网神 SecSSL 3600 安全接入网关系统

技术白皮书

移动应用安全事业部

2017 年 02 月

- 版权声明

- 文档信息

文档名称	网神 SecSSL 3600 安全接入网关系统技术白皮书		
扩散范围	销售/售前/客服/渠道商/用户	文档版本号	V16.9.1
作者	杨光	日期	2016.9.1
初审人	陈蛟	复审人	陈蛟

目录

一、 产品概述

网神作为国家密码管理局批准的商用密码产品生产定点单位和销售许可单位，推出了自主研发的网神 SecSSL 3600 安全接入网关系统系列产品。该系列 VPN 安全网关采用国家密码管理局指定的加密算法，遵循国家密码管理局的《SSL VPN 技术规范》，基于成熟可靠的专用硬件平台，在保证数据通信安全的同时提供了高性能的访问控制能力，可以有效实现数据传输的安全、用户接入的安全和对内网资源的访问安全。该级别 VPN 产品已广泛应用于各类小型企业、大型企业/单位分支机构。

网神 SecSSL 3600 安全接入网关系统是以国际标准 SSL/TLS 协议为基础的、自主研发的、专为企业定制的、基于应用层设计的远程接入产品，网神 SecSSL 3600 安全接入网关系统全面支持 IPv6 安全接入，满足下一代互联网安全接入需求，为企业远程接入提供了最好的解决方案，它使传统的 VPN 解决方案得到了升华，能让用户无论在世界的任何地方，只要使用浏览器就能够访问到公司总部的资源，如 WINDOWS、LIUIX、UNIX、MAC 等系统的商业文件和应用程序，系统可以集中管理企业内部的应用布置，配置细粒度的访问策略，可以更安全地实现权限控制，可以让不同级别的用户访问不同安全级别的应用系统。

网神 SecSSL 3600 安全接入网关系统精细化访问控制技术能够使你明确而容易地定义资源安全的发布，细粒度控制接入可以到用户级、资源级-甚至下到 URL 和文件级的权限。全范围身份认证方法的支持：系统支持广泛范围的身份认证技术，包括用户名/密码、数字认证、LDAP、RADIUS、AD、数据库认证以及其它通用的多因素等认证系统。网神 SecSSL 3600 安全接入网关系统产品让用户轻松而

安全地实现远程访问，让公司的网络应用布署更灵活，同时，系统还可以为企业最大化地节约成本为企业用户提供最好的整体解决方案。

网神 SecSSL 3600 安全接入网关系统通过結合 SSL/TLS 和代理技术來减少风险终端控制技术检测、保护使用者环境，从而授权使用者的访问级别，策略执行不仅基于使用者名称，还能检测使用者环境的信任级别，可以针对那些需要特殊环境的使用者，提供最好的解决方案。

系统提供了用户自己定义界面的功能 ，用户可以根据自己的个性，定制入口界面，用户还可以把登录的 LOGO 换成自己公司的，并且，可以让不同的用户定制属于自己的 VPN 界面。

随着移动互联网的发展，网神 SecSSL 3600 安全接入网关系统在移动端融合了 EMM 产品基础功能，实现了基于应用 APP 的安全封装技术，并且通过搭建企业内网的应用商店，定向推送安全封装以后的 APP 进行到指定的用户及用户组下载安装。移动端融合安全杀毒技术，保障用户在移动办公的设备环境安全。

二、 产品特色

网神 SecSSL 3600 安全接入网关系统为一款安全远程接入 VPN 的解决方案。它在允许远程访问的同时，实现了如上所述的种种安全功能，包括：

- 对 PC\移动用户进行统一的身份进行认证管理。
- 根据管理员定义的安全策略和客户端的安全状况，对用户进行授权。
- 检测远端用户接入设备的安全状态。
- 保证远端用户同内部网络的通信安全。
- 实时监控远程接入的安全连接。
- 云端接入解决方案保证云端通信安全。
- 软 Token 保证认证信息不被泄露。
- 移动终端管控，实现 MAM、MDM、MCM 三合一，保证数据
- 移动端 APP 安全封装技术，无需企业二次开发快速集成 VPN 功能。
- 移动端企业内部安全应用商店，保障合法白名单的应用定向推送用户。
- 移动端安卓设备安全杀毒功能，保障终端安全办公环境。

与此同时，考虑到网神 SecSSL 3600 安全接入网关系统作为一个网络安全设备在网络中部署的便利性，对各种不同的网络环境的适应性以及用户使用的安全便利性，系统提供了双机备份、多 ISP 接入、客户端智能选路等网络适应能力。同时，为了便于管理和审计，系统提供了灵活的用户管理方式和方便的日志管理功能。

2.1 业务连续性&安全性

2.1.1 全面防止中间人攻击

中间人攻击（Man-in-the-MiddleAttack，简称“MITM 攻击”）是一种“间接”的入侵攻击，这种攻击模式是通过各种技术手段将受入侵者控制的一台计算机虚拟放置在网络连接中的两台通信计算机之间，这台计算机就称为“中间人”。简而言之，所谓的 MITM 攻击就是通过拦截正常的网络通信数据，并进行数据篡改和嗅探，而通信的双方却毫不知情。

为了防止用户在登录业务系统时遭到中间人攻击，网神 SecSSL 3600 安全接入网关系统采用二维码认证/动态口令认证等方式。该认证方式采用独立 app（360ID）、硬件设备（ITS）进行认证。认证过程中，通过手机获取二维码信息/动态口令信息，该信息直接发送到 ITS 中，ITS 与安全接入网关系统直接在企业内网进行交互、确认，认证通过后，用户才可访问业务系统。该方式对认证信息进行了二次验证和确认，且认证信息采用独有编码方式进行加密，做到一人一机，黑客即使拦截到认证信息，也无法进行身份仿冒、信息截取和嗅探。

2.1.2 多种业务访问模式

企业的远程接入解决方案面对的是不同要求的客户，例如：需要给自己内部的员工提供对一些关键应用的访问服务，需要让 IT 人员能够通过其进行网络管理，需要为合作伙伴开放某一个专门的受 SSL 保护的 Web 服务等。因此，为了满足不同的远程访问要求，网神 SecSSL 3600 安全接入网关系统为远程用户提供如下六种接入模式：

