PIX/ASA 7.x 和 IOS：VPN 分段

目录

简介

本文档指导您完成解决数据包分段可能产生的问题所需的步骤。分段问题的一个例子是，尽管能够对某个网络资源执行 ping 命令，但无法使用特定应用程序（如电子邮件或数据库）连接到该资源。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- VPN 对等体之间的连接

使用的组件

本文档不限于特定的软件和硬件版本。

网络图

本文档使用以下网络设置：

相关产品

此配置也可用于以下硬件和软件版本：

- IOS 路由器
- PIX/ASA 安全设备

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

IP 支持最大长度为 65,536 字节的 IP 数据包，但大部分数据链路层协议支持的长度要小得多，该长度称为最大传输单元 (MTU)。根据支持的 MTU，可能需要对 IP 数据包进行分解（分段），以便通过特定的数据链路层介质类型进行传输。随后，传输目标必须将分段重组为原始的完整 IP 数据包。

当您使用 VPN 保护两个 VPN 对等体之间的数据时，会为原始数据增加额外开销，因而可能需要进行分段。下表列出了可能必须添加到保护数据以支持 VPN 连接的字段。请注意，可能有多个必要协议，这会增加原始数据包的大小。例如，如果在已实现 GRE 隧道的两个 Cisco 路由器之间使用 L2L DMVPN IPSEC 连接，则需要增加以下开销：ESP、GRE 和外部 IP 报头。如果数据流通过地址设备时存在与 VPN 网关的 IPSec 软件客户端连接，则需要增加网络地址转换穿透 (NAT-T) 的开销，以及隧道模式连接的外部 IP 报头。

分段问题

当源向目标发送数据包时，会在 IP 报头的控制标志字段中放置一个值，该值将影响中间设备对数据包的分段。控制标志的长度为三位，但只有前两位用于分段。如果第二位设置为 0，则允许对数据包进行分段；如果将其设置为 1，则不允许对数据包进行分段。第二位通常称为 *不分段 (DF)* 位。第三个位用于指定发生分段时此分段数据包是否是最后一个分段（设置为 0），或是还有其他组成该数据包的分段（设置为 1）。

需要进行分段时，可能会在以下四个方面产生问题：

- 执行分段和重组的两个设备需要增加 CPU 周期和内存的开销。
- 如果某个分段在传输至目标的过程中丢失，则无法重组数据包，必须重新对整个数据包进行分段和发送。这会产生另外一些吞吐量问题，尤其是所关注的数据流存在速率限制而源发送的数据流超过允许的限制的情况。
- 数据包过滤和状态防火墙可能难以处理分段。发生分段时，第一个分段包含外部 IP 报头、内部报头（如 TCP、UDP、ESP 及其他内容）和部分有效负载。原始数据包的后续分段包含一个外部 IP 报头和其余有效负载。此过程的问题是某些防火墙需要查看每个数据包的内部报头信息以做出智能过滤决策；如果缺少该信息，它们可能会在无意间丢弃除第一个分段外的所有分段。
- 数据包 IP 报头中的源可以将第三个控制位设置为 *不分段*，这意味着，如果中间设备收到数据包且必须对其进行分段，该中间设备将无法对其进行分段。这时，中间设备将丢弃该数据包。

主要任务

发现分段

大多数网络都使用以太网，默认 MTU 值为 1,500 字节，这是 IP 数据包的常用设置。要查明分段是否发生或是需要分段但无法完成（设置了 DF 位），首先启动 VPN 会话。随后可以使用以下四个步骤中的任意一个发现分段。

1. 对位于另一端的设备执行 ping 命令。此操作的假设前提是允许通过隧道执行 ping 命令。如果此操作成功，则尝试通过同一个设备访问应用程序；例如，如果 Microsoft 电子邮件或远程桌面服务器在通道另一端，则打开 Outlook 并尝试下载您的电子邮件，或尝试通过远程桌面访问服务器。如果此操作不成功，而名称解析正确，则很可能是分段存在问题。
2. 通过 Windows 设备使用以下命令：C:\> **ping -f -l packet_size_in_bytes destination_IP_address**。**-f** 选项用于指定数据包不能分段。**-l** 选项用于指定数据包的长度。首先用 1,500 的数据包大小尝试此操作。例如，ping **-f -l 1500 192.168.100**。如果需要进行分段但无法执行，您将收到一则类似如下内容的消息：*Packets need to be fragmented but DF set*。
3. 在 Cisco 路由器上执行 **debug ip icmp** 命令，然后使用 **extended ping** 命令。如果显示 *ICMP：dst (x.x.x.x) fragmentation needed and DF set, unreachable sent to y.y.y.y*（其中 x.x.x.x 是目标设备，y.y.y.y 是您的路由器），则表示中间设备通知您需要进行分段，但您在 Echo 请求中设置了 DF 位，中间设备无法对其进行分段以将其转发至下一跳。在这种情况下，可逐渐减小 ping 的 MTU 大小，直到找到有效的大小。
4. 在 Cisco 安全设备上使用捕获过滤器。ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80**注意：** 如果将源保留为 *any*，则允许管理员对任何网络地址转换 (NAT) 进行监控。ciscoasa(config)#access-list outside_test permit tcp host 172.22.1.1 eq 80 any**注意：** 如果将源和目标信息反转，则允许捕获返回数据流。`ciscoasa(config)# capture outside_interface access-list outside_test interface outside`用户需要通过应用程序 X 启动一个新会话。用户启动新的应用程序 X 会话后，ASA 管理员需要发出 **show capture outside_interface** 命令。

