PIX/ASA 7.x和IOS:VPN分段

目錄

簡介

本檔案將指導您完成減輕封包分段可能出現問題所需的步驟。分段問題的一個示例是能夠ping通網路資源，但無法連線到特定應用程式（如電子郵件或資料庫）的同一資源。

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

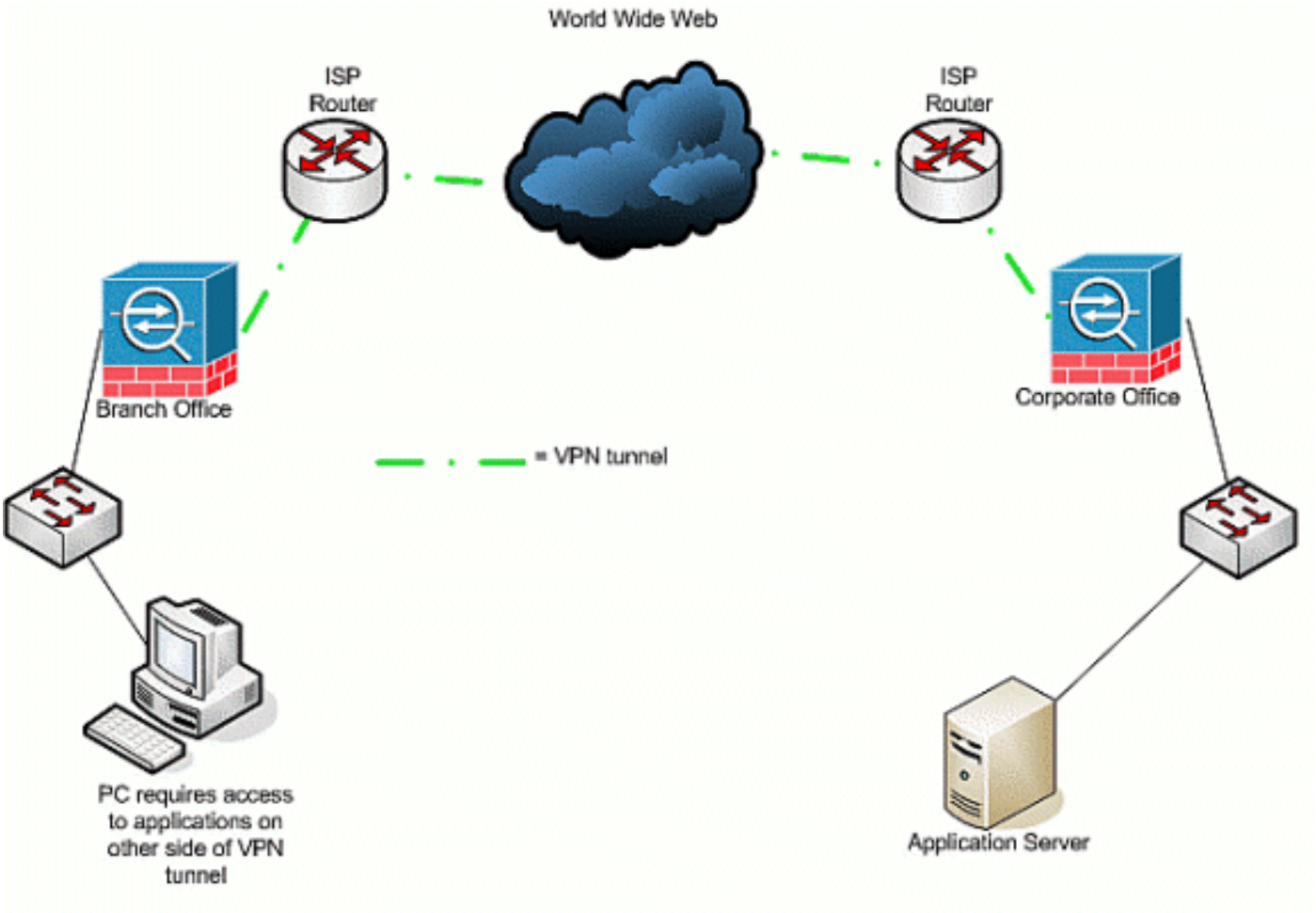
- VPN對等點之間的連線

採用元件

本文件所述內容不限於特定軟體和硬體版本。

網路圖表

本檔案會使用以下網路設定：



相關產品

此配置還可以用於以下硬體和軟體版本：

- IOS路由器
- PIX/ASA安全裝置

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

背景資訊

IP支援IP資料包的最大長度為65,536位元組，但大多數資料鏈路層協定支援更小的長度，稱為最大傳輸單元(MTU)。 根據支援的MTU，可能需要分段（分段）IP封包，以透過特定資料連結層媒體型別傳輸它。然後，目的地必須將片段重組回原始的完整IP封包。

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

當您使用VPN保護兩個VPN對等體之間的資料時，原始資料會增加額外開銷，這可能需要進行分段。此表列出為了支援VPN連線而可能必須新增到受保護資料的欄位。請注意，可能需要多個協定，這會增加原始資料包的大小。例如，如果在已實施GRE通道的兩台Cisco路由器之間使用L2L DMVPN IPSEC連線，則需要此額外開銷：ESP、GRE和外部IP報頭。如果流量通過地址裝置時具有IPSec軟體客戶端與VPN網關的連線，那麼網路地址轉換 — 遍歷(NAT-T)以及隧道模式連線的外部IP報頭都需要此額外開銷。

分段問題

當來源將封包傳送到目的地時，會在IP標頭的控制旗標欄位中放置一個值，影響中間裝置對封包的分段。控制標誌長度為三位，但在分段過程中僅使用前兩位。如果第二位設定為0，則允許將封包分段；如果設定為1，則不允許對資料包進行分段。第二個位元通常稱為*不分段*(DF)位元。第三位指定分段發生的時間、此分段的資料包是否是最後一個片段（設為0），或者是否有更多片段（設為1）組成資料包。

在需要分段時，有四個方面可能會出現問題：

- 執行分段和重組的兩個裝置需要額外的CPU週期和記憶體開銷。
- 如果在到達目的地的路上捨棄了一個片段，就不能再重組封包，而且必須將整個封包分段再重新傳送。這會產生額外的輸送量問題，尤其是當問題流量受速率限制，且來源傳送的流量超過允許限制時。
- 封包過濾和有狀態防火牆在處理片段時可能會遇到困難。分段時，第一個分段包含外部IP報頭、內部報頭（如TCP、UDP、ESP等）以及負載的一部分。原始資料包的後續片段會與外部IP報頭以及負載的繼續部分發生衝突。這個過程的問題是某些防火牆需要檢視每個資料包的內部報頭資訊，以便做出智慧過濾決策；如果缺少該資訊，則它們會無意中丟棄除第一個片段以外的所有片段。
- 封包IP標頭中的來源可將第三控制位設定為*不分段*，這表示如果中間裝置收到封包且必須將其分段，則中間裝置無法將其分段。相反，中間裝置丟棄資料包。

主要任務

發現分段

大多數網路使用乙太網，其預設MTU值為1,500位元組，通常用於IP資料包。若要瞭解是否發生或需要分段，但無法完成（已設定DF位元），請首先啟動VPN作業階段。然後，您可以使用這四個過程中的任何一種來發現分段。

1. 對位於另一端的裝置執行Ping。這是假設允許ping通過隧道。如果成功，請嘗試通過同一裝置訪問應用；例如，如果Microsoft電子郵件或遠端案頭伺服器通過隧道，請開啟Outlook並嘗試下載電子郵件，或嘗試將遠端案頭連線到伺服器。如果此操作不起作用，並且您有正確的名稱解析，則很可能存在碎片問題。
2. 在Windows裝置中，使用以下命令：C:\> **ping -f -l packet_size_in_bytes destination_IP_address**。**-f**選項用於指定資料包不能分段。**-l** 選項用於指定資料包的長度。首先使用封包大小1,500嘗試此操作。例如ping **-f -l 1500 192.168.100**。如果需要分段但無法執行，您會收到類似以下的訊息：*封包需要分段，但已設定DF*。
3. 在Cisco路由器上，執行**debug ip icmp**命令並使用**extended ping**命令。如果您看到需要*ICMP:dst(x.x.x.x)分段和設定DF，則無法傳送到y.y.y.y*，其中x.x.x.x是目的地裝置，y.y.y是路由器，中間裝置會告訴您需要分段，但由於您在回應要求中設定了DF位元，因此中間裝置無法將其分段以便轉送到下一個躍點。在這種情況下，請逐步降低ping的MTU大小，直到找到有效的執行。
4. 在思科安全裝置上，使用捕獲過濾器。ciscoasa(config)#`access-list outside_test permit tcp any host 172.22.1.1 eq 80`**注意：**如果將源保留為*any*，管理員可以監控任何網路地址轉換(NAT)。ciscoasa(config)#`access-list outside_test permit tcp host 172.22.1.1 eq 80 any`**注意：**反向傳送來源和目的地資訊時，系統允許擷取傳回流量。`ciscoasa(config)# capture outside_interface access-list outside_test interface outside`使用者需要啟動與應用程式X的新會話。使用者啟動新的應用程式X會話後，ASA管理員需要發出**show capture outside_interface**命令。

分段問題的解決方案

有多種方法可以解決分段問題。這些將在本節中討論。

方法1:靜態MTU設定

靜態MTU設定可以解決分段問題。

1. **路由器上的MTU更改：**請注意，如果您在裝置上手動設定MTU，則會告訴充當VPN閘道的裝置對接收的封包進行分段，然後再保護封包並將其傳送到通道中。這比讓路由器保護流量然後對其進行分段好，但裝置將其分段。**警告：**如果更改任何裝置介面上的MTU大小，將導致終止在該介面上的所有隧道被關閉並重建。在Cisco路由器上，使用**ip** 命令調整VPN終止介面上的MTU大小：
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **ASA/PIX上的MTU更改：**在ASA/PIX裝置上，使用mtucommand在全域性配置模式下調整MTU大小。預設情況下，MTU設定為1500。例如，如果安全裝置上有一個名為*Outside（VPN終止的位置）*的介面，並且您通過Discover Fragmentation部分中列出的測量方法確定想要使用1380作為片段大小，請使用以下命令：
```
security appliance (config)# mtu Outside 1380
```

方法2:TCP最大區段大小

TCP最大區段大小可解決分段問題。

注意：此功能僅適用於TCP;其他IP通訊協定必須使用另一個解決方案來解決IP分段問題。即使您在路由器上設定ip mtu ，也不會影響兩個終端主機在與TCP MSS的TCP三次交握中交涉的內容。

1. **路由器上的MSS更改：**由於TCP流量通常用於傳輸大量資料，因此會對TCP流量進行分段。TCP支援稱為TCP最大片段大小(MSS)的功能，此功能允許兩台裝置交涉適合TCP流量的大小。MSS值在每個裝置上靜態配置，它表示用於預期資料包的緩衝區大小。當兩台裝置建立TCP連線時，會比較三次交握中的本地MSS值與本地MTU值；兩者中較低者將被傳送到遠端對等裝置。然後，兩個對等體使用兩個交換值中的較低者。若要設定此功能，請執行以下操作：在Cisco路由器上，在終止VPN的介面上使用**tcp adjust-mss**命令。
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip tcp adjust-mss MSS_Size_in_bytes
```

2. **ASA/PIX上的MSS更改：**為了確保最大TCP資料段大小不超過設定的值且最大值不小於指定的大小，請在全域性配置模式下使用**sysopt connection**命令。若要還原預設設定，請使用此命令的**theno**形式。預設的最大值為1380位元組。預設情況下禁用最小功能（設定為0）。若要變更預設的最大MSS限制，請執行以下操作：
```
security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
```

   注意：如果將最大大小設定為大於1380，則資料包可能會分段，具體取決於MTU大小（預設情況下為1500）。 當安全裝置使用Frag Guard功能時，大量碎片可能會影響其效能。如果設定最小大小，將阻止TCP伺服器向客戶端傳送許多小型TCP資料包，並影響伺服器和網路的效能。若要變更最低MSS限制，請執行以下操作：
```
security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes
```
   安全裝置(config)# `sysopt connection tcp-mss minimum MSS_size_in_bytes`**註：**請參閱PIX/ASA 7.X問題文檔中的MPF配置以允許超過MSS的資料包部分：超出MSS - HTTP使用者端無法瀏覽到某些網站以瞭解詳細資訊，以便允許超出的MSS封包使用其他方法。

方法3:路徑MTU探索(PMTUD)

PMTUD可以解決分段問題。

TCP MSS的主要問題是管理員必須瞭解要在路由器上配置什麼值以防止分段發生。如果您與遠端VPN位置之間存在多個路徑，或者，當您執行初始查詢時，您發現第二或第三較小的MTU（而不是最小的）基於初始查詢中使用的路由決策，則可能會出現此問題。使用PMTUD時，您可以確定避免分段的IP封包的MTU值。如果路由器封鎖了ICMP訊息，則會破壞路徑MTU，並捨棄已設定DF位元的封包。使用**set ip df** 命令清除DF位元，並允許將封包分段和傳送。分段可以減慢網路上的封包轉送速度，但存取清單可用於限制清除DF位元的封包數量。

1. 三個問題可能導致PMTUD無法運作：中繼路由器可能捨棄封包而不使用ICMP訊息回應。這在Internet上並不常見，但是在路由器配置為不響應ICMP不可達消息的網路中很常見。中繼路由器可能使用ICMP無法到達消息進行響應，但在返回流中，防火牆會阻止此消息。這種情況更為常見。ICMP無法到達訊息順利傳回來源，但來源忽略分段訊息。這是三個問題中最不尋常的一個。如果您遇到第一個問題，可以清除來源放置於其中的IP標頭中的DF位元，或手動調整TCP MSS大小。若要清除DF位元，中間路由器必須將值從1變更為0。通常，這由網路中的路由器在封包離開網路之前完成。這是在基於IOS的路由器上執行此操作的簡單代碼配置：
```
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和GRE通道**預設情況下，路由器不會在其產生的GRE通道封包上執行PMTUD。若要在GRE通道介面上啟用PMTUD，並讓路由器參與穿越通道流量的來源/目的地裝置的MTU調整程式，請使用以下設定：Router(config) # `interface tunnel` tunnel_#Router(config-if)# `tunnel path-mtu-discovery`**tunnel path-mtu-discovery** 指令為路由器的GRE通道介面啟用PMTUD。可選的age-timer引數指定隧道介面重置發現的最大MTU大小的分鐘數，減去GRE報頭的24位元組。如果為計時器指定*infinite*，則不使用計時器。min-mtu引數指定組成MTU值的最小位元組數。
3. **PIX/ASA 7.x — 清除不分段(DF)或處**理大型檔案或資料包。您仍無法透過通道正確存取Internet、大型檔案或應用程式，因為它會提供以下MTU大小錯誤訊息：

