

Permitting PPTP/L2TP Connections Through the PIX/ASA/FWSM

Document ID: 18806

Introduction

Prerequisites

- Requirements
- Components Used
- Background Theory
- Conventions

PPTP with the Client Inside and the Server Outside

- Network Diagram
- Commands to Add for Version 6.2 and Earlier
- Commands to Add for Version 6.3
- Commands to Add for Versions 7.x and 8.0 using inspection
- Commands to Add for Versions 7.x and 8.0 using ACL
- Configuration for Versions 6.2 and Earlier

L2TP with the Client Inside and the Server Outside

PPTP with the Client Outside and the Server Inside

- Network Diagram
- Commands to Add to All Versions

L2TP with the Client Outside and the Server Inside

Allow L2TP Over IPsec Through PIX/ASA 7.x and Above

Verify

Troubleshoot

- Multiple PPTP/L2TP Connections Fail when using PAT
- Debug Commands

Information to Collect if You Open a TAC Service Request

Related Information

Introduction

This document discusses the configuration required on the Cisco Security Appliance/FWSM to allow a Point-to-Point Tunneling Protocol (PPTP)/Layer 2 Tunneling Protocol (L2TP) client to connect to a PPTP server through Network Address Translation (NAT).

The FWSM 3.1.x and later supports PPTP pass through with PAT. Use the PPTP inspection in order to enable this functionality.

Note: Use the same configuration of PIX for FWSM.

Refer to Configuring the Cisco Secure PIX Firewall to Use PPTP in order to configure a security appliance to accept PPTP connections.

In order to configure L2TP over IP Security (IPsec) from remote Microsoft Windows 2000/2003 and Windows XP clients to a PIX/ASA Security Appliance corporate office that use pre-shared keys with Microsoft Windows 2003 Internet, refer to L2TP Over IPsec Between Windows 2000/XP PC and PIX/ASA 7.2 Using Pre-shared Key Configuration Example.

Prerequisites

Requirements

In order to attempt this configuration, you must have a working PPTP server and client before you involve the PIX/ASA/FWSM.

Components Used

The information in this document is based on these software versions:

- Cisco PIX Firewall Versions 6.x and above
- Cisco ASA 5500 Series Security Appliance that runs version 7.x or above
- FWSM that runs version 3.1.x or above

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Theory

PPTP is described in RFC 2637 . This protocol uses a TCP connection that uses port 1723 and an extension of generic routing encapsulation (GRE) [protocol 47] to carry the actual data (PPP frame). The TCP connection is initiated by the client, followed by the GRE connection that is initiated by the server.

Version 6.2 and Earlier Information

Because the PPTP connection is initiated as TCP on one port and the response is GRE protocol, the PIX Adaptive Security Algorithm (ASA) does not know that the traffic flows are related. As a result, it is necessary to configure ACLs to allow the return traffic into the PIX. PPTP through the PIX with NAT (one-to-one address mapping) works because the PIX uses the port information in the TCP or User Datagram Protocol (UDP) header to keep track of translation. PPTP through the PIX with Port Address Translation (PAT) does not work because there is no concept of ports in GRE.

Version 6.3 Information

The PPTP fixup feature in version 6.3 allows the PPTP traffic to traverse the PIX when configured for PAT. Stateful PPTP packet inspection is also performed in the process. The **fixup protocol pptp** command inspects PPTP packets and dynamically creates the GRE connections and translations necessary to permit PPTP traffic. Specifically, the firewall inspects the PPTP version announcements and the outgoing call request/response sequence. Only PPTP Version 1, as defined in RFC 2637, is inspected. Further inspection on the TCP control channel is disabled if the version announced by either side is not Version 1. In addition, the outgoing call request and reply sequence is tracked. Connections and/or translations are dynamically allocated as necessary to permit subsequent secondary GRE data traffic. The PPTP fixup feature must be enabled for PPTP traffic to be translated by PAT.

Version 7.x Information

The PPTP Application Inspection Engine in version 7.x operates in the same fashion as **fixup protocol pptp** does in version 6.3.

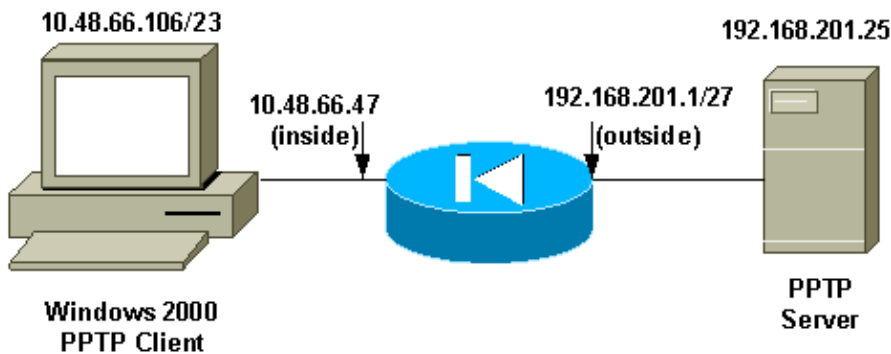
Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

PPTP with the Client Inside and the Server Outside

Network Diagram

This document uses this network setup:



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Commands to Add for Version 6.2 and Earlier

Complete these steps to add commands for version 6.2:

1. Define the static mapping for the inside PC. The address seen on the outside is 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 and apply the ACL to permit the GRE return traffic from the PPTP server to the PPTP client.

```
pixfirewall(config)#access-list acl-out permit gre host 192.168.201.25
                        host 192.168.201.5
```

3. Apply the ACL.

```
pixfirewall(config)#access-group acl-out in interface outside
```

Commands to Add for Version 6.3

Complete these steps to add commands for version 6.3:

1. Enable the fixup protocol pptp 1723 using this command.

```
pixfirewall(config)#fixup protocol pptp 1723
```

2. You do not need to define a static mapping because the PPTP fixup protocol is enabled. You can use PAT.

```
pixfirewall(config)#nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

```
pixfirewall(config)#global (outside) 1 interface
```

Commands to Add for Versions 7.x and 8.0 using inspection

Complete these steps to add commands for versions 7.x and 8.0 using the **inspect** command:

1. Add PPTP inspection to the default policy-map using the default class-map.

```
pixfirewall(config)#policy-map global_policy

pixfirewall(config-pmap)#class inspection_default

pixfirewall(config-pmap-c)#inspect pptp
```

2. You do not need to define a static mapping because the PIX now inspects PPTP traffic. You can use PAT.

```
pixfirewall(config)#nat (inside) 1 0.0.0.0 0.0.0.0 0 0

pixfirewall(config)#global (outside) 1 interface
```

OR

Commands to Add for Versions 7.x and 8.0 using ACL

Complete these steps to add commands for versions 7.x and 8.0 using ACL.

1. Define the static mapping for the inside PC. The address seen on the outside is 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 and apply the ACL to permit the GRE return traffic from the PPTP server to the PPTP client.

```
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. Apply the ACL.

```
pixfirewall(config)#access-group acl-out in interface outside
```

Configuration for Versions 6.2 and Earlier

PIX Configuration – Client Inside, Server Outside

```
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 with the Client Inside and the Server Outside

Complete these steps in order to add commands for versions 7.x and 8.x that use ACL. (This configuration assumes the PPTP client and the server IP addresses are the same as for L2TP client and server.)

1. Define the static mapping for the inside PC. The address seen on the outside is 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 and apply the ACL to permit the L2TP return traffic from the L2TP server to the L2TP client.

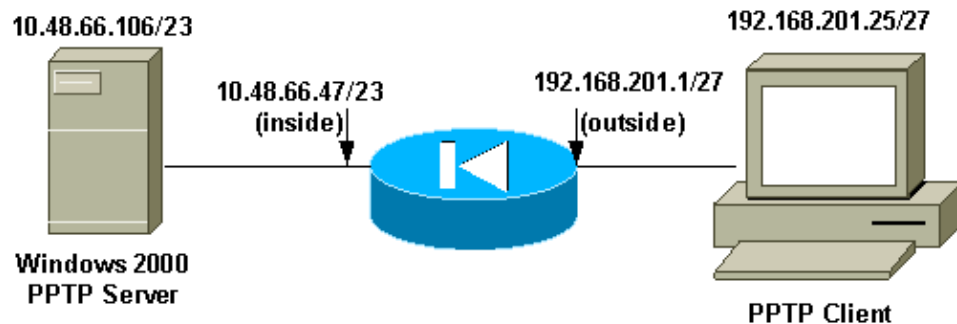
```
pixfirewall(config)#
pixfirewall(config)#access-list acl-out permit udp host 192.168.201.25
host 192.168.201.5 eq 1701
```

3. Apply the ACL.

```
pixfirewall(config)#access-group acl-out in interface outside
```

PPTP with the Client Outside and the Server Inside

Network Diagram



Note: The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Commands to Add to All Versions

In this configuration example, the PPTP server is 192.168.201.5 (static to 10.48.66.106 inside), and the PPTP client is at 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 with the Client Outside and the Server Inside

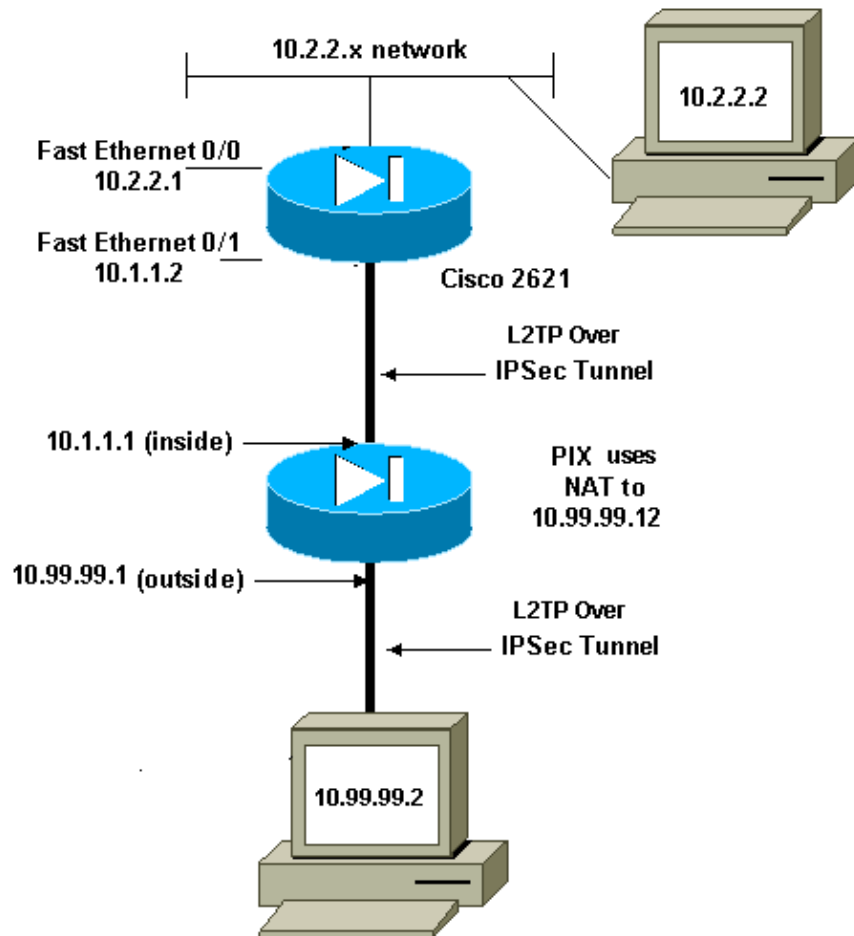
In this configuration example, the L2TP server is 192.168.201.5 (static to 10.48.66.106 inside), and the L2TP client is at 192.168.201.25. (This configuration assumes the PPTP client and server IP addresses are the same as for L2TP client and server.)

```
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
```

Allow L2TP Over IPsec Through PIX/ASA 7.x and Above

The outside L2TP client tries to establish the L2TP over IPsec VPN connection with the inside L2TP server. In order to allow the L2TP over IPsec packets through the middle PIX/ASA, you must allow the ESP, ISAKMP(500), NAT-T, and L2TP port 1701 to establish the tunnel. The L2TP packets are translated in PIX and sent through the VPN tunnel.



```
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
```

Verify

There is currently no verification procedure available for this document.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Multiple PPTP/L2TP Connections Fail when using PAT

You can only have one PPTP/L2TP connection through the PIX Security Appliance when you use PAT. This is because the necessary GRE connection is established over port 0 and the PIX Security Appliance only maps port 0 to one host.

Debug Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

This example shows a PPTP client inside the PIX initiating a connection to a PPTP server outside the PIX when there is no ACL configured to allow GRE traffic. With logging debug on the PIX, you can see the TCP port 1723 traffic initiation from the client and the rejection of the GRE protocol 47 return traffic.

```
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
```

Information to Collect if You Open a TAC Service Request

If you still need assistance after following the troubleshooting steps above and want to open a service request with the Cisco TAC, be sure to include the following information.

- Problem description and relevant topology details
- Troubleshooting performed before opening the service request
- Output from the **show tech-support** command
- Output from the **show log** command after running with the **logging buffered debugging** command, or console captures that demonstrate the problem (if available)

Please attach the collected data to your service request in non-zipped, plain text format (.txt). You can attach information to your service request by uploading it using the Service Request Query Tool (registered customers only) . If you cannot access the Service Request Query Tool, you can send the information in an email attachment to attach@cisco.com with your service request number in the subject line of your message.

Related Information

- [PPTP Support Page](#)
 - [PIX/ASA 7.x and Above IPsec Tunnel Pass Through a Security Appliance With use of Access List and MPF with NAT Configuration Example](#)
 - [Configuring an IPSec Tunnel through a Firewall with NAT](#)
 - [Cisco PIX Firewall Software](#)
 - [Cisco Secure PIX Firewall Command References](#)
 - [Security Product Field Notices \(including PIX\)](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 05, 2008

Document ID: 18806
