中数国科防火墙
产品白皮书

（中数国科集团）

■ 版权声明

目录

一、概述

随着互联网的普及，网络的资源共享进一步加强，信息安全问题日益突出。黑客们可以轻易地通过拒绝访问攻击瘫痪企业网络；木马、病毒等恶意软件也经常通过邮件、恶意的 Web 网页、文档下载等应用层途径使得病毒的危害范围和扩散速度加大。网络安全问题日益严重，如何创建一个安全的网络环境也成为一个热门课题。

中数国科防火墙采用先进的高性能多核架构，运行自主可控的操作系统，搭载接口丰富的硬件平台，结合智能路由等全面的网络层支撑以及双机热备保障业务处理高效可靠，场景支撑灵活全面；配备 WAF 级别的入侵防御功能和独特实时病毒拦截技术的病毒防护功能，通过单路径并行处理的安全检测引擎和应用识别，实现对用户、应用和内容的深入分析，为用户提供安全智能的一体化防护体系。

二、需求痛点

网络的快速发展正在改变人们的生活和工作方式，但网络是一把双刃剑，带来便利的同时存在一些难题：

网络场景复杂多变，部署方式各有不同；

- 网络攻击类型多样，攻击方式日新月异；
- 网络数据数量巨大，应用识别难度太大；
- 带宽使用杂乱无序，工作效率无法提高；
- 设备管控难度太大，运维投入居高不下；

三、产品特点

3.1 全网威胁情报，未知风险可防护

随着攻击的复杂性、多元化不断提升，传统安全设备不断受到挑战；新一代的攻击者常常向企业和组织发起针对性的网络攻击，也就是高级持续攻击（APT）。攻击者不断改变现有的攻击方式，开发新的方法。单独依赖防火墙、入侵防御系统和反病毒软件，无法阻止这些黑客的攻击。这类攻击无法通过恶意程序签名或者过去的攻击技术报告进行检测，攻防不对等，中数国科防火墙使用自主研发威胁情报平台，尽可能通过预知风险的方式，来消除这种不对等，让企业安全得到更有力的保障。

威胁情报数据指标很多种，包括 IP 信誉、DOMAIN 信誉、URL 信誉、文件信誉（MD5/SHA）、最新的攻击事件、攻击趋势与防范措施几种情报。这些情报主要用于提升中数国科防火墙、入侵防御系统、安全网关等以及其它技术的有效性和主动防御能力。将威胁检测及情报处理能力落地，降低平均威胁检测时间（MTTD）和平均威胁响应时间（MTTR）。

3.2 灵活高效全面，场景支持更丰富

中数国科防火墙搭载自主可控的操作系统，融合了丰富的网络特性，在满足 IPv4/IPv6 双协议栈的同时，配合智能路由和 DDNS 等，可在 802.1Q、RIP、OSPF 等各种复杂的网络环境中灵活组网；具备与第三方系统对接，数据共享，提升业务价值。中数国科防火墙产品具备优秀的适应性，适用各种复杂场景，更符合业务需要。

领先的多核架构及分布式搜索检测引擎，配合高性能的处理器，多业务并行处理，确保中数国科防火墙在各种大流量、复杂应用的环境下，仍能具备快速高效的业务处理和防护能力。

中数国科防火墙产品集防火墙、负载均衡、入侵防御、病毒过滤、应用识别、行为控制、VPN 接入、业务可视、安全认证等功能于一体，为用户提供了一个灵活、高效、全面的网络解决方案。

3.3 专业智能引擎，立体防护更安全

随着互联网的普及，网络的资源共享进一步加强，信息安全问题日益突出。黑客们可以轻易地通过拒绝访问攻击瘫痪企业网络；木马、病毒等恶意软件也经常通过邮件、恶意的 Web 网页、文档下载等应用层途径使得病毒的危害范围和扩散速度加大。中数国科防火墙具备超过 4000 种预定义攻击特征的 WAF 级入侵防御功能和海量病毒特征独特实时病毒拦截技术以及高效引擎的病毒防护功能，实时的对流量进行分析，从数据链路层到应用层有效的阻断网络中的攻击和病毒行为，全方位的立体保护用户的关键数据，避免机密文件泄露和经济损失。

3.4 数据深度识别，行为管控更细致

员工上班时间进行业务无关的行为无疑会降低职工的办公效率，如果不慎发表不正当言论，将会给企业单位带来舆论风险，对形象声誉造成负面影响。中数国科防火墙产品采用 DPI/DFI 融合识别技术，通过对用户流量进行全面的分析，能够深入识别应用的内置动作，例如针对微信可识别控制多达 12 种行为动作。使用中数国科防火墙产品能够避免员工上网娱乐的同时，帮助企业单位及时拦截不良言论，通过应用精细化管理让网络更有序。

3.5 带宽优化管理，用户体验更迅速

企业单位的出口带宽有限，带宽使用情况的不清晰不准确，造成了带宽未能有效的利用起来，带宽资源白白的被浪费掉。中数国科防火墙能帮助组织管理者透彻了解组织当前、历史带宽资源使用情况，并据此制定带宽管理策略，验证策略有效性。不但可以在工作时

间保障核心用户、核心业务所需带宽，限制无关业务对资源的占用，亦可以在带宽空闲时实现动态分配，以实现资源的充分利用，提升用户使用网络的体验。流量限额和时长限额区分用户权限，实现差分服务，助力营销。

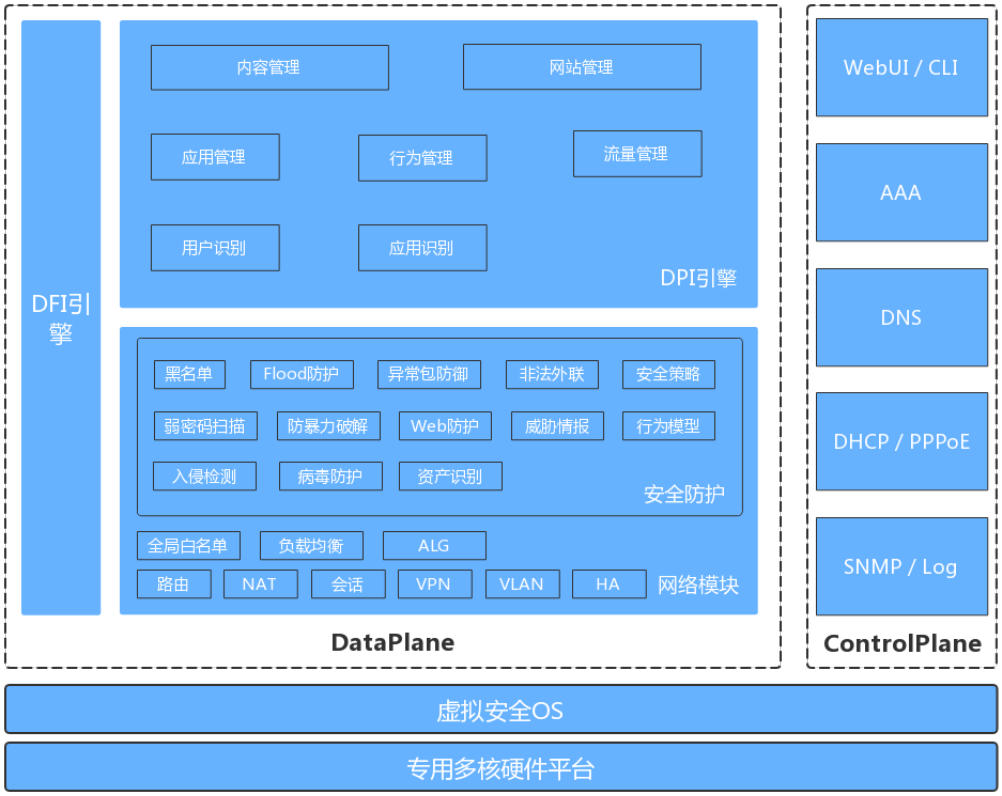
3.6 集中统一管控，网络运维更便捷

网络设备由于自身的专业性，非网络人员较难理解策略和日志的作用，日常管理和维护往往需要专业的网管人员；分支上线、分支业务变更，运维人员需要逐个分支进行配置，运维工作量大，周期较长。中数国科防火墙采用一体化安全策略，管理员只需要通过一条策略便可针对应用、网址、入侵防御、病毒查杀等内容进行统一管控，使用方便，维护简单。在大规模部署时，可配合集中管理系统对分布部署的中数国科防火墙进行零配置上线、统一策略管理、业务变更自学习、攻击事件监控、攻击事件分析、报表分析等。极大的降低了网络的更换难度，简化了运维的任务。

四、产品解析

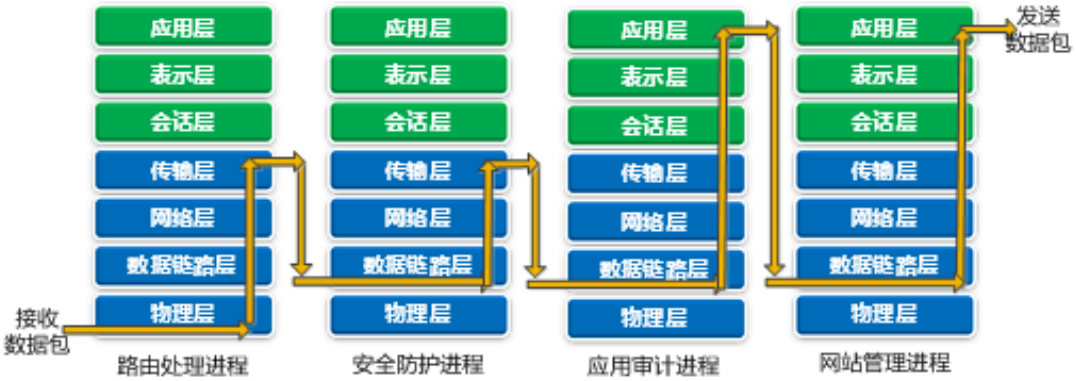
4.1 高性能多业务并行架构

中数国科防火墙采用最新最先进的多核硬件架构，在硬件架构上运行自主知识产权的安全 OS，高效的并行调度算法和内存管理机制提高了流量转发报文的性能。另外，将 CPU 处理的数据根据其特性分为 Data Plane（数据面）和 Control Plane（控制面）两类，简称 DP 和 CP。在多核系统一部分 CPU 专职 CP 工作，大部分 CPU 专职 DP 工作。这样就避免了因系统调度，导致设备转发性能降级或者无法响应管理操作等现象。具体 DP 和 CP 的 CPU 分布根据用户场景定义。

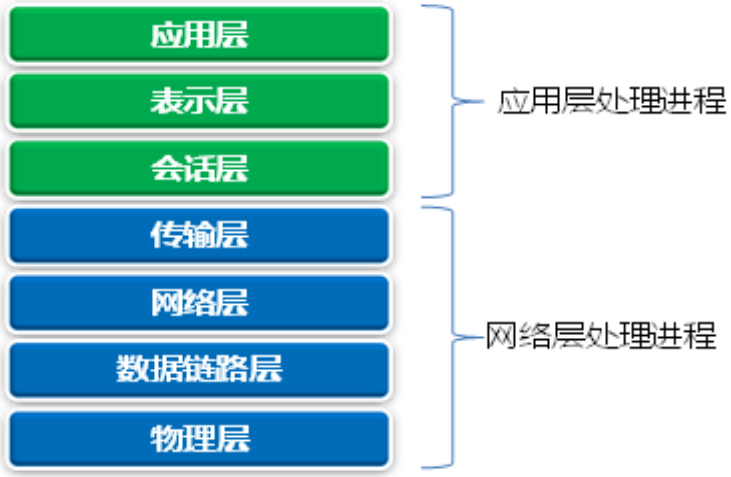


● 数据面

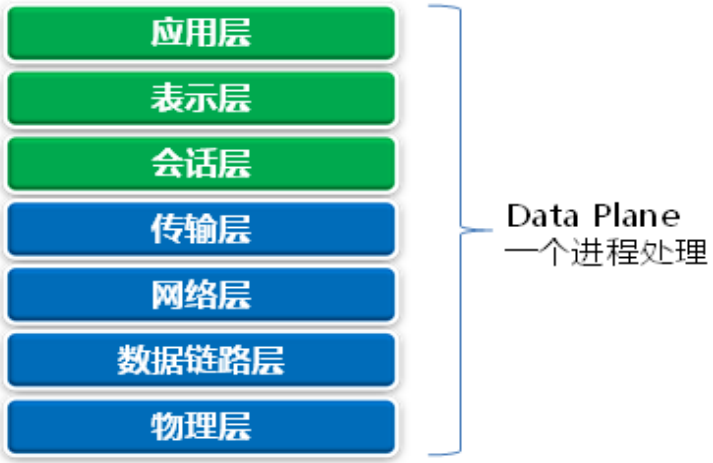
传统的网关设备为了降低设计和开发难度，会将各个模块以进程的方式存在，数据包每通过一个模块都要重复对数据的解析。增加了数据包在系统停留的时间，从而造成了网络延迟大的问题。



