

# TopVPN 网络卫士网关系列 IPSec/SSL VPN 多合一网关

## 产品说明



天融信

TOPSEC®

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

## 版权声明

本手册中的所有内容及格式的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。

版权所有 不得翻印© 1995-2006 天融信公司

## 商标声明

本安装手册中所谈及的产品名称仅做识别之用。手册中涉及的其他公司的注册商标或是版权属各商标注册人所有，恕不逐一列明。

TOPSEC® 天融信公司

## 信息反馈

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

# 目 录

<b>1</b>	<b>产品概述</b> .....	<b>1</b>
1.1	安全接入的应用趋势.....	1
1.2	安全接入的技术趋势.....	1
1.3	网络卫士 VPN 多合一产品介绍.....	2
<b>2</b>	<b>产品特点</b> .....	<b>4</b>
<b>3</b>	<b>产品主要功能</b> .....	<b>10</b>
<b>4</b>	<b>运行环境与标准</b> .....	<b>15</b>
<b>5</b>	<b>典型应用</b> .....	<b>16</b>
5.1	案例一：XX 邮政的多种 VPN 技术综合应用.....	16
5.2	案例二：防火墙与 VPN 整合应用.....	17
5.3	案例三：双机热备的 VPN 应用.....	17

# 1 产品概述

## 1.1 安全接入的应用趋势

移动要求越来越强、移动接入的目的日益多样性，多种安全接入手段要求日益多样。随着电子政务和电子商务信息化建设的快速推进和发展，越来越多的政府、企事业单位已经或即将构建网上办公系统和业务应用系统，使内部办公人员通过网络可以迅速地获取信息，使“在家办公”、“异地办公”、“移动办公”等多种远程办公模式得以逐步实现，同时使合作伙伴人员也能够访问到相应的信息资源。可是要享受通过互联网访问企业内部的信息资源的便利，就面临着非法访问、信息窃取和数据篡改等越来越多的来自外部和内部的安全威胁。而我们目前所使用的操作系统、网络协议和应用系统不可避免地存在着不少的安全漏洞。因此，在构建和应用这些应用系统时，必须要保障关键应用在开放网络环境中的安全，同时还需尽量降低实施和维护成本。

## 1.2 安全接入的技术趋势

目前安全接入组网技术有多种，它们所处的协议层次、解决的主要问题都不尽相同，每种技术都有其适用范围和优点，同时也有一定的缺点。主流的 VPN 技术主要有以下三种：

### 1. L2TP/PPTP VPN

L2TP/PPTP VPN 属于二层 VPN 技术。在 windows 主流的操作系统中都集成的 L2TP/PPTP VPN 拨号客户端软件，因此其无需安装任何客户端软件，部署使用都比较简单；但是由于协议自身的缺陷，没有强度较高的加密和认证手段，安全性较低；同时这种 VPN 技术仅解决了移动用户的 VPN 访问需求，对于 LAN-TO-LAN 的 VPN 应用无法解决；

### 2. IPSEC VPN

IPSEC VPN 属于三层 VPN 技术，协议定义了完整的安全机制，对用户数据的完整性和私密性都有完善的保护措施；同时工作在网络协议的三层，对应用程序是透明的，能够无缝支持各种 C/S、B/S 应用；既能够支持移动用户的 VPN 应用，也能支持 LAN-TO-LAN 的 VPN 组网；组网方式灵活，支持多种网络拓扑结构。其缺点是网络协议比较复杂，正

确配置 VPN 隧道需要较多的专业知识；而且需要在移动用户的机器上安装单独的客户端软件。

### 3. SSL VPN

SSL VPN 属于应用层 VPN 技术，协议定义了完整的安全机制，对用户数据的完整性和私密性都有完善的保护；由于在 windows 等操作系统中的 IE 浏览器已经支持了完整的 SSL 协议，因此原理上将对于 B/S 应用是无需安装客户端软件的，部署使用较为简单。主要适用与移动用户接入并访问 B/S 结构的应用系统，对于 C/S 应用的支持仍然需要安装客户端的插件。

各种 VPN 技术都有其优点和缺点，而在用户的实际应用中，往往需要将这几种技术进行综合应用，才能满足较为复杂的用户需求。

天融信将这几种 VPN 技术有机的进行了整合，实现了在一台设备中同时支持上述几种主流的 VPN 组网技术，同时集成了天融信成熟领先的防火墙和身份认证系统，形成了一个完整的安全接入解决方案。

## 1.3 网络卫士 VPN 多合一产品介绍

网络卫士 VPN 多合一网关是集天融信十几年研发经验，向用户提供的完整 VPN 接入解决方案（IPSec/SSL）的一部分，是天融信研制推出的最新一代网络安全接入产品。该产品以天融信自主知识产权的 TOS（Topsec Operating System）为系统平台，采用开放性的系统架构及模块化的设计，融合了身份认证、访问控制等安全手段，具有安全、高效、易于管理和扩展等特点。

网络卫士 VPN 多合一网关可为远程分支、移动办公员工、业务合作伙伴及客户提供他们所需应用和资源的安全便捷的接入服务。产品的 L2TP/PPTP/SSL 无需任何客户端软件，也无需投入更多人力进行修改或长期的维护。产品的 IPSEC VPN 可以构筑分支之间的 LAN-LAN 的 VPN 网络。

