PIX/ASA 7.x e IO: Fragmentação VPN

Índice

Introdução

Este documento acompanha as etapas necessárias para reduzir os problemas que podem ocorrer com a fragmentação de um pacote. Um exemplo de problemas de fragmentação é a capacidade para fazer ping de um recurso em rede, mas a incapacidade de se conectar à mesma característica com um aplicativo específico, como e-mails ou bancos de dados.

Pré-requisitos

Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

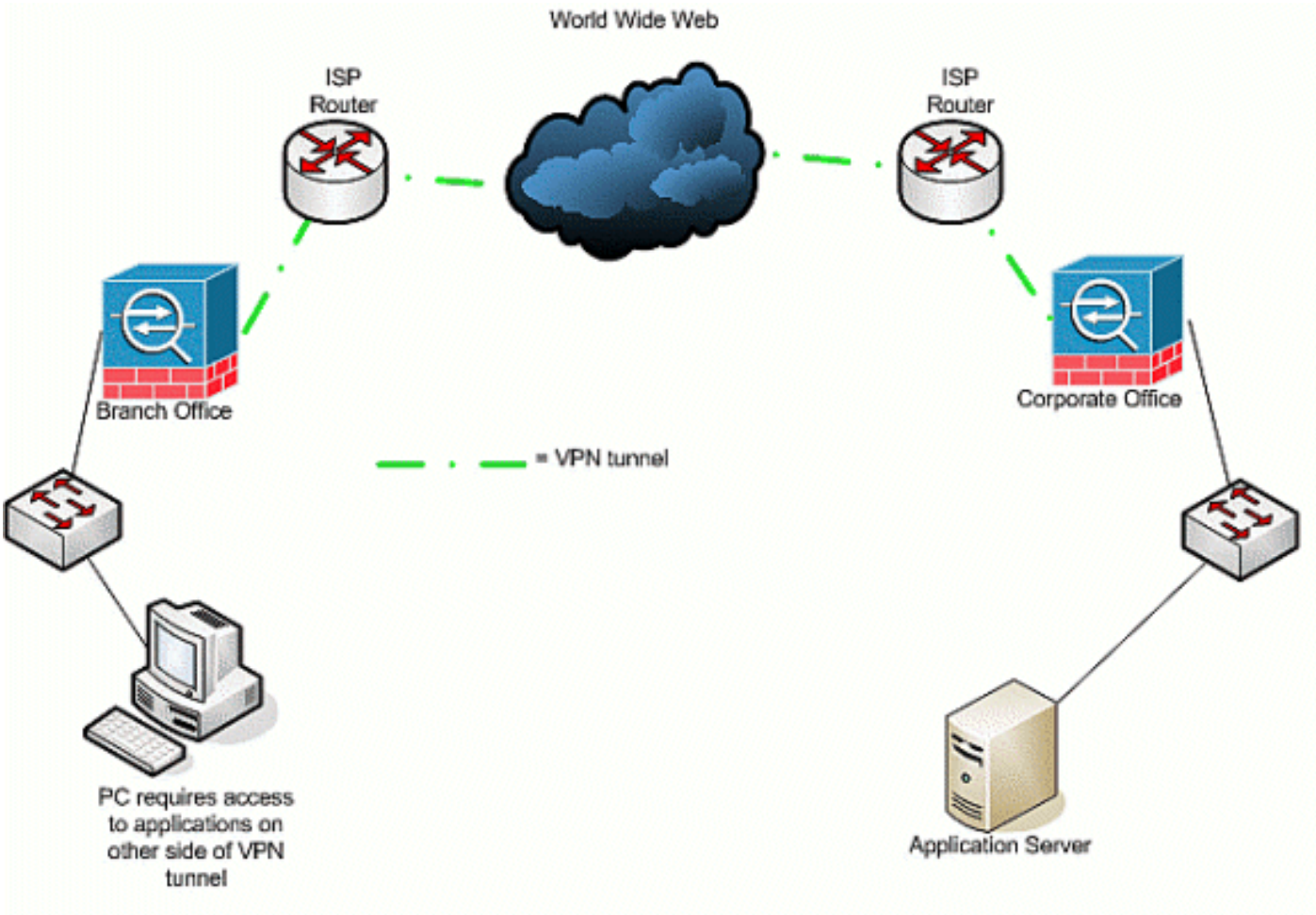
- Conectividade entre pares VPN

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Produtos Relacionados

Esta configuração também pode ser utilizada com estas versões de hardware e software:

- IOS Router
- Dispositivos de segurança PIX/ASA

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

O IP apoia um comprimento máximo de 65,536 bytes para um pacote IP, mas a maioria de protocolos de camada de link de dados apoiam um comprimento muito menor, chamado uma unidade de transmissão máxima (MTU). Baseado no MTU apoiado, pode ser necessário quebrar acima (fragmento) um pacote IP para transmiti-lo através de um tipo de mídia particular da camada de link de dados. O destino então tem que remontar os fragmentos de novo no pacote IP original, completo.

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

Quando você usa um VPN para proteger dados entre dois pares VPN, as despesas gerais adicionais estão adicionadas aos dados originais, que podem exigir que a fragmentação ocorre. Campos desta lista da tabela que potencialmente têm que ser adicionados aos dados protegidos a fim apoiar uma conexão de VPN. Note que os protocolos múltiplos podem ser necessários, que aumenta o tamanho do pacote original. Por exemplo, se você usa uma conexão IPSec L2L DMVPN entre dois roteadores Cisco, onde você executou um túnel GRE, você precisa estas despesas gerais adicionais: ESP, GRE, e o cabeçalho IP exterior. Se você tem uma conexão do cliente de software do IPsec a um gateway de VPN quando o tráfego atravessa um dispositivo do endereço, você precisa estas despesas gerais adicionais para a tradução de endereço de rede Traversal (NAT-T), assim como o cabeçalho IP exterior para a conexão do modo de túnel.

Edições com fragmentação

Quando a fonte envia um pacote a um destino, coloca um valor no campo dos flags de controle dos cabeçalhos IP que afeta a fragmentação do pacote por dispositivos intermediários. O flag de controle é três bit por muito tempo, mas os somente o primeiros dois são usados na fragmentação. Se o segundo bit é ajustado a 0, o pacote está permitido ser fragmentado; se é ajustado a 1, o pacote não está permitido ser fragmentado. O segundo bit é normalmente chamado de bit *Don't Fragment* (DF). O terceiro bit especifica quando a fragmentação ocorre, mesmo se este pacote fragmentado é o último fragmento (ajuste a 0), ou se há mais fragmentos (ajuste a 1) que compõem o pacote.

Há quatro áreas que podem criar problemas quando a fragmentação é exigida:

- As despesas gerais adicionais nos ciclos de CPU e na memória são exigidas pelos dois dispositivos que executam a fragmentação e a remontagem.
- Se um fragmento é deixado cair na maneira ao destino, o pacote não pode ser remontado e o pacote inteiro deve ser fragmentado e enviado outra vez. Isto cria problemas de ritmo de transferência adicionais, especialmente nas situações onde o tráfego na pergunta é limite de taxa, e a fonte envia o tráfego acima do limite permissível.
- O filtragem de pacote de informação e os firewall stateful podem ter a dificuldade que

processa os fragmentos. Quando a fragmentação ocorre, o primeiro fragmento contém um cabeçalho IP exterior, o cabeçalho interno, tal como o TCP, o UDP, o ESP e o outro, e parte do payload. Os fragmentos subsequentes do pacote original contratam um cabeçalho IP exterior e a continuação do payload. O problema com este processo é que determinados Firewall precisam de ver a informação de cabeçalho interno em cada pacote a fim fazer decisões de filtração inteligentes; se essa informação falta, inadvertidamente podem deixar cair todos os fragmentos, à exceção do primeiro.
- A fonte no cabeçalho IP do pacote pode ajustar o terceiro controle mordido ao *Don't Fragment*, assim que significa que, se um dispositivo intermediário recebe o pacote e deve o fragmentar, o dispositivo intermediário não pode o fragmentar. Em lugar de, o dispositivo intermediário deixa cair o pacote.

Tarefa principal

Descubra a fragmentação

A maioria de redes usam Ethernet, com um valor do MTU padrão de 1,500 bytes, que seja usado tipicamente para pacotes IP. A fim encontrar se a fragmentação ocorre ou é precisada mas não pode ser feita (o bit DF está ajustado), traga primeiramente sua sessão de VPN acima. Então você pode usar qualquer destes quatro procedimentos para descobrir a fragmentação.

1. Sibile um dispositivo encontrado no extremo oposto. Isto é sob a suposição que sibilar está permitido através do túnel. Se isto é bem sucedido, tente alcançar um aplicativo através do mesmo dispositivo; por exemplo, se um server do email ou do Desktop remoto de Microsoft é através do túnel, a probabilidade aberta e tenta transferir seu email, ou tenta ao Desktop remoto ao server. Se isto não trabalha, e você tem a resolução de nome correta, há uma boa possibilidade que a fragmentação é a edição.
2. De um dispositivo de Windows use isto: C:\ **> sibilo - f - l destination_IP_address dos packet_size_in_bytes**.**- A** opção **f** é usada para especificar que o pacote não pode ser fragmentado. **- L** opção é usado para especificar o comprimento do pacote. Tente primeiramente isto com um tamanho do pacote de 1,500. Por exemplo, sibilo **- f - l 1500 192.168.100**. Se a fragmentação é exigida mas não pode ser executada, você recebe uma mensagem tal como este: *Os pacotes precisam de ser fragmentados mas grupo DF*.
3. Nos roteadores Cisco, execute o comando **debug ip icmp** e use o comando **extended ping**. Se você vê o *ICMP: dst (x.x.x.x) a fragmentação necessária e o DF se ajustar, inacessível enviado ao y.y.y.y, onde x.x.x.x* é um dispositivo de destino, e o y.y.y.y são seu roteador, um dispositivo intermediário diz-lhe que que a fragmentação está precisada, mas porque você ajusta o DF mordido na requisição de eco, um dispositivo intermediário não pode fragmentá-lo a fim enviá-lo ao salto seguinte. Neste caso, diminua gradualmente o tamanho do MTU dos sibilos até que você encontre um que trabalha.
4. Em dispositivos do Cisco Security, use um filtro da captação.ciscoasa(config)#access-list outside_test permit tcp any host 172.22.1.1 eq 80**Note**: Quando você deixa a fonte como *alguns*, permite que o administrador monitore todas as traduções de endereço de rede (NAT).ciscoasa(config)#access-list outside_test permit tcp host 172.22.1.1 eq 80 any**Note**: Quando você inverte a informação de origem e de destino, permite que o tráfego de retorno esteja capturado.`a relação a mais outside_test da lista de acesso do outside_interface da captação do ciscoasa(config)# fora`O usuário precisa de iniciar uma

sessão nova com aplicativo X. Depois que o usuário iniciou uma sessão do aplicativo novo X, o administrador ASA precisa de emitir o comando do **outside_interface da captação da mostra**.

Soluções às edições de Framentation

Há umas maneiras diferentes que você pode resolver edições com fragmentação. Estes são discutidos nesta seção.

Método 1: Configuração MTU estática

A configuração MTU estática pode resolver edições com fragmentação.

1. **O MTU muda no roteador:**Note que se você ajusta manualmente o MTU no dispositivo, diz o dispositivo, que atua como um gateway de VPN, para fragmentar pacotes recebidos antes que os proteja e envie através do túnel. Isto é preferível a ter o roteador protege o tráfego e fragmenta-o então, mas o dispositivo fragmenta-o.**aviso:** Se você muda o tamanho do MTU em qualquer relação de dispositivo, causa todos os túneis terminados nessa relação a ser rasgada para baixo e reconstruído.Em roteadores Cisco, use o **mtucommand IP** para ajustar o tamanho do MTU na relação onde o VPN é terminado:
```
router (config)# interface type [slot_#/] port_#
router (config-if)# ip mtu MTU_size_in_bytes
```

2. **O MTU muda no ASA/PIX:**Em dispositivos ASA/PIX, use o **mtucommand** para ajustar o tamanho do MTU no modo de config global. À revelia, o MTU é ajustado a 1500. Por exemplo, se você teve uma relação em sua ferramenta de segurança que foi nomeada *Parte externa (onde o VPN é terminado)*, e você determinou (com as medidas alistadas na seção da fragmentação da descoberta) que você quis usar 1380 como o tamanho do fragmento, usa este comando:
```
security appliance (config)# mtu Outside 1380
```

Método 2: Maximum Segment Size TCP

O Maximum Segment Size TCP pode resolver edições com fragmentação.

Note: Esta característica trabalha somente com TCP; outros protocolos IP têm que usar uma outra solução para resolver problemas da fragmentação de IP. Mesmo se você ajusta o MTU IP no roteador, não afeta o que os dois host finais negociam dentro do cumprimento de três vias TCP com o TCP MSS.

