配置 Cisco Pix 防火墙和 NetScreen 防火墙之间的 IPSec LAN 到 LAN 隧道

目录

简介

本文档介绍使用最新软件在 Cisco PIX 防火墙和 NetScreen 防火墙之间创建 IPSec LAN 到 LAN 隧道的必要步骤。每个通过 IPSec 隧道与其他防火墙通信的设备后面都有一个专用网络。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 在受信/非受信接口上，使用 IP 地址对 NetScreen 防火墙进行配置。
- 建立与 Internet 的连接。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- PIX 防火墙软件版本 6.3(1)
- NetScreen 最新版本

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

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

配置

本文档使用以下配置：

- PIX 防火墙
- NetScreen 防火墙

配置 PIX 防火墙

PIX 防火墙

```
PIX Version 6.3(1)
interface ethernet0 10baset
interface ethernet1 100full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
domain-name cisco.com
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol ils 389
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
names
!--- Access control list (ACL) for interesting traffic
to be encrypted and !--- to bypass the Network Address
Translation (NAT) process. access-list nonat permit ip
10.0.25.0 255.255.255.0 10.0.3.0 255.255.255.0 pager
lines 24 logging on logging timestamp logging buffered
```

```
debugging icmp permit any inside mtu outside 1500 mtu
inside 1500 !--- IP addresses on the interfaces. ip
address outside 172.18.124.96 255.255.255.0 ip address
inside 10.0.25.254 255.255.255.0 ip audit info action
alarm ip audit attack action alarm pdm logging
informational 100 pdm history enable arp timeout 14400
global (outside) 1 interface !--- Bypass of NAT for
IPsec interesting inside network traffic. nat (inside) 0
access-list nonat nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !--
- Default gateway to the Internet. route outside 0.0.0.0
0.0.0.0 172.18.124.1 1 timeout xlate 0:05:00 timeout
conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00
h225 1:00:00 timeout h323 0:05:00 mgcp 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 local http
10.0.0.0 255.0.0.0 inside no snmp-server location no
snmp-server contact snmp-server community public no
snmp-server enable traps floodguard enable !--- This
command avoids applied ACLs or conduits on encrypted
packets. sysopt connection permit-ipsec !---
Configuration of IPsec Phase 2. crypto ipsec transform-
set mytrans esp-3des esp-sha-hmac crypto map mymap 10
ipsec-isakmp crypto map mymap 10 match address nonat
crypto map mymap 10 set pfs group2 crypto map mymap 10
set peer 172.18.173.85 crypto map mymap 10 set
transform-set mytrans crypto map mymap interface outside
!--- Configuration of IPsec Phase 1. isakmp enable
outside !--- Internet Key Exchange (IKE) pre-shared key
!--- that the peers use to authenticate. isakmp key
testme address 172.18.173.85 netmask 255.255.255.255
isakmp identity address isakmp policy 10 authentication
pre-share isakmp policy 10 encryption 3des isakmp policy
10 hash sha isakmp policy 10 group 2 isakmp policy 10
lifetime 86400 telnet timeout 5 ssh timeout 5 console
timeout 0 dhcpd lease 3600 dhcpd ping_timeout 750
terminal width 80
```

配置 NetScreen 防火墙

完成以下步骤，以便配置 NetScreen 防火墙。

1. 选择 **Lists > Address**，转至 Trusted 选项卡，然后单击 New Address。
2. 添加在隧道上加密的 NetScreen 内部网络，并单击 **OK**。**注意：** 确保已选择 Trust 选项。此示例采用网络 10.0.3.0，其掩码为 255.255.255.0。
3. 选择 **Lists > Address**，转至 Untrusted 选项卡，然后单击 New Address。
4. 添加 NetScreen 防火墙对数据包加密时所采用的远程网络，然后单击 **OK**。**注意：** 当您配置连接非 NetScreen 网关的 VPN 时，请勿使用地址组。如果使用地址组，VPN 互操作将失败。当使用地址组时，非 NetScreen 安全网关不知道如何解释 NetScreen 创建的代理 ID。此问题有几种解决方法：将地址组划分到各个通讯簿条目。根据每个通讯簿条目指定单独的策略。如有可能，请在非 NetScreen 网关（防火墙设备）上将代理 ID 配置为 0.0.0.0/0。此示例采用网络 10.0.25.0，其掩码为 255.255.255.0。
5. 选择 **Network > VPN**，转至 Gateway 选项卡，然后单击 New Remote Tunnel Gateway 以配置 VPN 网关（阶段 1 和阶段 2 IPsec 策略）。
6. 使用 PIX 外部接口的 IP 地址以便终止隧道，并配置要绑定的 Phase1 IKE 选项。完成后，单击**确定**。此示例采用以下字段和值。**Gateway Name：**To501**Static IP Address：**172.18.124.96**模式：**Main (ID Protection)**Preshared Key：**“testme”**Phase 1**

