H3C SecPath多级安全互联交换平台产品

用户 FAQ

目 录

H3C SecPath 多级安全互联交换平台用户 FAQ

本文档介绍 H3C SecPath 多级安全互联交换平台产品的用户常见问题及解答。

1 硬件类FAQ

1.1 平台重启后系统没有起来？

平台关闭电源后，不要马上打开电源开关，请等待 30 秒以上再开启电源，如果间隔过短，易造成系统内外端机启动异常。

1.2 硬件设备扩充插卡顺序？

G9020-PRE、G9020-POS 型号设备只支持首个万兆扩展槽位。

1.3 平台扩充插卡是否支持热插拔？

不支持。

2 业务功能类FAQ

2.1 多级安全互联交换平台调试及使用过程中如何确认设备通还是不通？

区别于常用路由交换设备。由于多级安全互联交换平台属隔离设备，目前不存在也不应该存在网络底层测试工具，能直接确认整体连通性。目前唯一能证明联通性的方法，只有应用测试才可确认。

2.2 应用不通如何排查问题？

(1) admin 账户登录平台，查看链路状态，若故障请排查前置和部件内端、后置和部件外端间网络连通性（可通过网络管理>网络诊断工具）

(2) 若链路状态正常，查看相应的应用通道是否开启

(3) 停用再启用通道，如果通道启用过程中存在错误，请联系售后部门。如果能够正常停用再启用通道，则说明平台内部通讯没有问题，通常问题都出在两端网络或平台配置上。

2.3 平台通道无法正常停用/启用怎么办？

检查链路状态，若链路故障请排查链路连通性；若链路状态正常，请联系售后。

2.4 如果通道可以正常停启用，应用还是不通，如何排错？

需要分两段检查平台两边网络问题，从客户端到前置之间排查网络问题，以及从后置到服务端之间排查网络问题。

客户端到前置之间的网络连通性：

(1) 业务链路管理—业务配置，查看链路配置中链路状态

(2) 客户端 telnet 平台应用通道的监听地址和端口

(3) 检查客户端到前置之间是否有其他安全产品拦截了，或者路由是否可达。

后置到服务端之间的网络连通性：

(1) 业务链路管理—业务配置，查看链路配置中链路状态

(2) 后置 telnet 应用服务器地址和端口

(3) 检查应用服务器端口是否开放，和平台通道目的端口是否一致

(4) 检查后置到应用服务器之间是否有其他安全产品拦截了，或者路由是否可达。

2.5 FTP应用，平台通道可以停启用，两边连通性也没问题，但是应用不通怎么办？

检查通道是否选用了 FTP 类型。

检查 FTP 服务器是否支持被动访问模式。由于 FTP 应用协议会动态协商数据端口，重新建立连接，平台出于安全考虑是禁止外部服务器随意进行连接的，所以数据端口只能由平台去连服务端，这就要求 FTP 服务器必须支持被动访问模式。

同理，客户端的数据端口也只能由平台来连客户端，因此客户端防火墙必须为此做相应调整。

2.6 oracle应用，通道可以停启用，两边连通性也没问题，但是应用不通怎么办？

如果 oracle 服务器是 Windows 平台的，并且使用默认的专用访问模式，则平台的通道类型要配置成为 oracle 类型。

如果 oracle 服务器是 Linux 或 UNIX 等平台，或者使用的是共享访问模式，则平台的通道类型就要配置成为 TCP 类型。

2.7 基于域名的WEB应用访问怎么配置？

当内部用户需要通过平台访问外部 WEB 应用服务。

(1) 解决 DNS 解析问题。配一条端口为 53 的 UDP 通道，目标 IP 为外网设置的 DNS 地址。随后将客户端 DNS 改成平台 UDP 通道中的监听 IP。

(2) 创建 HTTP 类型通道，直接将域名填入目的地址

2.8 文件同步出现同步任务消失怎么办？

平台配置>服务管理，选择相应链路，重启文件同步服务。

2.9 Mysql数据库同步表关联提示报错怎么办？

尝试没有外键表的优先添加。

表的同步方向和触发器类型尽量相同。

2.10 文件同步报错提示：共享目录已被使用怎么办？

尝试先手动选择目录。

2.11 登录帐号和密码忘了怎么办？

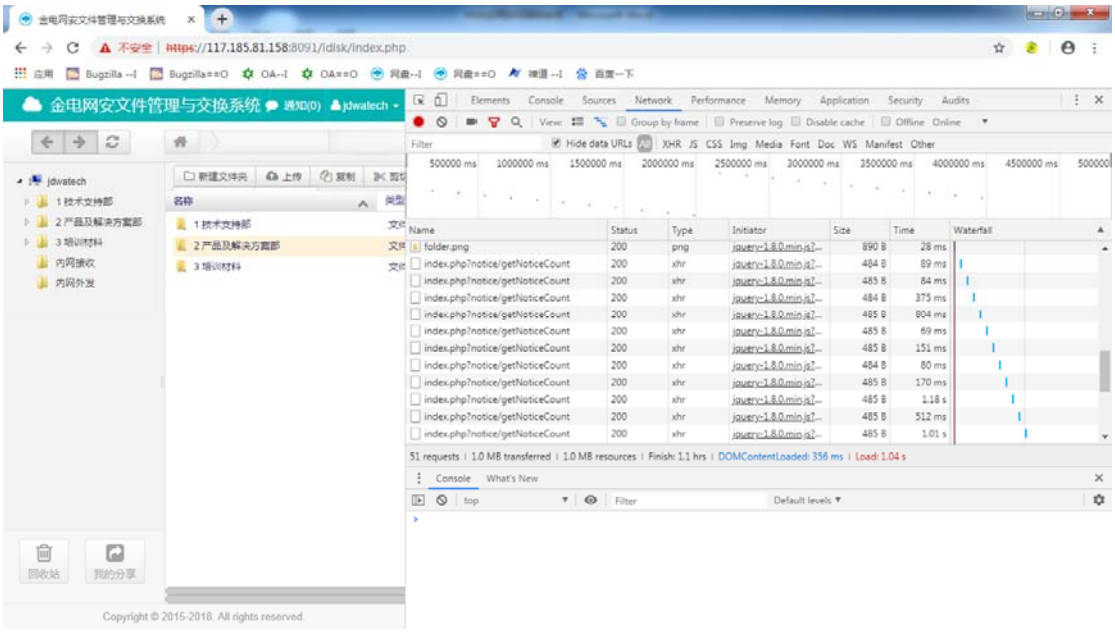
联系公司专人负责远程支持解决。

2.12 如何跟踪WEB应用访问中的会话？

平台两侧 TCP 连接正常；源端抓包未发现 TCP 握手失败的连接；抓包 follow 内外应用层信息，两边内容一致，但是过平台打不开页面，如何解决？

某些 WEB 应用访问不是单一会话构成的。可能在访问时会同时建立多个 http 会话。比如一些认证服务器。某些网站在登录帐号时，会寻求其他认证服务器的验证，因此会额外建立新的会话。由于这些 IP 和端口可能和原有应用不同，混在众多会话中难以查找和验证。如何跟踪一次 WEB 应用访问，调查页面卡在哪个 url 成了关键

操作方法：使用 google chrome 浏览器。按 F12 进入开发模式。然后打开要访问的页面



右边列表可以轻松看到打开的每个 URL。如果有资源连接不上，会显示红色。我们只要查这些红色的 url 是不是连接了新的域名或 IP 即可。很有可能服务器反馈了一个新的域名，导致内网无法直接做 DNS 解析，从而不再发送新的连接，最终导致抓包无法发现问题。

查找 302 重定向的包，比较容易看到此类现象。比抓包分析要方便。

2.13 文件同步发现按键界面错位。

更改电脑分辨率

2.14 SIP通道配置后，信令中的码流接受地址未替换成平台自身IP，怎么办？

按照国标GB/T28181和DB33的标准。平台在处理SIP信令时，需要将点播或录像的码流返回IP替换成平台自身地址。保证码流返回时，流媒体服务器发到平台上，并通过动态转发规则，将码流返回给客户端。而不是从流媒体服务器直接发往客户端IP。

2.15 平台运行一段时间后业务不通，重启通道恢复，多次出现类似情况怎么办？

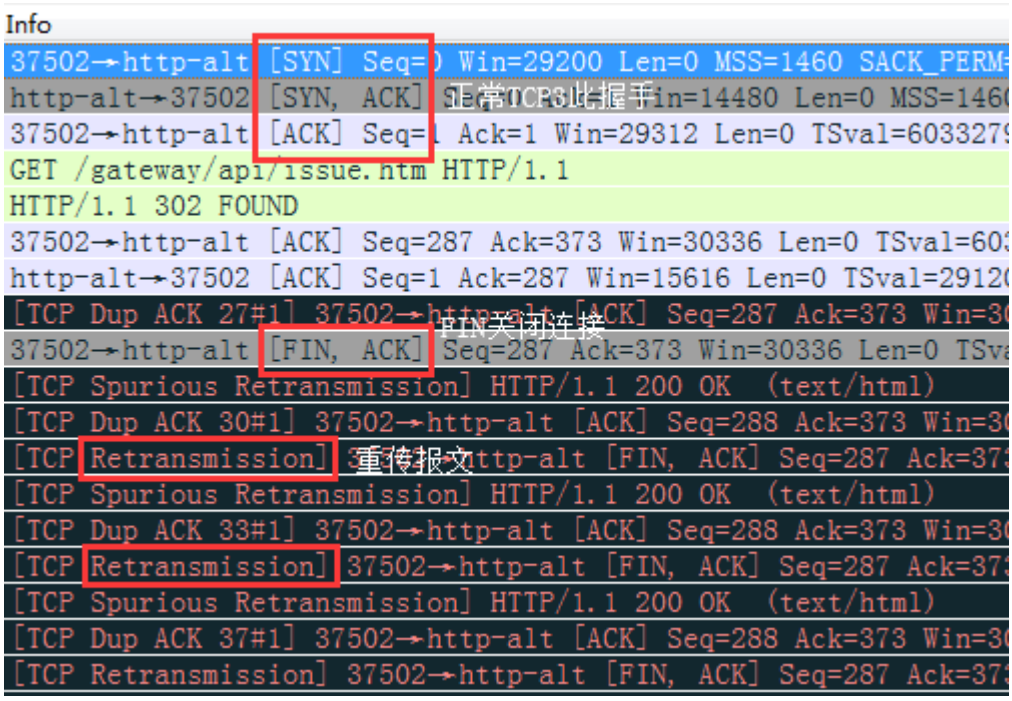
登录平台安全管理员界面，在系统管理>统计报表界面中查看通道连接数，检查是否存在连接数非常大且不减少的通道，若存在，检查此通道业务是否存在客户端不释放连接的情况。平台默认不主动释放连接，若为客户端某些情况下存在不释放连接的问题，需给通道配置空闲超时时间，在连接无数据传输时，平台主动释放连接。

2.16 配置TCP通道访问HTTP应用时，两边能够建立TCP会话，但是应用层数据无法交换，业务访问无法实现（页面显示不全或下载内容不完整）如何判断问题？

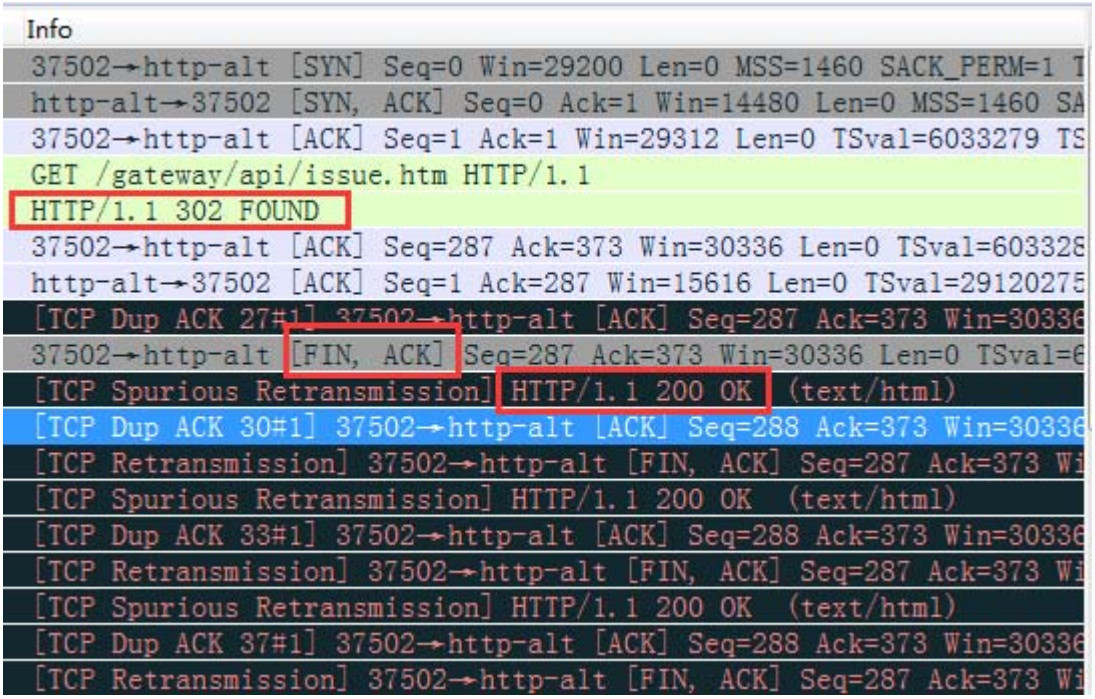
目前主要有两种情况：

1）半连接情况。两边会话建立起来后，其中一边提前发送了 FIN 包关闭连接，但另一边还没发送完数据，要等数据全部发送完之后才发送反向 FIN 包（在没有隔离平台时,TCP 允许的）。然而，平台两边只要其中一侧关闭连接，另一边也会立刻关闭。所以会导致后续数据无法通过平台。该问题，最好应用程序改会话控制，保证数据都发送完毕后，再互相发送 FIN 包关闭连接。

2）HTTP 请求被重定向或拦截。这种情况抓包后和第一种情况很类似，都是可以先看到一个 FIN 包，后面跟了很多重传报文



但是会有区别，如果页面是被重定向的，那 HTTP 反馈的信息不会是 200 OK，而是 302 FOUND。其次 FIN 包发送后，服务器的正常反馈信息才会发送到平台，如下图：



3）能够收到不同 HTTP 服务版本的响应。通常重定向的服务版本和正确的 HTTP 服务器版本不一样，如下面 2 图：

图1 重定向服务版本

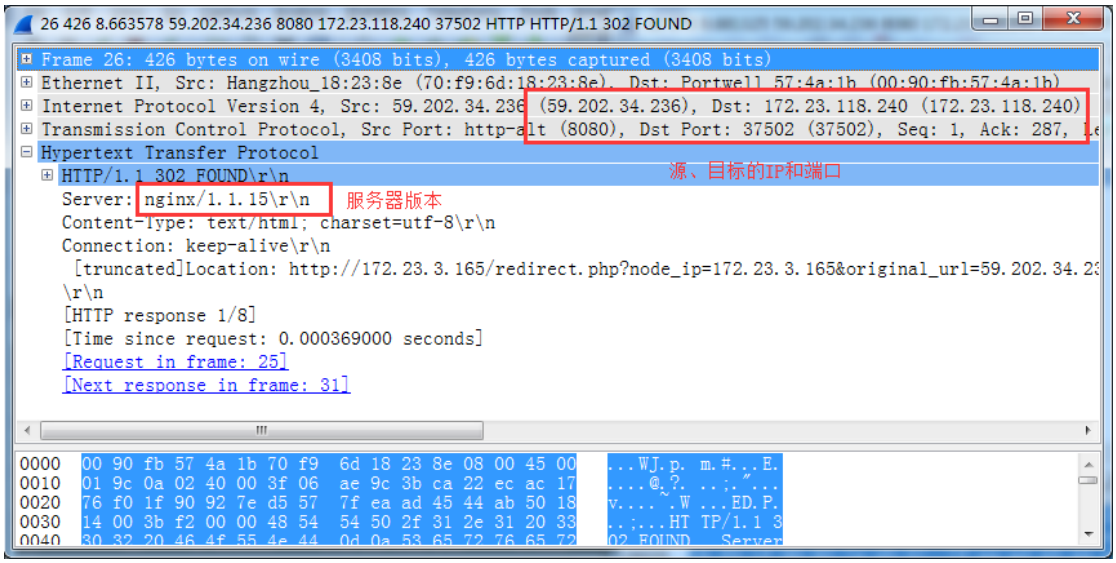
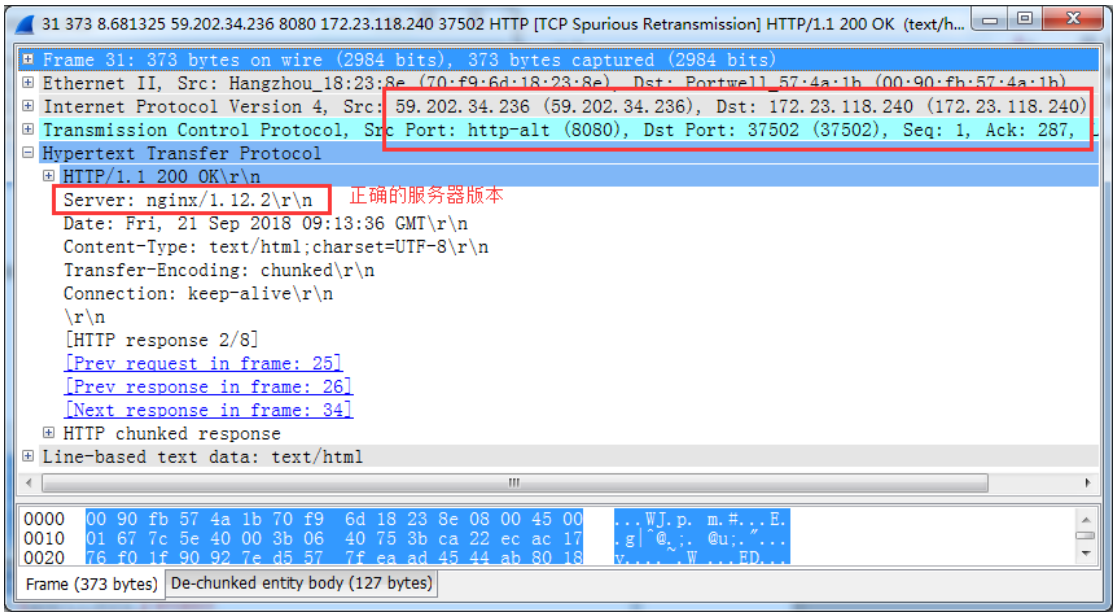


图2 正确服务器版本



如果发现相同的目标 IP、端口，能够收到 2 个不同 HTTP 服务版本的响应，那基本就能认定，发往服务器的包被重定向了。

解决办法：

链路上查找，有没有上网行为管理和准入认证功能的安全产品。比如第二代防火墙、准入系统、上网行为管理设备、安全网关等。让这些安全设备开放白名单，放行所有平台出去的包。

2.17 前后置设备内存使用率较高，影响正常业务访问怎么办？

secrecy 用户登录，查看系统管理>统计报表中各个通道的连接数是否存在比较高且一直不下降的情况。

针对 UDP 类型的通道：需要将端口类型更改为端口段类型。配置要求是监听端口与目的端口相同，需要注意修改其他设备的网络配置。

针对 TCP 类型的通道：连接数与业务相关，需要跟踪分析业务实现逻辑，如果对应的通道业务存在不主动释放连接问题，需要确认业务长连接时长，根据业务实际情况在平台通道上配置空闲超时时间。