Table of Contents

Configuring a GRE Tunnel over IPSec with OSPF

Document ID: 14381

Introduction

Normal IP Security (IPSec) configurations cannot transfer routing protocols, such as Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), or non−IP traffic, such as Internetwork Packet Exchange (IPX) and AppleTalk. This document illustrates how to route between different networks that use a routing protocol and non−IP traffic with IPSec. This example uses generic routing encapsulation (GRE) in order to accomplish routing between the different networks.

Prerequisites

Requirements

Before you attempt this configuration, ensure that you meet these requirements:

- Make sure that the tunnel works before you apply the crypto maps.
- For information about possible Maximum Transmission Unit (MTU) issues, refer to Adjusting IP MTU, TCP MSS, and PMTUD on Windows and Sun Systems.

Components Used

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

- Cisco 3600 that runs Cisco IOS® Software Release 12.1(8)
- Cisco 2600 that runs Cisco IOS Software Release 12.1(9)
- PIX Firewall Software Release 5.3(2)
- PIX Firewall Software Release 6.0(1)

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

For more information on document conventions, refer to Cisco Technical Tips Conventions.

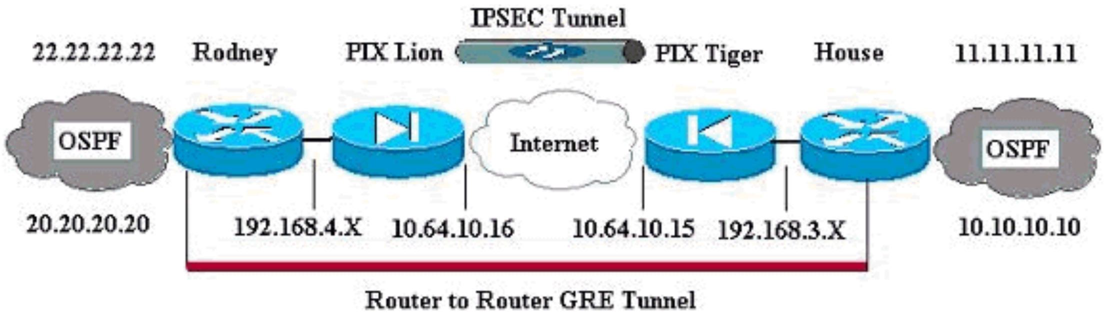
Configure

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

Note: In order to find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses the network setup shown in this diagram.



Configurations

This document uses these configurations.

- PIX Lion
- PIX Tiger
- Router Rodney
- Router House

PIX Lion

```
PIX Version 6.0(1)
nameif gb−ethernet0 dmz1 security60
nameif gb−ethernet1 dmz2 security40
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Lion
domain−name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
```

```
names

!--- Traffic from inside network.

access-list nonat permit ip 192.168.4.0 255.255.255.0 192.168.3.0 255.255.255.0
pager lines 24
interface gb-ethernet0 1000auto shutdown
interface gb-ethernet1 1000auto shutdown
interface ethernet0 auto
interface ethernet1 auto
mtu dmz1 1500
mtu dmz2 1500
mtu outside 1500
mtu inside 1500
ip address dmz1 127.0.0.1 255.255.255.255
ip address dmz2 127.0.0.1 255.255.255.255
ip address outside 10.64.10.16 255.255.255.224
ip address inside 192.168.4.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address dmz1 0.0.0.0
failover ip address dmz2 0.0.0.0
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
pdm history enable
arp timeout 14400
global (outside) 1 interface

!--- Do not Network Address Translate (NAT) traffic.

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 10.64.10.1 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 s0
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

!--- Trust IPSec traffic and avoid going through
!--- access control lists (ACLs)/NAT.

sysopt connection permit-ipsec
no sysopt route dnat

!--- IPSec configuration.

crypto ipsec transform-set pixset esp-des esp-md5-hmac
crypto map pixmap 20 ipsec-isakmp
crypto map pixmap 20 match address nonat
crypto map pixmap 20 set peer 10.64.10.15
crypto map pixmap 20 set transform-set pixset
crypto map pixmap interface outside
isakmp enable outside
```

```
!--- IKE parameters.

isakmp key ******** address 10.64.10.15 netmask 255.255.255.255
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 3600
telnet timeout 5
ssh 64.104.205.124 255.255.255.255 outside
ssh timeout 5
terminal width 80
Cryptochecksum:d39b3d449563c7cd434b43f82f0f0a21
: end
```