proposal：pre-g2-3des-sha成功创建远程隧道网关之后，将显示一个类似如下的屏幕。

7. 转至 P1 Proposal 选项卡，并单击 **New Phase 1 Proposal** 以配置提案 1。
8. 输入 Phase 1 Proposal 的配置信息，然后单击 **OK**。此示例对阶段 1 交换采用以下字段和值。**名称**：ToPix501**验证**：Preshare**DH Group**：第 2 组**加密**：3DES-CBC**哈希**：SHA-1**寿命**：3600 秒将阶段 1 成功添加到 NetScreen 配置之后，将显示一个类似如下的屏幕。
9. 转至 P2 Proposal 选项卡，并单击 **New Phase 2 Proposal** 以配置阶段 2。
10. 输入 Phase 2 Proposal 的配置信息，然后单击 **OK**。此示例对阶段 2 交换采用以下字段和值。**名称**：ToPix501**Perfect Forward Secrecy**：DH-2（1024 位）**加密算法:**3DES-CBC**Authentication Algorithm**：SHA-1**寿命**：26400 秒将阶段 2 成功添加到 NetScreen 配置之后，将显示一个类似如下的屏幕。
11. 选择 **AutoKey IKE** 选项卡，然后单击 New AutoKey IKE Entry 以创建和配置 AutoKeys IKE。
12. 输入 AutoKey IKE 的配置信息，然后单击 **OK**。此示例对 AutoKey IKE 采用以下字段和值。**名称**：VPN-1**Remote Gateway Tunnel Name**：To501（以前在 Gateway 选项卡上创建。）**Phase 2 Proposal**：ToPix501（以前在 P2 Proposal 选项卡上创建。）**VPN Monitor**：Enable (event)（此设置使 NetScreen 设备能够设置简单网络管理协议 [SNMP] 陷阱，以监控 VPN Monitor 的运行状况。）成功配置 VPN-1 规则之后，将显示一个类似如下的屏幕。
13. 选择 **Network > Policy**，转至 Outgoing 选项卡，然后单击 New Policy 以配置允许对 IPsec 流量加密的规则。
14. 输入策略的配置信息，并单击 **OK**。此示例对该策略采用以下字段和值。Name 字段是可选的，此示例未采用该字段。**源地址**：InsideNetwork（以前在 Trusted 选项卡上定义。）**目的地址**：RemoteNetwork（以前在 Untrusted 选项卡上定义。）**服务**：任一**操作**：通道**VPN Tunnel**：VPN-1（以前在 AutoKey IKE 选项卡上定义为 VPN 隧道。）**Modify matching incoming VPN policy**：已勾选（该选项自动创建与外部网络 VPN 流量匹配的入站规则。）
15. 添加策略时，请确保出站 VPN 规则位于策略列表之首。（为入站流量自动创建的规则位于 Incoming 选项卡上。）如果需要更改策略的顺序，请完成以下步骤：单击 Outgoing 选项卡。单击 Configure 列中的圆形箭头，以便显示 Move Policy Micro 窗口。更改策略顺序，以便 VPN 策略位于策略 ID 0 上（这样 VPN 策略处于列表上端）。转至 Incoming 选项卡，以便查看入站流量的规则。

验证

本部分提供的信息可用于确认您的配置是否工作正常。

验证命令

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。

- **ping** - 诊断基本网络连接。
- **show crypto ipsec sa** - 显示阶段 2 的安全关联。
- **show crypto isakmp sa** - 显示第 1 阶段的安全关联。

验证输出

下面显示了 **ping** 和 show 命令的示例输出。

此 ping 操作从 NetScreen 防火墙后的主机启动。

```
C:\>ping 10.0.25.1 -t Request timed out. Request timed out. Reply from 10.0.25.1: bytes=32
time<105ms TTL=128 Reply from 10.0.25.1: bytes=32 time<114ms TTL=128 Reply from 10.0.25.1:
bytes=32 time<106ms TTL=128 Reply from 10.0.25.1: bytes=32 time<121ms TTL=128 Reply from
10.0.25.1: bytes=32 time<110ms TTL=128 Reply from 10.0.25.1: bytes=32 time<116ms TTL=128 Reply
from 10.0.25.1: bytes=32 time<109ms TTL=128 Reply from 10.0.25.1: bytes=32 time<110ms TTL=128
Reply from 10.0.25.1: bytes=32 time<118ms TTL=128
```

下面显示了 **show crypto ipsec sa** 命令的输出。

```
pixfirewall(config)#show crypto ipsec sa interface: outside Crypto map tag: mymap, local addr.
172.18.124.96 local ident (addr/mask/prot/port): (10.0.25.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (10.0.3.0/255.255.255.0/0/0) current_peer: 172.18.173.85:500 PERMIT,
flags={origin_is_acl,} #pkts encaps: 11, #pkts encrypt: 11, #pkts digest 11 #pkts decaps: 11,
#pkts decrypt: 13, #pkts verify 13 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 0, #recv errors
1 local crypto endpt.: 172.18.124.96, remote crypto endpt.: 172.18.173.85 path mtu 1500, ipsec
overhead 56, media mtu 1500 current outbound spi: f0f376eb inbound esp sas: spi:
0x1225ce5c(304467548) transform: esp-3des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 3, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607974/24637) IV
size: 8 bytes replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas:
spi: 0xf0f376eb(4042487531) transform: esp-3des esp-sha-hmac , in use settings ={Tunnel, } slot:
0, conn id: 4, crypto map: mymap sa timing: remaining key lifetime (k/sec): (4607999/24628) IV
size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
```

