# Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance

## Contenu

# Introduction

Ce document contient les solutions les plus courantes aux problèmes de VPN IPsec. Ces solutions viennent directement de demandes de service que l'assistance technique Cisco a résolu. Beaucoup de ces solutions peuvent être mises en application avant le dépannage approfondi d'une connexion VPN IPsec. En conséquence, ce document fournit une liste de contrôle des procédures courantes à essayer avant de commencer le dépannage d'une connexion et d'appeler l'assistance technique Cisco.

Si vous avez besoin de documents donnant des exemples de configuration pour le VPN de site-à-site et le VPN d'accès à distance, référez-vous aux sections *VPN d'accès à distance, VPN de site à site (L2L) avec PIX, VPN de site à site (L2L) avec IOS,* et *VPN de site à site (L2L) avec VPN3000* de Exemples de configuration et Notes techniques.

**Remarque:** Quoique les exemples de configuration dans ce document servent sur des Routeurs et des dispositifs de sécurité, presque tous ces concepts s'appliquent également au concentrateur VPN 3000.

**Remarque:** Référez-vous au dépannage de sécurité IP - Comprenant et utilisant des commandes de débogage de fournir une explication des commandes de débogage communes qui sont utilisées pour dépanner des questions d'IPsec sur le logiciel de Cisco IOS® et PIX.

**Remarque:** ASA/PIX ne passera pas le trafic de multidiffusion via des tunnels VPN IPsec.

**Remarque:** vous pouvez rechercher toutes les commandes utilisées dans ce document avec l'Outil de recherche de commande (clients enregistrés seulement).

**Avertissement :** beaucoup des solutions présentées dans ce document peuvent mener à une perte provisoire de toute connectivité VPN IPsec sur un périphérique. Il est recommandé de mettre en application ces solutions avec prudence et selon votre politique de contrôle de modification.

# Conditions préalables

## Conditions requises

Cisco recommande que vous connaissiez la configuration de VPN IPsec sur ces périphériques Cisco :

- Dispositif de sécurité de la gamme Cisco PIX 500
- Dispositif de sécurité de la gamme Cisco ASA 5500
- Routeurs Cisco IOS
- Concentrateurs de la gamme Cisco VPN 3000 (*facultatif*)

### 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
- Dispositif de sécurité de la gamme Cisco PIX 500
- Cisco IOS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

### Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

## 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 mentionnées dans aucun ordre particulier, ces solutions peuvent être utilisées comme une liste de contrôle des éléments à vérifier ou à essayer avant que vous engagiez un dépannage approfondi et appeliez le TAC. Toute ces solutions viennent directement de demandes de service au TAC et ont résolu de nombreux problèmes clients.

- 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
- Vérifier que les commandes sysopt sont présentes (PIX/ASA seulement)
- Vérifier l'identité d'ISAKMP
- Vérifier le délai d'attente d'inactivité/de session
- Vérifiez qu'ACLs sont correct et sont Binded au crypto map
- 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
- Obtenir de groupe VPN épuisé
- Questions avec la latence pour le trafic de client vpn

**Remarque:** certaines des commandes dans ces sections ont été mises sur une deuxième ligne pour des questions d'espace.

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

Nat-Traversal ou NAT-T permet au trafic VPN de passer par des périphériques NAT ou PAT, tels qu'un routeur Linksys SOHO. Si NAT-T n'est pas activé, les utilisateurs de client VPN semblent souvent se connecter au PIX ou à l'ASA sans problème, mais ils ne peuvent pas accéder au réseau interne derrière le dispositif de sécurité.

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

De même, si vous ne pouvez pas ouvrir plusieurs sessions simultanées depuis la même adresse IP, le message d'erreur Secure VPN connection terminated locally by client. `Reason 412: The remote peer is no longer responding.` apparaît. 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 20 dans cet exemple est la durée de keepalive (par défaut).

### PIX/ASA 7.1 et antérieur

```
pix(config)#isakmp nat-traversal 20
```

### PIX/ASA 7.2(1) et ultérieur

```
securityappliance(config)#crypto isakmp nat-traversal 20
```

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

Dans le Client VPN Cisco, choisissez **Connection entries** et cliquez sur **Modify**. Une nouvelle fenêtre s'ouvre dans laquelle vous devez choisir l'onglet **Transport**. Sous cet onglet, choisissez **Enable Transparent Tunneling** et la case d'option **IPSec over UDP (NAT/PAT)**. Cliquez alors sur **Save** et testez la connexion.

**Remarque:** cette commande est identique pour PIX 6.x et PIX/ASA 7.x.

**Remarque:** Il est important d'autoriser l'UDP 4500 pour NAT-T, l'UDP 500 et les ports ESP lors de la configuration d'un ACL, parce que le PIX/ASA agit comme un périphérique NAT. Référez-vous à Configuration d'un tunnel IPsec par un pare-feu avec NAT pour plus d'informations afin d'en savoir plus sur la configuration d'un ACL dans PIX/ASA.

### Concentrateur VPN

Choisissez **Configuration > Tunneling and Security > IPSEC > NAT Transparency > Enable : *IPsec au-dessus de NAT-T*** afin d'activer NAT-T sur le concentrateur VPN.

**Remarque:** NAT-T permet également de plusieurs clients vpn de se connecter par un périphérique de PAT en même temps à n'importe quelle tête de réseau si c'est PIX, routeur ou concentrateur.

## Tester correctement la connectivité

Dans l'idéal, la connectivité VPN est testée à partir de périphériques derrière les périphériques qui font le cryptage, pourtant de nombreux utilisateurs testent la connectivité de VPN avec la commande **ping** sur les périphériques qui font le cryptage. Alors que le **ping** fonctionne généralement à cet effet, il est important que la source de votre ping vienne de la bonne interface. Si l'origine du **ping** est mal déterminée, il peut apparaître un échec de la connexion VPN alors qu'en fait cela fonctionne. Prenez ce scénario comme 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, l'origine d'un **ping** doit être déterminée à l'« intérieur » du réseau derrière l'un ou l'autre routeur. Cela est nécessaire, parce que les ACL de chiffrement sont seulement configurés pour crypter le trafic avec ces adresses sources. Un **ping** dont la source vient d'interfaces Internet de l'un ou l'autre routeur n'est pas crypté. Utilisez les options étendues de la commande **ping** dans le mode EXEC privilégié pour déterminer la source d'un ping depuis l'interface « interne » d'un routeur :

```
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 dans ce diagramme ont été remplacés par des dispositifs de sécurité PIX ou ASA. Le **ping** utilisé pour tester la connectivité peut également provenir de l'interface interne avec le mot clé **inside** :

```
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
```

**Remarque:** il n'est pas recommandé de cibler l'interface interne d'un appareil de sécurité avec votre **ping**. Si vous devez cibler l'interface interne avec votre **ping**, vous devez activer

**management-access** sur cette interface ou bien le dispositif ne répond pas.

```
securityappliance(config)#management-access inside
```

**Remarque:** quand un problème existe avec la connectivité, même la phase 1 du VPN ne fonctionne pas. Sur l'ASA, si la connectivité échoue, la sortie SA est semblable à cet exemple, ce qui indique probablement une configuration de l'homologue de chiffrement incorrecte et/ou une configuration de proposition ISAKMP incorrecte :

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG2
```

**Remarque:** l'état pourrait être de MM_WAIT_MSG2 à MM_WAIT_MSG5, ce qui indique un échec de l'échange d'état concerné en mode principal (MM).

**Remarque:** la sortie SA Crypto quand la phase 1 fonctionne est semblable à cet exemple :

```
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 monte tunnel s'établit, c'est probablement dû au fait qu'ISAKMP n'a 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`router(config)#crypto isakmp enable`
- Cisco PIX 7.1 et antérieur (remplacez **outside** par votre interface désirée)`pix(config)#isakmp enable outside`
- Cisco PIX/ASA 7.2(1) et antérieur (remplacez **outside** par votre interface désirée)`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 venir du fait que le client derrière l'ASA/PIS est soumis à un PAT au port UDP 500 avant qu'isakmp ne puisse être activé sur l'interface. Une fois que cette traduction PAT retirée (clear xlate), isakmp peut être activé.

**Remarque:** assurez-vous toujours que les numéros de port UDP 500 et 4500 soient réservés pour la négociation des connexions ISAKMP avec l'homologue.

**Remarque:** Quand l'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
```

**Remarque:** Afin de résoudre cette erreur, activez l'ISAKMP sur la crypto interface 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 du tunnel ; sinon, le tunnel IPsec LAN-à-LAN (L2L) n'est pas établi dans le

routeur PIX/ASA/IOS.

### PIX/ASA :

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

```
hostname(config-group-policy)#pfs {enable | disable}
```

Afin de retirer l'attribut PFS de la configuration en cours, saisissez la forme no de cette commande. Une stratégie de groupe peut hériter d'une valeur pour PFS d'une autre stratégie de groupe. Saisissez la forme no de cette commande afin d'éviter d'hériter d'une valeur.

```
hostname(config-group-policy)#no pfs
```

### Routeur IOS :

Afin de spécifier qu'IPsec doit demander le PFS quand de nouvelles associations de sécurité sont demandées pour cette entrée de la carte de chiffrement ou qu'IPsec requiert le PFS quand il reçoit des demandes de nouvelles associations de sécurité, utilisez la commande **set pfs** en mode configuration de carte de chiffrement. 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 — Spécifie qu'IPsec doit utiliser le groupe modulaire de nombres premiers 1 024 bits Diffie-Hellman quand le nouvel échange Diffie-Hellman est exécuté.

Exemple :

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

**Remarque:** 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.

## Effacer des associations de sécurité anciennes ou existantes (tunnels)

Si ce message d'erreur se produit dans le routeur IOS, le problème est que la SA 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.

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

Si vous effacez l'ISAKMP (phase I) et IPsec (associations de sécurité de phase II) (SAS), il est le plus simple et souvent la meilleure solution de résoudre des problèmes d'IPsec 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.

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

1. Afficher les associations de sécurité avant de les effacer**Cisco IOS**`router#show crypto isakmp sa router#show crypto ipsec sa` **Dispositifs de sécurité Cisco PIX/ASA**`securityappliance#show crypto isakmp sa securityappliance#show crypto ipsec sa` **Remarque:** ces commandes sont identiques pour Cisco PIX 6.x et PIX/ASA 7.x
2. Effacez les associations de sécurité. Chaque commande peut être saisie comme indiqué en gras ou avec les options montrées avec elles.**Cisco IOSISAKMP (phase I)**`router#clear crypto isakmp ? <0 - 32766> connection id of SA <cr>`**IPsec (phase II)**`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>`**Dispositifs de sécurité Cisco PIX/ASAISAKMP (phase I)**`securityappliance#clear crypto isakmp sa` **IPsec (phase II)**`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 divergence quelconque se produit dans la durée de vie d'ISAKMP, vous pouvez recevoir le message d'erreur **%PIX|ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision** dans PIX/ASA. Pour FWSM, vous pouvez recevoir le message d'erreur %FWSM-5-713092: `Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekeying attempt due to collision.` Configurez la même valeur dans les deux homologues afin de résoudre le problème.

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).

PIX/ASA

`hostname(config)#`**`isakmp policy 2 lifetime 14400`**
Routeur IOS

`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. Reason 426:` Maximum Configured Lifetime Exceeded.

Afin de résoudre ce message d'erreur, définissez la valeur **lifetime** à *0* afin de définir la durée de vie d'une association de sécurité IKE à l'infini. Le VPN sera toujours connecté et ne s'arrêtera 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 d'ISAKMP dans Cisco IOS avec cette commande :`router(config)#`**`crypto isakmp keepalive 15`**
- Utilisez ces commandes pour configurer les keepalives d'ISAKMP sur les dispositifs de sécurité PIX/ASA :Cisco PIX 6.x`pix(config)#`**`isakmp keepalive 15`** Cisco PIX/ASA 7.x et ultérieur, pour le groupe de tunnels nommé **10.165.205.222**`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 PIX/ASA 7.x et ultérieur, pour le groupe de tunnels nommé **10.165.205.222**Désactive le traitement du keepalive IKE qui est activé par défaut.`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**Choisissez **%System Root% > Program Files > Cisco Systems >VPN Client > Profiles** sur le PC client qui rencontre le problème afin de désactiver le keepalive IKE et modifier le **fichier PCF**, le cas échéant, pour la connexion.Remplacez **'ForceKeepAlives=0'** (valeur par défaut) par **'ForceKeepAlives=1'**.

**Remarque:** 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 tunnel 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.** Ressaisissez une clé pour être certain qu'elle soit correcte ; c'est une solution simple qui peut 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 rencontrer cette erreur si le nom de groupe/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... may 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)
```

Vous pouvez également récupérer une clé pré-partagée sans changement dans la configuration sur le dispositif de sécurité PIX/ASA. Référez-vous à PIX/ASA 7.x : Récupération de clé pré-partagée.

**Avertissement :** si vous supprimez des commandes relatives au chiffrement, vous risquez d'interrompre un ou tous vos tunnels VPN. Utilisez ces commandes avec prudence et référez-vous à la politique de contrôle de modification de votre organisation avant de suivre ces étapes.

- Utilisez ces commandes pour supprimer et ressaisir la clé pré-partagée **secretkey** pour l'homologue **10.0.0.1** ou le groupe **vpngroup** dans IOS :VPN Cisco de LAN-à-LAN`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`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 de** pour l'homologue **10.0.0.1** sur des dispositifs de sécurité PIX/ASA :Cisco PIX 6.x`pix(config)#`**`no isakmp key secretkey address 10.0.0.1`** `pix(config)#`**`isakmp key secretkey address 10.0.0.1`** Cisco PIX/ASA 7.x et ultérieur`securityappliance(config)#`**`tunnel-group 10.0.0.1 ipsec-attributes`** `securityappliance(config-tunnel-ipsec)#`**`no pre-shared-key`** `securityappliance(config-tunnel-ipsec)#`**`pre-shared-key secretkey`**

## Clé pré-partagée non correspondante

L'initiation du tunnel VPN se déconnecte. Ce problème peut se produire en raison d'une clé pré-partagée non correspondante pendant I des négociations.

Le message **MM_WAIT_MSG_6** dans la commande de **show crypto isakmp sa** indique un pre-

shared-key mal adapté suivant les indications de cet exemple :

```
ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 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, ressaisissez la clé pré-partagée dans les deux dispositifs ; la clé pré-partagée doit être unique et doit correspondre. Voyez Ressaisir ou récupérer les clé pré-partagées pour plus d'informations.

## Supprimer et ré-appliquer des cartes de chiffrement

Quand vous effacez des associations de sécurité, et lui ne résout pas un problème d'IPsec VPN, retire et réapplique le crypto map approprié afin de résoudre une grande variété de problèmes qui inclut la baisse intermittente du tunnel VPN et le manque de quelques sites VPN pour monter.

**Avertissement :** Si vous supprimez une carte de chiffrement d'une interface, cela interrompt **définitivement** tous les tunnels IPsec associés à cette carte de chiffrement. Suivez ces étapes avec prudence et tenez compte de la politique de contrôle de modification de votre organisation avant de commencer.

- Utilisez ces commandes pour supprimer 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**.`router(config-if)#no crypto map mymap` Continuez à utiliser la forme **no** pour supprimer une carte de chiffrement entière.`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 :`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 carte de chiffrement sur le PIX ou l'ASA :Commencez en supprimant la carte de chiffrement de l'interface. Utilisez la forme no de la commande **crypto map**.`securityappliance(config)#no crypto map mymap interface outside` Continuez à utiliser la forme **no** pour supprimer les autres commandes crypto map.`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 :`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`

**Remarque:** 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 (PIX/ASA seulement)

Les commandes **sysopt connection permit-ipsec** et **sysopt connection permit-vpn** permettent à des paquets d'un tunnel IPsec et à leurs charges utiles de sauter les ACL d'interface sur le dispositif 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 adéquate pour cette situation est **sysopt connection permit-ipsec**.

Dans le logiciel du dispositif de sécurité version 7.1(1) et ultérieure, la commande sysopt adéquate pour cette situation est **sysopt connection permit-vpn**.

Dans PIX 6.x, cette fonctionnalité est **désactivée** par Default. Avec PIX/ASA 7.0(1) et ultérieur, cette fonctionnalité est **activée** par défaut. Utilisez ces commandes show pour déterminer si la commande **sysopt** adéquate est activée sur votre périphérique :

- Cisco PIX 6.x`pix# **show 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 no sysopt uauth allow-http-cache **no sysopt connection permit-ipsec** *!--- sysopt connection permit-ipsec is disabled* no sysopt connection permit-pptp no sysopt connection permit-l2tp no sysopt ipsec pl-compatible`
- Cisco PIX/ASA 7.x`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 **sysopt** correcte pour votre périphérique :

- Cisco PIX 6.x et PIX/ASA 7.0`pix(config)#**sysopt connection permit-ipsec**`
- Cisco PIX/ASA 7.1(1) et ultérieur`securityappliance(config)#**sysopt connection permit-vpn**`

**Remarque:** Si vous ne souhaitez pas utiliser la commande de **connexion de sysopt**, alors vous devez explicitement permettre le trafic prié, qui est le trafic intéressant de la source à la destination, par exemple, du RÉSEAU LOCAL du périphérique distant au RÉSEAU LOCAL du périphérique local et du « port UDP 500" pour l'interface extérieure du périphérique distant à l'interface extérieure du périphérique local, dans l'ACL extérieur.

## Vérifier l'identité d'ISAKMP

Si le tunnel VPN d'IPsec a manqué dans la négociation d'IKE, la panne peut être due au PIX ou à l'incapacité de son pair d'identifier l'identité de son pair. 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 du pare-feu PIX est paramétrée 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 faire en sorte que l'IP de la phase 2 soit envoyée à l'homologue, utilisez la commande **isakmp identity** dans le 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 type
```

OU

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by
connection type; IP address for !--- preshared key or cert DN for certificate authentication.
```

OU

```
crypto isakmp identity hostname
```

```
!--- Uses the fully-qualified domain name of !--- the host exchanging ISAKMP identity
information (default). !--- This name comprises the hostname and the domain name.
```

Le tunnel VPN ne soulève pas après configuration mobile de PIX à l'ASA utilisant l'outil de transfert de configuration PIX/ASA ; ces messages apparaissent dans le log :

```
[IKEv1] : Le groupe = les x.x.x.x, IP = x.x.x.x, PeerTblEntry éventé fondent, retirant ! [IKEv1]
: Le groupe = le x.x.x.x, IP = x.x.x.x, retirant le pair de la table de corrélateur ont manqué,
aucune correspondance ! [IKEv1] : Groupe = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete() :
Aucun SPI pour identifier Phase 2 SA ! [IKEv1] : Le groupe = le x.x.x.x, IP = x.x.x.x, retirant
le pair de la table de corrélateur ont manqué, aucune correspondance !
```

Cette question se produit puisque PIX par défaut est placé pour identifier la connexion comme **adresse Internet** où l'ASA l'identifie comme **IP**. Afin de résoudre ce problème, utilisez la commande de **crypto isakmp identity** en mode de configuration globale comme affiché ci-dessous :

```
crypto isakmp identity hostname !--- Use the fully-qualified domain name of !--- the host
exchanging ISAKMP identity information (default). !--- This name comprises the hostname and the
domain name.
```

Quand vous recevez `reçu un` message d'erreur `non codé INVALID_COOKIE`, émettez la commande d'**adresse de crypto isakmp identity** afin de résoudre le problème.

**Remarque:** La commande **isakmp identity** a été abandonnée à partir de la version 7.2(1) du logiciel. Référez-vous à Référence de commandes des dispositifs de sécurité Cisco version 7.2 pour plus d'informations.

## 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 au bout de 30 minutes indépendamment de la configuration du délai d'attente et rencontre l'erreur PEER_DELETE-IKE_DELETE_UNSPECIFIED.

Configurez le **délai d'attente de veille** et le **délai d'attente de session** car **aucun** afin de composer le tunnel toujours, et de sorte que le tunnel ne soit jamais lâché même lorsqu'à l'aide des périphériques de tiers.

### PIX/ASA 7.x et ultérieur

Saisissez la commande **vpn-idle-timeout** dans le mode de configuration de la stratégie de groupe ou de configuration du nom d'utilisateur afin de configurer le délai d'attente de l'utilisateur :

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-idle-
timeout none
```

Configurez une durée maximale pour des connexions de VPN avec la commande **vpn-session-timeout** dans le mode de configuration de la stratégie de groupe ou de configuration du nom d'utilisateur :

```
hostname(config)#group-policy DfltGrpPolicy attributes hostname(config-group-policy)#vpn-
session-timeout none
```

**Remarque:** Quand vous avez tunnel-**tout** configuré, vous n'avez pas besoin de configurer l'inactif-**délai d'attente** parce que, même si vous configurez le délai d'attente de VPN-inactif, cela ne fonctionnera pas parce que tout le trafic va par le tunnel (puisque tunnel-tout est configuré). Par conséquent, le trafic intéressant (ou même le trafic généré par le PC) sera intéressant et ne

permettra pas l'Inactif-délai d'attente d'entrer dans l'action.

### Routeur Cisco IOS

Utilisez la commande **crypto ipsec security-association idle-time** dans le mode de configuration globale ou de configuration de la carte de chiffrement afin de configurer le temporisateur d'attente de SA IPsec. Par défaut, les temporisateurs de SA IPsec sont désactivés.

**crypto ipsec security-association idle-time** *seconds*
La durée en *seconds* est celle qui est autorisée par le temporisateur pour qu'un homologue inactif puisse maintenir une SA. Les valeurs valides pour l'argument seconds sont comprises entre 60 et 86 400.

## Vérifiez qu'ACLs sont correct et Binded au crypto map

Dans une configuration VPN IPsec classique, deux listes d'accès sont utilisées. L'une permet d'exempter le trafic destiné au tunnel VPN à partir du processus NAT, l'autre définit le trafic à crypter. Ceci inclut une ACL de chiffrement dans une configuration LAN-à-LAN ou une ACL transmission tunnel partagée dans une configuration d'accès à distance. Lorsque ces ACL ne sont pas correctement configurées ou qu'elles sont manquantes, le trafic risque de ne circuler que dans un seul sens dans le tunnel VPN ou de ne pas être envoyé du tout dans le tunnel.

**Remarque:** Veillez à lier le crypto ACL avec le crypto map à l'aide de la commande d'adresse de correspondance de crypto map 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.**Remarque:** Sur le concentrateur VPN, vous pourriez voir un journal comme ceci :`Tunnel Rejected: IKE peer does not match remote peer as defined in L2L policy`Afin d'éviter ce message et de faire fonctionner le tunnel, assurez-vous que les ACL de chiffrement ne superposent pas et que le même trafic intéressant n'est utilisé par aucun autre tunnel VPN configuré.
- N'utilisez pas une ACL deux fois. Même si vos listes de contrôle d'accès d'exemption NAT et de chiffrement indiquent le même trafic, utilisez deux listes d'accès différentes.
- Pour la configuration d'accès à distance, n'utilisez pas de liste d'accès pour le trafic intéressant avec la carte de chiffrement dynamique. Ceci peut rendre le client VPN incapable de se connecter au périphérique de tête de réseau. Si vous avez configuré de manière erronée l'ACL de chiffrement pour le VPN d'accès à distance, vous pouvez obtenir le message d'erreur %ASA-3-713042: `IKE Initiator unable to find policy:` Intf 2.**Remarque:** Si c'est un tunnel de site à site VPN, veillez à apparier la liste d'accès avec le pair. Ils doivent être en ordre inverse sur le pair.Référez-vous à Exemple de configuration d'authentification PIX/ASA 7.x et client VPN Cisco 4.x avec Windows 2003 RADIUS IAS (sur Active Directory) pour avoir un exemple de configuration qui montre comment configurer la connexion VPN

d'accès à distance entre un client VPN Cisco et le PIX/ASA.

- 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 le PIX ou l'ASA, cela signifie que vous utilisez la commande **nat (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 IOS est configuré pour exempter le trafic envoyé entre **192.168.100.0 /24** et **192.168.200.0 /24** ou **192.168.1.0 /24** depuis le 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`Ici, un PIX est configuré pour exempter le trafic envoyé entre **192.168.100.0 /24** et **192.168.200.0 /24** ou **192.168.1.0 /24** depuis le NAT. Par exemple, tout autre trafic est soumis à la surcharge NAT :`access-list **noNAT** extended permit ip 192.168.100.0 255.255.255.0 192.168.200.0 255.255.255.0 access-list **noNAT** extended permit ip 192.168.100.0 255.255.255.0 192.168.1.0 255.255.255.0 nat (inside) 0 access-list **noNAT** nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface` **Remarque:** 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 ACL d'exemption NAT ne fonctionnent pas avec les numéros de port (par exemple, 23, 25, etc.).**Remarque:** Dans un environnement VOIP, dans lequel les appels vocaux entre les réseaux sont communiqués par le VPN, les appels vocaux ne fonctionnent pas si les ACL NAT 0 ne sont pas correctement configurés. Avant de procéder à un dépannage approfondi de la VOIP, il est suggéré de contrôler l'état de la connectivité VPN, parce que le problème pourrait être la mauvaise configuration d'ACL d'exemption NAT.**Remarque:** Vous pouvez obtenir le message d'erreur indiqué s'il y a mauvaise configuration dans les ACL d'exemption NAT (nat 0).`%PIX-3-305005: **No translation group** found for icmp src outside:192.168.100.41 dst inside:192.168.200.253 (type 8, code 0) %ASA-3-305005: No translation group found for udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p`**Remarque: Exemple incorrect :**`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, alors essayez de la supprimer et émettez la commande **NAT 0** pour 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. Ceci signifie que les ACL doivent servir de **miroir** les unes pour les autres. Dans cet exemple, un tunnel de LAN-à-LAN est configuré entre **192.168.100.0 /24** et **192.168.200.0 /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`**Remarque:** Bien que ce ne soit pas illustré ici, ce même concept s'applique aussi aux dispositifs de sécurité PIX et ASA.Dans PIX/ASA, les ACL de transmission tunnel partagée pour configurations d'accès à distance doivent être des listes d'accès **standard** qui autorisent le trafic vers le réseau pour lequel les clients VPN ont besoin

d'accès. Les routeurs IOS peuvent utiliser une ACL étendue pour la transmission tunnel partagée.**Remarque:** dans la liste d'accès étendue, utiliser **'any'** à la source dans l'ACL de transmission tunnel partagée revient au même que désactiver la transmission tunnel partagée. Utilisez seulement les réseaux sources dans l'ACL étendue pour la transmission tunnel partagée.**Remarque: Exemple correct :**`access-list 140 permit ip **10.1.0.0 0.0.255.255** 10.18.0.0 0.0.255.255` **Remarque: Exemple incorrect :**`access-list 140 permit ip **any** 10.18.0.0 0.0.255.255` **Cisco IOS**`**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 PIX 6.**x**`pix(config)#**access-list 10 permit** 192.168.100.0 255.255.255.0 pix(config)#**vpngroup MYGROUP split-tunnel 10**` Cisco PIX/ASA 7.**x**`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**`

Cette erreur se produit dans ASA 8.3 si l'AUCUN ACL NAT pas misconfigured ou n'est pas configurée sur l'ASA :

```
%ASA-5-305013 : Règles NAT asymétriques appariées pour en avant et des flux inverses ; Connexion
pour l'extérieur de src d'UDP : intérieur de dst x.x.x.x/xxxxx : en raison refusé par x.x.x.x/xx
de la panne NAT de chemin inverse
```

Afin de résoudre ce problème, vérifiez la configuration est correct ou modifie si les configurations sont incorrectes.

**Configuration de nat exemption dans la version 8.3 ASA pour le tunnel VPN de site à site :**

Un site à site VPN doit être établi entre HOASA et BOASA avec les deux ASA utilisant la version 8.3. La configuration de nat exemption sur HOASA semble semblable 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 de site-à-site ne peuvent pas établir le tunnel avec le périphérique distant, vérifiez que **les deux homologues contiennent les mêmes valeurs de cryptage, d'authentification et de paramètre Diffie-Hellman** et quand la stratégie de l'homologue distant spécifie une durée de vie inférieure ou égale à celle de la stratégie que l'initiateur a envoyée. Si les durées de vie ne sont pas identiques, le dispositif de sécurité utilise la durée de vie plus courte. Si aucune correspondance acceptable n'existe, ISAKMP refuse la négociation et la SA n'est pas établie.

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

Voici 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, dropping
```

Ce message apparaît habituellement en raison de stratégies ISAKMP non correspondantes ou d'une déclaration NAT 0 manquante.

En outre, ce message apparaît :

```
Error Message    %PIX|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 mis en file d'attente après la fin de la phase 1. Ce message d'erreur peut avoir l'un des motifs suivants :

- Non correspondance de phase sur l'un des homologues
- L'ACL empêche les homologues de terminer la phase 1

Ce message vient habituellement après le message d'erreur Removing peer from peer table failed, no 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.

**Remarque:** Pour la stratégie ISAKMP et le jeu de transformation IPsec qui est utilisé sur le PIX/ASA, le client VPN Cisco ne peut pas utiliser une stratégie avec une combinaison de DES et de 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

Le routage est une partie capitale de presque chaque déploiement VPN IPsec. Assurez-vous que vos périphériques de cryptage, tels que des routeurs et des dispositifs de sécurité PIX ou ASA, ont les informations de routage appropriées pour envoyer le trafic via votre tunnel VPN. Par ailleurs, si d'autres routeurs existent derrière votre périphérique de passerelle, assurez-vous que ces routeurs sachent comment atteindre le tunnel et quels réseaux sont 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 Router A a été remplacé par un PIX ou 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 :`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 Router A a été remplacé par un PIX ou ASA, la configuration peut ressembler à ceci :`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, supposez que les clients VPN obtiennent des adresses comprises dans la plage de 10.0.0.0 /24 quand 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 :`crypto dynamic-map dynMAP 10`
`set transform-set mySET`

**`reverse-route`** `crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP`Dispositif de sécurité Cisco PIX ou ASA :`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`

**Remarque:** 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 Réseaux privés en superposition.

## 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 Référence des commandes du guide de configuration du dispositif de sécurité Cisco pour plus d'informations.

**Remarque:** Pour la stratégie ISAKMP et le jeu de transformation IPsec qui est utilisé sur le PIX/ASA, le client VPN Cisco ne peut pas utiliser une stratégie avec une combinaison de DES et de 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 dynamique de la carte de chiffrement **doit être** plus élevé que toutes les autres entrées statiques de la carte de chiffrement. 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!
```

**Remarque:** 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 :

```
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 cisco
```

**Remarque:** Les noms de cartes de chiffrement sont sensibles à la casse.

**Remarque:** Ce message d'erreur peut également être vu quand le crypto ordre dynamique d'homme n'est pas correct qui fait frapper le pair le crypto map faux, et également par une crypto liste d'accès mal adaptée qui définit le trafic intéressant : `%ASA-3-713042 : IKE Initiator unable to find policy:`

Dans les scénarios où plusieurs tunnels VPN doivent se terminer sur la même interface, nous avons besoin de créer une carte de chiffrement avec le même nom (une seule carte de chiffrement est permise par interface), mais avec un numéro de séquence différent. Il en va de même pour le routeur, le PIX et l'ASA.

Référez-vous à Configurer IPsec entre un concentrateur et des PIX distants avec un client VPN et l'authentification étendue pour plus d'informations afin d'en savoir plus sur la configuration PIX du

concentrateur pour la même carte de chiffrement avec des numéros de séquence différents sur la même interface. De même, référez-vous à PIX/ASA 7.X : Ajouter un nouveau tunnel ou accès à distance à un VPN L2L existant pour plus d'informations afin d'en savoir plus sur la configuration de la carte de chiffrement pour des scénarios VPN L2L et d'accès à distance.

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

Pour une configuration VPN IPsec de LAN-à-LAN (L2L) avec dispositif de sécurité PIX/ASA 7.x, vous devez spécifier le nom (**<name>**) du groupe de tunnels comme **adresse ip de l'homologue** distant (fin de tunnel distant) dans la commande **tunnel-group<name> type ipsec-l2l** pour la création et la gestion de la base de données des enregistrements spécifiques à la connexion pour IPsec. L'adresse IP de l'homologue doit correspondre dans les commandes **tunnel group name** et **Crypto map set address**. 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, ce qui peut être résolu par la configuration appropriée 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
```

Dans une configuration VPN IPsec de LAN-à-LAN (L2L) avec PIX 6.x, l'adresse IP de l'homologue (fin de tunnel distant) doit correspondre dans les commandes **isakmp key address** et **set peer** dans la carte de chiffrement pour que la connexion VPN IPsec fonctionne.

Quand l'adresse IP de pair n'a pas été configurée correctement sur la crypto configuration ASA, l'ASA ne peut pas établir le tunnel VPN et s'arrête dans l'étape *MM_WAIT_MSG4* seulement. Afin de résoudre ce problème, corrigez l'adresse IP de pair dans la configuration.

Voici la sortie de la commande de **show crypto isakmp sa** quand le tunnel VPN s'arrête à dans l'état MM_WAIT_MSG4.

```
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

```
%PIX|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.

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

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

**Both lines should 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 de LAN-à-LAN et un tunnel VPN d'accès à distance sont configurés sur la même carte de chiffrement, des informations sur XAUTH sont demandées à l'homologue LAN-à-LAN et le tunnel de LAN-à-LAN échoue avec « *CONF_XAUTH* » dans la sortie de la commande **show crypto isakmp sa**.

Voici un exemple de sortie SA :

```
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
```

**Remarque:** Cette question s'applique seulement au Cisco IOS et au PIX 6.x tandis que PIX/ASA 7.x n'est pas affecté par cette question puisqu'il utilise des groupes de tunnels.

Utilisez le mot clé **no-xauth** quand vous saisissez la clé isakmp, de sorte que le périphérique ne demande pas d'informations sur 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 :

```
router(config)#crypto isakmp key cisco123 address 172.22.1.164 no-xauth
```

Dans le scénario où le PIX/ASA 7.x agit en tant que serveur Easy VPN, le client vpn facile ne peut pas se connecter à la tête de réseau en raison de la question de Xauth. Désactivez l'authentification des utilisateurs dans le PIX/ASA afin de résoudre le problème comme montré :

```
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
```

Voyez la section Divers de ce document afin d'en savoir plus sur la commande **isakmp ikev1-user-authentication**.

## Obtenir de groupe VPN épuisé

Quand la plage des adresses IP assignées au groupe VPN ne sont pas suffisante, vous pouvez étendre la Disponibilité des adresses IP de deux manières :

1. Enlevez la plage existante, et définissez la nouvelle gamme. Voici un exemple :`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 au groupe VPN, vous pouvez définir deux groupes distincts VPN et les spécifier alors dans la commande sous le « groupe de tunnels attribue ». Voici un exemple :`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 l'ASA alloue des adresses de ces groupes dans la commande dans laquelle les groupes apparaissent dans cette commande.

**Remarque:** Les configurations d'address-pool dans les address-pool de stratégie de groupe commandent toujours le dépassement les configurations de groupe local dans l'ordre d'address-pool de groupe de tunnels.

## Questions avec la latence pour le trafic de client vpn

Quand il y a des questions de latence au-dessus d'une connexion VPN, vérifiez le suivant afin de résoudre ceci :

1. Vérifiez si le MSS du paquet peut être réduit plus loin.
2. Si IPsec/TCP est utilisé au lieu d'IPsec/d'UDP, alors configurez le conserve-VPN-écoulement.
3. Rechargez Cisco ASA.

# Les clients VPN ne peuvent pas se connecter à ASA/PIX

## 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 :

```
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 rétrécir vers le bas le problème, vérifiez d'abord l'authentification avec la base de données locale sur l'ASA.

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

Si ceci fonctionne bien, alors le problème devrait être lié à la configuration du serveur RADIUS.

Vérifiez la Connectivité du serveur de rayon de l'ASA. Si le ping fonctionne sans problème, alors vérifiez la configuration liée au rayon sur l'ASA et la configuration de base de données sur le serveur de rayon.

Vous pourriez utiliser la commande de **debug radius** de dépanner des questions connexes de rayon. Pour la sortie de **debug radius** témoin, référez-vous à cette sortie témoin.

**Remarque:** Avant que vous utilisiez la commande de **débogage** sur l'ASA, référez-vous à cette documentation : Message d'avertissement.

# La connexion de baisses de client vpn fréquemment sur connexion VPN de premier essai ou la « de Sécurité s'est terminée 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 peuvent recevoir cette erreur quand ils essayent la connexion avec le périphérique VPN de tête de réseau.

« La *connexion de baisses de client vpn fréquemment sur le premier essai* » ou la « *connexion VPN de Sécurité s'est terminée par le pair. Raison 433."* ou « *connexion VPN sécurisée terminée par la raison 433:(Reason de pair non spécifiée par le pair)* » ou « *tentée pour assigner le réseau ou pour annoncer l'adresse IP, retirant (x.x.x.x) du groupe »*

## Solution 1

Le problème pourrait être avec l'affectation de pool d'IP par ASA/PIX, serveur de rayon, serveur DHCP ou par le serveur de rayon agissant en tant que serveur DHCP. Utilisez la commande **debug crypto** afin 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

Cette question se produit également en raison de la panne de l'authentification étendue. Vous devez vérifier le serveur d'AAA pour dépanner cette erreur. Vérifier le mot de passe d'authentification de serveur sur le serveur et le client et le rechargement du serveur d'AAA pourraient résoudre ce problème.

## Solution 3

Un autre contournement pour cette question est de désactiver la configuration de détection de menace. Parfois quand il y a de plusieurs retransmissions pour différentes associations de sécurité inachevées (SAS), l'ASA avec la fonction activée de menace-détection pense qu'une attaque de lecture se produit et les ports VPN sont marqués en tant que contrevenant principal. Essayez de désactiver la configuration de menace-détection comme ceci peut entraîner beaucoup de temps système sur le traitement de l'ASA. Employez ces commandes afin de désactiver la détection de menace :

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

Pour plus d'informations sur cette caractéristique, référez-vous à la détection de menace.

**Remarque:** Ceci peut être utilisé comme contournement pour vérifier si ceci répare le problème réel. Assurez-vous que désactivant la détection de menace sur Cisco ASA compromet réellement

plusieurs fonctionnalités de sécurité telles qu'atténuer les tentatives de lecture, DOS avec le SPI non valide, les paquets qui échouent inspection d'application et sessions inachevées.

### Solution 4

Cette question se produit également quand un jeu de transformations n'est pas correctement configuré. Une configuration correcte du jeu 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
- Hairpinning
- Accès au LAN local
- Réseaux privés en superposition

### Impossible d'accéder aux serveurs dans DMZ

Une fois que le client VPN est établi, le tunnel IPsec avec le périphérique VPN de tête de réseau (routeur PIX/ASA/IOS), les utilisateurs du client VPN peuvent accéder aux ressources du réseau INTERNE (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

| ASA/PIX |
| --- |
| `ciscoasa#show running-config !--- Split tunnel for the inside network access access-list vpnusers_spitTunnelAcl permit ip 10.10.10.0 255.255.0.0 any !--- Split tunnel` |

```
for the DMZ network access access-list
vpnusers_spitTunnelAcl permit ip 10.1.1.0 255.255.0.0
any !--- Create a pool of addresses from which IP
addresses are assigned !--- dynamically to the remote
VPN Clients. ip local pool vpnclient 192.168.1.1-
192.168.1.5 !--- This access list is used for a nat zero
command that prevents !--- traffic which matches the
access list from undergoing NAT. !--- No Nat for the DMZ
network. access-list nonat-dmz permit ip 10.1.1.0
255.255.255.0 192.168.1.0 255.255.255.0 !--- No Nat for
the Inside network. access-list nonat-in permit ip
10.10.10.0 255.255.255.0 192.168.1.0 255.255.255.0 !---
NAT 0 prevents NAT for networks specified in the ACL
nonat . nat (DMZ) 0 access-list nonat-dmz nat (inside) 0
access-list nonat-in
```

### Configuration de version 8.3 ASA :

Cette configuration affiche comment configurer le nat exemption 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
```

### Vérifiez :

Si le tunnel a été établi, allez au **client VPN Cisco** et choisissez **Status > Route Details** pour vérifier que les routes sécurisées sont affichées pour les réseaux DMZ et INTERNES.

Référez-vous à PIX/ASA 7.x : Accès au serveur de messagerie sur l'exemple de configuration DMZ pour plus d'informations sur la façon de configurer le pare-feu PIX pour l'accès à un serveur de messagerie situé sur le réseau de Zone démilitarisée (DMZ).

Référez-vous à PIX/ASA 7.x : Ajouter un nouveau tunnel ou accès à distance à un VPN L2L existant afin d'obtenir les étapes nécessaires à l'ajout d'un nouveau tunnel VPN ou d'un VPN d'accès à distance à une configuration VPN L2L qui existe déjà.

Référez-vous à PIX/ASA 7.x : Permettre la transmission tunnel partagée pour des clients VPN sur l'exemple de configuration ASA afin d'obtenir des instructions pas à pas sur la façon de permettre l'accès de clients VPN à l'Internet tandis qu'ils sont reliés par tunnel dans un dispositif de sécurité adaptatif (ASA) Cisco de la gamme 5500.

Référez-vous à Exemple de configuration d'authentification PIX/ASA 7.x et client VPN Cisco 4.x avec Windows 2003 RADIUS IAS (sur Active Directory) pour plus d'informations sur la façon de configurer la connexion VPN d'accès à distance entre un client VPN Cisco (4.x pour Windows) et le dispositif de sécurité 7.x de le gamme PIX 500.

## Les clients VPN sont incapables de résoudre le DNS

Une fois le tunnel établi, si les clients VPN ne peuvent pas résoudre le DNS, le problème peut être

la configuration du serveur DNS dans le périphérique de tête de réseau (ASA/PIX). Contrôlez également la connectivité entre les clients VPN et le serveur DNS. La configuration du serveur DNS doit être effectuée sous la stratégie de groupe et être appliqué sous la stratégie de groupe dans les attributs généraux du groupe de tunnels ; par exemple :

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP
address(172.16.1.1) !--- and the domain name(cisco.com) in the group policy. 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 !--- using 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

La transmission tunnel partagée laisse les clients IPsec d'accès à distance diriger conditionnellement des paquets via le tunnel IPsec sous forme cryptée ou diriger des paquets vers une interface réseau sous forme de texte clair, décryptée, dans laquelle ils sont ensuite routés vers la destination finale. La transmission tunnel partagée est désactivée par défaut, c'est le trafic tunnelall.

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

Remarque: *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
```

Référez-vous à ces documents pour des exemples de configuration détaillés de transmission tunnel partagée :

- PIX/ASA 7.x : Permettre le split tunneling pour des clients VPN sur l'exemple de configuration de l'ASA
- Exemple de configuration d'un routeur autorisant les clients VPN à se connecter à IPsec et à Internet via la transmission tunnel partagée
- Exemple de configuration de transmission tunnel partagée pour clients VPN sur le concentrateur VPN 3000

## Hairpinning

Cette fonctionnalité est utile pour le trafic VPN qui entre dans interface, mais qui est ensuite routé hors de cette même interface. Par exemple, si vous avez un réseau VPN en étoile dans lequel le dispositif de sécurité est le concentrateur et les réseaux VPN à distance sont des rayons, pour qu'un rayon communique avec un autre, le trafic doit aller dans le dispositif de sécurité, puis ressortir pour aller vers l'autre rayon.

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

```
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 à PIX/ASA 7.x : Permettre l'accès au LAN local pour des clients VPN.

## Réseaux privés en superposition

### Problème

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

### Solution

Assurez-vous toujours que les adresses IP dans le pool à assigner pour les clients VPN, le réseau interne du périphérique de tête de réseau et le réseau interne de client VPN doivent être 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, voyez le *diagramme* et l'*exemple* de la section Impossible 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/PIX ; la connexion pour le 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
- Configurer ASA/PIX avec CLI
- Configurer un concentrateur

Pour plus d'informations, référez-vous à la section Configurer des stratégies de groupe de Procédures de configuration ASDM VPN sélectionnées pour la gamme Cisco ASA 5500 version 5.2.

## Configurer des procédures de connexion simultanées

Si la case à cocher **Inherit** dans l'ASDM est cochée, le nombre par défaut de procédures de connexion simultanées seulement est permis pour l'utilisateur. La valeur par défaut pour des procédures de connexion simultanées est trois.

Afin de résoudre ce problème, augmentez la valeur pour des procédures de connexion simultanées.

1. Lancez l'ASDM, puis allez à **Configuration > VPN > Group Policy**.
2. Choisissez le **Group** approprié et cliquez sur le bouton **Edit**.
3. Une fois dans l'**onglet General**, décochez la case à cocher **Inherit** pour **Simultaneous Logins** sous **Connection Settings**. Choisissez une valeur Appropriée dans le champ.**Remarque:** La valeur minimale pour ce champ est 0, ce qui désactive la procédure de connexion et empêche l'accès aux utilisateurs.**Remarque:** Quand vous ouvrez une session utilisant le même compte utilisateur d'un PC différent, la session en cours (la connexion établie d'un autre PC utilisant le même compte utilisateur) est terminée, et la nouvelle session est établie. C'est le comportement par défaut et est indépendant aux procédures de connexion simultanées VPN.

## Configurer ASA/PIX avec CLI

Effectuez ces étapes afin de configurer le nombre désiré de procédures de connexion simultanées. Dans cet exemple, 20 a été choisi comme valeur désirée.

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

Afin d'en savoir plus sur cette commande, référez-vous à Référence de commande des dispositifs de sécurité Cisco version 7.2.

Utilisez la commande **vpn-sessiondb max-session-limit** dans le mode de configuration globale afin de limiter les sessions VPN à une valeur plus faible que celle autorisée par le dispositif de sécurité. Utilisez la version no 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 :

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

## Configurer un concentrateur

```
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 le **Configuration > User Management > Groups > modifient 10.19.187.229 > le général > des procédures de connexion simultanées**, et changent le nombre de procédures de connexion 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 pour trouver si le serveur d'application est accessible depuis votre réseau. Cela peut être un problème avec la taille de segment maximale (MSS) pour les paquets temporaires qui traversent un routeur ou un périphérique PIX/ASA, en particulier des segments TCP avec le bit SYN paramétré.

## Routeur Cisco IOS — Changer 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 :

```
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 :

```
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 PIX/ASA 7.x et IOS : fragmentation de VPN.

## PIX/ASA 7.X — Se référer à la documentation PIX/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 ces documents afin de résoudre le problème :

- PIX/ASA 7.x et IOS : Fragmentation VPN
- Problème avec PIX/ASA 7.0 : MSS dépassée - Les clients HTTP ne peuvent pas naviguer vers certains sites Web

# Impossible d'initier un tunnel VPN depuis ASA/PIX

## Problème

Vous ne pouvez pas initier le tunnel VPN depuis l'interface d'ASA/PIX, et après l'établissement du tunnel, l'extrémité distante/client VPN ne peut pas soumettre de requête ping à l'interface interne d'ASA/PIX sur le tunnel VPN. Par exemple, il est possible que le client pn ne puisse pas initier une connexion SSH ou HTTP vers l'interface interne de l'ASA via le tunnel VPN.

## Solution

Une requête ping ne peut pas être soumise à l'interface interne du PIX depuis l'autre extrémité du tunnel à moins que la commande **management-access** soit configurée dans le mode de configuration globale.

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access inside
```

**Remarque:** cette commande également à initier une connexion ssh ou http vers l'interface interne de l'ASA via un tunnel VPN.

**Remarque:** Ces informations jugent vrai pour l'interface DMZ aussi bien. Par exemple, si vous voulez soumettre un requête ping à l'interface DMZ de PIX/ASA ou si vous voulez initier un tunnel depuis l'interface DMZ, la commande **management-access DMZ** est requise.

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

**Remarque:** Si le client VPN ne peut pas se connecter, alors assurez-vous que les ports ESP et UDP sont ouverts. Cependant, si ces ports ne sont pas ouverts, essayez une connexion sur TCP 10 000 avec la sélection de ce port sous l'entrée de connexion du client VPN. Cliquez avec le bouton droit sur **modify > transport tab > IPsec over TCP**. Référez-vous à PIX/ASA 7.x pour prendre en charge IPsec au-dessus de TCP sur n'importe quel exemple de configuration des ports pour plus d'informations sur IPsec au-dessus de TCP.

# Incapable de passer le trafic à travers le tunnel VPN

## Problème

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

## Solution

Cette question se produit en raison du problème décrit dans l'ID de bogue Cisco CSCtb53186 (clients enregistrés seulement). Afin de résoudre ce problème, rechargez l'ASA. Référez-vous au pour en savoir plus de bogue.

Cette question pourrait également se produire quand les paquets de l'ESP sont bloqués. Afin de résoudre ce problème, modifiant le tunnel VPN.

Cette question pourrait se produire quand des données ne sont pas chiffrées, mais seulement déchiffré au-dessus du tunnel VPN suivant les indications de cette sortie :

```
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 ce qui suit :

1. Si les cryptos Listes d'accès s'assortissent avec le site distant, et les Listes d'accès ce 0 NAT sont correctes.
2. Si l'acheminement est correct et le trafic frappe en dehors de l'interface traversant à l'intérieur. La sortie témoin prouve que le déchiffrement est fait, mais le cryptage ne se produit pas.
3. Si la commande de connexion-VPN d'autorisation de sysopt a été configurée sur l'ASA. Sinon configuré, configurez cette commande parce qu'elle permet à l'ASA d'exempter le trafic encrypted/VPN de vérifier d'ACL d'interface.

# Configurer un homologue de secours pour le tunnel vpn sur la même carte de chiffrement

## Problème

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

## Solution

Configurer plusieurs homologues est équivalent à fournir 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 devrait avoir une carte de chiffrement déjà configurée en tant qu'homologue primaire. 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 :

```
ASA(config)#crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

Pour plus d'informations, référez-vous à la section Crypto map set peer dans *Référence de commande des dispositifs de sécurité Cisco version 8.0*.

# 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 **crypto map interface** dans le mode de configuration globale pour supprimer une carte de chiffrement précédemment définie paramétrée pour une interface. Utilisez la forme **no** de cette commande afin de supprimer la carte de chiffrement de l'interface.

```
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.

```
hostname(config)#crypto map map-name interface interface-name
```

## Quelques tunnels non 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 la table d'ASP. C'est un problème connu et l'ID CSCtb53186 (clients enregistrés de bogue seulement) a été classé pour aborder ce problème. Afin de résoudre ce problème, rechargent l'ASA ou améliorent le logiciel à une version dans laquelle cette bogue est réparée.

## Erreur : - %ASA-5-713904 : Group = DefaultRAGroup, IP = x.x.x.x, Client is using an unsupported Transaction Mode v2 version. Tunnel terminated.

### Problème

Le message d'erreur %ASA-5-713904: `Group = DefaultRAGroup, IP = 99.246.144.186, Client is using an unsupported Transaction Mode v2 version.` Tunnel terminated apparaît.

### Solution

La raison du message d'erreur Transaction Mode v2 est que l'ASA prend en charge seulement IKE Mode Config V6 et pas l'ancien 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 d'un grand paquet 1220 (seuil 1206)

## Problème

Le message d'erreur %ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206) error message apparaît dans les messages du journal 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 d'arrêter la compression SVC compression avec la commande svc compression none qui résout le problème.

# Erreur : The authentication-server-group none command has been deprecated

## Problème

Si vous transférez la configuration VPN de PIX/ASA qui exécute la version 7.0.x à un autre dispositif de sécurité qui exécute la version 7.2.x, vous recevez ce message d'erreur :

```
ERROR: The authentication-server-group none command has been deprecated.
The "isakmp ikev1-user-authentication none" command in the ipsec-attributes should be used
instead.
```

## Solution

La commande **authentication-serveur-group** n'est plus prise en charge dans les versions 7.2(1) et ultérieures. Cette commande a été abandonnée et déplacée dans le mode de configuration des attributs généraux du groupe de tunnels.

Référez-vous à la section isakmp ikev1-user-authentication de la référence des commandes pour plus d'informations sur cette commande.

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

## Problème

Si vous activiez QoS à l'une des extrémités du tunnel VPN, vous pourriez 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 checking
```

## Solution

Ce message apparaît normalement quand une extrémité de tunnel utilise QoS. Ceci se produit quand un paquet est détecté comme étant en panne. Vous pouvez désactiver QoS pour arrêter ceci, mais le problème peut être ignoré tant que peut le trafic peut traverser le tunnel.

## AVERTISSEMENT : crypto map entry will be incomplete

### Problème

Quand vous exécutez la commande **crypto map mymap 20 ipsec-isakmp**, vous pourriez recevoir cette erreur :

```
AVERTISSEMENT : crypto map entry will be incomplete
```

Exemple :

```
ciscoasa(config)#crypto map mymap 20 ipsec-isakmp WARNING: crypto map entry will be incomplete
```

### Solution

C'est un avertissement habituel quand vous définissez une nouvelle carte de chiffrement, rappelant que les paramètres tels que access-list (match address), transform set et peer address doivent être configurés avant que cela puisse 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 Large ICMP packet from to on interface outside

### Problème

Impossible de passer un grand paquet ping à travers le tunnel vpn. Quand nous essayons de passer de grands paquets ping, nous obtenons l'erreur %ASA-4-400024: `IDS:2151 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, le ping fonctionne très bien.

Utilisez ces commandes afin de désactiver les signatures :

ASA(config)#ip **audit signature 2151 disable**

ASA(config)#ip **audit signature 2150 disable**

## Erreur : - %PIX|ASA-4-402119 : IPSEC : Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.

## Problème

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

`Erreur : - %PIX|ASA-4-402119 : IPSEC : Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay checking.`

## Solution

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

`hostname(config)#crypto ipsec security-association replay window-size 1024`

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

# Error Message - %PIX|ASA-4-407001: Deny traffic for local-host interface_name: inside_address, license limit of number exceeded

## Problème

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

`Error Message - %PIX|ASA-4-407001: Deny traffic for local-host interface_name: inside_address, license limit of number exceeded`

## 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 en mettant à niveau la licence à un nombre plus élevé d'utilisateurs. La licence utilisateur peut inclure 50, 100 ou un nombre illimité d'utilisateurs si nécessaire.

# Error Message - %VPN_HW-4-PACKET_ERROR:

## Problème

Le message d'erreur Error Message - %VPN_HW-4-PACKET_ERROR: indique que les paquets ESP avec HMAC reçus par le routeur présentent un problème de correspondance. Cette erreur pourrait être provoquée par ces problèmes :

- 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 : Command rejected: delete crypto connection between VLAN XXXX and XXXX, first.

### Problème

Ce message d'erreur apparaît quand vous essayez d'ajouter un VLAN autorisé sur le port d'agrégation d'un commutateur : `Command rejected:` delete crypto connection between VLAN XXXX and VLAN XXXX, first..

La liaison agrégée de la périphérie WAN ne peut pas être modifiée pour autoriser des VLAN supplémentaires. C'est-à-dire que vous ne pouvez pas ajouter de VLAN dans la liaison agrégée **IPSEC VPN SPA**.

Cette commande est rejetée, parce que l'autoriser aura comme conséquence une interface VLAN de chiffrement connectée qui appartient à la liste des VLAN autorisés de l'interface, ce qui ouvre une brèche potentielle dans la sécurité d'IPSec. 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)".

## Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropping packet - Invalid Window Scale option for session x.x.x.x:27331 to 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 :

```
Error Message - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropping packet - Invalid Window Scale option for session x.x.x.x:27331 to 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 mise à l'échelle des fenêtres a été ajoutée pour permettre une transmission rapide des données sur des réseaux LFN (Long Fat Network). 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 permettre à la mise à l'échelle des fenêtres de prendre en charge les LFN, la taille de la fenêtre TCP doit être supérieure à 65 535. Ce message d'erreur peut être résolu en augmentant la taille de la fenêtre TCP pour qu'elle soit supérieure à 65 535.

## %ASA-5-305013 : Règles NAT asymétriques appariées pour en avant et inverse. Veuillez mettre à jour les écoulements de cette question

### Problème

Ce message d'erreur apparaît une fois que le tunnel VPN est soulevé :

```
%ASA-5-305013 : Règles NAT asymétriques appariées pour en avant et inverse. Veuillez mettre à
jour les écoulements de cette question
```

### Solution

Afin de résoudre ce problème quand pas sur la même interface que l'utilisation d'hôte NAT, employez l'adresse tracée au lieu de l'adresse réelle pour se connecter à l'hôte. En outre, activez la commande d'**examiner** si l'application inclut l'adresse IP.

## %PIX|ASA-5-713068 : Non routiniers reçus informent le message : notify_type

### Problème

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

```
%PIX|ASA-5-713068 : Non routiniers reçus informent le message : notify_type
```

### Solution

Ce message se produit en raison de la mauvaise configuration (c'est-à-dire, quand les stratégies ou l'ACLs ne sont pas configurés pour être identiques sur des pairs). Une fois que les stratégies et l'ACLs sont appariés le tunnel monte sans problème.

## %ASA-5-720012 : (VPN-secondaire) pour mettre à jour des données d'exécution de Basculement d'IPSec sur l'équipement de réserve (ou) %ASA-6-720012 : (VPN-unité) pour mettre à jour des données d'exécution de Basculement d'IPsec sur l'équipement de réserve

## Problème

Un de ces messages d'erreur apparaissent quand vous essayez d'améliorer l'appliance de sécurité adaptable Cisco (ASA) :

```
%ASA-5-720012 : (VPN-secondaire) pour mettre à jour des données d'exécution de Basculement
d'IPSec sur l'équipement de réserve.

%ASA-6-720012 : (VPN-unité) pour mettre à jour des données d'exécution de Basculement d'IPsec
sur l'équipement de réserve.
```

## Solution

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

Ces messages apparaissent quand le sous-système de Basculement VPN ne peut pas mettre à jour des données d'exécution liées IPsec parce que le tunnel correspondant d'IPsec a été supprimé sur l'équipement de réserve. Afin de résoudre ces derniers, émettez la commande **de réserve de wr** sur l'unité d'active.

Deux bogues ont été classées pour adresser ces comportement et mise à jour à une version de logiciel d'ASA où ces bogues sont réparées. Référez-vous au pour en savoir plus CSCtj58420 (clients enregistrés seulement) et CSCtn56517 d'id de bogue Cisco (clients enregistrés seulement).

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

## Problème

`Le %ASA-3-713063 : L'adresse de pair d'IKE non configurée pour le` message d'erreur de `0.0.0.0 de destination` apparaît et le tunnel ne monte pas.

## Solution

Ce message apparaît quand l'adresse de pair d'IKE n'est pas configurée pour un tunnel L2L. Cette erreur peut être résolue en changeant le numéro de séquence du crypto map, alors retirant et réappliquant le crypto map.

# Erreur : %ASA-3-752006 : Percez un tunnel le gestionnaire n'a pas acheminé un message KEY_ACQUIRE.

## Problème

`Le %ASA-3-752006 : Percez un tunnel le gestionnaire n'a pas acheminé un message KEY_ACQUIRE. SIG-configuration probable du crypto map ou du groupe de tunnels. »` le message d'erreur est ouvert une session Cisco ASA.

## Solution

Ce message d'erreur peut sont provoqué par par une mauvaise configuration du groupe de crypto map ou de tunnel. Assurez-vous que chacun des deux sont configurés correctement. Pour plus d'informations sur ce message d'erreur, référez-vous à l'erreur 752006.

Voici certaines des actions correctives :

- Retirez le crypto ACL (par exemple, associé à la carte dynamique).
- Retirez la configuration associée par IKEv2 inutilisée éventuelle.
- Vérifiez que le crypto ACL s'est assorti correctement.
- Retirez les entrées de liste d'accès en double éventuelles.

# Erreur : %ASA-4-402116 : IPSEC : A reçu un paquet de l'ESP (SPI= 0x99554D4E, number= 0x9E d'ordre) de XX.XX.XX.XX (user= XX.XX.XX.XX) à YY.YY.YY.YY

Dans une installation de tunnel VPN d'entre réseaux locaux, cette erreur est reçue sur une extrémité ASA :

```
Le paquet interne désencapsulé n'apparie pas la stratégie négociée à SA.

Le paquet spécifie sa destination comme 10.32.77.67, sa source comme 10.105.30.1, et son
protocole comme ICMP.

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

## Solution

Vous devez vérifier les Listes d'accès du trafic intéressant définies sur les deux extrémités du tunnel VPN. Chacun des deux devraient s'assortir en tant qu'images retournées précises.

# Pour lancer l'installateur 64-bit VA pour activer l'adaptateur virtuel dû à l'erreur 0xffffffff

## Problème

`Pour lancer l'installateur 64-bit VA pour activer l'adaptateur virtuel dû au` message de log de l'`erreur 0xffffffff` est reçu quand AnyConnect ne se connecte pas.

## Solution

Procédez comme suit pour résoudre ce problème :

1. Allez aux **configurations de Gestion de système > de communication Internet > de communication Internet** et assurez-vous qu'**arrêtez les certificats racine automatiques que la mise à jour** est désactivée.

2. S'il est désactivé, alors désactivez la pièce **administrative** entière de **modèle du** GPO assigné à l'ordinateur et au test affectés de nouveau.

Référez-vous arrêtent le pour en savoir plus automatique de mise à jour de certificats racine.

## Erreur 5 : Aucune adresse Internet n'existe pour cette entrée de connexion. Incapable d'établir la connexion VPN.

### Problème

`L'erreur 5 : Aucune adresse Internet n'existe pour cette entrée de connexion. Incapable de faire le` message d'erreur de `connexion VPN` est reçue pendant une nouvelle installation PC.

### Solution

Cette question est due à l'ID de bogue Cisco CSCso94244 (clients enregistrés seulement). Référez-vous à ce bogue pour plus d'informations.

## Le Client VPN Cisco ne travaille pas avec la carte mécanographique sur le Windows 7

### Problème

Le Client VPN Cisco ne travaille pas avec la carte mécanographique sur le Windows 7.

### Solution

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

## Message d'avertissement : La « fonctionnalité VPN peut ne pas fonctionner du tout »

### Problème

En essayant d'activer l'ISAKMP sur l'interface extérieure de l'ASA, ce message d'avertissement 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, accès à l'ASA par le ssh. HTTPS est arrêté et d'autres clients SSL sont également affectés.

### Solution

Ce problème est dû aux mémoires réquises par différents modules tels que l'enregistreur et crypto. Assurez-vous que vous n'avez pas la commande du **logging queue 0**. Il fait la file d'attente classer le positionnement à 8192 et les augmenter d'allocation de mémoire rapidement.

Dans des Plateformes telles qu'ASA5505 et ASA5510, cette allocation de mémoire tend mémoire-à mourir de faim d'autres modules (IKE et etc.). L'ID de bogue Cisco CSCtb58989 (clients enregistrés seulement) a été enregistré d'adresser un genre semblable de comportement. Afin de résoudre ceci, configurez le logging queue à une peu de valeur, telle que 512.

# Erreur de remplissage d'IPSec

## Problème

Ce message d'erreur est reçu :

```
%PIX|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

La question se produit parce que l'IPSec VPN négocie sans algorithme de hachage. Le hachage de paquet assure le contrôle d'intégrité pour le canal de l'ESP. Par conséquent, sans hacher, des paquets mal formés sont reçus non détectés par Cisco ASA et il tente de déchiffrer ces paquets. Cependant, parce que ces paquets sont mal formés, l'ASA trouve des imperfections tout en déchiffrant le paquet. Ceci entraîne les messages d'erreur de remplissage qui sont vus.

La recommandation est d'inclure un algorithme de hachage dans le jeu de transformations pour le VPN et de s'assurer que le lien entre les pairs a la malformation minimum de paquet.

# Temps de retard d'air mort aux téléphones de site distant

## Problème

Le temps de retard d'air mort est éprouvé aux téléphones de site distant. Comment résoudre ce problème ?

## Solution

Désactivez inspection maigre et de sip afin de résoudre ce problème :

```
asa(config)# no inspect sip asa(config)# no inspect skinny
```

# Le tunnel VPN obtient déconnecté après toutes les 18 heures

## Problème

Le tunnel VPN obtient déconnecté après toutes les 18 heures quoique la vie soit placée pendant 24 heures.

## Solution

La vie est le temps maximum que SA peut être utilisée pour la nouvelle saisie. La valeur que vous écrivez dans la configuration car la vie est différente de la période de rekey de SA. Par conséquent, il est nécessaire de négocier une nouvelle paire SA (ou SA dans le cas d'IPsec) avant que l'en cours expire. Le temps de rekey doit toujours être plus petit que la vie afin de tenir compte de plusieurs tentatives au cas où la première tentative de rekey échouerait. Les RFC ne spécifient pas comment calculer le temps de rekey. Ceci est laissé à la discrétion des responsables de l'implémentation. Par conséquent, le temps variera selon la plate-forme utilisée, qui version de logiciel, etc.

Quelques réalisations peuvent employer un facteur aléatoire pour calculer le temporisateur de rekey. Par exemple, si l'ASA initie le tunnel, puis il est normal qu'il réintroduira à 64800 secondes = 75% de 86400. Si les initiés de routeur, alors l'ASA peuvent attendre plus long de donner au pair plus d'heure d'initier le rekey. Ainsi, il est normal que la session VPN obtienne a déconnecté toutes les 18 heures pour utiliser une autre clé pour la négociation VPN. Ceci ne doit poser aucune baisse ou problème VPN.

# La circulation n'est pas mise à jour après que le RÉSEAU LOCAL au tunnel de RÉSEAU LOCAL soit renégocié

## Problème

La circulation n'est pas mise à jour après que le RÉSEAU LOCAL au tunnel de RÉSEAU LOCAL soit renégocié.

## Solution

L'ASA surveille chaque connexion qui la traverse et met à jour une entrée dans sa table d'état selon la caractéristique 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). Pour le RÉSEAU LOCAL aux connexions VPN de RÉSEAU LOCAL, il met à jour les deux circulations différentes. On 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 le VPN est terminé, les détails d'écoulement pour cette SA particulière sont supprimés. Cependant, l'entrée de table d'état mise à jour par l'ASA pour cette connexion TCP devient éventée en raison d'aucune activité, qui entrave le téléchargement. Ceci signifie que l'ASA retiendra toujours la connexion TCP pour ce flux particulier tandis que l'application utilisateur se termine. Cependant, les connexions TCP deviendront bête perdue et par la suite délai d'attente après que le compteur de durée d'inactivité de TCP expire.

Ce problème a été résolu en introduisant une caractéristique appelée les écoulements percés un tunnel IPSec de Persistent. Une nouvelle commande, des conserve-VPN-écoulements de connexion de sysopt, a été intégrée dans Cisco ASA afin de retenir les informations de table d'état à la renégociation du tunnel VPN. Par défaut, cette commande est désactivée. En activant ceci, Cisco ASA mettra à jour les informations de table d'état de TCP quand le L2L VPN récupère de l'interruption et rétablit le tunnel.

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

# pour la crypto fonctionnalité

## Problème

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

```
Erreur : 20 mars 10:51:29 : %CERM-4-TX_BW_LIMIT : La limite maximum de bande passante de Tx de
85000 Kbps a atteint pour la crypto fonctionnalité avec le permis de module de la technologie
securityk9.
```

## Solution

C'est un problème connu qui se produit en raison des instructions strictes émises par le gouvernement des États-Unis. Selon ceci, le permis securityk9 peut seulement permettre un cryptage de charge utile jusqu'aux débits près de 90Mbps et limiter le nombre de sessions chiffrées tunnels/TLS au périphérique. Pour plus d'informations sur les cryptos restrictions à l'exportation, référez-vous à l'autorisation sec et HSEC d'ISR G2 de Cisco.

En cas de périphériques de Cisco, il est dérivé pour être moins que le trafic unidirectionnel 85Mbps dans ou hors du routeur d'ISR G2, avec un total bidirectionnel de 170 Mbits/s. Cette condition requise s'applique pour les 3900 Plateformes d'ISR G2 de Cisco 1900, 2900, et. Cette commande vous aide en vue ces limites :

```
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----
```

Il y a une bogue classée pour adresser ce comportement. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCtu24534 (clients enregistrés seulement).

Afin d'éviter ce problème, vous devez acheter un permis HSECK9. Un permis de caractéristique de "hseck9" fournit à la fonctionnalité améliorée de cryptage de charge utile le tunnel VPN accru compte et les sessions de voix sécurisée. Pour plus d'informations sur le routeur ISR de Cisco autorisant, référez-vous au lancement de logiciel.

# Problème : Le trafic sortant de cryptage dans un tunnel d'IPsec peut échouer, même si le trafic d'arrivée de déchiffrement fonctionne.

## Solution

Cette question a été observée sur une connexion d'IPsec après de plusieurs rekeys, mais l'état de déclencheur n'est pas clair. La présence de cette question peut être établie en vérifiant la sortie de la commande de **baisse d'asp d'exposition** et en la vérifiant que le compteur expiré de contexte VPN augmente pour chaque paquet sortant envoyé. Référez-vous au pour en savoir plus de l'ID de bogue Cisco CSCtd36473 (clients enregistrés seulement).

# 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_EXCH apparaît dans la sortie des commandes **show crypto isakmp sa** et **debug**. La raison peut être la non correspondance de stratégies isakmp ou le blocage du port UDP 500.

### 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

- Problème avec PIX/ASA 7.0 : MSS dépassée - Les clients HTTP ne peuvent pas accéder à certains sites Web
- PIX/ASA 7.x et IOS : Fragmentation VPN
- Dispositifs de sécurité de la gamme Cisco ASA 5500
- Dispositifs de sécurité de la gamme Cisco PIX 500
- Négociation IPSec/Protocoles IKE
- Concentrateurs VPN de la gamme Cisco 3000
- Support et documentation techniques - Cisco Systems