聚铭 VPN 安全网关

产品白皮书

聚铭网络科技有限公司

目录

1. 产品介绍 4

2. 关键技术 6

2.1. 系统架构 6

2.2. 多核并行处理技术 7

2.3. 一体化报文处理引擎 8

2.4. 基于用户、应用、终端和资源的控制策略 8

3. 产品特色功能 9

3.1 完善的 VPN 功能 9

3.1.1 组网能力 9

3.1.2 引流方式 10

3.1.3 智能选路 11

3.1.4 单臂连接 12

3.1.5 自动路由 12

3.1.6 客户端外网隔离 12

3.2 多样化用户识别 13

3.2.1 静态绑定 13

3.2.2 本地认证 13

3.2.3 Portal 认证 13

3.2.4 第三方认证 14

3.2.5 双因素认证 14

3.2.6 其他认证 14

3.3 安全一体化 15

3.4 精细化资源管控 15

3.5 上网行为管理 15

3.5.1 精准的应用控制 15

3.5.2 丰富的应用审计 16

3.5.3 强大的 Web 访问策略 17

3.6 全面的 IPv6 网络支持 17

3.7 HTTPS 深度检测 17

3.8 智能流量控制 18

3.9 统计分析和安全可视化 18

3.9.1 实时流量信息 18

3.9.2 深度流量分析 20

3.9.3 基于时间轴的日志展示 21

3.9.4 多维度 Web 访问分类展现 22

3.9.5 智能安全分析 22
3.10 系统高可用性 23
4. 典型组网 24
4.1. 分支安全互联 24
4.2. 轻量型零信任安全 24

声明

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

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. 产品介绍

VPN 安全网关是以现代密码技术为核心的传输安全设备，是一个具有物理安全保护措施的硬件设备，具有自主密钥管理机制，能将密码运算过程封装在其内部完成，为系统用户提供了完善的内部网络或应用程序的安全远程接入服务以及企业各分支机构局域网之间的端对端数据安全传输和安全访问。

VPN 安全网关提供 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、智能带宽管理，上网行为管控与审计等多重安全特性。 保证业务数据发送、接收到处理整个过程的安全性、有效性、完整性和不可抵赖性。

VPN 安全网关全面支持国产密码算法 SM1、SM2、SM3、SM4， 可广泛应用于金融、社保、能源、交通等行业。

2. 关键技术

2.1.系统架构

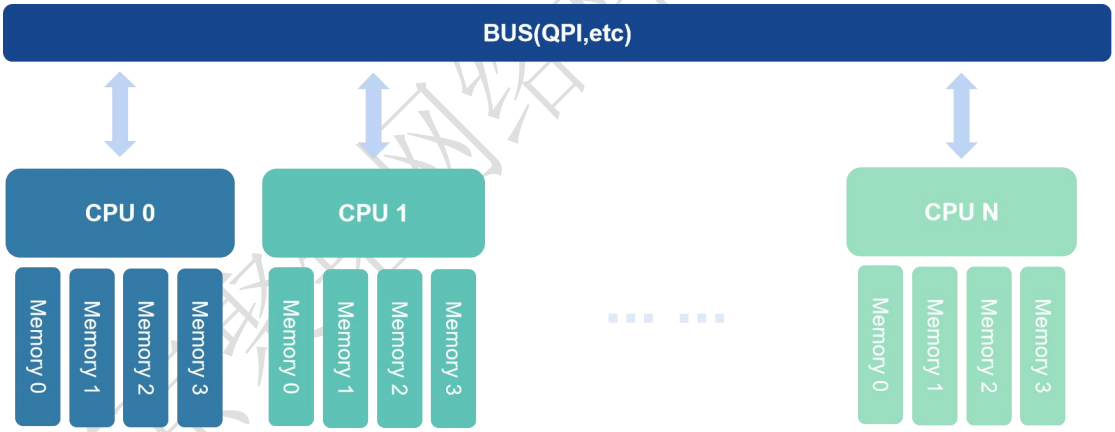
VPN 安全网关采用通用平台设计，对上层安全功能屏蔽硬件差异，提供统一的软件接口。因此，VPN 安全网关可运行于 X86、MIPS、ARM 及国产化多核平台上，或者基于上述平台的 KVM 和 VMware 虚拟化平台。在 Linux 的基础上着重增强了自身的安全性，并基于 UIO 技术对上层提供应用层零拷贝报文高速处理机制，显著提升了报文处理效率。

VPN 安全网关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，VPN 安全网关采用了先进的 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，VPN 安全网关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。

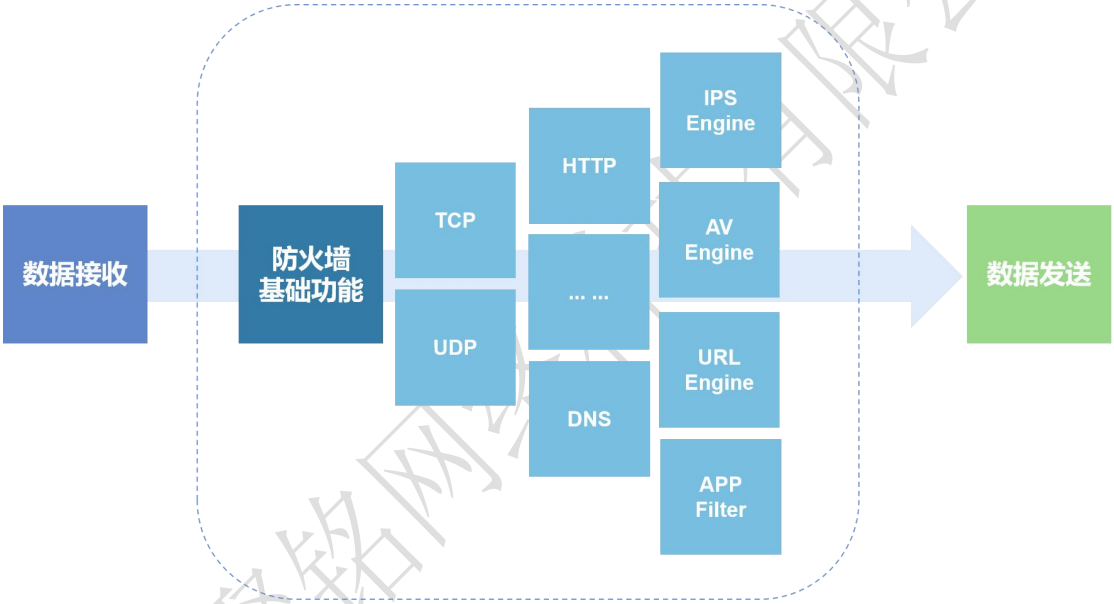
但是，数据包之间存在各种逻辑关系，例如应用层分片或者多连接应用。以往的基于多核技术的网络产品，有的会将数据包随机发送到各个处理核，忽略这种内在的逻辑关系，这样做的直接后果是无法正确处理应用层分片和多连接应用的相关业务，并且从现象上，经过该设备会出现较多的乱序报文。一个改进的做法是在特定的功能点（如 NAT、应用识别、内容审计）对特定的报文进行重组，报文在多个处理核之间传递（同时需要共享内存、共享流表等），需要使用锁等方式进行同步和互斥，对处理性能有较大影响。在 X86 平台下如果处理不当，还有可能造成跨节点访问，性能下降更加显著，甚至可能出现 CPU 核数越多，性能反而越低的现象。



通过智能分流器对流量进行分配。当数据包到达 VPN 安全网关时，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。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

认为，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 VPN 安全网关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。

VPN 安全网关提供了用户策略、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。

VPN 安全网关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 完善的 VPN 功能

VPN 安全网关支持主流的 VPN 技术，包括 IPSec VPN、SSL VPN、GRE、VXLAN、6in4 等；IPSecVPN 增加 SM1、SM2、SM3、SM4 国密算法的支持；具备专有的 VPN 接入客户端，同时支持多种平台，包括 Windows32 位/64 位、IOS、MAC、Android、国产化操作系统等，实现快捷安全互联。

VPN 安全网关能以网关模式、单臂模式进行部署；IPSecVPN 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。

3.1.1 组网能力

VPN 安全网关支持多种 VPN 解决方案，可以满足用户在不同场景下的组网需求，主要体现在以下几个方面。

- **隧道接口多元化：**支持以太网接口、聚合接口、VLAN 接口、4G/5G 接口、PPPoE 接口等多种类型的接口建立 VPN 隧道。

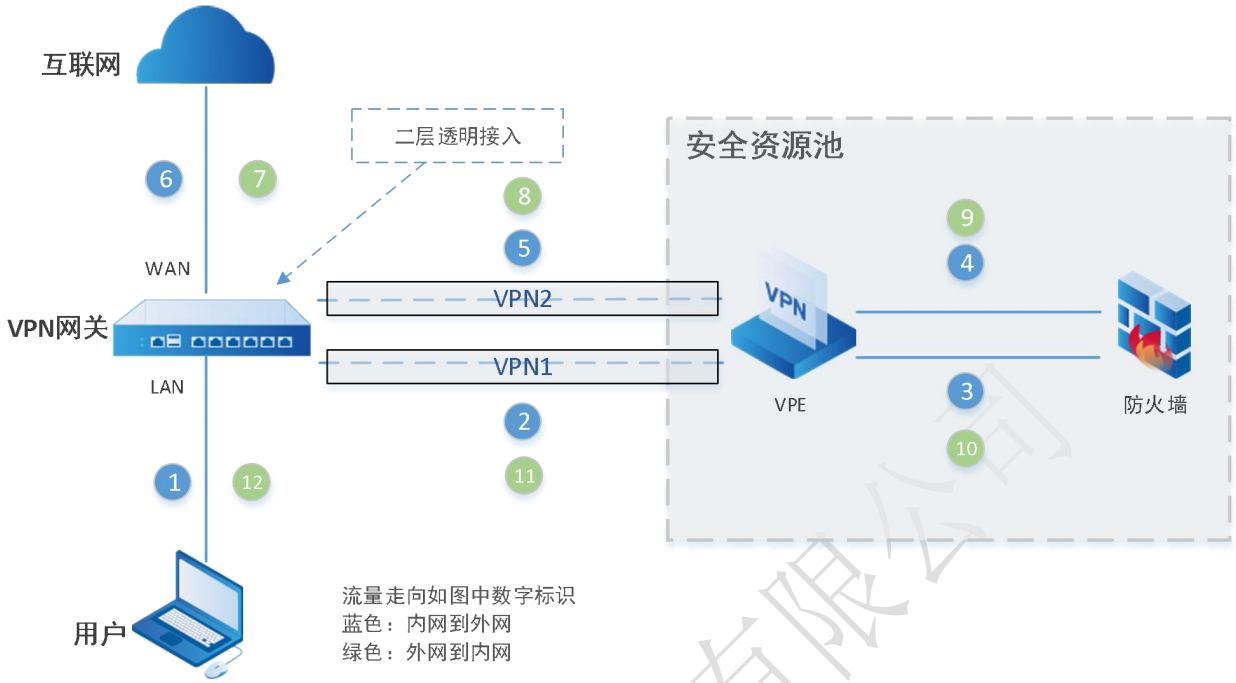
- **隧道类型多元化：** 支持丰富的 VPN 类型，包括：IPSec VPN、SSL VPN、GRE、VXLAN、6in4。
- **组网类型多元化：**支持多种组网形式，包括客户端到站点、站点到站点、Hub-Spoken、Full-Mesh 等。同时支持隧道备份和隧道负载。
- **算法多元化：**支持多种国际、国产密码算法，符合国家信息安全等级保护的要求。加密算法支持 DES、3DES、AES-128 (CBC/GCM)、AES-192 (CBC/GCM)、AES-256 (CBC/GCM)、SM1、SM4。认证算法支持 MD5、SHA1、SHA2-256、SHA2-512、SM3。
- **客户端多元化：**支持多种平台的客户端，包括 Windows32 位/64 位、IOS、MAC、Android、统信 UOS 等。

3.1.2 引流方式

VPN 安全网关支持多种引流方式，包括：静态路由引流、策略路由引流、引流策略。

当采用策略路由引流时，支持基于入接口、源安全域、源地址、目的地址、用户、服务、应用、时间等维度精细化控制进隧道的流量。

当采用引流策略引流时，支持在二层透明模式下基于入接口、源安全域、源地址、目的地址、用户、服务、应用、时间等维度精细化控制进隧道的流量。支持配置关联隧道实现将内网访问外网的流量引流到云端安全资源池进行流量清洗，清洗完后送回 VPN 安全网关，然后 VPN 安全网关再将流量转发到外网。使用场景示例图如下：

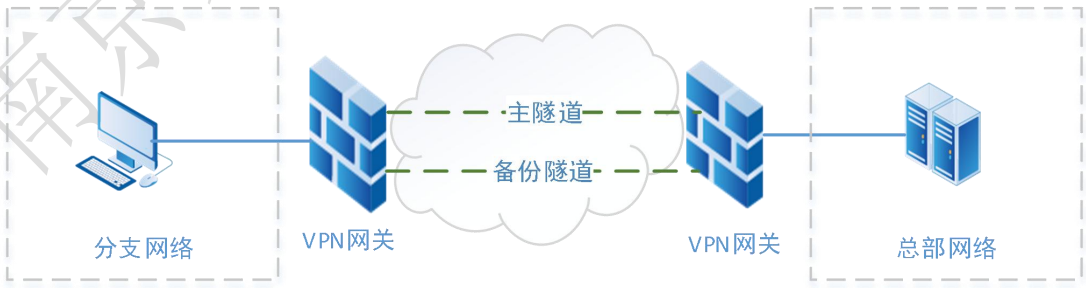


3.1.3 智能选路

VPN 安全网关支持智能选路功能，基于 5000+的精准应用识别和链路丢包、延时、抖动等参数的探测，在多条物理链路的场景中，实现多条 IPSecVPN 隧道间的备份和负载。

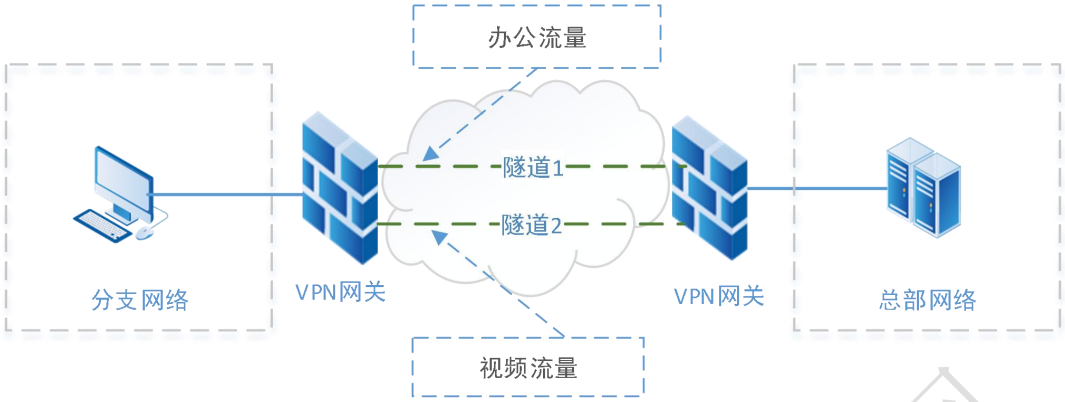
隧道备份场景：

在隧道备份场景中，对于主备链路上配置链路质量探测机制，当主隧道断开或探测链路质量下降时，则将业务流量动态切换到备份隧道，当主隧道恢复后再从备份隧道切换到主隧道。



隧道负载场景：

在隧道负载的场景中，可基于不同的用户、应用、服务等维度将流量在多条隧道中负载。



3.1.4 单臂连接

“单臂连接”模式下 VPN 安全网关作为 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。

3.1.5 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 VPN 安全网关的 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。

3.1.6 客户端外网隔离

VPN 安全网关支持“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 VPN 安全网关建立起加密隧道后，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。

3.2 多样化用户识别

VPN 安全网关智能用户识别，支持静态绑定、本地认证、第三方认证、微信认证、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。

3.2.1 静态绑定

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。VPN 安全网关支持本地认证和第三方认证两种方式。

3.2.2 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，VPN 安全网关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。

3.2.3 Portal 认证

VPN 安全网关支持提供完整的 Portal 认证解决方案。VPN 安全网关与 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 VPN 安全网关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，安全网关支持用户逃生，即无需认证即可进行上网。同时，用户在未认

证时，安全网关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。

3.2.4 第三方认证

VPN 安全网关支持 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，VPN 安全网关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，VPN 安全网关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 VPN 安全网关上。

3.2.5 双因素认证

VPN 安全网关在管理员登录和 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。安全网关支持动态口令认证、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，安全网关和 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，安全网关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，安全网关先校验证书的有效性，校验通过后，方可登录安全网关。

3.2.6 其他认证

VPN 安全网关还支持多种用户认证方式，包括微信认证、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。

3.3 安全一体化

VPN 安全网关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 精细化资源管控

VPN 安全网关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，基于安全网关用户策略，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。

3.5 上网行为管理

3.5.1 精准的应用控制

VPN 安全网关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。

3.5.2 丰富的应用审计

VPN 安全网关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

3.5.3 强大的 Web 访问策略

VPN 安全网关可以记录下 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。

3.6 全面的 IPv6 网络支持

VPN 安全网关支持全面的 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。

3.7 HTTPS 深度检测

VPN 安全网关的 HTTPS 审计功能，是基于 SSL 代理技术，对 HTTPS 加密流量进行解密，代理步骤如下：

- 安全网关截获客户端的 SSL 协商请求，作为服务器，使用自己的证书与客户端进行协商，建立与客户端的 SSL 隧道。
- 安全网关发起与真实服务器的 SSL 协商，建立与服务器的 SSL 隧道。
- 安全网关作为一个透明代理服务器，转发客户端与服务器的流量。从一边隧道收到的流量，先进行解密，再进行应用层安全检测，最后从另外一边的隧道加密发出。

在解密后可以做与普通 HTTP 相同的处置，提供全面的威胁防护，有效防御加密流量中的病毒、木马、蠕虫、恶意 URL 等网络威胁；精准识别加密流量中的行为与应用，进行精细化管控；同时还可对加密业务进行智能带宽管理。

3.8 智能流量控制

VPN 安全网关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	

VPN 安全网关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。

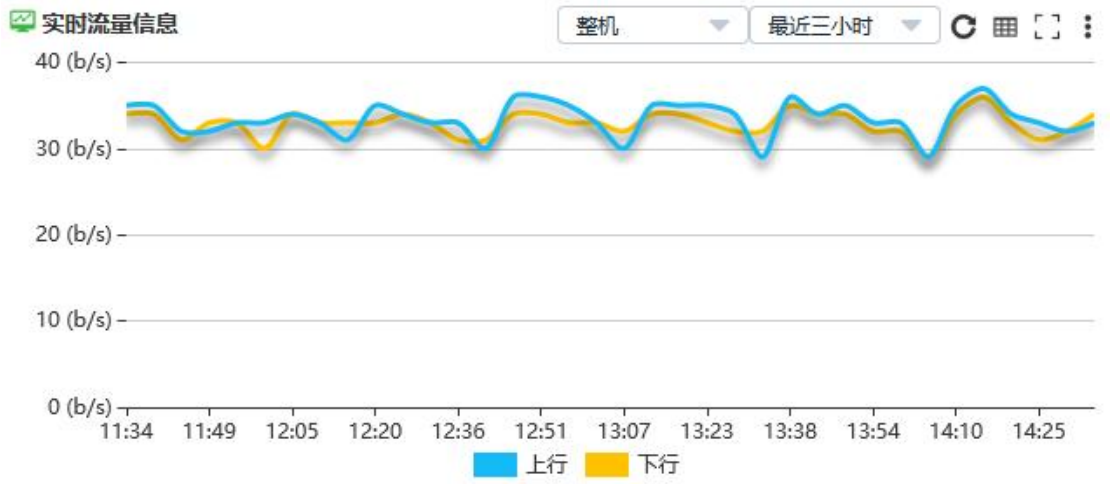
得益于强大的应用识别和用户识别功能，VPN 安全网关可实现对 P2P、流媒体等高带宽占用应用的有效限制，以及对 VOIP、即时通讯、网络游戏、邮件收发等低延迟需求进行有效的带宽保障。

3.9 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。VPN 安全网关提供了多种可视化统计分析功能。

3.9.1 实时流量信息

整机实时流量图：

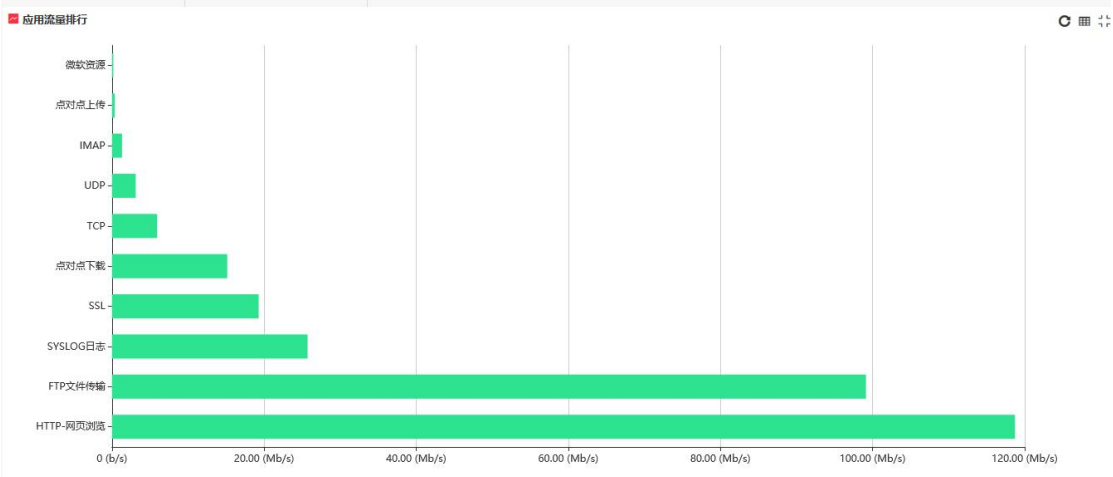


用户实时流量信息：

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：

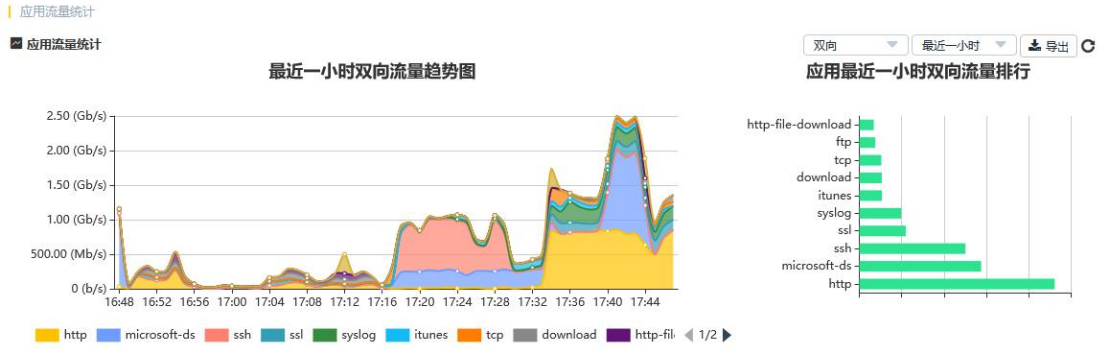


通过实时流量展现，可以方便直观地看到当前网络中的流量分布情况，便于对实时发生的流量异常状况进行定位和处理。

3.9.2 深度流量分析

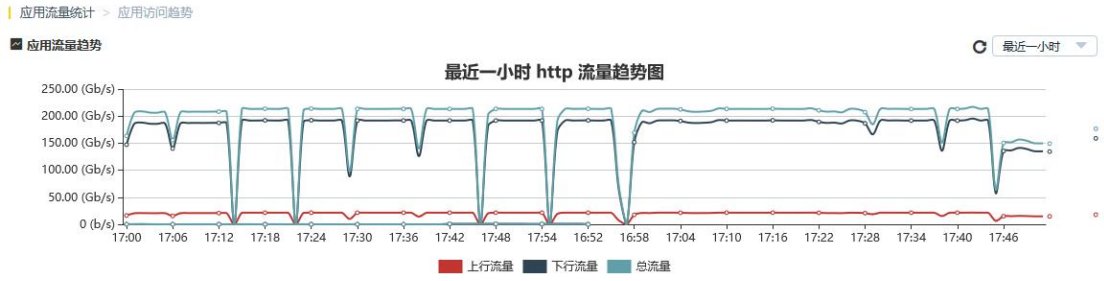
除了实时信息统计外，VPN 安全网关还提供了对一段时间内流量分布情况进行统计分析的工具，方便网络管理员分析网络流量分布的时间、空间、用户、应用等多个维度的信息，并进行相应的决策和管理。

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：

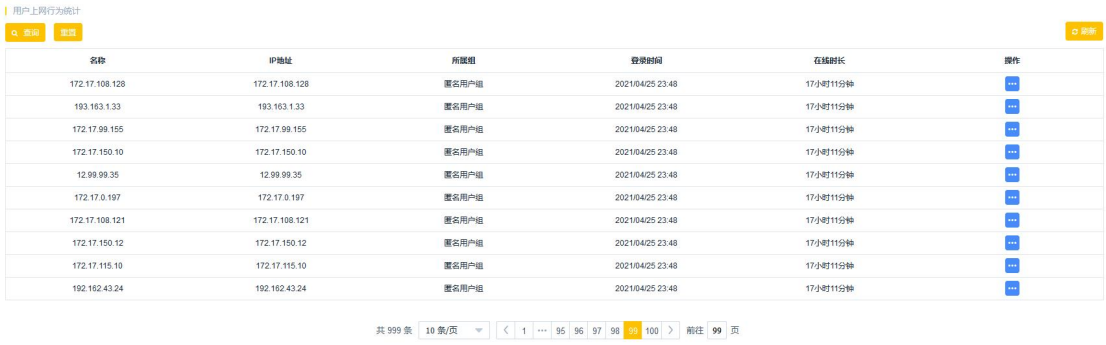


名称	上行流量	下行流量	总流量
172.17.10.178	826.08Mb	5.63Gb	6.43Gb
192.168.0.201	836.92Mb	5.49Gb	6.31Gb
124.200.190.62	65.36Mb	884.15Mb	949.51Mb
172.16.200.36	35.61Mb	611.03Mb	646.64Mb
172.16.0.68	18.76Mb	228.52Mb	247.28Mb
172.16.0.21	3.53Mb	84.97Mb	88.50Mb
172.19.0.238	4.03Mb	22.12Mb	26.15Mb
172.17.30.16	1.64Mb	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：

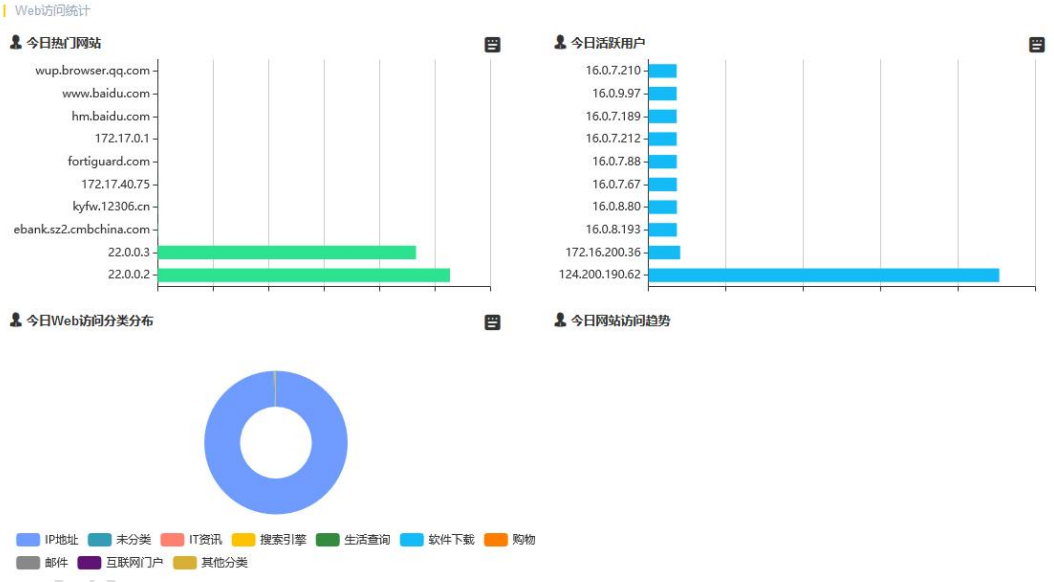


3.9.3 基于时间轴的日志展示

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 天等的用户日志情况。

3.9.4 多维度 Web 访问分类展现

VPN 安全网关可展现今日 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。



3.9.5 智能安全分析

VPN 安全网关支持基于黑客地理位置和资产视角进行网络安全分析，依托于安全网关产生的攻击数据，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，安全网关以资产为中心，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。

3.10 系统高可用性

硬件冗余：VPN 安全网关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。安全网关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，VPN 安全网关支持传统的桥接、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. 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。

4.2. 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。