



神州云科
Yunke China

云科负载均衡之 证书卸载与流量编排 SSL0

产品介绍

北京神州数码云科信息技术有限公司

www.yunke-china.com

产品概述



机构或企业需要保护关键资产免受来自内外部的威胁。但如今大多数流量都进行了加密，现有安全控制无法根据检查的要求进行解密，导致关键资产极易受攻击。云科 SSL Orchestrator 提供基于策略的编排，支持经济高效地查看任何网络拓扑、设备或应用的完整安全服务链。

挑战

对隐私的担忧推动了加密流量的增长，如今超过 80% 的页面加载都采用了 SSL/TLS 加密。这一增长带来了严峻的挑战：攻击者通常将威胁隐藏在加密的有效载荷中，并使用加密通道逃避检测，他们选择特定的加密算法，以绕过加密探测的保护。大多数机构或企业无法对安全链中常见的安全检测设备集中实施解密策略。因此，安全团队必须使用菊花链架构的设备或繁琐的手动配置来支持安全链检查，这就大大增加了延迟、复杂性和安全风险。

主要优势

- 获得加密流量的可视化。

通过对整个网络堆栈进行集中解密，发现隐藏的威胁。

- 最大限度地利用安全投资。

通过高效管理出入站加密流量优化性能。

- 改进风险管理和隐私保护。

实施合理的策略，在安全和隐私保护之间取得有效平衡

解决方案

云科SSL Orchestrator 可提供对出入站 SSL/TLS 流量的高性能解密，支持进行安全检查以发现威胁和阻止攻击。动态服务链和基于策略的流量导向支持机构或企业智能地管理整条安全设备链上的加密流量，并获得最佳可用性。

SSL Orchestrator 确保加密流量可以被解密、被安全的控制检查以及重新加密，提供了增强的可视化，可帮助规避网络中的威胁。这样，机构或企业可以最大限度地利用针对恶意软件、数据丢失防护（DLP）、勒索软件和下一代防火墙（NGFW）的安全服务投资，从而有效防止出入站威胁，包括漏洞利用、回调和数据外泄。

部署条件

云科 SSL Orchestrator 支持多种部署模式，可以轻松集成到复杂的体系架构中，为出入站流量提供集中解密功能。SSL Orchestrator 支持多种出入站拓扑模式（包括入站层 2/3、出站层 2 和出站显式/透明代理）和多种安全设备（包括 2/3 层、Tap、Web 代理、仅接收流量和基于 ICAP 的设备）

优化运营效率

安全团队习惯于手动连接产品，创建了包含多个组件的菊花链式安全堆栈。典型的堆栈可能包括 NGFW、DLP 扫描仪、Web 应用防火墙（WAF）、入侵防御系统（IPS）、恶意软件分析工具等组件。

静态配置的安全链运营效率低下，无法适应不断变化的网络状况。SSL Orchestrator 可动态地连接安全设备，独立监控和扩展这些设备，并通过上下文分类引擎智能管理跨整条安全链的解密。动态服务链和基于策略的流量导向降低了运营成本，并支持将菊花链架构的安全设备转换为高度可用的安全服务。



图：云科 SSL Orchestrator 动态服务链

功能介绍

SSL Orchestrator 可帮助团队简化安全服务部署，提升加密环境的敏捷性、控制和可视化。

SSL 可视化	支持软件可对进入安全设备前的 SSL 流量进行卸载，可将卸载完成后的流量送入到安全设备组进行流量内容检查。支持 ECDHE 等具有 PFS 的高级算法。
安全设备池化	可将接入的安全设备进行池化，并按照不同的负载均衡算法分配流量到一个安全设备组中的所有安全设备，使安全设备组具有动态平滑扩展功能。
安全设备健康检查	支持对安全设备进行健康检查，在安全设备失效后，不再对其进行流量分配。
安全设备接入支持	支持 IPS、WAF、NGFW、DLP、上网行为管理、防毒墙等安全设备的接入，并支持所接入安全设备的各种部署模式，包括 L2 透明、L3 网关、L3 透明、TAP 等部署模式。
动态服务链	支持对所接入的安全设备配置基于策略的动态服务链，可分配不同属性的用户流量经过不同动态服务链中安全设备顺次进行检查。
安全流量编排	可对不同属性用户的流量进行编排，使其流经不同的安全设备，并可实时将某个安全设备或安全设备组 Bypass。

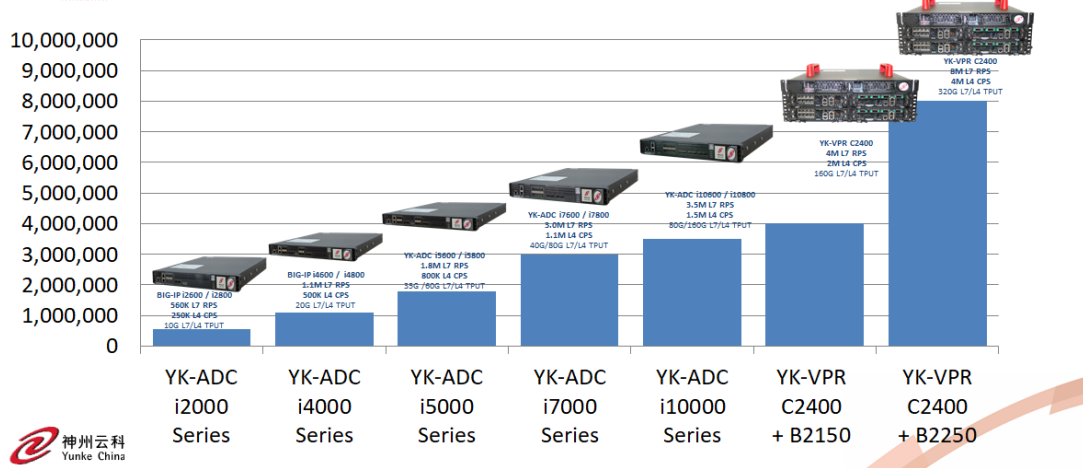
安全流量区分	可根据以下条件, 对用户流量进行区分, 可对不同属性的用户流量匹配到不同的动态服务链: 1、源 IP 2、目的 IP 3、目的端口 4、IP 地理信息 5、域名 6、IP 黑名单 7、URL 8、协议
可编程支持	支持基于 TCL 的可编程能力, 以适应复杂业务环境。
双机策略	支持双机主备部署, 并支持配置同步。
软件扩展性	可以软件形式附加到应用交付设备, 并与其整合部署, 实现对安全流量的编排。
部署模式	支持以下部署模式: 1、入向 L2 透明部署; 2、入向 L3 网关部署; 3、与现有应用交付设备整合部署。 4、出向 L2 透明部署; 5、出向 L3 透明部署; 6、出向 L3 代理部署
支持接入设备	1、支持 Web Proxy 设备接入; 2、支持透明二层设备接入; 3、支持三层设备接入; 4、支持基于 ICAP 的 DLP 设备接入; 5、支持 Received Only 类旁挂设备接入。
管理方式	全图形化向导部署, 简化用户运维管理。

产品系列

高性能可扩展的硬件平台

L7 RPS (inf-inf)

灵活的性能级别和按需扩展能力



神州云科
Yunke China

北京神州数码云科信息技术有限公司

Beijing Digital China Yunke Information Technology Limited

地址：中国·北京·海淀上地九街9号数码科技广场

网址：www.yunke-china.com

邮箱：yunkechina@digitalchina.com

热线电话：400-068-1180