PIX 6.x :使用NAT在靜態定址PIX防火牆和動態定址IOS路由器之間的動態IPsec配置示例

目錄

簡介

本文檔提供了如何啟用PIX以接受動態IPsec連線的示例配置。如果私有網路10.1.1.x訪問網際網路，遠端路由器將執行網路地址轉換(NAT)。從10.1.1.x到PIX後方的專用網路192.168.1.x的流量不屬於NAT過程。路由器可以啟動與PIX的連線，但PIX無法啟動與路由器的連線。

此配置使用PIX防火牆來建立動態IPsec LAN到LAN(L2L)隧道，該隧道帶有在其公共介面（外部介面）上接收動態IP地址的Cisco IOS®路由器。 動態主機設定通訊協定(DHCP)提供了一種機制，以便從服務提供商(ISP)動態分配IP位址。 這樣，當主機不再需要時，就可以重新使用IP地址。

有關路由器接受來自運行6.x的PIX安全裝置的動態IPsec連線的方案的詳細資訊，請參閱路由器到PIX的動態到靜態IPsec的NAT配置示例。

請參閱靜態IOS路由器與帶NAT的動態PIX/ASA 7.x之間的IPsec配置示例，以啟用PIX/ASA安全裝置來接受來自Cisco IOS路由器的動態IPsec連線。

請參閱靜態PIX/ASA 7.x與帶NAT的動態IOS路由器之間的IPsec配置示例，以瞭解有關PIX/ASA安全裝置運行軟體版本7.x及更高版本的相同方案的詳細資訊。

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco IOS軟體版本12.4
- Cisco PIX防火牆軟體版本6.3.1
- Cisco安全PIX防火牆515E
- 思科7206路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

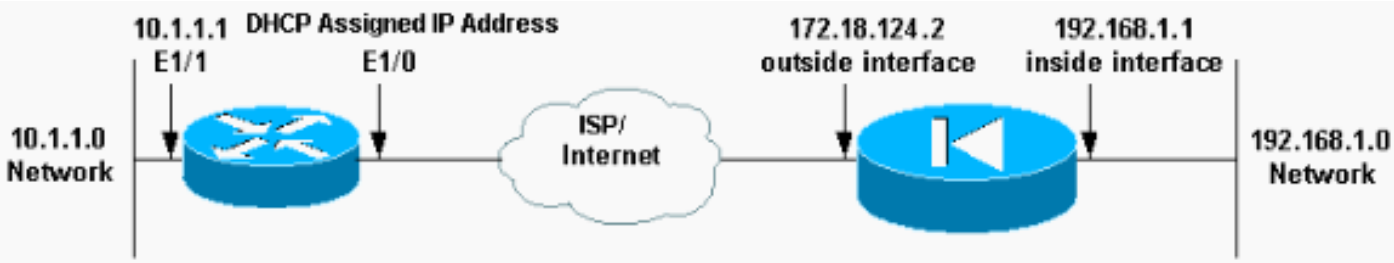
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用Command Lookup Tool(僅限註冊客戶)查詢有關本文檔中使用的命令的更多資訊。

網路圖表

本檔案會使用此網路設定。



組態

本檔案會使用這些設定。

- 精靈(PIX)
- Mop（思科7204路由器）

精靈(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 (思科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
```

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些show命令。使用OIT檢視show命令輸出的分析。

您可以在PIX和路由器上運行這些show命令。

- show crypto isakmp sa — 顯示對等體上的所有當前IKE安全關聯(SA)。
- show crypto ipsec sa — 顯示當前(IPsec)SA使用的設定。
- show crypto engine connections active — 顯示當前連線以及有關加密和解密資料包的資訊（僅限路由器）。

您必須清除兩個對等體上的SA。

- PIX命令在配置模式下執行。clear crypto isakmp sa — 清除第1階段SA。clear crypto ipsec sa — 清除第2階段SA。
- 路由器命令在啟用模式下執行。clear crypto isakmp — 清除第1階段SA。clear crypto sa — 清

除第2階段SA。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

疑難排解指令

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

附註：使用 **debug** 指令之前，請先參閱有關 Debug 指令的重要資訊。

- **show crypto isakmp sa** — 顯示對等體上的所有當前IKE SA。
- **show crypto ipsec sa** — 顯示當前(IPsec)SA使用的設定。
- **show crypto engine connections active** — 顯示當前連線以及有關加密和解密資料包的資訊（僅限路由器）。

相關資訊

- IPsec協商/IKE通訊協定支援頁面
- PIX 500系列安全裝置
- Cisco Secure PIX防火牆命令參考
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems