IPsec VTI를 사용하여 Secure eBGP 세션 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램](#)
[구성](#)
[다음을 확인합니다.](#)
[문제 해결](#)

소개

이 문서에서는 데이터 플레인 트래픽에 대한 물리적 인터페이스(비터널)와 함께 IPsec VTI(Virtual Tunnel Interface)를 사용하여 eBGP(Border Gateway Protocol) 인접 관계를 보호하는 방법에 대해 설명합니다.이 구성의 이점은 다음과 같습니다.

- 데이터 기밀성, 재전송 방지, 신뢰성 및 무결성으로 BGP 네이버 세션의 완벽한 프라이버시.
- 데이터 플레인 트래픽은 터널 인터페이스의 MTU(Maximum Transmission Unit) 오버헤드로 제한되지 않습니다.고객은 성능에 영향을 주거나 단편화 없이 표준 MTU 패킷(1500바이트)을 전송할 수 있습니다.
- SPI(Security Policy Index) 암호화/해독 기능은 BGP 컨트롤 플레인 트래픽으로 제한되므로 엔드포인트 라우터의 오버헤드가 줄어듭니다.

이 컨피그레이션의 이점은 데이터 플레인이 터널링 인터페이스의 제한에 제한되지 않는다는 것입니다.설계상, 데이터 플레인 트래픽은 IPsec 보안 상태가 아닙니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 알고 있는 것이 좋습니다.

- eBGP 컨피그레이션 및 검증 기본 사항
- 경로 맵을 사용하는 BGP PA(Policy Accounting) 조작
- ISAKMP(Basic Internet Security Association and Key Management Protocol) 및 IPsec 정책 기능

사용되는 구성 요소

이 문서의 정보는 Cisco IOS® Software Release 15.3(1.3)T를 기반으로 하지만 지원되는 다른 버전은 작동합니다.IPsec 컨피그레이션은 암호화 기능이므로 코드 버전에 이 기능 집합이 포함되어 있는지 확인하십시오.

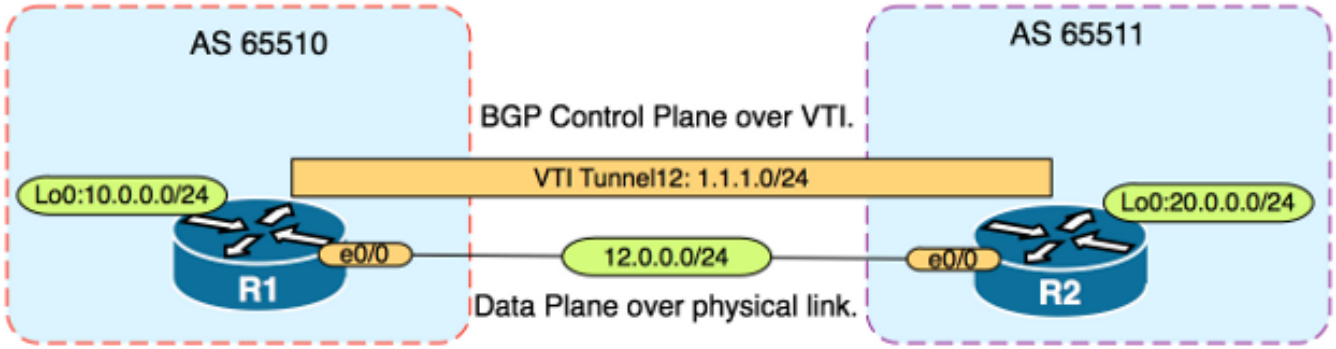
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

> **주의:**이 문서의 컨피그레이션 예제에서는 사용자 환경에 적합하거나 적합하지 않을 수 있는 적당한 암호 알고리즘을 사용합니다.다양한 암호 그룹 및 키 크기의 상대적 보안에 대한 자세한 내용은 Next Generation Encryption 백서를 참조하십시오.

구성

> **참고:**이 섹션에 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용합니다.

네트워크 다이어그램



구성

다음 단계를 완료하십시오.

1. R1의 사전 공유 키로 R1 및 R2에서 IKE(Internet Key Exchange) 1단계 매개변수 구성: **참고:**DH 그룹 번호 1, 2 또는 5는 열등하다고 간주되므로 사용하지 마십시오.가능한 경우 그룹 19, 20 또는 24와 같은 ECC(Elliptic Curve Cryptography)가 있는 DH 그룹을 사용합니다. AES(Advanced Encryption Standard) 및 SHA256(Secure Hash Algorithm 256)은 각각 DES(Data Encryption Standard)/3DES 및 MD5(Message Digest 5)/SHA1보다 뛰어난 것으로 간주됩니다.프로덕션 환경에서는 "cisco" 비밀번호를 사용하지 마십시오.**R1 구성**

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 19
R1(config-isakmp)exit

R1(config)#crypto isakmp key CISCO address 12.0.0.2
```

R2 구성

```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
```

```
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 19


R2(config-isakmp)exit

R2(config)#crypto isakmp key CISCO address 12.0.0.1
```

2. R1 및 R2의 NVRAM에 있는 사전 공유 키에 대한 레벨 6 비밀번호 암호화를 구성합니다. 이렇게 하면 라우터가 손상되었을 때 일반 텍스트로 저장된 사전 공유 키가 읽히지 않을 가능성이 줄어듭니다.

```
R1(config)#key config-key password-encrypt CISCOCISCO

R1(config)#password encryption aes

R2(config)#key config-key password-encrypt CISCOCISCO

R2(config)#password encryption aes
```

참고:레벨 6 비밀번호 암호화가 활성화되면 활성 컨피그레이션에서는 더 이상 사전 공유 키의 일반 텍스트 버전을 표시하지 않습니다.

```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```

3. R1 및 R2에서 IKE 단계 2 매개변수를 구성합니다. **R1 구성**

```
R1(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R1(config)#crypto ipsec profile PROFILE

R1(ipsec-profile)#set transform-set TRANSFORM-SET
R1(ipsec-profile)#set pfs group19
```

R2 구성

```
R2(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac

R2(config)#crypto ipsec profile PROFILE

R2(ipsec-profile)#set transform-set TRANSFORM-SET

R2(ipsec-profile)#set pfs group19
```

참고:PFS(Perfect Forward Secrecy)를 설정하는 것은 선택 사항이지만 IKE 2단계 SA 설정에서 새로운 대칭 키 생성이 필요하므로 VPN 강도를 향상시킵니다.

4. R1 및 R2에서 터널 인터페이스를 구성하고 IPsec 프로필을 사용하여 보안을 유지합니다. **R1 구성**

```
R1(config)#interface tunnel 12

R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#tunnel source Ethernet0/0

R1(config-if)#tunnel mode ipsec ipv4

R1(config-if)#tunnel destination 12.0.0.2

R1(config-if)#tunnel protection ipsec profile PROFILE
```

R2 구성

```
R2(config)#interface tunnel 12

R2(config-if)#ip address 1.1.1.2 255.255.255.0
```

```
R2(config-if)#tunnel source Ethernet0/0

R2(config-if)#tunnel mode ipsec ipv4

R2(config-if)#tunnel destination 12.0.0.1

R2(config-if)#tunnel protection ipsec profile PROFILE
```

5. R1 및 R2에서 BGP를 구성하고 루프백0 네트워크를 BGP에 알립니다. **R1 구성**

```
R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 remote-as 65511

R1(config-router)#network 10.0.0.0 mask 255.255.255.0
```

R2 구성

```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 remote-as 65510

R2(config-router)#network 20.0.0.0 mask 255.255.255.0
```

6. 터널이 아닌 물리적 인터페이스를 가리키도록 다음 hop IP 주소를 수동으로 변경하려면 R1 및 R2에서 경로 맵을 구성합니다.인바운드 방향에 이 경로 맵을 적용해야 합니다. **R1 구성**

```
R1(config)ip prefix-list R2-NETS seq 5 permit 20.0.0.0/24

R1(config)#route-map CHANGE-NEXT-HOP permit 10

R1(config-route-map)#match ip address prefix-list R2-NETS

R1(config-route-map)#set ip next-hop 12.0.0.2

R1(config-route-map)#end

R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 route-map CHANGE-NEXT-HOP in

R1(config-router)#do clear ip bgp *

R1(config-router)#end
```

R2 구성

```
R2(config)#ip prefix-list R1-NETS seq 5 permit 10.0.0.0/24

R2(config)#route-map CHANGE-NEXT-HOP permit 10

R2(config-route-map)#match ip address prefix-list R1-NETS

R2(config-route-map)#set ip next-hop 12.0.0.1

R2(config-route-map)#end

R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 route-map CHANGE-NEXT-HOP in

R2(config-router)#do clear ip bgp *

R2(config-router)#end
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)는 특정 **show** 명령을 지원합니다.**show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

IKE 1단계와 IKE 2단계가 모두 완료되었는지 확인합니다. VTI(Virtual Tunnel Interface)의 회선 프로토콜은 IKE 2단계가 완료될 때까지 "up"으로 변경되지 않습니다.

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
12.0.0.1 12.0.0.2 QM_IDLE 1002 ACTIVE
12.0.0.2 12.0.0.1 QM_IDLE 1001 ACTIVE

R1#show crypto ipsec sa | inc encaps|decaps
#pkts encaps: 88, #pkts encrypt: 88, #pkts digest: 88
#pkts decaps: 90, #pkts decrypt: 90, #pkts verify: 90
```

route-map을 적용하기 전에 다음 hop IP 주소는 터널 인터페이스인 BGP 인접 디바이스 IP 주소를 가리킵니다.

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 1.1.1.2 0 0 65511 i
```

트래픽이 터널을 사용하는 경우 MTU는 터널 MTU로 제한됩니다.

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set

*May 6 08:42:07.311: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:09.312: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:11.316: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:13.319: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:15.320: ICMP: dst (20.0.0.2): frag. needed and DF set.
Success rate is 0 percent (0/5)

R1#show interfaces tunnel 12 | inc transport|line

Tunnel12 is up, line protocol is up
Tunnel protocol/transport IPSEC/IP
Tunnel transport MTU 1406 bytes <---

R1#ping 20.0.0.2 size 1406 df-bit
Type escape sequence to abort.
Sending 5, 1406-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

route-map을 적용한 후 IP 주소는 터널이 아니라 R2의 물리적 인터페이스로 변경됩니다.

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 12.0.0.2 0 0 65511 i
```

터널이 표준 크기 MTU를 허용하는 대신 물리적 next hop을 사용하려면 데이터 평면을 변경합니다.

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.