiliser la liste de contrôle d'accès d'exemption NAT : Sur un routeur, cela signifie que vous utilisez la commande route-map.

Sur l'ASA, cela signifie que vous utilisez 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.

Ici, un routeur Cisco IOS® est configuré pour exempter le trafic qui est 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 ACL d'exemption NAT fonctionnent seulement avec l'adresse IP ou des réseaux IP, tels que ces exemples mentionnés (access-list noNAT), et doivent être identiques aux ACL de la carte de chiffrement.

Les listes de contrôle d'accès d'exemption NAT ne fonctionnent pas avec les numéros de port (par

exemple, 23, 25,...).

Dans un environnement VOIP, où les appels vocaux entre les réseaux sont communiqués via le VPN, les appels vocaux ne fonctionnent pas si les ACL NAT 0 ne sont pas correctement configurées.

Avant le dépannage, il est conseillé de vérifier l'état de la connectivité VPN, car le problème peut provenir d'une mauvaise configuration des listes de contrôle d'accès exemptées NAT.

Vous pouvez obtenir le message d'erreur indiqué s'il y a 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, essayez de la supprimer et émettez la commande NAT 0 afin qu'elle fonctionne.

Assurez-vous que vos ACL ne sont pas vers l'arrière et sont du bon type.

Les ACL de chiffrement et d'exemption NAT pour des configurations de LAN-à-LAN doivent être écrites avec la perspective du périphérique sur lequel l'ACL est configurée.

Cela signifie que 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 ici, ce même concept s'applique aux appareils de sécurité ASA.

Dans ASA, les listes de contrôle d'accès à tunnel partagé pour les configurations d'accès à distance doivent être des listes d'accès standard qui autorisent le trafic vers le réseau auquel les clients VPN ont besoin d'accéder.

Les routeurs Cisco IOS® peuvent utiliser une liste de contrôle d’accès étendue pour le split-tunnel. 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 NAT d'exception 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 ne FONCTIONNE pas, vérifiez que les stratégies ISAKMP correspondent avec les 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 cryptage, de hachage, d'authentification et de paramètre Diffie-Hellman.

Vérifiez si la stratégie d'homologue distant spécifie une durée de vie inférieure ou égale à la durée de vie dans la stratégie envoyée par l'initiateur.

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 le message détaillé du journal :

```
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 peut pas 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 transformations IPsec qui est utilisé 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 routage est correct

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.

Si d'autres routeurs existent derrière votre périphérique de passerelle, assurez-vous qu'ils savent comment atteindre le tunnel et quels sont les réseaux de l'autre côté.

Un composant clé du routage dans un déploiement VPN est le Reverse Route Injection (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 au périphérique sur lequel elles sont installées, ainsi qu'à d'autres périphériques dans le réseau, parce que des routes installées par RRI peuvent être redistribuées par un protocole de routage tel qu'EIGRP ou OSPF.

Dans une configuration de LAN-à-LAN, il est important pour chaque périphérique d'avoir une route ou des routes pour les réseaux pour lesquels il est censé crypter le trafic.

Dans cet exemple, Router A doit avoir des routes pour les réseaux derrière Router B via 10.89.129.2. Router B doit avoir une route semblable vers 192.168.100.0 /24 :

La première façon de s'assurer que chaque routeur connaît la route appropriée est de 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
```

Si un grand nombre de réseaux existe derrière chaque périphérique, la configuration des routes statiques devient difficile à maintenir.

Au lieu de cela, il est recommandé d'utiliser le Reverse Route Injection, comme décrit. Le RRI place dans la table de routage des routes pour tous les réseaux mentionnés dans l'ACL 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 un ASA, la configuration peut se présenter comme suit :

<#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 le dispositif de sécurité, ces routeurs doivent apprendre le chemin menant aux clients VPN d'une manière ou d'une autre.

