神州云科高级应用交付防火墙（AWAF）

产品介绍（YK-AWAF r10900）

北京神州数码云科信息技术有限公司

www.yunke-china.com

产品概述

  "世界正迎来百年一遇的大变局，以互联网、5G、人工智能技术的发展与普及为代表，以数字化、网络化、智能化为特征，第四次工业革命浪潮把我们带入了物联网时代。与此同时，新一轮科技革命，正在重塑全球经济结构。全球正在进入以信息产业为主导的经济发展期，网络风险和威胁也随之与日俱增，应用漏洞造成的后果愈发严重，网络安全技术成为把握命脉的核心技术，关系到人身安全、机构安全、城市安全，作为领先的中国应用交付解决方案供应商神州云科以独特的视角，强大的研发能力和品牌优势推出在新技术革命时代的安全防护体系解决方案——神州云科高级应用交付防火墙（AWAF）。

  随着更多的应用流量通过网络传输,敏感数据面临着被盗、安全漏洞和攻击的威胁,尤其是在应用层。神州云科 AWAF 产品是一个先进的 Web 应用防火墙,可显著减少和控制数据、知识产权和 Web 应用丢失或损 坏的风险。云科 AWAF 可以防护多种应用攻击,包括：第 7 层 DoS 和 DDoS、暴力攻击、XSS、SQL 注入、 参数篡改、敏感数据泄露、会话劫持、缓存溢流、Cookie 篡改、多种编码攻击、断开的接入控制、强制浏览、 隐藏字段操作、请求走私、XML 炸弹等。云科 AWAF 通过一个将应用交付与网络和应用加速及优化结合在 一起的平台,提供了无与匹敌的应用和网站防护、完整的攻击专家系统,并且可以满足关键的法规要求。云科 AWAF 是业内最全面的 Web 应用安全与应用完整性解决方案。对于对业务至关重要的应用,屡获殊荣的云科 AWAF 能够使其保持安全性、可用性和高性能,从而保护了企业的安全,并维护了企业的声誉。

主要优势

确保应用安全性和可用性

可抵御 7 层分布式拒绝服务（DDoS）、SQL 注入和 OWASP 十大攻击的全面地理位置攻击保护，并可为最新的交互式 AJAX 应用和 JSON 有效负荷提供保护。

降低成本并实现合规性

借助内置的应用保护和集中策略部署，实现安全标准合规性。 多功能集成于扁平化统一平台，高性价比。

获取即购即用的应用安全策略

预建的快速部署策略和最低配置即可提供强大保护。

增强应用安全性和性能

在提升性能和提高成本效益的同时提供了高级的应用安全。

灵活部署和集成外部智能

着重于在虚拟和云环境中提供快速应用开发和灵活的部署模式，同时集成外部智能防护应用来抵御有害 IP 来源的风险。

云科 AWAF 先进的内置安全防护和远程审计功能可帮助您的企业以经济高效的方式满足行业安全标准的要求,包括 PCI DSS、HIPAA、Basel II 和 SOX,您既不需要购置多个设备,也不需要对应用进行更改或重写。云科 WAF 提供了针对新型威胁的高级报告能力,例如第 7 层服务拒绝攻击(DoS)、暴力攻击和 SQL 注入攻击等。通过 PCI 报告功能,云科 WAF 列出了 PCI DSS 1.2 所要求的安全措施,并确定是否满足了要求,若未满足要求则详细说明为满足要求所需采取的措施。此外,云科 WAF 可以与 WhiteHat、Splunk 和 Secerno 集成,可支持漏洞评估、审计和实时数据库报告功能,从而实现安全违规检查、攻击防护和法规遵从。云科 Web 应用 防火墙的主要功能有:
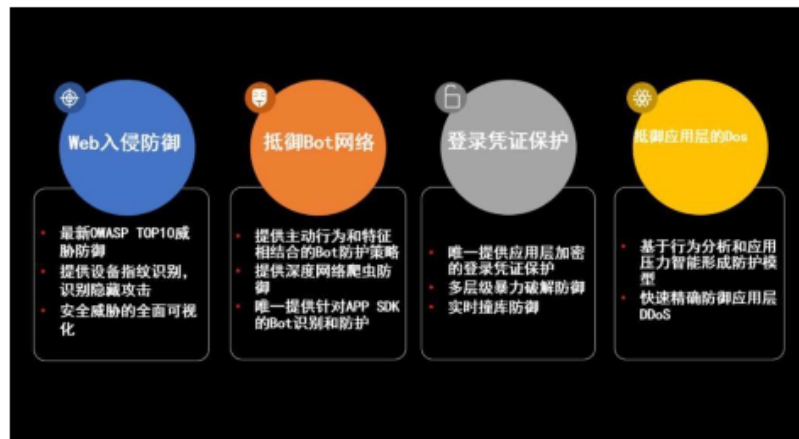
典型应用场景

应用基础架构安全

常见应用层攻击

OWASP 10, SQL/PHP 注入，保护应用和数据

账号保护

防止中间人攻击

防范垃圾账号注册、暴力攻击、撞库、恶意重置账号等

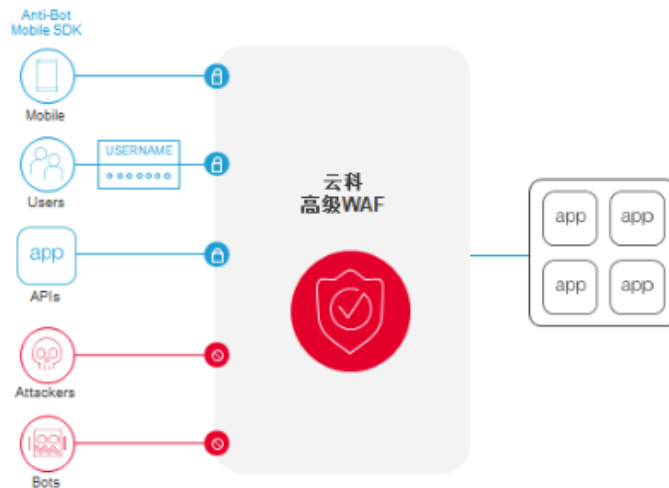### API 防护

业务活动保障：秒杀、促销 短信通道利用：短信炸弹；恶意查询等

阻止应用层拒绝服务攻击

时刻监控应用压力，自动检测并减缓攻击给业务带来的影响，减少人工参与

主动阻断机器人 BOT 攻击 验证码注入、终端安全检测、移动端 SDK 等 数据和隐私防护

登录和支付密码加密

机密数据脱敏和混淆等

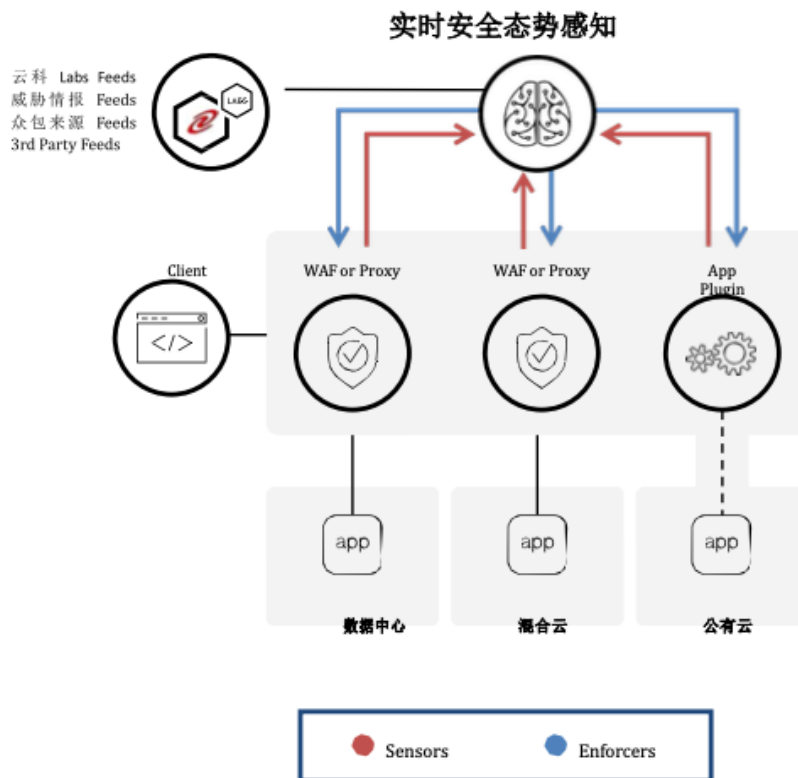## 威胁情报和安全服务

主动性流量和用户行为分析

正常流量 vs 恶意流量，行为分析，终端分析，流量特征

横向综合分析

基于风险的安全策略

威胁情报

联合安全产业专家，共同抵御各种安全威胁

多云安全分析

提供统一的威胁分析服务应对多云环境下的应用风险和应用健康保障

实时安全态势感知

云科 Labs Feeds
威胁情报 Feeds
众包来源 Feeds
3rd Party Feeds

Client　WAF or Proxy　WAF or Proxy　App Plugin

app　app　app

数据中心　混合云　公有云

● Sensors　● Enforcers

API 安全防护

全面协议校验

对 XML, JSON, GWT 等协议进行校验，如校验每个 API 请求的 Method

快捷导入

支持 Swagger 和 JSON schema 导入，API 安全与 API Server 快捷整合，无缝防护

精细化内容检测

对各种 API 协议的内容进行精细化内容检测，如检查签名特征，元字符，参数，长度等

实现统一的认证和授权

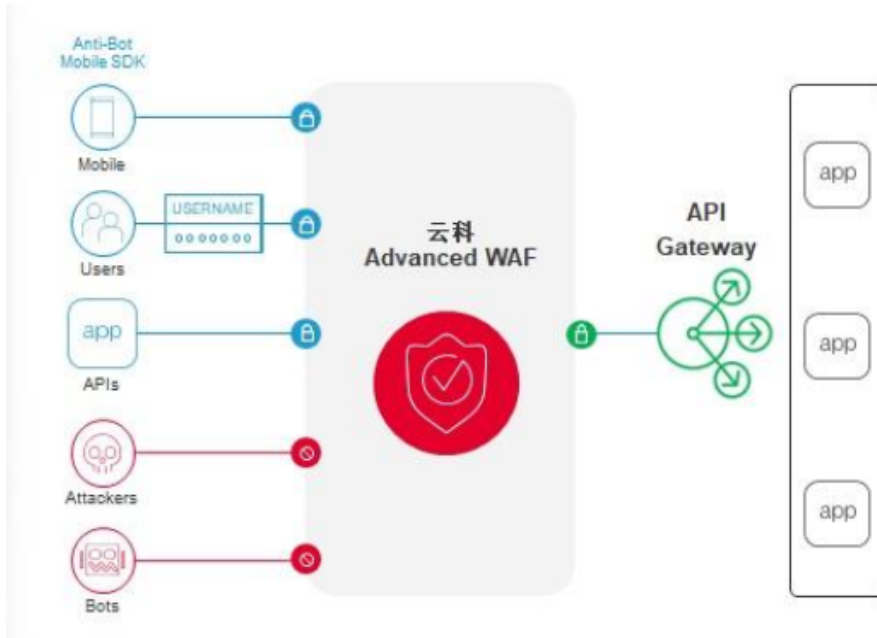支持 OAuth, OpenID, JWT 等授权，对 API访问源，访问方式等控制

速率与大小限制

根据不同应用，不同访问权限等进行 API 接口速率限制和 API 接口数据大小限制

零信任安全架构

对所有 API 接口内、外部访问者进行可信验证

提供完整的访问控制日志

实时记录所有 API 接口访问的日志，并实时对接日志平台或 SIEM 分析平台

API Bot 及 DDoS 攻击

暴力破解

策略自动化构建，无须人工干预，对 AJAX / JSON 登陆表单进行学习与防护

Bot 攻击

通过验证码挑战，Web 端 JavaScript 主动挑战，移动 App SDK 等来防御 Bot 攻击

DDoS 攻击

通过 TPS 限速来缓解基于 API 的 DDoS 攻击，通过 Behavioral DDoS 防御手段对 API 请求进行机器学习分析，更加高效的防御基于 API 的 DDoS 攻击

功能特点

◆ 现代架构平台设计

云科容翼应用交付控制器推出虚拟化架构，基于 Kubernetes，允许企业在同一台容翼设备中开启多个云科应用交付租户，以配合拓扑需求。多租户软件版本无需相同，多租户的部署、升级、修复过程(重啟)可分别独立进行，且内部配置、数据、管理访问和流量走向均独立存在。

◆ 自动化快速部署组件

容翼系列平台设计有全自动化平台，通过简单强大的声明式接口，可帮助减少人工操作的步骤，快速载入、支持整体配置和部署云科应用服务，将部署时间从几周缩短至几个小时。

◆ SSL 高速卸载

针对企业至关重要的关键数据，容翼平台系列可提供相比前代产品 2 倍性能的 SSL 卸载能力，支持前向加密扩展、增强的 ECC 椭圆曲线算法以及 3-7 层全栈安全防护。通过卸载成本高昂的 SSL 处理进程，加快密钥交换和批量加密速度，加速 SSL/TLS 应用。

提供保護關鍵數據所需的 SSL 容量–包括將 Galois Counter Mode（GCM）、Elliptical curve cryptography（ECC）、Camellia和Rivest Shamir Adleman（RSA）處理加強卸載至硬體–實現前向保密的擴展能力。

◆ FPGA 协助提升 CPU 性能

采用市场广泛使用的现场可编程门阵列（FPGA），通过与云科操作系统以及平台层紧密结合，协助提升 CPU 资源利用，提供前所未有的出色性能及更高的可扩展性。

◆ 支持灵活的迁移扩展

通过云科迁移工具，企业可将已有业务由旧版本云科应用交付软件（机箱或虚拟版本）平滑无摩擦地迁移至容翼平台系列新设备中。该工具支持图形化界面，可迁移所有 4-7 层配置，并支持跨平台迁移（机箱版本和不同平台的虚拟版本之间）。支持迁移后协助企业验证内存占用情况、集群状态和配置对象计数的指标，简化迁移流程，缩短迁移时间，最大程度降低对现存业务影响，有助于提高迁移状态的可视化并减少运行时问题。

◆ 可视化界面操作

建立在 Web 上的图形界面为企业提供了更直观的操作方式，通过图形界面可完成绝大多数配置管理操作，以及对当前云科应用交付软件性能的人工监测。

◆ 定制化的可编程控制器

为发挥云和软件定义架构的优势并按需扩展应用服务，云科为企业用户提供细粒度的流量观察和控制，可编程控制器允许用户轻松自定义代码、实时快速响应代码错误和安全漏洞，并支持新协议，可轻松集成到编排系统中。支持扩展到 JavaScript，降低了部署成本，并加快了部署速度。

◆ 風扇模組更換概述

　　平台中的風扇有助於維持整個機箱內的氣流，並在設備通電時持續運轉。隨著時間的推移，風扇可能會磨損，因此需要更換風扇模組。對於配備可拆卸風扇模組的平台，您可以在日常維護過程中或風扇發生故障時更換風扇模組。

r10000 / r12000 r系列電源線選項與要求：

製造零件號	描述	規格	評級／備註
YK-UPG-CBL-C15TOC14	C15 to C14, Universal Power Cord 适用于以下国家： 这是一款通用电源线，可在任何国家使用。	BLUE GRN/YEL BROWN	250 Volts - 10 Amp

价值体现

◆ 优秀的性能参数

最高 200K 的 TPS SSL (RSA 2k) 和压缩卸载，支持高达 190Gbps 的 4 层/7 层吞吐量，通过增加 SSL FPGA，对ECC 算法进行硬件加速，实现高达 140K TPS (ECDHE-ECDSA P-256)和110K TPS (ECDHE P-256-RSA 2k) 的行业领先的加密性能。

◆ 更低的总体拥有成本（TCO）

将应用和安全服务卸载至高性能的云科应用交付设备，优化网络架构，提升服务器工作效率，减少总体拥有成本和基础架构开销。

◆ 高效灵活的部署方式

企业无需搭建纯软件基础设施，可直接利用和实现 CI/CD 工具集、声明式 API 和基于遥测进行实施。依托"优先设计 API"架构，云科将为企业提供一个完全自动化的系统，提供企业所需的敏捷性和可靠性。

效率特性包括 80 Plus 白金認證電源供應器、前面板觸控式 LCD 管理、遠程啟動與多重啟動支持，以及 USB 支持

◆ 较低的操作难度

声明式 API 大大降低了操作难度，更有利于降低企业技术人员知识储备要求，减轻技术部门工作压力。同时能够减少操作步骤，从而减小重复操作引起误操作的风险。

技术参数

功能	详细描述
主要負載均衡功能	
伺服器负载均衡	完善的第四/七层交换功能，支持可定制的基于应用层的健康检查方式，支持基于 IP 地址、Cookie 等信息的会话保持，并可根据特定信息定制会话保持方式。具备关联应用的健康检查功能，确保关联应用的正常状态。具备跨端口业务的会话保持功能，能够对同一地址，不同端口的业务使用同一组会话保持, 以及關聯應用的健康檢查與應用連接狀態管理
多链路负载均衡 (AWAF/LTM 包括外發負載均衡，附加 DNS 授權可實現入站負載均衡）	可同时支持多条链路的智能选路功能，即：支持 Inbound/Outbound 双向多链路负载均衡，支持多路径链路健康检查方式，支持动态探测优选或静态地址列表匹配等丰富算法，Inbound 支持 DNS 智能解析，根据链路状态，解析域名，Outbound 实现多条运营商链路负载分担，监控链路状态，实现流量在多条链路上自动迁移。 可配置HTTP/2監控以监控伺服器池的HTTP/2服務健康狀態
全局负载均衡 (附加 DNS 授權）	支持基于轮询、全局可用性、应用可用性、拓扑结构、带宽、往返时间（RTT）和动态比例等多种算法的全局负载均衡（GSLB）。包括支持 DNS 安全和全局站点负载均衡功能的智能 DNS 服务。
源进源出负载均衡	网络 IP 重叠的情况下，根据数据源接口不同，不需要指定路由的情况下完成数据返回
防火墙负载均衡 (附加 AFM 授權）	支持三明治结构，要求能够实现异构防火墙多活工作及负载均衡
系统冗余	支持 Active-Active 及 Active-Standby 冗余方式；提供专用的硬件串口级心跳线和网络级冗余判断方式；提供连接会话的镜像功能，实现无缝故障切换；支持多台设备的 N+M 集群方式。
可编程流量管理	管理界面提供基于 TCL 编程语言自定义的流量控制方法，可通过自编程方式实现灵活的流量处理手段。支持负载均衡、DNS 处理、用户认证、NAT、路由转发、会话保持等功能的可编程控制。
API 接口	支持 Rest API 模式完成对设备的操作和查询（包含但不限如下：账户/密码、接口、路由、软件升级、特征库升级、免密登录、配置文件），并提供对接支持服务确保对接工作完成
私有云	与市场主流的私有云解决方案深度结合，集成 vmware SDDC, openstack,华为 Fusion Sphere,H3C VCF, AzureStack，可在云管平台中管理，编排，与监控。
基于 Node.js 环境的可编程控制	设备自带支持 Node.js 环境的可编程控制功能，支持 Javascript 语法。
虚拟化	支持虚拟负载均衡系统，虚拟数量不低于 36 个；虚拟负载均衡器分配独立的硬件资源，资源分配的单位可以是吞吐量或新建能力、并发能力。
服务器负载均衡算法	可支持最小连接数、轮询、比例等负载均衡算法。

服务器优先级组	同一种服务的服务器，设置不同的优先级，高优先级组低于负载要求数量时，自动实现低优先级组的服务器自动加入到负载中，共同提供服务
会话保持	实配基于源目的地址、基于 Cookie、Destination和Host的会话保持。
服务器健康检查	1. 支持 ICMP、TCP、TCP 半连接、UDP、HTTP、HTTPS、FTP、SNMP、WMI、MSSQL、DNS、NTP 等多种主动式服务器健康检查方法； 2. 支持被动式的健康检查方法。即：通过实时监控往返于客户端与服务器端的访问数据，一旦发现往返数据中包含应用访问失败等信息时，可及时将用户请求重新定向到另外的服务器，同时将该服务器定义为不可工作的状态； 3. 支持基于模仿用户实际访问的复杂检查方法。即：可通过设置，模拟一个用户从登录，访问应用，退出等流程准确校验一个用户应用交易的整个过程
多路连接复用	将一个用户的多个请求或者多个用户的请求合成一个连接发送到服务器，减小应用服务器的压力，提升用户响应速度
内存 Cache	利用内存来缓存用户频繁访问的 WEB 静态内容，从而减小应用服务器的压力，提升用户响应速度
NAT 技术	支持 NAT 和 PAT 技术，支持单个 IP 连接不同目的地址使用不同的NAT IP
链路聚合	支持将多条链路带宽进行捆绑，支持 LACP 协议
IPv6 支持	支持 IPv6/v4 双栈 要将云科设置为 IPv4 到 IPv6 网关，您需要创建一个由代表 IPv6 节点的成员组成的负载均衡池。同时，还需创建一个虚拟服务器，将流量负载均衡到这些池成员。
DNS 功能(附加 DNS 授權）	
全球地址库	设备自带全球地址库，提供 IP 地址的洲、国家、城市、运营商和组织等信息的查询。可实现基于用户位置信息的负载均衡，请提供配置界面截图
DNS 服务器	支持作为独立的 DNS Server 部署，支持 A, AAAA, CNAME, DNAME,HINFO, MX, NS, TXT, SOA, SRV 等记录类型
Secondary DNS	支持作为 Secondary DNS，从 Master DNS 复制 Zone 信息，并相应客户端查询，有效保护后台 DNS 服务器。
安全功能	
DOS/DDOS 攻击防护	支持防护以下应用层 DDoS 攻击： HTTP GET Flood 攻击防护： 云科 AWAF 集成了先进的拒绝服务（DoS）防护机制，您可以通过多种方式进行配置，有效缓解 GET Flood 攻击。 SSL 重协商攻击防护： 云科 AWAF 能够利用自身防护能力和脚本语言，有效抵御大规模协同发起的 SSL 重协商攻击。 Slowloris 攻击防护：

