IOS 라우터 컨피그레이션에서 NAT를 사용하는 IPSec/GRE 예

목차

소개

이 샘플 컨피그레이션에서는 GRE/IPSec 터널이 NAT(Network Address Translation)를 수행하는 방화벽을 통과하는 IPSec을 통한 GRE(Generic Routing Encapsulation)를 구성하는 방법을 보여줍니다.

시작하기 전에

표기 규칙

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

사전 요구 사항

이러한 유형의 컨피그레이션은 IPX(예: 여기 예시) 또는 라우팅 업데이트와 같이 일반적으로 방화벽을 통과하지 않는 트래픽을 터널링하고 암호화하는 데 사용할 수 있습니다.이 예에서 2621과 3660 사이의 터널은 LAN 세그먼트의 디바이스에서 트래픽이 생성되는 경우에만 작동합니다(IPSec 라우터에서 확장된 IP/IPX ping이 아님).디바이스 2513A와 2513B 간 IP/IPX ping을 사용하여 IP/IPX 연결을 테스트했습니다.

참고: PAT(Port Address Translation)에서는 작동하지 않습니다.

사용되는 구성 요소

이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® 12.4
- Cisco PIX Firewall 535
- Cisco PIX Firewall Software 릴리스 7.x 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

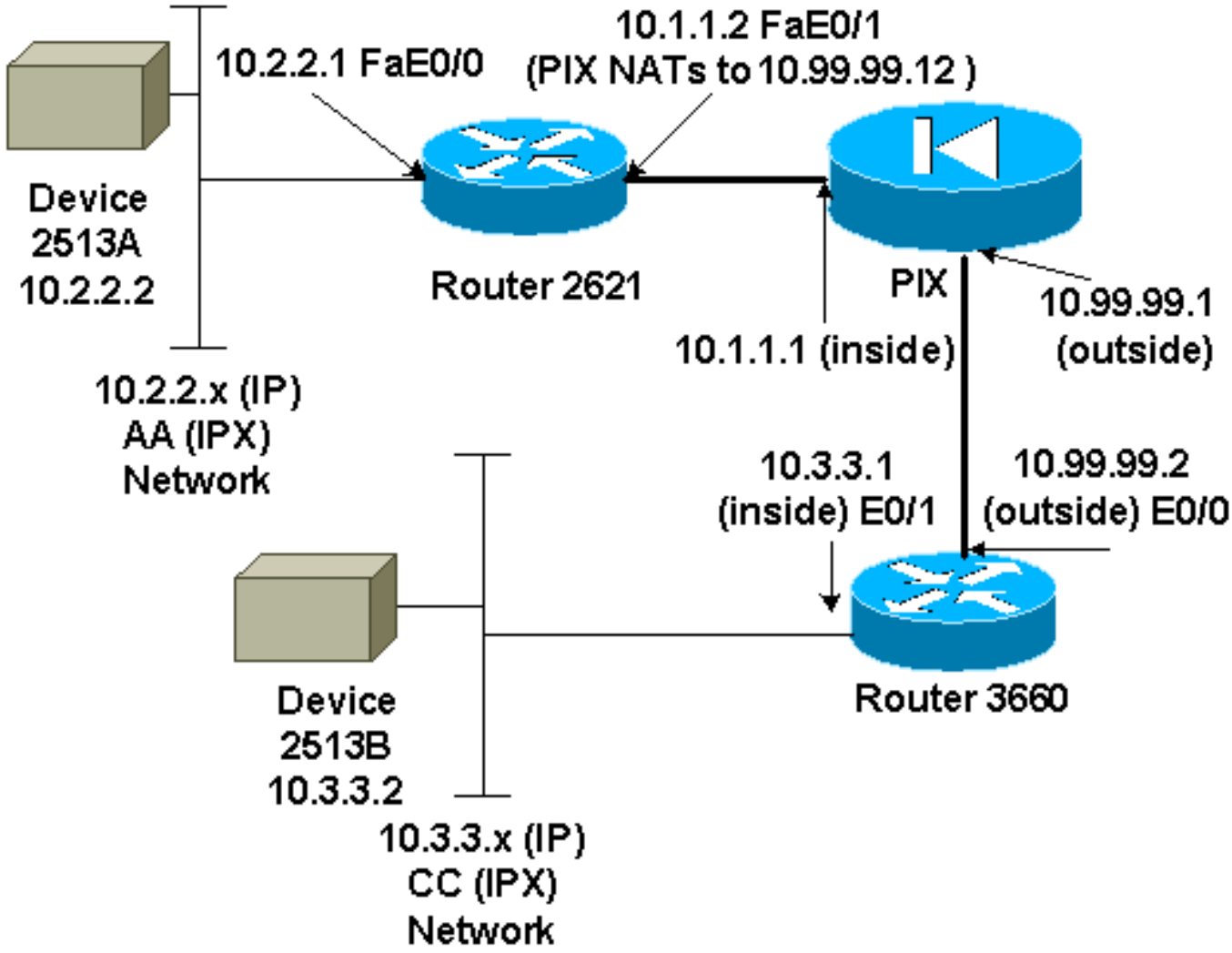
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

IOS 구성 참고: Cisco IOS 12.2(13)T 이상 코드(번호가 높은 T-트레인 코드, 12.3 이상 코드)를 사용하면 구성된 IPSEC "crypto map"은 물리적 인터페이스에만 적용되어야 하며 GRE 터널 인터페이스에 더 이상 적용할 필요가 없습니다.12.2.(13)T 및 이후 코드를 사용할 때 물리적 및 터널 인터페이스에 "crypto map"이 있는 것은 여전히 작동합니다.그러나 물리적 인터페이스에만 적용하는 것이 좋습니다.

네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.



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

네트워크 다이어그램 참고 사항

- 10.2.2.1에서 10.3.3.1(IPX 네트워크 BB) 사이의 GRE 터널
- 10.1.1.2(10.99.99.12)에서 10.99.99.2으로 IPSec 터널

구성

디바이스 2513A
ipx routing 00e0.b064.20c1 ! interface Ethernet0 **ip address 10.2.2.2 255.255.255.0** no ip directed-broadcast **ipx network AA** ! ip route 0.0.0.0 0.0.0.0 10.2.2.1 *!--- Output Suppressed*
2621
version 12.4

```
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 2621
!
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ipx routing 0030.1977.8f80
isdn voice-call-failure 0
cns event-service server
!
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
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.2
 set transform-set myset
 match address 101
!
controller T1 1/0
!
interface Tunnel0
 ip address 192.168.100.1 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/0
 tunnel destination 10.3.3.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.2.2.1 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 ipx network AA
!
interface FastEthernet0/1
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 duplex auto
 speed auto
 crypto map mymap
!
ip classless
ip route 10.3.3.0 255.255.255.0 Tunnel0
ip route 10.3.3.1 255.255.255.255 10.1.1.1
ip route 10.99.99.0 255.255.255.0 10.1.1.1
no ip http server
!
access-list 101 permit gre host 10.2.2.1 host 10.3.3.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
!
```

```
no scheduler allocate
end

!--- Output Suppressed
```

PIX

```
pixfirewall# sh run
: Saved
:
PIX Version 7.0
!
hostname pixfirewall
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.99.99.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
global (outside) 1 10.99.99.50-10.99.99.60
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
access-list 102 permit esp host 10.99.99.12 host
10.99.99.2
access-list 102 permit udp host 10.99.99.12 host
10.99.99.2 eq isakmp


route outside 0.0.0.0 0.0.0.0 10.99.99.2 1
route inside 10.2.2.0 255.255.255.0 10.1.1.2 1

!--- Output Suppressed
```

3660

```
version 12.4
service timestamps debug datetime
service timestamps log uptime
no service password-encryption
!
hostname 3660
!
memory-size iomem 30
ip subnet-zero
no ip domain-lookup
!
ipx routing 0030.80f2.2950
cns event-service server
!
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
crypto map mymap 10 ipsec-isakmp
 set peer 10.99.99.12
 set transform-set myset
 match address 101
!
interface Tunnel0
 ip address 192.168.100.2 255.255.255.0
 no ip directed-broadcast
 ipx network BB
 tunnel source FastEthernet0/1
 tunnel destination 10.2.2.1
 crypto map mymap
!
interface FastEthernet0/0
 ip address 10.99.99.2 255.255.255.0
 no ip directed-broadcast
 ip nat outside
 duplex auto
 speed auto
 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
 ipx network CC
!
ip nat pool 3660-nat 10.99.99.70 10.99.99.80 netmask
255.255.255.0
ip nat inside source list 1 pool 3660-nat
ip classless
ip route 0.0.0.0 0.0.0.0 Tunnel0
ip route 10.2.2.1 255.255.255.255 10.99.99.1
ip route 10.99.99.12 255.255.255.255 10.99.99.1
no ip http server
!
access-list 1 permit 10.3.3.0 0.0.0.255
access-list 101 permit gre host 10.3.3.1 host 10.2.2.1
!
line con 0
 transport input none
line aux 0
line vty 0 4
 login
!
end
!--- Output Suppressed
```

디바이스 2,513B

```
ipx routing 00e0.b063.e811
!
interface Ethernet0
 ip address 10.3.3.2 255.255.255.0
 no ip directed-broadcast
 ipx network CC
!
ip route 0.0.0.0 0.0.0.0 10.3.3.1
```

```
!--- Output Suppressed
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- show crypto ipsec sa - 2단계 보안 연결을 표시합니다.
- show crypto isakmp sa - 모든 암호화 엔진에 대한 현재 활성 암호화 세션 연결을 표시합니다.
- *선택적으로:* show interfaces tunnel *number* - 터널 인터페이스 정보를 표시합니다.
- show ip route - 모든 고정 IP 경로 또는 AAA(authentication, authorization, and accounting) 경로 다운로드 기능을 사용하여 설치된 경로를 표시합니다.
- show ipx route - IPX 라우팅 테이블의 내용을 표시합니다.

문제 해결

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

문제 해결 명령

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- debug crypto engine - 암호화된 트래픽을 표시합니다.
- debug crypto ipsec - 2단계의 IPSec 협상을 표시합니다.
- debug crypto isakmp - 1단계의 ISAKMP(Internet Security Association and Key Management Protocol) 협상을 표시합니다.
- *선택적으로:* debug ip routing - RIP(Routing Information Protocol) 라우팅 테이블 업데이트 및 route-cache 업데이트에 대한 정보를 표시합니다.
- 디버그 ipx 라우팅 {활동 | 이벤트} - 디버그 ipx 라우팅 {activity | events} - 라우터가 보내고 받는 IPX 라우팅 패킷에 대한 정보를 표시합니다.

SA(Security Associations) 지우기

- clear cryptpo ipsec sa - 모든 IPSec 보안 연결을 지웁니다.
- clear crypto isakmp - IKE 보안 연결을 지웁니다.
- *선택적으로:* clear ipx route * - IPX 라우팅 테이블에서 모든 경로를 삭제합니다.

관련 정보

- IP Security(IPSec) 제품 지원 페이지
- GRE 지원 페이지

- Technical Support - Cisco Systems