

# 网络卫士安全网关(UTM) TopGate 系列

## 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>

---

## 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

<b>1</b>	<b>产品概述</b> .....	<b>1</b>
<b>2</b>	<b>产品特点</b> .....	<b>2</b>
<b>3</b>	<b>产品功能</b> .....	<b>5</b>
<b>4</b>	<b>运行环境</b> .....	<b>11</b>
<b>5</b>	<b>典型应用</b> .....	<b>13</b>
<b>6</b>	<b>产品资质</b> .....	<b>14</b>

# 1 产品概述

天融信TopGate网络卫士安全网关(UTM)是北京天融信公司基于多年网络安全产品研发经验推出的包括防火墙、虚拟专用网(VPN)、入侵检测和防御(IPS)、网关防病毒、WEB内容过滤等安全防护特性的UTM产品。TopGate不但能为用户提供全方位的安全威胁防护方案,还为用户提供全面的策略管理、服务质量(QoS)保证、负载均衡、高可用性(HA)以及网络带宽管理等功能。

TopGate安全网关(UTM)可灵活部署在大中型企业及其分支机构或中小企业网络的网关处,保护用户网络免受黑客攻击、病毒、蠕虫、木马、恶意代码以及未知的“零小时”(zero-hour)攻击等混合威胁的侵害;同时还为用户提供简便统一地管理各种安全特性及相关日志、报告,大大降低了设备部署、管理和维护的运营成本。除此之外,TopGate还为企业提供了CleanVPN服务,使得用户通过VPN远程访问企业内网时,确保VPN数据没有病毒等有害内容。在新攻击的防护上,TopGate对VoIP, IM/P2P, 间谍软件, 网络钓鱼, 混合攻击等都有出色的表现。

TopGate UTM 在技术上采用先进的完全内容检测技术和独特的加速引擎处理技术,可通过简单的配置和管理,以较低的维护成本为用户提供一个高级别保护的“安全隔离区”。它对经过网关的数据流量进行病毒、蠕虫、入侵等进行高效检测,而且能够阻挡来自垃圾邮件、恶意网页的威胁,所有的检测都是在实时状态下进行,具有很高的网络性能。

TopGate UTM 在功能管理上采用独特的模块结构,由一些关键部件组成。主要包括内容处理加速模块、管理模块、背板总线模块、接口模块等。在系统上支持病毒扫描、内容过滤、状态检测防火墙、IPSec VPN、基于网络的IDP和流量管理应用等。模块化、智能化设计除了确保传送高速度的吞吐量,使得系统能方便地添入或修改新的功能,并确保万一有故障发生时的故障恢复零中断。



TopGate (TG-512/522/532-UTM)



TopGate(TG-502-UTM)



TopGate(TG-324/314-UTM)

## 2 产品特点

### ● 多功能与高性能的完美结合

TopGate 网络卫士安全网关是高性能与多功能的完美结合，它通过提供全系列产品而为不同类型的用户提供多功能与高性能的 UTM 产品。真正实现了一机多用，管理简单，节省大量成本。

TopGate 作为一款优秀的 UTM 产品，具备多种安全功能，既可以作为防火墙设备，也可以作为 VPN 设备、病毒网关或 IPS 设备，更重要的是这些功能融为一体，可同时任意组合使用，满足用户各种安全需求，为用户节省大量购置与维护成本：

- 1) 降低了复杂性：一体化设计简化了产品选择、集成和支持服务工作量。
- 2) 避免复杂的安装工作：容易安装和维护这些设备，可以远程操作进行。
- 3) 减少了维护量：这些设备通常都是即插即用，而且容易排除故障
- 4) 可以和高端软件解决方案协同工作：管理方式可以很好的和已安装的大型集中式的软件防火墙协同工作。
- 5) 简化了操作过程：降低了误操作隐患，提高了安全性。

## ● 完整的防火墙功能

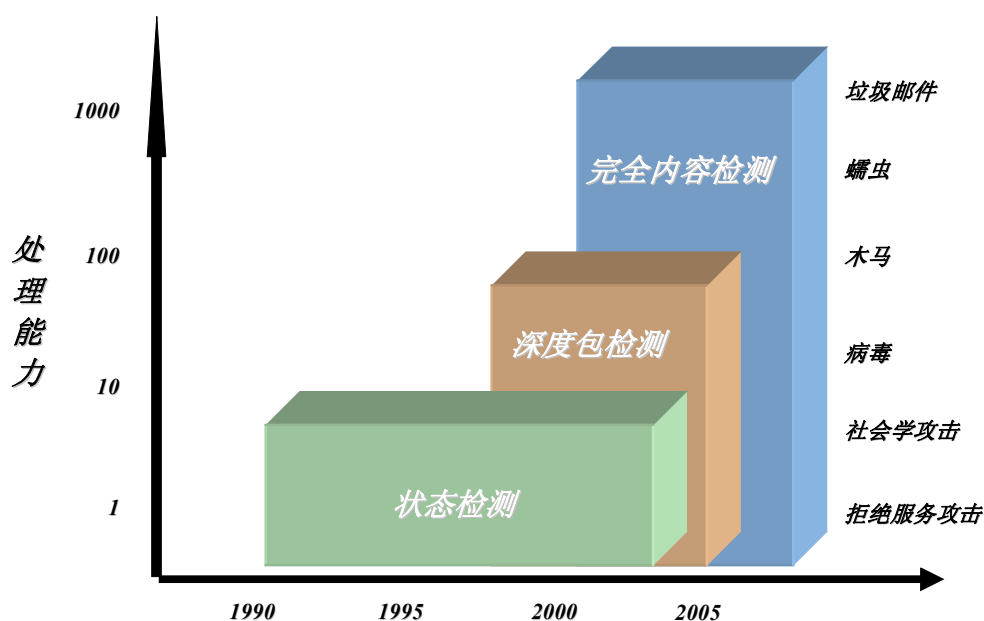
防火墙是网关设备重要的基本功能，TopGate 作为网关设备不但具有完整的 3 层协议以下的防火墙功能，而且还具有 4~7 层的防火墙防护功能。

## ● VPN 隧道内容过滤功能

企业对 VPN 应用越来越普及，但是当企业员工或合作伙伴通过各种 VPN 远程访问企业网络时，病毒、蠕虫、木马、恶意代码等有害数据有可能通过 VPN 隧道从远程 PC 或网络传递进来，这种威胁的传播方式极具隐蔽性，很难防范。

TopGate 同时具备防火墙、VPN、防病毒和内容过滤等功能，并且各功能相互融合，能够对 VPN 数据进行检查，拦截病毒、蠕虫、木马、恶意代码等有害数据，彻底保证了 VPN 通信的安全，为用户提供放心的 CleanVPN 服务。

## ● 完全内容检测 CCI 技术



CCI 是指 Complete Content Inspection，TopGate 采用了最新的完全内容检测技术，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。它不但可对还原出来的应用层数据进行病毒查杀、入侵防

御，还可检查是否存在不良 Web 内容、或是否属于间谍软件和网络钓鱼欺骗等其他威胁，真正实现了彻底检测和防范。

## ● 专业的安全服务选择

TopGate 在专业的安全服务方面可为用户提供多种选择：

### ➤ 防病毒服务

TopGate UTM 为用户提供了高效的防病毒引擎，用户通过购买防病毒服务，可获得最新的检测引擎和病毒库。防病毒服务为 TopGate 防病毒提供自动地更新，使它们能够防御最新的基于网络的攻击。在病毒库升级上可以用以下方法来满足不同客户的获得特征值和检测引擎升级的需求：①自动地“推动式升级”，②根据用户的时间表“拉动式升级”，③“立即升级”来当时获取升级。

TopGate UTM 能够 100%检测、消除感染现有网络的病毒和蠕虫，实时的扫描输入和输出邮件及其附件（支持 HTTP, SMTP, POP3, IMAP, FTP 等协议），高速度扫描技术。VPN 反病毒：消除 VPN 隧道的病毒和蠕虫，阻止远程用户及合作伙伴的病毒传播。

### ➤ 入侵检测和防御服务

TopGate UTM 入侵检测和防御系统帮助用户抵御恶意的或可疑的网络行为。用户通过购买入侵检测和防御服务，用户可通过图形化界面快速升级入侵检测和防御的检测库，为用户的新威胁提供安全保障。

