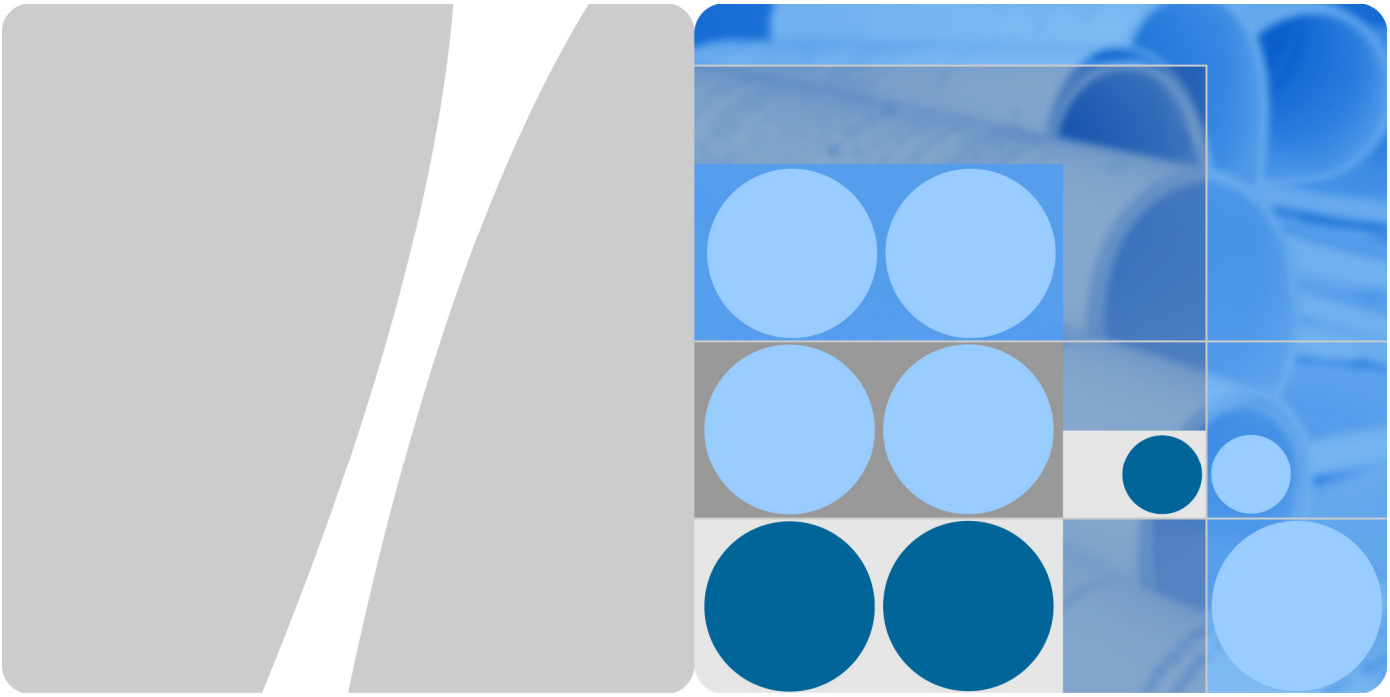


华为 SVN2000 & 5000 安全接入网关 产品概述

文档版本 01

发布日期 2012-07-12

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

1 前言

读者对象

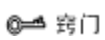
本文档介绍了 SVN2000/SVN5000 系列产品的定位、特点、软硬件结构、典型组网应用、操作和维护、遵循标准和技术指标。

本文档主要适用于以下工程师：

- 网络规划工程师
- 数据配置工程师
- 现场维护工程师
- 网管管理员

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
	表示能帮助您解决某个问题或节省您的时间。
	表示是正文的附加信息，是对正文的强调和补充。

通用格式约定

格式	说明
宋体	正文采用宋体表示。
黑体	一级、二级、三级标题、Block Label 采用黑体。
楷体	警告、提示等内容用楷体表示。
“Terminal Display”格式	“Terminal Display”格式表示屏幕输出信息。此外，屏幕输出信息中夹杂的用户从终端输入的信息采用加粗字体表示。
“”	用双引号表示文件路径。如“C:\Program Files\Huawei”。

命令行格式约定

格式	意义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1～n 次。
#	由“#”开始的行表示为注释行。

图形界面元素引用约定

格式	意义
“”	带双引号“”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件 > 新建 > 文件夹”，表示选择“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

键盘操作约定

格式	意义
加“ ”的字符	表示键名。如“Enter”、“Tab”、“Backspace”、“a”等分别表示回车、制表、退格、小写字母 a。
“键 1+键 2”	表示在键盘上同时按下几个键。如“Ctrl+Alt+A”表示同时按下“Ctrl”、“Alt”、“A”这三个键。
“键 1，键 2”	表示先按第一键，释放，再按第二键。如“Alt，F”表示先按“Alt”键，释放后再按“F”键。

鼠标操作约定

格式	意义
单击	快速按下并释放鼠标的一个按钮。
双击	连续两次快速按下并释放鼠标的一个按钮。
拖动	按住鼠标左键不放，移动鼠标。

修订记录

修改记录累积了每次文档更新的说明，最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2012-07-12)

分销版本

2 产品定位和特点

关于本章

SVN2000 和 SVN5000 系列产品是华为技术有限公司最新推出的一系列安全接入网关，主要应用于内网的入口处，实现对接入用户的控制管理，可以广泛的应用于各种运营级网络或者企业网络。

SVN 具有强大的 SSL VPN 功能、完备的整体安全防护、丰富的用户权限管理方式、强大的定制开发能力、灵活的组网适应能力、卓越的性能、电信级的可靠性设计和增强的易用功能。

2.1 产品定位

SVN2000 和 SVN5000 系列产品是华为技术有限公司最新推出的一系列安全接入网关，主要应用于内网的入口处，实现对接入用户的控制管理，可以广泛的应用于各种运营级网络或者企业网络。

SVN2000 和 SVN5000 系列产品采用电信级的可靠硬件平台，安全的实时嵌入式操作系统，为企业、行业、运营商的远程安全办公、远程维护以及其他远程安全接入应用提供了高性价比的解决方案。

SVN2000 和 SVN5000 系列产品集成了极为丰富的功能，包括 SSL VPN、IPSec VPN、GRE VPN、MPLS VPN、防火墙、攻击防范功能以及领先的三层特性，例如 IPv6、MPLS、动态路由、策略路由等，使得企业、行业和运营商用户可以在一台设备中部署各种所需的安全服务，能够有效降低安全方案的部署成本。基于这些丰富的功能，SVN 能够在多种组网环境下作为远程接入网关和多媒体隧道网关提供服务。

- 远程接入网关

  通过在企业内网的入口处部署 SVN2000 和 SVN5000 系列产品，移动办公用户、客户、企业分部员工只要可以上 Internet，就可以随时随地访问企业内网资源。

  SVN2000 和 SVN5000 系列产品也可以部署在运营商机房，由运营商租用给企业，企业租用 SVN2000 和 SVN5000 系列产品服务之后，外部用户如出差员工、企业

分部员工可以通过专有的门户、专线去访问企业总部的资源。用户还可以通过手机自带的 L2TP over IPSec VPN 等软件访问企业内网资源。

- 多媒体隧道网关

  在 VoIP 组网应用中，SVN2000 和 SVN5000 系列产品作为多媒体隧道网关部署在 VoIP 服务器所在网络的入口处，通过多媒体隧道功能使得 VoIP 客户端与 VoIP 服务器之间的通信不受 NAT 限制，能够穿越防火墙和 HTTP 代理服务器，为语音、视频等多媒体业务提供端到端的私网穿越和安全加密能力。

SVN2000 系列产品包括以下产品型号：

- SVN2230
- SVN2260

SVN5000 系列产品包括以下产品型号：

- SVN5530
- SVN5560

说明

文中如果没有特殊说明，则以 SVN 统称这四款产品。

2.2 产品特点

SVN 具有强大的 SSL VPN 功能、完备的整体安全防护、丰富的用户权限管理方式、强大的定制开发能力、灵活的组网适应能力、卓越的性能、电信级的可靠性设计和增强的易用功能。

2.2.1 强大的 SSL VPN 功能

SVN 支持 Web 代理、端口转发、文件共享、网络扩展和多媒体隧道等 SSL VPN 业务功能。

Web 代理

Web 代理提供外部客户端和内部局域网 Web 服务器通信中转功能，避免局域网 Web 服务器直接暴露给外网攻击者，为局域网 Web 服务器提供理想的安全保护。

Web 代理是指通过 SVN 可以安全的访问内网 Web 资源，包括 Webmail 和 Web 服务器，它将来自远端浏览器的页面请求（采用 HTTPS 协议）转发给内网 Web 服务器，然后将服务器的响应回传给终端用户。

用户只要在 SVN 的虚拟网关客户端 Web 页面上安装控件后即可访问 Web 资源。

端口转发

端口转发业务是提供基于 TCP 的应用程序的安全接入，是一种非 Web 的应用方式。

使用端口转发时，通过在客户端安装 ActiveX 控件来监听用户发起的 TCP 服务请求，控件将截获的数据流经 SSL 加密后传送给 SVN，由 SVN 解密并解析后传送给相应的应用服务器。端口转发在应用级对用户访问进行控制，控制是否提供各种应用的服务，如：Telnet、远程桌面、被动模式 FTP（File Transfer Protocol）、Email 等服务。

SVN 支持如下应用服务：

- 单端口单服务应用，如 MS RDP、Telnet、SSH、VNC（Virtual Network Computing）。
- 单端口多服务应用，如 Lotus Notes。
- 多端口应用，如 Email。
- 动态端口应用，如 FTP、Oracle。

文件共享

文件共享的主要功能是将不同的文件服务器（如支持 SMB 协议的 Windows 系统、支持 NFS 协议的 Linux 系统）的共享资源以网页的形式提供给用户访问。

用户直接通过浏览器就能在内网文件系统上创建和浏览目录，进行下载、上传、改名、删除等文件操作，就像对本机文件系统进行操作一样方便安全。

网络扩展

网络扩展功能通过建立 SSL（Secure Socket Layer）隧道，实现了对所有基于 IP 的内网业务的全面访问。用户远程访问内网资源就像访问本地局域网一样方便，适用于各种复杂的业务功能。

网络扩展提供了两种使用方式，用户可以通过登录 SVN 客户端页面，安装 ActiveX 控件启用网络扩展服务，或者下载安装独立的网络扩展客户端软件。

网络扩展支持三种访问模式：

- 全路由模式

  在全路由模式下，用户只与 SVN 建立网络连接，只能对企业内网进行访问。
- 分离模式

  在分离模式下，用户不仅能够经过 SVN 安全远程访问企业内网，同时也可以访问本地子网。
- 手动模式

  在手动模式下，用户不仅能访问企业内网的特定资源、本地子网，还能访问 Internet 的各种资源。

多媒体隧道

多媒体隧道功能支持 TLS 和 TLS+UDPS 两种隧道传输模式。主要为 IMS（Information Management System）核心网中的语音和视频等业务提供加解密和隧道穿越功能。隧道密钥可以定期更新，防止加密数据被破解，配合客户端安全组件为移动互联网时代的语音和视频业务提供端到端的安全护航。

- 支持多种移动智能终端

  第三方软件通过集成客户端安全组件，可以在苹果（iPhone）、塞班（Symbian）、安卓（Android）、黑莓（Blackberry）移动智能终端设备上运行，也可以运行在 Windows 系统的 PC 上。

客户端安全组件主要实现功能强大的虚拟协议栈，让用户的数据更为安全的通过加密隧道传输，有效防止终端监听和互联网监听。提供密钥定期更新功能，防止加密数据被破解，为用户提供端到端的安全。

- UDP 业务快转

  支持流媒体业务流量快速转发，减小网关处理时延，为用户提供更好的数据通信体验。

- UDP 报文压缩

  在移动互联网时代，智能终端的跨越式发展和网络带宽建设的滞后，使无线通讯平均带宽变得很小，UDP 报文压缩功能将传输的数据进行压缩以降低网络时延，提高网络使用率，为用户提供更经济和更高性能的数据通信服务。

虚拟桌面

用户可以使用虚拟桌面客户端通过 SSL VPN 网关，远程安全访问自己的办公电脑处理业务，大大提高了工作效率。

SSL 加速

SVN 提供 SSL 加速功能，将内网服务器上的 SSL 加解密工作卸载到自身处理，极大提高内网服务器的性能，提升用户访问内网服务的速度。

负载均衡

SVN 支持负载均衡功能，能够为用户提供 Web 服务的安全接入和负载均衡，提升用户访问 Web 服务的安全性和速度。

SVN 提供对内网 Web 服务器的负载均衡，根据负载均衡算法和会话保持算法选择内网 Web 服务器，并将客户端接入请求转发给该 Web 服务器。当 Web 服务器出现异常时 SVN 会通过健康检测功能自动识别，避免将客户端接入请求转发给不可用的 Web 服务器，以保证访问的可靠性。

2.2.2 完备的整体安全防护

SVN 提供完备的整体安全防护，包括接入终端的安全、SVN 网关设备的安全、内网服务器的安全以及数据传输的安全等特性。

接入终端安全保障

通过制定严格的终端安全检查策略，在允许设备接入企业内网之前验证和确保终端设备符合企业的安全规范，必要时可拒绝接入。通过这种方式将可能存在的安全威胁在事前进行防范。

通过绑定终端标识码，可以在远程终端接入时判断终端的标识码，只有被允许的终端才能够接入企业内网，获得访问资源的权限。

- 终端安全

  SVN 提供了终端安全特性，主要包括如下功能：

  - 主机检查

检查用户用来访问内网资源的主机是否符合安全要求。主机检查功能还支持基于角色进行访问控制，即将角色与主机检查策略进行关联，只有满足主机检查策略通过条件的角色才能访问内网资源。

检查规则支持以下多项自动检测和修复功能：

- 杀毒软件检查
- 防火墙检查
- 注册表检查
- 文件检查
- 端口检查
- 进程检查
- 操作系统检查
- 缓存清理

实现客户端的零痕迹访问。

缓存清理支持以下功能：

- 浏览器缓存清理
- 文件缓存清理
- 浏览器密码清除
- 访问历史记录清除
- 指定文件清除

- 终端标识码绑定

SVN 提供用户账号与指定终端绑定功能。用户登录时，SVN 的客户端软件将根据客户端的硬件信息提取接入终端的标识码，并发给 SVN 进行匹配，只有在匹配通过后才允许用户访问内网资源。终端标识码与终端一一对应。

终端标识码绑定策略有以下三种：

- 用户和标识码一对一绑定（即指定用户只能在指定终端接入）
- 用户和标识码一对多（一个用户绑定多台终端）
- 用户和标识码多对一（多个用户绑定一台终端）

- 安全桌面

用户登录时，SVN 的客户端软件可以在远程接入终端上创建一个与真实桌面系统隔离的安全桌面，SVN 客户端与内网资源服务器之间的数据交互被隔离在安全桌面内部。在用户退出时，根据用户的应用需求，这些数据可以被高强度加密保存在远程接入终端，只有当用户再次进入安全桌面后，这些加密数据才能够再次被使用。通过安全桌面可以避免企业内部网络中关键信息资产的流失。

在安全桌面提供以下数据防泄露功能：

- 禁止安全桌面与本地桌面数据通信
- 禁止复制到外部存储设备（如 USB，打印机，COM 等）
- 禁止共享网络文件
- 禁止编辑 windows 系统注册表

SVN 网关设备安全防护

SVN 网关设备采用华为公司具有自主知识产权的专有 VRP 操作系统，该系统经过专门安全加固，相比一般通用操作系统更加安全，并在华为公司交换机、路由器产品中经过全球用户长时间广泛使用，安全程度值得信赖。

SVN 网关设备对自身提供灵活的安全保活策略，数据报文在进行 SSL 协议处理之前，先经过了可配置的 TCP/IP 层过滤检查。可配置的 TCP/IP 层报文检测包括畸形报文检测、异常报文处理、IP 层基于流量统计的攻击检测、TCP 基于流量统计的攻击检测等。

数据传输安全

当远程用户通过 SVN 访问企业内网服务器时，数据的传输路径可以划分为两段。一是从客户端到 SVN，需要经过公网；另一部分是从 SVN 到内网服务器。内网的数据传输被视为是安全的。而客户端到 SVN 之间的数据传输则面临着诸多的安全威胁，SVN 网关能够提供强有力的措施来保护机密数据不被窃取或是篡改。

SVN 支持多种加密算法和 Hash 算法（包括 MD5、SHA-1），确保了数据传输的真实性、完整性。SVN 支持的加密算法如下：

- 对称加密算法，包括 3DES\DES、RC4、AES。
- 非对称密码算法，包括 RSA。

除了这些常用的标准加解密算法外，SVN 还支持更高强度的自定义加密算法的集成。另外，还提供了密钥定时更新的功能，用户可以根据实际需要配置密钥更新的时间间隔(最高频度为每一小时更新一次)，进一步降低了密钥被破解的风险，提高了整个系统数据传输的安全性。

内网服务器安全防护

无论用户是否是通过 VPN 接入访问内网服务器，SVN 网关都可以对内网服务器提供安全防护。

管理员可以在 SVN 网关上配置对内网服务器的安全防护策略，包括增强的报文过滤功能、状态检测功能、黑名单过滤恶意主机、IP 和 MAC（Media Access Control）绑定以及多种强大的攻击防范策略。即使用户是通过 VPN 远程接入访问内网服务器，管理员配置的安全防护策略仍能够有效保护内网服务器。

- 多种 ACL
  - 基本 ACL 可以根据源 IP 地址对报文进行访问控制。
  - 高级 ACL 可以根据源 IP 地址、目的 IP 地址、源端口、目的端口、协议报文进行访问控制。
  - 基于 MAC 的 ACL 可以根据源 MAC 地址、目的 MAC 地址、数据帧的类型和优先级对报文或二层以太网帧进行访问控制。
- 增强的报文过滤

  采用的快速流分类算法使系统在进行上万条 ACL 规则的查找时，性能基本不受影响，处理速度基本保持不变。

  ASPF（Application Specific Packet Filter）是针对应用层的包过滤，即基于状态的报文过滤，以便于实施内部网络的安全策略。ASPF 能够检测试图通过 SVN 的应

用层协议会话信息，阻止不符合规则的数据报文穿过。并提供对有害 Java Applets、有害 ActiveX 的阻断。

- 状态检测功能

  状态检测是一种高级通信过滤功能。它检查应用层协议信息并且监控基于连接的应用层协议状态。对于所有连接，每一个连接状态信息都被监控并用于动态地决定数据包是否被允许通过设备或丢弃。

  状态检测技术在网络层实现所有需要的安全能力，它既有包过滤机制的速度和灵活，也有代理型防火墙安全的优点。SVN 利用最新的状态检测技术提供高速的安全防范和报文处理能力。

- 黑名单过滤恶意主机

  SVN 网关可以提供丢弃黑名单用户的所有报文来为用户提供安全保证。当 SVN 网关根据报文的行为特征检测到特定 IP 地址的用户的攻击企图后，主动将其加入黑名单表项，过滤从该 IP 地址发送的报文，从而保障网络安全。

  黑名单可以由管理员手工添加，也可以由 SVN 网关动态地添加或删除。管理员还可以将黑名单与 ACL 关联，即报文命中黑名单后，查找黑名单关联的 ACL 策略，如果命中 ACL 策略并且策略允许通过，则报文可以通过，否则报文被过滤丢弃。

  黑名单仅对 IP 地址进行匹配，可以以很高的速度实现黑名单表项匹配，从而快速有效地屏蔽特定 IP 地址的用户。

- IP 和 MAC 地址绑定

  IP 地址和 MAC 地址绑定是避免 IP 地址假冒攻击的一种有效手段。

  管理员可以配置 IP 地址和 MAC 绑定，根据配置，SVN 网关在 IP 地址和 MAC 地址之间建立关联关系。

  - 对于源 IP 地址与源 MAC 地址不匹配指定的关联关系的报文，将予以丢弃。
  - 对于匹配目的 IP 地址的报文，SVN 将该报文发送到关联关系中该 IP 地址对应的 MAC 地址。

- 强大的攻击防范能力

  - 防范多种 DDoS 攻击

    SVN 网关可以有效地检测出这些类攻击报文，通过丢弃这些报文等处理措施避免攻击行为，同时将这些攻击行为记录在日志中。目前，可以防范多种 DDoS 攻击，主要包括：SYN Flood 攻击、ICMP Flood 攻击、SIP Flood 攻击、UDP Flood 攻击、tcp-illegal-session 攻击、HTTP Flood 攻击、Land 攻击、Smurf 攻击、Fraggle 攻击、WinNuke 攻击、ICMP 重定向或不可达报文、TCP 报文标志位（如 ACK、SYN、FIN 等）不合法、Ping of Death 攻击、Tear Drop 攻击等。

  - 防范扫描窥探攻击

    攻击者通过扫描窥探就能大致了解目标系统提供的服务种类和潜在的安全漏洞，为进一步侵入系统做好准备。SVN 网关通过比较分析，可以灵活高效地检测出这类扫描窥探报文，从而预先避免后续的攻击行为。

  - 防范其它攻击

    SVN 网关除了可以有效防范多种 DDoS 攻击和扫描窥探外，还可以有效防范 IP Spoofing 攻击、带源路由选项的 IP 报文攻击、带路由记录选项的 IP 报文攻击、利用 tracert 工具窥探网络结构等其他攻击，确保系统访问权的安全。

2.2.3 丰富的用户权限管理方式

SVN 支持多种用户认证方式，提供灵活的授权方式以及细粒度的访问控制。

用户身份认证

为保证远程接入用户的合法性，SVN 支持多种身份认证方式。

SVN 自身支持 VPNDB（Virtual Private Network Database）认证方式，即在 SVN 上建立本地用户数据库，对用户名、密码进行严格认证，用户无需另外建立认证系统。

同时，针对已建设起相对完善的认证体系的企业，SVN 还支持以下外部认证系统：

- 第三方认证服务器，包括 RADIUS（Remote Authentication Dial in User Service）、LDAP（Light Directory Access Protocol）、AD（Active Directory）、SecurID。
- 数字证书认证，包括 X.509 v3 数字证书、USBKEY+数字证书。

  SVN 支持多级证书，且支持证书的 CRL（Certificate Revocation List）和 OCSP（Online Certificate Status Protocol）检测，保证证书的有效和安全。

除此之外，SVN 还支持本地口令认证、短信认证、图形码校验和终端标识码校验，适应各种用户认证环境。

灵活的用户授权

SVN 网关提供基于角色/资源关联的授权方式。可访问的内网资源被关联到不同的用户角色上，属于某角色的用户可以访问该角色关联的内网资源。通过将可访问资源与具体用户剥离，可灵活应对企业组织架构中人员的调整，减少管理员权限管理的工作量。

SVN 网关提供外部组的授权映射，能够和企业已有的用户管理系统完美对接。对于已经建立起成熟的 IT 环境的企业，这些企业一般已经具有严格配置的用户权限管理，这些配置信息可能在 LDAP、RADIUS 等认证服务器中以用户组/组织机构等形式存在。SVN 网关提供外部组映射功能，通过这个功能，管理员能够将保存在 LDAP、RADIUS 等认证服务器中用户组/组织机构等信息映射到 SVN 网关中，SVN 网关将这些用户/用户组信息和具体的可访问资源关联起来完成 SVN 用户的访问授权。

SVN 提供基于接入终端安全等级的动态授权方式。管理员可以配置在远程用户接入 SVN 网关之前先进行接入终端的安全检查，并将安全检查结果作为获得用户角色的条件。在这种方式下，接入终端安全等级高的用户可获得更广泛的内网资源访问权限，同样的接入用户如果他所使用的接入终端的安全等级较低则可能仅获得受限的内网资源访问权限。

细粒度的访问控制

除了提供灵活的用户授权外，SVN 网关还提供基于 URL、IP 地址和端口的访问控制。

2.2.4 强大的定制开发能力

SVN 的多媒体隧道功能提供定制开发能力。跟多媒体隧道关联的客户端安全组件提供二次开发的 API 接口，可以将 SVN 的客户端安全组件和上层应用软件进行集成。通过

二次开发可以满足各种复杂特殊的应用场景。目前应用较多的是 VoIP 业务的安全加密、网络穿越的场景。

客户端安全组件

SVN 客户端组件称为“安全”加密组件，区别于传统的 SSL VPN 客户端，集成安全加密组件的客户端软件运行时，不需要在系统中安装虚拟网卡、不修改操作系统的注册表。

SVN 支持 PC、各种平台的智能手机终端的接入。SVN 通过提供多种跨平台客户端安全组件，终端开发商可以根据自身的操作系统类型集成相应平台的组件。终端通过使用安全加密组件的网络通信接口实现私网穿越和安全加密功能。

客户端安全加密组件提供以下功能：

- 最佳的防火墙、NAT、代理穿越能力。
- 端到端安全加密，防窃听、封杀和干扰。
- 自动检测网络穿越能力，智能选择 SSL 或 UDP 加密隧道。
- 根据业务需求，可封装指定的 SIP/RTP/RTCP 等报文通过 SSL 或 UDP 加密隧道传输。

客户端安全加密组件支持以下软终端的集成：

- Windows 系列操作系统（Windows XP、Windows Vista、Windows 7、Windows Server 2003、Windows Server 2008）的 PC 软终端
- 苹果（iPhone）、安卓（Android）、塞班（Symbian）、黑莓（BlackBerry）系列操作系统的手机软终端

媒体数据压缩

针对无线网络带宽资源紧张、昂贵的特点，SVN 安全加密组件还提供了对媒体数据流进行压缩的特性，该特性可以由管理员操作启动或者关闭。

特性启动状况下，在 UDPS 隧道中传输的流媒体报文将被压缩，同非压缩的报文相比较，报文大小最多可以减少 24 个字节，对于负载只有百来个字节的语音数据流报文，相当于节省带宽 20%左右，可以有效的减轻在网络状况不好的情况下的报文丢失和语音延迟问题。同时，由于启用压缩后报文大小变小，加快了该报文的后续处理速度，比如报文加密、转发等等，从而提高了 SVN 网关的处理效率。

另外，报文压缩也相应的提高了传输的安全性，因为报文中的很多重要信息被压缩，即使压缩报文被中途拦截，且拦截者知道压缩的原理，也无法将报文还原出来，从而无法进行相应的篡改和攻击。

2.2.5 灵活的组网适应能力

SVN 支持丰富的 VPN、路由协议，支持虚拟防火墙功能，能够很方便地适应各种组网。

- 丰富的 VPN 特性
  - SSL VPN

可以使企事业单位、政府机关等工作人员在居家办公、外地出差、移动办公等各种环境下方便地接入到企业办公网络，访问办公内网中各项业务资源。

- IPSec VPN

  可以对不同分支机构网络之间的数据通信提供安全顺畅的 VPN 加密保护，也可以对终端用户提供 IPSec VPN 接入企业内网的功能。同时手机用户可以使用自带的 IPSec VPN 客户端实现随处接入企业内网，特别适合已经习惯于使用 IPSec VPN 客户端软件的用户。

- L2TP VPN

  用户 PC 上只要安装 VPN Client 或者使用 PC 自带的 L2TP 客户端就可以方便的接入企业内网。用户也可以通过手机自带的 L2TP over IPSec VPN 等软件访问企业内网资源。

- GRE VPN

  主要用于两个边缘路由器或者终端系统与边缘路由器之间定期的安全通信链接，适合一些小型点对点的网络互连，实时性要求不高，要求提供地址空间重叠支持的网络。

- MPLS VPN

  可以直接作为 PE（Provider Edge）设备挂接在 MPLS 网络里面，提供对 MPLS 流量的边缘汇聚服务。

- 丰富的路由功能

  SVN 支持 IPv6、动态路由、MPLS VPN 等多种丰富的路由协议，可节省用户投资，降低组网成本。

  SVN 可以配置静态路由，支持 RIP-1、RIP-2、OSPF、BGP 等动态路由协议，还具有根据用户制定的策略进行路由选择的机制。

  SVN 可参与路由协议运算，实现多条链路负载均衡，与路由设备实现无缝对接。

- 虚拟防火墙

  SVN 针对小型私有网络的特点，提出多实例解决方案。即将一台 SVN 从逻辑上划分为多台虚拟防火墙，分别为多个小型私有网络提供独立的安全保障。对于网络运营商，可使用 SVN 向外出租网络安全保障服务。

  VPN 实例为虚拟防火墙提供相互隔离的 VPN 路由，VPN 实例与虚拟防火墙是一一对应的。目前，SVN 支持 IPSec 多实例、L2TP 多实例、NAT 多实例、LAN/WAN/DMZ 区域多实例、ACL 多实例、Session 多实例、黑名单多实例和路由多实例。

2.2.6 卓越的性能

SVN 基于多核处理器的硬件构架，保障了系统的整体性能。SVN5000 通过硬件加密卡实现 SSL 运算，具备极高的 SSL 处理能力，实现内核级的密钥交换和批量加密，保证系统响应毫秒级的延迟。除了硬件加速技术外，在软件结构上，通过 UDP 报文压缩功能将传输的数据进行压缩以降低网络时延，提高网络使用率，为用户提供更经济和更高性能的数据通信服务。

2.2.7 电信级的可靠性设计

SVN 提供电源备份、风扇备份、整机双机热备份和链路备份，保证了设备的高可靠性。

设备级可靠性

- SVN5000 系列产品采用双电源模块，两个电源模块可以互相热备份，并且支持热插拔，电源倒换时不影响系统运行。
- 风扇系统采用 N+1 冗余设计，共提供 6 个系统风扇，具有独立的风扇框。同时支持温度监控、风扇热插拔，可适应恶劣环境应用。

网络级可靠性

支持双机热备份功能，一个备份组内包括一个主用设备和一个备用设备。HRP 协议负责在主/备设备之间备份关键配置命令和会话表状态信息，从而确保主用 SVN 出现故障时能由备用 SVN 平滑地接替工作。

链路级可靠性

支持将多个物理上的以太网接口进行捆绑聚合成为一个逻辑上的 Eth-Trunk 接口，提高了点对点之间的最大数据传输效率。并且，如果 Eth-Trunk 接口中的某一条链路出现问题，其他链路将分担其流量，可广泛适用于各种组网环境，满足了大流量需求也提高了可靠性。

2.2.8 增强的易用功能

SVN 支持虚拟网关、定制页面、配置向导和可控的用户自助密码管理。

虚拟网关支持

SVN 网关支持虚拟网关功能，可以为不同的组织机构设置虚拟化、逻辑独立的 SVN 网关实现登录的隔离。不同的虚拟网关可以设置独立的 IP 地址或者域名登录地址，并进行完全独立的管理配置，实现完全的访问逻辑隔离，让各组织机构的用户感觉类似有单独的一台 SSL VPN 设备在为其服务。

可以为每个虚拟网关配置独立的虚拟网关管理员，该类型的管理员可以对所属的虚拟网关进行独立的配置和管理。

定制页面

SVN 网关支持对各虚拟网关进行独立的页面定制，SVN 的页面定制功能包含：

- 定制用户登录页面的窗口 Title、页面 Logo 图片和欢迎辞
- 定制用户登录后的页面跳转
- 完整的用户登录页面定制，可以将 SVN 的用户登录框集成到已有的 Portal 页面

配置向导

SVN 支持对用户常用的关键业务进行配置指导，在 Web 配置界面上提供配置向导，通过 step by step 的方式快速的指导入门级用户完成基本的配置。

SVN 提供如下配置向导：

- SSL VPN 远程接入业务的配置向导

- IPSec VPN 远程接入业务的配置向导

可控的用户自助密码管理

管理员可以灵活指定用户自主的密码管理策略，可以大幅简化大量用户的配置管理工作，提高企业的 IT 支持中心的效率。

- 允许/禁止用户自助修改密码
- 用户密码强度可以配置
- 用户密码有效期控制、超时前的提醒
- 配置要求用户首次登录修改密码

3 产品架构

关于本章

SVN 由一体化机箱和扩展插槽组成，提供风扇、电源。其中 SVN5000 系列产品的扩展插槽支持插入加密卡。

软件系统为模块化结构，各模块完成相应的特定功能并协同工作。

3.1 硬件结构

SVN 由一体化机箱和扩展插槽组成，提供风扇、电源。其中 SVN5000 系列产品的扩展插槽支持插入加密卡。

3.1.1 产品外观

介绍 SVN 的外观，包括前面板、后面板以及接口等情况。

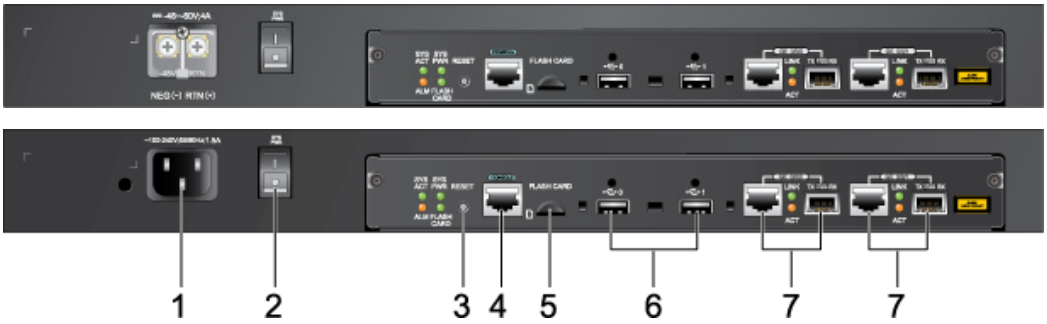
SVN2000 由一体化机箱、固定接口卡、SD 卡组成。设备的一体化机箱尺寸为 442mm×414mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。

SVN5000 由一体化机箱、加密卡组成。设备的一体化机箱尺寸为 442mm×560mm×43.6mm（宽×深×高），可以安装在 19 英寸标准机柜中。

SVN2000 前面板

SVN2000 分为直流机型和交流机型，前面板如图 3-1 所示。

图3-1 SVN2000 前面板



1.直流/交流电源插座　2.直流/交流电源开关　3.系统复位键

4.Console 接口　5.Micro-SD 卡接口　6.USB2.0 接口

7.GE Combo 接口

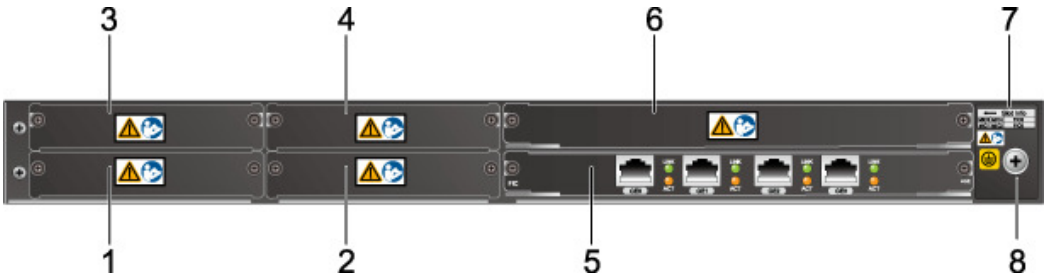
说明

Micro-SD 卡接口贴有防拆标签，请不要随意撕掉，否则可能导致机密信息被窃取，造成重大损失。

SVN2000 后面板

SVN2000 后面板如图 3-2 所示。

图3-2 SVN2000 后面板



1.MIC1 插槽　2.MIC2 插槽　3.MIC3 插槽

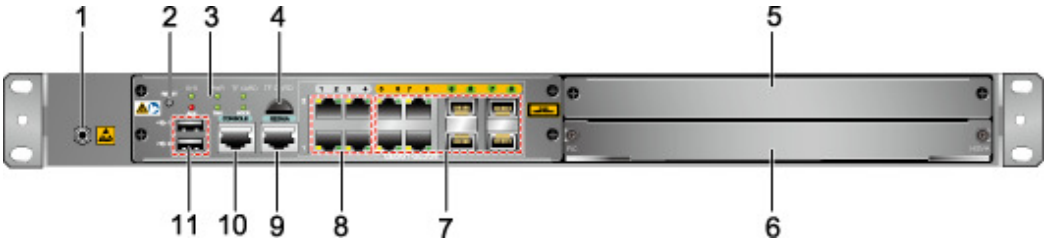
4.MIC4 插槽　5.FIC5 插槽（内置 4×GE 电接口卡）　6.FIC6 插槽

7.槽位标识　8.接地端子

SVN5000 前面板

SVN5000 前面板如图 3-3 所示。

图3-3 SVN5000 前面板



1.防静电手腕带插孔	2.系统复位键	3.指示灯
4.Micro-SD 卡接口	5.FIC2 插槽	6.加密卡
7.光电互斥接口	8.10/100/1000M 以太网电接口	9.带外管理口
10.Console 接口	11.USB 2.0 接口	

说明

- SVN5530/5560 支持 2 个 FIC 接口卡扩展插槽。其中 FIC1 插槽标配加密卡。
- 图 3-3 中“2”号系统复位键目前只有热重启功能。
- SVN5530/5560 暂不支持图 3-3 所示“4”号 Micro-SD 卡插槽。

SVN5000 后面板

SVN5530/5560 的后面板如图 3-4 和图 3-5 所示。

图3-4 SVN5000 直流机型后面板

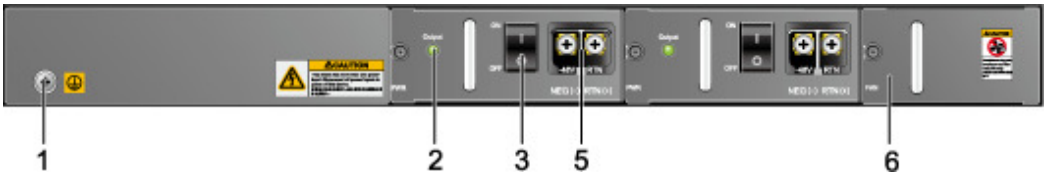
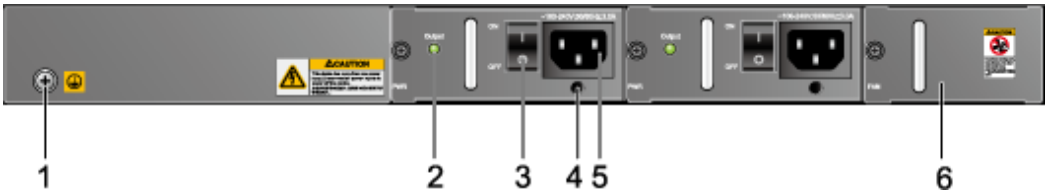


图3-5 SVN5000 交流机型后面板



1.接地端子	2.电源指示灯	3.电源开关
4.交流电源线扎线孔	5.电源接口	6.风扇框

3.1.2 加密卡

加密卡的主要功能是用于实现 SSL VPN 硬件加密，为 SVN 提供高性能的 SSL VPN 协议处理能力。

外观

只有 SVN5000 系列产品支持在 FIC 扩展插槽中插入加密卡。加密卡的外观如图 3-6 所示。

图3-6 加密卡外观图

技术指标

加密卡的技术指标如表 3-1 所示。

表3-1 加密卡技术指标

项目	描述
加密卡丝印	HSVA
加密卡尺寸（宽×深×高）	190.0mm×160.0mm×19.8mm
加密卡功耗	6W
可安装槽位	所有 FIC 扩展插槽 说明 SVN5000 系列产品标配加密卡，固定安装在 FIC1 插槽。

3.1.3 系统配置

介绍 SVN 主要硬件配置和环境要求。

SVN 的系统配置如表 3-2 所示。

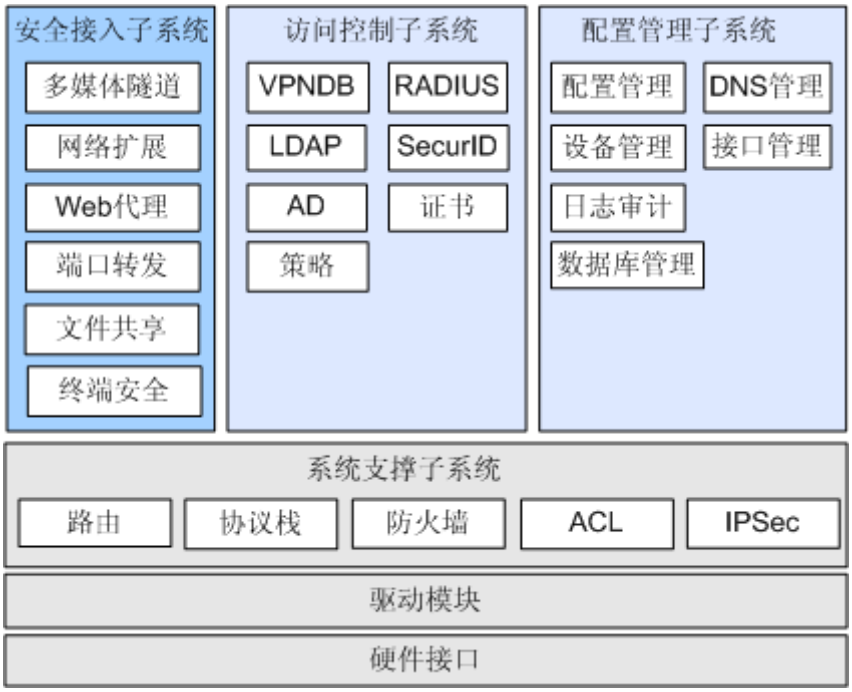
表3-2 SVN 的系统参数和整机设备参数

项目	SVN2000	SVN5000
扩展插槽	4 个 MIC 扩展插槽 2 个 FIC 扩展插槽 说明 FIC5 扩展插槽内置 4×GE 电接	2 个 FIC 扩展插槽，用于插加密卡

项目	SVN2000	SVN5000
	口卡，其他扩展插槽暂不使用。	
固定接口	1 个 Console 接口 1 个 SD 接口 2 个 USB2.0 接口 2 个 GE Combo 接口和 4 个 GE 电接口，其中 4 个 GE 电接口位于一个 FIC 扩展插槽中	1 个 Console 接口 1 个 10/100/1000M 带外管理口 2 个 USB 2.0 接口 4 个 GE Combo 接口和 5 个 GE 电接口
外型尺寸（W×D×H）	442mm×414mm×43.6mm	442mm×560mm×43.6mm
重量（满配）	5.4kg	8.4kg
额定输入电压	AC：100V～240V（50Hz/60Hz） DC：-48V～-60V	AC：100V～240V（50Hz/60Hz） DC：-48V～-60V
最大输入电压	AC：90V～264V（50Hz/60Hz） DC：-36V～-72V	AC：90V～264V（47Hz～63Hz） DC：-36V～-72V
整机最大功耗	100W	150W
工作环境温度	长期：0℃～45℃ 短期：-5℃～55℃	长期：0℃～45℃ 短期：-5℃～55℃
工作环境湿度	10%RH～90%RH，非冷凝	5%RH～95%RH，非冷凝

3.2 软件结构

软件系统为模块化结构，各模块完成相应的特定功能并协同工作。



安全接入子系统

安全接入子系统对 PC、智能移动手机等终端的安全接入提供保障。实现的主要功能有：多媒体隧道、网络扩展、Web 代理、端口转发、文件共享和终端安全。

访问控制子系统

访问控制子系统通过多种认证授权方式对访问内网的用户或者客户端进行访问控制，除此之外，还通过策略来过滤用户可以访问的资源和进行流控制。提供的认证授权方式有：VPNDB、RADIUS、LDAP、SecurID、AD 和证书等多种认证授权方式。

配置管理子系统

配置管理子系统实现与用户进行交互并提供了配置、测试、维护等接口。实现了配置管理、设备管理、文件系统管理、信息中心对日志和告警的管理、软件补丁管理和 VPNDB 数据库管理。

系统支撑子系统

系统支撑子系统对整个系统进行支撑。实现的主要功能有：路由功能、协议栈、防火墙功能、ACL 和 IPSec。

驱动模块和硬件接口

提供软件和硬件进行连接的基本支撑。

4 产品功能

提供 SVN 支持功能一览表，方便快速查阅。

SVN 系列产品支持的特性如表 4-1 所示。

表4-1 SVN 系列产品支持的特性

分类	说明	
SSL VPN 功能	多媒体隧道	• 支持 TLS 和 TLS+UDPs 两种隧道传输模式 • 支持 UDP 业务快转 • 支持 UDP 报文压缩
	网络扩展	• 所有复杂内网应用 • 支持 DHCP 方式或地址池方式分配客户端虚拟 IP 地址 • 支持用户绑定虚拟 IP 地址 • 支持组绑定虚拟 IP 地址池 • 支持三种模式：全路由模式、分离模式和手动模式
	Web 代理	• Web 链接
	端口转发	• 单端口单服务器应用：Telnet、MS RDP、SSH、VNC 等 • 单端口多服务器应用：Lotus Notes • 多端口应用：Email • 动态端口应用：FTP、Oracle
	文件共享	• SMB 文件系统（Windows） • NFS 文件系统（Linux） • 文件的下载、浏览、上传、改名、删除 • 目录的新建、浏览、改名、删除
	终端安全	• 支持终端标识码，可以基于终端硬件特征制定接入策略

分类	说明	
		• 支持主机检查，在接入时检查终端的操作系统版本、补丁版本、杀毒软件、防火墙软件等，实现基于终端安全级别的动态授权 • 支持缓存清理，在退出 SSL VPN 连接后清理终端上的访问痕迹，防止机密信息泄露 • 支持安全桌面，可以避免企业内部网络中关键信息的泄漏
	认证	• VPNDB • RADIUS • LDAP • AD • SecurID • X.509 v3 数字证书 • USBKEY+数字证书
	授权	• VPNDB • RADIUS • LDAP • AD • SecurID
	策略	• 虚拟网关源 IP 型 • 用户源 IP 型 • 用户目的 IP 型 • 用户 URL 型 • 组源 IP 型 • 组目的 IP 型 • 组 URL 型
	用户密码策略	• 首次登录可强制修改 • 用户密码复杂度策略可定制 • 设置和提醒定期修改
	防暴力破解	• 锁定具有相同用户名的用户 • 锁定来自用一源 IP 地址的用户 • 管理员可解锁指定的用户
	用户抓包	• 同一时间只可对一个建立稳态连接的用户进行抓包
	用户锁定	• 用户锁定 • 用户解锁
	密码算法	• 加密算法：3DES\DES、RC4、AES

分类	说明	
		• 非对称密码算法：RSA • Hash 算法：MD5、SHA-1
	协议版本	• SSL2.0 • SSL3.0 • TLS1.0
防火墙功能	ACL 和安全策略	• 支持基本 ACL 和高级 ACL • 支持基于时间段的 ACL • 支持基于 MAC 地址的 ACL • 支持动态维护 ACL 规则 • 支持黑名单、IP 和 MAC 地址绑定 • 支持应用层过滤、提供状态检测 • 提供端口映射机制
	NAT	• 地址转换（NAT 和 PAT） • 提供内部服务器 • 端口级 NAT 服务器 • 支持多种 NAT ALG
	攻击防范	• 防范多种 DoS 和 DDoS 攻击：SYN Flood、ICMP Flood、UDP Flood、Get Flood、WinNuke、ICMP 重定向和不可达报文、Land、Smurf、Fraggle、IP Spoofing 等 • 防范扫描窥探：包括地址扫描、端口扫描、IP 源站选路选项、IP 路由记录选项、时间戳、刺探路由 • 畸形报文攻击：畸形 IP 分片报文、畸形 TCP 报文、超大 ICMP 报文、TearDrop、Ping Of Death
	AAA	• 支持 RADIUS 协议，提供 PAP 和 CHAP 验证方式 • 支持提供 PPP、Login 登录用户认证 • 支持本地认证 • 支持多 ISP
	虚拟防火墙	• 支持虚拟防火墙
接入	Ethernet	• 支持三层以太网接口 • 支持三层以太网子接口
	Eth-Trunk	• 支持三层 Eth-Trunk 接口 • 支持三层 Eth-Trunk 子接口
IP 业务	ARP	• 静态 ARP • 动态 ARP

分类	说明	
		• ARP 代理 • 免费 ARP
	DNS	• 支持本地静态域名 • 支持 DNS Client • 支持 DNS 代理 • 支持 DDNS 动态域名服务
	DHCP	• 支持 DHCP Server • 支持 DHCP Client • 支持 DHCP 中继 • 支持 DHCP Snooping
	IP 单播策略路由	• 支持 IP 单播策略路由
	IPV6	• IPv6 over IPv4 • IPv4 over IPv6
路由	IPv4 路由	• 支持静态路由 • 支持 RIP、OSPF、BGP、ISIS 等动态路由 • 支持路由策略和路由叠代
	IPv6 路由	• 支持静态路由 • 支持 RIPng、OSPFv3、BGP4+、ISISv6 等动态路由 • 支持路由策略和路由叠代
系统管理	信息中心	• 对日志、告警、Debug 信息进行管理和输出
	SNMP	• 支持 Snmp v1 • 支持 Snmp v2c • 支持 Snmp v3
	Web 管理	• 支持通过 HTTP 协议对设备进行 Web 管理 • 支持通过 HTTPS 协议对设备进行 Web 管理
	NTP	• 支持 NTP 客户端/服务器服务方式 • 支持时钟对等体服务方式 • 支持 NTP 局域网广播服务方式 • 支持 NTP 组播服务方式 • 支持 NTP v3 协议，兼容 v2 和 v1 协议
	Ping/Tracert	• 支持 Ping/Tracert
维护和可靠	远程抓包	• 支持远程抓包

分类	说明	
性	端口映射	• 支持端口映射
	双机热备份	• 支持双机热备份
	Link-Group	• 支持 Link-Group
	电源 1+1 备份	• 支持电源 1+1 备份
	多种升级方式	• Web 方式升级 • FTP 方式升级 • TFTP 方式升级 • BootROM 方式升级
MPLS&VPN	BGP/MPLS IP VPN	• 支持 BGP/MPLS IP VPN
	L2TP VPN	• 支持 L2TP VPN
	IPSec VPN	• 支持 IPSec VPN
	GRE VPN	• 支持 GRE VPN
	CA 证书	• 支持 CA 证书
QoS	流量监管	• 支持流量监管
	流量整形	• 支持流量整形
	接口限速	• 支持接口限速
	拥塞管理	• 支持拥塞管理
	拥塞避免	• 支持拥塞避免
	基于类的 QoS	• 支持基于类的 QoS
日志	系统日志	• 系统重启记录 • 网口状态记录 • 温度告警记录 • 风扇坏记录 • License 导入记录
	用户日志	• 上下线时间 • 登录失败记录 • 操作行为
	管理员日志	• 上下线时间 • 登录失败记录

分类	说明	
		• 操作行为
	日志特性	• 分级查看 • 日志导出 • 条件查询

5 产品和应用场景

关于本章

5.1 移动办公组网应用

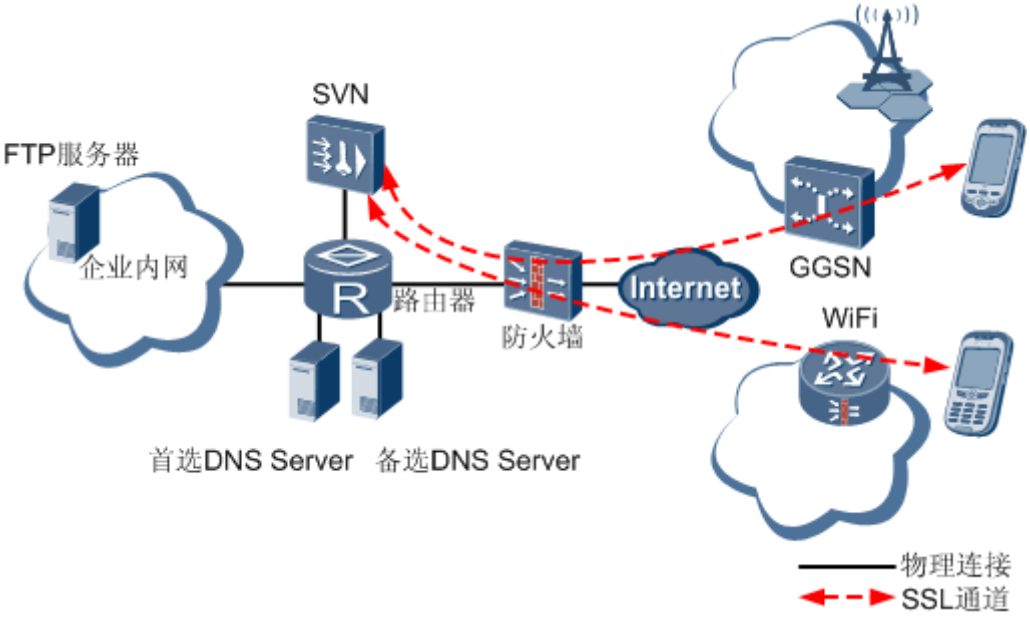
通过 SVN，用户可以在任何地点安全地访问管理员配置的网络资源，实现真正的移动办公。

5.1.1 智能手机移动办公组网应用

SVN 可以与智能手机配合使用，在不安全的公共网络上构建安全的多媒体隧道，满足大量智能手机移动办公用户的接入需求，同时保障数据的传输安全。

如图 5-1 所示，智能手机通过自带的 L2TP 等 VPN 软件，安全的接入企业内网。

图5-1 智能手机移动办公组网图

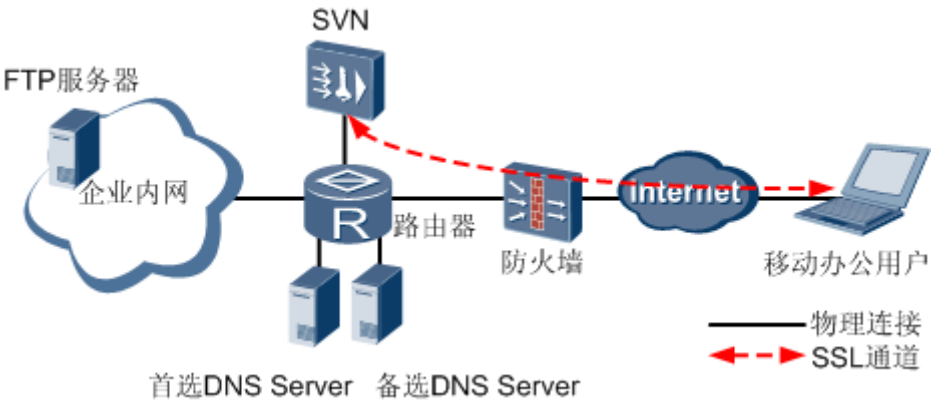


5.1.2 固定终端移动办公组网应用

固定终端移动办公用户通过网络浏览器或者客户端软件，就可以实现安全地访问管理员配置的网络资源。

如图 5-2 所示，移动办公用户通过 SSL 通道，安全的接入企业内网。

图5-2 固定终端移动办公组网图



5.2 VoIP 私网穿越组网应用

通过在运营商侧部署 SVN，将 VoIP 客户端软件与客户端安全组件集成，用户在启用 IMS（IP Multimedia Subsystem）业务时，能够不受 NAT 限制、穿越防火墙和 HTTP 代理设备，正常使用 IMS 业务。

IMS 由 3GPP（3rd Generation Partnership Project）在 R5 阶段引入，目的是将 Internet 的体验引入到移动网络，结合两者的优点。IMS 问世之后立即得到了 3GPP2、ETSI（European Telecommunications Standards Institute） TISPAN（Telecommunications and Internet converged Services and Protocols for Advanced Networking）、ITU-T（International Telecommunication Union-Telecommunication Standardization Sector）等众多标准化组织的认同，IMS 核心架构也得到了这些组织的完全重用。

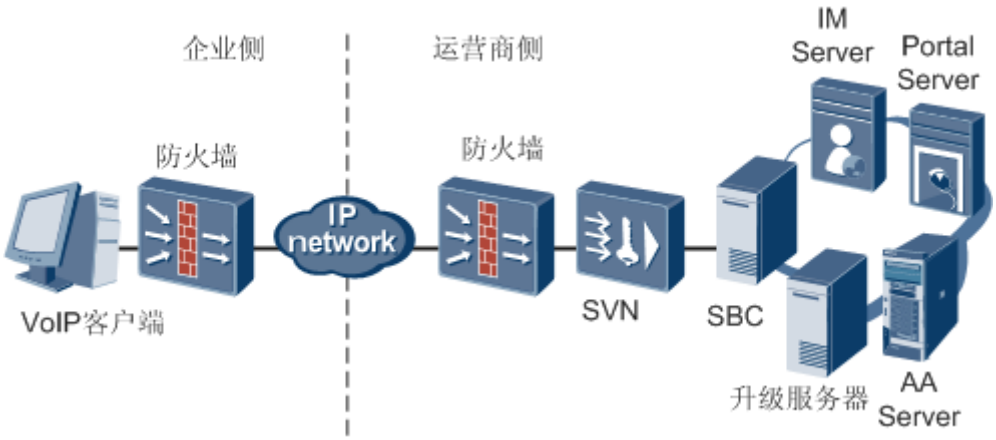
IMS 除全面考虑了会话控制、业务提供、业务触发、移动性、计费、寻址方式等特性之外，还考虑了 QoS（Quality of Service）、安全、NAT（Network Address Translation）穿透、与 PSTN（Public Switched Telephone Network）和 PLMN（Public Land Mobile Network）网络互通、固定移动融合等问题。IMS 是 IP 网上进行多媒体通信的可运营、可管理、可增值的一种完整解决方案。

在企业侧部署 IMS 业务时，面临以下威胁：

- 正常使用 IMS 业务需要开放大量的端口，而企业侧防火墙一般不开放 10000～65535 之间的 UDP 端口号，导致媒体流无法穿越防火墙。
- 大中型企业的用户普遍通过 NAT/HTTP 代理上网，SIP/RTP 报文无法穿越 NAT/HTTP 代理设备。

为了解决以上威胁，采取以下解决方案：在 SVN 设备上配置多媒体隧道功能，当用户登录 VoIP 客户端软件时，客户端安全组件与 SVN 之间建立 SSL 隧道，所有的 VoIP 通信数据都通过此 SSL 隧道传输。企业侧防火墙只要开放 443 端口，可以实现媒体流穿越防火墙的需求。将 SIP/RTP 报文封装，并通过 SSL 隧道传输，可以实现穿越 NAT 设备的需求。由于 SIP/RTP 报文是基于 UDP 的，HTTP 代理是基于 TCP 的，将 SSL 隧道配置成 TCP 和 UDP 的传输模式，可以实现 SIP/RTP 报文穿越 HTTP 代理设备的需求。

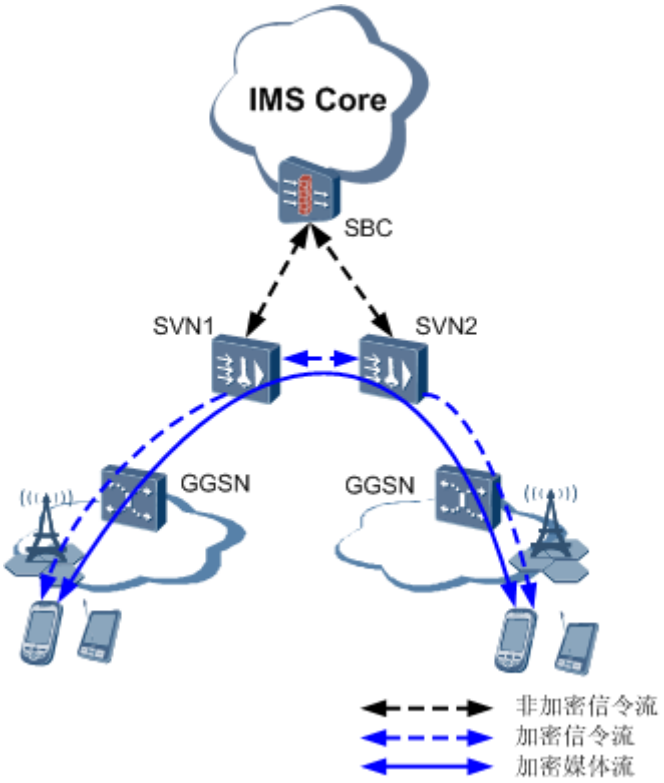
图5-3 VoIP 私网穿越组网图



5.3 VoIP 加密保护组网应用

当用户进行语音呼叫、收发即时消息时由 SVN 完成消息的加密和解密，确保用户通信的安全性。

图5-4 VoIP 加密保护组网图



VoIP 加密保护组网应用方案组网图如图 5-4 所示。

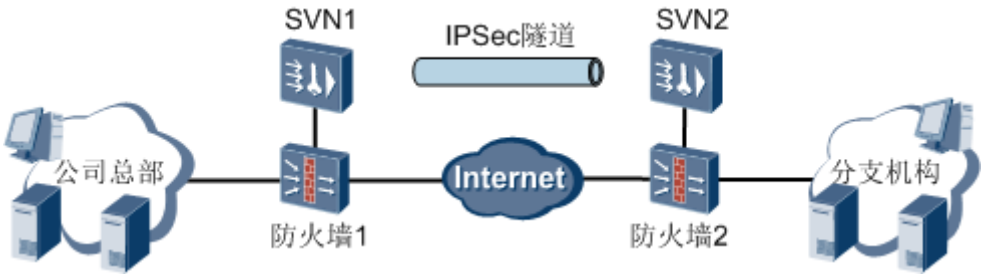
SVN 作为 IMS 网络中的标准网元，实现多媒体数据在复杂网络下的传输，为通讯过程中的报文传输提供安全保障。

用户只需在手机终端上运行与客户端安全组件集成的软件，客户端安全组件会自动与运营商部署的 SVN 建立加密通道提供语音、IM 等端到端加密的通信安全解决方案。用户在使用加密业务过程中，体验上与使用非加密业务完全一样。

5.4 作为 IPSec 设备进行总部到分支机构的互联组网应用

SVN1 与 SVN2 之间建立 IPSec 隧道，公司总部和分支机构能够通过 IPSec VPN 互访资源。

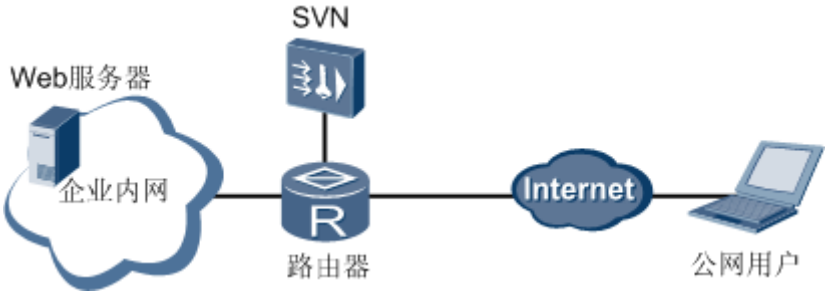
图5-5 作为 IPSec 设备进行总部到分支机构的互联组网图



5.5 作为 NAT Server 设备提供外网到内网服务器的访问组网应用

在企业内网部署了一台 Web 服务器，其真实 IP 是私网地址，通过 NAT Server 功能公网用户可以通过一个公网地址来访问该 Web 服务器。

图5-6 作为 NAT Server 设备提供外网到内网服务器的访问组网图



6 操作和维护

关于本章

6.1 多种设备配置管理方式

SVN 提供 Web 登录、Console 登录、Telnet 登录、SSH 登录对设备进行配置管理，还支持使用网管设备进行管理。

Web

SVN 提供基于 GUI（Graphic User Interface）的 Web 管理界面，为用户提供友好的配置和管理界面。SVN 支持通过 HTTP（Hyper Text Transfer Protocol）和 HTTPS（Secure Hyper Text Transfer Protocol）协议访问 Web 管理界面。

在 Web 管理界面中，可以配置网络区域（包括 LAN、WAN 和 DMZ）、ACL（Access Control List）、NAT（Network Address Translation）、攻击防范、黑名单、SSL VPN、IPSec VPN、策略路由、负载均衡、双机热备等功能和各种统计参数。

Console

支持配置终端与 Console 口相连后，在配置终端上对设备进行配置和维护。

Telnet

只要有到设备路由可达的配置终端，SVN 支持用 Telnet 方式在终端上对设备进行配置和维护。

SSH

支持 SSH（Secure Shell）维护管理方式，实现在不能保证安全的网络上提供安全信息保障和强大认证功能，以避免受到 IP 地址欺诈、明文密码截取等攻击。

基于 SNMP 的终端系统管理

SVN 提供网管接口，使用 SNMP（Simple Network Management Protocol）简单网络管理协议与网管系统通信。

SVN 支持以下网管系统的管理：

- 华为公司网管平台 M2000
- 华为公司网管平台 I2000
- 华为公司网管平台 U2000
- 华为公司网管平台 VSM

6.2 丰富的系统维护功能

SVN 提供远程抓包、丢包统计、多种升级方式、强大的 Debug 功能、灾备配置文件等系统维护功能，为故障分析和定位提供了有效的数据。

- 远程抓包

  远程抓包功能是将经过 SVN 的报文复制保存到内存中，然后将保存的报文发送到特定的主机，以实现在远程主机上对 SVN 的报文进行分析。

- 丢包统计

  SVN 提供多种丢包统计的数据，有效提供了丢包分析。

- 调试命令

  SVN 提供业务运行的 Debug 功能，在线记录用户指定的业务运行时刻的关键事件、报文处理、报文解析、状态切换等信息；为用户在调测设备及组网方案时提供了有利的支持；Debug 可以根据指定业务（如网络扩展业务）通过控制台打开或者关闭。SVN 提供系统操作的 Trace 功能，在线记录系统的任务切换、中断、队列读写、系统异常等重要事件，系统发生故障重起后，可以读出 Trace 信息作为故障定位参考。Trace 功能可以通过控制台命令打开或关闭。

- 灾备还原配置

  通过事先指定一份配置文件作为灾备配置文件，并指定灾备配置文件作为下次启动的配置文件，则在配置文件不可恢复时，可以还原最初任务时的状态达到正常使用最初业务的目的。

6.3 增强的日志管理

SVN 能输出文本方式的 Syslog 日志，为设备事件的记录提供了强有力的支撑。

- 丰富的日志信息
- 与 eLog 联动

  eLog 日志管理系统是华为技术有限公司推出的设备日志管理系统。通过高效地采集设备的日志，用户能及时了解安全设备和网络设备的运行情况，跟踪网络用户的行为，迅速识别并消除安全威胁。

  SVN 系列支持与 eLog 日志管理系统进行联动，实现日志信息的海量存储与快捷查询，有效帮助用户定位网络问题和设备运行的历史信息。
- 日志服务器容灾

  最多支持向 4 个日志服务器发送日志，日志发送方式支持轮询和并发两种。

7 技术指标

关于本章

7.1 环境指标

介绍 SVN 的环境指标。

表7-1 SVN 环境指标

项目	描述
气压	70kPa～106kPa
海拔	-60 m (-197 ft) to 1800 m (6000ft) 50℃ 1800 m (6000 ft) to 4000 m (13000 ft) 40℃
工作环境温度	长期：0℃～45℃ 短期：-5℃～55℃
环境相对湿度	10%RH～90%RH，非冷凝
存储温度	-40℃～70℃

7.2 遵循的标准和协议

介绍 SVN 遵循的标准和协议。

表7-2 ETS 相关标准

标准名	说明
ETS 300 019-2-2	Equipment Engineering; Environmental conditions and environmental tests for telecommunications equipment. part2-2: specification of environmental tests transportation
ETS 300 119-3	European telecommunication standard for equipment practice Part 3: Engineering requirements for miscellaneous racks and cabinets
EN 300 386 Version 1.2.1	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; ElectroMagnetic Compatibility (EMC) requirements

表7-3 IEC 相关标准

标准名	说明
IEC 61000	Electromagnetic compatibility (EMC)
IEC 61000-4-2	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 2: Electrostatic discharge immunity test - Basic EMC publication
IEC 61000-4-3	Electromagnetic compatibility (EMC) - Part 4-3: Testing and measurement techniques; Radiated, radio-frequency, electromagnetic field immunity tes
IEC 61000-4-4	Electromagnetic compatibility (EMC) - Part 4: Testing and measuring techniques - Section 4: Electrical fast transient/burst immunity test - Basic EMC publication
IEC 61000-4-5	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 5: Surge immunity test
IEC 61000-4-6	Electromagnetic compatibility (EMC) - Part 4: Testing and measurement techniques - Section 6: Immunity to conducted disturbances, induced by radio-frequency fields
IEC 61000-3-2	Electromagnetic compatibility (EMC) - Part 3-2: Limits; Limits for harmonic current emissions (equipment input current <kleiner =>16 A per phase)
IEC 61000-3-3	Electromagnetic compatibility (EMC) - Part 3: Limits; section 3: Limitation of voltage fluctuations and flicker in low-voltage supply systems for equipment with rated current <kleiner =>16 A
IEC 62151	Safety of equipment electrically connected to a telecommunication network

表7-4 ISO 相关标准

标准名	说明
ISO/IEC 11801	Information technology - Generic cabling for customer premises
ISO/IEC 15802-2	Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Common specifications - Part 2: LAN/MAN management

表7-5 CISPR 相关标准

标准名	说明
CISPR 22	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement

表7-6 ITU-T 相关标准

标准名	说明
I.430	[I.430] Recommendation I.430 (11/95) - Basic user-network interface - Layer 1 specification
I.431	[I.431] Recommendation I.431 (03/93) - Primary rate user-network interface - Layer 1 specification

表7-7 IEEE 相关标准

标准名	说明
IEEE802.3	Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specification
IEEE802.3u	Media Access Control (MAC) parameters, physical Layer, medium attachment units, and repeater for 100 Mb/s operation, type 100Base-T
IEEE802.1D	Media Access Control (MAC) Bridges
IEEE802.3af	DTE Power via MDI

表7-8 国家相关标准

标准名	说明
YDN028-1997	SDH 光缆系统及设备的线性复用段保护——线性复用段、自愈环

标准名	说明
	及其它类型结构
YDN 062-1997	PDH 通道、段和传输系统及 SDH 通道和复用段的故障检测和定位程序
GB/T 13543-92	数字通信设备环境试验方法
GB 2421-89	电工电子产品基本环境试验规程总则
GB 2423.1-89	电工电子产品基本环境试验规程试验 A：低温试验方法
GB 2423.2-89	电工电子产品基本环境试验规程试验 B：高温试验方法
GB/T 2423.3-93	电工电子产品基本环境试验规程试验 Ca：恒定湿热试验方法
GB/T 2423.5-1995	电工电子产品环境试验 第二部分：试验方法试验 Ea 和导则：冲击
GB/T 2423.6-1995	电工电子产品环境试验 第二部分：试验方法试验 Eb 和导则：碰撞
GB 2423.9-89	电工电子产品基本环境试验规程试验 Cb：设备用恒定湿热试验方法
GB/T 2423.10-1995	电工电子产品环境试验 第二部分：试验方法试验 Fc 和导则：振动（正弦）
GB 2423.22-87	电工电子产品基本环境试验规程 试验 N：温度变化试验方法
GB 2423.43-1995	电工电子产品环境试验 第二部分：试验方法 元件、设备和其他产品在冲击（Ea）、碰撞（Eb）、振动（Fc 和 Fd）和稳态加速度（Ga）等动力学试验中的安装要求和导则
GB2424.1-89	电工电子产品基本环境试验规程 高温低温试验导则
GB/T2424.2-93	电工电子产品基本环境试验规程 湿热试验导则
GB2424.13-81	电工电子产品基本环境试验规程 温度变化试验导则
SJ2170-82～ SJ2175-82	一般电子产品运输包装基本试验方法
SJ 3213-89～ SJ 3215-89	一般电子产品运输包装基本试验方法
SJ/Z 3216-89	电子产品防护、包装和装箱等级
GB 3873-83	通信设备产品包装通用技术条件
GB/T 4857.1-92	包装、运输包装件试验时各部位的标示方法
GB/T 14013-92	移动通信设备 运输包装
GB191-1990	包装储运图示标志

标准名	说明
GB6388-1986	运输包装收发货标志
GB/T 13426-1992	数字通信设备的可靠性要求和试验方法