PIX/ASA 7.x und IOS: VPN-Fragmentierung

Inhalt

Einführung

Dieses Dokument führt Sie durch die Schritte, die erforderlich sind, um Probleme zu beheben, die bei der Fragmentierung eines Pakets auftreten können. Ein Beispiel für Fragmentierungsprobleme ist die Fähigkeit, einen Ping an eine Netzwerkressource zu senden, aber die Unfähigkeit, eine Verbindung mit derselben Ressource mit einer bestimmten Anwendung herzustellen, z. B. E-Mail oder Datenbanken.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

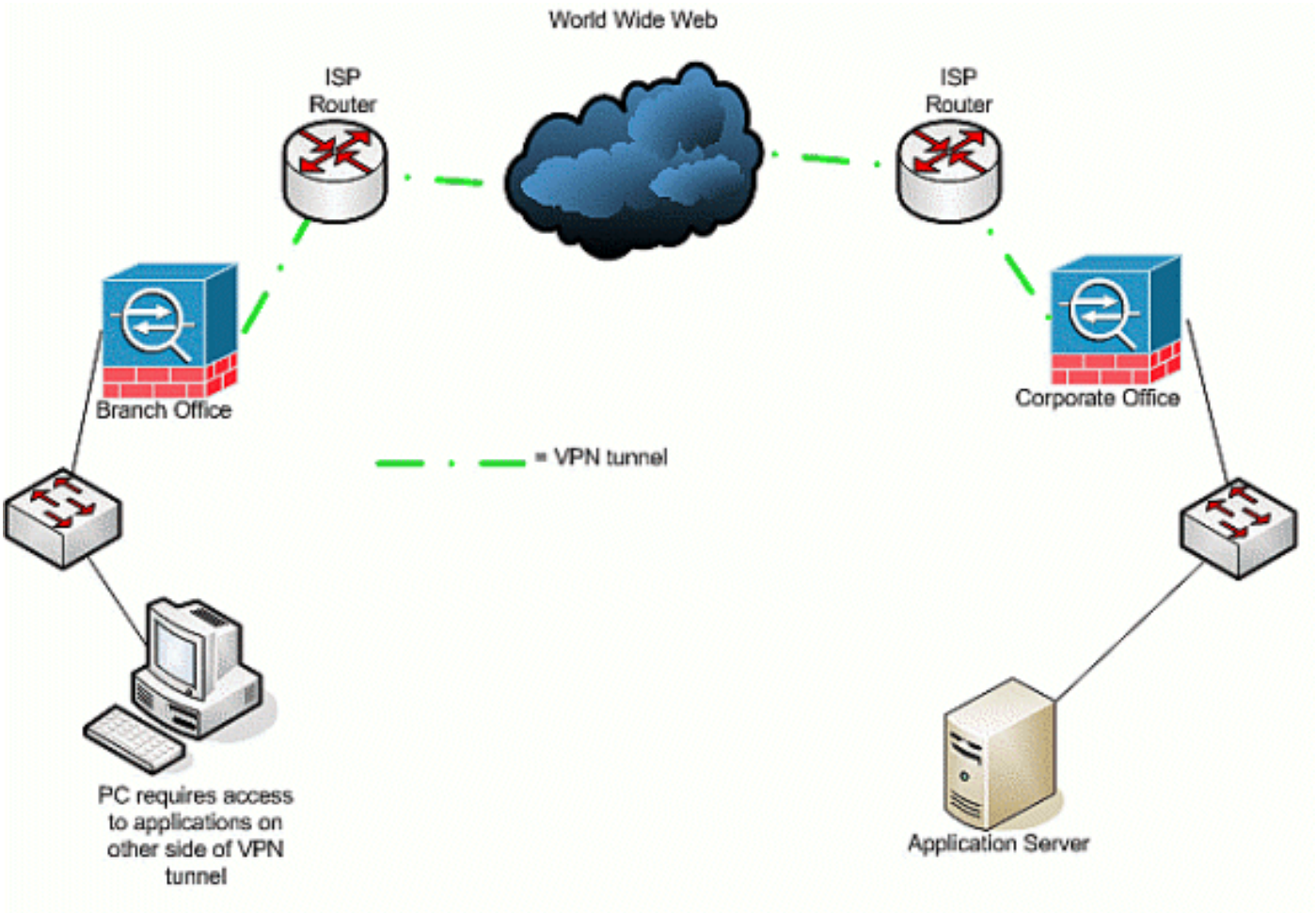
- Verbindungen zwischen VPN-Peers

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Zugehörige Produkte

Diese Konfiguration kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- IOS-Router
- PIX/ASA-Sicherheitsgeräte