分段问题的解决方法

解决分段问题可采用多种不同的方法。本部分将介绍这些方法。

方法 1：静态 MTU 设置

静态 MTU 设置可用于解决分段问题。

1. **路由器上的 MTU 更改：**请注意，如果手动设置设备的 MTU，它会指示作为 VPN 网关的设备在保护收到的数据包并通过通道发送这些数据包之前对它们进行分段。与由路由器保护数据流然后对其进行分段相比，由设备对其进行分段更为可取。**警告：** 如果更改任何设备接口的 MTU 大小，将导致以该接口为终端的所有通道被切断并重建。在 Cisco 路由器上，使用 **ip mtucommand** 调整 VPN 终止的接口的 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 设备上，使用 **mtucommand** 在全局配置模式下调整 MTU 大小。默认情况下，MTU 设置为 1500。例如，如果您的安全设备上有一个名为 *Outside* 的接口（VPN 在该接口终止），并且已通过“发现分段”部分列出的测量值确定要使用 1380 作为分段大小，则使用以下命令：
```
security appliance (config)# mtu Outside 1380
```

方法 2：TCP 最大分段大小

TCP 最大分段大小可用于解决分段问题。

注意： 此功能仅适用于 TCP；其他 IP 协议必须使用另一种解决方案解决 IP 分段问题。即使您在路由器上设置了 IP MTU，它也不会影响两个终端主机在与 TCP MSS 的 TCP 三方握手中的协商内容。

1. **路由器上的 MSS 更改：**由于 TCP 数据流通常用于传输大量数据，因此 TCP 数据流要进行分段。TCP 支持一种叫做 TCP 最大分段大小 (MSS) 的功能，该功能使两个设备可以协商 TCP 数据流的适当大小。MSS 值在每个设备上以静态方式进行配置，它表示要用于某个预期数据包的缓冲区大小。当两个设备建立 TCP 连接时，它们会在三方握手中对本地 MSS 值与本地 MTU 值进行比较；将较低者发送到远程对等体。随后两个对等体将使用两个交换值中较低的值。要配置此功能，请执行下列操作：在 Cisco 路由器上，对 VPN 终止的接口使用 **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：**为确保最大 TCP 段大小不超过您设置的值并确保最大值不小于指定大小，应在全局配置模式下使用 **sysopt connection** 命令。要恢复默认设置，请使用此命令的 no 形式。默认最大值为 1380 字节。最小值功能默认处于禁用状态（设置为 0）。要更改默认的最大 MSS 限制，请执行下列操作：
   ```
   security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
   ```

   注意： 如果设置的最大大小大于 1380，数据包会根据 MTU 大小（默认为 1500）进行分段。如果分段数量较大，则会在安全设备使用分段防护功能时影响设备的性能。如果设置最小大小，则会防止 TCP 服务器向客户端发送许多较小的 TCP 数据包而影响服务器和网络的性能。要更改最小 MSS 限制，请执行以下命令：
   ```
   security appliance (config)# sysopt connection tcp-mss MSS_size_in_bytes
   ```

   security appliance (config)# sysopt connection tcp-mss minimum MSS_size_in_bytes**注意：** 请参阅以下文档的允许数据包超过 MSS 的 MPF 配置部分：PIX/ASA 7.X 问题：超过 MSS - HTTP 客户端无法浏览某些网站以获得有关为超过 MSS 的数据包提供另一种方法的详细信息。

方法 3：路径 MTU 发现 (PMTUD)

PMTUD 可用于解决分段问题。

TCP MSS 的主要问题是管理员必须了解要在路由器上配置什么值才能防止分段发生。如果您与远程 VPN 位置之间存在多个路径，或者当您执行初始查询时发现第二小或第三小的 MTU（而不是最小 MTU）是以初始查询中使用的路由决策为基准的，这时就会遇到上述问题。使用 PMTUD，您可以确定防止分段的 IP 数据包 MTU 值。如果 ICMP 消息被路由器阻止，则会分解路径 MTU，并丢弃设置了 DF 位的数据包。使用 **set ip df** 命令可清除 DF 位并允许对数据包进行分段和发送。分段会降低在网络中转发数据包的速度，但是可以使用访问列表限制已清除 DF 位的数据包的数量。

1. 可能导致 PMTUD 不起作用的问题有以下三个：中间路由器可能会丢弃数据包而不响应 ICMP 消息。这在 Internet 中并不十分常见，但在路由器配置为不响应 ICMP 不可达消息的网络内可能很常见。中间路由器可能会响应 ICMP 不可达消息，但在返回流中，防火墙阻止此消息。这是一种更加常见的情况。ICMP 不可达消息使其返回源，但源会忽略分段消息。这是三种问题

中最少见的一种。如果遇到第一个问题，可以清除源在 IP 报头中放置的 DF 位，也可以手动调整 TCP MSS 大小。要清除 DF 位，中间路由器必须将该值从 1 更改为 0。通常会在数据包离开网络之前由网络中的路由器完成此操作。下面是在基于 IOS 的路由器上执行此操作的一种简单代码配置：

```
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 隧道**默认情况下，路由器不对自己生成的 GRE 隧道数据包执行 PMTUD。要在 GRE 隧道接口启用 PMTUD，并使路由器参与针对通过隧道的数据流进行的源/目标设备 MTU 调整过程，应使用以下配置：Router (config) # interface tunnel tunnel_#Router (config-if) # tunnel path-mtu-discovery**tunnel path-mtu-discovery** 命令为路由器的 GRE 隧道接口启用 PMTUD。可选的 age-timer 参数用于指定隧道接口重置发现的最大 MTU 大小（减去 GRE 报头的 24 字节）之前的分钟数。如果为计时器指定 *infinite*，则不使用计时器。min-mtu 参数用于指定组成 MTU 值的最小字节数。
3. **PIX/ASA 7.x - 清除不分段 (DF)** 或处理大文件或数据包。您仍然无法通过隧道正确访问 Internet、大文件或应用程序，因为它显示以下 MTU 大小错误消息：

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

为解决此问题，一定要从设备的外部接口清除 DF 位。在全局配置模式下使用 **crypto ipsec df-bit** 命令配置 IPSec 数据包的 Df 位策略。

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

具有 IPSec 隧道功能的 DF 位可用于指定安全设备能否清除、设置或复制封装的报头中的不分段 (DF) 位。IP 报头中的 DF 位确定是否允许设备对数据包进行分段。在全局配置模式下使用 **crypto ipsec df-bit** 命令可配置安全设备以指定封装报头中的 DF 位。在封装隧道模式 IPSec 数据流时，应对 DF 位使用 clear-df 设置。此设置允许设备发送大于可用 MTU 大小的数据包。此外，如果不知道可用 MTU 大小，也可以采用此设置。

注意： 如果仍然存在分段问题和数据包丢失，您还可以选择使用 **ip mtu tunnel interface** 命令手动调整 MTU 大小。在这种情况下，路由器会在保护数据包之前对其进行分段。此命令可以与 PMTUD 和/或 TCP MSS 结合使用。

验证

当前没有可用于此配置的验证过程。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

VPN 加密错误

假设已在路由器与 PIX 之间建立 IPSec 隧道。如果显示数据包丢失的加密错误消息，可完成下列步骤以解决此问题：

1. 执行从客户端到服务器的嗅探器跟踪，以查找可用的最佳 MTU。此外，也可以使用 ping 测试：

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

   192.168.1.1 是远程计算机的 IP 地址。
2. 继续以 20 为幅度降低 1400 值，直到出现应答为止。**注意：** 在大多数情况下，有效的值是 1300。
3. 达到适当的最大段大小后，针对使用中的设备适当调整该值：在 PIX 防火墙上：

   ```
   sysopt connection tcpmss 1300
   ```

   在路由器上：

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

RDP 和 Citrix 的问题

问题：

可以在 VPN 网络之间执行 ping 命令，但无法建立通过隧道的远程桌面协议 (RDP) 和 Citrix 连接。

解决方案：

可能是 PIX/ASA 后的 PC 的 MTU 大小存在问题。将客户端计算机的 MTU 大小设置为 1300，然后尝试建立通过 VPN 隧道的 Citrix 连接。

相关信息

- 解决 GRE 和 IPSEC 中的 IP 分段、MTU、MSS 和 PMTUD 问题
- PIX/ASA 7.0 问题：超出 MSS - HTTP 客户端无法浏览某些网站
- 最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案
- 使用 GRE 隧道时为什么不能访问 Internet
- 技术支持和文档 - Cisco Systems