**360 网神安全接入网关系统**

产品白皮书

360 企业安全集团

**目录**

[1. 引言 4](#_bookmark0)

[2. 360 网神安全接入网关系统 4](#_bookmark1)

[2.1 产品概述 4](#_bookmark2)

[2.2 产品架构 6](#_bookmark3)

[3. 产品特色 7](#_bookmark4)

[3.1 数据传输安全 7](#_bookmark5)

[*3.1.1* 隧道分离 *7*](#_bookmark6)

[*3.1.2* 国密算法 *7*](#_bookmark7)

[3.2 多样化的认证接入 8](#_bookmark8)

[*3.2.1* 独创的 *360ID* 认证 *8*](#_bookmark9)

[*3.2.2* 多因素身份认证 *9*](#_bookmark10)

[*3.2.3* 多 *ISP* 接入支持 *10*](#_bookmark11)

[*3.2.4* 跨平台兼容性 *10*](#_bookmark12)

[*3.2.5* 移动客户端接入 *11*](#_bookmark13)

[*3.2.6* 云端无缝接入 *12*](#_bookmark14)

[3.3 终端访问安全 13](#_bookmark15)

[*3.3.1* 安全桌面 *13*](#_bookmark16)

[*3.3.2* 虚拟工作区 *14*](#_bookmark17)

[*3.3.3* 终端安全检查 *14*](#_bookmark18)

[*3.3.4* 全面防止中间人攻击 *15*](#_bookmark19)

i

[*3.3.5* 集成企业级防火墙 *15*](#_bookmark20)

[3.4 保障业务连续性 16](#_bookmark21)

[*3.4.1* 多种业务访问模式 *16*](#_bookmark22)

[*3.4.2* 业务平滑对接 *17*](#_bookmark23)

[*3.4.3* 双机互备 *18*](#_bookmark24)

[*3.4.4 WSDP* 协议优化 *19*](#_bookmark25)

[*3.4.5* 移动应用单点登录 *19*](#_bookmark26)

[3.5 轻量级 EMM 19](#_bookmark27)

[*3.5.1* 移动终端杀毒 *19*](#_bookmark28)

[*3.5.2* 移动应用检测 *20*](#_bookmark29)

[*3.5.3* 移动应用封装 *20*](#_bookmark30)

[*3.5.4* 移动应用加固 *20*](#_bookmark31)

[*3.5.5* 移动应用商店 *21*](#_bookmark32)

[*3.5.6* 移动终端管理 *21*](#_bookmark33)

[3.6 运维管理强 22](#_bookmark34)

[*3.6.1* 客户端打点 *22*](#_bookmark35)

[*3.6.2* 集群 *22*](#_bookmark36)

[*3.6.3* 虚拟站点 *22*](#_bookmark37)

[*3.6.4* 集中管理 *22*](#_bookmark38)

[*3.6.5* 诊断修复工具 *23*](#_bookmark39)

[*3.6.6* 系统监控及日志功能 *23*](#_bookmark40)

[*3.6.7 Mini* 网关管理 *24*](#_bookmark41)

ii

[*3.6.8* 多维度授权机制 *24*](#_bookmark42)

[*3.6.9* 灵活、安全的应用服务 *24*](#_bookmark43)

[4. 客户收益 25](#_bookmark44)

[4.1 办公移动化 25](#_bookmark45)

[4.2 保障用户身份安全 26](#_bookmark46)

[4.3 降低采购部署成本 26](#_bookmark47)

[4.4 助力移动信息化平台搭建 26](#_bookmark48)

[5. 典型部署 27](#_bookmark49)

[5.1 单机模式组网示例 27](#_bookmark50)

[5.2 多 ISP 组网示例 27](#_bookmark51)

[5.3 HA 模式组网示例 28](#_bookmark52)

[5.4 SITE-SITE 模式组网示例 29](#_bookmark53)

iii


# 1. 引言

随着移动信息化的到来，企业由传统的业务办理模式逐渐的往移动办公模式 发展，企业员工、合作伙伴和客户可以通过移动终端对企业内部网络资源进行访 问，只要能连接上互联网， 办公人员可在任何时间（ Anytime）、任 何地点

（Anywhere）处理与业务相关的任何事情（Anything）。这种全新的办公模式， 可以摆脱时间和空间对办公人员的束缚，从而提高工作效率及远程协作能力，尤 其是可轻松处理常规办公模式下难以解决的紧急事务。

同时，这种网络连接也为企业带来了新的安全威胁，如果企业的传输中的数 据发生了篡改、或者客户数据发生泄漏的话，企业的损失将会非常严重。所以如 何保证移动办公的传输安全、数据安全和身份安全等是企业需要考虑的重中之重。

# 2. 360 网神安全接入网关系统

## 2.1 产品概述

360 网神安全接入网关系统是面向政府、企业、金融、能源、运营商等行业 客户推出的，助力企业完成移动信息化平台搭建的安全产品。该产品以保障企业 移动信息化安全为核心，在满足客户的身份认证、传输加密、访问授权、日志审 计等多种基础安全需求基础上，更加保护了移动终端设备的接入安全、移动应用 自身安全、移动应用数据安全，为客户提供移动信息化“一站式”安全办公解决 方案。

360 网神安全接入网关系统能够帮助企业实现领导、员工在任意时间、任意

4

地点，任意终端安全可靠远程办公，提供从终端到链路、再到应用的最完备的移

动办公解决方案。系统支持常见的国际通用商用密码算法，同时也支持国家密码 管理局规定的国产商用密码标准（SM1、SM2、SM3 和 SM4），保障用户业务安全。

网神具备近 10 年的 VPN 技术研发经验，自主研发的 360 网神安全接入网关 系统是 SSL VPN 和 IPSec VPN 二合一产品，具备轻量级 EMM、18 种认证对接方式、 独创软 token 和扫码登录等众多的优势功能，得到了众多行业标杆客户的认可。 产品在专用硬件平台基础上采用业界领先的安全转发引擎，提供超高并发、高安 全接入支撑，最高支持 6.5W 的并发用户，已经在众多大型客户当中稳定运行， 表现了成熟可靠的产品特性 。

随着移动互联网的发展和产品的不断的创新迭代，360 网神安全接入网关系 统在为客户解决链路加密、授权控制等问题的基础上，更融合了 EMM 功能，实现 了基于移动端应用 APP 的安全封装技术和安全加固技术。并且通过搭建企业内网 的应用商店，定向推送分发安全封装加固后的 APP 到企业指定的用户及用户组下 载安装，保障移动应用安全。

网神业内最领先、病毒样本库最全的病毒/查杀能力，产品集成了公司先进 的病毒查杀能力，可对安卓智能终端进行快速查杀，确保终端环境安全。

360 网神安全接入网关系统可提供身份令牌服务平台 ITS 与客户业务系统做 对接，在客户原有业务认证方式基础上，增加软 token 认证或者扫描二维码认证， 实现多因素认证，确保身份安全可靠，满足合规要求。

## 2.2 产品架构

产品整体方案架构如下图所示：



该解决方案架构共包含基础平台模块、基础安全模块、移动应用中心、VPN 管理中心和平台对接中心五个功能模块。

基础平台模块的设计主要结合目前新的移动互联应用趋势，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。

基础安全模块包含的主要功能有身份安全、动态双因素、精细化的访问 权限控制、数据安全、病毒/木马查杀和安全审计。

移动应用中心提供了企业移动管理功能，包括移动终端管理、移动终端 杀毒、移动应用管理、应用数据安全、移动终端准入和移动隧道安全功 能。

* VPN 管理中心支持 SSL VPN、IPSec VPN、L2TP/PPTP、虚拟化 VPN 和 MINI VPN 网关。VPN 隧道采用国密算法进行加密，支持 **SM1/SM2/SM3/SM4 国 密算法**，安全强度更高，破解难度更大。

 360 网神安全接入网关系统可与众多其他产品结合，形成“移动安全整

体解决方案”，包括有“智能终端移动办公解决方案”（天机+VPN）；“安 全 PC 办公解决方案”（天擎+VPN）；“移动协同安全办公解决方案”（蓝 信+VPN）；“安全邮件办公解决方案”（安全邮件+VPN）等，从而提供“云

+管+端”整体移动办公解决方案。

# 3. 产品特色

## 3.1 数据传输安全

### 3.1.1 隧道分离

360 网神安全接入网关系统能够将传输中的公私数据进行隔离，公司的业务 数据走 VPN 加密通道，非业务等其它数据走互联网通道。当启用隧道控制策略后， 用户接入 VPN 网络，禁止用户访问互联网。

### 3.1.2 国密算法

传输链路的安全性主要依靠 VPN 数据所采用的加密算法，360 网神安全接入 网关系统除了支持 AES、3DES、RSA 等多种国际主流的商用加密算法之外，还完 整支持国密办加密算法（SM1、SM2、SM3、SM4），保障数据传输安全。

## 3.2 多样化的认证接入

### 3.2.1 独创的 360ID 认证

360 网神安全接入网关系统使用独创 360ID（软 token）认证技术，省去了 客户单独购买硬件 Token、Token 认证服务器的成本，并且实现了动态多因子认 证，保障用户身份安全。360ID 以软件 app 形式部署在移动终端产品中，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 通过动态口令，以及易用性更高的二维码扫描和消息推送两种免密登 录的认证方式，实现了用户多因子的认证，保障了用户的身份安全。

#### 3.2.1.1 动态口令

用户通过 360ID 软件 app 从安全接入网关获取到动态口令，该动态口令在 使用 TOTP 标准协议基础上通过 SSL 进行加密，并且动态口令分发到 360ID 软 件 app 时不落地到存储中，而是暂存在内存中，保证动态口令安全性。360ID 动态口令采用“时间+密码”的校验方式，保证动态口令的时效性和准确性，防 止数据被窃取、窃听、篡改，保障数据安全。

**动态口令**

**认证确认**

**VPN设备**

**360ID**

#### 3.2.1.2 二维码扫描

二维码扫描技术作为一种全新的免密码登录方式，以智能手机为可信载体，

通过扫描 PC 端随机产生二维码进行登录。用户通过生物识别登录手机， 然后

通过扫描二维码登录业务系统, 全程不需要密码，真正做到了身份安全的可控。 不仅可有效防止木马监听键盘窃取密码，而且在用户操作体验上非常便捷。

#### 3.2.1.3 消息推送

对于移动端无法进行二维码扫码等情况，增加“一键登录”的消息确认方式 进行认证。当用户请求登录业务系统时，360ID 软件 app 会接收到一条确认登 录消息，点击确认后完成授权登录。不仅操作非常便捷，而且带外消息的方式可 以有效防止中间人攻击。

### 3.2.2 多因素身份认证

360 网神安全接入网关系统支持多种认证方式的多因素组合认证，除了支持 用户名密码方式的本地认证外，还支持证书认证、LDAP 认证、AD 认证、Radius 认证、POP3 认证、SMTP 认证、IMAP 认证、HTTP 认证、数据库认证、OCSP 认证、 360ID 认证、二维码认证、短信验证码认证、Radius 动态口令、邮箱验证码、蓝 信认证和多因素认证共 18 中认证方式。并且可以将其中任意 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。

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。

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。 多样化的身份认证方式以及组合认证方式，保障了企业用户账号的安全性。

### 3.2.3 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 360 网神安全接 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 360 网神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，360 网神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，360 网神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。

### 3.2.4 跨平台兼容性

360 网神安全接入网关系统能够让用户从各种不同的终端上访问企业内部 业务资源，不仅支持 Windows XP/Win7/win8/win10 等通用的 Windows 平台，同

时支还支持国产化中标麒麟、Linux 系统以及 MAC OS 系统，并且都具有相应的

VPN 客户端，登录后可以直接访问业务系统。 移动互联已成为新的应用趋势，360 网神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。系统支持 Android、IOS 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， 通过智能终端的 360Connect APP 即可实现 VPN 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 的移动办公需求。

### 3.2.5 移动客户端接入

360 网神安全接入网关系统对于智能终端用户，提供支持 Android、IOS 系 统的 360Connect APP 客户端，实现使用 Android、IOS 系统的移动设备的移动办 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。

360Connect APP 支持五种接入方式：

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，360Connect APP 使得智能终端和网关之间建 立一个加密通道，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，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数据加密访问。

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 360Connect APP SDK 的功能，不改变用户使用体验。

### 3.2.6 云端无缝接入

云 VPN 产品由云客户端、云 agent、云 VPN 中心组成，根据客户业务形态， 公有云和私有部署，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+云 VPN 中心



第二种业务私有部署形态，采用云客户端+云 agent+云 VPN 中心，



## 3.3 终端访问安全

### 3.3.1 安全桌面

360 网神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。

### 3.3.2 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离。个人数据与企业数 据进行隔离，落地数据加密，第三方应用或转发到其它设备当中无法打开查看。

启用虚拟工作区之后，终端数据落地加密，数据采用 AES256 或者 SM4 加密 算法，防止终端数据被拷贝出去而造成数据泄密。

当 360Connect 被卸载（或 360Connect 设备管理器服务被禁用）、设备进行 了 Root 或者设备超过一定时间不能连接上网关的情况下，移动终端数据可以远 程擦除，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。

### 3.3.3 终端安全检查

360 网神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。

### 3.3.4 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，360 网神安全接入网关系 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。

### 3.3.5 集成企业级防火墙

作为 HTTPS 服务器，所有 SSL VPN 都同样面临着 DOS 的威胁。所以大多数

SSL VPN 设备都需要前置防火墙保护其安全。而 360 网神安全接入网关系统自身

集成了企业级防火墙，具备防御 DOS 攻击、URL 过滤、QOS 限速、用户认证、应

用过滤、计费查询等防御功能。

## 3.4 保障业务连续性

### 3.4.1 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，360 网神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。

#### 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。

#### 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 360

网神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。

### 3.4.2 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（Android 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。

360 网神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) 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。

### 3.4.3 双机互备

360 网神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 360 网神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。

### 3.4.4 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 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%。

### 3.4.5 移动应用单点登录

360 网神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。

## 3.5 轻量级 EMM

### 3.5.1 移动终端杀毒

360 网神安全接入网关系统采用云查杀技术，集成移动终端杀毒引擎，对终

端进行病毒、木马的快速扫描，保障移动终端免受病毒木马侵扰，确保移动终端

安全，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。

### 3.5.2 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。360 网神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检 测，以保障移动应用安全。

### 3.5.3 移动应用封装

随着移动办公业务的快速发展，业务应用 APP 成为市场的主流，为了保障应 用安全、传输数据的安全，同时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，产品实现了应用封装功能，把业务应用 APP 与 VPN APP 进行封装， 解决移动办公场景下用户终端的 APP 数据加密传输及身份认证问题。

### 3.5.4 移动应用加固

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 能成为恶意程序的传播载体，使应用的用户遭受恶意广告骚扰，隐私信息被窃取 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，360

网神安全接入网关系统采用了企业级移动应用加固产品的技术，基于核心加密技 术，给安卓应用进行加密、加壳保护，可保护安卓应用远离恶意破解、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。

### 3.5.5 移动应用商店

通过应用商店，管理员可以根据不同的用户和用户组以及对应的权限来推送 不同应用 APP 到用户终端上，用户可以在终端上的应用商店列表直接下载安装对 应的 APP 进行使用。应用商店的 APP 的来源有两部分，一是直接从应用商店上传 的 APP，二是通过应用封装列表将已经封装成功的 APP 直接分发到应用商店。

### 3.5.6 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。

## 3.6 运维管理强

### 3.6.1 客户端打点

客户端打点功能，实现对 VPN 客户端异常中断、崩溃等情况下可以对进行数 据收集和上传，为后续分析提供必要的基础数据。此外，还能执行对 VPN 客户端 的灰度升级。

### 3.6.2 集群

新增集群功能，实现不同设备型号在负载设备的接入情况进行集群，满足大 企事业单位访问基数数量大的需求，可实现分布式集群和集中集群。

### 3.6.3 虚拟站点

虚拟站点功能，支持在 VPN 网关上建立多个虚拟站点，每个虚拟站点相互隔 离，有独立的管理界面，独立的用户、服务和策略管理，独立的域名解析。用户 只能属于一个虚拟站点，登录后只能使用所属虚拟站点的服务。虚拟站点管理页 面只能看到所属虚拟站点内的用户和管理日志。

### 3.6.4 集中管理

集中管理功能，实现对多 VPN 网关进行集中管理和策略下发，满足大企事业 单位对“互联网统一出口”要求，所有的管理员进行任何配置只能通过集中管理 进行统一配置和下发。

### 3.6.5 诊断修复工具

诊断修复工具，在 Windows 中为用户提供诊断修复工具，可以帮助用户修复 客户端环境，重置网络协议，Internet 选项，IE 设置和路由表等，也能生成网 络报告提供技术和研发人员排查问题。

### 3.6.6 系统监控及日志功能

作为企业网络的一个边界门户，360 网神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。

360 网神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，哪些用户利用传递的数据最大，哪些应用被使用得最多等信息。

360 网神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 器，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，360 网神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。

### 3.6.7 Mini 网关管理

360 网神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。

### 3.6.8 多维度授权机制

360 网神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。

### 3.6.9 灵活、安全的应用服务

360 网神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 360 网神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， 360 网神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。

360 网神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。

# 4. 客户收益

## 4.1 办公移动化

企业员工、领导可以在任意时间、任意地点、任意终端安全可靠远程办公。 360 网神安全接入网关系统提供相应的移动终端的 VPN 接入 APP，对 IOS、Android 等移动智能终端设备系统提供完美的支持。

网关系统能够结合企业管理架构，做到精细化访问权限控制，为不同职责员 工匹配不同业务应用。精细化访问控制技术能够使用户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，这样不同的用户拥有不同的访问权限，做到精细化访问控制。

## 4.2 保障用户身份安全

支持多达 18 种认证方式，任意 4 种认证方式可自由组合使用，保障用户的 身份安全。创新性提供 360ID 认证方式，该认证方式包括动态口令、以及二维码 扫描和消息推送的两种免密登录方式，确保用户身份安全可靠，满足合规要求。

通过 360ID 的动态口令提供多因子认证方案，增强应用身份认证强度，即便 是密码泄露，恶意攻击者无法获取用户的动态口令，仍然无法滥用账号访问应用 数据，同时，360ID 通过一系列的安全手段，确保其自身的安全，让攻击者无缝 可入；通过免密登录、单点登录门户方案更是从根本上杜绝了密码的使用，无密 码，就无密码泄露，达到极致的身份安全。

同时可提供身份令牌服务平台 ITS 与客户业务系统做对接，在客户原有业务 认证方式基础上，增加动态口令，二维码扫描或者消息推送认证，实现多因素认 证，确保身份安全可靠。

## 4.3 降低采购部署成本

传统的多因子认证解决方案包括硬件口令牌、UKEY 证书、短信验证码、邮 件多因子等，这些方案都依赖一个需要随时携带的硬件设备和网关服务器，其价 格不菲；360ID 作为纯软件解决方案，和硬件设备相比，以忽略不计的成本获取 更高的安全性。

## 4.4 助力移动信息化平台搭建

提供业内最完备的移动办公解决方案，从终端（PC 端、移动端）层面、到

链路层面、再到应用层面，实现“全方位”“一体化”整体解决方案。

360 网神安全接入网关系统可与众多其他产品结合，形成“移动安全整体解 决方案”，包括有“智能终端移动办公解决方案”（天机+VPN）；“安全 PC 办公”

（天擎+VPN）；“移动协同安全办公解决方案”（蓝信+VPN）；“安全邮件办公解决 方案”（安全邮件+VPN）等解决方案。

# 5. 典型部署

## 5.1 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。



## 5.2 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安全 接入网关系统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安全接入网关系统访问，可能会出现网

络质量不稳定的情况。尽管安全接入网关系统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，在安全接入网关系统上可以配置多个 WAN 接口，每一个接口 连接一个 ISP，再结合安全接入网关系统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。



## 5.3 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 模式部署两台安全接入网关系统设备时，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。



## 5.4 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 用户只需要安全接入网关系统就可以构建完整的 VPN 网络。

安全接入网关系统 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。

