安恒信息
DAS-security 安全中国

明御®安全网关（DAS-Gateway）

技术白皮书

文档版本：02

发布日期：2021-09-17

文档说明

产品名称		明御®安全网关（DAS-Gateway）	
拟制人	AH2898（基础安全-DAS-Gateway）	**评审组**	AH6861（远程技术支持-标准文档）
发布人	AH5888（远程技术支持-标准文档）	**备注**	受控文档

修订记录

日期	修订版本	修改记录	修改人
2020-09-22	01	初次发布	AH5506（远程技术支持-标准文档）
2021-09-17	02	◆ 产品变更名称为 DAS-Gateway ◆ 更新产品图标	AH6861（远程技术支持-标准文档）

目 录

前言

概述

感谢您选择安恒信息的网络安全产品。本手册对安恒信息明御®安全网关（DAS-Gateway）（以下简称“DAS-Gateway”）进行了全面的介绍，主要包括概述、产品价值、产品架构及功能、典型应用场景。

手册所提供的内容仅具备一般性的指导意义，并不确保涵盖所有型号产品的所有使用场景。因版本升级、设备型号、配置文件不同等原因，手册中所提供的内容与用户使用的实际设备界面可能不一致，请以用户设备界面的实际信息为准，手册中不再针对前述情况造成的差异一一说明。

出于功能介绍及配置示例的需要，手册中可能会使用 IP 地址、网址、域名等。如无特殊说明上述内容均为示意，不指代任何实际意义。

预期读者

本文档主要适用于期望了解 DAS-Gateway 功能特性及应用场景的读者，包括系统管理员、网络管理员、技术爱好者等。本文假设读者对以下领域的知识有一定了解：

- TCP/IP、SNMP 等基础网络通讯协议。
- 网络安全相关知识，包括 DDoS、SQL 注入、目录遍历、暴力破解等常见攻击原理及防护手段。
- 安全防护策略、NAT 地址转换、VPN、各类路由协议的基本工作原理和配置。

获得帮助

使用过程中如遇任何问题，请致电服务热线 400-6059-110。

请访问安恒社区 https://bbs.dbappsecurity.com.cn 获取更多文档。

联系信息

地址：浙江省杭州市滨江区西兴街道联慧街 188 号安恒大厦

邮编：310052

电话：0571-88380999　传真：0571-28863666

官网：http://www.dbappsecurity.com.cn

邮箱：400-doc@dbappsecurity.com.cn

1. 概述

随着互联网行业的迅猛发展，许多部门和企业的关键业务活动越来越多的依赖于网络，各种网络攻击、信息安全事件发生率在不断攀升，信息系统安全已经成为关系到政务、教育、商业甚至军事活动能否顺利开展的重要因素。

DAS-Gateway 秉持安全可视、简单有效的理念，以资产为视角，构建全流程防御的下一代安全防护体系。是集传统防火墙、入侵防御、病毒防护、上网行为管控、VPN、威胁情报等安全模块于一体的智慧化安全网关。产品采用高性能多核架构，搭载接口丰富的硬件平台，支持常见的路由协议，并支持双机热备等高可用特性，保障业务处理高效可靠，场景支撑灵活全面。

2. 产品价值

- **资产风险识别，安全防护无死角**

  DAS-Gateway 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。通过以资产为视角对各种安全事件进行关联分析统计，便于管理员定位风险主机，并根据关联的威胁事件进行针对性的防护。

- **策略精确分析，策略管理更简单**

  DAS-Gateway 通过策略分析引擎梳理问题策略，计算策略精确度，给出策略调整建议。让每一条策略直观可视，更易于使用和维护管理。

- **全网威胁情报，未知风险可防护**

  DAS-Gateway 基于大数据关联分析得到的威胁情报，可以推动管理员快速发现内网未知威胁、0day 攻击等，准确发现内部失陷主机，结合威胁情报提供的丰富上下文信息，帮助管理员提前做好安全防范、快速进行攻击检测与响应。

- **攻击链分析，事后回溯更清晰**

  DAS-Gateway 通过对检测出的威胁事件日志进行汇总分析整理，以攻击链的形式可视化展示攻击者的入侵路径、入侵程度等。精确、简单、统一、有效，便于管理员对内部网络进行分析，对攻击事件进行取证溯源。