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

IP unterstützt eine maximale Länge von 65.536 Byte für ein IP-Paket. Die meisten Layer-Protokolle für Datenverbindungen unterstützen jedoch eine viel kleinere Länge, die als Maximum Transmission Unit (MTU) bezeichnet wird. Basierend auf der unterstützten MTU kann es erforderlich sein, ein IP-Paket zu unterteilen (fragmentieren), um es über einen bestimmten Medientyp der Sicherungsschicht zu übertragen. Das Ziel muss dann die Fragmente wieder in das

ursprüngliche, vollständige IP-Paket einbauen.

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

Wenn Sie zum Schutz von Daten zwischen zwei VPN-Peers ein VPN verwenden, werden den ursprünglichen Daten zusätzliche Overhead hinzugefügt, was eine Fragmentierung erfordern kann. In dieser Tabelle sind Felder aufgeführt, die möglicherweise zu den geschützten Daten hinzugefügt werden müssen, um eine VPN-Verbindung zu unterstützen. Beachten Sie, dass mehrere Protokolle erforderlich sein können, wodurch die Größe des ursprünglichen Pakets erhöht wird. Wenn Sie beispielsweise eine L2L DMVPN IPSEC-Verbindung zwischen zwei Cisco Routern verwenden, bei der Sie einen GRE-Tunnel implementiert haben, benötigen Sie diesen zusätzlichen Overhead: ESP, GRE und der äußere IP-Header. Wenn Sie über eine IPSec-Software-Client-Verbindung mit einem VPN-Gateway verfügen, wenn der Datenverkehr durch ein Adressgerät geleitet wird, benötigen Sie diesen zusätzlichen Overhead für Network Address Translation-Traversal (NAT-T) sowie den äußeren IP-Header für die Tunnelmodusverbindung.

Probleme mit der Fragmentierung

Wenn die Quelle ein Paket an ein Ziel sendet, platziert sie einen Wert im Feld Control Flags der IP-Header, der die Fragmentierung des Pakets durch zwischengeschaltete Geräte beeinflusst. Das Steuerungs-Flag ist drei Bit lang, aber nur die ersten beiden werden in Fragmentierung verwendet. Wenn das zweite Bit auf 0 gesetzt ist, darf das Paket fragmentiert werden. Wenn es auf 1 gesetzt ist, darf das Paket nicht fragmentiert werden. Das zweite Bit wird häufig als *don't fragment* (DF) bezeichnet. Das dritte Bit legt fest, wann die Fragmentierung erfolgt, ob es sich bei diesem fragmentierten Paket um das letzte Fragment (auf 0 gesetzt) handelt oder ob es mehr Fragmente (auf 1 festgelegt) gibt, aus denen das Paket besteht.

Es gibt vier Bereiche, die Probleme verursachen können, wenn eine Fragmentierung erforderlich ist:

- Zusätzliche Overhead in CPU-Zyklen und im Arbeitsspeicher werden von den beiden Geräten benötigt, die Fragmentierung und Reassemblierung durchführen.
- Wenn ein Fragment auf dem Weg zum Ziel verworfen wird, kann das Paket nicht reassembliert werden, und das gesamte Paket muss fragmentiert und erneut gesendet

werden. Dies führt zu zusätzlichen Durchsatzproblemen, insbesondere in Situationen, in denen der betreffende Datenverkehr mit einer Ratenbeschränkung betrieben wird und die Quelle Datenverkehr über die zulässige Grenze sendet.
- Paketfilterung und Stateful-Firewalls können die Fragmente nur schwer verarbeiten. Bei einer Fragmentierung enthält das erste Fragment einen äußeren IP-Header, den inneren Header wie TCP, UDP, ESP und andere sowie einen Teil der Payload. Spätere Fragmente des ursprünglichen Pakets werden mit einem äußeren IP-Header und der Fortsetzung der Nutzlast verknüpft. Das Problem bei diesem Prozess besteht darin, dass bestimmte Firewalls die Informationen des inneren Headers in jedem Paket anzeigen müssen, um intelligente Filterentscheidungen treffen zu können. Wenn diese Informationen fehlen, können sie versehentlich alle Fragmente außer dem ersten löschen.
- Die Quelle im IP-Header des Pakets kann das dritte Kontrollbit so einstellen, dass es *nicht fragmentiert wird*, d. h., wenn ein zwischengeschaltetes Gerät das Paket empfängt und fragmentieren muss, kann das zwischengeschaltete Gerät es nicht fragmentieren. Stattdessen verwirft das zwischengeschaltete Gerät das Paket.

Hauptaufgabe

Fragmentierung erkennen

Die meisten Netzwerke verwenden Ethernet mit einem MTU-Standardwert von 1.500 Byte, der in der Regel für IP-Pakete verwendet wird. Um herauszufinden, ob eine Fragmentierung auftritt oder erforderlich ist, aber nicht durchgeführt werden kann (DF-Bit ist eingerichtet), sollten Sie zuerst Ihre VPN-Sitzung starten. Anschließend können Sie eine dieser vier Verfahren verwenden, um Fragmentierungen zu erkennen.

1. Pingen Sie ein Gerät am anderen Ende. Hierbei wird davon ausgegangen, dass Ping über den Tunnel zugelassen ist. Wenn dies erfolgreich ist, versuchen Sie, über dasselbe Gerät auf eine Anwendung zuzugreifen. Wenn sich beispielsweise ein Microsoft-E-Mail- oder Remote-Desktop-Server im Tunnel befindet, öffnen Sie Outlook und versuchen Sie, Ihre E-Mail herunterzuladen, oder versuchen Sie, den Remotedesktop auf den Server zu übertragen. Wenn dies nicht funktioniert und Sie über die richtige Namensauflösung verfügen, besteht eine gute Chance, dass die Fragmentierung das Problem ist.
2. Verwenden Sie auf einem Windows-Gerät Folgendes: C:\> **ping -f -l paket_size_in_bytes destination_IP_address**.Mit **-f** wird angegeben, dass das Paket nicht fragmentiert werden kann. Die Option **-l** wird verwendet, um die Länge des Pakets anzugeben. Versuchen Sie es zuerst mit einer Paketgröße von 1.500. Beispiel: ping **-f -l 1500 192.168.100**. Wenn eine Fragmentierung erforderlich, aber nicht ausgeführt werden kann, erhalten Sie eine Meldung wie die folgende: *Pakete müssen fragmentiert, aber DF-festgelegt werden*.
3. Führen Sie auf Cisco Routern den Befehl **debug ip icmp** aus, und verwenden Sie den Befehl **extended ping**. Wenn *ICMP:dst (x.x.x.x) fragmentiert und DF-festgelegt* wird*, unerreichbar an y.y.y.y gesendet* wird, wobei x.x.x.x ein Zielgerät ist und y.y.y Ihr Router ist, zeigt Ihnen ein zwischengeschaltetes Gerät, dass Fragmentierung erforderlich ist, aber da Sie das DF-Bit in der Echoanforderung festlegen, kann ein zwischengeschaltetes Gerät es nicht in der Reihenfolge fragmentieren um sie an den nächsten Hop weiterzuleiten. In diesem Fall reduzieren Sie schrittweise die MTU-Größe der Pings, bis Sie eine, die funktioniert.
4. Verwenden Sie auf Cisco Security Appliances einen

Erfassungsfilter.ciscoasa(config)#`access-list outside_test permit tcp any host 172.22.1.1 eq 80`**Hinweis:** Wenn Sie die Quelle wie *eine beliebige Quelle* verlassen, können Administratoren Netzwerkadressenübersetzungen (Network Address Translation, NAT) überwachen.ciscoasa(config)#`access-list outside_test permit tcp host 172.22.1.1 eq 80 any`**Hinweis:** Wenn Sie die Quell- und Zielinformationen rückgängig machen, können Rückgabedatenverkehr erfasst werden.`ciscoasa(config)# capture outside_interface access-list outside_test interface`Der Benutzer muss eine neue Sitzung mit Anwendung X starten. Nachdem der Benutzer eine neue Anwendung X gestartet hat, muss der ASA-Administrator den Befehl **show capture outside_interface** eingeben.

Lösungen zur Fragmentierung

Es gibt verschiedene Möglichkeiten, Probleme mit der Fragmentierung zu lösen. Diese werden in diesem Abschnitt behandelt.

