Configuring the PIX Firewall and VPN Clients Using PPTP, MPP

Table of Contents

Configuring the PIX Firewall and VPN Clients Using PPTP, MPPE and IPSec

Introduction

In this sample configuration, four different kinds of clients connect and encrypt traffic with the Cisco Secure PIX Firewall as tunnel endpoint:

- Users running CiscoSecure VPN Client 1.1 on Microsoft Windows 95/98/NT
- Users running the Cisco Secure VPN 3000 Client 2.5.x on Windows 95/98/NT
- Users running native Windows 2000/98 Point−to−Point Tunneling Protocol (PPTP) clients
- Users running the Cisco VPN Client 3.0.x on Windows 95/98/NT/2000.

In this example, we configured a single pool for IP Security (IPSec) and PPTP, but the pools could also be made separate.

Before You Begin

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Prerequisites

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the software and hardware versions below.

- PIX Software Release 6.1.1
- CiscoSecure VPN Client 1.1
- Cisco VPN 3000 Client version 2.5
- Cisco VPN Client 3.X
- Microsoft Windows 2000 and Windows 98 clients

Note: This was tested on PIX Software Release 6.1.1 but should work on Release 5.2.X and 5.3.1. PIX Software Release 6.X is required for the Cisco VPN Client 3.X. (Support for the Cisco VPN 3000 Client 2.5 was added in PIX Software Release 5.2.X. The configuration also works for PIX Software Release 5.1.x, except for the VPN 3000 client part.) IPSec and PPTP/Microsoft Point−to−Point Encryption (MPPE) should be made to work separately first. If they do not work separately, they will not work together.

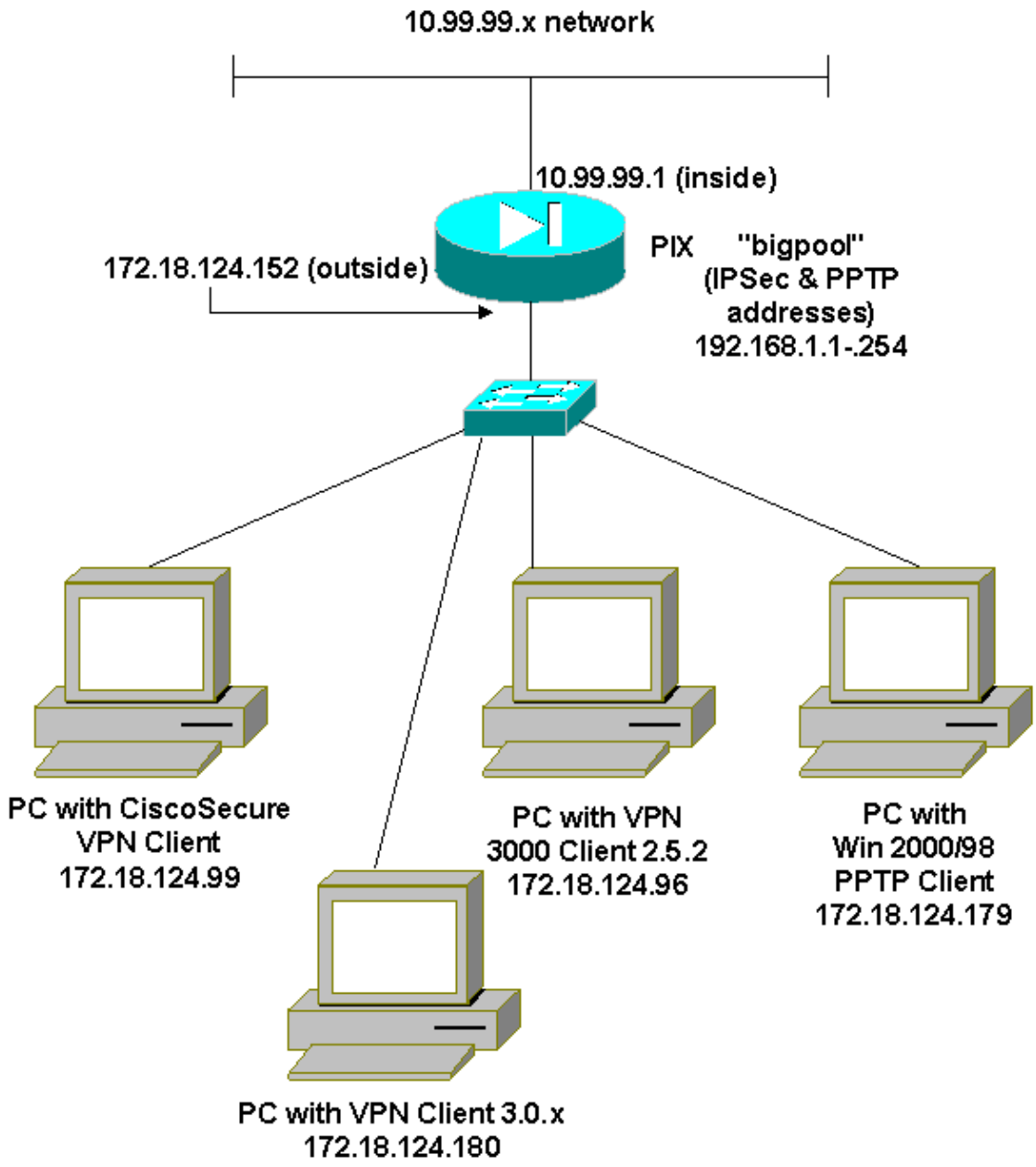
Configure

In this section, you are presented with the information to configure the PIX Firewall and VPN clients using PPTP, MPPE and IPSec.

Note: To find additional information on the commands used in this document, use the IOS Command Lookup tool.

Network Diagram

This document uses the network setup shown in the diagram below.



Configurations

This document uses the configurations shown below.

Cisco PIX Firewall

`PIX Version 5.2(3)`
`nameif ethernet0 outside security0`
`nameif ethernet1 inside security100`
`enable password 8Ry2YjIyt7RRXU24 encrypted`
`passwd 2KFQnbNIdI.2KYOU encrypted`
`hostname goss-515A`
`fixup protocol ftp 21`
`fixup protocol http 80`
`fixup protocol h323 1720`
`fixup protocol rsh 514`
`fixup protocol smtp 25`
`fixup protocol sqlnet 1521`

```
fixup protocol sip 5060
names
access-list 101 permit ip 10.99.99.0 255.255.255.0 192.168.1.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
no logging console
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface ethernet0 auto
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 172.18.124.152 255.255.255.0
ip address inside 10.99.99.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool bigpool 192.168.1.1-192.168.1.254
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
arp timeout 14400
nat (inside) 0 access-list 101
route outside 0.0.0.0 0.0.0.0 172.18.124.1 1
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
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
sysopt connection permit-pptp
no sysopt route dnat
crypto ipsec transform-set myset esp-des esp-md5-hmac
crypto dynamic-map dynmap 10 set transform-set myset
crypto map mymap 10 ipsec-isakmp dynamic dynmap
crypto map mymap client configuration address initiate
crypto map mymap client configuration address respond
crypto map mymap interface outside
isakmp enable outside

!--- CiscoSecure_VPNClient_key.

isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp identity address
isakmp client configuration address-pool local bigpool outside

!--- ISAKMP Policy for Cisco VPN Client 2.5 or
!--- CiscoSecure VPN Client 1.1.

isakmp policy 10 authentication pre-share
```

```
isakmp policy 10 encryption des
isakmp policy 10 hash md5

!--- The 1.1 and 2.5 clients use Diffie-Hellman (D-H)
!--- group 1 policy (PIX default).

isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
!

!--- ISAKMP Policy for VPN Client 3.0.

isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5

!--- The 3.0 clients use D-H group 2 policy
!--- and PIX 6.0 code.

isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
vpngroup vpn3000-all address-pool bigpool
vpngroup vpn3000-all dns-server 10.99.99.99
vpngroup vpn3000-all wins-server 10.99.99.99
vpngroup vpn3000-all default-domain password
vpngroup vpn3000-all idle-time 1800

!--- VPN 3000 group_name and group_password.

vpngroup vpn3000-all password ********
telnet timeout 5
ssh timeout 5
vpdn group 1 accept dialin pptp
vpdn group 1 ppp authentication pap
vpdn group 1 ppp authentication chap
vpdn group 1 ppp authentication mschap
vpdn group 1 ppp encryption mppe auto
vpdn group 1 client configuration address local bigpool
vpdn group 1 client authentication local


!--- PPTP username and password.

vpdn username cisco password cisco
vpdn enable outside
terminal width 80
```

CiscoSecure VPN Client 1.1

```
1- TACconn
      My Identity
           Connection security: Secure
           Remote Party Identity and addressing
           ID Type: IP subnet
           10.99.99.0
            255.255.255.0
           Port all Protocol all

      Connect using secure tunnel
           ID Type: IP address
           172.18.124.152
```

```
    Pre−shared Key=CiscoSecure_VPNClient_key

    Authentication (Phase 1)
    Proposal 1
        Authentication method: pre−shared key
        Encryp Alg: DES
        Hash Alg: MD5
        SA life: Unspecified
        Key Group: DH 1

    Key exchange (Phase 2)
    Proposal 1
        Encapsulation ESP
        Encrypt Alg: DES
        Hash Alg: MD5
        Encap: tunnel
        SA life: Unspecified
        no AH

2− Other Connections
       Connection security: Non−secure
       Local Network Interface
         Name: Any
         IP Addr: Any
         Port: All
```

Cisco VPN 3000 Client 2.5.x or Cisco VPN Client 3.0

Select **Options** > **Properties** > **Authentication**. Group−name and group password match the group_name and group_password on the PIX as in:

```
vpngroup vpn3000−all password ********
Host−name = 172.18.124.152
```

Windows 2000 or Win 98 PPTP Client Setup

You may contact the vendor who makes the PPTP client. For information on setting this up, see How to Configure the Cisco Secure PIX Firewall to Use PPTP.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

Troubleshooting Commands

Note: Before issuing **debug** commands, please see Important Information on Debug Commands.

PIX IPSec Debug

- **debug crypto ipsec** − To see the IPSec negotiations of phase 2.
- **debug crypto isakmp** − To see the Internet Security Association and Key Management Protocol (ISAKMP) negotiations of phase 1.
- **debug crypto engine** − Shows the traffic that is encrypted

PIX PPTP Debug

- **debug ppp io** − Display the packet information for the PPTP PPP virtual interface.
- **debug ppp error** − Display PPTP PPP virtual interface error messages.
- **debug vpdn error**− Display PPTP protocol error messages.
- **debug vpdn packets** − Display PPTP packet information about PPTP traffic.
- **debug vpdn events** − Display PPTP tunnel event change information.
- **debug ppp uauth** − Displays the PPTP PPP virtual interface AAA user authentication debugging messages.

Microsoft related issues:−

- **How to Keep RAS Connections Active After Logging Off** − When you log off from a Windows Remote Access Service (RAS) client, any RAS connections will be disconnected automatically. To remain connected after logging off, you may enable the KeepRasConnections key in the registry on the RAS client.
- **User Is Not Alerted When Logging On with Cached Credentials** − Symptoms − When you attempt to log on to a domain from a Windows−based workstation or member server and a domain controller cannot be located, no error message is displayed. Instead, you are logged on to the local computer using cached credentials.
- **How to Write an LMHOSTS File for Domain Validation and Other Name Resolution Issues** − There may be instances when you are experiencing name resolution issues on your TCP/IP network and you need to use Lmhosts files to resolve NetBIOS names. This article discusses the proper method of creating an Lmhosts file to aid in name resolution and domain validation.

Related Information

- **IP Security (IPSec) Product Support Pages**
- **PIX Command Reference**
- **PIX Product Support Page**
- **Requests for Comments (RFCs)**
- **Configuring IPSec Network Security**
- **Configuring Internet Key Exchange Security Protocol**
- **Technical Support − Cisco Systems**

Updated: Nov 04, 2002 Document ID: 14095