

网络卫士 VPN 系统

IPSec VPN 网关

产品说明



北京市海淀区上地东路 1 号华控大厦 100085

电话: +8610-82776666

传真: +8610-82776677

服务热线: +8610-8008105119

[http: //www.topsec.com.cn](http://www.topsec.com.cn)

版权声明

本手册的所有内容，其版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，天融信及其员工恕不承担任何责任。本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不承担另行通知之义务。

版权所有 不得翻印© 1995-2009 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

TopSEC®天融信

信息反馈

<http://www.topsec.com.cn>

目 录

1	产品概述	1
1.1	产品定义.....	1
1.2	产品简述.....	1
2	产品特点	3
3	产品主要功能	8
4	运行环境与标准	11
5	典型应用	13
5.1	大中型企业总部与分支机构之间构建 VPN 的解决方案.....	13
5.2	移动用户远程访问企业内部网络的 VPN 解决方案.....	14
5.3	小型企业 VPN 解决方案.....	16
6	产品资质	17

1 产品概述

1.1 产品定义

天融信 IPsec VPN 网关符合国密局最新制定的《IPSEC VPN 技术规范》，为用户基于因特网构建安全的虚拟专用网络而设计的系列产品形态。通过 IPsec VPN 产品用户可以实现总部与各个分支机构、企业与合作伙伴、移动办公人员的远程接入等多种网络互联需求，同时对这些远程网络中传输的数据提供私密性、完整性等安全防护手段。

1.2 产品简述

在信息化高度发展，电子商务、电子政务开始被企业和政府等行业普遍应用的今天，不同的分支机构之间、不同的信息系统之间有着非常迫切的联网需求，如我们经常提到的 ERP、CRM、SCM、OA、VOIP、视频等。对于企业来说，稍具规模的企业都不只具有一个分支机构，并且随着企业规模的不断扩大和业务的不断扩充，企业跨地区、跨国发展成为一种必然的趋势。同时企业中移动办公员工的数量也呈上升之势，企业之间的联系也日趋频繁、密切。政府及事业单位一直是中国信息化的先行者，政府网络的建设已经比较完善。随着“电子政务”建设的进一步深入，政府与自身各分支机构、外界相关单位信息交互的“外网”安全和互连互通就变得更为必要。政府部门的相关局、处、办、所往往遍布于城市的各区县，也经常需要与所管辖的事业单位交互信息。同时，政府人员的出差移动办公需求也日益迫切。

所有的应用，无论是企业信息化应用，还是电子政务应用，都离不开一个基本前提：都要先建立一个可以安全的、可靠的、互联互通的基础网络平台。建立这样的基础网络，传统的做法是采用电信提供的专线，例如 DDN、帧中继、MPLS 等，或者早期很多用户采用电话拨号的方式。一些特殊的行业，如金融、电力、铁路、政府等，他们对网络的可靠性、安全性有非常高的要求，一直以来都是采用物理专线的方式来连接地处不同位置的办公室、分支机构。但是对于大部分企业和很多政府机构来讲，无论在建设成本上还是后期维护上，要建立一个物理专网都是比较困难的。而利用拨号的方式对企业进行联网，不

仅速度慢、稳定性安全性差，而且费用很大、程度不可控。这种方式在企业及政府联网中已经基本被淘汰。

随着 Internet 的迅猛发展及 VPN 技术的出现，为企业、政府信息化应用提供了良机 and 更好的选择。VPN（Virtual Private Network，虚拟专用网）是利用公共网络资源来构建的虚拟专用网络，它是通过特殊设计的硬件或软件直接在共享网络中通过隧道、加密技术来保证用户数据的安全性，提供与专用网络一样的安全和功能保障。使得整个企业网络在逻辑上成为一个单独的透明内部网络，具有安全性、可靠性和可管理性。

早期的 VPN，由于需要专业的网络人员、固定 IP 地址、复杂的配置和宽带资源，以及产品的适应性等等诸多原因，一直难以推广。但是，最近两年中国的宽带互联网得到了飞速的发展，尤其是 ADSL 的发展，使互联网迅速普及到中国的各个角落，VPN 技术和应用也获得了空前的发展。今天，VPN 虚拟专用网已经具有与专线几乎相近的稳定性和安全性。事实上，利用 VPN 技术组建企业或行业的“专用网络”，已经成为今天大多数企业、政府、事业单位的首选解决方案。

IPSec VPN 网关就是在这样的应用背景下，基于天融信公司的系统平台 TOS 进行开发的 VPN 产品。IPSec VPN 既可以作为独立的 VPN 网关产品形态提供给用户，也可以作为一个 TOS 安全引擎（SE），与 TOS 上的其他安全引擎（如防火墙 SE、IDS SE 等）协同工作，为用户提供综合的集成化的安全网关产品。