TopGate UTM 的 IPS 模块是集访问控制、透明代理、数据包深度过滤、漏洞攻击防御、邮件病毒过滤、报文完整性分析为一体的网络安全设备，为用户提供完整的立体式网络安全防护。与现在市场上的入侵防御系统相比，新版本的 TopGate UTM 系统具有更高的性能、更细的安全控制粒度、更深的内容攻击防御、更大的功能扩展空间、更丰富的服务和协议支持，代表了最新的网络安全设备和解决方案发展方向，堪称网络入侵检测和防御系统的典范。

TopGate UTM 具有实时的网络入侵检测和阻断功能，它能够检测已知的 DOS、DDOS 攻击，以及绝大多数操作系统和应用协议的漏洞，还可对 MSN, Skype, Yahoo Messenger 等即时消息阻断，当监测到攻击时可同时向 3 个邮件地址自动发出警报。

## ➤ Web 内容过滤服务

TopGate UTM 的 Web 内容过滤服务用以防止未授权的 web 内容，保护企业网络。用户可以通过采购 Topgate UTM 的 web 内容过滤服务来保护企业网络。其特点是拥有庞大的 URL 数据库，包括庞大的 web 内容分类，域名分类，web 页面分类，配置极为方便。

TopGate UTM 处理所有的网页内容，阻挡不适当的内容和恶意脚本。支持 URL 域名、关键词模式匹配，支持黑白名单列表。支持 WEB 网页分类控制，数据库多达 2 千万条网站，上亿个网页类别，极高的识别率，可持续更新。免屏蔽列表：允许管理员设置专门的 URL 或关键字不被阻断。脚本过滤：阻止网页的插件，例如 ActiveX、Java Applets 和 Cookies。可定义的信息提示：支持内容过滤后的信息提示，可自编写提示页面。

## ● 管理

TopGate UTM在管理上通过浏览器界面，使用HTTPS, HTTP 远程登录管理；还可以通过命令行界面，使用SSH,Telnet 远程管理。

# 3 产品功能

类别	功能	详细描述
工作模式		◇ 支持透明、路由、混合、直连（虚拟线）模式

网络 安全性	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、IMAP、FTP 等协议的深度内容过滤。</li> <li>◇ 支持 URL 过滤。</li> <li>◇ 支持 DNS 过滤。</li> <li>◇ 支持 web 重定向。</li> <li>◇ 支持 HTTP URL 长度限制。</li> <li>◇ 支持伪装 http 连接识别。</li> <li>◇ 支持 DNS 过滤。</li> <li>◇ 支持 RSH 命令过滤。</li> <li>◇ 支持 telnet 命令过滤。</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>◇ 支持反垃圾邮件功能（用户配置黑白名单）</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和帐号过滤。</li> <li>◇ 可限制 BT, eMule, eDonkey, 迅雷等 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>
	防病毒	<ul style="list-style-type: none"> <li>◇ 支持 HTTP, FTP, POP3, SMTP, IMAP 协议的病毒查杀</li> <li>◇ 查杀邮件正文/附件、网页及下载文件中包含的病毒</li> <li>◇ 支持 100 万余种病毒的查杀，病毒库定期与及时更新</li> <li>◇ 支持木马病毒、蠕虫病毒、宏病毒、脚本病毒的查杀</li> <li>◇ 支持启发式扫描查杀未知病毒</li> <li>◇ 支持 ZIP/ARJ/CAB/RAR/GZIP/BZIP2 等压缩文件的病毒查杀</li> <li>◇ 支持 TAR 等多种打包文件的病毒查杀</li> <li>◇ 提供快速扫描及完全扫描两种扫描方式</li> </ul>
	访问控制	<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> <li>◇ 会话收集整理，由收集数据生成访问控制策略。</li> <li>◇ 访问控制策略分组管理。</li> <li>◇ 地址对象源目的发起连接数控制，支持全网段地址。</li> <li>◇ 支持大数量级的策略匹配加速算法。</li> <li>◇ 支持对于策略重复和策略冲突的检查。</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> <li>✧ 支持手动设置和根据 IDS 规则自动生成黑名单。</li> <li>✧ 支持手动设置和根据可信连接达到一定规模后升级为白名单用户。</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>
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、源/目的端口、协议类型、接口的策略路由。</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、BGP 动态路由协议。</li> <li>✧ 支持源路返回的智能选路方式。</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>✧ 交换口和子接口都支持 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> <li>✧ 支持对报文进行二次基于 802.1Q 封装的 vlan-vpn 应用。</li> </ul>
	生成树	<ul style="list-style-type: none"> <li>✧ 支持 802.1D 生成树协议。</li> </ul>
	端口聚合	<ul style="list-style-type: none"> <li>✧ 支持对物理端口的聚合, 提高带宽利用率。</li> <li>✧ 每个聚合组的端口数不做限制, 提高了聚合组的配置灵活性。</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> <li>✧ 可设置防 ARP 欺骗。</li> </ul>
	DHCP	<ul style="list-style-type: none"> <li>✧ 支持 DHCP Client、DHCP Server、DHCP relay。</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	<ul style="list-style-type: none"> <li>✧ 支持 X.509 V3 数字证书, 支持 DER/PEM/PKCS12 多种证书编码。</li> </ul>

