华为SVN2000/5000
销售指导书

(V1.0)

目 录

第 1 章 产品定位

1.1 SVN2000/5000 产品定位

SVN2000/5000系列产品是华为公司自主研发的安全接入网关，面向运营商、电子政务、教育、金融、交通、大中型企业等市场：

运营商市场：BSS系统远程维护VPN接入、移动办公安全接入、OSS远程VPN办公、远端呼叫座席VPN接入、互联网营业厅VPN接入、业务合作伙伴（如合作营业厅、卡类代销网点建设、新业务提供商等）VPN接入。

电子政务市场：移动办公安全接入、远程VPN接入办公、远程网管维护VPN接入、公众网上安全信息填报业务（如报税、报关等）的VPN接入。

教育行业市场：教师远程VPN办公、校园电子图书馆VPN接入、移动办公安全接入、校园网络远程网管维护VPN接入、教考信息网上VPN接入查询。

大中型企业市场：企业员工远程办公VPN接入、移动办公安全接入、远程网管维护VPN接入、合作伙伴（访问ERP等）远程等VPN接入。

金融市场：保险公司保单系统VPN访问、移动办公安全接入、员工远程办公接入、远程网管维护VPN接入。

交通、能源等市场：企业员工远程办公VPN接入、移动办公安全接入、远程网管维护VPN接入、远程数据安全上收等。

SVN2000/5000系列安全接入网关采用华为成熟的电信级硬件平台和安全的实时嵌入式操作系统，满足各种严苛的国际认证规范，并且采用低功耗硬件设计，实现了绿色节能、低碳环保，集成SSLVPN、IPSec VPN、GRE VPN、L2TP VPN、MPLS VPN和多媒体隧道网关功能于一体，具备广泛的适应性，支持各种计算机和移动终端设备，具有完备的整体安全防护和丰富的用户权限管理方式。

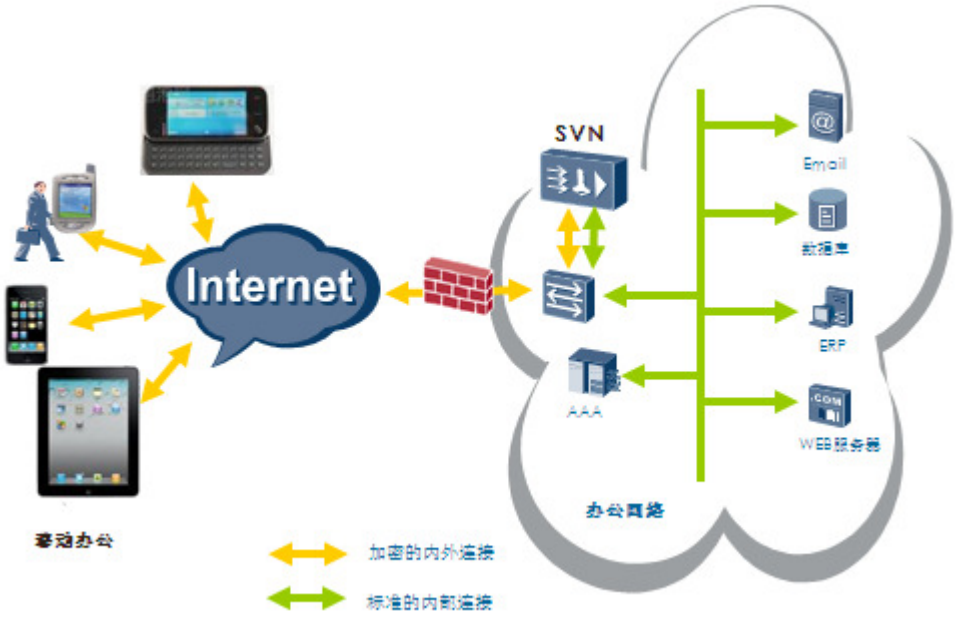
SVN2000系列包括SVN2300和SVN2260两个型号，均为模块化设备，服务中小型企业，应用于移动办公、远程接入、合作伙伴接入、分支机构互联等安全接入场景。

SVN5000系列包括SVN5530、SVN5560两个型号，均为模块化设备。服务中型企业，应用于移动办公、远程接入、合作伙伴接入、分支机构互联等安全接入场景。

1.2 产品典型应用场景

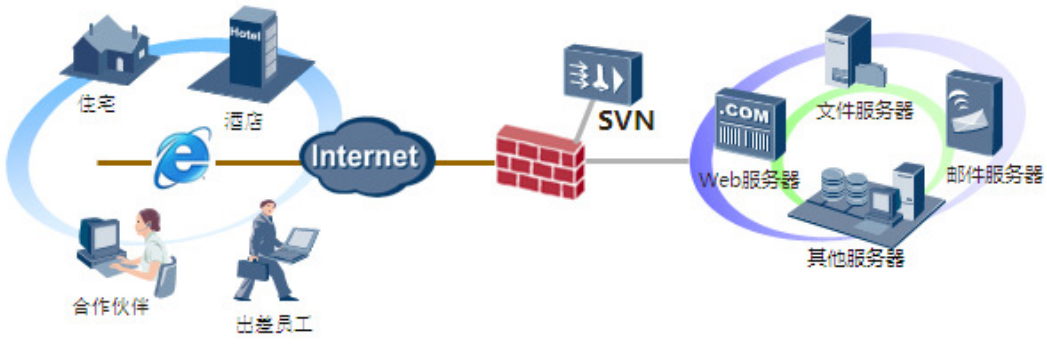
1.2.1 移动办公

在办公网络边界部署SVN2000/5000系列产品，在用户的各种智能移动终端上安装客户端软件，则用户就可以使用各种智能移动终端设备，与SVN2000/5000安全接入网关建立安全的隧道，业务数据在安全隧道内传输，同时采用身份认证技术和访问控制技术，这样就确保了用户使用任意的智能终端设备都能安全的接入公司办公网络，方便及时的处理办公业务，提高了工作效率。



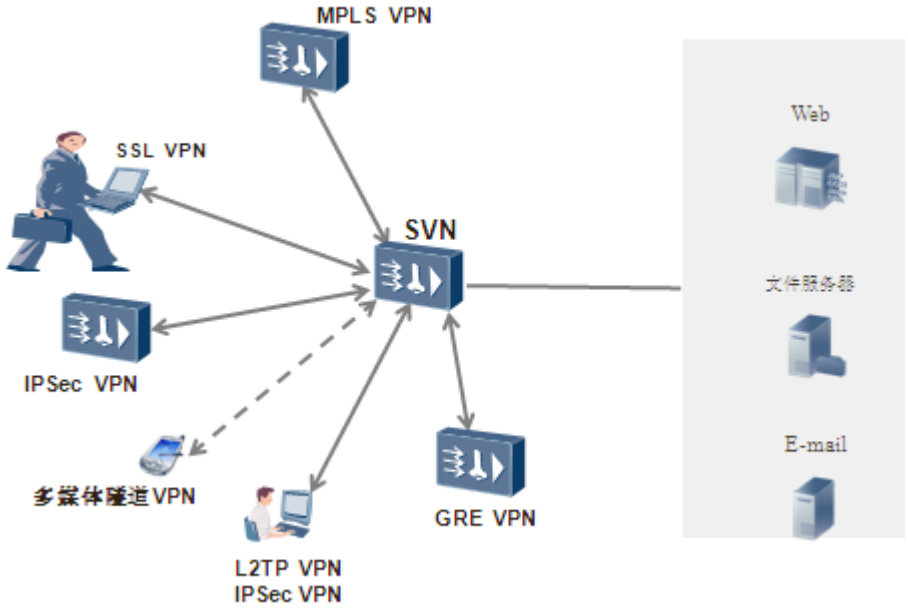
1.2.2 远程接入

营业厅系统（BOSS系统）、合作伙伴、出差员工等均可使用SVN2000/5000系列安全接入网关建立SSL安全隧道，从远程安全地接入内网，访问被授权的资源，处理业务。



1.2.3 一体化 VPN 接入

在合作伙伴和总部之间采用IPSec VPN网关模式，出差员工可以采用SSLVPN远程接入，分支机构的用户也可以采用L2TP VPN远程接入。我们的SVN2000/5000安全接入网关支持多种VPN方式同时接入。



第 2 章 产品卖点

3.1 主要评价指标

业界衡量SSL/IPSEC VPN产品主要评价的标准有以下几个方面：

- 性能
  a) 并发用户数：SSL VPN的主要指标，（IPSEC VPN指并发隧道数）
  b) 加解密吞吐量
- 业务能力（对Web资源、邮件系统（Notes）、C/S等业务的支持能力）
- 安全特性（设备自身系统安全性、对认证系统的支持、细粒度访问控制的能力等）
- 泛终端：支持的终端的类型数量

3.2 我司产品卖点

卖点 1：强大的移动办公安全接入能力

支持 Android、iOS(iPhone/iPad)、Linux、Symbian、Blackberry、Windows、MacOS 等主流平台，提供最广泛的移动终端适应性。

在移动终端上支持 Web 代理、虚拟桌面、SSLVPN 的 L3 VPN、L2TP/IPSec VPN、安全 SDK 组件与应用集成的安全接入方式，用户可以灵活选择适合自己的方式使用。

卖点 2：完备的整体安全防护

采用主机检查、访问痕迹清除和安全桌面技术，确保用户终端设备的安全。

丰富的身份认证和灵活的授权管理，提供基于 IP、端口、URL 的细粒度访问控制，保证了用户访问的可控可管。

采用高强度的加密算法和摘要算法，保证用户数据的传输安全。

安全的 OS 系统、强大的防火墙和专业的 Anti-DDos 功能，保证了网关设备自身的安全。

卖点 3：多年市场验证的电信级软硬件平台

采用数据压缩和传输优化技术，提供卓越性能和大容量用户的并发访问能力。

支持双机热备和链路备份技术，提供电信级设备、链路可靠性，确保用户业务长期稳定运行。

采用低功耗的硬件设计和功耗智能调节技术，实现了整机设备的绿色节能和低碳环保，有效降低用户的运营成本。

卖点 4：领先的虚拟化 SSLVPN 应用

采用业界领先的虚拟网关技术，最高支持 256 个虚拟 SSL VPN 网关，有效节省投资成本。

每个虚拟 SSL VPN 网关可进行独立的认证、配置与管理，方便管理员独立操作，简化维护成本，真正实现一机多用。

卖点 5：最全面的一体化 VPN

集成 SSLVPN、IPSec VPN、GRE VPN、L2TP VPN、MPLS VPN 和多媒体隧道网关功能于一体。

卖点 6：强大的 SSLVPN 业务能力

支持 Web 代理、文件共享、端口转发、网络扩展、多媒体隧道功能。

支持 Web 资源、C/S 应用程序资源、基于 IPv4 的资源、基于 IPv6 的资源。

支持 TLS 和 TLS+UDPS 两种隧道传输模式。

卖点 7：跨平台的开放安全 SDK

提供跨平台的安全 SDK 组件，和用户的各种应用实现无缝集成，使用户的应用能够安全访问业务资源。安全 SDK 面向第三方厂商和用户都是开放的，第三方厂商和用户可以快速集成，提升产品安全性。

支持 Android、Windows、 iOS(iPhone/iPad)、Linux、Symbian、Blackberry、MacOS 等主流平台，用户不需要考虑跨平台问题，易于使用。

第 4 章 销售状态

4.1 入网/测试情况说明

目前，SVN2000/5000已获得《计算机信息系统安全专用产品销售许可证》。

第 5 章 销售注意事项

5.1 关于终端的支持

采用web代理功能时，SVN2000/5000可以支持任意具备浏览器功能的终端。

采用网络扩展功能时，SVN2000/5000可以支持Windows(2k/xp/2003/2008/vista/win7)、Android、MacOS。

采用安全SDK组件功能时，SVN2000/5000可以支持iOS(iPhone/iPad)、Android、Windows系列(2k/xp/2003/2008/vista/win7)、Linux、Symbian、Blackberry、MacOS。

	Windows（2K/XP/2003/2008/Vista/win7）	iOS	MacOS	Android	Linux	Symbian	Blackberry
安全 SDK	√	√	√	√	√	√	√
Web 代理	√	√	√	√	√	√	√
端口转发	√	×	×	×	×	×	×
IPSec 客户端接入	√	√	√	√	√	√	√
安全桌面	√	×	×	×	×	×	×
网络扩展	√	×	√	√	√	×	×
文件共享	√	√	√	√	√	√	√
虚拟桌面	×	√	×	√	×	×	×

5.2 关于并发用户数 License

SSLVPN应用情况下，需要申请并配置SSL VPN并发用户数；

IPSec VPN应用情况下，需要申请并配置IPSec VPN并发用户数；

设备运行中SSL VPN并发用户数、IPSec VPN并发用户数之和不能超SSL VPN最大并发用户数；

IPSec VPN并发用户数未收费，由一线销售控制，决定是否赠送客户，以及赠送多少数量，IPSec VPN正式license需要申请。

设备出厂时，各类并发用户数都随主机带了10个，这10个并发用户数仅仅是为了客户体验和测试用的。当客户正式购买了我们license的时候，这些测试用license将被覆盖。

5.3 关于加密卡

SVN5530、SVN5560已经标配了硬件加密卡，不需要再单独配置。

5.4 关于虚拟网关数 License

设备出厂时，赠送了一个正式虚拟网关 license，客户后续购买虚拟网关并发数，将会被叠加，不会覆盖。

5.5 配套的网管软件

销售 SVN 产品时候可以再推荐客户购买华为公司的网管平台软件。
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

第 6 章 竞争分析和竞争策略

6.1 国内市场

6.1.1 主要竞争对手

	HW	Sangfor	Array
虚拟网关	√	×	√
支持 IPv6	√	×	√
多媒体隧道	√	×	×
iPhone 上的 IPSec 接入	√	√	×
认证方式	最丰富	较多	一般
短信认证	√	√	×
资源地址隐藏	√	√	×
国内快速定制开发	√	√	×
安全桌面	√	√	√
虚拟桌面	√	√	√

6.1.2 竞争对手分析和竞争策略

1）Sangfor

深信服公司属于在国内市场做的比较早的一家公司，其SSLVPN产品在国内的应用比较广泛，目前市场排名第一，是我司SVN2000/5000系列安全接入网关的最大竞争对手。

与SVN2000/5000展开竞争的产品是VPN2050、2150、3050、3150、4050、6050、7050、7150，其产品存在以下问题：

1. X86平台，开源linux系统，安全性差
2. 泛终端支持较弱，不支持Symbian、Blackberry
3. 不支持防火墙高级功能和复杂路由功能
4. 不支持完全独立的虚拟网关功能
5. 不支持IPv6
6. 不支持MPLS、GRE、L2TP VPN
7. 不支持Flash、JavaApplet等复杂HTTP页面的Web代理

技术规格上How to beat：

1. 要求支持Flash、JavaApplet等复杂HTTP页面的Web代理
2. 要求支持IPv6
3. 要求支持完全独立的虚拟网关功能
4. 要求支持防火墙高级功能和复杂路由功能
5. 要求支持MPLS、GRE、L2TP VPN

2）Array

Array在亚太地区具有较高知名度，进入中国市场较早，长期占据中国市场前两名。

与SVN2000/5000展开竞争的产品是SPX800、1800、2000、2800、3000、4800、5800，其劣势也是十分明显的，主要有以下几个方面：

1. 不支持防火墙高级功能和复杂路由功能
2. 不支持IPSEC VPN、MPLS VPN接入
3. 单电源配置导致可靠性降低
4. 不支持终端标识码校验
5. 价格高昂
6. 不支持短信认证

技术规格上How to beat：

1. 要求支持IPSec VPN、MPLS VPN接入功能
2. 要求支持终端标识码校验
3. 要求支持短信认证
4. 提供双电源的可靠性
5. 要求提供强大的网关设备安全防护（防火墙高级功能、防范Ddos等攻击）

6.2 海外市场

6.2.1 主要竞争对手

	HW	Juniper	Cisco
虚拟网关	√	√	√
支持 IPv6	√	√	√
多媒体隧道	√	×	×
iPhone 上的 IPSec 接入	√	√	√
认证方式	最丰富	一般	一般
短信认证	√	×	×
资源地址隐藏	√	×	×
国内快速定制开发	√	×	×
安全桌面	√	√	√
虚拟桌面	√	×	×

6.2.2 竞争对手分析和竞争策略

1）Cisco

Cisco 公司 SSLVPN 产品很早进入市场，长期处于全球市场前列，是我司 SVN2000/5000 系列安全接入网关的最大竞争对手。

与 SVN2000/5000 展开竞争的产品是 ASA5520、5540、5550、5580、5585，其产品存在以下问题：

1. 不支持虚拟桌面
2. 不支持短信认证
3. 价格昂贵
4. 不支持内置 CA
5. 不支持 Web 化可视网管界面

技术规格上 How to beat：

1. 要求支持短信认证
2. 要求提供内置 CA
3. 要求支持虚拟桌面
4. 要求支持 Web 化可视网管界面

2）Juniper

Juniper 长期居于 Gartner 第一象限，解决方案能力与市场份额全面领先，长期占据全球市场第一。

与 SVN2000/5000 展开竞争的产品是 MAG2600、4610、6610，其劣势也是十分明显的，主要有以下几个方面：

1. 不支持内置 CA
2. 不支持 MPLS VPN、IPSEC VPN 网关模式
3. 不支持 IPv6
4. 不支持终端标识码
5. 价格高昂
6. 没有命令行配置方式

技术规格上 How to beat：

1. 要求支持 MPLS VPN、IPSec VPN 网关模式
2. 要求支持终端标识码
3. 要求支持 IPv6
4. 要求支持内置 CA