PIX/ASA 7.x en IOS: VPN-fragmentatie

Inhoud

Inleiding

Dit document loopt u door de stappen die nodig zijn om problemen te verminderen die met de fragmentatie van een pakket kunnen voorkomen. Een voorbeeld van een fragmentatieprobleem is de mogelijkheid om een aangesloten bron te pingelen maar de onmogelijkheid om met hetzelfde middel te verbinden met een specifieke toepassing, zoals e-mail of databases.

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

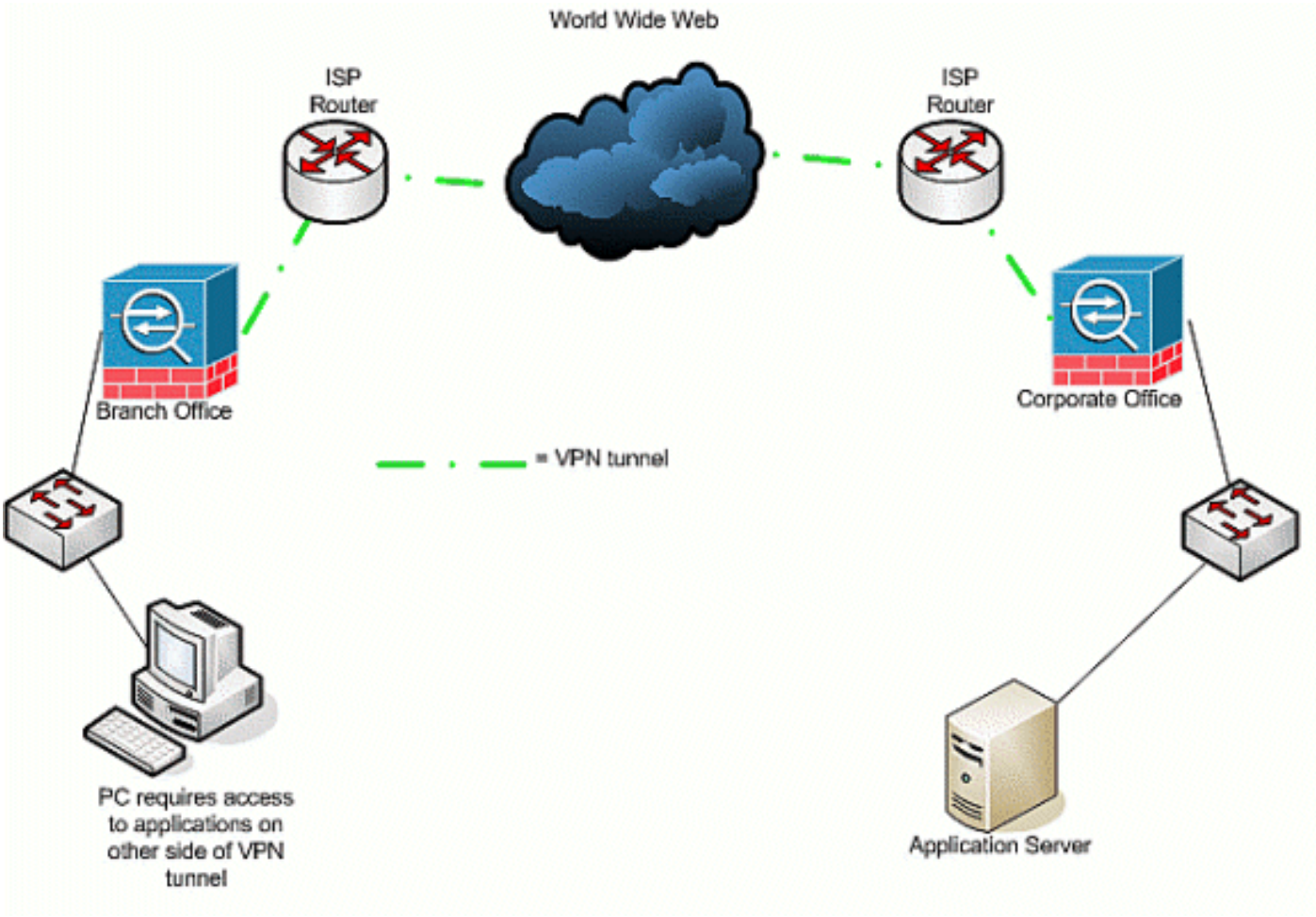
- Connectiviteit tussen VPN-peers

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Verwante producten

Deze configuratie kan ook worden gebruikt in combinatie met deze hardware- en softwareversies:

