Neusoft

东软集成安全网关
NISG/NISG-IPS 技术白皮书

东软公司 网络安全产品营销中心

目录

一、 前言

本文档适用于东软集团股份有限公司(以下简称东软公司、东软或者本公司)制造的东软集成安全网关（NISG）系列产品的销售工作，力图从产品技术角度提供必要的参考说明。

本文档主要内容包括 NISG 产品体系构架、功能特色和技术参数等方面的相关数据，便于阅读者快速掌握 NISG 产品的基本概况，提高对项目需求判断和设备选型的正确率。

同时，需要指出的一点是，本文档所包含的各项数据，尤其是产品技术型号、指标参数，均为现阶段的一般性数据，仅供阅读者了解、理解 NISG 产品的普遍情况使用。考虑到东软公司经营管理策略、技术研发进度和特定项目需求等因素，在实际供货时，所有数据指标均有可能发生更新变化，并将通过随机标准文档予以说明。

二、 NISG 产品概述

应用背景

安全网关的“3G”（The 3rd generation）时代来临。

随着网络与信息技术的发展，尤其是互联网的广泛普及和应用，网络正逐步改变着人类的生活和工作方式。越来越多的政府、企业组织建立了依赖于网络的业务信息系统，比如电子政务、电子商务、网上银行、网络办公等，对社会的各行各业产生了巨大深远的影响，信息安全的重要性也在不断提升。

提到安全网关,过去通常以网络安全市场中占有率最高的防火墙为代表。20 世纪末以来，防火墙技术的发展，历经了包过滤技术、应用层检测技术两个时代，每一次进步，都源于技术的创新。

包过滤技术可以有效的抵御 DOS/DDOS 攻击，而应用层检测技术可以在一定程度上提升对网络应用的安全防护能力。近年来，企业所面临的安全问题越来越复杂，安全威胁正在飞速增长，尤其混合威胁的风险，如黑客攻击、蠕虫病毒、木马后门、间谍软件、僵尸网络、DDoS 攻击、垃圾邮件、网络资源滥用（P2P 下载、IM 即时通讯）等，极大地困扰着用户，给企业的信息网络造成严重的破坏。此时，传统的安全网关已经无法有效的起到网络安全防护作用。如果简单的用堆叠的手段将反垃圾邮件网关、WAF 网关、IPS 等产品一并部署到用户网络中，既增加用户的投资，同时更会极大降低网络的稳定性。为了解决上述问题，东软率先推出了第三代安全网关—**东软集成安全网关（NISG）**。NISG 产品有效的解决了安全产品堆叠所带来的问题，在确保网络稳定的前提下，极大的提升安全防护能力。

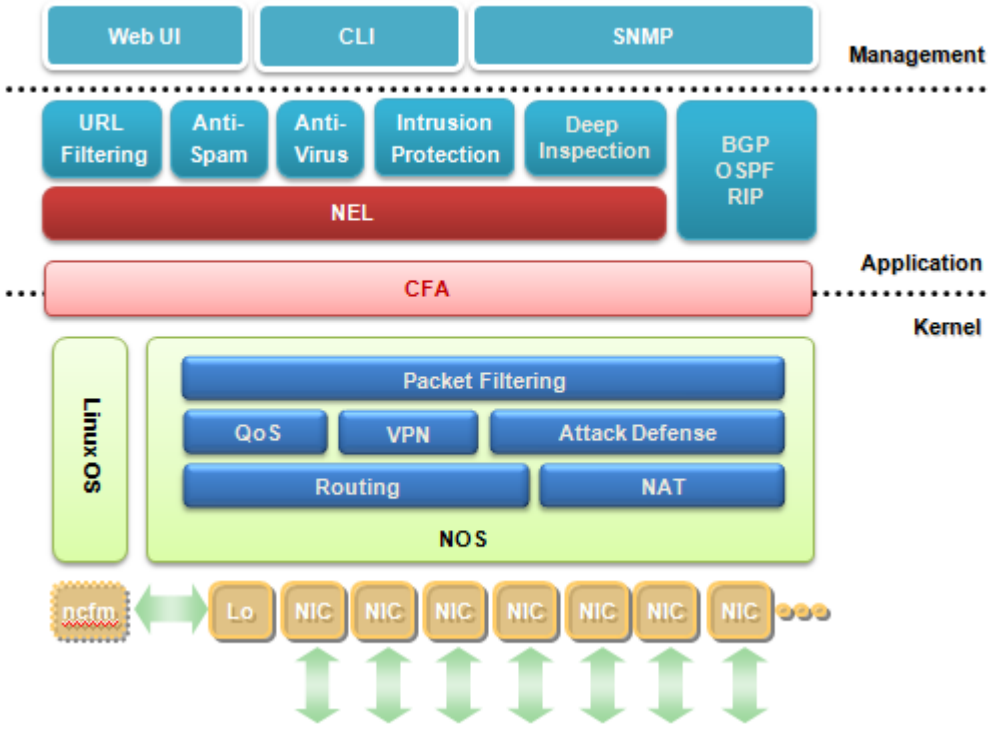
产品概述

针对日趋复杂的应用安全威胁和混合型网络攻击，东软网络安全适时推出东软集成安全网关（NISG）系列产品以满足用户的安全需求。东软集成安全网关（NISG）系列产品是东软拥有自主知识产权的新一代安全产品，其设计目标旨在完成传统防火墙访问控制功能基础上，为用户网络提供防病毒、反垃圾邮件、URL 过滤、入侵防御和深度检测等应用级别的安全防护。NISG 系列产品采用虚拟化技术、云检测技术，将 NEL 核心专利技术融入产品，使得本产品具备安全实用、高效过滤、检测准确的特点。NISG 系列产品弥补了防火墙、防毒墙、入侵检测系统和反垃圾邮件网关等单一产品的不足，提供动态的、深度的、主动的安全防御，为企业提供了一个全新的立体的网络安全解决方案。

三、 NISG 产品简介

3.1 NISG 产品软件系统架构

东软集成安全网关（NISG 系列产品）采用统一的、灵活的和高扩展性的安全产品系统架构。在传统的防火墙功能基础上，高效集成了应用层安全防护功能。NISG 系列产品可以实现防病毒、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，多层次的安全保障。



3.2 NISG 产品功能特色

东软集成安全网关（NISG）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。产品内置防病毒、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。

- 强大、稳定、高效的基础防火墙功能
- 业界领先的虚拟 UTM 技术
- 基于 NEL 核心技术的入侵检测
- 先进的“云安全”技术
- 完善的流量分析解决方案

3.2.1 强大、稳定、高效的基础防火墙功能

- 基于状态检测技术的访问控制

基于状态检测技术的访问控制东软集成安全网关（NISG）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）

东软集成安全网关（NISG）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了 I 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

东软集成安全网关（NISG）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，NISG 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

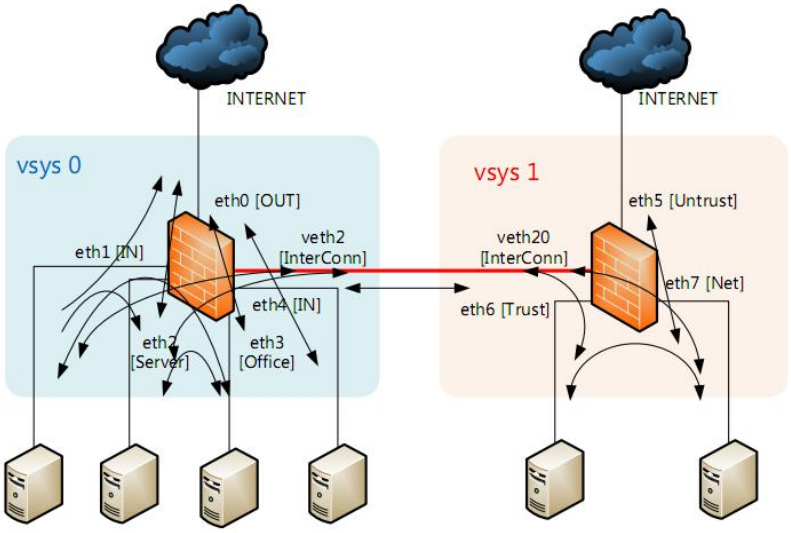
东软集成安全网关（NISG）系列产品实现了对多播相关协议的支持，包括互联网组管理协议 IGMP，DVMRP 等。由于 NISG 设备具有极低的时延，可以保证多播应用的顺畅和实时性。同时 NISG 还可以对多播数据的传送范围加以限制，提升多播应用安全的同时降低不必要的网络资源占用。

3.2.2 业界领先的虚拟 UTM 技术

虚拟防火墙技术是将一台独立的防火墙从逻辑上划分为多个彼此独立的防火墙。东软集成安全网关以虚拟防火墙技术为基础，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。虚拟 UTM 技术可以为各个虚拟系统的用户提供全方位的安全防护。东软集成安全网关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。

东软集成安全网关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，东软集成安全网关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。

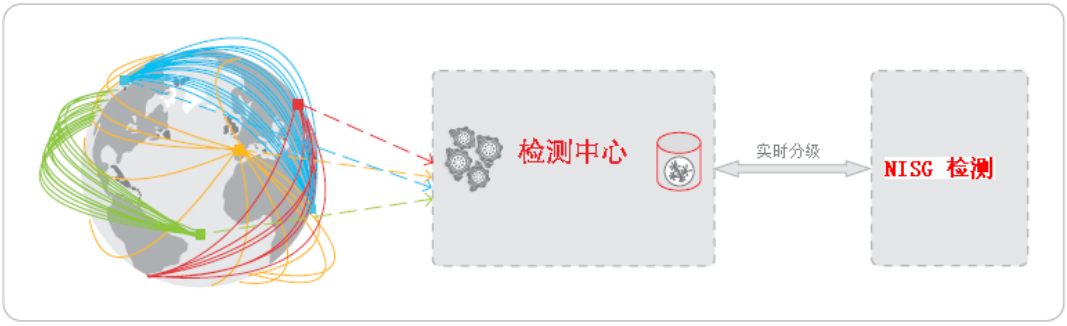


3.2.3 基于 NEL 核心技术的入侵检测

NEL 是东软集成安全网关（NISG）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。

3.2.4 先进的“云安全”技术

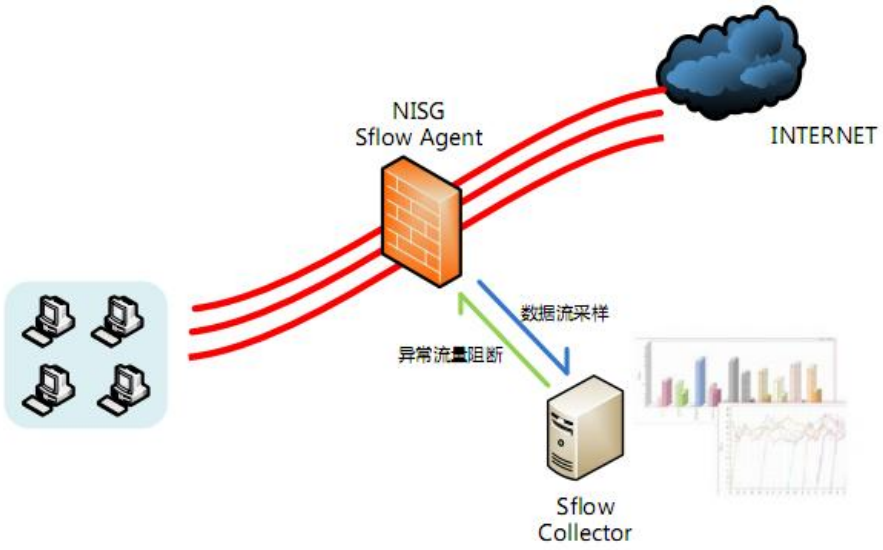
东软集成安全网关（NISG）系列产品采用了世界领先的云安全技术，可以通过互联网的检测中心，快速分析垃圾邮件、恶意 URL、病毒等风险，充分具备零时（Zero-Hour）防御能力。通过云检测技术，NISG 只需对邮件的关键字段进行 hash 运算，并将运算结果送到云中，更多的检测工作在云中实现，从而规避了 NISG 自身因为进行特征检测而导致的性能下降。



3.2.5 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。

东软集成安全网关（NISG）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。

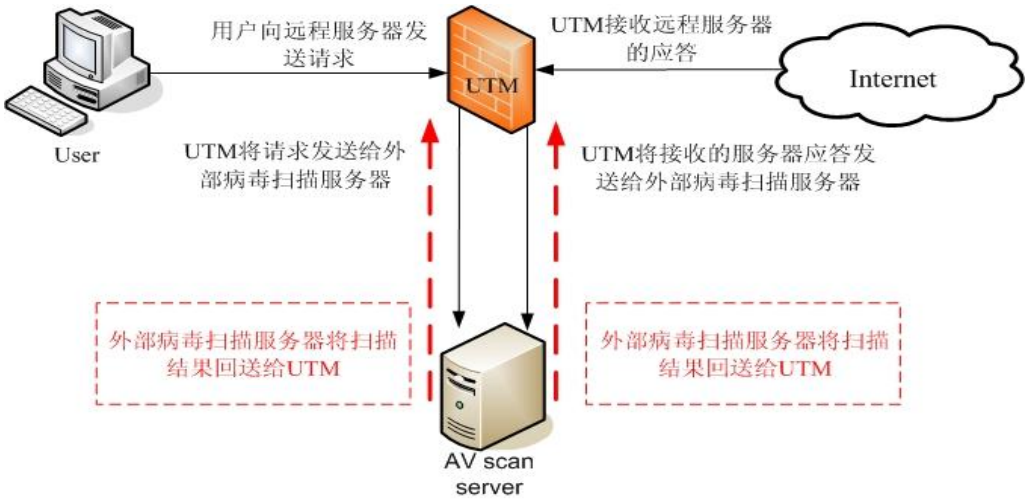


四、 NISG 系列产品主要功能

4.1 ICAP 外部病毒扫描功能

ICAP 技术主要用于东软集成安全网关（NISG）系列产品同分布式病毒服务器集群之的数据通信。NISG 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 NISG 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 NISG 产品只支持对 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。



4.2 强大的反垃圾邮件引擎

NISG 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览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，NISG 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。

4.3 细粒度的协议限制及协议异常检测

东软集成安全网关 NISG 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，NISG 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。东软集成安全网关 NISG 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。

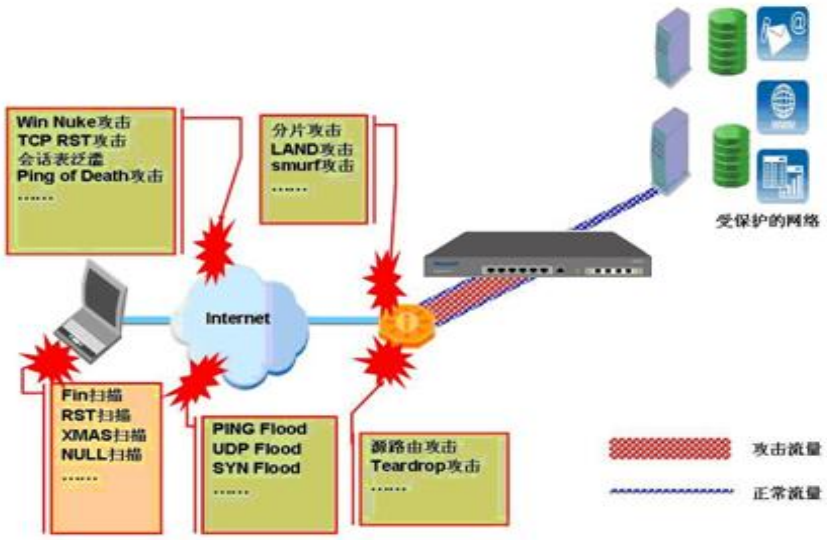
4.4 互联网域名访问加速机制

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。东软集成安全网关（NISG）系列产品提供了互联网域名访问加速机制，在 NISG 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，NISG 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，NISG 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。

4.5 强大的攻击防御能力

东软集成安全网关（NISG）系列产品能够识别和检测众多的网络攻击行为，有效防范对网络和主机的扫描攻击、IP 欺骗攻击、源路由攻击、IP 碎片攻击、以及 SYN-flood、smurf attack、ping of death、teardrop attack、land attack、ping sweep、ping flood、TFN（tribe flood network）等 DOS/DDOS 攻击。



4.6 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?

东软集成安全网关 NISG 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。东软集成安全网关 NISG 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，东软集成安全网关 NISG 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。东软集成安全网关 NISG 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 业务实时联通和最优选择。东软集成安全网关 NISG 产品提供了虚拟专用网级别的高可用性。

4.7 接口冗余

东软集成安全网关 NISG 产品支持接口冗余功能，一个逻辑冗余接口是一个物理接口对。在正常情况下，由主接口负责网络数据的传输，而备用接口是有流量通过。当主接口发生故障，备用接口成为主接口并接管流量，从而保证通信不被中断，从而提供物理层的高可用性保障。

在默认情况下，东软集成安全网关 NISG 产品的冗余接口故障转移取决于主物理接口的物理连接状态，也可以通过配置使冗余接口支持以链路连通性作为条件的故障切换。冗余接

口功能提供了灵活的物理层路径冗余保护的同时，也提升了设备的网络适应能力。

4.8 包过滤规则对域名的支持

目前市场上大部分防火墙的包过滤已经支持了 IP 地址，IP 地址范围以及 IP 地址对象的配置方式。但是在用户实际使用中常常会使用对于固定域名的访问控制，所以东软集成安全网关 NISG 产品增加针对域名的安全控制策略。

包过滤支持域名在适用性方面和 URL 过滤功能是有区别的。URL 过滤属于 UTM 应用层功能特性，用户使用 URL 过滤的目的是针对访问内容的分类限制；包过滤规则属于 3 层访问控制策略，用于针对 IP 地址的访问控制，使用域名的控制方式主要是方便与对可变地址服务器的控制，同时包过滤规则可以支持对指定域名的允许权限控制。

4.9 Unumbered IP

当隧道接口作为一个独立接口参与动态路由交换时，它需要一个 IP 地址作为标识。手工配置隧道接口的 IP 地址，造成 IP 地址资源的无谓消耗。此时 Unnumbered IP 机制允许隧道接口借用其他三层接口的 IP 地址作为自己的地址参与路由交换。这样既完成了隧道接口的路由交换，又节省了 IP 地址资源。

4.10 PPPOE 支持

随着网络普及，PPPOE 成为最为流行的广域网接入方式之一，尤其对于一些中小企业用户和个人，PPPOE 技术以其接入快捷，管理方便等诸多优点被用户广泛接受。一些大型用户也会选择采用 PPPOE 作为备用链路。东软集成安全网关 NISG 产品综合市场需求，在着眼高端全市场的同时需要满足中小企业用户的安全需求，支持了 PPPOE 接入方式，同时支持自动

拨号和按需拨号两种模式。

考虑到物理层的高可用性需求，冗余接口支持 PPPOE 连接，最大限度保证链路通畅。除了物理层的高可用性，东软集成安全网关 NISG 产品的 HA 功能也对 PPPOE 功能进行了支持，HA 除了对 PPPOE 的配置进行同步之外（动态获得的 IP 地址和 DNS），还对拨号成功后的状态信息进行了同步。在发生主备切换时，系统保证 PPPOE 的连接不被中断，最小化意外情况对网络连通性的影响。

4.11 安全集中管理

东软集成安全网关（NISG）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 NISG 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

东软集成安全网关（NISG）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

东软集成安全网关（NISG）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，东软集成安全网关（NISG）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。

4.12 产品可用性与易用度

在增强产品功能的同时，东软集成安全网关 NISG 产品也更为关注用户的使用感受，加大力度提升产品的可用性和易用度。在了解用户对以往产品的意见和建议，充分考虑用户使用习惯后，东软集成安全网关 NISG 产品提供了完善的策略管理，配置向导，系统的备份和恢复和一键式技术支持等可用性易用性优化措施。

东软集成安全网关 NISG 产品支持策略分页显示，避免成百上千条策略混乱地堆叠在一个页面中，解决了用户策略查询速度缓慢，维护和管理比较困难的问题。在此基础上，我们还可以根据名称、安全域、IP 地址和服务等条件的策略查询功能，用户可以在成百上千条规则中快速定位。此外， NISG 产品还提供策略备份与恢复功能。