SSL VPN 位于外部用户和内部用户之间，利用安全套接层(SSL)来提供安全的传输功能，而 SSL 在所有标准的 Web 浏览器中都具有的。SSL VPN 构建在经过强化的软硬件平台上，实现用户和资源的绑定。

SSL VPN 可提供 Web 接入、C/S 接入和全网接入等接入方式，以适应不同的用户需求，同时还具备强大的访问控制权限管理、细粒度的审计和日志记录等功能。

网络卫士 VPN 多合一网关包含完整的业界领先的防火墙功能，为用户提供全面的边界保护方案。

## 2 产品特点

### I 自主安全操作系统平台

采用自主知识产权的安全操作系统 — TOS (Topsec Operating System)，TOS 拥有优秀的模块化设计架构，有效保障了防火墙、VPN、内容过滤、抗攻击、流量整形等模块的优异性能，其良好的扩展性为未来迅速扩展更多特性提供了无限可能。

TOS 具有具有高安全性、高可靠性、高实时性、高扩展性及多体系结构平台适应性的特点。

### I 多种 VPN 技术有机融合

前面已经分析了目前主流的各种 VPN 技术的优缺点，这些技术有其不同的适用范围。在实际的用户网络中，不同的用户需求往往需要多种 VPN 技术综合应用，在这种情况下往往需要用户购买多台不同的 VPN 设备来满足需求，这既浪费资源又带来用户管理维护的工作量，同时网络环境变得更加复杂，网络运行的稳定性和安全性都会面临新的挑战。

网络卫士 VPN 多合一网关是天融信公司在多年各种独立的 VPN 产品研发和销售的基础上，推出的一款融合 IPSEC/SSL/PPTP/L2TP 等多种 VPN 技术的综合安全网关产品。在 TOS 平台强大的整合能力保障下，各种 VPN 模块进行了有机的整合，为用户提供一个统一完整的 VPN 接入平台。

### I 安全接入与安全防护无缝结合

VPN 网关作为网络边界设备，除了完成远端网络或移动用户的远程接入功能外，对用户网络边界安全也是至关重要的。网络卫士 IPSec/SSL VPN 多合一网关构建在天融信强大的 TOS 系统平台基础上，集成了天融信业内领先的防火墙功能模块，能够为用户的 VPN 网络提供高等级的边界安全防护。

网络卫士 VPN 多合一网关支持完善的基于内容检测的网络访问控制。内容检测技术发展至今，大致经历了三个阶段，从早期的状态检测 (Status Inspection) 到后来的深度包检测 (Deep Packet Inspection)，现在已经发展到了最新的完全内容检测 (CCI, Complete

Content Inspection)。状态检测只检查数据包的包头，深度包检测可对数据包内容进行检查，而 CCI 则可实时将网络层数据还原为完整的应用层对象（如文件、网页、邮件等），并对这些完整内容进行全面检查，实现彻底的内容防护。

网络卫士 VPN 多合一网关在 MAC 层提供基于 MAC 地址的过滤控制能力，同时支持对各种二层协议的过滤功能；在网络层和传输层提供基于状态检测的分组过滤，可以根据网络地址、网络协议以及 TCP、UDP 端口进行过滤，并进行完整的协议状态分析；在应用层通过深度内容检测机制，可以对高层应用协议命令、访问路径、内容、访问的文件资源、关键字、移动代码等实现内容安全控制；从而形成了立体的、全面的访问控制机制，实现了全方位的安全控制。

网络卫士 VPN 多合一网关提供了强大的网络应用控制功能。用户可以轻松的针对一些典型网络应用，如 BT、MSN、QQ、Edonkey、Skype 等实行灵活的访问控制策略，如禁止、限时、乃至流量控制。网络卫士防火墙还提供了定制功能，可以对用户所关心的网络应用进行全面控制。

网络卫士 VPN 多合一网关还拥有强大的地址转换能力。同时支持正向、反向地址转换，能为用户提供完整的地址转换解决方案。支持依据源或目的地址指定转换地址的静态 NAT 方式和从地址缓冲池中随机选取转换地址的动态 NAT 方式，可以满足绝大多数网络环境的需求。

网络卫士 VPN 多合一网关集成了天融信高级的 Intelligent Guard 技术提供了强大的入侵防护功能，能抵御常见的各种攻击，包括 Syn Flood、Smurf、Targa3、Syn Attack、ICMP flood、Ping of death、Ping Sweep、Land attack、Tear drop attack、IP address sweep option、Filter IP source route option、Syn fragments、No flags in TCP、ICMP 碎片、大包 ICMP 攻击、不明协议攻击、IP 欺骗、IP security options、IP source route、IP record route、IP bad options、IP 碎片、端口扫描等几十种攻击。

## I 多种 SSLVPN 技术结合实现应用系统全覆盖

目前 SSLVPN 接入技术大致分为三类：WEB 转发（WEB FORWARD）、端口转发（PORT FORWARD 或者称为 APP PROXY）和全网接入（NETWORK ACCESS 或者称为 IP TUNNEL）。这三种技术的技术特点和适用范围各不相同，在网络卫士 VPN 多合一网

