Conexões de permissão PPTP/L2TP com o PIX/ASA/FWSM

Índice

Introdução

Este documento discute a configuração exigida no Cisco Security Appliance/FWSM para permitir que um cliente do protocolo de tunelamento do Point-to-Point Tunneling Protocol (PPTP) /Layer 2 (L2TP) conecte a um servidor de PPTP com o Network Address Translation (NAT).

O FWSM 3.1.x e uns apoios mais atrasados PPTP passa completamente com PANCADINHA. Use a inspeção de PPTP a fim permitir esta funcionalidade.

Nota: Use a mesma configuração do PIX para o FWSM.

Refira configurar o firewall PIX segura Cisco para usar o PPTP a fim configurar uma ferramenta de segurança para aceitar conexões PPTP.

A fim configurar o L2TP sobre a Segurança IP (IPsec) dos clientes remotos de Microsoft Windows 2000/2003 e de Windows XP a um escritório corporativo da ferramenta de segurança PIX/ASA que usam chaves pré-compartilhada com Internet de Microsoft Windows 2003, refira o L2TP sobre o IPsec entre o exemplo de configuração de utilização de Windows 2000/XP PC e da chave pré-compartilhada PIX/ASA 7.2.

Pré-requisitos

Requisitos

A fim tentar esta configuração, você deve ter um servidor de PPTP e um cliente de trabalho antes que você envolva o PIX/ASA/FWSM.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Versões 6.x e mais recente do Cisco PIX Firewall
- Ferramenta de segurança do 5500 Series de Cisco ASA que executa a versão 7.x ou mais recente
- FWSM que executa a versão 3.1.x ou mais recente

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Material de Suporte

O PPTP é descrito no RFC 2637. Este protocolo usa uma conexão de TCP que use a porta 1723 e uma extensão do Generic Routing Encapsulation (GRE) [protocolo 47] para levar os dados reais (quadro PPP). A conexão de TCP é iniciada pelo cliente, seguido pela conexão GRE que é iniciada pelo server.

Informação de versão 6.2 e anterior

Porque a conexão PPTP é iniciada porque o TCP em uma porta e na resposta é protocolo GRE, o algoritmo de segurança de adaptação (ASA) PIX não sabe que os fluxos de tráfego são relacionados. Em consequência, é necessário configurar ACL para permitir o tráfego de retorno no PIX. O PPTP com o PIX com NAT (mapeamento de endereço linear) trabalha porque o PIX usa a informação de porta no encabeçamento TCP ou de User Datagram Protocol (UDP) para se manter a par da tradução. O PPTP com o PIX com tradução de endereço de porta (PAT) não trabalha porque não há nenhum conceito das portas no GRE.

Informação de versão 6.3

A característica dos PPTP fixup na versão 6.3 permite que o tráfego PPTP atravesse o PIX quando configurada para a PANCADINHA. A inspeção do pacote de PPTP do stateful é

executada igualmente no processo. **O comando fixup protocol pptp** inspeciona pacotes de PPTP e cria dinamicamente as conexões GRE e as traduções necessárias permitir o tráfego PPTP. Especificamente, o Firewall inspeciona os anúncios de versão do PPTP e o Outgoing Call ReQuest/sequência da resposta. Somente a versão de PPTP 1, como definido no RFC 2637, é inspecionada. Uma inspeção mais adicional no canal de controle TCP é desabilitada se a versão anunciada por um ou outro lado não é a versão 1. além, o Outgoing Call ReQuest e a sequência da resposta é seguida. As conexões e/ou as traduções são atribuídas dinamicamente como necessário para permitir o tráfego de dados secundário subsequente GRE. A característica dos PPTP fixup deve ser permitida para que o tráfego PPTP seja traduzido pela PANCADINHA.

Informação de versão 7.x

O motor da inspeção de aplicativo PPTP na versão 7.x opera-se na mesma forma que o **pptp do fixup protocol** faz na versão 6.3.

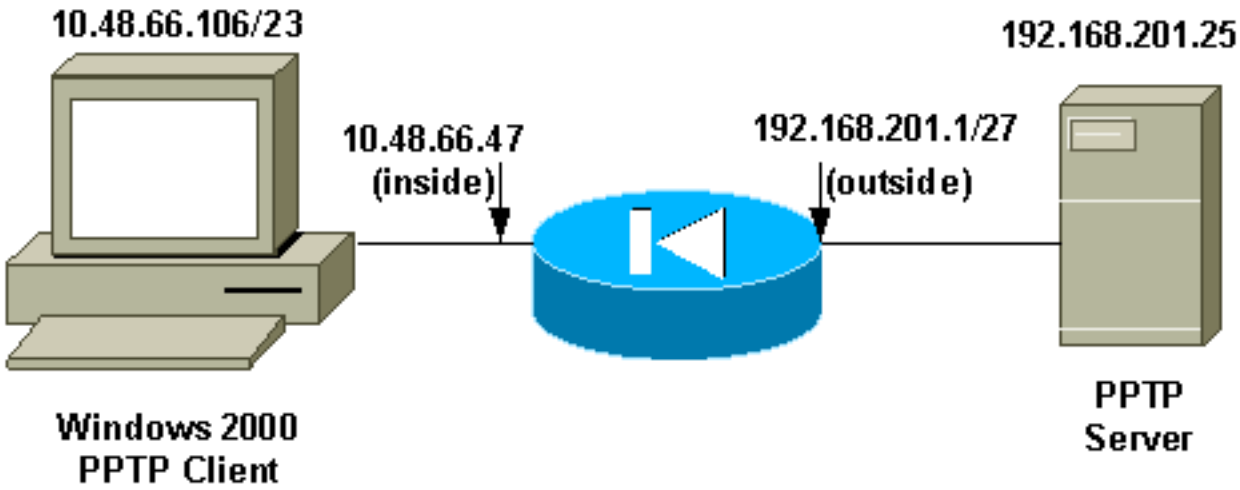
Convenções

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

PPTP com o cliente dentro e servidor de fora

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Comandos adicionar para a versão 6.2 e anterior

Termine estas etapas aos comandos add para a versão 6.2:

1. Defina o mapeamento estático para o PC interno. O endereço considerado na parte externa é 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106`**

netmask 255.255.255.255 0 0

2. Configurar e aplique o ACL para permitir o tráfego de retorno GRE do servidor de PPTP ao cliente de PPTP.`pixfirewall(config)#`**access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5**
3. Aplique o ACL.`pixfirewall(config)#`**access-group acl-out in interface outside**

Comandos para adicionar para a versão 6.3

Termine estas etapas aos comandos add para a versão 6.3:

1. Permita o pptp 1723 do fixup protocol usando este comando.`pixfirewall(config)#`**fixup protocol pptp 1723**
2. Você não precisa de definir um mapeamento estático porque o protocolo dos PPTP fixup é permitido. Você pode usar a PANCADINHA.`pixfirewall(config)#`**nat (inside) 1 0.0.0.0 0.0.0.0 0 0** `pixfirewall(config)#`**global (outside) 1 interface**

Comandos adicionar para versões 7.x e 8.0 usando a inspeção

Termine estas etapas aos comandos add para versões 7.x e 8.0 usando o **comando inspect**:

1. Adicionar a inspeção de PPTP ao mapa de política do padrão usando o mapa de classe do padrão.`pixfirewall(config)#`**policy-map global_policy** `pixfirewall(config-pmap)#`**class inspection_default** `pixfirewall(config-pmap-c)#`**inspect pptp**
2. Você não precisa de definir um mapeamento estático porque o PIX inspeciona agora o tráfego PPTP. Você pode usar a PANCADINHA.`pixfirewall(config)#`**nat (inside) 1 0.0.0.0 0.0.0.0 0 0** `pixfirewall(config)#`**global (outside) 1 interface** OU

Comandos adicionar para versões 7.x e 8.0 usando o ACL

Termine estas etapas aos comandos add para versões 7.x e 8.0 usando o ACL.

1. Defina o mapeamento estático para o PC interno. O endereço considerado na parte externa é 192.168.201.5.`pixfirewall(config)#`**static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0**
2. Configurar e aplique o ACL para permitir o tráfego de retorno GRE do servidor de PPTP ao cliente de PPTP.`pixfirewall(config)#`**access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5** `pixfirewall(config)#`**access-list acl-out permit tcp host 192.168.201.25 host 192.168.201.5 eq 1723**
3. Aplique o ACL.`pixfirewall(config)#`**access-group acl-out in interface outside**

Configuração para versões 6.2 e anteriores

Configuração de PIX - Cliente para dentro, server fora
`pixfirewall(config)#`**write terminal** Building configuration... : Saved : PIX Version 6.2(1) nameif ethernet0 outside security0 nameif ethernet1 inside security100 nameif ethernet2 intf2 security10 enable password Ujkil6aDv2yp6suI encrypted passwd OnTrBUG1Tp0edmkr encrypted hostname pixfirewall domain-name cisco.com fixup protocol ftp 21 fixup protocol http 80 fixup protocol h323 h225 1720 fixup protocol h323 ras 1718-1719 fixup protocol ils 389 fixup protocol rsh 514

```
fixup protocol rtsp 554 fixup protocol smtp 25 fixup
protocol sqlnet 1521 fixup protocol sip 5060 fixup
protocol skinny 2000 no names !--- This line allows GRE
traffic from the !--- PPTP server to the client. access-
list acl-out permit gre host 192.168.201.25 host
192.168.201.5 pager lines 24 logging on logging console
debugging logging trap debugging interface ethernet0
auto interface ethernet1 auto interface ethernet2 auto
shutdown mtu outside 1500 mtu inside 1500 mtu intf2 1500
ip address outside 209.165.201.1 255.255.255.224 ip
address inside 10.48.66.47 255.255.254.0 ip address
intf2 127.0.0.1 255.255.255.255 ip audit info action
alarm ip audit attack action alarm no failover failover
timeout 0:00:00 failover poll 15 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0 pdm history enable arp
timeout 14400 !--- This allows traffic from a low
security interface to !--- a high security interface.
static (inside,outside) 192.168.201.5 10.48.66.106
netmask 255.255.255.255 0 0 !--- This applies the ACL to
the outside interface. access-group acl-out in interface
outside timeout xlate 3:00:00 timeout conn 1:00:00 half-
closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 sip
0:30:00 sip_media 0:02:00 timeout uauth 0:05:00 absolute
uauth 0:04:00 inactivity aaa-server TACACS+ protocol
tacacs+ aaa-server RADIUS protocol radius aaa-server
LOCAL protocol local no snmp-server location no snmp-
server contact snmp-server community public snmp-server
enable traps no floodguard enable no sysopt route dnat
telnet timeout 5 ssh timeout 5 terminal width 80
Cryptochecksum:18bdf8e21bd72ec0533795549165ecf5 : end
[OK]
```

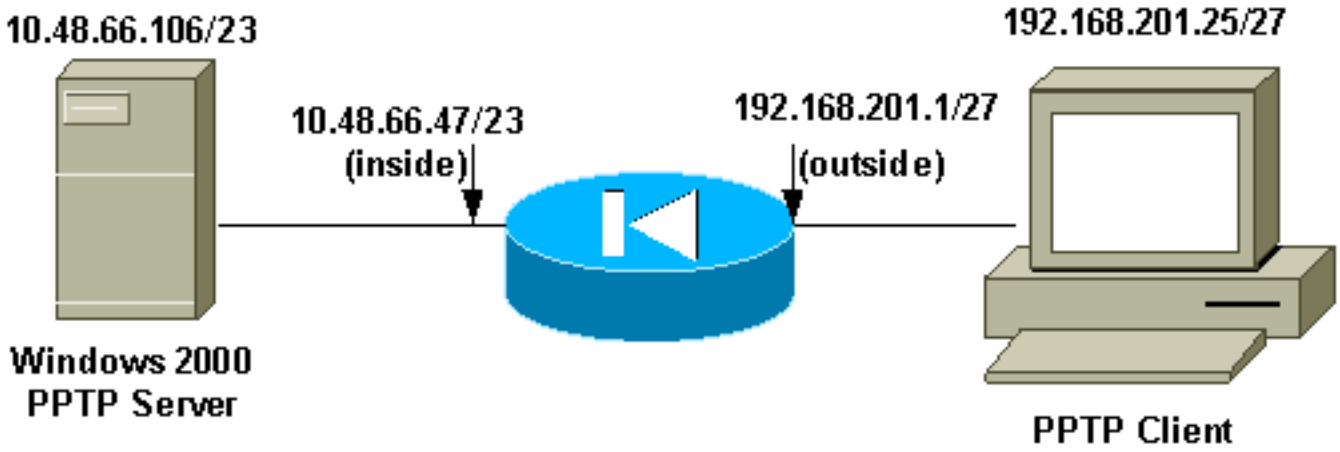
L2TP com o cliente dentro e servidor de fora

Termine estes comandos add das etapas para as versões 7.x e 8.x que usam o ACL. (Esta configuração supõe que o cliente de PPTP e os endereços IP do servidor são o mesmo que para o cliente e servidor L2TP.)

1. Defina o mapeamento estático para o PC interno. O endereço considerado na parte externa é 192.168.201.5.`pixfirewall(config)#`**`static (inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0`**
2. Configurar e aplique o ACL para permitir o tráfego de retorno L2TP do server L2TP ao cliente L2TP.`pixfirewall(config)#`
   `pixfirewall(config)#`**`access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701`**
3. Aplique o ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

PPTP com cliente externo e servidor interno

Diagrama de Rede



Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços da RFC1918 que foram usados em um ambiente de laboratório.

Comandos a serem adicionados a todas as versões

Neste exemplo de configuração, o servidor de PPTP é 192.168.201.5 (estático a 10.48.66.106 para dentro), e o cliente de PPTP está em 192.168.201.25.

```
access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5 access-list acl-out permit
tcp host 192.168.201.25 host 192.168.201.5 eq 1723 static (inside,outside) 192.168.201.5
10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in interface outside
```