	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> </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>
IPSEC VPN	协议	◇ 支持 ESP/AH/IKE/NATT 等标准 IPSEC 协议，支持隧道模式、传输模式
	算法	<ul style="list-style-type: none"> <li>◇ 支持 DES/3DES/AES 等标准加密算法，支持 MD5/SHA1 等标准 HASH 算法</li> <li>◇ 支持 DH GROUP1/2/5, RSA 1024/2048 非对称算法</li> <li>◇ 支持国家商密专用的 SSP02/SSF33/SCB2 算法</li> </ul>
	硬件加速	◇ 支持高速算法加速卡
	数据压缩	◇ 支持高效数据流压缩算法
	隧道认证	◇ 支持预共享密钥、数字证书认证，支持扩展认证
	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> <li>◇ 支持 GRE over IPsec 方式</li> <li>◇ 支持组播穿越 IPsec 隧道</li> <li>◇ 支持动态路由协议通过 IPsec 隧道扩散</li> <li>◇ 支持采用 XAUTH 的 IKE 协商</li> <li>◇ 支持隧道利用技术，单隧道承载多保护子网的方式</li> </ul>
	可信接入	<ul style="list-style-type: none"> <li>◇ 支持基于角色的可信接入</li> <li>◇ 支持检查接入机的操作系统</li> <li>◇ 支持检测操作系统的补丁</li> <li>◇ 支持可信接入分级授权</li> </ul>
	DDNS	<ul style="list-style-type: none"> <li>◇ 内置免费 DDNS 客户端与账号</li> <li>◇ 支持采用 DNS 域名建立隧道</li> </ul>
	集中管理	<ul style="list-style-type: none"> <li>◇ 支持 TopPolicy 的集中认证；</li> <li>◇ 支持 TopPolicy 集中制定并下发隧道策略；</li> <li>◇ 支持 TopPolicy 集中监控隧道状态、设备状态和移动用户状态；</li> <li>◇ 支持 TopPolicy 的集中远程配置。</li> </ul>
	流量统计	<ul style="list-style-type: none"> <li>◇ 支持隧道内加解密成功、失败流量统计</li> <li>◇ 支持隧道内认证成功、失败流量统计</li> <li>◇ 支持隧道持续时间统计等</li> </ul>
负载与备份	<ul style="list-style-type: none"> <li>◇ 支持多条隧道的负载均衡</li> <li>◇ 支持多条隧道的备份与自动切换</li> <li>◇ 支持多机之间的流量负载与自动切换</li> <li>◇ 支持隧道、专线之间的备份与自动切换</li> </ul>	

	移动客户端	<ul style="list-style-type: none"> <li>◇ 支持第三方标准 IPsec 客户端接入</li> <li>◇ 支持 VRC 客户端接入</li> <li>◇ 支持用户+口令的接入认证</li> <li>◇ 支持基于数字证书的接入认证</li> <li>◇ 支持动态口令卡接入认证</li> <li>◇ 支持证书+口令双因子认证</li> <li>◇ 支持 USB KEY 模式的身份认证</li> <li>◇ 支持移动用户硬件特征码认证功能</li> <li>◇ 支持为移动用户自动分配内部 IP 地址、DNS/WINS 服务器地址；</li> <li>◇ 支持基于角色的访问权限控制</li> <li>◇ 支持 Radius 下发权限</li> <li>◇ 支持 AD 服务器下发权限</li> <li>◇ 支持给证书用户单独授权</li> <li>◇ 支持基于时间的移动用户访问控制策略；</li> <li>◇ 支持多线路自动检测</li> <li>◇ 支持用户修改口令</li> <li>◇ 支持标准 X509 证书</li> <li>◇ 支持第三方 CA 认证</li> <li>◇ 支持本地用户认证、外部 Radius 认证、LDAP 认证、AD 认证等</li> <li>◇ 支持移动用户两网分离，支持安全版、限制版</li> <li>◇ 支持英文版，支持中英文切换</li> </ul>
安全接入	L2TP	◇ 支持远程用户通过 L2TP 接入，建立 L2TP 隧道访问内部网络
	PPTP	◇ 支持远程用户通过 PPTP 接入，建立 PPTP 隧道访问内部网络
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 日志格式的输出。</li> <li>◇ 支持日志分级和按类型输出。</li> <li>◇ 支持通过第三方软件来查看日志。</li> <li>◇ 可对日志进行加密传输。</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> </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>

	流量统计	<ul style="list-style-type: none"> <li>◇ 支持基于 IP 对 session 数的统计, 并有阈值报警功能。</li> <li>◇ 支持基于 IP 对流量的统计。</li> <li>◇ 支持基于传输层端口进行流量、session 数的统计。</li> <li>◇ 支持 NETFLOW 协议版本 5, 支持设置过滤条件。</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> <li>◇ 支持根据源/目的进行独享的带宽管理方式。</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-Standby)。</li> <li>◇ 支持负载均衡模式 (Active-Active)。</li> <li>◇ 支持连接保护模式 (Session Protect)。</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> <li>◇ 支持接口 Metric 值。</li> <li>◇ 支持连接同步确认。</li> <li>◇ 支持自动的配置同步功能。</li> <li>◇ 支持多台设备的配置同步。</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 TP 管理。</li> <li>◇ 支持基于 SSH、HTTPS 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>◇ 支持命令历史、命令补齐、命令错误提示等功能。</li> </ul>
	WEBUI	<ul style="list-style-type: none"> <li>◇ 支持初装配置向导。</li> <li>◇ 支持配置即时定义。</li> <li>◇ 支持即时的配置和状态提示。</li> <li>◇ 支持中文联机帮助。</li> <li>◇ 支持 HTTPS 客户端证书认证方式。</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>
	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> <li>◇ 支持 webui 升级。</li> <li>◇ 支持 ftp 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>◇ 可以进行完整配置的下载备份、上载恢复</li> <li>◇ 可以进行部分配置本地和异地的批量导出和导入。</li> </ul>
	时钟调整	◇ 支持网络时钟协议 <b>SNTP</b> ，可自动根据 <b>NTP</b> 服务器时钟调整本机时间。
入侵防御	工作模式	◇ 支持直连模式和 ( <b>IDS</b> 监听)。
	入侵防御	<ul style="list-style-type: none"> <li>◇ 支持路由、交换、直连、<b>IDS</b> 监听四种模式。</li> <li>◇ 支持基于源、目的、规则集的入侵检测。</li> <li>◇ 支持自定义动作。</li> <li>◇ 支持时间对象。</li> <li>◇ 支持与防火墙联动。</li> <li>◇ 支持 <b>bypass</b>。</li> </ul>
	DDOS 防御	<ul style="list-style-type: none"> <li>◇ 非法报文攻击: <b>land</b>、<b>Smurf</b>、<b>Pingofdeath</b>、<b>winnuke</b>、<b>tcp_sscan</b>、<b>ip_option</b>、<b>teardrop</b>、<b>targa3</b>、<b>ipspooof</b>。</li> <li>◇ 统计型报文攻击: <b>Synflood</b>、<b>Icmpflood</b>、<b>Udpflood</b>、<b>Portscan</b>、<b>ipsweep</b>。</li> <li>◇ 可记录攻击日志和报警。</li> </ul>
	规则库维护	<ul style="list-style-type: none"> <li>◇ 支持自定义规则库导入、导出。</li> <li>◇ 支持系统规则库手动、自动升级。</li> </ul>
	系统规则	系统定义超过 <b>2200</b> 条规则, 包含 <b>Backdoor</b> , <b>bufferoverflow</b> , <b>dosddos</b> , <b>im</b> , <b>p2p</b> , <b>vulnerability</b> , <b>scan</b> , <b>webcgi</b> , <b>worm</b> , <b>game</b> 。
	自定义规则	<ul style="list-style-type: none"> <li>◇ 支持自定义规则。</li> <li>◇ 支持自定义规则集。</li> </ul>

## 4 运行环境

电源:

TG-532/522/512-UTM 电源:

电压: AC100~240V

频率: 60~50HZ

电流: 8~5A

功率: 400W (MAX)

冗余: 支持

TG-502-UTM 电源:

电压: AC100~240V

频率: 60~50HZ

电流: 8~5A

功率: 350W (MAX)

冗余: 不支持

**TG-324/314-UTM 电源:**

电压: AC90~260V±10%

频率: 63~47Hz

电流: 8~5A

功率: 200W (MAX)

冗余: 不支持

**环境:**

**TG-532/522/512/502-UTM 环境:**

运行温度: 0~40 摄氏度

非运行温度: -40~70 摄氏度

相对湿度:5~95%RH, 非冷凝

**TG-324/314-UTM 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%RH, 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

IEC 61000-4-2 (静电放电 ESD 抗扰度)

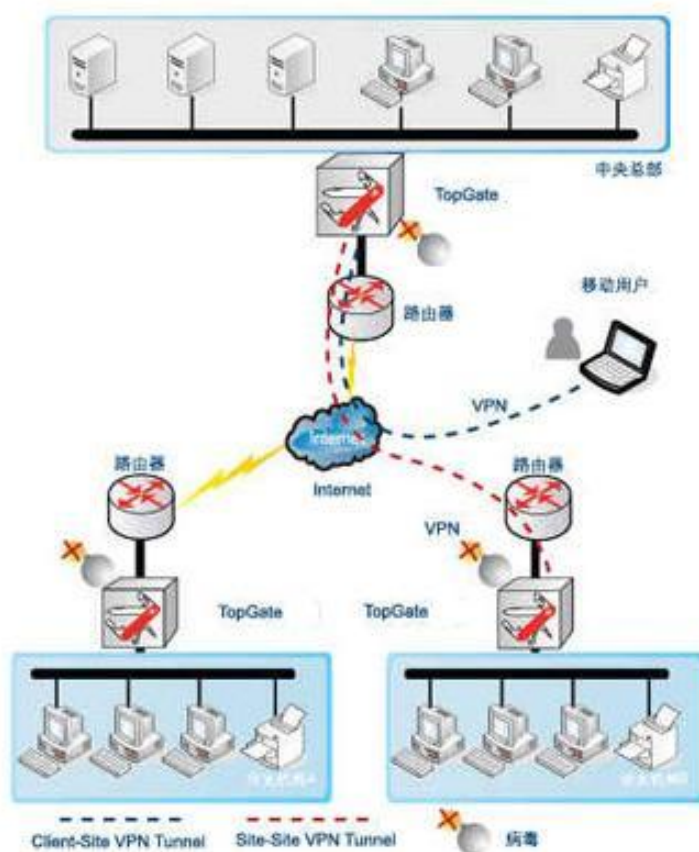
IEC 61000-4-3 (射频电磁场抗扰度)

IEC 61000-4-4 (电快速瞬变 EFT 抗扰度)

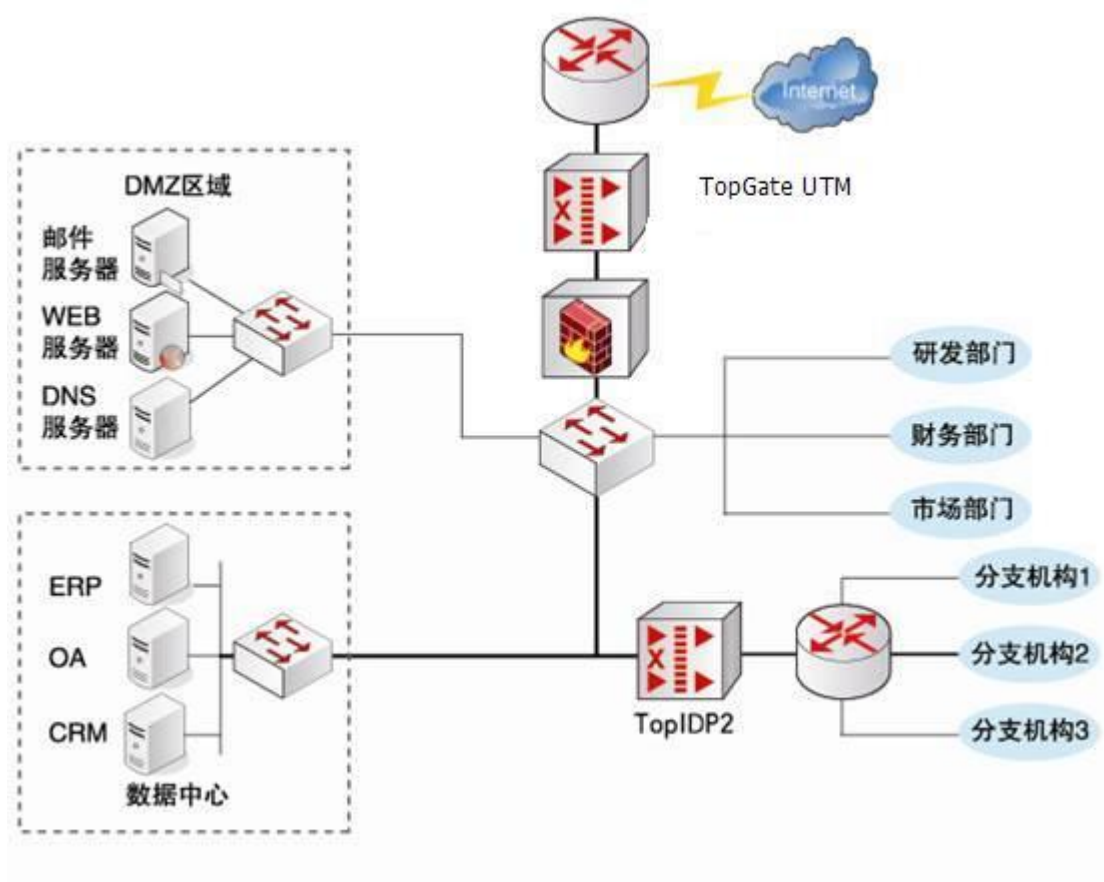
IEC 61000-4-5 (浪涌 Surge 抗扰度)

## 5 典型应用

TopGate网络卫士安全网关部署在企业网络入口。TopGate 中高端产品可部署于企业总部，TopGate 中低端产品可部署于各分支机构。既可以防范网络攻击、控制非法访问，也可以阻挡病毒入侵、免受垃圾邮件干扰，同时分支与总部之间、远程用户与企业网络之间可以进行CleanVPN访问，为整个企业提供了完整的混合威胁防护解决方案，让企业真正做到轻松防范各种威胁，有效保证企业业务正常运转。



面对复杂多变的网络环境，企业不仅需要有针对性重点区域的防护，还需要针对内部整个网络的全面防护。此时就需要在企业网络的出入口和重点服务器处分别部署TopGate网络卫士安全网关。两种部署方式的相互配合可以更好地保护企业的重要信息资产、提高企业网络整体的安全水平。部署示意图如下。



## 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
《涉密信息系统产品检测证书》	国家保密局涉密信息系统安全保密测评中心
《军用信息安全产品认证证书》	中国人民解放军信息安全测评认证中心

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。