配置有IPsec VTI的一安全eBGP会话

目录

简介

本文描述如何与物理接口(非通道)一起获取与使用的一种外部边界网关协议(eBGP)邻接关系IPsec虚拟隧道接口(VTI)数据层面流量的。此配置的好处包括：

- BGP邻居会话的完整保密性以数据机密性、反重放，真实性和完整性。
- 数据层面流量没有限制条件对隧道接口的最大传输单元(MTU)开销。客户能发送标准的MTU数据包(1500个字节)，不用性能影响或分段。
- 在端点路由器的较少开销，因为安全策略索引(SPI)加密/解密对BGP控制层面流量被限制。

此配置的好处是数据层面没有限制条件对隧道接口的限制。故意地，数据层面流量不是IPsec巩固了。

贡献的查尔斯Stizza， Cisco TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- eBGP配置和验证基本
- BGP策略统计(PA)处理使用route-map
- 基本互联网安全协会和密钥管理协议(ISAKMP)和IPsec策略功能

使用的组件

本文档中的信息根据Cisco IOS ? 软件版本15.3(1.3)T，但是其他支持的版本工作。因为IPSec配置

是一个密码功能，请保证您的编码版本包含此特性组。

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。

> **Caution**:在本文的配置示例使用可能或也许不适用与您的环境的普通的密码器算法。请参阅下一代加密白皮书关于多种密码器套件和密钥大小相对安全的讨论。

配置

> **Note**: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

完成这些步骤：

1. 配置在R1和R2的互联网密钥交换(IKE)阶段1参数与在R1的预先共享密钥：**Note**:因为他们被认为下等，请勿请使用DH组编号1， 2或者5。若可能请以椭圆曲线Cryptopgraphy (ECC)使用一DH组例如组19， 20或者24。应该认为高级加密标准(AES)和安全散列算法256 (SHA256)优越在数据加密标准(DES)/3DES和消息摘要5 (各自MD5)/SHA1。请勿请使用密码“cisco”在生产环境。**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. 配置预先共享密钥的级别6密码加密在R1和R2的NVRAM。这降低在从读的纯文本存储的预先共享密钥的可能性路由器是否折衷：

```
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
```

Note:一旦级别6密码加密启用，活动配置不再显示预先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. 配置在R1和R2的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
```

Note:因为强制在IKE SA第2阶段建立的新的对称密钥生成设置完整转发安全性(PFS)可选，但是改进VPN优点。

4. 配置在R1和R2的隧道接口并且巩固与IPSec简档：**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. 配置在R1和R2的BGP并且通告loopback0网络到BGP:**R1 的配置**

```
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 1.1.1.2 remote-as 65510
```

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

6. 配置在R1和R2的一route-map为了手工更改下一跳IP地址，以便指向物理接口而不是通道。您必须应用在入站方向的此route-map。**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。请使用Output Interpreter Tool为了查看show命令输出分析。

验证IKE相位1和IKE第2阶段完成。 在虚拟隧道接口(VTI)的线路通信协议不更改对“”，直到IKE第2阶段完成：

```
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
```
注意在route-map的应用程序之前，下一跳IP地址指向是隧道接口的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
```
当流量使用通道时， MTU限制条件到通道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
```
在应用route-map以后， IP地址没有更改对R2物理接口，没有通道：

```
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
```
换数据层面为了使用物理下一跳与通道许可证标准大小MTU:相对

```
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。