Neusoft

密级:秘密

东软 NetEye 万兆防火墙

技术白皮书

目录

一、 概述

从计算机与网络诞生的那一天起，业务及应用对速度的追求就从未停止过，特别是“三网融合”战略的实施、“云计算”应用的发展、“物联网”时代的到来，使得各种业务应用与发展越来越依赖于高速发展的互联网。日常生活与工作中的视频点播、文件传输、P2P 下载、大附件电子邮件、按需备份和恢复、企业 CRM、ERP 等业务系统提高着我们的生活品质与工作效率，视频会议、VoIP、视频监控与存储等技术使得地球成为一个村庄，远程教育、远程会诊、网络游戏、网格计算、科研协作等加强了企业协作和用户满意度。我们在享受着高品质网络服务的同时，也在消耗着共享的网络资源。应用和业务的发展是新技术发展的源动力，新技术的发展，使得“千兆桌面，万兆核心”的时代提前到来，不少企业开始大规模改造网络，以适应这一新时代的到来。万兆核心网络的普遍应用，也必然催生出万兆安全设备特别是万兆防火墙的诞生。

跨地域的超大企业集团、跨国企业和机构的业务规模和管理复杂度也呈现爆炸式的增长，企业信息化建设已经替代传统的运营管理模式，使得跨地域企业网的集中安全管理成为可能。萨班斯法案、等级保护、分级保护的颁布与应用，使各企业机构对网络安全重视程度日趋增强，各业务部门职能和权限划分越来越细化和清晰，根据业务部门的不同设置不同安全级别的安全域，成为企业信息安全建设的标准。安全域的划分，以及安全域之间有效的互访控制，使得对安全域进行隔离的基石——防火墙提出了更高的性能要求。

IT 基础设施越来越庞大，分布越来越广，使得 IT 系统变得更加复杂而难以管理；IT 设备对能源的巨大消耗越来越违背目前低碳发展的呼吁，这一切都推动了虚拟化技术的发展，做为网络安全的基础设备——防火墙，也开始向着高度虚拟化、低碳的方向发展，而虚拟化的要求，也向防火墙的性能提出了挑战，低碳经济的趋势也更对防火墙的体系架构提出了苛刻的要求。

东软 NetEye 万兆防火墙以其独特的多核+FPGA 架构加速着万兆核心时代的发展，满足着大型企业安全标准的需要，高密度的虚拟防火墙技术顺应着低碳发展的潮流。

二、 多核+FPGA 功能与性能的和谐统一

2.1 引领未来应用级芯片发展方向的 FPGA

近年来，处理器性能提升受到功耗的限制，使得其提升速度已经渐缓于摩尔定律，因而也大大制约着各种应用的发展。然而最新科学研究的发展却使得市场相信，基于应用级芯片将发生质的突破。

Intel 公司在“超级计算机 2010”会议宣称：处理器未来发展仍然取决于在芯片中集成更多内核，该公司的 SCC（单芯片云计算机）处理器“理论”上可以支持 1000 个内核。然而就在 Intel 对 1000 个内核 CPU 的研究还停留在理论上的同时，2010 年 12 月 30 日英国格接斯哥大学和美国马萨诸塞大学的科学家们已经制作出一种在一个芯片上有效包含 1000 多个内核的处理器。该处理器使用了一种称为 FPGA（现场可编程门阵列）的芯片，通过在一个 FPGA 芯片上创建 1000 个以上的微型电路，就能把这种芯片转变为一个 1000 个内核的处理器，每个内核按照自己的指令工作，这种芯片处理能力巨大而耗电量非常小。在测试中，它的处理速度高达每秒 5GB，是目前顶级多核台式电脑速度的 20 倍。该项研究的进展也向业界展示未来芯片的发展方向。

2.2 高性能硬件架构大比拼

国内外众多安全厂商防火墙产品在初级阶段的发展历程是相似的，百兆网络阶段甚至准千兆阶段的防火墙产品都是基于传统的 X86 架构。传统 x86 架构以其灵活性、扩展性、易开发性能够满足百兆和普通千兆网络的需要。

多核技术的发展也推动着防火墙处理性能的提升，迅速将防火墙的性能从准千兆提高到多千兆。它是将多个 CPU 集成在一块芯片上，充分发挥了 CPU 对应用层数据的处理优势，各个厂商尽其所能，优化算法，使得防火墙的功能和性能得到大幅度提高，但终因体系结构限制，万兆线速的处理能力成为其发展的极限。于是在万兆防火墙的开发上出现了多个分支，出现多种半导体解决方案，众多的解决方案中可以归类为 ASIC 和可编程器件两大类。

ASIC 技术固然可以提供高性能的万兆级高端产品，但由于其功能固定、灵活性有限、开发费用高、开发周期长等缺点，使只能用于功能固定简单防火墙产品。在今天客户日益对防

火墙功能要求增多的情况下，制约着 ASIC 类产品的发展，使得 ASIC 类的产品在功能上无法与可编程类产品进行竞争。

可编程器件类主要包括两类：NPU（网络处理器）和 FPGA。NPU 提供以处理器为中心的可编程特性，即以软件为中心，而 FPGA 则提供以硬件为中心的可编程特性，这使得以 NPU 技术为主的产品在性能上大低于以 FPGA 技术为主的产品，然而 NPU 与 FPGA 的差别不仅表现在性能上，还表现在下表中。

属　　性	NPU	FPGA
芯片数量	需要多个 NPU 芯片	只需要一块 FPGA 芯片
应用层数据处理	需要进行硬件软件的区分增加系统复杂度，系统延迟和功耗大	完全采用硬件并行处理，功耗和延迟小
软件可升级性	不具备代码复用性，产品升级困难，开发周期长	具有代码复用性，具有较强的软件升级功，开发周期短
硬件可升级性	只在处理器中可编程，对应用协议变化的适应性差	现场可编程，能够轻松升级，很好满足需求变化
开发周期	采用汇编代码，调试以及开发周期长	采用 HDL，调试以及开发周期短

因此，无论从未来发展方向还是目前的发展趋势看，FPGA 将会在应用类网络产品中扮演着性能杀手的角色。

2.3 多核+FPGA 技术

东软安全充分依托东软集团在软硬件开发上的优势，在 FPGA 芯片的开发和研究上一直处于业界领先地位，基于多核技术与 FPGA 技术的优势，东软创造性地将多核 CPU 技术与 FPGA 结合起来，既满足了性能的需求，又使功能的灵活性大大优于单纯的 FPGA 技术，达到性能与功能的和谐统一，将 FPGA 的优势发挥到了极致。

东软 NetEye 万兆防火墙采用双主处理模式，即多核处理器和 FPGA 均作为主处理器，为充分发挥 FPGA 的优势，利用 FPGA 技术实现完整的 TCP/IP 协议栈处理，包括 ARP 模块、IP 处理模块、TCP 处理模块、包分类模块、内存管理模块、事件管理模块等模块，策略匹配、特证识别等均由 FPGA 芯片快速处理，使其充分发挥芯片硬件加速优势。而对于事件调度、

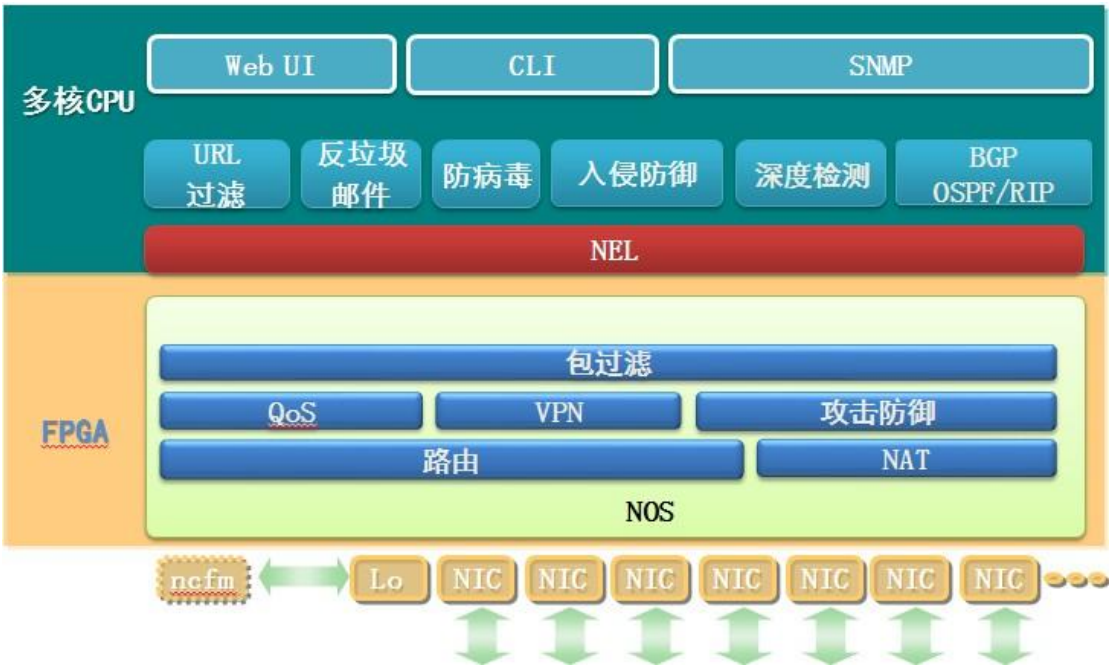
报表生成、高级复杂应用协议等则交由多核处理器完成，从而实现控制层、转发层、数据层的分工协作和并行处理优势。

三、 东软 NetEye 万兆防火墙

3.4 NetEye 万兆防火墙产品软件系统架构

东软 NetEye 万兆防火墙采用多核+FPGA 的架构，把对 TCP/IP 协议层数据分模块交给 FPGA 芯片处理，而将复杂的应用协议处理和深度包检测交给多核 CPU，从而高效集成了应用层安全防护功能，充分发挥了处理器处理应用协议的优势和 FPGA 芯片硬件加速的优势，使得东软 NetEye 万兆防火墙的性能得到了几何级的提升。

如下图所示，TCP/IP 协议层的功能如路由功能、NAT 功能、QoS 过滤、VPN 功能、DDOS 攻击防御、包过滤等功能由 FPGA 芯片完成。而多核 CPU 则会有充足的资源来实现防病毒、反垃圾邮件、URL 过滤、入侵防御和深度检测等高级安全防护功能，可为用户网络提供全方位，多层次的快速安全保障。



NetEye 万兆防火墙软件系统架构图

3.5 NetEye 万兆防火墙产品功能特色

NetEye 万兆防火墙系列产品具有高性能、高安全性、高可靠性和易操作性等特性。产品支持防病毒、反垃圾邮件及 URL 过滤功能，同时具备深度入侵防御、精细流量控制，以及细粒度的协议控制及协议异常检测等多项功能，能够为用户提供全面的安全网络体验。

3.5.1 高性能的基础防火墙功能

东软 NetEye 万兆防火墙凭借创造性的将基础防火墙功能移植到 FPGA 芯片上，使得防火墙基础功能在性能上得到大幅度提升。这些基础功能包括：

- 基于状态检测技术的访问控制

NetEye 万兆防火墙系列产品采用基于状态检测处理机制，可以根据数据包的源地址、目标地址、协议类型、源端口、目标端口、网络接口和 VLAN 标记等对通过防火墙的数据包进行严密的访问控制，实现了高性能、可扩展、透明的对应用层协议的支持和保护。

- 网络地址转换（NAT）

NetEye 万兆防火墙系列产品支持多种 NAT 转换：包括静态转换、动态转换、端口映射、地址映射（Mapped IP)。灵活的 NAT 地址转换功能不但可以帮助用户节省 IP 资源，同时也可以隐藏内网上主机的真实 IP 地址，从而提高网络的安全性。

- 完善的路由能力

NetEye 万兆防火墙系列产品支持静态路由、策略路由、动态路由（支持 RIP 、OSPF 和 BGP)。普通防火墙的路由策略只能根据单个 IP 包中的源地址进行判断，NetEye 万兆防火墙产品内置多个路由表，便于用户根据实际网络需要进行合理的路由选择，用户可以根据源 IP 地址、服务、入口接口和 ToS 值来细化路由选择，部署使用更加灵活。以高校为例，如果是由内部访问外网，可以根据预先制定的策略，访问免费地址使用教育网出口，访问其它地址使用电信出口。这种方案在保证网络资源得到有效利用的同时，降低了网络日常运行费用。

- 多播协议支持

NetEye 万兆防火墙系列产品实现了对多播相关协议的支持，包括互联网组管理协议 IGMP，DVMRP 等。由于 NetEye 万兆防火墙设备具有极低的时延，可以保证多播应用的顺

畅和实时性。同时 NetEye 万兆防火墙还可以对多播数据的传送范围加以限制，提升多播应用安全的同时降低不必要的网络资源占用。

3.5.2 业界领先的虚拟系统技术

虚拟系统技术是将一台独立的设备从逻辑上划分为多个彼此独立的设备。东软 NetEye 万兆防火墙以虚拟系统技术为基础，在虚拟系统中集成了防病毒（Anti-Virus）、反垃圾邮件（Anti-Spam）、URL 过滤和入侵防御等功能。东软 NetEye 万兆防火墙支持基于虚拟系统级别带宽管理功能，允许用户设置每个虚拟系统的最大带宽、保证带宽和优先级。用户可以通过此功能，可以合理调整网络资源分配比例，大大提高网络资源利用率。

东软 NetEye 万兆防火墙在虚拟系统中集成了 VPN 功能，每个虚拟系统都可以在网络中独立作为 VPN 网关进行部署。不仅丰富了用户构建虚拟专用网部署方案，而且大大为用户降低了部署虚拟专用网的成本。

在虚拟系统之间，东软 NetEye 万兆防火墙实现了接口虚拟化和网络虚拟化。虚拟系统之间的通信无需借助外部三层设备，直接在虚拟系统之间通过虚拟接口，虚拟网络来实现虚拟系统间的互访。相比传统的虚拟防火墙技术，虚拟接口和虚拟网络技术的实现大大提升虚拟化技术的网络适应性，为用户网络安全提供高度灵活，扩展性强的部署方案。

3.5.3 基于 NEL 核心技术的入侵防御功能

NEL 是 NetEye 万兆防火墙系列产品的核心检测技术（patent-pending：200610046168.1），该技术将引擎、协议分析和攻击检测分为三部分进行开发，然后再通过 NEL 将它们的工作结合起来，这样可以避免由一个或两个规模很大的开发小组来维护整个检测语言系统的开发工作。另外，NEL 增加了检测技术的适应性，可以共享各类事件库，从而能够更多的检测出各类攻击。另外，由于 NEL 检测粒度非常精细，所以能够更加准确的判断网络工具行为。

3.5.4 细粒度的协议限制及协议异常检测

NetEye 万兆防火墙产品针对应用层协议提供了细粒度的协议限制功能和协议异常检测

功能，支持的协议包括：HTTP、SMTP、POP3、IMAP 和 DNS 等。由于应用层协议本身比较复杂，考虑到一些用户无法全面了解协议的每一个细节，特意设计了高、中、低三种默认防护级别。此外，为了满足高级用户的配置需要，NetEye 万兆防火墙也预留了协议细节的配置接口，高级用户可以根据具体网络情况自定义协议细节以满足用户个体的安全需求。

考虑到攻击者常常通过发送针对特定应用协议的异常数据包来对被攻击者的信息进行收集，或发送大量异常协议数据包作为攻击手段对目标实施攻击。NetEye 万兆防火墙产品支持对应用级别协议进行异常检测，通过拒绝异常数据包来阻止这些非法的数据包，最大化保障网络安全。

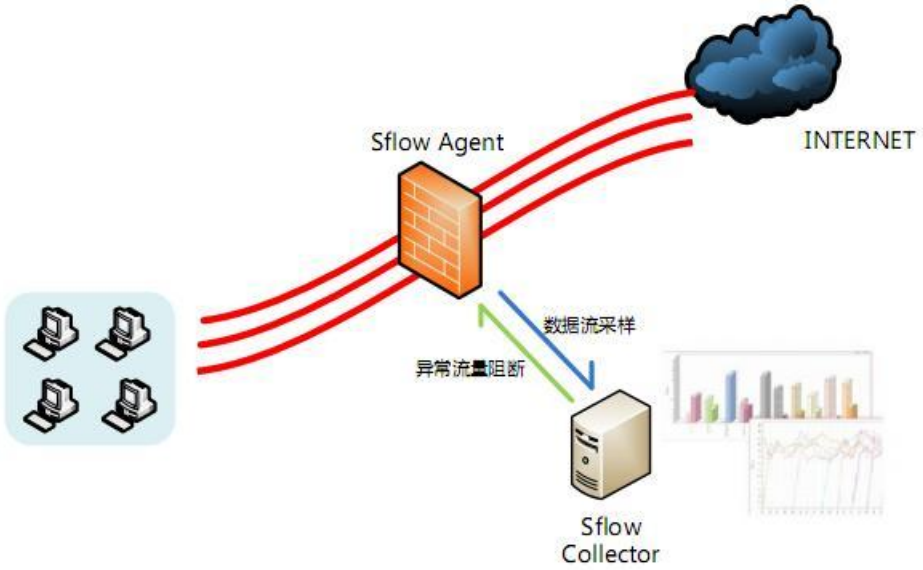
3.5.5 先进的“云安全”技术

NetEye 万兆防火墙系列产品采用了世界领先的云安全技术，可以通过互联网的检测中心，快速分析垃圾邮件、恶意 URL、病毒等风险，充分具备零时（Zero-Hour）防御能力。通过云检测技术，NetEye 万兆防火墙只需对邮件的关键字段进行 hash 运算，并将运算结果送到云中，更多的检测工作在云中实现，从而规避了 NetEye 万兆防火墙自身因为进行特征检测而导致的性能下降。

3.5.6 完善的流量分析解决方案

Flow 协议是具有三层交换技术的网络设备才能够支持的协议，而 Flow 记录能够提供传统 SNMP MIB 无法比拟的丰富信息，因此 Flow 数据被广泛用于高端网络流量测量技术的支撑，提供网络监控、流量图式分析、应用业务定位、网络规划、快速排错、安全分析(如 DDOS)、域间记帐等数据挖掘功能。

NetEye 万兆防火墙系列产品为了与先进的流量分析设备具备良好的兼容性，提供了 SFlow 记录输出功能。防火墙在网络中作为一个 sFlow Agent 进行部署，通过抽样技术获取网络流量状态并将整理好的抽样信息发送给 sFlow Collector。当发现异常流量时，SFlow Collector 可以与防火墙进行联动，发出阻断异常流量的命令，最大化提升网络安全性。



3.5.7 超强的抗 DDoS 攻击模块

东软 NetEye 万兆防火墙带有专业的抗 DDoS 攻击模块，该模块既可以集成于万兆防火墙产品，也可以单独作为专业的抗 DDoS 设备，它使用户能够以最高的性价比享受专业的 DDoS 攻击防护。针对 DDoS 攻击，该模块不同于传统安全设备采用超过阈值随机丢包的不负责任的防护算法。它在 FPGA 硬件上采用协议分析技术，对带有明显攻击特征的违反 RFC 标准的畸形数据包、攻击数据包直接进行丢弃，采用了自主研发的新一代基于统计和阈值、专有反向探测等防拒绝服务攻击算法，可以对流量型 DDoS 攻击如 SYN FLOOD、ACK FLOOD、TCP CONNECTION FLOOD、UDP FLOOD、ICMP FLOOD、FRAG FLOOD 等各种常见的危害很大而又易于发起的攻击方法进行快速有效的识别，在对网络数据报文进行统计的基础上，对于不同类型的 DDoS 攻击采取了相应的防御算法，从而可以准确而实时地在大流量背景下识别出恶意的 DDoS 流量，与其它同类产品相比，也减少了反向探测的数据流。它也可以在多核 CPU 上实现对应用层协议 DDoS 攻击的防护，如 Http Get Flood（CC 攻击）、Http Post Flood 攻击、连接耗尽型攻击等。

3.5.8 专业的 DNS 防护模块

东软安全有着长期为客户服务的经验，在 DNS 系统的防护方面积累了大量的经验，并具

有完整的针对 DNS 系统解决方案，该解决方案不仅能够对 DNS 系统自身安全进行有效地防护，还能够对来自于外部的攻击进行防护。为保证客户 DNS 服务器的正常运行，东软将该解决方案智能地整合为 DNS 防护模块，提供动态、主动、深度地防御。该模块也被嵌入在东软 NetEye 万兆防火墙产品中。基于 NEL 平台技术的 NetEye DNS 防御模块针对网络层、应用层的 DNS 攻击采用细粒度的协议限制和协议异常检测功能，能够主动防御已知和未知攻击，实时阻断针对 DNS 服务器的各种攻击。

3.5.9 高可靠的 VPN 隧道冗余技术

随着 VPN 技术的成熟和发展，虚拟专用网被得到企业用户的广泛认可。VPN 也逐渐取代专线连接，成为远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的连接的首选安全解决方案。在 VPN 被广泛应用的同时，问题也随之而来。VPN 网关具有单点故障的风险，我们如何在保证信息传输安全的同时为虚拟专用网提供高可用性机制呢?

NetEye 万兆防火墙产品在国内产品中率先引入了国际上流行的 VPN 高可用性机制---VPN 冗余网关技术。用户可以选择连接不同 VPN 网关的几条隧道，建立一个隧道组。NetEye 万兆防火墙产品按照指定的选择算法选择优先级最高的可用隧道建立 VPN 连接。当出现故障导致优先级最高的可用隧道断开时，NetEye 万兆防火墙产品会按照优先级或指定的选择算法选出一个可用隧道，已建立的连接和新建立的连接都切换到新选择出的隧道。NetEye 万兆防火墙产品同时提供监控机制，若发现优先级更高的隧道恢复正常，则会话会立即被切换回优先级最高的隧道。这样几条可用隧道可以互为备份，可以提供 VPN 隧道冗余机制，最大化保证 VPN 业务实时连通和最优选择。NetEye 万兆防火墙产品提供了虚拟专用网级别的高可用性。

3.5.10 ICAP 外部病毒扫描功能

ICAP 技术主要用于 NetEye 万兆防火墙系列产品同分布式病毒服务器集群之间的数据通信。NetEye 万兆防火墙系列产品内置一个 ICAP Client，将其获取的所有数据按照 ICAP 约定的格式封装好，发送给支持 ICAP 协议的分布式病毒服务器集群进行病毒扫描。ICAP 技术的的使用将病毒扫描的工作交由分布式病毒服务器集群进行“云”查杀，降低了 NetEye 万兆防火墙产品设备的负荷，节约了系统资源，大大提升了设备性能和稳定性。

目前 NetEye 万兆防火墙产品支持对 HTTP 协议数据流进行 ICAP 封装，采用分布式病毒服务器集群进行病毒扫描。

3.5.11 强大的反垃圾邮件引擎

NetEye 万兆防火墙产品的防垃圾邮件包括自动扫描和手动配置过滤功能，全面满足不同用户的不同需求。自动扫描功能采用了业界领先的“服务器端加用户设备端”的整体架构。服务器能够将来自于全球的邮件来源历史和最新的发件人信誉数据进行汇总分析；采用先进的循环模式检测技术自动从鸟瞰图中汇总所有发件人信息，并实时区分合法发件人、有效发件人、垃圾邮件等。服务器端能跟踪超过数千万个 IP 地址的流量，且每周实时对数十亿封邮件进行分类。用户设备端将联合服务器端进行邮件扫描，能最大程度防御网络中的垃圾邮件。相对于传统的单机内容过滤模式，NetEye 万兆防火墙产品的垃圾邮件扫描功能可以做到：过滤更加准确，响应速度更快，在真正做到一劳永逸的解决网络垃圾邮件的问题的同时降低了设备的负载，优化了系统资源分配，大大提升设备的稳定性和工作效率。同时手动可配置项包括针对 IP 地址、邮件地址、关键词建立黑白名单，达到传统垃圾邮件过滤的功能。

3.5.12 实用的互联网域名访问加速机制

随着互联网的进一步发展，人们对网络浏览速度的要求也越来越高。在网络访问过程中域名解析服务也成为影响网络访问速度的原因之一。NetEye 万兆防火墙系列产品提供了互联网域名访问加速机制，在 NetEye 万兆防火墙上将内网用户的 DNS 请求的解析结果进行动态的收集，存储在防火墙上的 DNS 缓冲区中。当网络中的用户再次请求这个域名时，NetEye 万兆防火墙会提取缓存中的结果快速进行应答，避免再次向 Internet 转发 DNS 解析请求数据包，从而大大提升了域名解析效率，提高网络访问速度。此外，NetEye 万兆防火墙还提供了静态缓存机制，DNS 中继代理功能和主机 DNS 解析服务等一套完善的域名解析服务体系，提高网络访问速度的同时可以为用户提供安全、稳定、高效的域名服务解决方案。

3.5.13 人性化的安全集中管理

NetEye 万兆防火墙系列产品支持集中管理，大大降低了大型网络部署的维护难度和控制

难度。日志审计管理相对于传统一对一的网络安全管理模式，用户可以在一台 SCM Console 上一次性完成对所有被管理设备的日志审计工作。有效降低网络安全管理的复杂度，达到为企业减少网络安全管理成本的目的。同时 NetEye 万兆防火墙安全集中管理系统为用户提供的日志过滤和日志查询等工具能够大幅提升用户在处理日志审计时的工作效率，节省审计时间。

- 网络安全状况实时监控

NetEye 万兆防火墙系列产品安全集中管理系统的实时监控功能为用户提供了一种集中监控网络安全情况的手段。通过集中收集网络中所有防火墙上的数据，实时监控功能可以为用户提供所有防火墙和网络连通性的实时监控信息。用户可以通过这套系统对网络当前的流量和使用率进行全面的统计和分析。用户还可以通过此系统来生成不同的网络流量监控图表。通过这项功能，用户可以最大程度的监控网络上的安全状况。

- 报表生成

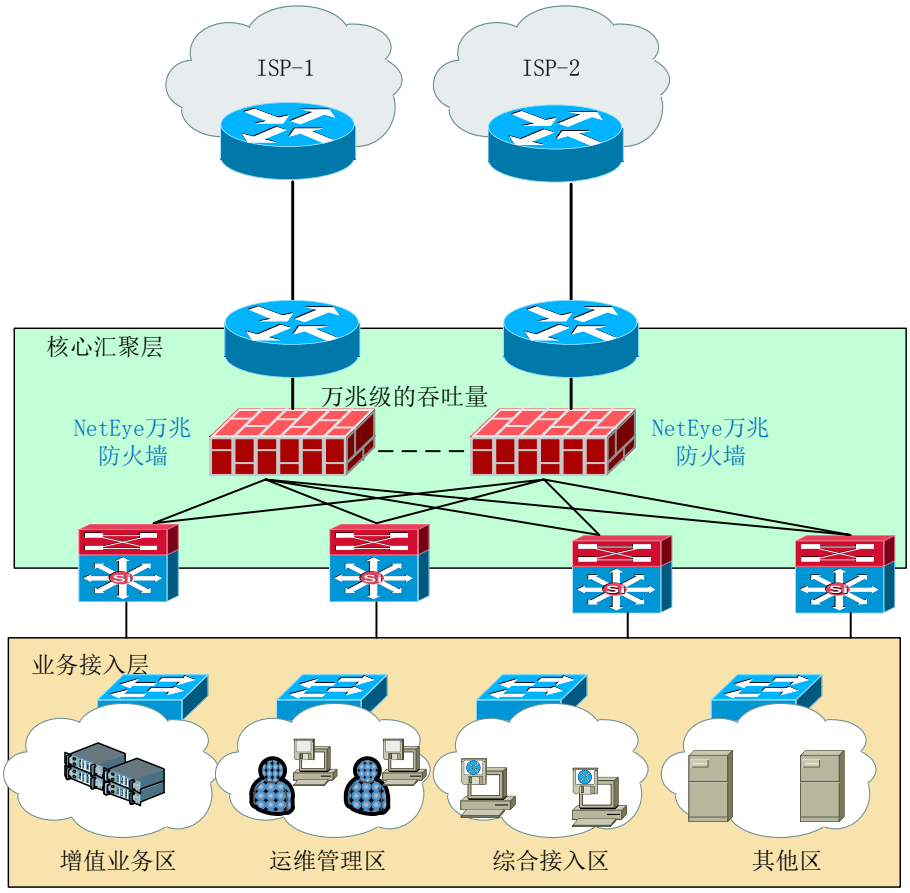
NetEye 万兆防火墙系列产品安全集中管理的报表生成功能以系统收集到的安全事件和实时监控信息为基础，可以为用户生成多种灵活、直观的历史报表。通过报表，用户可以从一个总体角度来了解网络安全的状况。

- 按设备划分管理域

为了满足用户对不同网络安全设备的不同管理需求，NetEye 万兆防火墙系列产品安全集中管理系统实行了按设备划分管理域的概念。核心理念是：不同的用户可以和与其相关的设备和设备组进行绑定。同时，用户被赋予了对这些设备不同的访问权限。通过这种方式 SCM 系统可以实现将指定设备或设备组和访问权限划分给特定的用户，以达到对设备和其访问权限的区域化管理。

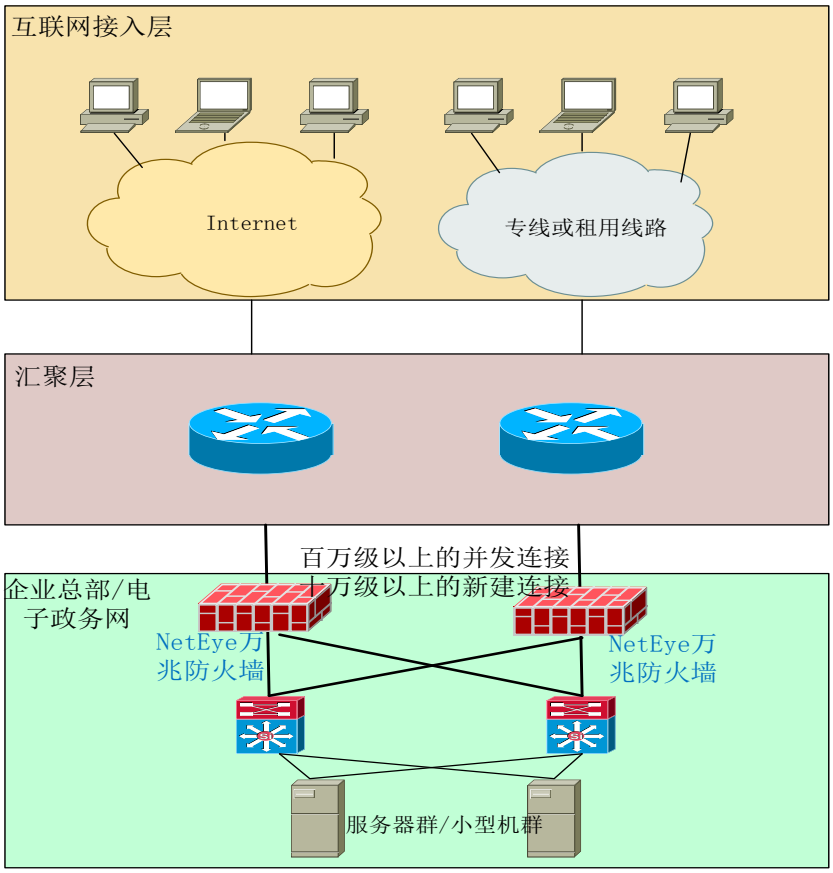
四、 典型应用场景

4.1 大型企业数据中心安全防护



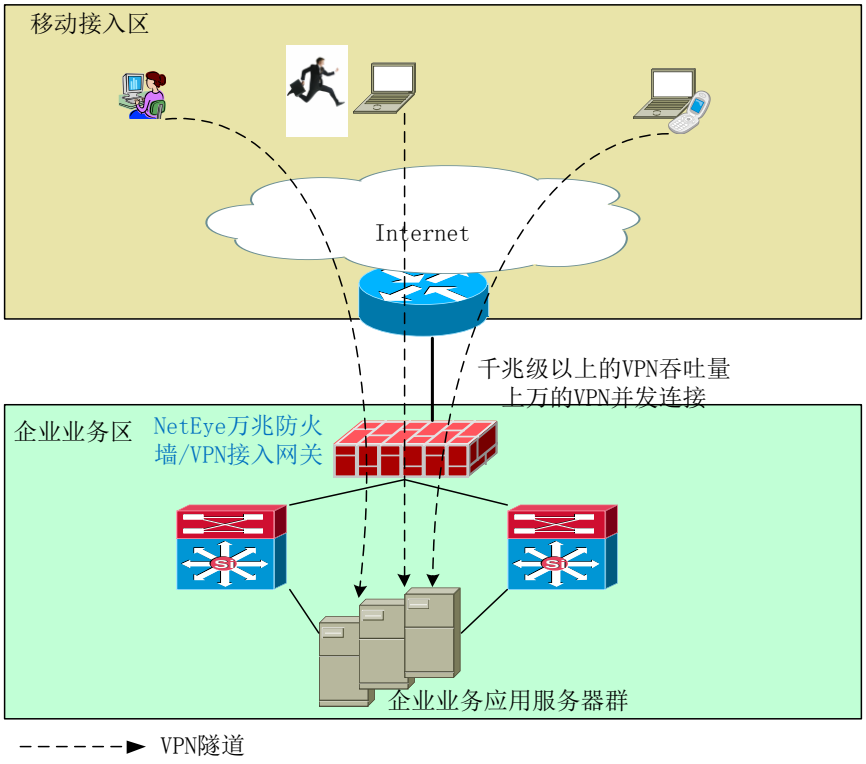
NetEye 万兆防火墙在大型企业数据中心的应用

4.2 政府和大型企业网络安全防护



NetEye 万兆防火墙在政府和大型企业网络中的应用

4.3 移动办公网络的安全防护



NetEye 在移动办公网的应用