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

Document ID: 23102

Contents

Introduction

This document provides a sample configuration for how to enable the PIX to accept dynamic IPsec connections. The remote router performs Network Address Translation (NAT) if private network 10.1.1.x accesses the Internet. Traffic from 10.1.1.x to private network 192.168.1.x behind the PIX is excluded from the NAT process. The router can initiate connections to the PIX, but the PIX cannot initiate connections to the router.

This configuration uses a PIX firewall in order to create dynamic IPsec LAN−to−LAN (L2L) tunnels with a Cisco IOS® router 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 service provider (ISP). This allows IP addresses to be reused when hosts no longer need them.

Refer to Router−to−PIX Dynamic−to−Static IPsec with NAT Configuration Example for more information on a scenario where the router accepts dynamic IPsec connections from a PIX Security Appliance that runs 6.x.

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

Refer to IPsec Between a Static PIX/ASA 7.x and a Dynamic IOS Router 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 6.3.1
- Cisco Secure PIX Firewall 515E
- Cisco 7206 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.
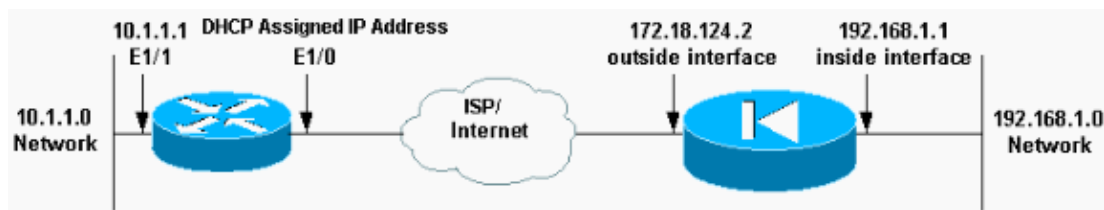
Configure

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.

- Elf (PIX)
- Mop (Cisco 7204 Router)

Elf (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
```

```
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname elf
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
```

!--- *Access control list (ACL) to avoid NAT on the IPsec packets.*

access-list nonat permit ip 192.168.1.0 255.255.255.0 10.1.1.0 255.255.255.0
```
pager lines 24
logging on
logging buffered debugging
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
mtu outside 1500
mtu inside 1500
mtu intf2 1500
```
ip address outside 172.18.124.2 255.255.255.0
ip address inside 192.168.1.1 255.255.255.0
```
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
global (outside) 1 interface
```

!-- *Binds ACL nonat to the NAT statement to avoid NAT on the IPsec packets*

nat (inside) 0 access-list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

!--- *Permits Internet Control Message Protocol (ICMP) traffic for testing.*
!--- *Do not enable it in a live network.*

conduit permit icmp any any
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
aaa-server LOCAL protocol tacacs+
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
```
sysopt connection permit-ipsec
```
no sysopt route dnat
```

```
!--- IPsec configuration

crypto ipsec transform-set router-set esp-des esp-md5-hmac
crypto dynamic-map cisco 1 set transform-set router-set
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside

!--- Internet Security Association and Key Management Protocol (ISAKMP)
!--- policy for accepting dynamic connections from remote PIX.
!--- Note: In real show run output, the pre-shared key appears as *******.

isakmp key cisco123 address 0.0.0.0 netmask 0.0.0.0
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
terminal width 80
Cryptochecksum:eeb67d5df47045f7e6ac4aa090aab683
: end
[OK]
elf#
```

Mop (Cisco 7204 Router)

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

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mop
!
!
ip subnet-zero
!
!
no ip domain-lookup
!
ip cef
ip audit notify log
ip audit po max-events 100
!

!--- Internet Key Exchange (IKE) policies

crypto isakmp policy 1
 hash md5
 authentication pre-share
crypto isakmp key cisco123 address 172.18.124.2
!
!

!--- IPsec policies

crypto ipsec transform-set pix-set esp-des esp-md5-hmac
!
```

```
crypto map pix 10 ipsec-isakmp
 set peer 172.18.124.2
 set transform-set pix-set
 match address 101
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface Ethernet1/0
ip address dhcp
ip nat outside
duplex half
crypto map pix
!
interface Ethernet1/1
ip address 10.1.1.1 255.255.255.0
ip nat inside
duplex half
!

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

ip nat inside source route-map nonat interface Ethernet1/0 overload
ip classless
ip route 0.0.0.0 0.0.0.0 Ethernet1/0
no ip http server
ip pim bidir-enable
!

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

access-list 101 permit ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255

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

access-list 110 deny ip 10.1.1.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 110 permit ip 10.1.1.0 0.0.0.255 any
!
route-map nonat permit 10
 match ip address 110
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 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.

You can run these **show** commands on the PIX and on the router.

- **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.

- The PIX commands are performed in config mode.

    ♦ **clear crypto isakmp sa** Clears the Phase 1 SAs.
    ♦ **clear crypto ipsec sa** Clears the Phase 2 SAs.
- The router commands are performed in enable mode.

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

Troubleshoot

This section provides information you can use 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** Shows 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

- **IPsec Negotiation/IKE Protocols Support Page**
- **PIX 500 Series Security Appliances**
- **Documentation for PIX Firewall**
- **Cisco Secure PIX Firewall Command References**
- **Requests for Comments (RFCs)** ⬈
- **Technical Support & Documentation – Cisco Systems**