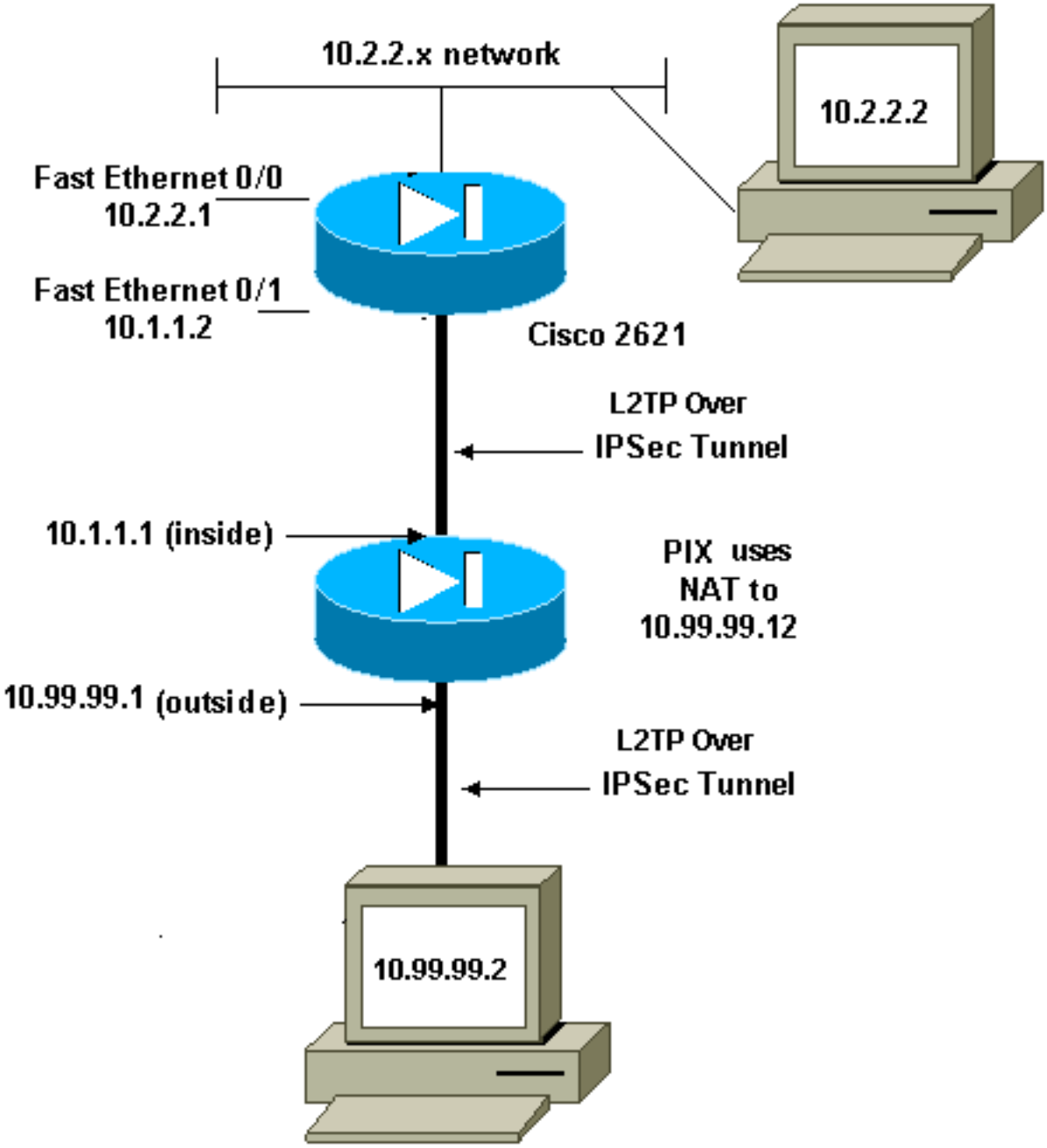
L2TP com o cliente de fora e servidor dentro

Neste exemplo de configuração, o server L2TP é 192.168.201.5 (estático a 10.48.66.106 para dentro), e o cliente L2TP está em 192.168.201.25. (Esta configuração supõe que o cliente de PPTP e os endereços IP do servidor são o mesmo que para o cliente e servidor L2TP.)

```
access-list acl-out permit udp host 192.168.201.25 host 192.168.201.5 eq 1701 static
(inside,outside) 192.168.201.5 10.48.66.106 netmask 255.255.255.255 0 0 access-group acl-out in
interface outside
```

Permita o L2TP sobre o IPsec com PIX/ASA 7.x e acima

O cliente exterior L2TP tenta estabelecer o L2TP sobre a conexão do IPSec VPN com o server interno L2TP. A fim permitir o L2TP sobre pacotes de IPsec com o PIX/ASA médio, você deve permitir que a porta 1701 ESP, de ISAKMP(500), NAT-T, e L2TP estabeleça o túnel. Os pacotes L2TP são traduzidos no PIX e enviados através do túnel VPN.




```
global (outside) 1 interface
nat (inside) 0 0.0.0.0 0.0.0.0
static (inside,outside) 10.99.99.12 10.1.1.2 netmask 255.255.255.255
access-group outside_access_in in interface outside

access-list outside_access_in remark Access Rule to Allow ESP traffic
access-list outside_access_in extended permit esp host 10.99.99.2
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow ISAKMP to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq isakmp
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 4500 (NAT-T) to
            host 10.99.99.12
access-list outside_access_in extended permit udp host 10.99.99.2 eq 4500
            host 10.99.99.12

access-list outside_access_in remark Access Rule to allow port 1701 (L2TP) to
            host 10.99.99.12
```

```
access-list outside_access_in extended permit udp host 10.99.99.2 eq 1701
            host 10.99.99.12
```

