JUMING 聚铭

JUMING 聚铭

聚铭下一代防火墙产品白皮书

聚铭网络科技有限公司

目录

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

1. 产品背景

1.1 网络安全威胁演变

随着数字化进程以迅猛之势加速，网络空间已然成为各方角逐的关键战场，网络攻击手段也随之呈现出日新月异的变化态势。

Check Point 公司发布的《2025 年网络安全报告》显示，全球网络攻击次数相较于去年同期呈现出惊人的 44% 增幅 。这一数据揭示了网络威胁生态系统正快速成熟且扩张，新型攻击手段层出不穷，给企业、机构乃至个人带来了前所未有的挑战。

从攻击类型来看，信息窃取程序攻击在 2024 年激增 58%。攻击者利用先进技术，精心设计各类信息窃取程序，从企业和个人设备中盗取敏感数据，如商业机密、用户账号密码、财务信息等。这类攻击增长迅猛，表明网络生态系统中攻击者的手段日益精进，他们通过精准定位目标，绕过多层防护，成功获取有价值的数据，并将其用于进一步的恶意活动，如数据贩卖、诈骗等。

勒索软件攻击模式也在不断演变。传统基于加密的攻击方式逐渐被数据泄露和勒索所取代。数据泄露勒索攻击不仅实施相对容易，攻击者可通过窃取企业核心数据，如客户信息、研发资料等，再以公开或售卖这些数据相威胁，迫使企业支付高额赎金，从而实现非法所得的最大化。医疗行业在这一趋势下深受其害，成为勒索软件攻击的第二大目标，所遭遇的攻击次数同比增长 47%。医疗数据的敏感性和重要性使得医疗机构成为攻击者眼中的 “肥肉”，一旦数据泄露，不仅会对患者隐私造成极大损害，还可能导致医疗机构面临法律诉讼和声誉损失。

教育行业则连续第五年成为网络攻击的首要目标，攻击次数同比增长 75%。校园网络环境复杂，学生和教职工安全意识参差不齐，加上学校拥有大量有价值的数据，如学生学籍信息、科研成果等，吸引了众多攻击者。例如，一些黑客通过在校园周边设置伪装成 “校园免费网络” 的恶意 Wi-Fi 热点，诱导学生连接。某高校学生小李在校园附近咖啡馆连接名为 “Campus-Free-WiFi” 的网络后，教务系统账号被盗，课程信息被篡改，黑客甚至通过邮件勒索赎金。此类攻击不仅影响学生正常学习生活，也对学校的教学秩序和声誉造成严重冲击。

从漏洞利用角度而言，2024 年，高达 96% 的漏洞利用攻击利用的是前一年披露的漏洞 。这一现象凸显了企业和机构在漏洞管理方面存在严重不足。许多组织未能及时对已知漏洞进行修复，使得攻击者能够轻易利用这些漏洞发动攻击。同时，攻击者在漏洞利用手

段上不断创新。在 2024 年的攻防演练期间，共监测到 197 个有攻击代码披露的漏洞 。他们越来越多地利用逻辑类和传输加密类 0day 漏洞，此类漏洞由于尚未被广泛知晓，防御者难以察觉，使得攻击具有更高的隐蔽性。攻击者还将战前储备 0day 漏洞与后期新挖掘 0day 相结合，并倾向于通过多个 0day、Nday 组合利用，开发自动化攻击工具形成攻击链，极大增强了攻击的有效性和危害性。

在攻击源方面，边缘设备成为了新的重灾区。受感染的路由器、VPN 及其他边缘设备已成为攻击者入侵企业网络的关键切入点。据统计，超过 200,000 台设备已被 Raptor Train 等超大型攻击者运营的高级僵尸网络控制 。这些被控制的边缘设备如同隐藏在网络中的 “定时炸弹”，攻击者可通过它们发动大规模的 DDoS 攻击，或进一步渗透进入企业内部网络，窃取敏感信息。

国际层面，国家间的网络攻击事件也频繁发生。2022 年 4 月 12 日，西北工业大学电子邮件系统遭境外黑客网络攻击 。经调查，此次攻击源头系美国国家安全局（NSA）。美国 NSA 下属特定入侵行动办公室（TAO）在近年里对中国国内网络目标实施了上万次恶意网络攻击，控制了数以万计的网络设备，窃取了超过 140GB 的高价值数据 。美方先后使用 41 种专用网络攻击武器装备，对西北工业大学发起攻击窃密行动上千次，严重危害了中国国家安全和公民个人信息安全。

传统防火墙在面对一系列新型威胁时，逐渐暴露出诸多局限性，显得捉襟见肘。例如，高级持续威胁（APT）攻击具备极强的隐蔽性与持续性，常常巧妙利用零日漏洞，悄无声息地潜入系统内部，宛如隐匿于暗处的 “间谍”，长时间潜伏并持续窃取敏感信息，给企业和组织带来难以估量的损失。应用层攻击则将矛头精准指向 Web 应用、数据库等核心业务系统，像 SQL 注入攻击，通过精心构造恶意 SQL 语句，非法获取、篡改甚至破坏数据库中的关键数据；跨站脚本攻击（XSS）则利用 Web 应用程序对用户输入过滤不足的漏洞，在用户浏览页面时植入恶意脚本，进而窃取用户会话信息、实施钓鱼攻击等，这些攻击方式能够轻松绕过传统基于端口和 IP 的防护机制，犹如在坚固城墙下挖出的隐秘地道。而加密技术的广泛普及，虽然在很大程度上保障了合法数据传输的安全性，但也不幸被攻击者所利用。恶意软件如今频繁借助加密通道进行传播与躲避检测，它们如同披上了一层“隐形外衣”，使得传统依赖明文检测的安全防护手段难以察觉其踪迹，极大地增加了网络安全防护的难度与复杂性。

1.2 企业安全需求升级

企业的运营模式与技术架构不断革新，这也促使企业安全需求从传统范畴向更为多元和复杂的领域拓展。以下从通用安全场景、云计算场景、工控场景、物联网场景、合规场景等多个维度，深入剖析企业安全需求的升级态势。

1.2.1通用安全场景

企业内部网络作为业务流转的基石，面临着来自内部员工不当操作与外部黑客蓄意攻击的双重威胁。在内部，员工可能因疏忽或安全意识淡薄，点击恶意链接、下载不明来源软件，致使恶意软件入侵企业网络，进而在内部肆意传播，导致数据泄露、系统瘫痪等严重后果。外部攻击者则常常试图利用网络协议漏洞、弱密码等途径，非法闯入企业网络，窃取商业机密、客户信息等关键数据，对企业的核心竞争力与商业信誉造成沉重打击。因此，企业急需能够全方位监测网络流量、精准识别异常行为，并迅速响应阻断威胁的安全防护体系，以保障内部网络的稳定与安全。

1.2.2云计算场景

随着企业逐步向云端迁移核心业务，云计算场景下的安全需求愈发凸显。在数据存储方面，企业的数据分散存储于云端不同区域，如何确保数据在存储过程中不被非法访问、篡改或泄露，成为首要难题。例如，一些云服务提供商的存储系统可能存在安全漏洞，若企业数据存储其中，极易成为攻击者的目标。同时，数据在本地与云端之间传输时，也面临着传输链路被劫持、数据被窃取或篡改的风险。此外，多租户环境下的资源隔离与权限管理也至关重要。不同企业在同一云平台上租用资源，若隔离措施不到位，可能导致租户之间的信息泄露。企业需要云防火墙、云加密技术等多种手段，保障云环境下数据全生命周期的安全，以及资源的合理分配与使用。

1.2.3工控场景

工业控制系统广泛应用于制造业、能源等关键领域，其安全性直接关系到国家经济命脉与社会稳定。在工控场景中，工业设备之间通过特定的工业协议进行通信，这些协议往往存在历史遗留的安全漏洞，如早期的 Modbus 协议缺乏有效的认证与加密机制，容易被攻击者利用来篡改设备控制指令，进而影响生产流程的正常运行，甚至引发生产事故。同时，工控系统的更新换代相对缓慢，难以快速适应新的安全威胁。此外，随着工业互联网的发展，工控系统与外部网络的连接日益紧密，这使得攻击者有更多机会渗透进入工控网络。企业必须针对工控系统的特点，制定专门的安全防护策略，包括工业协议深度检测、设备身份认证、安全隔离等措施，确保工控系统的安全稳定运行，保障生产活动的连续性。

1.2.4物联网场景

物联网设备在企业中的大规模应用，如智能传感器、智能摄像头等，为企业运营带来了便利，但也带来了诸多安全隐患。物联网设备通常资源有限，难以运行复杂的安全防护软件，这使得它们容易成为攻击者的突破口。攻击者可通过破解设备密码、利用设备固件漏洞等方式，控制物联网设备，进而入侵企业网络。例如，一些智能摄像头若存在安全漏洞，攻击者可远程获取摄像头拍摄的视频画面，甚至控制摄像头转向，窥探企业内部情况。而且，大量物联网设备产生的海量数据在传输与存储过程中，也面临着数据泄露风险。企业需要构建针对物联网设备的全生命周期安全管理体系，涵盖设备身份识别、固件安全更新、数据加密传输与存储等方面，以保障物联网环境下企业资产与信息的安全。

1.2.5合规场景

在法律法规日益完善的今天，企业面临着严格的合规要求。不同行业有着各自的合规标准，如金融行业需遵循《支付卡行业数据安全标准》（PCI DSS），保护客户支付信息安全；医疗行业要符合《健康保险流通与责任法案》（HIPAA），确保患者医疗数据的隐私与安全。企业一旦违反这些合规要求，将面临巨额罚款与声誉损失。企业不仅要保障自身业务系统的安全，还需通过技术手段与管理措施，确保安全防护体系符合相关法律法规的要求。这包括建立完善的安全审计机制，定期对网络活动进行审计与记录；加强员工的合规培训，提高员工对合规要求的认知与遵守意识；采用符合合规标准的安全技术产品与解决方案，如加密技术、访问控制技术等，以应对日益严格的合规监管。

2. 产品概述

2.1 产品定义与定位

聚铭聚铭下一代防火墙是一款打破传统防火墙功能边界，融合了多元先进安全技术的综合性安全设备。它深度整合网络防护、应用识别、入侵检测与防范以及数据安全保护等关键能力，不再局限于简单的网络层访问控制。在网络防护方面，它突破传统端口与 IP 地址的限制，对网络流量进行全面、深入的检测与过滤。应用识别功能可精准洞察网络中的各类应用程序，无论其采用何种端口或加密方式，都能准确识别，包括新兴的小众应用以及不断变种的恶意应用。入侵检测与防范技术更是通过多维度检测机制，实时捕捉并阻断各类网络攻击行为。数据安全保护则贯穿数据的传输、存储与使用全生命周期，确保企业核心数据的保密性、完整性与可用性。

2.1.1 产品定位

面向多元用户群体：主要面向企业、政府机构、金融组织等对网络安全有高要求的用户群体。企业在数字化转型进程中，面临着复杂多变的网络威胁，聚铭下一代防火墙可保障其内部网络稳定，助力业务持续高效开展，无论是传统企业的信息化升级，还是新兴互联网企业的快速扩张，都能提供坚实的安全支撑。政府机构处理大量关乎国计民生的重要数据，对网络安全的可靠性与合规性要求极高，聚铭下一代防火墙能满足其严格的安全防护标准，确保政务信息系统安全稳定运行，维护政府公信力。金融组织涉及海量金融交易数据与客户隐私信息，安全风险容不得半点疏忽，聚铭下一代防火墙为其构建严密的安全防线，抵御各类金融攻击，保障金融秩序稳定。

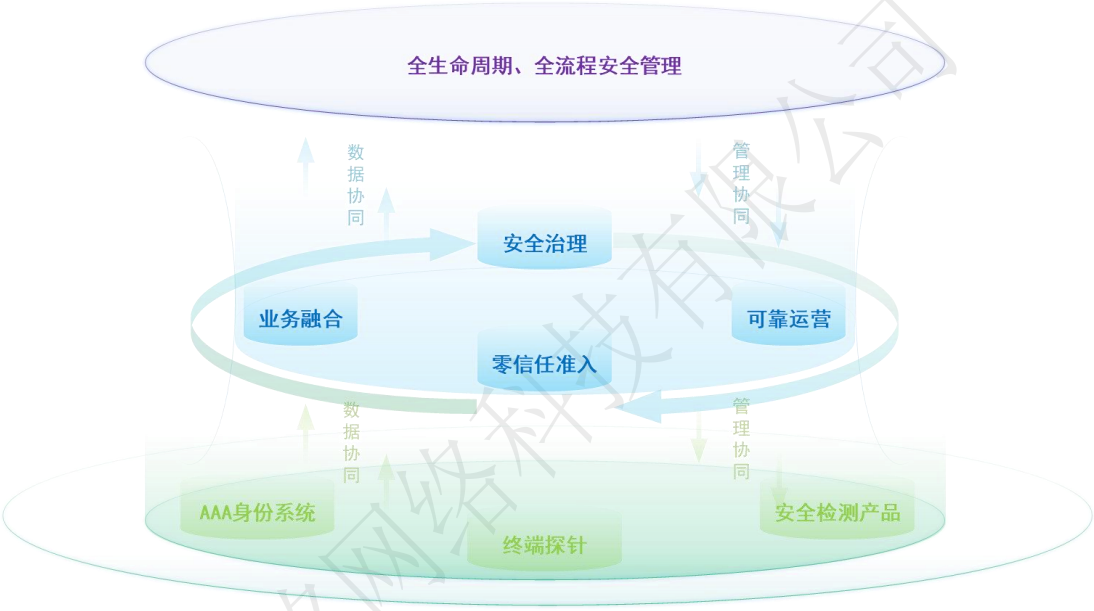
应对复杂网络威胁：在当前网络安全威胁日益复杂的大环境下，聚铭下一代防火墙定位于提供全方位、多层次的网络安全防护。面对高级持续威胁（APT），它凭借深度包检测技术与威胁情报集成功能，能够深入分析网络流量，及时发现并阻断潜伏在系统中的恶意程序，防止敏感信息被长期窃取。针对应用层攻击，如 SQL 注入、跨站脚本攻击（XSS）等，借助强大的应用识别与入侵检测防范技术，精准识别攻击特征，迅速采取阻断措施，保护 Web 应用、数据库等关键业务系统安全。在加密流量安全防护方面，可穿透加密通道，识别其中隐藏的恶意软件与非法应用，有效应对加密技术被攻击者利用的安全挑战。

保障业务连续性与数据安全：保障业务连续性与数据安全是聚铭下一代防火墙的核心定位之一。它通过实时监测网络流量，及时发现并解决潜在的安全问题，避免因网络攻击导致业务中断，确保企业关键业务应用（如 ERP、CRM 系统）始终正常运行。在数据安全保护上，从数据在网络中的传输，到存储于企业内部或云端的数据，都提供加密、访问控

制等多重防护手段，防止数据泄露、篡改，维护数据的完整性与保密性，为企业的可持续发展奠定坚实基础。

2.2 产品框架

聚铭下一代防火墙产品架构围绕全生命周期、全流程安全管理展开，以安全治理、业务融合、可靠运营和零信任准入为核心环节，通过数据协同和管理协同，整合底层的 AAA 身份系统、终端探针和安全检测产品，形成一个有机的整体。这种架构设计旨在应对当今复杂多变的网络安全威胁，为企业提供全方位、多层次的安全防护。



2.2.1 产品架构核心环节

以零信任准入为基础，融合场景化业务，提供网络边界安全治理机制，安全协同可靠运营，实现全生命周期、全流程安全管理。

2.2.1.1 零信任准入

零信任准入是聚铭下一代防火墙架构中的基础理念，它摒弃了传统的 “信任内部网络”的观念，对所有的网络访问请求都进行严格的身份认证和安全检查。

持续认证：在用户或设备接入网络后，持续对其身份和安全状态进行检测。除了初始的身份认证外，还会根据用户的行为、设备的状态等因素，实时进行动态认证。如果用户的行为出现异常，或者设备的安全状态发生变化，如未安装最新的杀毒软件，零信任准入机制可以及时发现并采取相应的措施，如限制访问权限或强制其进行安全修复。

最小权限原则：根据用户的身份和业务需求，为其分配最小的访问权限。用户只能访问其工作所需的资源，避免因权限过大而导致的安全风险。例如，普通员工只能访问与自

己工作相关的文件和应用程序，而不能访问企业的核心机密数据。通过最小权限原则，可以有效降低数据泄露和越权访问的风险。

区域隔离：将整体网络划分为多个微小的安全区域，对每个区域进行独立的访问控制和安全管理。不同区域之间的访问需要经过严格的认证和授权，即使攻击者成功入侵了某个区域，也难以在整个网络中扩散。区域隔离技术可以有效防止内部网络中的横向移动攻击，提高网络的整体安全性。

2.2.1.2 业务融合

在当下数字化办公与业务拓展的进程中，聚铭下一代防火墙所具备的网络建设、智能流控、智能选路、安全组网等价值，与企业业务深度融合，在提升业务效率和安全方面发挥着关键作用。

从网络建设来看，企业业务形态各异，对网络需求也不尽相同。聚铭下一代防火墙可助力构建定制化网络架构，如为连锁企业实现总部与门店间安全且高效的数据交互，通过 VPN 加密传输保障交易数据安全，同时针对门店复杂网络环境，合理区分管理业务流量，优先保障收银等关键业务带宽，确保业务连续性。

智能流控功能则能精准匹配业务需求。企业核心业务如在线交易、视频会议等对网络要求苛刻，智能流控可依据优先级精细管理流量，在网络拥塞时也能保障关键业务流畅运行。同时，还能识别与工作无关的应用，限制其在工作时间占用带宽，将资源集中于工作相关应用，显著提升员工工作效率。

智能选路可确保业务数据快速传输。企业业务数据在不同节点间交互频繁，聚铭下一代防火墙能实时监测网络链路状态，依据带宽利用率、延迟等指标，自动选择最优路径，避免数据传输中断。在多云业务部署场景下，还能综合考量云平台性能、成本等因素，灵活调度业务，实现多云间高效互联。

安全组网为业务开展筑牢安全防线。企业业务网络面临内外部多重安全威胁，防火墙通过严格的访问控制策略，限制非法访问，审计内部操作，集成 IDS/入侵防御功能功能实时监测异常，保障网络安全稳定。在与合作伙伴协同业务时，借助安全的 VPN 连接实现数据安全共享，精细管理访问权限，保护商业机密，促进业务合作顺利推进 。

2.2.1.3 安全治理

在数字化时代，企业面临着复杂多变的网络安全威胁，聚铭下一代防火墙的安全治理功能基于用户和业务制定精准的访问权限，进行全面的安全检测与防护，并依据安全现状

进行安全定级，直观呈现安全风险，为企业构建起坚实的网络安全屏障。

基于用户和业务制定访问权限是安全治理的基础。企业内部用户角色多样，从普通员工到管理层，不同角色对业务资源的访问需求差异明显。同时，企业的各类业务系统，如财务系统、研发系统等，重要性和敏感性也各不相同。聚铭下一代防火墙能够深入分析用户的身份信息、部门属性以及业务的安全需求，为用户和业务制定精细化的双向访问权限策略。例如，只允许财务部门的特定人员访问财务系统，且限制其操作权限，防止越权操作和数据泄露；对于研发业务，仅开放给相关的研发人员，并严格控制外部访问，确保核心技术的保密性。

全面的安全检测和防护是安全治理的关键环节。防火墙运用深度包检测（DPI）、入侵检测与防范（IDS/入侵防御功能）等先进技术，对网络流量进行全方位监测。不仅能识别常见的网络攻击，如 SQL 注入、DDoS 攻击等，还能检测出隐藏在加密流量中的恶意行为。一旦发现安全威胁，防火墙会立即采取阻断、隔离等措施，防止攻击扩散，保障业务系统的正常运行。

基于安全现状的安全定级以及直观呈现安全风险，让企业对自身的安全状况一目了然。聚铭下一代防火墙会综合评估网络中的资产价值、漏洞情况、威胁来源等因素，对企业的安全现状进行科学定级。同时，通过直观的可视化界面，将安全风险以图表、报告等形式呈现出来，如展示不同区域的安全威胁分布、各类风险的占比等。企业管理者可以根据这些信息，清晰地了解安全薄弱环节，有针对性地制定改进措施，合理分配安全资源，提升整体安全防护水平。

2.2.1.4 可靠运营

在网络安全体系中，聚铭下一代防火墙的可靠运营至关重要。通过 SNMP、Syslog、API 等接口，防火墙能与各类安全产品及管理平台实现安全协同，为企业网络的可靠运营提供全方位保障。

SNMP（简单网络管理协议）接口是防火墙与管理平台实现高效通信的桥梁。借助 SNMP，管理平台可以实时获取防火墙的运行状态信息，包括 CPU 使用率、内存占用情况、网络接口流量等。这些数据能帮助管理员及时发现防火墙性能瓶颈，如在业务高峰期，若发现 CPU 使用率持续过高，可及时调整策略或增加硬件资源，确保防火墙稳定运行。同时，防火墙也能通过 SNMP 接收管理平台的配置指令，快速调整安全策略，应对不断变化的网络威胁，实现对网络的精细化管理。

Syslog 接口则在日志管理和安全事件追溯方面发挥着关键作用。防火墙产生的大量日志信息，如访问记录、攻击检测日志等，可通过 Syslog 接口发送至日志管理系统或其他安全产品。安全团队能够对这些日志进行集中分析，从中挖掘潜在的安全风险和异常行为。例如，通过分析访问日志，发现某个 IP 地址频繁尝试登录关键业务系统且失败次数较多，可能是遭受暴力破解攻击，进而及时采取措施进行防范。此外，详细的日志记录也为安全事件的事后追溯提供了有力证据，便于查明事件原因和责任。

API（应用程序编程接口）为防火墙与其他安全产品的深度集成提供了可能。防火墙可以通过 API 与入侵检测系统、防病毒软件等安全产品进行数据共享和功能协同。当入侵检测系统发现可疑流量时，可通过 API 将相关信息快速传递给防火墙，防火墙立即对该流量进行阻断或进一步检测；防病毒软件检测到恶意文件时，也能借助 API 通知防火墙，阻止文件的传输路径。这种协同机制大大增强了安全防护的及时性和有效性，形成一个有机的安全防护整体，共同保障企业网络的可靠运营，抵御各种复杂的网络安全威胁。

2.2.2 数据协同、管理协同

2.2.2.1 数据协同

在聚铭下一代防火墙架构中，各个组件之间实现数据的共享和交互，通过整合和分析不同来源的数据，提高安全检测和防护的准确性和有效性。

信息共享：AAA 身份系统、终端探针和安全检测产品将收集到的用户身份信息、设备状态信息、网络行为数据和安全事件等，实时共享给安全治理、业务融合、可靠运营和零信任准入等核心环节。这些信息为各个核心环节的决策和操作提供了丰富的数据支持，例如，安全治理可以根据这些数据制定更精准的安全策略；业务融合可以根据用户身份和网络行为数据，对业务应用进行更合理的访问控制。

数据分析与挖掘：通过对共享数据的综合分析和挖掘，发现潜在的安全威胁和风险。利用大数据分析技术，对大量的网络行为数据进行分析，识别出异常行为模式和攻击趋势；利用机器学习算法，对安全事件进行分类和预测，提前发现可能的安全漏洞和攻击行为。通过数据分析与挖掘，可以提高聚铭下一代防火墙的智能性和自适应性，更好地应对不断变化的网络安全威胁。

2.2.2.2 管理协同

在聚铭下一代防火墙架构中，各个组件之间在管理层面上实现协同工作，确保安全策略的一致性和有效性，提高管理效率。

策略同步：安全治理制定的安全策略能够同步下发到各个组件中，确保各个组件按照统一的策略进行操作。当安全策略发生变化时，能够及时通知各个组件进行更新，避免出现策略不一致的情况。例如，当安全治理决定禁止某个应用程序的访问时，AAA 身份系统、终端探针和安全检测产品等都能够及时接收到该策略，并对相关的访问请求进行阻止。

工作协调：各个组件之间在工作上进行协调配合，共同完成网络安全防护任务。当安全检测产品发现安全威胁时，能够及时通知终端探针和 AAA 身份系统，对相关的终端设备和用户进行处理；终端探针在监测到设备异常时，能够及时将信息反馈给安全治理和可靠运营，以便采取相应的措施进行修复和优化。通过工作协调，可以提高聚铭下一代防火墙的整体工作效率和响应速度，更好地保障网络安全。

综上所述，聚铭下一代防火墙的产品架构通过底层支撑组件、核心环节以及协同机制的有机结合，形成了一个功能强大、灵活可扩展的安全防护体系，能够有效应对当今复杂多变的网络安全威胁，为企业的网络安全提供全面的保障。

2.3 产品价值

聚铭下一代防火墙在当今复杂的网络环境中，凭借多维度的功能特性，为企业、机构等各类用户带来显著的产品价值，主要体现在以下几个关键方面。

2.3.1 强大的安全防护能力

抵御新型威胁：随着网络攻击手段的不断演变，高级持续威胁（APT）、零日漏洞攻击以及加密流量中的恶意软件传播等新型安全威胁层出不穷。聚铭下一代防火墙集成了先进的威胁检测技术，如深度包检测（DPI）、入侵检测与防范（IDS/入侵防御功能）以及威胁情报分析。DPI 技术能够对网络数据包进行全内容解析，识别出隐藏在正常流量中的恶意代码和非法应用，即使是加密流量也能洞察其本质。IDS/入侵防御功能则通过特征检测、异常检测和信誉检测相结合的方式，实时监测网络流量，一旦发现入侵行为，立即采取阻断措施，有效防范新型威胁对企业网络的侵害。

全面的应用控制：企业网络中应用程序繁多，包括各类办公软件、即时通讯工具、在线视频以及业务专用应用等。聚铭下一代防火墙可精准识别数千种网络应用，不仅能区分不同应用类型，还能对同一应用的不同版本和功能进行细致识别。通过制定灵活的应用控制策略，企业可以根据业务需求，允许或限制特定应用的使用，确保员工在工作时间专注于与工作相关的应用，提高工作效率，同时防止因滥用应用导致的网络带宽浪费和安全风险。例如，在工作时间禁止员工使用在线视频应用，保障关键业务应用的网络带宽。

2.3.2 优化网络性能

智能流量管理：网络流量的不均衡和拥塞常常影响业务的正常运行。聚铭下一代防火墙具备智能流量管理功能，能够实时监测网络流量状况，根据预设的策略对不同类型的流量进行优先级划分和带宽分配。对于企业的核心业务应用，如在线交易系统、视频会议等对实时性要求较高的应用，防火墙会优先保障其网络带宽，确保数据传输的流畅性，避免因网络延迟或丢包导致业务中断。同时，对于非关键业务流量，如文件下载、网页浏览等，在网络拥塞时适当限制其带宽，使网络资源得到合理利用，提升整体网络性能。

高效选路与负载均衡：在企业网络中，尤其是拥有多个分支机构或与多个云服务提供商合作的企业，需要确保数据能够通过最优路径传输，并实现网络设备和服务器的负载均衡。聚铭下一代防火墙的智能选路功能可以根据网络链路的实时状态，如带宽利用率、延迟、丢包率等指标，自动选择最佳的网络路径，将数据流量引导至最合适的链路，避免因某条链路拥塞而导致数据传输缓慢。此外，防火墙还可作为负载均衡器，将来自不同用户的访问请求均匀分配到多个服务器上，充分利用服务器资源，提高服务器的响应速度和处理能力，保障业务的高效运行。

2.3.3 提升业务连续性

保障关键业务运行：企业的关键业务系统，如企业资源规划（ERP）、客户关系管理（CRM）等，是企业运营的核心。聚铭下一代防火墙通过强大的安全防护和网络优化功能，为这些关键业务系统提供稳定可靠的运行环境。防火墙能够有效抵御外部网络攻击，防止黑客入侵窃取业务数据或破坏业务系统；同时，通过智能流量管理和选路，确保关键业务系统在网络拥塞或链路故障时仍能持续运行，减少因网络问题导致的业务中断时间，保障企业的正常运营和客户服务质量。

支持远程办公与移动办公：随着远程办公和移动办公的日益普及，员工需要随时随地安全地访问企业内部资源。聚铭下一代防火墙为远程办公和移动办公提供了安全便捷的解决方案。通过建立安全的 VPN 连接，员工可以在任何有网络的地方，通过加密通道安全地接入企业内部网络，访问所需的业务系统和文件资源。防火墙对远程接入的用户进行严格的身份认证和权限管理，确保只有合法授权的用户才能访问相应的资源，同时对传输的数据进行加密保护，防止数据在传输过程中被窃取或篡改，保障远程办公和移动办公的安全性和稳定性，提升员工的工作效率和业务灵活性。

2.3.4 助力合规与审计

满足法规合规要求：不同行业和地区对企业的网络安全和数据保护有着严格的法规要求，如金融行业的 PCI DSS 标准、医疗行业的 HIPAA 法规等。聚铭下一代防火墙提供了丰富的安全功能和管理工具，帮助企业满足这些法规合规要求。防火墙可以对网络访问进行详细的记录和审计，确保用户的访问行为符合企业的安全策略和法规要求；同时，通过数据加密、访问控制等功能，保护企业敏感数据的安全性和保密性，避免因数据泄露导致的法律风险和声誉损失。

便捷的安全审计与报表生成：企业需要定期对网络安全状况进行审计，以便及时发现潜在的安全问题并采取改进措施。聚铭下一代防火墙内置了强大的审计功能，能够收集和存储大量的网络活动日志，包括用户登录信息、访问记录、安全事件等。通过直观的管理界面，管理员可以方便地查询和分析这些日志数据，生成详细的安全审计报表。这些报表不仅有助于企业了解网络安全现状，还能为企业的安全决策提供数据支持，推动企业不断优化安全策略和防护措施，提升整体网络安全水平。

3. 产品技术

3.1 身份准入

3.1.1 技术概述

身份准入是聚铭下一代防火墙的基础环节，它确保只有经过授权的用户或设备能够接入网络。通过严格的身份验证机制，可以有效防止非法用户入侵网络，保护网络资源的安全性和可用性。

多维度身份校验，关联终端、风险扫描和权限分析等安全信息，动态调整访问权限，实现零信任身份准入

3.1.2 面向内网用户身份验证场景及类型

聚铭下一代防火墙产品的身份准入在多种场景中发挥关键作用，需结合客户具体需求选择合适的上网身份准入机制。

在办公场景中，聚铭下一代防火墙产品身份准入通过用户名 / 密码、证书等认证方式，确保员工使用公司网络资源时身份真实，依据部门、职位分组与角色定义，赋予不同权限，规范工作时间网络行为，保障业务正常开展。

访客场景下，可为访客提供临时账号密码，或通过微信等社交账号认证，限制其访问权限至特定网络区域，既能满足访客上网需求，又保障企业内部网络安全。

第三方对接场景里，产品与 AD、Radius 等第三方认证系统集成，在合作伙伴接入企业网络时，精准识别身份，依据合作协议分配访问权限，实现安全、高效的数据交互与协作 。

3.1.2.1办公场景认证

3.1.2.1.1 账号密码认证

账号密码认证是最基础且常见的认证方式。用户在接入网络时，系统会提示输入预先分配的用户名和密码。系统将用户输入的信息与存储在本地数据库或远程认证服务器中的用户信息进行比对。为确保安全性，密码通常会经过加密存储，如使用哈希算法（如 MD5、SHA - 256 等）。在认证过程中，系统对用户输入的密码进行相同的哈希处理后再与存储的哈希值进行比较。如果匹配成功，则允许用户接入网络；反之，则拒绝。

应用场景：广泛应用于企业内部网络，员工通过账号密码登录公司网络，访问内部资源。例如，员工使用公司分配的账号和密码登录办公网络，访问邮件系统、文件共享服务器等。

3.1.2.1.2 无密码类绑定认证

硬件绑定认证：将用户的网络接入与特定的硬件设备进行绑定，如网卡 MAC 地址、USB Key 等。当用户尝试接入网络时，系统会检查接入设备的硬件标识是否与预先绑定的标识一致。如果一致，则允许接入。这种方式利用了硬件设备的唯一性来确保认证的安全性。

IP 地址绑定认证：为用户分配特定的 IP 地址，并将其与用户身份进行绑定。用户只能通过该绑定的 IP 地址接入网络。系统在用户接入时，会检查其使用的 IP 地址是否合法。

应用场景：适用于对设备安全性要求较高的场景。例如，企业中某些重要部门的员工使用特定的办公电脑，通过硬件绑定认证确保只有该电脑能够接入公司网络，防止他人使用其他设备非法接入。

3.1.2.1.3 办公软件类认证

借助办公软件的认证机制来实现网络接入认证。例如，使用企业邮箱、办公协作软件（如钉钉等）的账号进行认证。当用户在办公软件中登录成功后，系统会获取用户的认证信息，并将其同步到网络接入认证系统中。如果办公软件的认证成功，则允许用户接入网络。这种方式利用了办公软件已有的安全认证体系，减少了用户额外的认证操作。

应用场景：在企业中，员工日常工作依赖办公软件进行沟通和协作。通过办公软件类认证，员工在登录办公软件的同时即可完成网络接入认证，提高了工作效率。例如，员工使用钉钉账号登录后，即可自动接入公司网络。

3.1.2.1.4 生物和所持类认证

生物特征认证：包括指纹识别等。系统通过生物特征识别设备（如指纹识别仪等）采集用户的生物特征信息，并将其与预先注册的特征模板进行比对。由于生物特征具有唯一性和稳定性，因此可以提供较高的认证安全性。

所持类认证：如使用智能卡、手机令牌等。用户在接入网络时，需要提供相应的认证令牌。系统会验证令牌的有效性，只有当令牌合法时，才允许用户接入网络。

应用场景：在对安全性要求极高的企业或机构中应用广泛。例如，金融机构的员工通过指纹识别或智能卡认证接入内部网络，确保敏感信息的安全。

3.1.2.1.5 Agent 认证

在用户终端上安装认证 Agent 软件。该软件会与网络接入认证系统进行通信，收集用户终端的相关信息，如操作系统信息、安装的软件列表等，并将其发送到认证系统。认证系统根据预设的规则对这些信息进行评估，如果符合要求，则允许用户接入网络。Agent 认证可以实现更细致的终端安全检查和认证。

应用场景：企业可以通过 Agent 认证确保员工终端符合安全标准。例如，要求终端安装指定的杀毒软件、操作系统补丁等，只有满足这些条件的终端才能接入公司网络。

3.1.2.2 访客场景认证

3.1.2.2.1 账号密码自注册

访客在接入网络时，系统会引导其进行账号密码的自注册。访客需要填写一些基本信息，如姓名、联系方式等，并设置自己的账号和密码。系统会对访客填写的信息进行初步验证，如检查邮箱地址的格式是否正确等。注册成功后，访客使用注册的账号和密码进行网络接入认证。这种方式为访客提供了一种便捷的接入方式，同时也便于企业对访客进行管理。

应用场景：适用于企业、酒店、商场等公共场所。例如，企业举办会议时，访客可以通过自注册的方式获取临时的网络接入权限。

3.1.2.2.2 微信认证

利用微信的开放平台接口实现认证。访客在接入网络时，系统会提供一个微信扫码认证的界面。访客使用微信扫描二维码后，系统会获取访客的微信唯一标识（如 openid），并将其发送到认证系统。认证系统根据预设的规则判断该微信用户是否具有接入权限。如果允许接入，则为访客分配网络接入权限。

应用场景：在商场、餐厅等公共场所较为常见。例如，顾客在餐厅用餐时，可以通过微信认证快速接入餐厅提供的无线网络。

3.1.2.2.3 短信认证

访客在接入网络时，需要输入自己的手机号码。系统会向该手机号码发送一条包含验证码的短信。访客输入收到的验证码后，系统会验证验证码的有效性。如果验证码正确，则允许访客接入网络。短信认证利用了手机号码的唯一性和短信验证码的一次性，提高了认证的安全性。

应用场景：广泛应用于各种公共场所的网络接入认证。例如，酒店为客人提供短信认证的方式接入客房内的无线网络。

3.1.2.3 与第三方 AAA 认证系统对接场景

AAA（Authentication、Authorization、Accounting）认证系统提供了认证、授权和计费的功能。聚铭下一代防火墙产品可以与第三方 AAA 认证系统进行对接，通过标准的协议（如 RADIUS、LDAP 等）实现用户认证信息的交互。当用户尝试接入网络时，聚铭下一代防火墙系统将用户的认证请求转发给第三方 AAA 认证系统。第三方 AAA 认证系统对用

户信息进行验证，并将认证结果返回给聚铭下一代防火墙系统。聚铭下一代防火墙系统根据认证结果决定是否允许用户接入网络。

应用场景：在企业中，如果已经部署了第三方的 AAA 认证系统（如 PPPOE、城市热点、Radius 等），聚铭下一代防火墙产品可以与之对接，实现统一的用户认证和管理。这样可以避免重复建设认证系统，提高管理效率。

3.1.3 面向防火墙管理人员身份验证

在网络安全体系中，防火墙管理人员肩负着保障企业网络安全稳定运行的重任。多维度身份校验、资产管理、风险管理以及安全策略分析等技术，是他们实现这一目标的重要手段。以下将从这些维度详细介绍相关技术原理。

3.1.3.1 多维度身份校验

3.1.3.1.1 匹配可管理的界面权限

防火墙管理界面功能丰富且复杂，不同的管理人员职责和权限各异。匹配可管理的界面权限技术，依据管理人员的角色，精准分配对应的界面操作功能。普通管理员或许仅能查看网络流量统计、配置基础的访问控制规则；高级管理员则拥有更高级的权限，诸如系统参数配置、安全策略的全面调整等。在管理人员登录管理界面时，防火墙系统依据其身份信息，加载与之匹配的操作界面和功能模块，严格限制其只能执行权限范围内的操作，避免误操作或恶意操作引发系统故障或安全问题。例如，在大型企业中，初级网络管理员只能对特定区域的网络访问规则进行微调，而高级管理员则可以对整个企业的安全架构进行重新规划和部署。

3.1.3.1.2 匹配可管理的组织结构权限

企业组织结构复杂，不同部门、层级的管理需求不同。匹配可管理的组织结构权限技术，基于企业的组织结构，为管理人员分配相应的网络访问管理权限。总部管理人员有权管理整个企业网络的安全策略，包括分支机构；分支机构管理员则仅能管理本地网络资源和安全设置。防火墙系统根据管理人员所属的组织结构信息和预设权限策略，判断其对特定网络资源的管理和操作权限。这有助于实现分级管理，提高管理效率，保障网络安全。如跨国企业中，总部管理员可制定全球统一的安全标准，各地区分支机构管理员在遵循标准的基础上，根据本地实际情况进行适当调整。

3.1.3.1.3 自定义的管理端口校验

管理端口是管理人员远程访问和配置防火墙的通道。自定义的管理端口校验技术，允

许防火墙管理人员根据安全需求，自定义设置管理端口，并对访问这些端口的操作进行严格校验。通过使用非默认端口，可降低被攻击者扫描和利用的风险。当有访问请求时，防火墙系统对请求者进行身份验证和权限检查，只有授权用户且操作符合权限策略，才能成功访问管理端口。例如，将默认的 Web 管理端口 80 修改为 8888，并限定只有特定 IP 地址段的管理员才能访问，可有效增强管理通道的安全性。

3.1.3.1.4 信任 IP、MAC 地址校验

防火墙管理人员可设置信任 IP 和 MAC 地址列表，对来自这些地址的访问请求给予特殊处理。信任 IP 地址如企业内部服务器、特定合作伙伴的地址；信任 MAC 地址则对应特定设备。来自信任地址的访问请求，防火墙系统依据预设规则给予一定信任和权限；非信任地址则进行严格检查和过滤。管理人员需谨慎管理信任列表，定期更新，结合其他安全技术对信任地址的访问进行实时监测，确保网络安全。例如，企业内部的关键服务器设置为信任 IP，可减少不必要的安全检查，提高数据传输效率，同时对访问行为进行实时监控，防止内部攻击。

3.1.3.1.5 双因子认证（可选）

双因子认证是增强身份验证的重要方式。在防火墙管理操作中，除用户名和密码外，还需提供另一种认证因素，如手机验证码、硬件令牌动态密码等。在登录管理界面或进行重要操作时，系统触发双因子认证流程。通过双因子认证，可有效防止管理员账号被盗用，保障防火墙管理的安全性。例如，在修改核心安全策略前，要求管理员输入手机验证码，只有验证通过才能继续操作，降低因账号泄露导致的安全风险。

3.1.3.1.6 密码强度校验

防火墙管理人员设置密码强度规则，对用户密码进行校验。规则涵盖密码长度、字符类型等要求。用户设置或修改密码时，系统依据规则检查，不符合要求则提示修改。强密码可提高账号安全性，降低被破解风险。例如，要求密码长度不少于 8 位，包含字母、数字和特殊字符，可有效抵御暴力破解攻击。

3.1.3.2 资产管理

3.1.3.2.1 终端资产绑定、录入

防火墙管理人员将终端设备与相关信息进行绑定和录入，包括 IP 和 MAC 地址、终端类型、操作系统等。这些信息有助于识别和管理终端设备，确保只有授权设备才能接入网络。通过建立完善的资产信息库，管理人员可实时掌握网络内设备的分布和使用情况，为安全策略制定提供依据。例如，新员工入职，其办公设备信息录入系统并与账号绑定，确保设备合法接入，同时便于后续管理和维护。

3.1.3.2.2 资产状态监测

防火墙系统实时监测终端资产的状态，包括设备的在线状态、运行状况、安全软件安装情况等。当设备出现异常，如长时间离线、安全软件未更新，系统及时发出警报。管理人员可根据资产状态信息，及时采取措施，保障设备安全运行。例如，发现某台服务器安全软件过期，立即通知相关人员更新，防止因软件漏洞导致安全事故。

3.1.3.3 风险管理

3.1.3.3.1 风险分析

防火墙系统对网络流量、用户行为、设备状态等数据进行深度分析，识别潜在风险。通过机器学习和人工智能算法，分析历史数据和实时数据，发现异常行为模式和安全威胁。例如，检测到某个 IP 地址频繁尝试登录不同账号，可能是暴力破解攻击；某台设备流量异常增大，可能感染恶意软件。

3.1.3.3.2 制定终端接入基线

基于风险分析结果，防火墙管理人员制定终端接入基线。明确终端设备接入网络的安全标准，如操作系统版本要求、安全软件安装规定、补丁更新情况等。不符合基线要求的设备限制接入或进行整改，从源头上降低安全风险。例如，规定接入企业网络的设备必须安装最新版杀毒软件和操作系统补丁，否则禁止接入。

3.1.3.3.3 风险应对与处置

当发现安全风险，防火墙系统及时采取应对措施，如阻断异常流量、隔离受感染设备、限制违规用户访问等。管理人员根据风险严重程度和影响范围，制定相应的处置方案，跟踪处理过程，确保风险得到有效控制和消除。例如，发现某台设备感染勒索病毒，立即将其隔离，防止病毒扩散，同时组织技术人员进行病毒清除和数据恢复。

3.1.3.4 安全策略分析

3.1.3.4.1 问题策略分析

防火墙管理人员定期对现有安全策略进行分析，查找存在的问题和漏洞。检查策略的一致性、有效性和合理性，如是否存在冲突的策略规则、是否有不必要的宽松策略。例如，发现两条访问控制策略对同一资源的权限设置相互矛盾，需及时调整。

3.1.3.4.2 问题策略解决建议

针对分析出的问题策略，提出具体的解决建议。优化策略规则，简化复杂策略，提高策略的可管理性和执行效率。同时，根据网络环境和安全需求的变化，及时更新和完善安全策略。例如，随着企业业务拓展，新增了云服务应用，需相应调整安全策略，保障云环境下的网络安全。

3.2 网络融合

3.2.1 动态路由

动态路由是一种根据网络拓扑结构和流量情况自动调整路由表的技术。与静态路由相比，动态路由具有更高的灵活性和适应性，可以在网络发生变化时自动更新路由信息，确保网络的连通性和性能。

3.2.1.1 RIP（Routing Information Protocol）

原理：RIP 是一种基于距离向量的动态路由协议。它通过定期向相邻路由器发送路由更新信息，告知对方自己所知道的网络可达性和距离。距离通常以跳数（Hop Count）来衡量，即数据包从源节点到目的节点经过的路由器数量。RIP 协议规定最大跳数为 15，超过 15 跳的网络被认为不可达。

工作流程：每个路由器会维护一个路由表，记录自己所知道的网络信息和对应的距离。当路由器启动时，它会向相邻路由器发送自己的路由表信息。相邻路由器接收到信息后，会根据自己的路由表进行更新，并向其他相邻路由器转发更新信息。这个过程会不断重复，直到整个网络中的路由器都达成一致的路由信息。

应用场景：RIP 协议简单易懂，适用于小型网络。例如，在一个小型企业的局域网中，路由器数量较少，网络拓扑结构相对简单，使用 RIP 协议可以实现基本的动态路由功能。

3.2.1.2 OSPF（Open Shortest Path First）

原理：OSPF 是一种基于链路状态的动态路由协议。它通过收集网络中各个链路的状态信息（如带宽、延迟等），使用 Dijkstra 算法计算出最短路径，并生成路由表。OSPF 协议将网络划分为多个区域（Area），每个区域内的路由器会维护相同的链路状态数据库，通

过区域边界路由器进行区域间的路由信息交换。

工作流程：路由器首先会发现相邻路由器，并建立邻居关系。然后，通过发送链路状态通告（LSA）来交换链路状态信息。每个路由器会根据接收到的 LSA 信息更新自己的链路状态数据库，并使用 Dijkstra 算法计算出最短路径树，从而生成路由表。

应用场景：OSPF 协议适用于大型网络，具有收敛速度快、支持大规模网络拓扑等优点。例如，在一个大型企业的广域网中，网络拓扑结构复杂，路由器数量众多，使用 OSPF 协议可以实现高效的动态路由。

3.2.1.3 BGP（Border Gateway Protocol）

原理：BGP 是一种用于在不同自治系统（AS）之间交换路由信息的外部网关协议。自治系统是指由一个或多个网络组成的、在同一个管理机构控制下的网络集合。BGP 协议通过交换路由信息，实现不同自治系统之间的互联互通。BGP 路由器会根据一系列的策略和规则来选择最佳的路由路径。

工作流程：BGP 路由器首先会建立与相邻自治系统的 BGP 邻居关系。然后，通过发送 BGP 消息（如 OPEN、UPDATE、KEEPALIVE 等）来交换路由信息。每个 BGP 路由器会维护一个 BGP 路由表，记录从不同自治系统学到的路由信息。在选择路由时，BGP 会考虑多个因素，如 AS 路径长度、路由优先级等。

应用场景：BGP 协议主要应用于互联网服务提供商（ISP）之间的路由交换。例如，不同的 ISP 之间通过 BGP 协议交换路由信息，实现全球互联网的互联互通。

3.2.2 地址转换

地址转换（Network Address Translation，简称 NAT）的核心目的是实现 IP 地址空间的灵活利用和网络层的地址映射。在互联网发展进程中，IPv4 地址资源逐渐稀缺，而大量内部网络设备需要接入互联网，地址转换技术应运而生。

防火墙在执行地址转换时，主要基于数据包的 IP 地址和端口信息进行操作。当内部网络中的设备（源设备）向外部网络发送数据包时，防火墙会将数据包中的源 IP 地址替换为防火墙自身的一个公网 IP 地址（或多个公网 IP 地址中的一个），同时记录源设备的内部 IP 地址、端口与转换后的公网 IP 地址、端口之间的映射关系。这个映射关系存储在防火墙的 NAT 表中。当外部网络设备响应数据包返回时，防火墙依据 NAT 表中的映射信息，将数据包中的目的 IP 地址转换回内部源设备的 IP 地址，从而确保数据包能够准确无误地送达内部设备。

3.2.2.1 双栈源地址转换

双栈源地址转换主要应用于同时支持 IPv4 和 IPv6 双栈协议的网络环境。当网络中的主机（源设备）发起通信请求时，防火墙会根据预先设定的规则，对源 IP 地址进行转换。如果源主机使用的是 IPv4 地址，防火墙可以将其转换为 IPv6 地址，反之亦然。具体来说，防火墙会在内部维护一个地址映射表，记录源主机的原始 IP 地址（无论是 IPv4 还是 IPv6）与转换后的目标 IP 地址之间的对应关系。当数据包从源主机发送到防火墙时，防火墙依据映射表，将数据包中的源 IP 地址替换为目标 IP 地址，并将转换后的数据包转发出去。在通信过程中，防火墙还会跟踪连接状态，确保响应数据包能够准确无误地返回给源主机。

应用场景：在企业网络中，部分老旧设备仍在使用 IPv4 协议，而新部署的系统和设备则采用 IPv6 协议。通过双栈源地址转换，企业可以让这些不同协议的设备在同一网络环境中协同工作。例如，企业内部的一台运行 IPv4 协议的服务器需要与外部 IPv6 网络中的云服务进行通信，防火墙通过双栈源地址转换，将服务器的 IPv4 源地址转换为 IPv6 地址，使得服务器能够顺利访问云服务，实现了不同协议设备之间的跨网络通信。

3.2.2.2 双栈目的地址转换

双栈目的地址转换与双栈源地址转换相对应，主要针对数据包的目的 IP 地址进行转换。当数据包进入防火墙时，防火墙会检查数据包的目的 IP 地址。若目的地址与内部网络中的实际服务器或设备的地址不一致，防火墙会根据配置的转换规则，将目的 IP 地址转换为内部网络中真实服务或设备的 IP 地址（可以是 IPv4 到 IPv6 的转换，也可以是 IPv6 到 IPv4 的转换）。同样，防火墙会维护一个目的地址映射表，用于记录转换前后的地址对应关系。当外部网络向内部网络发送请求时，防火墙依据映射表对目的地址进行转换，确保数据包能够准确送达内部网络中的目标设备。

应用场景：假设企业对外提供 Web 服务，同时支持 IPv4 和 IPv6 访问。外部用户无论是通过 IPv4 网络还是 IPv6 网络访问企业的 Web 服务，防火墙都可以通过双栈目的地址转换，将用户请求的目的 IP 地址（公网 IP 地址）转换为内部 Web 服务器的实际 IP 地址（可能是 IPv4 或 IPv6）。这样，企业无需为不同协议的访问分别部署不同的 Web 服务器，简化了网络架构，提高了资源利用效率。

3.2.2.3 NAT46

NAT46 是一种专门用于实现 IPv4 网络与 IPv6 网络互联互通的地址转换技术。其核

心原理是将 IPv4 数据包封装在 IPv6 数据包中进行传输。当 IPv4 网络中的设备向 IPv6 网络发送数据时，防火墙会在 IPv4 数据包的外层添加一个 IPv6 包头，将源 IPv4 地址和目的 IPv4 地址分别映射到 IPv6 地址空间中的特定地址。在传输过程中，IPv6 网络中的路由器可以根据 IPv6 包头进行路由转发。当数据包到达目标 IPv6 网络中的防火墙时，防火墙会剥离外层的 IPv6 包头，将内部的 IPv4 数据包转发给目标 IPv4 设备。NAT46 技术使得 IPv4 网络中的设备能够直接与 IPv6 网络中的设备进行通信，无需对现有 IPv4 设备进行大规模升级改造。

应用场景：在 IPv4 向 IPv6 过渡阶段，许多企业和网络运营商面临着 IPv4 和 IPv6 网络并存的局面。NAT46 技术为这种混合网络环境提供了一种有效的解决方案。例如，一些企业的核心业务系统仍然运行在 IPv4 网络上，但希望能够与外部的 IPv6 网络进行通信，如访问 IPv6 网络中的云服务提供商或合作伙伴的网络。通过部署支持 NAT46 的防火墙，企业可以在不改变现有 IPv4 网络架构的前提下，实现与 IPv6 网络的互联互通，逐步推进 IPv6 的应用。

3.2.2.4 NAT64

NAT64 与 NAT46 相反，它主要用于将 IPv6 数据包转换为 IPv4 数据包，实现 IPv6 网络与 IPv4 网络的通信。NAT64 技术需要一个 IPv4 地址池，当 IPv6 网络中的设备需要与 IPv4 网络中的设备通信时，防火墙会从 IPv4 地址池中为其分配一个临时的 IPv4 地址。防火墙将 IPv6 数据包中的源 IPv6 地址和目的 IPv6 地址转换为对应的 IPv4 地址，然后将转换后的 IPv4 数据包发送到 IPv4 网络中。在响应数据包返回时，防火墙再将 IPv4 数据包中的源 IPv4 地址和目的 IPv4 地址转换回 IPv6 地址，转发给 IPv6 网络中的源设备。NAT64 技术通过地址转换和协议转换，解决了 IPv6 网络与 IPv4 网络之间的通信障碍。

应用场景：随着 IPv6 的普及，越来越多的企业和用户开始部署 IPv6 网络。然而，互联网上仍然存在大量仅支持 IPv4 的服务和资源。通过 NAT64 技术，IPv6 网络中的用户可以访问这些 IPv4 资源。例如，家庭用户升级到 IPv6 网络后，仍然可以通过 NAT64 技术访问那些尚未支持 IPv6 的在线游戏服务器、视频网站等。对于企业而言，NAT64 技术可以帮助其在逐步推进 IPv6 部署的过程中，保持与现有 IPv4 网络中的合作伙伴和客户的通信畅通，确保业务的连续性。

防火墙的双栈源地址转换、双栈目的地址转换、双栈双向地址转换、NAT46 以及

NAT64 等地址转换功能，在 IPv4 与 IPv6 共存的网络环境中，为实现不同协议网络之间的互联互通、优化网络架构、保障网络安全以及提升网络资源利用效率提供了强有力的支持。这些功能的合理运用，将助力企业和网络运营商顺利完成向 IPv6 的过渡，推动互联网技术的持续发展。

3.2.3 网络代理

网络代理是连接客户端与目标服务器的中间桥梁。它能隐藏客户端真实 IP 增强隐私，可进行访问控制，限制特定网站访问；还具备缓存功能，加速网页访问；支持处理不同协议通信，如 HTTP、SSL 等，让数据传输更灵活安全，适用于多种网络场景。

3.2.3.1 HTTP 代理

HTTP 代理是一种位于客户端和目标 HTTP 服务器之间的中间服务器。客户端向 HTTP 代理发送 HTTP 请求，代理服务器接收请求后，代替客户端向目标服务器发起请求，获取响应后再将其返回给客户端。它工作在应用层，主要处理基于 HTTP 协议的网络通信。

3.2.3.1.1 技术原理

请求接收：客户端将原本要直接发送给目标服务器的 HTTP 请求发送到 HTTP 代理服务器。这个请求包含了目标服务器的地址、请求方法（如 GET、POST）、请求头和请求体等信息。

请求转发：代理服务器解析客户端的请求，提取出目标服务器的地址和请求内容，然后以自己的名义向目标服务器发送请求。

响应处理：目标服务器接收到代理服务器的请求后，返回 HTTP 响应。代理服务器接收该响应，并将其转发给客户端。在这个过程中，代理服务器可以对响应进行修改，如添加或删除响应头信息。

3.2.3.1.2 应用场景

访问控制：企业可以通过 HTTP 代理限制员工访问某些特定的网站，实现上网行为管理。

缓存加速：代理服务器可以缓存经常访问的网页内容，当客户端再次请求相同内容时，直接从缓存中返回，减少对目标服务器的访问，提高访问速度。

隐藏真实 IP：客户端通过代理服务器访问目标网站，目标服务器只能看到代理服务器的 IP 地址，从而隐藏了客户端的真实 IP，增强了隐私保护。

3.2.3.2 DNS 代理

DNS（Domain Name System）代理是一种用于处理域名解析请求的代理服务器。客户端将域名解析请求发送给 DNS 代理，代理服务器根据自身的规则和配置，对请求进行处理，并返回相应的 IP 地址。

3.2.3.2.1 技术原理

请求接收：客户端向 DNS 代理发送域名解析请求，请求中包含要解析的域名。

解析处理：DNS 代理服务器接收到请求后，首先检查自身的缓存中是否有该域名的解析记录。如果有，则直接返回缓存中的 IP 地址；如果没有，则根据配置的规则，向其他 DNS 服务器发送解析请求。

结果返回：当从其他 DNS 服务器获取到域名的解析结果后，DNS 代理将结果返回给客户端，并将该结果缓存起来，以便后续的请求可以更快地得到响应。

3.2.3.2.2 应用场景

访问控制：通过 DNS 代理，可以对特定域名的解析进行限制，禁止客户端访问某些不良或不安全的网站。

负载均衡：DNS 代理可以根据服务器的负载情况，将域名解析到不同的 IP 地址，实现服务器的负载均衡。

加速访问：DNS 代理可以缓存常用域名的解析结果，减少客户端向外部 DNS 服务器发送请求的次数，提高域名解析的速度，从而加速网站的访问。

3.2.3.3 二级代理

二级代理是指在一级代理的基础上，再增加一层代理服务器。客户端的请求先发送到一级代理，一级代理再将请求转发给二级代理，二级代理最终将请求发送到目标服务器。这种多层代理的结构可以提供更高的匿名性和灵活性。

3.2.3.3.1 技术原理

多级转发：客户端将请求发送到一级代理服务器，一级代理服务器对请求进行初步处理后，将其转发给二级代理服务器。二级代理服务器接收到请求后，再向目标服务器发起请求。

隐藏真实路径：由于请求经过了多级代理，目标服务器只能看到二级代理服务器的 IP 地址，无法直接追踪到客户端的真实 IP 地址，增加了客户端的匿名性。

3.2.3.3.2 应用场景

增强隐私保护：在需要高度匿名性的场景下，如网络爬虫、隐私浏览等，使用二级代理可以更有效地隐藏客户端的真实身份和位置。

突破网络限制：在某些网络环境中，可能会对代理服务器进行限制。通过使用二级代理，可以绕过这些限制，继续访问目标网站。

分布式网络应用：在一些分布式网络应用中，二级代理可以用于实现数据的分发和传输，提高系统的可靠性和性能。

3.2.4 智能 DNS

智能 DNS 技术通过对多种因素的综合分析，如用户的地理位置、网络运营商、服务器负载等，为用户提供最优的域名解析结果。其核心目标是提高用户对网站或服务的访问速度和质量，同时实现服务器的负载均衡和容灾备份。

3.2.4.1 基于地理位置的解析

智能 DNS 服务器会根据用户的 IP 地址判断其地理位置。不同地理位置的用户在访问网站时，智能 DNS 会将其解析到距离最近的服务器节点。例如，当一个位于北京的用户访问某网站时，智能 DNS 会将其解析到北京或周边地区的服务器，减少网络延迟。

智能 DNS 服务器通常会维护一个 IP 地址与地理位置的映射数据库，通过查询该数据库来确定用户的地理位置。同时，服务器还会实时监测各个服务器节点的性能和可用性，确保为用户提供最佳的解析结果。

3.2.4.2 基于网络运营商的解析

不同的网络运营商之间可能存在网络互通问题，导致用户访问速度受到影响。智能 DNS 会根据用户所使用的网络运营商，将其解析到该运营商网络内的服务器节点。例如，当一个使用中国移动网络的用户访问网站时，智能 DNS 会将其解析到中国移动网络内的服务器，避免跨运营商网络带来的延迟。

智能 DNS 服务器通过分析用户的 IP 地址，判断其所属的网络运营商。同时，服务器会与各个网络运营商进行合作，获取其网络拓扑和性能信息，以便更准确地进行解析。

3.2.4.3 基于服务器负载的解析

智能 DNS 会实时监测各个服务器的负载情况，将用户的请求解析到负载较轻的服务器上。通过这种方式，可以实现服务器的负载均衡，提高服务器的处理能力和响应速度。

智能 DNS 服务器会与服务器节点进行通信，获取服务器的 CPU 使用率、内存使用率、网络带宽等负载指标。根据这些指标，服务器会动态调整域名解析结果，将用户的请求分配到合适的服务器上。

3.3 智能流控

在现代网络环境中，随着网络应用的不断丰富和用户数量的增加，网络带宽的合理分配和有效管理变得至关重要。防火墙的带宽管理技术能够对网络流量进行精细化的控制和优化，确保网络资源的合理利用，提高网络的整体性能和服务质量。

3.3.1 带宽限制

带宽管理主要是通过对网络流量进行分类和限制来实现的。防火墙能够识别不同类型的网络应用（如网页浏览、文件下载、视频流媒体等）产生的流量，然后根据预先设定的策略对这些流量进行控制。它是基于流量识别和策略应用的机制。

流量识别：通过深度包检测（DPI）技术，防火墙可以解析数据包的内容，识别出数据包所属的应用协议。例如，通过分析数据包中的特征字段，能够区分出是 HTTP 协议的网页流量，还是 FTP 协议的文件传输流量。

策略应用：一旦识别出流量类型，就可以根据管理员设定的带宽策略来处理这些流量。策略可以包括限制某些应用的带宽上限、为不同应用分配不同的优先级等。例如，对于企业办公网络，可以设定视频流媒体应用的带宽上限为总带宽的 30%，以防止其过度占用带宽，影响其他关键业务应用。

3.3.1.1 实现方式

基于端口的带宽管理：传统的网络应用通常会使用特定的端口进行通信，防火墙可以根据端口号来识别和管理流量。例如，HTTP 协议通常使用端口 80，FTP 协议使用端口 21 和 20。通过对这些端口的流量进行限制，可以实现对相应应用的带宽管理。然而，这种方法的局限性在于，一些应用可能会使用动态端口或者伪装端口，导致流量识别不准确。

基于应用层协议的带宽管理：随着网络应用的复杂化，越来越多的应用采用非标准端口或者加密通信，基于端口的管理方式已经不能满足需求。因此，基于应用层协议的带宽管理应运而生。通过 DPI 技术，防火墙可以直接识别应用层协议，而不受端口的限制。这种方式能够更准确地识别流量，从而实现更有效的带宽管理。

3.3.2 带宽保障

带宽保障的核心目标是确保关键业务应用在网络拥塞的情况下，仍然能够获得足够的带宽，以保证其正常运行。它是通过为关键业务预留一定的带宽资源来实现的。

带宽预留机制：管理员可以在防火墙中设定关键业务应用的最小带宽保障值。当网络流量增加，总带宽趋于饱和时，防火墙会优先保障关键业务应用的带宽需求。例如，对于企业的在线交易系统，可以设定其最小带宽保障为总带宽的 50%，这样在网络繁忙时，如促销活动期间，即使其他非关键业务的流量受到限制，在线交易系统仍然能够正常处理客户订单。

3.3.2.1 应用场景

带宽保障在对业务连续性要求较高的行业中应用广泛。

金融行业：证券交易、网上银行等金融业务对实时性和稳定性要求极高。防火墙通过带宽保障技术，确保交易指令的快速、准确传输，避免因网络拥塞导致交易延迟或失败。

医疗行业：医院的远程医疗诊断系统、医疗信息管理系统等需要稳定的网络带宽。带宽保障可以防止其他非医疗相关的网络应用（如医院内部的员工在线娱乐）对医疗业务产生干扰，保证患者的诊断和治疗过程不受影响。

3.3.3 带宽限额

带宽限额是对特定用户、应用或设备的带宽使用进行限制，以防止其过度占用网络资源。它是通过设定带宽上限来实现的。

用户层面的带宽限额：可以根据用户的身份或者 IP 地址来设定带宽限额。例如，在企业网络中，为普通员工设定的最大下载带宽为 10Mbps，为高级管理人员设定的最大下载带宽为 20Mbps，以满足不同用户群体的需求，同时防止个别用户过度占用带宽。

应用层面的带宽限额：针对不同的网络应用设定带宽限额。如限制 P2P 下载应用的最大带宽为总带宽的 20%，因为 P2P 应用通常会消耗大量带宽，如果不加以限制，可能会影响其他用户和应用的正常使用。

设备层面的带宽限额：对于网络中的服务器、打印机等设备，也可以设定带宽限额。例如，限制公司内部文件服务器的最大上传带宽为 50Mbps，以防止其在备份数据等操作时过度占用网络带宽，影响其他业务的正常运行。

3.3.3.1 实现方式

静态带宽限额：为用户、应用或设备设定固定的带宽限额，在一段时间内保持不变。这种方式简单直接，适用于网络使用模式相对稳定的场景。

动态带宽限额：根据网络的实际运行情况，动态地调整带宽限额。例如，在网络空闲时段，可以适当提高某些非关键应用的带宽限额；在网络繁忙时段，则降低这些应用的带宽限额，以确保关键业务的正常运行。这种方式需要防火墙具备一定的智能分析能力，能够实时监测网络流量和负载情况。

3.3.4 智能流控

智能流控是一种更加高级的带宽管理技术，它结合了流量识别、用户行为分析、网络负载评估等多种手段，对网络流量进行智能的控制和分配。

流量行为分析：智能流控能够分析流量的行为模式，如流量的突发性、持续性、周期性等。例如，对于一些周期性产生大量流量的应用（如定时备份的业务系统），可以在其非备份时段适当提高其带宽限额，在备份时段则严格控制其带宽，以避免对其他业务产生影响。

用户优先级设定：根据用户的身份、角色以及业务的重要性，为用户设定不同的优先级。例如，在企业网络中，将参与紧急项目的员工的网络访问优先级设定为最高，在网络拥塞时优先保障这些员工的网络使用，以确保紧急项目的顺利进行。

网络负载感知：智能流控能够实时感知网络的负载情况，根据负载的轻重来调整流量控制策略。当网络负载较轻时，可以适当放松对非关键业务的带宽限制；当网络负载较重时，则加强对非关键业务的控制，优先保障关键业务的带宽。

3.3.4.1 应用场景

智能流控适用于复杂多变的网络环境。

企业园区网络：企业内部员工的网络需求多样，包括办公、学习、娱乐等。智能流控可以根据员工的工作状态（如工作时间、休息时间）和业务需求，灵活地分配带宽，提高员工的工作效率和满意度。

数据中心网络：数据中心承载着众多的服务器和应用，不同应用的流量特性和重要性各不相同。智能流控可以根据数据中心的负载情况和应用的优先级，优化网络流量，提高数据中心的整体性能和服务质量。

防火墙的带宽管理技术（包括带宽管理、带宽保障、带宽限额和智能流控）能够有效地提高网络资源的利用效率，保障关键业务的正常运行，为网络的稳定和高效提供了坚实的保障。

3.4 智能选路

智能选路是一种基于防火墙的网络技术，它可以对网络流量进行智能的路径选择。通过对网络链路的实时状态（如带宽利用率、延迟、丢包率等）、业务需求（如应用类型、服务质量要求等）以及其他策略因素（如成本、安全性等）进行综合评估，防火墙能够自动将不同的网络流量引导至最合适的网络路径，从而优化网络性能、提高用户体验和保障业务连续性。

3.4.1 链路状态监测

根据网络带宽质量进行指标收集：

- 带宽利用率：防火墙通过监测链路接口的输入和输出带宽，计算出链路的带宽利用率。例如，一条 100Mbps 的链路，如果当前的输入和输出流量总和为 60Mbps，那么带宽利用率为 60%。
- 延迟：通过发送探测数据包（如 ICMP Echo 请求）并测量往返时间，来确定链路的延迟。例如，从防火墙向目标服务器发送一个 ICMP Echo 请求，记录发送时间和收到响应的时间，两者之差就是延迟时间。
- 丢包率：通过发送一定数量的测试数据包，统计未收到响应的数据包数量占总发送数据包数量的比例。例如，发送 100 个数据包，有 5 个没有收到响应，那么丢包率为 5%。

根据收集到的性能指标，防火墙对链路的健康状况进行评估。例如，如果一条链路的带宽利用率长期超过 80%、延迟超过一定阈值（如 100ms）或者丢包率超过可接受范围（如 3%），则认为该链路处于不健康状态。

3.4.2 流量识别与分类

应用类型识别：防火墙利用深度包检测（DPI）技术和协议分析，识别网络流量所属的应用类型。例如，通过分析数据包中的特征字段，可以区分 HTTP 流量（网页浏览）、FTP 流量（文件传输）、VoIP 流量（网络电话）等。

业务优先级划分：根据企业的业务策略，为不同的应用类型划分优先级。例如，对于企业的在线交易系统、视频会议系统等关键业务，赋予高优先级；对于员工的在线娱乐应用，赋予低优先级。

3.4.3 智能选路算法

基于策略的选路：根据预先设定的策略进行选路。例如，企业规定所有访问特定合作

伙伴网络的流量必须通过某条专线链路，防火墙就会按照此策略进行选路。

基于性能的选路：当有多个可选链路时，防火墙会选择性能最佳的链路。性能评估可以基于延迟、带宽、丢包率等因素的综合考量。例如，对于高优先级的实时视频会议流量，防火墙会选择延迟最低、丢包率最小的链路。

负载均衡选路：为了充分利用多条链路的资源，避免单点链路过载，防火墙可以采用负载均衡选路算法。例如，对于低优先级的文件下载流量，可以将其均匀分配到多条链路，根据各链路的负载情况动态调整分配比例。

3.4.4 动态路径调整

防火墙会根据链路状态的实时变化和流量的动态情况，实时调整选路决策。例如，如果某条链路的延迟突然增加，防火墙会将原本经过该链路的高优先级流量切换到其他性能更好的链路。

在路径调整过程中，对于需要保持会话连续性的应用（如 TCP - based 应用），防火墙会采用会话保持技术。例如，通过记录会话的五元组（源 IP 地址、源端口、目的 IP 地址、目的端口、协议）信息，确保在路径切换后，同一会话的后续数据包仍然能够正确地到达目的地，避免会话中断。

3.5 VPN（Virtual Private Network）

VPN 是一种通过公共网络（如互联网）建立安全、加密的专用网络连接的技术。它可以让远程用户或分支机构安全地访问企业内部网络资源，就像直接连接到企业内部网络一样。

VPN 主要包括 入侵防御功能 ec VPN、SSL VPN、L2TP VPN、PPTP VPN。入侵防御功能 ec VPN 工作在网络层，通过对 IP 数据包进行加密和认证保障通信安全，主要用于站点到站点连接和远程访问，确保企业分支机构间及员工与公司网络通信的保密性和完整性。SSL VPN 利用 SSL/TLS 协议基于浏览器建立安全通道，侧重于加密 HTTP 流量，方便移动办公用户远程访问公司网络，也适用于为外部合作伙伴提供有限访问权限。L2TP VPN 是第二层隧道协议，结合了相关协议特点，通过建立隧道传输数据，通常与 入侵防御功能 ec 配合使用，用于远程访问，在多种网络类型上建立连接较方便。PPTP VPN 是早期技术，在 PPP 连接基础上建隧道传输数据，工作在网络层和数据链路层之间，有一定加密功能，曾在小型企业和家庭网络远程访问中使用较多。

3.5.1 VPN 的种类

3.5.1.1 入侵防御功能 ec VPN 技术

入侵防御功能 ec（Internet Protocol Security）是一组为保护 IP 通信而设计的协议套件，它工作在网络层，能够为 IP 数据包提供机密性、完整性和身份验证等安全服务。入侵防御功能 ec VPN 利用 入侵防御功能 ec 协议在公共网络上建立安全的隧道，实现不同网络之间的安全通信。

3.5.1.1.1 技术原理

入侵防御功能 ec 通过安全关联（SA）来管理和维护安全通信。SA 是两个 入侵防御功能 ec 实体之间的单向逻辑连接，它定义了用于保护数据包的安全参数，如加密算法、认证算法、密钥等。每个 SA 由一个三元组（安全参数索引 SPI、目的 IP 地址、安全协议）唯一标识。

入侵防御功能 ec 主要包括两个协议：AH（Authentication Header）和 ESP（Encapsulating Security Payload）。AH 协议提供数据完整性和身份验证服务，但不提供数据加密；ESP 协议则提供数据加密、完整性和身份验证服务。在实际应用中，通常使用 ESP 协议来保证数据的安全性。

入侵防御功能 ec 支持两种工作模式：隧道模式和传输模式。隧道模式将整个原始 IP 数据包封装在新的 IP 数据包中，适用于不同网络之间的通信；传输模式只对 IP 数据包的有效负载进行加密，适用于主机之间的通信。

入侵防御功能 ec VPN 适用于企业内部网络之间的安全连接，如总部与分支机构之间的通信、企业数据中心之间的备份和容灾等。它能够提供高强度的安全保障，适合对安全性要求较高的场景。

3.5.1.2 SSL VPN 技术

SSL（Secure Sockets Layer）是一种用于在客户端和服务器之间建立安全连接的协议，后来发展为 TLS（Transport Layer Security）。SSL VPN 利用 SSL/TLS 协议在应用层建立安全的隧道，实现远程用户对企业内部资源的安全访问。

3.5.1.2.1 技术原理

SSL VPN 的建立过程基于 SSL/TLS 握手协议。客户端和服务器首先进行身份验证，交换证书和密钥，协商加密算法和会话密钥。握手协议确保了通信双方的身份真实性和密钥的安全性。

在握手协议完成后，客户端和服务器使用协商好的加密算法和会话密钥对数据进行加密传输。SSL/TLS 协议支持多种加密算法，如 AES、RSA 等，能够提供高强度的加密保护。

SSL VPN 通常采用应用层代理的方式，将用户的请求转发到企业内部的服务器。用户通过浏览器或专门的客户端软件访问企业内部资源，无需在客户端安装复杂的 VPN 软件。

SSL VPN 适用于远程用户对企业内部资源的访问，如员工在家办公、出差人员访问公司内部系统等。它具有无需安装客户端软件、易于部署和管理等优点，适合对便捷性要求较高的场景。

3.5.1.3 L2TP VPN 技术

L2TP（Layer 2 Tunneling Protocol）是一种二层隧道协议，它结合了 PPTP（Point-to-Point Tunneling Protocol）和 L2F（Layer 2 Forwarding）的优点，能够在公共网络上建立虚拟的二层链路。L2TP VPN 通常与 入侵防御功能 ec 协议结合使用，提供更高的安全性。

3.5.1.3.1 技术原理

L2TP 协议通过控制消息建立隧道，客户端和服务器之间交换控制消息，协商隧道的参数和配置。隧道建立后，客户端和服务器之间可以通过隧道传输二层数据帧。

为了提高安全性，L2TP VPN 通常与 入侵防御功能 ec 协议结合使用。入侵防御功能 ec 协议为 L2TP 隧道提供加密和身份验证服务，确保数据在传输过程中的安全性。

在隧道建立和安全协商完成后，客户端和服务器之间可以通过 L2TP 隧道传输数据。数据在传输过程中先经过 L2TP 封装，再经过 入侵防御功能 ec 加密和封装，最后在公共网络上传输。

L2TP VPN 适用于需要建立虚拟二层链路的场景，如远程用户访问企业内部局域网、企业分支机构之间的连接等。它结合了 L2TP 协议的灵活性和 入侵防御功能 ec 协议的安全性，适合对安全性和灵活性都有一定要求的场景。

3.5.2 VPN 的使用场景

3.5.2.1 企业远程办公场景

跨地区企业协作：跨地区企业在全球不同国家和地区设有办公室或分支机构。例如，一家大型科技公司，其总部位于美国，在欧洲、亚洲等地都有研发中心和销售办事处。通过 VPN，这些分布在世界各地的团队成员可以安全地访问公司总部的核心研发数据库、共

享的项目文件以及统一的企业资源规划（ERP）系统。员工无论身处何处，只要有网络连接，就能像在公司内部局域网一样进行工作，实现高效的跨国协作。

移动办公人员访问公司资源：对于经常需要外出拜访客户的销售人员或现场技术支持人员，VPN 是必不可少的工具。他们可以使用笔记本电脑、平板电脑甚至智能手机通过 VPN 连接公司内部网络。如销售代表在与客户洽谈业务时，通过 VPN 访问公司的客户关系管理（CRM）系统，实时查询客户订单信息、产品库存等，以便为客户提供更精准的服务。现场技术支持人员也可以通过 VPN 获取公司内部知识库中的技术文档和解决方案，及时为客户解决技术问题。

3.5.2.2 个人隐私保护场景

公共 Wi-Fi 环境下的安全上网：在公共场所，如咖啡馆、机场、酒店等提供的免费公共 Wi-Fi 网络，存在较大的安全风险。黑客可能会通过这些开放的网络窃取用户的个人信息，如登录账号、密码、银行账户信息等。个人用户使用 VPN 后，数据传输会被加密，即使连接到公共 Wi-Fi，他人也很难截获和破解传输的数据。例如，用户在机场候机时，通过 VPN 连接访问自己的电子邮箱或网上银行，其账号密码等敏感信息在传输过程中会得到保护。

绕过地理限制访问内容：在一些情况下，某些网站或在线服务可能会根据用户的地理位置限制访问。比如，一些国外的流媒体平台可能只允许在特定国家或地区内访问其内容。个人用户可以通过 VPN 改变自己的 IP 地址，模拟位于其他地区的网络访问请求，从而突破这种地理限制，访问自己想要的内容。不过需要注意的是，这种绕过地理限制访问内容的行为可能涉及到版权和服务协议等法律问题。

3.5.2.3 企业与合作伙伴安全互联场景

业务合作与数据共享：企业在与供应商、经销商等合作伙伴开展业务合作时，往往需要共享一些敏感数据，如产品设计图纸、销售数据、库存信息等。通过 VPN 建立安全的连接通道，企业可以在保障数据安全的前提下，与合作伙伴进行高效的数据共享和业务协同。例如，一家汽车制造企业与零部件供应商之间，通过 VPN 连接，汽车制造企业可以将最新的零部件需求计划及时发送给供应商，同时供应商也可以反馈零部件的生产进度和库存情况，确保汽车生产供应链的顺畅运行。

3.5.2.4 云服务访问场景

安全访问企业云资源：随着企业越来越多地采用云计算服务，如企业云存储、云办公软件等，VPN 可以保障企业员工安全地访问这些云资源。例如，企业将重要文件存储在云存储服务提供商的服务器上，员工通过 VPN 连接访问云存储时，数据传输过程中的安全性得到保障，防止数据在从员工设备传输到云服务器过程中被窃取或篡改。同时，对于一些对数据安全要求较高的企业云应用，如金融企业的云财务系统，VPN 可以提供额外的安全层，确保只有经过授权的员工能够访问相关的云服务。

3.6 多位一体安全策略

防火墙一体化策略功能是一种综合性的网络安全策略管理方式，它将多种安全防护维度和访问权限管理进行整合，形成一个统一的、高效的防护体系，能够更好地应对复杂多变的网络威胁。

3.6.1 以用户为中心的访问权限管理

3.6.1.1 结合管理基线

管理基线是企业或组织根据自身的安全需求、行业法规以及最佳实践制定的一套基本安全规则。它涵盖了网络访问的基本要求，如最小化权限原则，即用户仅被授予完成工作所需的最小权限。例如，在金融机构中，普通柜员只能访问和操作与日常业务相关的客户账户信息，而不能进行系统配置或访问高级别的财务数据。

防火墙的一体化策略将管理基线融入其中。通过预先定义好的基线规则，对用户的访问进行严格的初始限制。当用户发起访问请求时，防火墙会首先参照管理基线进行检查。例如，如果管理基线规定只有特定部门的用户才能访问某一敏感服务器，那么防火墙在收到访问请求时，会核对用户所属部门是否符合要求。

3.6.1.2 以用户为中心组合条件

防火墙能够识别用户的身份，这通常通过多种认证方式实现，如用户名/密码、数字证书、双因素认证等。在识别用户身份后，会获取用户的相关信息，如所属部门、职位、角色等。例如，企业员工使用数字证书登录公司网络，防火墙在验证证书合法性的同时，获取员工的职位信息。

根据用户的身份和其他相关条件（如时间、地理位置、设备类型等）构建访问策略。例如，对于企业的高级管理人员，可以设置在工作时间内，从公司内部办公区域的特定设备类型（如企业配发的笔记本电脑）访问公司核心财务数据服务器的权限；而对于普通员工，禁止在非工作时间访问核心财务数据服务器，即使是在公司内部网络。

3.6.2 基于多维度的一体化防护

3.6.2.1 应用层维度防护

防护元素包括源 IP 地址、目的 IP 地址、源端口、目的端口、协议、应用特征、URL、服务类型和用户。这些元素完整地描述了网络流量的特征。例如，在企业网络中，一个员工从自己的办公电脑（源 IP 地址）通过 HTTP 协议（协议），从源端口 8080 访问公司内部的文件服务器（目的 IP 地址）的 80 端口（目的端口），获取文件服务（服务类型），这个过程中的信息就完整地刻画了这一网络行为。

防火墙的一体化策略可以根据七元组的信息进行细粒度的访问控制。例如，允许特定部门的用户从指定的 IP 地址范围（源 IP 地址），通过特定的端口和协议（如 SSH 协议，端口 22）访问公司内部的开发服务器（目的 IP 地址），而拒绝其他来源或不符合条件的访问请求。同时，还可以对七元组中的每个元素进行流量监测和限制，如限制某个源 IP 地址在一定时间内的连接次数，或者限制特定服务类型的带宽使用。

3.6.2.2 地理维度防护

防火墙利用地理定位技术来确定网络流量的来源或目的地的地理位置。这通常是通过查询 IP 地址数据库来实现的，这些数据库将 IP 地址与地理位置信息（如国家、城市等）

进行关联。例如，当接收到一个来自外部网络的访问请求时，防火墙可以快速确定该请求是来自哪个国家或城市。

根据地理位置信息制定防护策略。例如，对于来自高风险地区（如网络安全威胁高发国家或地区）的访问请求，可以进行更严格的审查或直接拒绝。或者，对于企业在不同国家的分支机构，根据当地的法律法规和网络安全环境，制定不同的访问权限和防护措施。例如，限制某些国家的分支机构访问包含敏感数据的特定服务器，以防止数据泄露风险。

3.6.2.3 时间维度防护

防火墙的一体化策略具有时间控制功能，能够根据预先设定的时间规则来允许或禁止网络访问。例如，可以设置在工作时间（如周一至周五，上午 9 点 - 下午 5 点）允许员工访问公司内部的大部分资源，而在非工作时间，除了一些必要的系统维护人员外，禁止其他员工访问关键业务系统。

这种时间维度的防护在很多场景下都非常有用。例如，对于一些在特定时间段内容易受到攻击的系统（如电商平台在促销活动期间），可以在活动开始前加强防护，在活动结束后恢复正常防护级别。同时，也可以通过时间维度的策略来规范员工的网络行为，提高企业网络的整体安全性。

3.6.2.4 侵防御维度防护

一体化防火墙策略集成了入侵防御系统（入侵防御功能）的功能。入侵防御功能能够实时检测和阻止网络入侵行为，如恶意代码注入、SQL 注入、DDoS 攻击等。当防火墙检测到网络流量中可能存在入侵迹象时，会触发入侵防御功能进行深度检测。例如，当接收到一个包含可疑 SQL 命令的数据包（可能是 SQL 注入攻击），防火墙会将该数据包发送给入侵防御功能进行详细分析。

防火墙根据入侵的严重程度采取不同的防护策略。对于低级别威胁，可能会进行记录和警告；对于高级别威胁，如正在进行的 DDoS 攻击，防火墙会立即阻断相关的网络连接，同时入侵防御功能会对攻击源进行溯源和分析，以便采取进一步的防范措施。

3.6.2.5 病毒防护维度防护

防火墙一体化策略包含病毒防护功能，能够检测和清除网络流量中的病毒。它通常采用病毒特征码匹配和启发式检测等方法。病毒特征码匹配是通过与已知病毒的特征码数据库进行对比来检测病毒；启发式检测则是根据病毒的行为模式和代码特征来判断是否存在

病毒，即使是未知病毒也有一定的检测能力。例如，当一个带有病毒特征的可执行文件通过网络传输时，防火墙的病毒防护功能能够检测到并阻止其传输。

在检测到病毒后，防火墙会采取相应的措施，如隔离感染文件、清除病毒或者直接拒绝包含病毒的网络访问。同时，还可以根据病毒的传播路径和感染情况，调整网络访问控制策略。例如，如果发现某个外部网络是病毒的主要来源，防火墙可以暂时限制该网络的访问权限，直到病毒传播得到控制。

3.6.2.6 威胁情报维度防护

防火墙能够获取和整合外部的威胁情报。这些威胁情报来源广泛，包括安全厂商发布的安全通告、行业组织共享的安全信息以及政府部门发布的网络安全预警等。例如，当安全厂商发布了关于一种新型勒索病毒的预警信息，防火墙可以及时获取并整合这些情报。

根据威胁情报调整防护策略。例如，如果情报显示某一特定的 IP 地址段被用于传播恶意软件，防火墙可以立即将该 IP 地址段加入黑名单，禁止来自该区域的访问请求。同时，还可以利用威胁情报来优化其他防护维度的策略，如更新病毒防护的特征码数据库、加强入侵防御针对新型攻击的检测能力等。

3.7 入侵攻击检测和防护

入侵是指在未经授权的情况下，对信息系统资源进行访问、窃取和破坏等一系列使信息系统不可靠或不可用的行为。常见的入侵方式包括大众熟悉的木马、蠕虫、注入攻击、僵尸网络、DDoS 攻击、跨站脚本攻击、暴力破解等。近年来间谍软件和广告软件等灰色软件的占比也日益增加。入侵朝着利益驱动、多方面渗透的方向发展。根据国家互联网应急中心发布的《2020 年中国互联网网络安全报告》统计，2020 年全年捕获恶意程序样本数量超过 4200 万个，被恶意程序攻击的 IP 地址高达 5000 多万个。

导致这些入侵行为得逞的重要因素之一，就是各类系统中存在的安全漏洞。安全漏洞指的是硬件、软件、协议实现或系统安全策略上存在的缺陷，攻击者通过这些缺陷能够对系统进行非法访问或破坏。虽然系统供应商会从安全事件中识别到安全漏洞，并发布补丁或新的版本来修复系统安全漏洞。但是，系统供应商的更新需要一定的周期。入侵防御技术的主要工作就是检测和防御针对各种安全漏洞的攻击，在系统供应商更新之前，也能提供安全防护能力。因此入侵防御也成为了企业基础网络安全建设的重要组成部分。

入侵防御，即对入侵行为的防御，通常使用以下几种技术进行入侵行为的检测：

3.7.1 入侵检测和防御的技术

入侵防御，即对入侵行为的防御，通常使用以下几种技术进行入侵行为的检测：

- 基于签名的检测技术：该方法将网络流量与已知威胁的签名进行匹配。签名代表了入侵行为的特征，如果该流量匹配了签名则判定为入侵行为的恶意流量。但该方法只能识别出已有签名的入侵，而无法识别新的入侵。
- 基于异常的检测技术：该方法通过采集网络活动的随机样本，并与基线标准进行比较，来判断是否为入侵行为。基于异常的检测技术比基于签名的检测技术识别范围更广，但也增加了误报的风险。
- 基于安全策略的检测技术：该方法使用频率低于前两种，网络管理员会在设备上配置安全策略。任何违反这些策略的访问行为会被阻止。

检测到入侵行为后，入侵防御可以根据配置的响应动作进行自动处置，包括产生告警、丢弃数据包、阻止来自源地址的流量或重置连接。

3.7.2 入侵检测和防御的处理流程

3.7.2.1 数据采集

网络接口监听：入侵防御功能通过网络接口卡（NIC）在网络中进行数据采集。通常会将 NIC 设置为混杂模式，这样它就能够捕获流经该网络节点的所有数据包，而不仅仅是发送到该设备本身的数据包。例如，在企业网络的网关位置部署入侵防御功能，它可以捕获来自外部互联网进入企业内部网络以及企业内部网络之间传输的所有数据流量。

流量镜像：除了直接在网络路径上捕获数据包，还可以通过流量镜像的方式获取数据。交换机可以将一个或多个端口的流量复制到另一个端口，入侵防御功能连接到这个被复制流量的端口上，从而获取需要检测的网络流量。这种方式在不影响原有网络正常通信的情况下，为 入侵防御功能提供了数据来源。

3.7.2.2 数据包预处理

协议解析：采集到数据包后，入侵防御功能会对数据包进行协议解析。它会根据网络协议（如 TCP/IP 协议栈）的层次结构，依次解析数据包的各个协议头部。例如，对于一个 TCP/IP 数据包，会先解析以太网头部，确定源 MAC 地址和目的 MAC 地址；然后解析 IP 头部，获取源 IP 地址、目的 IP 地址、协议类型等信息；最后解析 TCP 或 UDP 头部，确定端口号等。

数据提取：在解析协议的基础上，入侵防御功能会提取数据包中的关键信息，如应用层数据。对于 HTTP 协议的数据包，会提取 URL、请求方法（GET、POST 等）、HTTP 头部

信息以及请求体中的内容。这些提取的信息将作为后续检测的重要依据。同时，还会对数据进行格式化处理，以便更高效地进行检测。

3.7.2.3 威胁检测

特征匹配检测：入侵防御功能拥有一个庞大的威胁特征库，其中包含了各种已知的攻击模式、恶意软件签名、漏洞利用代码等特征。将预处理后的数据包与威胁特征库进行匹配。例如，如果数据包中的数据包含了与已知病毒签名相同的字节序列，或者符合某种 SQL 注入攻击的模式（如在 URL 或 POST 数据中包含特定的 SQL 命令字符串），就会触发特征匹配检测机制。

行为分析检测：除了特征匹配，入侵防御功能还会进行行为分析。它会监测网络流量的行为模式，包括连接的建立和拆除频率、数据传输的速率、数据包的大小分布等。例如，如果某一 IP 地址在短时间内频繁尝试连接不同的端口，这可能是端口扫描行为的迹象；或者如果一个内部主机突然向外发送大量的数据，可能是数据泄露的行为。通过分析这些行为是否偏离正常的网络行为模式，来检测潜在的威胁。

异常检测（基于统计和机器学习）：利用统计方法和机器学习算法来检测异常情况。通过对历史网络流量数据进行统计分析，建立正常网络行为的模型。当新的网络流量与这个模型产生较大偏差时，就视为异常。例如，通过对一段时间内企业内部网络中各主机之间正常通信的流量大小、频率等数据进行统计建模，当出现超出正常范围的流量时，入侵防御功能就会对其进行重点检测。

3.7.2.4 威胁判定与决策

威胁程度评估：当检测到可能的威胁后，入侵防御功能会对威胁的严重程度进行评估。这会综合考虑多个因素，如攻击类型（DDoS 攻击通常比单个主机的扫描攻击更严重）、攻击目标（针对关键服务器的攻击比针对普通终端的攻击更值得关注）、攻击的成功率等。例如，检测到一个针对企业财务服务器的恶意代码注入攻击，且该攻击已经部分成功绕过了服务器的第一层安全防护，这种情况下，入侵防御功能会判定为高威胁程度。

决策策略：根据威胁程度评估的结果，入侵防御功能会做出相应的决策。对于低威胁程度的情况，可能只采取记录日志的方式，以便后续进行分析；对于中等威胁程度的情况，可能会发出警报通知网络管理员，并对可疑的数据包进行隔离观察；对于高威胁程度的情况，如正在进行的 DDoS 攻击或恶意代码传播，入侵防御功能会立即采取阻断措施，如丢弃可疑的数据包、切断可疑的网络连接等。

3.7.2.5 响应与防御措施

实时阻断：入侵防御功能最直接的防御措施是实时阻断威胁。对于被判定为恶意的数据包或网络连接，入侵防御功能会在网络入口处将其拦截。例如，当检测到来自外部网络的包含恶意软件的数据包试图进入企业内部网络时，入侵防御功能会直接丢弃这些数据包，阻止恶意软件在企业内部网络中传播。

连接重置：除了丢弃数据包，入侵防御功能还可以对可疑的网络连接进行重置。当发现某个网络连接存在异常行为，如频繁的非法访问尝试或疑似被攻击者控制的连接时，入侵防御功能会向连接的两端发送连接重置信号，使连接中断，从而防止攻击进一步进行。修改访问控制策略：入侵防御功能可以与访问控制列表（ACL）等访问控制机制相结合。当检测到特定的威胁后，入侵防御功能可以动态地修改 ACL 规则，限制可疑源 IP 地址或用户的访问权限。例如，发现某个外部 IP 地址正在进行暴力破解攻击，入侵防御功能可以临时禁止该 IP 地址对企业内部网络特定资源（如登录页面）的访问。

3.7.2.6 事件记录与反馈

事件记录：入侵防御功能会对整个入侵防御过程中的所有事件进行详细记录。包括检测到的威胁类型、威胁发生的时间、涉及的 IP 地址和端口、采取的防御措施等信息。这些记录会存储在系统日志中，以便后续的审计和分析。例如，在一次网络攻击事件后，安全管理员可以通过查看 入侵防御功能的日志，了解攻击的全过程，包括攻击是如何发起的、经过了哪些步骤、入侵防御功能是如何进行防御的等。

反馈机制：入侵防御功能会根据事件记录和防御效果，向安全策略管理系统或网络管理员提供反馈信息。例如，如果发现某种新型的攻击方式频繁绕过现有的检测机制，入侵防御功能会提醒管理员更新威胁特征库或调整检测策略。同时，管理员对事件的处理结果（如确认某些警报是误报、对攻击事件进行深入调查后的结论等）也会反馈给 入侵防御功能，帮助 入侵防御功能不断优化检测和防御策略。

3.8 病毒防护

计算机病毒（Computer Virus）是一种在计算机系统内进行破坏、传播和自我复制的恶意软件。是恶意代码中的一种，详见《网络安全之恶意代码》。它通常通过电子邮件附件、网络共享、软件下载等方式传播，能够破坏计算机的操作系统、数据文件和应用程序，导致计算机系统出现各种问题。计算机病毒是人为故意编写的，其目的是为了窃取个人信息、破坏计算机系统或者制造混乱等。

下一代防火产品具备深度包检测能力，不仅可以依据病毒特征码进行检测，还能深入分析数据包的内容、结构和行为模式，及时发现隐藏在正常数据中的病毒代码。在防护策略上，基于用户身份和应用场景进行精细化的病毒防护管理，针对不同用户、不同应用程序的访问行为制定特定的防护策略，有效防止病毒通过特定应用或用户行为入侵系统。并且与云端威胁情报紧密结合，实时获取最新的病毒信息和防护策略，快速应对不断变化的病毒攻击态势，为用户提供全方位、实时性的病毒防护保障。

3.8.1 病毒防护检测原理

3.8.1.1 病毒特征码检测原理

病毒特征码是病毒程序中具有代表性的、独一无二的一段代码序列。安全研究人员通过对已知病毒进行深入分析，提取出这些能够唯一标识病毒的代码片段。例如，对于一种特定的文件型病毒，其在感染文件时会在文件头部或尾部添加一段特定的代码用于自我复制和传播，这段代码就可以被提取出来作为特征码。这些特征码会被存储在病毒特征库中，病毒特征库会随着新病毒的发现而不断更新。

当进行病毒检测时，病毒防护软件会扫描计算机系统中的文件、内存、网络流量等可能被病毒感染的对象。对于文件检测，软件会逐字节地读取文件内容，然后将读取的内容与病毒特征库中的特征码进行比对。如果发现文件中的某一段代码与特征库中的病毒特征码完全匹配，就会判定该文件被病毒感染。以电子邮件附件检测为例，当用户收到一封带有附件的电子邮件时，病毒防护软件会在用户打开附件之前，对附件的内容进行扫描，检查是否存在与病毒特征码匹配的内容。

3.8.1.2 启发式检测原理

启发式检测主要基于对程序行为的分析来判断是否存在病毒。它会监控程序在计算机系统中的各种行为，如文件的读写操作、注册表的修改、网络连接的建立等。例如，一个正常的文本编辑程序通常不会主动连接到外部网络并发送大量数据，但如果一个程序在运行过程中频繁地向外发送数据，并且尝试修改系统关键文件，这就可能是病毒的行为迹象。

除了行为分析，启发式检测还会对程序的代码结构进行分析。它会检查程序是否具有病毒程序常见的代码结构特征，如加密、自我修改、代码混淆等。例如，一些病毒为了躲避检测，会对自身的代码进行加密，在运行时再解密执行。启发式检测软件可以识别这种异常的代码结构，从而判断程序可能是病毒。

启发式检测会根据一系列预先定义的规则和算法来评估程序的行为和代码结构。这些规则和算法是通过对大量已知病毒的行为和代码特征进行总结得到的。例如，根据规则，如果一个程序在短时间内尝试修改多个系统文件的扩展名，并且隐藏自身进程，就会被判定为具有较高的病毒风险。

3.8.1.3 文件完整性检查原理

文件完整性检查是通过计算文件的哈希值来实现的。哈希函数是一种单向加密算法，它可以将任意长度的文件内容转换为固定长度的哈希值。例如，常用的哈希算法有 MD5、SHA - 1、SHA - 256 等。对于一个文件，在初始状态下计算其哈希值并存储起来。例如，操作系统的重要文件在安装完成后会计算其哈希值并记录在安全数据库中。

在后续的使用过程中，定期或不定期地重新计算文件的哈希值，并与初始存储的哈希值进行对比。如果文件的哈希值发生变化，就说明文件可能被修改，有可能是病毒感染导致的。例如，一个病毒可能会修改系统文件的内容来实现自身的传播和破坏目的。当发现文件哈希值改变时，就会触发进一步的检查，如对文件进行病毒扫描或者恢复文件的原始版本。

3.9 DDOS 防护

DDoS（分布式拒绝服务）攻击是一种恶意的网络攻击行为。攻击者利用控制的大量计算机（组成僵尸网络），向目标服务器同时发送海量请求数据包。这些请求会大量占用目标服务器的带宽和系统资源，致使服务器无法正常处理合法用户的请求，使目标服务器资源耗尽，无法为正常用户提供服务。其攻击类型多样，包括流量攻击、连接耗尽攻击、协议攻击以及混合攻击等。DDoS 攻击对个人可能造成网页加载缓慢、无法访问网站等问题；对企业会导致业务中断、客户流失、经济损失等严重后果；甚至可能引发大规模的网络拥堵和瘫痪。

聚铭下一代防火墙持续对网络中的流量进行实时监测，能够快速发现流量的异常变化，比如在短时间内某一 IP 地址或 IP 地址段发送的数据包数量急剧增加、特定协议的流量突然增大等情况，这些都可能是 DDoS 攻击的前兆。

不仅监测流量的大小和速率，还对数据包的内容、协议类型、连接模式等进行深度分析。例如，通过分析 HTTP 请求的头部信息、TCP 连接的建立过程等，判断是否存在异常的通信模式，以便更准确地识别 DDoS 攻击。

下一代防火能够识别各种常见的 DDoS 攻击类型，如 SYN Flood（同步包风暴攻击，通过向目标服务器发送大量的伪造的 TCP SYN 包，使服务器的半连接队列被占满，无法处理正常的连接请求）、UDP Flood（用户数据报协议泛洪攻击，向目标服务器发送大量的 UDP 数据包，占用网络带宽和服务器资源）、ICMP Flood（互联网控制报文协议泛洪攻击，发送大量的 ICMP 数据包，如 Ping 请求，使目标服务器忙于处理这些请求而无法响应正常的业务请求）等。

3.9.1 防御策略与机制

- 流量清洗

当检测到 DDoS 攻击流量时，防火墙会将这些流量引导到专门的流量清洗设备或系统中进行处理。清洗过程会去除恶意的数据包，只将合法的流量转发到目标服务器，从而保证业务的正常运行。流量清洗可以基于多种技术，如数据包过滤、协议分析、行为模式识别等。

- 带宽限制

对进入网络的流量进行带宽限制，防止恶意流量占用过多的网络带宽，影响正常业务的通信。可以根据不同的 IP 地址、协议类型、应用程序等设置不同的带宽限制策略，确保关键业务的带宽需求得到满足。

- 连接限制

限制单个 IP 地址或 IP 地址段在一定时间内建立的连接数，防止攻击者通过建立大量的连接来消耗服务器的资源。例如，设置每个 IP 地址每分钟只能建立 100 个连接，如果某个 IP 地址的连接数超过了这个限制，防火墙就会将其视为异常行为并进行拦截。

- SYN Cookie 防御

针对 SYN Flood 攻击，采用 SYN Cookie 技术。在收到客户端的 SYN 请求时，防火墙不立即分配资源建立连接，而是生成一个包含客户端 IP 地址、端口号和时间戳等信息的加密 Cookie，并发送 SYN/ACK 响应给客户端。当客户端返回 ACK 包时，防火墙验证 Cookie 的有效性，只有合法的连接才能建立，从而有效减少服务器上的半开放连接数，防止资源耗尽。

- IP 黑名单与白名单

维护 IP 黑名单和白名单列表。将已知的攻击源 IP 地址或 IP 地址段添加到黑名单中，防火墙会自动拦截来自这些 IP 的流量；而将信任的 IP 地址或 IP 地址段添加到白名单中，确保这些 IP 的流量能够顺利通过防火墙，提高访问的安全性和效率。

3.10 安全管理

3.10.1 日志分析和报表

聚铭下一代防火墙能够全面收集网络活动相关的各种日志信息。这些信息包括但不限于网络连接的源 IP 地址、目的 IP 地址、端口号、协议类型、访问时间，还有安全事件相关的如入侵检测警报、病毒防护记录、DDoS 攻击迹象等。通过将这些日志数据进行集中存储，为后续的深度分析提供了丰富的数据基础。

在分析之前，防火墙会对收集到的日志数据进行预处理。这包括数据清洗，去除无效或重复的数据，例如一些由于网络抖动产生的错误连接记录。同时，还会对数据进行格式化处理，将不同格式的数据统一转化为便于分析的格式。比如，将时间戳统一转化为特定的日期时间格式，将 IP 地址等信息按照标准格式进行存储，为后续的关联分析等操作提供便利。

采用关联分析技术来挖掘日志数据中的隐藏信息。例如，当发现一个 IP 地址在短时间内频繁触发入侵检测警报，并且同时与多个异常的网络连接相关联，防火墙就可以通过关联分析判断这个 IP 地址可能是一个潜在的攻击者。这种技术还可以将不同安全功能模块的日志进行关联，比如将病毒防护记录和网络访问记录关联起来，以确定病毒是通过何种途径进入网络的。

3.10.1.1 数据报表

聚铭下一代防火墙具有预定义的报表模板，这些模板可以根据不同的需求生成各种类型的报表。例如，有安全事件汇总报表，会列出在一定时间范围内检测到的各类安全事件的数量、类型、严重程度等信息；还有网络流量分析报表，会展示不同时间段内的流量峰值、流量来源和去向等信息。管理员可以根据自己的需求选择合适的模板，快速生成报表。

除了模板化报表，还支持定制化报表的生成。管理员可以根据特定的业务需求和安全管理要求，选择需要在报表中呈现的内容。比如，对于关注特定业务系统安全的管理员，可以定制只包含与该业务系统相关的网络访问和安全事件的报表。通过定制化报表，能够更精准地满足不同用户对信息的需求。

报表功能支持将生成的数据以多种格式（如 PDF、CSV、Excel 等）导出，方便管理员将报表发送给其他相关人员进行共享和进一步分析。例如，安全团队可以将安全事件报表发送给管理层，以便管理层了解网络安全状况；也可以将网络流量分析报表发送给网络优化团队，为网络带宽调整等决策提供数据支持。

运用可视化技术将报表数据以直观的图形、图表等形式呈现。例如，使用柱状图来展示不同类型安全事件的数量对比，用折线图来展示网络流量在一段时间内的变化趋势，用饼图来展示不同来源的安全威胁所占的比例等。这种可视化的方式使得复杂的数据变得易于理解，方便管理员快速把握网络安全的关键信息。

3.10.2 威胁多维告警

聚铭下一代防火墙具备强大的多维度告警功能，为网络安全管理提供了全面且及时的风险预警机制。它突破了传统单一告警模式的局限，能够从多个层面精准捕捉安全威胁，并通过灵活多样的组合告警方式，确保管理员能在第一时间获取关键信息，及时采取应对措施。

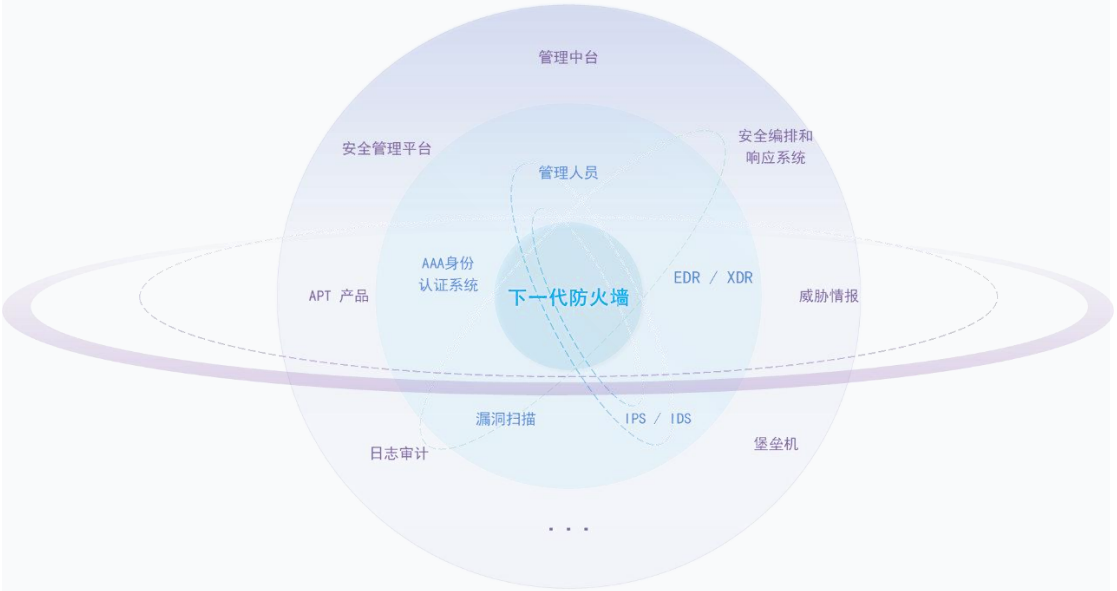
从多维度告警来看，聚铭下一代防火墙可依据丰富的网络活动数据进行智能判断。在网络流量层面，一旦监测到流量出现异常波动，如短时间内流量急剧上升或特定端口流量远超正常阈值，系统立即触发告警。例如，某企业网络在日常工作时段，正常网络流量维持在 100Mbps 左右，突然在某一时刻流量飙升至 500Mbps，防火墙会迅速识别这一异常，将其作为告警触发点。在入侵检测维度，当检测到有外部 IP 地址尝试利用已知漏洞进行攻击，或是发现内部网络存在可疑的端口扫描行为时，也会即刻生成告警信息。此外，针对病毒防护方面，若检测到文件传输中包含恶意病毒代码，亦会触发相应告警。

在告警方式上，聚铭下一代防火墙支持短信、邮件、日志等多种组合形式。短信告警具有即时性强的特点，管理员无论身处何地，只要手机信号正常，就能在第一时间收到简短且关键的告警通知，如 “[时间]，防火墙检测到 [源 IP] 对 [目标 IP] 发起 SYN Flood 攻击”，以便迅速了解网络安全紧急情况。邮件告警则能提供更详细的信息，邮件内容不仅包含告警事件的具体描述，还会附上相关的日志截图、攻击特征分析等，方便管理员深入研究。同时，防火墙会将所有告警事件完整记录在日志中，这些日志不仅可作为后续安全审计的重要依据，还能帮助管理员回溯网络安全事件的发展过程，分析攻击路径与可能的漏洞所在。

通过将这些告警方式进行组合，聚铭下一代防火墙能够满足不同场景下的管理需求。对于紧急且需要立即响应的安全事件，如正在进行的大规模 DDoS 攻击，短信和邮件同时发送告警，确保管理员不会错过重要信息。而对于一些需要长期跟踪和分析的安全态势变化，日志记录则发挥着关键作用，管理员可定期查阅日志报表，总结规律，优化网络安全策略。这种多维度告警与多样化组合告警方式的结合，极大地提升了聚铭下一代防火墙在网络安全防护中的有效性和灵活性，为企业网络安全保驾护航。

3.10.3 接口联动

聚铭下一代防火墙通过 syslog、SNMP、API 等接口实现的联动机制，极大地增强了其在网络安全管理中的效能，为构建全面、智能且高效的安全防护体系奠定了坚实基础。



3.10.3.1 syslog 接口联动技术

syslog 是一种标准的日志记录协议，广泛应用于各类网络设备与系统。在聚铭下一代防火墙中，syslog 接口扮演着关键的数据输出角色。防火墙将大量的网络活动信息，如访问日志、安全事件记录、系统状态变化等，通过 syslog 接口以特定格式的消息发送出去。这些消息包含了丰富的元数据，例如时间戳、设备标识、事件类型以及详细描述等。

当聚铭下一代防火墙检测到重要事件时，例如有外部 IP 地址频繁尝试暴力破解内部服务器的登录密码，防火墙即刻按照 syslog 协议的规范生成相应的日志消息。这些消息会被发送到预先配置好的 syslog 服务器。在 syslog 服务器端，管理员可以利用专业的日志分析工具对这些消息进行集中处理。通过设置规则和过滤器，能够快速筛选出关键信

息，例如按照事件严重级别、源 IP 地址或者特定的攻击类型进行分类。这样，管理员可以直观地了解到网络中发生的各类安全事件，为后续的应急响应和策略调整提供有力依据。

syslog 接口联动的优势在于其简单性和通用性。几乎所有支持 syslog 协议的设备和软件都能接收和处理防火墙发送的日志消息，这使得防火墙能够轻松地与企业现有的日志管理系统集成。在大型企业网络中，存在众多的网络设备和应用系统，通过 syslog 接口将防火墙的日志整合到统一的日志管理平台，有助于实现对整个网络安全状况的全局监控。例如，安全运维团队可以在一个控制台中查看防火墙、路由器、交换机等设备的日志，快速发现跨设备的安全威胁线索。

3.10.3.2 SNMP 接口联动技术

简单网络管理协议（SNMP）用于管理 IP 网络上的设备。聚铭下一代防火墙配备的 SNMP 接口，允许其与网络管理系统（NMS）进行通信。防火墙通过 SNMP 接口向 NMS 提供自身的各种状态信息，包括网络流量统计、设备资源使用情况（如 CPU 利用率、内存占用）、安全策略执行状态等。同时，NMS 也可以通过 SNMP 接口向防火墙发送指令，实现对防火墙的远程管理和配置。

当防火墙的某些关键性能指标或安全状态发生变化时，它会通过 SNMP 的陷阱（Trap）或通知（Inform）机制主动向 NMS 发送消息。比如，当防火墙检测到自身 CPU 利用率持续超过 80%，可能意味着系统负载过高，影响正常的安全防护功能。此时，防火墙会通过 SNMP 接口向 NMS 发送一个包含 CPU 利用率信息的陷阱消息。NMS 接收到消息后，可以根据预先设定的规则采取相应的措施，如自动调整防火墙的资源分配策略，或者向管理员发送警报通知，提醒其关注防火墙的运行状态。此外，NMS 还可以通过 SNMP 的 Get 和 Set 操作，定期查询防火墙的状态信息，或者修改防火墙的配置参数，以适应网络环境的变化。

SNMP 接口联动使得防火墙能够无缝融入企业的网络管理架构。通过与 NMS 的联动，管理员可以在一个统一的管理界面中对防火墙以及其他网络设备进行集中管理。在网络规模较大、设备众多的情况下，这种集中管理方式能够大大提高管理效率。例如，网络管理员可以通过 NMS 实时监控防火墙的流量负载，当发现某个区域的网络流量出现异常增长时，及时调整防火墙的策略，限制非关键业务的带宽使用，保障核心业务的正常运行。

3.10.3.3 API 接口联动技术

聚铭下一代防火墙的 API 接口为其与其他系统的深度集成提供了强大的支持。API（应用程序编程接口）允许开发人员通过调用特定的函数或接口，实现对防火墙的各种操

作，包括查询防火墙的配置信息、获取实时的网络流量数据、创建或修改安全策略等。防火墙通常会提供 RESTful API，这种基于 HTTP 协议的 API 具有简洁、易于使用的特点，方便与各类 Web 应用和其他系统进行集成。

在实际应用中，企业的其他业务系统或安全工具可以通过 API 接口与防火墙进行联动。例如，企业的安全信息和事件管理（SIEM）系统可以定期通过 API 从防火墙获取最新的安全事件数据。当 SIEM 系统检测到一系列相关的安全事件，可能暗示存在潜在的高级持续性威胁（APT）时，它可以通过 API 接口向防火墙发送指令，动态调整防火墙的访问控制策略。比如，临时禁止某个可疑 IP 地址段的所有访问，或者加强对特定端口的流量监控。此外，一些自动化运维工具也可以利用防火墙的 API 实现对防火墙配置的自动化部署和更新，减少人工操作的繁琐性和出错概率。

API 接口联动为聚铭下一代防火墙的应用带来了更多创新的可能性。例如，在云计算环境中，云服务提供商可以利用防火墙的 API，根据用户的业务需求动态调整防火墙的安全策略。当用户在云平台上创建新的虚拟机实例时，云服务管理系统可以通过 API 接口自动配置防火墙，为新实例提供相应的网络安全防护。又如，在物联网场景中，大量的物联网设备接入企业网络，通过 API 接口，防火墙可以与物联网设备管理平台联动，根据不同设备的类型和安全需求，定制个性化的访问控制策略，确保物联网设备在安全的网络环境中运行。

聚铭下一代防火墙的 syslog、SNMP、API 等接口联动技术，各自发挥着独特的作用，从不同角度提升了防火墙的管理效率、监控能力和与其他系统的协同性，为企业网络安全提供了全方位、智能化的保障。

3.10.4 集中管理

在复杂的网络环境中，聚铭下一代防火墙的集中管理功能对于提升网络安全管理效率、保障网络稳定运行至关重要。它通过整合多种关键技术，实现了对防火墙设备的全面、高效管控。

3.10.4.1 设备状态监测

聚铭下一代防火墙集中管理系统运用实时数据采集技术，持续收集各防火墙设备的状态信息。通过私有 API 接口的方式，获取设备的 CPU 使用率、内存占用、网络接口流量、连接数等关键指标。这些数据会被实时传输至集中管理平台，平台运用数据分析算法对数据进行处理与分析，以直观的可视化界面呈现设备状态，例如以仪表盘、图表形式展示

CPU 负载趋势，当指标超出预设阈值时，即刻触发警报，提醒管理员及时处理，保障设备始终处于最佳运行状态。

3.10.4.2 特征库和版本统一升级

特征库升级：集中管理平台与防火墙设备建立安全可靠的通信通道，定期从官方安全数据库获取最新的病毒、入侵检测等特征库数据。采用增量更新技术，仅将新增和变更的特征数据推送至各防火墙设备，大幅减少数据传输量。设备端在接收到特征库更新包后，通过校验机制确保数据完整性与准确性，随后自动加载新特征库，无需人工干预，使防火墙能够及时应对新型网络威胁。

版本统一升级：集中管理平台会监测防火墙的软件版本信息，当有新版本发布时，平台先对新版本进行兼容性测试与评估。确认无误后，利用自动化部署技术，按照预先设定的升级计划，将新版本软件有序推送至各防火墙设备。设备在升级过程中，采用先备份原版本、再进行升级安装的方式，确保升级失败时可快速回滚，保障设备正常运行。

3.10.4.3 统一备份维护

集中管理平台借助网络存储技术，为各防火墙设备创建统一的备份存储空间，定期按照预设策略，通过安全加密通道将防火墙的配置文件、日志数据等重要信息备份至存储设备。备份过程中，运用数据压缩与去重技术，减少存储空间占用，同时确保数据的安全性与完整性。

在设备需要维护时，管理员可通过集中管理平台远程连接至防火墙设备，进行设备重启、配置参数调整等操作。对于设备硬件故障，平台会结合设备状态监测数据，及时定位故障设备，并可远程指导现场人员进行初步排查与处理，提升维护效率。

3.10.4.4 日志统一收集

聚铭下一代防火墙通过 syslog 协议或专用的日志收集代理，将各类日志信息（包括访问日志、安全事件日志、系统运行日志等）发送至集中管理平台。平台运用日志聚合技术，对来自不同防火墙设备的日志进行汇总，并按照统一格式进行存储与管理。借助大数据分析技术，平台可对海量日志数据进行深度挖掘，例如关联分析不同设备的日志，发现潜在的安全威胁线索，生成详细的日志报表，为网络安全审计与策略优化提供有力依据。

3.10.4.5 策略下发

策略制定与编辑：管理员在集中管理平台上，通过直观的图形化界面或策略编辑语言，制定详细的安全策略，包括访问控制策略、入侵防御策略、病毒防护策略等。平台支持策

略模板功能，可快速创建适用于不同场景的策略模板，提高策略制定效率。

策略下发：对于批量下发，平台利用组策略技术，将防火墙设备按照不同的组织架构、功能区域等进行分组，针对不同组制定统一的策略并批量推送。对于单个设备的特殊需求，管理员可单独编辑并下发策略。策略在下发过程中，采用加密传输与校验机制，确保策略准确无误地应用到目标设备，保障网络安全策略的一致性与有效性。

通过以上集中管理技术，聚铭下一代防火墙能够实现对网络中多台设备的高效管理，提升网络安全防护能力，降低管理成本，为企业网络安全提供坚实保障。

4. 应用场景

聚铭下一代防火墙在当今复杂的网络环境中具有广泛且关键的应用场景，为不同规模和类型的网络提供了强有力的安全保障。

4.1 企业网络边界防护

企业网络直接与外部互联网相连，面临着诸多安全威胁，如恶意软件入侵、黑客攻击以及 DDoS 攻击等。聚铭下一代防火墙部署在企业网络边界，能发挥多重作用。一方面，它通过精细的访问控制策略，依据源 IP、目的 IP、端口号、协议以及应用类型等多维度条件，严格限制外部非授权流量进入企业内部网络，同时规范内部用户对外网资源的访问。例如，阻止来自特定高风险地区的 IP 访问企业核心服务器，禁止员工在工作时间访问非工作相关的娱乐网站。另一方面，其强大的入侵防御功能可实时监测并阻断各类已知和未知的入侵行为，如利用系统漏洞发起的攻击。结合病毒过滤功能，能有效查杀进入网络的病毒文件，防止勒索病毒、挖矿病毒等恶意软件在企业内部扩散，保护企业的业务数据和信息系统安全。

4.2 数据中心安全防护

数据中心存储着大量企业关键数据和运行着核心业务应用。聚铭下一代防火墙在此处可实现对数据中心内不同区域（如服务器区、存储区、网络设备区等）之间以及数据中心与外部网络之间的流量管控与安全防护。通过应用识别技术，它能精准区分不同的应用流量，如数据库访问、文件传输、Web 服务等，从而针对不同应用制定差异化的安全策略。例如，对数据库应用实施更严格的访问控制，只允许特定的服务器和用户进行连接，并对传输的数据进行加密监测，防止数据泄露。在数据中心面临 DDoS 攻击时，聚铭下一代防火墙凭借其高性能的流量清洗和负载均衡能力，确保关键业务应用的正常运行，避免因攻

击导致服务中断。

4.3 分支办公网络连接与安全保障

许多企业拥有多个分支机构，分布在不同地理位置。聚铭下一代防火墙可用于构建分支机构与总部之间安全、稳定的连接。通过 VPN（虚拟专用网络）功能，在公网基础上建立加密通道，保证分支机构与总部之间数据传输的保密性和完整性。同时，在分支机构本地，防火墙可对内部网络进行安全防护，执行与总部统一的安全策略，如上网行为管理，限制员工在办公时间访问与工作无关的网站和应用，提高工作效率并降低安全风险。而且，当聚铭下一代防火墙与集中管理平台结合时，企业可以对分布在各地的分支防火墙设备进行统一管理，包括设备状态监测、特征库和版本统一升级、策略批量下发等，极大地提升了管理效率，确保整个企业网络安全策略的一致性和有效性。

4.4 云环境安全防护

在云计算日益普及的今天，无论是企业自建私有云还是使用公有云服务，都面临着云环境下特有的安全挑战。聚铭下一代防火墙可在云环境中发挥重要作用。对于私有云，它可部署在云平台的边界以及内部不同租户或业务单元之间，实现对云内网络流量的精细管控。例如，防止不同租户之间的非法访问和恶意攻击，保障每个租户数据和应用的隔离与安全。

在公有云环境中，云服务提供商可利用聚铭下一代防火墙为用户提供安全增值服务，对用户上传和下载的数据进行病毒扫描和入侵检测，确保云服务的安全可靠。同时，云租户也可自行部署聚铭下一代防火墙，根据自身业务需求定制安全策略，进一步增强在公有云环境中的数据安全性和应用稳定性。

4.5 物联网（IoT）网络安全防护

随着物联网设备的大量接入，物联网网络安全问题愈发突出。聚铭下一代防火墙能够为物联网网络提供必要的安全防护。它可以识别和管理各类物联网设备的网络流量，由于物联网设备种类繁多且通信协议复杂，聚铭下一代防火墙的深度包检测和应用识别技术可准确区分不同设备的流量特征。例如，对于智能家居设备、工业物联网传感器等，根据其特定的通信模式和协议进行流量过滤和访问控制，阻止未经授权的设备接入网络或恶意软件利用物联网设备漏洞进行传播。此外，通过与物联网管理平台联动，当聚铭下一代防火墙检测到异常流量或安全威胁时，可及时通知管理平台采取相应措施，如隔离受感染设备，

保障整个物联网网络的安全运行。

4.6 工业/工业互联防护

在工业领域，生产环境复杂且对网络稳定性要求极高。聚铭下一代防火墙的集中管理技术可针对工业网络中的各类设备，如可编程逻辑控制器（PLC）、数据采集与监控系统（SCADA）等，进行统一防护策略配置。通过集中管理平台，管理员能精准识别工业网络中的关键资产，对不同区域的设备设置差异化的访问控制规则，阻挡外部非法入侵以及内部违规操作。例如，在智能工厂中，可依据生产流程的不同环节，将网络划分为多个区域，对每个区域内的设备实施集中管控，防止因某一设备遭受攻击而引发整个生产系统的瘫痪，有效保障工业生产的连续性与安全性 。