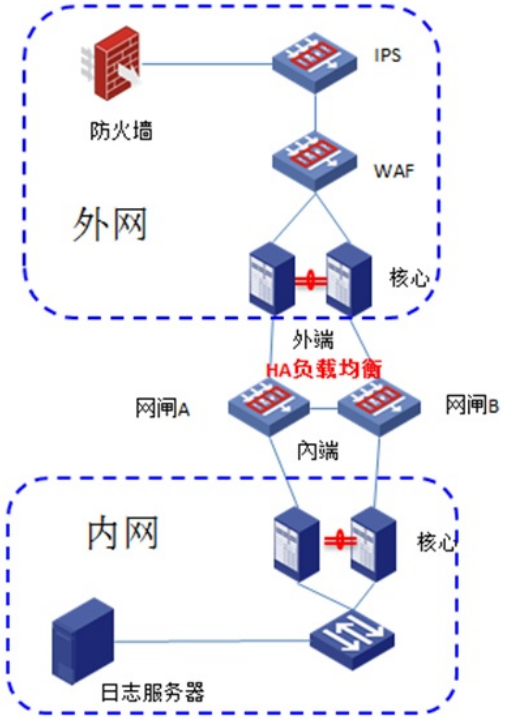
某局点SecPath GAP2000-A HA负载均衡部署后内网日志服务器接收不到日志的经验案例

Syslog日志 网闸 丁佳欣 2020-03-15 发表

组网及说明

客户两台SecPath GAP2000-A网闸设备形成HA负载均衡连接外网核心设备和内网核心设备，外网的IPS和防火墙的日志通过网闸传输到内网的日志服务器。



外网防火墙地址：10.100.0.2；外网IPS地址：10.100.2.100；网闸A外端机地址：10.100.10.238，内端机地址：172.18.10.238；网闸B外端机地址：10.100.10.234，内端机地址：172.18.10.234；内网日志服务器地址：172.18.12.66。

问题描述

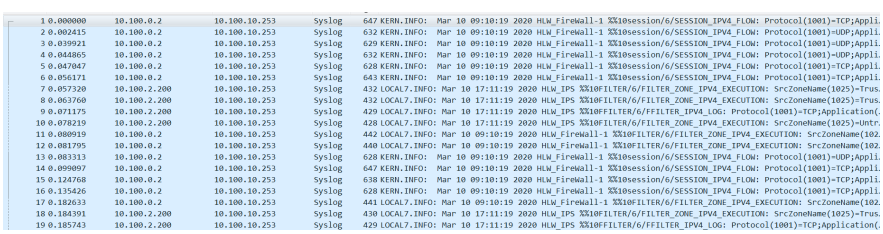
客户反馈过网闸内网的日志服务器接收不到外网防火墙和IPS的日志信息。

过程分析

1、日志服务器没接收到外网防火墙（10.100.0.2）和ips设备（10.100.2.100）的syslog日志信息，那么到底是防火墙和ips设备日志发送的问题还是中间传输问题导致日志信息的接收失败呢？指导客户在网闸设备上抓包，判断外网设备的日志信息到底有没有发出来？发出来了又传输到哪一步？确认故障点处于什么位置。

抓包配置，采用网闸本身的抓包工具，在两台网闸上分别配置抓取UDP端口514和主机172.18.12.66（日志服务器）和主机10.100.10.238 （网闸A外端机），主机10.100.10.234（网闸B外端机）的信息:

通过抓包发现在网闸B外端机上有日志信息（目的地址为配置的虚服务地址）：



1	0.000000	10.100.0.2	10.100.10.253	Syslog	647 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=TCP;Appli
2	0.002415	10.100.0.2	10.100.10.253	Syslog	632 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;Appli
3	0.039921	10.100.0.2	10.100.10.253	Syslog	629 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;Appli
4	0.044865	10.100.0.2	10.100.10.253	Syslog	632 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;Appli
5	0.047047	10.100.0.2	10.100.10.253	Syslog	628 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=TCP;Appli
6	0.056171	10.100.0.2	10.100.10.253	Syslog	643 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=TCP;Appli
7	0.057320	10.100.2.200	10.100.10.253	Syslog	432 LOCAL7.INFO: Mar 10 17:11:19 2020 HLW_IPS %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=Trus
8	0.063760	10.100.2.200	10.100.10.253	Syslog	432 LOCAL7.INFO: Mar 10 17:11:19 2020 HLW_IPS %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=Trus
9	0.071175	10.100.2.200	10.100.10.253	Syslog	429 LOCAL7.INFO: Mar 10 17:11:19 2020 HLW_IPS %%10FFILTER/6/FFILTER_IPV4_LOG: Protocol(1001)=TCP;Application(
10	0.078219	10.100.2.200	10.100.10.253	Syslog	428 LOCAL7.INFO: Mar 10 17:11:19 2020 HLW_IPS %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=Untr
11	0.080919	10.100.0.2	10.100.10.253	Syslog	442 LOCAL7.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(102
12	0.081795	10.100.0.2	10.100.10.253	Syslog	440 LOCAL7.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(102
13	0.083313	10.100.0.2	10.100.10.253	Syslog	628 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=UDP;Appli
14	0.099097	10.100.0.2	10.100.10.253	Syslog	647 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=TCP;Appli
15	0.124768	10.100.0.2	10.100.10.253	Syslog	638 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=TCP;Appli
16	0.135426	10.100.0.2	10.100.10.253	Syslog	628 KERN.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10session/6/SESSION_IPV4_FLOW: Protocol(1001)=TCP;Appli
17	0.182633	10.100.0.2	10.100.10.253	Syslog	441 LOCAL7.INFO: Mar 10 09:10:19 2020 HLW_FireWall-1 %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(102
18	0.184391	10.100.2.200	10.100.10.253	Syslog	430 LOCAL7.INFO: Mar 10 17:11:19 2020 HLW_IPS %%10FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=Trus
19	0.185743	10.100.2.200	10.100.10.253	Syslog	429 LOCAL7.INFO: Mar 10 17:11:19 2020 HLW_IPS %%10FFILTER/6/FFILTER_IPV4_LOG: Protocol(1001)=TCP;Application(

而内端机抓包没有信息，那么判断问题在于日志信息在网闸上从外端到内端没有得到正常传输。而外端机和内端机通过通道来传输信息，因此问题在于通道。

2、检查通道配置：

网闸A的日志通道配置，监听地址为10.100.10.238（外端机接口地址），目的地址为日志服务器（172.18.12.66），172.18.10.238为连接地址：

	86	外端 → 内端	UDP	10.100.10.238	514	172.18.12.66	514		172.18.10.238	是

HA负载均衡虚服务配置：

	89	10.100.10.253	514	外端机	SLOT1/1

虚服务对应实服务配置（虚服务地址所映射的实服务地址，两个地址需同一网段）：

	ID	IP地址	网卡	所属设备
	216	10.100.10.238	SLOT1/1	本机
	217	10.100.10.234	SLOT1/1	对端机

网闸B的日志通道配置，监听地址为10.100.10.234（外端机接口地址），目的地址为日志服务器（172.18.12.66），172.18.10.234为连接地址：

	86	外端 → 内端	UDP	10.100.10.234	514	172.18.12.66	514		172.18.10.234	是

HA负载均衡虚服务配置：

	89	10.100.10.253	514	外端机	SLOT1/1

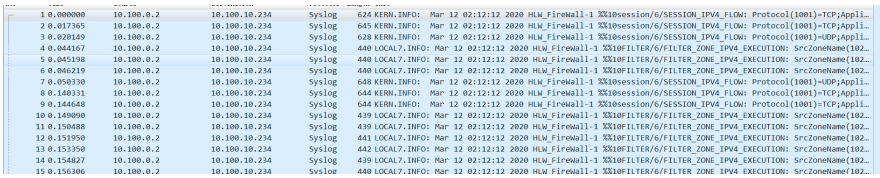
虚服务对应实服务配置：

	ID	IP地址	网卡	所属设备
	175	10.100.10.238	SLOT1/1	对端机
	176	10.100.10.234	SLOT1/1	本机

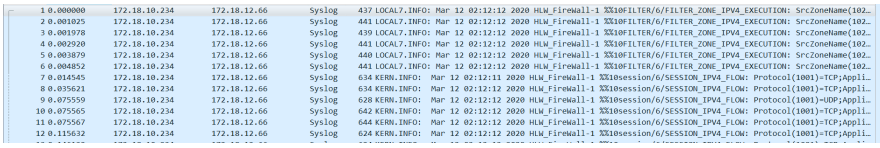
通道的配置没有问题。

3、此时考虑到去掉该通道负载均衡配置，仅保留正常通道配置测试，此时在网闸的内外端均抓包到了日志报文，内网日志服务器也接收到防火墙和IPS设备日志信息。

网闸B外端机抓包信息（由于删除负载均衡配置，因此抓取到目的地址为网闸B外端机真实地址）：



网闸B内端机抓包信息，有发送到日志服务器（172.18.12.66）的日志信息：



内网服务器也显示收到了来自外网防火墙和IPS设备的日志。问题得到解决。

后续确认到当前的最新版本ESS 6005的网闸设备的负载均衡功能仅支持TCP、HTTP、SMTP、POP3通道，而syslog日志通道属于UDP通道，因此通道增加了负载均衡的配置后无法向内网服务器传送syslog日志。

解决方法

当前的最新版本ESS 6005的网闸设备的负载均衡功能仅支持TCP、HTTP、SMTP、POP3通道，日志通道作为UDP通道不受支持，无法传输信息。仅保留日志通道配置，删除日志通道负载均衡的配置部分后问题解决。