领信防火墙*技术白皮书* V3.0

LinkTrust™

CyberWall Family

SN:200301124

更体贴您的每一项安全需要

We know more …

Your security

安氏互联网安全系统（中国）有限公司
Information Security One (China) Ltd.

安氏互联网安全系统(中国)有限公司广州分公司
地址：广州市天河北路 689 号光大银行大厦 12 楼 C3-E2 室　邮编：510630
总机：020-38731555、38732069、38730525 转 2013　传真：020-38730144
手机：13600056899　　网址：http://www.is-one.net

版权声明

1）权利归属
本文档中的 LinkTrust™的所有权和运作权归安氏互联网安全系统（中国）有限公司（下称安氏公司），安氏公司提供的服务将完全按照其发布的版权声明以及相关的操作规则严格执行。LinkTrust™ 是安氏公司的商标。因 LinkTrust™所产生的一切知识产权归安氏公司,并受版权、商标、标签和其他财产所有权法律的保护。

2）其它产品说明
本文档中所提及的所有其他名称是各自所有者的品牌、 产品、商标或注册商标。

3）授权声明
任何组织和个人对安氏公司产品的拥有、使用以及复制都必须经过安氏公司书面的有效授权。

4）服务修订
安氏公司保留可能更改本文档中所包含的信息而不需预先知照用户的权利；如果该信息非从安氏公司接收，它们将有被更改或变更的可能，安氏公司不需对用户或第三方负责。

5）特别提示
用户对该信息的使用承担风险，并须在"原封不动"条件下使用。安氏公司对此不作任何类型的担保，不论是明确的或隐含的，包括商业性和某个特定目的适应性的保证。

6）有限责任
安氏公司仅就产品信息预先说明的范围承担责任，安氏公司对引起使用或传播的任何损害（包括直接的、间接的、偶然的、附加的、重要的或特殊的以及继起的损害）不负任何责任（即使已经建议安氏公司这些损害的可能性）。

7）管理
用户对信息和服务的使用是根据所有适用于安氏公司的国家法律、地方法律和国际法律标准的。

8）目的
本声明仅为文档信息的使用而发表，非为广告或产品背书目的。

9）服务
安氏公司在产品发布前完全检查过对 Internet 资源的链接和地址，但是 Internet 不断变化的性质使安氏公司不能保证资源内容的连续性或存在性。如有可能，将参考包含使用其他方法可获得信息的预备站点或关键词。

10）法律
上述条款要与中华人民共和国的法律解释相一致，用户和安氏公司一致同意遵循中国司法管辖之原则。如发生上述条款与中华人民共和国法律相抵触时，则这些条款将完全按照法律规定重新解释，而其他条款则依旧保持原法律效力和影响。

支持信息

如果希望得到关于 CyberWall 产品的报价、产品信息以及技术支持，请查阅公司网站：http://www.is-one.net。如果从 www 网站上仍然得不到你所需要的技术支持，请致电本公司技术支持部。

安氏互联网安全系统（中国）有限公司
Information Security One (China) Ltd.

安氏客服中心

北京：010-88083566-1600

上海：021-52396026-2100

广州：020-38731555-2013

目 录

1 防火墙技术

随着政府上网、企业上网、电子商务、远程教育、远程医疗等一系列网络应用的蓬勃发展，Internet 正在越来越多地离开原来单纯的学术环境，融入到社会的各个方面。一方面，网络用户成分越来越多样化，出于各种目的的网络入侵和攻击越来越频繁；另一方面，网络应用越来越深地渗透到金融、商务、国防等等关键要害领域。换言之，Internet 网的安全，包括其上的信息数据安全和网络设备服务的运行安全，日益成为与国家、政府、企业、个人的利益休戚相关的“大事情”。

“防火墙的目的是在内部、外部两个网络之间建立一个安全控制点，通过允许、拒绝或重新定向经过防火墙的数据流，实现对进、出内部网络的服务和访问的审计和控制”（参见国标 GB/T 18019-1999）。防火墙技术当前已经成为网络安全领域的最为重要的、活跃的领域之一，成为保证网络安全、保护网络数据的重要手段，必选的网络安全设备之一。

一个好的防火墙防御体系应该具有以下五方面的特性：

所有在内部网络和外部网络之间传输的数据必须通过防火墙

只有被授权的合法数据即防火墙系统中安全策略允许的数据可以通过防火墙

防火墙本身运行稳定，不受各种攻击的影响

使用目前最新的信息安全技术，例如现代密码技术等

人机界面良好，用户配置使用方便，易管理

随着防火墙技术的日益成熟以及网络攻击技术的发展，许多防火墙防御体系失败的原因不再是防火墙系统本身，而是防火墙系统的策略制定和管理维护。所以，在用户考察、选择产品提供者时，防火墙策略咨询、评估以及外包管理（MSS）等形式的售后服务的提供能力成为非常重要的因素。

1.1 防火墙的主要功能

包过滤

包过滤（Packet Filtering）防火墙是出现最早的一类防火墙。事实上，路由器本身就具有包过滤防火墙的功能。理论上，包过滤器可以配置为根据协议报头的任何部分进行判断，但实际上，大多数的包过滤实现都针对最为有用的数据域：协议类型、IP 地址、端口号等。通常源地址、目的地址、协议类型、源端口、目的端口以及包到达或发出的接口等构成包过滤防火墙的基本安全控制和审计手段。

简单的包过滤防火墙（大部分路由器形式的包过滤防火墙）只检查序号为 0 的 IP 分包，可以容易地被攻击者定制 IP 分包的方法绕过防火墙策略，所以在安全性方面存在较为严重的缺陷，当前基本上已经被基于状态检查包过滤的专业防火墙所取代。

状态检查（Stateful Inspection）是介于简单包过滤和应用级防火墙之间的一种中间方式，它使用基于维持连接状态和协议信息的复杂过滤器来阻断或通过数据包。在大幅度提高安全性的同时，能够以非常高的速度进行包过滤，成为当前主流防火墙优先采用的工作方式。

网络地址翻译

网络地址翻译（Network Address Translation），又称 IP 伪装（IP Masquerade），它通过将内部主机的 IP 地址翻译到外部网络的 IP 地址，从而达到隐藏内部主机 TCP/IP 层次信息的目的。NAT 允许在内部网络中使用任何网络运行者希望的 IP 网络地址。NAT 技术的出现带来网络安全的同时，在很大程度也缓解了当前 Internet 中 IP 地址匮乏的问题，为网络设计和建设带来了巨大的方便。

按照地址翻译的工作方式，NAT 又可分为以下几种：

静态翻译（Static NAT）， 每一个内部地址对应一个外部地址，也简称为 1:1 NAT。此时，地址翻译带来的安全性、节约地址方面的优点全部消失。但是，在内部网络存在对外提供服务的服务器主机时，静态翻译非常必要。

动态翻译（Dynamic NAT），大段的内部网络地址对应于一个或者一小段外部网络地址。根据实施的细节又可分为 N:1 和 N:M(N>M)两种方式。

应用代理

应用代理（Application Proxy）防火墙的工作方式不同于包过滤防火墙，它首先对带有代理并且按照策略规则允许通过的数据包接收并重新产生,然后忽略掉那些没有相应代理的数据包。应用代理可以提供比包过滤防火墙更为细致的网络安全策略和更好的安全水平，体现在下面几点：

- ✧ 阻断了内外的直接网络连接，不必存在内外网络的直接路由
- ✧ 隐藏了内部网络的客户，对外表现为一个较为繁忙的主机
- ✧ 能够在应用层进行内容和协议过滤，实现精细安全控制
- ✧ 能够对应用层协议进行一致性检查，防止了某些恶意定制的攻击性网络分包
- ✧ 提供了单点的访问、控制和日志记录功能

通常，最为常用的应用代理是 HTTP、Telnet、FTP 等。

当然，应用代理在带来了很高的安全性的同时，也附加了许多不利因素：

- ✧ 单点错误，应用代理的崩溃会导致整个网络连接的中断
- ✧ 客户机必须支持代理的工作方式
- ✧ 每个服务都要有相应的代理才能配置

代理往往会成为速度瓶颈。代理需要在应用层处理数据，所以性能方面大大弱于包过滤方式的防火墙。

身份认证

身份认证（Authentication）技术能够识别从外部网进来访问的用户的身份，从而决定是否允许它们访问内部网络，达到在用户级进行访问控制、对安全策略进行细化的目的。

身份认证经常会带来安全方面的降低，例如：

防火墙必须在某些端口进行监听，这样很容易暴露防火墙的存在

身份认证过程可能有问题，会导致外部互联网的用户有机会在防火墙上面打开一个缺口

虚拟专网

虚拟专网（VPN）帮助用户在不安全的公网上面建设一个相对安全的、接近于专用网络的通信环境。虚拟专网使用以下几个基本安全功能来实现：IP 封装、加密的身份认证、数据包净荷加密等。

一般来说，局域网之间的虚拟专网可以通过服务器计算机、防火墙、路由器等来建立。单纯的虚拟专网并不能提供有效的保护，与防火墙的结合可以很大程度上提高虚拟专网的安全性。所以，虚拟专网成为当代防火墙的一个重要功能。

1.2 防火墙的分类

“虽然防火墙的体系结构和技术多种多样，但防火墙产品基本上可分成两类：包过滤防火墙和应用级防火墙”（参见国标 GB/T 18020-1999）。它们各有所长，具体选用哪一种类型或是选择它们的混合型，要看具体需要。

1.包过滤防火墙

一般是基于源地址和目的地址、应用或协议以及每个 IP 包的端口来作出通过与否的判断。一个路由器便是一个"传统"的包过滤防火墙。大多数的路由器都能通过检查这些信息来决定是否将所收到的包转发，但它不能根据一个 IP 包的前后文进行判断。

先进的状态检查包过滤防火墙可以判断这一点，它可以判断连接状态和一些数据流的内容，把判断的信息同规则表进行比较，检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则能符合，防火墙就会使用默认规则。一般情况下，默认规则就是要求防火墙丢弃该包。

下面是某一包过滤防火墙的访问控制规则：

(i) 允许网络 123.0.0.1 使用 FTP(21 口)访问主机 150.0.0.1；
(ii) 允许 IP 地址为 202.103.1.18 和 202.103.1.14 的用户 Telnet(23 口)到主机 150.0.0.2
(iii) 允许任何地址的 E-mail(25 口)进入主机 150.0.0.3；
(iv) 允许任何 WWW 数据（80 口）通过；
(v) 不允许其他数据包进入。

包过滤防火墙简洁、速度快，并且对用户和应用透明，但是因为它只检查地址和端口，对网络更高协议层的信息无理解能力，对网络的保护受到限制。

2.应用级防火墙

应用级防火墙能够检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级防火墙能够理解应用层上的协议，能够做复杂一些的访问控制，并做精细的认证和审核。应用级防火墙可以雇佣代理服务器筛选数据包。但每一种协议需要相应的代理软件，使用时工作量大，效率不如包过滤防火墙。

应用级防火墙有较好的访问控制，是目前最为安全的防火墙技术。但实现较为困难，而且有的应用级防火墙缺乏“透明度”，经常成为网络速度瓶颈。在实际使用中，用户在受信任的网络上通过防火墙访问 Internet 时，经常会发现存在延迟并且必须进行多次登录（Login）才能访问 Internet 或 Intranet。应用级防火墙通常与包过滤控制配合使用。

3.混合型防火墙

该防火墙结合了包过滤防火墙和应用级防火墙的特点。它同包过滤防火墙一样能够通过 IP 地址和端口号，过滤进出的数据包，也能够检查 SYN 和 ACK 标记和序列数字是否逻辑有序。另一方面，它也能象应用级防火墙一样，在应用层上检查数据包的内容，查看这些内容是否能符合既定的网络安全规则。

目前在市场上技术领先的防火墙大多属于混合型防火墙，因为该防火墙对于用户透明，在应用层上加密数据，不需要修改客户端的程序，也不需对每个需要在防火墙上打开的服务额外增加代理。

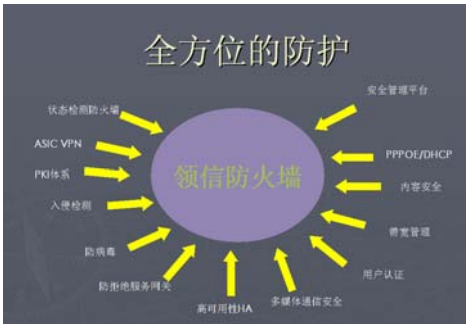
另外，也可以从防火墙表现形式上进行分类。专用型防火器和软件防火墙是两类不同的表现形式。前者表现为硬件形式，自带操作系统和标准配置，开机即可工作；后者表现为软件形式的分发包，管理员需要首先在选定作为防火墙的计算机上面安装操作系统，然后安装防火墙软件，然后进行相应的配置。一般来说，前者的安装过程较为简单直观，对管理员要求较低；后者的安装过程较为费时复杂，对管理员的技术水平要求较高。

专用防火墙又可以根据实现的方式分为固态防火墙和硬盘式防火墙。前者是用固态形式的快速 EEPROM 或 Flash 作为系统载体，机械装置很少；而后者使用标准计算机构成，使用传统的硬盘作为系统载体，出现硬件故障的机会较大。

2 LinkTrust™ CyberWall领信防火墙概述

现代企业利用互联网与客户、合作伙伴及供应商进行沟通，从而以全新的方式进行经营活动，将工作效率提高到了前所未有的水平。但是，当今的互联世界在为企业带来许多机会的同时也给企业资产及业务处理带来极大的风险，安全问题制约着企业发展，因此，值得依赖的安全互联解决方案将成为企业获得成功的关键因素。

“安全威胁是复杂多变的，这就要求我们的安全设备为客户提供的防护是全方位的，同时是一个可自我调整的有机体”，这就是安氏领信防火墙（LinkTrust™ CyberWall）的设计理念，她虽然还被称之为防火墙，但从应用角度上看，她所能充当众多的安全角色已经远远超过了普通防火墙的意义范畴。领信防火墙的设计理念基于安氏独有的 P^2DR 安全模型理论，突破了传统的防火墙静态防御技术，组成了以企业安全策略为核心，以防护、检测、响应为动态防护圈的坚而有韧的主动安全体系，是一个极富生命活力的有机体。



P2DR模型示意图

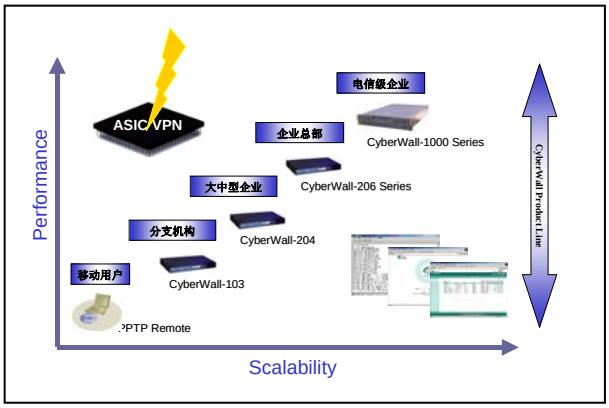
领信防火墙基于专门设计的硬件平台，以安氏安全实验室“iS-One Securtiy Lab”自行定制的安全操作系统 LTOS 为核心，高度集成了防火墙、ASIC VPN、入侵检测、带宽管理、防拒绝服务网关、多媒体通信安全、认证授权、内容安全控制、ADSL 接入安全、高可用性配置能力等众多安全角色，提供高度安全、可信和健壮的安全解决方案，真正实现了单一设备对您的网络的全方位防护。

领信防火墙家族产品能为各种规模的客户提供全面、实时的安全，支持宽带接入与千兆级主干网络流量，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。领信防火墙采用具有安氏专利的“Fast Forwarding”、“Smart Polling”技术显著的提高了状态检测的处理速度，有效的解决了安全性与高性能之间的矛盾。领信防火墙是专用的免维护安全设备，即插即保护，可轻松部署到您的网络环境中，管理配置简洁方便，是即实用又好用的防火墙。无论您是需要低成本的的用于小型网络的解决方案,还是需要电信级的核心任务实施方案,每一款 LinkTrust™ CyberWall 都能让您构建高质量的体系结构,享受简单安装、直观管理和 iS-One 工程师全方位的“全天候式(follow-the-sun) ”支持便利。

目前，领信防火墙正广泛应用于教育、金融、企业、电力、政府、电信、移动等众多行业，她被中国人民银行评选为金融系统的指定防火墙，并且在第 21 届世界大学生运动会、上海 APEC 会议上大显身手。

3 领信家族系列防火墙

领信防火墙家族产品线能为各种规模的客户提供全面、实时的安全，支持宽带接入与千兆级主干网络流量，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。无论您是需要低成本的用于小型网络的解决方案，还是需要电信级的核心任务实施方案，每一款 LinkTrust™ CyberWall 都能让您构建高质量的体系结构，享受简便安装、直观管理和 iS-One 工程师全方位的“全天候式”(follow-the-sun)支持便利。



CyberWall-103

CyberWall-103 专为中小企业和公司分支机构规模的网络而设计，以简洁、快速配置为原则，使复杂的的安全实施得以简化。她充分考虑中小型用户特点，支持 PPPoE 与 DHCP，集成防火墙、VPN、IDS、带宽管理功能，为那些希望以合理价格实现安全的中小企业提供了一站式的经济完整的解决方案。

CyberWall-204

CyberWall-204 是当今可应用最广的防火墙，它集成 4 个 10/100M 自感应端口，在传统防火墙内、外、DMZ 的基础上增加了一个物理端口供用户灵活配置。它含盖了 CyberWall-103 系列产品的所有特性，并提供更高的性能和稳定性。

CyberWall-206F

CyberWall-206F 为 CyberWall-206 系列产品之一，专为具有复杂网络结构及严密安全需求的用户而设计的，配备 6 个 10/100M 自感应以太端口，采用先进的安全域（Security Zone）概念结构。

CyberWall-206SP

CyberWall-206SP 为 CyberWall-206 系列产品之一，除了具备 206F 的所有特性外，自身还集成了 IPSec VPN 硬加速处理器“Security Processor 200”，赋予了它可怕的数据加密处理能力，使其在 IP 安全通讯领域中承担着 VPN 中央数据加密处理核心节点的位置。

CyberWall-1000F

CyberWall-1000F 为 CyberWall-1000 系列产品之一，可以满足电信级、网络服务运营商和大型数据中心等千兆位网络环境的安全需求，采用 2U 专用千兆安全服务器平台，完全模块化可扩展结构，提供最高的安全性、处理速度与可靠性。更多介绍参见《领信千兆防火墙技术白皮书》

CyberWall-1000A

CyberWall-1000A 为 CyberWall-1000 系列产品之一，除了具备 1000F 的所有特性外，自身还集成了千兆位 IPSec VPN 硬加速处理器“Security Processor GIGA”，为安氏 Esafelink 高性能网络安全解决方案注入了惊人的数据加密封装力量。更多介绍参见《领信千兆防火墙技术白皮书》

3.1 中小型企业产品：LinkTrust™ CyberWall-103

CyberWall-103 专为中小企业和公司分支机构规模的网络而设计，以简洁、快速配置为原则，使复杂的的安全实施得以简化。她充分考虑中小型用户特点，支持 PPPOE 与 DHCP，集成防火墙、VPN、IDS、带宽管理功能，为那些希望以合理价格实现安全的中小企业提供了一站式的经济完整的解决方案。

关键特性和优势

- 让中小型用户享受无以伦比的性价比
- 混合型防火墙（状态检测、应用代理）可工作在路由、透明、NAT 模式下
- 轻松部署，支持 PPPOE 协议，提供 ADSL 接入方式，具备智能拨入、断线重连特性
- 设置简洁，通过 LCD 配合五分钟内即可完成 CyberWall-103 的全功能配置
- 集成 Smart Protector，提供经济的入侵检测解决方案
- 支持 DHCP 服务器功能，节省用户网络管理投资；
- 支持 DHCP 客户端，防火墙可动态获得 IP
- 64K 精细粒度带宽控制，充分满足中小型及拨号用户网络管理需求
- 内容过滤功能提供对 URL、邮件、指令、Activx/Java 和诡异木马探测
- 提供对 H.323 协议的完美支持

安氏互联网安全系统(中国)有限公司广州分公司
地址：广州市天河北路 689 号光大银行大厦 12 楼 C3-E2 室　邮编：510630
总机：020-38731555、38732069、38730525 转 2013　传真：020-38730144
手机：13600056899　网址：http://www.is-one.net

3.2 当今应用最广泛的产品：LinkTrust™ CyberWall-204

CyberWall-204 是当今可应用最广的防火墙，它集成 4 个 10/100M 自感应端口，在传统防火墙内、外、DMZ 的基础上增加了一个物理端口供灵活配置，用户可根据需要将其设定成 IDS 镜像口、带外管理口或 HA 心跳口，或不做任何配置默认作为流量通讯过滤口使用。CyberWall-204 涵盖了 CyberWall-103 产品的所有特性，处理速度比其提高了 25%，并提供了更高的性能与稳定性。CyberWall-204 简洁通用的硬件设计和出色的性能优势可使其轻松的部署于各种规模的网络环境之中。

关键特性和优势

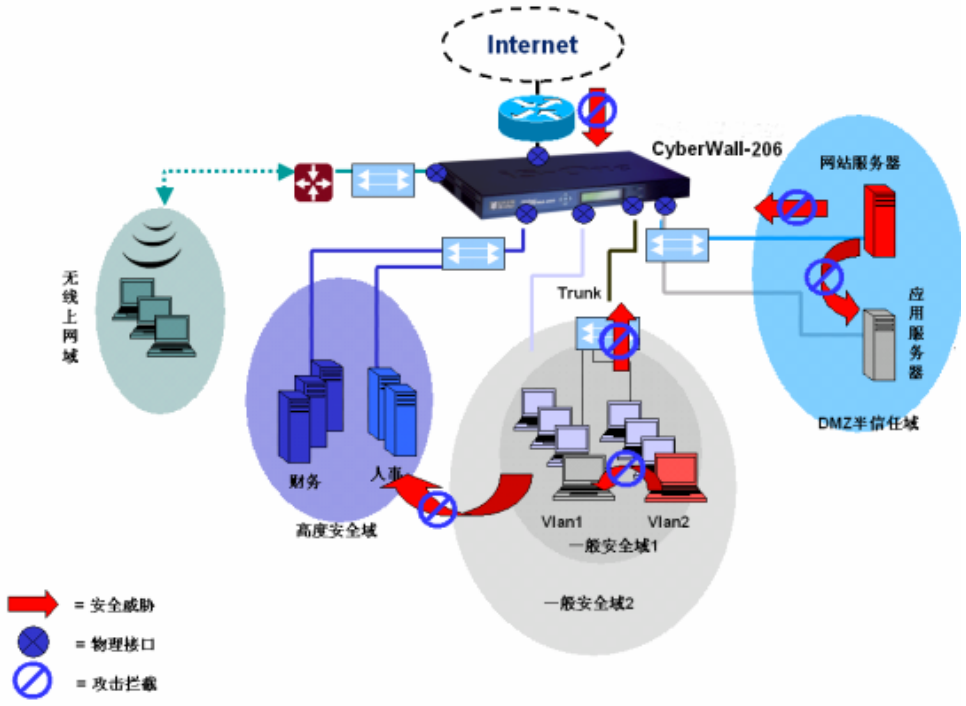
- 先进的安全域(Security Zone)概念结构，策略设置更趋灵活合理
- 集成防火墙、入侵检测、VPN、带宽管理、认证、审计的全方位防护
- 混合型防火墙（状态检测、应用代理）可工作在路由、透明、NAT 模式下
- 支持业界标准的 802.1Q VLAN 协议，可划分逻辑子接口并提供路由和透明模式下的 802.1Q VLAN Trunk 能力，充分考虑您的网络环境，全面满足您的需求
- 维护方便、易于管理，提供 LCD、Console、SSH、HTTPS 等多种管理手段
- 防拒绝服务网关，可抵御 SYNflood, UDPflood, ICMPflood, Tear Drop, Smurf, Land Attack, Ping of Death 等多种当今流行的 DoS/DDoS 攻击
- 高可靠性(HA)提供对链路和设备的自动检测，小于 1 秒的切换时间可避免单点故障造成的网络瘫痪，保证网络持续运作能力
- 强大的负载均衡功能提供对后台高达 8 台服务器的负载均衡
- 全面的用户认证功能，提供 Radius,MSNT 域，Secure ID 和 LDAP 等多种认证方式
- Smart Protector 的入侵检测功能可以提供 250 种以上的攻击检测
- 内容过滤功能提供对 URL、邮件、指令、Activx/Java 和诡异木马探测
- 提供对 H.323 协议的完美支持

3.3 多子网复杂结构企业产品：LinkTrust™ CyberWall-206 Series

CyberWall-206 系列防火墙共分两种型号 CyberWall-206F 和 CyberWall-206SP，它们专为具有复杂网络结构及严密安全需求的大中型企业用户而设计，配备 6 个 10/100M 自感应端口，采用先进的安全域（Security Zone）概念结构，提供了复杂网络多子网之间的安全控制方案，防火墙上的每个物理网口可以挂接任意多个逻辑子网，通过划分安全级别域和设置访问控制规则来实现各端口、子网、安全域之间的数据包转发，高度集成了防火墙、ASIC VPN、入侵检测、带宽管理、防拒绝服务网关、多媒体通信安全、认证授权、内容安全控制、ADSL 接入安全、高可用性配置能力等众多安全角色，提供高度安全、可信和健壮的安全解决方案。另外，206SP 自身还集成了 ASIC VPN 处理器 Security Processor 200，它支持处理所有的与安全相关的协议包括 IPSec, IKE, SSL 和 TLS，处理能力相当于 1000MIPS，等同于 12－18 颗的 Pentium III 级微处理器对数据加密的处理能力，赋予了它可怕的数据加密处理能力，在 IP 安全通讯领域中承担着 VPN 中央数据加密处理核心节点的位置。

关键特性和优势

- 先进的安全域(Security Zone)概念结构，策略设置更趋灵活合理
- 集成防火墙、入侵检测、VPN、带宽管理、认证、审计的全方位防护
- 混合型防火墙（状态检测、应用代理）可工作在路由、透明、NAT 模式下
- 多网口防火墙，满足复杂环境多子网访问控制需求
- 支持业界标准的 802.1Q VLAN 协议，可划分逻辑子接口并提供路由和透明模式下的 802.1Q VLAN Trunk 能力，充分考虑您的网络环境，全面满足您的需求
- 维护方便、易于管理，提供 LCD、Console、SSH、HTTPS 等多种管理手段
- 防拒绝服务网关，可抵御 SYNflood, UDPflood, ICMPflood, Tear Drop, Smurf, Land Attack, Ping of Death 等多种当今流行的 DoS/DDoS 攻击
- 高可靠性(HA)提供对链路和设备的自动检测，小于 1 秒的切换时间可避免单点故障造成的网络瘫痪，保证网络持续运作能力
- 强大的负载均衡功能提供对后台高达 8 台服务器的负载均衡
- 全面的用户认证功能，提供 Radius,MSNT 域，Secure ID 和 LDAP 等多种认证方式
- 支持 ASIC VPN，提供高性能的 VPN 解决方案
- Smart Protector 的入侵检测功能可以提供 250 种以上的攻击检测
- 内容过滤功能提供对 URL、邮件、指令、Activx/Java 和诡异木马探测
- 提供对 H.323 协议的完美支持



CyberWall-206Series 多安全域访问控制解决方案

安氏互联网安全系统(中国)有限公司广州分公司
地址：广州市天河北路 689 号光大银行大厦 12 楼 C3-E2 室 邮编：510630
总机：020-38731555、38732069、38730525 转 2013 传真：020-38730144
手机：13600056899 网址：http://www.is-one.net

3.4 数据中心、电信骨干网产品：LinkTrust™ CyberWall-1000 Series

CyberWall-1000 系列防火墙共分两种型号 CyberWall-1000F 和 CyberWall-1000A，它们专为千兆位流量的网络服务运营商，大型数据中心等电信级骨干网络而设计，采用 2U 专用千兆安全服务器平台，完全模块化可扩展结构，具有热插拔特性的冗余部件为您提供最大的不间断运行时间。CyberWall-1000 Series 标配 2 个多模光纤接口，最多可扩展至 6 个千兆光口或 10 个百兆接口，充分满足您的定制需求。1000A 将强大的千兆防火墙和 ASIC VPN 相结合，集成千兆位 VPN 加速器“Security Processor GIGA”，为安氏 Esafelink 高性能网络安全解决方案注入了惊人的数据加密封装力量。

领信千兆防火墙关键技术

- **独立总线技术 (LinkTrust™ Independent BUS)**

一般情况下防火墙系统内部只有一根系统总线（通常为 32 位 33M），所有防火墙网络接口卡使用同一根总线与中央处理单元通讯，这种处理方式在数据流量非常大的时候就会出现防火墙系统的不同网络接口卡争夺总线带宽问题，防火墙系统会发生严重丢包，双向流量严重不均衡，甚至不能进行正常响应。LinkTrust™ Cyberwall 千兆防火墙系统采用高速多系统总线结构，为防火墙每个网络接口卡使用一根独立的高速系统总线（64 位 66M），保证了流量很大情况下的通畅，不会出现总线带宽争夺问题。

- **分布处理技术 （LinkTrust Interface Processor）**

通常的防火墙系统的过滤处理完全依赖于中央处理单元或由某些协处理单元提供加速，这种技术一个很明显的缺点就是系统达不到线速。LinkTrust™ Cyberwall 千兆防火墙系统采用分布式处理方式，除了中央处理单元以外在每个网络接口上有一个独立的 MIPS 处理器用于对数据包做复杂的处理，减少了中央处理单元的负荷；这种体系明显了防火墙在千兆环境下的性能表现。

- **快速转发技术（LinkTrust Fast Forwarding）**

一个数据包在通过一个传统的路由防火墙时需要防火墙系统多次检查状态表和地址翻译表，虽然这些查表过程通过 HASH 算法的优化可以做得非常快速，但是依然不能像达到线速工作，尤其是在千兆环境下。LinkTrust™ Cyberwall 防火墙利用自己的特有的快速转发（Fast Forwarding）技术，从根本上面减少了上述操作过程，通过将系统的状态表、翻译表和转发表结合起来，把三层上面的路由过程转化成了二层以下快速转发过程。该技术极大地提升了防火墙在千兆以及百兆小数据包环境下的性能表现。

- **灵巧轮询（LinkTrust Smart Polling）**

一般情况下，防火墙网络接口卡采用中断方式工作。网卡每次收到一个 packet 都会产生一次中断，通知系统有数据包到达。按照这种处理方式，防火墙在数据包流量非常大的时候（尤其是小包），会在一个转发还没有完成时，再次被中断，这时防火墙会陷入内核中断中，既无法转发数据包，也不能响应用户的操作，陷入所谓的“活锁”。 LinkTrust™ Cyberwall 防火墙采用完全不同的网络响应方式: CPU 空闲时会主动询问网卡是否有数据包可用。这样就不会出现消耗在中断中的上下文切换，也不会出现一个数据包没有处理完被打断。为了提供基本的流量保证，系统在时钟中断情况下也会去查询网卡。这样就保证了在系统很忙的情况下也会给网络

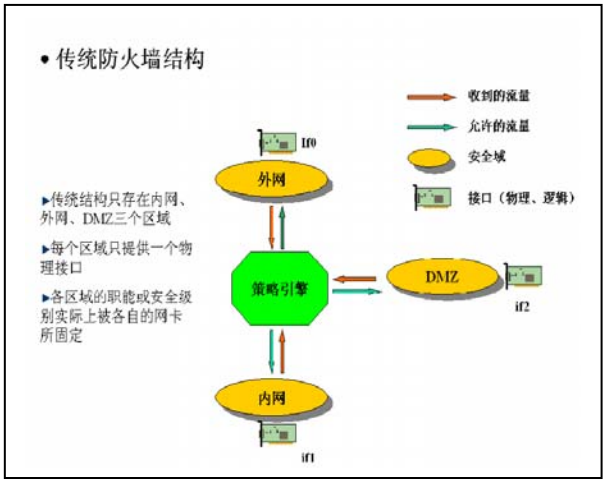
接收的机会。同时也保证了即使防火墙流量巨大，也会对用户的输入有及时的响应。

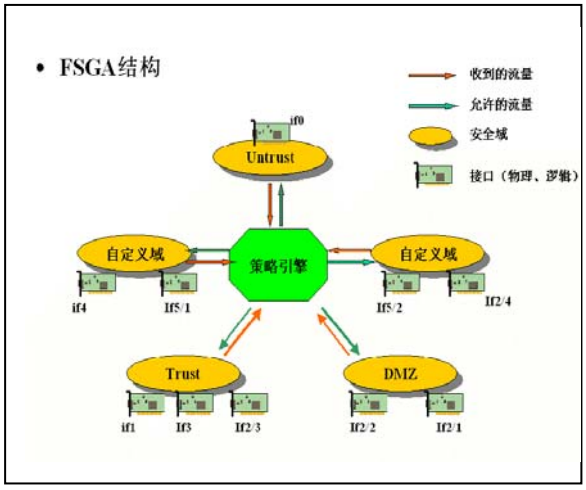
关键特性和优势

- 支持千兆位数据流量，满足电信级骨干网需求
- 先进的安全域(Security Zone)概念结构，策略设置更趋灵活合理
- 集成防火墙、入侵检测、VPN、带宽管理、认证、审计的全方位防护
- 混合型防火墙（状态检测、应用代理）可工作在路由、透明、NAT 模式下
- 多网口防火墙，满足复杂环境多子网访问控制需求
- 支持业界标准的 802.1Q VLAN 协议，可划分逻辑子接口并提供路由和透明模式下的 802.1Q VLAN Trunk 能力，充分考虑您的网络环境，全面满足您的需求
- 维护方便、易于管理，提供 Console、SSH、HTTPS 等多种管理手段
- 千兆级防拒绝服务网关，抵御 SYNflood, UDPflood, ICMPflood, Tear Drop, Smurf, Land Attack, Ping of Death 等多种当今流行的 DoS/DDoS 攻击
- 高可靠性(HA)提供对链路和设备的自动检测，小于 1 秒的切换时间可避免单点故障造成的网络瘫痪，保证网络持续运作能力
- 模块化结构，可扩展性强，部署灵活，维护方便，易于管理
- 冗余可热插拔部件设计，提供最大的网络正常运行时间
- 强大的负载均衡功能提供对后台高达 8 台服务器的负载均衡
- 全面的用户认证功能，提供 Radius,MSNT 域，Secure ID 和 LDAP 等多种认证方式
- CyberWall-1000A 自身集成 ASIC VPN， 提供千兆级 VPN 解决方案
- 在 VPN 连接方面支持网关到网关，拨号客户到网关，移动子网到网关及星型拓扑连接
- 同时支持上万条 VPN 隧道，易于大规模 VPN 部署。
- Smart Protector 的入侵检测功能可以提供 250 种以上的攻击检测
- 内容过滤功能提供对 URL、邮件、指令、Activx/Java 和诡异木马探测
- 提供对 H.323 协议的完美支持

4 领信防火墙的体系结构

LinkTrust™ CyberWall 防火墙采用安氏安全实验室最新设计的灵巧安全网关架构 FSGA(Flexible Security Gateway Architecture)，它旨在解决传统防火墙所存在的种种局限以及提供更适应现代企业安全需求的强大功能，设计能力支持多达 64 个物理以太网口和上千个 VLAN 逻辑子接口，能够配置支持最高达到 400 个虚拟防火墙网关系统，提供完全对称的配置及防护能力，结合灵活的安全域定制，使得策略设置更加随心所欲，可轻松适应甚至是最复杂的网络环境。另外，FSGA 的引入使得一系列安全功能成为可能，虚拟子系统（VSFW）是 FSGA 最新设计，FSGA 架构将成为 CyberWallOS 的发展基石，并且将支持领信防火墙家族今后推出的所有产品

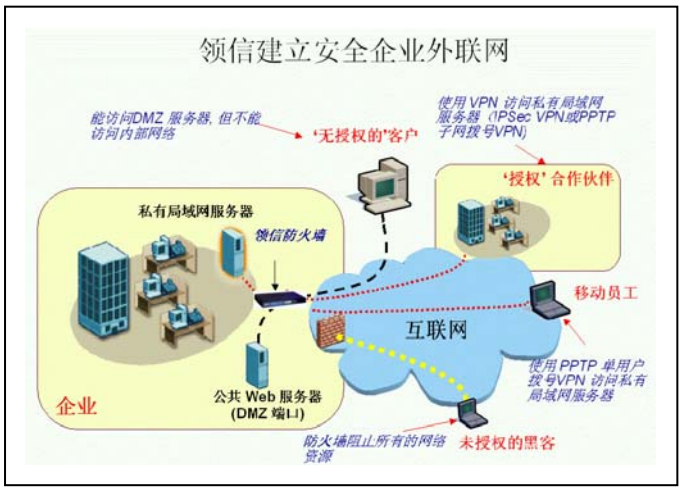




- 对所有物理接口及逻辑子接口提供等同的配置能力
- 真正的安全域概念（接口的角色与安全域角色完全分开）
- 支持多安全域的定制，提供细粒度网络安全级别的划分
- 每个安全域可配置有多个物理接口与 VLAN 逻辑子接口，
- 基于安全域设置策略
- 高度灵活可扩展性，满足企业网络扩建与安全需求的发展

5 领信防火墙主要功能

5.1 支持最先进的第三代包过滤状态检查技术



LinkTrust™ CyberWall 防火墙采用基于状态检查的包过滤技术，快速实现基于源/目的 IP 地址，服务，用户，组（网络，服务）和时间的精细粒度的访问控制。

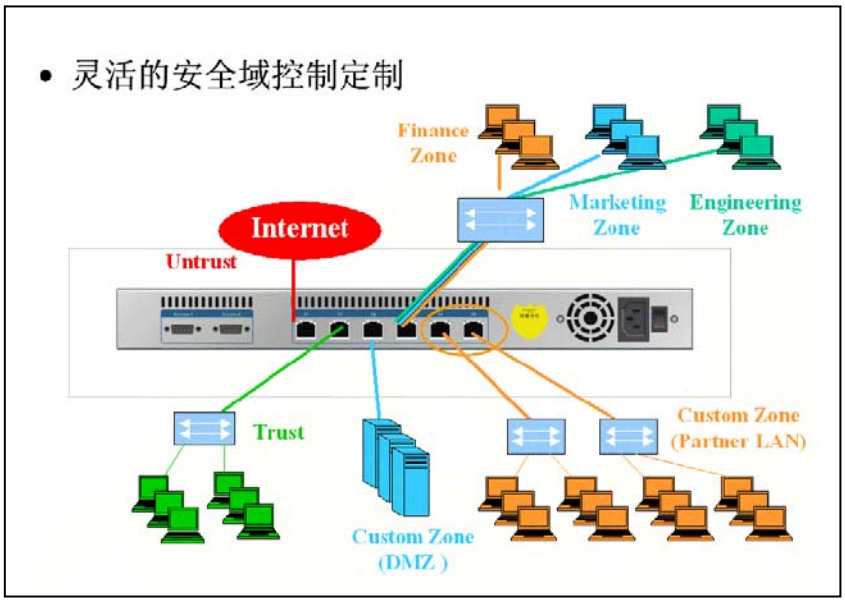
包过滤技术是一种简单、有效的安全控制技术，它通过在网络间相互连接的设备上加载允许、禁止来自某些特定的源地址、目的地址、TCP 端口号等规则，对通过设备的数据包进行检查，限制数据包进出内部网络。包过滤的最大优点是对用户透明，传输性能高。但由于安全控制层次在网络层、传输层，安全控制的力度也只限于源地址、目的地址和端口号，因而只能进行较为初步的安全控制，对于恶意的拥塞攻击、内存覆盖攻击或病毒等高层次的攻击手段，则无能为力。

与包过滤相类似的、更为有效的安全控制方法是状态检测。对新建的应用连接，状态检测检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成状态表。对该连接的后续数据包，只要符合状态表，就可以通过。这种方式的好处在于：由于不需要对每个数据包进行规则检查，而是一个连接的后续数据包（通常是大量的数据包）通过散列算法，直接进行状态检查，从而使得性能得到了较大提高；而且，由于状态表是动态的，因而可以有选择地、动态地开通 1024 号以上的端口，使得安全性得到进一步地提高。LinkTrust™ CyberWall 防火墙采用了一个检测模块(一个在网关上执行网络安全策略的软件引擎)。检测模块在不影响网络正常工作的前提下，采用抽取相关数据的方法对网络通信的各层实施监测，抽取部分数据(状态信息)并动态地保存起来，作为以后制定安全决策的参考。检测模块支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充。

5.2 基于安全域的访问控制

安氏领信防火墙基于先进的“安全域”(Security Zones)结构，在国内率先将基于“接口”的访问控制上升到基于“安全域”的访问控制，具有划时代的意义。领信防火墙从体系结构上根本解决了传统防火墙防外不防内的局限，相对于只有一个内网区域的传统防火墙来讲，领信防火墙支持多安全域的划分，根据企业的安全需求可将内网中具有不同信任度（安全等级）的网段划分成独立的安全域，通过在这些安全域间加载独立的访问控制策略来限制内网中不同信任度网络之间的相互访问，也就是说，领信防火墙提供了更加细粒度的安全控制，这样即使某

个低安全等级的区域出现了安全裂缝，但由于受到防火墙的控制，其它安全域也不会受其影响。这样就好象在内网中设置了层层关卡，安全裂缝被限制在自己的域中，无法对其它区域造成威胁，进而保证了整个内网的安全。那些不忠实的员工再也无法尝试破解财务服务器的密码以窃取机密信息，因为从根本上防火墙就不允许他所在的安全域对财务服务器区域的访问；同样那



些不满的员工或被值入木马的主机发出的拒绝服务攻击也不再对内网产生威胁，黑客再也无法通过被攻陷的内网服务器当作跳板对其它的内网区域进行攻击，那些中了蠕虫或病毒的机器所发出的恶意数据包也无法肆意在内网中传播，因为防火墙根本就没有赋予它访问权限！

随着互联网应用的不断发展，企业的业务模式也在发生着变化，企业的内网已延伸到合作伙伴、大客户、供应商和顾问团的网络，这给企业的网络安全问题带来了新的挑战，这些业务实体对企业来讲具有不同的信任度，他们与企业网之间的连接需要不同程度的访问限制，领信防火墙通过先进的安全域结构和域间访问控制策略，同样可以解决企业外联网之间复杂的互联安全威胁。

5.3 先进的内核代理和透明代理

LinkTrust™ CyberWall 防火墙综合业界最先进的内核代理与透明代理技术提供丰富全面的应用代理，覆盖了大多数用户常用应用程序，包括 TELNET、HTTP、FTP、TFTP、ICMP、SMTP 等。同时，LinkTrust™ CyberWall 防火墙支持多线程代理，提供高性能的连接速度。

LinkTrust™ CyberWall 防火墙支持透明代理，所谓透明代理是指用户不需要知道代理服务器的存在，就可以完成内外网络的通讯，当内网用户需要使用代理访问外部资源时，无需在用户端进行配置，代理服务器会建立透明的通道，让用户能够与外界通信。这样极大的方便用户的使用，避免使用中的错误，降低使用防火墙时固有的安全风险和出错概率。

LinkTrust™ CyberWall 防火墙支持双向代理，在从外到内的访问控制中仍可以使用代理服务，这样就实现了从外部访问内部资源时的内容检查和过滤，限制外网对内部特定信息的访问，最大限度的提高了内网资源的机密性与完整性。

LinkTrust™ CyberWall 防火墙提供了多种内核级别代理机制，例如 FTP 代理 TFTP 代理和 ICMP 代理可以大大增强特殊网络应用安全性。

5.4 全面地址翻译解决方案

LinkTrust™ CyberWall 防火墙的 NAT 技术完全遵循 RFC 1631 标准，支持多种网络地址翻译方式和双向地址翻译能力，为用户提供完整的地址转换解决方案

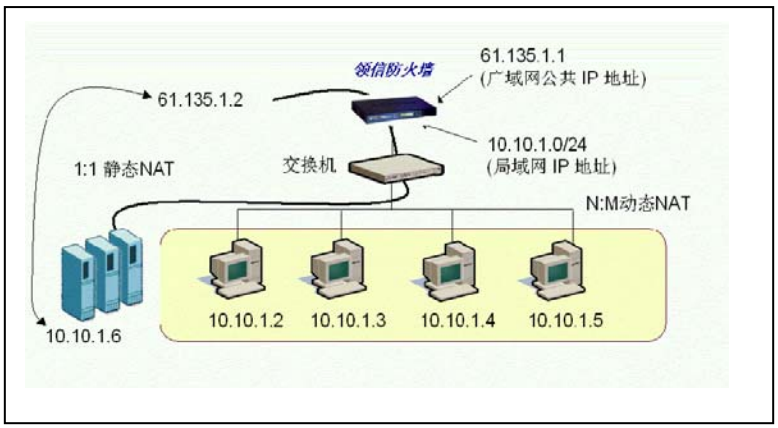
LinkTrust™ CyberWall 防火墙提供的地址翻译方式包括：

静态地址翻译：

1 ： 1 的静态地址翻译，即内部地址和外部地址一对一的映射。经过静态地址翻译的主机可以用翻译后的公网合法地址访问 Internet，也可以用翻译后的公网合法地址接受外部的访问请求。对公众网来说，与之通讯的对象完全是防火墙转换后的地址，有效的隐藏了内网拓扑等重要信息。

动态地址翻译：

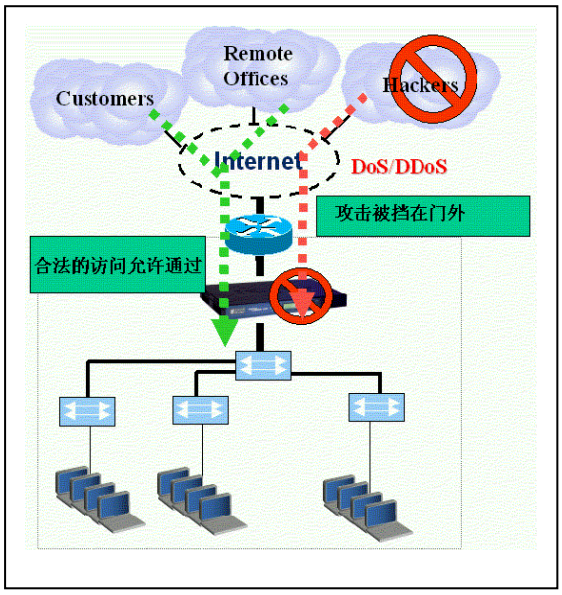
N ： M 的动态地址翻译（N≥M、M≥1），即 N 个内部地址与 M 个外部地址的动态随机映射。当这 N 个内网主机的某个用户需要对外访问时，防火墙系统将会从定义好的 M 个外部合法地址中动态分配抽取一个没有使用的 IP 地址给用户，使用户得到合法的 IP 地址与外部访问。当用户完成访问时，系统将回收这个 IP 地址，将它分配给另外一个用户使用。对公众网来说，访问完全来自防火墙转换后的地址，有效的隐藏了内部网络的拓扑结构等重要信息，同时内部用户共享使用这些合法地址，自身仍可以灵活的使用内部保留地址，有效的解决了合法 IP 地址不足的问题。



端口定向能力：

$IP_A + PORT_M$ ： $IP_B(C, D, E, ...) + PORT_N(O, P, Q...)$方式的地址及端口重定向，通过防火墙外网卡绑定的某个外部合法地址 IP_A 的某个端口 M 映射多个内部地址 $IP_B(C, D, E, ...)$的特定端口(O,P,Q…)，这个外网卡上绑定的用做重定向 IP 又叫做 VIP。这样，外部对 VIP 某个端口的访问可以被重定向到内部多台主机。既节省公网合法 IP 资源又可以隐藏内部服务器地址。更重要的是，通过端口定向可以实现服务器负载均衡，同时也是一种高效的隐藏企业内部服务器端口的方式,同时提高了一台服务器的使用效率。

5.5 独特的Anti-DoS网关防御技术



DoS（Denial of Service）和 DDoS（Distributed Denial of Service）是未来几年中 Internet 上黑客最常用的也是最难防御的攻击方式。在 2001 年，世界许多知名机构和网站都不同程度的遭受了它的攻击，世界最大的门户网站雅虎(Yahoo.com)遭受损失高达上亿美元。拒绝服务方式的攻击行为使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至于瘫痪而停止提供正常的服务，最常见的 DoS 攻击有网络带宽攻击和连通性攻击。带宽攻击指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求无法通过，比如 smurf 攻击。连通性攻击指用大量的连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的请求，比如 synflood 攻击，在此基础之上的分布式拒绝服务攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力。网络入侵检测工具（NIDS）只能检测到 DoS 攻击，并不能有效的阻止它的破坏行为，因此在网关的 Anti-DoS 技术成为当前网络安全厂商的攻坚课题。LinkTrust™ CyberWall 防火墙在国内率先实现了针对多种 DoS 或 DDoS 的攻击防范，在攻击包进入企业网络之前将其堵在门外，系统可以根据用户的设置对访问信息进行检查，从而抵挡住以下类型的 DoS 或 DDoS 攻击：

Synflood 攻击：Synflood 是当今最常见的 DOS 攻击，它通过向服务器发送大量的虚假 SYN 请求包耗尽服务器资源，导致合法用户无法访问。LinkTrust™ CyberWall 防火墙通过增强的 Syn-Cookie 技术实现了对 Synflood 攻击的防范。在收到客户端的 Syn 包后，防火墙代替服务器向客户端发送 Syn-Ack 包，如果客户端在一段时间内没有应答或中间的网络设备发回了 ICMP 错误消息，防火墙则丢弃此状态信息；如果客户端的 Ack 到达，防火墙代替客户端向服务器发送 Syn 包，并完成后续的握手最终建立客户端到服务器的连接。通过这种 Syn-Cookie 技术，保证了每个 Syn 包源的真实有效性，确保服务器不被虚假请求浪费资源，从而彻底防范了对服务器的 Synflood 攻击。

Land 攻击：在 Land 攻击（一种 SYN 攻击的简单混合）中，大量的 SYN 数据包发送到目标系统，这些特别打造的 SYN 包中的原地址和目标地址都伪装成目标系统的网络地址。这时将导致目标系统向它自己的地址发送 SYN 一 ACK 消息，结果这个地址又发回 ACK 消息并创建一个空连接，每一个这样的连接都将保留直到超时掉，即使在修正了 SYN 漏洞的系统上，有些系统也会被 Land 攻击以至出现问题。LinkTrust™ CyberWall 防火墙通过丢弃所有源地址和目的地址相同的数据包实现对 Land 攻击的防范。

Tear Drop 攻击：IP 数据包在 Internet 上传递时，数据包可以分成更小的片断。每个片断看起来都象原来的 IP 数据包，不同之处在于，每个片断里都包含一个偏移字段，说明这个片断是原来数据包的哪一部分， Teardrop 程序可以生成一系列 IP 片断，这些 IP 片断的偏移字段彼

此重叠。当这些 IP 片断到达目标主机，进行重组的时候，某些系统就会崩溃、挂起或重启动。LinkTrust™ CyberWall 防火墙通过识别分片包的偏移量来实现对 Tear Drop 攻击和其它 IP 碎片攻击的防范。

Ping of Death 攻击：由于在早期的阶段路由器对所传输的文件包最大尺寸都有限制，许多操作系统对 TCP／IP 的实现在 ICMP 包上都是规定 64KB，并且在对包的标题头进行读取之后，要根据该标题头里包含的信息来为有效载荷生成缓冲区，一旦产生畸形即声称自己的尺寸超过 ICMP 上限的包，也就是加载的尺寸超过 64KB 上限时，就会出现内存分配错误，导致 TCP／IP 堆栈崩溃，致使接收方当机。一般这种字节数大于 64KB 的包都是通过 IP 分片发送，LinkTrust™ CyberWall 防火墙通过重组分片包来识别并挫败这种攻击。

Smurf 攻击：Smurf 是一种强力攻击，它向路由器发送大量目标地址为广播地址的 ICMP echo 请求包，路由器会把 ICMP echo 请求以广播形式发给网络上的所有主机，如果有大量主机，那么这种广播就会造成巨大的 ICMP echo 请求及响应流量，如果攻击时使用了虚假的源地址，那么攻击所造成的流量不仅会阻塞目标网络，还会阻塞被冒用源地址所在的网络。LinkTrust™ CyberWall 防火墙可以丢弃所有目标地址为广播地址的 ICMP 包，从而挫败 Smurf 攻击。

ICMP Flood 攻击：大量的 ICMP 包会造成网络堵塞或服务器资源耗尽，防火墙通过限制 ICMP 包的流量来实现对这种攻击的防范。

5.6 内核级TCP标志位检测

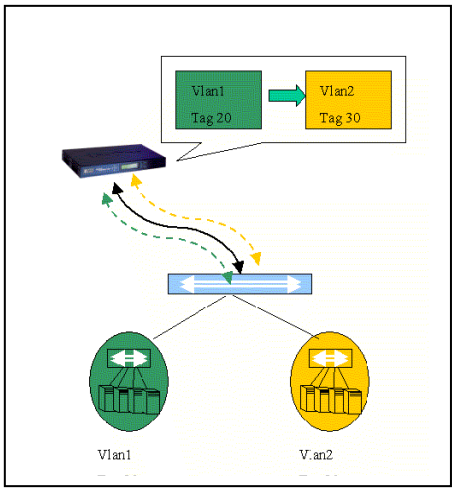
国内外大多数的防火墙都缺少对连接是从哪方主动发起进行判断能力，这将导致一个潜在的安全隐患是攻击者可能可以从一个外部主机的某个常用服务端口连入内部主机的高端口。例如，如果允许内部主机访问外部主机的 telnet 服务，这个方向连接的所有包应该是必须包含 ACK 位的，也就是说，不是主动发起的连接。但通常的防火墙的包过滤功能里并没有检查 ACK 位的设置，因此，攻击者就可以从外部主机的源 23 端口发起连接到内部主机的高端口(>1023)。LinkTrust™ CyberWall 防火墙在内核级对数据包的 SYN/ACK 等标志位进行合法性检测和判断，防止不法攻击者利用常用服务的低端口与内部主机的高端口的连接从而攻击内部主机。

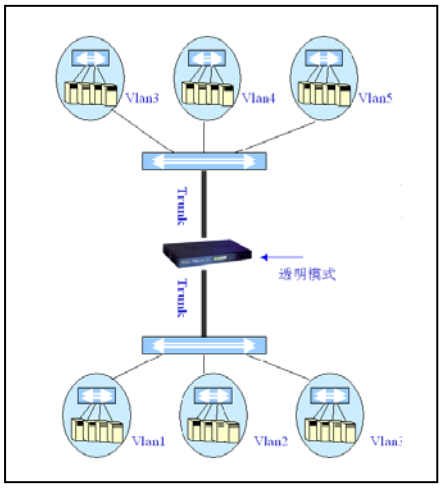
5.7 支持802.1Q　VLAN Trunk 协议

VLAN Trunk 是一个在一个或多个交换端口与另一个网络设备（例如路由器或交换机）之间的点到点连接（Point-To-Point Link）。Trunk 通过一个单独的物理线路负载多个 VLAN 的数据通信，并允许你在整个网络内扩展多个 VLAN。我们常见的有以下两种应用场合：

1. 路由器通过一个 Trunk 口接交换机的 Trunk 口，来完成该交换机上不同 VLAN 之间数据包的转发。这时如果要使用防火墙代替路由器，完成不同 VLAN 的包转发，就需要防火墙支持 Trunk 协议。否则防火墙只能通过使用自己的多个接口来分别挂接这些 VLAN 来实现访问控制。LinkTrust CyberWall 领信防火墙在千兆以太网口上支持工业标准的 802.1q VLAN Trunk 封装协议，可以使用防火墙的一个以太口与交换机的 Trunk 口相连，从效果上看相当于利用一个以太口完成了交换机上多个局域网之间的包转发，下图只是一个最简单的例子，实际上领信防火墙最多可以支持在一个以太口上划分 15 个 VLAN，以适应最复杂的网络结构。

2．另一种场合是一个具有路由模块或三层交换功能的交换机，通过一个 Trunk 口与一个交换机相连，来完成两个交换机上同一 VLAN 的通信，并完成两个交换机或一个交换机上不同 VLAN 之间的通信。这时，领信防火墙由于支持 Trunk 协议，可以用透明模式工作在已经架设好的两个 Trunk 口之间，实现 VLAN 间的访问控制。





在现今的交换式网络环境中，Trunk 功能被广泛应用，领信防火墙对这一功能的支持大大增加了防火墙对网络环境的适应能力。

5.8 带宽管理

LinkTrust™ CyberWall 防火墙为网络管理者提供了监测和管理网络带宽的手段，可以按照用户的需求对带宽进行控制，以防止带宽资源的不正常消耗，从而使网络在不同的应用中合理分配带宽，保证重要服务的正常运行。带宽管理可分为 8 个优先级，确保对于流量要求苛刻的企业，最大限度的满足网络管理的需求。LinkTrust™ CyberWall 防火墙的带宽管理可以实现：

多区域之间的带宽管理：国内外大多数防火墙目前只能实现内网与外网之间的带宽管理，对外网访问 DMZ 与 内网访问 DMZ 的流量无法控制。LinkTrust™ CyberWall 防火墙可以灵活实现企业各个区域之间的带宽管理，充分满足用户的各种需要。

对流量带宽的双向控制：LinkTrust™ CyberWall 防火墙可以对一个访问连接的上行流量（客户端到服务器）与下行流量（服务器到客户端）分别进行控制，保证这个连接的两个方向的流量有独立的控制策略。这样可以确保某些应用不会因为某一方向的带宽占用过多而导致另一方向没有可用的带宽资源。比如某企业对 HTTP 协议有整体的带宽限制要求，当某个用户利用 HTTP 协议在网页上下载软件时，必然导致下行流量在整个 HTTP 应用中占去很多带宽，如果防火墙不能分别控制上行与下行的流量，这种过多使用下行流量的行为将得不到限制，有可能将整个分配给 HTTP 协议使用的带宽耗尽，导致其他用户无法使用 HTTP。

从最精细到最宏观的管理策略：LinkTrust™ CyberWall 防火墙支持基于源 IP 地址、目的 IP 地址、协议、服务、方向、时间段的精细粒度的带宽管理策略，通过对每一个粒度元素设定可以满足对最精细流量控制的要求。LinkTrust™ CyberWall 防火墙也可以通过只设定少量的粒度元素（其它元素为”any”）来实现对流量的宏观控制，比如某企业需要控制整个企业的 HTTP

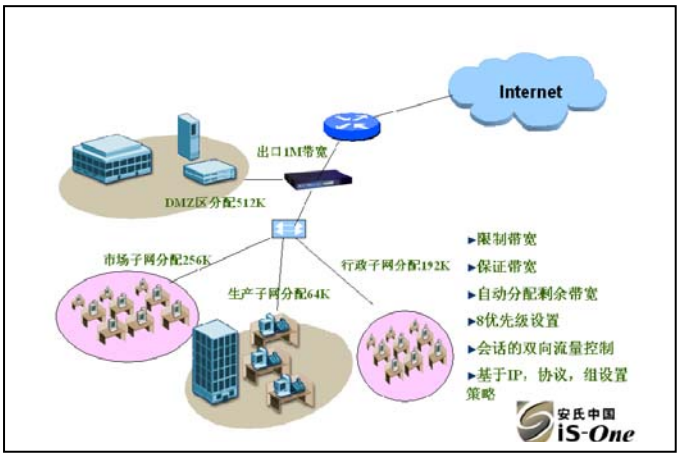
带宽，那么可以通过设定源 IP 和协议、服务来实现。

多层分布式带宽管理：LinkTrust™ CyberWall 防火墙支持多层分布式的带宽管理，可以完全虚拟带宽应用的实际环境。比如，某企业的 Solution 部门中有售前、售后和销售三个子部门，每个子部门有多个小组，为实现针对不同组织级别的流量控制，我们在防火墙上可以设置部门带宽、子部门带宽、小组带宽和个人带宽多层次的带宽管理策略，每下一层的带宽是在上一层的带宽基础上继续分配，这样避免了单层集中管理的缺点，优化网络资源的利用，提高了网络资源应用效率。

支持确保带宽与最大带宽：LinkTrust™ CyberWall 防火墙支持“确保带宽”与“最大带宽”的设定。通过“确保带宽”的设定可以保证重要用户和应用能够拥有足够带宽，保证关键业务不受网络负荷影响；同时，防火墙也能限制某些不重要的应用或用户网络带宽的上限值—“最大带宽”，保证网络资源的合理分配。

允许空闲带宽自动分配：当实际流量小于策略所规定的“确保带宽”时，就存在一定的空闲带宽，LinkTrust™ CyberWall 防火墙可以将这部分空闲带宽分配给其它的带宽需求，避免宝贵的带宽资源被浪费。

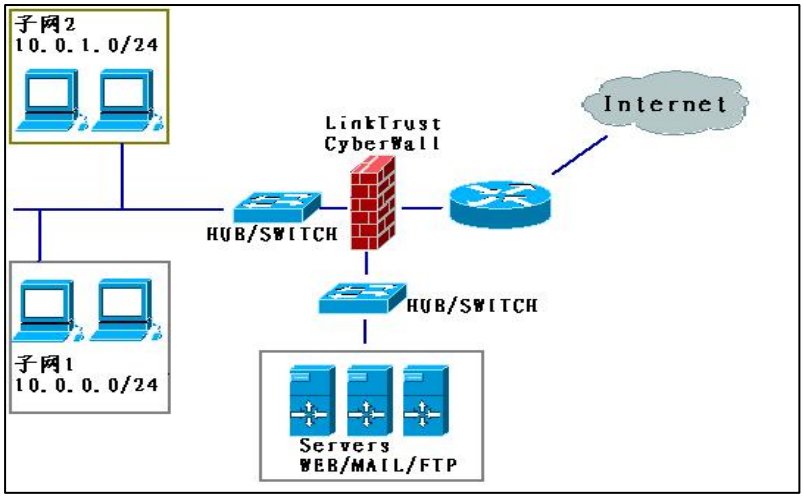
八种带宽分配优先级设置：LinkTrust™ CyberWall 防火墙支持八个级别的带宽分配优先级设定。在总带宽进行分配时，按照从高到低的优先级顺序满足带宽需求，同种优先级之间按照 Round-Robin 算法分配带宽。



透明模式下的带宽管理：LinkTrust™ CyberWall 防火墙支持透明模式下的带宽管理。

5.9 支持网络别名设置（划分子接口）

网络别名指的是在防火墙的一个接口上可以设置（绑定）多个 IP 地址，这些 IP 可以是相同或不同网段的，也可以叫做划分子接口。防火墙对这一功能的支持，使得其可以通过一个接口来实现不同网段之间的包转发，并对不同网段之间的访问进行控制。这对于需要划分子网但又缺少支持 VLAN 和 3 层交换设备的中小型网络是一个经济的解决方案，如图所示，



为实现子网 1 和子网 2 之间（甚至更多子网间）的包转发和访问控制，企业没有必要去购买具有多端口的价格相对昂贵的防火墙，使用 LinkTrust CyberWall-100SE 三网口的防火墙就可以解决问题。通过在防火墙的内网口上分别设置子网 1 和子网 2 网段的 IP 地址，防火墙即可完成子网间的访问控制及包转发。领信防火墙支持在任意接口设置网络别名（划分子接口），每个接口最多可划分 15 个子接口，为多样化的用户网络需求提供了适应性强、灵活多变的经济解决方案。

5.10 Smart Protector

防火墙与入侵检测是一套完整的网络安全解决方案重要的两个部分，二者各有所长，形成互补，一个好的入侵检测产品可以弥补防火墙静态防御的不足，而防火墙也可以加强入侵检测的响应力度。但同时部署防火墙和入侵检测产品将是一笔较大的资金投入，对于中小型企业来说将是一个非常昂贵的解决方案。

LinkTrust™ CyberWall 防火墙内置的 Smart Protector 入侵检测模块将防火墙与入侵检测功能有机的结合到一起，在节约用户投资的同时，为特定需求的用户群提供了业界领先的一站式安全防御系统。Smart Protector 具备如下特点：

不影响防火墙的包转发过程：Smart Protector 模块既要保证入侵检测的实时性，又要保证防火墙的包转发的速度不受影响，因此系统只是将通过防火墙的流量复制后交给 Smart Protector 进行检查，包转发的过程不受入侵检测模块的迟延，最大程度的降低了对防火墙性能的影响。

强硬的入侵响应力度：Smart Protector 模块虽然检测的是复制流量，但在检测到攻击后能够立即清除防火墙中已建立的状态表信息，实时切断已建立的恶意连接。防火墙还可以根据用户需要，从 Smart Protector 模块中提取攻击源信息，在系统中建立访问控制黑名单实时封杀攻击源，以实现对攻击行为最强的响应力度。另外，对 TCP 攻击，Smart Protector 还可以向攻击源发送 RST 包使其复位。

高效的检测能力：传统的入侵检测解决方案无法按照用户实际安全需求有选择性的配置监控流量，夹杂着大量无用数据的监测流量导致 IDS 系统资源被白白占用，致使 IDS 的检测能力

下降。LinkTrust™ CyberWall 的 Smart Protector 模块从以下两方面保证了检测流量的实用与精简，保证了高效的检测能力：

- Smart protector 工作在防火墙包过滤引擎的上层，只有防火墙过滤规则允许通过的数据包才进行检测，避免了入侵检测资源的浪费。
- iS-One 独有的 Policy Mirror Engine 允许用户按策略配置流量进行高效监控。通过防火墙规则策略的配置，用户可以根据实际安全需求有选择性的将某些规则对应的流量复制到 Smart Protector 模块进行检查，充分保证检测流量的实用性和高效的检测能力。

多种报警方式：Smart Protector 的报警可以通过 Syslog，SNMP Trap，Email 发送给日志服务器和管理员，或在防火墙的管理控制台上直接显示报警。

超过 250 种攻击手法的检测能力：Smart Protector 支持超过 250 种攻击的检测能力，覆盖当今世界范围内针对各种操作系统平台或网络设备的所有攻击手法，按照攻击类型分类，包括：

- DoS 攻击 10 种
- DDoS 攻击 30 种
- BackDoor 攻击 37 种
- WEB-IIS 攻击 26 种
- SNMP 攻击 14 种
- Port Scan 攻击 20 种
- NETBIOS 攻击 14 种
- TELNET 攻击 10 种
- APACHE 攻击 14 种
- SMTP 攻击 15 种
- FINGER 攻击 14 种
- DNS 攻击 15 种
- FTP 攻击 31 种

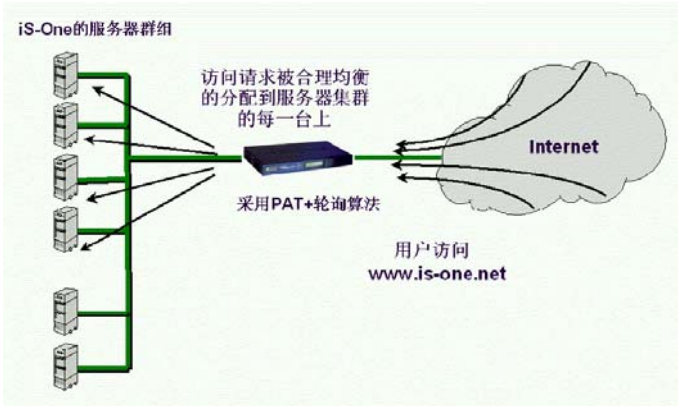
支持攻击特征库在线升级：Smart Protector 特征库的每个 Signature 都符合 CVE 标准，配合 iS-One 网站每月一次的更新速度，充分保证了攻击特征库的永久先进性。

用户自定义检测模板：用户可根据实际网络环境与安全需求，自行配置检测模板选用适合自己网络的攻击检测项，提供具有高度可定制性的入侵检测解决方案。

超负载保护能力：Smart Protector 在工作时紧密结合防火墙内核层(LTOS)，智能判断系统负荷是否过载，拥有超负载保护能力。

支持与 VPN 同时工作。

5.11 服务器负载均衡



LinkTrust™ CyberWall 防火墙利用端口 NAT 和系统内部集成的 Round-Robin 轮询算法提供了服务器负载均衡能力。防火墙将所有要送到某特定公共 IP(VIP)地址上某个 port 的包通过高效轮询算法合理的分别转送到某几个私有 IP 地址的内部机器的特定 port 上，从而实现负载均衡。目前的 LinkTrust™ CyberWall 防火墙可支持 8 个地址/端口的负载均衡，能让更多台服务器共同承担任务，从而以较低成本消除服务器瓶颈，大大提高了服务器的效率。

5.12 完整的H.323协议族支持

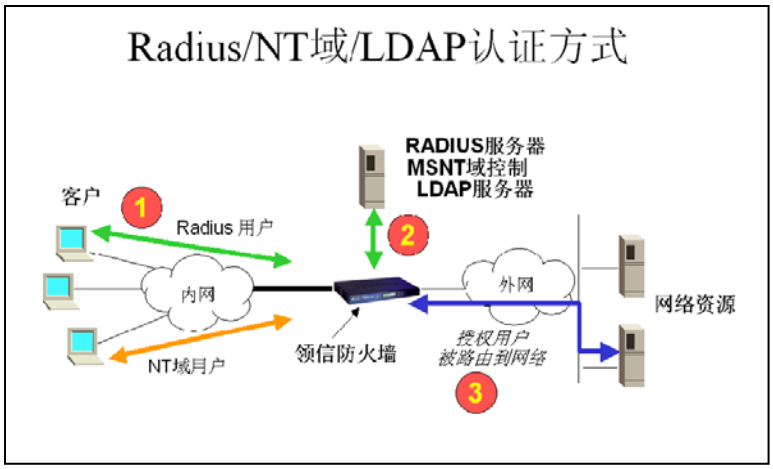
H.323 标准是为在网络上实现多媒体业务（实时的语音、视频和数据）而制定的，它规范了多媒体业务的成分、协议以及处理过程。H.323 可以实现语音（IP Phone）、视频（可视电话）和数据的融合（即现在所说的"三网合一"）。这在消费、商业以及娱乐业都有广泛的用途。目前中国主要电信运营商如吉通、网通、中国电信等的 IP 电话均使用 H.323 协议作为通讯协议。LinkTrust™ CyberWall 防火墙支持最完整的 H.323 协议族，包括 EP、MCU、GK 各组件的通讯，支持在透明、路由和 NAT 等所有工作模式下的各个方向的呼叫通讯。领信防火墙的 H.323 代理属于透明的双向核心级代理，可与包过滤模块和地址转换模块相互作用，动态打开需要的端口，从而增加了安全性，内部主机与外部主机可以通过 Netmeeting 呼叫对方，与对方的 Netmeeting 建立连接，使用 Netmeeting 提供的多媒体通信(声音、图象)和数据通信(聊天、白板、文件传送、共享)。

5.13 完整的SIP协议支持

在未来的 NGN 的网络环境中，SIP(Session Initiation Protocol)协议是 SoftSwitch 体系架构下的主要通讯协议。SIP 是一个面向 Internet 会议和电话的简单信令协议，用于建立、修改或结束一个或几个参与者的会议，它最初由 IETF MMUSIC (Multiparty Multimedia Session Control) 工作组提出。SIP 通过代理和重定向请求到用户当前位置来支持用户的移动性。由于 SIP 没有捆绑于任何特定的会议控制协议，因而协议具有普遍重要性，特别适用于电话相关的应用。具体来说，除典型应用于 IP 网络外，SIP 也被用于 ATM AAL5、IPX、 Frame Relay 或 X.25。LinkTrust™ CyberWall 防火墙根据 NGN 的体系架构，构建了自己完整的 SIP 功能模块，支持在透明、路由和 NAT 等所有工作模式下的 SIP 通讯控制。

5.14 多样化身份认证解决方案

LinkTrust™ CyberWall 防火墙支持全面的身份认证方式包括业界先进的认证技术与大量部署的流行认证方式，包括：内置认证数据库，支持用户名、口令，数字证书及用户地址等在本地的认证,支持 RADIUS 远程访问认证协议，支持 LDAP 轻量级目录访问协议，支持微软的 Windows 域控制协议，支持 RSA 的 SECURE ID，支持 PKI，支持 PAP 口令认证协议，支持 CHAP 挑战握手认证协议；我们综合多年在网络安全领域的经验在网络用户认证方式上采用主动认证与被动认证相结合的方式，各种认证方式具体应用如下



✧ **用户地址认证：**

应用于防火墙管理主机的地址认证。

✧ **数字证书认证：**

应用于防火墙管理员用户的数字证书认证

✧ **内置认证数据库提供的用户名、口令认证：**

应用于防火墙管理员用户的身份认证

应用于防火墙内网的网络用户或用户组可以使用网络服务的主动认证

✧ **RADIUS 远程访问认证协议、LDAP 轻量级目录访问协议及 Windows 域控制器支持：**

应用于防火墙内网的网络用户或用户组可以使用网络服务的主动认证，提供整个网络综合部署认证方式。

✧ **SecureID 认证支持：**

SecureID 认证方式提供了更加健壮的 Two-Factor Authentication 的认证方式，并能提供一次性动态口令、挑战/响应式认证支持。

✧ **PAP、CHAP、PKI 支持：**

用于企业组建虚拟专网（VPN）时，形成 VPN 隧道对象之间的身份认证，PKI 用于 IPSEC VPN 隧道建立身份认证。PAP、CHAP 用于 PPTP VPN 隧道建立身份认证。

✧ **主动认证：**

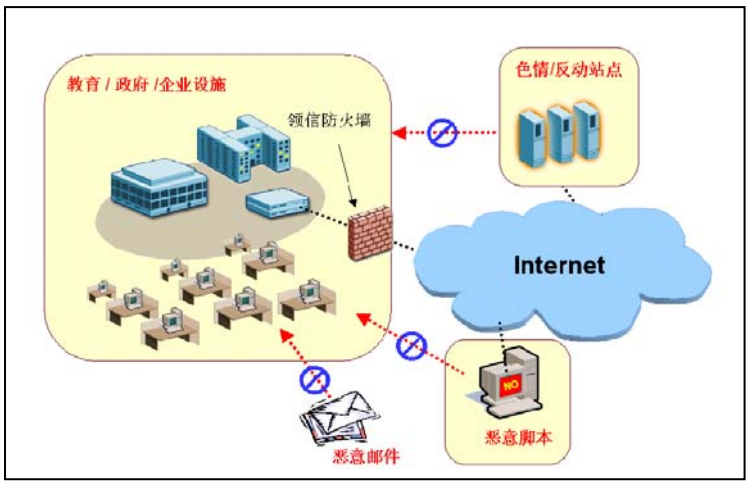
在包过滤策略中，管理员可以设置授权规则作为该过滤规则的响应方式。授权规则中的用户或用户组应按此规则的认证方式进行认证，这种方式为主动认证。通过了主动认证，符合该包过滤策略规则的包才能允许通过防火墙。主动认证适用于认证规则中的用户以及用户组中的成员用户。主动认证的方法为：通过 Web 浏览器，以 SSL 方式连接到防火墙，输入相应的用户名和密码,进行主动认证。我们支持的主动认证方式包括 RADIUS 认证,LDAP 认证、Windows

域认证和防火墙自身的认证。

✧ **被动认证**

另外，为方便用户的认证执行过程，领信防火墙对于 HTTP 代理策略的认证授权采用了被动认证的方式。用户在进行 HTTP 通讯之前不需要主动的登陆防火墙进行认证，当用户进行通讯时，防火墙收到 HTTP 请求，会主动返回一个 web 页面要求用户进行认证，认证通过后，通讯过程才能继续。

5.15 内容安全过滤



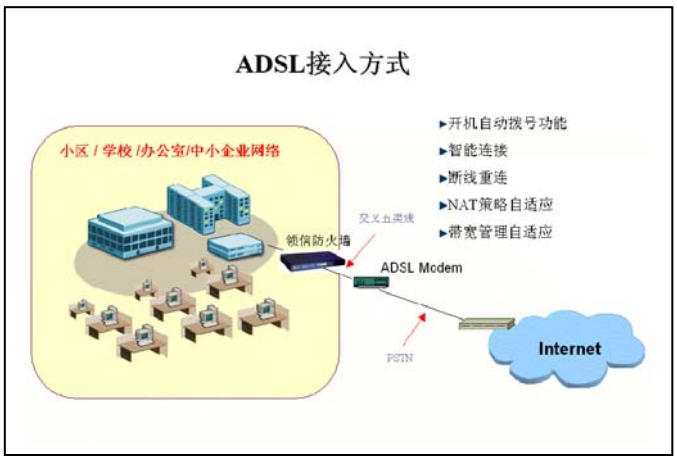
防火墙根据访问规则进行访问控制，一般只是对 IP 报头进行检查，不查看数据的具体内容，这样一些符合访问规则但含有恶意攻击代码的数据包也将能进入防火墙，而且一些怀有非法企图的网站通过利用在客户机系统中执行网页上的脚本进行攻击，如某些 JavaScript，这些都会给系统和网络带来安全隐患，对内网安全造成威胁；同时，在日常的网络管理中，管理员经常需要控制内部网络对某些站点的访问，如禁止用户访问暴力、色情、反动的主页或站点中的某些目录或文件，这就需要有方便有效的管理工具来给管理员提供严格管理的控制手段。LinkTrust™ CyberWall 防火墙提供多种内容安全过滤与内容访问控制功能，既能有效的防止外部恶意代码进入内网，也能控制内网用户对外部资源不良内容的访问及用户对网络服务的使用。CyberWall 提供的过滤控制手段包括：

- URL 屏蔽、监控
- Java/JavaScript/Active-X 过滤封堵
- FTP 命令控制 (内核级实现)
- ICMP 恶意代码过滤（内核级实现）
- 电子邮件中的收发信人地址和信件大小的过滤
- SMTP 命令的控制

5.16 基于时间控制的网络访问黑名单

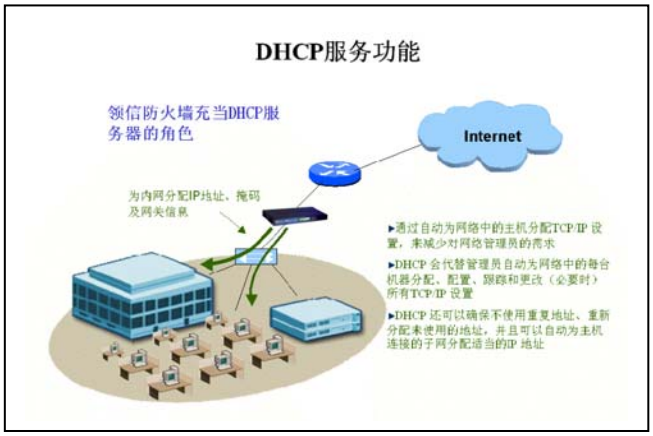
LinkTrust™ CyberWall 防火墙提供了阻止主机黑名单功能，对那些防火墙以外的 Internet 上的恶意站点及不希望内部员工在上班期间访问的站点进行按照时间段阻止，同时对内部滥用网络资源的 IP 进行按时间断阻止其向外访问。

5.17 支持PPPoE/宽带接入方式



领信防火墙的 PPPoE 模块专为 ADSL 拨号接入的用户而设计，利用 PPPoE 协议，防火墙可以方便的接入拨号网络，提供安全的网关防护功能。防火墙可以根据拨入后分配的外网口 IP 地址动态的调整 NAT 设置，确保实际获得的网络参数与防火墙本身配置的一致性。领信防火墙的 PPPoE 支持开机自动拨入功能，极大的方便了用户的使用，断线自动重连功能保证了拨号接入网络的可用性。另外，为节省用户的宽带接入费用，管理员可以根据本网络的使用情况，设定某段时间内无数据通过外网接口时，可暂时断开连接，当重新有数据通过时，可短时间内连接成功。值得一提的是，领信防火墙使用 PPPoE 拨号接入后，可以自动检测到 ISP 为此用户网络分配的出口带宽，并智能的调整防火墙的带宽管理策略使之适应动态变化的总出口带宽资源，实现用户网络价值的最大化。

5.18 支持 DHCP服务器功能



DHCP 功能省去了公司企业为单独设置 DHCP 服务器所消耗的成本，防火墙在启用了 DHCP 功能后，用户可以直接从防火墙所提供的 DHCP 服务上获得相应的 IP 地址、子网掩码、默认网关、DNS 等必要网络参数，方便了网络的统一管理。领信防火墙的任意接口区域都支持 DHCP 服务器功能，不限于内网。另外，在防火墙上集成 DHCP 服务器的功能与单独架设 DHCP 服务器相比，除了具有节省投资成本的好处，更重要的是保证了防火墙访问控制策略的完整性（Integrity），即内部数据与外部真实环境的一致性。如果防火墙与 DHCP 服务器分开设置，防火墙将不知道 DHCP 服务器给哪些主机分配了哪些地址，因此很难使用 IP 地址来进行访问控制；如果防火墙本身集成 DHCP 服务器功能进行 IP 地址分配，防火墙就可以知道主机获得的动态 IP 地址，从而进行访问控制。领信防火墙通过基于网络对象/组的 IP 分配技术和特殊 IP 预留分配技术来实现防火墙访问控制策略（内部数据）与实际 IP 分配（外部真实环境）的一致性。

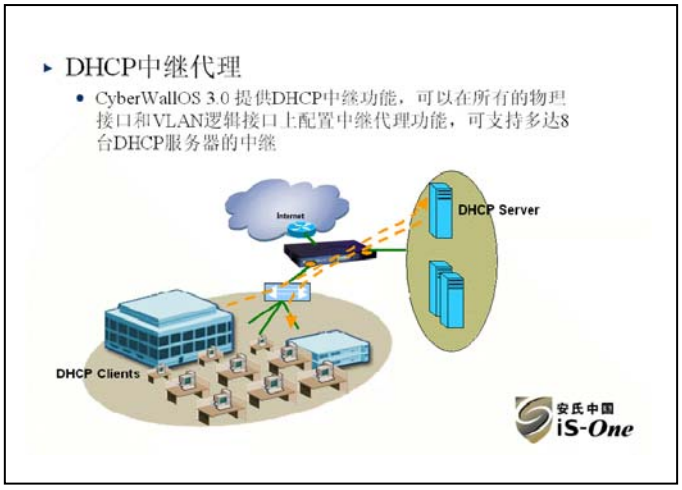
5.19 支持DHCP 客户端接入方式

对于一些小型企业网络，网关的外部地址是由 ISP 的 DHCP 服务器动态分配的，这就要求防火墙支持 DHCP 客户端接入方式，从 ISP 的服务器那里接受分配来的 IP 地址、掩码、默认网关、DNS 等参数信息，并动态的调整防火墙的 NAT 策略设置使之适应新分配的网络参数。整个参

数接收过程和策略的调整适应过程自动进行，无需管理员的参与。

5.20 DHCP中继代理

领信防火墙提供 DHCP 中继代理功能，可以在所有的物理接口和 VLAN 逻辑接口上配置中继代理功能，可支持多达 8 台 DHCP 服务器的中继



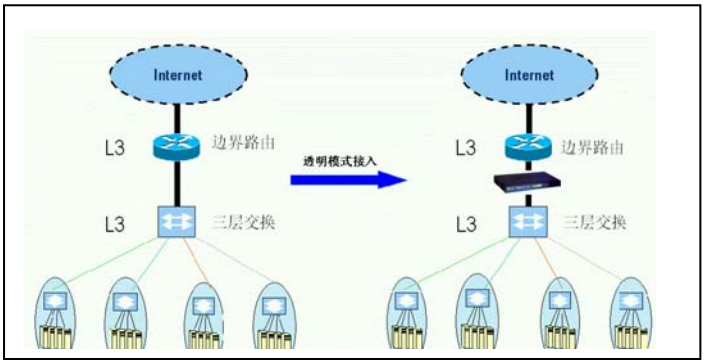
5.21 基于IP地址与MAC地址绑定的包过滤

在内部网络的应用中，经常会遇到内部网络用户擅自修改 IP 地址，以获取一个特定的 IP 地址来进行相应的网络应用，这样会使内部网络在地址资源的分配和使用上出现混乱，大大影响内部网络的正常运行，而且，在网络事故发生以后，也加大了地址追寻的难度。

LinkTrust™ CyberWall 防火墙所具有的 IP 与 MAC 地址绑定功能可以很好地解决这个问题。每一块网卡都具有一个唯一的物理标识号码，也就是网卡的 MAC 地址，每一个网卡的 MAC 地址都是独一无二的，对于网络协议为 TCP/IP 的两台设备进行通讯时，网络接口具有 IP 地址，当网络用户被分配或自行设定一个 IP 地址以后，可以在防火墙系统上建立 IP 地址与 MAC 地址的绑定关系，这样可限定 IP 地址只能在一台指定的工作站上使用，大大方便了网络的 IP 地址管理。

5.22 支持透明接入包过滤网桥

LinkTrust™ CyberWall 防火墙还支持网桥功能，可以实现局域网之间基于数据链路层的连接，在网络中传送由 MAC 控制信息、LLC 控制信息和网络层分组成的数据帧。



当防火墙接收到来自局域网 X 的数据帧后，在 MAC 子层去掉

MAC 的控制信息（X）交给 LLC 子层，一旦防火墙的 LLC 子层发现数据分组是发送到局域网 Y 中的某个工作站的，则把该 LLC 帧通过 MAC 子层加上控制信息送到局域网 Y 中，由局域网 Y 中的相应工作站接收。这样，局域网 X、Y 通过防火墙连接后，就好像在同一个局域网络里一样，网络中任何一台工作站都可以发送帧到任何其他工作站。而且，相对于一般桥接器的桥接功能，LinkTrust™ CyberWall 防火墙在进行桥接功能的同时，还能实现包过滤功能，可以对通过防火墙的数据报进行安全检测，并且根据一定的安全策略对某些数据包进行拦截，从而保证在完成桥接功能的同时，维护网络的安全性。

5.23 丰富的日志与强大审计分析能力

LinkTrust™ CyberWall防火墙提供丰富的日志信息，用户可根据特定的需要进行日志选项（不做日志、系统日志、访问控制策略日志、应用层协议日志、应用层内容日志、VPN日志、HA日志）。独创的网络实时监测信息，可详细审计命令级操作，便于入侵行为的分析和追踪。大大提高防火墙的审计分析的有效性,日志传送管理方式支持如下：

模块化的日志结构，采用模块、级别和处理方式相结合的方式配置日志，可以对单一模块、多个模块的组合以及所有模块指定处理方式。

提供从 Debug 到 Emergency 的八种级别的日志信息，在界面上以颜色区分，用户可根据实际情况定制日志级别

日志分字段显示，清晰明了，并提供从策略到相应日志的检索查询

LinkTrust™ CyberWall 防火墙支持 SNMP Trap 日志传送方式

LinkTrust™ CyberWall 防火墙支持标准的 Syslog 日志传送方式

LinkTrust™ CyberWall 防火墙支持重点日志 Email 传送方式

LinkTrust™ CyberWall 的日志输出支持 WELF 标准（WebTrends Enhanced Log Format）,用户可以直接将 CyberWall 产生的日志利用 Syslog 方式输送给 WebTrends，利用 WebTrends 提供的强大的日志分析和报表功能处理日志信息

LinkTrust™ CyberWall 防火墙具有日志审计功能，并有专门的日志接收与管理审计软件（LinkTrust™ Logman），提供给用户方便的过滤筛选、相关性分析、日志备份等丰富功能

5.24 多样化的告警方式

LinkTrust™ CyberWall 防火墙支持丰富的告警方式，提供给管理员多种的手段了解网络运行安全情况及防火墙系统自身运行情况。包括如下：

控制台方式：通过管理控制台可以实时监控日志告警信息。

SNMP TRAP（V2）：通过向支持 SNMP 协议的工作站发送 TRAP 方式，将告警信息发送给管理工作站

Syslog：以 Syslog 方式向管理工作站发送告警信息

电子邮件：通过向管理员定制的电子邮件帐号发送电子邮件来发送报警信息

上述的告警方式管理员可以依据管理的方便性灵活定制哪一类警报信息使用哪种方式。

5.25 网络与系统状态监控

5.25.1 网络流量统计

LinkTrust™ CyberWall 防火墙提供对于流经防火墙的数据流的字节数的统计功能，根据用户定义的统计规则分段采样数据并进行保留，用户可以随时通过生成的直观的统计图了解防火墙的各个时段的工作负荷和数据类型。

5.25.2 网络连接数统计

网络连接数与状态检测类防火墙的动态状态表资源密不可分，LinkTrust™ CyberWall 防火墙能够通过远程管理 Web 界面或本地液晶显示屏实时统计当前活动连接数，曾达到的最大连接数与 TCP、UDP、ICMP 的连接次数。

5.25.3 CPU负载与流量实时监视

LinkTrust™ CyberWall 防火墙通过前端的液晶显示屏可以让用户以图形的方式实时的了解防火墙的 CPU 负载与通过防火墙的流量变化与峰值情况。

5.25.4 电子邮件发送统计图

LinkTrust™ CyberWall 防火墙支持 Email 发送统计图功能，使网络管理员能方便的进行日常的流量监控

5.26 系统内核的在线升级能力

LinkTrust™ CyberWall 防火墙支持系统内核的在线升级，在不中断、不影响防火墙正常工作的情况下，能够从网络对系统内核版本进行升级。

5.27 系统内核的自动备份

为防止单内核损坏时系统无法工作，LinkTrust™ CyberWall 防火墙提供系统内核的自动备份与恢复功能。

5.28 防火墙配置信息的备份

LinkTrust™ CyberWall 防火墙支持配置信息的备份，配置信息加密存储在防火墙上，并能以文件形式通过 Web 管理界面远程下载保存。同时，CyberWall 防火墙支持在不中断、不影响系统正常工作的情况下对配置信息的在线恢复与更新。

5.29 防火墙配置文件的智能化加载

LinkTrust™ CyberWall 防火墙支持配置文件的智能化加载。由于防火墙内核版本的升级或

安装了扩展模块的许可证（License）会使得原有的配置文件中的系统配置信息或规则配置信息与现有环境不兼容，在加载配置文件时，防火墙会自动检查文件的兼容性，提取出有效的部分加载，把不兼容的部分剔除，并在界面上提示用户，避免了由于兼容性问题带来的所有配置信息丢失或错误信息的加载。

5.30 全面的自身安全与高可靠性设计

LinkTrust™ CyberWall 防火墙从软、硬件的角度多方位的保证系统的自身安全性与高可靠性，CyberWall 的软件系统：

通过了世界权威的安全平估工具 ISS Internet Scanner 的强力扫描测试

采用专门设计，根据各种攻击测试结果不断加固的操作系统（LTOS 核心）

系统双内核与系统配置、安全策略的备份，在最大程度上确保系统的可靠性

双机热备功能，确保系统 7X24 小时不间断运转

CyberWall 的硬件系统：

采用基于 Intel 架构的专门硬件搭载平台，支持多种操作系统，具有高可靠性、安全性、环境适应性等特点，广泛用于军事、金融、政府等领域，其技术成熟性保证了硬件的可靠性

高指标的电气参数要求，保证对环境更加广泛的适应性，从而保证了硬件的可靠性

- 工作温度：0 度---50 度
- 储存温度：-20 度~+70 度
- 相对湿度：5%----95%，无凝露等。

结构设计上充分考虑通风、散热及电磁兼容等特性的要求，具备过压和短路保护，辐射和噪声符合 EN55022、EN55011 的 B 级标准，通过了 UL、VDE 及 CSA 等安规认证，符合 CE 标准，MTBF 指标高达 100000 小时。

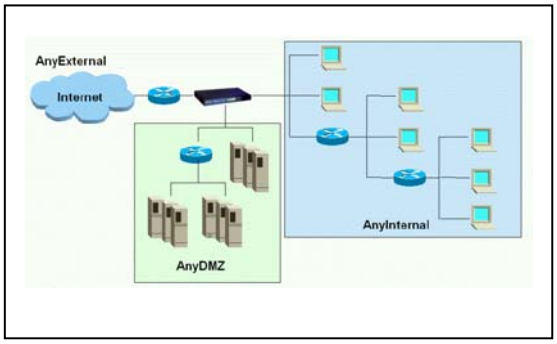
5.31 支持远程集中管理

LinkTrust™ CyberWall 防火墙通过数字证书认证、管理主机地址认证等完善的认证措施与管理信息的加密传输实现全局防火墙设备的集中管理。实现统一的安全策略部署，保证各环节安全策略的一致性，提供了整个系统的安全强度。同时，LinkTrust™ CyberWall 防火墙的集中管理具有方便易用的特点，用户不需要安装专门的管理软件，只需使用支持 128 位 SSL（安全套接字层）加密的浏览器，就可以在不同操作系统平台和不同地域对全局防火墙进行配置。

5.32 面向对象的管理机制

LinkTrust™ CyberWall 防火墙支持面向对象的管理方式，对象是由各类资源（主机，网络，服务，用户，时间，网络接口等）组成的实体，通过定义好的对象所建立的策略规则使控制更加细化，更加直观，易用性更强，提高了管理员的配置效率和配置的灵活性。

5.33 内网复杂结构的简单配置



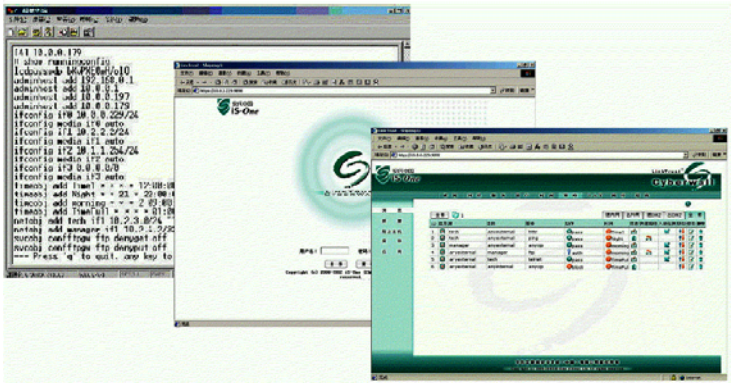
对于内网或 DMZ 区有复杂的网络结构时，既可以通过 ANYINTERNAL/ ANYDMZ 系统保留字实现多网段共同的访问策略的定制，又可以根据不同的网段分别配置不同的访问策略。

5.34 支持多种工作模式

LinkTrust™ CyberWall 防火墙支持透明、路由和 NAT 等多种工作模式，适应各种网络结构和用户需求。

5.35 多种配置管理界面

- ✧ 提供安全、友好、易用的全中文的 Web 管理界面
- ✧ 提供专业人员熟悉和喜欢的快速的命令行配置界面
- ✧ 在防火墙机箱的前面版上，提供液晶显示屏（LCD）和迷你键盘，用户可以在上面对防火墙进行简单的配置操作和相关信息的查询操作
- ✧ SSH 远程管理
- ✧ Global Manager 管理软件，提供简洁的集中管理功能，实现企业安全策略的完整性。



5.36 精细粒度安全角色分级管理

目前网络应用的发展步伐很快，企事业的网络规模不断增大，网络管理的任务也越来越复

杂，简化管理任务的一个办法是对管理任务进行分割，对管理用户进行角色分工，按角色的不同分配不同的管理任务。对不同角色或权限的管理员来说，所见的防火墙系统是不一样的。超级管理用户对防火墙具有无限制的管理权，而其余管理用户的管理权限均由超级管理用户分配。领信防火墙的多级用户管理功能就是为了简化防火墙管理员任务和实现安全分级控管而量身定做的。防火墙的管理用户分为以下角色：

超级管理用户（Super Admin）：对防火墙具有完全、无限制的管理权限。

普通管理用户（General Admin）：对防火墙的管理权限由超级管理用户授予其对系统不同功能模块的配置权限。

另外，为用户使用方便考虑，系统内置了两个管理帐号，一个是超级用户管理帐号(admin)，另一个是对各功能模块仅具只读权限的普通帐号（guest）。

分级管理使对防火墙的管理更加安全可控，避免人为因素带来的安全风险。

5.37 安全的管理员访问控制机制

LinkTrust™ CyberWall 防火墙对管理员有严格的访问控制机制：

登录失败时，系统提供自动保护能力，防止用户名、口令的暴力破解

- 通过 WEB 浏览器登录的系统管理员，如果连续登录失败的次数超过 3 次，则该管理地址将被禁止进行管理，需授权通过的管理主机的系统管理员重新启用该管理地址。
- 通过控制台终端进行登录的系统管理员，每一次登录失败，系统自动延时 1 秒后，再重新提示管理员登录信息。

5.38 智能型配置精灵

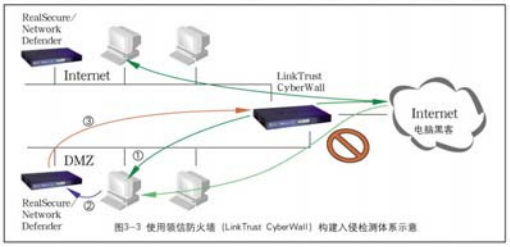
LinkTrust™ CyberWall 防火墙支持智能的配置精灵（Wizard）功能，通过分步界面引导用户如何配置防火墙基本信息，并提示您配置中的错误。即使您是初次使用者，也可以通过配置精灵的帮助清楚地掌握如何配置防火墙。

5.39 完整的IDS联动解决方案

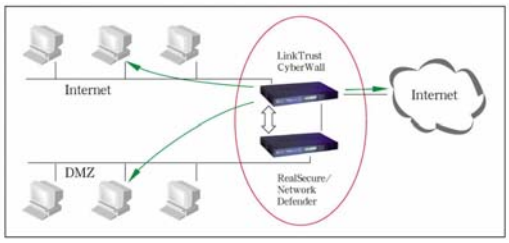
入侵检测能力是衡量一个防御体系是否完整有效的重要因素。强大的、完整的入侵检测体系可以弥补防火墙相对静态防御的不足。但是，传统的设计中，防火墙和 IDS 各成体系，互不相通，难以提高整体防御体系的智能性和及时性。

LinkTrust™ CyberWall 防火墙在设计中利用安氏公司在 IDS 技术方面深厚的积累，充分考虑了用户系统的实际需求，独特的设计可以使防火墙与 IDS 系统完全融为一体，即在使用 CyberWall 的插件后，RealSecure 在特定事件配置其响应策略时，可以选择通过 CyberWall 禁止特定数据包来进行访问控制，达到保护内部网络和 IDS 系统的双重目的。与 IDS 联动提供如下能力：

- LinkTrust™ CyberWall 防火墙可灵活设置专门的 IDS 流量镜像端口，支持通过该端口



专用响应方式



端口镜像方式

流量的双向转发，IDS 响应方式中的 TCP reset 直接作用于攻击连接；

- 支持 IDS 按策略监视网络流量，提供了一种独特的网络安全架构，提供给用户重点监视可疑网络流量的能力，减轻了 IDS 无效负载。
- IDS 将直接把攻击信息通过 EsafeLink Protocol 通知 LinkTrust™ CyberWall 防火墙，将其列入网络访问黑名单（阻止主机列表），封杀攻击源。
- 用户对攻击源的封杀可以依据时间段来配置。
- LinkTrust™ CyberWall 防火墙可以实施阻断已经建立的攻击 session.

5.40 安全性和高可扩展性的EsafeLink Protocol协议

LinkTrust™ CyberWall 防火墙采用专有的 Esafelink protocol 协议与 ISS RealSecure 及 LinkTrust Network Defender 实现互操作，为用户提供更高的安全性与可扩展性。Esafelink protocol 协议基于 HTTP、SSL 与 XMLRPC 等标准协议，具有以下特点：

封装形式标准，利用了 http 通用的协议进行封装，减少了自定义协议带来的不全面和不安全的风险。

协议解析简单，不需要专用的协议解析模块，通信双方对于需要实现的功能，通过 RPC 调用，并以标准的 XML 进行封装。

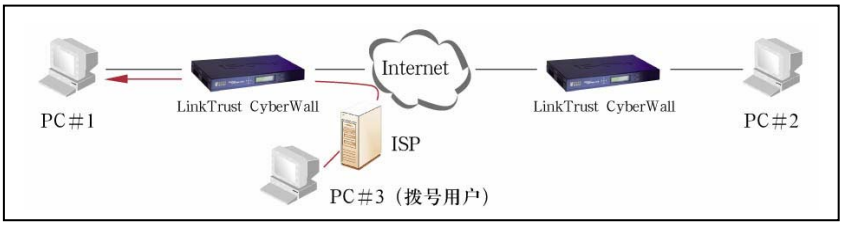
可扩展性好，对于任何与 LinkTrust 安全管理平台通信的产品部件，只需要它提供 API，利用 EsafeLink Agent 调用 API，通过 EsafeLink protocol 即可实现与安全管理平台的通信。

5.41 无缝虚拟专网支持

所谓 VPN（Virtual Private Network）虚拟专用网络，是指利用虚电路在公网上面传输专用业务的网络。它提供了一种通过公用网络安全地对企业内部专用网络进行远程访问的连接方式。VPN 由客户机、传输介质和服务器这三部分组成，VPN 连接使用隧道作为传输通道，这个隧道是建立在公共网络或专用网络基础之上的，如：Internet 或 Intranet。

LinkTrust™ CyberWall 防火墙可以扩展 VPN 模块支持，既可以利用因特网（Internet）IP 通道为用户提供具有保密性，安全性，低成本，配置简单等特性的虚拟专网服务，也可以为移动的用户提供一个安全访问公司内部资源的途径，通过对 PPTP 协议的支持，用户可以从外部虚拟拨号，从而进入公司内部网络。CyberWall 的虚拟专网具备以下特性：

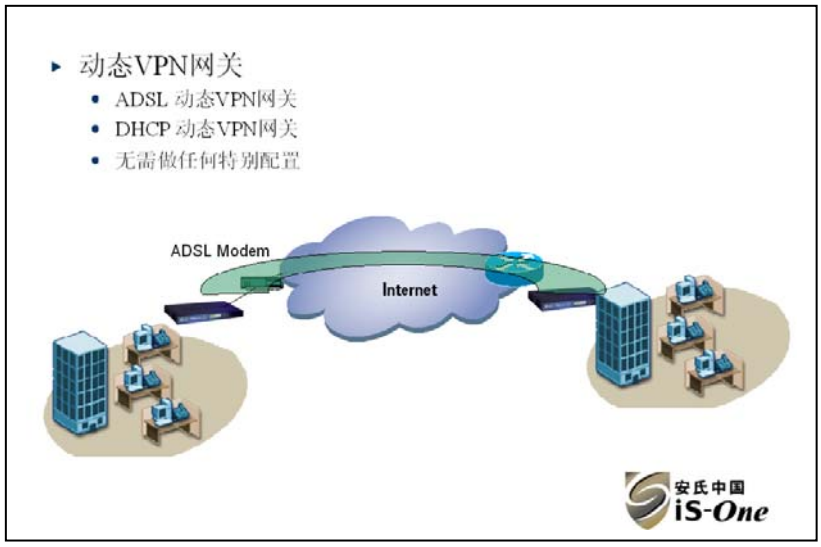
- 标准的 IPSEC,IKE 与 PPTP 协议
- 支持 Gateway-to-Gateway 网关至网关模式虚拟专网
- 支持 VPN 的星形（star）连接方式
- 支持 IP 与非 IP 协议通过 VPN
- 支持手工密钥，预共享密钥与 X.509 V3 数字证书,PKI 体系支持
- IPSEC 安全策略的灵活启用：管理员可以根据自己的实际需要，手工禁止和启用单条 IPSEC 安全策略，也为用户提供了更大的方便。
- 支持密钥生存周期可定制
- 支持完美前项保密
- 支持多种加密与认证算法：
  - 加密算法：DES, 3DES,AES,CAST,BLF，PAP，CHAP
  - 认证算法：SHA, MD5, Rmd160



- 支持 Client-to-Gateway 移动用户模式虚拟专网
- 支持 PPTP 定制：管理员可以根据自己的实际需要，手工禁止和启用 PPTP。由于 PPTP

需要使用一个 1723 的 TCP 端口进行连接，是防火墙比较脆弱的部位，对整个防火墙构成了潜在的威胁。当用户不使用 PPTP 功能、或对安全性要求较高时，用户可以禁止启用这一功能，大大提高了防火墙的性能及安全性。

5.42 动态IP VPN 网关



随着 ADSL、城域网的发展，越来越多的用户通过这种方式接入到 Internet，但是 ADSL、城域网的 IP 地址大多数为动态的，也就是说：利用 ADSL 接入的防火墙每一次接入时的 IP 地址都不一样。这给 VPN 建设提出了新的挑战，因为要建立 VPN 的时候必须知道对方的 IP 地址，而 ADSL 接入的 IP 地址是动态的。同样，对于防火墙利用 DHCP 获取外网口 IP 地址的接入方式也存在这种问题，因此需要 VPN 设备支持动态 IP 的 VPN 隧道建立。

领信防火墙支持一端为动态 IP，另一端为固定 IP 的 VPN 自动组网方式。动态端通过加密的数据传输，把接入后分配到的 IP 信息通知固定端，固定端对此信息进行身份认证后，根据传来的信息自动调整 VPN 隧道策略，重新与动态端完成 VPN 的组建。对于用户来讲，根本不必关心每次接入时分配到的 IP 地址，整个过程不需要任何的人工参与，完全由防火墙自动完成，动态端在每一次接入后，自动完成与固定端 VPN 通道的建立。

5.43 Patent pending 的 LinkTrust™ Security Processor

LinkTrust™ Security Processor 是一颗专门用于 IP 通讯安全的高性能安全处理器，他支持处理所有的与安全相关的协议包括 IPSec, Internet Key Exchange (IKE), Secure Socket Layer (SSL) and Transport Layer Security (TLS)，处理能力相当于 1000MIPS，等同于 12－18 颗的 Pentium III 级微处理器对数据加密的处理能力。LinkTrust™ Security Processor 赋予了 LinkTrust™CyberWall-100 可怕的数据加密处理能力，在 IP 安全通讯领域中承担着，VPN 中央数据加密处理核心节点的位置。

对 IPSEC 数据加密处理 时使用 3DES, HMAC-SHA-1 组合性能为 100M 线速

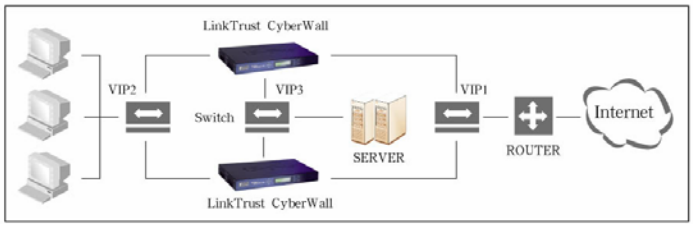
LinkTrust™ Security Processor 对 SA 拥有无限制的支持能力，

LinkTrust™ Security Processor 对 Diffie-Hellman 的密钥交换提供每秒超过 250 次的支持能力(1024-bit public key, 180-bit private key).

LinkTrust™ Security Processor 同时提供对 IKE、SSL、TLS 的 100M 线速处理支持能力。

LinkTrust™ Security Processor 为安氏 Esafelink 高速网络解决方案注入了惊人的数据加密封装力量。目前这颗安全处理器的技术正在专利申请之中。

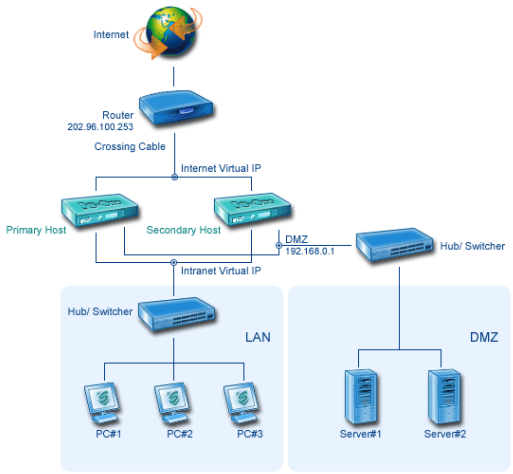
5.44 LinkTrust™ VRRP双机热备份功能



所谓双机热备，是指为了解决单机单点故障引起的防火墙系统瘫痪问题而提供的两台防火墙实时热备功能，即除主机以外，还有一台防火墙处于热备状态，这两台机器共同拥有一个对外的虚拟 IP 地址，有机地构成了一个具有实时热启动的高可靠性防火墙系统。其中一台主机被指定为“主机”，另外一台被定义为“备机”，处于“主”状态的防火墙实时广播数据包，而处于“备份”状态的防火墙则通过监听数据包的方式来发现系统故障或者线路故障，当“主”状态系统出现故障时，处于“备份”状态的防火墙将在很短的时间内转变成“主”状态防火墙，从而为系统提供 7x24 小时不间断服务。

LinkTrust™ CyberWall 防火墙的 HA 架构设计，通过加强的 VRRP 协议，为用户提供了最高可用性的产品，CyberWall 的 HA 功能具备以下特性：

- 设备发生故障时自动切换
- 链路发生故障时自动切换
- 手工宣告切换
- 切换时间小于 1 秒



6 附录：联系方式

北京公司总部

北京东长安街 1 号东方广场办公楼 W3 座 1208 室　　邮编：100738

电话：010-85181101　　传真：010-85184777

安氏实验室

北京市海淀区三里河路 15 号中建大厦 A 座 8 层　　邮编：100037

电话：010-88083566　　传真：010-88083172

广州分公司

地址：广州市天河北路 689 号光大银行大厦 12 楼 C3-E2 室　　邮编：510630

总机：020-38731555、38732069、38730525 转 2013

手机：13600056899　　传真：020-38730144