- **全流程防御，闭环体系更安全**

  事前感知预警、事中防护响应、事后分析取证溯源，并持续检测分析，帮助企业大幅度降低安全事件产生的不良影响。

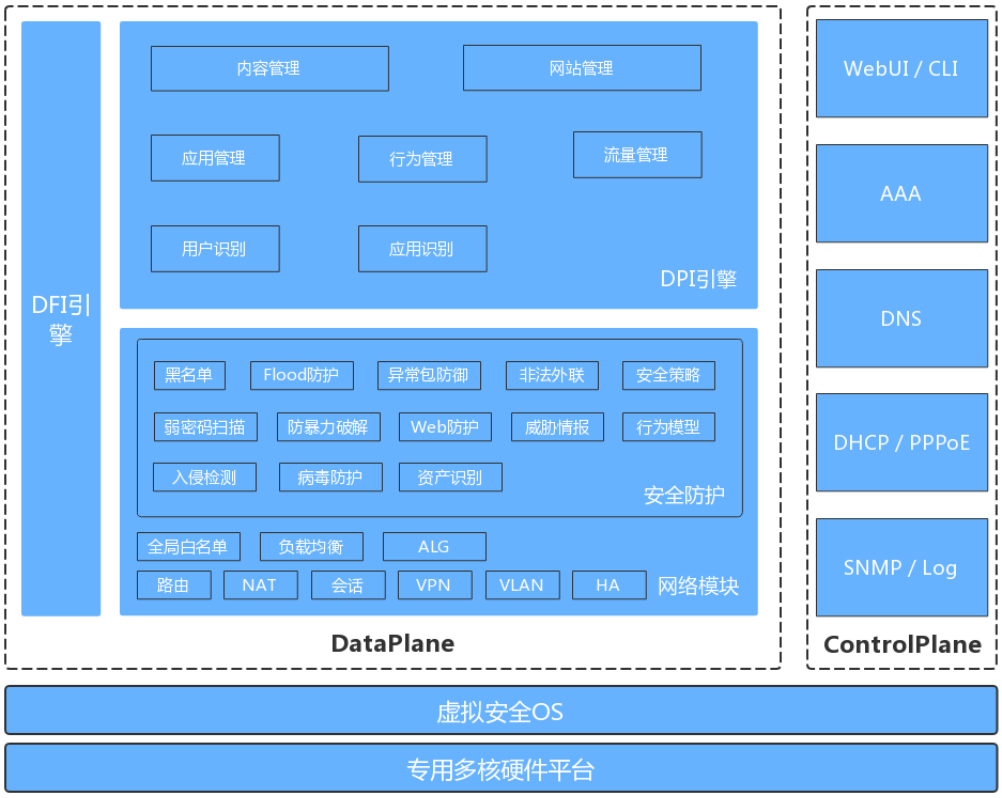
- **协同防御，避免产品孤岛**

  DAS-Gateway 与安恒多个产品形成深度联动能力，在通用网络安全、物联网场景构建可落地的协调防御方案。

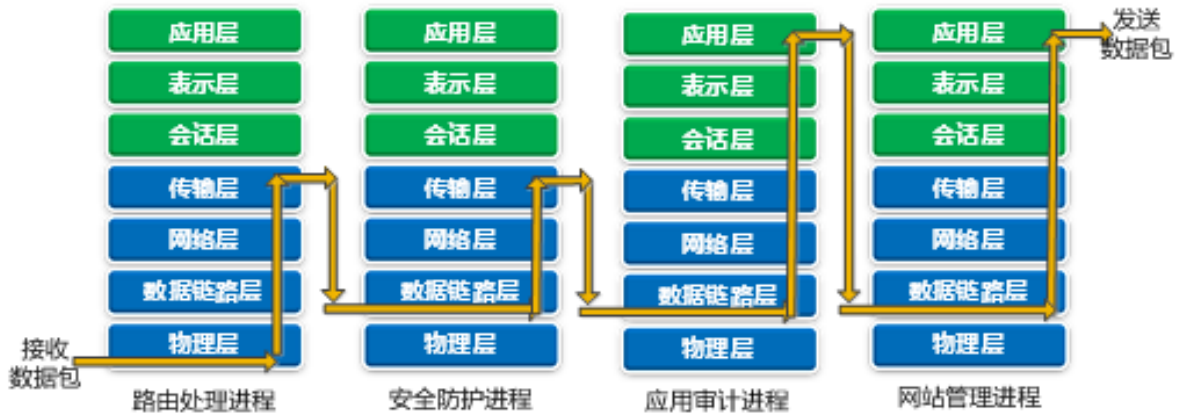
3. 产品架构及功能

3.1 系统架构设计

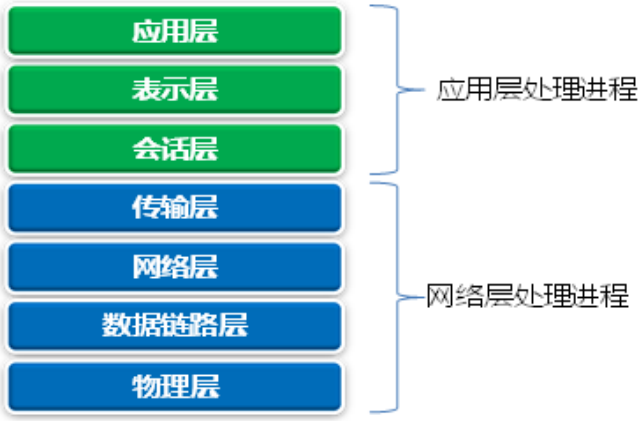
DAS-Gateway 采用先进的多核硬件架构、高效的并行调度算法和内存管理机制，提高了流量处理性能。另外，将 CPU 处理的数据根据其特性分为 Data Plane（数据面）和 Control Plane（控制面）两类，简称 DP 和 CP。在多核系统中少部分 CPU 专职于 CP 工作，大部分 CPU 专职于 DP 工作。这样就避免了因系统调度导致设备转发性能降级或者无法响应管理操作等现象。具体工作于 DP 和 CP 的 CPU 分布，根据用户场景定义。



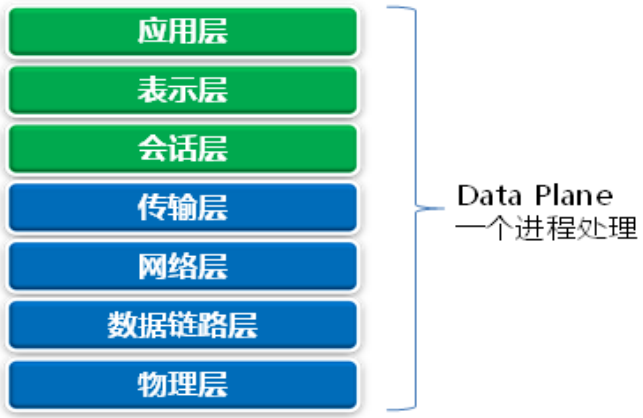
传统的网关设备为了降低设计和开发难度，会将各功能模块对应不同的进程，数据包每通过一个模块都要对数据进行解析。增加了数据包在系统停留的时间，从而造成了网络延迟大的问题。



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。



DAS-Gateway 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。



3.2 网络特性

3.2.1 支持多种部署方式

DAS-Gateway 支持多种部署方式，可以灵活地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。

3.2.2 全面支持 IPv6 网络

DAS-Gateway 已全面支持 IPv6 网络，基础功能如 SNMPv6、NTPv6、策略路由 v6、DNS 代理 v6、DHCPv6、PPPoEv6、NAT46、NAT64、NAT66 等。安全功能如 ND 攻击防护、IPS、AV、Web 防护等都已支持 IPv6 网络。

3.2.3 路由功能

DAS-Gateway 支持丰富的路由协议，包括静态路由、RIP、OSPF 等动态路由协议，支持路由链路探测等基础功能，同时还支持基于七元组的策略路由。预置中国电信（China Telecom）、中国联通（China Unicom）、教育网（China Education）、中国移动（China Mobile）四个主流运营商的地址库的 ISP 路由，另支持自定义增加 ISP 条目。DAS-Gateway 可满足用户绝大部分场景下的路由功能的需求。

3.2.4 地址转化

DAS-Gateway 对 NAT 功能进行了优化。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 能够适用于用户规模大、承载流量大、业务稳定性要求高的应用场景。

3.2.5 负载均衡

3.2.5.1 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，多出口在提升了网络出口稳

定性的同时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。以上诸多问题通过 DAS-Gateway 的链路负载均衡功能即可迎刃而解。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，DAS-Gateway 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
  DAS-Gateway 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，从而达到高效利用出口链路带宽的目的。
- 智能应用路由
  DAS-Gateway 能识别应用，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 请求得到快速、稳定的响应，大幅度提升客户的上网体验。

3.2.5.2 服务器负载均衡

DAS-Gateway 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。

DAS-Gateway 能够实现在多台服务器同时工作的情况下，即时动态检查各个服务器的工作状态，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。

DAS-Gateway 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：可保持同一用户的所有访问会话分配至同一台服务器进行处理

3.2.6 动态域名服务

DDNS（Dynamic Domain Name Server，动态域名服务）是将动态 IP 地址映射到一个固定的域名解析服务上，节点每次连接网络的时候客户端程序就会通过信息传递把该节点的动态 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 DDNS 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），用户若想在网络上发布自己的网站，利用 DNS 提供的域名和 IP 地址的绑定会导致节点的 IP 地址发生变化时，DNS Server 无法动态地更新域名和 IP 地址的映射关系，动态域名服务提供了解决方案。它可以自动更新节点每次变化的浮动 IP，然后将其与网络域名相对应，这样其他上网用户就可以通过域名访问。

DAS-Gateway 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。

3.2.7 VPN

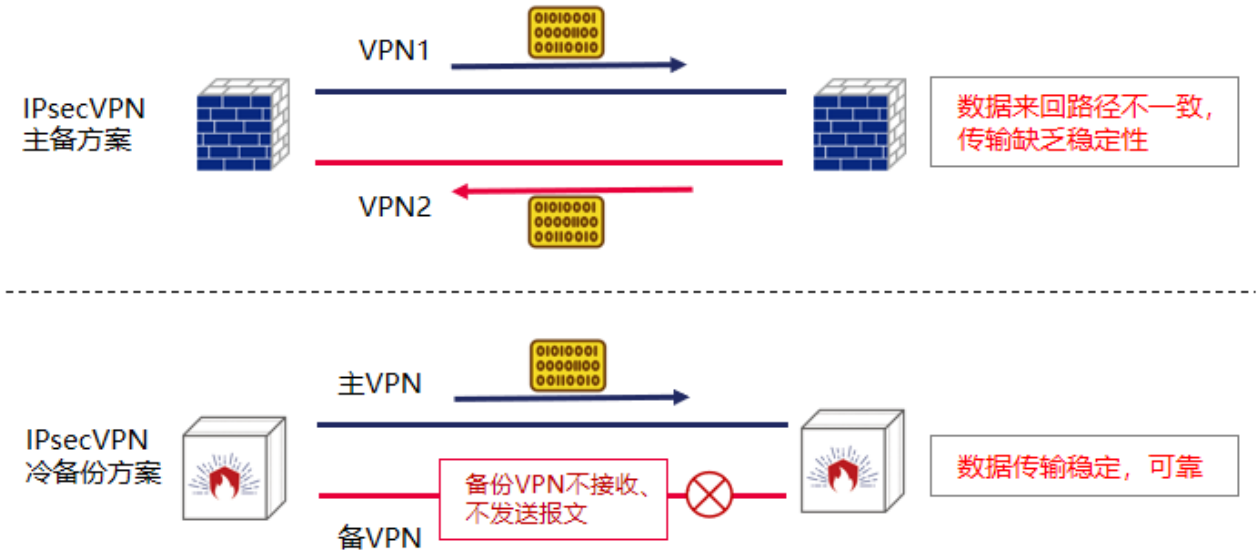
DAS-Gateway 支持常见的 VPN 使用场景，支持多种 VPN 隧道业务，包括 IPsec、GRE、SSL VPN 等。

3.2.7.1 IPsec VPN

IPsec 是 VPN 中使用最为广泛的协议栈。IPsec 不是一个单独的协议，它给出了应用于 IP 层上网络数据安全的一整套体系结构。该体系结构包括认证头协议（Authentication Header）、封装安全负载协议（Encapsulating Security Payload）、密钥管理协议（Internet Key Exchange）和用于网络认证及加密的一些算法等。IPsec 规定了如何在对等体之间选择安全协议、确定安全算法和密钥交换，向上提供了访问控制、数据源认证、数据加密等网络安全服务。

- **IPsec VPN 冷备份**

  IPsec VPN 一般会承载客户关键数据，业界为了保障其可靠性，会使用 IPsec VPN 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。DAS-Gateway 创新性推出了 IPsec VPN 冷备份功能，该功能设定待命 VPN 隧道不接收和发送报文，避免了数据包来回路径的问题。DAS-Gateway 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。



◆ **IPsec VPN 快速零配置上线**

DAS-Gateway 的 IPsec VPN 除了支持复杂的第三方对接之外，还可实现 IPsec VPN 快速零配置上线。快速对接模式下，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，解决分支运维能力弱的问题。而主备切换零丢包技术，可实现 TCP 业务不中断，解决 HA 切换业务中断的问题，可让管理员高枕无忧。

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。DAS-Gateway 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、高性价比等特性，同时无需变更网络拓扑。

3.2.7.2 SSL VPN

DAS-Gateway 的 SSL VPN 功能适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，企业内部员工及合作伙伴间的信息交互逐渐频繁，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。

DAS-Gateway 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。通过虚拟网卡，SSL 加密隧道等一系列加密技术，确保通信过程中数据安全。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。

SSL VPN 是当前业界解决远程用户访问公司数据最安全、最简单的技术手段，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。