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

   為了解決此問題，請務必從裝置的外部介面清除DF位元。在全域性配置模式下使用**crypto ipsec df-bit**命令為IPSec資料包配置DF位策略。

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

   使用IPSec通道的DF位元功能，您可以指定安全裝置是否可以從封裝標頭中清`(DF)`」位元。IP標頭中的DF位元可判斷是否允許裝置將封包分段。在全域性配置模式下使用**crypto ipsec df-bit**命令配置安全裝置以指定封裝報頭中的DF位。封裝通道模式IPSec流量時，請使用DF位元的`clear-df`設定。此設定允許裝置傳送大於可用MTU大小的資料包。如果您不知道可用的MTU大小，此設定也適用。

注意：如果仍然遇到分段問題和丟棄的資料包，則可以使用**ip mtu tunnel interface命令手動調整MTU大**小。在這種情況下，路由器對封包進行分段後再對其進行保護。此命令可與PMTUD和/或TCP MSS結合使用。

驗證

目前沒有適用於此組態的驗證程序。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

VPN加密錯誤

假設路由器和PIX之間已建立IPSec隧道。如果您看到丟棄資料包的加密錯誤消息，請完成以下步驟以解決問題：

1. 執行從使用者端到伺服器的監聽器追蹤，以確定哪一個是要使用的最佳MTU。您也可以使用ping測試：

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

192.168.1.1是遠端電腦的IP地址。

2. 繼續將1400的值減少20，直到得到回覆。**註：**大多數情況下適用的魔力值為1300。
3. 達到適當的最大網段大小後，針對正在使用的裝置對其進行適當調整：在PIX防火牆上：

```
sysopt connection tcpmss 1300
```

在路由器上：

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

RDP和Citrix問題

問題：

您可以在VPN網路之間執行ping，但無法通過隧道建立遠端案頭協定(RDP)和Citrix連線。

解決方案：

問題可能是PIX/ASA後面的PC上的MTU大小。將客戶端電腦的MTU大小設定為1300，並嘗試通過VPN隧道建立Citrix連線。

相關資訊

- 使用GRE和IPSEC解決IP分段、MTU、MSS和PMTUD問題
- PIX/ASA 7.0問題：超出MSS - HTTP客戶端無法瀏覽某些網站
- 最常見的L2L和遠端訪問IPSec VPN故障排除解決方案
- 使用GRE通道時為什麼無法瀏覽Internet
- 技術支援與文件 - Cisco Systems