Conexiones de permiso PPTP/L2TP con el PIX/ASA/FWSM

Contenido

Introducción

Este documento discute la configuración requerida en el Cisco Security Appliance/FWSM para permitir que un cliente del Protocolo de Tunelización Point-to-Point Tunneling Protocol (PPTP) /Capa 2 (L2TP) se conecte con un servidor PPTP a través de la Traducción de Dirección de Red (NAT).

El FWSM versión 3.1.x y posteriores soporta la transferencia PPTP con PAT. Utilice la inspección PPTP para habilitar esta funcionalidad.

Nota: Utilice la misma configuración del PIX para el FWSM.

Consulte Configurar Cisco Secure PIX Firewall para utilizar el PPTP y configurar un security appliance para validar las conexiones PPTP.

Para configurar el L2TP sobre la seguridad IP (IPSec) de los clientes remotos de Microsoft Windows 2000/2003 y de Windows XP a una oficina corporativa de Security Appliance de PIX/ASA que utilizan claves previamente compartidas con Internet de Microsoft Windows 2003, consulte L2TP sobre el IPSec entre Windows 2000/XP PC y PIX/ASA 7.2 usando el Ejemplo de Configuración de claves previamente compartidas.

prerrequisitos

Requisitos

Para intentar esta configuración, debe tener un servidor PPTP que funcione y un cliente antes de incluir el PIX/ASA/FWSM.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco PIX Firewall Versiones 6.x y superiores
- Cisco ASA 5500 Series Security Appliance que ejecuta la versión 7.x o superiores
- FWSM que ejecuta la versión 3.1.x o superiores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Teoría Precedente

El PPTP se describe en RFC2637 . Este protocolo utiliza una conexión TCP que usa el puerto 1723 y una extensión del generic routing encapsulation (GRE) [protocolo 47] para transportar los datos reales (trama PPP). El cliente inicia la conexión TCP, luego el servidor inicia la conexión GRE.

Información de versión 6.2 y anteriores

Debido a que la conexión PPTP se inicia como TCP en un puerto y la respuesta es protocolo GRE, el PIX Adaptive Security Appliance (ASA) no sabe que los flujos de tráfico están relacionados. Como consecuencia, es necesario configurar las ACL para permitir el tráfico de retorno en el PIX. El PPTP a través del PIX con NAT (mapping de direcciones una a una) funciona porque el PIX utiliza la información de puerto en el TCP o User Datagram Protocol (UDP) para rastrear la traducción. El PPTP a través del PIX con la Traducción de Dirección de Puerto (PAT) no funciona porque no hay concepto de puertos en el GRE.

Información de la versión 6.3

La función Reparación de PPTP en la versión 6.3 permite que el tráfico PPTP atraviese el PIX

cuando está configurado para el paquete PPTP PAT. Stateful también se realiza una inspección en el proceso. El comando **fixup protocol pptp** examina los paquetes PPTP y crea dinámicamente las conexiones GRE y las traducciones necesarias para permitir el tráfico PPTP. Específicamente, el firewall examina los anuncios de versión de PPTP y la solicitud de llamada saliente/secuencia de respuesta. Solamente se examina el PPTP versión 1, según lo definido en el RFC2637. Se inhabilita la inspección adicional en el canal de control TCP si la versión anunciada por cualquier lado no es la Versión 1. además, la solicitud de llamada saliente y se rastrea la secuencia de respuesta. Las conexiones o las traducciones se asignan dinámicamente según sea necesario para permitir tráfico de datos secundario posteriorGRE. La función reparación de PPTP debe estar habilitada para que PAT traduzca el tráfico PPTP.

Información de la versión 7.x

El Motor de Inspección de Aplicaciones PPTP en la versión 7.x funciona de la misma manera que el **pptp del protocolo fixup** en la versión 6.3.

