

**sco – Configuring PIX-to-Router Dynamic-to-Static IPsec with**

# Table of Contents

<a href="#"><u>Configuring PIX-to-Router Dynamic-to-Static IPsec with NAT</u></a> .....	1
<a href="#"><u>Introduction</u></a> .....	1
<a href="#"><u>Configure</u></a> .....	1
<a href="#"><u>Components Used</u></a> .....	1
<a href="#"><u>Network Diagram</u></a> .....	1
<a href="#"><u>Configurations</u></a> .....	2
<a href="#"><u>Verify</u></a> .....	5
<a href="#"><u>Troubleshoot</u></a> .....	5
<a href="#"><u>Troubleshooting Commands</u></a> .....	5
<a href="#"><u>Tools Information</u></a> .....	5
<a href="#"><u>Related Information</u></a> .....	6

# Configuring PIX-to-Router Dynamic-to-Static IPSec with NAT

---

## **Introduction** **Configure**

Components Used  
Network Diagram  
Configurations  
**Verify**  
**Troubleshoot**

Troubleshooting Commands

**Tools Information**

**Related Information**

---

## **Introduction**

This document provides a sample configuration for enabling the PIX to accept dynamic IPSec connections. The remote router performs Network Address Translation (NAT) to connect the private network 10.1.1.x to private network 192.168.1.x behind the PIX. The router can initiate connections to the PIX, but the PIX cannot initiate connections to the router.

## **Configure**

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

**Note:** To find additional information on the commands used in this document, use the Cisco IOS® Command Lookup tool; a link to this tool can be found in the Cisco TAC Tools for VPN Technologies.

## **Components Used**

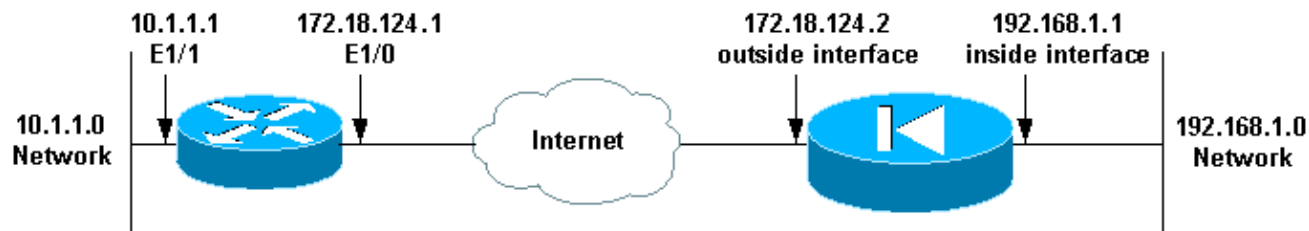
This configuration was developed and tested using the software and hardware versions below.

- Cisco IOS Software Release 12.2.(8)T
- Cisco PIX Firewall Software Release 6.1.3
- Cisco Secure PIX Firewall 515
- Cisco 7204 Router

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

## **Network Diagram**

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



## Configurations

This document uses the configurations shown below.

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

### Elf (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.1(3)
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
!--- 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
!-- Binding 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
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
!--- ISAKMP policy for accepting dynamic connections from remote PIX
isakmp key ***** 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 12.2
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
!
!---- 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 172.18.124.1 255.255.255.0
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 0.0.0.0 172.18.124.2
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

There is currently no verification procedure available for this configuration.

## Troubleshoot

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

### Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter tool, which allows you to view an analysis of **show** command output; a link to this tool can be found in the Tools Information section of this document.

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

The following **debug** commands must be running on both IPsec peers.

- **debug crypto isakmp** – Displays errors during Phase 1. (Router and PIX)
- **debug crypto ipsec** – Displays errors during Phase 2. (Router and PIX)
- **debug crypto engine** – Displays information from the crypto engine. (Router only)

The following **show** commands can be run on the PIX and on the router.

- **show crypto isakmp sa** – View 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 enable mode; the router commands are performed in non-enable mode.

- **clear crypto isakmp sa** – Clears the Phase 1 SAs. (PIX)
  - **clear crypto ipsec sa** – Clears the Phase 2 SAs. (PIX)
  - **clear crypto isakmp** – Clears the Phase 1 SAs. (Router)
  - **clear crypto sa** – Clears the Phase 2 SAs. (Router)
- 

## Tools Information

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

---

## Related Information

- [VPN Top Issues](#)
  - [IPSec Technical Tips](#)
  - [IP Security \(IPSec\) Product Support Pages](#)
  - [PIX Top Issues](#)
  - [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 \(RFCs\)](#)
- 

All contents are Copyright © 1992—2002 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

---

Updated: May 16, 2002

Document ID: 23102

---