PIX/ASA 7.x et IOS : Fragmentation VPN

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Diagramme du réseau
Produits connexes
Conventions
Informations générales
Problèmes avec la fragmentation
Tâche principale
Découvrir la fragmentation
Solutions aux problèmes de fragmentation
Vérifiez
Dépannez
Erreur de chiffrement VPN
Problèmes RDP et Citrix
Informations connexes

Introduction

Ce document vous guide tout au long des étapes nécessaires pour remédier aux problèmes qui peuvent se poser avec la fragmentation d'un paquet. Un exemple des problèmes de fragmentation est la capacité d'exécuter une commande ping sur une ressource réseau mais l'incapacité de se connecter à cette même ressource avec une application spécifique, telle que la messagerie électronique ou les bases de données.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

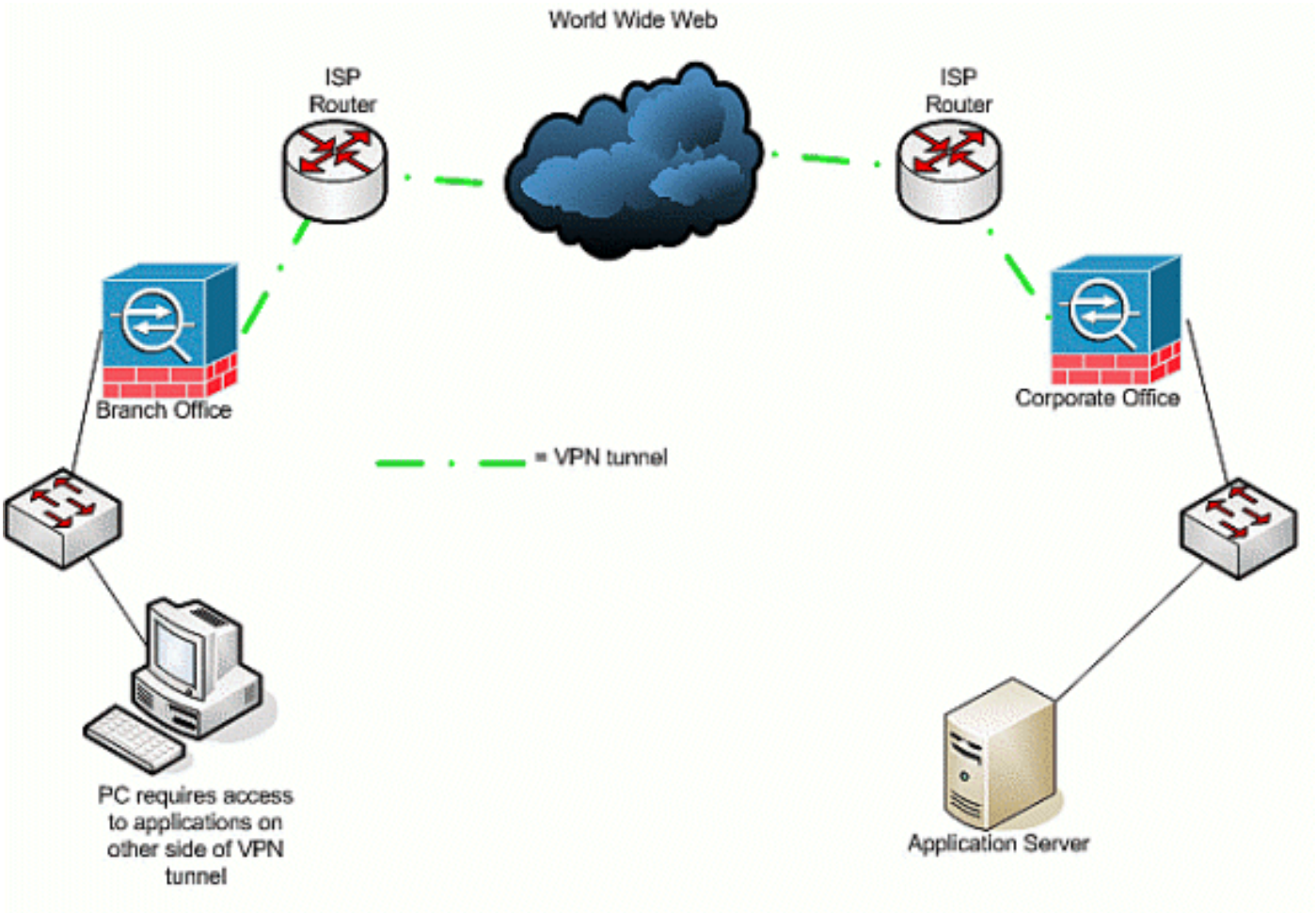
- Connectivité entre les homologues VPN

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Produits connexes

Cette configuration peut également être utilisée avec les versions de matériel et de logiciel suivantes :

- Routeurs IOS
- Périphériques de sécurité PIX/ASA

Conventions

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

Informations générales

IP prend en charge une longueur maximale de 65 536 octets pour un paquet IP, mais la plupart des protocoles de couche de liaison de données prennent en charge une longueur beaucoup plus petite, appelée Unité de transmission maximale (MTU). Selon le MTU pris en charge, il peut être nécessaire de diviser (fragmenter) un paquet IP pour le transmettre à travers un type de support particulier de couche de liaison de données. La destination doit alors réassembler les fragments

dans le paquet IP initial et complet.

Protocol	Additional Bytes
ESP (encryption and hash)	56
AH	24+
GRE	24
NAT-T/IPsec over UDP (UDP part)	8
IPsec over TCP (TCP part)	20
L2TP	12