3.3 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。

3.3.1 一体化安全策略

DAS-Gateway 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。

3.3.2 策略分析

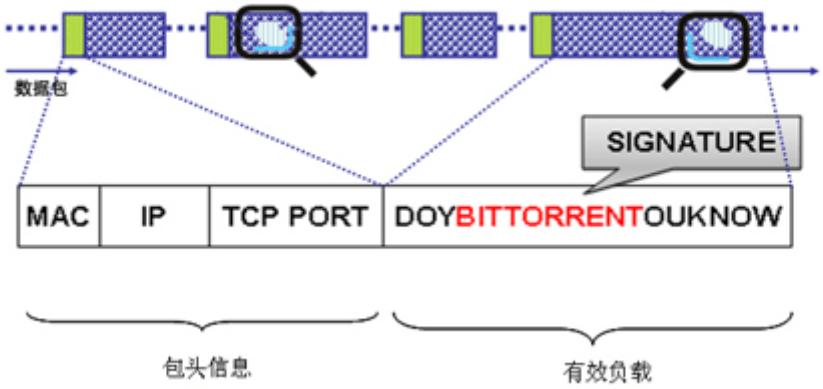
防火墙规则及策略的配置是防火墙使用过程最大的难题。当前网络环境的复杂性越来越高，网络服务与网络终端越来越多样，相应的防火墙设备就需要更多、更复杂的控制策略。这些控制策略经过一段时间的积累，往往会造成老策略不敢删，新策略不断增加，单台防火墙积累成千上万的策略，极大降低设备性能和用户体验。

DAS-Gateway 支持一键分析当前的冲突、冗余、隐藏、合并、过期和空策略等，并给出调整建议，使每一条策略都直观可视。一定程度上帮助安全管理人员优化访问控制列表，满足访问控制规则数量最小化的等保 2.0 强制要求。让防火墙更易于使用、便于维护管理。

3.3.3 入侵防御

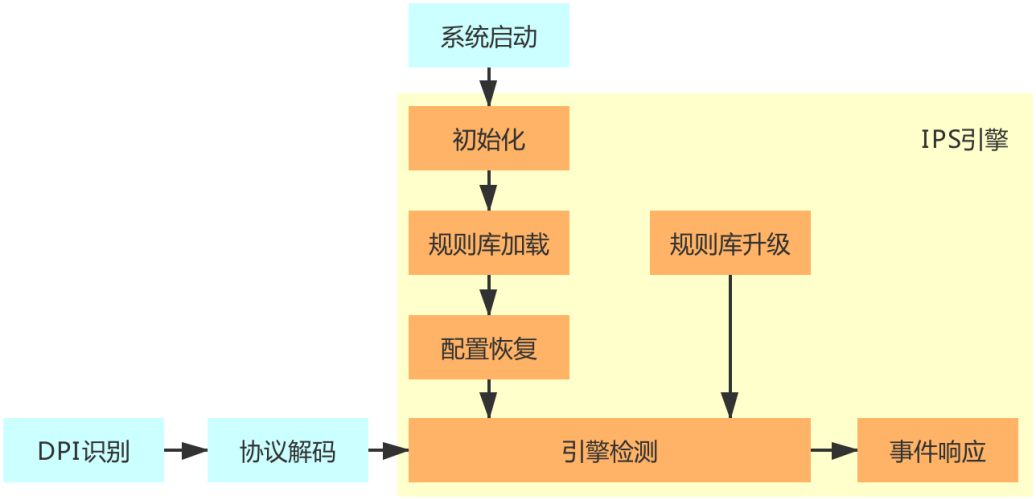
Gartner 报告指出企业面临的网络攻击中 70%来自应用层，传统防火墙以及应用层安全设备功能单一，面对复杂的应用层攻击捉襟见肘。安恒信息经过多年的技术沉淀，打造了一支资深的攻击特征库团队和安全服务团队。在蠕虫、后门、木马、间谍软件、Web 攻击、拒绝服务等攻击的防御方面具备了完善的检测、阻断、限流、审计报警等防御手段，并随时关注业界最新发现的安全漏洞和接收全球用户反馈的攻击特征，在第一时间做出响应和提供更新，实时完善攻击特征库，提供及时、全面的入侵防御策略。

入侵防御安全引擎的功能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，从而能够通过非授的方式权操作后台数据库，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 服务器操作系统等目的。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。



- 多种预定义攻击特征
- 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、可疑行为、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、欺骗劫持等
- 保证基础网络安全
- 分级事件及操作配置

- 虚拟补丁管理

部分攻击者利用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此类攻击因而难以检测。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。

3.3.4 病毒防护

DAS-Gateway 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 DAS-Gateway 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 400 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。
- 支持 ZIP、GZIP 等压缩文件的病毒查杀,默认支持检测到 5 层，最大可检测到 20 层。
- 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、记录日志。

3.3.5 Web 防护

DAS-Gateway 的 Web 防护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。

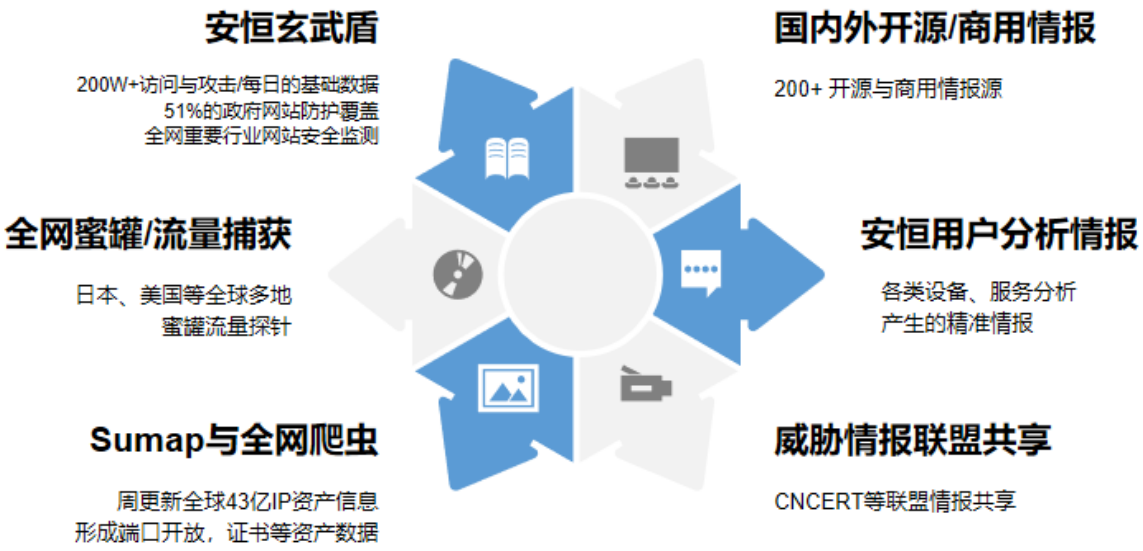
Web 防护引擎能有效抵御各种注入式攻击，包括 SQL 注入、系统命令注入、LDAP 注入、SSI 注入、邮件注入、请求体 PHP 注入等攻击；对于常见的 XSS 攻击的防护结合基于语义分析和攻击指纹两种方式，相比传统只基于攻击指纹的检测方法，检测准确率更高，误报率更低，防逃避能力更强；为了检测出恶意攻击者对 Web 站点的扫描行为，Web 防护引擎支持多种检测方式，多种扫描方式，同时也具备检测恶意爬虫的能力，其中包括 Acunetix、Appscan、Nessus、Sqlmap、Arachni、Netsparke、Webinspect、绿盟极光等。其它的防护还包括会话劫持检测、木马检测等。

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。

3.3.6 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。

DAS-Gateway 通过自研的威胁情报云平台，依托安恒信息玄武盾 SaaS 云防护、蜜罐网络、全球资产探测等能力。国内外数百家情报源集成，通过大数据、机器学习与文件自动化分析等技术，提炼形成涵盖 C&C、僵尸网络、恶意代理等 60 余类的情报数据，以及全球的网络资产基础数据，日更新高活跃情报数据 80 万条。



DAS-Gateway 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。

DAS-Gateway 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 DAS-Gateway，网关可进行一站式向导配置。提前做好安全防御。

3.3.7 其他防护

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/端口扫描异常

  通过 IP 扫描，黑客得以窥知目的端内网络结构和情形；通过端口扫描，黑客可以得知目标主机已开启的服务端口。

- 网络流量异常

  突然产生大量的 TCP SYN、TCP、UDP、ICMP、IGMP 等数据包，会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/端口扫描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。

DAS-Gateway 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。

3.3.8 安全分析

3.3.8.1 资产发现&安全分析

为帮助安全管理人员掌握内网的资产情况，识别潜在风险。DAS-Gateway 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，能够获取到设备的操作系统、使用的浏览器、杀毒软件、开启的应用服务。

DAS-Gateway 通过以资产为核心，对各种安全事件进行关联分析统计，为安全管理人员提供一种资产的视角来感知网络中的威胁情况：资产是否受到 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。以此标识出资产的风险级别，便于管理员定位风险主机，并根据关联的威胁事件进行针对性的防护。

3.3.8.2 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。

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。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。

3.3.9 安全管理

3.3.9.1 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。DAS-Gateway 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。还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，可帮助管理员快速定位网络故障；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。

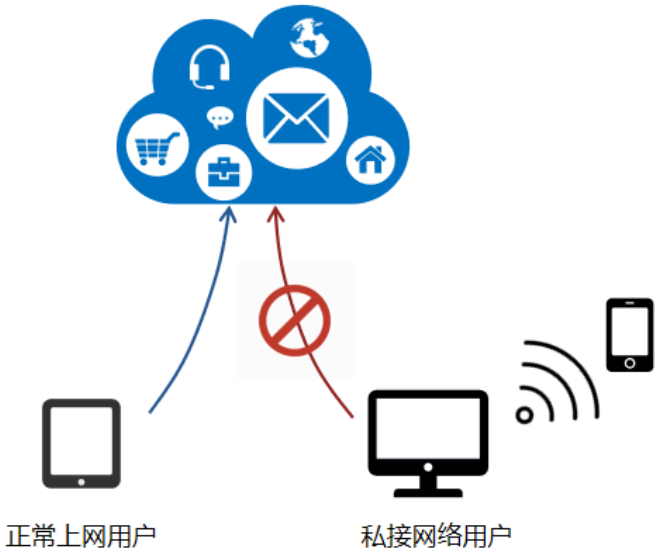
3.3.9.2 黑名单

DAS-Gateway 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。

3.3.9.3 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。DAS-Gateway 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 DAS-Gateway 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。



3.4 管理特性

3.4.1 用户管理

用户管理模块作为防火墙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。

DAS-Gateway 的用户类型包括第三方用户、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。支持自动同步用户。DAS-Gateway 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。支持设备上的 AD 域用户自动同步和 Excel 自定义导入功能。用户管理更便捷、更全面。

3.4.1.1 用户组管理

DAS-Gateway 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 DAS-Gateway 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。

3.4.1.2 身份认证

DAS-Gateway 具备丰富的身份认证方式，可有效地区分用户。这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基础。

DAS-Gateway 支持以下认证方式：

- 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：微信公众号认证，可通过微信小程序获取手机号。
- 访客二维码认证：审核人通过扫描访客终端弹出的认证二维码完成认证。
- 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 域一次认证即可登录相互信任的应用，减免频繁认证。

3.4.2 应用识别

应用识别（Application identification）是 DAS-Gateway 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。

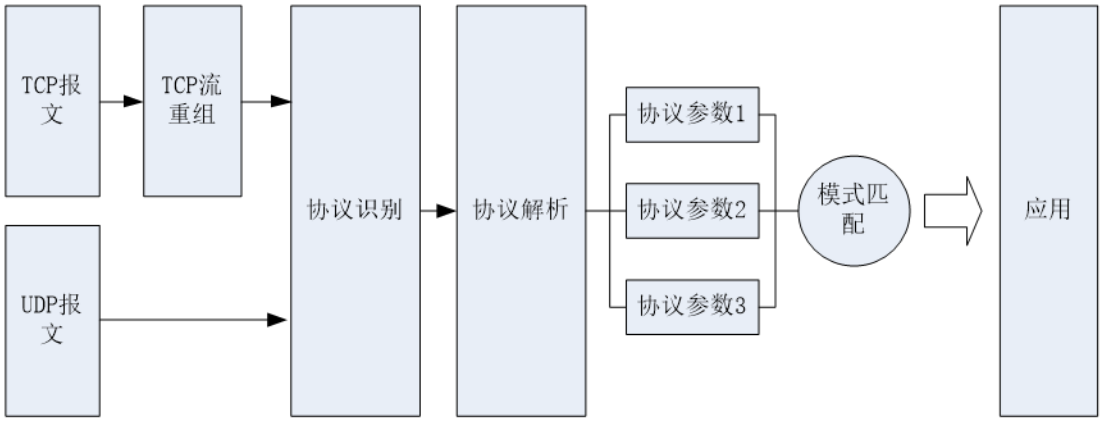
随着 P2P 应用的广泛流行和基于 Web 的应用的兴起，传统的利用固定端口来区分应用类型的设备无能无力。应用识别功能把对报文的协议解析、深度内容检测以及关联分析结合起来，通过对大量实际环境中的流量的分析，总结出每种应用的流量模型。把对数据包的协议解析、深度内容检测和关系分析的结果综合起来，由决策引擎通过与流量模拟的匹配程度，智能的判定应用类型。相比传统的应用识别技术，还具有以下特点：

- 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，防火墙产品通过自带的应用特性库无法对企业应用系统进行识别、审计和管理。DAS-Gateway 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

DAS-Gateway 对已知协议和 RFC 规范的深入理解，可准确、高效地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。



3.4.2.1 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、高效地识别出网络流量的应用类型，而且可以精准地识别出应用的行为。

3.4.2.2 应用路由

DAS-Gateway 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。

DAS-Gateway 的应用路由功能不是基于端口，而是基于应用来实现的。当发现某种应用的流量的时候，会把对应的 IP 和端口信息缓存在系统中，相同的 IP 和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。

3.4.2.3 基于应用的流量管理

DAS-Gateway 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。

3.4.3 终端识别

终端识别引擎是主要提供用户身份验证、终端类型和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 管理员可以查看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。

DAS-Gateway 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。

3.4.4 访问管控

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，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 DAS-Gateway 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，能有效地实现用户、应用的访问控制。

3.4.4.1 应用管控

DAS-Gateway 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。

DAS-Gateway 内置 5000+应用行为特征，管理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，帮助企业规范上网行为，规避法律风险。

3.4.4.2 URL 管控

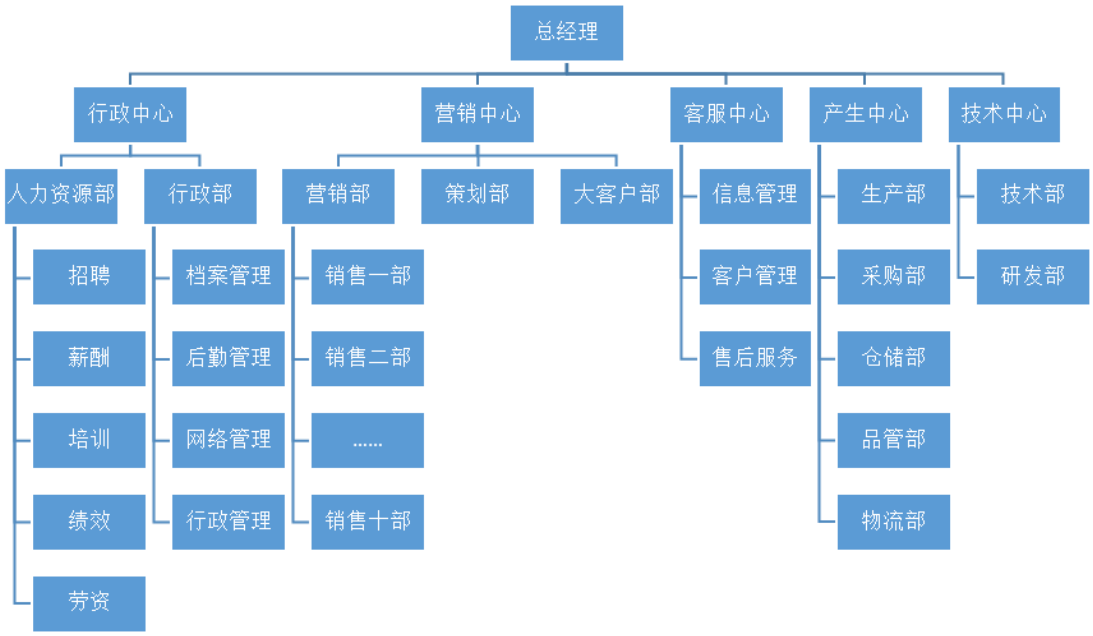
- DAS-Gateway 内置千万级 URL 库，预置 57 类非加密 URL 种类，13 类加密 URL 种类，涵盖游戏、网上交易、成人、证券、在线聊天等主流网站，让用户通过网站分类的选择，轻松控制网站访问。
- 支持审计过滤加密网站和加密网站的搜索内容，全面控制用户的网站访问行为。
- 支持自定义 URL、恶意 URL、URL 白名单和 HTTPS 域名对象等内容，可灵活应对用户管理需求。

3.4.5 流量管理

DAS-Gateway 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。

3.4.5.1 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。



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带宽管理需求，策略主要支持基于用户/用户组、应用/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	

3.4.5.2 弹性带宽分配

DAS-Gateway 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。

3.4.5.3 流量及时长限额

在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。

DAS-Gateway 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。

DAS-Gateway 可提供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。

3.4.5.4 每 IP 或用户限速

DAS-Gateway 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，如果有多个用户使用该通道时，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。

