PIX 6.x ：静态寻址的PIX防火墙和动态寻址的带NAT的IOS路由器之间的动态IPSec配置示例

目录

简介

本文档对于如何使 PIX 接受动态 IPsec 连接提供了一个示例配置。如果专用网络 10.1.1.x 接入 Internet，则远程路由器将执行网络地址转换 (NAT)。从10.1.1.x到PIX后面的专用网络192.168.1.x的数据流被排除在NAT程序之外。路由器可以发起到 PIX 的连接，但 PIX 无法发起到路由器的连接。

此配置使用 PIX 防火墙与 Cisco IOS® 路由器之间创建动态 IPsec LAN 到 LAN (L2L) 隧道，这些隧道在其公共接口（外部接口）上接收动态 IP 地址。动态主机配置协议 (DHCP) 提供一种机制，以便动态地从服务提供商 (ISP) 分配 IP 地址。这样，当主机不再需要这些 IP 地址时，就可以重用它们。

有关路由器从运行 6.x 版软件的 PIX 安全设备接受动态 IPsec 连接的情况的详细信息，请参阅路由器到 PIX 的动态到静态 IPsec（含 NAT）配置示例。

要启用 PIX/ASA 安全设备以接受来自 Cisco IOS 路由器的动态 IPsec 连接，请参阅静态 IOS 路由器和使用 NAT 的动态 PIX/ASA 7.x 之间 IPsec 配置示例。

要了解有关 PIX/ASA 安全设备运行 7.x 及更高软件版本的同一方案的详细信息，请参阅对 NAT 配置静态 PIX/ASA 7.x 和动态 IOS 路由器之间的 IPsec 的示例。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 软件版本 12.4
- Cisco PIX 防火墙软件 6.3.1 版
- Cisco Secure PIX 防火墙 515E
- Cisco 7206 路由器

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： 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

本文档使用此网络设置。

配置

本文档使用以下配置。

- Elf (PIX)
- Mop（Cisco 7204 路由器）

Elf (PIX)

```
Building configuration...
: Saved
:
PIX Version 6.3(1)
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
!--- Access control list (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
!-- Binds 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
!--- Permits Internet Control Message Protocol (ICMP)
traffic for testing. !--- Do not enable it in a live
network. 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
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy for accepting dynamic
connections from remote PIX. !--- Note: In real show run
output, the pre-shared key appears as *******. isakmp
key cisco123 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 路由器）

```
mop#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
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
!
!--- Internet Key Exchange (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 dhcp
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 Ethernet1/0
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
```

验证

使用本部分可确认配置能否正常运行。

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。

可以在 PIX 上和路由器上运行以下这些 **show** 命令。

- **show crypto isakmp sa** — 显示对等体上的所有当前 IKE 安全关联 (SA)。
- **show crypto ipsec sa** - 显示当前 (IPsec) SA 所采用的设置。
- **show crypto engine connections active** - 显示有关加密和解密数据包（仅限路由器）的当前连接和信息。

必须在两个对等体上都清除 SA。

- 在配置模式下执行以下 PIX 命令。**clear crypto isakmp sa** — 清除第 1 阶段 SA。**clear crypto ipsec sa** - 清除第 2 阶段的 SA。
- 在启用模式下执行以下路由器命令。**clear crypto isakmp** - 清除第 1 阶段的 SA。**clear crypto sa** - 清除第 2 阶段的 SA。

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

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。

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。
- **show crypto ipsec sa** - 显示当前 (IPsec) SA 所采用的设置。
- **show crypto engine connections active** - 显示有关加密和解密数据包（仅限路由器）的当前连接和信息。

相关信息

- **IPsec 协商/IKE 协议支持页**
- **PIX 500 系列安全设备**
- **Cisco Secure PIX 防火墙命令参考**
- **请求注解 (RFC)**
- **技术支持和文档 - Cisco Systems**