当ipsec隧道丢包，且丢包统计类型为 MTU check failure时的处理方法

IPSec VPN 徐猛 2022-04-03 发表

问题描述

如下，当ipsec两端业务存在丢包的情况，通过display ipsec statistics查看ipsec包计数，发现大量MTU check failure导致的丢包计数。

==========display ipsec statistics==========

IPsec packet statistics:

Received/sent packets: 3447/52344

Received/sent bytes: 1194040/35307392

Dropped packets (received/sent): 0/413937

Dropped packets statistics

No available SA: 0

Wrong SA: 0

Invalid length: 0

Authentication failure: 0

Encapsulation failure: 0

Decapsulation failure: 0

Replayed packets: 0

ACL check failure: 0

MTU check failure: 413937

Loopback limit exceeded: 0

Crypto speed limit exceeded: 0

解决方法

对于现场的ipsec MTU check error丢包的情况，需要配置：

（1）ipsec global-df-bit clear

（2）ipsec fragmentation afer-encryption

如下为命令详解：

1.1.29 ipsec global-df-bit

ipsec global-df-bit命令用来为所有接口设置IPsec封装后外层IP头的DF位。

undo ipsec global-df-bit命令用来恢复缺省情况。

【命令】

ipsec global-df-bit { clear | copy | set }

undo ipsec global-df-bit

【缺省情况】

IPsec封装后外层IP头的DF位从原始报文IP头中拷贝。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

clear：表示清除外层IP头的DF位，IPsec封装后的报文可被分片。

copy：表示外层IP头的DF位从原始报文IP头中拷贝。

set：表示设置外层IP头的DF位，IPsec封装后的报文不能分片。

【使用指导】

该功能仅在IPsec的封装模式为隧道模式时有效（因为传输模式不会增加新的IP头，因此对于传输模式无影响）。

该功能用于设置IPsec隧道模式封装后的外层IP头的DF位，原始报文IP头的DF位不会被修改。

转发报文时对报文进行分片、重组，可能会导致报文的转发延时较大。若设置了封装后IPsec报文的DF位，则不允许对IPsec报文进行分片，可以避免引入分片延时。这种情况下，要求IPsec报文转发路径上各个接口的MTU大于IPsec报文长度，否则，会导致IPsec报文被丢弃。如果无法保证转发路径上各个接口的MTU大于IPsec报文长度，则建议清除DF位。

【举例】

为所有接口设置IPsec封装后外层IP头的DF位。

system-view

[Sysname] ipsec global-df-bit set

1.1.28 ipsec fragmentation

ipsec fragmentation命令用来配置IPsec分片功能。

undo ipsec fragmentation命令用来恢复缺省情况。

【命令】

ipsec fragmentation { after-encryption | before-encryption }

undo ipsec fragmentation

【缺省情况】

IPsec分片功能为封装前分片。

【视图】

系统视图

【缺省用户角色】

network-admin

context-admin

【参数】

after-encryption：表示开启IPsec封装后分片功能。

before-encryption：表示开启IPsec封装前分片功能。

【使用指导】

IPsec封装前分片功能处于开启状态时，设备会先判断报文在经过IPsec封装之后大小是否会超过发送接口的MTU值，如果封装后的大小超过发送接口的MTU值，且报文的DF位未置位那么会先对其分片再封装；如果待报文的DF位被置位，那么设备会丢弃该报文，并发送ICMP差错控制报文。

IPsec封装后分片功能处于开启状态时，无论报文封装后大小是否超过发送接口的MTU值，设备会直接对其先进行IPsec封装处理，再由后续业务对其进行分片。

【举例】

开启IPsec封装后分片功能。

system-view

[Sysname] ipsec fragmentation after-encryption