

专业负载均衡|云应用交付平台

软件定义智慧金融

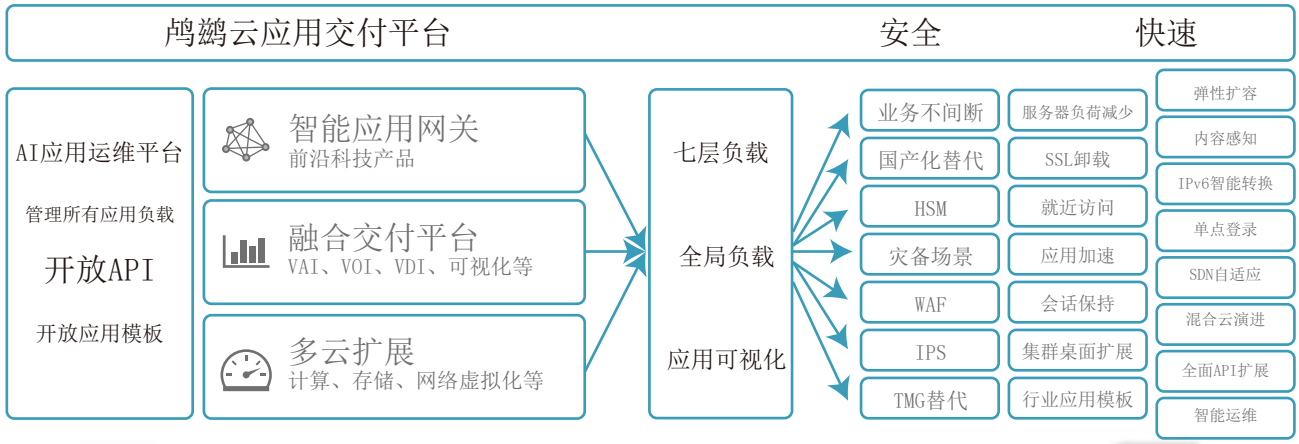
金融信创系列产品手册

鸿鹟科技（深圳）有限公司
www.LucciTech.com

公司介绍

产品能力-软件定义智慧应用

鸿鹄科技作为国家高新企业、国家信创成员企业，其核心团队拥有十余年的专业交付和安全产品经验，一直以来秉承IT服务精神。历经十余年的技术积累和研发公关，推出了媲美国际一流技术水平的国产自主可控产品——鸿鹄应用网关，并以专业的应用网关为基础，构建了可以帮助企业构建现代化应用架构的解决方案——鸿鹄云应用交付平台，帮助应用更安全更快速更智能化为目标，帮助应用实现多云多架构的安全管理、负载调度和自动化运维，比肩国外 F5 和 Citrix 等同类领军厂商，赋能国产化乃至全球应用产业。





产品优势

比肩国际一流技术、国产自主可控

发展优势

完全自主研发的第三代产品（应用负载+全局负载+联合认证+统一应用质量监控报警+零信任业务和智能化运维要求等），技术上是 F5 国产化替代的最佳选择，同时符合零信任安全理念，细粒度用户的边界安全和优化。

成本优势

国外F5的高端市场，成本比F5优势特别明显，并有能力为金融客户正在中高端产品需求中，提供创新的稳定技

性能优势

传统国内基于开源产品修改的大同类型产品，单设备稳定性能只有10G以内，作为国家信创成员企业的鸿鹄产品单设备可以到达最高100G的稳定吞吐性能，进入国际顶尖行列。功能上我们提供大量的健康检查算法，可以帮助用户平滑过度之前 F5 使用过程中的依赖，并提供配置迁移办法。

理念优势

国内大厂在此细分领域，无法形成生产力工具，我们最终有机会形成互补，在新基建中对应用安全和技术融合以及人工智能要求的提升，包括 5G、边缘计算、自动化运维、开发一致性保证等领域会有极大的帮助，并获得众多国内外比赛优胜和业界

平台优势

基于应用的监控和自动化运维方面，目前只有国外厂商可以提供高性能昂贵的解决方案，鸿鹄产品优势是可以全局的视角看应用整体安全，提供统一应用运维平台，帮助用户分角色分管理，为自动化安全提供关键数据支持提供国产化云应用交付平台（结合桌面云集群）的扩展方案（支持传统应用向国产化 PC（龙芯：鲲鹏：飞腾：海光：兆芯等+麒麟：统信等） 的转移和简化运维方向的应用交付管理），提供除了后端应用交付方案外+前端应用交付的整

产品概述

LucciTech提供灵活的交付方式，适合于数据中心，云计算平台和虚拟环境的业务系统的可用性,可靠性和安全性的云应用交付系列产品、服务和前沿解决方案。立志于让国产化应用更快、更安全、更智能的专业负载均衡国产化第一品牌。

LCA系列是立足于专业的服务器负载均衡、全局负载均衡、SSL卸载和加速、Web应用防火墙、安全单点登录和应用加速功能的交付网络产品，为用户带来高性价比的应用交付整体解决方案.更支持Openflow的SDN(软件可定义网络)等前沿科技，让业务系统和网络完美融合。

LCD系列是针对国产化适配针对容器和数据中台等的专业加固安全应用网关产品。

LCV/LCC/LCD系列秉承LCA的强大优势,提供广泛的支持：私有云平台（VMware、Microsoft Hyper-V、Citrix Xen、Oracle Virtualbox、各类的基于KVM的私有云平台等）、公有云服务商（亚马逊AWS、Microsoft Azure、腾讯云、阿里云、华为云等）和中台容器环境，配合云应用开发商共同提供高附加值的保障方案，以成为混合云的使能者为目标。

Luccitech智能多云应用交付平台解决方案在深层次的解决了传统应用中心的体验、安全性、工作效率等满足了业务的智能需求,无论是专业金融场景还是智慧政务、智慧城市、智慧法务、智慧旅游、智慧园区、智慧校园、智慧图书馆、金融第三方互联等业务方式,还是其他行业的智慧应用，一样可以用软件重新定义，我们称之为软件定义智慧应用（SDSA）。

鸿鹟现有优势

完全的自主知识产权，解决信创替代问题而不是替换

近年来，对信息化系统安全的要求，让我们行业在负载均衡领域做了“国产化替换”的尝试，但实际上因为在这个细分领域原有使用的国际厂商F5产品远超传统国内产品一代以上。更换后，导致其支撑的应用质量有所下降，并在新场景部分无法得以保障。所以我们需要以”信创替代”为目标，这样才能够让应用能力和国际市场同步，并在智慧城市等场景中领先其他行业。

