配置在IPsec的一GRE隧道与OSPF

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[配置](#)
[网络图](#)
[配置](#)
[验证](#)
[故障排除](#)
[故障排除命令](#)
[相关信息](#)

简介

普通的 IP 安全 (IPSec) 配置不能传输路由协议，例如增强型内部网关路由协议 (EIGRP) 和开放式最短路径优先 (OSPF)，也不能传输非 IP 数据流，例如网间数据包交换 (IPX) 和 AppleTalk。本文说明如何路由以IPsec使用一个路由协议和非IP数据流的区别网络之间。为了实现不同网络之间的路由，此示例使用了通用路由封装 (GRE)。

有关详细信息，请参阅 PIX/ASA 7.x 及更高版本：与OSPF配置示例的VPN/IPsec关于如何为与开放最短路径优先(OSPF)的一VPN/IPsec配置的更多信息没有在Cisco PIX安全工具软件版本7.x或Cisco可适应安全工具(ASA)的一GRE隧道。

参考配置与通信的IPSec路由器到路由器星型网Spoke之间关于如何配置在三路由器之间的一星型网IPsec设计的信息。

有关如何用在使用网络地址转换 (NAT) 的 GRE 隧道上配置基本 Cisco IOS® 防火墙配置的信息，请参阅在使用 IOS 防火墙和 NAT 的 GRE 隧道上配置路由器到路由器 IPSec（预共享密钥）。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 在您应用加密映射之前，请确保隧道处于正常状态。
- 有关可能出现的最大传输单元 (MTU) 问题，请参阅在 Windows 和 Sun 系统上调整 IP MTU、TCP MSS 和 PMTUD。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行 Cisco IOS 软件版本 12.4(8) 的 Cisco 3600
- 运行 Cisco IOS 软件版本 12.4(8) 的 Cisco 2600
- PIX防火墙(Lion)软件版本6.3(5)
- PIX防火墙(Tiger)软件版本6.3(5)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

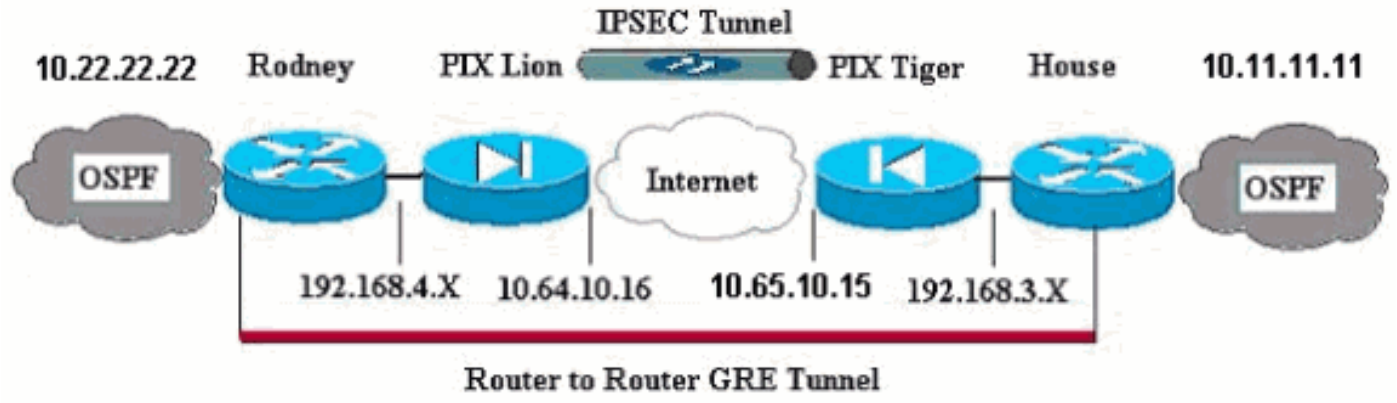
配置

本部分提供用于配置本文档所述功能的信息。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些是已在实验室环境中使用的 RFC 1918 地址。

注意： crypto不支持Cisco 7600系列路由器。您可以必须安装VPN模块为了此能工作。

配置

本文档使用以下配置：

- PIX Lion
- PIX Tiger
- 路由器 Rodney

- 路由器 House

PIX Lion

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Lion 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 !---
Defines interesting traffic that is protected by the
IPsec tunnel. access-list 101 permit gre 192.168.4.0
255.255.255.0 192.168.3.0 255.255.255.0 !--- Do not
perform NAT for traffic to other PIX Firewall. access-
list nonat permit ip 192.168.4.0 255.255.255.0
192.168.3.0 255.255.255.0 pager lines 24 mtu outside
1500 mtu inside 1500 mtu intf2 1500 mtu intf3 1500 mtu
intf4 1500 mtu intf5 1500 ip address outside 10.64.10.16
255.255.255.224 ip address inside 192.168.4.1
255.255.255.0 !--- Output suppressed. 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 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 h323 0:05:00 mgcp 0:05:00 sip 0:30:00
sip_media 0:02:00 timeout sip-disconnect 0:02:00 sip-
invite 0:03:00 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 !--- Trust IPSec
traffic and avoid going through !--- access control
lists (ACLs)/NAT. sysopt connection permit-ipsec !---
IPsec configuration. crypto ipsec transform-set pixset
esp-des esp-md5-hmac crypto map pixmap 20 ipsec-isakmp
crypto map pixmap 20 match address 101 crypto map pixmap
20 set peer 10.65.10.15 crypto map pixmap 20 set
transform-set pixset crypto map pixmap interface outside
isakmp enable outside !--- IKE parameters. isakmp key
******** address 10.65.10.15 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 10.104.205.124
255.255.255.255 outside ssh timeout 5 terminal width 80
Cryptochecksum:d39b3d449563c7cd434b43f82f0f0a21 : end
```

PIX Tiger

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
nameif ethernet3 intf3 security6
nameif ethernet4 intf4 security8
nameif ethernet5 intf5 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname Tiger 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
access-list 101 permit gre 192.168.3.0 255.255.255.0
192.168.4.0 255.255.255.0 access-list nonat permit ip
192.168.3.0 255.255.255.0 192.168.4.0 255.255.255.0 mtu
outside 1500 mtu inside 1500 mtu intf2 1500 mtu intf3
1500 mtu intf4 1500 mtu intf5 1500 ip address outside
10.65.10.15 255.255.255.224 ip address inside
192.168.3.1 255.255.255.0 !--- Output suppressed. 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
h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
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 parameters. crypto ipsec transform-set pixset esp-
des esp-md5-hmac crypto map pixmap 20 ipsec-isakmp
crypto map pixmap 20 match address 101 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
```

