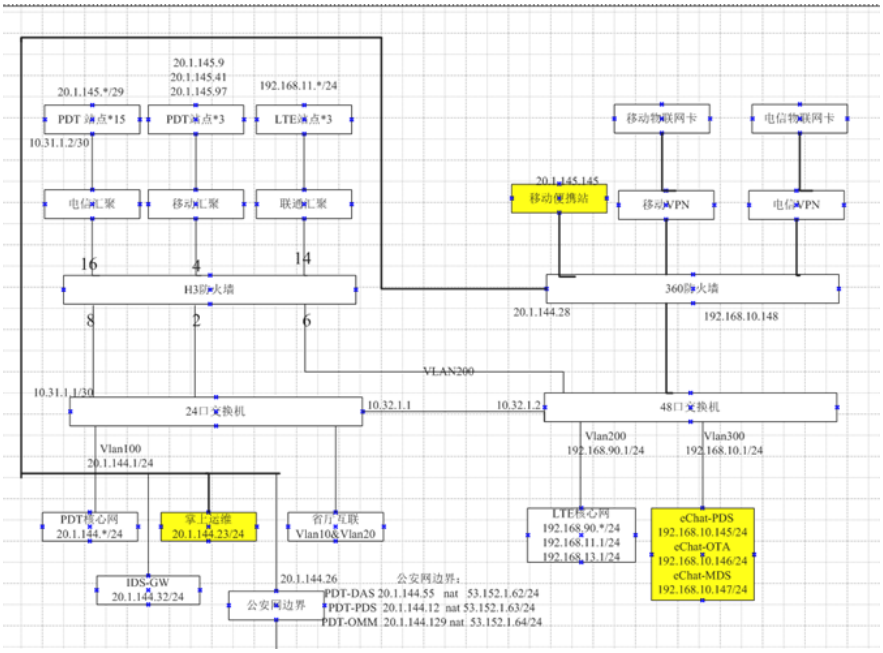
SCTP业务过防火墙报文被丢业务异常问题

域间策略/安全域　吴昊A　2021-12-21 发表

组网及说明



问题描述

防火墙F1000-AK1414（R8601P2412）二层透传到设备组网中，客户24口交换机若直接使用光口26端口连接电信汇聚设备，则24口交换机下联业务能正常运行。后面使用23端口上联我司防火墙二层透传，我司防火墙通过14端口和电信汇聚设备相连，SCTP业务出现异常。

过程分析

故障期间的会话状态为 **State: SCTP_COOKIE_ECHOED**，非 SCTP_ESTABLISHED完成状态

dis session table ipv4 sou 20.1.145.1 des 20.1.144.11 ver

Slot 1:

Initiator:

  Source   IP/port: 20.1.145.1/2904

  Destination IP/port: 20.1.144.11/60000

  DS-Lite tunnel peer: -

  VPN instance/VLAN ID/Inline ID: -/500/-

  Protocol: SCTP(132)

  Inbound interface: GigabitEthernet1/0/14

  Source security zone: Untrust

Responder:

  Source   IP/port: 20.1.144.11/60000

  Destination IP/port: 20.1.145.1/2904

  DS-Lite tunnel peer: -

  VPN instance/VLAN ID/Inline ID: -/500/-

  Protocol: SCTP(132)

  Inbound interface: GigabitEthernet1/0/6

  Source security zone: Trust

State: SCTP_COOKIE_ECHOED

Application: OTHER

Rule ID: 0

Rule name: pass

Start time: 2021-12-15 00:43:29 TTL: 29s

Initiator->Responder: 192 packets   23742 bytes

Responder->Initiator: 1266 packets   218618 bytes

正常时候sctp四次握手都是正常的

904	20.1.145.1	20.1.144.11	SCTP	90	0x5379 (21369)	INIT
922	20.1.145.1	20.1.144.11	SCTP	90	0x537a (21370)	INIT
103	20.1.144.11	20.1.145.1	SCTP	162	0x9b4d (39757)	INIT_ACK
347	20.1.144.11	20.1.145.1	SCTP	60	0x9b4e (39758)	COOKIE_ACK
741	20.1.145.1	20.1.144.11	SCTP	134	0x537b (21371)	COOKIE_ECHO
904	20.1.145.1	20.1.144.11	M2UA	70	0x537c (21372)	DATA [Malformed Packet]
989	20.1.144.11	20.1.145.1	SCTP	62	0x9b4f (39759)	SACK
174	20.1.144.11	20.1.145.1	S1AP	98	0x9b50 (39760)	[UNKNOWN PER: unknown extension root index in
229	20.1.145.1	20.1.144.11	SCTP	62	0x537d (21373)	SACK

异常时候防火墙上连口抓包缺少20.1.145.11发来的COOKIE ack报文导致sctp连接未建立，防火墙丢弃了COOKIE—ack报文导致业务异常

10.818998	20.1.145.1	20.1.144.11	SCTP	90	0x5a56 (23126)	INIT
10.819314	20.1.144.11	20.1.145.1	SCTP	162	0xf475 (62581)	INIT_ACK
10.820369	20.1.145.1	20.1.144.11	SCTP	134	0x5a57 (23127)	COOKIE_ECHO
11.642217	20.1.144.11	20.1.145.1	S1AP	90	0xf47d (62589)	
11.702083	20.1.144.11	20.1.145.1	S1AP	98	0xf48a (62602)	
11.762028	20.1.144.11	20.1.145.1	S1AP	98	0xf48b (62603)	

解决方法

后经定位为防火墙软件问题，需要出补丁解决，其他防火墙如果出现类似问题，需要升级最新版本。