	与 UDP Flood 或类似攻击不同，慢速 HTTP 攻击不需要大量僵尸网络，使 DDoS 攻击更易于实施。这类攻击对仅监控第 2/3 层的防火墙来说极具挑战性，增加了防护难度。为有效防御此类攻击，建议使用云科 AWAF，其内置了针对慢速 HTTP 攻击的专门防护机制。 慢速 HTTP Post 攻击防护： 云科 AWAF 默认包含对 Slow POST 等慢速事务攻击的防护。根据实际攻击和环境情况，您只需调整相关防护参数，并通过日志文件检查防护机制是否正常工作。
系统监控告警	支持监控设备系统资源的实时状况，必须包括 CPU、内存、接口带宽、日志容量、策略数、会话数等对象
远程管理 IP 限制	可以对远程管理设备的 IP 地址进行限制。
HTTPS, SSH 登录	可以通过 HTTPS、SSH 方式登录管理
SNMP v3 支持	支持 SNMP v3 管理协议，提供设备和日后版本升级后的 MIB 库可对设备（包含但不限如下：接口、路由、账户、HA、CPU、内存、存储空间、温度）进行查询和操作。支持 2 台以上 SNMP 平台管理
网络防火墙 (附加 AFM 授權)	支持通过许可扩展网络防火墙功能，实现流量过滤。支持入侵防护系统（IPS）功能，可对多种应用层协议进行合规性检查，并基于特征库进行攻击检测。包括支持网络连接活动的访问控制和日志记录的网络防火墙功能。
远程访问管理功能 (附加 APM 授權)	远程访问管理功能，提供SSL VPN、应用代理、终端安全和单点登录。
管理功能	
日志管理	支持标准 RSyslog 日志格式；支持通过 RSyslog、SNMP Trap 方式将系统日志、告警日志转发到指定 2 台以上 Syslog 设备日志收集
大数据引擎	通过实时高速日志引擎对接大数据分析平台，实现业务数据的可视化，从而提供用户/网络体验监控，用户行为分析，应用性能管理等能力。
抓包工具	系统自身提供实时抓包工具，可以对通过自身设备的数据包进行抓包分析，生成的抓包文件支持 Sniffer 或 Wireshark 等分析工具
其他	
基于专用设备的单一操作系统平台	云科 AWAF 已对基础主机操作系统进行了修改，并针对该基础操作系统的所有已报告漏洞进行了响应。使用 microservices platform layer 的设备均采用该操作系统，所有软件版本均运行在此基础操作系统上。
SSL 连接与会话镜像	高可用性（HA）包含设备能够在设备服务集群（DSC）配置中，将连接和持久性信息镜像到另一台设备，以防止故障转移期间服务中断。

	这使得主动流量组与设备组中的镜像对等体之间可以进行镜像。 启用虚拟服务器的连接镜像后，将相关虚拟地址设为主动浮动流量组成员，该流量组即可将其连接镜像到另一台设备上的对应待命流量组。 也可将云科 AWAF 配置为将 SSL 会话数据镜像到对等设备成员。
HTTP/2 支持	云科 AWAF 引入了 HTTP/2 完整代理模式下的 Web 加速配置文件支持。 带有 HTTP/2 配置文件的虚拟服务器，会以完整代理架构处理连接，代表客户端发起请求。
HTTP content 修改	REWRITE::payload。查询或操作 REWRITE 载荷（内容）信息。通过此指令，可检索内容、查询内容大小或替换特定内容。 本地流量策略匹配动作。插入/移除：可将 HTTP 头插入或移除于请求、响应、HTTP 代理连接、HTTP 代理请求或 HTTP 代理响应中。
自动维护页面（Sorry Page）含图片	当虚拟服务器资源（资源池或资源池成员）不可用时，云科 AWAF 可响应维护页面。 当云科 AWAF 收到对无可用资源（如资源池标记为关闭且无可用成员）的虚拟服务器请求时，可设置 iRule 向客户端发送 HTTP 响应（如维护页面）。
IP 地理定位资料	云科 AWAF 使用地理定位软件来识别客户端或 Web 应用用户的地理位置。默认 IP 地理位置数据库可提供 IPv4 地址的洲、国家、省/州、ISP 与组织级别信息，IPv6 地址则提供洲与国家级别信息。
Auto Last Hop 设置	**Auto Last Hop** 允许云科 AWAF 追踪进站连接的来源 MAC 地址，并将来自资源池的回传流量送回来源 MAC 地址，不受路由表限制。 跨多个网络对象（如互联网连接）配置 Auto Last Hop 时： 在 Tunnel/VLAN 组/VLAN/SNAT/NAT/虚拟服务器对象上设

	为 Default 时，继承全局设置；设为非 Default 时，该设置优先于全局设置。
资料链路层探索协议（LLDP）	云科 AWAF 支持资料链路层探索协议（LLDP），这是一种二层产业标准协议（IEEE 802.1AB），允许如云科 AWAF 等网络设备向多厂牌邻近设备广播其身份与能力。
NATs 与 SNATs	SNAT 类似于 NAT，但有以下差异： • NAT：只能将一个原始地址对应到一个转换地址（一对一） • SNAT：可将多个原始地址对应到单一转换地址
应用服务模板	应用服务模板（Application Services Templates）可轻松有效地在云科 AWAF 上以 AS3 部署应用。 通过模板部署的 AS3 应用可用专属网页表单建立与修改，并可查看目前云科 AWAF 上已配置的 AS3 应用。 此扩充套件提供模板化及管理 AS3 应用的工具集。
统计报告与图表	当启用应用可视化与报告（AVR）时，可在分析图表中查看统计数据。 总览画面集中显示所有 HTTP 统计，包括每秒交易数（TPS）、请求与响应吞吐量、服务器延迟（网络状况）、页面加载时间、并发会话数与新会话数。 当分析配置文件收集用户会话（用户上下文）时，AVR 模块会在 HTTP 响应中设置 AVR 用户会话 Cookie，该 Cookie 值为解码识别码，AVR 用来识别应用流量中的唯一用户会话信息。
X-Forwarded-For (XFF) HTTP 头保留原始客户 IP	当云科 AWAF 将进站数据包的源 IP 地址转换为 SNAT 地址时，Web 服务器会将请求视为来自 SNAT 地址，而非原始客户端 IP 地址。如果 Web 服务器需要记录请求的原始客户端 IP 地址，SNAT 地址转换行为可能会导致问题。 为避免记录 SNAT 地址，您可以配置云科 AWAF 在 X-Forwarded-For（XFF）HTTP 头中插入原始客户端 IP 地址，并配置接收请求的 Web 服务器从该头记录客户端 IP 地址，而非 SNAT 地址。
CPU 使用率性能图	云科 AWAF 提供历史 CPU 使用率测量记录，并存于 Round Robin Database (RRD) 数据库，可用于基准分析、容量规划、根因分析或故障排除。 可通过第三方应用程序处理，类似 iHealth 与配置工具仪表板的性能图。
使用 sFlow 监控流量	sFlow 是业界标准的高速交换网络监控技术。可设置云科 AWAF 轮询内部数据来源并将数据样本发送至 sFlow 接收器，进而分析经过云科 AWAF 的流量，协助了解流

	量模式与系统使用情况，用于容量规划、问题排查及安全策略评估。
Hybrid SSL 加速	Hybrid SSL 加速功能允许云科 AWAF 将 SSL 卸载分配于硬件加速器与 CPU 之间。
机器人/僵尸网络防御	保护应用免受机器人及其他恶意工具的自动化攻击。WAF 可主动防御自动化攻击，包括第七层 DoS、网页爬虫及暴力破解。 当客户端首次访问受保护网站时，云科 AWAF 会向浏览器发送 JavaScript 挑战，需支持 JavaScript 的浏览器。若客户端成功通过挑战并回传有效 Cookie，则允许请求进入服务器，否则请求不会送达 Web 服务器，未带 Cookie 的非 HTML 请求将被丢弃并视为机器人。
请求速率限制控制	可依据以下方式限制请求速率： • 客户来源 IP：若客户端经 NAT 设备访问，建议使用 X-Forwarded-For 头取得客户 IP 并据此限速。 • 指纹（Fingerprint）：为每个访问网站的浏览器分配设备 ID，据此限速或封锁客户。
带宽控制器	根据所配置的策略，可用带宽控制器对流量实施速率限制，或标记超出限制的流量。
Web 加速配置文件	通过将 Web 加速配置文件与虚拟服务器关联，云科 AWAF 可实现 HTTP 缓存。HTTP 缓存为系统内存储存的 HTTP 对象集合，后续连接可重用，减少对原始 Web 服务器的流量负载，目标是减少对同一对象的重复请求，并在多数情况下免去完整响应。
自定义 ASM 阻挡页面	可在自定义 ASM 响应中使用 base64 图片于 HTML 代码，或进行 URL 重定向。
高级应用防护	结合机器学习、威胁情报与深度应用专业知识。
主动式机器人防御	保护应用免受机器人及其他恶意工具自动化攻击。
浏览器内数据加密	于应用层加密数据，以防止数据窃取型恶意软件与浏览器内攻击。
行为式 DoS 防御	行为分析与机器学习提供高度准确的第七层 DoS 侦测与缓解。
API 协议安全	部署工具保护 GraphQL、REST/JSON、XML 及 GWT API。
OWASP Top 10 防御	防御当前最严重的安全威胁，包括 OWASP Top 10 所列。
盗用凭证保护	防止利用盗用凭证进行暴力破解攻击。
服务器端请求伪造（SSRF）防护	云科 AWAF 可识别易受 SSRF 攻击的 URI 参数，并可于安全策略中明确定义 URI 参数或使用自动侦测功能。于高

	级保护中将特定主机（IP 或主机名称）加入 SSRF 主机清单，以限制访问。
威胁活动订阅服务	威胁活动（Threat Campaigns）为威胁情报功能，包含由 Threat Labs 持续更新的活动威胁/攻击活动信息。 例如，没有威胁活动更新时，WAF 可能侦测到单一攻击模式，但无法将其与更大规模的威胁活动关联。威胁活动功能提供当前攻击活动的具体信息，几乎可消除误报。 该服务利用元数据与多向威胁情报，协助识别活跃攻击活动的单一行为。
CAPTCHA 语音支持	CAPTCHA 防御机制包含预设语音响应档案，为视障人士提供语音验证，符合 Web 内容无障碍指引 2.0（WCAG2/AA）标准。
事件驱动控制脚本	可建立事件驱动的安全自动化流程： 云科 AWAF 将所有监控日志推送至 Elastic。 Elastic 储存所有数据并利用 Watcher 过滤、判断条件。 Watcher 发现符合条件时，发送 webhook 及数据给 Event Driven Ansible。 Event Driven Ansible 的规则触发并调用 Ansible Automation Platform 内的模板，传递来自 Elastic 的数据。 Ansible Automation Platform 执行 playbook，利用来自 EDA（原自 Elastic）的数据强化云科 AWAF 安全。
即时收集访问日志记录	作为网络安全设备，云科 AWAF 可设置将日志资料与 SNMP Trap 发送至 SIEM 设备，以供即时安全事件分析与合规报告。 可将所有请求的响应日志记录至远端存储，便于线上查阅、操作及历史资料存储。 日志显示格式： 如特定请求的违规与支持 ID 会以粗体显示以强调。 如需图形化报表，请至 Security > Event Logs > Bot Defense > Bot Traffic。
日志检视器	可检视云科 AWAF 上本地储存的应用安全管理器系统日志，包含一般系统事件与用户活动。
导出 WAF 事件日志	可使用 iControl REST 以文字格式导出 WAF 事件日志，便于后续操作与报表产生。
韧性系统管理设施	Always-On Management（AOM）为独立子系统，通过 10/100/1000 以太网管理端口以 SSH 或序列主控台进行

	远程管理。 AOM 允许即使主系统关闭也能管理平台。主系统与 AOM 子系统独立运作，AOM 故障时主系统不受影响且流量不中断。供电时 AOM 始终开启。若主系统无响应，可用 AOM 指令菜单重置主系统。
设备管理	管理端口的 GUI 与 CLI 默认通讯协议。
10G SR 光模块兼容性	支持 SFP+ 10GbE 光纤模块，支持热插拔。 OPT-0016-xx 说明：收发器，SFP+，10GIG，850NM，300M，LC UPC，多模，LIMITING，DDM SKU: UPG-SFP+-R 说明：现场升级，SFP+ 光纤接头（10G-LC/850NM），ROHS 这些为 10GBASE-SR（短距离）以太网收发模块规格： 模块：10GBASE-SR（短距离）10G 以太网收发模块 光波长：850 nm（多模） 接头类型：双工 LC UPC 操作距离/线缆规格： OM1 200MHz-km 62.5μm 多模光纤，最长 33 米 OM2 500MHz-km 50.0μm 多模光纤，最长 82 米 OM3 2000MHz-km 50.0μm 多模光纤，最长 300 米 OM4 最长 550 米 数字诊断功能（DDM）：有
认证支持	**GB 42250-2022** 信息安全技术 网络安全专用产品安全技术要求
用户配置文件(UCS)导入和导出	用户配置文件可以导入和导出，便于在不同平台之间进行迁移。

产品规格

规格	r10900
智能流量处理：	每秒 L7 请求数：6.6M 每秒 L4 连接数：2.5M 每秒 L4 HTTP 请求数：37M 最大 L4 并发连接数：180M 吞吐量：190 Gbps/190 Gbps L4/L7
硬件卸载 SSL/TLS：	SSL：200K TPS (2K 密钥) ECC：140K TPS（ECDSA P-256） 　　　110K TPS (P-256-RSA-2k) 95 Gbps 批量加密
硬件压缩：	90 Gbps
硬件 DDoS：	每秒 SYN cookie 数：160M
软件架构：	64 位 TMOS
租户个数：	最多 36 个
处理器：	系统：12 个 vCPU 租户：36 个 vCPU
内存：	256 GB
硬盘：	2 个 1TB U.2 企业级 SSD
管理端口：	1 个 1000BASE-T 1 个 USB3.0 1 个 串行控制台
100G/40G 光纤端口：	4 个 100G/40G QSFP28/QSFP+ 端口
25G/10G 光纤端口：	16 个 25G/10G SFP28/SFP+ 端口
电源：	2 个 1200 W 100-240 VAC (+/- 10%) 自动切换铂金
功耗：	680W（双电源，48V DC 或 110V AC 输入）
输入电压/热输出：	2325 BTU/小时（双电源，110V 输入） 2290 BTU/小时（双电源，230V 输入）
尺寸：	1.72"（4.37 厘米）高 x 17.4"（44.2 厘米）宽 x 30.6"（77.72 厘米）深 1U 行业标准机架安装式机箱
重量：	36 磅（16.33 千克）（双电源）
操作温度：	0-40℃
操作相对湿度：	5% 到 85%，40°C

Features:

Modern Architecture Platform Design

The Yunke R-series application delivery controller features a virtualized architecture based on Kubernetes, allowing enterprises to launch multiple Yunke application delivery tenants within the same device to meet topological needs. Multi-tenant software versions do not need to be the same, and the deployment, upgrade, and repair processes (reboot) can be carried out independently, with internal configurations, data, management access, and traffic direction all existing separately.

Automated Rapid Deployment Components

The R-series platform is designed with a fully automated platform that through a simple yet powerful declarative interface helps reduce manual operations, quickly load, support overall configuration, and deploy Yunke application services, shortening deployment time from weeks to hours.

High-Speed SSL Offloading

For critically important enterprise data, the R-series platform provides SSL offloading capabilities that are twice as effective compared to previous products, supporting forward encryption extensions, enhanced ECC elliptic curve algorithms, and full-stack security protection from layers 3 to 7. By offloading costly SSL processing, it accelerates key exchange and bulk encryption speeds, speeding up SSL/TLS applications.

Deliver the SSL capacity required to protect critical data—including enhanced offload of Galois Counter Mode (**GCM**), Elliptical curve cryptography (**ECC**), **Camellia**, Rivest Shamir Adleman(**RSA)** processing to hardware—enabling forward secrecy scaling.

FPGA Assistance to Enhance CPU Performance

Utilizing widely adopted Field Programmable Gate Arrays (FPGAs), it works closely with the Yunke operating system and platform layer to enhance CPU resource utilization, providing exceptional performance and higher scalability.

Flexible Migration Expansion

Through Yunke migration tools, enterprises can smoothly and frictionlessly migrate existing operations from older versions of Yunke application delivery software (both chassis and virtual versions) to the new R-series platform devices. The tool supports a graphical interface, migrating all layer 4 to 7 configurations, and supports cross-platform migration. It assists enterprises in verifying memory usage, cluster status, and configuration object counts post-migration, simplifying the process and minimizing impact on existing operations.

Visual Interface Operations

A web-based graphical interface provides enterprises with a more intuitive operation

method, completing most configuration management tasks and enabling manual monitoring of current Yunke application delivery software performance.

Customizable Programmable Controllers

To leverage cloud and software-defined architecture advantages and expand application services on demand, Yunke provides fine-grained traffic observation and control. Programmable controllers allow users to easily customize code, quickly respond to code errors and security vulnerabilities in real-time, and support new protocols, facilitating integration into orchestration systems. It supports extensions to JavaScript, reducing deployment costs and accelerating deployment speed.
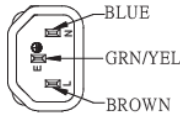
Fan tray replacement overview

The fans in platforms help maintain airflow throughout the chassis and run constantly while the unit is powered on. Over time, the fans can wear out, requiring you to replace the fan tray. For platforms that have a removable fan tray, you can change or replace the fan tray as part of the routine maintenance of the unit, or in the event of a fan failure.

Fan tray

Power cable options and requirements of r10000 / r12000 rSeries:

Manufacturing Part Number	Description	Profile	Rating/ Comments
YK-UPG-CBL-C15TOC14	C15 to C14, Universal Power Cord Applicable to the following country: This is a Universal Power Cord and could be used in any country	BLUE GRN/YEL BROWN	250 Volts - 10 Amp

Value Proposition

- **Excellent Performance Parameters**

  Up to 190 Gbps of layer 4/7 throughput, achieving industry-leading encryption performance of up to 200K TPS (RSA 2k), 140K TPS (ECDHE-ECDSA P-256) and 110K TPS (ECDHE P-256-RSA 2k) through SSL FPGA hardware acceleration and compression offloading.

- **Lower Total Cost of Ownership (TCO)**

  Offloading application and security services onto high-performance Yunke application delivery devices optimizes network architecture, enhances server efficiency, and reduces overall ownership costs and infrastructure expenses.

- **Efficient and Flexible Deployment**

  Enterprises do not need to build pure software infrastructure; they can directly utilize and implement CI/CD toolsets, declarative APIs, and telemetries. With the "priority design API" architecture, Yunke provides a fully automated system that offers the agility and reliability enterprises need.

  Efficiency features include 80 Plus Platinum certified power supplies as well as frontpanel touchscreen LCD management, remote boot and multi-boot support, and USB support.

- **Reduced Operational Difficulty**

  The declarative API significantly lowers operational complexity, making it easier to reduce the knowledge reserve requirements for technical personnel, relieving pressure on technical departments, and minimizing operational steps to reduce the risk of errors caused by repetitive actions.

Technical Parameters

Features	Detail Description
Main Load Balancing Features	
Server Load Balancing	Comprehensive layer 4/7 switching capabilities, supporting customizable application-layer health checks, session persistence based on IP address, cookies, etc., and health checks for associated applications, and application connection state management
Multi-Link Load Balancing (AWAF/LTM including outgoing load balancing, while add-on DNS license for the incoming load balancing)	Supports intelligent routing for multiple links simultaneously, including inbound/outbound bidirectional multi-link load balancing and rich algorithms for path health checking. Can configure HTTP/2 monitors to monitor the health of the HTTP/2 service of your server pools
Global Load Balancing (Add-on DNS license)	Supports global load balancing (GSLB) with various algorithms based on polling, global availability, application availability, topology, bandwidth, RTT, and dynamic ratios. Including Intelligent DNS services that enable DNS security and Global Site Load Balancing functions
Source-In Source-Out Load Balancing	Under network IP overlap, data can be returned without specifying routing, based on different source interfaces.
Network Firewall Load Balancing (Add-on AFM license)	Supports heterogeneous firewall active-active work and load balancing.
System Redundancy	Supports Active-Active and Active-Standby redundancy modes, providing dedicated hardware serial heartbeat lines and network-level redundancy detection. Provides session mirroring functionality to achieve seamless failover; supports N+M clustering of multiple devices.
Programmable Traffic Management	Management interface provides customizable traffic control methods based on TCL programming language.
API Interface	Supports Rest API mode for device operations and queries, including accounts/passwords, interfaces, routing, software upgrades, and configuration files.
Private Cloud Integration	Deep integration with mainstream private cloud solutions, supporting VMware SDDC, OpenStack, Huawei FusionSphere, H3C VCF, Azure Stack.
Programmable Control Based on Node.js Environment	The device comes with built-in programmable control features that support a Node.js environment and JavaScript syntax.
Multi-tenant	Supports multi-tenants with no fewer than 36 tenants; the tenant is allocated with independent hardware resources, and resource allocation can be based on vCPU and Memory.

Server Load Balancing Algorithms	Supports load balancing algorithms such as Round Robin, Least Connections, Ratio;
Server Priority Groups	Servers providing the same service can be assigned different priorities. When the high-priority group falls below the required load, servers from the low-priority group automatically join to share the load and provide service together.
Session Persistence	Supports session persistence based on source IP, cookie, Destination and host.
Server Health Check	1. Supports multiple active health check methods, including ICMP, TCP, TCP half-connection, UDP, HTTP, HTTPS, FTP, SNMP, WMI, MSSQL, DNS, NTP, etc. 2. Supports passive health check methods, monitoring real-time data between clients and servers. If application access failures are detected, user requests can be redirected to another server while marking the faulty server as unavailable. 3. Supports complex check methods that simulate actual user access, allowing for verification of the entire transaction process from login to application access and logout.
Multipath Connection Multiplexing	Combines multiple requests from a single user or multiple users into one connection sent to the server, reducing pressure on application servers and improving user response speed.
Memory Cache	Utilizes memory to cache frequently accessed web static content, reducing pressure on application servers and enhancing user response speed.
NAT Technology	Supports NAT and PAT technologies, allowing a single IP to connect to different destination addresses using different NAT IPs.
Link Aggregation	Supports bundling of multiple link bandwidths and supports the LACP protocol.
IPv6 Support	Supports IPv6/v4 dual stack. To setup Yunke to function as an IPv4-to-IPv6 gateway, you create a load balancing pool consisting of members that represent IPv6 nodes. You also create a virtual server that load balances traffic to those pool members.
DNS Features (Add-on DNS feature)	
Global Address Database	The device comes with a global address database, providing information such as continent, country, city, operator, and organization for IP address queries. It enables load balancing based on user location information.

DNS Server	Supports deployment as an independent DNS server, supporting record types such as A, AAAA, CNAME, DNAME, HINFO, MX, NS, TXT, SOA, and SRV.
Secondary DNS	Supports functioning as a Secondary DNS, copying zone information from the Master DNS and responding to client queries, effectively protecting the backend DNS servers.
Security Features	
Application DDoS Attack Protection	Support protect against below Application DDoS attacks: **Mitigating HTTP GET flood attacks:** Yunke AWAF includes advanced Denial of Service (DoS) protection mechanisms that you can configure in a wide variety of ways to effectively mitigate a GET flood. **SSL Re-negotiation attacks:** Yunke AWAF is able to repel the large and coordinated attack using Yunke AWAF and the scripting language. **Slowloris attacks:** Unlike UDP floods or similar attacks, slow HTTP attacks do not require large numbers of bots, making DDoS attacks easier to execute. This attack is challenging to handle with firewalls that monitor Layers 2/3, which adds to its complexity. To effectively defend against such attacks, utilizing Yunke AWAF, which includes specific protections against Slow HTTP Attacks, is recommended. **Slow HTTP Post:** Yunke AWAF includes protection against slow transaction attacks such as Slow POST, by default. Depending on the attack and environment, you may only need to tune the parameters controlling this protection and ensure that the mechanisms are working by checking the log files.
System Monitoring and Alerts	Supports real-time monitoring of the device's system resources, including CPU, memory, interface bandwidth, log capacity, number of policies, and number of sessions.
Remote Management IP Restriction	Allows restrictions on the IP addresses for remotely managing the device.
HTTPS, SSH Login	Management can be accessed via HTTPS and SSH.
SNMP v3 Support	Supports the SNMP v3 management protocol, providing a MIB library for device queries and operations after device and future version upgrades. Supports management of more than two SNMP platforms.
Network Firewall	Supports extending network firewall functionality through a license, allowing for traffic filtering. Supports IPS functionality for compliance checks on various application

(Add-on AFM license)	layer protocols and attack checks based on a signature database. Including Network firewall functions that support access control and logging on network connection activities.
Remote access management features (Add-on APM license)	Remote access management functions to provide SSLVPN, application proxy, end-point security and single sign on.
Management Functions	
Log Management	Supports standard RSyslog log format; allows forwarding of system logs and alarm logs to more than two designated Syslog devices via RSyslog and SNMP Trap for log collection.
Big Data Engine	Integrates with big data analysis platforms through a real-time high-speed log engine to achieve visualization of business data, providing capabilities for user/network experience monitoring, user behavior analysis, and application performance management.
Packet Capture Tool	Yunke AWAF provides a real-time packet capture tool that can analyze data packets passing through the device. The generated packet capture files are compatible with analysis tools such as Sniffer or Wireshark.
ETC	
Appliance-based platform with a single purpose operating system	Yunke AWAF has been modified the one base host operating system and responds to all reported vulnerabilities for that base operating system. The operating system for the platforms that use a microservices platform layer. All software versions run a base operating system.
SSL Connection and Session mirroring	High availability includes the ability for a device to mirror connection and persistence information to another device in a device service clustering (DSC) configuration, to prevent interruption in service during failover. This enables mirroring between an active traffic group and a mirroring peer in the device group. When you enable connection mirroring on a virtual server, and you then make the relevant virtual address a member of an active floating traffic group, the traffic group can mirror its connections to its corresponding standby traffic group on another device. Can also configure Yunke AWAF to mirror SSL session data to peer device group members.

HTTP/2 Support	Yunke AWAF introduced the support for webacceleration profile in HTTP/2 full proxy mode. A virtual server with an associated HTTP/2 profile processes connections using the full proxy architecture for the purpose of making requests on behalf of clients
HTTP content modification	**REWRITE::payload.** Queries for or manipulates REWRITE payload (content) information. With this command, you can retrieve content, query for content size, or replace a certain amount of content. **Actions for local traffic policy matching.** <u>Insert/Remove</u>: Inserts or Remove an HTTP Header into the request, response, HTTP proxy connect, HTTP proxy request, or HTTP proxy response.
Automatic maintenance page sorry page with images	Yunke AWAF to respond (with a maintenance page) if the virtual server resources (pool or pool members) are unavailable. When Yunke AWAF receives a request for a virtual server that does not have available resources (for example, the pool is marked down with no available pool members) you can configure an iRule to send an HTTP response, such as a maintenance page, to the client.
IP geolocation data	Yunke AWAF uses geolocation software to identify the geographic location of a client or web application user. The default IP geolocation database provides IPv4 addresses at the continent, country, state, ISP, and organization levels, and IPv6 addresses at the continent and country levels.
Auto Last Hop Setting	**Auto Last Hop** is a setting that allows Yunke AWAF to track the source MAC address of incoming connections and return traffic from pools to the source MAC address, regardless of the routing table. **Auto Last Hop configured across multiple network objects (like internet links):** When you configure **Auto Last Hop** with a value of **Default** at the Tunnel/VLAN group/VLAN//SNAT/NAT/virtual server object, it inherits the **Global** setting. When you configure **Auto Last Hop** with a value other than **Default** at the Tunnel/VLAN group/VLAN/SNAT/NAT/Virtual Server object, its setting takes precedence over the **Global** setting.
Link layer discovery protocol	Yunke AWAF supports Link Layer Discovery Protocol (LLDP). LLDP is a Layer 2 industry-standard protocol (IEEE 802.1AB) that enables a network device such as Yunke AWAF to

	advertise its identity and capabilities to multi-vendor neighbor devices on a network
NATs and SNATs	A SNAT is similar to a NAT, except for the differences listed below: **NATs:** Can map only one original address to a translation address. (1-to-1) **SNATs:** Can map multiple original addresses to a single translation address
Application Services Templates	Application Services Templates are an easy and effective way to deploy applications on Yunke AWAF using AS3. AS3 applications deployed through template can be managed using Application Services Templates which auto-generates web forms custom to your templates for creating and modifying applications, and provides visibility into what AS3 applications are configured on Yunke AWAF. The Extension provides a toolset for templating and managing AS3 Applications on Yunke AWAF.
Statistical report and chart	Can examine the statistics in the Analytics charts when Application Visibility and Reporting (AVR) is provisioned. The Overview screen shows all of the HTTP statistics in one place, including averages for transactions per second (TPS), request and response throughput, server latency (Network Condition), page load time, concurrent sessions, and new sessions. When configure the statistics gathering configuration of an Analytics profile to collect user sessions (user context) as one of the collected metrics, the AVR module sets an AVR user session cookie in HTTP responses. The cookie value is a decoded identifier set that the AVR module uses to identify unique user session information in application traffic.
X-Forwarded-For (XFF) HTTP header to preserve the original client IP address	When Yunke AWAF translates the source IP address of the incoming packet to the SNAT address, the web server sees the request as originating from the SNAT address, not the original client IP address. If the web servers are required to log the original client IP address for requests, the SNAT address translation behavior may become problematic. To avoid logging the SNAT address, you can configure the Yunke AWAF to insert the original client IP address in an **X-Forwarded-For** (XFF) HTTP header and configure the

	web server that is receiving the request to log the client IP address from the header instead of the SNAT address.
CPU Utilization performance graphs	Yunke AWAF provides details of historical measurements of CPU utilisation readily available as records in the Round Robin Database (RRD) database maintained by Yunke AWAF, it can be used for the purposes of e. g. baselining, capacity planning, root cause analysis or troubleshooting The processing can be performed via third-party applications in a manner e. g. similar to performance graphs available in iHealth and the Configuration Utility dashboard.
Monitoring Traffic with sFlow	*sFlow* is an industry-standard technology for monitoring high-speed switched networks. You can configure Yunke AWAF to poll internal data sources and send data samples to an sFlow receiver. You can then use the collected data to analyze the traffic that traverses Yunke AWAF. This analysis can help you understand traffic patterns and system usage for capacity planning and charge back, troubleshoot network and application issues, and evaluate the effectiveness of your security policies.
Hybrid SSL acceleration	The hybrid SSL acceleration feature enables Yunke AWAF to split SSL offload between the hardware accelerator and the CPU.
Robots/Botnets Prevention	Protects apps from automated attacks by bots and other malicious tools. WAF can proactively defend your applications against automated attacks by bots. The bot defense method identifies Layer 7 DoS attacks, web scraping, and brute force attacks and prevents them from starting. When clients access a protected site for the first time, Yunke AWAF sends a JavaScript challenge to the browser. Therefore, if you plan to use this feature, it is important that clients use browsers that allow JavaScript. If the client successfully evaluates the challenge and resends the request with a valid cookie, your policy allows the client request to reach the server. Requests that do not answer the challenge are not sent to the web server. Requests sent to non-HTML URLs without the cookie are dropped and considered to be bots.
Request Rate Limit control	**Limit the request rate via:** **Client Source IP address:** If the clients come by using a NAT device before Yunke AWAF better use the X-Forwarded-For header to get the client ip address and rate limit by it.

	Fingerprint: Client fingerprinting refers to a method in which a device ID is assigned to each browser that visits a website, to rate limit and block clients.
Bandwidth Controller	Depending on the type of policy you configure, you can use bandwidth controllers to apply specified rate enforcement to traffic flows or mark traffic that exceeds limits.
Web Acceleration profile	HTTP caching on Yunke AWAF by associating a Web Acceleration profile with a virtual server. An HTTP cache is a collection of HTTP objects stored in the system's memory that subsequent connections can reuse to reduce traffic load on the origin web servers. The goal of caching is to reduce the need to send frequent requests for the same object and eliminate the need to send full responses in many cases.
Custom ASM block page	For custom ASM Response with images, they can use a base64 image in their html code or do a Redirect URL.
Advanced application protection	Combines machine learning, threat intelligence, and deep application expertise
Proactive bot defense	Protects apps from automated attacks by bots and other malicious tools
In-browser data encryption	Encrypts data at the app layer to protect against data-extracting malware and man-in-the-browser attacks
Behavioral DoS	Behavioral analytics and machine learning provide highly accurate L7 DoS detection and mitigation
API protocol security	Deploys tools to secure GraphQL REST/JSON, XML, and GWT APIs
Defenses for the OWASP Top 10	Defends critical apps from today's biggest security concerns, including those listed in the OWASP Top 10
Stolen credential protection	Protects against brute-force attacks that use stolen credentials
Server-side request forgery (SSRF) protection	Yunke AWAF can Identify parameters of data type URI that are subjected to SSRF attack and explicitly define the URI parameters in your security policy or use the Auto-detect Parameter feature to automatically detect URI parameters in your application. From these parameters, identify the specific hosts to which you want disallow access, and, in your security policy under Advanced Protection, for SSRF Protection, add these specific hosts (IP addresses or host names) to the SSRF Hosts list.
Threat Campaign subscription service	Threat Campaigns is a threat intelligence feature which includes frequent update feeds containing contextual information about active threat/attack campaigns currently being observed by Threat Labs that WAF can provide protection against. As an example, without threat campaign

	updates WAF may detect an attack pattern in a web application form parameter, but it cannot correlate the singular attack incident as part of a more extensive and sophisticated threat campaign. Threat Campaigns' contextual information is very specific to current attack campaigns, allowing false positives to be virtually non-existent. Threat Campaigns service users Metadata and Multi-Vector Threat Intelligence to help identify the individual actions of an active attach campaign.
CAPTCHA audio support	CAPTCHA mitigation mechanism includes a default response audio file for audio reading of the CAPTCHA challenge to provide accessibility to the visually impaired. This feature conforms to the Web Content Accessibility Guidelines 2.0, Level AA (WCAG2/AA) standards.
Event-based control scripting	Creates a well-oiled setup with the code and the flows setup we can now create proactive event based security: • Yunke AWAF is pushing all the monitoring logs to Elastic. • Elastic is taking all that data and storing it while utilizing a watcher with its filters and criteria, • The Watcher finds something that matches its criteria and sends the webhook with payload to Event Driven Ansible. • Event Driven Ansible's Rulebook triggers and calls a template within Ansible Automation Platform and sends along the payload given to it from Elastic. • Ansible Automation Platforms Template executes a playbook to secure Yunke AWAF using the payload given to it from EDA (originally from Elastic).
Real time collection of access log records	As a network security device, Yunke AWAF can be configured to send log data and SNMP traps to a SIEM device to help provide real-time analysis of security events and generate reports for compliance purposes. Can Log responses for all requests to remote storage for further online log viewing, manipulation and historical logging data storage. **Logging display formats:** Like the violations for a specific request and support ID number appear in bold text for emphasis.

	To view a graphical version of the report, go to **Security** > **Event Logs** > **Bot Defense** > **Bot Traffic**.
Log viewer for log records	Can view locally stored system logs for the Application Security Manager on Yunke AWAF. These are the logs that include general system events and user activity.
Export WAF event logs	Can export WAF event logs using iControl REST in text format for further manipulation and report generation
Resilient system management facilities	Always-On Management (AOM) is a separate subsystem that provides lights-out management for Yunke AWAF using the 10/100/1000 Ethernet management port over secure shell (SSH) or the serial console. AOM enables you to manage the platforms using SSH (most platforms) or the serial console, even if the host subsystem is turned off. The host subsystem and the AOM subsystem operate independently. If AOM is reset or fails, the host subsystem continues to operate and there is no interruption to load-balanced traffic. AOM is always turned on when power is supplied to the platform. If the host subsystem stops responding, you can use the AOM Command Menu to reset it.
Device Management	Default protocol for GUI and CLI access to the management port
10G SR Transceiver compatible	**Fiber SFP+ modules** These fiber 10GbE SFP+ transceiver modules are supported in the hardware platforms, and support for hot swap of optical transceiver modules. **OPT-0016-xx** Description: Transceiver, SFP+, 10GIG, 850NM, 300M, LC UPC, MMF, LIMITING, DDM **SKU: UPG-SFP+-R** Description: Field Upgrade, SFP+ Fiber Connector (10G-LC/850NM), ROHS These are specifications for the 10GBASE-SR (Short Range) ethernet transceiver module. **Specifications:** Module: 10GBASE-SR (Short Range) 10G ethernet transceiver module Optical wavelength: 850 nm (multi-mode) Connector type: Duplex LC UPC Operating distance/cable specifications:

	- 33 meters maximum for type OM1 200MHz-km 62.5µm MMF - 82 meters maximum for type OM2 500MHz-km 50.0µm MMF - 300 meters maximum for type OM3 2000MHz-km 50.0µm MMF - 550 meters maximum for type OM4 Digital Diagnostic Function (DDM): Yes
Certification Support	**GB 42250-2022** Information security technology—Security technical requirements for specialized cybersecurity products
Import and Export of Configuration File	Configuration file (User Configuration Set) can be imported and exported for easy migration

SPECIFICATIONS	r10900
Intelligent Traffic Processing:	L7 requests per second: 6.6M L4 connections per second: 2.5M L4 HTTP requests per second: 37M Maximum L4 concurrent connections: 180M Throughput: 190 Gbps/190 Gbps L4/L7
Hardware Offload SSL/TLS:	200K TPS (RSA 2k keys) 140K TPS (ECDHE-ECDSA P-256) 110K TPS (ECDHE P-256-RSA 2k) 95 Gbps bulk encryption
Hardware Compression:	90 Gbps
Hardware DDoS Protection:	160M SYN Cookies per second
Software Architecture:	64-bit TMOS 64-bit F5OS
Multi-Tenancy:	Up to 36
Processor:	12 vCPU's Reserved for F5OS, and 36 vCPU's Available for Tenancy.
Memory:	256 GB DDR
Hard Drive:	2x 1TB U.2 Enterprise-class SSD (RAID 1 Mirrored)
Management Ports:	1x 1000BASE-T, 1x USB 3.0, 1x serial console
100/40 Gigabit Fiber Ports:	4 x 100G/40G QSFP28/QSFP+ ports
25/10 Gigabit Fiber Ports:	16 x 25G/10G SFP28/SFP+ ports
Power Supply:	2 x 1200 W 100-240 VAC (+/- 10%) AUTO Switching Platinum, Dual DC PSU Optional
Typical Consumption:	680W (dual power supply, 48V DC or 110V AC input)
Input Voltage / Typical Heat generated:	Dual Power supply 110 VAC input: 2325 BTU/hour 230 VAC input: 2290 BTU/hour
Dimensions:	H: 1.72 inches (4.37 cm) x W: 17.1 inches (44.20 cm) x D: 30.6 inches (77.72 cm) (per unit) 1U industry standard rack-mount chassis
Weight:	36.0 pounds (16.33 kg) with two power supply units (PSUs) (per unit)
Operating Temperature:	32 to 104°F (0 to 40°C)
Operational Relative Humidity:	5% to 85% (40 C) non-condensing