PIX Tiger

```
PIX Version 5.3(2)
nameif gb-ethernet0 intf2 security10
nameif gb-ethernet1 intf3 security15
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Tiger
domain-name cisco.com
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
names
access-list nonat permit ip 192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0
pager lines 24
logging on
no logging timestamp
no logging standby
logging console debugging
no logging monitor
no logging buffered
no logging trap
no logging history
logging facility 20
logging queue 512
interface gb-ethernet0 1000auto shutdown
interface gb-ethernet1 1000auto shutdown
interface ethernet0 auto
interface ethernet1 auto
mtu intf2 1500
mtu intf3 1500
mtu outside 1500
mtu inside 1500
ip address intf2 127.0.0.1 255.255.255.255
ip address intf3 127.0.0.1 255.255.255.255
ip address outside 10.64.10.15 255.255.255.224
ip address inside 192.168.3.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
```

```
failover timeout 0:00:00
failover poll 15
failover ip address intf2 0.0.0.0
failover ip address intf3 0.0.0.0
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
arp timeout 14400
global (outside) 1 interface

!−−− Do not NAT traffic.

nat (inside) 0 access−list nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 10.64.10.1 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 s0
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
sysopt connection permit−ipsec
no sysopt route dnat

!−−− IPSec parameters.

crypto ipsec transform−set pixset esp−des esp−md5−hmac
crypto map pixmap 20 ipsec−isakmp
crypto map pixmap 20 match address nonat
crypto map pixmap 20 set peer 10.64.10.16
crypto map pixmap 20 set transform−set pixset
crypto map pixmap interface outside

!−−− IKE parameters.

isakmp enable outside
isakmp key ******** address 10.64.10.16 netmask 255.255.255.255
isakmp identity address
isakmp policy 20 authentication pre−share
isakmp policy 20 encryption des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 3600
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:a0a7ac847b05d9d080d1c442ef053a0b
: end
```

Router Rodney

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password−encryption
!
hostname rodney
!
memory−size iomem 15
ip subnet−zero
```

```
!
ip audit notify log
ip audit po max-events 100
!
interface Loopback0
ip address 20.20.20.20 255.255.255.0
!
interface Loopback1
ip address 22.22.22.22 255.255.255.0
!
interface Tunnel0
ip address 1.1.1.2 255.255.255.0

!--- Tunnel source.

tunnel source Ethernet0/1

!--- Tunnel destination.

tunnel destination 192.168.3.2
!
interface Ethernet0/0
no ip address
!
interface Serial0/0
no ip address
shutdown
!
interface Ethernet0/1
ip address 192.168.4.2 255.255.255.0
!
interface Serial0/1
no ip address
shutdown
!
router ospf 22
log-adjacency-changes
network 1.1.1.0 0.0.0.255 area 0
network 22.22.22.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.4.1
ip route 10.10.10.0 255.255.255.0 Tunnel0
no ip http server
!
line con 0
line aux 0
line vty 0 4
login
!
end!
End
```

Router House

```
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house
!
ip subnet-zero
```

```
no ip domain-lookup
!
interface Loopback0
ip address 10.10.10.10 255.255.255.0
!
interface Loopback1
ip address 11.11.11.11 255.255.255.0
!
interface Tunnel0
ip address 1.1.1.1 255.255.255.0

!--- Tunnel source.

tunnel source FastEthernet0/1

!--- Tunnel destination.

tunnel destination 192.168.4.2
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.3.2 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet4/0
no ip address
shutdown
duplex auto
speed auto
!
router ospf 11
log-adjacency-changes
network 1.1.1.0 0.0.0.255 area 0
network 11.11.11.0 0.0.0.255 area 0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.3.1
ip route 20.20.20.0 255.255.255.0 Tunnel0
ip http server
!
line con 0
line aux 0
line vty 0 4
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

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

For additional information on troubleshooting a PIX and IPSec tunnel, refer to Troubleshooting the PIX to Pass Data Traffic on an Established IPSec Tunnel.

