使用 nat 0 access-list 命令在路由器和 PIX 之间配置 IPSec

目录

简介

本文档介绍了路由器与 Cisco Secure PIX 防火墙之间的 IP 安全 (IPSec) 配置。在总部 LAN 与远程 LAN 之间传输数据流时，我们希望使用专用内部 IP 地址；当用户访问 Internet 时，我们希望将 LAN 主机转换为可路由的 IP 地址。不过，用户也可以使用 **route-map** 命令，在不通过隧道传输数据流的情况下访问 Internet 上的公共页面。

请参阅 ASA/PIX：安全设备到 IOS 路由器 LAN 到 LAN IPsec 隧道配置示例，了解有关路由器与 Cisco 安全设备 PIX/ASA 之间的 LAN 到 LAN 隧道配置方案的更多信息。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

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 12.0(7)T 的 Cisco 路由器
- Cisco PIX 防火墙版本 5.1 (1)

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

背景理论

在 PIX 上，**access-list** 和 **nat 0** 命令协同工作。当10.1.1.0网络的一个用户去10.2.2.0网络时，我们使用访问列表允许10.1.1.0网络流量加密，不用网络地址转换(NAT)。然而，当那些同样用户去别处时，他们翻译对172.17.63.210地址通过端口地址转换(PAT)。在路由器上，**route-map** 和 access-list 命令用于允许 10.2.2.0 网络数据流在没有 NAT 的情况下被加密。然而，当那些同样用户去别处时，他们翻译对172.17.63.210地址通过端口地址转换(PAT)。

要使通过隧道的数据流不经过 PAT，而访问 Internet 的数据流经过 PAT，需要在 PIX 防火墙上执行以下配置命令。

```
access-list nonat permit ip 10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 nat (inside) 0 access-list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
```

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 要查找有关本文档中使用的命令的其他信息，请使用 IOS 命令查找工具。

网络图

本文档使用下图所示的网络设置。

配置

本文档使用如下所示的配置。

总部 PIX

```
PIX Version 5.1(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
!--- Traffic to the router: access-list ipsec permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0 !--- Do
not Network Address Translate (NAT) traffic to the
router: access-list nonat permit ip 10.1.1.0
255.255.255.0 10.2.2.0 255.255.255.0 enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname HQ_PIX fixup protocol ftp 21 fixup
protocol http 80 fixup protocol smtp 25 fixup protocol
h323 1720 fixup protocol rsh 514 fixup protocol sqlnet
1521 names pager lines 24 no logging timestamp no
logging standby no logging console no logging monitor no
logging buffered no logging trap no logging history
logging facility 20 logging queue 512 interface
ethernet0 auto interface ethernet1 auto mtu outside 1500
```

```
mtu inside 1500 ip address outside 172.17.63.213
255.255.255.240 ip address inside 10.1.1.1 255.255.255.0
no failover failover timeout 0:00:00 failover ip address
outside 0.0.0.0 failover ip address inside 0.0.0.0 arp
timeout 14400 global (outside) 1 172.17.63.210 !--- Do
not NAT traffic to the router: nat (inside) 0 access-
list nonat nat (inside) 1 10.1.1.0 255.255.255.0 0 0
conduit permit icmp any any route outside 0.0.0.0
0.0.0.0 172.17.63.209 1 timeout xlate 3:00:00 conn
1:00:00 half-closed 0:10:00 udp 0:02:00 timeout rpc
0:10:00 h323 0:05:00 timeout uauth 0:05:00 absolute aaa-
server TACACS+ protocol tacacs+ aaa-server RADIUS
protocol radius aaa-server partner protocol tacacs+ no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- IPSec policies: sysopt connection permit-
ipsec crypto ipsec transform-set avalanche esp-des esp-
md5-hmac crypto ipsec security-association lifetime
seconds 3600 crypto map forsberg 21 ipsec-isakmp crypto
map forsberg 21 match address ipsec crypto map forsberg
21 set peer 172.17.63.230 crypto map forsberg 21 set
transform-set avalanche crypto map forsberg interface
outside !--- IKE policies: isakmp enable outside isakmp
key westernfinal2000 address 172.17.63.230 netmask
255.255.255.255 isakmp identity address isakmp policy 21
authentication pre-share isakmp policy 21 encryption des
isakmp policy 21 hash md5 isakmp policy 21 group 1
telnet timeout 5 terminal width 80
Cryptochecksum:e36245da9428c4c07b489f787c8ccd3b : end
```

分支路由器

```
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Branch_Router
!
!
!
!
!
!
ip subnet-zero
!
!
!--- IKE policies: crypto isakmp policy 11 hash md5
authentication pre-share crypto isakmp key
westernfinal2000 address 172.17.63.213 ! ! !--- IPSec
policies: crypto ipsec transform-set sharks esp-des esp-
md5-hmac ! ! crypto map nolan 11 ipsec-isakmp set peer
172.17.63.213 set transform-set sharks !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. match address 120 ! ! ! interface
Ethernet0 ip address 172.17.63.230 255.255.255.240 no ip
directed-broadcast ip nat outside no ip route-cache
crypto map nolan ! interface Ethernet1 ip address
10.2.2.1 255.255.255.0 no ip directed-broadcast ip nat
inside ! interface Serial0 no ip address no ip directed-
broadcast no ip mroute-cache shutdown no fair-queue !
interface Serial1 no ip address no ip directed-broadcast
shutdown ! ip nat pool branch 172.17.63.230
```

```
172.17.63.230 netmask 255.255.255.240 !--- Except the
private network from the NAT process: ip nat inside
source route-map nonat pool branch overload ip classless
ip route 0.0.0.0 0.0.0.0 172.17.63.225 no ip http server
!--- Include the private-network-to-private-network
traffic !--- in the encryption process: access-list 120
permit ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255 !---
Except the private network from the NAT process: access-
list 130 deny ip 10.2.2.0 0.0.0.255 10.1.1.0 0.0.0.255
access-list 130 permit ip 10.2.2.0 0.0.0.255 any !---
Except the private network from the NAT process: route-
map nonat permit 10 match ip address 130 ! ! line con 0
transport input none line 1 16 line aux 0 line vty 0 4 !
end
```

验证

本部分所提供的信息可用于确认您的配置是否正常工作。

输出解释器工具支持某些 **show** 命令（只限于注册用户），通过它可以查看 show 命令输出的分析。

- **show crypto isakmp sa** - 查看对等体上的所有当前 IKE 安全连接 (SA)。
- **show crypto ipsec sa** - 显示当前 [IPSec] 安全关联所使用的设置。
- **show crypto engine connections active**-（仅路由器）显示有关加密和解密数据包的当前连接和信息。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

输出解释器工具支持某些 **show** 命令（只限于注册用户），通过它可以查看 show 命令输出的分析。

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

以下在两个 IPSec 对等体上运行以下调试。

- **debug crypto isakmp** -（路由器和 PIX）显示第 1 阶段的错误。
- **debug crypto ipsec** -（路由器和 PIX）显示第 2 阶段的错误。
- **debug crypto engine** -（仅路由器）显示来自加密引擎的信息。

必须在两个对等体上清除安全关联。在启用模式下执行 PIX 命令；在非启用模式下执行路由器命令。

- **clear crypto isakmp sa** - (PIX) 清除第 1 阶段安全关联。
- **clear crypto ipsec sa** - (PIX) 清除第 2 阶段安全关联。
- **clear crypto isakmp** -（路由器）清除第 1 阶段安全关联。
- **clear crypto sa** -（路由器）清除第 2 阶段安全关联。

