PIX 6.x ：在静态寻址IOS路由器和动态地寻址的带有NAT的PIX防火墙之间的动态IPSec配置示例

Contents

Introduction

本文提供如何显示您enable (event)接受从PIX防火墙的动态IPSec连接的IOS ®路由器的一配置示例。如果专用网络 10.0.0.x 访问 Internet，则远程路由器会执行网络地址转换 (NAT)。NAT 进程中不包括从 10.0.0.x 到 PIX 之后专用网络 10.1.0.x 的数据流。PIX 防火墙可以发起与路由器的连接，但路由器无法发起与 PIX 的连接。

此配置使用 Cisco IOS 路由器以创建与 PIX 防火墙之间的动态 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) 提供一种从 Internet 服务提供商 (ISP) 动态分配 IP 地址的机制。这样，当主机不再需要这些 IP 地址时，就可以重用它们。

要了解有关 Cisco PIX 安全设备运行软件版本 6.x 的相同方案的详细信息，请参阅 PIX 6.x：使用 NAT 在静态寻址的 PIX 防火墙和动态寻址的 IOS 路由器之间配置动态 IPsec 的配置示例，以获取有关 PIX 接受来自路由器的动态 IPsec 连接的方案的详细信息。

有关详细信息，请参阅 PIX/ASA 7.x 及更高版本：使用 NAT 在静态寻址的 PIX 和动态寻址的 IOS 路由器之间配置动态 IPsec 的配置示例，以使 PIX/ASA 安全设备可以接受来自 IOS 路由器的动态 IPsec 连接。

有关详细信息，请参阅 PIX/ASA 7.x 及更高版本：使用 NAT 在静态寻址的 IOS 路由器和动态寻址的 PIX 之间配置动态 IPsec 的配置示例，以了解有关 PIX/ASA 安全设备运行软件版本 7.x 及更高版本的同一方案的详细信息。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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 6.3.4 版
- Cisco Secure PIX 防火墙 515E
- Cisco 2811 路由器

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

Refer to Cisco Technical Tips Conventions for more information on document conventions.

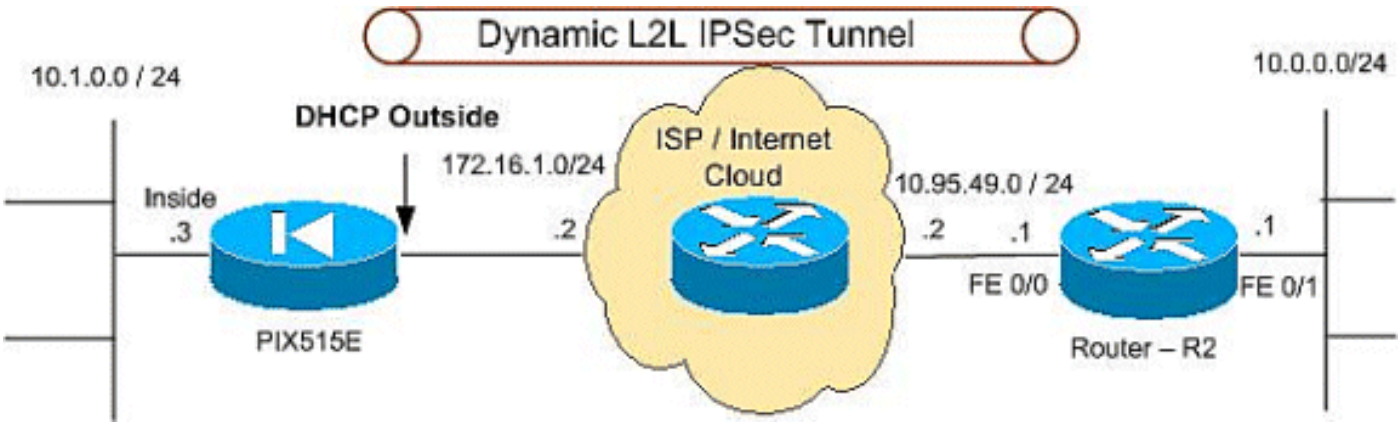
Configure

本部分提供有关如何配置本文档所述功能的信息。

Note: 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）。

Network Diagram

本文档使用以下网络设置：



配置

本文档使用以下配置：

- PIX 515E
- R2（Cisco 2811 路由器）

PIX 515E

```
PIX Version 6.3(4)
interface ethernet0 100full
interface ethernet1 100full
interface ethernet2 shut
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security4
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX515E
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

!--- The access control list (ACL) to avoid NAT on the
IPsec packets. access-list NO-NAT permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
!--- The ACL to apply on crypto map. !--- Include the
private-network-to-private-network traffic !--- in the
encryption process. access-list 101 permit ip 10.1.0.0
255.255.255.0 10.0.0.0 255.255.255.0
pager lines 24
logging on
mtu outside 1500
mtu inside 1500
mtu intf2 1500
!--- ISP will providthe the Outside IP address.
ip address outside dhcp

ip address inside 10.1.0.3 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list NO-NAT
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 10.0.0.0 255.255.255.0 172.16.1.5 1
timeout xlate 3:00:00
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 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 configuration, Phase 2. crypto ipsec
transform-set DYN-TS esp-des esp-md5-hmac
crypto map IPSEC 10 ipsec-isakmp
crypto map IPSEC 10 match address 101
crypto map IPSEC 10 set peer 10.95.49.1
crypto map IPSEC 10 set transform-set DYN-TS
crypto map IPSEC interface outside
!--- Internet Security Association and Key Management
Protocol (ISAKMP) !--- policy, Phase 1. !--- Note: In
real show run output, the pre-shared key appears as
*******.

isakmp enable outside
isakmp key cisco123 address 10.95.49.1 netmask
255.255.255.255
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
console timeout 0
terminal width 80
Cryptochecksum:f0294298e214a947fc2e03f173e4a405
: end
```

R2（Cisco 2811 路由器）

```
R2#show running-configuration
Building configuration...

Current configuration : 1916 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname r1800
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
```

```
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
no ftp-server write-enable
!
!
!--- ISAKMP policy, Phase 1. crypto isakmp policy 10
hash md5
authentication pre-share
crypto isakmp key 6 cisco123 address 0.0.0.0 0.0.0.0
!
!
!--- IPsec policy, Phase 2. crypto ipsec transform-set
DYN-TS esp-des esp-md5-hmac
!
crypto dynamic-map DYN 10
set transform-set DYN-TS
match address 101
!
!
crypto map IPSEC 10 ipsec-isakmp dynamic DYN
!
!
!
interface FastEthernet0/0
ip address 10.95.49.1 255.255.255.0
ip nat outside
ip virtual-reassembly
load-interval 30
duplex auto
speed auto
crypto map IPSEC
!
interface FastEthernet0/1
ip address 10.0.0.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
!
ip classless
ip route 10.1.0.0 255.255.255.0 10.95.49.2
!
ip http server
no ip http secure-server
!--- Except the private network from the NAT process. ip
nat inside source list 102 interface FastEthernet0/0
overload
!
!--- Include the private-network-to-private-network !---
traffic in the encryption process. access-list 101
permit ip 10.0.0.0 0.0.0.255 10.1.0.0 0.0.0.255
```

```
!--- Except the private network from the NAT process.
access-list 102 deny ip 10.0.0.0 0.0.0.255 10.1.0.0
0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!
!
control-plane
!
!
line con 0
exec-timeout 0 0
line aux 0
line vty 0 4
exec-timeout 0 0
login
!
end
```

Verify

Use this section to confirm that your configuration works properly.

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。

- **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。

Troubleshoot

使用本部分可排除配置故障。

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。

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

- **show crypto isakmp sa** - 查看对等体上当前的所有 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。

Related Information

- **最常用的 L2L 和远程访问 IPSec VPN 故障排除解决方案**
- **Cisco PIX 防火墙软件**
- **Cisco Secure PIX防火墙命令参考**
- **请求注解 (RFC)**
- **IPsec 协商/IKE 协议**