1. **O MSS muda no roteador:**A fragmentação ocorre com tráfego TCP porque o tráfego TCP é usado normalmente para transportar grandes quantidades de dados. O TCP apoia uma característica chamada o Maximum Segment Size TCP (MSS) que permita que os dois dispositivos negociem um tamanho apropriado para o tráfego TCP. O valor MSS é configurado estaticamente em cada dispositivo e representa o tamanho de buffer para usar-se para um pacote previsto. Quando dois dispositivos estabelecem conexões de TCP comparam o valor local MSS com o valor local MTU dentro do cumprimento de três vias; qualquer é mais baixo é enviado ao peer remoto. Os dois pares usam então o mais baixo

dos dois valores trocados. A fim configurar esta característica, faça isto:Nos roteadores Cisco, use o comando **tcp adjust-mss** na interface em que a VPN é terminada.

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

2. **O MSS muda no ASA/PIX:**A fim assegurar-se de que o tamanho do segmento do máximo TCP não exceda o valor que você se ajusta e que o máximo é não menos que um tamanho especificado, use o **comando connection do sysopt no** modo de config global. A fim restaurar a configuração padrão, use o formulário do theno deste comando. O máximo padrão de valor é 1380 bytes. Os recursos mínimos são desabilitados à revelia (ajuste a 0).A fim mudar o máximo padrão do limite MSS, faça isto:

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

   Note: Se você ajusta o tamanho máximo para ser maior de 1380, os pacotes podem tornar-se fragmentados, dependente do tamanho do MTU (que é 1500 à revelia). Um grande número fragmentos podem impactar o desempenho da ferramenta de segurança quando usa os recursos de proteção de Frag. Se você ajusta o tamanho mínimo, impede que o servidor TCP envie muitos pacotes de dados pequenos TCP ao cliente e impacte o desempenho do server e da rede.A fim mudar o limite do mínimo MSS, faça isto:

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

   security appliance (config)**#** sysopt connection tcp-mss minimum MSS_size_in_bytes**Note**: Refira a configuração MPF para permitir os pacotes que excedem a seção MSS da edição do documento PIX/ASA 7.X: MSS excedido - Os clientes HTTP não podem consultar a alguns sites para mais informação a fim permitir aos pacotes excedidos MSS um outro método.

Método 3: Path MTU Discovery (PMTUD)

O PMTUD pode resolver edições com fragmentação.

O problema principal com TCP MSS é que o administrador tem que saber que valor a configurar em seu roteador para impedir a ocorrência da fragmentação. Este pode ser um problema se mais de um trajeto existe entre você e o lugar remoto VPN, ou, quando você faz sua pergunta inicial, você encontra que segundo-ou um MTU terceiro-mais pequeno, em vez do menor, está baseado na decisão de roteamento usada dentro de sua pergunta inicial. Com PMTUD, você pode determinar um valor MTU para pacotes IP que evite a fragmentação. Se os mensagens ICMP são obstruídos por um roteador, o MTU de caminho é quebrado, e os pacotes com o jogo do bit DF são rejeitados. Use o **comando df do grupo IP** cancelar o DF mordido e permitir que o pacote seja fragmentado e enviado. A fragmentação pode retardar a velocidade do encaminhamento de pacote na rede, mas as Listas de acesso podem ser usadas para limitar o número de pacotes em que o bit DF é cancelado.

1. Três edições podem fazer com que o PMTUD não funcione:Um roteador intermediário pode deixar cair o pacote e não responder com um mensagem ICMP. Isto não é muito comum no Internet, mas pode ser comum dentro de uma rede onde o Roteadores seja configurado para não responder com mensagens que não chega a seu destino do ICMP.Um roteador intermediário pode responder com um mensagem que não chega a seu destino do ICMP, mas, no fluxo do retorno, um Firewall obstrui esta mensagem. Esta é uma ocorrência mais comum.O mensagem que não chega a seu destino do ICMP faz sua maneira de volta à

fonte, mas a fonte ignora a mensagem da fragmentação. Este é o mais raro das três edições.Se você experimenta a primeira edição, você poderia qualquer um cancelar o DF mordido no cabeçalho IP que a fonte colocada lá ou ajusta manualmente o tamanho TCP MSS. Para limpar o bit DF, um roteador intermediário deve alterar o valor de 1 para 0. Normalmente, isso é feito por um roteador em sua rede antes do pacote sair da rede. Esta é uma configuração simples do código que faça esta em um roteador baseado em 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 e túneis GRE**Àrevelia, um roteador não executa o PMTUD nos pacotes de túnel GRE que gerencie próprio. A fim permitir o PMTUD em interfaces do túnel GRE e mandar o roteador participar no processo de ajustamento MTU para a fonte/dispositivos de destino para o tráfego que atravessa o túnel, use esta configuração:Roteador (configuração) # tunnel_# do `túnel da relação`Router (config-if) # tunnel path-mtu-discovery**O comando tunnel path-mtu-discovery** permite o PMTUD para a interface do túnel GRE de um roteador. O parâmetro opcional do temporizador de duração especifica o número de minutos depois do qual a interface de túnel restaura o tamanho do MTU máximo descoberto, menos 24 bytes para o cabeçalho de GRE. Se você especifica *infinito* para o temporizador, o temporizador não está usado. O parâmetro minuto-MTU especifica o número mínimo de bytes que compreende o valor MTU.
3. **PIX/ASA 7.x - Limpeza do Bit Don't Fragment (DF)** ou manuseio de arquivos grandes ou pacotes.Você ainda não é capaz de acessar adequadamente a Internet, arquivos grandes ou aplicativos por meio do túnel devido à seguinte mensagem de erro de tamanho de MTU:

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

   Para resolver esse problema, certifique-se de limpar o bit DF da interface externa do dispositivo. Configure a política de bit DF para pacotes IPSec com o comando **crypto ipsec df-bit** no modo de configuração global.

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

   O bit DF com recurso de túneis de IPSec permite especificar se o security appliance pode limpar, definir ou copiar o bit Don't Fragment (DF) do cabeçalho encapsulado. O bit DF no cabeçalho IP determina se um dispositivo tem permissão para fragmentar um pacote.Use o comando **crypto ipsec df-bit** no modo de configuração global para configurar o security appliance para especificar o bit DF em um cabeçalho encapsulado.Ao encapsular o tráfego IPSec no modo de túnel, use a configuração clear-df para o bit DF. Esta configuração permite que o dispositivo envie pacotes maiores que o tamanho da MTU disponível. Esta configuração também é apropriada se você não conhece o tamanho da MTU disponível.

Note: Se você ainda experimenta questões de fragmentação e pacotes descartado, opcionalmente, você pode manualmente ajustar o tamanho do MTU com o comando da **interface de túnel MTU IP**. Neste caso, o roteador fragmenta o pacote antes que o proteja. Este comando pode ser usado conjuntamente com PMTUD e/ou TCP MSS.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Troubleshooting

Erro de criptografia de VPN

Suponha que o túnel IPSec tenha sido estabelecido entre o roteador e o PIX. Se houver mensagens de erro de criptografia informando que pacotes foram perdidos, siga estes passos para resolver o problema:

1. Execute um rastreamento de varredura do cliente para o servidor para descobrir qual é a melhor MTU a ser usada.Você também pode usar o teste de ping:

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

   192.168.1.1 é um endereço IP do computador remoto.
2. Continue a reduzir o valor de 1400 de 20 em 20 até receber uma resposta.**Note**: O valor mágico, que trabalha na maioria de exemplos, é 1300.
3. Após o tamanho máximo apropriado do segmento ser atingido, ajuste-o adequadamente para os dispositivos em uso:On the PIX Firewall:

   ```
   sysopt connection tcpmss 1300
   ```

   No roteador:

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

Problemas de RDP e Citrix

Problema:

É possível enviar pings entre as redes VPN, mas o Remote Desktop Protocol (RDP) e as conexões Citrix não podem ser estabelecidas pelo túnel.

Solução:

O problema pode ser o tamanho da MTU no PC por trás do PIX/ASA. Defina o tamanho da MTU como 1300 para o computador cliente e tente estabelecer a conexão Citrix pelo túnel VPN.

Informações Relacionadas

- Fragmentação de IP da resolução, edições MTU, MSS, e PMTUD com GRE e IPSEC
- Problema PIX/ASA 7.0: MSS Excedido - Os Clientes HTTP não Podem Consultar Alguns

Web Sites

- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Porque não posso eu consultar o Internet ao usar um túnel GRE
- Suporte Técnico e Documentação - Cisco Systems