路由器 Rodney

```
version 12.4
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 Loopback1 ip address 10.22.22.22 255.255.255.0
! interface Tunnel0 ip address 10.1.1.2 255.255.255.0 !-
-- 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 10.1.1.0 0.0.0.255 area 0 network 10.22.22.0
0.0.0.255 area 0 ! ip classless ip route 0.0.0.0 0.0.0.0
192.168.4.1 !--- The 10.11.11.0 traffic is passed
through !--- the GRE tunnel. ip route 10.11.11.0
255.255.255.0 Tunnel0 no ip http server ! line con 0
line aux 0 line vty 0 4 login ! end! End
```

路由器 House

```
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname house ! ip subnet-zero no ip domain-lookup ! !
interface Loopback1 ip address 10.11.11.11 255.255.255.0
! interface Tunnel0 ip address 10.1.1.1 255.255.255.0 !-
-- 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 10.1.1.0 0.0.0.255 area 0 network 10.11.11.0
0.0.0.255 area 0 ! ip classless ip route 0.0.0.0 0.0.0.0
192.168.3.1 !--- The 10.22.22.0 traffic is passed
through !--- the GRE tunnel. ip route 10.22.22.0
255.255.255.0 Tunnel0 ip http server ! line con 0 line
aux 0 line vty 0 4
```

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

参考排除故障PIX通过在已建立的IPSec隧道的数据流关于排除故障PIX和IPSec隧道的更多信息。

故障排除命令

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输

出的分析。

注意： 使用 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

PIX IPSec成功调试

- **show crypto isakmp sa** - 显示对等体之间建立的 Internet 安全连接和密钥管理协议 (ISAKMP) 安全关联 (SA)。`Lion#**show crypto isakmp sa** Total : 1 Embryonic : 0 dst src state pending created 10.65.10.15 10.64.10.16 QM_IDLE 0 1 Tiger#**show crypto isakmp sa** Total SAs : 1 Embryonic : 0 dst src state pending created 10.65.10.15 10.64.10.16 QM_IDLE 0 1`
- **show crypto engine connection active** - 显示已建立的每个阶段 2 SA 和已发送的流量数。`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** - 显示调试输出。`Lion#**show debug debug crypto ipsec debug crypto isakmp debug crypto engine** crypto_isakmp_process_block: src 10.65.10.15, 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 10.65.10.15, 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 10.65.10.15, 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 10.65.10.15 to 10.64.10.16 for prot 3 return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 10.65.10.15, 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= 10.65.10.15, 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 10.65.10.15 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 10.65.10.15 (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= 10.65.10.15, 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= 10.65.10.15, 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`

路由器 GRE 传输路由和 Ping

- **show ip route** - 显示 IP 路由表条目。`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
10.0.0.0/24 is subnetted, 1 subnets C 10.1.1.0 is directly connected, Tunnel0 10.0.0.0/24 is
subnetted, 1 subnets C 10.20.20.0 is directly connected, Loopback0 10.0.0.0/24 is subnetted,
1 subnets C 10.22.22.0 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 10.0.0.0/32 is subnetted, 1 subnets O 10.11.11.11 [110/11112] via
10.1.1.1, 03:34:01, Tunnel0 S* 0.0.0.0/0 [1/0] via 192.168.4.1 rodney# rodney#ping
10.11.11.11 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.11.11.11,
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 10.0.0.0/24 is
subnetted, 1 subnets C 1.1.1.0 is directly connected, Tunnel0 10.0.0.0/24 is subnetted, 1
subnets S 10.20.20.0 is directly connected, Tunnel0 10.0.0.0/32 is subnetted, 1 subnets O
10.22.22.22 [110/11112] via 10.1.1.2, 03:33:39, Tunnel0 10.0.0.0/24 is subnetted, 1 subnets
C 10.10.10.0 is directly connected, Loopback0 10.0.0.0/24 is subnetted, 1 subnets C
10.11.11.0 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 10.22.22.22 Type escape
sequence to abort. Sending 5, 100-byte ICMP Echos to 10.22.22.22, timeout is 2 seconds:
!!!!! Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/4 ms
```

相关信息

- IPsec 协商/IKE 协议
- Cisco Secure PIX 防火墙命令参考
- PIX 产品支持
- 技术支持和文档 - Cisco Systems