代理服务（Proxy）

代理服务（端口转发模式）可以帮助企业，实现任意基于 TCP 的应用延伸到 Internet 可以到达的地方，从而实现移动办公。

网络连接（Network Connection）

网络连接（虚拟网卡模式）方式可以使远程访问用户，访问企业内部网络的任意资源，可以帮助 IT 人员对企业网络实现远程维护或者部署一些 VoIP 服务。

安全桌面（VSD）

系统为用户提供了一种安全的桌面服务 ,能够保证用户在远程接入环境下使用时其访问的应用数据在 PC 端的安全加密的存储空间运行，确保终端数据防泄漏。参见 3）详细介绍。

远程业务发布（WSDP）

系统具有远程应用发布功能，实现快速将 C/S 模式的资源 B/S 化。远程应用接入采用基于服务器计算的应用模式，应用程序的安装、配置、管理、维护以及应用的执行均集中在服务器上进行，用户通过远程客户端登录服务器操作，输入输出内容（键盘输入、鼠标移动、运行结果在屏幕上的显示输出）则通过网络传输到客户端。安卓、IOS 操作系统的智能终端只需要安装网神云桌面客户端，即可满足用户移动办公的需求。参见 4）详细发布。

目的地址映射（DNAT）

顾名思义，DNAT 可以为企业提供网络层的服务映射，使得企业可以通过网神 SecSSL 3600 安全接入网关系统对外提供一些开放的服务。

虚拟服务（Virtual Service）

虚拟服务可以在系统上，为用户提供基于 SSL 加密的服务代理，这种应用模

式可以保护企业的一些公开访问服务。

2.1.3 业务平滑对接

适用于 windows 操作系统的业务系统，无缝迁移到移动端（安卓和 IOS），并且不需要客户二次开发。并且某些 C/S 的系统架构在互联网中应用，面临最大的问题就是兼容性和响应效率问题。不少 C/S 模式的系统，对安装移动终端的系统环境有着特定的要求；而在系统运作过程，客户机和服务器之间也需要反复传输数据和指令，这在互联网上容易被带宽以及线路的稳定性所影响。

网神 SecSSL 3600 安全接入网关系统具有远程应用发布功能，实现快速将 C/S 模式的资源 B/S 化。远程应用接入采用基于服务器计算的应用模式，应用程序的安装、配置、管理、维护以及应用的执行均集中在服务器上进行，用户通过远程客户端登录服务器操作，输入输出内容（键盘输入、鼠标移动、运行结果在屏幕上的显示输出）则通过网络传输到客户端。这样模式的好处：

a) 软件的客户端也是安装运行在服务器上的，因此对客户端的运行环境就没有相关的要求限制，可以不用满足原来客户端要求的特定环境，也可以不要求客户端拥有比较高的硬件配置要求；

b) 由于传输内容不包括应用数据，因此可大大降低网络数据传输量；

c) 网神的远程应用发布技术与 VPN 技术集成后，可为远程应用接入提供一个更加安全、更加完备的远程应用发布解决方案。

2.1.4 双机互备&负载均衡

网神 SecSSL 3600 安全接入网关系统作为提供远程接入解决方案的门户，必

须提供高可用的服务。系统支持双机热备，可以提供主从、主主两种业务模式。系统的 HA 功能，可以在不同的型号之间实现 HA，只要软件版本相同即可，这样可以使用户既可以提供高可用性，也可以节约用户的投资。

在主从模式下，两台网神 SecSSL 3600 安全接入网关系统构成一个 HA 对，其中只有主设备会对远程用户提供服务。两台设备上的接口可以对应形成一组，每一组接口可以使用一个浮动 IP 地址（Float IP），该浮动 IP 地址即为远程用户的访问地址，管理员可以通过浮动 IP 地址，也可以通过接口地址来访问系统进行管理。两台设备中只有主设备拥有浮动 IP 地址，即如果访问浮动 IP 地址就是访问了主设备。在 HA 的主从模式下，管理员可以在任意一台设备上进行管理，其管理动作的结果将同时作用在两台设备上，从而实现设备间配置的同步。对从设备的管理只能使用接口地址。

在主主模式下，构成 HA 的两台设备都会对远程用户提供服务。同样可以为每组接口提供一个浮动的 IP 地址，用户可以通过这个浮动 IP 访问系统，客户端能够根据两台设备的负载情况，自动地选择其中一台作为服务。并能够根据链路质量的变化和设备的负载情况动态切换。当系统是经过防火墙/NAT 设备映射访问时，则客户端不能访问设备的接口 IP 地址，而是智能地访问映射地址。这就是在主主模式下，可以选择为系统配置 MAP IP 的原因。

2.1.5 满足基于 IP 协议的需求

企业内部有时需要部署一些诸如 VoIP 的业务系统。这些应用需要使用一些动态的端口，而且需要任意两个端点之间可以通信。这就要求通过远程接入的用户需要能够被动地被他人访问，这是一般的网神 SecSSL 3600 安全接入网关系统

的代理方式和 Web 转换方式无法满足的。

针对这种情况，网神 SecSSL 3600 安全接入网关系统提供了网络连接访问方式。客户端登录系统之后，实现了客户端同 Intranet 之间网络层面的互连，客户端可以从服务器上获取 Intranet 的 IP 地址。从逻辑上看，远程客户就好像是在企业内部网络一样，因此网络连接访问方式可以承载任何基于 IP 的应用。

同时，系统可以实现在网络连接基础上的细粒度的访问控制，可以根据角色来实现对不同用户访问不同服务的控制。在精细控制的基础上，系统还可以允许通过网络连接登录用户之间的相互访问，使得系统真正为远程用户提供了局域网应用体验。

2.1.6 WSDP 协议优化

智能终端用户通过 WSDP 实现内部各种应用系统业务交付。网神 WSDP 协议是网神的通过优化 RDP 协议而来，其传输速度是 RDP 的 2 倍以上，其压缩率达到 60-70%。

2.1.7 移动应用单点登录

网神 SecSSL 3600 安全接入网关系统预留可扩展的移动应用单点登录模块，在移动办公系统逐渐增多、各个系统间用户名/密码不同的情况下，为用户提供企业应用一键单点登录的功能，免除用户 反复多次输入繁琐的用户名密码的麻烦，提高用户对单位 IT 部门的满意度。

2.1.8 良好的网络适应性

网神 SecSSL 3600 安全接入网关系统在网络部署上具有高度的灵活性和适应性，不会影响用户的网络部署，不需要改变用户的网络配置，特别是支持代理穿越和域名解析功能。

系统服务的配置和客户端的访问均可以支持域名方式，方便用户服务理解和管理。即使用户没有部署域名服务器，也可以通过系统内置的域名解析功能，手工添加或者导入用户定义的域名、IP 地址对。

2.2 数据保密性&完整性

2.2.1 安全桌面实现数据终端无痕

网神 SecSSL 3600 安全接入网关系统安全桌面功能采用沙箱技术来实现。

A、启用安全桌面

认证结束后，在计算机终端自动开启一个虚拟的办公环境，对于终端客户来说是呈现出一个新的桌面，称之为安全桌面。在这个安全桌面内，操作性和原本的默认桌面是一致的，所以用户可以在安全桌面内保持其原有的操作习惯。在安全桌面中访问业务系统，并且其它相关的办公软件，如 office、CAD 等办公软件采用沙箱技术来实现都可以正常使用。

B、数据安全规范

安全桌面内所有客户端信息只能放在安全桌面中进行编辑、查看等操作、无法把各种业务数据拷贝到默认桌面，无法使用各种外设进行拷贝，并无法通过截屏、录屏等方式获取业务系统中的资料。

C、访问记录

在安全桌面内进行的访问在严格的监管和监控之下，独立的数据中心记录用户访问的时间、访问资源等信息。

D、安全桌面退出，自动清除所有遗留文件

业务系统访问完毕之后，退出安全桌面，安全桌面内遗留的业务文件，将会被自动清除，留在原有硬盘文件中的系统信息，也会被自动清除。

2.2.2 移动终端数据安全

移动终端数据落地加密，移动终端落地数据采用 AES256 加密算法，防止终端数据被拷贝出去而造成数据泄密。

移动终端数据远程擦除，当移动终端丢失后，可对移动终端进行远程数据擦除，防止数据泄密。

移动终端隧道控制策略，实现移动终端连接 VPN 以后，移动终端数据只能走 VPN，不能访问互联网，从而实现防止数据泄密。

2.2.3 国密算法

为了满足“国产”信息安全的需要，网神 SecSSL 3600 安全接入网关系统完整支持国密办算法，包括 SM1、SM2、SM3、SM4。

2.2.4 虚拟工作区

同一移动终端设备上既有个人应用，又有企业数据和应用，个人应用可以随意访问、存 取企业数据，企业应用同样也会触及到个人数据。为此防止工作区的

数据遗落到个人数据区，所以采用虚拟工作区进行数据分立。

2.2.5 协同办公（与蓝信配合）

网神 SecSSL 3600 安全接入网关系统具有即时沟通功能：垂直沟通更快捷，横向沟通更流畅；企业信息实时推送，任意时间、任意地点、安全可靠随时办公（发起电话 会议、视频会议、访问 OA 系统等）。

2.3 终端安全&适用性

2.3.1 移动终端接入访问

对 IOS、Android 等系统移动智能终端设备提供完美的支持，提供相应的 VPN 接入 APP，并且会根据终端设备的类型调整登录界面，为用户提供最好的显示效果。

2.3.2 硬件绑定

远程接入用户可以通过能够使用的任意主机，尝试接入企业内部网络，这些主机可能是用户公司所配置的，也可能是由机场或饭店等机构提供的公共主机。由于公司私有主机一般比公共主机配置了更加完备的安全策略，因此，用户使用已知的可信主机接入企业，是保证网络安全的更好选择。

网神 SecSSL 3600 安全接入网关系统支持硬件绑定功能，强制用户只能从指定主机接入企业内网才能够成功。接入主机的高可信度提高了远程接入的安全性，同时，在确认该主机安全的情况下，也绝对防止了非法用户盗用用户账号后，从

其他主机访问企业的非法行为。

系统还将硬件绑定细分为三种模式，在不同模式下，用户拥有不同的取消绑定或重绑定能力，从而满足了企业不同安全级别的需求。

2.3.3 国产操作系统

支持国产化中标麒麟操作系统客户端 APP，在 Linux 系统平台下不依赖火狐浏览器，具备独立的 SSLVPN 客户端。

2.3.4 MAC 系统 APP

支持 MAC 操作系统，并采用安装网神 SecSSL 3600 安全接入网关系统专业 APP 安全访问业务系统，提升客户的易用性。

2.3.5 智能终端杀毒

网神集成移动终端杀毒引擎，保障移动终端免受病毒木马侵扰，避免移动终端被攻击者利用成为渗透企业内网的跳板。拥有完善的病毒防护体系，不但查杀能力出色，对于新生病毒和恶意软件也能够第一时间进行防御，为用户的移动设备提供严密保护。

2.3.6 移动应用检测

移动终端的不断发展，移动应用越来越广泛，移动应用安全成为焦点。网神 SecSSL 3600 安全接入网关系统可对移动应用在封装和分发到移动终端之前进行安全监测，以保障移动应用安全。

2.3.7 移动应用安全加固

由于 Android 操作系统的开源特性，导致 Android 应用程序极大可能被他人反编译、恶意篡改、二次打包等，不仅给开发者带来名誉和金钱上的损失，还可能成为恶意程度的传播载体，使应用的用户遭受恶意广告骚扰，隐私信息窃取甚至资金被窃取。

为了保护 APP 应用不被非法篡改和二次打包，确保其自身代码的安全，我们与 360 企业级移动应用加固服务进行强强联合，基于 360 核心加密技术，给安卓应用进行加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁，同时给应用提供数据加密、签名校验、防内存修改、完整性校验、应用安全检测等保护。

2.3.8 移动应用封装

应用 APP 成为市场的主流，为了保障应用的安全及不改变客户的使用习惯，减少客户的工作量和提升工作效率，网神实现应用封装功能，把应用 APP 与网神 APP 进行封装，展现出来的体验是应用的体验，完美的解决了客户的需求。

2.3.9 移动应用商店

应用封装完成新的 APP 如何展现在客户的智能终端上？客户的应用 APP 有很多如何根据不同的人员属性来开放应用 APP？网神应用商店解决了这样的问题。通过网神的应用商店可以根据不同的人员属性来推送不同应用 APP，包括封装好的 APP。

2.3.10 智能准入控制

智能终端准入控制是根据终端杀毒扫描结果、终端是否 root/越狱结果来决定是否允许登录。

2.3.11 情景感知授权

情景感知授权是根据终端杀毒扫描结果、终端是否 root/越狱结果来决定给予不同用户组及用户访问不同资源的权限。

2.3.12 移动终端管理

- 移动终端外设管理

为了保障数据安全性，需要对移动终端的外设进行控制管理，如摄像头，防止在某些环境下造成数据的泄露。

- 移动终端密码策略管理

为了保障移动终端安全，防范因为密码简单而造成的损失，需要对移动终端的密码强度进行管理，加强密码复杂度和难度。

2.3.13 客户端安全检查

网神 SecSSL 3600 安全接入网关系统作为远程接入设备延伸了企业网络的边界，使得远程接入的用户可以访问内部的应用或者整个网络。因此，远程用户的计算机的安全要求，必须符合企业的安全策略，以避免因为远程计算机上的安全漏洞导致整个内部网络受到攻击。因此，确保远程接入到企业内部网络的用户终

端上的安全措施，能够满足企业的安全策略要求，成为了确保企业整体系统安全的一个重要环节。

系统支持基于用户的终端安全检查和缓存清除，可以根据管理员的设定，检查远程计算机上是否安装了合适的防病毒软件、是否存在间谍软件、是否开启了不该开启的网络应用等。系统还可以根据管理员的定义清除指定的文件夹。这种灵活的终端安全措施，可以帮助企业实施自己的终端安全策略，确保企业信息系统的安全。

2.4 接入&认证多样性

2.4.1 独创二维码/动态口令二合一

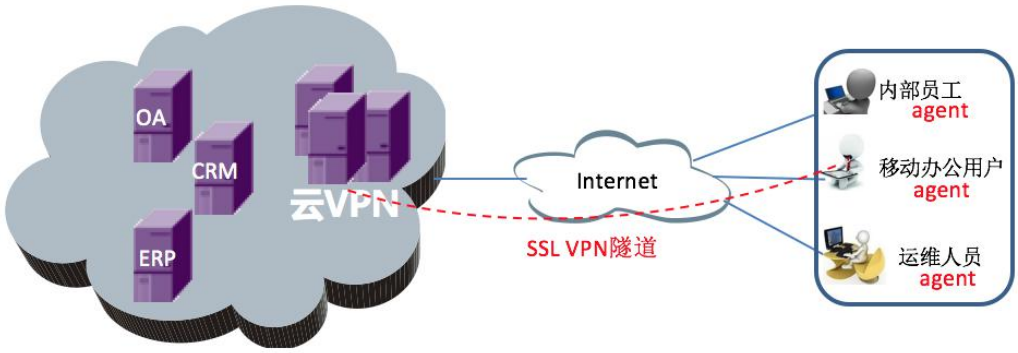
为了客户独购买硬件 Token、Token 认证服务器的成本，网神 SecSSL 3600 安全接入网关系统独创 360ID（软 token）。360ID 以软件 app 形式部署在移动终端产品中，并通过模块化的 license 控制植入在硬件 VPN 中。360ID 可适用于 Android、iOS 系统，通过 app 安装方式部署在手机、平板等移动设备中。360ID 中动态口令/二维码采用“时间+密码”的校验方式，保证动态口令/二维码的时效性和准确性，防止数据被窃取、窃听、篡改，保障数据安全。

2.4.2 云端无缝接入

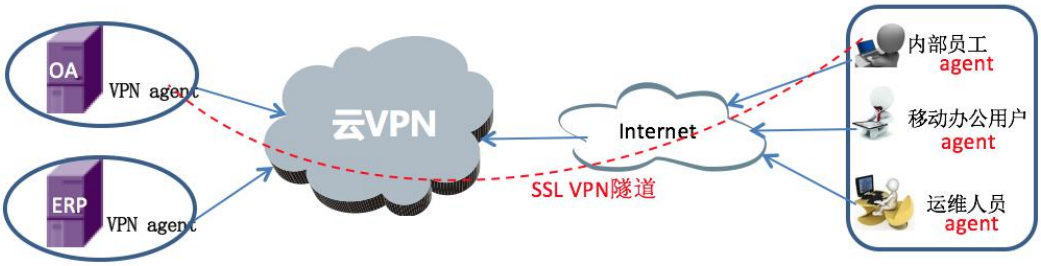
网神云 VPN 产品由云客户端、云 agent、网神云 VPN 中心组成，根据客户业

务形态，公有云和私有部署，网神云 VPN 具备两种部署方式：

第一种业务公有云形态，采用云客户端+网神云 VPN 中心



第二种业务私有部署形态，采用云客户端+云 agent+网神云 VPN 中心，



2.4.3 IPv6 远程接入

为了满足客户 IPv6 网络远程用户接入的需求，网神 SecSSL 3600 安全接入网关系统已经完全满足并做到以下特点：

产品自身支持基于 IPV6 的网络配置和管理 ,可以无缝的部署在 IPV6 网络中；

产品支持 IPV4 和 IPV6 客户端的代理和 NC 模式实现网络安全接入，支持双栈工作和 IPV4 和 V6 之间的协议转换；

产品可以同时发布工作在 IPV6 和 IPV4 协议之上的应用服务；

产品可以与工作在 IPV6 协议上的认证服务器和日志服务器配合工作。

2.4.4 适应不同类型客户使用环境

网神 SecSSL 3600 安全接入网关系统提供的远程接入解决方案，能够让用户从各种不同的计算终端上访问企业内部网络，不仅包括 Windows XP/Win7/win8 等通用的 Windows 平台，同时支持各种通用的 Linux 平台、MAC 平台。

系统支持移动终端用户采用 360Connect app /L2TP over IPsec/PPTP 等模式安全接入到 VPN 中，实现了智能手机、Pad 的安全远程接入。

系统的这种跨平台特性，为用户提供了方便的访问特性，极大地满足了用户的移动性需要。

2.4.5 多 ISP 接入支持

远程用户可能从不同的 ISP 接入到 Internet，因此，如果网神 SecSSL 3600 安全接入网关系统设备不能提供连接多个 ISP 的功能，那么就可能使得从不同运营商接入的客户具有不同的系统连接体验，甚至出现不能访问系统的情况。

为了解决这个问题，就要求网神 SecSSL 3600 安全接入网关系统设备能够同时连接多个 ISP，为客户提供多个可以连接的 IP 地址。但是远程客户往往不能判断自己应该使用哪一个 IP 地址，因此，网神 SecSSL 3600 安全接入网关系统需要能够根据客户的接入情况，智能地选择接入 IP 地址。

系统支持多 ISP 接入的功能，可以解决该问题。系统的每一个接口，可以标注为 Internal 接口或者 External 接口。如果为 External 接口，那么就可以为该接口指定默认网关。如果有多个 External 接口有默认网关，那么就可以实现连接多个 ISP。同时，网神 SecSSL 3600 安全接入网关系统的客户端组件，能够

从系统获取有多少个 IP 地址是可以使用的，并根据各个 IP 地址不同的连通性情况来决定使用哪一个 IP 地址作为连接地址，从而保证远程用户能够得到很好的使用体验。

2.4.6 L2tp over IPSec 的接入方式

网神 SecSSL 3600 安全接入网关系统通过 L2TP over IPsec 的模式接入 IOS 和 Android 客户端。这种接入方式主要应用于客户的业务系统专门针对于 IOS 和 Android 开发客户端，通过智能终端与系统建立隧道，然后通过业务客户端访问业务系统。

2.4.7 PPTP 的接入方式

网神 SecSSL 3600 安全接入网关系统通过 PPTP 的模式接入 IOS 和 Android 客户端。这种接入方式主要应用于客户的业务系统专门针对于 IOS 和 Android 开发客户端，通过智能终端与系统建立隧道，然后通过业务客户端访问业务系统。

2.4.8 360Connect APP 的接入方式

网神 SecSSL 3600 安全接入网关系统对于智能终端用户，支持安装安卓、IOS 的网神 360Connect APP，实现安卓手机、安卓 PAD、IOS 手机、IOS PAD 的移动办公。这种方式可以避免用户安装各种应用系统的移动客户端，减少用户开发投资以及降低移动办公的复杂度。

网神 360Connect APP 支持五种方式：

第一种：虚拟化 WSDP 协议来实现，通过传输客户端图像和坐标来实现数据

的传输，这种方式需要远程应用发布服务器一起来实现。

第二种：通过 NC 方式来实现，网神 360Connect APP 使得智能终端和网关之间建立一个加密通过，然后应用 APP 访问应用服务器实现业务访问。

第三种：通过代理方式来实现，客户的应用是纯 WEB 的登陆方式，网神 360Connect APP 内置浏览器可对业务进行安全访问。

第四种：提供 360Connect APP SDK 包给应用 APP 厂商，让应用 APP 厂商把 360Connect APP SDK 结合进去，实现二者无缝结合从而实现应用访问。

第五种：提供应用 APP 安全封装功能，管理员只需要 3 分钟即可自助完成 APP 集成网神 360Connect APP SDK 的功能，不改变用户使用体验。详见 29)。

2.4.9 多认证方式任意组合

网神 SecSSL 3600 安全接入网关系统作为远程接入解决方案，可以把用户局域网络的边界延伸到 Internet 可以到达的地方。那么接入终端用户的安全性，将可能影响到整个企业网络的安全性。因此，保护用户登录口令的安全将至关重要。

为保障用户口令的安全，系统提供如下多种措施：

支持本地用户名/密码认证 提供基本的身份认证方式，可利用此方式为基石与其他认证方式结合。

支持数字证书认证并提供安全接入平台系统设备自建 CA 中心功能 提供自建 CA，可极大的降低企业使用成本并可与第三方 CA 体系进行结合。

提供基于安全接入平台系统接入终端的硬件鉴权 支持自动审批，并支持多对多绑定策略，有效防止非法终端接入。

支持短信网关认证可帮助企业轻松实现双因素认证，提高身份认证安全级别。

与第三方认证体系的无缝集成 可与 LDAP，Microsoft AD，RADIUS 等第三方认证体系进行无缝集成，便于接入人员身份的统一管理。

支持动态令牌认证进一步提升身份认证安全性。

多种认证方式组合可实现多种认证方式组合，为企业提供最安全的组合认证手段。

帐号绑定实现了安全接入平台系统帐号与访问资源帐户对应绑定，增强了认证强度。

LDAP 认证加密 在 LDAP 认证中，保证用户敏感信息不泄漏。

提供软键盘和图形码验证功能 可以有效的避免安全接入平台系统设备受到恶意软件的骚扰。

用户密码保护功能 首次登陆强行修改密码，限定密码位数并进行密码过期前提示，多少天后强行修改密码，有效降低密码被破解风险。网神 SecSSL 3600 安全接入网关系统的多种用户口令保护措施，有效地保护了远程用户的口令的安全，从而保障了企业的远程接入的安全性。

2.4.10 自助注册管理

部署安全接入平台系统需要为每一个使用者分配用户账号和访问密码，这对于管理员而言是一个重复、繁琐的工作，网神 SecSSL 3600 安全接入网关系统创新的为用户提供一种用户自注册服务，实现了用户按需注册，指定人员审批的用户添加模式。在大型企业采用这种方式部署安全接入平台系统能够最大化的降低管理员的管理符合，提高产品的部署效率。

2.4.11 多因素身份认证

本地认证、数据库认证、短信网关认证、Ukey 认证、动态口令认证、邮箱认证、AD 域认证、LDAP 认证、RADIUS 认证、数字证书认证、OCSP 认证、HTTP 认证及多因素认证等。可以将其中任意 4 种方式组合启用，并且配合硬件特征码绑定策略组合使用，满足客户特定应用场景的强身份认证需求。

2.5 设备易管理&自安全

2.5.1 二维码扫描下载

支持 Android 系统 APP 提供二维码扫描下载，可以把生成的二维码提供给相应用户，用。扫描即可下载安装 APP。

2.5.2 系统监控及日志功能

作为企业网络的一个边界门户，网神 SecSSL 3600 安全接入网关系统除了能够对用户进行认证/授权/控制之外，还需要能够记录用户经过系统的行为，为系统审计提供数据基础。

网神 SecSSL 3600 安全接入网关系统为管理员提供详细的 Log 记录，包括终端用户的登入、登出、认证、资源访问等，管理员对系统的设置信息等。同时，系统提供基于用户和服务的 Top N 信息的统计和导出，从而方便管理员了解应用使用情况。通过 Top N 信息，管理员可以知道哪些用户使用远程接入的时间最多，哪些用户登录次数最多，哪些用户利用统传递的数据最大，哪些应用被使用得最多等信息。

网神 SecSSL 3600 安全接入网关系统还支持对 Log 的定期导出，系统可以根据管理员的设置定期地将符合条件的 Log 形成文件，并传递到指定 FTP 服务器上，便于数据的长期保存。系统也支持实时地通过 Syslog，将数据传递到外部的日志服务，便于企业对信息系统的 Log 进行统一管理。为方便管理员的审计活动，系统支持 log session 管理，将用户一次登录过程中的所有活动按照时间先后顺序整理到一个会话中，方便管理员查询、检索和分析。

同时，网神 SecSSL 3600 安全接入网关系统还支持用户通过系统访问业务后的详细日志记录，如用户访问业务后的所采取的 POST、GET 等，以及访问业务各种 URL 地址，为用户管理事后溯源和追查起到积极作用。

2.5.3 防火墙与 IPSec vpn

网神 SecSSL 3600 安全接入网关系统网关同时具备网络防火墙、IPsecVPN 功能，是史无前例的功能最丰富的安全接入平台系统网关。这些功能使得企业只需购买一台安全接入平台系统网关即可全面解决企业互联网出口的安全管理。

2.5.4 Mini 网关管理

网神 SecSSL 3600 安全接入网关系统能够对 Mini 网关进行管理，统一固件推送，在线 Mini 网关管理，并能进行策略推送实现 portal 认证。

2.5.5 多维度授权机制

网神 SecSSL 3600 安全接入网关系统授权机制以多个安全策略纬度为中心。用户登录时，会根据用户的属性查询用户的相关安全策略的分配情况，以决定授

予用户哪些服务资源，对用户的哪些服务访问采取单点登录策略，对用户的主机绑定策略，以及对用户执行哪些安全策略检查。多纬度的授权机制保证了各个安全策略能够独立制定，并分别应用在不同用户身上。

2.5.6 站点到站点的 IPsec VPN

网神 SecSSL 3600 安全接入网关系统除了可以提供远程用户接入之外，还可以提供两个网络之间的互连。该功能使得企业可以利用系统设备构建自己完整的 VPN 网络，而无需分别建设远程接入和网络 VPN。系统支持构建星型和网状的两种 VPN 网络。

2.5.7 灵活、安全的应用服务

网神 SecSSL 3600 安全接入网关系统可定义一个服务，并指定服务所在的地址、端口、服务类型、关联的客户端应用程序、是否隐藏服务、服务应用到的角色等。

在地址的定义方式上，管理员有三种选择：

完整的域名、IP 地址、主机名@IP 地址

这三种地址指定方式，可以满足多数企业应用的需求，尤其是“主机名@IP 地址”的设定方式，使得网神 SecSSL 3600 安全接入网关系统能够跟 Windows 系统应用融合在一起。

在系统的服务定义中可以添加多个端口。这种方式满足了那些在一台服务器上配置多个应用服务的应用需求，同时也可以部分地解决使用动态端口的应用系统的需要。

对于多台服务器提供同一个服务的情况，管理员一般希望只让用户看到其中的一个服务器，而不必了解具体有多少服务器在同时提供服务。针对这种要求，网神 SecSSL 3600 安全接入网关系统为每一个服务提供了一个开关。根据这个开关的设置，系统就知道该给用户显示哪个服务，而把其他的作为备份的服务器隐藏起来。

网神 SecSSL 3600 安全接入网关系统对安全的考虑也非常充分，可以针对应用服务提供内容过滤的功能，例如，针对 HTTP、FTP、Telnet，系统可以实现基于关键字的过滤，使得管理员能够更加细致地控制用户对业务系统的访问。

三、 技术优势

3.1 自主知识产权的 SecOS 安全操作系统

网神 SecSSL 3600 安全接入网关系统网关采用具有完全自主知识产权的 SecOS 安全操作系统，采用模块化的设计，实现独立的安全协议栈，消除了因操作系统漏洞带来的安全性问题，以及操作系统升级、维护对网神 SecSSL 3600 安全接入网关系统功能的影响。同时也减少了因为硬件平台的更换带来的重复开发问题。由于采用先进的设计理念，使该 SecOS 具有更高的安全性、开放性、扩展性和可移植性。

3.2 业界独创二维码/动态码认证，便捷无缝接入

网神 SecSSL 3600 安全接入网关系统独创 360ID 技术（软 token）。360ID 以软件 app 形式部署在移动终端产品中，并通过模块化的 license 控制植入在硬件 VPN 中。为客户节约购买硬件 Token、Token 认证服务器的硬件成本。

3.3 应用安全加固技术，拒绝反编译

网神 SecSSL 3600 安全接入网关系统采用多项 360 核心加密技术，对应用程序深度加密处理，独有的程序文字信息加密功能，能有效防止应用被反编译和恶意篡改和，保护应用不被二次打包，保护数据信息不会被黑客窃取。给予官方应用最强保护，从源头消灭恶意盗版应用。

3.4 全面支持 IPv6 网络 IPv6

网神 SecSSL 3600 安全接入网关系统网关全面支持 IPv6 网络，满足基于 IPv6 安全接入的需求，支持 IPv6 双栈，IPv6 Over IPv4 与 IPv4 over IPv6，支持 IPv6 协议邻居发现等。

3.5 先进的多核并行技术

采用领先的 AMP 技术，动态的对各个内核进行任务分配，每个内核之间运行一个（或一些）完整的安全引擎实例，各个实例之间无干扰式的运转。

3.6 多链路智能选路技术

网神 SecSSL 3600 安全接入网关系统的每一个接口，可以标注为 Internal 接口或者 External 接口。如果为 External 接口，那么就可以为该接口指定默认网关。如果有多个 External 接口有默认网关，那么就可以实现连接多个 ISP。同时，系统的客户端组件，能够从系统获取有多少个 IP 地址是可以使用的，并根据各个 IP 地址不同的连通性情况来决定使用哪一个 IP 地址作为连接地址，从而保证远程用户能够得到很好的使用体验。

3.7 稳定的安全桌面技术

网神虚拟安全桌面采用沙箱（沙盒）技术实现，认证结束后，在计算机终端自动开启一个虚拟的办公环境，对于终端客户来说是呈现出一个新的桌面，称之为安全桌面。在这个安全桌面内，操作性和原本的默认桌面是一致的，用户可以在安全桌面内保持其原有的操作习惯。数据较为敏感，系统所有客户端信息只能放在安全桌面中进行编辑、查看等操作、无法把各种业务数据拷贝到默认桌面，无法使用各种外设进行拷贝，并无法通过截屏、录屏等方式获取业务系统中的资料。业务系统访问完毕之后，退出安全桌面，安全桌面内遗留的业务文件，将会被自动清除，留在原有硬盘文件中的系统信息，也会被自动清除。

3.8 多种移动终端接入技术

目前移动互联已成为新的应用趋势，网神 SecSSL 3600 安全接入网关系统提供多种终端接入，通过智能终端即可方便的实现远程办公。传统的

windowsXP\7\8\10 以及 MAC 系统、国产化中标麒麟、LINUX 系统等均具备相应的客户端；对于 Android、苹果系统的智能终端，提供相应的 360Connect APP。支持使用全网接入模式和 WEB 转发模式的接入；不需要安装任何软件，直接使用智能终端的 VPN 客户端即可实现 VPN 接入。

3.9 TCP 协议优化、数据流压缩技术

网神 360Connect APP 实现应用虚拟化技术，通过传递应用画面、鼠标键盘的消息传递到移动端，通过 TCP 协议优化及数据\数据流压缩技术实现传输速率的提升以及带宽占用率的降低；

3.10 领先的移动端杀毒功能，确保移动办公终端环境安全。

移动端用户运行 360Connect 首先针对终端环境进行病毒查杀扫描，只有符合安全要求的智能终端才被授权访问业务（WEB、APP）系统。

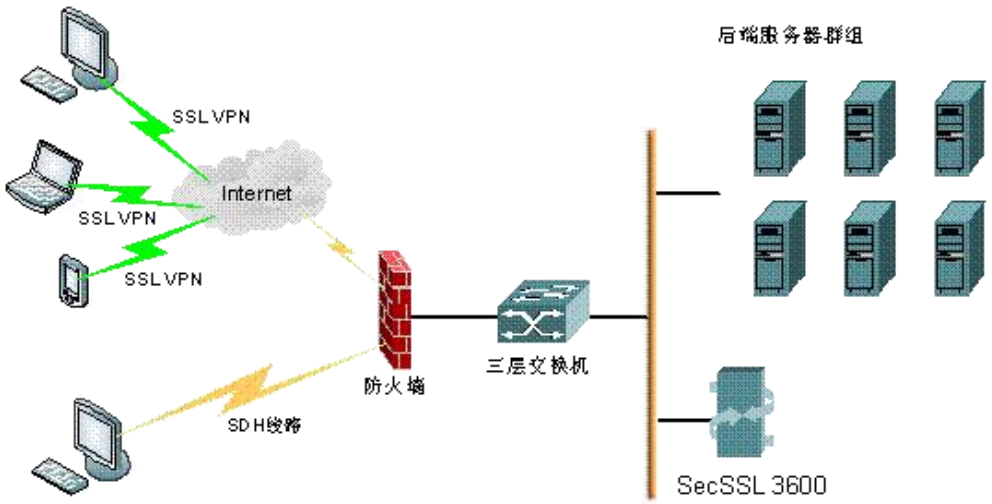
3.11 前沿的虚拟工作区技术，为业务数据提供安全隔离加密防护。

360Connect 帮助用户在不影响操作体验的前提下确保业务数据在移动端加密隔离存储，防止数据泄密。

四、 典型组网模式介绍

4.1 单机模式组网示例

单机模式为最简便的部署方式，适用于不需要区分多 ISP 的组网。一个典型的单机模式组网示例，如下图所示。



单机模式组网示例图

4.2 多 ISP 组网示例

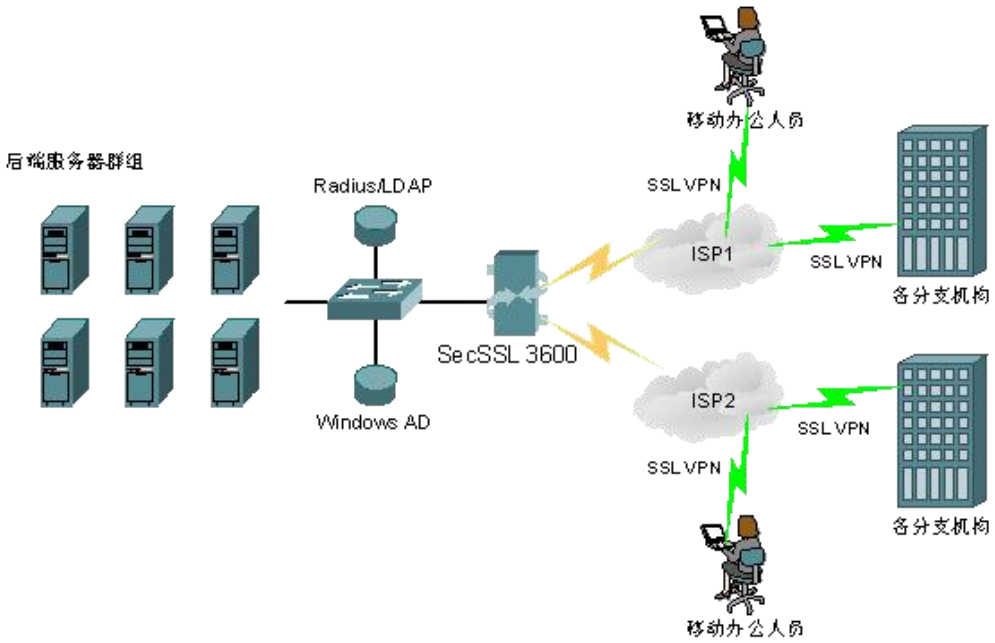
多 ISP 组网模式适用于需要区分多 ISP 的组网，以便解决跨运营商访问 SecSSL 3600 可能出现的低速和不稳定的问题。

在企业网络中，如果跨运营商直接对 SecSSL 3600 访问，可能会出现网络质量不稳定的情况。尽管 SecSSL 3600 的客户端智能可以在低速和不稳定的链路上保持连接畅通，但是有些应用因为对网络环境的要求比较苛刻，可能会导致不能使用。

为解决该问题，在 SecSSL 3600 上可以配置多个 WAN 接口，每一个接口连接

一个 ISP，再结合 SecSSL 3600 客户端的智能选路功能，从而保障了从不同 ISP 接入的客户，都能够得到良好的网络应用体验。

一个典型的多出口模式组网示例，如下图所示。



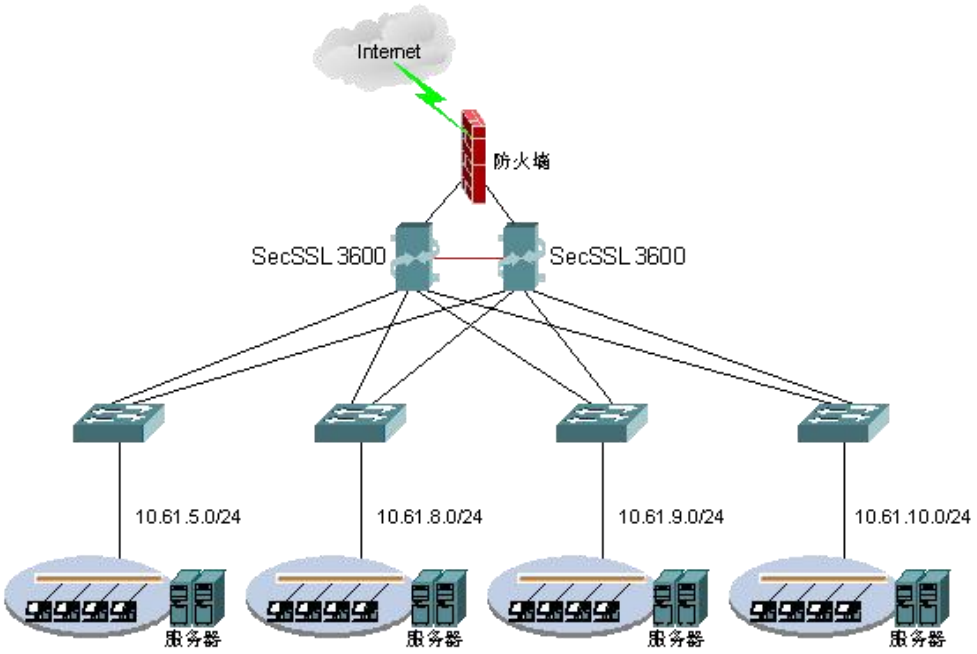
多 ISP 模式组网示例图

4.3 HA 模式组网示例

HA 模式适用于需要提供高可用性的组网，可最大程度地保证系统可靠性，确保远程用户可随时远程接入内部网络。

当按 HA 模式部署两台 SecSSL 3600 设备时，系统支持以 AA 模式和 AP 模式运行。如果两台设备以 AA 模式运行，则还可获得负载均衡后的性能提升。

一个典型的 HA 模式组网示例，如下图所示。

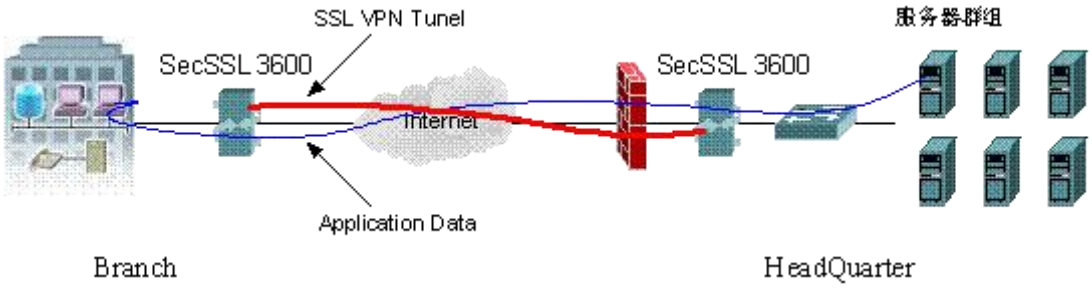


HA 模式组网示例图

4.4 Site-Site 模式组网示例

Site-Site 模式用于提供对两个分支机构之间的 VPN 连接和资源共享，使得用户只需要 SecSSL 3600 就可以构建完整的 VPN 网络。

SecSSL 3600 Site-Site 模式支持网状或者星型组网模式，而且无需考虑地址冲突和地址转换的问题。



Site-Site 模式组网示例图