Dans cet exemple, supposons que les clients VPN reçoivent des adresses dans la plage de 10.0.0.0 /24 lorsqu'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 :

```
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 du routage se produit si le pool des adresses IP assignées pour les clients VPN se superposent avec des réseaux internes du périphérique de tête de réseau. Pour plus d'informations, référez-vous à la section Chevauchement de réseaux privés .

Vérifier que le jeu de transformation est correct

Assurez-vous que le cryptage IPsec et les algorithmes de hachage à utiliser 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 transformations IPsec qui est utilisé 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 les numéros et le nom de la séquence de la carte de chiffrement, et vérifier que la carte de chiffrement est appliquée dans la bonne interface, dans laquelle le tunnel IPsec commence/s'arrête

Si des homologues statiques et dynamiques sont configurés sur la même carte de chiffrement, l'ordre des entrées dans la carte de chiffrement est très important.

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 ont des numéros plus élevés que l'entrée dynamique, les connexions avec ces homologues échouent et les débogages indiqués apparaissent.

```
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 permise pour chaque interface dans le dispositif de sécurité.

Voici un exemple de carte de chiffrement correctement numérotée qui contient une entrée statique et une entrée dynamique. Notez que l'entrée dynamique a le numéro de séquence le plus élevé et que de la place a été laissée 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 man dynamique n'est pas correcte, 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 intéressant : **`%ASA-3-713042 : l'initiateur IKE ne parvient pas à trouver la stratégie :`**

Dans un scénario où plusieurs tunnels VPN doivent être terminés dans la même interface, créez une crypto-carte avec le même nom (une seule crypto-carte est autorisée par interface) mais avec un numéro de séquence différent.

Cela est vrai pour le routeur et ASA.

De même, référez-vous àASA : Ajouter un nouveau tunnel ou un accès à distance à un VPN L2L existant - Cisco pour plus d'informations sur la configuration de crypto-carte pour le scénario L2L et le scénario VPN d'accès à distance.

Vérifier que l'adresse IP de l'homologue est correcte

Créer et gérer la base de données des enregistrements spécifiques à la connexion pour IPsec.

Pour une configuration VPN IPsec LAN à LAN (L2L) d'un dispositif de sécurité ASA, spécifiez le<name>du groupe de tunnels comme l'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 tunnel et aux commandes d'adresse Crypto map set.

Lorsque que vous configurez le VPN avec l'ASDM, il a généré le nom du groupe de tunnels automatiquement avec la bonne adresse IP de l'homologue.

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 n'est pas en mesure d'établir le tunnel VPN et se bloque uniquement dans l'étape MM_WAIT_MSG4.

Afin de résoudre ce problème, corrigez l'adresse IP du pair dans la configuration.

Voici le résultat 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 quand un tunnel est supprimé, 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 les protocoles existants déjà 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 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 s'applique uniquement à Cisco IOS® alors qu'ASA n'est pas affecté par ce problème car il utilise des groupes de tunnels.

Utilisez le mot-clé no-xauthkeyword lorsque vous entrez la clé isakmp, de sorte que le périphérique n'invite pas l'homologue pour les informations XAUTH (nom d'utilisateur et mot de passe).

Ce mot clé désactive XAUTH pour les homologues IPsec statiques. Saisissez un commande semblable à celle-ci sur le périphérique pour lequel un VPN L2L et un VPN RA sont configurés sur la même carte de chiffrement :

<#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 du problème Xauth.

Désactivez l'authentification de l'utilisateur dans l'ASA afin de résoudre le problème comme indiqué :

<#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
```

Reportez-vous à la section Divers de ce document afin d'en savoir plus sur la commande isakmp

ikev1-user-authenticationcommand.

Réserve VPN en voie d'épuisement

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. Enlevez la plage existante et définissez la nouvelle plage. Voici un exemple :

```
<#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. Quand des sous-réseaux non contigus doivent être ajoutés à la réserve VPN, vous pouvez définir deux groupes VPN distincts et les spécifier alors dans la commande sous le « tunnel-group attributes (attributs de 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
```

La commande dans laquelle vous spécifiez les groupes est très importante parce que ASA attribue des adresses de ces groupes dans la commande dans laquelle les groupes apparaissent dans cette commande.

Les configurations de réserve d'adresses (address-pool) dans la commande des bassins

d'adresses des politiques de groupe l'emportent sur les réglages de bassin local dans la commande de bassin d'adresses du groupe de tunnels.

Problèmes de latence pour le trafic du client VPN

En cas de problèmes de latence sur une connexion VPN, vérifiez ces conditions afin de résoudre ceci :

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 authentifier quand le X-auth est utilisé avec le serveur Radius.

Solution

Le problème peut être que le xauth expire. Augmentez la valeur d'attente pour le serveur AAA afin de 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

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

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

Si cela fonctionne correctement, le problème est lié à la configuration du serveur Radius.

Vérifiez la Connectivité du serveur Radius à partir du ASA . Si le ping fonctionne sans problème, alors vérifiez la configuration liée à Radius sur le ASA et la configuration de base de données sur le serveur Radius.

Vous pouvez utiliser la commande debug radius pour résoudre 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 documentation : Message 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 « Secure VPN Connection terminated by Peer 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 l'homologue. Raison 433.

Connexion VPN sécurisée interrompue 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

Le problème peut être lié à l'affectation du pool d'adresses IP via ASA, le serveur Radius, le

serveur DHCP ou le serveur Radius qui agit comme serveur DHCP.

Utilisez la commande debug cryptoafin de vérifier que le masque de réseau et les adresses IP sont corrects. En outre, vérifiez que le pool n'inclut pas l'adresse du réseau et l'adresse de diffusion.

Les serveurs Radius doivent pouvoir assigner les adresses IP propres aux clients.

Solution 2

Ce problème se produit également en raison des défaillances 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. Recharger le 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 incomplètes, l'ASA avec la fonctionnalité de détection de menace activée pense qu'une attaque d'analyse s'est produite et que les ports VPN sont marqués comme le principal contrevenant.

Essayez de désactiver la configuration de détection des menaces comme ceci peut créer beaucoup charger le traitement du ASA . Employez ces commandes afin de désactiver la détection des menaces :

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

Ceci peut être utilisé comme solution pour vérifier si ceci règle le problème réel.

Assurez-vous que pour désactiver la détection des menaces sur le Cisco ASA compromet réellement plusieurs fonctionnalités de sécurité telles que la limitation des tentatives d'analyse, le DoS 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 quand un ensemble de transformations n'est pas correctement configuré. Une configuration correcte de l'ensemble de transformations 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 de l'accès à distance n'ont aucune connectivité Internet une fois qu'ils se connectent 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 afin de résoudre ce 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 dans 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), mais ils ne peuvent pas accéder au réseau DMZ (10.1.1.0/24).

Diagramme

Vérifiez que la configuration transmission tunnel partagée, NO NAT est ajoutée dans le périphérique de tête de réseau pour accéder aux ressources dans le réseau DMZ.

Exemple :

Configuration ASA :

Cette configuration affiche 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
```

Après avoir ajouté une nouvelle entrée pour la configuration NAT, effacez la traduction Nat.

```
Clear xlate
Clear local
```

Vérifier :

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

Référez-vous à ASA : Ajouter un nouveau tunnel ou un accès à distance à un VPN L2L existant - Cisco pour les étapes requises pour ajouter un nouveau tunnel VPN ou un VPN d'accès à distance à une configuration VPN L2L qui existe déjà.

Référez-vous à ASA : Allow Split Tunneling for VPN Clients sur l'exemple de configuration ASA pour des instructions détaillées sur la façon d'autoriser les clients VPN à accéder à Internet tout en utilisant un tunnel dans 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 parviennent pas à résoudre le DNS, le problème peut être la configuration du serveur DNS dans le périphérique de tête de réseau (ASA).

Contrôlez également la connectivité entre les clients VPN et le serveur DNS. La configuration du serveur DNS doit être configurée sous la stratégie de groupe et appliquée sous la stratégie de groupe dans les attributs généraux du groupe de tunnels ; par exemple :

<#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 sont incapables de se connecter à des serveurs internes par le nom

Le client VPN ne peut pas soumettre une requête ping aux hôtes ou aux serveurs du réseau interne distant ou en tête de réseau par le nom. Vous devez activer l'option split-dns configure sur l'ASA afin de 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, déchiffrée, où ils sont routés vers une destination finale.

Le split-tunnel est désactivé par défaut, ce qui désinstalle tout le trafic.

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

L'option excludespecified est uniquement prise en charge pas les clients VPN Cisco, pas 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 : exemple de configuration d'autorisation de split tunneling pour les clients VPN sur 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 interface, mais qui est ensuite routé hors de cette même interface.

Par exemple, dans un réseau VPN Hub and Spoke, où l'appliance de sécurité est le concentrateur et les réseaux VPN distants sont des rayons, le trafic de communication satellite à satellite doit entrer dans l'appliance de sécurité, puis sortir à nouveau vers l'autre rayon.

Utilisez la configuration same-security-traffic pour autoriser le trafic à entrer et sortir de la même interface.

<#root>

```
securityappliance(config)#
```

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

Accès au LAN local

Les utilisateurs de l'accès à distance se connectent au VPN et peuvent se connecter au réseau local seulement.

Pour un exemple de configuration plus détaillé, référez-vous àASA : Autoriser l'accès LAN local pour les clients VPN.

Réseaux privés en superposition

Problème

Si vous ne pouvez pas accéder au réseau interne après l'établissement du tunnel, contrôlez l'adresse IP assignée au client VPN qui se superpose au réseau interne derrière le périphérique de tête de réseau.

Solution

Vérifiez que les adresses IP du pool à attribuer aux clients VPN, au réseau interne du périphérique de tête de réseau et au réseau interne du client VPN se trouvent dans des réseaux différents.

Vous pouvez assigner le même réseau principal avec différents sous-réseaux, mais parfois les problèmes de routage se produisent.

Pour d'autres exemples, consultez la sectionDiagramme etExemple de l'impossibilité d'accéder aux serveurs dans DMZ.

Impossible de connecter plus de trois utilisateurs de client VPN

Problème

Seuls trois clients VPN peuvent se connecter à ASA/; 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 paramétrage de procédures de connexion simultanées dans la stratégie de groupe et à la limite de session maximale.

Essayez ces solutions afin de résoudre ce 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 est cochée dans ASDM, seul le nombre par défaut de connexions simultanées est autorisé pour l'utilisateur. La valeur par défaut pour les connexions simultanées est trois (3).

Afin de résoudre ce problème, augmentez la valeur pour des procédures de connexion 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 zéro (0), ce qui désactive la connexion et empêche l'accès utilisateur.

   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.

C'est le comportement par défaut et est indépendant aux procédures de connexion VPN simultanées.

Configuration de l'ASA avec CLI

Complétez ces étapes pour configurer le nombre souhaité de connexions simultanées. Dans cet exemple, on a choisi vingt (20) comme valeur souhaitée.

<#root>

```
ciscoasa(config)#
```

group-policy Bryan attributes

```
ciscoasa(config-group-policy)#
vpn-simultaneous-logins 20
```

Afin d'en savoir plus sur cette commande, référez-vous àRéférence des commandes du dispositif de sécurité Cisco.

Utilisez la commande vpn-sessiondb max-session-limit en mode de configuration globale afin de limiter les sessions VPN à une valeur inférieure à celle autorisée par l'appliance de sécurité.