Troubleshooting Commands

Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

Note: Before you issue **debug** commands, refer to Important Information on Debug Commands.

PIX IPSec Good Debug

- **show crypto isakmp sa** Shows the Internet Security Association Management Protocol (ISAKMP) Security Association (SA) built between peers.

  ```
  Lion# show crypto isakmp sa
  Total : 1
  Embryonic : 0
  dst src state pending created
  10.64.10.15 10.64.10.16 QM_IDLE 0 1


  Tiger# show crypto isakmp sa
  Total SAs : 1
  Embryonic : 0
  dst src state pending created
  10.64.10.15 10.64.10.16 QM_IDLE 0 1
  ```
- **show crypto engine connection active** Shows each Phase 2 SA built and the amount of traffic sent.

  ```
  Lion# show crypto engine connection active
  Crypto Engine Connection Map:
  size = 8, free = 6, used = 2, active = 2


  Tiger# show crypto engine connection active
  Crypto Engine Connection Map:
  size = 8, free = 6, used = 2, active = 2
  ```
- **show debug** Displays the debug output.

  ```
  Lion# show debug
  debug crypto ipsec
  debug crypto isakmp
  debug crypto engine
  crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
  OAK_MM exchange
  ISAKMP (0): processing SA payload. message ID = 0

  ISAKMP (0): Checking ISAKMP transform 1 against priority 20 policy
  ISAKMP: encryption DES−CBC
  ISAKMP: hash MD5
  ISAKMP: default group 1
  ISAKMP: auth pre−share
  ISAKMP: life type in seconds
  ISAKMP: life duration (basic) of 3600
  ISAKMP (0): atts are acceptable. Next payload is 0
  ISAKMP (0): SA is doing pre−shared key authentication using id type ID_IPV4_ADDR
  return status is IKMP_NO_ERROR#
  crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
  OAK_MM exchange
  ISAKMP (0): processing KE payload. message ID = 0

  ISAKMP (0): processing NONCE payload. message ID = 0
  ```

```
ISAKMP (0): processing vendor id payload

ISAKMP (0): speaking to another IOS box!

ISAKMP (0): ID payload
next−payload : 8
type : 1
protocol : 17
port : 500
length : 8
ISAKMP (0): Total payload length: 12
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
OAK_MM exchange
ISAKMP (0): processing ID payload. message ID = 0
ISAKMP (0): processing HASH payload. message ID = 0
ISAKMP (0): SA has been authenticated

ISAKMP (0): beginning Quick Mode exchange, M−ID of 1220019031:48b80357IPSEC(key.
IPSEC(spi_response): getting spi 0xa67177c5(2792454085) for SA
from 10.64.10.15 to 10.64.10.16 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.64.10.15, dest 10.64.10.16
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 1220019031

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_DES
ISAKMP: attributes in transform:
ISAKMP: encaps is 1
ISAKMP: SA life type in seconds
ISAKMP: SA life duration (basic) of 28800
ISAKMP: SA life type in kilobytes
ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0
ISAKMP: authenticator is HMAC−MD5
ISAKMP (0): atts are acceptable.IPSEC(validate_proposal_request): proposal part,
(key eng. msg.) dest= 10.64.10.15, src= 10.64.10.16,
dest_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp−des esp−md5−hmac ,
lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4

ISAKMP (0): processing NONCE payload. message ID = 1220019031

ISAKMP (0): processing ID payload. message ID = 1220019031
ISAKMP (0): processing ID payload. message ID = 1220019031map_alloc_entry: allo2
map_alloc_entry: allocating entry 1

ISAKMP (0): Creating IPSec SAs
inbound SA from 10.64.10.15 to 10.64.10.16 (proxy 192.168.3)
has spi 2792454085 and conn_id 2 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytes
outbound SA from 10.64.10.16 to 10.64.10.15 (proxy 192.168.)
has spi 285493108 and conn_id 1 and flags 4
lifetime of 28800 seconds
lifetime of 4608000 kilobytesIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
(key eng. msg.) dest= 10.64.10.16, src= 10.64.10.15,
dest_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
src_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp−des esp−md5−hmac ,
lifedur= 28800s and 4608000kb,
spi= 0xa67177c5(2792454085), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(initialize_sas): ,
(key eng. msg.) src= 10.64.10.16, dest= 10.64.10.15,
src_proxy= 192.168.4.0/255.255.255.0/0/0 (type=4),
dest_proxy= 192.168.3.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp−des esp−md5−hmac ,
lifedur= 28800s and 4608000kb,
spi= 0x11044774(285493108), conn_id= 1, keysize= 0, flags= 0x4

return status is IKMP_NO_ERROR
```

Router GRE Passing Routing and Ping

- **show ip route** Displays IP routing table entries.

```
rodney#show ip route
Codes: C − connected, S − static, I − IGRP, R − RIP, M − mobile, B − BGP
D − EIGRP, EX − EIGRP external, O − OSPF, IA − OSPF inter area
N1 − OSPF NSSA external type 1, N2 − OSPF NSSA external type 2
E1 − OSPF external type 1, E2 − OSPF external type 2, E − EGP
i − IS−IS, L1 − IS−IS level−1, L2 − IS−IS level−2, ia − IS−IS inter area
* − candidate default, U − per−user static route, o − ODR
P − periodic downloaded static route

Gateway of last resort is 192.168.4.1 to network 0.0.0.0

1.0.0.0/24 is subnetted, 1 subnets
C 1.1.1.0 is directly connected, Tunnel0
20.0.0.0/24 is subnetted, 1 subnets
C 20.20.20.0 is directly connected, Loopback0
22.0.0.0/24 is subnetted, 1 subnets
C 22.22.22.0 is directly connected, Loopback1
C 192.168.4.0/24 is directly connected, Ethernet0/1
10.0.0.0/24 is subnetted, 1 subnets
S 10.10.10.0 is directly connected, Tunnel0
11.0.0.0/32 is subnetted, 1 subnets
O 11.11.11.11 [110/11112] via 1.1.1.1, 03:34:01, Tunnel0
S* 0.0.0.0/0 [1/0] via 192.168.4.1
rodney#
rodney#ping 11.11.11.11

Type escape sequence to abort.
Sending 5, 100−byte ICMP Echos to 11.11.11.11, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round−trip min/avg/max = 1/2/4 ms



house#show ip route
Codes: C − connected, S − static, I − IGRP, R − RIP, M − mobile, B − BGP
D − EIGRP, EX − EIGRP external, O − OSPF, IA − OSPF inter area
N1 − OSPF NSSA external type 1, N2 − OSPF NSSA external type 2
E1 − OSPF external type 1, E2 − OSPF external type 2, E − EGP
i − IS−IS, L1 − IS−IS level−1, L2 − IS−IS level−2, ia − IS−IS inter area
* − candidate default, U − per−user static route, o − ODR
P − periodic downloaded static route

Gateway of last resort is 192.168.3.1 to network 0.0.0.0
```

```
1.0.0.0/24 is subnetted, 1 subnets
C 1.1.1.0 is directly connected, Tunnel0
20.0.0.0/24 is subnetted, 1 subnets
S 20.20.20.0 is directly connected, Tunnel0
22.0.0.0/32 is subnetted, 1 subnets
O 22.22.22.22 [110/11112] via 1.1.1.2, 03:33:39, Tunnel0
10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Loopback0
11.0.0.0/24 is subnetted, 1 subnets
C 11.11.11.0 is directly connected, Loopback1
C 192.168.3.0/24 is directly connected, FastEthernet0/1
S* 0.0.0.0/0 [1/0] via 192.168.3.1

house#ping 22.22.22.22

Type escape sequence to abort.
Sending 5, 100−byte ICMP Echos to 22.22.22.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round−trip min/avg/max = 1/3/4 ms
```

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- **IPSec Negotiation/IKE Protocols**
- **Documentation for PIX Firewall**
- **PIX Command Reference**
- **PIX Product Support**
- **Technical Support & Documentation − Cisco Systems**

Updated: Jun 22, 2005 Document ID: 14381