- IOS-routers
- PIX-/ASA-beveiligingsapparaten

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

IP ondersteunt een maximale lengte van 65.536 bytes voor een IP-pakket, maar de meeste data-link Layer protocols ondersteunen een veel kleinere lengte, genaamd een maximum transmissie-eenheid (MTU). Gebaseerd op de ondersteunde MTU, kan het nodig zijn om een IP-pakket te splitsen (fragment) om het over een bepaald media-type van de datalink-laag te verzenden. De bestemming moet de fragmenten vervolgens opnieuw in het oorspronkelijke, volledige IP-pakket monteren.

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

Wanneer u een VPN gebruikt om gegevens tussen twee VPN-peers te beschermen, wordt extra overhead toegevoegd aan de oorspronkelijke gegevens, wat fragmentatie kan vereisen. Deze tabel maakt een lijst van velden die mogelijk aan de beschermde gegevens moeten worden toegevoegd om een VPN-verbinding te ondersteunen. Merk op dat er meerdere protocollen nodig kunnen zijn, waardoor de grootte van het oorspronkelijke pakje wordt vergroot. Als u bijvoorbeeld een L2L DMVPN IPSEC-verbinding tussen twee Cisco routers gebruikt, waar u een GRE-tunnel hebt geïmplementeerd, hebt u deze extra overhead nodig: ESP, GRE, en de buitenste IP-header. Als u een IPSec software client verbinding hebt naar een VPN-gateway wanneer het verkeer door een adresapparaat gaat, hebt u deze extra overhead nodig voor Network Address Translation-Traversal (NAT-T), evenals de buitenste IP header voor de verbinding met de tunnelmodus.

Problemen met fragmentatie

Wanneer de bron een pakje naar een bestemming stuurt, plaatst het een waarde in het veld Besturingsvlaggen van de IP-headers die fragmentatie van het pakje door intermediaire apparaten beïnvloeden. De control flag is drie bits lang, maar alleen de eerste twee worden gebruikt in fragmentatie. Als het tweede bit op 0 is ingesteld, mag het pakje gefragmenteerd zijn; als het pakket op 1 is ingesteld , mag het niet worden gefragmenteerd . Het tweede bit wordt algemeen het DF-bit (*don*-bit) genoemd. Het derde bit specificeert wanneer de fragmentatie zich voordoet, of dit gefragmenteerde pakket het laatste fragment is (ingesteld op 0) of als er meer fragmenten zijn (ingesteld op 1) die het pakket vormen.

Er zijn vier gebieden die problemen kunnen veroorzaken wanneer fragmentatie nodig is:

- Aanvullende overhead in CPU-cycli en -geheugen wordt vereist door de twee apparaten die fragmentatie en hermontage uitvoeren.
- Als één fragment op de route naar de bestemming is gevallen, kan het pakje niet opnieuw worden geassembleerd en moet het hele pakket gefragmenteerd en opnieuw worden verzonden. Dit creëert extra doorvoerproblemen, vooral in situaties waarin het verkeer in kwestie aan een snelheidsbeperking onderhevig is en de bron het verkeer verstuurt boven de toegestane limiet.

- Packet-filtering en stateful firewalls kunnen de verwerking van de fragmenten bemoeilijken. Wanneer fragmentatie optreedt, bevat het eerste fragment een buitenste IP-header, de binnenste header, zoals TCP, UDP, ESP en andere, en een deel van de lading. Latere fragmenten van het oorspronkelijke pakketcontract, een externe IP-header en de voortzetting van de lading. Het probleem met dit proces is dat bepaalde firewalls de binnenveldinformatie in elk pakje moeten zien om intelligente filterbeslissingen te kunnen nemen; als deze informatie ontbreekt , kunnen zij per ongeluk alle fragmenten laten vallen , behalve de eerste .
- De bron in de IP-header van het pakket kan het derde controlebit instellen om *geen fragment* te *bevatten*, wat betekent dat, als een tussenpersoon het pakket ontvangt en het moet fragmenteren, het tussenstation het niet kan fragmenteren. In plaats daarvan laat het tussenstation het pakje vallen.

Hoofdtaak

Fragmentation ontdekken

De meeste netwerken gebruiken Ethernet, met een standaard MTU waarde van 1.500 bytes, die normaal gebruikt wordt voor IP-pakketten. Om te weten te komen of de fragmentatie optreedt of nodig is maar niet kan worden gedaan (het DF-bit is ingesteld), breng eerst uw VPN-sessie omhoog. Dan kun je elk van deze vier procedures gebruiken om fragmentatie te ontdekken.

1. Een apparaat tegen het andere uiteinde draaien. Dit is in de veronderstelling dat pingelen is toegestaan door de tunnel. Als dit succesvol is, probeer dan toegang te krijgen tot een toepassing over hetzelfde apparaat; Als een Microsoft E-mail- of Remote Desktop-server bijvoorbeeld in de tunnel staat, opent u Outlook en probeert u uw E-mail te downloaden of probeert u Remote-desktop naar de server te brengen. Als dit niet werkt, en je hebt de juiste naamresolutie, is er een goede kans dat fragmentatie het probleem is.
2. Gebruik dit programma vanuit een Windows-apparaat: C:\> **ping-f -l Packet_size_in_bytes target_IP_adres**.De **-f** optie wordt gebruikt om aan te geven dat het pakket niet kan worden gefragmenteerd. De optie **-l** wordt gebruikt om de lengte van het pakket op te geven. Probeer dit eerst met een pakketgrootte van 1.500. Bijvoorbeeld, ping**-f-l 1500 192.168.100**. Als fragmentatie vereist is maar niet kan worden uitgevoerd, ontvangt u een bericht zoals dit: *Pakketten moeten gefragmenteerd zijn maar DF-instelling*.
3. Op Cisco routers voert u de **debug ip-**opdracht **uit** en gebruikt u de **uitgebreide** ping-opdracht. Als u *fragmentatie van ICMP:dst (x.x.x.x) en DF nodig* ziet*, onbereikbaar naar y.y.y.y*, waar x.x.x.x een doelapparaat is en y.y.y.y.y uw router, vertelt een tussenapparaat u dat fragmentatie nodig is, maar omdat u het bit in het echo-verzoek instelt, kan een tussenapparaat niet in fragmenteren om het naar de volgende hop te sturen. In dit geval, verlaag geleidelijk de MTU grootte van de pings tot je er een vindt die werkt.
4. Gebruik op Cisco security applicaties een opnamefilter.ciscoasa (configuratie)#`access-list beyond_test vergunning tcp elke host 172.22.1.1 eq 80`**Opmerking:** Wanneer u de bron als *enige* verlaat, kan de beheerder alle netwerkadresvertalingen (NAT) controleren.ciscoasa (configuratie)#`access-list` buiten`_test, tcp host 172.22.1.1 eq 80`**Opmerking:** wanneer u de bron- en doelinformatie omgekeerd doet, kan er retourverkeer worden opgenomen.`CiscoCATALYA (COMPONENTEN)# opname buiten_interface toegang-list buiten_test interface buiten_interface`De gebruiker moet een nieuwe sessie met toepassing X starten. Nadat de gebruiker een nieuwe toepassing X sessie is gestart, moet de ASA beheerder de

show opname externe_interface opdracht uitgeven.

Oplossingen voor fragmentatieproblemen

Er zijn verschillende manieren om problemen met fragmentatie op te lossen. Deze worden in deze paragraaf besproken.

Methode 1: Statische MTU-instelling

De statische MTU-instelling kan problemen met fragmentatie oplossen.

1. **MTU wijziging op de router:**Merk op dat als u handmatig de MTU op het apparaat instelt, het apparaat, dat als gateway van VPN fungeert, vertelt om ontvangen pakketten te fragmenteren voordat het bescherming biedt en hen over de tunnel verstopt. Dit is beter dan de router het verkeer te beschermen en het vervolgens te fragmenteren, maar het apparaat fragmenteert het.**Waarschuwing:** Als u de grootte van de MTU op een willekeurige apparaatinterface wijzigt, wordt alle op die interface afgesloten tunnels afgebroken en opnieuw opgebouwd.Op Cisco routers kunt u de **ip-**knop gebruiken om de grootte van de MTU aan te passen op de interface waar VPN wordt beëindigd:
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **MTU-wijziging op de ASA/PIX:**Op ASA/PIX-apparaten, gebruik de mucommand om de grootte van MTU aan te passen in de globale configuratiewijze. Standaard wordt de MTU ingesteld op 1500. Als u bijvoorbeeld een interface op uw security apparaat had die *Buiten* genoemd werd *(waar VPN wordt beëindigd)* en u deze opdracht (via de maatregelen in het gedeelte Discover Fragmentation) wilt gebruiken om 1380 als de fragmentatiegrootte te gebruiken, gebruikt u dan deze opdracht:
```
security appliance (config)# mtu Outside 1380
```

Methode 2: TCP maximale segmentgrootte

De TCP maximum segmentgrootte kan problemen met fragmentatie oplossen.

Opmerking: deze optie werkt alleen met TCP; Andere IP protocollen moeten een andere oplossing gebruiken om IP-fragmentatieproblemen op te lossen. Zelfs als u de ip mtu op de router instelt, beïnvloedt het niet wat de twee eindgastheren binnen de TCP 3-weg handdruk met TCP MSS onderhandelen.

1. **MSS-verandering op de router:**Fragmentation treedt op met TCP-verkeer omdat TCP-verkeer normaal wordt gebruikt om grote hoeveelheden gegevens te transporteren. TCP ondersteunt een eigenschap die TCP maximum segmentgrootte (MSS) wordt genoemd die de twee apparaten toestaat om een geschikte grootte voor TCP verkeer te onderhandelen. De MSS-waarde wordt op elk apparaat statistisch ingesteld en vertegenwoordigt de buffergrootte om voor een verwacht pakket te gebruiken. Wanneer twee apparaten TCP verbindingen instellen vergelijken zij de lokale MSS waarde met de lokale MTU waarde binnen de drierichtingshanddruk; welke lager is, wordt naar de externe peer verzonden. De twee peers gebruiken vervolgens de laagste van de twee uitgewisselde waarden. Dit doet u

zo om deze functie te configureren:Op Cisco routers gebruikt u de opdracht **TCP-aanpassen-mss** op de interface waarop VPN wordt beëindigd.

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

2. **MSS-wijziging op de ASA/PIX:**Om te verzekeren dat de maximum TCP segmentgrootte de waarde niet overschrijdt die u instelt en dat het maximum niet minder dan een gespecificeerde grootte is, gebruik het bevel van de **systeemverbinding** in globale configuratiewijze. Om de standaardinstelling te herstellen, gebruikt u **het** formulier van deze opdracht. De standaard maximale waarde is 1380 bytes. De minimale optie is standaard uitgeschakeld (ingesteld op 0).U kunt de standaard maximale MSS-limiet als volgt wijzigen:

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

   Opmerking: als u de maximale grootte instelt op meer dan 1380, kunnen pakketten gefragmenteerd worden, afhankelijk van de grootte van de MTU (die standaard 1500 is). Grote aantallen fragmenten kunnen van invloed zijn op de prestaties van het security apparaat wanneer het de functie Frag Guard gebruikt. Als u de minimumgrootte instelt, voorkomt het dat de TCP server vele kleine TCP gegevenspakketten naar de client verstuurt en de prestaties van de server en het netwerk beïnvloedt.U kunt de minimale MSS-limiet als volgt wijzigen:

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

   security apparaat (configuratie)# `sysopt verbinding tcp-mss minimum MSS_size_in_bytes`**N.B.:** Raadpleeg de MPF-configuratie om pakketten mogelijk te maken die hoger zijn dan de MSS-sectie van het document PIX/ASA 7.X-probleem: MSS overschreden - HTTP-clients kunnen niet naar bepaalde websites bladeren om meer informatie te verkrijgen, zodat de overschreden MSS-pakketten met een andere methode kunnen worden verzonden.

Methode 3: Pad MTU Discovery (PMTUD)

PMTUD kan problemen met fragmentatie oplossen.

Het belangrijkste probleem met TCP MSS is dat de beheerder moet weten welke waarde om op uw router te configureren om het voorval van fragmentatie te voorkomen. Dit kan een probleem zijn als er meer dan één pad tussen u en de externe VPN-locatie bestaat, of als u uw initiële query doet, merk je dat de tweede of derde kleinere MTU in plaats van de kleinste, is gebaseerd op de routebeslissing die binnen uw initiële query is gebruikt. Met PMTUD kunt u een MTU-waarde bepalen voor IP-pakketten die fragmentatie voorkomen. Als ICMP-berichten door een router worden geblokkeerd, wordt het pad-MTU verbroken en worden pakketten met het PDF-bit-set verwijderd. Gebruik de **ingestelde ip df** opdracht om het PDF-bit te wissen en het pakket te fragmenteren en te verzenden. Fragmentation kan de snelheid van het pakkettransport op het netwerk vertragen, maar de toegangslijsten kunnen worden gebruikt om het aantal pakketten te beperken waarop het PDF-bit wordt gewist.

1. Drie problemen kunnen ervoor zorgen dat PMTUD niet functioneert:Een intermediaire router kan het pakket laten vallen en niet met een ICMP-bericht antwoorden. Dit komt niet zo veel voor op het internet, maar kan ook gewoon zijn binnen een netwerk waar routers zo zijn geconfigureerd dat ze niet reageren met onbereikbare ICMP-berichten.Een intermediaire router kan met een onbereikbaar bericht van ICMP reageren maar, op de terugkeerstroom, blokkeert een firewall dit bericht. Dit komt vaker voor.Het ICMP onbereikbare bericht maakt zijn weg terug naar de bron maar de bron negeert het fragmentatiebericht. Dit is het meest

ongewone van de drie kwesties.Als u het eerste probleem ervaart, kunt u het PDF-bit in de IP-header wissen dat de bron daar geplaatst is, of handmatig de TCP MSS-grootte aanpassen. Om het DF-bit te wissen, moet een intermediaire router de waarde van 1 tot 0 wijzigen. Normaal gesproken wordt dit gedaan door een router in uw netwerk voordat het pakket het netwerk verlaat. Dit is een eenvoudige codeconfiguratie die dit op een IOS-gebaseerde router doet:

```
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- en GRE-tunnels**Standaard voert een router geen PMTUD uit op GRE-tunnelpakketten die deze zelf genereert. Gebruik deze configuratie om PMTUD op GRE-tunnelinterfaces mogelijk te maken en de router te laten deelnemen aan het tuningproces van MTU's voor bron-/doelapparaten voor verkeer dat door de tunnel loopt:Router (configuratie) # `interface tunneltunnel _`#router (configuratie-als) # `tunnelpad-mtu-discovery`De opdracht **tunnelpad-mtu-discovery** maakt PMTUD mogelijk voor de GRE-tunnelinterface van een router. De optionele age-timer parameter specificeert het aantal minuten waarna de tunnelinterface de maximale ontdekte grootte van MTU terugstelt, min 24 bytes voor de GRE-header. Als u *oneindig* specificeert voor de timer, wordt de timer niet gebruikt. De min-mtu parameter specificeert het minimale aantal bytes dat de MTU-waarde omvat.
3. **PIX/ASA 7.x - Clear Don't Fragment (DF)** of de verwerking van grote bestanden of pakketten.U hebt nog steeds geen toegang tot het internet, grote bestanden of toepassingen via de tunnel omdat deze MTU size-error melding maakt:

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

   Om dit op te lossen, moet u het PDF-bit uit de buiteninterface van het apparaat wissen. Configureer het DF-bit beleid voor IPSec-pakketten met de opdracht **crypto ipsec df-bit** in de mondiale configuratiemodus.

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

   Met het PDF-bit met IPSec-tunnels kunt u specificeren of het security apparaat het bit `Don` Fragment `(DF)` uit de ingekapselde header kan wissen, `instellen of` kopiëren. Het DF-bit in de IP-header bepaalt of een apparaat een pakket mag fragmenteren.Gebruik de opdracht **crypto ipsec df-bit** in de mondiale configuratiemodus om het security apparaat te configureren om het DF-bit in een ingekapselde header te specificeren.Wanneer u tunnelmodus IPSec-verkeer inkapselt, gebruikt u de `heldere-df`-instelling voor het PDF-bit. Deze instelling laat het apparaat pakketten verzenden die groter zijn dan de beschikbare grootte van MTU. Deze instelling is ook geschikt als u de beschikbare MTU-grootte niet kent.

Opmerking: Als u nog steeds fragmentatie-problemen hebt en pakketten hebt geworpen, kunt u naar keuze de grootte van de MTU handmatig aanpassen met de opdracht **ip mtu-tunnelinterface**. In dit geval, fragmenteert de router het pakket voordat het het beschermt. Deze opdracht kan worden gebruikt in combinatie met PMTUD en/of TCP MSS.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Problemen oplossen

VPN-encryptie-fout

Stel dat de IPSec-tunnelheid tussen de router en PIX heeft ingesteld. Als u foutmeldingen ziet met een codering die worden verzonden, worden de volgende stappen voltooid om het probleem op te lossen:

1. Voer een snuffelspoor van de cliënt naar de serverkant uit om te ontdekken wat de beste MTU is om te gebruiken.U kunt ook de ping-test gebruiken:

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

   192.168.1.1 is het IP-adres van de afstandsmachine.
2. Blijf de waarde van 1400 met 20 verminderen tot er een antwoord is.**Opmerking:** De magische waarde, die in de meeste gevallen werkt, is 1300.
3. Pas het segment, nadat het juiste maximale segmentformaat is bereikt, op voor de gebruikte apparaten:In de PIX-firewall:

   ```
   sysopt connection tcpmss 1300
   ```

   Op de router:

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

Problemen met RDP en Citrix

Probleem:

U kunt tussen de VPN-netwerken pingelen, maar de verbindingen op Remote Desktop Protocol (RDP) en Citrix kunnen niet via de tunnel worden gerealiseerd.

Oplossing:

Het probleem kan de grootte van de MTU op de PC achter de PIX/ASA zijn. Stel de MTU-grootte in op 1300 voor de clientmachine en probeer de Citrix-verbinding in te stellen via de VPN-tunnel.

Gerelateerde informatie

- Oplossen van IP-fragmentatie, MTU, MSS en PMTUD-problemen met GRE en IPSEC
- Uitgifte van PIX/ASA 7.0: MSS overschreden - HTTP-clients kunnen niet naar bepaalde

websites bladeren

- Meest gebruikelijke L2L- en IPSec VPN-oplossingen voor probleemoplossing
- Waarom kan ik niet door het internet bladeren bij gebruik van een GRE-tunneleffect
- Technische ondersteuning en documentatie – Cisco Systems