关中对这三种 SSLVPN 接入技术都做了很好的支持，用户可以根据自身应用系统的特点选择使用一种或多种接入方式。

WEB 转发模式可以实现用户的完全无客户端接入，支持各种操作系统和客户浏览器平台。但其缺点是仅支持 B/S 模式的应用系统，而且对客户应用系统的依赖性较强。网络卫士 VPN 多合一网关通过在 WEB 转发模式中应用独创的智能 URL 重定向技术和自动分布式页面重构技术大大提高了对用户 B/S 系统的支持率和处理性能。同时通过开放的页面替换规则框架，支持为用户个性化的业务系统自定义特殊的 URL 替换规则，进一步提高了系统的适应性。

端口转发模式通过客户端本地代理技术实现对用户访问请求的 SSL 协议封装和转发。这种模式的适应性比 WEB 转发要好，但其要求在客户端安装一个 ACTIVEX 控件。网络卫士 VPN 多合一网关实现了客户端透明代理，用户不需要修改本地的任何配置即能完成代理控件的安装和使用，大大简化了用户操作步骤。

全网接入模式通过 SSL 隧道转发客户端所有的 IP 请求报文，其适应性最好，能够支持基于 IP 协议的所有 B/S 和 C/S 业务系统，其同样要求在客户端系统上安装一个 ACTIVEX 的控件。网络卫士 VPN 多合一网关通过全网接入模式能够实现移动用户的虚拟 IP 地址分配，实现各种访问控制策略的下发，支持移动用户以分离隧道(SPLIT TUNNEL 即可以同时访问 VPN 和因特网)或完全隧道(FULL TUNNEL 即只能访问 VPN 不能访问因特网)的方式接入 VPN 网络，大大提高了网络的整体安全性。

## I 完善的身份认证技术确保内部资源安全

VPN 的接入用户都具有远程访问部分企业内部资源的权限，而这些移动用户的接入地点是非常分散的，如果在接入时没有对用户身份进行严格的认证和授权，将会给企业内网带来很严重的安全隐患。

网络卫士 VPN 多合一网关为通过 SSL 隧道接入的用户提供了完整的身份认证手段。如果移动用户接入的环境比较简单、可信，管理员可以配置简单的“用户名+口令”认证方式，从而达到简单易用的效果；为了防止线路窃听和重播攻击，管理员可以采用“用户名+口令+图形验证码”的方式对移动用户进行身份认证；对于需要强身份认证机制的用户，管理员可以采用“数字证书”的认证方式，通过强度非常高的密码运算来保证用户的用户的身份标识不会受到“字典攻击”等暴力攻击的威胁；当然，还可以通过“数字证书

+UKEY+口令”的双因子认证方式来确保移动用户的证书不会被盗用，来进一步加强认证的安全性。

网络卫士 VPN 多合一网关除了能够在本地对用户进行身份认证，还支持通过 RADIUS/TARCAS/LDAP 等标准协议与外部专用的用户身份认证管理系统进行互动，从而能够实现动态口令认证、域认证等高级的认证方式。这既可以与用户的其他应用系统和安全产品共用用户认证数据库，实现用户集中管理和认证，又可以充分利用用户已有的资源，避免管理员大量重复的体力劳动。

为了便于管理员的管理配置，同时也方便企业的合作伙伴能够及时方便地与其进行信息共享，有时需要建立一个级别较低共用帐户，满足众多移动用户的快速接入。网络卫士 VPN 多合一网关支持配置多个不同权限的公共帐户，并且能够实时监控每个采用公共帐户登录的用户的行为，对于存在异常访问行为的用户可以强制其下线，而不会影响其他使用该帐户的合法用户的正常访问。

## I 多级用户授权机制提供灵活的用户授权组合

授权是对移动用户通过身份认证接入网关后，允许访问的内网资源权限进行控制，是保护内网资源安全的主要技术手段。管理员对用户授权的需求往往是复杂多样的，最简单直接的需求是能够根据用户的身份划分多个组，每个组享有不同的资源访问权限；有时某个用户可能具有多重身份，分属于多个用户组，享有多个组的访问权限；有时在同一个用户组下面，可能某一个或某几个用户在具备用户组访问权限的同时，还有部分特权能够访问更高安全级别的资源，等等。网络卫士 VPN 多合一网关采用多级授权机制和用户授权继承的策略，完全满足上述的各种用户授权需求。

在用户授权的粒度上，网络卫士 VPN 多合一网关支持基于 URL/目录/文件等访问内容的控制策略，支持用户行为动作的访问控制策略，支持基于访问时间的控制策略，能够充分满足管理员的各种用户授权需求。

## I 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。网络卫士多合一 VPN

产品全面支持标准 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 提交在线证书认证请求。具体 PKI 功能包括:

- Ø 支持标准 X509.V3 格式数字证书;
- Ø 支持 DER、PEM、PKCS12 等多种证书编码格式;
- Ø 支持通过内置 CA 模块为用户签发标准数字证书;
- Ø 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;
- Ø 支持通过 OCSP/LDAP 等标准协议向第三方 CA 进行在线证书认证;
- Ø 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; ;
- Ø 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。

## I 卓越的网络及应用环境适应能力

网络卫士 VPN 多合一网关构建于强大的 TOS 系统平台之上,天融信在网络与信息安全领域多年的技术积累和庞大的用户群为其提供了卓越的网络及应用环境适应能力。其支持众多网络通信协议和应用协议,如 VLAN、ADSL、PPP、ISL、802.1Q、Spanning Tree、H.323、MMS、RTSP、ORACLE SQL\*NET、MS RPC 等等,适用网络的范围非常广泛,充分保证了用户的网络的可用性。

同时,针对国内用户动态 IP 地址较多的现状,网络卫士多合一网关整合了天融信公司独立维护的 EZVPN 动态域名系统,为天融信的 VPN 用户提供专用的动态地址域名解析服务,从而很好地解决了动态地址的 VPN 接入问题。

## I 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。

## I 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。

## I 支持中英文自动切换

用户登录界面可根据使用者的操作系统的语言，自动调整成为中文或英文界面，亦可手动切换成中文或英文界面。

## I 集成功能强大的防火墙功能

天融信 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在 VPN 产品中都具有，具体功能请参见网络卫士系列防火墙的产品说明。

### 3 产品主要功能

类别	功能	详细描述
工作模式	工作模式	<ul style="list-style-type: none"> <li>  支持透明、路由、混合模式</li> </ul>
网络适应性	路由	<ul style="list-style-type: none"> <li>  支持静态路由、动态路由。</li> <li>  支持基于源/目的地址、接口、Metric 的策略路由。</li> <li>  支持单臂路由，可通过单臂模式接入网络，并提供路由转发功能。</li> <li>  支持 Vlan 路由，能够在不同的 VLAN 虚接口间实现路由功能。</li> <li>  支持 RIP、OSPF 等路由协议。</li> </ul>
	组播	<ul style="list-style-type: none"> <li>  支持 IGMP 组播协议。</li> <li>  支持 IGMP SNOOPING。</li> <li>  可有效地实现视频会议等多媒体应用。</li> </ul>
	VLAN	<ul style="list-style-type: none"> <li>  可与交换机的 Trunk 接口对接，并且能够实现 Vlan 间通过安全设备传播路由。</li> <li>  支持 802.1Q，能进行封装和解封。</li> <li>  支持 ISL，能进行 ISL 的封装和解封。</li> <li>  在同一个 Vlan 内能进行二层交换。</li> </ul>
	生成树	<ul style="list-style-type: none"> <li>  支持 802.1D 生成树协议。</li> </ul>
	ARP	<ul style="list-style-type: none"> <li>  支持 ARP 代理、ARP 学习。</li> <li>  可设置静态 ARP。</li> </ul>
	DHCP	<ul style="list-style-type: none"> <li>  支持 DHCP Client、DHCP Server。</li> </ul>
	接入	<ul style="list-style-type: none"> <li>  支持 ADSL 等宽带接入。</li> <li>  支持 PPPOE 拨号接入。</li> </ul>
	其它	<ul style="list-style-type: none"> <li>  支持网络时钟协议 SNTP，可以自动根据 NTP 服务器的时钟调整本机时间。</li> <li>  支持 IPX、NetBEUI 等非 IP 协议。</li> </ul>
	PKI	证书格式
本地 CA		<ul style="list-style-type: none"> <li>  支持内置 CA，为其他设备或移动用户签发证书</li> <li>  支持本地 CA 根证书、根私钥的更新</li> <li>  支持证书废弃，支持生成标准 CRL 列表</li> <li>  支持证书请求的生成，由第三方 CA 进行签名</li> </ul>
第三方 CA		<ul style="list-style-type: none"> <li>  支持同时导入多个第三方 CA 的根证书和 CRL 列表，对不同 CA 证书用户进行身份认证，支持通告 HTTP 协议定时下载 CRL 列表</li> <li>  支持通过 OCSP/LDAP 等协议在线认证证书</li> </ul>
SSL VPN	协议类型	<ul style="list-style-type: none"> <li>  支持 SSL 协议</li> </ul>
	数据压缩	<ul style="list-style-type: none"> <li>  支持高效流压缩算法</li> </ul>

类别	功能	详细描述
	用户认证	<ul style="list-style-type: none"> <li>  支持“用户名+口令”、“用户名+口令+图形认证码”认证</li> <li>  支持 X.509 数字证书认证</li> <li>  支持数字证书+UKEY+口令多因子认证</li> <li>  支持公共帐户登陆, 支持临时禁止帐户登录</li> <li>  支持本地数据库认证</li> <li>  支持基于 LDAP/RADIUS/TACAS 等协议的外部服务器认证</li> </ul>
	用户授权	<ul style="list-style-type: none"> <li>  支持分组授权、支持独立用户授权和授权继承</li> <li>  支持基于 URL、访问路径、访问文件、访问动作的细粒度授权</li> <li>  支持基于时间的访问授权方式</li> <li>  支持本地授权、支持外部组映射授权、支持证书用户授权</li> </ul>
	应用支持	<ul style="list-style-type: none"> <li>  支持 HTML、JAP、ASP、JAVA APPLET、ACTIVE、Cookies 等各种 Web 应用</li> <li>  支持基于 IP 协议的各种 C/S 应用, 如 EMAIL,FTP,ERP,CRM,DB 等</li> <li>  支持 Windows/CIFS 远程文件共享</li> </ul>
	实时监控	<ul style="list-style-type: none"> <li>  实时监控在线用户的登录时间、在线时间、访问流量, 认证方式等多种信息</li> <li>  支持对使用公共帐户登录用户进行独立监控</li> <li>  支持主动中断在线用户的隧道连接</li> </ul>
	日志审计	<ul style="list-style-type: none"> <li>  详细审计用户登录认证过程、各种认证授权错误、内网资源访问情况等信息</li> <li>  支持多级审计日志, 可以灵活配置审计级别</li> <li>  支持日志本地保存, 支持将日志上传到外部日志服务器</li> <li>  支持天融信专用的 TA-L 日志服务器, 可以对日志内容进行深度分析和统计</li> </ul>
	端点安全	<ul style="list-style-type: none"> <li>  支持接入客户端痕迹清除, 能够清楚 cookie、缓存、历史记录等各种访问痕迹</li> <li>  支持拔 KEY 隧道自动中断</li> <li>  支持用户超时自动退出, 超时时间可以设置</li> </ul>
可信接入	可信接入	<ul style="list-style-type: none"> <li>  支持检查接入主机的信息</li> <li>  支持可信接入分级授权</li> </ul>
国际化	语言支持	<ul style="list-style-type: none"> <li>  支持中、英文界面</li> <li>  支持中、英文自动切换</li> <li>  支持中、英文手动切换</li> </ul>
DDNS	DDNS	<ul style="list-style-type: none"> <li>  支持 DDNS 动态域名注册</li> <li>  支持使用域名进行隧道定义及协商</li> <li>  支持使用域名向 TP 进行集中认证</li> </ul>
IPSEC VPN	协议	<ul style="list-style-type: none"> <li>  支持国密局最新制定的《IPSEC VPN 技术规范》</li> <li>  支持 ESP/AH / NATT 等协议, 支持隧道模式、传输模式</li> </ul>
	算法	<ul style="list-style-type: none"> <li>  支持国密局批准的 SSF28、SCB2(SM1)硬件加密算法。</li> </ul>
	数据压缩	<ul style="list-style-type: none"> <li>  支持高效数据流压缩算法</li> </ul>
	隧道认证	<ul style="list-style-type: none"> <li>  支持数字证书认证, 支持扩展认证</li> </ul>

类别	功能	详细描述
	网络适应性	<ul style="list-style-type: none"> <li>  支持网状、树型、星型等多种 VPN 网络拓扑</li> <li>  支持隧道的 NAT 穿越、双向 NAT 隧道建立</li> <li>  支持全动态 IP 地址间的 VPN 组网</li> <li>  支持隧道转发</li> <li>  支持多机多隧道的负载均衡和冗余备份方案</li> <li>  支持隧道内的访问控制</li> </ul>
L2TP VPN	L2TP	<ul style="list-style-type: none"> <li>  支持远程用户通过 L2TP 接入，建立 L2TP 隧道访问内部网络</li> </ul>
PPTP VPN	PPTP	<ul style="list-style-type: none"> <li>  支持远程用户通过 PPTP 接入，建立 PPTP 隧道访问内部网络</li> </ul>
防火墙	内容过滤	<ul style="list-style-type: none"> <li>  采用完全内容检测（Complete Content Inspection）技术。</li> <li>  支持基于流、数据包、透明代理的过滤方式。</li> <li>  支持对 HTTP、SMTP、POP3、FTP 等协议的深度内容过滤。</li> <li>  支持 URL 过滤。</li> <li>  支持对移动代码如 Java applet、Active-X、VBScript、Java script 的过滤。</li> <li>  支持对邮件的收发邮件地址、文件名、文件类型过滤。</li> <li>  支持对邮件主题、正文、收发件人、附件名、附件内容等关键字匹配过滤。</li> <li>  支持 MSN，QQ，Skype 等 Instant Messenger 通信，并可以对于这些应用进行登陆限制。</li> <li>  可限制 BT，eMule，eDonkey 等 P2P 应用。</li> <li>  可屏蔽受保护主机/服务器系统信息，如替换服务器（FTP、SMTP、POP3、telnet,HTTP）的 BANNER 信息。</li> </ul>
	包过滤	<ul style="list-style-type: none"> <li>  基于状态检测的动态包过滤。</li> <li>  基于源/目的 IP 地址、MAC 地址、端口和协议、时间、用户的访问控制。</li> <li>  支持基于用户的 PPTP 的访问控制。</li> <li>  支持报文合法性检查。</li> <li>  动态端口支持协议：H.323、SIP、FTP、RTSP、SQL*NET、MMS、RPC、TFTP、PPTP。</li> <li>  可实现 IP/MAC 绑定。</li> </ul>
	防御攻击	<ul style="list-style-type: none"> <li>  非法报文攻击：land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspooof。</li> <li>  统计型报文攻击：Synflood、Icmpflood、Udpflood、Portscan、ipsweep。</li> <li>  Topsec 联动：可与支持 TOPSEC 协议的 IDS 设备联动，以提高入侵检测效率。</li> <li>  端口阻断：可以根据数据包的来源和数据包的特征进行阻断设置。</li> <li>  SYN 代理：对来自定义区域的 Syn Flood 攻击行为进行阻断过滤。</li> <li>  CC 攻击：可通过设置端口和阈值阻断 CC 攻击。</li> <li>  可记录攻击日志和报警。</li> </ul>
	NAT	<ul style="list-style-type: none"> <li>  支持双向 NAT。</li> <li>  支持动态地址转换和静态地址转换。</li> <li>  支持多对一、一对多和一对一等多种方式的地址转换。</li> <li>  支持虚拟服务器功能。</li> </ul>

类别	功能	详细描述
安全管理	用户认证	<ul style="list-style-type: none"> <li>  支持使用一次性口令认证（OTP）、本地认证、双因子认证（SecurID）以及数字证书（CA）等常用的安全认证方式。</li> <li>  支持使用第三方认证，如 RADIUS、TACACS/TACACS+、LDAP、域认证等安全认证方式。</li> <li>  支持 Session 认证、HTTP 会话认证。</li> <li>  支持认证保活功能。</li> <li>  可将认证用户信息加密存放在本地数据库。</li> </ul>
	日志	<ul style="list-style-type: none"> <li>  支持 Welf、Syslog 等多种日志格式的输出。</li> <li>  支持通过第三方软件来查看日志。</li> <li>  支持日志分级。</li> <li>  支持对接收到的日志进行缓冲存储。</li> <li>  支持安全审计系统（TA-L），获得更详尽的日志分析和审计功能。</li> <li>  TA-L 除接受防火墙日志外还能接受交换机、路由器、操作系统、应用系统和其他安全产品的日志进行联合分析。</li> <li>  可对日志进行加密传输。</li> </ul>
	监控	<ul style="list-style-type: none"> <li>  支持网络接口、CPU 利用率、内存使用率、操作系统状况、网络状况、硬件系统、进程、进程内存、加密卡状况的监测。</li> <li>  可根据配置文件进行错误恢复。</li> </ul>
	报警	<ul style="list-style-type: none"> <li>  内置了“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类。</li> <li>  支持邮件、NETBIOS、声音、SNMP、控制台等多种组合报警方式。</li> </ul>
带宽管理	QoS 流量整形	<ul style="list-style-type: none"> <li>  QOS 带宽管理。</li> <li>  根据 IP、协议、网络接口、时间定义带宽分配策略。</li> <li>  支持最小保证带宽和最大限制带宽。</li> <li>  支持分层的带宽管理。</li> </ul>
	优先级	<ul style="list-style-type: none"> <li>  支持 8 级优先级控制。</li> </ul>
高可用性	双机热备	<ul style="list-style-type: none"> <li>  支持双机热备（Active-Active，与 Active-Standby 两种模式）。</li> <li>  支持系统故障切换，包括主设备抢状态开关功能，控制主设备是否在设备恢复正常情况时抢回主设备状态。</li> <li>  支持 VPN 网关的双机热备功能。</li> </ul>
	其它功能	<ul style="list-style-type: none"> <li>  支持链路备份功能。</li> <li>  支持双系统引导。</li> <li>  支持 Watchdog 功能。</li> </ul>
配置管理	配置方式	<ul style="list-style-type: none"> <li>  支持 WEB 图形配置、命令行配置。</li> <li>  支持本地配置、远程配置。</li> <li>  支持基于 SSH、SSL 的安全配置。</li> </ul>
	命令行	<ul style="list-style-type: none"> <li>  支持配置命令分级保护。</li> <li>  支持中英文。</li> <li>  支持命令超时、历史命令、命令补齐、命令帮助、命令错误提示等功能。</li> </ul>
	SNMP	<ul style="list-style-type: none"> <li>  支持 SNMP 的 v1、v2、v2c、v3 版本。</li> <li>  与当前通用的网络管理平台兼容，如 HP Openview 等。</li> </ul>

类别	功能	详细描述
	系统升级	<ul style="list-style-type: none"><li>  支持双系统升级。</li><li>  支持远程维护和系统升级。</li><li>  支持 TFTP 升级。</li></ul>
	报文调试	<ul style="list-style-type: none"><li>  提供强大的报文调试功能，可以帮助网络管理员或安全管理员发现、调试和解决问题。</li><li>  支持发送虚拟报文。</li></ul>
	配置恢复	<ul style="list-style-type: none"><li>  可以进行配置文件的备份、下载、删除、恢复和上载。</li></ul>
	时钟调整	<ul style="list-style-type: none"><li>  支持网络时钟协议 SNTP，可自动根据 NTP 服务器时钟调整本机时间。</li></ul>

## 4 运行环境与标准

### 电源：

电压：AC 110/220V

频率：50/60HZ

电流：3.0A (最大)

功率：350W (最大)

### 环境：

运行温度： 0 - 45 摄氏度

非运行温度： -20 - 65 摄氏度

相对湿度： 10 - 90% @40 摄氏度，非冷凝

### 国家标准：

GB/T18336-2001

GB/T18019-1999

GB/T18020-1999

### 抗干扰性：

IEC 1000 4 2 ( ESO )

IEC 1000 4 3 ( 辐射敏感性 )

IEC 1000 4 4 ( 电快速瞬变 )

IEC 1000 4 5 ( 电源 )

IEC 1000 3 2 ( 谐波 )

## 5 典型应用

### 5.1 案例一：XX 邮政的多种 VPN 技术综合应用

XX 省邮政系统以前各支局独立建立了办公网，现在整个邮政系统要上一套办公系统，要求整个各分支形成统一的虚拟专用网，同时一些领导要能够移动办公。

天融信公司分析了用户的需求，在省局安装了 IPSEC/SSL 多合一网关，在分局安装了 IPSEC 网关，这样整个邮政系统组成了一个完整的虚拟专用网，分局通过 IPSEC VPN 访问省局的 OA 服务器，领导通过 SSL VPN 进行网上办公，同时以前有些系统中原有的 L2TP 用户则平滑地移到了 IPSEC/SSL 多合一网关的 L2TP 上。方案如下图所示。

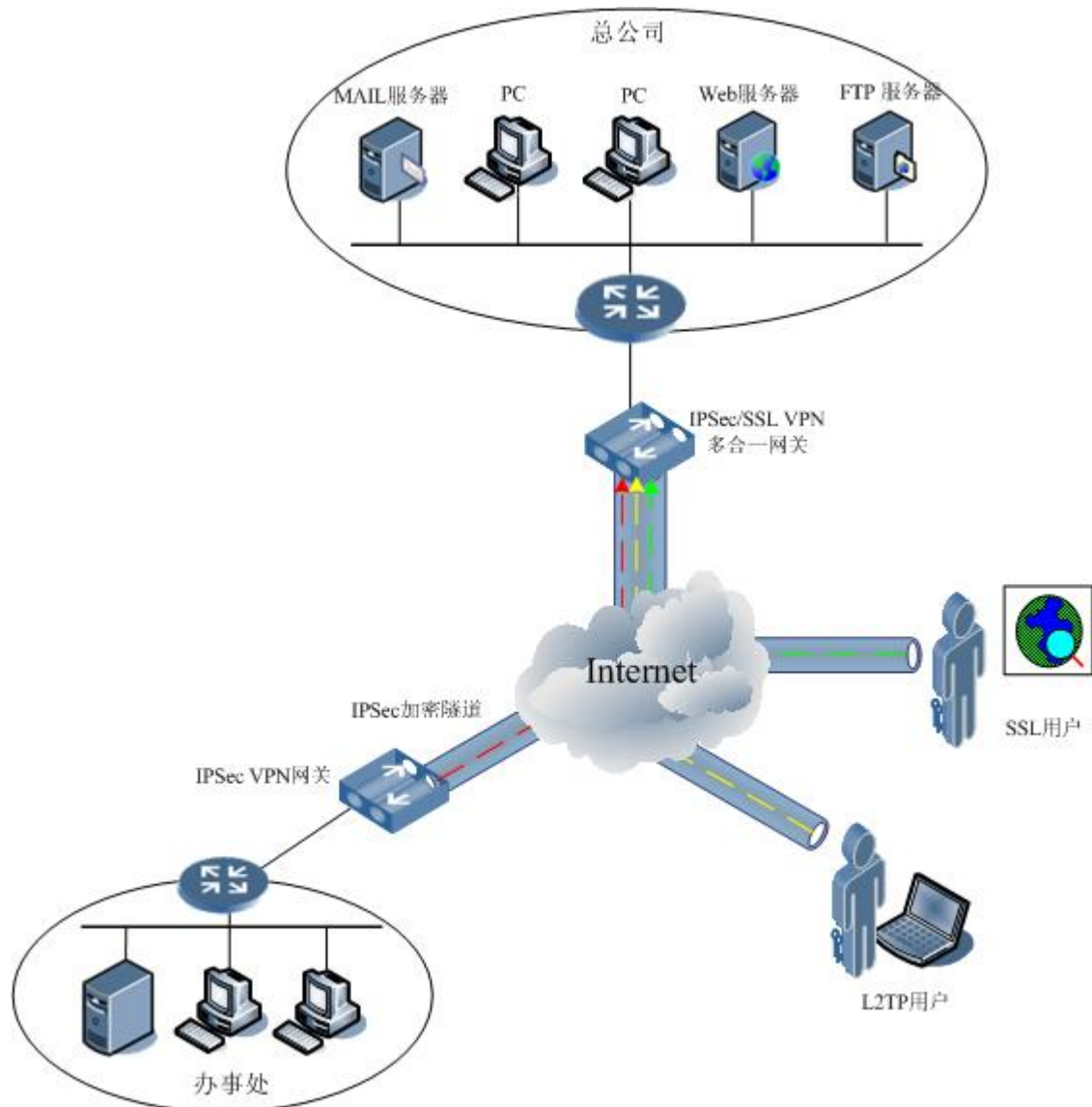


图 5-1 多种 VPN 综合应用示意图

## 5.2 案例二：防火墙与 VPN 整合应用

天融信的防火墙产品无论是品牌还是市场占有率都是国内第一的，其功能和性能都得到广大用户的长期认可。一个电力的用户在采购 SSL VPN 时，发现天融信的 IPSEC/SSL 多合一网关产品不仅完全满足了方便安全接入的需求，而且提供了更为可靠、全面的网络边界防护功能，用户毫不犹豫选择了 IPSEC/SSL 多合一网关产品。

IPSEC/SSL 多合一网关产品不仅使用户感受到非常高的性价比，而且使在享受 VPN 带来的方便和便捷的同时享受国内一流防火墙产品所提供的安全防护。

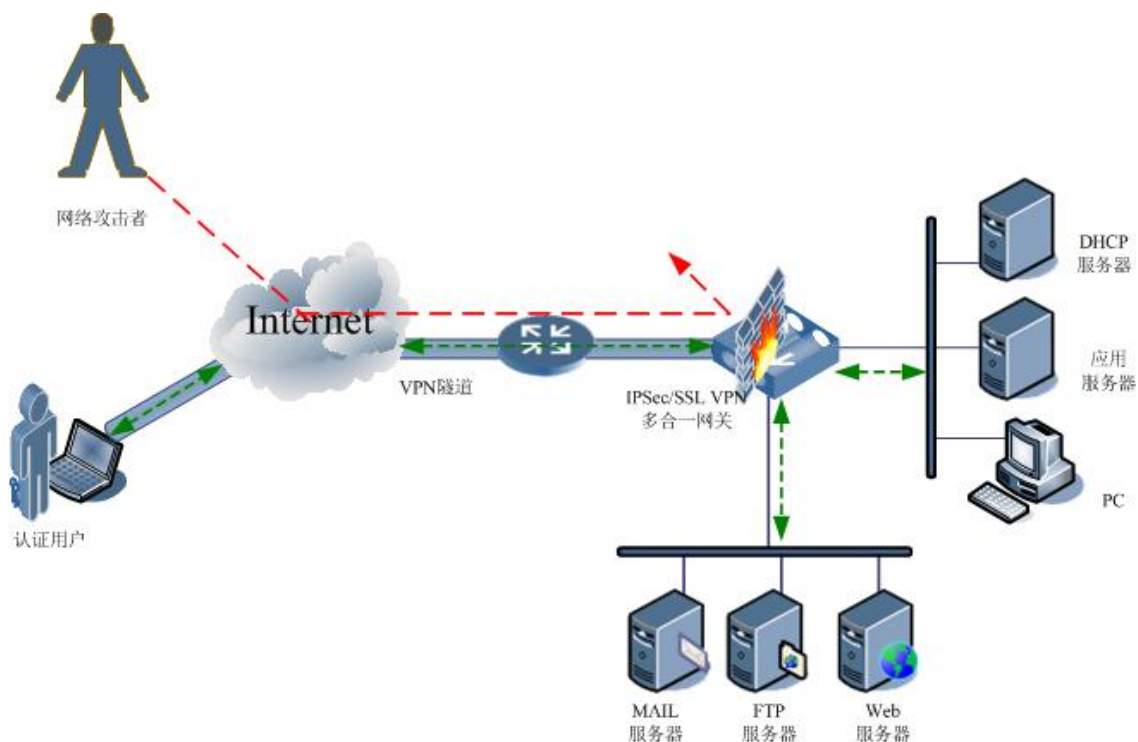


图 5-2 防火墙与 VPN 的综合应用

## 5.3 案例三：双机热备的 VPN 应用

VPN 网络中往往会承载用户的业务数据流，网络的可用性是用户选择 VPN 产品非常重要的一个因素。VPN 多合一网关产品在天融信统一的安全产品软件系统平台 TOS 上开发完成的，与天融信的防火墙、IPSEC VPN 网关产品一样具有非常丰富的网络冗余备份功能，支持完善的双机热备份功能，为用户的关键业务节点提供可靠的网络接入方案。

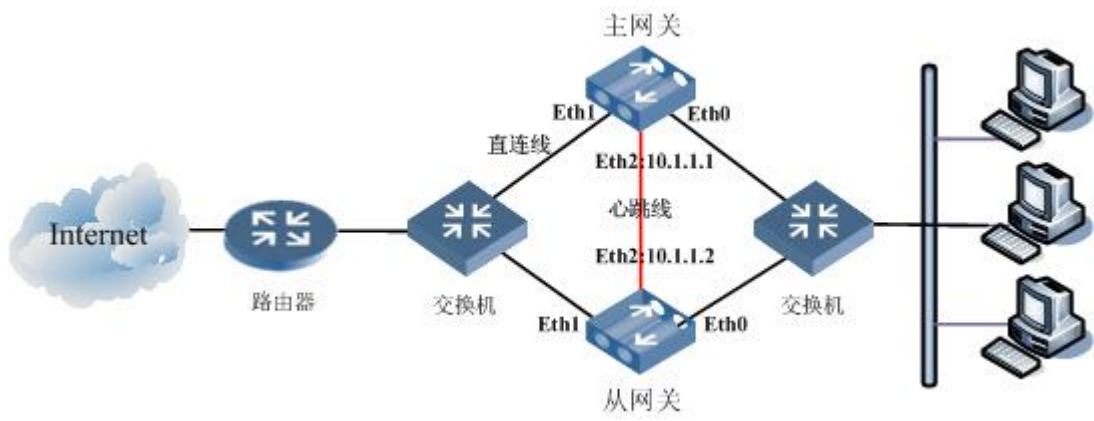


图 5-3 双机热备模式下的 VPN 应用

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，产品功能和性能请以产品说明书为准。
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。