Methode 1: Statische MTU-Einstellung

Die statische MTU-Einstellung kann Probleme mit der Fragmentierung beheben.

1. **MTU-Änderung auf dem Router:**Wenn Sie die MTU manuell auf dem Gerät festlegen, weist es das Gerät, das als VPN-Gateway fungiert, an, die empfangenen Pakete zu fragmentieren, bevor es geschützt wird, und sendet sie über den Tunnel. Dies ist vorzuziehen, wenn der Router den Datenverkehr schützt und dann fragmentiert, aber das Gerät fragmentiert.**Warnung:** Wenn Sie die MTU-Größe auf einer beliebigen Geräteschnittstelle ändern, werden alle auf dieser Schnittstelle terminierten Tunnel beendet und neu erstellt.Verwenden Sie auf Cisco Routern den Befehl **ip** mtuBefehl, um die MTU-Größe für die Schnittstelle anzupassen, an der das VPN terminiert wird:
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **MTU-Änderung auf ASA/PIX:**Verwenden Sie auf ASA/PIX-Geräten den Befehl mtucommand, um die MTU-Größe im globalen Konfigurationsmodus anzupassen. Standardmäßig ist die MTU auf 1500 festgelegt. Wenn Sie z. B. eine Schnittstelle auf Ihrer Sicherheitslösung mit dem Namen *Outside (an der das VPN terminiert wird)* hatten und (mithilfe der im Abschnitt Fragmentierung aufgeführten Maßnahmen) festgestellt haben, dass Sie die 1380 als Fragmentgröße verwenden möchten, verwenden Sie den folgenden Befehl:
```
security appliance (config)# mtu Outside 1380
```

Methode 2: Maximale TCP-Segmentgröße

Die maximale TCP-Segmentgröße kann Probleme mit der Fragmentierung beheben.

Hinweis: Diese Funktion funktioniert nur mit TCP. Andere IP-Protokolle müssen eine andere Lösung verwenden, um IP-Fragmentierungsprobleme zu lösen. Selbst wenn Sie die IP-MTU auf dem Router festlegen, hat dies keine Auswirkungen darauf, was die beiden End-Hosts im Drei-Wege-TCP-Handshake mit TCP-MSS aushandeln.

1. **MSS-Änderung auf dem Router:**Bei TCP-Datenverkehr findet eine Fragmentierung statt, da

TCP-Datenverkehr normalerweise zum Transport großer Datenmengen verwendet wird. TCP unterstützt eine Funktion namens TCP Maximum Segment Size (MSS), mit der die beiden Geräte eine geeignete Größe für TCP-Datenverkehr aushandeln können. Der MSS-Wert wird auf jedem Gerät statisch konfiguriert und stellt die Puffergröße für ein erwartetes Paket dar. Wenn zwei Geräte TCP-Verbindungen herstellen, vergleichen sie den lokalen MSS-Wert mit dem lokalen MTU-Wert im Drei-Wege-Handshake. welches niedriger ist, wird an den Remote-Peer gesendet. Die beiden Peers verwenden dann den unteren der beiden ausgetauschten Werte. Gehen Sie wie folgt vor, um diese Funktion zu konfigurieren:Verwenden Sie auf Cisco Routern den Befehl **tcp adjust-mss** auf der Schnittstelle, auf der das VPN terminiert wird.

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

2. **MSS-Änderung auf ASA/PIX:**Um sicherzustellen, dass die maximale TCP-Segmentgröße den von Ihnen festgelegten Wert nicht überschreitet und der maximale Wert nicht kleiner als eine angegebene Größe ist, verwenden Sie den Befehl **sysopt connection** im globalen Konfigurationsmodus. Um die Standardeinstellung wiederherzustellen, verwenden Sie **das** Formular dieses Befehls. Der Standardwert ist 1380 Byte. Die Mindestfunktion ist standardmäßig deaktiviert (auf 0 gesetzt).Gehen Sie wie folgt vor, um das standardmäßige maximale MSS-Limit zu ändern:

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

   Hinweis: Wenn Sie die maximale Größe auf mehr als 1380 festlegen, können Pakete fragmentiert werden, abhängig von der MTU-Größe (standardmäßig 1500). Eine große Anzahl von Fragmenten kann die Leistung der Sicherheitsappliance beeinträchtigen, wenn sie die Funktion "Frag Guard" verwendet. Wenn Sie die Mindestgröße festlegen, verhindert dies, dass der TCP-Server viele kleine TCP-Datenpakete an den Client sendet und die Leistung des Servers und des Netzwerks beeinträchtigt.Gehen Sie wie folgt vor, um den MSS-Mindestgrenzwert zu ändern:

