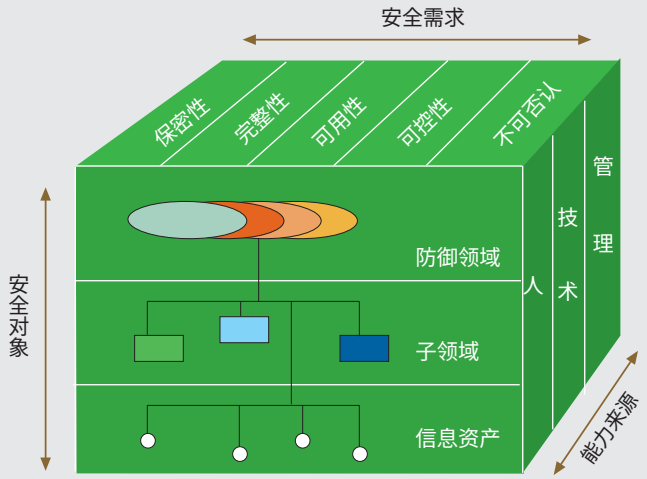
# LinkTrust®
## Unified Threat Management
## 领信网络统一威胁管理解决方案

"Threat management security appliances are defined as a combination of hardware, software, and networking technologies whose primary function is to perform specific or multiple security functions. Threat management security appliances consist of hardware with a hardened operating system (OS), a limited applications set, and no user software installation. Threat management security appliances may also include other features such as security management, policy management, quality of service (QoS), load balancing, high availability, and bandwidth management. However, these features are designed only to support the primary security workload." -- IDC Report "worldwide Threat Management Security Appliances 2004-2008 Forecast and 2003 Vendor Shares:The Rise of the Unified Threat Management Security Appliance"

随着各种新应用的出现和网络业务的扩张，传统概念上的网络边界已经越来越模糊，由于多业务、多应用共同增长，使边界触角已经深入到网络中各个环节，相伴相生的各种基于内容的攻击(如SQL Slammer,MSBlaster等)使得人们对网络应用层安全的关注上升到了一个前所未有的新高度。纵览现在很多企业或组织的安全基础设施，很多安全防护设计架构还是基于传统的防火墙加网络入侵检测结构，在面对这些新式复合性威胁的时候，我们窘迫地发现，这些针对单一威胁进行设计的安全方案不再如以往那么表现出色，显得是那么力不从心，过时的设计已经远远满足不了对付新一代网络威胁的安全需要了。“ 魔高一尺，道高一丈 ”，新威胁的出现也对新的网络安全技术和措施提出了新需求—— 市场需要有能应对不断增长的新威胁的安全设备，而它还要能满足基于网络和基于应用层面的多种新型威胁的整体安全防护。

LinkTrust® UTM是安氏领信科技发展有限公司所开发的领信(LinkTrust)家族产品中的一员，它特别为面向网络威胁统一管理市场需要而专门设计。它基于国际先进的高可靠性嵌入式硬件平台，以领信安全实验室 “ LinkTrust® Security Lab ” 的网络安全软件平台LTOS为核心，在LTOS核心层融会设计了安全检测引擎，并高度集成了被市场多年来证明是行之有效的防病毒、防火墙、内容安全控制、入侵检测/防护、高可用性、VPN、带宽管理、Anti-X服务、多媒体通信安全、认证授权、远程安全接入等众多安全技术于一身，提供了全套高安全性、高可信度和高健壮性的安全解决方案。它可以对来自Internet和内部网的基于内容的混合攻击进行很好防护，实现了单一设备对网络的全方位防护。

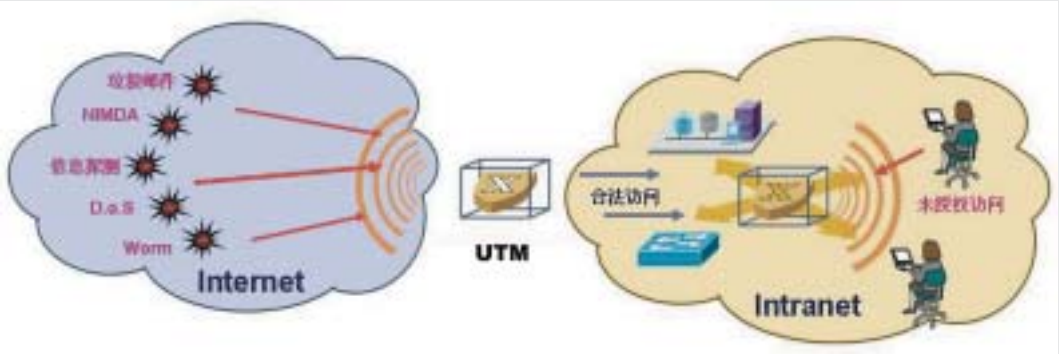
领信家族产品的设计理念采用了安氏领信信息安全保障模型理论，突破了传统理论局限将安全防护深入到了安全保障领域；该理论以安全需求、安全对象和能力来源为基础，通过划分防御领域来区别对待防御措施，以此构成一个立体深度防御体系。作为该体系中的重要组成部分——主动防御体系（Proactive Protection System）的核心部件，LinkTrust® UTM可为企业网提供完整的内容安全解决方案，而通过一体化的新型芯片和支持内容处理的软件架构使其具备概念独创、技术先进、性能优异、健壮稳定等多项特性。




安氏信息安全保障模型

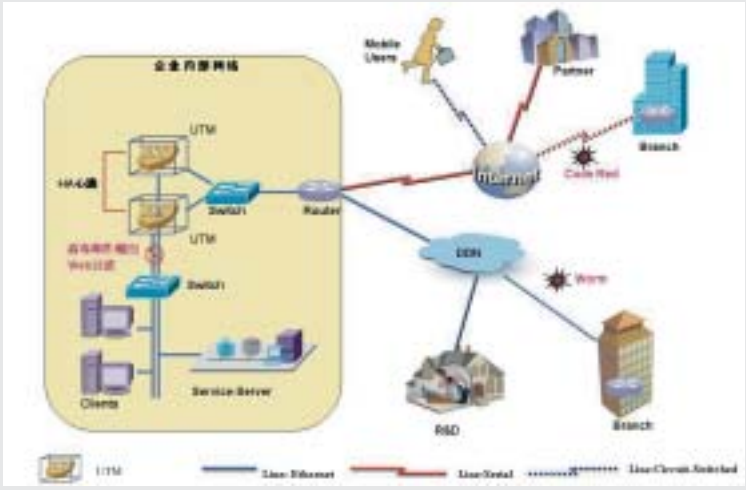
LinkTrust® UTM的设计目标之一就是为用户提供高性能的、高可靠性的、多功能整合型的一体化安全解决方案，除了要可对用户资产提供永续化的可信赖安全保护之外，还要能在最大程度上提供高效的网络层和应用层上的安全防护。

基于此，LinkTrust® UTM应用多种安全手段来实现这个目标，它采用了状态检测防火墙技术来提供网络层的防护，进而识别非法网络访问、非法报文、无效包头和各种网络层攻击；它应用安氏领信专有的抗拒绝服务攻击技术可有效对抗对多种网络Flood攻击，其中SynProxy技术更是对SynFlood有特效；它采用深度包检测引擎技术提供应用级别上的内容安全防护，再配合反病毒和反垃圾邮件等综合过滤技术后，更使其具备超强过滤和深度防护能力。




全方位Anti-X防御

LinkTrust® UTM提供了丰富的应用程序安全防护、Anti-X防御、安全接入和细粒度访问控制等技术，对于中小企业用户来说，这种“多合一”解决方案特别适合其资金预算有限情况下的最大投资回报。它多功能组件的可配置性保证了系统整体功能可灵活定制，而简化配置、易于上手操作、快速故障排除和“即插即用”的便利性也特别适合一般用户的需求，其不经意间所显现出的高性能表现更会给您带来惊喜。LinkTrust® UTM不但能为保护企业网络提供广泛而深入的安全功能，还能降低与实现这种全新安全水平相关的总部署成本、总运营成本及复杂性。




多应用安全防护部署

在复杂的分布式部署环境中，您也不用担心由“于机构规模快速增长所带来的维护烦恼，LinkTrust® UTM提供强大的集群化统一安全管理平台——“LinkTrust® GSM领信集中安全管理系统”，它可为全网LinkTrust® UTM安全威胁库（防病毒、反垃圾邮件、攻击检测特征库等）提供统一的集中式升级管理服务，能有效地提高工作效率，保证网络持续具备最新安全防护能力。

LinkTrust® GSM领信集中安全管理系统以管理企业全网系统的安全策略为核心，以安全事件为驱动，实时监控设备工作状态，提供全网范围内安全事件与网络信息的集中、分析、审计与报告功能，通过风险评估能发现潜在的攻击征兆和系统安全态势，确保任何安全事件、事故得到及时的响应和处理，并可与安全策略形成灵活高效的双向互动通道，保证网络系统的安全最大化。


分布式环境下的统一管理

实时状态监控

集中安全管理

# 主要特性

■ 主动防护系统（PPS）

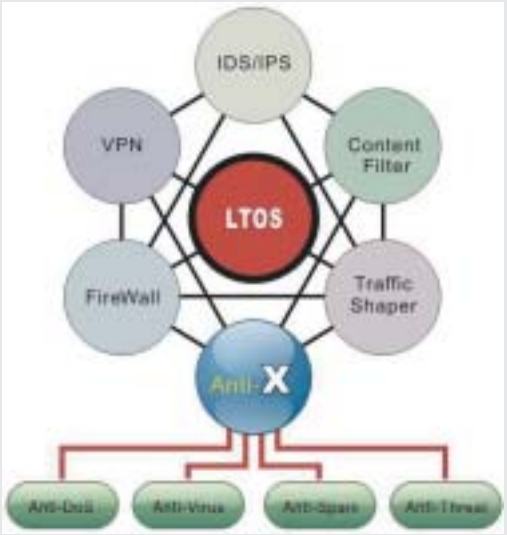
Proactive Protection System可实时检测系统状态，可对基于网络和基于应用的威胁尚未入侵到核心应用之前，就发出威胁预警并采取动态防御措施。

■ 状态检测防火墙引擎

在网络层由检查引擎截获数据包并抽取出与应用层状态有关的信息，维护一个动态状态信息表并对后续数据包进行检查,并以此作为依据来确定是否允许数据通过，它可有效的发现并阻断伪造数据包和地址欺骗等攻击。

■ 深度包检测（L7）引擎

该引擎可对网络数据流中应用层的负载数据进行检查，并根据数据特征库对数据内容进行对比分析以作出进一步判断。该引擎采用了统计建模、异常分析、状态检测等方面技术，不仅仅维持了底层上的网络连接，同时也维持着应用层通讯隧道状态。




主动防御体系
Proactive Protection System

■ 攻击检测（IDS）和防护机制（IPS）

内置超强特征签名库可对各种端口扫描、信息探测、恶意攻击进行准确检测与有效阻断，使其对应用层攻击具备了全方位防护能力，特有的流量Mirror Port功能使网管对网络活动了如指掌。

■ Anti-X机制

Anti-DoS、Anti-Virus、Anti-Spam和Anti-Threat防御技术能根据事件风险分析对各种混合威胁进行有效防护，终止威胁流量，特有的关联预警能力可检测并实时适应新威胁。

■ 高层协议分析机

以深度包检测引擎为基础，并可使系统具备强劲的内容处理能力，除可对Web内容（如URL、JavaScript/JavaApplet插件和ActiveX控件等）进行过滤外，还可对垃圾邮件和不良内容进行筛选和鉴别，并具备即时消息（MSN、Yahoo Messenger等）过滤能力。

■ 嵌入式病毒引擎

可实时检测出隐含在高层应用协议中的病毒、木马、蠕虫和恶意代码，除了实时响应、主动阻断之外还可动用多种手段通知到管理员。

■ 垃圾邮件检测引擎

智能识别多国语言，配合采用连接控制、转发控制、邮件控制、目录攻击控制、异常控制、流量控制和延时投递等综合安全控制手段，可达到95%以上的识别率和低于3%的漏报率的效果，还您一“安静”的数字空间。

■ 服务质量保证（QoS）

精细粒度的Traffic Shaper提供保证带宽、最大带宽、上下行流量管理和带宽优先级设置，确保关键服务的QoS，充分满足用户网络带宽管理的各种需求。

■ 企业级虚拟网络（VLAN）

支持高达32个802.1q VLAN子接口划分，结合多安全域划分手段为企业级内网管理问题提供彻底解决方案。

■ 虚拟专用网（VPN）

支持标准工业级的IPSec、PPTP、L2TP VPN，SSL VPN；桥下VPN功能不需对网络地址重新规划就可让私密数据享受高强度安全防护，而NAT-T（NAT穿越）以及星型连接更使网络具备灵活的扩展能力。

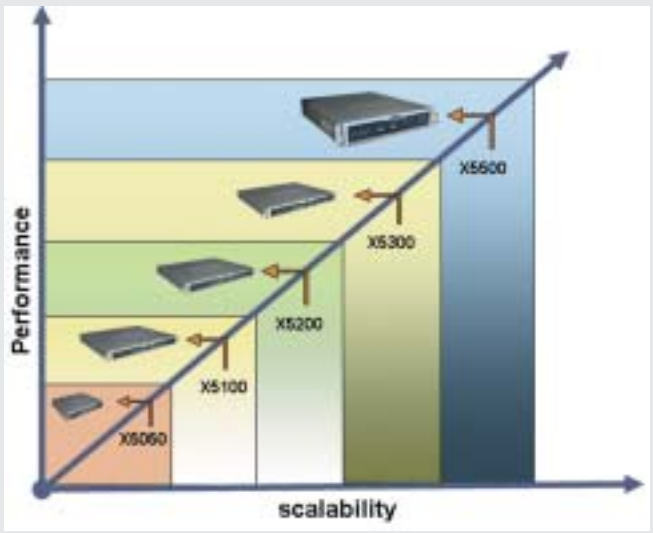
■ 高可用性（HA）

小于1秒的HA快速切换能力可避免因单点故障而导致的关键业务失败，亦可对后台多个服务器提供超强负载均衡能力。

■ 分权管理与强制认证

提供符合GB/T 18336-2001安全设计要求的分级管理体系，AAA认证协议可保证对用户身份强制认证和安全审计。

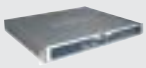
遵循安氏信息安全保障模型理念设计的领信家族产品能为各种规模的客户提供全面、实时的安全保障，其广泛的产品线可满足从远程用户、SOHO、小型办公室，到企业分支机构、电子商务站点、大型企业总部，再到电信级、网络服务运营商、数据中心网络环境的安全需求。




| | |
|---|---|
| X5050 | X系列中专门针对SOHO一族和家庭用户安全防护需求而特别设计的桌面级产品。它采用高效低能耗处理器，并应用了“即插即用”式部署方式，支持PPPoE协议，提供ADSL接入方式，同时在网关处提供对Web和邮件的内容过滤处理和病毒防护能力，免维护的病毒库可在线自动升级，免除用户因忘记升级病毒库所引起的病毒入侵。 |
| X5100 | X系列的部门级产品，它通过集成的防蠕虫、防火墙、Anti-Spam、Anti-DoS、VPN、Traffic Shaper、认证、审计等全方位防护手段为企业级用户提供完善的解决方案。它可以满足企业分支机构设计对一体化安全解决方案的需求。 |
| X5200 | X系列的企业级产品，它充分考虑了大部分企业的安全需求而设计。其内嵌的病毒检测引擎可以通过优化内容搜索、模式识别和数据分流等技术，使您的网络避免因Web冲浪和邮件收发导致的病毒、木马和蠕虫入侵，给您创造一个绿色安全的网络世界。 |

| | |
|---|---|
| X5300 | 融合了高效防病毒处理引擎和攻击防护机制的X5300专为企业核心设计，通过集成的防蠕虫、防火墙、Anti-X、VPN、Traffic Shaper、认证、审计等全方位防护手段为企业级用户提供高度安全的一体化解决方案，它可以使企业网轻松面对种种复杂恶意攻击。 |
| X5500 | X系列的旗舰产品，它可以满足大型企业及ISP网络对千兆级产品的需求。X系列所特有的全对等安全域设计理念加上对802.1Q VLAN的支持，使其可以轻松自如部署在各种典型环境中，结合其强大的VPN加密安全协处理器可以提供惊人的加解密能力；小于1秒的HA快速切换能力可避免因单点故障而导致的关键业务失败,保证了设备不停机永续化工作，而支持多ISP接入能力更使其具备高灵活性。 |

LinkTrust® UTM系列

| 详细指标 | | X5050 | X5100 | X5200/VPN Plus | X5300/VPN Plus | X5500 |
|---|---|---|---|---|---|---|
| | |  |  |  |  |  |
| 系统配置 | 机型 | Mini | 1U | 1U | 1U | 2U |
| | Flash | 64M | 64M | 64M | 64M | 64M |
| | 10/100Base-TX (Fast Ethernet) | 3 | 4 | 4 | 6 | N/A |
| | 1000Base-TX (Gigabit Ethernet) | N/A | N/A | N/A | N/A | 4 |
| | 1000Base-SX (Gigabit Ethernet) | N/A | N/A | N/A | N/A | 2 多模/SC接口,可扩充 |
| | 最大VLAN接口数 | 15 | 32 | 100 | 100 | 100 |
| 系统性能 | 防火墙吞吐量 | 100 Mbps | 300Mbps | 400Mbps | 600Mbps | 3Gbps |
| | 威胁流量处理能力 | 50 Mbps | 150Mbp | 280Mbps | 400Mbps | 2Gbps |
| | VPN吞吐量(AES+MD5) | 60 Mbps | 270Mbp | 300Mbps | 350Mbps | 800Mbps |
| | IPSec隧道数 | 128 | 512 | 1,024 | 2,048 | 10,000 |
| | VPN拨号用户数 | 50 | 128 | 256 | 256 | 1024 |
| | 最大并发连接数 | 80,000 | 400,000 | 500,000 | 800,000 | 1,500,000 |
| | 每秒最大新建连接数 | 4,000 | 12,000 | 19,000 | 20,000 | 60,000 |
| | 最大策略数 | 1,024 | 2,048 | 4,096 | 10,000 | 20,000 |



LinkTRUST 安氏
安氏领信科技发展有限公司
LinkTrust Technologies Development Co., Ltd.
中国北京市海淀区北三环西路43号青云国际研发中心A座三层（100086）
Floor 3 Tower A,Beijing Keeven International Research & Development Center,
No.43,West Road,North Third Ring Haidian District,Beijing100086 PR China
电话：(010)82119889
传真：(010)82119880
网址：www.linktrust.com.cn