调试输出示例

- 总部 PIX 调试
- 分支路由器调试

总部 PIX 调试

```
ISAKMP (0): beginning Main Mode exchange
IPSEC(ipsec_encap): crypto map check deny

02303: sa_request,
  (key eng. msg.) src= 172.17.63.213, dest= 172.17.63.230,
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4004


crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority
    21 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_ERRORIPSEC(ipsec_encap): crypto
    map check deny


crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
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_ERRORIPSEC(ipsec_encap):
    crypto map check deny
```

```
crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
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
   -1448244754:a9ad89eeIPSEC(key_engine): got a
   queue even
IPSEC(spi_response): getting spi 0x5cfcf6e9(1560082153)
    for SA from   172.17.63.230 to
    172.17.63.213 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 172.17.63.230,
    dest 172.17.63.213
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID =
    -1448244754

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 #1,
    (key eng. msg.) dest= 172.17.63.230,
    src= 172.17.63.213,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (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 =
     -1448244754

ISAKMP (0): processing ID payload. message ID =
     -1448244754
ISAKMP (0): processing ID payload. message ID =
    -1448244754
ISAKMP (0): processing NOTIFY payload 96 protocol 3
        spi 1510339082, message ID = -1448244754
ISAKMP (0): processing responder lifetime
ISAKMP (0): responder lifetime of
    3600sIPSEC(map_alloc_entry):
    allocating entry 3

IPSEC(map_alloc_entry): allocating entry 4


ISAKMP (0): Creating IPSec SAs
        inbound SA from   172.17.63.230 to
```

```
    172.17.63.213
        (proxy 10.2.2.0 to 10.1.1.0)
        has spi 1560082153 and conn_id 3 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytes
        outbound SA from   172.17.63.213 to
    172.17.63.230
        (proxy 10.1.1.0 to 10.2.2.0)
        has spi 183633242 and conn_id 4 and flags 4
        lifetime of 3600 seconds
        lifetime of 4608000 kilobytesIPSEC(key_engine):
    got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.17.63.213, src=
    172.17.63.230,
    dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x5cfcf6e9(1560082153), conn_id= 3, keysize= 0,
    flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.17.63.213, dest=
    172.17.63.230,
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xaf2055a(183633242), conn_id= 4, keysize= 0,
    flags= 0x4

return status is IKMP_NO_ERROR602301: sa created,
  (sa) sa_dest= 172.17.63.213, sa_prot= 50,
    sa_spi= 0x5cfcf6e9(1560082153),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 3
602301: sa created,
  (sa) sa_dest= 172.17.63.230, sa_prot= 50,
    sa_spi= 0xaf2055a(183633242),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 4
```

分支路由器调试

```
Branch_Router#
01:27:08: ISAKMP (0): received packet from 172.17.63.213
    (N) NEW SA
01:27:08: ISAKMP (0:1): processing SA payload.
    message ID = 0
01:27:08: ISAKMP (0:1): Checking ISAKMP transform 1
    against priority 11 policy
01:27:08: ISAKMP:      encryption DES-CBC
01:27:08: ISAKMP:      hash MD5
01:27:08: ISAKMP:      default group 1
01:27:08: ISAKMP:      auth pre-share
01:27:08: ISAKMP:      life type in seconds
01:27:08: ISAKMP:      life duration (basic) of 3600
01:27:08: ISAKMP (0:1): atts are acceptable. Next
    payload is 0
01:27:08: CryptoEngine0: generate alg parameter
01:27:10: CRYPTO_ENGINE: Dh phase 1 status: 0
01:27:10: CRYPTO_ENGINE: Dh phase 1 status: 0
01:27:10: ISAKMP (0:1): SA is doing pre-shared key
    authentication
01:27:10: ISAKMP (1): SA is doing pre-shared key
    authentication using id type ID_IPV4_ADDR
```

```
01:27:10: ISAKMP (1): sending packet to 172.17.63.213
    (R) MM_SA_SETUP
01:27:10: ISAKMP (1): received packet from 172.17.63.213
    (R) MM_SA_SETUP
01:27:10: ISAKMP (0:1): processing KE payload. message
    ID = 0
01:27:10: CryptoEngine0: generate alg parameter
01:27:12: ISAKMP (0:1): processing NONCE payload.
    message ID = 0
01:27:12: CryptoEngine0: create ISAKMP SKEYID for
    conn id 1
01:27:12: ISAKMP (0:1): SKEYID state generated
01:27:12: ISAKMP (0:1): processing vendor id payload
01:27:12: ISAKMP (0:1): speaking to another IOS box!
01:27:12: ISAKMP (1): sending packet to 172.17.63.213 (R)
    MM_KEY_EXCH
01:27:12: ISAKMP (1): received packet from 172.17.63.213
    (R) MM_KEY_EXCH
01:27:12: ISAKMP (0:1): processing ID payload.
    message ID = 0
01:27:12: ISAKMP (0:1): processing HASH payload.
    message ID = 0
01:27:12: CryptoEngine0: generate hmac context for
    conn id 1
01:27:12: ISAKMP (0:1): SA has been authenticated
    with 172.17.63.213
01:27:12: ISAKMP (1): ID payload
        next-payload : 8
        type         : 1
        protocol     : 17
        port         : 500
        length       : 8
01:27:12: ISAKMP (1): Total payload length: 12
01:27:12: CryptoEngine0: generate hmac context
    for conn id 1
01:27:12: CryptoEngine0: clear dh number for
    conn id 1
01:27:12: ISAKMP (1): sending packet to
    172.17.63.213 (R) QM_IDLE
01:27:12: ISAKMP (1): received packet from
    172.17.63.213 (R) QM_IDLE
01:27:12: CryptoEngine0: generate hmac context for
    conn id 1
01:27:12: ISAKMP (0:1): processing SA payload.
    message ID = -1448244754
01:27:12: ISAKMP (0:1): Checking IPSec proposal 1
01:27:12: ISAKMP: transform 1, ESP_DES
01:27:12: ISAKMP:   attributes in transform:
01:27:12: ISAKMP:      encaps is 1
01:27:12: ISAKMP:      SA life type in seconds
01:27:12: ISAKMP:      SA life duration (basic)
    of 28800
01:27:12: ISAKMP:      SA life type in kilobytes
01:27:12: ISAKMP:      SA life duration (VPI) of
    0x0 0x46 0x50 0x0
01:27:12: ISAKMP:      authenticator is HMAC-MD5
01:27:12: validate proposal 0
01:27:12: ISAKMP (0:1): atts are acceptable.
01:27:12: IPSEC(validate_proposal_request):
    proposal part #1, (key eng. msg.)
    dest= 172.17.63.230, src= 172.17.63.213,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
```

```
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
01:27:13: validate proposal request 0
01:27:13: ISAKMP (0:1): processing NONCE payload.
    message ID = -1448244754
01:27:13: ISAKMP (0:1): processing ID payload.
    message ID = -1448244754
01:27:13: ISAKMP (1): ID_IPV4_ADDR_SUBNET src
    10.1.1.0/255.255.255.0 prot 0 port 0
01:27:13: ISAKMP (0:1): processing ID payload.
    message ID = -1448244754
01:27:13: ISAKMP (1): ID_IPV4_ADDR_SUBNET dst
    10.2.2.0/255.255.255.0 prot 0 port 0
01:27:13: IPSEC(key_engine): got a queue event...
01:27:13: IPSEC(spi_response): getting spi 183633242
    for SA
    from 172.17.63.213 to 172.17.63.230 for prot 3
01:27:13: CryptoEngine0: generate hmac context for
    conn id 1
01:27:13: ISAKMP (1): sending packet to 172.17.63.213
    (R) QM_IDLE
01:27:13: ISAKMP (1): received packet from 172.17.63.213
    (R) QM_IDLE
01:27:13: CryptoEngine0: generate hmac context
    for conn id 1
01:27:13: ipsec allocate flow 0
01:27:13: ipsec allocate flow 0
01:27:13: ISAKMP (0:1): Creating IPSec SAs
01:27:13:         inbound SA from 172.17.63.213
    to 172.17.63.230  (proxy 10.1.1.0 to 10.2.2.0)
01:27:13:         has spi 183633242 and conn_id 2000
    and flags 4
01:27:13:         lifetime of 28800 seconds
01:27:13:         lifetime of 4608000 kilobytes
01:27:13:         outbound SA from 172.17.63.230
    to 172.17.63.213  (proxy 10.2.2.0 to 10.1.1.0)
01:27:13:         has spi 1560082153 and conn_id
    2001 and flags 4
01:27:13:         lifetime of 28800 seconds
01:27:13:         lifetime of 4608000 kilobytes
01:27:13: ISAKMP (0:1): deleting node -1448244754
01:27:13: IPSEC(key_engine): got a queue event...
01:27:13: IPSEC(initialize_sas): ,
   (key eng. msg.) dest= 172.17.63.230, src=
    172.17.63.213,
    dest_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0xAF2055A(183633242), conn_id= 2000,
    keysize= 0, flags= 0x4
01:27:13: IPSEC(initialize_sas): ,
   (key eng. msg.) src= 172.17.63.230,
    dest= 172.17.63.213,
    src_proxy= 10.2.2.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.1.1.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-des esp-md5-hmac ,
    lifedur= 28800s and 4608000kb,
    spi= 0x5CFCF6E9(1560082153), conn_id= 2001,
    keysize= 0, flags= 0x4
01:27:13: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.17.63.230, sa_prot= 50,
    sa_spi= 0xAF2055A(183633242),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2000
```

```
01:27:13: IPSEC(create_sa): sa created,
  (sa) sa_dest= 172.17.63.213, sa_prot= 50,
    sa_spi= 0x5CFCF6E9(1560082153),
    sa_trans= esp-des esp-md5-hmac , sa_conn_id= 2001
```

相关信息

- PIX IPSec
- 请求注解 (RFC)
- 技术支持 - Cisco Systems