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

   security appliance (config)# `sysopt connection tcp-mss minimum MSS_size_in_bytes`**Hinweis:** Weitere Informationen finden Sie im Abschnitt MPF-Konfiguration zum Zulassen von Paketen, die MSS überschreiten im Dokument PIX/ASA 7.X-Problem: MSS Exceeded - HTTP-Clients können nicht zu einigen Websites nach weiteren Informationen durchsuchen, um die Überschreitung der MSS-Pakete einer anderen Methode zuzulassen.

Methode 3: Path MTU Discovery (PMTUD)

Die PMTUD kann Probleme mit der Fragmentierung beheben.

Das Hauptproblem bei TCP-MSS besteht darin, dass der Administrator wissen muss, welchen Wert er auf dem Router konfigurieren muss, um eine Fragmentierung zu verhindern. Dies kann problematisch sein, wenn mehr als ein Pfad zwischen Ihnen und dem Remote-VPN-Standort vorhanden ist. Wenn Sie Ihre erste Abfrage durchführen, stellen Sie fest, dass die zweite oder dritte kleinere MTU, nicht die kleinste, auf der Routing-Entscheidung basiert, die in Ihrer ursprünglichen Abfrage verwendet wird. Mit der PMTUD können Sie einen MTU-Wert für IP-Pakete bestimmen, der eine Fragmentierung vermeidet. Wenn ICMP-Nachrichten von einem Router blockiert werden, wird die Pfad-MTU unterbrochen, und Pakete mit dem DF-Bit-Satz werden verworfen. Mit dem Befehl **set ip df** löschen Sie das DF-Bit, und lassen Sie zu, dass das Paket fragmentiert und gesendet wird. Eine Fragmentierung kann die Paketweiterleitung im

Netzwerk verlangsamen, aber mithilfe von Zugriffslisten kann die Anzahl der Pakete begrenzt werden, für die das DF-Bit gelöscht wird.