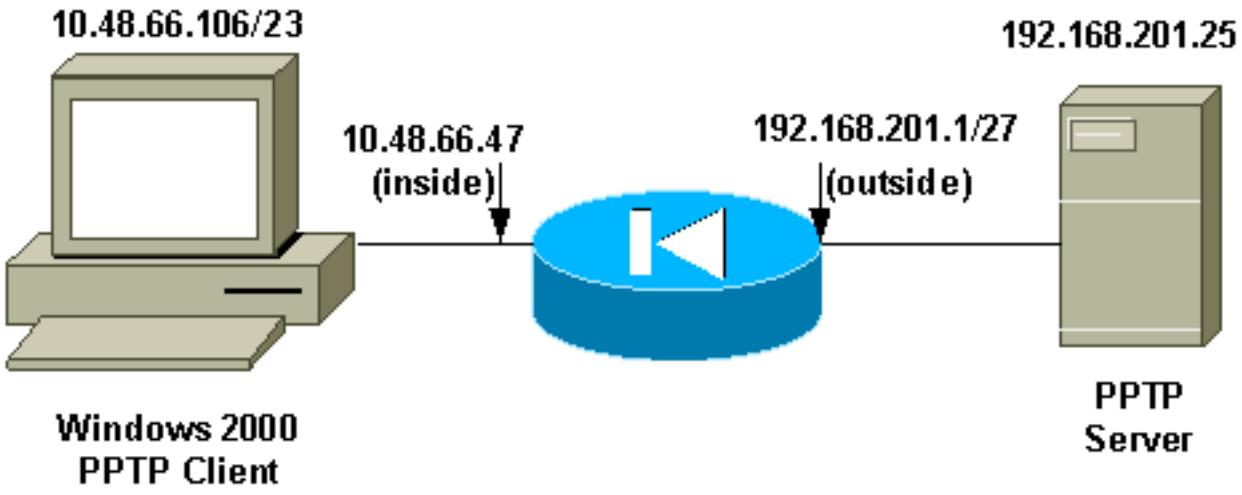
Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

PPTP con el Cliente Adentro y el Servidor Afuera

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Comandos que se agregarán para la versión 6.2 y anteriores

Siga estos pasos para agregar comandos para la versión 6.2:

1. Defina el mapping estático para la PC interior. La dirección que se muestra en el exterior es

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. Configure y aplique el ACL para permitir el tráfico de retorno GRE del servidor PPTP al cliente PPTP.`pixfirewall(config)#`**`access-list acl-out permit gre host 192.168.201.25 host 192.168.201.5`**
3. Aplique ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

Comandos que se agregarán para la versión 6.3

Complete estos pasos para agregar los comandos para la versión 6.3:

1. Habilite el protocolo fixup pptp 1723 con este comando.`pixfirewall(config)#`**`fixup protocol pptp 1723`**
2. No necesita definir un mapping estático porque el protocolo PPTP fixup está habilitado. Usted puede utilizar PAT.`pixfirewall(config)#`**`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`**
`pixfirewall(config)#`**`global (outside) 1 interface`**

Comandos que se agregarán para las versiones 7.x y 8.0 con inspección

Complete estos pasos para agregar los comandos para las versiones 7.x y 8.0 usando el comando **inspect**:

1. Agregue la inspección PPTP al policy-map predeterminado usando el class-map predeterminado.`pixfirewall(config)#`**`policy-map global_policy`** `pixfirewall(config-pmap)#`**`class inspection_default`** `pixfirewall(config-pmap-c)#`**`inspect pptp`**
2. No necesita definir un mapping estático porque el PIX ahora examina el tráfico PPTP. Usted puede utilizar PAT.`pixfirewall(config)#`**`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`**
`pixfirewall(config)#`**`global (outside) 1 interface`** O

Comandos que se agregarán para las versiones 7.x y 8.0 con ACL

Complete estos pasos para agregar los comandos para las versiones 7.x y 8.0 usando la ACL.

1. Defina el mapping estático para la PC interior. La dirección que se muestra en el exterior es 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. Configure y aplique el ACL para permitir el tráfico de retorno GRE del servidor PPTP al cliente 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 ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

Configuración para las versiones 6.2 y anteriores

Configuración PIX - Cliente Adentro, Servidor Afuera
`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]
```

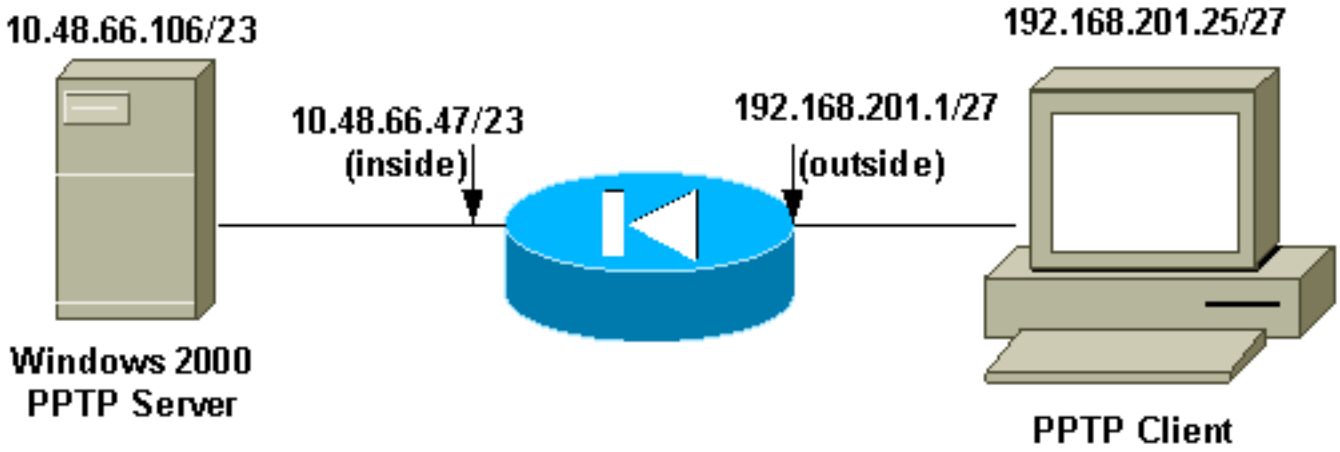
L2TP con el Cliente Adentro y el Servidor Afuera

Complete estos pasos para agregar los comandos para las versiones 7.x y 8.x que usan la ACL. (Esta configuración asume que el cliente PPTP y los dirección IP del servidor son lo mismo que para el cliente y servidor L2TP.)

1. Defina el mapping estático para la PC interior. La dirección que se muestra en el exterior es 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. Configure y aplique la ACL para permitir el tráfico de retorno L2TP del servidor L2TP al 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 ACL.`pixfirewall(config)#`**`access-group acl-out in interface outside`**

PPTP con el cliente afuera y el servidor adentro

Diagrama de la red



Nota: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son las direcciones RFC1918 que se han utilizado en un entorno de laboratorio.

Comandos que se agregarán a todas las versiones

En este ejemplo de configuración, el servidor PPTP es 192.168.201.5 (estático a 10.48.66.106 adentro), y el cliente PPTP está establecido en 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
```

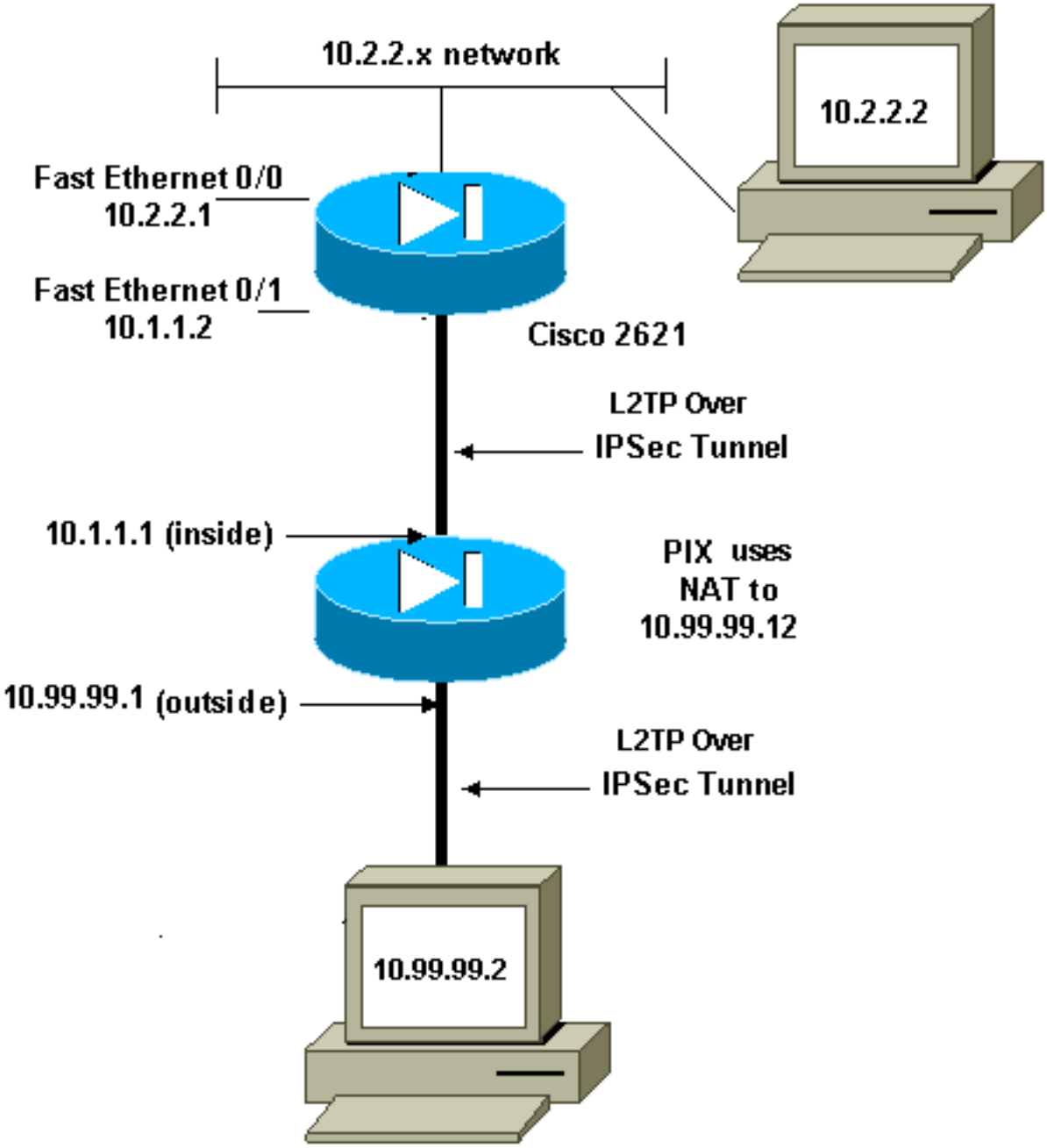
L2TP con el Cliente Afuera y el Servidor Adentro

