**网络设备控制面安全防护**

**1、背景**

网络设备接入Internet时，会面对大量网络攻击。设备控制面CPU面临的攻击威胁主要包括：非法用户通过远程设备登录访问、恶意的DoS（Deny of Service）攻击消耗CPU系统资源、各种泛洪流量影响设备的本地处理、利用TCP/IP协议栈存在的漏洞攻击设备的应用等。

设备控制面安全防护需要对从接口板上送到CPU处理的报文进行安全保护。主要包括对攻击报文进行过滤、对已建立连接（如TCP连接）的业务进行保护，主动过滤攻击流量，保障设备业务正常运行，保护设备的CPU以及系统存储资源，实现设备安全性能的提升的目的。



上图是路由器设备的基本硬件架构图，以路由器设备为例，控制平面安全技术应用的主要目的，是通过系统中不同模块的协作来保护线卡CPU和协议处理卡CPU不被来自网络中的有意或无意的攻击流量破坏，保证设备业务的正常运行。

**2、现有解决方案**

以路由器设备为例，设备上部署了大量业务，为保证这些业务的正常运行，避免CPU的影响，设备提供了一系列静态安全策略，主要包括：

1. ACL安全配置策略：对设备需要上送CPU处理的业务，通过静态配置ACL策略进行安全过滤
2. 协议限速功能：对CPU上运行的协议，进行协议的限速配置，接口接收到超过速率的报文会被丢弃
3. 协议优先级队列：不同的协议通过不同的优先级队列进行区分，通过优先级队列调度策略，目的是让攻击流量进入低优先级，与设备运行的高优先级业务进行隔离区分

现有方案存在的问题：

当前的控制面安全方案（ACL策略、限速配置、优先级队列调度机制）都是基于静态配置，需要根据场景、业务模型深入分析当前的业务量，通过预置配置的方式，将这些安全策略静态配置到设备上。人工计算出的配置也无法与系统CPU能力相结合，设备开通时，现场工程师需要承受的工作量和能力要求非常大。系统需要有自动调整机制，包括智能场景的攻击识别和策略自动调整能力。

1. **问题**

请结合自身知识，结合计算机网络安全、TCP/IP协议，调研分析网络设备安全的现状，给出自己的分析理解和拟解决方案，实现网络设备智能安全防护。

方案加分项：

1. 提供智能安全策略，设备不需要根据场景与业务模型预置繁琐的静态安全策略，而是通过智能策略实现设备的安全防护，方便用户运维部署。
2. 具体的案例实现：对于TCP各类攻击，方案如何做到保证已建立TCP连接的业务不受攻击影响。

要求：请您以Word输出整体运作方案，并将其中要点以PPT形式进行输出，在极致挑战环节进行宣讲。