NetEye Firewall 3.1
VPN 解决方案

沈阳东软软件股份有限公司

目录

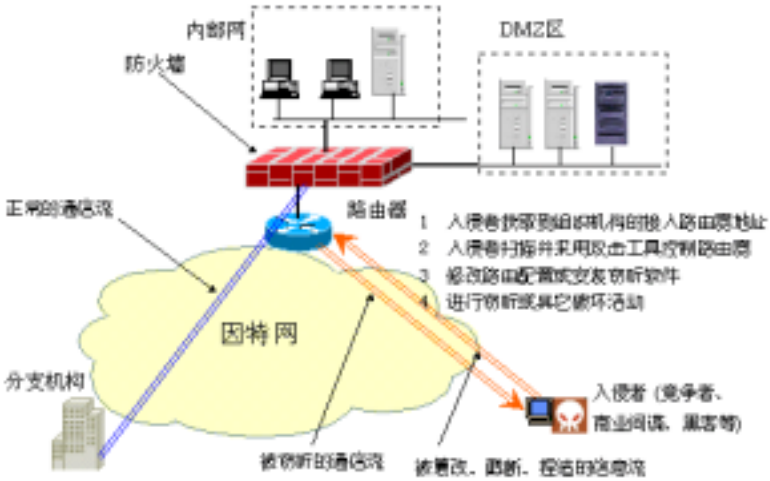
一、来自因特网的信息安全威胁

比尔盖羡在＜＜数字化生存＞＞中预言，信息流将在 21 世纪取代资金流成为各行各业高效运作，抢占市场先机的最关键因素。随着骨干网带宽的扩展和基于因特网的应用软件的日益丰富，未来的商业组织、政府机构的运营模式中，因特网必将成为不可缺少的关键一环。

现在，100M 的光纤接入已经很普遍，即使是家庭用户也可以采用带宽 2M 以上的 ADSL 接入，可以连网打游戏、看电影；商业机构则开始计划合作伙伴的联网，以便实现零库存、零反应时间；异地的分支机构可以随时把最新的客户订货传回总部，而总部则把神经中枢发出的各种指令和信息以光速发到每一个分支机构，即使它远在另一个大洲。而伴随着这一切的，必将是更便利的商业运作：在线销售、在线报关、在线技术交流…… 随之到来的将是满意的客户、满意的利润、满意的股东…… ，等一等，是否忽略了一些东西？

与强大而灵活的网络运营相伴随的就是风险。您是否考虑过此时一个入侵者已经攻入了您的主机系统，窃取了宝贵的客户资料，也可能业务数据已被改得一塌糊涂，也可能机密的决策指示已经被竞争对手非常轻易地得到了……在因特网上，没有人负责保卫您网络和信息的安全。

一个普通的黑客可以轻易地获取企业或组织接入 ISP 的路由器地址，通过路由器的配置错误或是软件漏洞，就可以在路由器上安装窃听软件或把信息路由到其它地方而不被发觉，这样，信息传递过程完全没有任何机密性可言。在一个恶意的商业竞争对手或有组织的商业间谍机构面前，通过因特网传递的财务报表、技术秘密、机密文件将没有任何安全性可言。

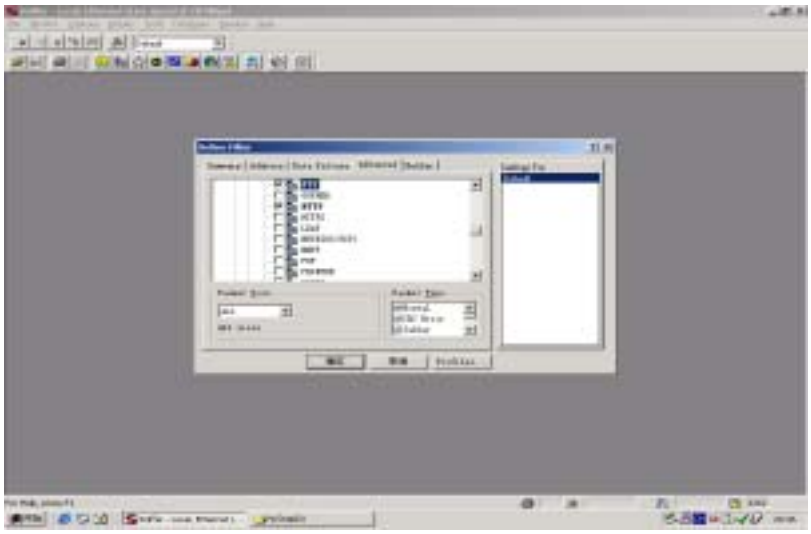


入侵者攻击示意图

尽管 ISS 等安全厂商不断推出扫描路由器安全漏洞和配置错误的产品，而路

由器厂商也不断发布软件补丁，但由于因特网上路由器数目庞大、又是由很多不同的厂商提供，原有的错误配置和漏洞难以被完全消除，新的漏洞不断被发现，所以，不采用任何安全措施就把因特网做为基础通信平台是十分危险的。

更为严重的是，由于 sniffer 等网络攻击工具随手可得，企业机构中的任何一名普通的员工，只要在自己的机器上随便安装一个网络侦听工具，再进行简单的配置，那么他可以查看他所在内部网络中传送的所有数据，包括组织机构内部传送的技术资料、财务报表、战略决策、运营数据等等，这些组织内部的机密信息在他面前没有任何秘密而言。如图二所示，一个网络监听工具功能是十分强大的，它可以截获 Email，FTP 文件、HTTP 页面、网络中传送的登录口令，而使用又是极其简单，不会有任何人察觉。对于竞争对手来说，在一个机构或组织内部安排商业间谍是易如反掌。



设置 sniffer 截取网络数据包

那么，如何才能解决您的网络与信息安全问题？

二、 东软－您可信赖网络信息安全专家

解决网络与信息安全问题，在充分利用互联网确立竞争优势的同时，又不必为潜在的入侵者、窃听者、恶意的黑客烦心，答案只有一个：寻找一个战略性合作伙伴－负责为您解决网络与信息安全方面的问题。他需要有全线安全产品来保证网络和信息安全，以保证您能全速前进；他需要有一支优秀的咨询团队，以便量体裁衣，设计最贴近需求的安全方案；他要有全国分布的、服务及时的支持队伍，以便在紧急情况发生时，在第一时间作用响应，化解危机。只有这样，才可以保证网络和通信的安全性，使您专注于核心业务。

东软，秉承一贯的“ 软件创造客户价值 ”理念，选择了信息安全作为主要的

产品方向，就是把解决客户的网络信息安全作为我们的责任。作为网络安全产品提供商，东软不仅仅是简单地卖产品，而更多地致力于提供一种服务－一种快速的响应能力，以安全咨询顾问的角色来为客户提供整体网络安全方案。

做信息安全，东软具有研发和销售网络的优势，也有资金和规模的优势，公司每年在安全方面有上千万元的投入。东软最新推出的核心产品 NetEye VPN，包含了构建安全的虚拟专用网络所需的功能：

信息加密功能：NetEye VPN 已通过国家密码管理委员会颁发的鉴定证书，产品名称命名为 SJW20 网络密码机。系统的安全性、密码协议、加密算法及保密强度均得到了国家权威机构的认可。在 NetEye VPN 的保护下，客户可以进行安全保密的远程办公、实施基于因特网的 ERP 系统、召开保密的视频会议等等，而无需再担心是否会有人正在窃听或破坏。

防火墙功能：NetEye VPN 集成了 NetEye 防火墙 3.0 的全部功能，并增加了对多播的支持。这样，它可以保护企业组织的内部网络，阻止 DoS 攻击、过滤恶意的 WWW 页面和邮件，甚至可以用来实现 VLAN。

身份认证功能：NetEye VPN 提供认证客户端软件，支持 RADIUS 协议及 RSA SecureID 产品，使客户可以构建强大的身份认证和授权管理系统。

东软不能够提供客户需要的所有网络与信息安全产品，为此，东软与 CA、冠群金辰等著名网络安全厂商进行强强联合，把他们最优秀的产品作为整体方案中的一部分，为客户构造一个全面而完整的网络安全解决方案。

三、 VPN－网络与信息安全的核心

在开放的因特网环境中，要保证公司、组织或机构业务的稳定高效运行，就必须应用提供强大的安全服务，来保证对资源的受控访问、信息的机密性及业务的可靠性。这些服务包括信息加密、身份认证、访问授权与控制，以及为上层协议及应用提供透明的数据机密性与数据完整性服务的 IPSec 协议。

密码技术：保证信息的保密和不可篡改

确保信息在发送和接收过程中的保密性和完整性，可以通过使用密码技术很容易实现。密码技术密码编码学和密码分析学。在实际中得到大量应用的是密码编码技术。它又可分为对称加密、公钥加密、认证（杂凑）函数设计等不同的分支。我们通常所说的加密指的是对称加密。

通常的情况是，信用卡号码、用户的个人信息、商业秘密、以及保密文件都

被静静地、毫无保护地置于网络设备上。保护这些信息的最为简单的方法就是采用加密技术。加密可以把信息"搞乱"，一旦网络上的某些人访问这些信息，加密技术将使得它们不可读。

网络传输过程中的信息保密技术，还涉及密钥协商技术。密码协商是指在通信双方协商起只为双方所知的密钥，加密传输的信息。这种技术可以确保在公共网络中流动的信息的安全性。截获的加密信息对窃听者来说莫名其妙，无法理解。

密码技术的另一个重要方面是保证数据的完整性。不管数据是处于静止状态还是传输状态，数据的完整性，即不可篡改性，对任何商业交易来说都至关重要。认证技术（杂凑函数，又称散列函数、哈希函数）有保证数据完整性的能力，从而，可以探知信息是否已经遭到损害或篡改，即使传输的文件前后只差一个空格。

身份认证与授权：保证实体身份的可鉴别性与资源的受控访问

虚拟专用网络安全的另一块重要基石，就是身份认证及授权技术。在用户对重要数据资产和资源进行访问之前，必须对其身份进行认证和核实，并检查其权限。实际上，企业或组织的虚拟专用网络每天都会被满腹牢骚的前公司员工、寻求刺激的少年、或深具竞争性的商业间谍们进行袭击。传统的口令认证可以被专门的口令破译工具在几分钟或几小时之内破译。网络监听工具则可以完完全全地将网络中传输的口令或密码截获下来。所以，尽管口令已经得到了最为广泛的使用，但口令本身却是最为脆弱的身份认证方式。因此，要想虚拟专用网络的安全，必须采用更安全的认证方式－双因素身份认证。

双因素身份认证使得用户在对受保护的网络资源进行访问前，必须以两种形式出示身份。与银行的自动取款机（ATM）一样，采用这种方法，用户必须知道自己的 PIN 码，并拥有自己的身份认证装置（令牌）。两种身份的组合，将证明访问者与其真实身份相符。采用这种方式，信息、数据将会象存储在银行的数十亿的资金一样，处于严密的保护之下。

IPSec 安全协议

现在，不同的密码技术及产品使得整个企业 IT 应用及资源的管理更加复杂：发送邮件要用邮件加密工具；而保护 Web 站点需要 SSL 或 SHTTP；进行安全地 TCP／IP 连接需要使用 SSH；或许还远不止这些。但是，能否有一个简单的安全方案来为尽可能多的应用提供足够强的信息安全保护？答案是有。这就是目前已被广泛应用的 IPSec 技术。它可为网络通信提供了 IP 级的安全，包括了分层身

份认证、访问控制、加密、信息完整性、以及重放保护等安全服务。IPSec 对发送到 IP 层、或从 IP 层接收到的 IP 信息包进行分析，允许那些符合安全策略的数据顺利通过，而不符合安全策略的数据包，将被全部丢弃掉。

IPSec 使得信息安全策略被应用在信息发送者与接收者（二者都不需要了解 IPSec）的一个或多个网络段中，从而使得信息安全服务对通讯终点透明。它既可以实现网络－网络的通信安全，也可以实现主机－主机的通信安全。

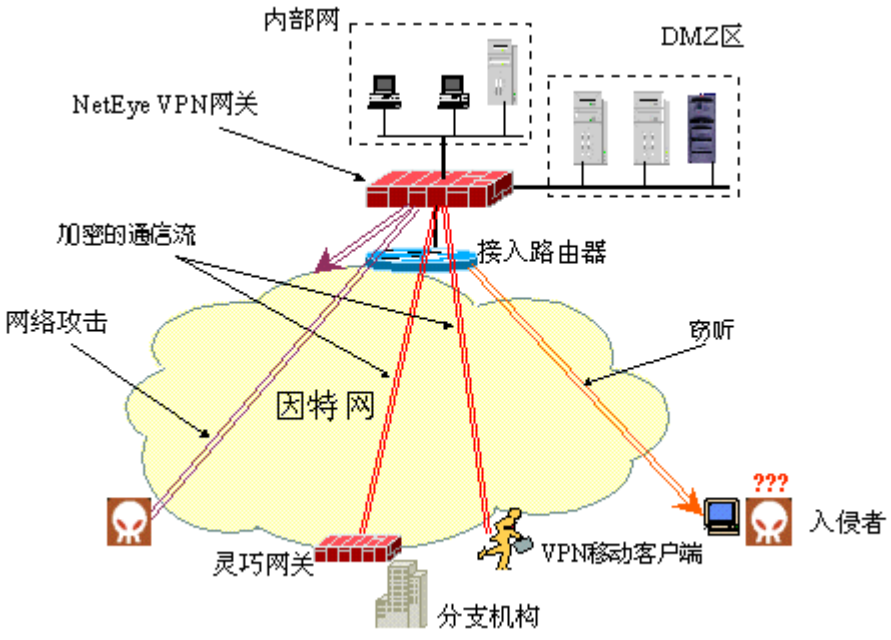
东软股份推出的 NetEye VPN 解决方案包括了前面所述的所有技术特性：

采用我国自主研制的加密认证算法及加密卡保证信息的机密性和完整性；

支持 RADIUS 协议，客户可以方便地在 VPN 系统中集成 RSA SecureID 或其它任何第三方的双因素认证产品。

完全按照最新的 IPSec 协议实现，支持多种接入方式，包括 ADSL、ISDN、拨号接入、DDN；基于 PKI／KMC 的密钥管理方式使得系统的密钥管理简便易行。

四、 NetEye VPN 网络与信息安全解决方案

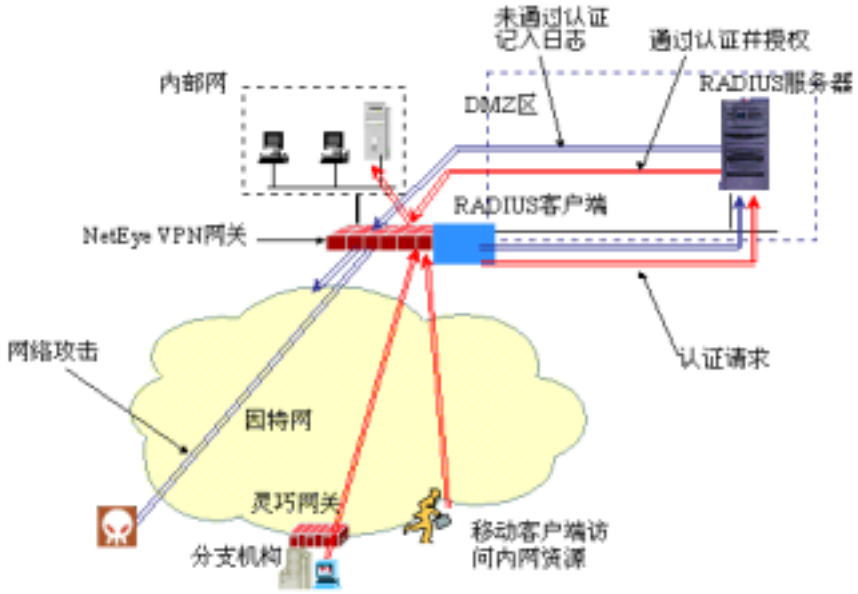


NetEye VPN 应用示意之一－网络保护与信息传输加密

NetEye VPN 由中心网关、灵巧网关和 VPN 移动客户端组成。中心网关与灵巧网关、VPN 移动客户端之间可以建立高强度的加密隧道，这样，信息是以加密的形式在公网上传输的，而且附加了认证信息，防止信息被篡改或被伪造，第三方即使截获或窃听到加密的数据，也只是一堆毫无意义的字符，无法了解信息的真实意义。而由于 NetEye VPN 具有强大的防火墙功能，它会把 Ping-of-Death、

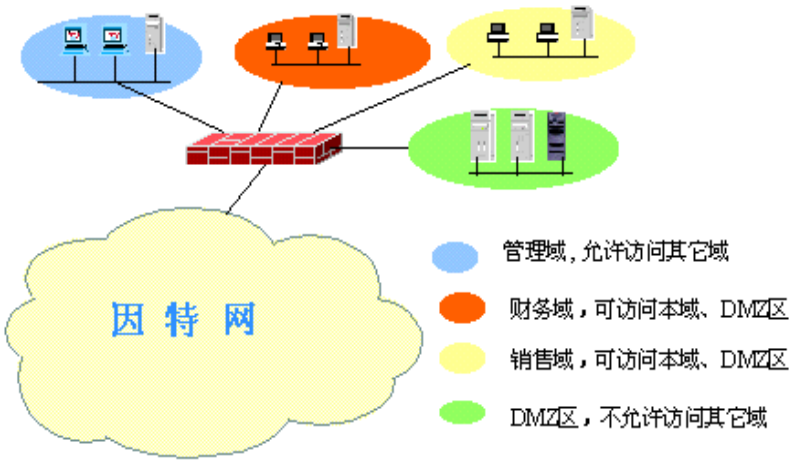
Ping-Flooding、UDP-Flooding、SYN-Flooding 等 DoS 攻击拒之门外。

为了最大限度地保证您的网络安全，所有远程用户在访问内部网络之前，必须向 VPN 网关证明自己的身份，由网关通过 RADIUS 代理将认证请求转发给 RADIUS 认证服务器，由 RADIUS 服务器认证用户身份并查看用户的授权信息。如果身份得到确认而且允许用户访问其所请求的资源，那么用户顺利联入内网并访问相应的资源。而一个无法证实自己身份的访问者或者与授权信息不符的访问将会被 VPN 网关丢弃掉，并将访问的详细信息，如用户 ID、IP 地址、访问的服务和目标等等记入审计日志，以便随后进行分析和追查。如下图所示。



身份鉴别、授权审核过程与访问的审计

NetEye VPN 支持 SVN（安全虚拟网络），即在公网上构建了一个 VPN 网络之后，进一步通过安全策略和安全规则的制定，把网络划分成不同的安全区域，控制不同的安全区域之间的访问，这样，使网络的安全性得到进一步的提升，并一定程度上防止内部人员的误操作和恶意行为。以上图为例，通过制定安全策略，可以控制管理域、财务域的信息只在本域内传播，而不会传输到其它域中去，从而在一定程度上减少了内部窃听的风险和不安全因素。



利用 VPN 网关实现安全域的区隔

五、 NetEye VPN 解决方案的技术优势

NetEye VPN 可以保护组织内部网络安全、信息传输安全、实现安全便捷的身份认证、移动与远程办公等等，为客户提供全面、稳定、有着良好扩展性的网络安全整体解决方案，成为您 IT 运营系统中的关键组成部分和基础安全通信平台。NetEye VPN 主要的技术优势包括：

强大的网络与信息安全保护功能，透明接入现有网络。

支持多种接入方式，上层应用不需做任何修改。

灵巧网关为客户提供经济实用的组网方案。

严密的、基于 PKI／KMC 架构的密钥管理框架

清晰简洁的密钥管理流程，直观明了的加密隧道设置与管理。

完善的自保护机制，高性能的流过滤防火墙模块。

5.1 强大的网络与信息安全保护功能

高加密强度的 VPN 功能

NetEye VPN 采用国际标准安全协议-IPSec(IP Security)安全协议，对用户数据提供加密、完整性验证,并与身份认证系统一起，为信息传输提供安全保护。密钥协商协议采用 IKE 密钥协商和管理协议及基于 PKI 的密钥管理框架，参照 X.509 数字证书标准，实现安全可靠的密钥分发与管理。

VPN 网关采用的加密器件为国密办批准使用的高速硬件加密卡，对称加密算法及杂凑算法的密钥长度均为 128 位：采用 1024 位 RSA 公钥算法的数字签名进行 VPN 网关间的身份认证。算法具有极高的安全强度。以 128 位的对称加密算法为例，如果采用穷举攻击，即使是每秒运算一万亿次的超级计算机也要计算三百亿亿年！

透明支持各种应用服务

NetEye VPN 在 IP 层对数据包进行安全处理，在为上层协议如 HTTP、FTP、SMTP 等提供安全保护的同时，上层应用不受任何影响，对上层协议完全透明。并可透明接入用户现有网络.

强大的防火墙功能

NetEye VPN 可防范 Ping-of-Death、Ping-Flooding 等多种 DOS 攻击，提供对攻击活动的识别和告警；支持双向隐藏的 NAT 功能；提供 IP 与 MAC 地址绑定功能；提供认证客户端软件，用户身份认证过程对应用和协议透明支持；支持通过第三方 RADIUS 服务器实现一次性口令认证。

透明的应用代理级功能

NetEye VPN 可以提供 HTTP 过滤，阻断小程序(Java Applet 和 ActiveX)及指定的 URL，提供 WWW 页面内容过滤，并可对 HTTP 和 FTP 操作进行命令级控制。提供 SMTP 过滤功能：如主题过滤、正文过滤等等。

5.2 支持多种接入方式提供广泛的适用性

随着宽带技术的发展，接入方式日益多样化。为了最大限度地适应用户的网络环境，NetEye VPN 灵巧网关支持 ADSL、ISDN、DDN、拨号接入等多种接入方式；NetEye VPN 网关也支持 DDN 接入和 100M／1000M 光纤接入。在某些情况下，可以使用 VPN 网关直接接入 ISP，不再需要布署接入路由器，从而了节省了用户 VPN 网络的建设成本，最大程度上保证方案的经济性及实用性。

5.3 全面的产品线保证组网方案的经济性与灵活性

NetEye VPN 包括中心网关、灵巧网关和 VPN 移动客户端三个组件，提供了全面的产品线为用户构造完整的 VPN 解决方案。部署经济、操作简单而便捷的灵巧网关是 NetEye VPN 系统的一大特色。

灵巧网关定位于小型分支机构一级，安全策略固化为允许对外访问而禁止外部对内的访问，同时保留了建立安全隧道和数据加密等 VPN 核心功能。灵巧网关支持 ADSL、ISDN、拨号接入等多种接入方式，当分支机构网络规模较小，只需实现与总部的网络互联而无需对外提供服务时，选择灵巧网关，可以大大降低整体 VPN 方案的成本。

5.4 严密的、基于 PKI／KMC 架构的密钥管理方案

NetEye VPN 采用基于 PKI／KMC 架构的密钥管理方案，整体密钥管理方案

设计与实现的安全性经国家密码管理委员会的专家审定。密钥管理中心是离线的，使密钥管理系统免受外部攻击的威胁，而且管理员在密钥管理中心所作的操作均有详细的审计记录，进一步强化了密钥管理系统的安全特性。

5.5 清晰简洁的密钥管理流程

NetEye VPN 采用基于 PKI／KMC 架构的密钥管理方案带来的优势之一就是密钥管理流程十分清晰和简洁。配置 VPN 系统使用的密钥分为三个步骤：

1 配置密钥管理中心。为其生成和配置密钥 IC 卡和管理员身份 IC 卡。

2 使用密钥管理中心生成 VPN 网关使用的密钥 IC 卡及全局公钥文件，并分发到网关管理员手中。

3 配置 VPN 网关使用的密钥 IC 卡和全局公钥文件。全局公钥文件使用管理中心的私钥签名，可以防止在传送过程中被替换或篡改。

至此，即完成了 VPN 系统全部的密钥配置工作，以后只要在界面上设置网关间的加密隧道及其参数，VPN 网关间就可以自动地进行密钥协商，并用协商好的密钥对数据进行加密。密钥的更新也是由 VPN 网关自动完成的。

5.6 直观明了的加密隧道设置与管理

NetEye VPN 的加密隧道设置极为简单，如下图所示，只要设定对端 VPN 网关的 IP 地址及密钥交换协议使用的端口，同时对端 VPN 网关也进行对称的设置，即可完成加密隧道的配置。应用工程后，VPN 网关自动进行密钥协商并建立加密隧道。

基于图形界面的加密隧道设置

NetEye VPN 其它的主要功能特性包括

- 支持双向隐藏的 NAT 功能
- 防范 Ping-of-Death、Ping-Flooding、UDP-Flooding、SYN-Flooding、KillWin、WinNuke、LAND、IGMP2、IP 碎片等多种 DOS 攻击
- 提供认证客户端软件，用户身份认证过程对应用和协议透明
- 支持通过第三方 RADIUS 服务器实现一次性口令认证
- 提供 IP 与 MAC 地址梆定
- 支持 VLAN Trunk 协议（ISL、IEEE 802.1Q）
- 支持多播
- 支持基于 IP、用户的流量周期管理
- 提供了完备的审计功能。审计数据可以保存在本地或网络数据库中
- 提供网络工作情况的实时监控和图表显示
- 支持 SNMP，可以使用 HP Openview、Cisco works 等对防火墙进行监控
- 提供对攻击活动的识别和告警