Systrix UTM LAN Gate

技术白皮书

地址: 广东省广州市天河区科韵路 24-26 号天河软件园禾田大厦 8 层
电话: 86-20-85571438 传真: 86-20-85572063

目 录

前言 **3**

版权申明 *3*
商标申明 *3*
有限保证 *3*
LAN Gate支持解决方案 *4*
有关LAN Gate 产品的更多信息 *4*

产品简介 **5**

简介 5
关键技术 5

产品功能和特点 **6**

产品优势 6
主要的特性和益处 6
LAN Gate管理界面 *7*
基于网络的防病毒 *7*
基于用户策略的安全管理 *7*
VPN功能 *7*
防火墙功能 *8*
内容过滤功能 *8*
入侵检测功能 *8*
带宽管理功能 *9*
垃圾邮件过滤防毒功能 *9*
系统报表和系统自动警告 *9*
LAN Gate提供整体解决方案 *9*
LAN Gate 系列产品性能一览表 *10*

产品系列介绍 **12**

LG-40 12
LG-1040 12
LG-2040 12
LG-3060 12
LG-4060 12
LG-5060 12
LG-6060 13

LAN GATE典型应用方案 **14**

中小型企业应用 14
大中型企业应用 15

分布型企业应用 16

前言

欢迎阅读 LAN Gate 技术白皮书。本技术白皮书为您提供 LAN Gate 安全设备的技术框架和功能应用信息。

注：请定期登录<http://www.systrix.net/product-download.html>查看本用户手册及其他 LAN Gate 产品与服务文档的最新版本。

版权申明

商标申明

有限保证

Systrix Technologies 保证产品在材料及工艺方面无缺陷，保证期从产品发送到客户的发货期（在任何情况下都不得超过 Systrix Technologies 最初发货后九十［90］天内）算起十二（12）个月内，前提是正常使用。此有限保证仅适用于产品原始最终用户，不得转让。Systrix Technologies 及其供应商的全部责任以及客户的唯一补救是发送替换产品。Systrix Technologies 可自行决定替换产品在功能上与原产品相当或更强大，在质量上最新或几乎全新。从客户按照 Systrix Technologies 的一贯支持服务策略的条款退回有缺陷的产品，Systrix Technologies 即开始承担此保证下的责任。

此保证不适用于由于异常电应力、意外损坏、滥用、误用或错误应用、或未经 Systrix Technologies 书面允许进行修改等造成故障的产品。

保证免责声明。除本保证规定的范围外，所有明示或暗示条件、表述及保证，包括但不限于任何暗示的可销售性、特殊用途合适性、不侵权、令人满意的质量或由于交易、法律、使用或贸易惯例导致的保证

或条件，且都不包括在适用法律允许的最大范围内。对不能包括在保证范围内的暗示保证，该保证仅限于在保证期内。因为一些州或司法部门不允许限制暗示保证的期限，上述限制可能仅限于您。此保证赋予您特殊的法律权利，且根据当地法律，您也可能享有其它权利。本免责声明和排除条件同样适用于规定了上述基本用途故障的明示保证。

责任免责声明。Systrix Technologies 的唯一责任是依照上述有限保证发送替换产品。Systrix Technologies 或其供应商在任何情况下都不对任何形式的损坏承担责任，包括但不限于利润损失、业务中断、信息损失或其他由于产品的使用或无法使用而导致的金钱上的损失，或由于使用或无法使用硬件或软件所引起的特殊、间接、后续性、附带或惩罚性损失，即便 Systrix Technologies 或其供应商已经得到可能会发生该损失的通知。在任何情况下，Systrix Technologies 或其供应商对客户的债务，无论是在合同、民事侵权行为（包括疏忽）或其他，都不得超过客户支付的价格。即使在上述保证未履行其基本目的的情况下，以上限制仍然适用。

LAN Gate 支持解决方案

LAN Gate 功能强大的安全解决方案为您的网络提供空前的保护，免受各种互联网攻击和内部攻击的威胁。LAN Gate 的综合支持服务保护您的网络安全投资并为您提供您所需的支持服务——无论您何时需要。

有关 LAN Gate 产品的更多信息

有关 LAN Gate 产品及服务的更多信息，请与 Systrix Technologies 联系：
网址：http://www.systrix.net
E-mail：solutions@systrix.net
电话：86-20-85571438
传真：86-20-85572063

产品简介

简介

LAN Gate 是专用的基于专用芯片的硬件产品，在网络边界处提供了实时的保护。基于 LANGate OS，LAN Gate 能够在不显著影响网络性能情况下检测有害的病毒、蠕虫及其他基于内容的安全威胁的产品，系统还集成了***防火墙、VPN、入侵检测、垃圾邮件过滤和防毒、内容过滤和流量监控和带宽管理***功能。并且提供了高性价比、方便的和强有力的解决方案来检测、阻止攻击，防止不正常使用和改善关键网络应用的服务。能够在不降低网络运行性能的前提下优化网络通讯资源。

LAN Gate 是一个易管理的安全设备，它具备如下系列服务：
•应用层服务--- 如防病毒保护、内容过滤、垃圾邮件过滤和防毒。
•网络层服务--- 如防火墙，入侵检测、VPN、流量监控和带宽管理等。

LAN Gate 家族产品的每一款都具有管理灵活、性能全面的特性，可为企业提供多层次的防护措施，包括应用层的病毒防护、内容过滤服务以及在网络层的防火墙、入侵检测、虚拟专用网（VPN）、流量监控和带宽管理等服务措施。

关键技术

专用硬件平台
采用专用芯片直接在网络上实现流重组，数据包的内容检查和特征匹配等，查找速率可以达到上亿字节每秒，网络中的流量直接在专用芯片中处理，高速转发、阻断、限流、统计分析；LAN Gate 设备稳定，高效，在保障用户网络安全的前提下，不影响正常的网络传输。

产品功能和特点

产品优势

提供完整的网络保护： 基于网络的病毒防御，WEB 内容过滤，防火墙，VPN，IDS，带宽管理和垃圾邮件过滤和防毒功能	用户策略提供了灵活的网络分段和策略控制能力
保持网络性能的基础下，消除病毒和蠕虫的威胁	VLAN（802.1q）支持 提供了 HA 高可用端口，保证零中断服务
基于专用的硬件体系，提供了高性能和高可靠性	强大的系统报表和系统自动警告功能
Systrix 服务器提供了 24*7 的不间断自动更新	多种管理方式：SSH；SNMP；WEB。基于 WEB（GUI）的配置界面提供了中/英文语言支持

主要的特性和益处

特性	描述	益处
基于网络的病毒防御	实时检测和清除病毒和蠕虫。扫描进出的 E-MAIL 附件(SMTP,POP3)	在网络的边界处消除了危险的入侵
防火墙	业界标准的状态检测防火墙	安全可靠的系统防御，良好的性能和稳定性
WEB 内容过滤	处理所有的 WEB 内容，可以屏蔽有害的 WEB 页面和代码，支持 URL 和关键字	提高企业的生产力，有效利用网络资源，提供了完善的管理和监控能力
VPN	业界标准的 PPTP，L2TP 和 ICSA 认证的 IPSEC 支持	极大降低的运营及管理成本，使企业可以在 Internet 上构筑自己的私有网络
IDS（入侵检测）	可选择的数据库（>1000）	监控外部的攻击
透明模式	提供网桥模式下 WEB 内容过	适应复杂的网络环境，简化配

	滤，策略控制等应用	置和管理
远程访问	支持远程用户的加密访问，提供了 IPSEC 客户端软件	提供了廉价的无处不在的网络服务和安全控制

LAN Gate 管理界面

LANGate 提供了非常友好的基于 WEB（GUI）的管理界面，支持多种管理语言(中文、英文)。
LANGate 的 SSH 命令行管理界面为网络管理和调试提供了方便。
LANGate 支持 SNMP 协议，可通过网管软件对防火墙进行管理。

为保证防火墙自身的安全，LANGate 提供分级管理机制，并可设置允许从防火墙的哪一个端口及哪一种管理界面进行管理。

基于网络的防病毒

互联网是一个连接全球丰富资源的大网络，它让成千上万亿的线上用户运用廉价（或免费）的资料，交换彼此的想法、直接而实时的沟通。随着互联网应用的飞速发展，用户对网络信息的依赖性也倍速增长，网络病毒也伴随着网络的发展而迅速增长，互联网的技术支持需求随之成为企业 IT 部门最主要的业务负担。为了保障互联网的畅通和安全，为网络全方位安全而设计基于网络的 LAN Gate 系列无疑是 IT 人员的最佳帮手。LAN Gate 是网关级的安全设备，它不同于单纯的防病毒产品。LAN Gate 在网关上做 HTTP、SMTP、POP 和 IMAP 的病毒扫描，并且可以通过策略控制流经不同网络方向的病毒扫描或阻断，其应用的灵活性和安全性将消除用户不必要的顾虑。

基于用户策略的安全管理

整个网络安全服务策略可以基于用户进行管理，相比传统的基于 IP 的管理方式，提供了更大的灵活性。

VPN 功能

LAN Gate 产品系列工业标准的 VPN 在两个 LAN Gate 保护的网络或 LAN Gate 与支持 IPSec、PPTP 或 L2TP 的第三方 VPN 保护的网络之间建立加密流量传输隧道。

LAN Gate VPN 的特性包括以下几点
支持 IPSec 安全隧道模式
支持基于策略的 VPN 通信
硬件加速加密 IPSec,DES,3DES
X509 证书和 PSK 论证
集成 CA

HMAC MD5 或 HMAC SHA 认证和数据完整性
自动 IKE 和手工密钥交换
SSH IPSEC 客户端软件, 支持动态地址访问，支持 IKE
通过第三方操作系统支持的 PPTP 建立 VPN 连接
通过第三方操作系统支持的 L2TP 建立 VPN 连接
IPSec 和 PPTP
支持无线连接

VPN 穿越使你的内部网络的计算机或子网能够连接到互联网上的 VPN 网关
IPSec NAT 在途径 NAT 设备阻断的情况下建立 IPSec 隧道
支持 HUB-and-Spoke

星型 VPN，该功能允许在分支机构与总部之间容易的建立 VPN 隧道，这样减轻了管理员在许多分支机构与总部之间维护需要安全通讯的 VPN 隧道

防火墙功能

LAN Gate 系列产品防火墙都是基于状态检测技术的，保护你的计算机网络免遭来自 Internet 的攻击。防火墙通过仔细地设置接口，提供了安全控制策略，甚至在复杂的情况下仍可做详细的控制。

状态检测防火墙
多个 WAN 连接提供负载均衡和连接备份
静态 NAT 和动态 NAT
可将整个内部网络分成安全隔离的子网
基于用户的内部子网的权限策略
深度包检测屏蔽 P2P
VOIP、视频会议的支持
IP/MAC 地址绑定

内容过滤功能

LAN Gate 的内容过滤不同于传统的基于主机系统结构内容处理产品，LAN Gate 设备内是网关级的内容过滤，是基于专用芯片硬件技术实现的。LAN Gate 专用芯片内容处理器包括功能强大的特征扫描引擎，能使很大范围类型的内容与成千上万种关键词或其它模式的“特征”相匹配。具有根据关键字、URL 或脚本语言等不同类型内容的过滤，还提供了免屏蔽列表和组合关键词过滤的功能。

入侵检测功能

LAN Gate 网络入侵侦测系统(IDS)是一种实时网络入侵检测传感器，它能对外界各种可疑的网络活动进行识别及采取行动。IDS 使用攻击特征库来识别超过 1000 多种的攻击。为通知系统管理员有攻击，IDS 将此攻击及一切可疑流量记录到攻击日志中，并根据设置发送报警邮件。

可定期更新攻击数据库。您可下载并手动安装攻击数据库。也可设置 LAN Gate 自动查询和下载更新的 IDS 数据库。

可以检测多种类型攻击，例如拒绝服务攻击（包括 Smurf flood，TCP SYNflood,UDP flood 和 ICMP flood，Ping of Death，Tear drop 等）。

带宽管理功能

带宽管理提供五种不同的内置策略，用户可以自定义优先级和网络流量的使用量。根据不同的服务使用流量策略并实施到不同的 IP 或者网络中。

垃圾邮件过滤防毒功能

对 SMTP 服务器的 IP 进行黑白名单的识别
垃圾邮件指纹识别
实时黑名单技术
对所有的邮件信息病毒扫描

系统报表和系统自动警告

系统内置 28 种报表，对网络安全进行全方位的实时统计；用户可以自定义阀值，所有超过阀值的事件将自动通知管理管理人员，通知方式有 Email 及短信方式。

LAN Gate 提供整体解决方案

LAN Gate 在网络边界布署应用层内容过滤服务，具备防火墙、虚拟专用网 VPN、网络入侵检测、防病毒/蠕虫、Web 内容过滤等功能，在维持网络传输速度的同时，确保网络安全的实时性、有效性，提供完整的全方位网络与信息安全解决方案。

LAN Gate 系列产品众多，无论是个人办公、SOHO 一族，还是中小型企业，或是大型企业和运营服务商，LAN Gate 都能提供最佳选择。

LAN Gate 系列产品性能一览表

系列	brone系列		argent系列		doré系列		
型号	LG-40	LG-1040	LG-2040	LG-3060	LG-4060	LG-5060	LG-6060
包过滤方式	Yes	Yes	Yes	Yes	Yes	Yes	Yes
防火墙功能							
包过滤方式	Yes	Yes	Yes	Yes	Yes	Yes	Yes
外形	1U	1U	1U	1U	1U	2U	2U
LAN Gate专用CPU	Yes	Yes	Yes	Yes	Yes	Yes	Yes
网口数量	4	4	4	6	6	6	6
端口	1WAN+1DMZ+2LAN 端口自定义	2WAN+1DMZ+1LAN 端口自定义	2WAN+1DMZ+1LAN 端口自定义	2WAN+1DMZ+3LAN 端口自定义	2WAN+1DMZ+3LAN 端口自定义	2WAN+1DMZ+3LAN 端口自定义	2WAN+1DMZ+3LAN 端口自定义
防火墙吞吐量	30M	90M	200M	300M	800M	1G	2.7G
用户数	无限制	无限制	无限制	无限制	无限制	无限制	无限制
最大并发连接数	3000	12000	35000	150000	500000	550000	600000
DoS, DDoS防范	Yes	Yes	Yes	Yes	Yes	Yes	Yes
支持透明模式	Yes	Yes	Yes	Yes	Yes	Yes	Yes
动态NAT	Yes	Yes	Yes	Yes	Yes	Yes	Yes
静态NAT	Yes	Yes	Yes	Yes	Yes	Yes	Yes
反向地址映射	Yes	Yes	Yes	Yes	Yes	Yes	Yes
端口转换	Yes	Yes	Yes	Yes	Yes	Yes	Yes
最大防火墙策略数	100	1000	1500	3000	10000	10000	10000
最大NAT策略数	64	128	128	128	128	128	128
支持VLAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes
支持VOIP和视频会议	Yes	Yes	Yes	Yes	Yes	Yes	Yes
屏蔽P2P	Yes	Yes	Yes	Yes	Yes	Yes	Yes
网络流量监测	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPSec VPN 功能							
包括VPN功能	Yes	Yes	Yes	Yes	Yes	Yes	Yes
加密方式	3DES/AES	3DES/AES/Twofish/Blowfish/CAST	3DES/AES/Twofish/Blowfish/CAST	3DES/AES/Twofish/Blowfish/CAST	3DES/AES/Twofish/Blowfish/CAST	3DES/AES/Twofish/Blowfish/CAST	3DES/AES/Twofish/Blowfish/CAST
身份论证	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1
密匙管理	IKE, 手工	IKE, 手工	IKE, 手工	IKE, 手工	IKE, 手工	IKE, 手工	IKE, 手工
VPN的兼容性	经验证IPSec标准的VPN	经验证IPSec标准的VPN	经验证IPSec标准的VPN	经验证IPSec标准的VPN	经验证IPSec标准的VPN	经验证IPSec标准的VPN	经验证IPSec标准的VPN
点对点VPN通道数	10	50	100	150	500	1000	
最大VPN客户端数	30	100	200	650	1500	2500	3000
3DES最大处理速度	30Mbps	50Mbps	75Mbps	75Mbps	200Mbps	350Mbps	500Mbps
AES最大处理速度	30Mbps	50Mbps	75Mbps	75Mbps	200Mbps	350Mbps	500Mbps
NetBIOS广播	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAT 穿透	Yes	Yes	Yes	Yes	Yes	Yes	Yes
支持动态IP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PFS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.509数字证书	Yes	Yes	Yes	Yes	Yes	Yes	Yes
星状VPN结构	No	Yes	Yes	Yes	Yes	Yes	Yes
网络支持							
负载均衡	No	Yes	Yes	Yes	Yes	Yes	Yes
多链路备份	No	Yes	Yes	Yes	Yes	Yes	Yes
支持接口备份	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP地址和MAC地址绑定	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP中继	Yes	Yes	Yes	Yes	Yes	Yes	Yes
L2TP终端	Yes	Yes	Yes	Yes	Yes	Yes	Yes
静态路由	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP支持	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DNS代理	Yes	Yes	Yes	Yes	Yes	Yes	Yes
动态DNS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NTP	Yes	Yes	Yes	Yes	Yes	Yes	Yes

管理							
HTTP/HTTPS管理方法	Yes	Yes	Yes	Yes	Yes	Yes	Yes
远程管理	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP管理	Yes	Yes	Yes	Yes	Yes	Yes	Yes
软件升级方式	浏览器	浏览器	浏览器	浏览器	浏览器	浏览器	浏览器
系统诊断工具	Yes	Yes	Yes	Yes	Yes	Yes	Yes
日志	Yes	Yes	Yes	Yes	Yes	Yes	Yes
系统报表和自动警告	Yes	Yes	Yes	Yes	Yes	Yes	Yes
增强模块							
带宽管理	Yes	Yes	Yes	Yes	Yes	Yes	Yes
内容过滤	Yes	Yes	Yes	Yes	Yes	Yes	Yes
垃圾邮件过滤和防毒	Yes	Yes	Yes	Yes	Yes	Yes	Yes

产品系列介绍

LG-40

LG-40 是一款紧凑的、易于安装的适合小型办公室或家庭办公（SOHO）网络安全的产品。LAN Gate 系列产品强大的功能在业内无人能出其右，并且能够满足从小型企业和分支机构到大型企业和服务提供商不同用户群的需求。

LG-1040

LG-1040 是适合需要特佳性能的小型企业网络安全产品。它包含一个 DMZ 口用来提供本地 Email 和 Web 服务器的。并且容易安装，可通过方便的 Web 界面管理。LG 1040 是 LAN Gate 系列产品的一款，该系列产品满足从小型企业到大型企业和服务提供商的安全需求，是一套全面的、有效的解决方案。

LG-2040

LG-2040 为中型企业或企业分支机构提供了最好的性价比。能够支持内部带有硬盘，用来记录日志和做攻击分析。LG-2040 易于管理，与 LAN Gate 其他产品完全兼容。LG-2040 是 LAN Gate 系列产品的一款，该系列产品满足从小型企业到大型企业和服务提供商的安全需求，是一套全面的、有效的解决方案。

LG-3060

LG-3060 是满足中型企业或企业分支机构网络安全需求的产品，尤其更适合大型的远程访问环境。LG-3060 能够很容易的集成到现有的网络，和 LAN Gate 其他产品完全兼容。该产品家族满足从小型企业到大型企业和服务提供商的安全需求，是一套全面的、有效的解决方案。

LG-4060

LG-4060 是企业级的网络安全产品，它的六个端口能够配置成独立的安全区域，包括专用的高可用性端口。它是重要应用的完美选择，并且能够很容易的集成到现有的网络，和 LAN Gate 其他产品完全兼容。适合从小型企业到大型企业和服务提供商的应用。

LG-5060

LG-5060 为企业、部门层次级的细粒度安全和内容控制提供了空前的能力，具有 6 个可配置端口，能够使

网络分段成不同的区，对不同的段配置不同的策略。LG -5060 支持冗余配置以保证最大的在线时间，和 LAN Gate 其他产品完全兼容。适合大型企业和服务提供商的应用。

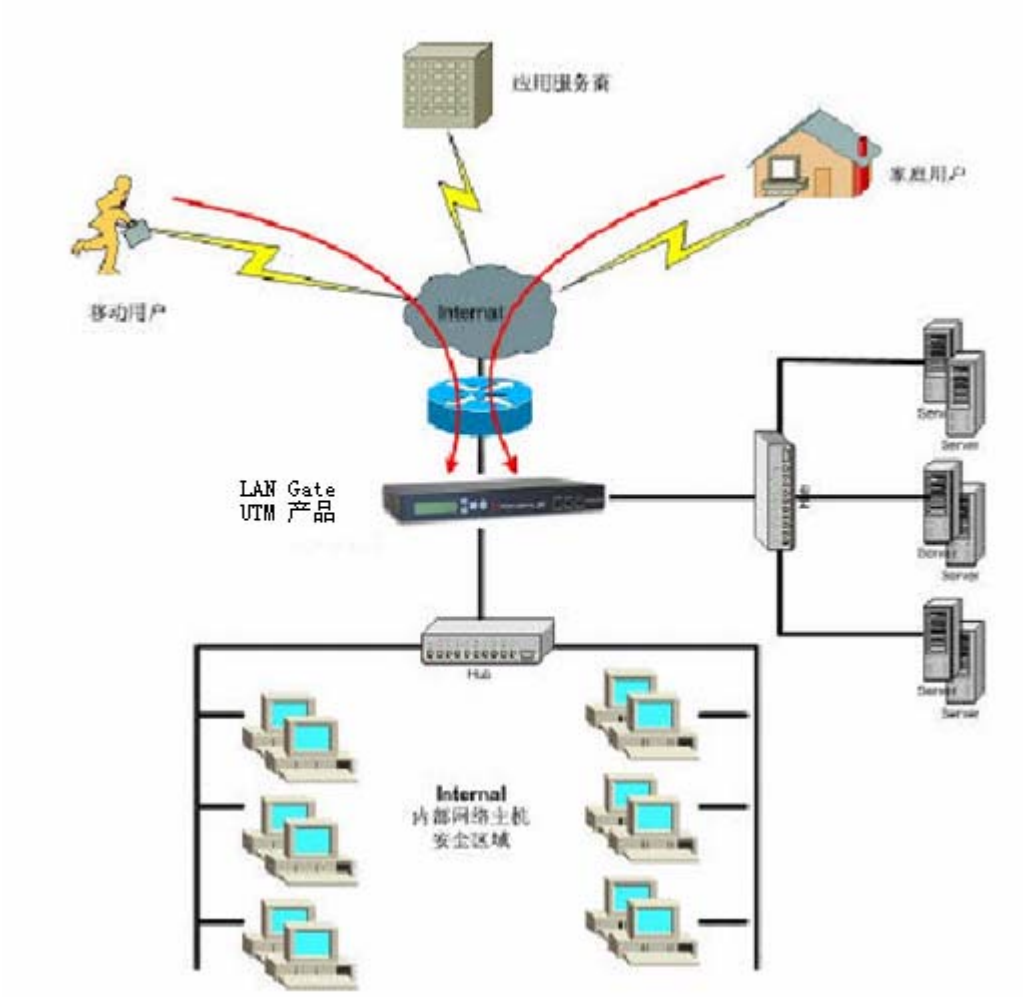
LG-6060

LG-6060 病毒防火墙是适合多个千兆网络的运营商级别的安全产品，使企业和服务提供商能够提供高价值的、高可用的安全和内容控制服务。支持实时的防病毒扫描，有 1Gbps 吞吐量和 VPN 3DES 加密 500Mbps 的性能。多区域配置能够使端口分配到一个组，并设置唯一的策略。LG -6060 达到了空前的性能，是提供不同管理服务的理想平台。支持冗余电源提高可靠性，自带的高可用性端口保证了在不间断运行的情况下透明的进行灾难恢复。

LAN Gate 典型应用方案

中小型企业应用

- 策略控制
- 病毒防御
- 网络攻击防御
- 带宽管理
- 垃圾邮件过滤和防毒
- 内部主机NAT地址翻译
- 内部服务器地址和端口保护
- 远程VPN安全访问

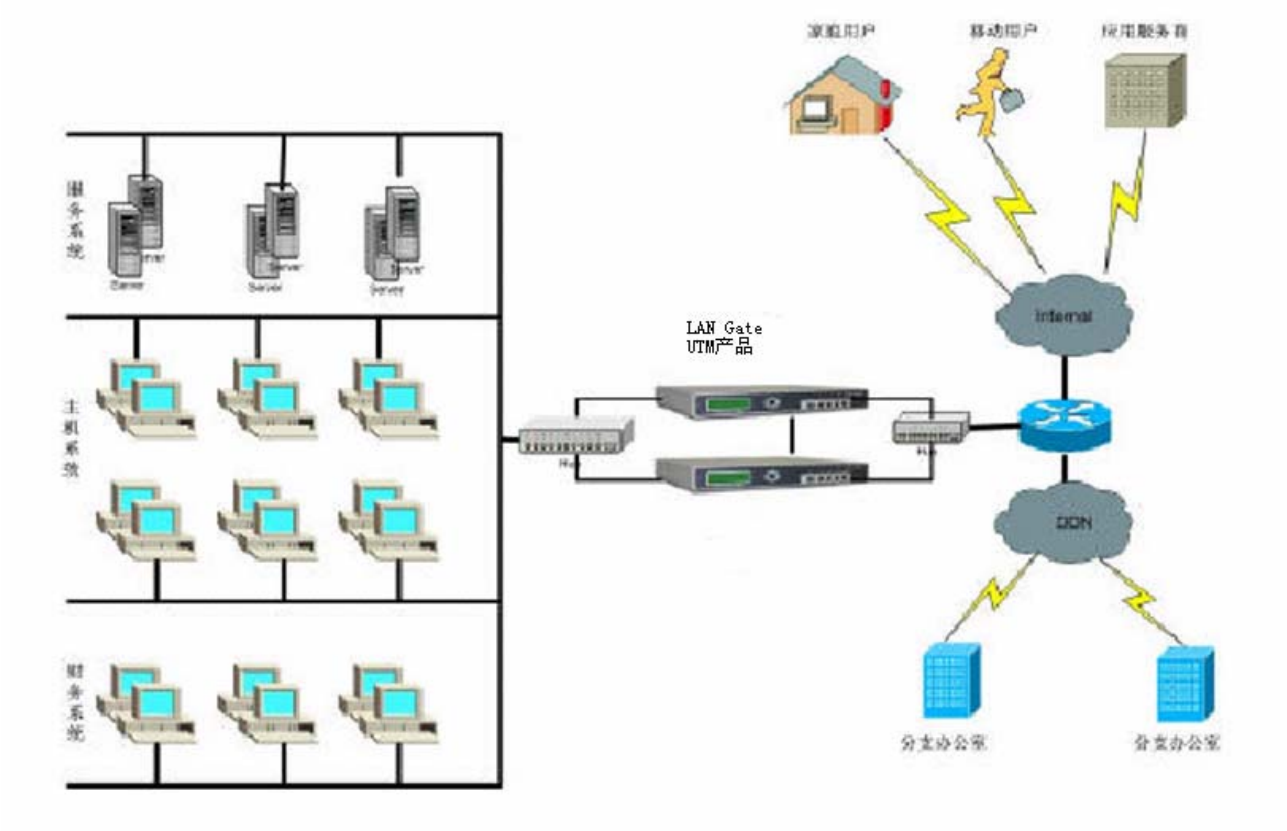


在本应用案例中，企业内部网络被划分成两个物理网段，对外发布信息的服务器放置在 DMZ（非军事区），

通过策略控制来限制外部用户的合法访问。内部主机放置在 Internal 网络中，通过防火墙 NAT 地址翻译访问 Internet 公网资源，同时可以根据用户的不同部门通过防火墙屏蔽有害的邮件（像红色代码、求知信、尼姆达等病毒的入侵），对于放置在 DMZ 区的邮件服务器和 Web 服务器来说可以通过 LAN Gate UTM 产品提供内容层的保护，屏蔽有害邮件和恶意攻击。

大中型企业应用

- 策略控制
- WEB内容和有害网页控制
- 网络攻击防御
- 带宽管理
- 垃圾邮件过滤和防毒
- 内部主机NAT地址翻译
- 内部服务器地址和端口保护
- 远程VPN安全访问
- HA双冗余配置

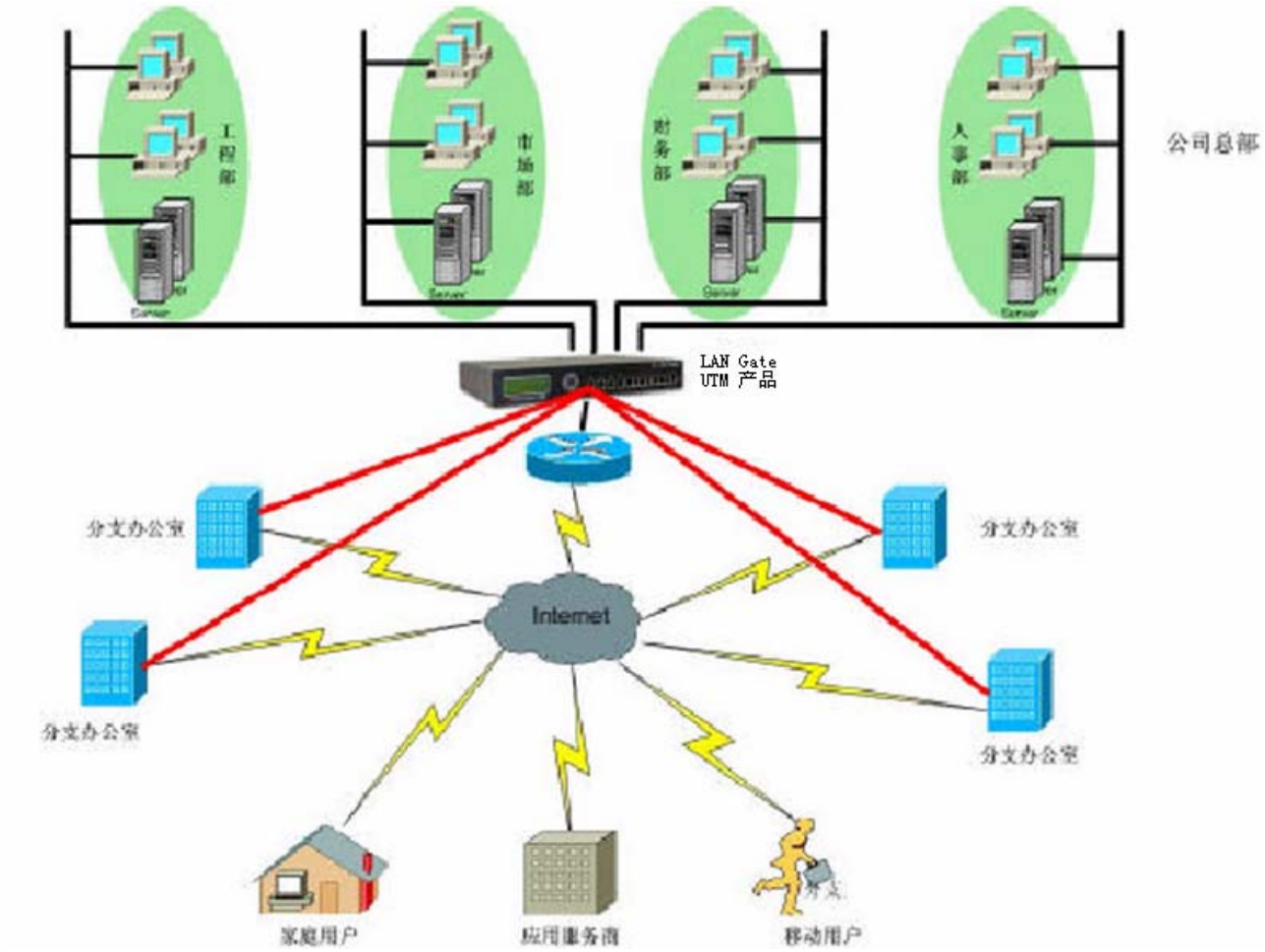


在本应用案例中，企业内部网络在Internet出口配置两台LAN Gate，采用了双机冗余的配置，避免单

点故障的发生。对外发布信息的服务器和内部主机都放置在Internal内部网络，通过VIP地址影射和端口影射发布服务，同时通过策略控制来限制外部用户的合法访问。内部主机通过防火墙NAT地址翻译访问Internet公网资源，同时可以根据用户的不同部门限制其所访问的WEB内容和地址，还可以建立基于时间的访问策略来控制对一些聊天、游戏、电影等于工作无关内容的访问，避免占用有效的网络带宽。

分布型企业应用

- 策略控制
- WEB内容和有害网页控制
- 带宽管理
- 垃圾邮件过滤和防毒
- 网络攻击防御
- 内部主机NAT地址翻译
- 内部服务器地址和端口保护
- 分支企业和总部的VPN安全访问



在本应用案例中，企业总部网络在 Internet 出口配置 LG-6060，LG-6060 可以提供 6 个接口，充分解决了企业总部不同部门之间的安全控制。

如图所示，企业总部有四个主要的应用部门，分别是工程部、市场部、财务部和人事部。通过 LG-6060 的多接口和安全控制功能，物理隔离了四个部门，使部门之间的访问通过集中的管理进行限制，对外发布信息的服务器和内部主机分布在不同的部门之间或集中到一个网络，通过 VIP 地址影射和端口影射服务开放服务，同时通过策略控制来限制外部用户及分支企业的合法访问。

内部不同部门通过防火墙 NAT 地址翻译访问 Internet 公网资源，同时可以根据用户的不同部门限制其所访问的 WEB 内容和地址，还可以建立基于时间的访问策略来控制对一些聊天、游戏、电影等于工作无关内容的访问，避免占用有效的网络带宽。

各企业分支机构可以和总部建立 VPN 的隧道连接，利用 3DES168 位最高加密算法提供了高强度的数据安全。
一般网络系统中，如果网络系统总部和各分支机构之间采用公网网络进行连接，其最大的弱点在于缺乏足够的安全性。总部企业网络接入到公网中，会暴露出两个主要危险：
1.来自公网的未经授权的对企业内部网的存取。
2.当网络系统通过公网进行通讯时，信息可能受到窃听和非法修改。

利用 LG-6060 完整的集成化的企业范围的 VPN 安全解决方案，提供了在公网上安全的双向通讯，以及透

明的加密方案以保证数据的完整性和保密性。

VPN 系统使分布在不同地方的专用网络在不可信任的公共网络上安全的通信。它采用复杂的算法来加密传输的信息，使得敏感的数据不会被窃听。其处理过程如下：

a) 要保护的主机发送明文信息到连接公共网络的 VPN 设备；

b) VPN 设备根据网管设置的规则，确定是否需要对数据进行加密或让数据直接通过。

c) 对需要加密的数据，VPN 设备对整个数据包进行加密和附上数字签名。

d) VPN 设备加上新的数据包头，其中包括目的地 VPN 设备需要的安全信息和一些初始化参数。

e) VPN 设备对加密后的数据、鉴别包以及源 IP 地址、目标 VPN 设备 IP 地址进行重新封装，重新封装后的数据包通过虚拟通道在公网上传输。

当数据包到达目标 VPN 设备时，数据包被解封装，数字签名被核对无误后，数据包被解密。