鸿鹟目前可以提供的产品是第三代产品（第一代产品立足应用分发，第二代产品关注应用安全加速优化，第三代关注多云分布式架构保障 ,我们提供专业应用级别的负载

2021中国信创500强

2021年中国信创500强！|版权|曙光_网易订阅 (163.com)



2021年度中国信创TOP500（401-500）

RK	企业	得	护	得	得
401	奥威	78.40	84.10	71.47	77.99
402	熵基科技	78.40	84.00	71.47	77.96
403	时代亿信	78.40	84.10	71.26	77.92
404	快立方科技	78.30	84.00	71.38	77.89
405	青藤云安全	78.20	83.80	71.42	77.81
406	盈高科技	78.20	84.10	71.13	77.81
407	大道云行	78.20	84.00	71.14	77.78
408	鸿鹟科技	78.20	84.00	71.12	77.77
409	源杰半导体	78.10	84.10	71.10	77.77

国家高新技术企业



深圳市信息技术应用创新联盟理事单位



信息技术应用创新工作委员会会员单位



LCA/LCV/LCC/LCD系列

LCA/LCV/LCC/LCD系列是应用交付专业产品，提供基于IP网络上的四层和七层优化应用交付，从而确保业务的持续可用性、高性能、快速响应时间及全面的安全性。

LCA/LCV/LCC/LCD系列能够将ADC服务、计算资源及虚拟化服务转变为集成应用交付虚拟化基础架构。该产品扩展了我们面向虚拟数据中心和云计算环境的ADC解决方案，能够提供更高的业务灵敏性、应用故障恢复能力和运营简便性，同时显著降低成本。

LCA/LCV/LCC/LCD系列对业务提供了三种类型的安全保障:一、业务的可持续和弹性扩容保障,二、业务的安全认证、加固和防御保障，三、稳定可靠的应用构架支撑，三种形态的交付方式

硬件平台：基于ASIC硬件架构,单台设备最高提供100G的七层吞吐，透过N+M集群，支持1500G以上的七层集群吞吐。

私有云平台：支持所有主流的虚拟机平台，虚拟机版本最高支持10G的七层吞吐。

公有云平台:支持Microsft Azure、Amazon AWS、VMWare vCloudAir、阿里云、华为云、金蝶苍穹云等，最高

主要功能

支持10G的七层吞吐。
四层和七层服务器负载均衡
基于状态的热备切换HA
全局负载GSLB
服务器和应用的健康监测
IP和七层的会话保持
七层内容切换
SSL加速和卸载
数据缓存加速
数据压缩加速
WAF安全模块支持
SDN自适应
SSO多重安全认证单点登录
Azure等公有云VPN安全对接
多云智能安全应用管理平台（金融级云交付管理）对接
国产化云应用交付平台（软件定义智慧应用）对接
私有云平台支持
（VMware/Hyper-V/VBox/Kvm/Xen/OpenStack等）
公有云平台支持
（Azure/AWS/vCloud Air/阿里云/华为云等）
大数据应用支持（Splunk等）
N+1集群部署F5、Cisco ACE等的第三方ADC配置迁移
丰富的应用优化方案和配置模板
支持和Exchange的集成,可以提供单点登陆和论证页面,实现

产品优势

基于ASIC硬件的SSL卸载和加速,最高支持每秒17万的SSL新建连接(2048bit证书)。

全面支持基于四层和七层的服务器负载,提供可自定义的服务器健康状态检查。

全面支持IPv6,适合IPv6和IPv4的混合网络部署实施,并支持高效的Http/2协议。

多重安全认证单点登录,提供客户端访问业务系统的单点登录管理,并支持多种论证模式,包括LDAP,RADIUS,RSA-SecureID,Certificate,Radius,LDAP和SAML2.0。

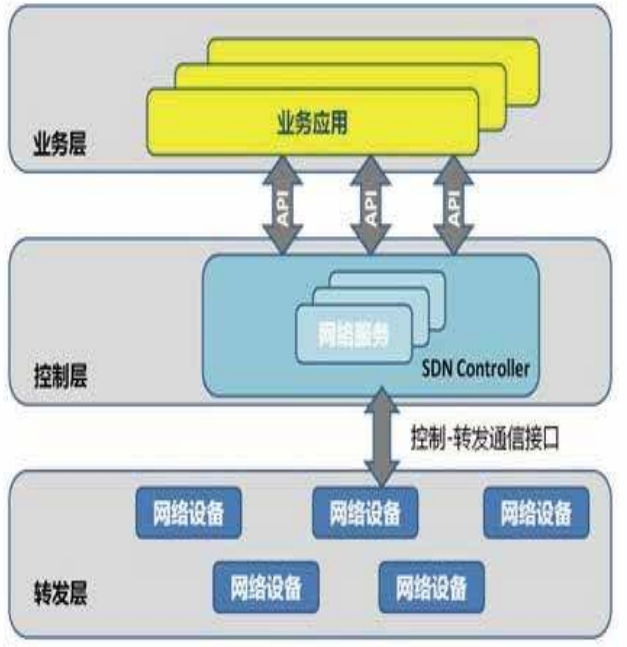
N+M集群,支持并行的集群部署,可以弹性的扩展能。

VMWare无缝集成,实现虚拟环境的动态资源分配。

支持Azure VPN无缝对接,实现混合云安全交付。

WAF安全模块支持全球特征库和自定义动态规则。

支持SDN(软件可定义网络),基于SDN控制器对网络全局视图的把握,能够开展更合理的负载均衡,制定更



云应用交付平台（软件定义智慧应用）扩展方案的支持。

F5、Cisco ACE等的第三方ADC配置迁移,帮助传统用户向新业务构架安全演进。

支持丰富的传统应用/互联网/大数据优化方案和模板，包含Microsoft、IBM、Oracle、SAP、Splunk等应用,还有金融、医疗、教育等行业配置方案和模板。

灵活的网络部署方式

支持单臂，路由和三角传输的部署方式。

支持端口聚合,可采用802.3ad或Active-Backup协议。

支持VLAN Trunking(802.1Q)。

支持IPv6,并可以部署在IPv6和IPv4的混合网络。

支持HA冗余模式部署，采用Active-Standby的冗余部署方式，支持四层连接和七层会话镜像。

支持N+1集群方式部署。

提供虚拟机版本，支持在虚拟环境下部署，对于VMWare的虚拟网络，提供VMWarevCenter的无缝集成，可以动态分配资源。

支持传统网络/私有云/公有云计算平台的部署。

支持IPSec点对点VPN，适合于对端是VPN的网络环境，支持自有设备以及和Azure等国内外公有云的无缝对接。

支持SDN自适应，适合于SDN网络环境。

全局负载均衡

提供多个数据中心的业务系统的高可用性和容灾，同时适合于私有云和公有云的业务系统迁移切换。

内嵌算法包括：轮询,权重轮询,固定权重，业务系统的负荷，根据用户访问位置的经纬度，根据用户访问位置离数据中心的就近性。

根据数据中心站点是否为公有站点和私有站点设定访问策略。

自定义站点不可用时的恢复模式:即手动恢复或自动恢复.

支持全局负载均衡的会话保持。

支持和DNS的无缝集成。

内置IP(IPv6和IPv4)的位置数据库，并定时更新。

支持外置部署方式:即将设备部署在数据中心外，统一提供高可用性和容灾。

支持自定义地区，自定义IP地址和地区的映射。

支持集群部署：即在每个数据中心均部署设备提供全局负载均衡，对外作为一台逻辑的设备。

集群部署模式下，支持设备之间的配置自动同步，支持设备的统一内核升级管理。



四层/七层服务器负载均衡

确保业务系统的99.999%的可用性.通过可定义的服务器健康状态检查,确保业务系统的稳定和快速响应。

四层负载均衡的内嵌算法包括：轮询，权重轮询，最小连接，权重最小连接，固定权重，权重响应时间，源IP哈希，代理模式和SDN算法。

七层会话保持的内嵌算法包括：源IP地址，HTTP包头，HTTP包头和源IP地址混合，服务器Cookie，服务器Cookie和源IP地址混合，设备Cookie，设备Cookie和源IP地址混合，URL哈希，Cookie和源IP哈希，任意HTTP Header和Query，SSL SessionID，UDP SIP。

支持基于IP、基于Cookie、基于主机名或基于任意字段的保持、原路返回机制支持插入Cookie、改写Cookie、X-Forward-For或任意字段和内容的改写。HTTP/HTTPS1.0/1.1,HTTP/2,RemoteTerminal,SIP,FTP,DNS等各类应用协议充分支持e.

支持URL重定向、HTTP请求过滤、自定义HTTP错误页面的服务器健康检查支持多种协议包括ICMP,HTTP,HTTPS,TCP,Mail,NTTP,FTP,Telnet,POP3,IMAP,DNS服务器健康检查支持十六进制数据报文的请求/响应模式,可自定义数据报文内容

服务器支持虚拟节点的嵌套，可以为一个业务系统指定多个虚拟子节点，每个虚拟子节点可以定义不同的内容策略和健康检查等。

服务器健康检查支持服务器的嵌套，可以自定义服务器的状态阀值数量；可自定义关键主机，任何关键主机的状态为宕机，则虚拟服务的状态也是宕机。

支持业务系统的ACL访问控制。

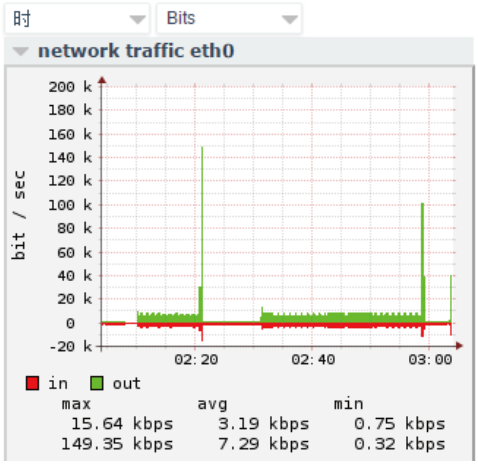
支持HTTP到HTTPS的七层会话迁移。

提供强大的七层内容引擎，可以根据HTTP包头内容对数据报文重定向，比如：去除服务器敏感信息，将请求定向到服务器根目录，将HTTP请求重写并定向到HTTPS,强制关闭连接，保证Cookie的安全性。

七层内容引擎支持编程，可使用正则表达式对HTTP数据包头进行解析匹配。

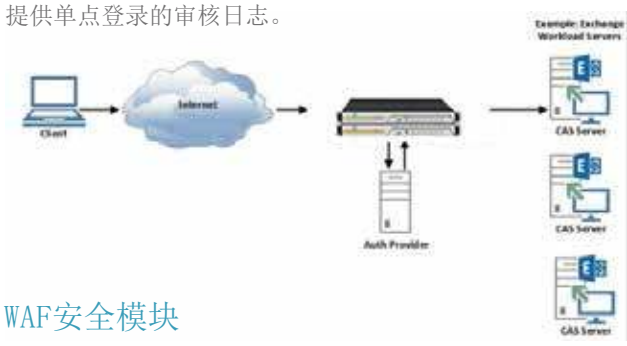
支持在服务器安装客户端，可自定义服务器或业务系统的负荷进行负载均衡。

支持虚拟服务器温暖上线,温暖下线



多云联合认证

支持多重安全认证单点登录，可以和LDAP，Radius等论证服务器无缝集成，对客户端的身份进行验证,从而为多个虚拟服务提供单点登录功能，内置单点登录页面，并提供单点登录的审核日志。

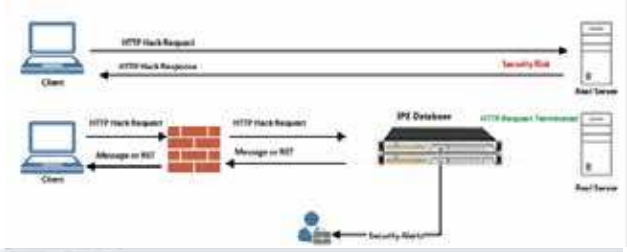


WAF安全模块

对业务系统提供WAF(Web应用防火墙)的安全防护。

支持IPS,确保应用服务免受网络攻击，TCP SYN-Flood攻击和DoS/DDos攻击。

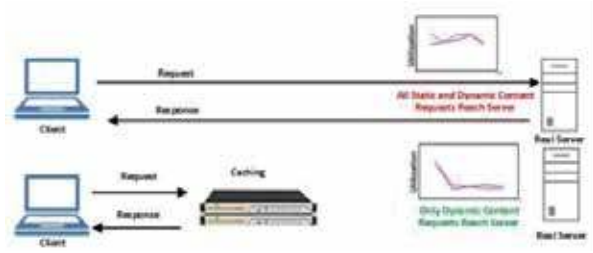
支持全球特征库和自定义动态规则。





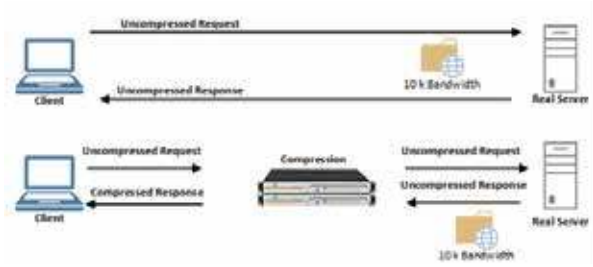
缓冲加速和数据压缩加速

TCP应用加速,支持TCP连接复用



支持动态压缩，可以对业务系统的数据传输提供工业标准的压缩处理，最大压缩比例100:1。

支持高性能的内存缓存。



SSL/TLS卸载和加速套件（金融/行业版）

基于ASIC硬件SSL/TLS加速,提供业界领先的性能.

支持SSL3.0,TLS1.0,TLS1.1/TLS1.2/TLS1.3的协议

支持1024位,2048位和4096位的SSL证书

支持设备与服务器之间的数据进行SSL加密证书管理、可自定义算法集组合.

支持SSL/TLS桥接模式

虚拟服务可以共享证书

支持外置的OCSP服务器对客户端证书的论证

支持生成证书请求文件和私钥,支持自签证书

支持导入证书和密钥

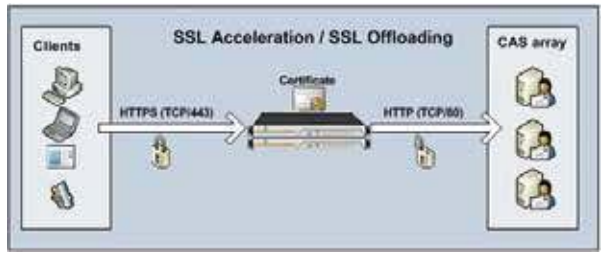
支持扩展证书、证书备份与恢复、通配型证书

支持和外置HSM(硬件安全模块)无缝集成

支持客户端证书验证及双向证书验证

支持证书链、导入根证书和中间证书

支持基于证书的访问控制



SDN(软件可定义网络)自适应

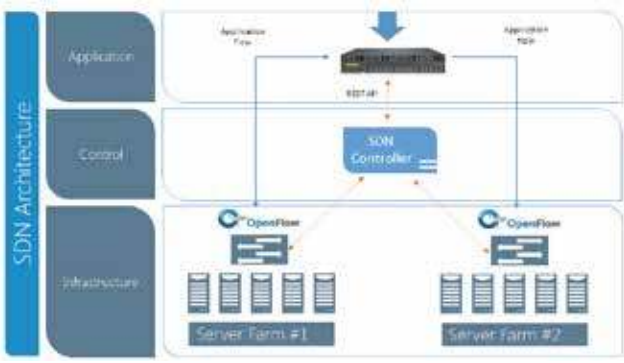
支持Openflow和SDN无缝集成

通过和SDN的集成，应用交付的智能化、扩展性、业务感知能力将获得极大改善，为云计算环境下的客户提供 按需、快速、敏捷的应用网络服务。

支持和SDN控制器的无缝集成。

根据从SDN控制器获取的二层网络信息如网络延时等，动态调整业务系统的负载均衡调度。

实时生成虚拟服务到设备的网络路径和拓扑。



管理和日志功能

基于浏览器的管理界面(WUI)

SSH和HTTPS(WUI)远程管理

基于向导的配置

基于Web的实时帮助

高度灵活的虚拟节点配置和管理

节点性能和可用性的实时统计信息

透明的真实节点管理

支持RJ45的Console管理

支持远程日志服务器syslogd

策略备份和恢复

支持Connection Draining

在线或离线LucciTech™固件更新

支持命令行

支持SNMP

内置数据包截取诊断工具

系统日志、Email自动发送、支持Syslog日志服务器

CPU的实时报表

流量管理套件扩展

支持云负载集群管理平台套件扩展提供对所有设备实例的集中管理，包括物理设备，部署在公有云或私有云的设备实例。

智能多云集群管理平台(运营商/金融版)

智能多云集群管理平台，能对业务控制、监测和诊断中应用的关键指标，提高运营效率，集中管理和降低资源闲赋时间，专业应用交付网关框架包括中央管控平台,视窗化的服务器负载设备集群管理（支持LCA/LCV/LCC等系列产品）和服务运营监控平台提供主动的监测和诊断，减少并消除在传统应用架构问题的影响管理提供基于Web的管理界面。

提供基于Web的管理界面。

提供CLI的命令行管理界面。

支持SNMPv2和SNMPv3以及私有MIB库，方便和第三方系统集成。

提供完整的SOAP API

支持不同访问权限的用户管理

提供Syslog的远程日志

支持不同事务等级的邮件通知

实时性能和数据统计报表

配置备份和恢复

提供用户操作的审核日志

管理用户支持LDAP和Radius论证

传统应用/互联网/大数据优化方案和模板

Microsoft

---Microsoft Dynamics

---Direct Access 2012 R2

---Microsoft Exchange 2010/2013/2016

---Microsoft Lync 2010/2013/

---Microsoft IIS等

---ADFS v2/v3/v4

---Remote Desktop Services

---Print Server

---Microsoft SharePoint

---Microsoft Skype for Business

---Microsoft Dynamics AX等

容器支持

当前，越来越多的行业企业开始建设容器化平台部分银行甚至已经试水将部分业务部署至容器化平台在容器平台体系中,以Kubernetes这样的容器为例容器平台的网络以及服务的最终对外暴露一直以来都是一块较大的挑战，如何选择符合企业的网络模型，采取何种方式将服务对外暴露都是容器化平台建设的考虑重点。K8S原生的各种服务发布方案，存在各有各的不足，有的是不支持更加复杂的7层访问策略，有的是需要一定的外部解决方案辅助，有的是无法进行有效的链接控制等等。Ingress恰恰是用来解决上述问题的，Ingress是k8s中的一种资源对象其主要负责定义更加复杂的7层应用路由策略.

例如基于Hostname，URI策略分配，SSL终结、会话保持等配置Ingress本身并不用来具体的proxy流量，因此需要有一个具体的proxy来执行这样的工作.

例如 nginx，haproxytraefik，AWS ALB，linkerd等无论ingress支持哪些高级L7策略，最终需要具体的proxy来实现，也就是说proxy的实现决定了最终L7策略功能实现.

目前鸿鹄的容器负载均衡有两种方式

--- Kubernetes内置的Ingress或Nodeport，Nodeport对外发布都是高位端口比如30169，容易被防火墙屏蔽，缺乏会话保持SSL卸载、HTTP/2等功能支持，而且性能不佳。

---开源的NGINX/HAProxy提供的Ingress Controller，通常只针对HTTP协议，并且NGINX在同步配置时会导致服务中断，另外负载均衡功能较弱，性能不佳。

我们产品对K8S负载解决如下功能

--- 支持所有四层到七层的K8S应用对外发布

---K8S服务自动发现，POD自动发现，POD自动同步

--- 支持会话保持

--- HTTP/2支持

--- 高性能的SSL卸载，支持TLS 1.3

--- 支持高级安全功能：WAF和身份认证

--- 支持流量管理：对每个VS的带宽，并发连接，新建并发进和HTTP RPS行限制，支持缓存和压缩

--- 支持高级路由：通过内容策略，实现用户访问对POD访问的优化

--- 本身作为流量探针，提供IPFIX格式的流数据给第三方netflow分析平台，提供网络和应用的实时统计数据，提供网络和应用的可视化

--- 解决开发人员和网络人员在K8S环境下的接口问题

--- 可同时提供针对K8S应用和传统数据中心应用的负载均衡

目前的容器应用场景中，大部分的时间应用无需对外提供服务或没有实际用户访问，应用需要提供服务或用户访问时间段比较集中，此情况下应用服务器长期开启但未提供服务明显会造成资源浪费。

为解决此场景中的问题，鸿鹄负载均衡可以配合制定。通过快速启停集群中各应用服务，来实现大部分时间应用停止以及快速拉起的功能，并达到对数据中心节能的效果，为行业新一代数据中心的节能减排和双碳目标做出贡献。

可视化内容策略引擎Vrules

鸿鹄科技的vRules同时兼顾替代和配置简单的特点，具备对应的成熟能力以及对新场景支持的潜力

能力如下:

--- 支持对HTTP所有包头、URL、内容、方法的操作

--- 支持正则表达式

--- 支持策略的逻辑嵌套

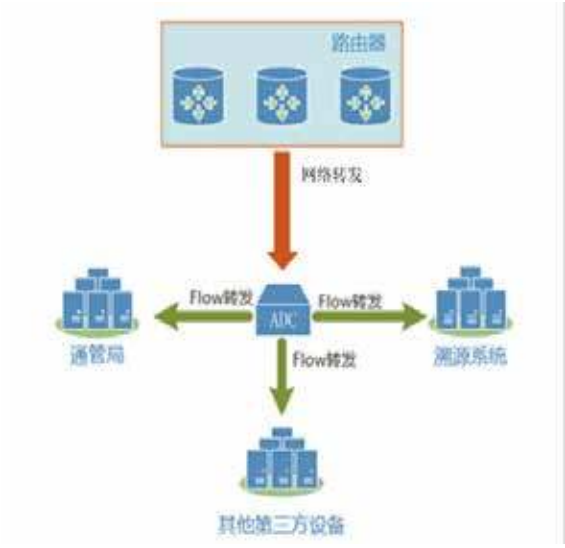
--- 对部分特殊需求进行单独处理，比如根据用户组定向到不同的服务器，将SSL 证书、协议等信息写入HTTP自定义包头等



--- 方向：下行对应when HTTP_REQUEST
--- HTTP包头和内容：
对应if { [HTTP::host] equals "domain.com" }
--- 重写：对应HTTP:
header replace "Host" "newdomain.com"

实时探针

实时流量分析能力，对网络溯源非常重要，尤其是在关键的应用保障场景和分布式架构的复杂场景中。
NetFlow是网络流量统计的标准协议，与DPI技术相比，基于Flow的检测技术处理速度更快、配置部署更方便快捷、维护成本更低，因此被广泛应用在网络流量分析、DDoS攻击检测攻击溯源等多个方向。
NetFlow是网络流量统计的标准协议，与DPI技术相比，基于Flow的检测技术处理速度更快、配置部署更方便快捷、维护成本更低，因此被广泛应用在网络流量分析、DDoS攻击检测攻击溯源等多个方向。



鸬鹚的实时业务质量监控（实时探针功能）Netflow
--- 负载针对发布的业务系统提供流量探针功能
--- 以IPFIX格式提取流量，并实时发送到第三方Netflow/IPFIX的采集和分析系统
--- 提取IP地址、端口、协议、吞吐、时间、网络延时/抖动和2-7层协议

	协议	说明
Layer 2	ARP	
	MAC	
	VLAN标记	
	端口索引	
Layer 3/4	NPM	IP地址、端口协议 Bytes、packets flow TCP标记包括时间戳和信号 网络性能参数包括RTT、SRT TCP重传、jitter TCP扩展遥测包括TTL、SYN包大小 默认TCP窗口
	NPM扩展	
Layer 7	DHCP	
	DNS	
	HTTP	
	Email Application ID	
	Samba	
	VoIP/SIP	
	SSL/TLS	
	MS SQL Server	
	PostgreSQL	
	MySQL	

方案特定

--- 无需安装代理
--- 负载在提供应用交付发布功能的同时，提供所有经过负载（业务系统的流量）数据报文的实时提取和发送
--- 支持IPv6
--- 采用IPFIX协议，只占实际吞吐的1/250，和原始数据包抓取相比，性能优越
--- 支持和所有基于Netflow/IPFIX的第三方采集器无缝集成

解决如下问题

--- 跟踪业务系统的用户体验、定位性能瓶颈和网络延时分析　　---定位最消耗带宽的用户/IP/应用
---跟踪业务系统和用户的网络性能参数(RTT、SRT、jitter)了解历史状况为未来规划提供数据基础

场景化方案

云原生架构能力提升与容器应用

随着云原生逐渐从社区走向行业机构，适应行业场景要求的云原生架构逐步形成。如果把过去行业集中式架构（中央大脑）的统一控制视为坐标轴的“左端”，完全开源式的分布式云原生作为坐标轴的“右端”，那么在云原生架构下，行业机构所需要的技术架构就是在左右两端之间寻求一个平衡点，做到既拥有行业的安全性、强一致性、可靠性，又具备适当的容错性、可扩展性和快速响应的能力。以“强局部自治、弱中心控制”为原则，云原生架构把那些需要综合多方因素判断的复杂逻辑交由全局系统（中央大脑）完成，发挥其汇聚全局要素和高效计算的优势，而大量的日常简单判断和执行动作则可放在局部系统内闭环完成，提升容错性和敏捷应变能力，进而提高整个系统的稳健性。



通过以上这张图可以看出云原生虽然让我们的业务系统更加容器并快速上线，但复杂架构尤其是分布式场景中，对云原生的分布式架构连接、业务安全保障，自动化运维的要求也会越来越高，针对上图的五种状态，鸿鹄提供不同的能力对应各种状态的要求，更好的帮助用户达到对应的要求。
设计态（高质量准备方案，分析设计，架构治理、设计原则、中台框架）
研发态（稳定性保障、研发洞察、架构治理方案）
运行态（微服务支持、动态配置、存储连接与安全加固、软负载增强、消息网络、应用服务保障<容器、虚拟机、联邦集群、大数据安全等
运维态（监控、诊断、线上管控、测试准备、架构感知、蓝绿部署、资金安全、云管）
容灾态（同城、异地、单元化、灾备工具配套）
举几个关键例子，解释一下专业负载均衡尤其是鸿鹄第三代负载均衡对业务的重要性。

多活+单元化架构（主要技术全局负载）

行业企业在建设多活的数据中心时，两个数据中心之间的物理距离可能会导致跨数据中心的交易服务访问延时过大甚至出现超时。在这种情况下，计算跟存储之间的跨城通讯是不满足业务需求的。如果采用单元化架构，计算跟存储基本封闭在一个逻辑数据中心（Logical Data Center，LDC）里面完成，可以根据需求控制交易服务的流量，及时调节访问压力。

在跨城、跨数据中心的多活应用部署情况下，业务访问根据路由策略进入LDC的某个单元内绝大多数业务服务交互可以在一个单元内就近调用访问完成，避免出现大量的跨数据中心交互访问交易的延迟性问题也可以得到很好的控制。

此外，有些业务仍会存在跨单元、跨数据中心、跨城通信情况业务访问也将基于最小化数据跨域的服务调用策略进行交互访问可以最大化地解决跨城数据服务通讯的时滞问题。

故障隔离和自愈（主要技术：多云业务质量监控与智能化运维准备）

行业企业对系统稳定性要求极高，物理服务器故障对业务产生的影响很大。如果物理服务器规模较小，很容易导致部分核心系统的应用服务分布过于集中,一旦服务器宕机势必直接影响业务的正常开展后果十分严重。

基于云原生架构，行业企业可根据业务特点和应用等级去制定策略确保所有的调度不会集中在个别的物理服务器上即把负载“打散”。

此外，在云原生架构下，行业企业可以随时监控和探测系统的健康状态配置中心能自动发现物理服务器上的容器问题并及时报警和自动处置。

精细化处理（主要技术：极致业务健康检查与性能）

业务场景增多、业务变化加快、业务模块之间关联度日趋复杂会造成系统运行中出现突发事件。有一些平常流量非常少的业务场景在业务量突然增大后，会导致周边相关系统受到冲击。

这种情况很可能导致部分服务器请求遭到积压，情况严重时会出现“雪崩”效应，从而使业务陷于瘫痪。此外，金融交易中经常遇到的热点账户问题，也很容易导致全行的“交易抖动”。如果可以识别甚至预判不同业务所导致的热点并做到有效隔离，那么偶发情况就不会影响到其他业务场景。

应用发布能力（主要技术：应用负载与开放的API）

高效灵活的应用发布变更是云原生的重要能力对于行业企业来说，每次发布必须做到审批有据可查，数据安全无损，过程可实时监控，应急可回退复原。云原生可以将安全生产理念融入应用发布的全流程管理。

在架构层面上提供“可灰度，可回滚（应急）可监控、可审计”的能力。

云原生加固

在新冠肺炎疫情冲击下，许多行业企业快速构建线上服务、云上营业厅、音视频服务、场景行业服务、为个人和企业客户等提供了便捷和全时在线的数字行业服务。这类数字化行业服务对相关应用的敏捷性、弹性和韧性提出了更高要求，行业企业需要在短时间内上线新应用，快速伸缩资源以满足突增的访问量，确保系统持续正常运转。

这种敏捷应变的需求是单靠传统IT架构难以实现的。云原生架构便成为这些机构加快系统迭代升级、跟上行业数字化转型步伐的利器。从本质上看，云原生包括规范用云的架构模式、技术标准管理理念、应用实施的工具和方法，其目标是让行业企业摆脱对基础设施的大量投入，将精力集中到业务创新和产品研发上来。

借助云原生理念和工具，企业可以像使用水电气等公共设施那样，使产品设计、开发调试、部署测试、资源消费等业务能够即插即用地对接到任何一朵云上，从而在节省资源的同时实现灵活的部署运行，并获得强大的算力支持和安全保障所以在这样的场景背景下，鸿鹄必然将对业务的帮助越来越大。

智能多云的新场景保障

解决新场景，容器与云原生应用交付困难

多云分发与策略同步

多云分发的核心技术是全局负载均衡技术，适用于多个位于不同物理位置的站点，比如分布在不同地区的多个数据中心。

当主站点无法访问时，备用站点将自动提供服务，从而保证对外提供服务的稳定性和冗余。另外，全局负载均衡还可以保证客户端访问最快的数据中心或最近的数据中心，保证客户访问的快速。

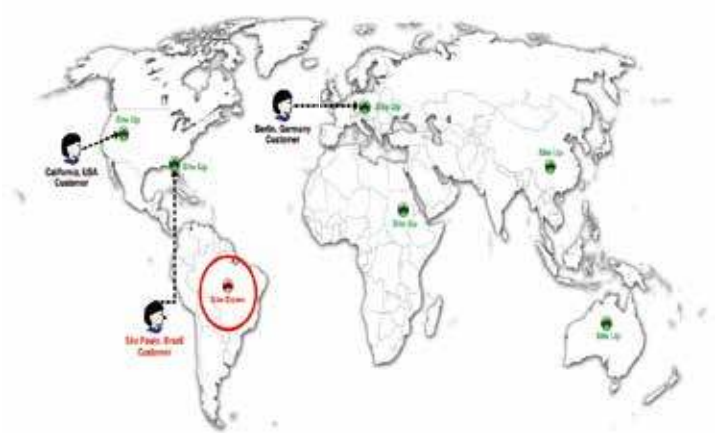
全局负载均衡是网域应用交付设备个一个功能模块，全局负载均衡提供高级的健康检查机制，健康检查可以针对应用，也可以针对数据中心，这样确保当应用或数据中心不可用时，对用户而言是透明的，确保用户一直访问健康的应用或数据中心。

全局负载均衡提供丰富的调度算法，包括轮询、加权轮询、基于固定权重的备份和站点恢复、基于真实节点的负荷的智能调度基于用户和数据中心物理位置的就近性算法、基于经纬度的就近访问等。

全局负载均衡的部署方式非常灵活，提供分布式的Active-Active的HA配置，多组HA冗余设备可以安全、自动的同步信息。
支持和现有的DNS集成，只需要做简单的配置，就可以和现有的DNS集成。
全局负载均衡支持集群，通过集群，可以对应用、服务器、数据中心进行统一的健康检查。

GSLB涵盖如下功能

功能	说明
健康检查	
标准算法	ICMP TCP HTTP(S) 服务器负载集成 集群健康检查
健康阀值	支持自定义健康检查时间间隔，次数和超时
调度算法	
标准算法	轮询(权重) 主备 地区就近性 经纬度就近性 业务系统性
会话保持	支持会话保持，来自相同客户端的DNS请求 分发到同一个数据中心
安全	
DNSSEC	DNSSEC协议支持
IP黑名单	内置全球IP黑名单，并自动更新
IP白名单	自定义IP白名单
IP地区库	全局IP和地区映射数据库
其他	
SOA	支持自定义SOA
数据中心内外的路由策略	支持私有站点和公有站点区分路由
站点故障的切合模式	支持自动和手工切合
网络部署	
网络	支持IPv4（A）和IPv6（AAAA） 支持CNAME、MX、TXT 支持多网口监听DNS请求
集群	支持各个数据中心的集群部署 集群配置和性能数据自动同步
管理	
管理界面	支持WEB和Console WEB管理界面支持中英文
API	提供JSON和XML(Web服务)API接口



特有的集群同步协议

在每个数据中心部署是最可靠的部署方式，因为任何一个数据中心的全局负载设备出现问题，都不会影响整个全局负载的工作集群部署需要各个设备的配置自动同步和性能数据自动同步，全局负载特有的集群同步协议确保在高延时的异构网络环境中同步的可靠性，目前这个能力是现有开源解决方案中最难做到的点。

全局负载和服务器负载无缝集成

全局负载需要判断每个数据中心的状态，全局负载通过和服务器负载集成，也就是说通过服务器负载去收集和判断数据中心业务系统的状态，这个是最可靠的方式。

安全性

DNS的安全是网络安全的重要组成部分。全局负载提供如下两个安全功能：第一是DNSSEC，这个是DNS安全扩展协议在每个DNS上部署证书确保DNS请求和转发的合法性，避免DNS劫持等安全漏洞。

第二是全球IP黑名单，在这个黑名单上的IP地址如果访问全局负载均衡设备的域名，是被阻断的。全局负载内置全局IP黑名单并定时更新（最少每3天更新一次）

多云认证与零信任

鸿鹋产品作为所有信息系统的统一入口，以反向代理的方式将所有信息系统隐藏在后面，避免了信息系统直接被攻击的可能性

鸿鹋产品成为整个系统架构的第一道防线，也是被攻击的第一个目标，因此安全认证网关自身的安全性显得尤为重要。鸿鹋产品的自身安全性包括三个方面：

数据传输安全

所有客户端和 鸿鹋产品之间的数据传输，全部采用 SSL/TLS 加密，加密协议默认采用 TLS 1.2，安全证书采用 2048 bit并提供 SSL/TLS 加密的弹性机制：支持 TLS 1.3 4096bit 证书自定义加密套件，HSTS 标签，客户端数字证书透传。

鸿鹋产品和第三方认证系统的数据传输支持加密，比如和AD 认证支持 StartTLS或 LDAPS 加密协议，和 SAML 身份提供 方如AD FS 认证支持 m-TLS 双向数字证书验证

鸿鹋产品和信息系统之间，考虑到加密对信息系统的性能影响默认采用明文传输；但是支持从 Luccitech多云应用网关和信息系统之间的数据传输加密。

鸿鹋产品和信息系统之间的安全认证支持 Kerberos。当用户部署越来越多不同的服务器和应用时，单点登录问题就显得突出。专业云应用管理平台提供单点登录需求可以提供统一的安全论证。

统一登录窗口安全

支持人机识别，避免机器人攻击。
支持登录失败次数/账户锁定以及超时自动登出。
支持设定公网/私网登录方式。
登录窗口的 URL 自动生成一次性 Token 字符串避免被盗刷。
登录窗口的用户名/密码均采用私有算法加密。

系统安全

采用 DPDK 开发，并非基于标准 Linux 内核，在提升性能的同时，其精简的架构也最大程度保证系统本身的安全性。总之，和传统的零信任相比，作为第三代产品我们支持多个节点（也就是多云）的登陆，支持不同业务和不同认证系统提升应用安全和加固自身安全。通过这样的能力，我们可以更好的为复杂场景的大安全提供更有力的保障。

自动化运维与AIOps准备

解决以业务自愈与自御为目标的，自动化运维纬度低与难度大的落地困局。
今天，行业企业的业务场景与过去相比发生了很大变化，比较典型的就是很多业务都搬到了线上，大家去柜台办理业务的次数应该是越来越少，这就要求行业企业的应用系统需要保持7*24在线，因为随时随地都会有用户通过线上的方式办理行业业务。除了保持应用系统7*24在线外，行业企业也越来越关注应用系统的客户体验，在以线上服务为主的场景下与客户最终打交道的不再是柜台员工，而是APP，一次不好的APP使用体验，可能就会使行业企业失去一个客户的评价因此如何及时的发现应用异常并且进行快速响应和修复也成为了关键。

这些行业业务的发展和变化就促使行业企业的运维方式也在相应改变，从原始的手工运维到使用工具来逐步提高效率，再到自动化运维，人工成本大幅降低。但是自动化运维也只解决了过程自动化，什么时候需要做什么操作仍然需要运维人员来做判断和决策。这时候AIOps智能运维这个理念就应运而生了，借助人工智能来实现判断和决策的自动化

要实现AIOps需要有三个关键要素，第一是大数据，必须要有足够丰富的数据来给AI做判断和决策依据。第二是算法和机器学习，不断训练AI去做出更加精准的判断。而自动化则是这一切的基础，当AI做出决策而无法自动执行的话这一切也就没有了意义。

鸬鹚新一代产品作为应用交付过程中最重要的一环，可以协助用户向AIOps迈进。
一方面，作应用交付设备，所有的应用访问数据鸬鹚都可以提供，无需另外探针的方式，直接启用Netflow模块，在任何环境下为AI提供充足的数据。

另一方面，我们具备丰富的API接口以及配合行业龙头生态系统实现行业属性的定制，当AIOps根据鸬鹚产品提供的数据作出智能判断，需要变更时，鸬鹚的应用交付设备可以接收AIOps平台的指令并自动执行变更操作，实现无人干预例如当AIOps平台发现某一数据中心承载压力过大，可以通过API向鸬鹚的智能DNS下发指令，将部分流量分流至其它数据中心。

总之，在行业繁复应用多，对多重安全的要求，在行业的各种场景中，现有我们的底层及时能力，支持各类应用的安全保障和多云可扩展，实现更低投入,更有效的统一管理、统一安全认证、统一运维扩展，提供业务模版简化业务部署,保证多云安全融合架构保证业务不间断，通过多种加速技术提升业务响应，解耦业务应用模块,七层应用安全保障解决大部分通用安全问题,多云版本适配,多服务器多云架构保证高并发能力,结合行业实现各种算法让应用更加智能更加快速和安全，高性能，让业务更加简单却又更加安全、快速、智能化，并解决用户需求，未来可以满足行业客户的各种需求的收费模式，为应用更好形成行业标准和提供生产力工具。

LCA/LCV/LCC/LCD系列产品规格表行业版

型号	LCA318	LCA1519	LCA6020	LCA8020	LCAX020
吞吐量(Gbps)	3.6	15	60	80	100
千兆以太网端口数	4	8	2	2	2
光纤端口(SFP+)	无	4*10G	4*10G+4*25G	4*10G+4*40G	4*10G+4*100G
最大TLS(SSL)TPS（2K密钥）	1500	16,000	75,000	75,000	170,000
最大TLS(SSL)TPS（1K密钥）	1500	12,000	75,000	75,000	170,000
最大并发连接数（pps）	8,600,000	35,000,000	200,000,000	250,000,000	300,000,000
Web应用防火墙包(WAF)	无	支持	支持	支持	支持
SSO安全验证	支持	支持	支持	支持	支持
全局负载	支持	支持	支持	支持	支持
SDN支持	无	支持	支持	支持	支持
数据压缩加速	支持	支持	支持	支持	支持
内容缓冲加速	支持	支持	支持	支持	支持
设备外观	2U	2U	4U	3U	4U
冗余电源	不支持	支持	支持	支持	支持
平均无故障时间MTBF	4年	5年	8年	6年	8年

云计算版（含国产化云应用安全API网关）

产品型号	LCV/LCC18	LCV/LCC188	LCV/LCC488	LCV/LCC888	LCD188	LCD488
吞吐量(Gbps)	0.2	2	5	10	2	5
TLS(SSL)TPS（2K密钥）	200	1,000	10000	12000	1,000	5000
TLS(SSL)TPS（1K密钥）	200	1000	10000	12000	1000	5000
最大并发连接数（pps）	300,000	300,000	3,000,000	3,000,000	-	-
Web应用防火墙包(WAF)	无	无	支持	支持	支持	支持
SSO联合验证	支持	支持	支持	支持	支持	支持
全局负载	支持	支持	支持	支持	支持	支持
SDN支持	无	无	支持	支持	无	无
数据压缩加速	支持	支持	支持	支持	支持	支持
内容缓冲加速	支持	支持	支持	支持	支持	支持
云支持	LCC型号对应公有云版本 （MicrosoftAzure、AmazonAWS、阿里云、华为云等）、 LCV型号对应私有云版本 （VMware、Hyper-V、XenFull、XenPara、Oracle Virtualbox、KVM、OpenStack等各类私有云平台） LCD型号对应数据中台容器版本（以上产品已经陆续完成国产化芯片、操作系统、数据库等适配中）					

增值模块

模块编号	模块名称	配置	模块编号	模块名称	配置
LCA-SDN	SDN自适应模块	内置	LCA-WAF	WAF模块	内置，可定制策略
LCA-G	全局负载模块	内置	LCA-PMT	策略迁移工具	第三方配置迁移工具，可定制服务
LCA-QT	单边加速模块	内置	LCA-PPS	智能流量管理套件	外置，按照流控压力定制硬件
LCA-QB	缓冲加速模块	内置，可定制缓存硬件	LCA-LBC	多云集群管理套件	外置，按照按照业务规模定制
LCA-QS	SSL加速软件模块	内置	LCA-CS	云应用交付配置服务	原厂专业应用、网络配置优化服务
LCA-QSH	SSL加速硬件套件	内置，可定制硬件支持国密算法	LC-OCS	多云零信任顾问服务	多云零信任安全顾问及架构服务
LCA-VPN	VPN模块	点对点隧道接入，支持多云互联等	LC-AOS	紧急运维服务	勒索病毒恢复等紧急运维支持服务

鸽鹦科技

服务热线：400-014-9467
广州|苏州|宁波分公司
华中|华北|西南|海南|广西服务中心

深圳总部
深圳南山数字文化产业基地东塔1008

深圳市宝安区三区金融街建安一路
9号恒明珠国际金融中心8楼鸽鹦科技

版本号:M7-11002015-20200607-C-1.2
www.LucciTech.com