1. Drei Probleme können dazu führen, dass die PMTUD nicht funktioniert:Ein zwischengeschalteter Router kann das Paket verwerfen und nicht mit einer ICMP-Meldung reagieren. Dies ist im Internet nicht sehr häufig der Fall, kann aber in Netzwerken üblich sein, in denen Router so konfiguriert sind, dass sie nicht mit nicht erreichbaren ICMP-Nachrichten reagieren.Ein zwischengeschalteter Router kann mit einer ICMP-Meldung reagieren, die nicht erreichbar ist. Beim Rücklauf blockiert jedoch eine Firewall diese Nachricht. Dies tritt häufiger auf.Die Meldung "ICMP Unreachable" geht zurück zur Quelle, aber die Quelle ignoriert die Fragmentierungsmeldung. Dies ist die ungewöhnlichste der drei Themen.Wenn das erste Problem auftritt, können Sie entweder das DF-Bit im IP-Header löschen, den die Quelle dort platziert hat, oder die TCP-MSS-Größe manuell anpassen. Um das DF-Bit zu löschen, muss ein zwischengeschalteter Router den Wert von 1 auf 0 ändern. Normalerweise wird dies von einem Router in Ihrem Netzwerk durchgeführt, bevor das Paket das Netzwerk verlässt. Dies ist eine einfache Codekonfiguration für einen IOS-basierten Router:
```
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- und GRE-TunnelStandardmäßig führt ein Router die PMTUD für GRE-Tunnelpakete nicht aus, die er selbst generiert. Um die PMTUD auf GRE-Tunnelschnittstellen zu aktivieren und den Router am MTU-Tuning-Prozess für Quell-/Zielgeräte für den Datenverkehr, der den Tunnel passiert, teilzunehmen, verwenden Sie die folgende Konfiguration:Router (config) # `Interface Tunnel` _#Router (config-if) # `tunnel path-mtu-discovery`Der Befehl **tunnel path-mtu-discovery** aktiviert die PMTUD für die GRE-Tunnelschnittstelle eines Routers. Der optionale Parameter "age-timer" gibt die Anzahl der Minuten an, nach denen die Tunnelschnittstelle die maximal erkannte MTU-Größe zurücksetzt, abzüglich 24 Byte für den GRE-Header. Wenn Sie *unendlich* für den Zeitgeber angeben, wird der Zeitgeber nicht verwendet. Der min-mtu-Parameter gibt die Mindestanzahl von Bytes an, die den MTU-Wert umfasst.
3. PIX/ASA 7.x - Clear Don't Fragment (DF) oder Verarbeitung großer Dateien oder Pakete.Sie können über den Tunnel immer noch nicht ordnungsgemäß auf das Internet, große Dateien oder Anwendungen zugreifen, da diese MTU-Größenfehlermeldung angezeigt wird:

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

   Um dies zu beheben, sollten Sie das DF-Bit von der externen Schnittstelle des Geräts löschen. Konfigurieren Sie die DF-Bit-Richtlinie für IPSec-Pakete mit dem Befehl **crypto ipsec df-bit** im globalen Konfigurationsmodus.

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

   Das DF-Bit mit der IPSec-Tunnelfunktion ermöglicht Ihnen anzugeben, ob die Sicherheits-Appliance das `DF-Bit (Don't Fragment)` aus dem gekapselten Header löschen, festlegen oder

kopieren kann. Das DF-Bit im IP-Header bestimmt, ob ein Gerät ein Paket fragmentieren darf.Konfigurieren Sie die Sicherheits-Appliance mithilfe des Befehls **crypto ipsec df-bit** im globalen Konfigurationsmodus, um das DF-Bit in einem gekapselten Header anzugeben.Wenn Sie Tunnel-Modus-IPSec-Datenverkehr kapseln, verwenden Sie die `clear-df`-Einstellung für das DF-Bit. Bei dieser Einstellung kann das Gerät Pakete senden, die größer als die verfügbare MTU-Größe sind. Diese Einstellung ist auch dann angebracht, wenn Sie die verfügbare MTU-Größe nicht kennen.

Hinweis: Wenn weiterhin Fragmentierungsprobleme auftreten und Pakete verworfen werden, können Sie optional die MTU-Größe mithilfe des Befehls **ip mtu tunnel interface** manuell anpassen. In diesem Fall fragmentiert der Router das Paket, bevor er es schützt. Dieser Befehl kann in Verbindung mit der PMTUD und/oder TCP-MSS verwendet werden.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Fehlerbehebung

VPN-Verschlüsselungsfehler

Nehmen Sie an, dass der IPSec-Tunnel zwischen Router und PIX eingerichtet wurde. Wenn Sie Verschlüsselungsfehlermeldungen sehen, dass Pakete verworfen werden, führen Sie die folgenden Schritte aus, um das Problem zu beheben:

1. Führen Sie eine Sniffer-Trace vom Client zur Serverseite durch, um herauszufinden, welche MTU am besten geeignet ist.Sie können auch den Ping-Test verwenden:

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

   192.168.1.1 ist die IP-Adresse des Remote-Systems.
2. Fahren Sie fort, den Wert von 1400 um 20 zu reduzieren, bis eine Antwort vorliegt.**Hinweis:** Der magische Wert, der in den meisten Fällen funktioniert, ist 1300.
3. Nachdem die entsprechende maximale Segmentgröße erreicht wurde, passen Sie sie an die verwendeten Geräte an:PIX-Firewall:

   ```
   sysopt connection tcpmss 1300
   ```

   Auf dem Router:

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

RDP- und Citrix-Probleme

Problem:

Sie können einen Ping zwischen den VPN-Netzwerken senden, aber Remote Desktop Protocol (RDP)- und Citrix-Verbindungen können nicht über den Tunnel hergestellt werden.

Lösung:

Das Problem kann die MTU-Größe auf dem PC hinter dem PIX/ASA sein. Legen Sie die MTU-Größe für den Client-Computer auf 1300 fest, und versuchen Sie, die Citrix-Verbindung über den VPN-Tunnel herzustellen.

Zugehörige Informationen

- Lösung von Problemen mit IP-Fragmentierung, MTU, MSS und PMTUD mit GRE und IPSEC
- Problem mit PIX/ASA 7.0: MSS übersprungen - HTTP-Clients können nicht zu einigen Websites wechseln
- Häufigste L2L- und Remote Access IPSec VPN-Lösungen zur Fehlerbehebung
- Warum kann ich nicht im Internet surfen, wenn ich einen GRE-Tunnel verwende?
- Technischer Support und Dokumentation - Cisco Systems