360 安全接入平台

产品白皮书

移动应用安全事业部

2016 年 09 月

目录

一、 产品概述

360 安全接入平台是以国际标准 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，360 安全接入平台全面支持 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。

360 安全接入平台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。360 安全接入平台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。

360 安全接入平台通过結合 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，360 安全接入平台在移动端融合了 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、 产品价值

- 通过多年积累的远程接入解决方案经验，帮助企业高效快速的进行远程办公。
- 通过虚拟安全桌面和其他终端安全解决方案，帮助企业解决远程办公实施中的终端数据安全和准入安全问题。
- 通过 WSDP 远程桌面发布，帮助企业快速迁移传统业务系统至移动终端。
- 通过一体化的企业移动管理，帮助企业进行移动化布局，同时满足 MAM、MDM、MCM 等各方面的移动需求。
- 通过应用封装和 SDK 方式，帮助企业快速将安全接入能力整合到其自有移动业务系统。
- 通过创新的 Mini 网关接入方式，帮助企业简单快速的实现企业分支机构的安全接入和集中管理。
- 通过完整的国密算法支持，帮助企业实现 IT 合规。

三、 产品特色

360 安全接入平台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 360 安全接入平台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。

3.1 业务连续性&安全性

3.1.1 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 安全接入平台为远程用户提供如下六种接入模式：代理服务（Proxy）、网络连接（Network Connection）、安全桌面（VSD）、远程业务发布（WSDP）、目的地址映射（DNAT）、虚拟服务（Virtual Service）

3.1.2 业务平滑对接

适用于 windows 操作系统的业务系统，无缝迁移到移动端（安卓和 IOS），并且不需要客户二次开发。360 安全接入平台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。

3.1.3 双机互备&负载均衡

360 安全接入平台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。360 安全接入平台的 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。

3.1.4 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%。

3.1.5 移动应用单点登录

360 安全接入平台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。

3.2 数据保密性&完整性

3.2.1 安全桌面实现数据终端无痕

360 安全接入平台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。

3.2.2 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。

3.2.3 国密算法

为了满足“国产”信息安全的需要，360 安全接入平台完整支持国密办算法，包括 SM1、SM2、SM3、SM4。

3.2.4 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。

3.2.5 协同办公（与蓝信配合）

网神 SecSSL 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）。

3.3 终端安全&适用性

3.3.1 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。并可以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。

3.3.2 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 安全接入平台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。

3.3.3 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。

3.3.4 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。

3.3.5 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。

3.4 接入&认证多样性

3.4.1 独创软 Token

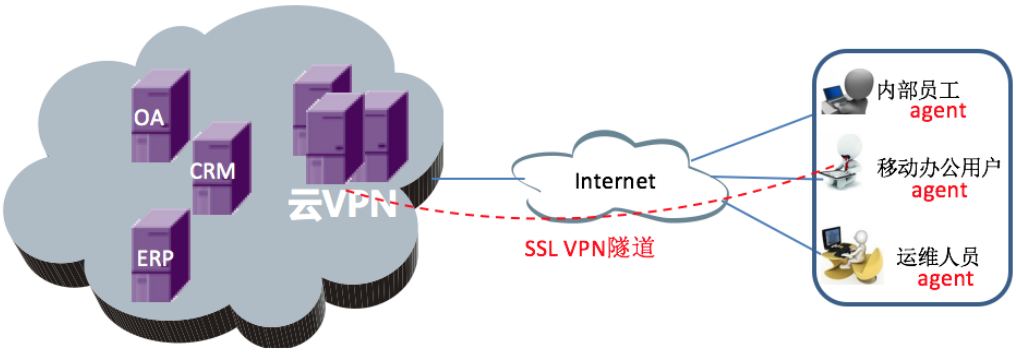
为了客户独购买硬件 Token、Token 认证服务器的成本，360 安全接入平台独创 SecToken 技术（软 token）。SecToken 以软件 app 形式部署在移动终端产品中，并通过模块化的 license 控制植入在硬件 VPN 中。360ID 可适用于 Android、iOS 系统，通过 app 安装方式部署在手机、平板等移动设备中。360ID 中动态口令采用“时间+密码”的校验方式，保证动态口令的时效性和准确性，防止数据

被窃取、窃听、篡改，保障数据安全。

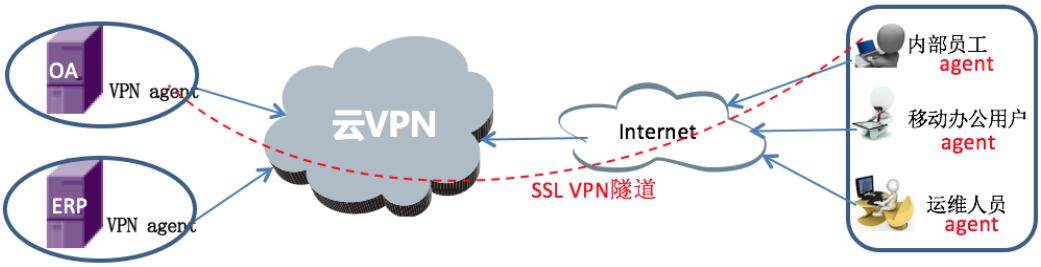
3.4.2 云端无缝接入

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，



3.4.3 适应不同类型客户使用环境

360 安全接入平台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。

360 安全接入平台支持移动终端用户采用 SecMobi 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。

3.4.4 多 ISP 接入支持

360 安全接入平台支持多 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 安全接入平台的客户端组件，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。

3.4.5 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。

3.5 设备易管理&自安全

3.5.1 系统监控及日志功能

360 安全接入平台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，哪些用户利用系统传递的数据最大，哪些应用被使用得最多等信息。

3.5.2 防火墙与 IPSec vpn

360 安全接入平台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。

3.5.3 Mini 网关管理

360 安全接入平台能够对 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。

3.5.4 多维度授权机制

360 安全接入平台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。

3.5.5 灵活、安全的应用服务

360 安全接入平台可定义一个服务，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