3.4.5.5 流控策略白名单

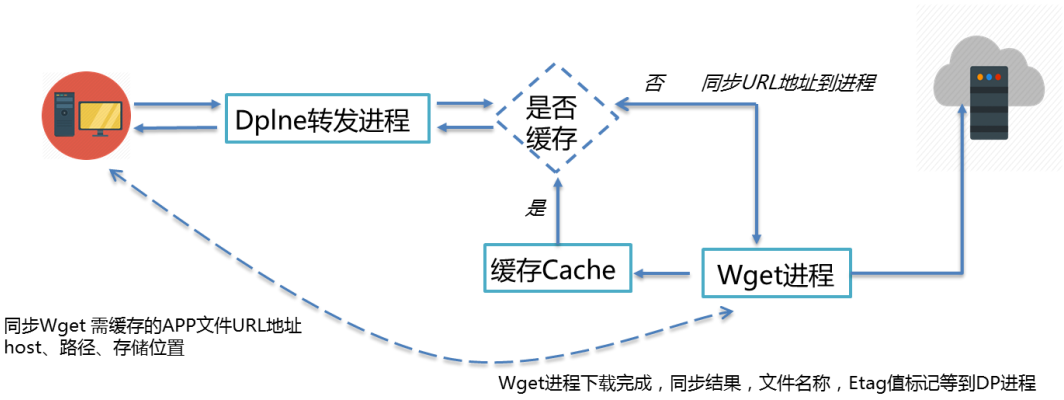
网络管理过程中，重要来宾和企业重要人员往往不希望受流控策略的限制，DAS-Gateway 根据用户需求，增加了流控策略白名单功能，白名单 IP 和用户将不受 DAS-Gateway 任何流量策略的限制，保障管理更加人性化。

3.4.6 广告推送

企业于投放通知或营销信息时，需向用户快速地下发消息，传统的消息传播方式速度慢且成本较高，非常不适用。DAS-Gateway 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，DAS-Gateway 多广告推送功能极具优势。

3.4.7 应用缓存

DAS-Gateway 创新性地将 APP 缓存在设备本地，当用户下载时直接推送，下载几十 MB 的文件只要几秒钟，极大地提升了带宽利用率的同时提升了用户体验；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。DAS-Gateway 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。



3.4.8 报表管理

DAS-Gateway 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。针对大中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。

3.5 合规特性

3.5.1 SSL 网站解密

互联网时代越来越多的网站启用 HTTPS 协议，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地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，DAS-Gateway 提供了 SSL 审计功能。DAS-Gateway 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。

3.5.1.1 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。

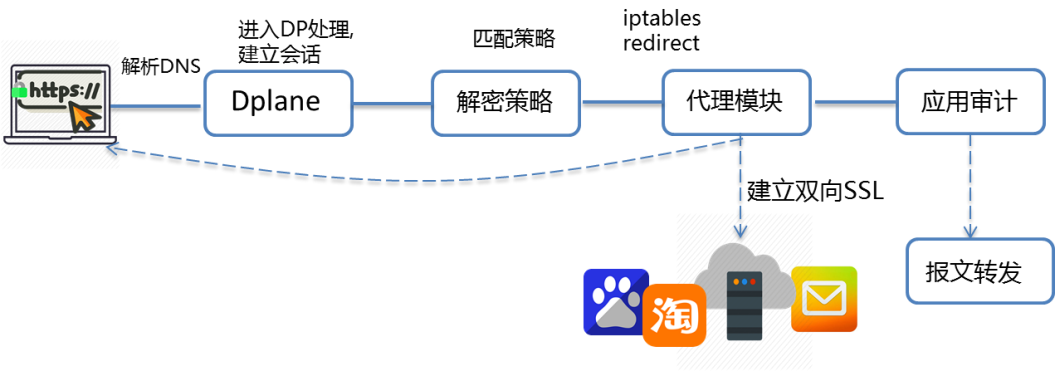
转发报文流经设备，判断 TCP 443、995、993、465 端口进入解密策略匹配流程。依次匹配入接口、源地址对象、目的地址对象、若为 443 端口判断目的 IP 是否存在于 DNS 解析的 IP 中，若均匹配上报文送入 Linux 内核，通过内核的 iptables redirect 功能重定向到本机代理进程。

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。

3.5.1.2 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。

- HTPPS 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。



3.5.2 清晰事后审计

DAS-Gateway 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。同时，DAS-Gateway 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。

3.5.3 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。

DAS-Gateway 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。

3.6 运维特性

3.6.1 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），开局人使用此 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。

3.6.2 高可靠性

DAS-Gateway 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：

- HA：主主、主备模式保证网络持续运行，支持 VPN 级别的 HA 功能。DAS-Gateway 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。DAS-Gateway 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。
- 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。
- 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

3.6.3 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状况，DAS-Gateway 提供强大的应用识别功能，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。

3.6.4 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，如何提高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。

DAS-Gateway 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，帮助管理员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。

3.6.5 端口镜像

DAS-Gateway 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。为管理员提供运维工具，并节省一台交换机的成本。

3.6.6 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。DAS-Gateway 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。

3.6.7 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。DAS-Gateway 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。

3.6.8 业务告警

DAS-Gateway 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。

3.6.9 集中管理与日志分析系统

随着网络规模、业务应用不断增长，网络安全事件也随之增加。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地进行安全检测和控制。

为了方便网络管理员进行操作和维护，安恒信息推出了集中管理与日志分析系统，以实现对 DAS-Gateway 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，通过数据挖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。利用集中管理与日志分析系统，管理员可以高效地管理各 DAS-Gateway 设备，全面掌握网络的整体安全状况。

DAS-Gateway 集中管理与日志分析系统通过 API 接口与 DAS-Gateway 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，DAS-Gateway 集中管理与日志分析系统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、高效数据导入等特性。

3.6.9.1 采用高性能数据存储和查询

DAS-Gateway 集中管理与日志分析系统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。

DAS-Gateway 集中管理与日志分析系统支持 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集中管理与日志分析系统前日志存储 1 个月产生 500GB 数据，而采用 DAS-Gateway 集中管理与日志分析系统后，数据 1 个月存储减少至 60GB，这样大大节省了用户的存储硬件成本。

3.6.9.2 深层次数据挖据分析

DAS-Gateway 集中管理与日志分析系统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。

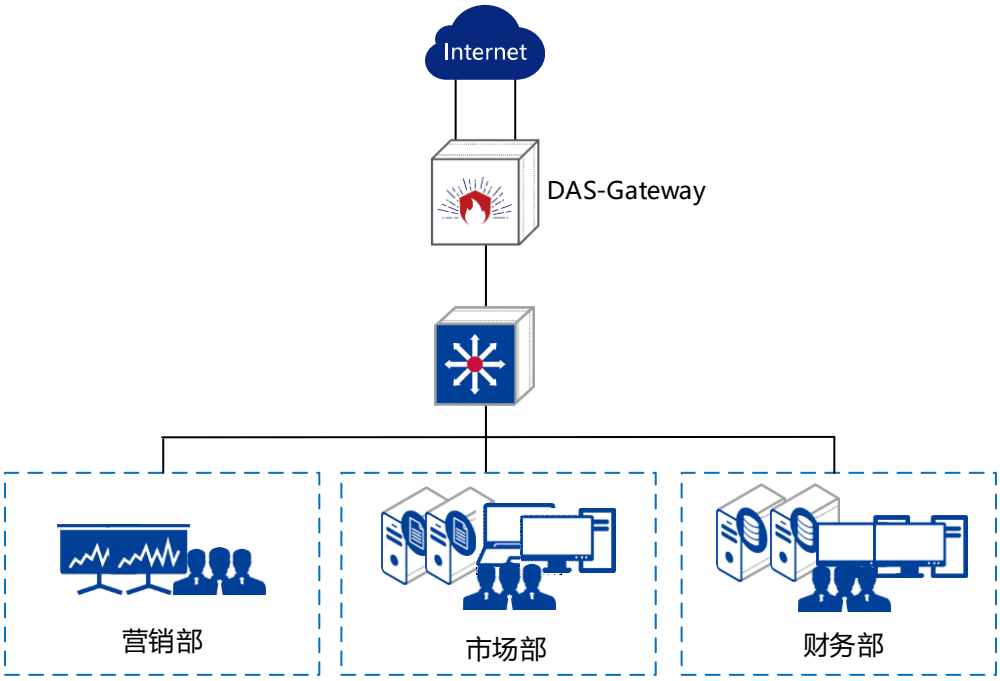
数据仓库中包含 ETL、数据模型、信息展现等主要关键技术。

- 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。

4. 典型应用场景

4.1 边界网关部署

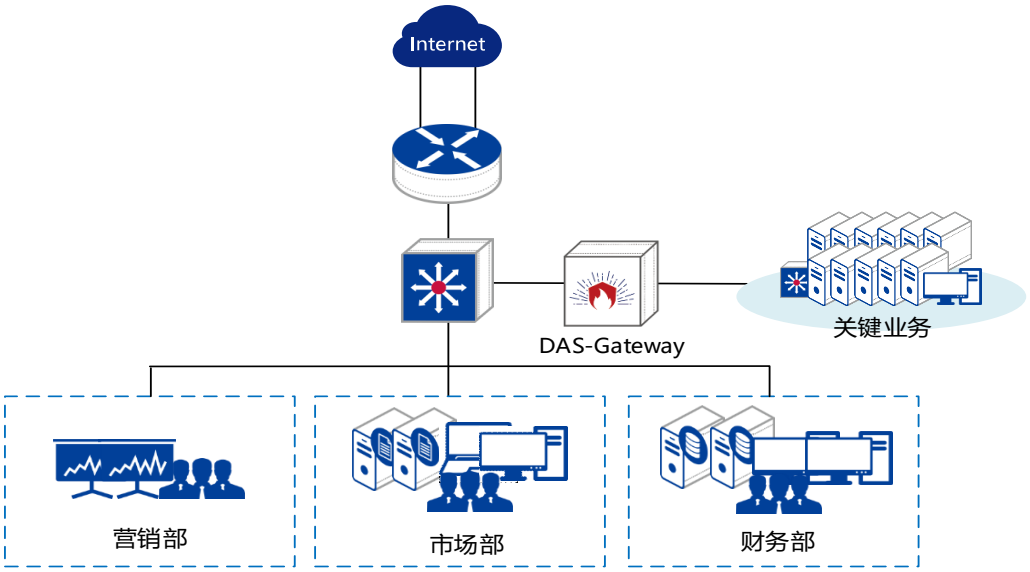
- 适用于互联网出口场景，以网关模式部署于网络出口，通过 DAS-Gateway 的链路负载均衡、NAT 等出口特性功能，实现多个 ISP 和教育网出口的智能路选。
- 以用户资产为视角进行风险分析，构建对 IT 资产实现多维度的安全分析监控。
- 抵御内外网的入侵防御，对网络中的病毒进行过滤查杀。
- 威胁情报联动实现全网威胁实时同步，及时发现内网未知威胁，0day 攻击等。
- 对网络社区/P2P/IM/网络游戏/炒股/网络视频/网络多媒体/非法网站访问等各种应用进行监控和管理，保障关键应用和服务的带宽。



4.2 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，根据实际网络环境部署。
- 通过 DAS-Gateway 的资产发现功能以用户资产为视角进行风险分析，构建对 IT 资产实现多维度的安全分析监控。
- 通过 DAS-Gateway 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。
- 通过 DAS-Gateway 的威胁情报功能及时发现内网未知威胁，0day 攻击等，提前做好安全防范。

- DAS-Gateway 支持从策略梳理和分析，一定程度上解决访问控制策略管理的难题，使每一条策略都直观可视，易于使用、便于维护。
- 提供以资产和攻击维度的安全智能可视化的分析，便于管理员分析取证溯源。



4.3 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。
- DAS-Gateway 支持多种认证方式，支持对接多种认证服务器，实现用户认证上网。
- DAS-Gateway 可以为总部和分支提供 AV、IPS 等保护，有效的抵御各种网络威胁。
- 通过 DAS-Gateway 的威胁情报功能及时发现内网未知威胁，0day 攻击等，提前做好安全防范。
- IPsec VPN 配置简单易用，全自动收敛，自适应多线路，完美地解决分支运维能力弱的问题。
- 支持 U 盘零配置上线，集中管理平台实现分部多台设备的统一管理和日志分析。