Verificar

Não há atualmente nenhum procedimento de verificação disponível para este documento.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

As conexões múltiplas PPTP/L2TP falham ao usar a PANCADINHA

Você pode somente ter uma conexão PPTP/L2TP através da ferramenta de segurança PIX quando você usa a PANCADINHA. Isto é porque a conexão GRE necessária é estabelecida sobre a porta 0 e o host somente dos mapas da ferramenta de segurança PIX da porta 0 a uma. A ação alternativa é permitir a inspeção de PPTP na ferramenta de segurança.

Erro 800 ao tentar conectar a PPTP VPN de entrada

Quando você tenta conectar a PPTP VPN de entrada, este Mensagem de Erro aparece:

```
Error 800: The remote connection was not made because the attempted VPN tunnels failed. The VPN
server might be unreachable. If this connection is attempting to use an L2TP/IPsec tunnel, the
security parameters required for IPsec negotiation might not be configured properly.
```

Esta edição ocorre geralmente quando a transmissão PPTP ou L2TP não é permitida no ASA intermediário entre o cliente e o dispositivo de fim de cabeçalho. Permita a transmissão PPTP ou L2TP e verifique a configuração a fim resolver a edição.

Comandos debug

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.

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Este exemplo mostra um cliente de PPTP dentro do PIX que inicia uma conexão a um servidor de PPTP fora do PIX quando não há nenhum ACL configurado para permitir o tráfego GRE. Com registro debugar no PIX, você pode ver o início de tráfego da porta TCP 1723 do cliente e a rejeição do tráfego de retorno do protocolo GRE 47.

```
pixfirewall(config)#loggin on pixfirewall(config)#loggin console 7 pixfirewall(config)#302013:
Built outbound TCP connection 4 for outside: 192.168.201.25 /1723 (192.168.201.25 /1723) to
inside:10.48.66.106/4644 (192.168.201.5 /4644) 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5 106010: Deny inbound protocol 47 src
outside:192.168.201.25 dst inside:192.168.201.5
```

Informações a serem coletadas se você abrir um pedido de serviço de TAC

Se você ainda precisa o auxílio após ter seguido os passos de Troubleshooting acima e o quer abrir um pedido do serviço com o tac Cisco, seja certo incluir a informação seguinte.
• Descrição do problema e detalhes relevantes de topologia • Troubleshooting realizado antes da abertura da solicitação de serviço • Saída do **comando show tech-support** • Saída do comando show log após a execução com o comando de depuração de registro colocado em buffer ou capturas do console que demonstram o problema (se disponível) Anexe os dados coletados à sua requisição de serviço em um texto não compactado e simples (.txt). Você pode anexar a informação a seu pedido do serviço transferindo arquivos pela rede o que usa a ferramenta de consulta do pedido do serviço (clientes registrados somente). Se você não pode alcançar a ferramenta de consulta do pedido do serviço, você pode enviar a informação em um anexo de Email a attach@cisco.com com seu número do pedido do serviço na linha de assunto de sua mensagem.

Informações Relacionadas

- Página de suporte do PPTP
- PIX/ASA 7.x e acima da passagem do túnel de IPsec com uma ferramenta de segurança com uso da lista de acessos e o MPF com exemplo da configuração de NAT
- Configurando um túnel de IPsec com um Firewall com NAT
- Cisco PIX Firewall Software
- Referências do comando Cisco Secure PIX Firewall
- Avisos de campo de produto de segurança (incluindo PIX)
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems