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

목차

소개

이 문서에서는 IOS® 라우터가 PIX 방화벽에서 동적 IPsec 연결을 수락하도록 활성화하는 방법을 보여 주는 샘플 컨피그레이션을 제공합니다.사설 네트워크 10.0.0.x가 인터넷에 액세스하는 경우 원격 라우터는 NAT(Network Address Translation)를 수행합니다.10.0.0.x에서 PIX를 따르는 프라이빗 네트워크 10.1.0.x로의 트래픽은 NAT 프로세스에서 제외됩니다.PIX 방화벽은 라우터에 대한 연결을 시작할 수 있지만 라우터는 PIX에 대한 연결을 시작할 수 없습니다.

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

PIX [6.x 참조:정적으로 주소가 지정된 PIX 방화벽과 NAT 컨피그레이션이 있는 동적 IOS 라우터 간 동적 IPsec](#)에 대한 자세한 내용은 PIX가 라우터에서 동적 IPsec 연결을 허용하는 시나리오에 대한 예를 참조하십시오.

PIX/[ASA 7.x 이상을 참조하십시오.PIX](#)/ASA Security Appliance[가 IOS 라우터에서](#) 동적 IPsec 연결을 허용하도록 [정적으로 주소가 지정된 PIX와 NAT 컨피그레이션을 사용하는 동적 IOS 라우터 간](#)의 동적 IPsec.

PIX/[ASA 7.x 이상을 참조하십시오.PIX](#)/ASA Security Appliance[에서](#) 소프트웨어 버전 7.x 이상을 실행하는 동일한 시나리오에 대해 자세히 알아보려면 [정적으로](#) 주소가 지정된 IOS 라우터와 NAT 컨

피그레이션이 포함된 동적 PIX 간 동적 IPsec 예를 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 6.3.4
- Cisco Secure PIX Firewall 515E
- Cisco 2811 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.

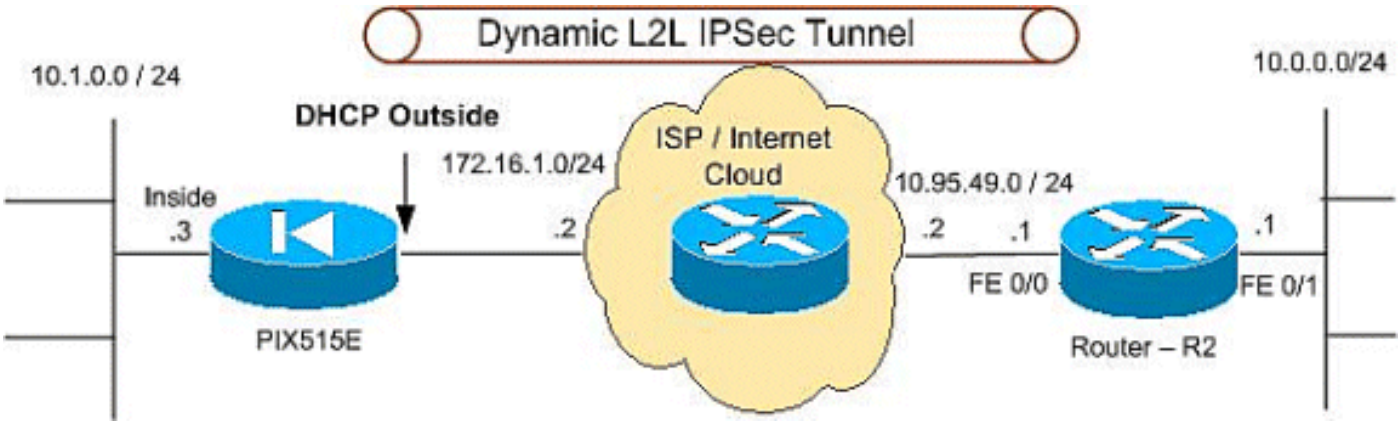
구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

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

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- PIX 515E
- R2(Cisco 2811 Router)

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 Router)

```
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
```

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.

- **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.

컨피그레이션 모드에서 이러한 PIX 명령을 수행합니다.

- **clear crypto isakmp sa** - 1단계 SA를 지웁니다.
- **clear crypto ipsec sa** - 2단계 SA를 지웁니다.

활성화 모드에서 이러한 라우터 명령을 수행합니다.

- **clear crypto isakmp** - 1단계 SA를 지웁니다.
- **clear crypto sa** - 2단계 SA를 지웁니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

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** - 피어에서 현재 모든 IKE SA를 봅니다.
- **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

- 가장 일반적인 L2L 및 원격 액세스 IPSec VPN 문제 해결 솔루션
- Cisco PIX 방화벽 소프트웨어
- Cisco Secure PIX Firewall 명령 참조
- RFC(Request for Comments)
- IPsec 협상/IKE 프로토콜