2 产品特点

● CleanVPN

天融信 VPN 产品是集 VPN 功能、防火墙功能、路由功能、防病毒功能等于一身的网络安全产品，隧道策略、防火墙策略和防病毒策略可以组合使用。CleanVPN 病毒扫描可以对所有的 VPN 数据流进行扫描，从而阻止病毒和蠕虫通过 VPN 隧道传播，在总部、分支、远程用户和合作伙伴之间建立干净的 VPN 网络。

● 全面支持国密局 IPSec 协议规范

IPSec 作为一个通用性的安全标准，要求所有 IPSec 的实现必须严格遵循其各种协议规范，以便实现不同产品之间的互通。天融信 IPSec VPN 产品经过国家密码管理局的严格鉴定，符合国密局最新制定的《IPSEC VPN 技术规范》，可以和其他符合规范的的 VPN 产品实现互通。

本产品遵循国密局最新制定的《IPSEC VPN 技术规范》标准协议。

- 支持 ESP、AH 加密认证协议
- 支持隧道模式、传输模式的协议封装格式
- 支持密钥交换协议
- 支持主模式、快速模式多种协商模式
- 支持证书认证方式
- 支持国密局审批的专用加密卡

● 支持全动态 IP 地址间建立 VPN 隧道

目前国内常用的因特网接入方案，包括电话拨号、ISDN 拨号、ADSL 宽带接入等，都是由 ISP 为接入用户动态分配临时 IP 地址。如果企业的两个分支机构均采用动态 IP 地址方式接入因特网，那么这两个分支机构之间的 VPN 隧道策略参数必须进行动态调整，这为企业 VPN 网络的广泛应用和管理人员的维护工作带来很大麻烦。天融信 IPSec VPN

网关产品通过集中的 VPN 策略管理方式和 DDNS 无缝结合技术成功解决了双动态 IP 之间自动建立 VPN 隧道的问题。

● 支持 NAT 穿越（NATT）功能

NAT 技术是目前国内企业共享上网、小区和智能大厦宽带接入、城域网宽带接入所使用的主流技术。NAT 与 IPSec 协议在原理上存在一定的矛盾，所以在应用 IPSec 技术组建 VPN 网络时，一定要考虑选用的 VPN 设备是否具有“NAT 穿越”的功能。IPSec VPN 的全系列产品均支持 NATT 功能，具有非常好的网络适应性。IPSec VPN 产品还通过隧道路由转发技术支持双向 NAT 穿越。

● 通过隧道路由技术实现 VPN 网络的灵活自动部署

在实际物理网络部署中，网络管理员首先通过物理线路（可能是光纤、双绞线、电话线等）连接各个路由设备，然后通过路由器上配置静态路由或者动态路由完成各种规模网络的灵活部署。在 IPSec VPN 网络中，将每一条隧道视为连接两台 VPN 设备的虚拟网络线路，隧道建立成功后，虚拟线路连接工作就完成了。基于这些虚拟线路，网络管理员可以在 IPSec VPN 网关上采用同样的方法配置静态、动态路由协议，完成整个 VPN 网络的灵活部署。这种隧道路由机制的优点在于：

- 网关的配置概念和方法与路由器类似，减少网络管理员对于部署 VPN 网络的学习和熟悉过程；
- 通过隧道路由规则的配置，可以完成 VPN 数据流在 VPN 网关之间的灵活转发，从而可以实现星型网络拓扑，并解决双向 NAT 穿越问题；
- 通过动态隧道路由协议的配置，可以实现整个 VPN 网络的自适应部署，VPN 网络拓扑的自动学习、自动寻径；
- 通过基于策略的隧道路由配置，可以实现 VPN 网关的冗余备份和负载均衡。

● 完善的 VPN 网络集中管理功能

利用基于互联网的 VPN 技术构建企业基础网络设施，低成本、高效率是其天然的优势，但与此相伴的则是安全性和可管理性的潜在风险。尤其是对于分支机构、营业网点遍

布全国的大型企业来讲，其业务网络系统具有分布地域广泛、接入点多、网络结构复杂等特点。如何确保企业内部网络的安全，有效地管理、维护遍布企业各个结点的 VPN 设备，保证网络的稳定运行，是 VPN 产品供应商必须解决的问题。IPSec VPN 在综合了大量的用户需求后，逐步形成了“统一认证、集中监控、分级管理”的 VPN 网络管理方案。并成功运用于许多特大型企业的 VPN 建设中。

● 完善的 PKI 体系提高用户网络的安全等级

随着 VPN 技术在政府、金融等高安全性要求领域的应用不断深入，用户对 VPN 网络的认证功能与其原有的 PKI 体系进行无缝结合的需求也越来越强烈。网络卫士 IPSec VPN 网关全面支持标准 PKI 体系结构，既能够通过内置的 CA 模块独立为移动用户签发数字证书，又能够通过导入 CA 根证书+CRL 列表方式对第三方 CA 签发的证书进行认证，同时还能够通过 OCSP/LDAP 等标准协议向第三方 CA 提交在线证书认真请求。具体 PKI 功能包括：

- 支持标准 X509.V3 格式数字证书；
- 支持 DER、PEM、PKCS12 等多种证书编码格式；
- 支持通过内置 CA 模块为用户签发标准数字证书；
- 支持同时导入多个 CA 根证书和 CRL 列表，对不同 CA 签发证书进行认证；
- 支持通过 OCSP/LDAP 等标准协议向第三方 CA 进行在线证书认证；
- 支持生成 PKCS10 格式的证书请求，可生成证书请求，由第三方 CA 签名；
- 支持 CRL 列表文件的导入和通过 HTTP 自动下载；

天融信与吉大正元、上海格尔、天威诚信、江南计算所等国内主要 CA 厂商有着长期的合作，网络卫士 VPN 多合一网关与这些厂商的 CA 系统均能够无缝集成。

● 支持组播穿越隧道

普通的 IPSEC VPN 不能支持组播协议，因为 IPSEC VPN 只能将组播包路由到某一个特定的对端。天融信 VPN 经过创新后，可以支持组播穿越，这样可以在整个 VPN 组网内部利用组播来召开视频会议。

同时，利用组播穿越隧道，还可以轻松的实现隧道内的动态路由。VPN 设备可以将一端学习到的路由发布到另外一端，从而大大简化网络的部署难度，提升网络的管理效率。

● 多机多线路负载均衡与备份

天融信 VPN 产品可以在多台设备与多条链路之间实现隧道内数据负载均衡，如果某条线路发生故障，系统能自动的将数据流切换到其它线路，如果某台设备发生故障，系统能自动的将数据流切换到其它设备。

● 支持灵活的移动用户接入策略

VPN 技术在远程移动办公领域的应用越来越广泛，因此支持安全灵活的移动用户接入策略已经成为 VPN 产品竞争的焦点。IPSec VPN 产品支持丰富的移动用户接入策略，为各种需求的用户提供了完善的解决方案。

- 支持基于用户+口令的接入认证机制；
- 支持基于数字证书的接入认证机制；
- 支持基于证书+口令的双因子认证机制；
- 支持 RADIUS/TARCAS/LDAP 标准用户认证协议；
- 支持 USB KEY、动态口令卡等强身份认证机制；
- 支持基于服务的移动用户的访问授权；
- 支持基于时间的移动用户访问控制；
- 支持移动用户的硬件特征码绑定机制。
- 客户端版本支持中英文自动切换；

● 分级可信接入体系

可信接入是指对远程接入的 VPN 客户端的主机安全性进行检查，对不符合条件的客户端，即使账号信息是正确的，拒绝接入内网。

天融信 VPN 产品对客户端的接入实行可信接入检查，对于检查结果进行分级，不同的级别可以授予不同的权限，对不满足安全要求的主机，可以根据其缺陷程度分别实行隔离、修复和有限访问。

● 移动用户两网分离

天融信 VPN 产品可以控制 VPN 客户端接入 VPN 网络时, 实行 VPN 网络与因特网隔离, 不允许移动用户在使用 VPN 网络时访问因特网, 以保证 VPN 网络的安全。

天融信的 VPN 客户端可以实现安装软件后不允许上因特网与可以实现在启动隧道时不允许上因特网进行两网隔离。

● 丰富多样的认证与授权

天融信 VPN 产品内置有用户认证数据库, 同时支持多种外部认证, 如: RADIUS 认证、AD 认证、LDAP 认证等, 并支持外部认证服务器对用户授权与计费。通过外部认证, 可以方便的与用户原有的认证系统无缝的结合。

● 集成功能强大的防火墙功能

IPSec VPN 产品集成了天融信强大的防火墙产品功能, 为用户的 VPN 网络提供高等级的边界安全防护。网络卫士防火墙产品所具有的防火墙功能大都被 IPSec VPN 产品所继承了。

● 集成强大的网络路由功能

IPSec VPN 网关为用户组网提供了强大的网络路由功能, 完全可以作为独立的网络设备进行配置使用, 主要功能如下:

- 支持静态路由、动态路由协议;
- 支持 VLAN 划分;
- 支持完善的带宽管理功能;
- 支持 DNS 代理功能;
- 支持 DHCP 服务器。

3 产品主要功能

主功能	功能描述
网络工作模式	路由模式； 透明模式； 路由透明混合模式。
网络接入链路	10/100/1000M 以太网链路； ADSL 拨号链路； DHCP 接入。
支持 PKI 体系	支持 X.509 证书体系； 支持 DER/PEM 证书编码格式； 支持 PKCS12 证书编码格式； 支持 USB Key 存储设备私钥和证书； 支持设备证书导入、查看、删除； 支持根证书导入、查看、删除； 支持 CRL 导入、查看、删除； 支持通过 LDAP 协议认证 CA 证书； 支持通过 HTTP 协议自动下载 CRL； 支持生成设备证书请求； 支持为移动用户生成并发放证书。
密钥交换协议	第一阶段协商支持主模式； 第二阶段协商支持快速模式； 第一阶段身份认证支持 RSA（数字证书）方式； 支持完全向前保密 PFS； 支持 DPD 协议探测隧道状态； 支持隧道断线自动重建； 支持隧道内的 XAUTH 认证。
标准 IPSec 协议	支持国密局最新制定的《IPSEC VPN 技术规范》 支持 ESP、AH 封装协议； 支持隧道模式、传输模式； 与符合国密局规范的 IPSecVPN 产品互通； 支持隧道压缩协议； 支持 NAT 穿越和双向 NAT 穿越。
算法支持	支持国密局审批的 SSF28、SCB2(SM1)专用硬件加密卡。

移动客户端接入	<p>支持 L2TP/PPTP 客户端接入；</p> <p>支持 VRC 客户端接入；</p> <p>支持用户+口令的接入认证；</p> <p>支持 LDAP/AD/Radius 远程接入认证；</p> <p>支持基于数字证书的接入认证；</p> <p>支持动态口令卡接入认证；</p> <p>支持证书+口令双因子认证；</p> <p>支持 USB KEY 模式的身份认证；</p> <p>支持移动用户硬件特征码认证功能；</p> <p>支持为移动用户自动分配内部 IP 地址、DNS/WINS 服务器地址；</p> <p>支持为移动用户定义访问权限；</p> <p>支持基于时间的移动用户访问控制策略；</p> <p>支持两网分离；</p> <p>支持多线路自动检测；</p> <p>支持用户在线修改口令；</p> <p>支持移动用户接入状态的监控和审计。</p>
用户管理	<p>支持基于角色的用户管理；</p> <p>支持本地用户管理；</p> <p>支持外部 Radius 认证、LDAP 认证、AD 认证等。</p>
用户授权	<p>支持基于角色的用户授权；</p> <p>支持个别用户的单独授权；</p> <p>支持外部认证用户的授权；</p> <p>支持对外部认证用户分组授权。</p>
可信接入	<p>支持检查接入主机的信息；</p> <p>支持可信接入分级授权。</p>
支持复杂网络拓扑	<p>固定 IP 网关之间互通；</p> <p>固定 IP 网关与动态 IP 网关之间互通；</p> <p>动态 IP 网关之间互通；</p> <p>双向 NAT 穿越；</p> <p>支持网状拓扑、星形拓扑、树状层次拓扑等复杂的网络拓扑；</p> <p>支持隧道路由转发；</p> <p>全动态 IP 网络的隧道组建。</p>
支持 DDNS	<p>支持 DDNS 动态域名注册；</p> <p>支持使用域名进行隧道定义及协商；</p> <p>支持使用域名向 TP 进行集中认证。</p>
支持集中管理	<p>支持 TP 的集中认证；</p> <p>支持 TP 集中制定并下发隧道策略；</p> <p>支持 TP 集中监控隧道状态、设备状态和移动用户状态；</p> <p>支持 TP 的集中远程配置。</p>

本地管理	<p>支持串口 CLI 管理； 支持 Telnet CLI 管理； 支持 SSH CLI 管理； 支持 WebUI 管理； WebUI 支持 SSL 加密； 支持权限不同的多管理员； 同时只支持一个可修改策略的管理员登录； 支持系统配置保存、恢复； 支持远程软件升级。</p>
SNMP 支持	<p>支持 SNMP v2； 支持 SNMP v3； 支持 SNMP MIB 扩展； 支持 SNMP 查询； 支持 SNMP Trap 通告； 支持 OpenView 等网关软件管理。</p>
日志管理	<p>支持对各种审计事件的记录、导出； 支持 WELF 格式的审计日志； 支持向 TA 输出审计日志。</p>
国际化	<p>VRC 支持中英文版本； VRC 支持中英文自动切换。</p>
可靠性支持	<p>支持双机热备； 支持多台工作设备之间互为备份并自动切换； 支持灵活的隧道负载与备份功能； 可通过 TP 指定两点之间的各种线路组合关系； 可以通过 TP 指定各条线路之间是备份还是负载的关系。</p>

4 运行环境与标准

电源:

电压: AC 110/260V

频率: 47-63HZ

输入电流: 8.0/5.0A @115/230V

功率: 350W (最大)

环境:

运行温度: 0-45 摄氏度

非运行温度: -40-70 摄氏度

相对湿度: 5-95%, 非冷凝

国家标准:

GB/T18336-2001

GB/T18019-1999

GB/T18020-1999

参考的安全规范及标准(相对参考):

GB4943-2001

UL 1950

TUV-IEC 950

电磁兼容标准:

GB9254-1998

GB17618-1998

FCC Class A

抗干扰性:

IEC 61000-4-2 (静电放电 ESD 抗扰度)

IEC 61000-4-3 (射频电磁场抗扰度)

IEC 61000-4-4 (电快速瞬变 EFT 抗扰度)

IEC 61000-4-5 (浪涌 Surge 抗扰度)



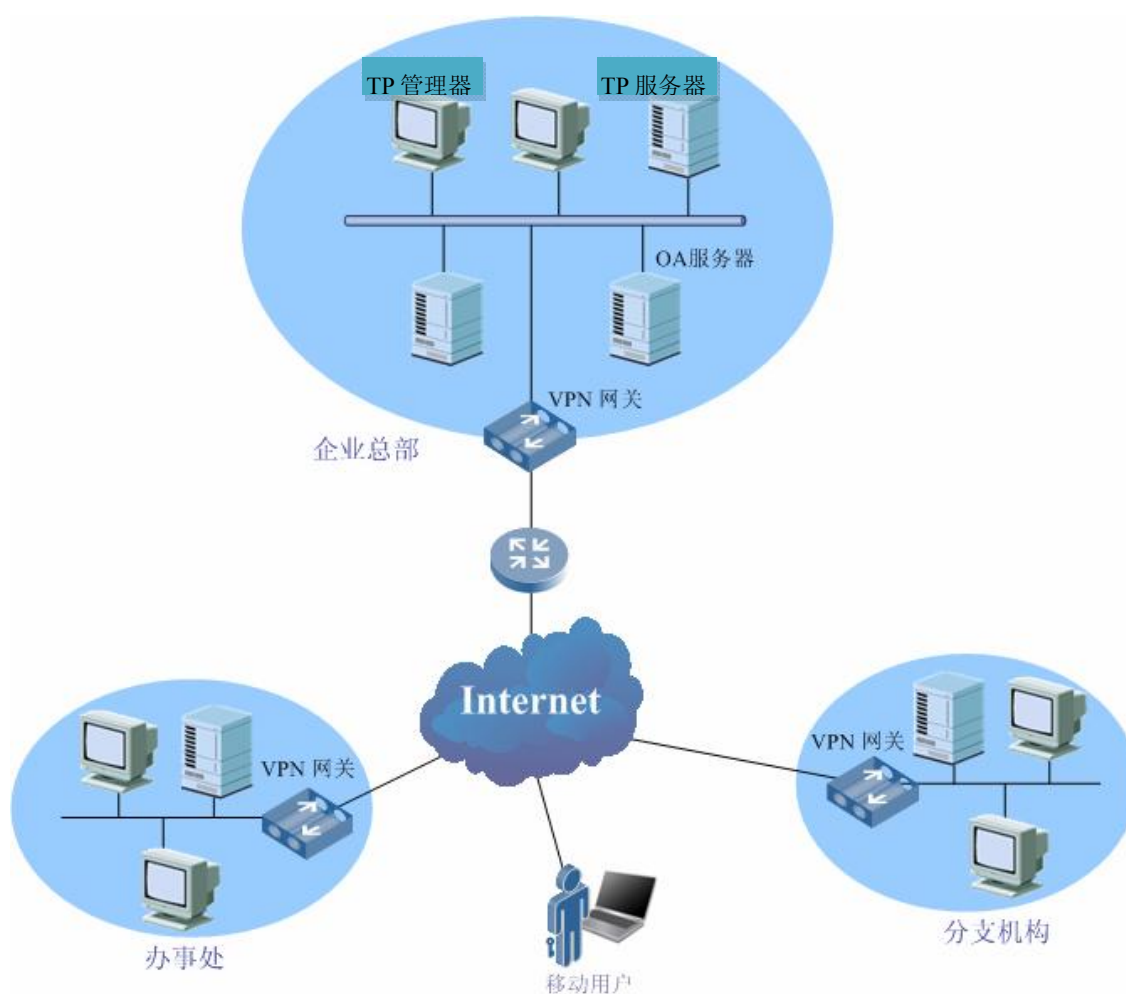
提示

-
- ✧ IPSec VPN 网关不同型号产品的具体参数可能因产品规格不同有所差异，请以产品背板标识为准。
-

5 典型应用

5.1 大中型企业总部与分支机构之间构建 VPN 的解决方案

许多大中型企业在全国各地都建有分支机构或者办事处，随着企业信息化程度的不断提高，一般在企业总部会部署如 OA 系统、ERP 系统等应用软件，将企业分布在各地的分支机构和办事处与企业总部互联，达到安全地共享数据和软件资源的目的，这是 VPN 网络的典型应用之一。利用 IPSec VPN 的解决方案见下图：



1. 产品部署方案

企业总部：总部一般来讲是企业信息存放、处理的中心，网络内部主机数量多、数据流量大、安全性和实时性要求高，因此推荐部署 VPN 处理能力强、硬件可靠性高的高端

IPSec VPN 网关，对于实时要求很高的企业用户，可以在总部采用 VPN 网关的双机热备份方案，以提高企业 VPN 网络的容错性；对于规模比较大、分支机构较多的企业，应该在总部的内部网络中部署天融信安全集中管理平台（TP），完成对整个网络中 VPN 设备的集中身份认证，集中状态监控和对全网 VPN 安全策略的集中制定及下发。

分支机构：企业分支机构一般指分布在全国各地规模不等的分公司，公司内部建有规模不等的局域网，同时通过当地 ISP 提供的宽带等各种方式接入因特网。在这种环境下推荐使用中端 IPSec VPN 网关产品。VPN 网关部署在企业内部网与因特网的接口处，可以直接与 ISP 提供的接入设备相连。VPN 网关可以完成自动接入因特网、代理内部主机访问因特网信息、为内部主机提供功能完善的防火墙保护等功能。同时 VPN 网关自动向总部的安全集中管理平台（TP）进行身份认证，认证通过之后自动从 TP 下载 VPN 隧道策略，建立 VPN 隧道，完成与总部或其他分支机构之间的隧道通讯工作。

办事处：一般指企业在全国各地建立的小型办事机构，通常仅有少量的工作人员和业务处理主机。在这种环境下推荐使用体积小、功能灵活的低端桌面式 IPSec VPN 产品，它的接入方法和所完成的功能与其他型号 IPSec VPN 网关基本相同。

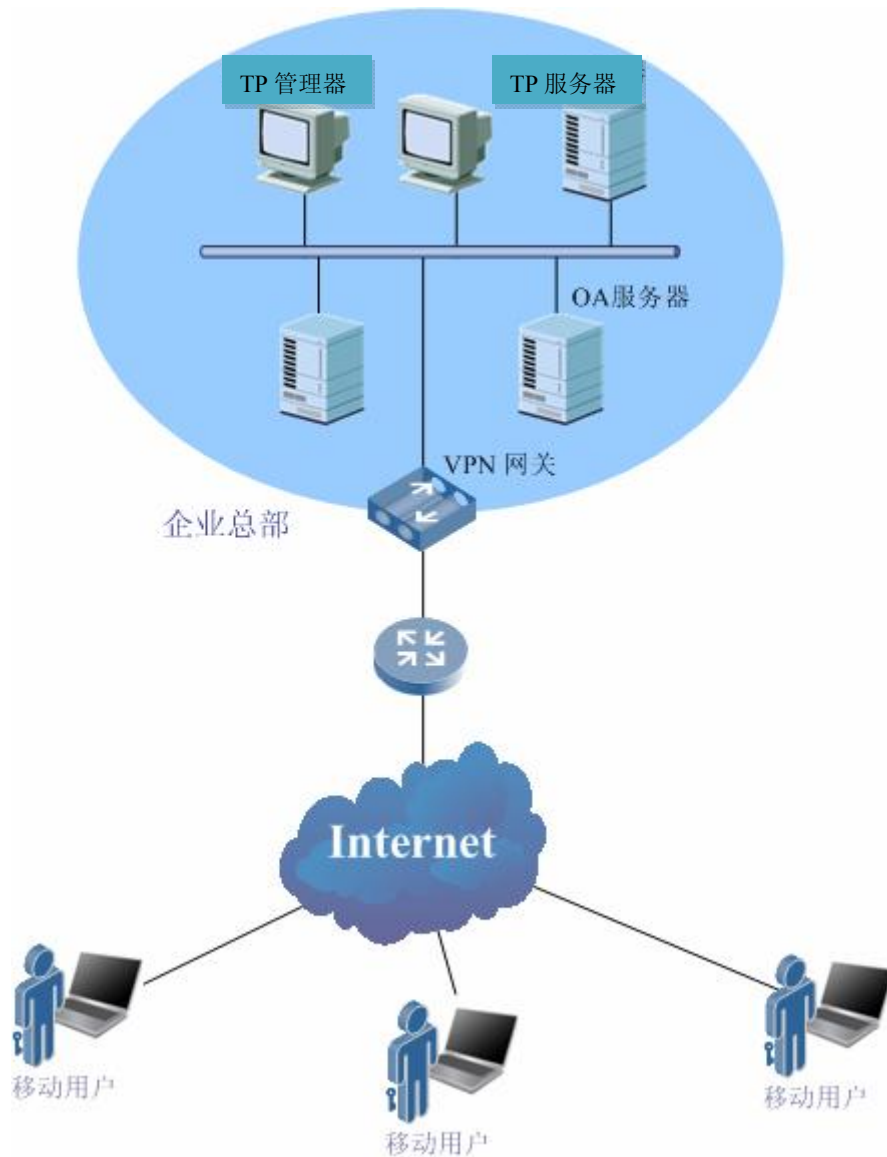
2. 解决方案能够为企业提供的 VPN 服务

分支机构与总部、分支机构之间能够任意建立网状的 VPN 隧道，企业员工可以象访问局域网一样访问远程的网络资源。例如：通过“网上邻居”共享数据文件，访问远程的企业资源数据库，在公司内部建立自己的 IP 电话系统、视频会议系统，远程使用“电子白板”等协同工作系统。

总部的网络管理员通过安全集中管理平台（TP），可以对整个 VPN 网络进行集中的状态监控、集中的 VPN 策略制定和下发以及对 IPSec VPN 网关的远程管理配置，可以在各个 VPN 节点设置动态的流量管理策略，为企业实时业务和多媒体数据流提供良好的带宽保证。

5.2 移动用户远程访问企业内部网络的 VPN 解决方案

在传统网络中，移动用户如果希望访问企业内部的网络资源，可以通过远程电话拨号接入企业的“远程接入服务器（RAS）”，这种方式往往需要企业支付较高的长途电话费用，而且网络速度慢，无法支持大量移动用户的同时访问需求。这正是 VPN 技术所能够解决的另外一种典型应用，解决方案示例如下图：



1. 产品部署方案

企业总部的信息中心: 如果用户希望能够对所有分支机构的移动用户进行集中的身份认证和授权, 并希望对全网的移动用户接入状态进行监控和审计, 则需要在企业总部的信息中心部署安全集中管理平台系统 (TP)。

企业各分支机构: 在企业各分支机构的局域网与因特网的接口处, 根据移动用户接入数量选择适当的 IPSec VPN 网关产品型号。

移动用户: 在移动用户的机器上安装 VPN 远程客户端软件 (VRC)。

2. 解决方案能够为移动用户提供的 VPN 服务

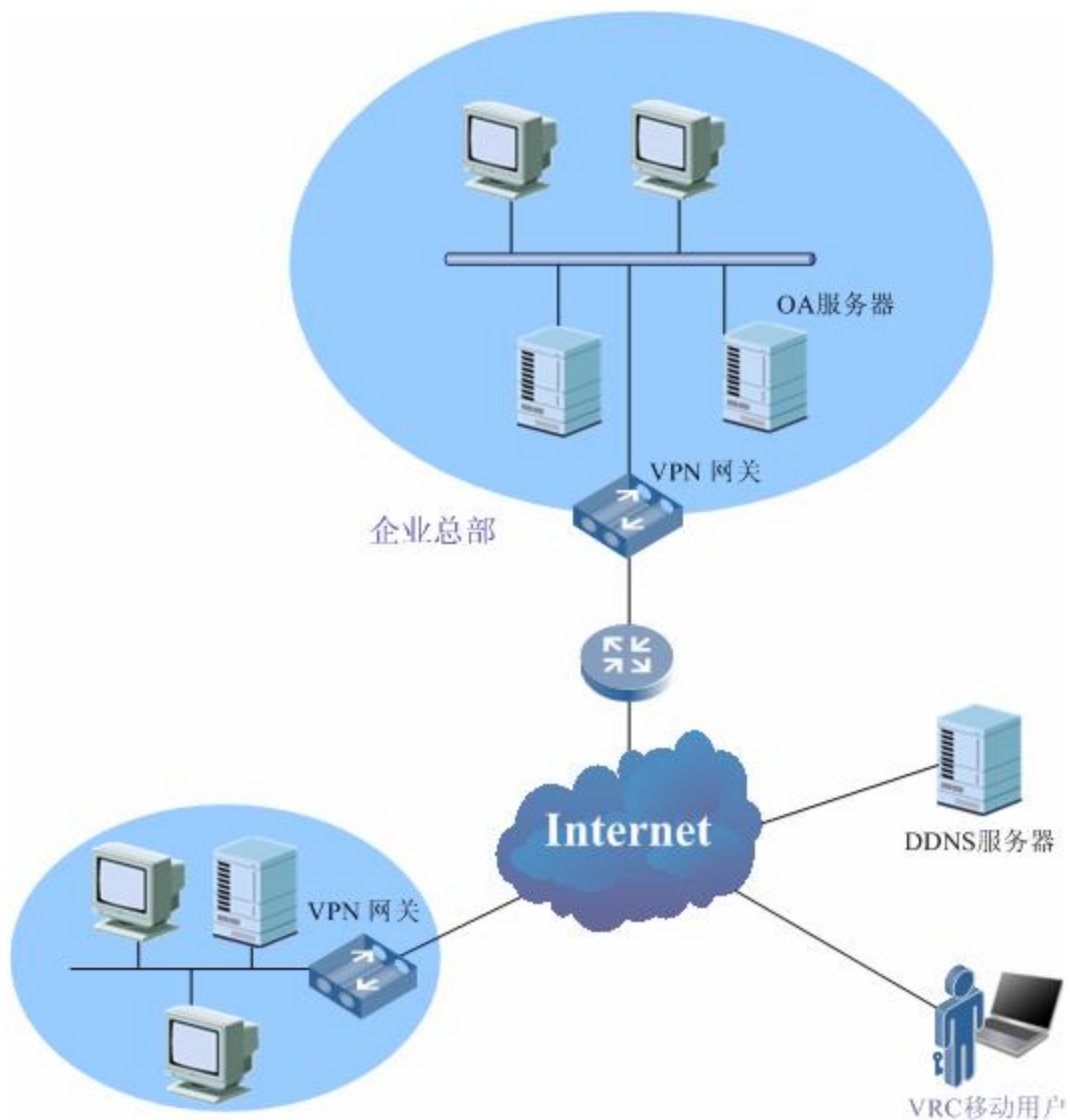
可以提供丰富的移动用户接入身份认证解决方案, 具体多种移动客户端接入认证模式。

移动用户接入认证完成后，即可根据接入网关（或者 TP）为其分配的权限访问相应的内部网络资源。

自动为移动用户分配内部 IP 地址、内部 DNS/WINS 服务器地址，使其访问内网资源更加安全、便捷。

5.3 小型企业 VPN 解决方案

许多小型企业在全国范围内可能仅有几家规模较小的分支机构，而且所有的分支机构均以动态 IP 地址方式接入因特网。在这种情况下，企业希望能够有一种配置灵活、投入较少的 VPN 解决方案，以完成所有的分支机构的相互访问需求。通过 IPSec VPN 产品内置的动态域名（DDNS）注册、解析机制和静态 VPN 隧道配置，可以构建性价比非常高的小型企业 VPN 网络。其解决方案如下图：



1. 产品部署方案

企业各分支机构:在企业分支机构安装低端桌面式 IPSec VPN 网关,并设置 IPSec VPN 网关内置的 DDNS 域名注册机制; 向因特网上的 DDNS 服务器注册唯一的 DDNS 域名; 在各个 IPSec VPN 网关之间建立以动态域名为端点标识的静态隧道。

企业的移动用户: 在企业移动用户的机器上安装 VPN 远程客户端软件, 并配置接入网关的 DDNS 域名。

2. 解决方案能够为用户提供的 VPN 服务

企业可以通过 DDNS 系统快速组建自己的全动态 VPN 网络, 实现各个分支机构的互联互通。同时企业还可以利用注册的动态域名完成自己对外信息发布平台(如对外的 WEB 网站、FTP 服务器等)的建设。

企业的移动用户也可以通过接入网关的动态域名实现远程接入和移动办公。

6 产品资质

证书名称	颁发单位
《计算机信息系统安全专用产品销售许可证》	公安部
《国家信息安全认证产品型号证书》	中国国家信息安全测评认证中心
《商用密码产品生产定点单位证书》	国家密码管理局
《商用密码产品销售许可证》	国家密码管理局
《计算机软件著作权登记证书》	国家版权局

声明:

1. 本手册所提到的产品规格及资讯仅供参考, 有关内容可能会随时更新, 天融信恕不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异, 此可能产生的差异为正常现象, 相关问题请咨询天融信客户服务中心 400-610-5119 或者 800-810-5119。
3. 本手册中没有任何关于其他同类产品的对比或比较, 天融信也不对其他同类产品表达意见, 如引起相关纠纷应属于自行推测或误会, 天融信对此没有任何立场。
4. 本手册中提到的信息为正常公开的信息, 若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失, 天融信及其员工不承担任何责任。