关于 IPTV 业务网络信息安全风险控制的研究

张文杰
新疆电信，新疆 乌鲁木齐 830000

[摘要]IPTV 即宽带电视，为用户提供基于互联网电视、信息等服务。IPTV 业务已经逐渐成为通信运营商的基础业务之一，正在飞速的发展。确保 IPTV 的网络信息安全，具有非常重要的政治意义，这为深入研究和有效应对新形势对 IPTV 业务安全生产提出的新要求和新挑战。为进一步落实维护管理和风险控制要求，确保风险可管可控，文中针对风险控制维度进行了深入的分析，找到业务关键换节点进行自动化脚本部署。实现了当业务出现内容篡改或信息安全风险时，第一时间将问题控制在一定的范围内，具备业务一键处置能力。

[关键词]IPTV；风险控制；网络信息安全
DOI：10.33142/sca.v5i1.5574　　中图分类号：F626;TP309　文献标识码：A

Research on Network Information Security Risk Control of IPTV Service

ZHANG Wenjie
Xinjiang Telecom, Urumqi, Xinjiang, 830000, China

Abstract: IPTV is broadband TV, which provides users with Internet-based TV, information and other services. IPTV service has gradually become one of the basic services of communication operators and is developing rapidly. Ensuring the network information security of IPTV has very important political significance, which puts forward new requirements and challenges for in-depth research and effective response to the new situation on the safe production of IPTV business. In order to further implement the requirements of maintenance management and risk control and ensure that the risk can be managed and controlled, this paper makes an in-depth analysis on the risk control dimension, finds the key business nodes for automatic script deployment. When there is content tampering or information security risk in the business, the problem can be controlled within a certain range at the first time, and the business can be handled with one key.

Keywords: IPTV; risk control; network information security

引言

在做好 IPTV 平台日常维护和安全防护的情况下，当出现内容信息安全问题，需要对影响面进行控制，将负面影响降至最低，切实做好业务风险一键处置能力是关键。

1 风险控制的实现思路

从业务实现角度出发，将业务风险点逐个进行分解，找到业务关键控制点，通过集成播控平台执行处置脚本，实现业务风险的一键处置能力。

1.1 直播

业务实现：IPTV 直播业务通过组播方式从播控平台传输至 IPTV 平台。

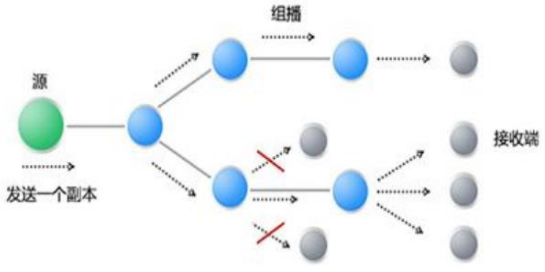

图 1　直播业务实现

风险控制思路 1：通过集成播控平台关闭直播节目，使得问题内容进行下线操作。

风险控制思路 2：从源端切断问题内容。通过自动化脚本部署，登陆交换机，启用 ACL 对直播频道进行限制，实现内容下线操作。通过该方法可实现直播频道从源端快速切断。

1.2 点播

业务实现：通过客户端的播放器，向服务器发起媒体业务请求，该服务为点对点的服务。

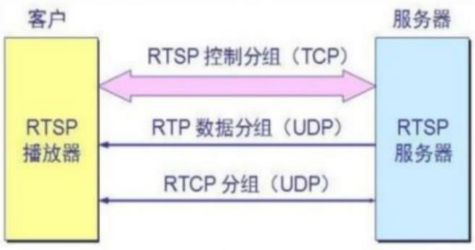

图 2　点播业务实现

风险控制思路 1：通过内容播控平台对风险节目内容进行下线操作，使得 CDN 的服务器上没有风险内容。该方

式为正常情况下，需要使用的控制方式。

风险控制思路 2：通过自动化脚本的部署，对点播服务的 CDN 节点服务器进行网络层面限制。登陆问题节点所在交换设备，取消下发缺省路由，能够快速实现节点服务终止。该方式，在思路 1 无法控制的情况下使用。[1]

1.3 EPG

业务实现：通过 HTTP 协议实现用户电子节目单服务。

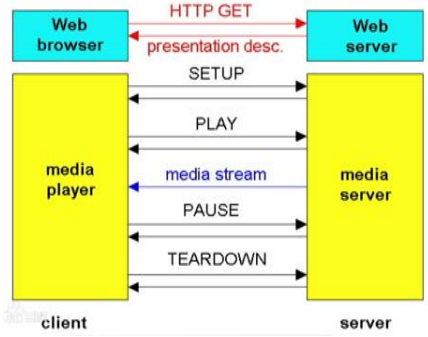

图 3 EPG 业务实现

风险控制思路 1：通过集成播控平台，对有问题的页面文件进行恢复操作。

风险控制思路 2：通过部署自动化脚本，对问题 EPG 服务停止，降低负面问题影响面。该方式当方法 1 无法恢复，可以使用。

2.4 用户终端设备

业务实现：用户终端设备，通过网关获取 IP 地址，来进行服务端的业务请求。

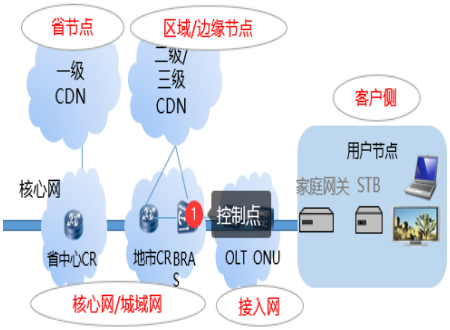

图 4 用户终端设备业务实现

风险控制思路：通过限制用户终端的网关设备（控制点 1），禁止流量转发，来降低负面问题影响面。[2]

2 风险控制实现方法

通过上一章节，通过对业务流程的梳理，我们找到了应对的思路。本小节将针引用一些通用的实现和回退操作的方法。

2.1 直播

2.1.1 华为交换机：

2.1.1.1 关闭直播节目

```
sys                    //进入系统模式
acl number  XXX        //建 ACL，编号为 xxx
description shutdown-zhibo  //描述，单个组播，（非指令）
```

据播控平台所选频道，传递组播地址（ip source 后面的 IP，为变量），rule 后面的数字 1 和 5 为变量，根据所选频道的个数，以 5 的倍数递增，例如选了三个频道，则指令为：

```
rule 1 deny  ip source  xxx.xxx.xxx.xxx    //组播 IP1（所选第一个频道）
rule 5 deny  ip source  xxx. xxx.xxx.xxx    //组播 IP2（第二个需关停频道）
quit      //退出一次
pim       //进入 PIM
source-policy  xxx  //pim 下应用 ACL 策略
quit
```

2.1.1.2 恢复直播节目

```
sys       //进入系统模式
acl number  xxx    //建 ACL，编号为 xxx
undo rule 1  deny  ip source  xxx.xx.xxx.xxx //组播 IP
undo rule 5  deny  ip source  xxx.xx.xxx.xxx //对一键关停的 rule 操作指令前增加 undo
quit    //退出一次
pim     //进入 pim
source-policy    xxx       //pim 下应用策略
quit    //退出一次
```

实施效果：通过去除访问控制列表后，节目可恢复正常。

2.1.2 中兴交换机

2.1.2.1 关闭直播节目

```
configure terminal          //进入配置模式
```

//据页面所选频道，传递组播地址（ip source 后面的 IP，为变量），rule 后面的数字 1 和 2 为变量，根据所选频道的个数，以 1 为步长递增：

```
ipv4-access-list shutdown-zhibo    //创建过滤的 ACL，名称为 shutdown-zhibo
rule 1 deny ip any xxx.xxx.xxx.xxx 0.0.0.0  //拒绝的频道
rule 9999 permit ip any any    //其他频道允许
exit  //退出 1 次
```

2.1.2.2 恢复直播节目

```
configure terminal          //进入配置模式
```

删除 acl 中相应的 rule，示例为：

```
ipv4-access-list shutdown-zhibo      //进入名称为 shutdown-zhibo 的 ACL
no rule #                  //删除前期拒绝的频道，#代表为前期拒绝组播频道添加的 rule id
exit  //退出 1 次
```

exit //退到#模式
exit //退出会话
实施效果：与华为交换机类似

2.2 CDN 节点服务限制

通过取消缺省路由，限制服务器的通信。我们以华为交换机为例。

2.2.1 节点服务限制
sys //进入系统模式
ospf 1 //进入 ospf 进程
undo default-route-advertise always //取消下发缺省路由策略
quit
quit //退出 2 次
2.2.2 取消限制：
sys //进入系统模式
ospf 1 //进入 ospf 进程
undo default-route-advertise always //取消下发缺省路由策略
quit
quit //退出 2 次：
实施效果：通过取消默认路由，节点网络无法进行数据转发。

2.3 用户终端网络限制

在用户终端的网关设备上开启，禁止数据转发，以华为路由器设备为例:

2.3.1 用户端网络限制
sys //进入系统模式
acl xxxx //新建 ACL
rule 1 deny ip source user-group iptv destination any //策略规则，拒绝所有请求
quit //退出一次
traffic classifier iptv //进入 iptv 域
if-match acl xxxx //此类引用策略 acl xxxx
quit //退出一次

2.3.2 取消限制
sys //进入系统模式
traffic classifier iptv //进入 iptv 域
if-match acl xxxx //取消此类引用策略 acl xxxx
quit //退出一次
undo rule xxxx //删除 ACL 策略
实施效果：引入控制策略后，机顶盒所在网络无法与外部网络通信。

2.4 EPG

以 linux 系统，下部署的 httpd 服务为例：

2.4.1 限制服务：
ssh -p xxxx xxx.xxx.xxx.xxx “service httpd stop”
//远程连接服务器-执行业务关停指令
2.4.2 恢复服务：
ssh -p xxxx xxx.xxx.xxx.xxx “service httpd start”
//远程连接服务器-执行业务恢复指令
实施效果：通过服务停止，使得业务端口无法监听。

3 结束语

总的来说，IPTV 业务的安全是重中之重，在有限的情况下，通过控制问题的影响面，在特殊事件发生时能够起到非常重要的作用。通过在集成播控平台集成网络信息安全风险控制模块，解决了值班人员知识能力较弱，无法第一时间处置问题，同时可以大大提升应急处置的处理响应速度和效率。

[参考文献]

[1]聂祥.浅析现阶段 IPTV 业务的应用及运营[J].电信科学,2005,1(2):1-5.
[2]许永明.IPTV 技术与应用实践[D].北京:电子工业出版社,2006.

作者简介：张文杰，男，汉族，新疆电信，产品研发工程师，从事 IPTV 平台相关专业 12 年，曾获得自治区通信管理局科技创新三等奖。