IPSec LAN−to−LAN Tunnel for Cisco VPN 5000 Concentrator to

Table of Contents

Configuring an IPSec LAN−to−LAN Tunnel for Cisco VPN 5000 Concentrator to Cisco Secure PIX Firewall

Cisco has announced the end of sales for the Cisco VPN 5000 Series Concentrators. For more information, please see the End−of−Sales Announcement.

Introduction

This document gives an overview of the configuration required to allow a Cisco Secure PIX Firewall and a Cisco VPN 500x Concentrator to open an IPSec LAN−to−LAN tunnel. For information about how to establish basic connectivity, or for reference on configuration syntax, please consult the VPN 5000 Concentrator documentation and the PIX documentation.

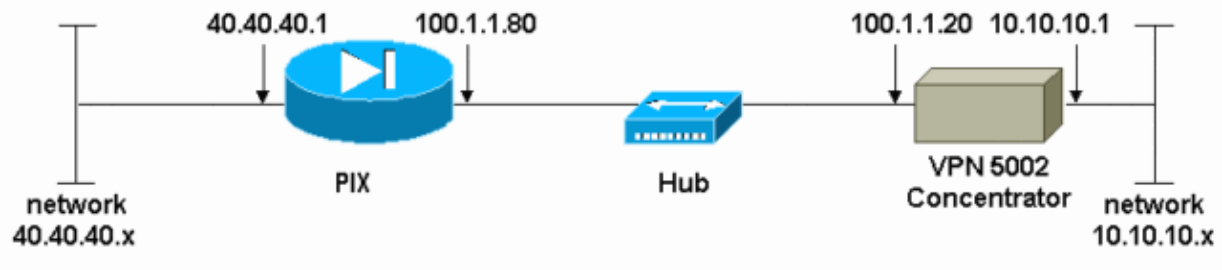
Hardware and Software Versions

This configuration was developed and tested using the software and hardware versions below.

- PIX Software release 5.1(2)
- VPN 5002 Concentrator with the 5.2.15US and 6.0.20US software releases

Note: The configuration for the 6.0.20US software release is differentiated with by two asterisks (**).

Network Diagram



Configurations

PIX Configuration

```
:
PIX Version 5.1(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
names
!--- Create crypto access list to specify interesting IPSec traffic
!--- for packets from PIX inside network to VPN 5002.
access-list 100 permit ip 40.40.40.0 255.255.255.0 10.10.10.0 255.255.255.0
!--- Exempt IPSec traffic from using NAT from PIX to VPN 5002.
access-list 101 permit ip 40.40.40.0 255.255.255.0 10.10.10.0 255.255.255.0
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 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 100.1.1.80 255.255.255.0
ip address inside 40.40.40.1 255.255.255.0
arp timeout 14400
!--- Exempt IPSec traffic from using NAT from PIX to VPN 5002 (access list 101).
nat (inside) 0 access-list 101
conduit permit icmp any any
route outside 0.0.0.0 0.0.0.0 100.1.1.20 1
timeout xlate 3:00:00 conn 1:00:00 half-closed 0:10:00 udp 0:02:00
timeout rpc 0:10:00 h323 0:05:00
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
!--- Create IPSec transform set named "myset" using DES for ESP
!--- and ESP with the MD5 (HMAC variant) authentication algorithm
!--- with transport mode. Note that Authentication Header is not used.
crypto ipsec transform-set myset esp-des esp-md5-hmac
!--- Create crypto map "newmap" and assign sequence number 10, which is used
!--- to rank multiple entries within one crypto map set (the lower the sequence
!--- number, the higher the priority). Use IKE to establish Security Associations;
!--- use IPSec for traffic specified in access list 100. Specify VPN 5002 as remote
!--- IPSec peer, and assign transform set "myset" for policy information.
crypto map newmap 10 ipsec-isakmp
crypto map newmap 10 match address 100
crypto map newmap 10 set peer 100.1.1.20
crypto map newmap 10 set transform-set myset
!--- Evaluate traffic going through outside interface against the crypto map
!--- "newmap" to determine whether it needs to be protected.
crypto map newmap interface outside
!--- Enable IPSec IKE on outside interface.
isakmp enable outside
!--- Specify pre-shared key and remote peer (VPN 5002) for SA negotiation.
isakmp key cisco123 address 100.1.1.20 netmask 255.255.255.255
!--- Use IP address for ISAKMP identity during IKE negotiation.
isakmp identity address
!--- Use pre-shared key for IKE, DES encryption, MD5, Diffie Hellman Group type 1
!--- (768 bit) and SA lifetime of 1000 seconds.
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 1000
telnet timeout 5
terminal width 80
Cryptochecksum:21e462e1e749c3138288bfe7ede24ed4
: end
[OK]
```

VPN 5000 Configuration

```
[ IP Ethernet 0:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 10.10.10.1

[ IP Ethernet 1:0 ]
Mode                    = Routed
SubnetMask              = 255.255.255.0
IPAddress               = 100.1.1.20

[ General ]
DeviceName              = "rtp5002"
IPSecGateway(**VPNGateway)= 100.1.1.80
EthernetAddress         = 00:00:a5:e9:c8:00
DeviceType              = VPN 5002/8 Concentrator
ConfiguredOn            = Timeserver not configured
ConfiguredFrom          = Command Line, from Console

[ IP Static ]
40.40.40.0 255.255.255.0 vpn 1 1

[ Tunnel Partner VPN 1 ]
LocalAccess             = "10.10.10.0/24"
```

```
Peer                    = "40.40.40.0/24"
Mode                    = Main
Transform               = esp(md5,des)
KeyManage               = Auto (**Reliable)
SharedKey               = "cisco123"
BindTo                  = "ethernet 1:0"
Partner                 = 100.1.1.80
**InactivityTimeout       = 120
**TunnelType                  = IPSec
**KeepaliveInterval       = 120
**KeyLifeSecs             = 3500
**Certificates            = Off

[ IP VPN 1 ]
Numbered                = Off
Mode                    = Routed

[ IKE Policy ]
Protection              = MD5_DES_G1

[ VPN Group "rtp" ]
DNSPrimaryServer        = 100.100.100.100
BindTo                  = "ethernet 1:0"
StartIPAddress          = 10.10.10.50
IPNet                   = 10.10.10.0/24
Transform               = esp(md5,des)
MaxConnections          = 10

[ VPN Users ]
omar config="rtp" sharedkey="letmein"

Configuration size is 1388 out of 65500 bytes.
```

debug and show Commands

Before attempting any **debug** commands, please see Important Information on Debug Commands.

VPN 5000 Debug

- **show sys log buffer** − View previously buffered events.
- **vpn trace dump all** − Shows information about all matching VPN connections, including information about the time, the VPN number, the real IP address of the peer, which scripts have been run, and in the case of an error, the routine and line number of the software code where the error occurred.

PIX Debug

- **debug crypto ipsec** − Displays errors during Phase 2.
- **debug crypto isakmp** − Displays errors during Phase 1.
- **debug crypto engine** − Displays information from the crypto engine.

VPN 5000 show Commands

- **show vpn partners** − Shows the following information: the VPN port number to which the peer is connected; the tunnel peer's IP address; the UDP port for the connection; whether the tunnel peer is connected to this concentrator's Tunnel Partner Default section instead of a specific Tunnel Partner section; the IP address used as the local endpoint of the tunnel; and how long the partners have been connected.

- **show vpn statistics** − Shows the following information for Users and Partners, and the total for both: current active connections; currently negotiating connections; the highest number of concurrent active connections since the last reboot; the total number of successful connections since the last reboot; the number of tunnel starts; the number of tunnels for which there were no errors; and the number of tunnels with errors.

PIX show Commands

- **show crypto ipsec sa** − Shows Phase 2 security associations.

- **show crypto isakmp sa** − Shows Phase 1 security associations.

- **show crypto engine** − Shows information regarding encrypted and decrypted packets.

Tools Information

For additional resources, refer to Cisco TAC Tools for VPN Technologies and Cisco TAC Tools for Security Technologies.

Related Information

- **Cisco VPN 5000 Series Concentrators End−of−Sales Announcement**
- **VPN Top Issues**
- **Cisco VPN 5000 Concentrator and Client Technical Tips**
- **Cisco VPN 5000 Concentrator Product Support Pages**
- **Cisco VPN 5000 Client Product Support Pages**
- **IP Security (IPSec) Product Support Pages**
- **PIX Top Issues**
- **PIX IPSec Configuration Guide**
- **Documentation for PIX Firewall**
- **More PIX Firewall Technical Tips**
- **PIX Command Reference**
- **Security Product Field Notices (including PIX)**
- **PIX Product Support Page**
- **Requests for Comments (RFCs)**

Updated: Jul 08, 2002 Document ID: 14094