有的设备则将网络层处理与应用处理分别在两个进程上实现，这样就出现了数据包多次拷贝的情况，增加了内存访问次数，降低了系统性能。



中数国科防火墙系列的 DP 主要处理转发相关的工作，通过对数据包一次解析，按层次由对应模块处理，可以节省不同模块间重复解析数据包所消耗的资源，从而降低网络延迟。



4.2 网络特性

4.2.1 多种部署方式

中数国科防火墙支持多种部署方式，可以灵活的部署在用户的网络中。设备支持通过路由模式串接在用户网络用户中，实现用户数据的转发，为用户网络提供安全防护；设备

支持通过透明桥接模式串接在用户网络中，不做为网关设备，只对出入网络的流量进行检测或者阻断；设备支持路由和桥接混合的模式（混合模式）接入到网络中；设备支持以旁挂的形式接入到网络中，对网络出口的镜像流量进行分析，及时发现和上报可疑文件和动作，为用户提供安全防御依据和建议。

4.2.2 支持的路由特性

网络的迅猛发展，安全设备的静态路由已经无法满足企业网络实时自适应网络结构变化的需求。中数国科防火墙产品为用户而丰富的路由协议，支持静态路由、策略路由、ISP路由，RIP、OSPF 等路由功能。中数国科防火墙可满足用户绝大部分场景下的路由功能的需求。

- ISP 路由

用户出口有多个运营商线路时，跨运营商线路访问资源时，会出现网络访问缓慢，服务质量下降等问题。中数国科防火墙 ISP 路由主要用于解决此问题。中数国科防火墙预置中国电信（ChinaTelecom）、中国联通（Chinaunicom）、教育网（ChinaEducation）、中国移动（ChinaMobile）四个主流运营商的地址库，支持自定义增加 ISP 条目。管理员可指定运营商和出接口，当访问请求解析后按照预定的出接口或下一条进行转发，从而使得业务质量最优。

- 策略路由

策略路由，也叫做基于策略的路由，是指在决定一个 IP 包的下一跳转发地址时，不是简单的根据目的或源 IP 地址来决定，而是综合考虑多种因素决定。是一种比基于目标网络进行路由转发更加灵活的数据包转发机制。它转发分组到特定网络需要基于预先配置的策略，这个策略可能指定从一个特定的网络发送的通信应该被转发到一个指定的接口。通过策略路由配置实现对于满足所定义策略的报文，从指定的出接口或者下一跳转发的需求。

中数国科防火墙支持基于七元组进行策略配置，可将应用流量通过预定义的网关或者出接口进行转发，以实现流量分流的效果。

4.2.3 链路均衡负载

- 链路负载均衡

随着带宽成本的下降及业务需求，企业通常存在两个或两个以上的网络出口，多出口提升了网络出口稳定性同时又带来了多链路带宽利用率低、多链路带宽差异大、各运营商网络质量差异、内网应用对带宽需求差异等问题；以上诸多问题只需通过中数国科防火墙提供的链路负载均衡即可迎刃而解。具体实现主要基于以下几点：

- 实时多链路监测

实时监测每条出口链路的逻辑连通性，即使端口处于 UP 状态，但可能由于远端故障导致的检测报文超时，中数国科防火墙同样会执行链路切换的动作，以保证网络连接的可用性，实现多条链路的冗余备份。

- 基于权重流量分担

中数国科防火墙提供了基于优先级和权重的多链路流量分担算法以满足不同应用场景的需求，从而达到高效的利用出口链路带宽的目的。

- 智能应用路由

中数国科防火墙内置超过 1500 种以上的应用识别能力，将网络中各种应用进行准确分类和精细识别，让不同的应用分别使用不同的出口线路，保证重要业务不中断。

- DNS 透明代理

通过透明代理技术，完成对客户 dns 流量的无感知代理，从而保证客户的 dns 请求得到最快，最稳定的响应，大幅度提升客户的上网感受。

- 服务器负载均衡

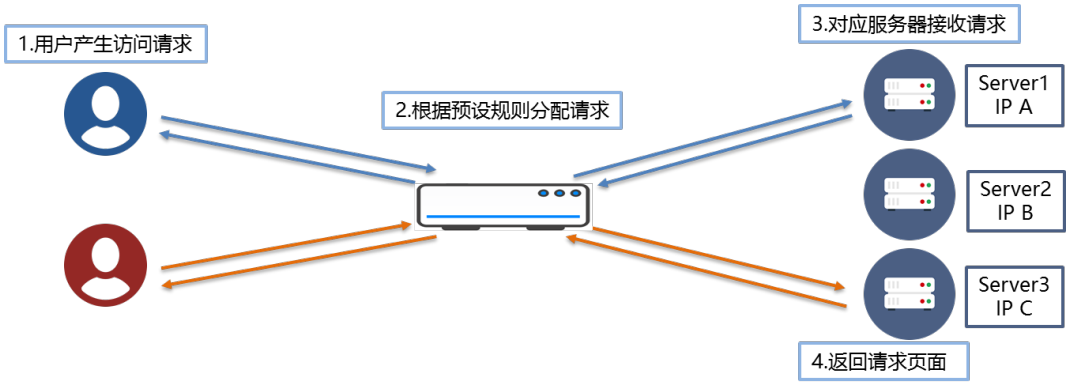
中数国科防火墙服务器负载均衡可以对一组服务器提供负载均衡业务，这一组服务器一般来说都是处于同一个局域网中，并同时对外提供一组或者多组相同或相似的服务。

中数国科防火墙能够实现在客户访问多台同时工作的服务器的情况下，即时按需动态检查各个服务器的状态，根据预设的规则将请求分配给最有效率的服务器，实现数据流合

理的分配，使每台服务器的处理能力都能得到充分的发挥，提高整体性能，改善应用系统的可用性。

中数国科防火墙服务器负载均衡包含三个基本元素：

- 负载算法：权重算法、源地址散列+权重算法
- 服务器健康检查：提供 ICMP 的探测方式
- 会话保持功能：可保持用户所有访问会话分配至同一台服务器上处理



4.2.4 地址转化

中数国科防火墙拥有优化过的 NAT 性能。支持源地址和目的地址转换，支持动态和静态的地址转换。此外支持 NAT44，可生成和维护用户地址映射表，实现运营商级 NAT 转换；并实现用户溯源关系向 AAA 服务器和日志服务器上报。

相对传统的企业网 NAT 应用，NAT44 具备更高的性能、稳定性和安全性。NAT44 能够支持用户规模更大、承载流量大、业务稳定性要求更高的服务要求。

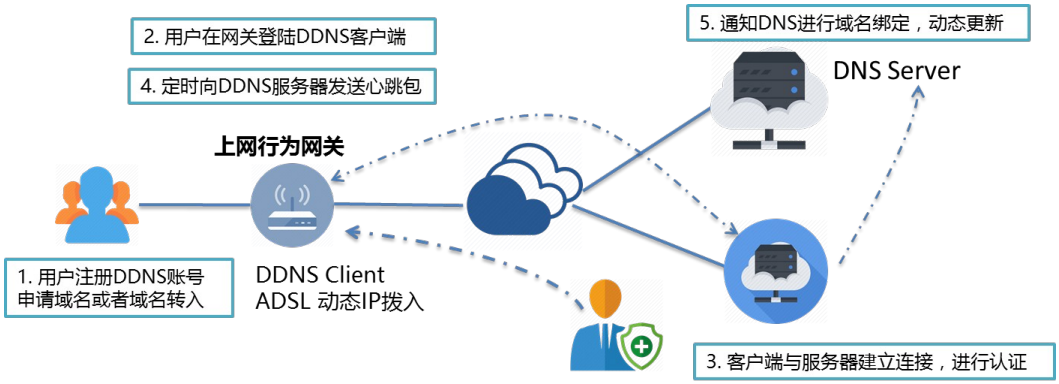
4.2.5 动态域名服务

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。动态域名服务是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候客户端程序就会通过信息传递把该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务

器程序负责提供 DNS 服务并实现动态域名解析。

目前 ISP 大多提供动态 IP（如拨号上网），若想在网际网络上以自己的网域公布，动态域名服务提供了解决方案，它可以自动更新用户每次变化的浮动 IP，然后将其与网络域名相对应，这样其他上网用户就可以透过网络域名来交流了。

中数国科防火墙提供动态域名服务功能。可解决动态 IP 地址场景下管理，以及 IPsec VPN 场景使用域名连接等问题。



4.2.6 虚拟化功能

● 网络功能虚拟化

中数国科防火墙支持网络功能虚拟化（NFV），并且支持 KVM、VMware ESX 等业界主流虚拟化环境。

NFV 技术使得中数国科防火墙打破功能模块依赖于硬件的局面，安全资源可被充分利用，新业务开通上线快、部署灵活。可基于客户实际业务需要进行弹性伸缩。可应用于运营商、云服务商、数据中心、园区网等多种场景。更低成本的解决方案，开放的 API 接口，可为客户获得更多、更灵活的网络能力。

● VRF 路由

在传统网络中，如果网络中有较多的网络部署划分，就可能需要部署多台出口路由设备，不仅建设成本高，而且占用更多宝贵的机房空间，维护成本和难度也居高不下。

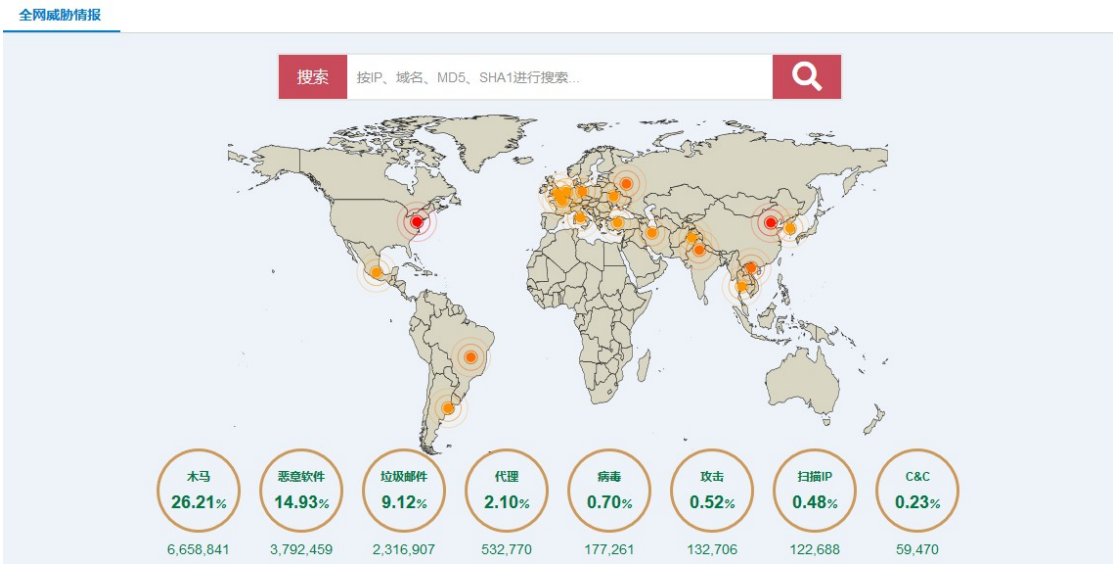
传统路由设备的不足，推动了虚拟化技术的普遍发展。中数国科防火墙迎合网络时代潮流，自主开发了 VRF 功能。中数国科防火墙可以将不同的端口加入创建的 VRF 组中，每个 VRF 组之间可以独立控制和转发，相互隔离，可以看做是不同的路由器，可以使用相同的或者是重叠的 IP 地址而不会产生冲突。VRF 功能提供了从一台物理路由器变成多台虚拟路由器的功能，可以为用户节省大量的建设成本和维护成本，维护也更加简单。

4.3 安全特性

互联网在快速发展的同时，也催生了一些安全隐患。黑客们可以轻易地通过拒绝访问攻击瘫痪企业网络；木马、病毒等恶意软件也经常通过邮件、恶意的 Web 网页、文档下载等应用层途径使得病毒的危害范围和扩散速度加大。

4.3.1 威胁情报

随着攻击的复杂性、多元化不断提升，传统安全设备不断受到挑战；新一代的攻击者常常向企业和组织发起针对性的网络攻击，也就是高级持续攻击（APT）。攻击者不断改变现有的攻击方式，开发新的方法。传统的规则匹配已经无法防御这样的攻击。中数国科防火墙通过自研威胁情报云平台，整合对接 60 余家商业、开源威胁情报，包括微步在线、IBM 安全、VirusTotal、天际友盟、PluseDive 等等。提供全网威胁情报查询功能，支持对可疑 IP、域名、文件 Hash 进行搜索，并查看关联分析。



中数国科防火墙支持与威胁情报云平台对接，用威胁情报发现内网有威胁的会话、文件传输行为等等。支持对内网产生的威胁进行分类，并对 Top 威胁进行排序。管理员可以根据实际情况，对内网威胁进行处理。

