

PIX 6.x: Dynamic IPsec Between a Statically Addressed IOS Router and the Dynamically Addressed PIX Firewall with NAT Configuration Example

Document ID: 66173

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- Network Diagram
- Configurations

Verify

Troubleshoot

- Troubleshooting Commands

Related Information

Introduction

This document provides a sample configuration that shows you how to enable the IOS[®] router to accept dynamic IPsec connections from a PIX Firewall. The remote router performs Network Address Translation (NAT) if private network 10.0.0.x accesses the Internet. Traffic from 10.0.0.x to private network 10.1.0.x behind the PIX is excluded from the NAT process. The PIX Firewall can initiate connections to the router, but the router cannot initiate connections to the PIX.

This configuration uses a Cisco IOS router in order to create dynamic IPsec LAN-to-LAN (L2L) tunnels with a PIX Firewall that receives dynamic IP addresses on their public interface (outside interface). Dynamic Host Configuration Protocol (DHCP) provides a mechanism in order to allocate IP addresses dynamically from the Internet service provider (ISP). This allows IP addresses to be reused when hosts no longer need them.

Refer to PIX 6.x: Dynamic IPsec Between a Statically Addressed PIX Firewall and the Dynamically Addressed IOS Router with NAT Configuration Example for more information on the scenario where the PIX accepts dynamic IPsec connections from the router.

Refer to PIX/ASA 7.x and later: Dynamic IPsec Between a Statically Addressed PIX and a Dynamically Addressed IOS Router with NAT Configuration Example in order to enable the PIX/ASA Security Appliance to accept dynamic IPsec connections from the IOS router.

Refer to PIX/ASA 7.x and later: Dynamic IPsec Between a Statically Addressed IOS Router and a Dynamically Addressed PIX with NAT Configuration Example in order to learn more about the same scenario where the PIX/ASA Security Appliance runs software version 7.x and later.

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 12.4
- Cisco PIX Firewall Software Release 6.3.4
- Cisco Secure PIX Firewall 515E
- Cisco 2811 Router

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.

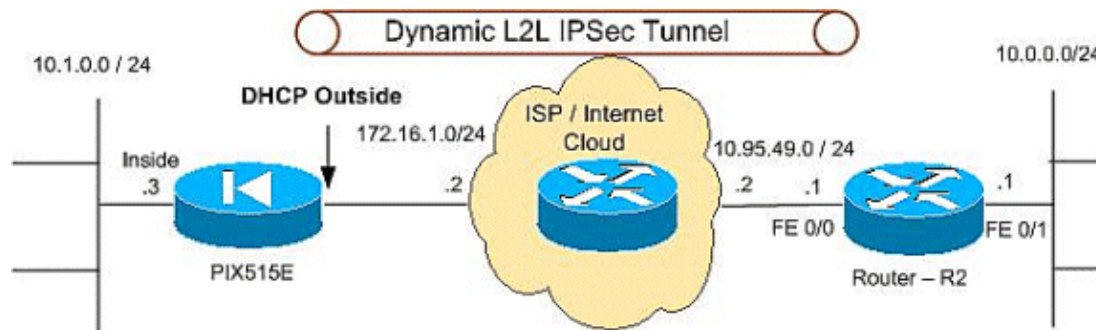
Configure

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:



Configurations

This document uses these configurations:

- PIX 515E
- R2 (Cisco 2811 Router)

PIX 515E

PIX Version 6.3(4)

```

interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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
names

!--- The access control list (ACL) to avoid NAT on the IPsec packets.

access-list NO-NAT permit ip 10.1.0.0 255.255.255.0 10.0.0.0 255.255.255.0

!--- The ACL to apply on crypto map.
!--- Include the private-network-to-private-network traffic
!--- in the encryption process.

access-list 101 permit ip 10.1.0.0 255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500

!--- ISP will providthe the Outside IP address.

ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 10.0.0.0 255.255.255.0 172.16.1.5 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 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 TACACS+ max-failed-attempts 3

```

```
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
```

```
!--- IPsec configuration, Phase 2.
```

```
crypto ipsec transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
```

```
!--- Internet Security Association and Key Management Protocol (ISAKMP)
!--- policy, Phase 1.
!--- Note: In real show run output, the pre-shared key appears as *****.
```

```
isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask 255.255.255.255
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 86400
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
: end
```

R2 (Cisco 2811 Router)

```
R2#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
```

```
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!

!--- ISAKMP policy, Phase 1.

crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!

!--- IPsec policy, Phase 2.

crypto ipsec transform-set DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server

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

ip nat inside source list 102 interface FastEthernet0/0 overload
!

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

```
access-list 101 permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255

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

access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
login
!
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 isakmp sa** Shows all current IKE security associations (SAs) at a peer.
- **show crypto ipsec sa** Shows the settings used by current (IPsec) SAs.
- **show crypto engine connections active** Shows current connections and information regarding encrypted and decrypted packets (router only).

You must clear SAs on both peers.

Perform these PIX commands in config mode.

- **clear crypto isakmp sa** Clears the Phase 1 SAs.
- **clear crypto ipsec sa** Clears the Phase 2 SAs.

Perform these router commands in enable mode.

- **clear crypto isakmp** Clears the Phase 1 SAs.
- **clear crypto sa** Clears the Phase 2 SAs.

Troubleshoot

Use this section to troubleshoot your configuration.

Troubleshooting 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.

- **show crypto isakmp sa** View all current IKE SAs at a peer.
 - **show crypto ipsec sa** Shows the settings used by current (IPsec) SAs.
 - **show crypto engine connections active** Shows current connections and information regarding encrypted and decrypted packets (router only).
-

Related Information

- **Most Common L2L and Remote Access IPSec VPN Troubleshooting Solutions**
 - **Cisco PIX Firewall Software**
 - **Cisco Secure PIX Firewall Command References**
 - **Security Product Field Notices (including PIX)**
 - **Requests for Comments (RFCs)**
 - **IPsec Negotiation/IKE Protocols**
 - **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: Mar 08, 2007

Document ID: 66173