Utilisez la version de cette commande afin de supprimer la limite de session. Utilisez de nouveau la commande afin de remplacer la configuration actuelle.

```
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

Effectuez ces étapes afin de configurer le nombre désiré de procédures de connexion simultanées. Vous pouvez également essayer de paramétrer les procédures de connexion simultanées à 5 pour cette SA :

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

Utilisez la commande ping pour vérifier le réseau ou 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 afin de changer 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 montrent la sortie de débogage pour la MSS de TCP :

<#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)]
```

La MSS est ajustée à 1 300 sur le routeur comme configuré.

Pour plus d'informations, référez-vous à ASA et Cisco IOS® : Fragmentation VPN.

ASA : reportez-vous à la documentation /ASA

Il y a impossibilité d'accéder à l'Internet correctement ou le transfert est lent via le tunnel, parce qu'il en résulte le message d'erreur de taille du MTU et des problèmes de MSS.

Référez-vous à ce document afin de résoudre le problème :

- ASA et Cisco IOS® : fragmentation VPN

Impossible d'initier le 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 d'ASA sur le tunnel VPN.

Par exemple, le client VPN peut ne pas être en mesure d'établir une connexion SSH ou HTTP aux ASA à l'intérieur de l'interface sur le tunnel VPN.

Solution

L'interface interne du ne peut pas recevoir de requête ping à partir 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 avec l'initiation ssh ou la connexion http à l'interface interne de l'ASA via un tunnel VPN.

Ces informations valent également pour l'interface 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 la commande management-access DMZ est requise.

<#root>

```
ASA-02(config)#
management-access DMZ
```

Si le client VPN ne parvient pas à se connecter, vérifiez 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 passer le trafic à travers un tunnel VPN.

Solution

Ce problème peut également se produire lorsque les paquets ESP sont bloqués. Afin de résoudre ce problème, reconfigurez le tunnel VPN.

Ce problème peut 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
```

Afin de résoudre ce problème, vérifiez ces conditions :

1. Si les listes d'accès chiffrées s'assortissent avec le site distant, et que les listes d'accès NAT 0 sont correctes.
2. Si le routage est correct et que le trafic atteint l'interface externe qui passe par l'interface interne. L'exemple d'affichage montre que le déchiffrement se fait, mais le cryptage ne se produit pas.
3. Si la commande sysopt permit connection-vpn a été configurée sur l'ASA. S'il n'est pas configuré, configurez cette commande car elle permet à l'ASA d'exempter le trafic chiffré/VPN de la vérification de l'ACL d'interface.

Configurer l'homologue de sauvegarde pour le tunnel VPN sur la même crypto-carte

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 en tant qu'homologue principal. L'homologue secondaire pourrait être ajouté après le primaire.

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

Afin de désactiver temporairement le VPN tunnel et redémarrer le service, exécutez la procédure décrite dans cette section.

Solution

Utilisez la commande d'interface crypto map en mode de configuration globale pour supprimer une carte de chiffrement précédemment définie définie pour une interface.

Utilisez la forme de cette commande afin de supprimer l'ensemble de crypto-cartes de l'interface.

<#root>

```
hostname(config)#
no crypto map
 map-name
interface
 interface-name
```

Cette commande supprime une carte de chiffrement paramétrée pour toute interface active du dispositif de sécurité et rend le tunnel VPN IPsec inactif dans cette 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, ... version v2 du mode de transaction non prise en charge.Fin du tunnel.

Problème

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

Solution

La raison `du` message d'erreur `Transaction Mode v2` est que ASA prend en charge uniquement IKE Mode Config V6 et non l'ancienne version du mode V2.

Utilisez IKE Mode Config V6 afin de résoudre cette erreur.

Erreur : - %ASA-6-722036 : Groupe client-groupe Utilisateur xxxx IP x.x.x.x Transmission du paquet volumineux 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)`** s'affiche dans les journaux de l'ASA.

Que signifie ce message de journal et comment ceci peut être résolu ?

Solution

Ce message du journal déclare qu'un grand paquet a été envoyé au client. La source du paquet ne reconnaît pas le MTU du client.

Ceci peut également être dû à la compression de données incompressibles. La solution de contournement est de désactiver la compression SVC avec la commande nonecommand de compression vc, qui résout le problème.

Message d'erreur quand 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 ceci, mais le problème peut être ignoré tant que peut le trafic peut traverser le tunnel.

AVERTISSEMENT : entrée de crypto-carte incomplète

Problème

Lorsque vous exécutez la commande crypto map mymap 20 ipsec-isakmp, vous pouvez recevoir cette erreur :

AVERTISSEMENT : entrée de crypto-carte incomplète

Exemple :

<#root>

```
ciscoasa(config)#
```

crypto map mymap 20 ipsec-isakmp

WARNING: crypto map entry incomplete

Solution

Il s'agit d'une alerte habituelle lorsque vous définissez une nouvelle crypto-carte ; un rappel que des paramètres tels que access-list (match address), transform set et peer address doivent être configurés avant de pouvoir fonctionner.

Il est également normal que la première ligne que vous avez saisie afin de définir la carte de chiffrement ne s'affiche pas dans la configuration.

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

Problème

Impossible de passer un grand paquet ping à travers le tunnel vpn. Lorsque nous essayons de transmettre des paquets ping volumineux, nous obtenons l'erreur**%ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside.**

Solution

Désactivez les signatures 2150 et 2151 afin de résoudre ce problème.Une fois les signatures désactivées, la commande ping fonctionne correctement.

Utilisez ces commandes afin de désactiver les signatures :

ASA(config)#ip audit signature 2151 disable

ASA(config)#ip audit signature 2150 disable

Erreur : - %ASA-4-402119 : IPSEC : a reçu un paquet de protocole (SPI=spi, numéro de séquence= num_séquence) de remote_IP (nom d'utilisateur) vers local_IP qui n'a pas pu être vérifié.

Problème

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

Erreur : - %|ASA-4-402119 : IPSEC : a reçu un paquet de protocole (SPI=spi, numéro de séquence= num_séquence) de remote_IP (nom d'utilisateur) vers local_IP qui n'a pas pu être vérifié.

Solution

Afin de résoudre cette erreur, utilisez la commande crypto ipsec security-association replay window-size afin de varier la taille de la fenêtre.

<#root>

hostname(config)#

crypto ipsec security-association replay window-size 1024

Cisco recommande que vous utilisiez la taille de fenêtre maximale (1 024) pour éliminer tous les problèmes d'anti-relecture.

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

Problème

Quelques hôtes ne peuvent pas se connecter à l'Internet et ce message d'erreur apparaît dans le syslog :

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 quand le nombre d'utilisateurs dépasse la limite d'utilisateurs de la licence utilisée. Cette erreur peut être résolue par la mise à niveau de la licence vers un nombre d'utilisateurs plus élevé.

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 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

Afin de 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 : Commande rejetée : supprimez d'abord la connexion de chiffrement entre VLAN XXXX et XXXX.

Problème

Ce message d'erreur apparaît lorsque vous tentez d'ajouter un VLAN autorisé sur le port trunk d'un commutateur :`Commande rejetée : supprimer la connexion de chiffrement entre VLAN XXXX et VLAN XXXX, d'abord..`

La liaison agrégée de la périphérie WAN ne peut pas être modifiée pour autoriser des VLAN supplémentaires. En d'autres termes, vous ne pouvez pas ajouter de VLAN dans le SPAtrunk VPN IPSEC.

Cette commande est rejetée parce qu'elle aboutit à un VLAN d'interface connecté par chiffrement qui appartient à la liste des VLAN autorisés, ce qui constitue une brèche de sécurité IPSec potentielle.

Notez que ce comportement s'applique à tous les ports d'agrégation.

Solution

Au lieu de `la` commande `no switchport trunk allowed vlan (vlanlist)`, utilisez `la commande switchport trunk allowed vlan` none ou la commande`"switchport trunk allowed vlan remove (vlanlist)"`.

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 [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 [Initiator(flag 0, factor 0) Responder (flag 1, factor 2)]`

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).

Ce sont généralement des connexions avec une très grande bande passante, mais également avec une latence élevée.

Les réseaux avec des connexions satellites sont un exemple de LFN, puisque les liaisons satellites ont toujours des délais de propagation élevés, mais ont généralement une grande bande passante.

Pour que la fonction d'échelle de fenêtre prenne 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 la fenêtre TCP à plus de 65 535.

%ASA-5-305013 : Les règles NAT asymétriques correspondent pour le transfert et le retour . 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 : Les règles NAT asymétriques correspondent pour le transfert et le retour . Mettez à jour les flux liés à ce problème

Solution

Afin de résoudre ce problème lorsqu'il n'est 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 non routinier reçu : notify_type

Problème

Ce message d'erreur apparaît si le tunnel VPN n'apparaît pas :

%ASA-5-713068 : message de notification non routinier reçu : notify_type

Solution

Ce message se produit en raison de la mauvaise configuration (c'est-à-dire, quand les politiques ou les ACL ne sont pas configurés pour être identiques sur les pairs).

Une fois que les politiques et les ACL sont appariés, le tunnel s'affiche sans problème.

%ASA-5-720012 : (VPN-Secondary) échec de la mise à jour des données d'exécution du basculement IPSec sur l'unité en veille

(ou) %ASA-6-720012 : (VPN-unit) échec de la mise à jour des données d'exécution du basculement IPSec sur l'unité en veille

Problème

Un de ces messages d'erreur apparaît quand vous essayez d'améliorer le dispositif de sécurité adaptable Cisco (ASA) :

%ASA-5-720012 : (VPN secondaire) échec de la mise à jour des données d'exécution du basculement IPSec sur l'unité en veille.

%ASA-6-720012 : (unité VPN) échec de la mise à jour des données d'exécution du basculement IPsec sur l'unité en veille.

Solution

Ces messages d'erreur sont des erreurs à titre informatif. Les messages n'affectent pas la fonctionnalité de l'ASA ou du VPN .

Ces messages apparaissent lorsque le sous-système de basculement VPN ne peut pas mettre à jour les données d'exécution liées à IPsec, car le tunnel IPsec associé a été supprimé sur l'unité en veille.

Afin de résoudre ces problèmes, émettez la commande wr standby sur l'unité active.

Erreur : - %ASA-3-713063 : adresse homologue IKE non configurée pour la destination 0.0.0.0

Problème

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

Solution

Ce message apparaît quand l'adresse de pair IKE n'est pas configurée pour un tunnel L2L .

Cette 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 distribuer un message KEY_ACQUIRE.

Problème

%ASA-3-752006 : Tunnel Manager n'a pas pu envoyer un message KEY_ACQUIRE.Configuration probablement incorrecte de la crypto-carte ou du groupe de tunnels."Le message d'erreur est consigné 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 :

- Retirez l'ACL chiffré (par exemple, lié à la carte dynamique).
- Retirez la configuration IKE liée à v2 inutilisée, le cas échéant.
- Vérifiez que l'ACL chiffré est correctement assorti.
- Retirez les entrées de liste d'accès en double, le cas échéant.

Erreur : %ASA-4-402116 : IPSEC : a reçu un paquet ESP (SPI= 0x99554D4E, numéro de séquence= 0x9E) de XX.XX.XX.XX (utilisateur= 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.

SA spécifie son proxy local à 10.32.77.67/255.255.255.255/ip/0 et son remote_proxy (proxy distant) à 10.105.42.192/255.255.255.224/ip/0.

Solution

Vous devez vérifier les listes d'accès du trafic intéressant définies sur les 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

Échec du lancement du programme d'installation VA 64 bits pour activer la carte virtuelle en

raison du message d'erreur 0xffffffflog reçu lorsque AnyConnect ne parvient pas à se connecter.

Solution

Procédez comme suit pour résoudre ce problème :

1. Accédez à Système > Gestion des communications Internet > Paramètres de communication Internet et assurez-vous que Désactiver la mise à jour automatique des certificats racine est désactivé.
2. Si elle est désactivée, désactivez alors la partie entièreAdministrativeTemplate de l'objet de stratégie de groupe assigné à la machine affectée 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 sur Windows 7

Problème

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

Solution

Le Client VPN Cisco installé sur le Windows 7 ne fonctionne pas avec les connexions 3G puisque des cartes de données ne sont pas prises en charge sur des clients VPN installés sur un ordinateur Windows 7.

Alerte : "La fonctionnalité VPN peut ne pas fonctionner du tout"

Problème

Lors des tentatives d'activation de isakmp sur l'interface externe de l'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.
```

En ce moment, l'accès à l'ASA se fait par ssh. HTTPS est arrêté et d'autres clients SSL sont également touchés.

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 ne disposez pas de 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.

La recommandation est d'inclure un algorithme de hachage dans la série de transformations pour le VPN et de s'assurer que le lien entre les pairs comporte le nombre minimal de malformations de paquet.

Le tunnel VPN se déconnecte après 18 heures.

Problème

Le tunnel VPN se fait déconnecter après 18 heures même si la durée de vie est de 24 heures.

Solution

La durée de vie est la durée maximale pendant laquelle l'association de sécurité peut être utilisée pour la 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.

Par conséquent, il est nécessaire de négocier une nouvelle SA (ou paire de SA dans le cas d'IPsec) avant que l'actuelle expire.

Le temps de réintroduction d'une clé doit toujours être plus petit que la durée de vie afin de permettre plusieurs tentatives au cas où la première tentative de réintroduction d'une clé échouerait.

Les RFC ne spécifient pas comment calculer le temps de réintroduction d'une clé. Ceci est laissé à la discrétion des responsables de l'implantation.

Par conséquent, le temps varie selon 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, alors il est normal qu'il se reconnecte à 64800 secondes = 75% de 86400.

Si les initiés de routeur, alors l'ASA peut attendre plus longtemps avant de donner au pair plus de temps pour redonner une clé.

Ainsi, il est normal que la session VPN se déconnecte toutes les 18 heures pour utiliser une autre clé pour la négociation VPN. Ceci ne doit poser aucune baisse ou problème 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 le traverse et conserve une entrée dans sa table d'état conformément à la fonctionnalité d'inspection d'application.

Les détails chiffrés du trafic qui traversent le VPN sont mis à jour sous forme de base de données de l'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'une 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.

Cependant, 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 dans l'ASA de Cisco afin de retenir les données du tableau d'état à 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 de bande passante maximale de 85000 Kbits/s a été 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 cette directive, la licence securityk9 peut uniquement autoriser un cryptage de charge utile jusqu'à des débits proches de 90 Mbits/s et limiter 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 de Cisco ISR G2.

Pour les périphériques Cisco, il est dérivé pour être moins que le trafic 85 Mbit/sec unidirectionnel dans ou hors du routeur ISR G2, avec un total bidirectionnel de 170 Mbit/sec.

Cette condition requise s'applique aux plateformes Cisco 1900, 2900, 3900 et 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 à la fonctionnalité améliorée de cryptage des données utiles avec un plus grand nombre de tunnels VPN et les sessions de voix sécurisée.

Pour plus d'informations sur la licence du routeur Cisco ISR, reportez-vous à Activation logicielle.

Problème : le trafic de chiffrement sortant dans un tunnel IPsec échoue, même si le trafic de déchiffrement entrant fonctionne.

Solution

Ce problème a été observé sur une connexion d'IPsec après plusieurs recompositions, mais 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 vous vérifiez que 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 indebugoutput aussi.

La raison peut être due à une non-correspondance des politiques isakmp ou si le port udp 500 est bloqué en cours de route.

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.

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.