威胁情报支持热点事件实时推送，在网络上刚爆发的蠕虫、勒索病毒等等，均可以在第一时间推送到中数国科防火墙，网关可进行一站式向导配置。提前做好安全防御。

4.3.2 策略分析与清理

防火墙规则及策略的复杂度是企业安全人员最大的防火墙难题，而且当前网络环境的复杂性越来越高，网络服务与网络终端的多样性，相应的防火墙设备就需要更多、更复杂的控制策略。这些控制策略经过一段时间的积累，往往会造成老策略不敢删，新策略不断增加，单台防火墙积累成千上万的策略，极大降低设备性能和用户体验。

策略分析支持一键分析当前的冲突、冗余、隐藏、合并、过期和空策略，一定程度上解决防火墙管理的难题，使每一条策略都直观可视，让中数国科防火墙更易于使用、便于维护管理。本功能将策略按照匹配范围，匹配顺序，行为三个维度来进行分析。整理出冗余策略、隐藏策略、冲突策略、过期策略、空策略、可合并策略六类问题策略：

本策略与其他策略比起来

范围	顺序	行为	结论
大	先	相同	其他策略为隐藏策略
		不同	
	后	相同	其他策略为冗余策略
		不同	其他策略为冲突策略
小	先	相同	本策略为冗余策略
		不同	本策略为冲突策略
	后	相同	本策略为隐藏策略
		不同	
存在交集	-	不同	互为冲突策略
可合并	-	相同	两条或多条策略为可合并策略
空	-	-	本策略为空策略
时间过期	-	-	本策略为过期策略

策略的状态即对该策略分析后的结果显示，目前分为 6 类：冲突策略、冗余策略、隐藏策略、可合并策略、空策略、过期策略，下面对几种状态进行简要说明。

● 冲突策略：第一种情况，根据匹配的前后顺序（先匹配 A 策略再匹配 B 策略），如果 A 策略匹配的所有数据流会被 B 策略包含在里面，且 AB 策略的行为不同，则 A 策略为冲突策略；第二种情况，不区分匹配的前后顺序，若策略 A 和策略 B 存在数据流交集（非包含和被包含关系），且 AB 策略的行为不同，则 A 和 B 互为冲突策略；

● 冗余策略：根据匹配的前后顺序（先匹配 A 策略匹配 B 策略），如果 A 策略匹配的所有数据流会被 B 策略包含在里面，删除 A 策略不会对其余策略产生影响，如果 AB 策略行为相同，那么 A 策略会被计算为冗余策略；

● 隐藏策略：根据匹配的前后顺序（先匹配 A 策略在匹配 B 策略），如果 B

策略匹配的所有数据流会被 A 策略包含在里面，那么不论行为是否相同 B 策略会被计算为隐藏策略；

● 可合并策略：不区分匹配的前后顺序，策略内元组信息只有一项不同（且可合并）的情况下，则认为是可以合并的策略；

● 空策略：当策略中匹配的任何一个对象为空时，那么该策略会被计算为空策略，

● 过期策略：发现当前策略中，匹配的时间范围已经不会再次出现的策略；

4.3.3 攻击链可视化分析

当前网络安全设备有一个很重要的问题就是日志量太多，且没有关联分析。造成攻击发生了却不能及时在日志中发现；大量无效的日志淹没了关键日志，对攻击的取证和溯源也造成很大的困扰；各类攻击的日志分别呈现，管理员在分析时也无法关联；

而攻击链就是为了解决这一类问题，通过对检测出的威胁时间日志进行汇总分析整理实现以攻击链的形式可视化展示攻击者的入侵路径，入侵程度，影响登录等等。一次完整的攻击往往过程复杂，手段多样，当前的安全产品无法检测出所有过程和手段，更无法对所有的过程和手段进行关联，所以以攻击链的形式可视化展示，就可以对攻击者的入侵路径进行完整的呈现。精确、简单、统一、有效，便于管理员对内部网络进行分析，对攻击者进行取证溯源。

攻击链实现所有安全日志按照攻防逻辑进行编排，一目了然的进行安全事件回顾和溯源分析，把攻击者入侵分为前期阶段、入侵阶段、控制阶段、外传阶段形成针对资产维度和针对攻击者维度两条链。资产维度的攻击链可以对内网某资产进行针对性分析，准确把握其安全威胁情况，让普通网络管理员也能进行安全分析，明确感知到安全事件的严重性。攻击者维度的攻击链可针对某攻击者进行分析，帮助管理员修复内部安全漏洞。

4.3.4 一体化安全策略

中数国科防火墙采用一体化安全策略，管理员只需要通过一条策略便可完成对源接口源地址、用户、目的接口、目的地址、应用、服务、时间等维度的匹配，并针对应用、URL、入侵防御、病毒查杀等内容进行统一管控，使用方便，维护简单。

4.3.5 入侵防御

Gartner 报告指出企业面临的网络攻击中 70%来自应用层，传统防火墙以及应用层安全设备功能单一，面对复杂的应用层攻击捉襟见肘。中数国科集团经过多年网络安全领域的沉淀和积累，打造了一支资深的攻击特征库团队和安全服务团队，在蠕虫、后门、木马、间谍软件、Web 攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计报警等防御手段，并随时关注业界最新发现的安全漏洞和接收全球用户反馈的攻击特征，并在第一时间做出响应和提供更新，实时完善攻击特征库，提供最及时、最全面的入侵防御。

入侵防御安全引擎的巩固走原理是检测数据包有效载荷，提取特征（如下图），然后与设备加载的攻击特征码进行比对，设备加载的特征码都是从已知通用应用协议或应用系统漏洞中提取出来的，专门针对这类通用漏洞的攻击防护，大部分能通过打补丁的方式解决。然而，经业界众多专业厂商研究分析，目前攻击者大多采用的是针对网站代码内容的攻击手段，而不是采用传统特征库中已有的通用攻击手段。IPS 具备了针对已知通用应用协议或应用系统漏洞的防护，但对于目前普遍定制开发的 Web 站点系统，由于网站应用代码中的漏洞而带来的应用攻击，不能提供有效的防御，尤其是对一些逻辑关系复杂的应用攻击。

如果代码编写者对用户提交的数据未做适当的检查及验证，恶意攻击者可以利用 Web

页面中提交数据的表单构造访问后台数据库的 SQL 指令，从而能够非授权操作后台数据库，达到获取敏感信息、破坏数据库内容和结构、甚至利用数据库本身的扩展功能控制 Web 服务器操作系统，如此不仅能够达到网页挂马，还可以构成对 Web 服务器的其他攻击，篡改网页内容更是轻而易举。

入侵防御安全引擎通过多个流程将报文逐步分解，主要包括：协议解码、自定义规则匹配、签名防护等等。

- 4000 种预定义攻击特征
- 实时在线更新
- 提供 WAF 级别的安全防护，有效的防御和预警 Web 服务器的攻击，包括网页防爬虫、网页防篡改、HTTPS 防护、DDoS 攻击防护、Web 攻击过滤、漏洞防护自学习等
- 处理网络类威胁，包括安全漏洞、木马后门、可以行为、CGI 访问、CGI 攻击、缓存溢出、拒绝服务、蠕虫病毒、网络数据库攻击、间谍软件、安全扫描、网络设备攻击、欺骗劫持
- 保证基础网络安全
- 分级事件及操作配置
- 虚拟补丁管理

部分攻击者具有网络中特有的攻击方式或者尚未出现过的漏洞，此时特征库尚未覆盖到。入侵防御安全引擎提供自定义规则功能，通过对进入设备报文的协议类型，协议字段，字段内容形成匹配条件，并通过逻辑与、逻辑或形成多条件匹配的方式实现入侵防御。安全管理员可以使用自定义规则功能，自己写签名进行防护。自定义规则检测是基于流检测的，支持多种协议字段，其中包括 IP、UDP、TCP、FTP、HTTP、ICMP、POP3、SMTP 协议。对于字符串字段，可支持正则和非正则匹配的方式。灵活多样，防御力强。

4.3.6 Web 防护

中数国科防火墙的 Web 应用防火墙不但可以帮助用户进行 Web 安全防御，提高网站安全性，而且集成了网络爬虫识别和过滤、网站资源盗链防护、内容关键字过滤、HTTP 协议合规性和 URL 参数合规性检查等功能，可以帮助用户对网站的访问进行过滤和优化，提高网站运营的稳定性和服务质量。

WEB 防护引擎能有效抵御各种注入式攻击，包括 SQL 注入、系统命令注入、LDAP 注入、SSI 注入、邮件注入、请求体 PHP 注入等攻击；对于常见的 XSS 攻击的防护结合基于语义分析和攻击指纹两种方式，相比传统只基于攻击指纹的检测方法，检测准确率更高，误报率更低，防逃避能力更强；为了检测出恶意攻击者对 WEB 站点的扫描行为，WEB 防护引擎支持多种检测方式，多种扫描方式，同时也具备检测恶意爬虫的能力，其中包括 Acunetix、Appscan、Nessus、Sqlmap、Arachni、Netsparke、Webinspect、绿盟极光等。其它的防护还包括会话劫持检测、木马检测等。

WEB 防护引擎里面还集成了一些高级防护功能，精确访问控制的自定义规则功能、防盗链、CSRF 攻击检测、CC 攻击防护、应用隐藏、防篡改。这些高级防护能够对 WEB 站点资源进行保护、防止 HTTP FLOOD 攻击、内容防泄漏等。

4.3.7 病毒防护

中数国科防火墙拥有海量病毒特征库，配合先进的防病毒引擎，能够精准识别并清除流行木马和顽固病毒。病毒检测引擎针对非缓存流检测模式进行了全面结构调整和优化，使中数国科防火墙的病毒检测率和处理性能获得质的突破：在保持高病毒检测率的同时，系统性能下降不超过 20%。

- 可以在 HTTP,SMTP,FTP,POP3,IMAP 等多种协议下病毒防御，支持非标准端口的 HTTP,SMTP,FTP,POP3,IMAP 协议中的病毒检测。
- 支持路由、透明、混合等各种工作模式下的网络病毒检测，支持无 IP 地址

的透明桥下的网络病毒检测模式，支持 VPN 模式下的病毒扫描。

● 采用高效的病毒防御引擎和国内知名病毒厂商特征库，可检测不少于 300 万以上种病毒。

● 可以根据不同的源 IP 地址、目的 IP 地址、服务、时间、接口、用户等，采用不同的病毒防御策略。

● 可以过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒

● 特征库定时更新，支持病毒库本地升级，病毒库可实时在线升级。

● 支持基于病毒防护策略设置阻断、清除、记录日志。

4.3.8 安全管理

1. 会话管理

会话监控、会话控制功能是专业化管理内网必不可少的功能。中数国科防火墙可对当前设备的会话进行监控，管理员可查看会话的发起用户、源目地址、端口、协议、策略、存在时间和超时时间等，具有完备的状态检测表追踪连接会话状态；中数国科防火墙支持对当前所有会话进行峰值统计，方便管理员快速筛选内网异常用户和 IP，可帮助管理快速定位网络故障；管理员支持针对全局基于 IP 进行并发会话和新建会话的限制，保障内网所有访问行为均在正常数值范围内，确保内网安全。

2. 黑名单

中数国科防火墙支持黑名单设置并支持黑名单时长设定，用户上网行为中触发防攻击规则后源地址自动进入黑名单。有效提升了用户网络安全性

3. 资产发现 & 安全分析

如果看不到，则无法提供保护。深入了解网络设备、应用、用户、操作系统和文件等利用这些信息能更好地了解网络行为，识别违规操作，并评估入侵风险。

采用主动扫描和监控主机流量的方式识别网络中的资产信息，能够识别出网络中的设

备类型，包括 PC、交换机、打印机等；能够识别设备的操作系统、使用的浏览器、杀毒软件、开启的应用服务；能够帮助安全管理人员掌握内网的资产情况，识别潜在风险。资产发现可以从流量中发现资产标识，也可以通过主动的端口扫描发现资产。

中数国科防火墙支持对资产开启的服务，操作系统，浏览器以及关联的安全日志等分析出资产整体安全风险级别。

根据产生的日志信息，多维度分析资产风险。包括是否受到 IPS 攻击、是否下载了病毒文件、是否存在弱密码，是否往外传输文件等。以确认资产的风险情况，对存在风险的资产发出告警，可以帮助安全管理人员及时调整安全策略。

4. 攻击防护

当受到攻击时，伴随而来的会出现网络异常情形发生，网络异常大概可分为以下三种：

- 通信协议异常

例如由外界网络流入大量过长的 IP 数据包、大量的 IP 碎片数据包、异常的 TCP 通信协议连机状态、被截断的 IP 数据包、无法重组的 IP 数据包等。

- IP/Port 的扫描异常

通过 IP 扫瞄，黑客得以窥知目的端内网络结构和情形；通过 Port 扫描，黑客可以得知

目标主机已开启的服务端口。

● 网络流量异常

例如突然产生大量的 TCP SYN、TCP、UDP、ICMP、IGMP 等数据包，占据正常网络使用带宽。

当上述攻击数据包发起时，经过改造的恶意数据包可能会造成企业内部网络系统死机无法对外提供正常的服务；IP/Port 扫瞄的行为将让企业内部的网络架构轻易被黑客得知；大量的异常流量数据包也可能造成企业核心路由器、交换机等因承载过重而死机。

中数国科防火墙内置异常包攻击防御模块，可以检测各项偏离预期的网络行为。依据 RFC 标准规范制作通信协议异常检测模块，可以阻止不符合标准通信协议规范的数据包。支持网络流量异常检测，不单只使用计数的方式，还使用专门的统计算法，可以准确地检测网络流量的异常情形。

● 支持 ARP 防欺骗、支持 IP、MAC 地址绑定。

● 支持 ARP Flood 攻击防护、支持基于接口的 ARP 学习控制。

● 支持 Ping of Death、Land-Base、Tear Drop、TCP flag、Winnuke、Smurf、IP 选项、IP Spoof、Jolt2 等异常包攻击的防御。

● 支持基于 IPv6 的 Winnuke、Land-Base、TCP flag、Fraggle、IP Spoof 等异常包攻击的防御。

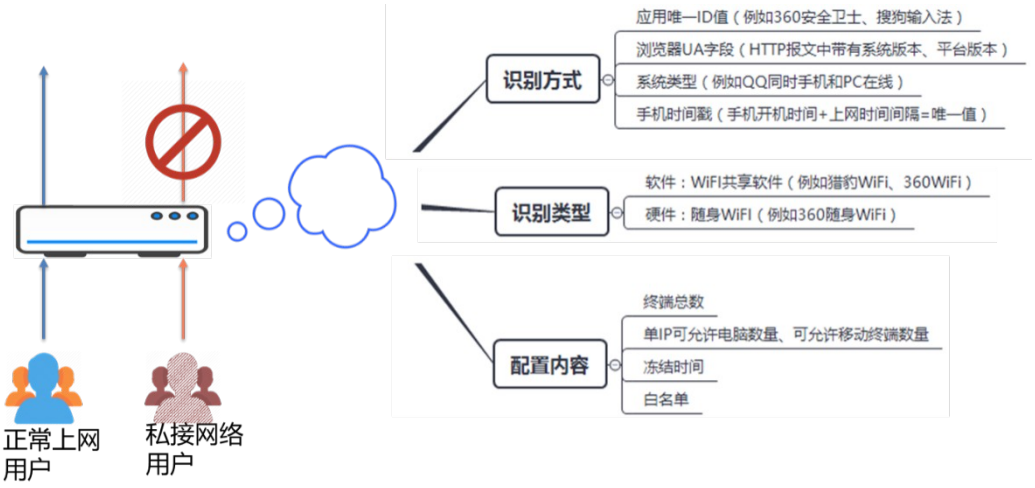
● 支持基于接口的端口扫描防护和 IP 扫描防护。

● 支持 SYN flood、UDP flood、ICMP flood、DNS flood 攻击防护，支持自定义阈值。

5. 防私接路由

上网用户私接 WiFi 或路由器行为会造成无法校验用户身份、安全性能难以保障、占用额外带宽资源等问题。中数国科防火墙能够快速识别“一拖 N”的网络私接行为，精准定位“N”即私接用户数量，并进行有效的管控；及时发现非法热点预防个人用户私接路由，拒绝未知网络终端节点，保护运营商利益；同时中数国科防火墙支持同步和展示认证用户信息，

支持同步 PPPOE 账号等认证服务器账号信息。让整个网络拓扑清晰可控，有效预防数据泄露的安全风险；极大的降低了管理员网络维护的工作量。



4.4 管理特性

4.4.1 设备管理

中数国科防火墙提供丰富、安全和全面的管理方式，帮忙网络管理员更便捷高效的管理网络。

- 双因子设备管理

传统的账号密码设备管理方式安全性较低，容易被黑客截获破译，且认证唯一性难以保障。中数国科防火墙提供双因子认证功能，用户登陆设备界面时，需在 PC 终端插入 U-Key，同时进行账号密码校验；否则无法登陆设备界面。

此功能极大的提高了网络设备的安全性，且具备操作简单，携带方便的特点。

- 中英文切换

中数国科防火墙内置中文、英文两种语言，管理员可根据场景需求，切换使用界面的语种。

- 三权管理

中数国科防火墙默认管理模式为普通模式，普通模式默认存在 admin 账号，该账号可添加、修改、删除所有管理账号，且可管理所有界面模块，无细致权限划分。

中数国科防火墙可将管理模式切换为三权模式。切换后系统默认存在四种管理账号：

- 权限管理员（Authority），为系统管理员分配权限，可设置读写分离，支持设置模块分离管理
- 账号管理员（Account），添加、删除管理员账号
- 审核员（audit），查看所有管理员操作记录
- 管理员（admin），系统功能配置与管理

每个管理账号被赋予不同的权限，相互之间形成权限制约，避免了普通模式下超级管理员权限过大带来的管理风险，保障了设备管理安全。

- 管理方式

中数国科防火墙本地管理支持多种管理方式，且所有接口均可用于系统管理，管理方式包括 PING、HTTPS、TELNET、SSH、HTTP 等。

4.4.2 用户管理

用户管理模块作为行为管理设备必不可少的模块，使用频率在大幅提高，已经从初期的有无，是否可用，到用户作为系统的一个重要资源，在访问控制策略、认证等功能上都会相应使用。

中数国科防火墙的用户类型有：第三方用户，匿名用户和认证用户，可以实现基于用户的搜索，支持用户的移动、修改、导出、导入和批处理等功能。提供基于 IP、MAC 和 IP&MAC 的用户识别方式。用户支持自动同步，中数国科防火墙可以自动发现配置的网段中的终端设备，并自动录入为用户。省去大量人工录入的操作。自动发现的用户支持 CSV 格式导出，IP/MAC 绑定等。用户支持设备上的 AD 导入和 Excel 自定义导入功能。用户管理更便捷、更全面。

4.4.3 用户组管理

中数国科防火墙支持对用户组灵活管理，可提供纵向、横向两种维度对用户进行分类以树形结构展示，支持创建、批量移动、批量删除、清除所有用户组、搜索等功能，方便用户进行集中管理；此外中数国科防火墙支持导入导出功能，管理员可将用户组织结构保存在本地，降低因用户组编辑而导致策略配置匹配错误的几率，避免用户组误删除的操作，增加数据冗余可靠性。

4.4.4 身份认证

中数国科防火墙具备丰富身份认证方式，可有效的区分用户。是部署差异化授权和审计策略、有效防御身份冒充、权限扩散与滥用等的管理基础。

中数国科防火墙的身份认证方式有：

- 本地认证：Web 认证、用户名/密码认证、IP/MAC/IP-MAC 绑定；
- 第三方认证：RADIUS、LDAP 等；
- 短信认证：传统的认证方式，方便快捷；
- 免认证：认证用户无需进行身份认证，即可快速上网；
- APP 认证：不需要借助数据中心软件，无需 APP 修改，避免协调沟通成本；
- 微信认证：强制关注，自动弹出“一键微信连 WIFI”并关注微信公众号；
- 混合认证：界面配置选择多种认证方式，用户可根据需要更换认证方式；
- 单点登录： AD 域一次认证，减免频繁认证。

➢ **一键微信认证**

微信认证作为国内最知名的手机移动应用之一，已经得到了大量普及。虽然原始认证的方法短信认证和本地密码认证可以解决动态认证问题的，但是繁琐的操作或者短信费用几乎成为了大众的噩梦。因此，微信认证应运而生，即解决了动态认证的问题，又减少了

认证操作的步骤，且没有额外的资费，还帮助商家推广微信公众账号。

微信采用双 ID 实名审计和商业推广两面大旗，即微信 ID 和 openId。微信 ID 用来标识用户唯一性。openId 是微信 ID 与公众号 ID 共同产生的唯一标识。在公众平台只认 openId 不认微信 ID，有了 openId 和微信认证平台结合，对于同一个公众号就能根据微信用户所在的不同地点，推送不同的推广信息，辅助客户完成精准广告推送。

为了简化用户的认证过程，中数国科防火墙支持二次到店免认证，直接关联上 SSID 即可自动认证通过并上网，用户无感知；管理员可选择配置强制关注，认证时必须关注公众号，否则无法正常使用网络；给用户超预期的体验，提高企业品牌认可度。

一键认证步骤：

- 连接商家的 WIFI；
- 弹出微信认证界面；
- 点击“一键打开微信连 Wi-Fi”；
- 点击“立即连接”即可通过认证。

➢ APP **认证**

近年来企业纷纷业推出自己 APP，紧跟 e-commerce、O2O 时代步伐，用于丰富自己业务线、推广营销、会员返利活动。然而 APP 如何进行高性价比推广，为此 APP 认证孕育而生。

APP 认证首先需要管理员在中数国科防火墙预定义配置 APP 特征，中数国科防火墙会根据此 APP 特征生成符合设备可识别的特征文件加入到特征库中， 当移动终端连接上 WIFI 后并打开相应的 APP 触发网络流量，中数国科防火墙自动识别流量并进行特征匹配，即可判断连接上的移动终端是否合法。

➢ AD **域单点登录**

大型企业中，内网用户均需进行 AD 域身份校验，若内网同时存在其他身份验证，用户需逐次进行认证，且操作步骤繁琐。中数国科防火墙可与企业 AD 域进行联动，内网用户只

需一次认证，即可完成所有身份校验，简化认证步骤，提升用户体验。

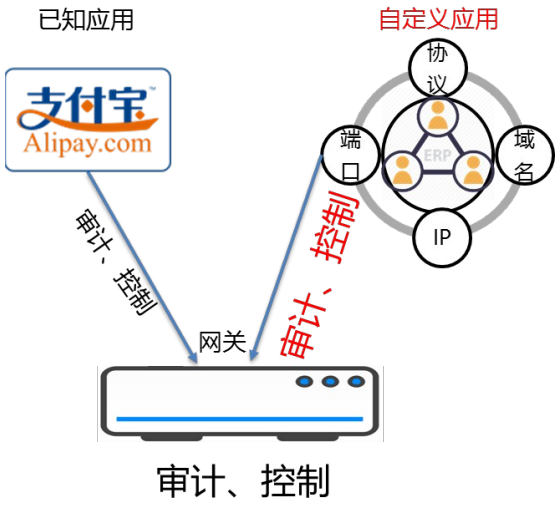
4.4.5 应用识别

应用识别（Application identify)是中数国科防火墙的重要功能。借助于应用识别功能，可以准确识别网络上正在运行的应用，应用流量的准确识别不但可洞悉整个网络的运行情况，而且可针对具体需求做用户行为的准确管控，这在一定程度上既可保证业务流的高效运行也可预防由于内网机器受到攻击而生产的威胁，同时识别应用类型也是应用审计与应用流量控制的基础。

随着 P2P 应用的广泛流行和基于 Web 的应用的兴起，令传统的利用固定端口来区分应用类型的设备无能无力。应用识别功能把对报文的协议解析、深度内容检测以及关联分析结合起来，通过对大量实际环境中的流量的分析，总结出每种应用的流量模型，把对数据包的协议解析、深度内容检测和关系分析的结果综合起来，由决策引擎通过与流量模拟的匹配程度，智能的判定应用类型，相比传统的应用识别技术，还具有以下特点：

- 自定义应用

办公自动化的趋势下，客户内网均已搭建了企业的应用系统，例如 OA、ERP 系统等。面对这种情况，上网行为管理产品通过自带的应用特性库无法对企业应用系统机型识别、审计和管理。中数国科防火墙具备自定义应用功能，管理员可根据协议、目标端口、IP、域名等维度创建应用特征，进而针对企业应用进行审计、流量统计和控制。

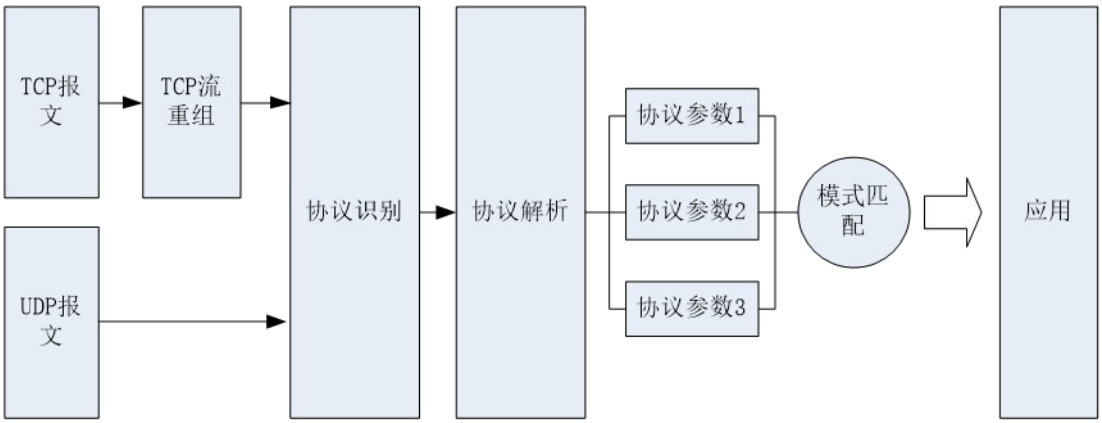


- 基于协议状态分析

中数国科防火墙对已知协议和 RFC 规范的深入理解，可准确、高效的对各种协议进行解析。例如，对于一次 HTTP 访问，先由协议解析出访问的 URL、Host、User-Agent 等信息，再将解析出来的信息进行特征匹配，这样可以带来以下优点：

提高性能，不需要对整个报文进行模板匹配，可以提高应用识别的性能。

降低误识别率，因为进行模式匹配的字段由整个报文缩小为特定的协议参数，可使特征写的更加精确，减少误识别率。



- 行为检测

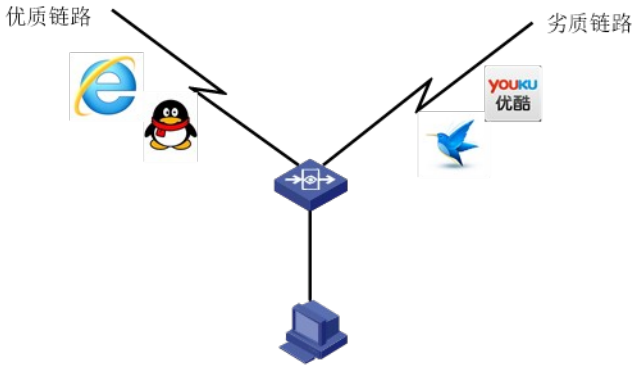
不同的应用类型体现在会话连接或数据流上的状态各有不同；基于这一系列流量的行为特征，通过分析会话连接流的包长、连接速率、发送/接收的流量比例、包与包之间的间

隔等信息来识别应用类型。

只有在准确识别应用协议的基础上，才能对应用做到深入、全面和准确地控制。不但可以准确、高效的识别出网络流量的应用类型，而且可以精准的识别出应用的行为。随着特征库的不断更新，支持的应用和行为在不断增加。网络中的应用日新月益，拥有强大的安全服务团队的支持，可以随时对网络中的新应用进行跟踪分析，持续的更新应用特征库。

- 应用路由

中数国科防火墙通过配置策略路由，可以实现基于应用的路由选择。在用户有多条链路的情况下，不同的应用分别使用不同的线路，使办公、游戏等重要应用的流量使用链路状态较好的线路，使 P2P、视频等流量走链路状态较差的线路，帮助用户合理的分配链路资源，即保证重要业务的使用，也不影响 P2P、视频等的使用。



中数国科防火墙的应用路由功能是不是基于端口，而基于应用来实现的，当发现某种应用的流量的时候，会把对应的 IP + 端口信息缓存在系统中，相同的 IP + 端口再次新建会话的会话，会命中相应的缓存，从而实现应用路由的功能。

- 基于应用的流量管理

中数国科防火墙系列可以实现基于应用的带宽分配，帮忙用户更好的限制 P2P、视频等占用带宽比较高的业务，保障重要业务的运行。

4.4.6 终端识别

中数国科防火墙提供以终端识别引擎为核心的安全策略、行为审计、来宾访问、日志

分析四大功能。核心思想是帮助 IT 管理员使整个网络易用、安全。IT 管理员可以从用户、设备、应用、行为等多个视角来管理网络。

- 终端识别

终端识别引擎是主要提供用户身份验证、和终端、系统类型识别的功能。当员工携带自己的设备连接到公司的网络之后，不需要安装任何客户端，只需要打开浏览器，就可以轻松的完成用户身份认证，并获得相应的授权，这样不仅可以减少 IT 管理员的负担，最重要的是，简化了操作，提高了员工使用自带设备的积极性。在不安装任何客户端软件的情况下，通过身份识别引擎的设备分析模块，IT 管理员可以看到员工加入的网络中的设备的操作系统、硬件类型和生产厂商。

中数国科防火墙识别用户系统、终端的方式有两种：通过 Web 访问的 User-Agent 域来识别终端类型。

```
GET / HTTP/1.1
Host: m.baidu.com
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_3_3 like Mac OS X; zh-cn)
AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8J2 Safari/
6533.18.5
Accept: application/xml,application/xhtml+xml,text/html;q=0.9,text/
plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
Cookie: Hm_lvt_e8499b7329e8d5d44f3f4c8902bb043a=1372659521;
```

通过移动应用来识别。比如在应用的流量中发现了来自淘宝网(IOS)客户端的流量，那么会通过这些流量判断用户的设备类型为 iOS。

- 安全策略

IT 管理员可能针对不同的场景，针对特殊的人员和设备类型，灵活的制定安全策略，一般来说，对于访客，对设备类型做比较少的限制，同时给只给予少量的权限，对于公司的管理人员，在给予更多权限的基础上，还要对设备类型做出更严格的控制，下面给出一些例子：

安全级别	人员	设备类型	权限
低	访客	任意设备	Internet
中	员工	iPhone	Internet、公司邮箱
高	经理	iPad	OA 系统

- 来宾访问

当有访客携带自己的智能手机/平板电脑尝试加入到公司网络中，这些访客可以使用来宾访问的功能。

不需要通过复杂的验证，不用安装客户端，就可以正常的连续到网络中

受限的访问控制，确保公司内部资料不会被泄露。

支持上网行为审计，如有需要，可以对来宾开启网络行为控制。

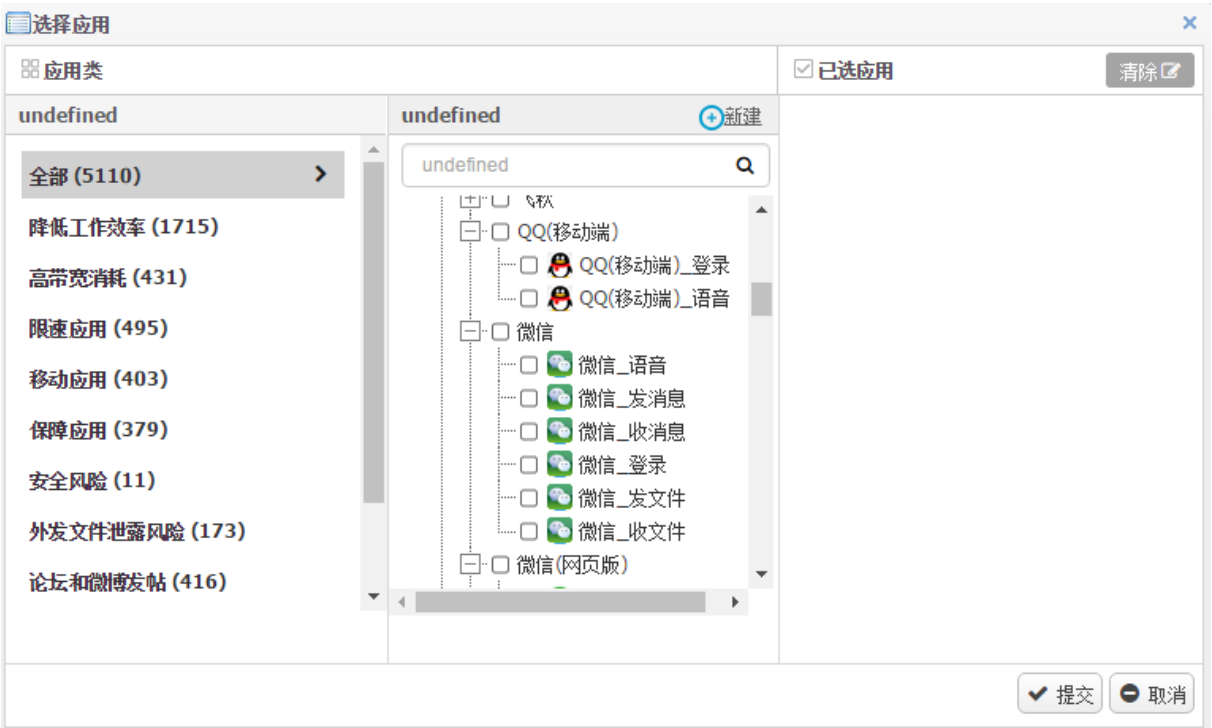
- 访问策略

随着互联网络科技的迅速发展，互联网络已经深入到千家万户，许多人的工作和生活已经离不开互联网了，上网已经成为不少人学习、工作和生活的一部分。网络应用的爆炸式增长和动态端口的新应用层出不穷，使得传统网关产品采用五元组的访问控制方式早已变得力不从心，而中数国科防火墙的出现让访问控制变得简单，基于 7 元组以及时间的访问控制策略，能有效的控制自然人、应用的访问控制。

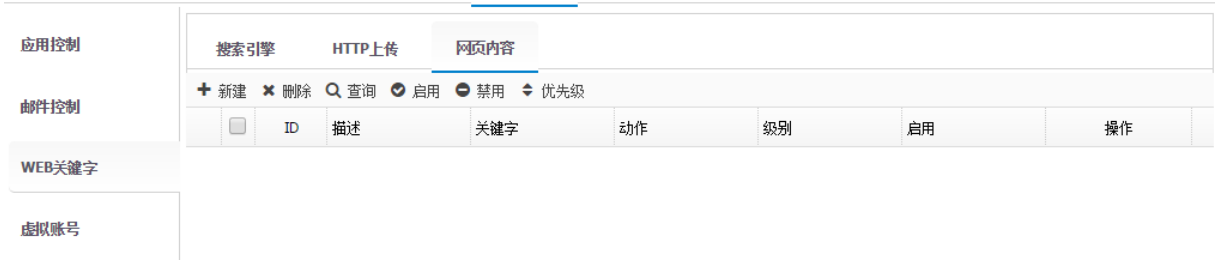
- 应用管控

中数国科防火墙通过对数据包的深入解析，匹配用户、IP 地址、时间、端口和终端类型等条件，针对应用、邮件、关键字、虚拟账号等维度进行精细化控制。

中数国科防火墙内置5000+应用行为特征，管理人员结合业务可制定人性化的上网权限。例如微信，可组合或单个控制微信的“语音”、“发消息”、“收消息”、“登录”、“发文件”和“收文件”等应用操作。

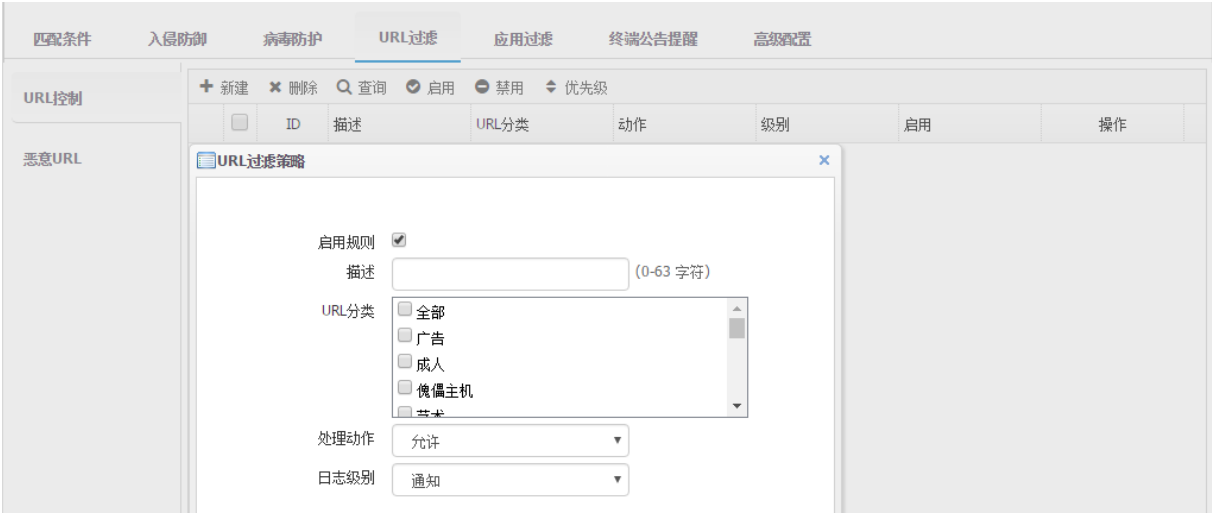


支持基于搜索行为、http协议上传行为和网页内容的关键字进行访问控制，有效屏蔽员工发表不良言论或访问违法网站，帮忙企业规范上网行为，规避法律风险。



- URL 管控

中数国科防火墙预置 57 类非加密 URL 种类，13 类加密 URL 种类，涵盖游戏、网上交易、成人、证券和在线聊天等主流网站，支持审计过滤加密网站和加密网站的搜索内容，全面控制用户的网站访问行为。



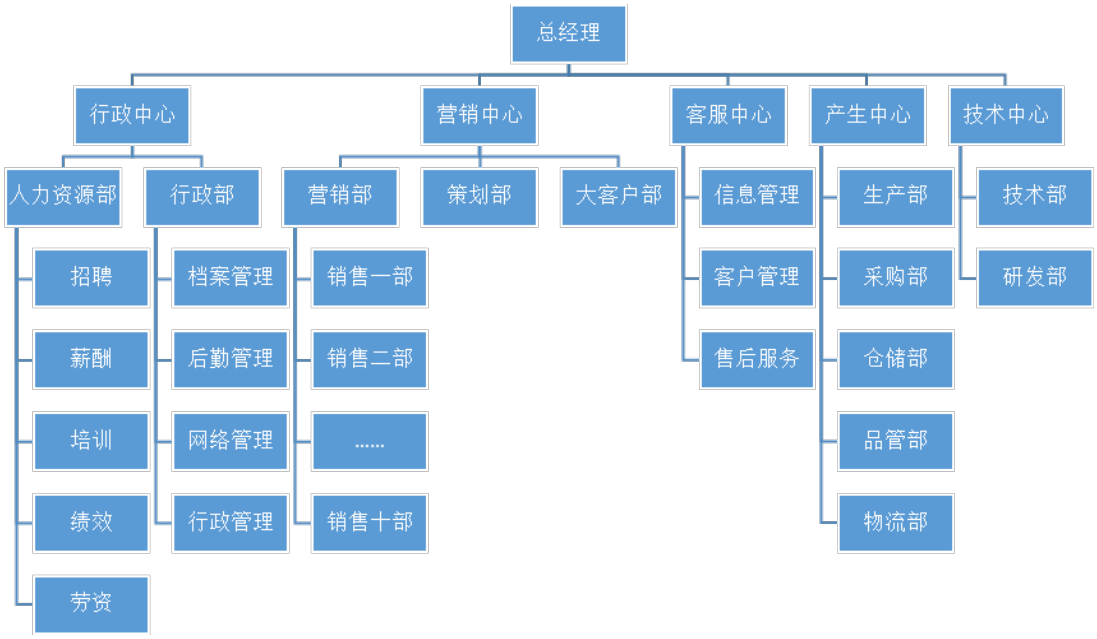
支持自定义 URL、恶意 URL、UR 白名单和 HTTPS 域名对象等内容，可灵活应对用户管理需求。

4.4.7 流量管理

中数国科防火墙使用了 DPI 和 DFI 融合应用识别技术，能够对流量进行深度解析，实现流量的细致化管控。

- 4 级通道管控

随着企业规模的不断扩大，网络带宽管理需要更精细的管理。对于大多数企业组织架构通常由中心、部门、子部门组成，如下图：



由上图可知，3 级流控只能满足到基层部门的流控制，对于部门下的应用控制已经明显力不从心，为此中数国科防火墙系列提出了 4 级流控概念，可将物理线路划分为若干虚拟线路和流控通道，可以满足大中型企业普遍带宽管理需求，策略主要支持基于用户/组、应用/组、服务、源地址等七元组的方式实现带宽管理细化，满足用户各种带宽管理的需求。如下图：

	线路名称	匹配条件					上行(出)			下行(入)			优先级	操作
		源地址	用户	服务	应用	时间	保障带宽	最大带宽	每IP	保障带宽	最大带宽	每IP		
1	某企业	-	-	-	-	-	↑100M	↑100M	-	↓100M	↓100M	-		-
2	营销中心	-	营销中心	-	所有应用	always	↑10M	↑50M	-	↓10M	↓50M	-	高	
3	大客户部	-	大客户部	-	所有应用	always	↑5M	↑20M	-	↓5M	↓20M	-	高	
4	策划部	-	策划部	-	所有应用	always	↑2M	↑20M	-	↓2M	↓20M	-	高	
5	营销部	-	营销部	-	所有应用	always	↑5M	↑40M	-	↓5M	↓40M	-	高	
6	销售一部	-	销售一部	-	所有应用	always	↑2M	↑10M	-	↓2M	↓5M	-	高	
7	P2P限制	-	所有用户	-	迅雷,迅	always	↑50kb	↑1M	-	↓50kb	↓1M	-	高	
8	邮件保障	-	所有用户	-	广东省邮	always	↑2M	↑5M	-	↓2M	↓5M	-	高	
9	默认通道(名	-	-	-	-	always	↑400kb	↑10M	-	↓400kb	↓5M	-	低	
10	销售二部	-	销售二部	-	所有应用	always	↑2M	↑5M	-	↓2M	↓5M	-	高	
11	销售三部	-	销售三部	-	所有应用	always	↑2M	↑5M	-	↓2M	↓5M	-	高	

- 弹性带宽分配

中数国科防火墙弹性带宽管理，可以使空闲通道不占用大量带宽，减少带宽的浪费，减少因空闲通道占用带宽，流量达到极限出现丢包现象。弹性带宽就是为了解决带宽浪费的问题，空闲通道会自动让出部分带宽给繁忙的通道。一旦空闲通道带宽不足时，将自动抢占回借用出去的带宽。此特性避免了带宽浪费，实现价值最大化。

- 流量、时长限额

用户体验至上的服务理念趋势下，企业为用户提供更灵活和细致的服务，已达到用户差分服务的效果。例如银行网点中，铜卡用户可免费上网 3 小时，银卡用户可免费上网 5 小时，金卡用户不限时上网。单纯的流控策略是无法满足企业的管理需求。

中数国科防火墙提供流量和在线时长限额的功能。通过预设用户的流量额度或者在线时长的阀值，设备统计该用户的对应参数，当对应参数超过设置阀值，设备立即对该用户进行惩罚，惩罚方式可选择禁止上网或流量限速。

中数国科防火墙可提供极为强大的管理网络流量的方法和手段，解决用户应用场景的流控细致化、差异化需求。

- 每 IP 或用户限速

中数国科防火墙采用了自动均分带宽，当在某个通道中只有一个用户使用时，该用户可以使用全部的带宽，如果有更多用户使用该通道时，管理员可设置将带宽按 IP 数量或用户数量均分，提升用户上网体验。

- 流控策略白名单

网络管理过程中，重要来宾和企业重要人员往往是不希望受流控策略的限制，中数国科防火墙根据用户需求，增加了流控策略白名单功能，白名单 IP 和用户将不受中数国科防火墙任何流量策略的限制，保障管理更加人性化。

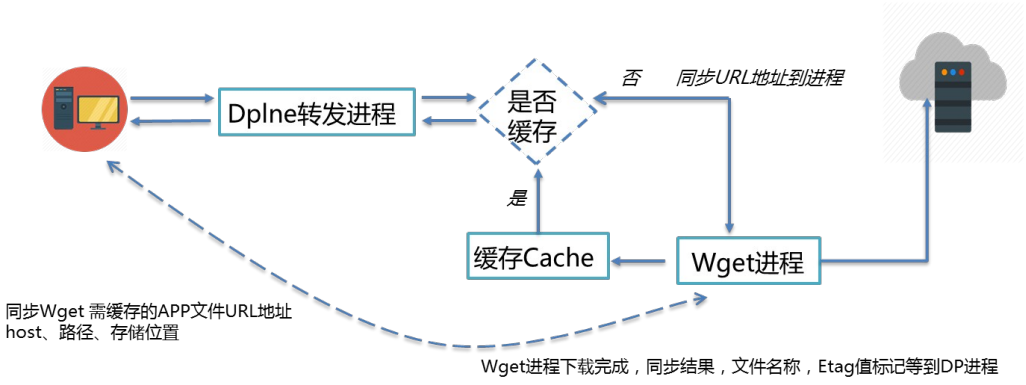
4.4.8 多广告推送

企业于投放通知或营销信息时，需向用户快速的下发消息，传统的消息传播方式速度慢且成本较高，非常不适用。中数国科防火墙提供多广告推送功能，可基于五元组维度向

用户访问的网页中插入弹窗页面，支持同时弹送 4 个页面，且弹送位置可自定义，具备极高的灵活性，复用已有网络线路，节省成本。在营销场景中，中数国科防火墙多广告推送功能极具优势。

4.4.9 应用缓存

中数国科防火墙创新的将 APP 缓存在设备本地，当用户下载时直接推送，几十 M 的文件只要几秒钟，极大的提升了带宽利用率的同时大大加速和提升了用户体验；具备精确缓存、模糊缓存特性，可解决 Android 平台升级 URL 变更频繁问题；支持动态缓存，自动更新 APP，无需管理员频繁手动上传，业界技术领先；中数国科防火墙应用缓存功能在低成本的投入下同时为客户的终端营销推广开辟了新的方向。

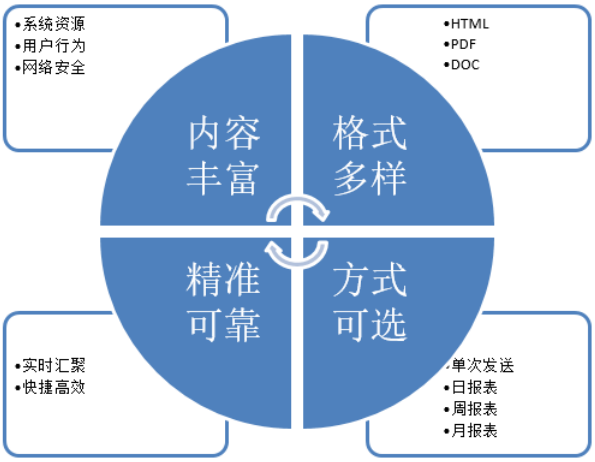


4.4.10 报表管理

中数国科防火墙为满足广泛而复杂的需求场景，运用领先的设计理念设计出强大的审计报表功能。高度可配置的报表管理功能，方便用户进行报表的分类管理、在线查看、定

时发布等。用户可自主添加新报表，及时满足大数据时代企业的快速业务变化和安全需求。针对中大型企业多人并发访问的场景，提供报表缓存，历史报表下载等功能，有效提高功能可用性。

统计报表可以定期将网络状况，用户行为，安全状况等汇报给相关管理人员，支持配置单次发送，周期性自动发送等，可将网络整体状况完整的呈现在管理人员面前。报表支持最常见的 HTML，PDF 等格式，可以跨设备无障碍浏览。



4.5 合规特性

4.5.1 SSL 网站解密

互联网时代，越来越多的网站启用 HTTPS，而随之而来的是员工利用这种加密方式泄露企业敏感信息的可能性也越来越大；并且由于 HTTPS 网页经过了加密，采用普通的流量分析方式是无法审计到访问行为的，企业是无法清晰准确的了解员工的工作状态和网络的运行状态。

为了保障企业有清晰的事后审计，保护企业机密，中数国科防火墙提供了 SSL 审计功能，中数国科防火墙采用特有的加密流量识别技术，能够对主流的加密网站、加密网站搜索记录、加密邮件，包括 Webmail 和客户端 Mail 等行为进行识别。管理员可以采用自定义

的方式，定向审计用户和加密网站，让网络运行情况更加清晰明了，做到管理规划有据可循、有的放矢。

- 工作原理

解析 DNS 报文，设备获取 DNS 回应报文，匹配解密策略的源地址组，解析出域名对应的 IP，往当前策略上添加 IP 域名信息。

转发报文流经设备，判断 TCP 443、995、993、465 端口进入解密策略匹配流程。依次匹配入接口、源地址对象、目的地址对象、若为 443 端口判断目的 IP 是否存在于 DNS 解析的 IP 中，若均匹配上报文送入 linux 内核，通过内核的 iptables redirect 功能重定向到本机代理进程。

代理进程建立双向 SSL 连接，并对数据进行加解密，解密后的数据封装 SKB 后送入审计流程。

- 解密策略

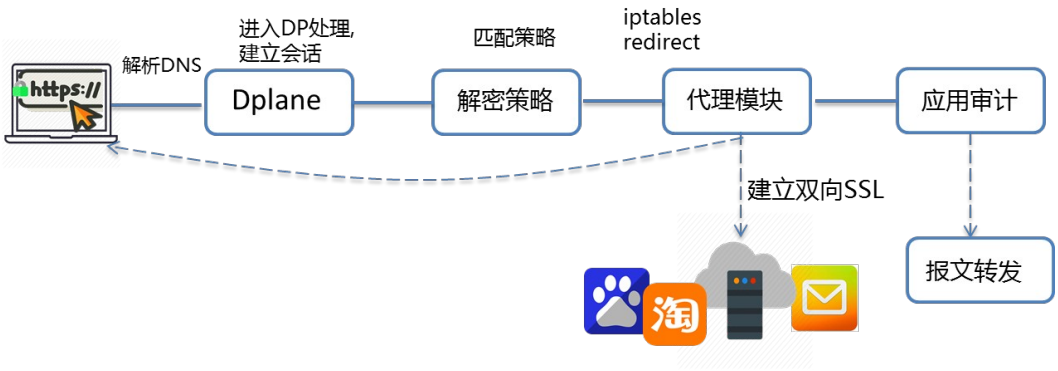
解密功能通过策略的方式检查哪些流量需要进入解密流程，匹配流程放在报文转发流程中，不需要对本机报文进行解密。

https 解密策略从四个维度判断是否处理当前报文：入接口、源地址、目的地址。域名

IP。

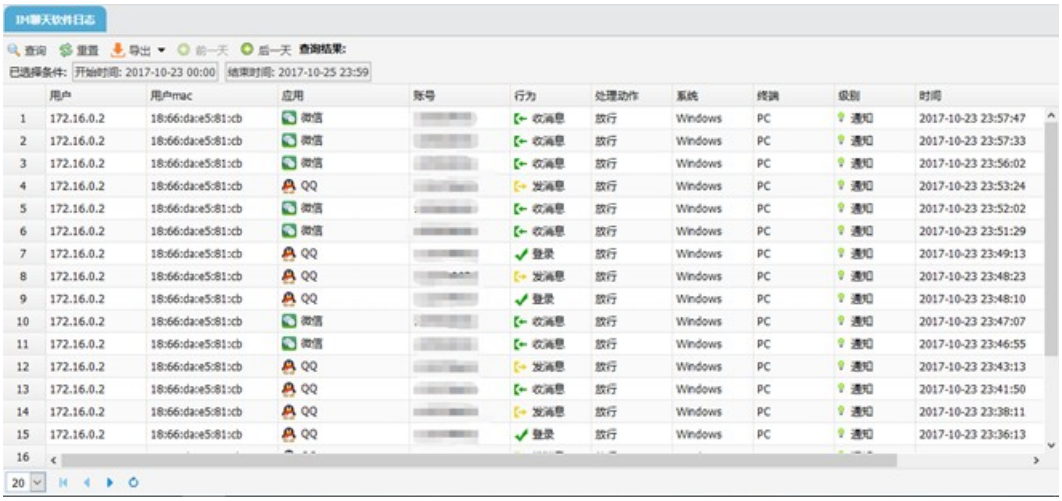
邮箱类解密策略从三个角度判断是否处理当前报文：入接口、源地址、目的地址。

网页版邮箱需匹配第四个维度-域名，该域名系统内置。



4.5.2 清晰事后审计

中数国科防火墙系列产品支持详细、清晰、易用的日志特性，可以全面记录审计用户上网行为、使用流量、访问网站、所用终端系统及设备类型平台等信息，可满足公安部要求的上网日志留存 6 个月的要求；日志支持定制化过滤器，可根据 IP 地址、认证用户、访问应用、访问 URL、发帖内容等要素进行搜索，让事后审计省时省力,可支持对 HTTPS、邮箱类解密策略的配置。同时，中数国科防火墙产品提供丰富美观的报表，以柱状图、饼状图、百分比等形式最直观地体现网络运行状况，让网络管理规划有据可循、有的放矢。



4.5.3 审计日志导出

随着国家净化互联网环境的趋势，对于网络监管力度不断增加；并且企业为了预防关键信息泄露，提升员工工作效率，对上网行为审计日志的需求愈加强烈。

中数国科防火墙支持按照自定义时间段导出日志，定期留存日志，实现对历史记录有据可查，保障内网信息安全。

4.6 运维特性

4.6.1 U盘零配置上线

企业的网络运维人员流动性较大，技术水平层次不齐，设备上线时，往往会面临较多技术问题，实施周期相对较长。管理员对不同局点的设备完成预配置，保存在U盘中（保存在U盘中的配置文件经过加密），开局人员拿着此U盘插入开局的设备，设备通过序列号获取U盘内的配置内容，完成设备的零配置上线工作。方便了设备的快速上线，极大的缩短了实施周期。

4.6.2 高可靠性

中数国科防火墙产品具备高可靠性，具体体现在软件和硬件两个方面。

- **软件部分**

  - 接口：接口支持最多配置200个从属IP，保障接口有充足的地址使用；
  - 路由：ISP路由、策略路由、负载均衡等路由，保障流量按需分流；
  - 策略：按需分配上网权限，保障网络正常运行；
  - 日志：攻击行为有迹可查；
  - HA：主主、主备模式保证网络持续运行，支持VPN级别的HA功能。中数国科防火墙除了支持主主、主备模式功能，同步配置、运行状态、会话、用户上线状态、特征库等内容之外，能够同步IPsec VPN状态。VPN对于电信级业务来说是命脉，如果普通设备的VPN断开重连，按照协议标准，算上DPD超时和IKE建立的时间，估计在100秒到120秒，其中的时间成本是企业无法承担的。中数国科防火墙完美的解决了这个问题，主备设备同步VPN的状态，主备切换时，零丢包零中断，保障用户的关键业务不中断，极大的避免了企业的损失；
  - 配置备份：设备的关键配置自定义备份，支持多配置切换，可保障设备快

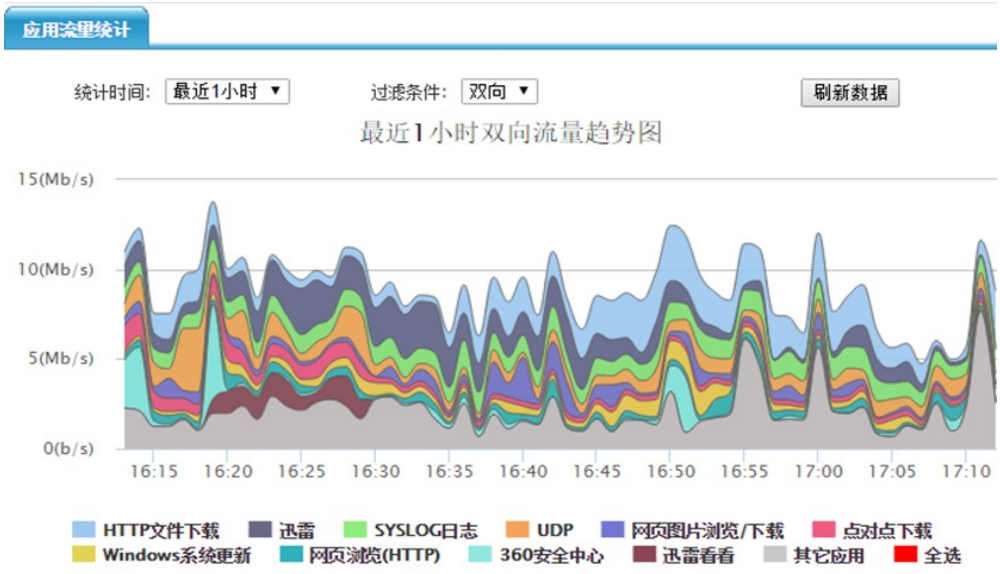
速恢复；

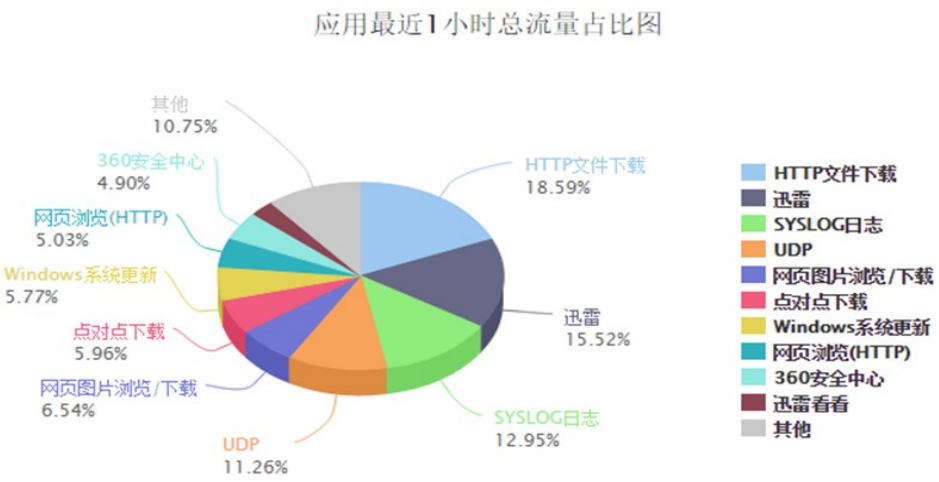
➢ **硬件部分**

- 接口：接口数量丰富；
- 电源：提供冗余电源；
- 风扇：提供冗余风扇；
- Bypass：支持硬件 Bypass

4.6.3 应用和用户流量统计

企业网络是业务基础，所以网络管理员往往会每个月汇报网络报告，中数国科防火墙提供强大的应用识别，用户可以通过应用流量统计查看到网络中的应用流量组成，准确了解网络的使用情况，为网络情况提供重要依据。

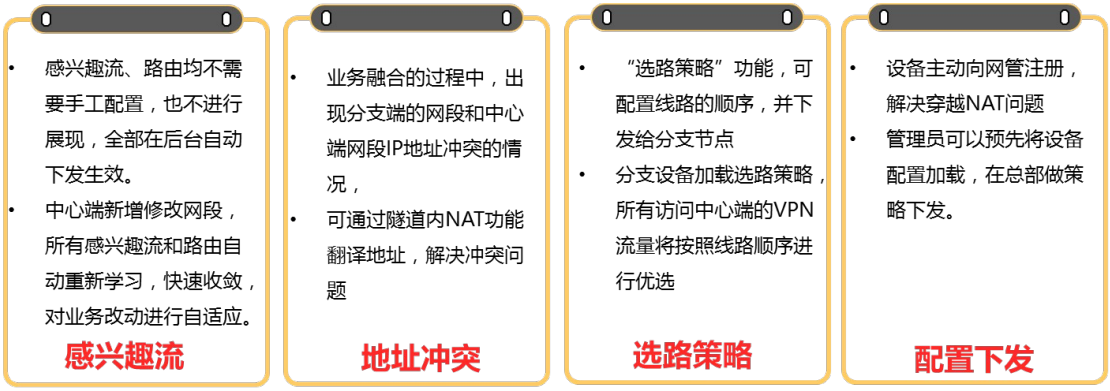




4.6.4 快易 IPsecVPN

中数国科防火墙的 IPsec VPN 模块具有业界领先技术，在复杂网络环境下大大简化了管理员的维护工作量，配合集中管理和日志分析平台，可实现 IPsec VPN 快速零配置上线。快速对接模块式下，隧道接口感兴趣流等可无需配置自动协商，整个 IPsec VPN 网络全自动收敛，自适应多线路，完美的解决了分支运维能力弱的问题。而独创的主备切换 0 丢包技术，可实现 TCP 业务不中断，完美的解决 HA 切换业务中断的问题，可让管理员高枕无忧。

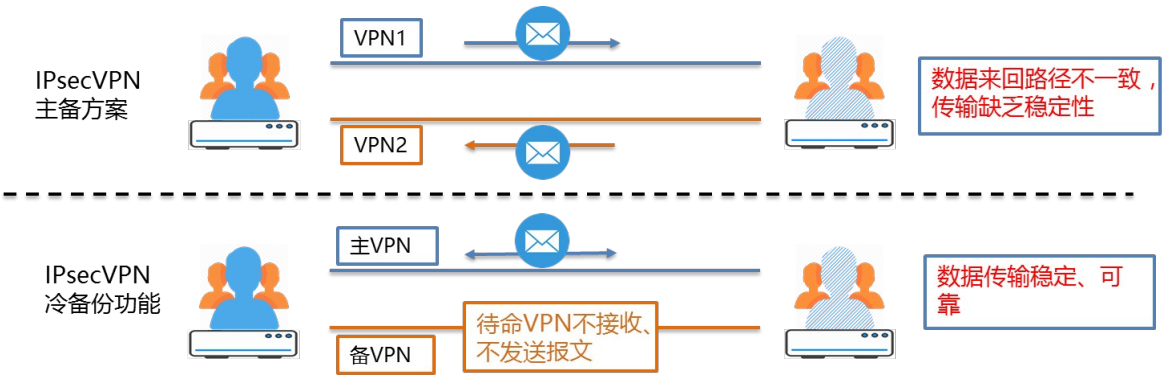
对金融、能源、交通等行业一些分散型的营业网点，对于业务连续性以及内网数据安全要求非常高。在租用运营商的固网光纤专线作为主链路的同时，还需一条安全稳定的备份链路以应对突发状况，专线成本高、灵活性差的缺点暴露无遗；中数国科防火墙支持 4G 网络并支持 4G IPsec VPN 加密连接进行链路备份。连接提供按需拨号，无需改变原有网络架构，在主线路故障时主动承接和中心端的网络加密通信，具备数据完整性、数据传输安全、高性价比、网络无改变等特性。



4.6.5 IPsecVPN 冷备份

IPsecVPN 一般会承载客户关键数据，业界为了保障其可靠性，会使用 IPsecVPN 主备方案。但该方案在特殊场景中由于主备链路的 SA 阶段均处于 UP 状态，所以会导致数据包来回路径不一致，隧道稳定性较差的问题。

中数国科防火墙创新性的推出了 IPsecVPN 冷备份功能，该功能设定待命 VPN 隧道不接受和发送报文，避免了数据包来回路径的问题。中数国科防火墙提供数据加密的同时，提升了数据传输的可靠性，避免业务损失。

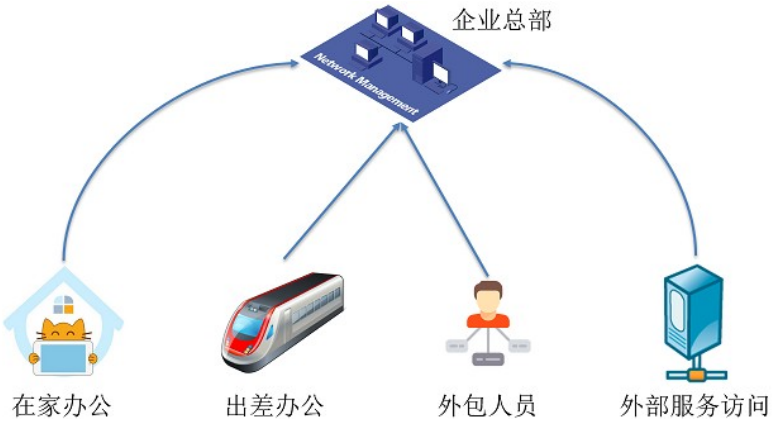


4.6.6 SSL VPN 远程办公

中数国科防火墙的 SSL VPN 功能比较适合用于移动用户的远程接入，适用于 Client – Site 场景。随着信息技术的发展，加剧了企业内部员工及合作伙伴间的信息交互，如何通过互联网访问企业内部系统，实现远程办公成为企业发展的必然要求。

中数国科防火墙的 SSL VPN 功能是基于 OpenSSL 加密库中的 SSLv3/TLSv1 协议函式库实现的一种数据封装技术。包括虚拟网卡，SSL 加密隧道等一系列加密技术，确保通信中数据安全。虚拟网卡是使用网络底层编程技术实现的一个驱动软件，安装后在主机上多出现一个网卡，可以像其它网卡一样进行配置。服务程序可以在应用层打开虚拟网卡，如果应用软件向虚拟网卡发送数据，则服务程序可以读取到该数据，如果服务程序写合适的数据到虚拟网卡，应用软件也可以接收得到。在 SSL VPN 中，如果用户访问一个远程的虚拟地址（属于虚拟网卡配用的地址系列，区别于真实地址），则操作系统会通过路由机制将数据包（TUN 模式）或数据帧（TAP 模式）发送到虚拟网卡上，服务程序接收该数据并进行相应的处理后，通过 SOCKET 从外网上发送出去，远程服务程序通过 SOCKET 从外网上接收数据，并进行相应的处理后，发送给虚拟网卡，则应用软件可以接收到，完成了一个单向传输的过程，反之亦然。

可以说，SSL VPN 是当前业界解决远程用户访问公司数据最安全简单的解决技术，任何安装了 SSL VPN 客户端的用户电脑均可使用 SSL VPN 通过公网方便地远程接入企业内网相比于 IPSec VPN，SSL VPN 主要的优势是配置简单，性能强大，安全稳定。



4.6.7 服务质量管理

网站和关键服务器的链路质量是企业重点关注的问题之一，如何衡量服务器提供的业务质量，是网络维护人员的值得思考的问题。

中数国科防火墙的服务质量探测，使用 PING、DNS、TCP 等探测协议，检测目标地址的成功率、延时等数据，帮忙网管及时的发现服务质量较差的服务，从整体上展示关键服务的状态，达到优化整体网络，提升关键业务的服务质量。

4.6.8 端口镜像

中数国科防火墙在审计所经过流量的同时，可提供端口镜像功能，支持将对应接口按照入流量、出流量或双向流量等规则类型进行流量镜像，提供流量分析功能，帮忙网络管理员提供运维工具，并节省一台交换机的成本。

4.6.9 多配置切换

总分型连锁场景中，网络运维力量相对较弱，灾备情况时，用户的关键业务无法快速切换，正常业务无法得到保障。中数国科防火墙支持通过命令行或者预留的 API 接口切换配置文件，设备的业务数据和访问规则快速切换，保障网络的正常可用。

4.6.10 管理端口自定义

当前较多网络设备使用默认端口和默认密码， 极易被黑客攻击，造成经济损失。中数国科防火墙提供管理端口自定义功能，管理员可配置非常用端口号，增强设备的安全性，避免经济损失。

4.6.11 业务告警

中数国科防火墙支持业务告警功能，可针对 CPU、内存、会话、整机流量和 IPsecVPN

连接断开等关键设备内容进行告警，提供页面弹窗和邮件告警提醒，快速定位故障点，及时向网络管理提供设备状态，助力运维。

4.6.12 集中管理与数据分析系统

随着网络规模、业务应用不断增长，网络安全时间逐渐增加，在网络安全建设方面，用户往往通过多台安全设备，实现对信息网络的分域分级保护。通常，网络安全产品多聚焦在安全策略上，通过策略缓解网络威胁。但是在缺乏有效集中安全管理手段的前提下，部署多台安全设备总是孤立的进行安全检测和控制，为了方便网络管理员对中数国科防火墙进行操作和维护，推出了数据中心与集中网管，中数国科防火墙日志分析与管理平台。中数国科防火墙日志分析与管理平台是提供对中数国科防火墙的集中监控、配置和升级，并且对上报的安全相关信息收集存储，通过数据发掘提供详尽灵活的统计图、报表，从而辅助管理员进行安全信息审计。利用日志分析与管理平台，管理员可以高效地管理各中数国科防火墙设备，全面掌握网络的整体安全状况。

中数国科防火墙日志分析与管理平台通过 API 接口与中数国科防火墙设备进行交互通信、管理与维护。具有设备注册与管理、策略管理、日志收集与分析、统计报表等等一系列功能。在技术实现上，中数国科防火墙日志分析与管理平台采用高性能数据仓库，具有“高性能查询”、“高数据压缩比”、“基于列存储”、“定期聚合，快速响应”、“高效数据导入”等等特性。

- 采用高性能数据存储和查询

中数国科防火墙日志分析与管理平台采用高性能数据仓库，此数据仓库是一款基于网格技术的列式数据库。简单易用，快速安装部署，使用中无需复杂操作，能大幅度减少管理工作；在应对 50TB 甚至更多数据量进行多并发复杂查询时，更能够显示出令人惊叹的速度。

中数国科防火墙日志分析与管理平台支持 TB 级原始数据量的高性能查询，大数据量查询性能强劲、稳定：查询性能高，如百万、千万、亿级记录数条件下，同等的 SELECT 查

询语句，速度比 MyISAM、InnoDB 等普通的 MySQL 存储引擎快 5～60 倍。高效查询主要依赖特殊设计的存储结构对查询的优化，帮助用户快速定位网络问题，查询各种条件的审计检索。

高数据压缩比，能够帮助用户节省存储成本，支持普通 X86 服务器，无需专用硬件设备和存储，在某实验局没有采用日志分析与管理平台前日志存储 1 个月产生 500G 数据，而采用中数国科防火墙日志分析与管理平台后，数据 1 个月存储减少至 60 多 G，这样大大节省了用户的存储硬件成本。

● 深层次数据挖据分析

中数国科防火墙日志分析与管理平台采用了先进的数据挖掘分析技术，从收集到的大量数据当中进行深层的数据挖掘及分析，该子系统由日志代理、日志审计中心、日志数据库、审计系统管理器、日志分析中心五个部分组成。日志代理负责收集区域内各种操作系统、网络安全设备、应用程序的日志信息，过滤后发送给日志审计中心处理。日志审计中心负责接受区域内日志代理和各种安全设备、系统转发的日志信息，集中保存在日志数据库，日志分析中心负责对日志数据进行深度挖掘。

日志数据的深度分析工作主要由日志分析中心来完成。日志分析中心首先通过 ETL 处理，利用专用的数据抽取工具，将日志数据按照定义的规则，通过复杂的抽取、转换、清洗及聚合，最后装载至数据仓库 DW 中，生成满足多维分析的数据仓库数据，即事实表和维表。通过 OLAP 多维分析技术和 BI 前端展现工具，提供针对日志数据仓库的日常查询、统计报表、OLAP 分析、数据挖掘、KPI 统计分析和监控告警等决策分析功能，并将结果通过 Web/GUI 方式展现给用户。

数据仓库是在企业管理和决策中面向主题的、集成的、与时间相关的、不可修改的数据集合。与其他数据库应用不同的是数据仓库更像一种过程，对分布在企业内部各处的业务数据的集合、加工和分析的过程。

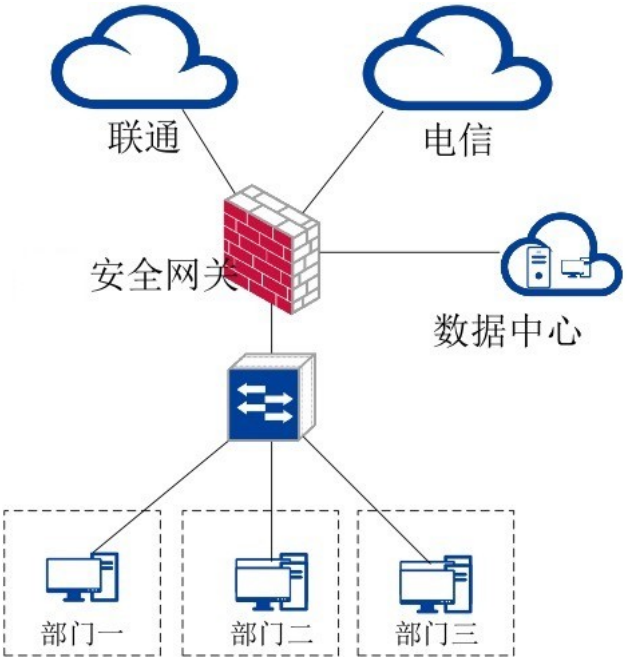
数据仓库中包含 ETL、数据模型、信息展现等主要关键技术。ETL 是数据抽取（Extract）、清洗（Cleaning）、转换（Transform）、装载（Load）的过程。它是构建数

据仓库的重要一环，用户从数据源抽取出所需的数据，经过数据清洗,最终按照预先定义好的数据仓库模型，将数据加载到数据仓库中去。数据模型的重要性在于对数据做标准化定义，实现统一的编码、统一的分类和组织。标准化定义的内容包括：标准代码统一、业务术语统一。ETL 依照模型进行初始加载、增量加载、缓慢增长维、慢速变化维、事实表加载等数据集成，并根据业务需求制定相应的加载策略、刷新策略、汇总策略、维护策略。

五、典型组网应用

5.1 企业边界网关部署

- 适用于大中型企业用户，以网关方式在线部署于网络出口
- 抵御内外网的入侵防御，对网络中的病毒进行过滤查杀。
- 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽
- 支持 VPN/MPLS/ VLAN/PPPoE 等复杂网络环境；支持设备本地日志记录和集中分析处理，可多台分布式部署统一管理

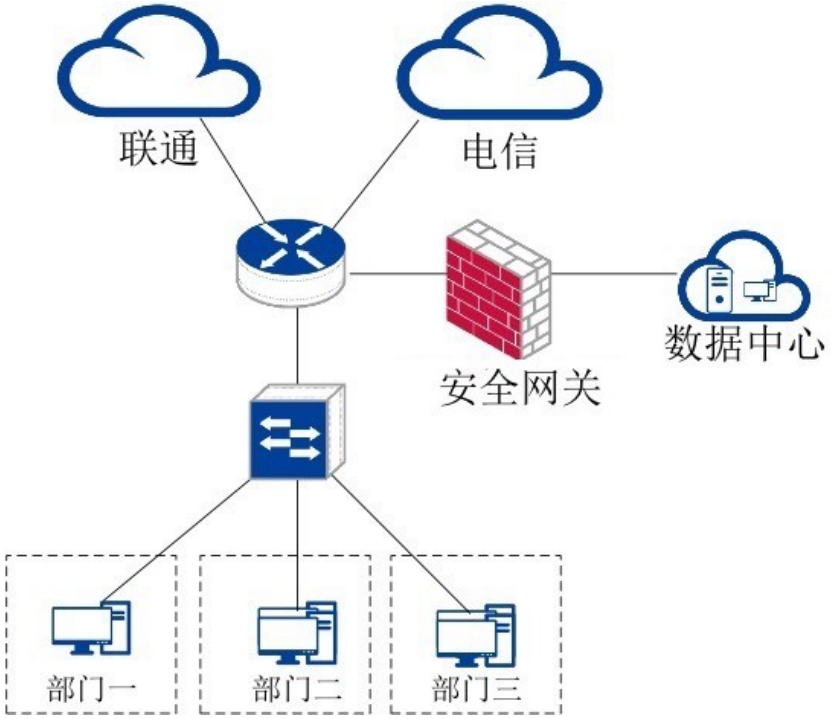


5.2 关键业务串行防护

● 适用于数据中心机房，可灵活的以串行路由或者透明方式部署于数据中心机房出口，根据实际网络环境署简单；

● 通过中数国科防火墙的 AV 和 IPS 功能的保护，除了对外网针对数据中心的暴力攻击能有效阻挡之外，还可对所有进出的封包均进行详细的七层分析，让黑客利用合法方式进行非法存取的攻击将无所遁形；

● 支持设备本地日志记录，日志也可发送到集中管理和数据分析中心处理，并可进行数据分析。



5.3 总分型网络集中部署

● 适用于大型总分型网络，以边界设备方式部署在总部和分支网络的出口；

● 中数国科防火墙可以为总部和分支提供 AV 和 IPS 保护，有效的抵御各种网络威胁；

● IPsec VPN 配置简单易用，零配置上线，全自动收敛，几乎零配置，自适应多线路，完美地解决分支运维能力弱的问题；

● 支持设备本地日志记录，日志也可发送到集中管理和数据分析中心处理，可多台分布式部署统一管理，并可进行大数据分析。