PIX 6.x:정적으로 주소가 지정된 PIX 방화벽과 NAT 컨피그레이션을 사용하는 동적으로 주소가 지정된 IOS 라우터 간의 동적 IPsec 예

목차

소개

이 문서에서는 PIX가 동적 IPsec 연결을 수락하도록 하는 방법에 대한 샘플 컨피그레이션을 제공합니다.사설 네트워크 10.1.1.x가 인터넷에 액세스하는 경우 원격 라우터는 NAT(Network Address Translation)를 수행합니다.10.1.1.x에서 PIX를 따르는 프라이빗 네트워크 192.168.1.x로의 트래픽은 NAT 프로세스에서 제외됩니다.라우터는 PIX에 대한 연결을 시작할 수 있지만 PIX는 라우터에 대한 연결을 시작할 수 없습니다.

이 컨피그레이션에서는 PIX 방화벽을 사용하여 공용 인터페이스(외부 인터페이스)에서 동적 IP 주소를 수신하는 Cisco IOS® 라우터를 사용하여 동적 IPsec LAN-to-LAN(L2L) 터널을 생성합니다. DHCP(Dynamic Host Configuration Protocol)는 ISP(Service Provider)에서 동적으로 IP 주소를 할당하는 메커니즘을 제공합니다. 이렇게 하면 호스트가 더 이상 필요하지 않을 때 IP 주소를 재사용할 수 있습니다.

라우터가 6.x를 실행하는 PIX Security Appliance에서 동적 IPsec 연결을 수락하는 시나리오에 대한 자세한 내용은 NAT 컨피그레이션이 있는 Router-to-PIX Dynamic-to-Static IPsec 예를 참조하십시오.

PIX/ASA Security Appliance가 Cisco IOS 라우터에서 동적 IPsec 연결을 허용하도록 하려면 고정 IOS 라우터와 NAT가 있는 동적 PIX/ASA 7.x 간 IPsec를 참조하십시오.

PIX/ASA Security Appliance에서 소프트웨어 버전 7.x 이상을 실행하는 동일한 시나리오에 대한 자세한 내용은 고정 PIX/ASA 7.x 및 NAT 컨피그레이션이 포함된 동적 IOS 라우터 간의 IPsec를 참조하십시오.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Software 릴리스 12.4
- Cisco PIX Firewall Software 릴리스 6.3.1
- Cisco Secure PIX Firewall 515E
- Cisco 7206 Router

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

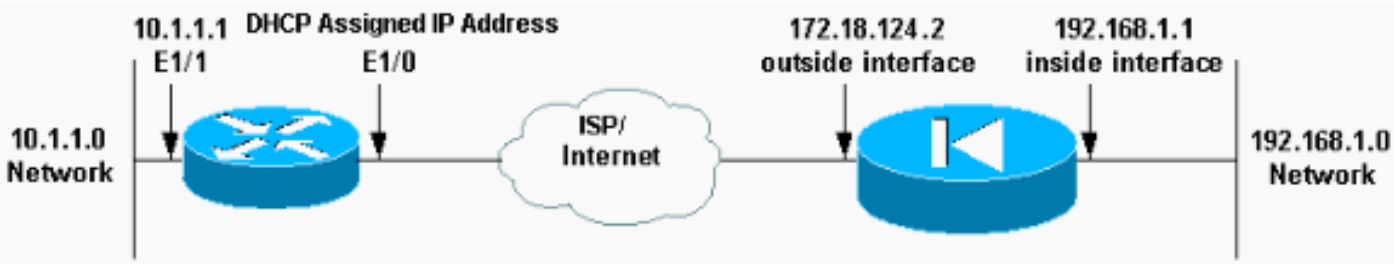
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 이 네트워크 설정을 사용합니다.



구성

이 문서에서는 이러한 구성을 사용합니다.

- Elf(PIX)
- Mop(Cisco 7204 Router)

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 Router)

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

PIX 및 라우터에서 이러한 **show** 명령을 실행할 수 있습니다.

- **show crypto isakmp sa** - 피어의 현재 IKE SA(Security Association)를 모두 표시합니다.
- **show crypto ipsec sa** - 현재(IPsec) SA에서 사용하는 설정을 표시합니다.
- **show crypto engine connections active(암호화 엔진 연결 활성** 표시) - 현재 연결 및 암호화 및 암호 해독된 패킷에 대한 정보를 표시합니다(라우터에만 해당).

두 피어 모두에서 SA를 지워야 합니다.

- PIX 명령은 컨피그레이션 모드에서 수행됩니다.**clear crypto isakmp sa** - 1단계 SA를 지웁니다 .**clear crypto ipsec sa** - 2단계 SA를 지웁니다.
- 라우터 명령은 활성화 모드에서 수행됩니다.**clear crypto isakmp** - 1단계 SA를 지웁니다.**clear crypto sa** - 2단계 SA를 지웁니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

참고: debug **명령**을 사용하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **show crypto isakmp sa** - 피어의 현재 IKE SA를 모두 표시합니다.
- **show crypto ipsec sa** - 현재(IPsec) SA에서 사용하는 설정을 표시합니다.
- **show crypto engine connections active(암호화 엔진 연결 활성** 표시) - 현재 연결 및 암호화 및 암호 해독된 패킷에 대한 정보를 표시합니다(라우터에만 해당).

관련 정보

- IPsec 협상/IKE 프로토콜 지원 페이지
- PIX 500 Series 보안 어플라이언스
- Cisco Secure PIX Firewall 명령 참조
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems