

PIX 6.x : IPsec Tunnel Pass Through a PIX Firewall With use of Access List and with NAT Configuration Example

Document ID: 14138

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands
- Clearing Security Associations

Related Information

Introduction

This document provides a sample configuration for an IPsec tunnel through a firewall that performs network address translation (NAT). **This configuration does not work with port address translation (PAT) if you use Cisco IOS® Software Releases prior to and not including 12.2(13)T.** This kind of configuration can be used to tunnel IP traffic. This cannot be used to encrypt traffic that does not go through a firewall, such as IPX or routing updates. Generic routing encapsulation (GRE) tunneling is appropriate for that kind of configuration. In the example in this document, the Cisco 2621 and 3660 Routers are the IPsec tunnel endpoints that join two private networks, with conduits or access control lists (ACLs) on the PIX in between to allow the IPsec traffic.

Note: NAT is a one-to-one address translation, not to be confused with PAT, which is a many (inside the firewall)-to-one translation. Refer to Verifying NAT Operation and Basic NAT Troubleshooting or How NAT Works for more information on NAT operation and configuration.

Note: IPsec with PAT might not work properly because the outside tunnel endpoint device cannot handle multiple tunnels from one IP address. You need to contact your vendor to determine if the tunnel endpoint devices work with PAT. Additionally, in versions 12.2(13)T and later, the NAT Transparency feature can also be used for PAT. Refer to IPsec NAT Transparency for more information. Refer to Support for IPsec ESP Through NAT for more information about these features in versions 12.2(13)T and later. Also, before you open a case with TAC, refer to NAT Frequently Asked Questions, which has many answers to common questions.

Refer to IPsec Tunnel Pass Through a Security Appliance With use of Access List and MPF with NAT Configuration Example for more information on how to configure an IPsec tunnel through a firewall with NAT on PIX/ASA version 7.x.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

- Cisco IOS Software Release 12.0.7.T [up to but not including 12.2(13)T]

Refer to IPsec NAT Transparency for more recent versions.

- Cisco 2621 Router that runs Cisco IOS Software Release 12.4
- Cisco 3660 Router that runs Cisco IOS Software Release 12.4
- Cisco PIX Firewall that runs 6.x

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.

Conventions

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

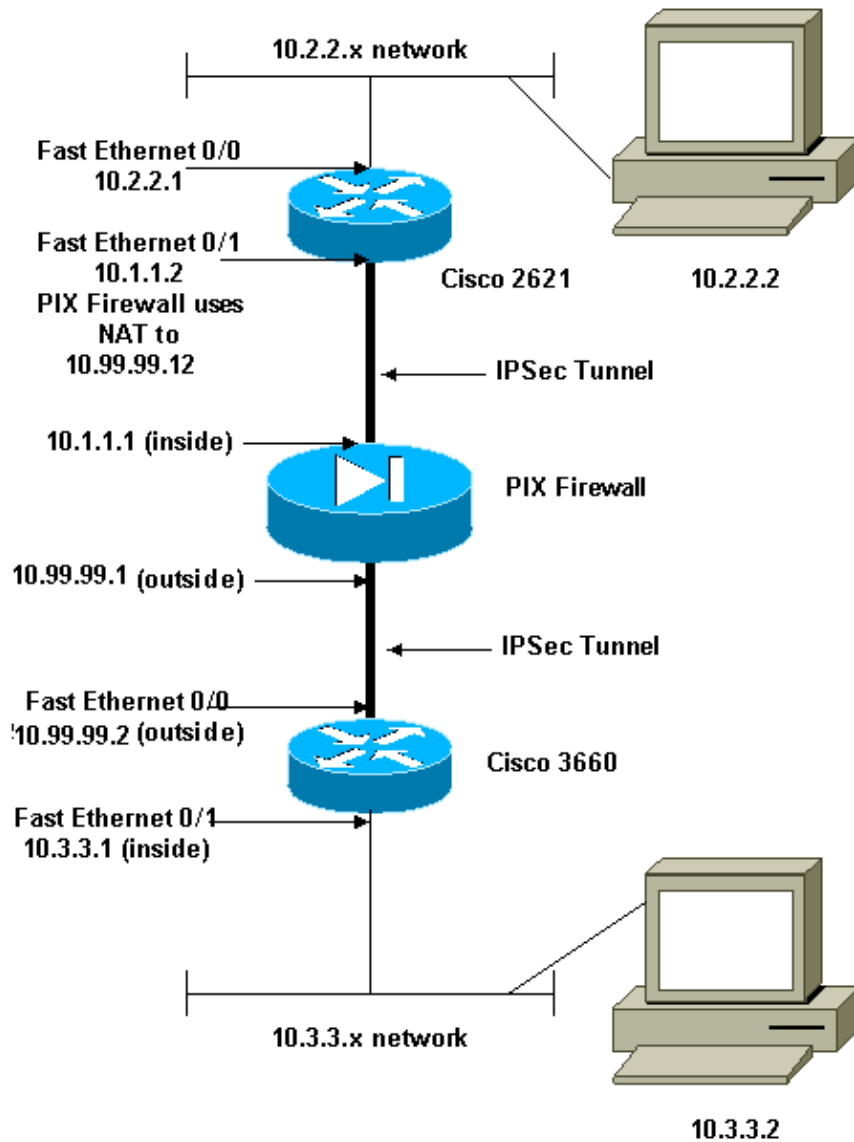
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

Network Diagram

This document uses this network setup:



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

Configurations

This document uses these configurations:

- Cisco 2621 Configuration
- Cisco PIX Firewall Partial Configuration
- Cisco 3660 Configuration

Cisco 2621 Configuration

```
Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-2621
!
```

```

ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
isdn voice-call-failure 0
cns event-service server
!

!--- IKE Policy

crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 10.99.99.2
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/1

!--- IPsec Policy

crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset

!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

  match address 101
!
controller T1 1/0
!
interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
!
interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto

!--- Apply to interface.

  crypto map mymap
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.1.1.1
no ip http server

!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

access-list 101 permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
line con 0
  transport input none
line aux 0
line vty 0 4
!
no scheduler allocate
end

```

```

fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69

!--- The fixup protocol esp-ike command is disabled by default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0

!--- Range of registered IP addresses for use.

global (outside) 1 10.99.99.50-10.99.99.60

!--- Translate any internal source address when
!--- going out to the Internet.

nat (inside) 1 0.0.0.0 0.0.0.0 0 0
static (inside,outside) 10.99.99.12 10.1.1.2 netmask 255.255.255.255 0 0

!--- or

access-list acl-out permit esp host 10.99.99.2 host 10.99.99.12
access-list acl-out permit udp host 10.99.99.2 host 10.99.99.12 eq isakmp
access-list acl-out permit udp host 10.99.99.2 host 10.99.99.12 eq 4500

!--- It is important to permit UDP port 4500 for NAT-T because the PIX is acting
!--- as a NAT device between the routers.

access-group acl-out in interface outside

isakmp enable outside
isakmp enable inside
Command configured in order to enable NAT-T
isakmp nat-traversal 20
route outside 0.0.0.0 0.0.0.0 99.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1

```

Note: The **fixup protocol esp-ike** command is disabled by default. If a **fixup protocol esp-ike** command is issued, the fixup is turned on, and the PIX Firewall preserves the source port of the Internet Key Exchange (IKE). It also creates a PAT translation for ESP traffic. Additionally, if the esp-ike fixup is on, Internet Security Association and Key Management Protocol (ISAKMP) cannot be enabled on any interface.

Cisco 3660 Configuration

```

version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-3660
!

```

```
ip subnet-zero
!
cns event-service server
!

!--- IKE Policy

crypto isakmp policy 10
  hash md5
  authentication pre-share
crypto isakmp key cisco123 address 10.99.99.12
!
crypto ipsec transform-set myset esp-des esp-md5-hmac
!
crypto map mymap local-address FastEthernet0/0

!--- IPSec Policy

crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.12
  set transform-set myset

!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

  match address 101
!
interface FastEthernet0/0
  ip address 10.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto

!--- Apply to interface.

  crypto map mymap
!
interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
!
interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
!
interface Ethernet3/1
  no ip address
  no ip directed-broadcast
interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
!
interface TokenRing4/0
  no ip address
```

```

no ip directed-broadcast
shutdown
ring-speed 16
!

!--- Pool from which inside hosts translate to
!--- the globally unique 10.99.99.0/24 network.

ip nat pool OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0

!--- Except the private network from the NAT process.

ip nat inside source route-map nonat pool OUTSIDE
ip classless
ip route 0.0.0.0 0.0.0.0 10.99.99.1
no ip http server
!

!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

access-list 101 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 101 deny ip 10.3.3.0 0.0.0.255 any

!--- Except the private network from the NAT process.

access-list 110 deny ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
access-list 110 permit ip 10.3.3.0 0.0.0.255 any
route-map nonat permit 10
match ip address 110
!
line con 0
transport input none
line aux 0
line vty 0 4
!
end

```

Verify

Use this section to confirm that your configuration works properly.

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

- **show crypto ipsec sa** Shows the phase 2 security associations.
- **show crypto isakmp sa** Shows the phase 1 security associations.
- **show crypto engine connections active** Use to see the encrypted and decrypted packets.

Troubleshoot

Use this section to troubleshoot your configuration.

Troubleshooting Commands

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

- **debug crypto engine** Shows the traffic that is encrypted.
- **debug crypto ipsec** Use to see the IPSec negotiations of phase 2.

- **debug crypto isakmp** Use to see the ISAKMP negotiations of phase 1.

Clearing Security Associations

- **clear crypto isakmp** Clears IKE security associations.
 - **clear crypto ipsec sa** Clears IPSec security associations.
-

Related Information

- **Cisco PIX 500 Series Security Appliances**
 - **Documentation for PIX Firewall**
 - **Cisco Secure PIX Firewall Command References**
 - **NAT Support Page**
 - **Request 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: Sep 26, 2008

Document ID: 14138