PPTP	48
Outer IP header in IPsec tunnel mode or PPTP/L2TP	20
PPPoE	8

Quand vous employez un VPN pour protéger des données entre deux homologues VPN, la surcharge supplémentaire est ajoutée aux données originales, ce qui peut nécessiter que cette fragmentation se produise. Ce tableau répertorie les champs qui doivent potentiellement être ajoutés aux données protégées afin de prendre en charge une connexion VPN. Notez que plusieurs protocoles peuvent être nécessaires, ce qui augmente la taille du paquet original. Par exemple, si vous utilisez une connexion L2L DMVPN IPSEC entre deux routeurs Cisco, où vous avez mis en application un tunnel GRE, vous avez besoin de cette surcharge supplémentaire : ESP, GRE et l'en-tête IP externe. Si vous avez une connexion de client logiciel IPSec à une passerelle VPN quand le trafic passe par un périphérique d'adresse, vous avez besoin de cette surcharge supplémentaire pour NAT-T (Network Address Translation- Traversal), aussi bien que de l'en-tête IP externe pour la connexion de mode tunnel.

Problèmes avec la fragmentation

Quand la source envoie un paquet à une destination, elle place une valeur dans le champ des indicateurs de contrôle des en-têtes IP qui affecte la fragmentation du paquet par des périphériques intermédiaires. L'indicateur de contrôle est long de trois bits, mais seuls les deux premiers sont utilisés dans la fragmentation. Si le deuxième bit est défini à 0, on permet au paquet d'être fragmenté ; si le deuxième bit est défini à 1, on ne permet pas au paquet d'être fragmenté. Le deuxième bit est généralement appelé le bit *ne pas fragmenter* (DF). Le troisième bit spécifie quand la fragmentation se produit, si ce paquet fragmenté est le dernier fragment (défini à 0), ou s'il y a plus de fragments (définis à 1) qui composent le paquet.

Il y a quatre zones qui peuvent créer des problèmes quand la fragmentation est requise :