下面显示了 **show crypto isakmp sa** 命令的输出。

```
pixfirewall(config)#show crypto isakmp sa Total : 1 Embryonic : 0 dst src state pending created
172.18.124.96 172.18.173.85 QM_IDLE 0 1
```

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

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

- **debug crypto engine** - 显示有关加密引擎的消息。
- **debug crypto ipsec** - 显示有关 IPsec 事件的信息。
- **debug crypto isakmp** — 显示关于 IKE 事件的消息。

调试输出示例

下面显示了 PIX 防火墙的示例调试输出。

```
debug crypto engine
debug crypto ipsec
debug crypto isakmp

crypto_isakmp_process_block:src:172.18.173.85,
  dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing SA payload. message ID = 0

ISAKMP (0): Checking ISAKMP transform 1 against priority 10 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
```

```
ISAKMP:      default group 2
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (basic) of 28800
ISAKMP (0): atts are acceptable. Next payload is 0
ISAKMP (0): processing vendor id payload

ISAKMP (0): processing vendor id payload

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:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
OAK_MM exchange
ISAKMP (0): processing KE payload. message ID = 0

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

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
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): 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
ISAKMP (0): sending INITIAL_CONTACT notify
ISAKMP (0): sending NOTIFY message 24578 protocol 1
VPN Peer: ISAKMP: Added new peer: ip:172.18.173.85/500
   Total VPN Peers:1
VPN Peer: ISAKMP: Peer ip:172.18.173.85/500 Ref cnt
   incremented to:1
   Total VPN Peers:1
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
ISAKMP (0): processing DELETE payload. message ID = 534186807,
   spi size = 4IPSEC(key_engin
e): got a queue event...
IPSEC(key_engine_delete_sas): rec'd delete notify from ISAKMP
IPSEC(key_engine_delete_sas):
   delete all SAs shared with 172.18.173.85

return status is IKMP_NO_ERR_NO_TRANS
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode: OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 4150037097

ISAKMP : Checking IPSec proposal 1

ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      SA life type in seconds
ISAKMP:      SA life duration (VPI) of 0x0 0x0 0x67 0x20
```

```
ISAKMP:      encaps is 1
ISAKMP:      authenticator is HMAC-SHA
ISAKMP:      group is 2
ISAKMP (0): atts are acceptable.
IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,
    dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x24

ISAKMP (0): processing NONCE payload. message ID = 4150037097

ISAKMP (0): processing KE payload. message ID = 4150037097

ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (0): ID_IPV4_ADDR_SUBNET src 10.0.3.0/255.255.255.0
   prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 4150037097
ISAKMP (0): ID_IPV4_ADDR_SUBNET dst 10.0.25.0/255.255.255.0
   prot 0 port 0IPSEC(key_engine)
: got a queue event...
IPSEC(spi_response): getting spi 0x1225ce5c(304467548) for SA
        from   172.18.173.85 to   172.18.124.96 for prot 3

return status is IKMP_NO_ERROR
crypto_isakmp_process_block:src:172.18.173.85,
   dest:172.18.124.96 spt:500 dpt:500
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAITmap_alloc_entry: allocating entry 3
map_alloc_entry: allocating entry 4

ISAKMP (0): Creating IPSec SAs
        inbound SA from 172.18.173.85 to 172.18.124.96
          (proxy 10.0.3.0 to 10.0.25.0)
        has spi 304467548 and conn_id 3 and flags 25
        lifetime of 26400 seconds
        outbound SA from 172.18.124.96 to 172.18.173.85
          (proxy 10.0.25.0 to 10.0.3.0)
        has spi 4042487531 and conn_id 4 and flags 25
        lifetime of 26400 secondsIPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 172.18.124.96, src= 172.18.173.85,
    dest_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
    src_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 26400s and 0kb,
    spi= 0x1225ce5c(304467548), conn_id= 3,
       keysize= 0, flags= 0x25
IPSEC(initialize_sas): ,
  (key eng. msg.) src= 172.18.124.96, dest= 172.18.173.85,
    src_proxy= 10.0.25.0/255.255.255.0/0/0 (type=4),
    dest_proxy= 10.0.3.0/255.255.255.0/0/0 (type=4),
    protocol= ESP, transform= esp-3des esp-sha-hmac ,
    lifedur= 26400s and 0kb,
    spi= 0xf0f376eb(4042487531), conn_id= 4, keysize= 0, flags= 0x25

VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
   incremented to:2 Total VPN Peers:1
VPN Peer: IPSEC: Peer ip:172.18.173.85/500 Ref cnt
   incremented to:3 Total VPN Peers:1
return status is IKMP_NO_ERROR
```

相关信息

- IPsec 协商/IKE 协议
- Cisco PIX 防火墙软件
- Cisco Secure PIX 防火墙命令参考
- 安全产品 Field Notices（包括 PIX）
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems