NEUSOFT 东软

软 件 创 造 客 户 价 值

SJW20网络密码机系统

NetEve VPN

技 术 白 皮 书

沈 阳 东 软 软 件 股 份 有 限 公 司

1、网络安全与 VPN 技术

Internet自出现以来，就以迅雷不及掩耳之势改变着人们的生活、学习和工作方式，同时Internet的发展也给企业带来了革命性的变革和开放，企业正努力通过它来提高市场反应速度和管理效率，以更具竞争力。但由于Internet自身的一些特点，也带来了一系列安全问题。例如在无保护的公共网络上传输的数据对于许多种形式的攻击都无法防范。数据在途经某一路由器时，可以被任何访问此路由器的人读取、改写或伪造。协议分析器可以读包并且获得秘密信息。黑客可以利用各种工具篡改数据报，并且通过干扰、消减或阻止网络通信来进行破坏活动。

所以当前企业在充分利用 Internet 这一先进的生产工具的同时，如何有效地保护其网络和网络应用系统的安全，也是关系到企业生存和发展的重要课题。就目前而言，保护企业网络和网络应用系统的安全技术主要包括四个部分，它们是：

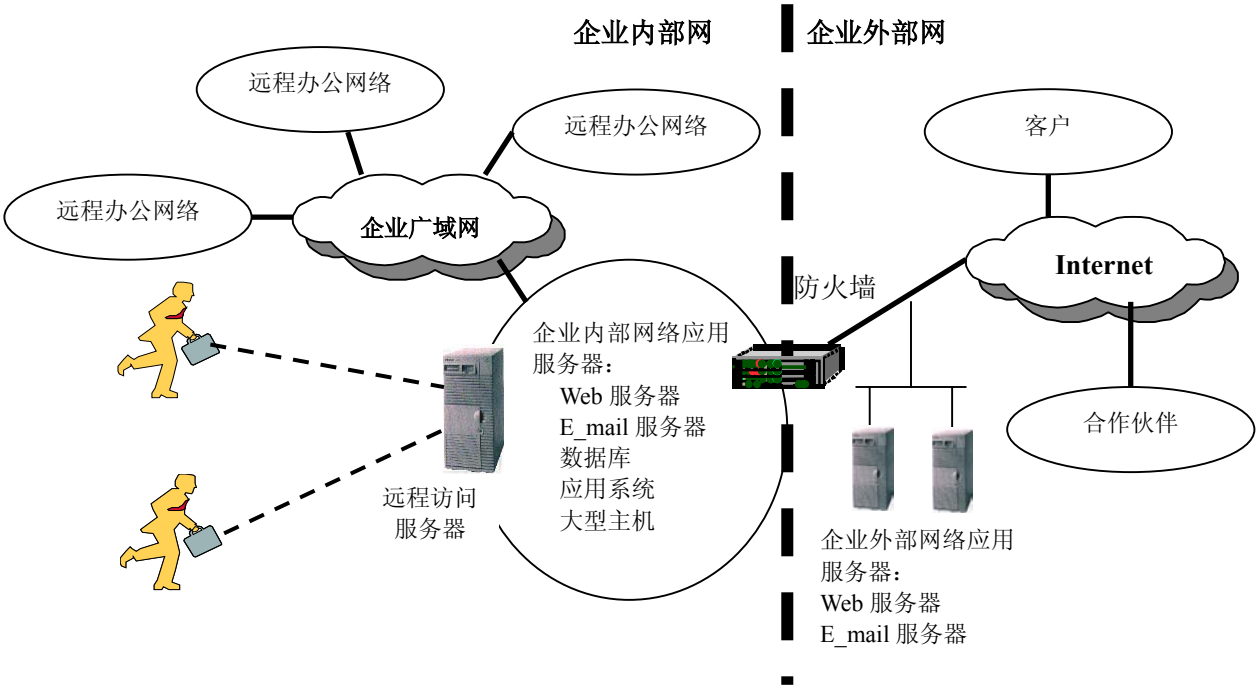
- 防火墙技术：　　企业网络的边界防御体系
- VPN 技术：　　企业电子商务的安全通信平台
- 网络实时监控/报警技术：　　实时防范网络攻击
- 审计/日志技术：　　分析安全隐患、查证攻击来源

虚拟专用网络(Virtual Private Network, VPN)是 Internet 技术迅速发展的产物，它最简单的定义就是“在公众数据网络上建立属于自己的私有数据网络”。也就是说不再使用长途专线建立私有通信网络，而是将其建立在拥有完善架构的公众数据网络上。它的基本点就是“化公为私”，使每个企业可以临时从公用网中获得一部分资源供自己专用。既可以连到公网所能达到的任何地点，而且保密性、安全性、可管理性的问题也容易解决，还可以降低网络的使用成本。

虚拟专用网络实现的基础是身份认证、数据加密与密钥交换协议。使用 VPN 产品，企业可以利用 Internet 建立一个安全统一的虚拟内部网络，该网络不受地域限制，企业合法用户在任何地点通过 VPN 透明地访问企业内部服务器。同时，VPN 系统可有效地防止外部非法或未被授权用户对内部网络的访问，并利用加密技术充

分保证敏感信息在公网上传输的安全性，从而达到保护企业与个人利益的目的。

2、当前企业网络结构

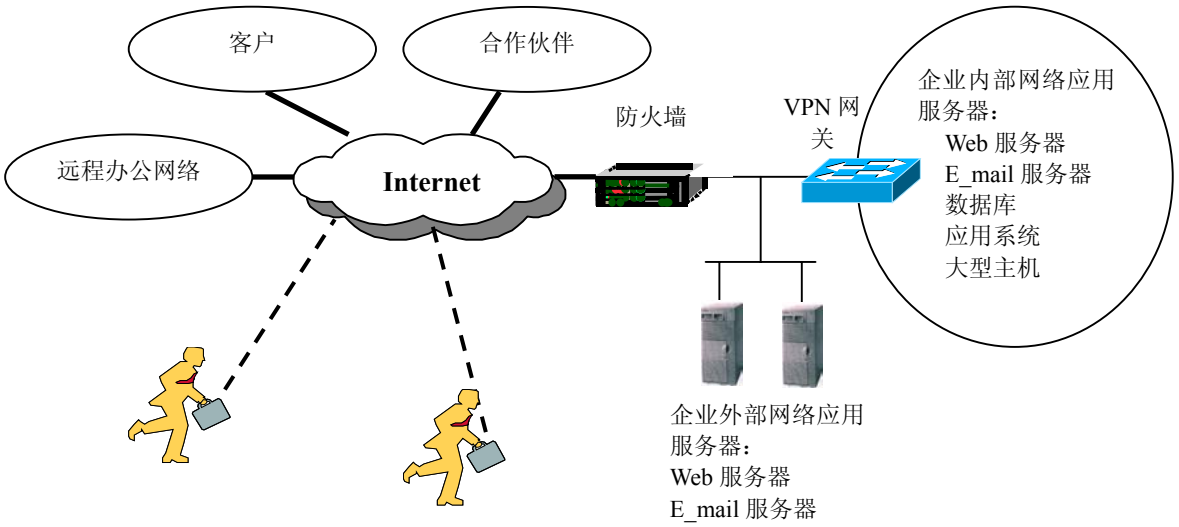


当前，大多数企业内联网是一个封闭的系统，企业内部网与 Internet 之间使用防火墙隔离。企业的各个远程办公网络之间采用专线连接，移动用户访问企业内部网络必须采用远程拔号方式连接。为了保证内部网的安全，企业不允许客户与合作伙伴通过 Internet 访问其内部网，而只允许他们访问企业设在防火墙外的应用服务器。这种网络的缺点是：

- 企业内部网络运营成本高，主要表现在租用专线的成本昂贵；远程拔号的通讯费用昂贵；网络复杂，管理费用昂贵。
- 移动用户使用不便，通讯质量不易得到保证。
- 企业合作伙伴和客户无法访问企业内部网，企业无法建立基于 Extranet 的电子商务平台。

3、企业 VPN 网络结构

随着 VPN 技术的发展，VPN 产品已被越来越多的企业所接受，并成为新型企业内部网结构的重要组成部分，企业使用 VPN 来保护敏感的服务器系统，任何经过企业授权的用户，包括远程办公用户、移动用户、客户、合作伙伴，均可利用 VPN 技术方便和安全地通过 Internet 访问企业内部网，形成一个建立在 Internet 上的企业虚拟网络。采用 VPN 技术，可有效地降低企业投资在网络建设 、网络管理以及网络运行等方面的成本，同时为企业构建新的电子商务模式提供必要的安全网络平台。



4、SJW20 网络密码机系统概要

SJW20 网络密码机是采用标准的 IPSec 协议设计的高安全性、高可靠性的 VPN 产品。它在 IP 层实现了数据加密、数据完整性认证、访问控制以及审计等安全机制，它结合网络访问控制技术，抵抗各种外来攻击。SJW20 网络密码机系统可有效保护信息的传输安全并防范对企业内部网的非法访问和攻击，如侦听破译、篡改报文、重发或少发报文、冒名顶替、非法访问、旁路攻击等等。

SJW20 网络密码机采用国密办批准使用的硬件加密和认证（哈希）算法；同时还可以根据国家密码管理政策和用户需求添加新的算法。新算法的添加对管理员和用户是完全透明的。遵循 ISAKMP/OAKLEY 密钥协商和管理协议，采用公钥认证

方式，因而密钥管理和分配安全性高，配置简便。

SJW20 网络密码机的构成包括 SJW20 网络密码机、移动客户端和网络密码机管理中心等三部分组成。

- SJW20 网络密码机是运行在安全操作系统平台上的 VPN 系统，运行在专门的硬件平台之上。它包含 NetEye 防火墙的核心结构和功能，具有动态包过滤和防 DoS 攻击能力；同时各个网络密码机之间可以通过公钥认证方式建立安全隧道，对通过隧道的数据包实行数据加密和封装；
- SJW20 网络密码机移动客户端是运行在 Windows 操作系统下的应用程序，每个移动用户都具有一个专用的电子证书，通过该电子证书与网络密码机建立安全隧道，从而使移动用户通过 Internet 就可以安全地访问企业内部网服务器；
- SJW20 网络密码机管理中心是该系统的管理软件包，通过它可以集中管理企业的所有网络密码机，配置其上的安全策略，维护各网络密码机之间的安全隧道；并有管理企业移动用户，分配移动用户对内部网络访问权限等功能。

5、SJW20 网络密码机系统功能概要

5.1 保证信息传输的高度机密性和不可篡改性

SJW20 网络密码机之间及网络密码机与移动客户端之间建立的安全隧道具有以下安全指标：

加密算法：国密办批准使用的对称加密算法；

认证方式：1024bits RSA 数字签名认证方式；

认证（哈希）算法：国密办批准使用的认证算法；

密钥管理协议：采用 IKE、Diffie-Hellman 等协议；

支持的协议：TCP/IP、IPSec、ESP/AH；

安全标准：IPSec、IKE-XAUTH、RSA、PKCS7/10/12；

5.2 状态包过滤

SJW20 网络密码机实现了对 TCP 连接、UDP 会话状态的监控。它采用状

态包过滤技术，监视每一个有效连接的状态，通过跟踪网络连接状态并根据状态信息动态进行包过滤。不仅对通过网络密码机的信息包进行过滤，同时能够依据数据包之间的状态信息进行更加全面的过滤；而且在对包的网络层信息进行过滤的同时，更强调对应用层信息的过滤和对服务器的保护技术，因此大大提高了包过滤系统的性能和安全性。在状态包过滤里，信息包在网络层就被截取了，然后网络密码机从接收到的数据包中提取与安全策略相关的状态信息，来决定这个数据包操作：直接通过、VPN 封装还是丢弃等。因此它的处理效率高、应用范围广。

5.3 双向 NAT

SJW20 网络密码机支持在内部网使用保留的 IP 地址，通过地址转换功能实现对外部网的访问。它支持两种 NAT 转换方式：即一对一的地址转换和多对单或多对多的地址转换，这样内部主机 IP 地址就可以通过 NAT 转换成外部有效 IP 地址，并且外部主机能够通过访问内部主机经 NAT 转换后得到的有效 IP 地址来访问内部主机提供的服务。另一种是更灵活的方式，可以支持针对服务端口的一对多映射，即内部的多个机器可以通过一个外部有效地址访问外部网络，同时内部的多台机器可以分别映射到该地址的若干个端口，通过这些端口对外部提供服务，比如 202.118.6.100 是一个外部有效地址，内部的“192.168.1.*”网段的机器通过该地址访问外部网络，同时，该地址的 80 端口对应于内部的 IP 地址为 192.168.1.50 的机器，外部网络对 202.118.6.100:80 的访问都构成了对 192.168.1.50:80 的访问，而 202.118.6.100:25 端口对应于内部的邮件服务器 192.168.1.60，对外提供邮件服务。这种 NAT 转换可以更有效地利用 IP 地址资源，对外隐藏网络拓扑结构，提供更好的安全性。

5.4 审计功能

SJW20 网络密码机的审计包括两个部分：事件审计和流量审计。事件审计负责记录网络密码机上曾经发生过的事件；流量审计负责审计经过网络密码机的网络数据包并记录审计信息。

5.5 网络实时监控功能

网络实时监控的主要功能是对网络当前连接的监视和控制，强调实时性、可

视性和可控性。具有连接状态实时显示、流量显示、中断网络中正在活动的非法的连接、网络负荷分析、网络密码机的资源占用率分析等功能。

5.6 图形化的网络密码机远程配置管理

在企业的运营网络中，网络密码机往往分布在相距遥远的远程办公网络中，管理员往往需要对数十台网络密码机进行配置并保证相互之间安全策略的一致性，这种情况下采用分散管理是不可想象的。SJW20网络密码机提供了对网络密码机的图形化集中管理方式，通过一个直观的界面，就可以完成对所有网络密码机的配置和管理工作。这样系统管理员在一个地方就可以完成所有管理工作。通过这一功能有效提高了管理的方便性、统一性和灵活性。

VPN管理器与网络密码机之间的信息在一个独立的网络通道中传输，为了保证控制信息的安全性，所有信息均进行了高强度的数据加密。对称加密算法的密钥长度为128位。

5.7 SJW20 网络密码机移动客户端

随着企业远程移动用户的增多，远程访问企业内部网变得越来越重要。通过 VPN 的移动客户端软件可以通过 Internet 实现安全的对企业内部网络的拨号访问。如果某个移动用户希望访问企业内部网的资源，则通过拨号到本地 ISP 的拨号服务器，登录到 Internet 上，与布置在企业内部的网络密码机建立一条安全通道。此时的远程用户终端设备上必须加装相应的 VPN 软件。

SJW20网络密码机移动客户端是一种虚拟拨号方式，与通常的拨号方式不同，远程用户使用从内部网络密码机获得的企业内部地址而不是从ISP的拨号服务器获得的一个临时的公共IP地址来与企业内部网通信。由于使用内部地址，企业内部网中的防火墙可以对远程用户进行更严格的身份认证和访问控制，使得身在远处的员工也能如同在公司总部的办公室一样自由访问公司的资源。

SJW20网络密码机移动客户端软件运行在Windows操作系统上，它不仅可以节省员工长途拨号的费用及企业设备投资费用，而且还能保证数据传输的安全性。

5.8 高性能数据处理

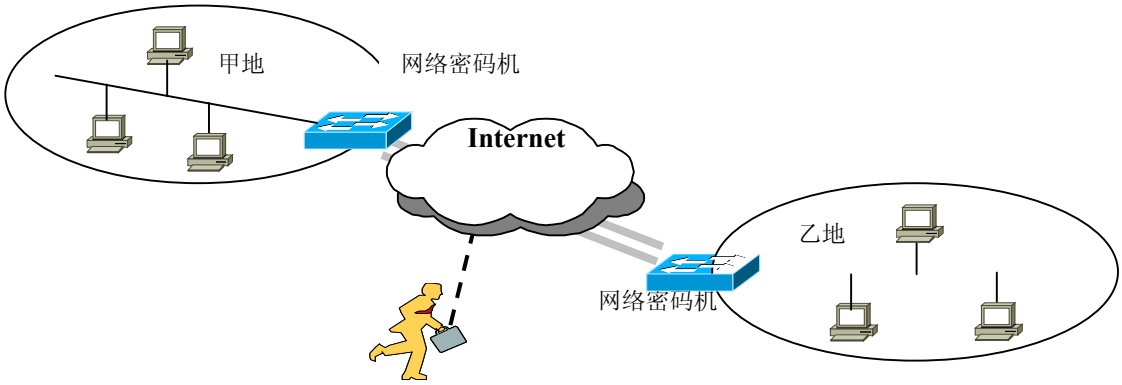
SJW20 网络密码机采用分布式处理技术，根据用户的要求可以提供

24Mbps~88Mbps 的高加密强度的数据处理能力。

6、SJW20 网络密码机系统的应用方案

6.1 企业和政府 VPN 应用方案

由于 SJW20 网络密码机包含了防火墙的基本功能和 VPN 的所有功能，企业和政府只需在其内部网络与公共网络的连接处安装一台 SJW20 网络密码机，即可起到边界防御和建立 VPN 安全通道的双重功能，使用 SJW20 网络密码机组建 VPN 网络，企业和政府无需改变现有的网络结构和网络应用，从而有效地保护了企业在系统建设方面的已有投资。



6.2 ISP/ICP VPN 应用方案

VPN 技术对网络服务运营商而言带来了巨大商机，主要体现在：

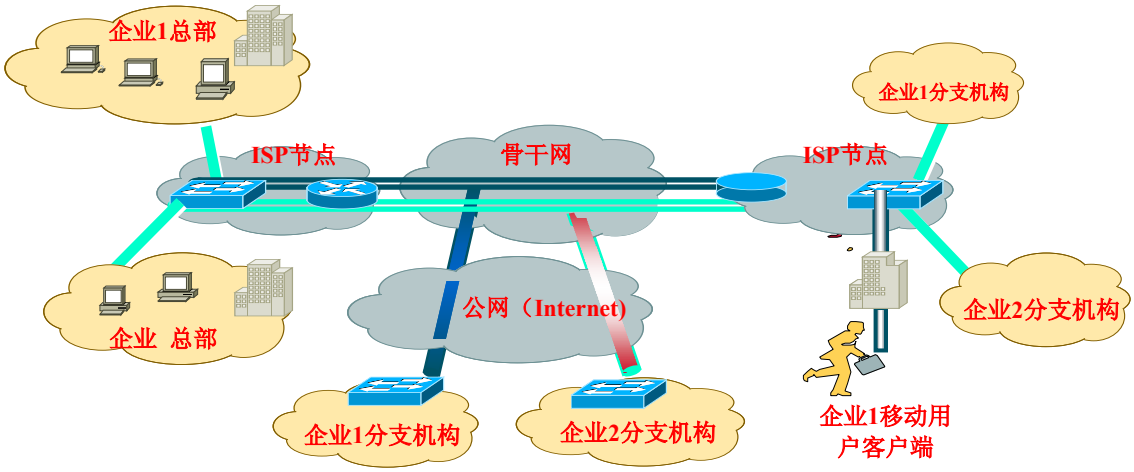
1、通过提供各种增值服务，给事业的发展带来机遇，扩大客户基数和服务地域，提高资产回报率。

2、可通过互联网或其 IP 骨干网为企业提供远程访问和分支机构连接服务； -增加运营的收入现金流；

3、为客户提供高度细化的增值服务；4、同大企业客户建立起长期的合作关系；

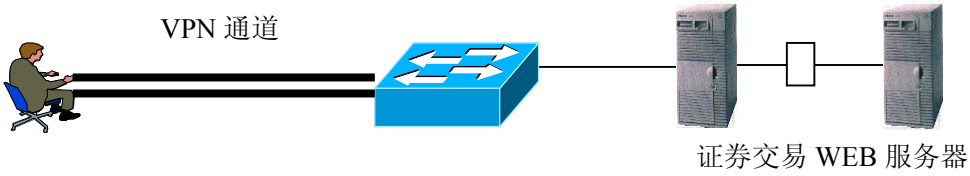
5、同其他的 ISP 合作，通过虚拟的服务提供点(Virtual Point of Presence)扩展业务覆盖范围；

6、充分利用现有的网络设施，以很少的投资快速布署新的服务，提高网络利用率，提高边际利润率并缩短投资回收期



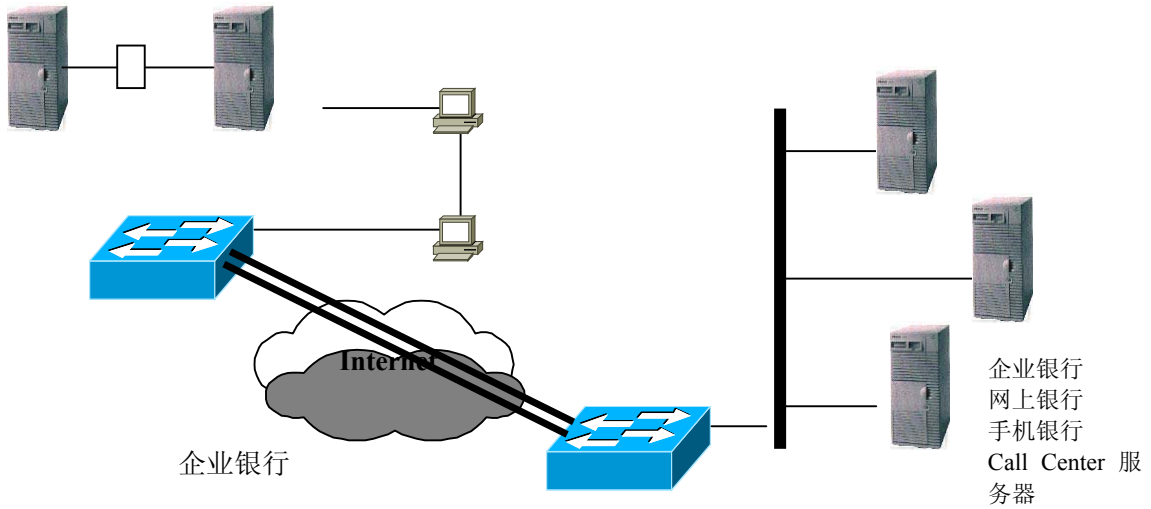
6.3 证券行业 VPN 应用方案

证券行业对信息安全有着较高的要求，需要对营业部和证券公司总部的信息网络系统进行保护，同时对于网上交易的网站需要防御外来的攻击和蓄意的破坏，各营业部与总部、营业部与营业部之间信息的传输需通过 VPN 保障信息传输的安全。



6.4 网上银行 VPN 应用方案

网上银行可帮助金融系统利用互联网技术，开拓新业务，更好地服务客户和贴近用户，SJW20 网络密码机可确保网上交易和信息传输的安全。



7、SJW20 网络密码机系统安全特性及性能指标

7.1 安全特性

- ✓ 对称加密算法：国家密码管理委员会批准使用的对称加密算法；公钥算法：高速硬件实现的 RSA 算法认证方式：1024bits RSA 数字签名认证；
- ✓ 认证算法：国家密码管理委员会批准使用的认证算法；；密钥管理协议：采用 IKE、Diffie-Hellman 等协议；支持的协议：TCP/IP、IPSec、ESP/AH；
- ✓ 遵循的安全标准：IPSec、IKE-XAUTH、RSA、PKCS7/10/12；

7.2 SJW20 网络密码机性能指标

- ✓ 每个网络密码机可支持 2000 对 VPN 通道；
- ✓ 网络加密速度：12Mbps~88Mbps 范围内可选择；
- ✓ 支持最大连接数：120，000 个
- ✓ 支持的访问控制规则记录数：24000 条

沈 阳 东 软 软 件 股 份 有 限 公 司
地址：沈阳浑南高新技术产业开发区·东大软件园
传真：024-23784036　邮编：110179
网址：www.neusoft.com