ipsec总部对多分支的模板方式注意事项

IPSec VPN 吴昊A 2022-11-07 发表

问题描述

1. SA都有的情况下基本上ipsec的相关配置没有太大的问题，但是在一个总部和多个分支之间有vpn的情况下，如果有分支之间的感兴趣流存在被包含的情况，比如分支1是10.1.1.0/24的网段配置，但是分支2是10.1.0.0/16，甚至有些分支为了偷懒写的0.0.0.0网段，这样可能在一段时间的运行过程中是没有问题的，但是偶尔会出现突然断网不通，原因就是有可能在回程的报文匹配到了另外一个分支的感兴趣流走掉导致的，所以一定要注意到分支感兴趣流的配置规范性。

该问题需要在总部上dis ipsec sa 仔细查看有没有分支的感兴趣流冲突和相互包含的情况。

例如，

```
< F1020 >disp ipsec sa
-------------------------------
Interface: GigabitEthernet1/0/16
-------------------------------

  -----------------------------
  IPsec policy: ipsec-policy
  Sequence number: 2
  Mode: Template
  -----------------------------
    Tunnel id: 0
    Encapsulation mode: tunnel
    Perfect Forward Secrecy:
    Inside VPN:
    Extended Sequence Numbers enable: N
    Traffic Flow Confidentiality enable: N
    Path MTU: 1436
    Tunnel:
      local  address: 122.119.15.241
      remote address: 221.13.6.82
    Flow:
      sour addr: 172.16.96.0/255.255.255.0  port: 0  protocol: ip
      dest addr: 172.16.134.64/255.255.255.224  port: 0  protocol: ip

    [Inbound ESP SAs]
      SPI: 1193058372 (0x471ca044)
      Connection ID: 811748818955
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/1727
      Max received sequence-number: 0
      Anti-replay check enable: Y
      Anti-replay window size: 64
      UDP encapsulation used for NAT traversal: Y
      Status: Active

    [Outbound ESP SAs]
      SPI: 2385543736 (0x8e308238)
      Connection ID: 811748818954
      Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
      SA duration (kilobytes/sec): 1843200/3600
      SA remaining duration (kilobytes/sec): 1843200/1727
      Max sent sequence-number: 0
      UDP encapsulation used for NAT traversal: Y
      Status: Active

  -----------------------------
  IPsec policy: ipsec-policy
  Sequence number: 3
  Mode: Template
```

```
-----------------------------
  Tunnel id: 1
  Encapsulation mode: tunnel
  Perfect Forward Secrecy:
  Inside-VPN:
  Extended Sequence Numbers enable: N
  Traffic Flow Confidentiality enable: N
  Path MTU: 1444
  Tunnel:
    local  address: 122.119.15.241
    remote address: 59.173.61.178
  Flow:
    sour addr: 172.16.96.0/255.255.255.0  port: 0  protocol: ip
    dest addr: 0.0.0.0/0  port: 0  protocol: ip

  [Inbound ESP SAs]
    SPI: 1605723628 (0x5fb565ec)
    Connection ID: 1060856922112
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/3004
    Max received sequence-number: 0
    Anti-replay check enable: Y
    Anti-replay window size: 64
    UDP encapsulation used for NAT traversal: N
    Status: Active

  [Outbound ESP SAs]
    SPI: 1649564177 (0x62525a11)
    Connection ID: 1060856922113
    Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-SHA1
    SA duration (kilobytes/sec): 1843200/3600
    SA remaining duration (kilobytes/sec): 1843200/3004
    Max sent sequence-number: 0
    UDP encapsulation used for NAT traversal: N
    Status: Active
```

上面这种就是典型的感兴趣流有包含的情况。

过程分析

总部对多分支模板方式的ipsec，分支感兴趣流存在冲突覆盖的情况下，总部侧会出现匹配错隧道的问题，为了避免配置中出现这种问题，建议开启ipsec流量重叠检测功能，此功能打开后会出现日志告警，提示对应冲突的分支合理修改感兴趣流的acl。

解决方法

开启命令如下：

ipsec flow-overlap check enable

ipsec flow-overlap check enable命令用来开启IPsec流量重叠检测功能。

undo ipsec flow-overlap check enable命令用来关闭IPsec流量重叠检测功能。

【命令】

ipsec flow-overlap check enable

undo ipsec flow-overlap check enable

【缺省情况】

IPsec流量重叠检测功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

非缺省vSystem不支持本命令。

在中心-分支组网环境中，通常中心侧采用IPsec安全策略模板方式协商IPsec SA，当分支侧分支众多时，需保护的数据流范围可能会重叠。此时通过开启本功能，在协商IPsec SA时，设备会检测新建隧道与已有隧道的需保护数据流是否存在重叠。若重叠，则IPsec SA协商失败，设备将生成IPsec流量重叠检测失败的告警信息，提示用户当前需要保护的数据流存在流量重叠。当IPsec SA协商失败时，管理员需要针对当前组网环境，重新规划分支侧的ACL配置。

中心侧设备判断是否存在IPsec流量重叠的方法为：检测待保护数据流的目的IP地址范围是否与已有隧道保护的数据流的目的IP地址范围重叠。若重叠，则认为待保护的数据流与已有隧道保护的数据流发生了重叠。

本功能的实现情况如下：

- 建议在中心-分支组网环境中的中心侧配置本功能。
- 仅在设备采用IPsec安全策略模板方式协商IPsec SA时生效。
- 仅支持对新建的IPsec SA进行流量重叠检测，不支持对已有的IPsec SA进行流量重叠检测。
- 仅支持在同一接口、同一VPN实例下进行流量重叠检测。
- 不支持对IPsec重协商后生成的IPsec SA进行流量重叠检测。
- 流量重叠检测时不会判断源IP地址范围是否与已有隧道保护的数据流的源IP地址范围重叠。
- 流量重叠检测对设备性能有一定的影响，建议仅在进行网络升级扩容等操作时开启，并在操作完成后及时关闭。

【举例】

开启IPsec流量重叠检测功能。

<Sysname> system-view

[Sysname] ipsec flow-overlap check enable