聚铭下一代防火墙

产品白皮书

聚铭网络科技有限公司

2023 年 11 月

目录

声明

未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

在本文中如无特别说明，聚铭网络均指南京聚铭网络科技有限公司和北京聚铭信安科技有限公司。

JUMING 聚铭图标为聚铭网络的商标。对于本手册出现的其他公司的商标、产品标识和商品名称，由各自权利人拥有。

除非另有约定，本手册仅作为使用指导，本手册中的所有陈述、信息和建议不构成任何明示或暗示的担保。

本手册内容如发生更改，恕不另行通知。

如需要获取最新手册，请联系聚铭网络技术服务部。

联系信息

北京总部：北京市海淀区丹棱街 18 号创富大厦 9 层

南京总部：南京市雨花台区软件大道 180 号南京大数据产业基地 7 栋 4 层

电　　话：025-52205520/52205570

传　　真：025-52205565

全国服务热线：400-1158-400

网　　址：www.juminfo.com

产品支持：support@juminfo.com

聚铭网络技术服务以及营销网络覆盖全国，并在各地设有办事处和分支机构，为客户提供无微不至的解决方案和高效的服务支持。聚铭专家团队 7x24 小时全天候在线，确保在安全事件发生时提供分钟级应急响应。

1. 概述

1.1. IT 基础架构的演变，迫切需要新的安全解决方案

如今，异地分支机构、远程办公、物联网以及云服务使用量的不断增加促使更多数据远离传统 “边界”，完全绕过了传统的安全控制点。此外，许多企业都采用了自带设备 (BYOD) 模式，允许员工用自己的私人计算机或移动设备访问内部网络的业务应用。事实上，有超过 67% 的员工在工作中使用自己的设备，且这一数字呈持续上升趋势。通过 Wi-Fi 网络连接移动设备和笔记本电脑是一种普遍现象，甚至对日常业务运营至关重要。

此外，绝大多数组织用户还需要直接访问互联网，而现在越来越多的基于云的关键应用和数据都驻留在互联网中。网络架构跨越多类云服务、操作系统、硬件设备、数据库等部署工作负载。应用和数据变得更加分散，网络也随之变得更加多样化。

IT 基础架构的这种演变极大地增加了攻击暴露面，使保护网络、数据和用户的工作变得更加复杂。

网络安全已成为一项艰巨任务，如今的人员无法再继续尝试管理大量的单点安全解决方案、云资源和设备。我们必须寻求不同以往的方法。

1.2. 网络安全解决方案，需要新一代技术作为支撑

网络不断发展以适应新的业务方式，网络安全也必须跟上。

在当前的分布式 IT 资产环境中，需要保护各种网络基础设施、互联设备和业务系统免受攻击威胁。因此，在整个网络交换矩阵中建立策略实施点，进一步靠近需要保护的信息或应用，在物理和逻辑控制点创建微边界是形势急需。我们将以新一代的防火墙作为敏捷、集成网络安全技术的基础平台，从而为当前和未来的发展提供支持。

在此背景下，聚铭结合多年对 IT 基础架构和网络安全的研究，发布新型下

一代防火墙产品。它提供 L2 到 L7 层安全防护能力，包括边界访问控制、DOS 防护、入侵检测与防护、病毒防护等，还向用户提供 APT 高级威胁防护、内容安全、威胁情报联动、态势感知、EDR 联动、VPN、智能带宽管理，上网行为管控与审计等多重安全特性。

聚铭下一代防火墙采用高性能多核架构，支持多种国产 CPU、多种国产操作系统；全面适配云环境，支持主流的虚拟化平台，包括 VMware、KVM 等。

结合全面丰富的联动和 RESTful API 可编程接口，聚铭下一代防火墙具备高效的协同防御能力，包括沙箱联动，EDR 联动，威胁情报联动，态势感知联动等，为构建网络立体化防护提供有力支撑。

与此同时，聚铭下一代防火墙还具备 SD-WAN 智能组网能力，设备支持零接触上线（ZTP），可通过云端管理平台实现对业务配置统一编排、设备集中运维、状态实时监控及可视化，最大程度的简化了运维管理的工作，降低资金和人力投入。

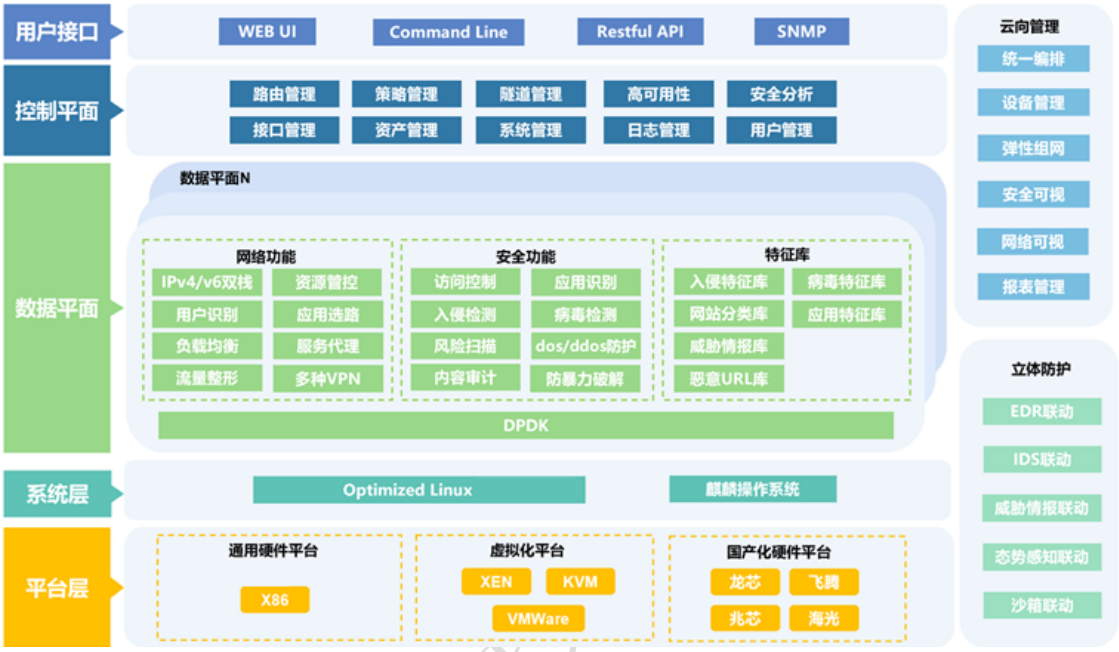
2. 关键技术

2.1. 系统架构

聚铭下一代防火墙采用通用平台设计，系统对上层安全功能屏蔽硬件差异，提供统一的软件接口。因此，聚铭下一代防火墙可运行于 X86、MIPS、ARM 及国产化多核平台上，或者基于上述平台的 KVM 和 VMware 虚拟化平台。着重增强了自身的安全性，并基于 UIO 技术对上层提供应用层零拷贝报文高速处理机制，显著提升了报文处理效率。

聚铭下一代防火墙在软件架构上采用了控制与业务分离的设计，根据业务类型分为控制面（Control Plane，简称 CP）和数据面（Data Plane，简称 DP）两部分，CP 主要处理鉴权、配置、路由、日志和高可用性等管理业务，并提供 WebUI、命令行、云管理平台和 SD-WAN API 等管理接口。DP 则处理网络层、应用层解析和各项安全策略的执行。每个 CP 或 DP 都与一个逻辑处理器进行绑

定，避免由于系统调度对性能产生负面影响。同时，聚铭下一代防火墙采用了先进的 DPDK 快速数据包处理技术，旨在解决 linux 内核瓶颈，大幅提升了网络转发性能。

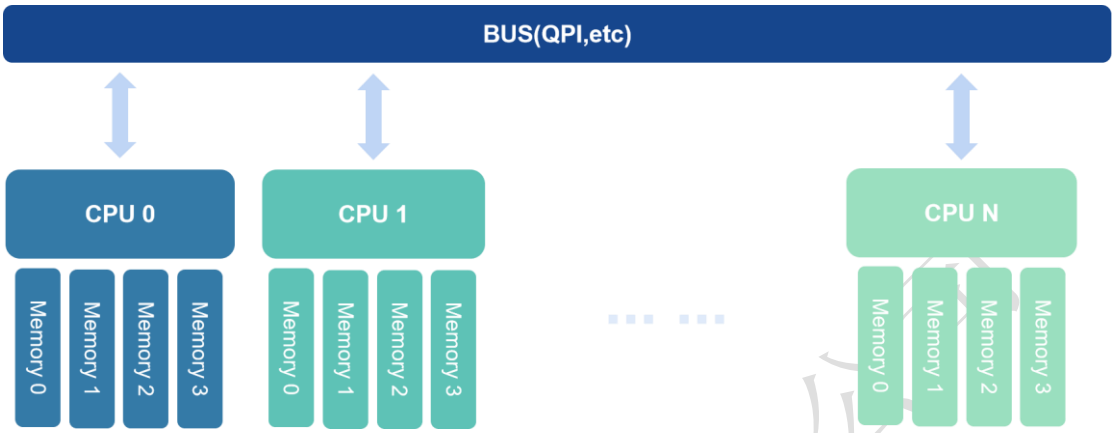


2.2. 多核并行处理技术

为了更好地发挥多核平台的性能，聚铭下一代防火墙会根据硬件平台的不同调整 CP 和 DP 的实例数，以实现性能的最大化。在处理业务数据的过程中，每个 DP 都采用 Run-to-completion 的方式，即一个数据包从接收到所有业务处理完毕，均在同一个 DP 中完成，这种处理方式能够显著提高处理性能。

但是，数据包之间存在各种逻辑关系，例如应用层分片或者多连接应用。以往的基于多核技术的网络产品，有的会将数据包随机发送到各个处理核，忽略这种内在的逻辑关系， 这样做的直接后果是无法正确处理应用层分片和多连接应用的相关业务，并且从现象上，经过该设备会出现较多的乱序报文。一个改进的做法是在特定的功能点（如 NAT、应用识别、内容审计）对特定的报文进行重组，报文在多个处理核之间传递（同时需要共享内存、共享流表等），需要使用锁等方式进行同步和互斥，对处理性能有较大影响。在 X86 平台下如果

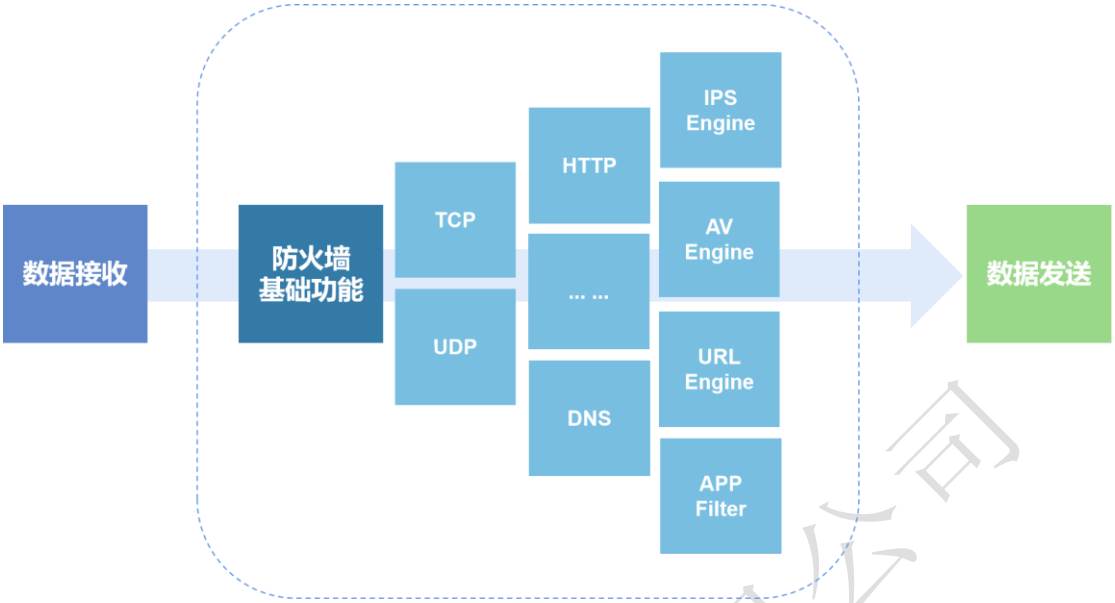
处理不当，还有可能造成跨节点访问，性能下降更加显著，甚至可能出现 CPU 核数越多，性能反而越低的现象。



聚铭通过智能分流器对流量进行分配。当数据包到达聚铭下一代防火墙时，首先由智能分流器对数据包进行初步分类。智能分流器根据当前启用的上层功能以及数据包的网络层、应用层信息，决定将该数据包投递到哪个处理核。智能分流器保证了数据包能在单个处理核上完成所有所需的处理（出于对某些特殊情况的处理，系统仍提供核间报文互操作机制），避免了跨节点访问内存的高昂开销，是保证多核并发性能的关键技术。

2.3. 一体化报文处理引擎

传统的报文处理流程中，多个功能模块往往是串行的关系，每个模块的处理相对独立，或者只共享少量的信息。这样做的好处是每个模块的实现相对简单，降低了开发的技术难度。但是各个模块重复解析，有的还存在报文多次拷贝，降低了处理性能。更重要的是多个模块之间缺乏逻辑上的一致性导致难以综合所有信息进行高级策略管理和行为分析。聚铭采用了一体化报文处理引擎完成报文的统一解析。引擎首先分析用户配置的各项功能，决定进行哪些分析，随后一次性对二至七层所有需要进行解析的内容进行统一处理，并将结果一并送至策略控制模块。策略控制模块依据这些解析结果，匹配用户配置的策略进行报文的后续处理。



一体化报文处理引擎配合智能分流器，在单个处理核的处理进程上完成从报文接收、报文解析、策略控制、报文发送的所有工作。一次解析，统一处理，避免了多模块、多进程之间的重复工作和报文拷贝。在策略统一处理时，还可基于用户策略、应用策略、安全策略等，进行更高层次的抽象，制定基于基础策略的高级策略

2.4.基于用户、应用、终端和资源的控制策略

任何行为的背后都有对应的用户，任何行为的途径都可以抽象为一种应用。规范用户的行为就保证了网络资源的安全，所以聚铭下一代防火墙应以用户和应用为中心。用户的属性应具有一致性和延续性，用户通过不同方式访问网络资源，应用于该用户的策略应始终保持一致。此外，基于用户的策略也更有利于在网络访问权限与组织架构之间建立映射关系，简化网络管理员的配置管理工作。

聚铭下一代防火墙提供了用户策略、应用策略、终端策略、访问策略、防护策略、路由策略、流控策略、NAT 策略等多种控制策略，这些策略全部都围绕用户和应用进行组织：用户策略规定了用户如何接入网络，用户所属的类别，以及具备的访问权限等等。应用策略规定了哪些人可以使用哪些应用，以及这些应用可以进行哪些行为。访问策略规定了用户和应用对网络资源的访问

权限。路由策略规定了用户和应用如何进行网络选路，达到负载均衡、优化广域网访问等目的。流控策略规定了用户和应用对网络带宽资源的使用方式。NAT 策略规定了用户和应用跨内外网互访问的映射方式。

聚铭下一代防火墙将上述几类策略区分开来，并非因为这些功能在实现上相互分离——实际上所有功能都在一体化报文处理引擎中完成。功能实现的集中有助于提高引擎工作的效率和实施更有效的控制，而控制策略的适度分散则能明显降低策略的复杂度，简化网络管理员的配置管理工作。

3.产品特色功能

3.1.全方位防御体系

聚铭下一代防火墙通过事前风险监测、事中防护响应、事后取证分析形成了全方位的安全防御体系，为用户提供全面的安全防护。

- **事前风险监测：**聚铭防火墙能够在事前自动识别网络内主机资产和服务器资产的网络信息，能够识别内网资产的开放端口、弱密码等安全风险，同时提供多种可视化系统监控数据，帮助用户有效监测和预知网络风险。
- **事中防护响应：**聚铭防火墙在事中提供了深入的全方位安全防护

能力，包括入侵防护、病毒防护、DOS/DDOS 攻击防护、URL 过滤、防暴力破解、威胁情报应急响应、APT 攻击防护、EDR 联动防护等，为用户提供一个多层次防御体系，保障企业和组织的网络安全。

- **事后追溯审计：**聚铭防火墙在事后能够进行追踪溯源、取证分析，根据日志分析事件来源和原因，并进行针对性加固措施；能够通过黑客视角或资产视角对攻击事件进行综合分析，将抽象的网络形象化，将攻击行为可视化，帮助用户快速了解网络的安全情况。

3.2. 深度安全防护

聚铭下一代防火墙提供了全方位的深度安全防护，从多个维度上为网络的安全防护提供坚实壁垒。

3.2.1. 入侵防护

聚铭下一代防火墙内置了入侵防护引擎，支持对缓冲区溢出、SQL 注入、暴力猜测、DoS 攻击、扫描探测、蠕虫病毒、木马后门等各类黑客攻击和恶意流量进行实时检测、报警或拦截；同时超过 3000 种的入侵防护特征库，可满足大部分的业务需求。

- **基于流重组**

当前，很多的攻击行为采用了 TCP 流分段组合的方式，导致基于单个数据包检测的入侵防护引擎失效。聚铭下一代防火墙内置的入侵防护引擎在攻击检测的过程中，可以进行 TCP 会话的还原，从而准确有效的检测出隐蔽在多个数据包中的攻击，得到完整的攻击特征。

- **基于协议状态分析**

聚铭下一代防火墙内置的入侵防护引擎，它的协议分析技术，是对已知协议和 RFC 规范的深入理解，可准确、高效的识别各种已知攻击。目前，可支持防护 HTTPS、Telnet、FTP、HTTP、SMTP、SNMP、DNS 等多达 30 种的主流应用层协议。

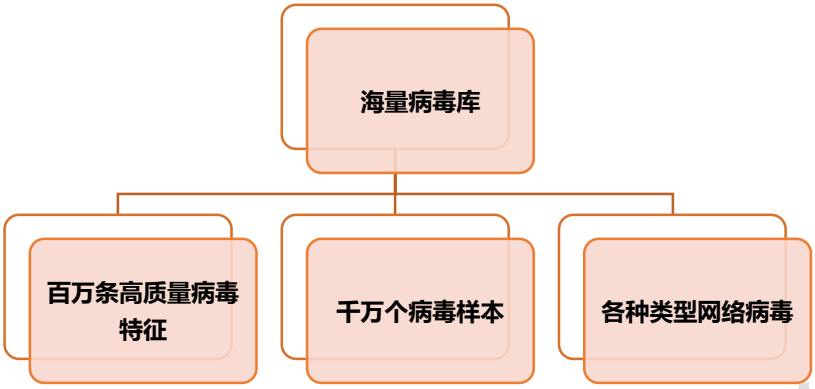
目前，聚铭下一代防火墙内置的入侵防护引擎采用的基于协议状态的检测技术，使它具有了明显的优势：

- 利用协议分析，在处理数据帧和连接时更加迅速和有效准确，减少了误报的可能性。
- 能够关联数据包前后的内容，对孤立的数据包不进行检测，这和普通入侵防护检测所有数据包有着本质的区别。一方面因为这种检测机制的高效性降低了系统在网络探测中的资源开销，大幅度提高了检测性能，另一方面因为在攻击指令到达操作系统之前，模拟了它的执行，以确定它是否具有恶意，有效减少了误报。
- 它具有判别通信行为真实意图的能力，它不会受到像 URL 编码、干扰信息、IP 分片等入侵防护规避技术的影响。
- 当检测到的所有数据信息经过应用协议分析后， 将真实的应用数据与签名库进行攻击特征的匹配，因为我们知道特征匹配仍然是检测效率最高的和最准确的检测技术。只是这种匹配，与普通基于模式匹配的检测机制有着本质上的区别，它是在协议分析和还原以后真实有效的数据，这种真实可靠的有效数据的匹配，一方面提高了检测效率；另一方面，增强了检测攻击的准确度，减少了误报的概率。

3.2.2. 病毒防护

- **全规则高速引擎**

聚铭下一代防火墙内置的反病毒引擎是最快速的网络病毒检测引擎，可使用海量本地病毒库，具备 760 多万条高质量病毒特征；支持与沙箱联动，可检测数千万个病毒样本。



➢ **全方位病毒检测**

聚铭下一代防火墙内置的反病毒引擎可以检测蠕虫、病毒、木马、黑客工具、流氓软件、风险程序等各种类型；提供非完整流、完整流、文件、URL 等不同对象的检测；适用于 HTTPS、HTTP、FTP、SMTP、POP3、IMAP 等 TCP 协议并通过严格的白名单过滤认证，有效降低误报。

类型	对象	协议
•蠕虫 •木马 •黑客工具 •流氓软件 •风险程序 •...	•非完整流 •完整流 •文件 •URL	•HTTPS •HTTP •FTP •SMTP •POP3 IMAP

3.2.3. 攻击防护

聚铭下一代防火墙通过分析和提取攻击特征，能够有效防御多种 DOS/DDOS 攻击。

➢ **Flood 攻击防护**

泛洪攻击通常以大量攻击包试图消耗网络资源或服务器性能，因此防火墙一方面以其强大的性能作为支撑，另一方面采用最新技术手段，以最少的系统资源来抵御 DDOS 攻击，从而既阻止了外部的恶意攻击，又能确保网络服务的

正常运行。防火墙既支持 syn flood、udp flood、icmp flood，tcp flood 等流量型攻击防护；也支持 HTTP Flood、DNS query flood、ARP Flood 等应用型攻击防护。

- **异常包攻击防护**

支持防护 jolt2、land_base、ping_of_death syn flag、 tear_drop 、winnuke 、smurf、 ip spoof 等多种异常包类型。通过检测报文的状态、分片、偏移、负载等特征信息来识别异常报文，从而进行防护。

- **抗恶意扫描**

支持基于 TCP、UDP 和 PING 协议的恶意扫描防护。当攻击者试图探测目标上的开放端口或存活主机时，防火墙能够识别并阻止非法探测行为，防止攻击者发起进一步攻击。

- **防 ARP 欺骗**

支持 ARP 欺骗防护，能够从报文有效性和用户合法性角度对 ARP 报文进行分析和校验，能够有效防御通过 ARP 欺骗仿冒网关或者终端用户的攻击行为，保证网络的正常运行。

- **防暴力破解**

支持 TELNET、HTTP、POP3、SMTP、IMAP、FTP、RLOGIN 等多种协议的登录报文进行检测，通过监测统计的方法分析攻击行为，若在短时间内产生大量的登录行为，则被判断为暴力破解用户密码行为，根据阈值进行响应和阻断。

- **DNS 隧道检测**

防火墙能提取分析 DNS 隧道特征，根据上万条正常报文和异常报文进行对比分析，提取出 DNS 隧道特征，通过监测 DNS 请求域名长度、DNS 会话中的报文个数等来进行 DNS 隐蔽隧道特征分析，防火墙支持基于异常报文和流量模

型的检测方式来识别 DNS 威胁隧道，防止攻击者利用 DNS 请求和响应来承载和隐藏真实数据内容，并采取相应的防护措施

3.3. 安全一体化

聚铭下一代防火墙支持基于应用和用户的一体化安全策略，在技术实现上，将涉及到的安全业务模块进行统一化处理，包括协议分析、威胁检测和网络处理等一系列安全业务，最终保证系统的高性能和低延迟；在配置上，实现了配置的一体化，一条安全策略覆盖入侵防御、反病毒、URL 过滤、应用管控等全方位安全管控，简化了配置难度，提升了管理员的运维效率；在性能上，通过业务处理上的一体化，安全策略只需对报文进行一次检测，即可完成所有安全模块的检测和分析，简化了业务处理流程，大大提升了产品性能。

3.4. 多样化用户识别

聚铭下一代防火墙智能用户识别，支持静态绑定、本地认证、第三方认证、短信认证等多种认证方式，并且会将未识别的用户自动归类为匿名用户，便于网络管理员按照需要指定这部分用户的访问策略。例如，未识别用户仅允许访问有限的资源、特定的应用，或者不允许访问任何资源。

3.4.1. 静态邦迪

静态绑定指的是网络管理员手动建立每个用户与一个或一组 IP 的对应关系，过程对用户透明，但是可能出现仿冒，因此还需结合其他措施确保 IP 的合法使用。认证登录解决了仿冒的问题，但是它要求用户通过某种方式进行登录。聚铭下一代防火墙支持本地认证和第三方认证两种方式。

3.4.2. 本地认证

用户接入网络后，可自动获取或手动指定 IP，以匿名用户的身份进行网络访问。如果匿名用户需要访问需要登录才可授权的资源，对于 Web 资源，聚铭下一代防火墙会自动将用户重定向到登录页面，通过用户名、密码进行身份验

证后即可进行访问；如果访问非 Web 资源，则必须首先通过 Web 进行登录，方可授权进行访问。

3.4.3. Portal 认证

聚铭下一代防火墙支持提供完整的 Portal 认证解决方案。聚铭下一代防火墙与 Portal 服务器对接之后，未认证的用户浏览任何页面时，直接重定向到指定的页面进行认证。用户认证成功后，可访问互联网。用户上网结束后，可以使用 Portal 功能通知用户下线；当聚铭下一代防火墙侦测到用户下线或者主动切断用户连接时，也能告知 Portal 服务器。当在 portal 服务器连接异常或故障时，防火墙支持用户逃生，即无需认证即可进行上网。同时，用户在未认证时，防火墙支持自动识别并阻断非 HTTP 流量，以减少 portal 服务器的处理压力。

3.4.4. 第三方认证

聚铭下一代防火墙支持 LDAP、RADIUS 等第三方认证技术。如果用户环境中已经存在用于统一身份认证的服务器，可在配置用户认证策略时直接指定通过第三方认证。这种方式后续的认证过程与本地认证类似，区别仅在于实际认证时，聚铭下一代防火墙会与第三方认证服务器进行交互确认认证信息的有效性。

此外，聚铭下一代防火墙还提供了便于其他特殊认证系统集成的 API，允许其他认证系统将认证信息同步到聚铭下一代防火墙上。

3.4.5. 双因素认证

聚铭下一代防火墙在管理员登录和 VPN 远程接入时支持双因素认证，即除了基础的用户身份认证方式（用户名密码）之外，还需进行其他认证方式，从而实现双因素认证。聚铭防火墙支持动态口令认证、硬件特征码认证和证书认证等多种辅助认证方式，同时也支持多因素认证，如用户名密码+动态口令+硬

件特征码等多种认证因素同时开启，以加强用户审计，提升用户登录的安全性。

动态口令认证是根据一定的算法基于时间和密钥而生成一次性密码，防火墙和 VPN 客户端分别生成动态密码，每次登录校验动态密码的一致性，从而实现用户认证。

硬件特征码认证是在用户使用 VPN 客户端登录时，防火墙支持对用户终端进行硬件码的识别、绑定和数量限制功能，通过限制每个用户下硬件特征码的数量来实现用户认证。

证书认证是在管理员登录时，需先向浏览器或 USB Key 中导入用户证书，防火墙先校验证书的有效性，校验通过后，方可登录防火墙。

3.4.6. 其他认证

聚铭下一代防火墙还支持多种用户认证方式，包括短信认证、访客二维码认证、混合认证、AD 域单点登录、免认证等，能够覆盖多元化的用户使用场景，结合用户访问策略，全场景覆盖，实现精准用户管控。

3.5. 智能应用识别

聚铭下一代防火墙的重要特点是能够准确地基于应用进行精细化的访问控制，而这依赖于高效、精确的应用识别。聚铭下一代防火墙支持基于深度包检测，深度流检测以及智能行为分析三种应用识别技术。

3.5.1. 深度包检测技术

聚铭深度包检测技术包括碎片重组、协议分析和特征匹配三部分。碎片重组不仅能够在网络层对分片的 IP、TCP 等进行重组，还能够在应用层进一步对报文内容进行还原。还原后的报文通过协议分析进行预处理，提取出超过数百种协议变量，然后由特征匹配对这些协议变量进行识别，这种精细匹配有效提高了识别准确度。聚铭研发的快速匹配算法，可同时对多个协议变量进行匹

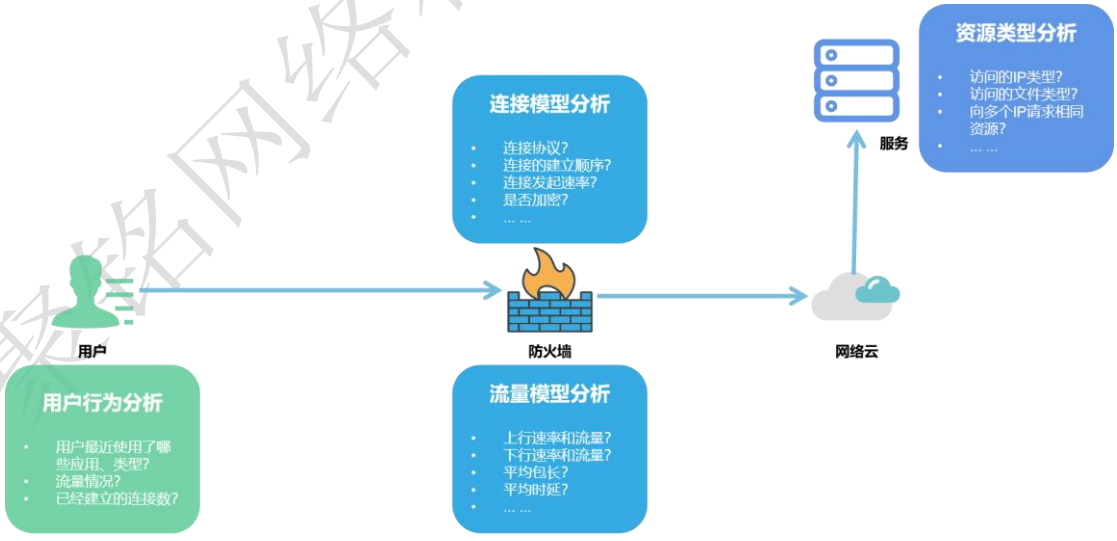
配，并充分利用硬件平台加速能力，有效提高的深度包解析的速度。

3.5.2. 深度流检测技术

对于私有协议，有时无法通过深度包检测进行有效的分析处理，由此引出深度流检测技术。深度流检测技术将数据包的传输序列中的其他信息作为特征进行识别，通过数据包序列长度、数据包内容关联分析等手段，有效识别多种私有协议。

3.5.3. 智能行为分析技术

互联网时代，每天出现的新应用都成千上万。深度包检测技术和深度流检测技术是基于已知特征的检测技术，无法对所有新应用都进行有效的识别和处理。为此聚铭开发了应用智能行为分析技术。虽然新应用的数量繁多，但是每一类应用都有一些相似的行为模式，通过对这些行为模式的分析研究，我们可以归纳出一类应用的公共特征，从而识别未知应用。这是智能分析技术的核心思想。



用户的行为有时间和空间上的关联性，智能行为分析技术充分发挥聚铭下一代防火墙基于用户的特性，从用户当前使用的已知应用、用户网络使用统计情况，到多个连接的连接模型、流量模型分析，再到访问的目的资源类型分

析，并结合基础事件关联分析，判断未知流量属于哪一类应用，以及是否存在潜在风险。

3.6.精细化资源管控

聚铭下一代防火墙支持所有接入用户对内网资源的精细化管控，包括 VPN 接入用户、本地认证用户、远程服务器认证用户等多种认证用户，基于防火墙用户策略，将资源对象全局化，进而实现对内网资源的权限控制。用户认证通过后，支持用户对资源进行细粒度管控，不仅能控制对资源的访问权限，还能够控制用户对资源访问的时效。通过加强对资源的管控，能够有效增强内网资源访问的可控性，减少内网信息泄漏的发生概率。

3.7.上网行为管理

3.7.1. 精准的应用控制

聚铭下一代防火墙针对网络应用的管控更全面、精准、便捷。针对应用的细分功能精准控制，可以基于用户、位置、时间、应用、行为、内容等 6 个维度来配置策略，比如可以配置以下策略：

- 上班时间不允许发送含有 xx 关键字的微博。
- 只允许 QQ 通过，阻断其它应用。
- 不允许发送含有附件的邮件等。
- 只允许特定的用户在办公室登录 QQ 等。

3.7.2. 丰富的应用审计

聚铭下一代防火墙支持对以下分类的应用行为及内容进行审计：

- 即时通讯
- 搜索引擎
- 社交网络
- 电子邮件
- 文件共享
- 在线购物

3.7.3. 强大的 Web 访问策略

聚铭下一代防火墙可以记录下 Web 访问的时间、用户、IP、主机、URL、网页分类、网页标题等信息。同时能智能排除不是 Html 的 Web 访问，提高日志的可用性。内置上百种站点分类，结合千万+URL 库，并提供定期更新服务。

3.8. 全面的 IPv6 网络支持

聚铭下一代防火墙支持全面的 IPv4/IPv6 双栈，包括网络应用和安全防护；同时，也支持多种 IPv6 隧道技术，全面支持 IPv6 在过渡阶段不同时期的网络适应性和兼容性。

- 支持基于 IPv6 的源 NAT、目的 NAT；
- 支持跨协议转换 NAT64 和 NAT46；
- 支持基于 IPv6 的静态路由、策略路由和动态路由（RIPng、OSPFv3）；
- 支持基于 IPv6 的流量管控、应用审计和用户识别；
- 支持基于 IPv6 的资产管理、会话管理和黑名单管理等；
- 支持基于 IPv6 的入侵防御、反病毒、URL 过滤、应用识别、抗

DDOS 和风险扫描；

- 支持 IPV6 手工隧道、isatap、6to4 等多种 IPv6 隧道技术。

3.9. 完善的 VPN 功能

聚铭下一代防火墙支持主流的 VPN 技术，包括 IPSec VPN、SSL VPN、GRE 等；具备专有的移动终端 VPN 接入客户端，同时支持多种平台，包括 Windows32 位/64 位、IOS、Android 等系统，实现快捷安全互联。

聚铭下一代防火墙能以网关模式、单臂模式进行部署；IPSec 全面支持 NAT 穿越，支持 Hub-Spoken、Full-Mesh 等部署；SSL VPN 支持安全隧道应用方式，支持端到端部署。

3.9.1. 单臂连接

“单臂连接”模式下下一代防火墙聚铭下一代防火墙作为 VPN 服务器或主机，专门处理 VPN 报文的加解密。从实现技术上而言，单臂连接结合了上述串行连接和并行连接两者的优势，实现了部署和性能的最优化。

3.9.2. 自动路由

使用 VPN 设备建立隧道通信时，一个通常的前提条件是，需要双方子网的缺省路由都指向 VPN 设备的内网口；如果是内网有多个网段的情况，则需要在内网的三层交换机或各路由器上添加到对端 VPN 网络路由

"自动路由技术"使得 VPN 设备收到对端设备（或客户端软件）发过来的密文后，在执行解密操作后进行地址转换，将对端的私网 IP 地址转换成本地内网的 IP（通常是聚铭下一代防火墙的 LAN 口 IP），用转换后的本地内网 IP 与本地子网进行通信。通过该技术，使得 VPN 不同子网之间的通信实际上变成了本地内网之间的通信，从而无需改变任何内网路由的配置。

3.9.3. 客户端外网隔离

聚铭下一代防火墙支持“内外网隔离”技术。是当 VPN 客户端用户在使用安全客户端软件和远端的聚铭下一代防火墙建立起加密隧道后，只能通过 VPN 隧道访问内部网络的信息资源（即：只能访问 intranet），而不能访问外网（即：internet 网）。通过这种方式，实现"内联网 intranet"和"互联网 internet"的逻辑隔离，这样当用户在使用企业内部应用系统时，就和 internet 网络"逻辑"上断开了，大大减少了被病毒侵害和木马程序窃听的风险，尤其是避免了很多在线攻击程序通过 VPN 隧道从分支机构向总部发起攻击。

3.10. 智能流量控制

聚铭下一代防火墙支持基于接口的虚拟线路，网络管理员可以规定每个线路的带宽，作为流控的基准。在虚拟线路下，最多可支持 4 级通道的设定，满足网络管理员对不同部门及其下级机构设置具有层级关系的流量控制策略。每一级通道都可按照不同的用户、应用、地址和时间等，设置带宽限制、带宽保障、每 IP 带宽等等，并可允许在最大带宽范围内进行智能带宽借用（弹性带宽），在网络线路不繁忙时最大限度地利用网络带宽资源。

流控策略

+ 新建　↑上移　↓下移　刷新

线路名称	带宽管理(出)				带宽管理(入)				匹配条件					操作
	配置保障带宽	生效保障带宽	最大带宽	每IP	配置保障带宽	生效保障带宽	最大带宽	每IP	地址	用户	服务	应用	时间	
test	8M	8M	8M	0	8M	8M	8M	0						
网关产品线	1000K	1000K	1000K	0	1000K	1000K	1000K	0	any	any	any	any	always	
开发一组	500K	500K	500K	0	500K	500K	500K	0	any	any	any	any	always	
测试一组	300K	300K	300K	0	300K	300K	300K	0	any	any	any	any	always	
性能测试	100K	100K	100K	0	100K	100K	100K	0	any	any	any	any	always	

聚铭下一代防火墙支持带宽保障和弹性带宽功能。保障带宽是从总带宽中划分出一部分带宽为某种指定流量独享。保障带宽可以保证即使在网络繁忙时，指定流量也能够独占保证带宽。当网络中没有指定流量时，保障带宽部分

也能被其他网络流量使用。

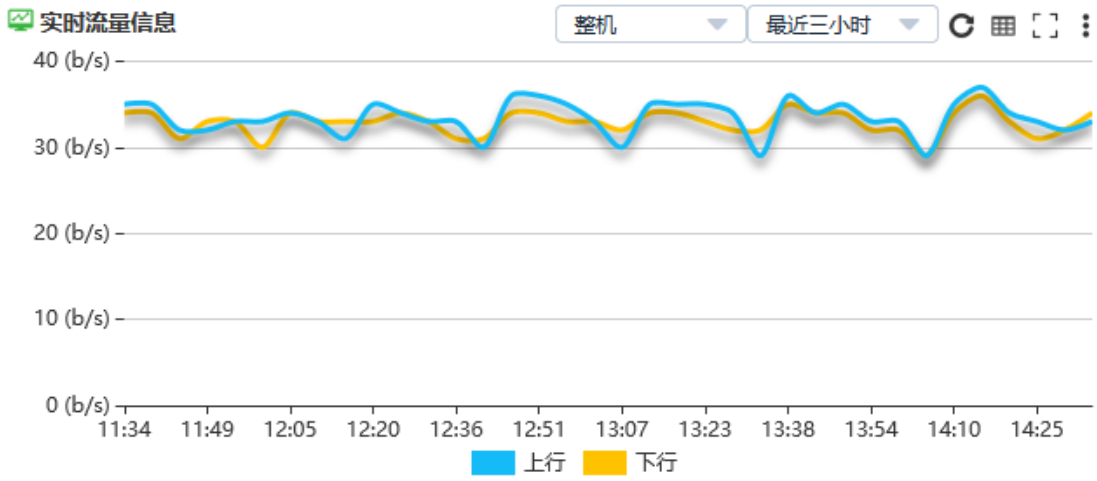
得益于强大的应用识别和用户识别功能，聚铭下一代防火墙可实现对P2P、流媒体等高带宽占用应用的有效限制，以及对 VOIP、即时通讯、网络游戏、邮件收发等低延迟需求进行有效的带宽保障。

3.11. 统计分析和安全可视化

统计分析与可视化是网络管理员有效管理网络的最有效工具。聚铭下一代防火墙提供了多种可视化统计分析功能。

3.11.1. 实时流量信息

整机实时流量图：

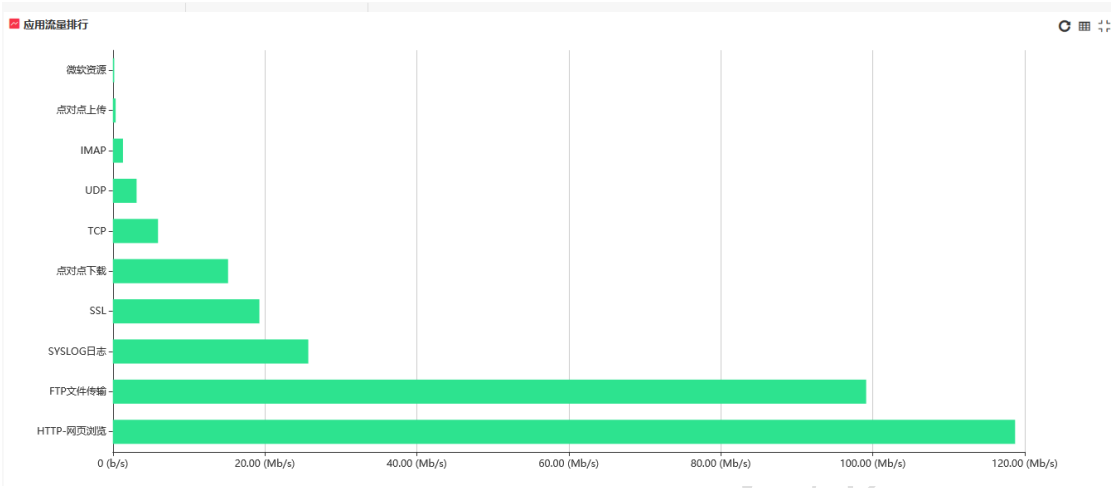


用户实时流量信息：


用户流量排名

用户	用户组	上行	下行	总转发率
124.200.190.62		34.99 (Mb/s)	17.29 (Mb/s)	52.28 (Mb/s)
192.168.0.201		5.84 (Mb/s)	37.46 (Mb/s)	43.30 (Mb/s)
172.17.10.178		5.01 (Mb/s)	35.82 (Mb/s)	40.83 (Mb/s)
172.17.120.78		11.90 (Mb/s)	0.00 (b/s)	11.90 (Mb/s)
172.17.0.254		3.06 (Mb/s)	0.00 (b/s)	3.06 (Mb/s)
172.16.200.36		77.42 (Kb/s)	1.32 (Mb/s)	1.40 (Mb/s)
172.19.0.238		11.66 (Kb/s)	147.70 (Kb/s)	159.36 (Kb/s)
172.17.110.1		15.77 (Kb/s)	40.99 (Kb/s)	56.77 (Kb/s)
211.101.36.78		50.09 (Kb/s)	990.63 (b/s)	51.08 (Kb/s)
172.17.40.95		9.05 (Kb/s)	36.61 (Kb/s)	45.66 (Kb/s)

应用实时流量信息：

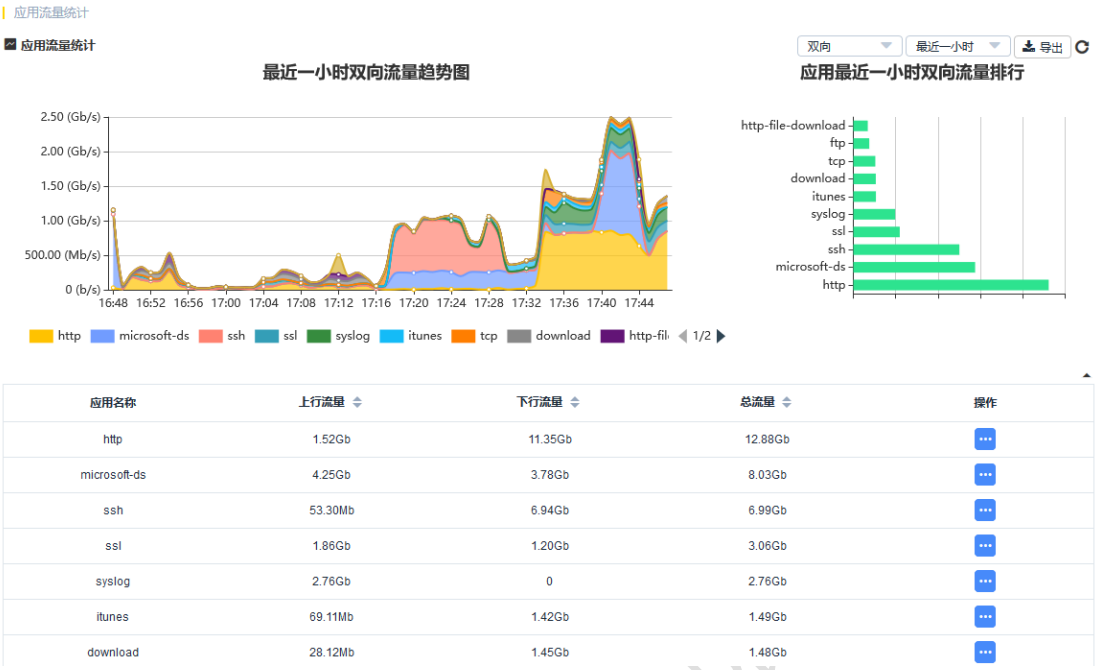


通过实时流量展现，可以方便直观地看到当前网络中的流量分布情况，便于对实时发生的流量异常状况进行定位和处理。

3.11.2. 深度流量分析

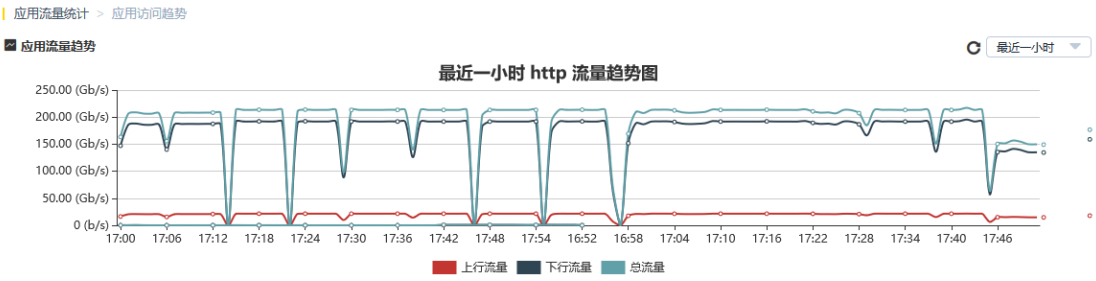
除了实时信息统计外，聚铭下一代防火墙还提供了对一段时间内流量分布情况进行统计分析的工具，方便网络管理员分析网络流量分布的时间、空间、用户、应用等多个维度的信息，并进行相应的决策和管理。

查看一段时间内所有应用流量统计信息：



应用名称	上行流量	下行流量	总流量	操作
http	1.52Gb	11.35Gb	12.88Gb	
microsoft-ds	4.25Gb	3.78Gb	8.03Gb	
ssh	53.30Mb	6.94Gb	6.99Gb	
ssl	1.86Gb	1.20Gb	3.06Gb	
syslog	2.76Gb	0	2.76Gb	
itunes	69.11Mb	1.42Gb	1.49Gb	
download	28.12Mb	1.45Gb	1.48Gb	

查看一段时间内特定应用的流量分布情况：



名称	上行流量	下行流量	总流量
172.17.10.178	826.08Mb	5.63Gb	6.43Gb
192.168.0.201	836.92Mb	5.49Gb	6.31Gb
124.200.190.62	65.36Mb	884.15Mb	949.51Mb
172.16.200.36	35.61Mb	611.03Mb	646.64Mb
172.16.0.68	18.76Mb	228.52Mb	247.28Mb
172.16.0.21	3.53Mb	84.97Mb	88.50Mb
172.19.0.238	4.03Mb	22.12Mb	26.15Mb
172.17.30.16	1.64Mb	17.81Mb	19.45Mb
172.18.100.222	1.81Mb	16.43Mb	18.23Mb
172.16.0.83	5.72Mb	12.42Mb	18.13Mb

查看所有用户的流量统计：

用户名	上行流量	下行流量	总流量	操作
124.200.190.62	4.34Gb	6.65Gb	11.00Gb	
192.168.0.201	906.49Mb	6.17Gb	7.06Gb	
172.17.10.178	882.86Mb	6.18Gb	7.04Gb	
172.18.17.191	52.47Mb	6.93Gb	6.98Gb	
172.16.0.163	4.23Gb	69.33Mb	4.30Gb	
172.16.0.20	15.46Mb	3.75Gb	3.77Gb	

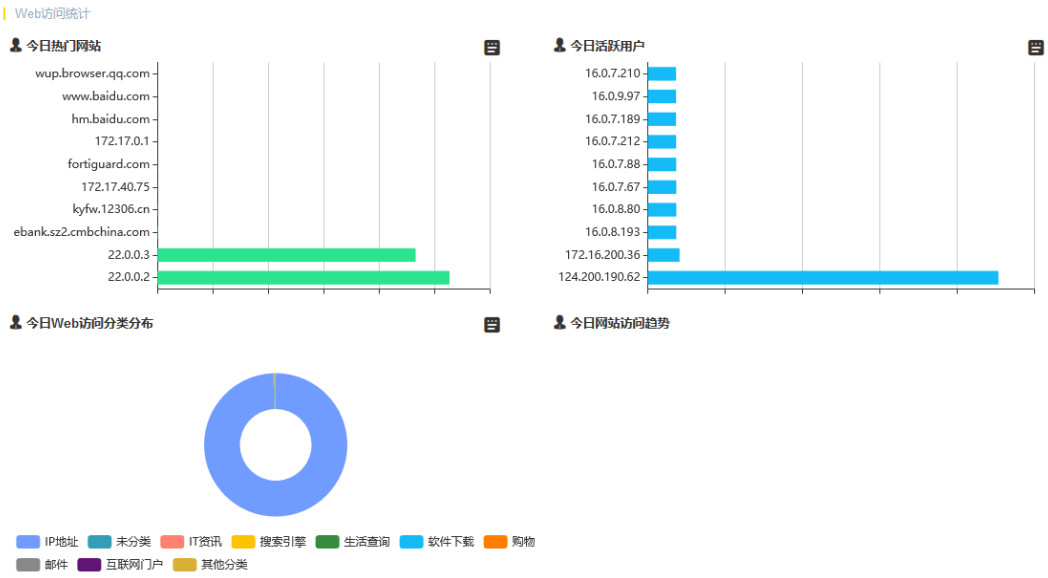
查看每个用户的上网行为统计：

3.11.3. 基于时间轴的日志展示

基于时间维度来索引用户的日志，方便用户查看最近一天、最近 24 小时、最近一周、最近 30 等的用户日志情况。

3.11.4. 多维度 Web 访问分类展现

聚铭下一代防火墙可展现今日 TOP 10 网站、TOP 10 用户、热门网络分类及网站访问趋势，可以基于用户、分类、网络三个维度进行关联分析。



3.11.5. 智能安全分析

聚铭下一代防火墙支持基于黑客地理位置和资产视角进行网络安全分析，依托于防火墙产生的攻击数据，从多个维度进行可视化数据分析，通过多种形式的图表展示，让网络情况清晰明了，只有“看清”网络安全，才能更有针对

性的进行安全决策和防护加固。

地域安全分析，通过整合统计全类别攻击数据，以攻击者 IP 为中心，分析攻击者的来源分布、攻击次数和攻击时间范围等，同时，还支持将攻击者 IP 一键加入黑名单，方便用户快速阻断攻击。

资产安全分析，基于资产视角，展示出每个资产的风险等级和防护状态等安全信息，同时，防火墙以资产为中心，根据攻击事件分析统计出资产的被攻击趋势、所受攻击的类别占比情况以及该资产所处攻击链状态，以此方便用户来了解资产的网络安全情况。

3.12. 智能管理

于企业而言，IT 运维的价值主要体现在对业务正常稳定的运行保障上，而随着网络的发展，网络越来越复杂，IT 运维的投入也越来越大，运维的效率和成本直接影响了企业效益，因此，对 IT 运维提效降本是企业迫切需要解决的问题。

3.12.1. 策略智能分析

基于上述问题，聚铭下一代防火墙支持智能策略分析、信息监控、故障定位等多种功能，以提升运维效率。策略分析能够自动实时检测出冗余策略、隐藏策略、冲突策略、可合并策略、空策略、过期策略等多种问题策略，同时给出优化建议，帮助管理员高效管理防火墙策略；同时防火墙支持对系统信息监控，如 CPU、内存、硬盘等异常情况，可自动告警通知；支持系统诊断信息和异常信息的收集和导出，帮助运维人员快速收集了解系统情况。

3.12.2. 智能云向管理

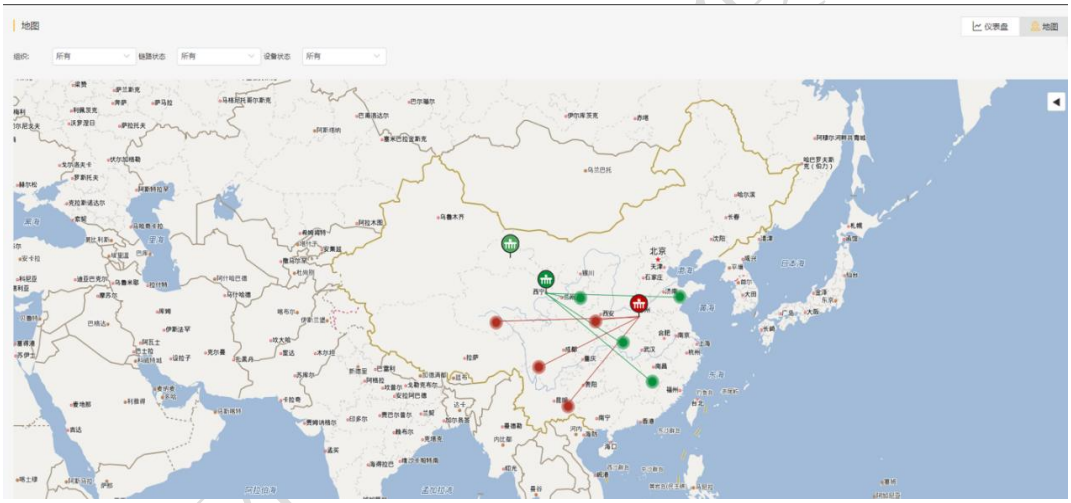
聚铭下一代防火墙既可以应用于互联网出口等边界部署场景，也可以作为 CPE 设备应用于 SD-WAN 场景。配合聚铭矩阵产品，基于 SD-WAN 思想，通过对业务的统一编排，集中运维，可视化管理，实现了软件定义企业分支机构及

云数据中心跨广域网的安全互联、链路优化、协同防护等，减轻了用户配置负担，降低了用户运维成本。

配合聚铭矩阵，聚铭下一代防火墙提供家用路由器级方式连通上线，即插即用；同时设备支持零接触配置，网络管理人员足不出户即可完成分支机构设备的管理和维护，运维周期单位从天数级骤降至分钟级。

3.12.3. 全局可视化

配合聚铭矩阵平台，可提供基于地图等可视化界面和报表，图形化呈现网络和设备状态。提升网络运维人员操作体验和工作效率。



3.13. 系统高可用性

- **硬件冗余：**聚铭下一代防火墙能够在核心网络中同所有网络设备一起构建高安全性及高可用性的拓扑结构，自身能够实现主主、主备部署和配置同步，能够实现动态的链路切换。同时提供了电源冗余功能，Bypass 切换功能，最大限度地满足了网络的健壮性及稳定性，保证了整个网络的不间断工作。

- **系统冗余：**支持双系统备份，当主系统启动失败或系统异常时，重新启动时可选择启动备份系统，恢复故障主系统，保障业务正常运转。同时支持多个配置文件的备份和恢复，避免因配置不当或系统异常导致的业务中断。

➢ **软件冗余：**支持链路备份功能，当所有可用负载分担链路发生故障或不可用时，可使用备份链路进行通信。防火墙还支持端口聚合功能，对多个物理接口进行绑定，实现流量的聚合，同时当其中一个或多个接口故障后，流量会转移到正常的接口进行通信，以此来实现冗余，提升网络的可靠性。

4. 典型组网

在部署方面，聚铭下一代防火墙支持传统的桥接、路由、旁路和混合部署模式，并可以 VNF 的形态部署在 NFV 环境中。配合聚铭云安全管理平台，可以支持各种主流大二层网络技术，重新定义云数据中心内部网络边界，使得安全防护成为可能。同时，通过 NFV 技术实现安全功能资源池化，部署更灵活，更具有弹性，可以根据业务按需扩展，解决单一设备性能瓶颈的问题。

4.1. 轻量型零信任安全

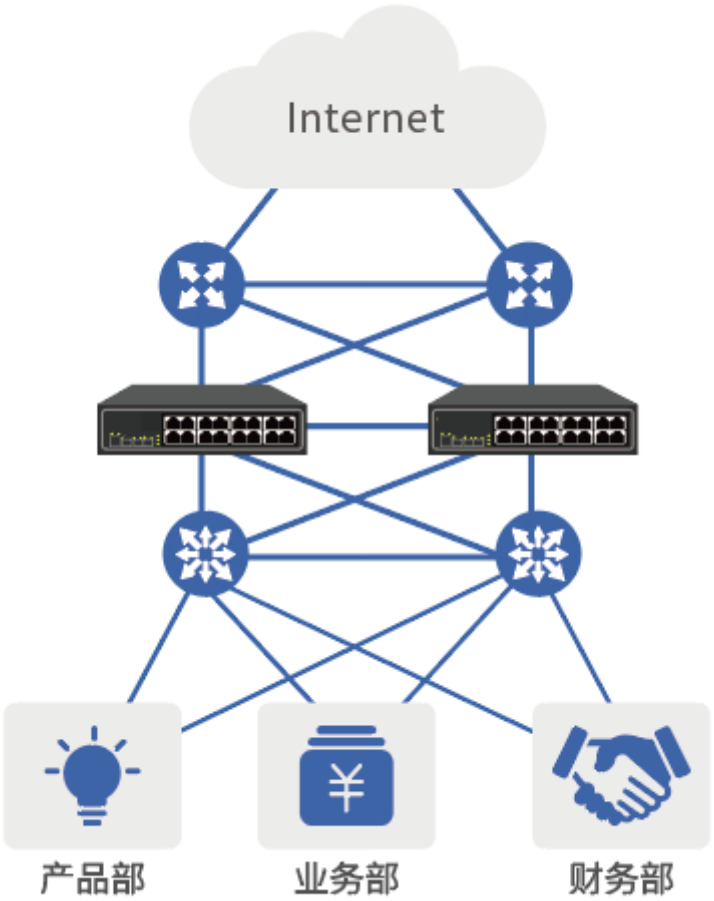
零信任代表着演进中的网络安全最佳实践，它打破传统的基于网络边界防护的理念，将防护重心从网络转移到内部资源上，无论用户位于什么物理/网络位置，均对其身份进行验证，并对用户可访问的内部资源做精细化的管控。

通过本地认证、第三方身份认证、访客认证等身份认证方式，验证每一位接入用户的身份。

基于用户身份进行内部资源的授权访问，严格控制该用户和资源的访问权限。

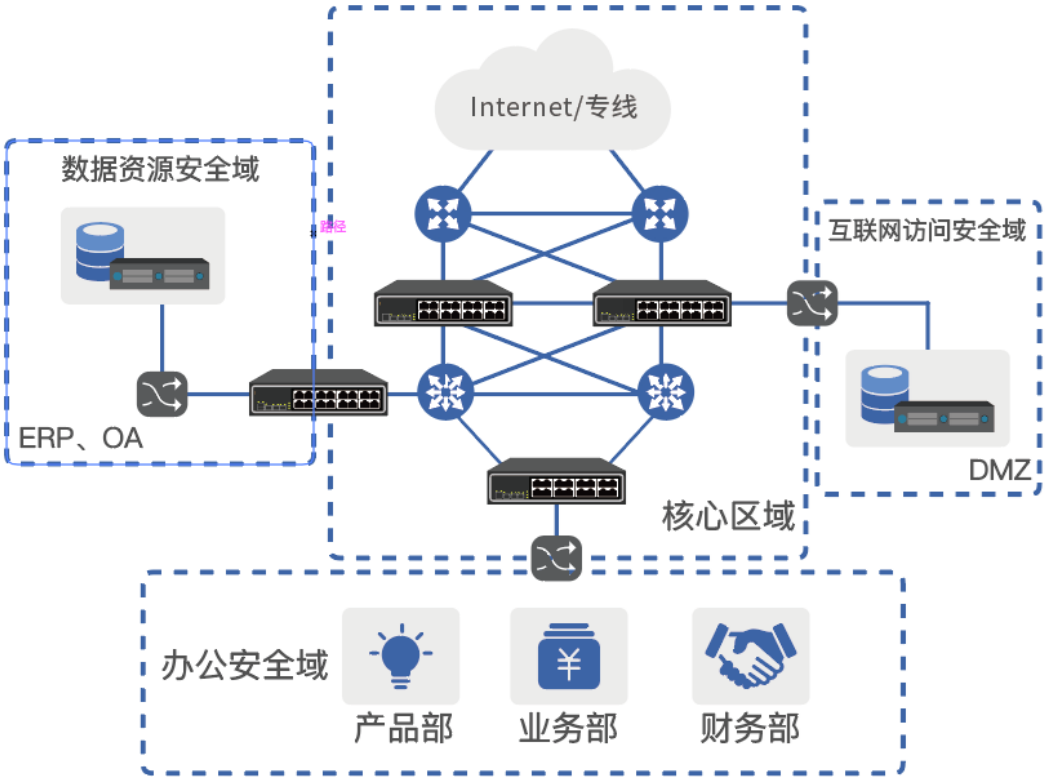
4.2. 网络出口安全防护

- 挑战：上网行为不可控，安全风险高 ；P2P 应用滥用，造成带宽浪费；外部威胁多，业务时刻面临着互联网带来的安全风险。
- 价值：全面抵御互联网威胁，精细化应用和上网行为管控；多链路负载调度及流量管理，提升业务和流量健壮性；支持会话级 HA，提高可靠性。



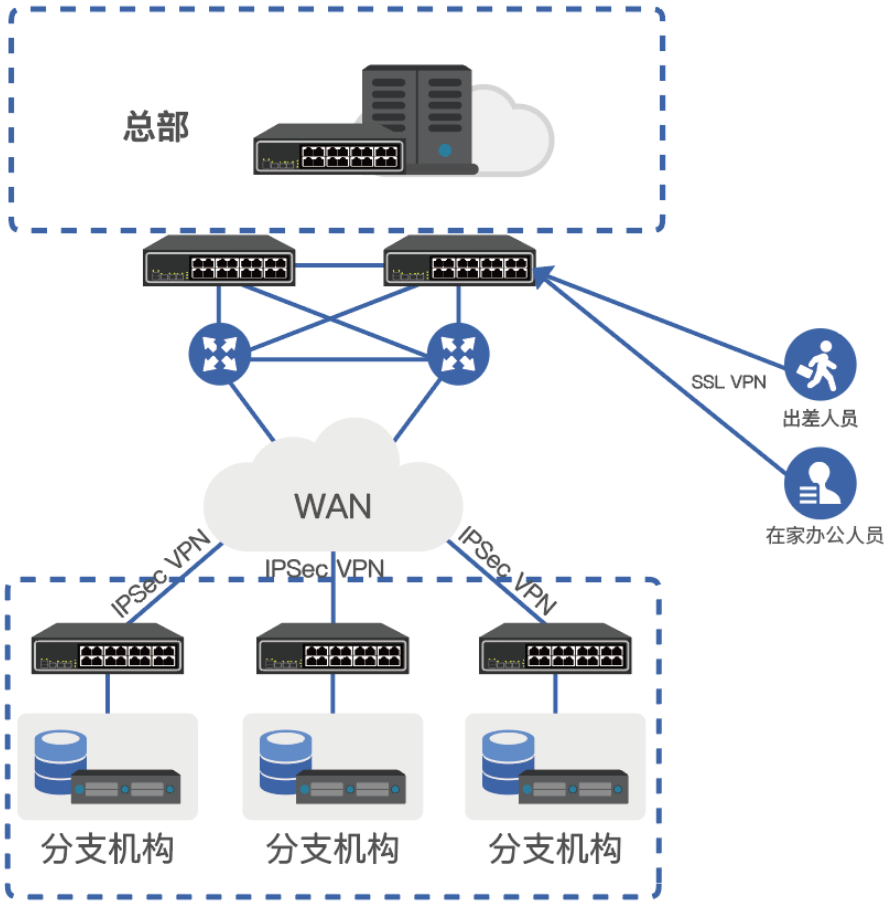
4.3. 域间安全隔离

- 挑战：员工跨区域越权访问企业核心资源系统；域间互访，流量无统计、不可视；内部员工恶意攻击传播安全风险。
- 价值：支持基于用户、应用、时间等多维度访问控制，防止网络威胁在不同域间蔓延，保护核心服务器业务安全；支持访问日志审计，满足企业合规要求。



4.4. 分支安全互联

- 挑战：出差员工和 SOHO 用户需要安全的访问内部资源；通过互联网进行数据传输容易被窃取和篡改；资源滥用，挤占关键业务带宽。
- 价值：高吞吐、低延时 VPN 安全连接；支持多种高性能 VPN，如 IPSec、SSL VPN 等，数据传输安全有保障；支持固网、4G/5G 双链路备份，出现故障自动切换；支持 WIFI 接入，满足分支办事处 BYOD 移动端接入需求。


总部
SSL VPN
出差人员
在家办公人员
WAN
IPSec VPN
IPSec VPN
IPSec VPN
分支机构
分支机构
分支机构