- La surcharge supplémentaire dans les cycles CPU et la mémoire est requise par les deux périphériques qui exécutent la fragmentation et le réassemblage.
- Si un fragment est abandonné sur le chemin de la destination, le paquet ne peut pas être réassemblé et le paquet entier doit être fragmenté et envoyé de nouveau. Ceci crée des problèmes de débit supplémentaires, particulièrement dans les situations où le trafic en

question est limité en débit, et la source envoie le trafic au-dessus de la limite permise.
- Le filtrage des paquets et les pare-feu avec état peuvent avoir des difficultés pour traiter les fragments. Quand la fragmentation se produit, le premier fragment contient un en-tête IP externe, l'en-tête interne, tel que TCP, UDP, ESP et d'autres, et une partie de la charge utile. Les fragments ultérieurs du paquet original contractent un en-tête IP externe et la suite de la charge utile. Le problème avec ce processus est que certains pare-feu doivent consulter les informations d'en-tête interne dans chaque paquet afin de prendre des décisions de filtrage intelligentes ; si ces informations sont manquantes, ils peuvent par distraction abandonner tous les fragments, excepté le premier.
- La source dans l'en-tête IP du paquet peut définir le troisième bit de contrôle *ne pas fragmenter*, ce qui signifie que, si un périphérique intermédiaire reçoit le paquet et doit le fragmenter, le périphérique intermédiaire ne peut pas le fragmenter. Au lieu de cela, le périphérique intermédiaire abandonne le paquet.

Tâche principale

Découvrir la fragmentation

La plupart des réseaux utilisent Ethernet, avec une valeur de MTU par défaut de 1 500 octets, qui est typiquement utilisée pour des paquets IP. Afin de découvrir si la fragmentation se produit ou est nécessaire mais ne peut pas être faite (le bit DF est défini), ouvrez d'abord votre session VPN. Vous pouvez ensuite employer n'importe laquelle de ces quatre procédures pour détecter la fragmentation.

1. Exécutez une commande ping sur un périphérique situé à l'autre extrémité. C'est dans l'hypothèse où l'exécution d'une commande ping est autorisée à travers le tunnel. Si l'opération réussit, essayez d'accéder à une application à travers le même périphérique ; par exemple, si un serveur Microsoft de messagerie électronique ou Bureau à distance est dans le tunnel, ouvrez Outlook et essayez de télécharger votre messagerie électronique, ou essayez d'établir une connexion Remote Desktop au serveur. Si ceci ne fonctionne pas, et que vous avez la résolution de noms correcte, il est très probable que la fragmentation est le problème.
2. Àpartir d'un périphérique Windows, utilisez ceci : C:\> **ping -f -l packet_size_in_bytes destination_IP_address**.L'option **-f** est utilisée pour spécifier que le paquet ne peut pas être fragmenté. L'option **-l** est utilisée pour spécifier la longueur du paquet. Essayez d'abord ceci avec une taille de paquet de 1 500. Par exemple, exécutez la commande ping **-f -l 1500 192.168.100**. Si la fragmentation est requise mais ne peut pas être effectuée, vous recevez un message de ce type : *Des paquets doivent être fragmentés mais DF est défini*.
3. Sur des routeurs Cisco, exécutez la commande **debug ip icmp** et utilisez la **commande ping étendue**. Si vous voyez le message *ICMP: dst (x.x.x.x) fragmentation needed and DF set, unreachable sent to y.y.y.y* où x.x.x.x est un périphérique de destination et y.y.y.y est votre routeur, un périphérique intermédiaire vous indique que la fragmentation est nécessaire, mais parce que vous avez défini le bit DF dans la demande d'écho, un périphérique intermédiaire ne peut pas le fragmenter afin de le transférer au prochain saut. Dans ce cas, diminuez graduellement la taille du MTU des pings jusqu'à ce que vous en trouviez un qui fonctionne.
4. Sur les dispositifs de sécurité Cisco, utilisez un filtre de capture.ciscoasa(config)#access-list

outside_test permit tcp any host 172.22.1.1 eq 80**Note**: Quand vous laissez la source sous la forme *any*, cela permet à l'administrateur de contrôler toutes les traductions d'adresses réseau (NAT).ciscoasa(config)#access-list outside_test permit tcp host 172.22.1.1 eq 80 any**Note**: Quand vous inversez les informations de source et de destination, cela permet de capturer le trafic de retour.`ciscoasa(config)# capture outside_interface access-list outside_test interface outside`L'utilisateur doit lancer une nouvelle session avec l'application X. Une fois que l'utilisateur a lancé une nouvelle session de l'application X, l'administrateur ASA doit émettre la commande **show capture outside_interface**.

Solutions aux problèmes de fragmentation

Il existe plusieurs moyens de résoudre les problèmes de fragmentation. Ceux-ci sont discutés dans cette section.

Méthode 1 : Paramètre statique de MTU

Le paramètre statique de MTU peut résoudre les problèmes de fragmentation.

1. **Modification de MTU sur le routeur :**Notez que si vous définissez manuellement le MTU sur le périphérique, il indique au périphérique, qui agit en tant que passerelle VPN, de fragmenter les paquets reçus avant de les protéger et de les envoyer à travers le tunnel. Cela est préférable au fait d'avoir le routeur qui protège le trafic, puis le fragmente, mais le périphérique le fragmente.**Avertissement :** Si vous modifiez la taille du MTU sur n'importe quelle interface de périphérique, tous les tunnels terminés sur cette interface sont démolis, puis reconstruits.Sur les routeurs Cisco, employez la commande **ip mtu** pour régler la taille du MTU sur l'interface où le VPN est terminé :
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **Modification de MTU sur ASA/PIX :**Sur les périphériques ASA/PIX, employez la commande **mtu** pour régler la taille du MTU dans le mode de configuration globale. Par défaut, le MTU est défini à 1500. Par exemple, si vous aviez une interface sur votre dispositif de sécurité nommée *Outside (où le VPN est terminé)* et que vous avez déterminé (par les mesures listées dans la section Découvrir la fragmentation) que vous vouliez utiliser 1380 comme taille de fragment, utilisez cette commande :
```
security appliance (config)# mtu Outside 1380
```

Méthode 2 : Taille maximale de segment TCP

La taille maximale de segment TCP peut résoudre les problèmes de fragmentation.

Note: Cette fonctionnalité fonctionne seulement avec TCP ; d'autres protocoles IP doivent employer une autre solution pour résoudre les problèmes de fragmentation IP. Même si vous définissez ip mtu sur le routeur, cela n'affecte pas ce que les deux hôtes d'extrémité négocient dans la connexion en trois temps TCP avec MSS TCP.

1. **Modification de MSS sur le routeur :**La fragmentation se produit avec le trafic TCP parce que le trafic TCP est normalement utilisé pour transporter un grand nombre de données. TCP

prend en charge une fonctionnalité appelée MSS (taille maximale de segment) TCP qui permet aux deux périphériques de négocier une taille appropriée pour le trafic TCP. La valeur de MSS est configurée statiquement sur chaque périphérique et représente la taille du tampon à utiliser pour un paquet prévu. Quand deux périphériques établissent des connexions TCP, ils comparent la valeur de MSS locale à la valeur de MTU locale dans la connexion en trois temps ; la valeur la plus basse est envoyée à l'homologue distant. Les deux homologues utilisent alors la valeur la plus basse des deux valeurs échangées. Afin de configurer cette fonctionnalité, faites ceci :Sur les routeurs Cisco, utilisez la commande **tcp adjust-mss** sur l'interface sur laquelle le VPN est terminé.

```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip tcp adjust-mss MSS_Size_in_bytes
```

2. **Modification de MSS sur ASA/PIX :**Afin de vous assurer que la taille maximale de segment TCP ne dépasse pas la valeur que vous avez définie et que le maximum n'est pas inférieur à une taille spécifiée, utilisez la commande **sysopt connection** dans le mode de configuration globale. Afin de restaurer la configuration par défaut, utilisez la forme no de cette commande. La valeur maximale par défaut est de 1 380 octets. La fonctionnalité minimum est désactivée par défaut (définie à 0).Afin de modifier la limite MSS maximum par défaut, faites ceci :

   ```
   security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
   ```

   Note: Si vous avez défini une taille maximale supérieure à 1380, les paquets peuvent devenir fragmentés, selon la taille du MTU (qui est 1500 par défaut). Un grand nombre de fragments peut affecter les performances du dispositif de sécurité quand il utilise la fonctionnalité Frag Guard. Si vous avez défini la taille minimale, elle empêche le serveur TCP d'envoyer beaucoup de petits paquets de données TCP au client et d'affecter les performances du serveur et du réseau.Afin de modifier la limite MSS minimum, faites ceci :

   ```
   security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
   ```

   security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes**Note**: Consultez la section Configuration MPF pour autoriser les paquets qui dépassent MSS du document Problème avec PIX/ASA 7.X : MSS dépassé - Les clients HTTP ne peuvent pas accéder à certains sites Web pour plus d'informations afin de permettre une autre méthode pour les paquets MSS dépassés.

Méthode 3 : Découverte de MTU de chemin (PMTUD)

PMTUD peut résoudre les problèmes de fragmentation.

Le problème principal avec MSS TCP est que l'administrateur doit savoir quelle valeur configurer sur votre routeur pour empêcher l'occurrence de la fragmentation. Ceci peut être un problème si plus d'un chemin existe entre vous et l'emplacement VPN distant ou, quand vous faites votre requête initiale, vous constatez que le deuxième ou troisième plus petit MTU, au lieu du plus petit, est basé sur la décision de routage utilisée dans votre requête initiale. Avec PMTUD, vous pouvez déterminer une valeur de MTU pour des paquets IP qui évite la fragmentation. Si des messages ICMP sont bloqués par un routeur, le MTU de chemin est cassé et les paquets avec le bit DF défini sont ignorés. Utilisez la commande **set ip df** pour effacer le bit DF et permettre au paquet d'être fragmenté et envoyé. La fragmentation peut ralentir la vitesse de la transmission de paquets sur le réseau, mais des listes d'accès peuvent être utilisées pour limiter le nombre de paquets sur lesquels le bit DF est effacé.

1. Trois problèmes peuvent entraîner le non-fonctionnement de PMTUD :Un routeur intermédiaire peut abandonner le paquet et ne pas répondre avec un message ICMP. Ce n'est pas très commun sur Internet, mais peut l'être à l'intérieur d'un réseau où des routeurs sont configurés pour ne pas répondre avec des messages d'inaccessibilité d'ICMP.Un routeur intermédiaire peut répondre avec un message d'inaccessibilité d'ICMP mais, sur le flux de retour, un pare-feu bloque ce message. C'est une occurrence plus commune.Le message d'inaccessibilité d'ICMP revient à la source, mais la source ignore le message de fragmentation. C'est le plus rare des trois problèmes.Si vous rencontrez le premier problème, vous pouvez effacer le bit DF dans l'en-tête IP que la source a placé là ou régler manuellement la taille de MSS TCP. Afin d'effacer le bit DF, un routeur intermédiaire doit changer la valeur de 1 à 0. normalement que ceci est fait par un routeur dans votre réseau avant que le paquet parte du réseau. C'est une configuration simple de code qui fait ceci sur un routeur basé sur IOS :
```
Router (config) # access-list ACL_# permit tcp any any
Router (config) # route-map route_map_name permit seq#
Router (config-route-map) # match ip address ACL_#
Router (config-route-map) # set ip df 0
Router (config-route-map) # exit
Router (config) # interface type [slot#/]port #
Router (config-if) # ip policy router-map route_map_name
```

2. PMTUD et tunnels GREPar défaut, un routeur n'effectue pas PMTUD sur les paquets de tunnel GRE qu'il génère lui-même. Afin d'activer PMTUD sur des interfaces de tunnel GRE et de faire en sorte que le routeur participe au processus de réglage MTU pour les unités source/de destination pour le trafic qui traverse le tunnel, utilisez cette configuration :Router (config) # interface tunnel tunnel_#Router (config-if) # tunnel path-mtu-discoveryLa commande tunnel path-mtu-discovery active PMTUD pour l'interface de tunnel GRE d'un routeur. Le paramètre age-timer facultatif spécifie le nombre de minutes après quoi l'interface du tunnel réinitialise la taille de MTU maximale détectée, moins 24 octets pour l'en-tête GRE. Si vous spécifiez *infinite* pour le compteur, le compteur n'est pas utilisé. Le paramètre min-mtu spécifie le nombre minimal d'octets qui comporte la valeur de MTU.
3. PIX/ASA 7.x - Clear Don't Fragment (DF) ou gestion de grands fichiers ou paquets.Vous ne pouvez toujours pas accéder correctement à Internet, à de grands fichiers ou à des applications par le tunnel parce que le message d'erreur lié à la taille suivant s'affiche :

   ```
   PMTU-D packet 1440 bytes greater than effective mtu 1434,
    dest_addr=10.70.25.1, src_addr=10.10.97.55, prot=TCP
   ```

   Afin de résoudre ceci, assurez-vous d'effacer le bit DF de l'interface externe du périphérique. Configurez la stratégie de bit DF pour les paquets IPSec avec la commande crypto ipsec df-bit dans le mode de configuration globale.

   ```
   pix(config)# crypto ipsec df-bit clear-df outside
   ```

   Le bit DF avec la configuration de tunnels IPSec vous permet de spécifier si le dispositif de sécurité peut effacer, définir ou copier le bit Don't Fragment (DF) de l'en-tête encapsulé. Le bit DF dans l'en-tête IP détermine si un périphérique est autorisé à fragmenter un paquet.Utilisez la commande crypto ipsec df-bit dans le mode de configuration globale afin de configurer le dispositif de sécurité pour spécifier le bit DF dans un en-tête encapsulé.Quand vous encapsulez le trafic IPSec de mode tunnel, utilisez le paramètre clear-df pour le bit DF. Ce paramètre permet au périphérique d'envoyer des paquets plus

grands que la taille du MTU disponible. Ce paramètre est également approprié si vous ne connaissez pas la taille du MTU disponible.

Note: Si vous rencontrez toujours des problèmes de fragmentation et des paquets abandonnés, vous pouvez à titre facultatif régler manuellement la taille du MTU avec la commande **ip mtu tunnel interface**. Dans ce cas, le routeur fragmente le paquet avant de le protéger. Cette commande peut être utilisée en même temps que PMTUD et/ou MSS TCP.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Dépannez

Erreur de chiffrement VPN

Supposez que le tunnel IPSec est établi entre le routeur et PIX. Si vous voyez des messages d'erreur de chiffrement indiquant que des paquets sont abandonnés, complétez ces étapes pour résoudre le problème :

1. Effectuez un tracé de l'analyseur de réseau du client vers le côté serveur pour découvrir quel est le meilleur MTU à utiliser.Vous pouvez également utiliser le test ping :

   ```
   ping  -l   1400  192.168.1.1 -f
   ```

   192.168.1.1 est l'adresse IP de l'ordinateur distant.
2. Continuez à réduire la valeur de 1400 par 20 jusqu'à ce qu'il y ait une réponse.**Note**: La valeur magique, qui fonctionne dans la plupart des instances, est 1300.
3. Après que la taille maximale de segment appropriée a été atteinte, réglez-la convenablement pour les périphériques en service :Sur le pare-feu PIX :

   ```
   sysopt connection tcpmss 1300
   ```

   Sur le routeur :

   ```
   ip tcp adjust-mss 1300
   ```

Problèmes RDP et Citrix

Problème :

Vous pouvez exécuter une commande ping entre les réseaux VPN, mais des connexions du protocole RDP (Remote Desktop Protocol) et Citrix ne peuvent pas être établies à travers le tunnel.

Solution :

Le problème peut être la taille du MTU sur le PC derrière PIX/ASA. Affectez la taille 1300 au MTU pour l'ordinateur client et tentez d'établir la connexion Citrix à travers le tunnel VPN.

Informations connexes

- Résoudre les problèmes de fragmentation IP, MTU, MSS et PMTUD avec GRE et IPSEC
- Problème avec PIX/ASA 7.0 : MSS dépassée - Les clients HTTP ne peuvent pas accéder à certains sites Web
- Solutions de dépannage les plus fréquentes concernant un VPN IPsec LAN à LAN et d'accès à distance
- Pourquoi ne puis-je pas surfer sur Internet lorsque j'utilise un tunnel GRE ?
- Support et documentation techniques - Cisco Systems