En este ejemplo de configuración, el servidor L2TP es 192.168.201.5 (estático a 10.48.66.106 adentro), y el cliente L2TP está establecido en 192.168.201.25. (Esta configuración asume que el cliente PPTP y las direcciones del servidor IP son las mismas que para el cliente y 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 el L2TP sobre el IPSec con PIX/ASA versión 7.x y superiores

El cliente exterior L2TP intenta establecer el L2TP sobre la conexión del IPSec VPN con el servidor interior L2TP. Para permitir el L2TP sobre los paquetes IPsec con el PIX/ASA medio, debe permitir que el puerto ESP, de ISAKMP(500), NAT-T, y L2TP 1701 establezca el túnel. Los paquetes L2TP son traducidos en el PIX y se envían a través del 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
```

Verificación

Actualmente no hay un procedimiento de verificación disponible para este documento.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Varias Conexiones PPTP/L2TP Fallan al usar PAT

Solamente puede tener una conexión PPTP/L2TP a través del Security Appliance PIX cuando utiliza PAT. Esto se debe a que la conexión GRE necesaria se establece sobre el puerto 0 y el PIX Security Appliance sólo mapea el puerto a un host. La solución alternativa es habilitar la inspección PPTP en el dispositivo de seguridad.

Error 800 al intentar conectar con PPTP VPN entrante

Cuando usted intenta conectar con PPTP VPN entrante, este mensaje de error 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.
```

Este problema ocurre generalmente cuando el passthrough PPTP o L2TP no se habilita en el ASA intermedio entre el cliente y el dispositivo de cabecera. Habilite el passthrough PPTP o L2TP y marque la configuración para resolver el problema.

Comandos de Debug

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Nota: Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Este ejemplo muestra un cliente PPTP dentro del PIX que inicia una conexión a un servidor PPTP fuera del PIX cuando no se ha configurado una ACL para permitir el tráfico GRE. Con el debug de registro en el PIX, puede ver la iniciación de tráfico del puerto TCP 1723 del cliente y el rechazo del tráfico de retorno del 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
```

Información para recopilar si abre un pedido de servicio del TAC

Si aún necesita ayuda después de seguir los pasos de

Troubleshooting anteriores y desea abrir una solicitud de servicio con el TAC de Cisco, asegúrese de incluir la siguiente información.
• Descripción del problema y detalles relevantes de la topología • Resolución de problemas realizada antes de abrir el servicio solicitado • Resultado del comando show tech-support • Resultado del comando show log después de la ejecución con el comando logging buffered debugging o capturas de consola que muestran el problema (si están disponibles) Adjunte los datos recolectados a su pedido de servicio en formato de texto sin comprimir (.txt). Usted puede adjuntar información a su solicitud de servicio al cargarla usando la herramienta Service Request Query Tool(clientes registrados solamente). Si no puede acceder a la herramienta Service Request Query Tool, puede enviar la información en un archivo adjunto del correo electrónico a attach@cisco.com con su número de solicitud de servicio en el asunto de su mensaje.

Información Relacionada

- Página de soporte de PPTP
- PIX/ASA versión 7.x y superiores Túnel IPsec a un Security Appliance con el uso de la Lista de Acceso y el MPF con el Ejemplo de Configuración NAT
- Configurar un túnel IPsec con un Firewall con el NAT
- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems