使用IPsec VTI配置安全eBGP会话

目录

简介

本文档介绍如何使用IPsec虚拟隧道接口(VTI)和数据平面流量的物理接口（非隧道）保护外部边界网关协议(eBGP)邻居关系。此配置的优点包括：

- BGP邻居会话的完全隐私，具有数据机密性、反重播、真实性和完整性。
- 数据平面流量不受隧道接口的最大传输单位(MTU)开销限制。客户可以发送标准MTU数据包（1500字节），而不会影响性能或分段。
- 由于安全策略索引(SPI)加密/解密仅限于BGP控制平面流量，因此终端路由器的开销较低。

此配置的优点是数据平面不受隧道接口的限制。根据设计，数据平面流量不受IPsec保护。

先决条件

要求

Cisco 建议您了解以下主题：

- eBGP配置和验证基础
- 使用路由映射的BGP策略记帐(PA)操作
- 基本互联网安全关联和密钥管理协议(ISAKMP)和IPsec策略功能

使用的组件

本文档中的信息基于Cisco IOS®软件版本15.3(1.3)T，但其他受支持的版本适用。由于IPsec配置是加密功能，请确保您的代码版本包含此功能集。

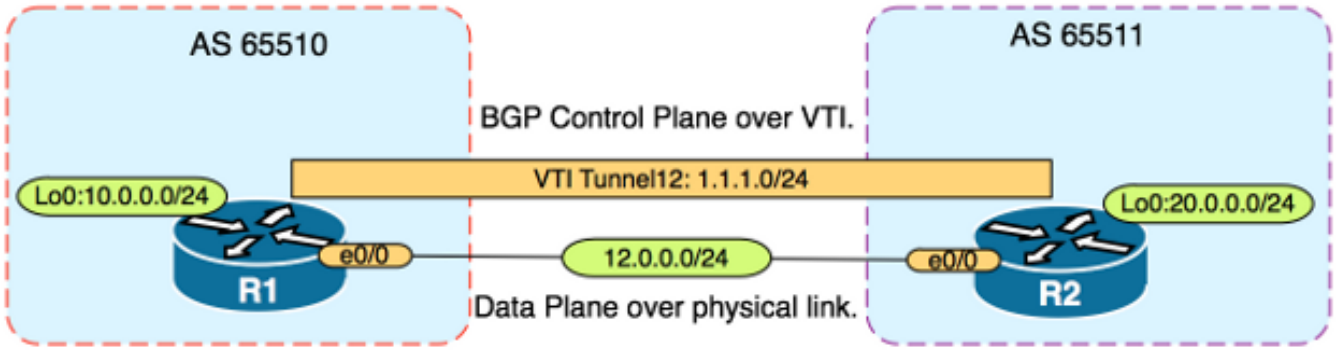
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

> **警告：**本文档中的配置示例使用可能或可能不适合您环境的少量加密算法。有关各种密码套件和密钥大小的相对安全性的讨论，请参阅下一代加密白皮书。

配置

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图



配置

请完成以下步骤：

1. 在R1和R2上使用R1的预共享密钥配置Internet密钥交换(IKE)第1阶段参数： **注意：**请勿使用DH组编号1、2或5，因为它们被视为次级。如果可能，请使用带椭圆曲线加密(ECC)的DH组，例如组19、20或24。高级加密标准(AES)和安全散列算法256(SHA256)应被视为优于数据加密标准(DES)/3DES和消息摘要5(MD5)MD5)/SHA1。切勿在生产环境中使用密码“cisco”。**R1的配置**

```
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 配置

```
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. 在R1和R2的NVRAM中为预共享密钥配置6级密码加密。这降低了在路由器受到危害时以明文形式存储的预共享密钥被读取的可能性：

```
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
```

注意：启用6级密码加密后，活动配置将不再显示预共享密钥的纯文本版本：

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

!
```

3. 在R1和R2上配置IKE第2阶段参数： **R1 的配置**

```
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 配置

```
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
```

注意：设置完全向前保密(PFS)是可选操作，但提高了VPN强度，因为它强制在IKE第2阶段SA建立中生成新的对称密钥。

4. 在R1和R2上配置隧道接口，并使用IPsec配置文件保护： **R1 的配置**

```
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 配置

```
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. 在R1和R2上配置BGP，并将loopback0网络通告到BGP: **R1配置**

```
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 配置

```
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. 在R1和R2上配置路由映射，以手动更改下一跳IP地址，使其指向物理接口而非隧道。您必须在入站方向上应用此路由映射。 **R1 的配置**

```
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 配置

```
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
```

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

验证IKE第1阶段和IKE第2阶段是否已完成。 在IKE第2阶段完成之前，虚拟隧道接口(VTI)上的线路协议不会更改为“up”：

```
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
```

请注意，在应用路由映射之前，下一跳IP地址指向隧道接口BGP邻居IP地址：

```
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
```

当流量使用隧道时，MTU被限制为隧道MTU:

```
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
```

应用路由映射后，IP地址将更改为R2的物理接口，而不是隧道：

```
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
```

更改数据平面以使用物理下一跳，而非隧道允许标准大小MTU:

```
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
```

故障排除

目前没有针对此配置的故障排除信息。