PIX 6.x: 액세스 목록을 사용하고 NAT 컨피그레이션을 사용하는 PIX 방화벽을 통과하는 IPsec 터널 예

목차

소개

이 문서에서는 NAT(Network Address Translation)를 수행하는 방화벽을 통한 IPSec 터널에 대한 샘플 컨피그레이션을 제공합니다. **12.2(13)T 이전 및 12.2(13)T를 포함하지 않고 Cisco IOS® Software Release를 사용하는 경우 이 컨피그레이션은 PAT(Port Address Translation)에서 작동하지 않습니다.** 이러한 컨피그레이션은 IP 트래픽을 터널링하는 데 사용할 수 있습니다. IPX 또는 라우팅 업데이트와 같이 방화벽을 통과하지 않는 트래픽을 암호화하는 데 사용할 수 없습니다. GRE(Generic Routing Encapsulation) 터널링은 이러한 유형의 컨피그레이션에 적합합니다. 이 문서의 예에서 Cisco 2621 및 3660 라우터는 IPSec 트래픽을 허용하기 위해 PIX에서 관로 또는 ACL(Access Control List)을 사용하여 두 개의 프라이빗 네트워크를 연결하는 IPSec 터널 엔드포인트입니다.

참고: NAT는 일대일 주소 변환이며, PAT와 혼동하지 마십시오. PAT는 많은(방화벽 내부) 대 원 변환입니다. NAT 작업 및 컨피그레이션에 대한 자세한 내용은 NAT 작업 확인 및 기본 NAT 트러블슈팅 또는 NAT 작동 방식을 참조하십시오.

참고: 외부 터널 엔드포인트 디바이스에서 하나의 IP 주소에서 여러 터널을 처리할 수 없으므로 PAT를 사용하는 IPSec이 제대로 작동하지 않을 수 있습니다. 터널 엔드포인트 디바이스가 PAT에서 작동하는지 확인하려면 공급업체에 문의해야 합니다. 또한 버전 12.2(13)T 이상에서는 NAT 투명도 기능을 PAT에도 사용할 수 있습니다. 자세한 내용은 IPSec NAT 투명도를 참조하십시오. 버전 12.2(13)T 이상의 이러한 기능에 대한 자세한 내용은 IPSec ESP Through NAT 지원을 참조하십시오. 또한 TAC에서 케이스를 열기 전에 NAT FAQ(자주 묻는 질문)를 참조하십시오. NAT는 일반적인 질문에 대한 많은 답변을 제공합니다.

PIX/ASA 버전 7.x에서 NAT가 있는 방화벽을 통해 IPSec 터널을 구성하는 방법에 대한 자세한 내용은 액세스 목록을 사용하는 보안 어플라이언스를 통과하는 IPsec 터널 통과 및 NAT 컨피그레이션을 사용하는 MPF 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 12.0.7.T [최대 12.2(13)T 포함 안 함]최신 버전은 IPSec NAT 투명도를 참조하십시오.
- Cisco IOS Software 릴리스 12.4를 실행하는 Cisco 2621 Router
- Cisco IOS Software 릴리스 12.4를 실행하는 Cisco 3660 Router
- 6.x를 실행하는 Cisco PIX Firewall

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.

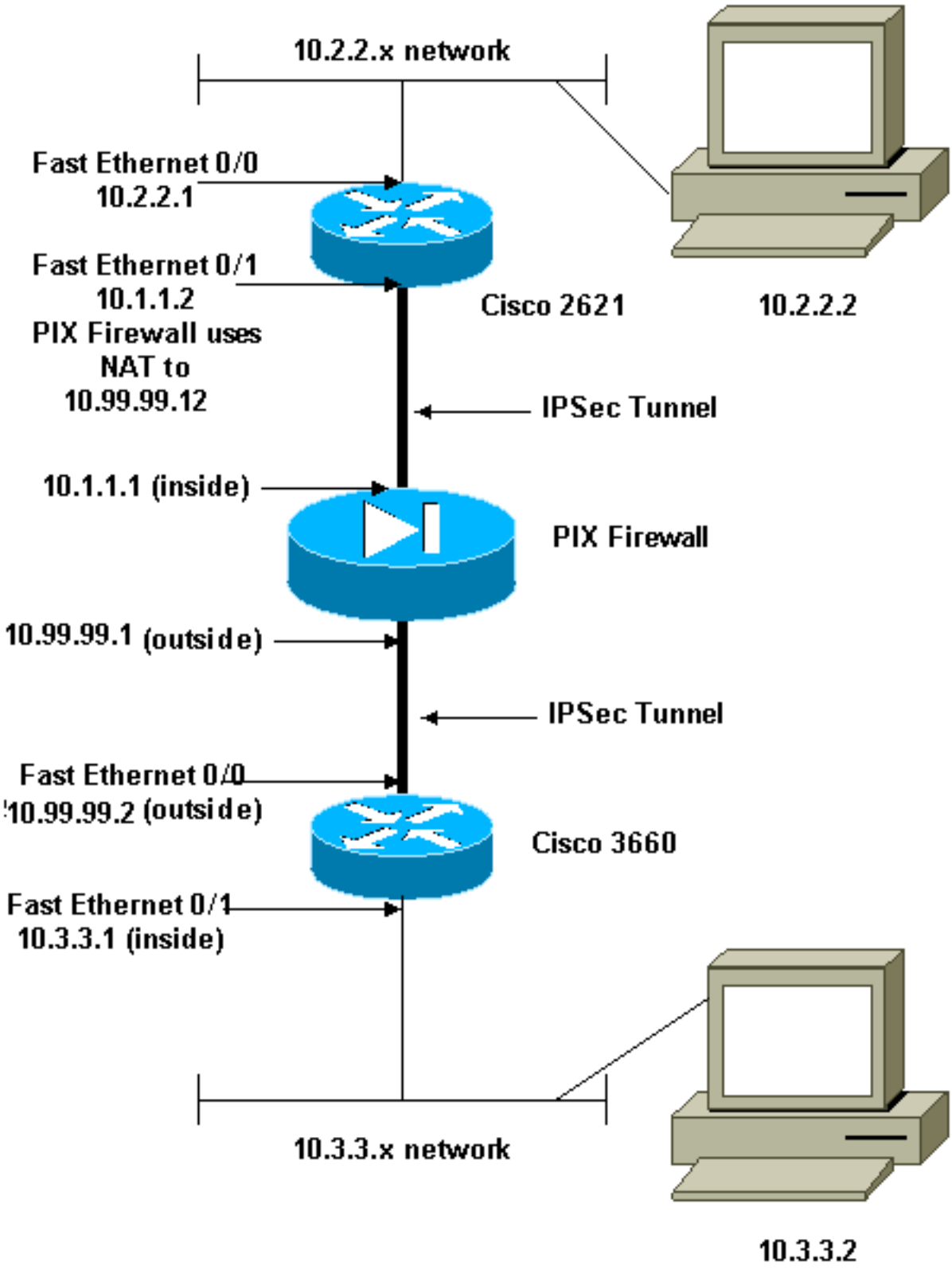
구성

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.



참고: 이 구성에 사용된 IP 주소 지정 체계는 인터넷에서 합법적으로 라우팅할 수 없습니다. 이는 실습 환경에서 사용된 RFC 1918 주소입니다.

구성

이 문서에서는 다음 구성을 사용합니다.

- Cisco 2621 구성
- Cisco PIX 방화벽 부분 구성
- Cisco 3660 구성

Cisco 2621 구성

```
Current configuration:
 !
 version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-2621
 !
 ip subnet-zero
 !
 ip audit notify log
 ip audit po max-events 100
 isdn voice-call-failure 0
 cns event-service server
 !
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.2
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/1
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.2
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 controller T1 1/0
 !
 interface FastEthernet0/0
  ip address 10.2.2.1 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !
 interface FastEthernet0/1
  ip address 10.1.1.2 255.255.255.0
  no ip directed-broadcast
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.1.1.1
 no ip http server
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 no scheduler allocate
 end
```

Cisco PIX 방화벽 부분 구성

```
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
!--- The fixup protocol esp-ike command is disabled by
default.

fixup protocol esp-ike

ip address outside 10.99.99.1 255.255.255.0
 ip address inside 10.1.1.1 255.255.255.0
 !--- Range of registered IP addresses for use. global
(outside) 1 10.99.99.50-10.99.99.60 !--- Translate any
internal source address when !--- going out to the
Internet. nat (inside) 1 0.0.0.0 0.0.0.0 0 0
 static (inside,outside) 10.99.99.12 10.1.1.2 netmask
255.255.255.255 0 0

 !--- or access-list acl-out permit esp host 10.99.99.2
host 10.99.99.12
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq isakmp
 access-list acl-out permit udp host 10.99.99.2 host
10.99.99.12 eq 4500
!--- It is important to permit UDP port 4500 for NAT-T
because the PIX is acting !--- as a NAT device between
the routers. access-group acl-out in interface outside
isakmp enable outside isakmp enable inside Command
configured in order to enable NAT-T isakmp nat-traversal
20 route outside 0.0.0.0 0.0.0.0 99.99.99.2 1 route
inside 10.2.2.0 255.255.255.0 10.1.1.2 1
```

참고: fixup **protocol esp-ike** 명령은 기본적으로 비활성화되어 있습니다. fixup **protocol esp-ike** 명령이 실행된 경우 수정 기능이 켜지고 PIX 방화벽은 IKE(Internet Key Exchange)의 소스 포트를 유지합니다. 또한 ESP 트래픽에 대한 PAT 변환을 생성합니다. 또한 esp-ike fixup이 설정되어 있으면 어떤 인터페이스에서도 ISAKMP(Internet Security Association and Key Management Protocol)를 활성화할 수 없습니다.

Cisco 3660 구성

```
version 12.4
 service timestamps debug uptime
 service timestamps log uptime
 no service password-encryption
 !
 hostname goss-3660
 !
 ip subnet-zero
 !
 cns event-service server
 !
```

```
 !--- IKE Policy crypto isakmp policy 10
  hash md5
  authentication pre-share
 crypto isakmp key cisco123 address 10.99.99.12
 !
 crypto ipsec transform-set myset esp-des esp-md5-hmac
 !
 crypto map mymap local-address FastEthernet0/0
 !--- IPSec Policy crypto map mymap 10 ipsec-isakmp
  set peer 10.99.99.12
  set transform-set myset
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. match address
101
 !
 interface FastEthernet0/0
  ip address 10.99.99.2 255.255.255.0
  no ip directed-broadcast
  ip nat outside
  duplex auto
  speed auto
 !--- Apply to interface. crypto map mymap
 !
 interface FastEthernet0/1
  ip address 10.3.3.1 255.255.255.0
  no ip directed-broadcast
  ip nat inside
  duplex auto
  speed auto
 !
 interface Ethernet3/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface Serial3/0
  no ip address
  no ip directed-broadcast
  no ip mroute-cache
  shutdown
 !
 interface Ethernet3/1
  no ip address
  no ip directed-broadcast
 interface Ethernet4/0
  no ip address
  no ip directed-broadcast
  shutdown
 !
 interface TokenRing4/0
  no ip address
  no ip directed-broadcast
  shutdown
  ring-speed 16
 !
 !--- Pool from which inside hosts translate to !--- the
globally unique 10.99.99.0/24 network. ip nat pool
OUTSIDE 10.99.99.70 10.99.99.80 netmask 255.255.255.0
 !--- Except the private network from the NAT process.
ip nat inside source route-map nonat pool OUTSIDE
 ip classless
 ip route 0.0.0.0 0.0.0.0 10.99.99.1
 no ip http server
 !
```

```
 !--- Include the private-network-to-private-network
traffic !--- in the encryption process. access-list 101
permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255
 access-list 101 deny   ip 10.3.3.0 0.0.0.255 any
 !--- Except the private network from the NAT process.
access-list 110 deny   ip 10.3.3.0 0.0.0.255 10.2.2.0
0.0.0.255
 access-list 110 permit ip 10.3.3.0 0.0.0.255 any
 route-map nonat permit 10
  match ip address 110
 !
 line con 0
  transport input none
 line aux 0
 line vty 0 4
 !
 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 ipsec sa** - 2단계 보안 연결을 표시합니다.
- **show crypto isakmp sa** - 1단계 보안 연결을 표시합니다.
- **show crypto engine connections active**(암호화 엔진 연결 **활성** 표시) - 암호화된 및 해독된 패킷을 확인하는 데 사용합니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결할 수 있습니다.

문제 해결 명령

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

- **debug crypto engine** - 암호화된 트래픽을 표시합니다.
- **debug crypto ipsec** - 2단계의 IPSec 협상을 확인하는 데 사용합니다.
- **debug crypto isakmp** - 1단계의 ISAKMP 협상을 확인하는 데 사용합니다.

보안 연결 지우기

- **clear crypto isakmp** - IKE 보안 연결을 지웁니다.
- **clear crypto ipsec sa** - IPSec 보안 연결을 지웁니다.

관련 정보

- Cisco PIX 500 Series 보안 어플라이언스

- Cisco Secure PIX Firewall 명령 참조
- NAT 지원 페이지
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems