前言

互联网的发展给政府机构、银行、证券、企事业单位带来了革命性的改革和变化。互联网技术的迅猛发展使企业通过利用互联网来提高办事效率和市场反应速度，以便更具竞争力。通过使用互联网技术，任何一个单位的数据资料的传输和存取都变得方便、快捷，但同时也面对 Internet 开放带来的数据安全的新挑战和新危险：即客户、销售商、移动用户、异地员工和内部人员的安全访问；以及保护国家机关、企事业的机密信息不受黑客和商业间谍的入侵。越来越多的通信都通过电子邮件进行；移动员工、远程办公人员和分支机构都利用互联网来从远程连接他们的企业网络；而在互联网上通过 WWW 方式完成的商业贸易现在已经成为企业收入的重要组成部分。但是这个庞大的网络及其相关的技术为不断增长的安全威胁提供了可乘之机，因而企业必须学会保护自己免受这些威胁的危害。在捍卫网络安全的过程中，防火墙受到人们越来越多的青睐。作为一种提供信息安全服务、实现网络和信息安全的基础设施，防火墙采用将内部网和公众网如 Internet 分开的方法，可以作为不同网络或网络安全域之间信息的出入口，根据企业的安全策略控制出入网络的信息流。再加上防火墙本身具有较强的抗攻击能力，能有效地监控内部网和 Internet 之间的任何活动，从而为内部网络的安全提供了有力的保证。

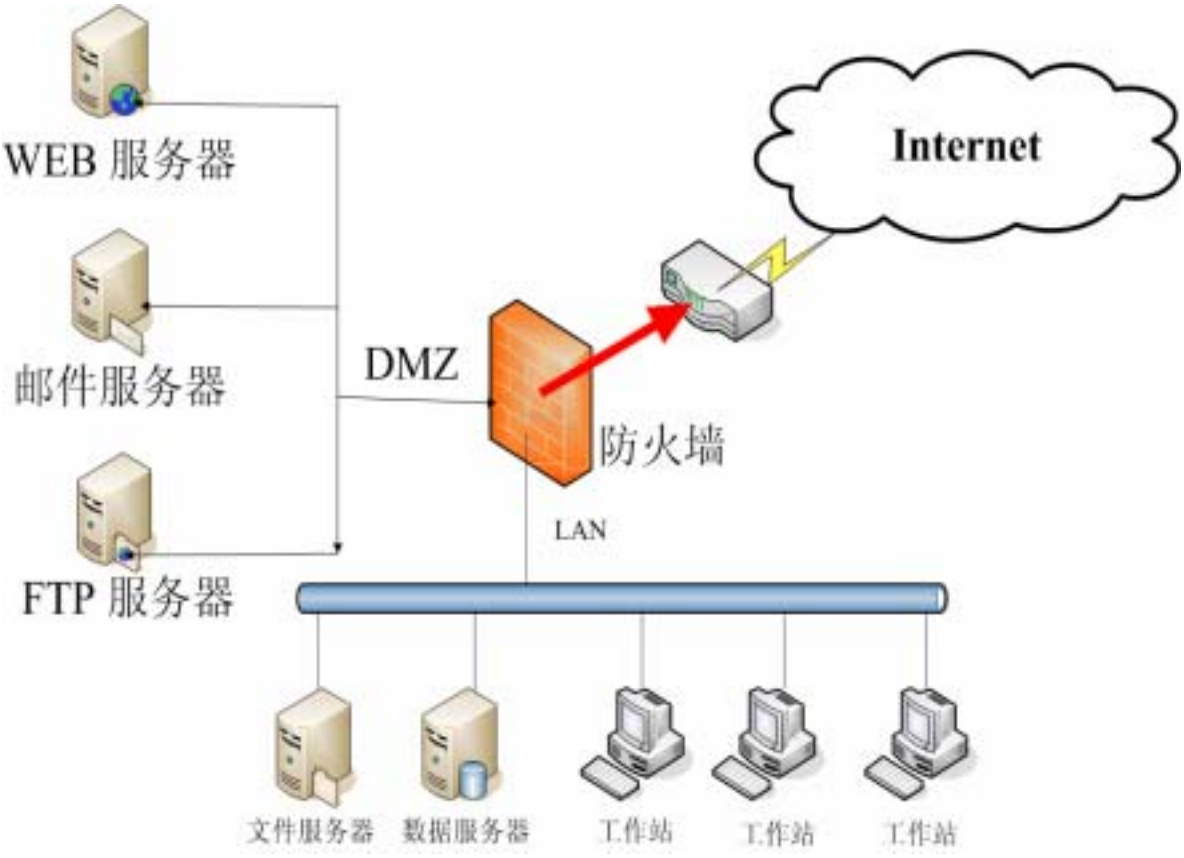
随着当今社会的不断发展网络技术可为无所不在，无论是公司还是个人办公都越来越离不开网络。因而也就有新的问题产生了随着企业的不断扩大分支机构越来越多，合作伙伴越来越多，移动用户越来越多，企业希望能通过无处不在的因特网来实现方便快捷的访问，既经济又安全的企业间的互连成了一个很重要的问题。如果采用专用线路构建企业专网，往往需要租用昂贵的跨地区数据专线。如何能够利用现有的 Internet 来建立企业的安全的专有网络呢？虚拟专用网（VPN）技术就成为一个很好的解决方案。虚拟专用网（VPN）是指在公共网络中建立专用网络，数据通过安全的“加密通道”在公共网络中传播。但企业只需要租用本地的数据专线或 ADSL，甚至宽带小区等上网方式，连接上本地的 Internet，各地的机构就可以互相传递信息；同时，企业还可以利用 Internet 的拨号接入设备，让自己的用户拨号到 Internet 上，就可以连接进入企业网中。使用 VPN 有节省成本、提供远程访问、扩展性强、便于管理和实现全面控制等优点，将会成为今后企业网络发展的趋势。

第一章 防火墙的技术介绍

1.1 什么是防火墙

防火墙是一类防范措施的总称，它使得内部网络与 Internet 之间或者与其他外部网络互相隔离、限制网络互访用来保护内部网络。防火墙简单的可以只用路由器实现，复杂的可以用主机甚至一个子网来实现。设置防火墙目的都是为了在内部网与外部网之间设立唯一的通道，简化网络的安全管理。

位于内部网（信任域）和 Internet(非信任域)之间的防火墙，如图



在这种情况下，防火墙的主要的功能有：

1、过滤掉不安全服务和非法用户

2、控制对特殊站点的访问

3、提供监视 Internet 安全和预警的方便端点

1.2 防火墙的基本类型

根据防火墙所采用的技术不同，可以将它分为三种基本类型：包过滤型、代理型

和全状态检测型。

1.2.1 包过滤型

包过滤是第一代防火墙技术，它按照安全规则，检查所有进来的数据包，而这些安全规则大都是基于低层协议的，如 IP、TCP。如果一个数据包满足以上所有规则，过滤路由器把数据向上层提交，或转发此数据包，否则就丢弃此包。

包过滤的优缺点

优点：一个过滤路由器能协助保护整个网络；数据包过滤对用户透明；过滤路由器速度快、效率高。

缺点：不能彻底防止地址欺骗；一些应用协议不适合于数据包过滤；正常的数据包过滤路由器无法执行某些安全策略。

1.2.2 代理型

代理是一种较新型的防火墙技术，这种防火墙有时也被称为应用层网关，这种防火墙的工作方式和过滤数据包的防火墙、以路由器为基础的防火墙的工作方式稍有不同。它是基于软件的。

电路层网关是建立应用层网关的一个更加灵活和一般的方法。虽然它们可能包含支持某些特定 TCP/IP 应用程序的代码，但通常要受到限制。如果支持应用程序，那也很可能是 TCP/IP 应用程序。在电路层网关中，可能要安装特殊的客户机软件，用户可能需要一个可变用户接口来相互作用或改变他们的工作习惯。

代理技术的优缺点

优点：代理易于配置；代理能生成各项记录；代理能灵活、完全地控制进出的流量、内容；代理能过滤数据内容；代理能为用户提供透明的加密机制；代理可以方便地与其他安全手段集成。

缺点：代理速度较路由器慢；代理对用户不透明；对于每项服务代理可能要求不同的服务器；代理服务不能保证你免受所有协议弱点的限制；代理不能改进底层协议的安全性。

1.2.3 全状态检测型

全状态检测型防火墙是新一代的产品，这一技术实际已经超越了最初的防火墙定义。全状态检测型防火墙能够对各层的数据进行主动的、实时的监测，在对这些数据加以分析的基础上，全状态检测型防火墙能够有效地判断出各层中的非法侵入。同时，这种检测型防火墙产品一般还带有分布式探测器，这些探测器安置在各种应用服务器和其他网络的节点之中，不仅能够检测来自网络外部的攻击，同时对来自内部的恶意破坏也有极强的防范作用。据权威机构统计，在针对网络系统的攻击中，有相当比例的攻击来自网络内部。因此，全状态检测型防火墙不仅超越了传统防火墙的定义，而且在安全性也超越了前两代产品。

SonicWALL 就是采用全状态检测技术的防火墙。

第二章 SonicWALL 第四代网络安全产品线

SonicWALL 公司成立于 1991 年，主要进行全面互联网安全解决方案的设计、开发和生产，为广大的市场提供访问安全、增值安全服务和交易安全产品。其著名的 SonicWALL 系列防火墙，采用全状态检测防火墙的技术，并提供各种企业级功能，功能强大、齐全，价格低廉，是目前世界上性能价格比最高的网络防火墙产品。所服务的对象包括：SOHO、SME、企业、服务提供商、电子商务、政府、教育和医疗机构。目前，全球 SonicWALL 防火墙的销量已突破 50 万台。

SonicWALL 公司从 2003 年 11 月推出第四代产品以来，已推出以下四款产品：PRO 4060 、PRO 3060、PRO 2040 和 TZ 170 。同时推出另外新的操作系统 SonicOS ，客户根据网络环境的需求选择不同的操作系统。

2.1 TZ 170 适合小型公司，小型办事处，连锁店，家庭办公使用

1) 3 安全地区 (Zones)
   - SonicOS 标准版软件 (LAN, WAN, WorkPort)
   - SonicOS 加强版软件 (可自订)
2) 7 个以太网端口
   - WAN 端口
   - 5 个 LAN 端口 (二层交换机)
   - 可选项端口
3) RJ45 串行口。CLI 管理用 (SonicOS 加强版软件)
4) 90 Mbps 防火墙吞吐量

SonicWALL generation 4 product specification matrix

5) 30+ Mbps 3DES 和 AES VPN 吞吐置
6) 硬件 AES 加密/解密
7) 8 MB Flash, 64 MB RAM
   - 预留内存给将来安全服务使用
8) 6,000 TCP/IP 并发连接
9) 高达 250 条防火墙规则 (SonicOS 加强版软件)

2.1.1 SonicWALL TZ 170 无限用户

> 跟 SonicOS 标准版软件
> 支持 ISP 客错 (Failover), 措施式 (Policy Based) 的 NAT
> 中小企业的理想型号
> 没有用户数量的限制
> 10 site-to-site VPN 隧道, 包括 1 个 Global VPN Client (最多 50 个)
> 可升级至 SonicOS 加强版软件

2.1.2 SonicWALL TZ 170 25 用户

> 跟 SonicOS 标准版软件
> 小型公司的理想型号
> 包括 25 个用户 licenses (LAN 的 IP 地址)
> 10 site-to-site VPN 隧道, 包括 1 个 Global VPN Client (最多 50 个)
> 可升级至 SonicOS 加强版软件

2.1.3 SonicWALL TZ 170 10 用户

> 跟 SonicOS 标准版软件
> 小型公司和在家办工的理想型号
> 包括 10 个用户 licenses (LAN 的 IP 地址)
> 10 site-to-site VPN 隧道, Global VPN Clients 为可选项 (最多 5 个)
> 可升级至 SonicOS 加强版软件

2.2 **PRO 2040 适合中/小商业,分支机构（100-250 节点)。**

1) ４安全地区 (Zones)
   - SonicOS 标准版软件 (LAN, WAN, DMZ)
   - SonicOS 加强版软件 (可自订)
2) 4 个以太网端口
   - 1 个 WAN 端口
   - 1 个 LAN 端口
   - 自定义端口
3) RJ45 串行口。CLI 管理用 (SonicOS 加强版软件)
4) 200 Mbps 防火墙吞吐量
5) 50 Mbps 3DES 和 AES VPN 吞吐置
6) 硬件 AES 加密/解密
7) 64MB Flash,128 MB RAM
8) 32,000 TCP/IP 并发连接

9) 高达 512 条防火墙规则 (SonicOS 加强版软件)
10) 50 site-to-site VPN 隧道, 包括 1 0 个 Global VPN Client (最多 100 个)

2.3 **PRO 3060 适合中/大型商业（200-300 节点）**

1) 6 安全地区 (Zones)
   - SonicOS 标准版软件 (LAN, WAN, DMZ)
   - SonicOS 加强版软件 (可自订)
2) 6 个以太网端口
   - 1 个 WAN 端口
   - 1 个 LAN 端口
   - 自定义端口
3) RJ45 串行口。CLI 管理用 (SonicOS 加强版软件)
4) 300+ Mbps 防火墙吞吐量
5) 75 Mbps 3DES 和 AES VPN 吞吐置
6) 硬件 AES 加密/解密
7) 64MB Flash,256 MB RAM
8) 128,000 TCP/IP 并发连接
9) 高达 500 条防火墙规则 (SonicOS 加强版软件)
10) 1000 site-to-site VPN 隧道, 包括 25 个 Global VPN Client (最多 500 个)

2.4 **PRO 4060 适合大型商业/小企业 （200-300 节点或大 VPN 流量）**

1) 6 安全地区 (Zones)
   - SonicOS 标准版软件 (LAN, WAN, DMZ)
   - SonicOS 加强版软件 (可自订)
2) 6 个以太网端口
   - 1 个 WAN 端口
   - 1 个 LAN 端口
   - 自定义端口
3) RJ45 串行口。CLI 管理用 (SonicOS 加强版软件)
4) 300+ Mbps 防火墙吞吐量
5) 190 Mbps 3DES 和 AES VPN 吞吐置
6) 硬件 AES 加密/解密

7) 64MB Flash,256 MB RAM
8) 500,000 TCP/IP 并发连接
9) 高达 10,000 条防火墙规则 (SonicOS 加强版软件)

3000 site-to-site VPN 隧道, 包括 1009 个 Global VPN Client (最多 3000 个)

SonicWALL 第四代产品参数表（见下表）

	低端		中端		高端	
	TZ170 Standard	TZ170 Enhanced	PRO2040 Standard	PRO2040 Enhanced	PRO3060 Standard	PRO306 Enhance
防火墙						
防火墙认证	ICSA lab		ICSA lab		ICSA lab	
操作系统	SonicOS		SonicOS		SonicOS	
版本	2.0.0.8	2.0.1.5	2.1.0.0	2.1.0.0	2.0.0.2	2.0.1.
外形	Standalone		1U 机架式		1U 机架式	
CPU	SonicWALL All-in-One CPU		Intel 专用 800MHz ASIC CPU		Intel 专用 2GHz AS CPU	
RAM	64MB		128MB		256MB	
Flash memory	8MB		64MB		64MB	
端口数量	7		4		6	
端口	5xLAN, WAN, WorkPort	5xLAN, WAN, OPT	LAN, WAN, DMZ	LAN, WAN, 2x 没有定义	LAN, WAN, DMZ	LAN, WA 4x 没有定
端口速度	10/100 Mbps		10/100Mbps		10/100Mbps	
用户数	10	25 无限	无限		无限	
吞吐量	90 Mbps		200+ Mbps		300+ Mbps	
最大并发连接数	6,000		32,768		128,000	
包过滤方式	全状态检测		全状态检测		全状态检测	
DoS, DDoS 防范	是		是		是	
Transparent mode	Yes	No	Yes	No	Yes	No
地址转换（NAT）	支持		支持		支持	
端口转换（NPT）	支持		支持		支持	
预设服务	支持		支持		支持	
自定义服务	支持		支持		支持	
最大防火墙策略数	100	250	1,000		5,000	
最大 NAT 策略数	64	128	64	128	64	128
带宽管理	支持		支持		支持	
IPSec VPN						
IPSec 认证	ICSA lab		ICSA lab		ICSA lab	
VPN 功能	包括		包括		包括	
加密方式	DES, 3DES, AES, ArcFour		DES, 3DES, AES, ArcFour		DES, 3DES, AES, ArcFour	
身份认证	MD5, SHA-1		MD5, SHA-1		MD5, SHA-1	
密匙管理	IKE, manual		IKE, manual		IKE, manual	
IKE 模式	Main, Aggressive,		Main, Aggressive,		Main, Aggressive,	

	Quick and Group modes			Quick and Group modes	Quick and Group modes	
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 V	
Site-to-Site VPN 通道数	2	10	10	50	500	1,000
最大 VPN 客户端连接数	5	50	50	100	500	
随产品附送客户端用户数	0	1	1	10	25	
3DES (168-bit) 最大处理速度	30+ Mbps			50Mbps	75Mbps	
AES 最大处理速度	30+ Mbps			50Mbps	75Mbps	
NetBIOS broadcast	支持			支持	支持	
NAT Traversal	支持			支持	支持	
DHCP over VPN	支持			支持	支持	
DH (Diffie Hellman) 组	1, 2, 5			1, 2, 5	1,2,5	
Perfect forward secrecy	支持			支持	支持	
Prevent replay attacks	支持			支持	支持	
Hub and Spoke GroupVPN	支持			支持	支持	
Keep alives	支持			支持	支持	
DPD (Dead Peer Detection)	支持			支持	支持	
用户身份认证	RADIUS, SecureID, SonicWALL 自带的数据库			RADIUS, SecureID, SonicWALL 自带的数据库	RADIUS, SecureID SonicWALL 自带的数据	
PKI/数字证书	支持			支持	支持	

SonicWALL Generation 4 Product Specification Matrix

	LOW-END		MID-RANGE		HIGH-E	
	TZ170 Standard	TZ170 Enhanced	PRO2040 Standard	PRO2040 Enhanced	PRO3060 Standard	PRO306 Enhanc
基于策略的管理						
Zone Objects	No	20	No	20	No	20
Address Objects	No	100	No	256	No	256
Address Object Groups	No	20	No	64	No	64
Address Object Group Depth	No	TBA	No	TBA	No	10
User Objects	No	150	No	256	No	500
User Object Groups	No	32	No	64	No	64
Service Objects	No	100	No	100	No	100
Service Object Groups	No	20	No	20	No	100
Service Object Group Depth	No	TBA	No	TBA	No	20
Schedule Objects	No	50	No	50	No	50
Schedule Object Group	No	10	No	10	No	10
网络支持						
VPN client pass through	支持		支持		支持	
PPPoE support	支持		支持		支持	
DHCP client support	支持		支持		支持	
DHCP server support	支持		支持		支持	
DHCH Server Scopes	1	64	1	50	1	255
DHCP Server Leases	1,024	1,024	2,048	2,048	255	4,096
L2TP client support	支持		支持		支持	
L2TP server support	支持		No		No	
PPTP client support	No		支持		支持	

静态路由	128	192	256
管理			
管理方法	HTTP, HTTPS	HTTP, HTTPS	HTTP, HTTPS
远程管理	HTTPS, VPN	HTTPS, VPN	HTTPS, VPN
全球管理	SonicWALL GMS	SonicWALL GMS	SonicWALL GMS
SNMP 管理	支持	支持	支持
串口管理	支持	支持	支持
软件升级方式	浏览器	浏览器	浏览器
Built-in database users	500	500	500
诊断工具	Ping, trace, nslookup, traceroute, TSR	Ping, trace, nslookup, traceroute, TSR	Ping, trace, nslooku traceroute, TSR
日志和警报	Syslog, email	Syslog, email	Syslog, email
SonicWALL 日志报表	支持	支持	支持
Viewpoint 报表	可选	可选	可选
内容过滤			
内容过滤 CFS 2.0	可选(over 4.2 million bad sites)	可选 (over 4.2 million bad sites)	可选 (over 4.2 millio bad sites)
内容过滤 CFS Premium	可选(over 15 million bad sites)	可选(over 15 million bad sites)	可选 (over 15 millio bad sites)
N2H2 支持	是	是	是
Websense 支持	是	是	是
自定义过滤	支持	支持	支持
关键字过滤	支持	支持	支持
Malicious code filtering	Java, ActiveX, proxy, cookies, digital certificates	Java, ActiveX, proxy, cookies, digital certificates	Java, ActiveX, proxy cookies, digital certificates
安全服务			
强制防病毒管理	可选	可选	可选
病毒报告	支持	支持	支持
Email 附件过滤	EXE, VBS, custom	EXE, VBS, custom	EXE, VBS, custom

SonicWALL Generation 4 Product Specification Matrix

	LOW-END		MID-RANGE		H	
	TZ 170 Standard	TZ170 Enhanced	PRO2040 Standard	PRO2040 Enhanced	PRO3060 Standard	PRO Enh
支持双 WAN 口和双机热备						
WAN 备份	No	支持	No	支持	No	支
WAN 负载均衡	No	支持	No	支持	No	支
WAN 负载均衡的方式	No	Round robin, Spillover and Bandwidth percentage	No	Round robin, Spillover and Bandwidth percentage	No	Roun Spillo Ban perc
双机热备	No		No	支持	No	支
双机热备方式	No		No	Active-Standby / Mirroring	No	Active / Mi
保护互联网的攻击						
DoS Attack						
Christmas Tree Scan attack	支持		支持		支持	
Fragmented Packet attack	支持		支持		支持	
Land attack	支持		支持		支持	
NetBus attack	支持		支持		支持	
Ping of Death attack	支持		支持		支持	
Striker attack	支持		支持		支持	
SYN Flood attack	支持		支持		支持	
DDoS Attack						
Smurf Amplification attack	支持		支持		支持	
Trojan Horse Attack						
Back Orifice attack	支持		支持		支持	

INI Killer attack	支持	支持	支持
Net Spy attack	支持	支持	支持
Priority attack	支持	支持	支持
Ripper attack	支持	支持	支持
Senna Spy attack	支持	支持	支持
Sub Seven attack	支持	支持	支持
Other Attack			
IP Spoofing attack	支持	支持	支持
Possible Port Scan attack	支持	支持	支持
TCP FIN Scan attack	支持	支持	支持

第三章 SonicWALL 防火墙的功能

3.1 全状态检测防火墙

SonicWALL 使用目前最先进的第三代防火墙技术——“Stateful packet inspection”全状态检测技术，不但能够根据数据包的源地址、目标地址、协议类型、源端口、目标端口以及网络接口等数据包进行控制，而且能够记录通过防火墙的连接状态，直接对分组里的数据进行处理；具有完备的状态检测表追踪连接会话状态，并且结合前后分组里的关系进行综合判断决定是否允许该数据包通过，通过连接状态进行更迅速更安全的过滤。有效阻止 DoS、DDoS 等各种攻击。有效的保护您的局域网和公用服务器免受来自 Internet 上的黑客和入侵者的攻击、破坏。SonicWALL 防火墙能够根据数据包报头进行以下控制：

- ✧ 源和目的地址
- ✧ 源和目的接口
- ✧ “欺诈”的IP地址
- ✧ IP协议号
- ✧ TCP和UDP端口号
- ✧ 端口范围
- ✧ ICMP信息类型
- ✧ IP和TCP中都有的选项类型
- ✧ IP 和 TCP 标记组合

3.2 强大的防御功能

SonicWALL防火墙提供对黑客攻击强大的防御功能：

- ✧ 防止黑客对网络的TCP/UDP端口扫描
- ✧ 防止Ping Of Death、Syn-Flood、Teardrop等多种DOS/DDOS的攻击
- ✧ 可防御源路由攻击、IP 碎片包攻击、假冒 IP 攻击

3.3 SonicWALL 防火墙的售后服务

SonicWALL 防火墙的硬件保修是一年，软件升级是 90 天。SonicWALL 防火墙定时会自动到 SonicWALL 网站检查有无最新的软件；同时当有新的软件发布时，SonicWALL 将自动发送电子邮件给系统管理员，系统管理员看到邮件后到 Sonicwall 公司的网站（https://www.mysonicwall.com）上下载最新的防火墙软件。由于黑客的攻击方式不断推陈出新，现有的防火墙软件如果不及时升级，就很难防范新的攻击方式，所以 SonicWALL 防火墙软件的升级最大程度的保护了用户的投资和保障能防御最新的黑客技术。

3.4 SonicWALL 防火墙的操作系统

SonicWALL 防火墙的操作系统是自己开发的操作系统，不基于任何操作系统，避免操作系统的漏洞导致防火墙安全性能实效。当今的客户越来越多注重产品的性能

价格比这一参数，不再去为用不着的功能和部件去花费高昂的购买费用，甚至维护费用。SonicWall 防火墙正是针对这种理性的消费理念而对产品进行定位的，SonicWall 以网络安全领域专家角度为客户设计和生产客户实用、可用、好用的网络安全产品。故 SonicWALL 是目前唯一同一产品支持两套操作系统,根据客户的网络环境和需求选择不同的操作系统。

3.5支持动态IP（DHCP Client）

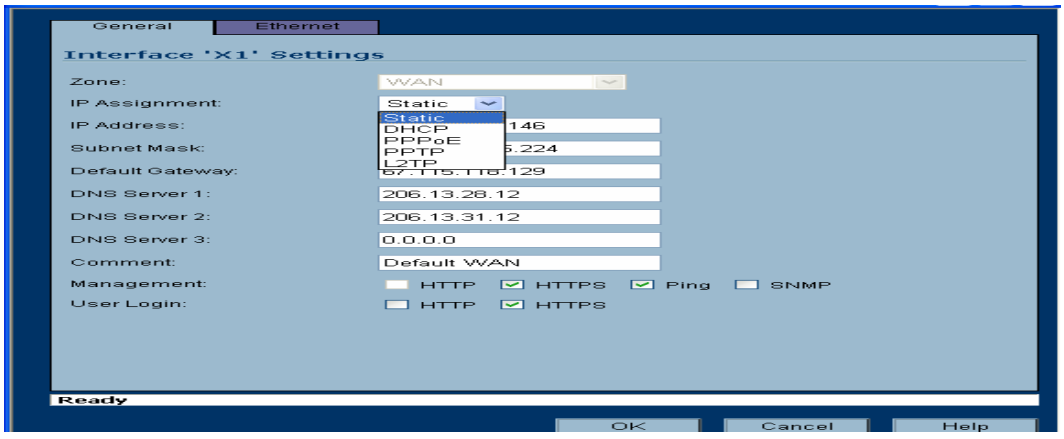
用户如果通过城域网、小区宽带或Cable Modem 等方式接入Internet时，其IP地址为动态分配的。这时候安装防火墙的时候，需要防火墙支持动态IP才能对数据包进行访问控制。SonicWALL防火墙支持动态IP，其接口可以动态的获得IP地址，方便灵活的接入用户的网络环境。

3.6 支持ADSL 接入

目前国内越来越多的企业通过ADSL接入Internet，而ADSL需要拨号以后才能获得IP地址。这时如果要安装防火墙需要防火墙必须支持PPPoE协议，否则无法完成拨号过程，无法接入网络。SonicWALL防火墙支持PPPoE协议，通过在防火墙上输入用户名和口令后便可以ADSL接入，可以通过ADSL获得动态IP地址进行地址转换、VPN等操作。同时SonicWALL还支持带有固定IP的ADSL的线路。

3.7 支持 DDN、PPTP 或 L2TP 等多种上网方式

SonicWALL 防火墙除了支持动态IP和ADSL上网外，还支持DDN专线、PPTP或L2TP，甚至ISDN拨号、电话线拨号。根据不同上网接入方式，可采用不同网络地址的模式。



3.8 NAT(Network Address Translation)地址转换

NAT英文全称是，称是网络地址转换，它是一个IETF标准，允许一个机构以一个地址出现在Internet上。NAT将每个局域网节点的地址转换成一个IP地址，反之亦然。它也可以应用到防火墙技术里，把个别IP地址隐藏起来不被外界发现，使外界无法直接访问内部网络设备，同时，它还帮助网络可以超越地址的限制，合理地安排网络中

的公有Internet 地址和私有IP地址的使用。

SonicWALL防火墙支持常见的NAT功能（多对一）外，还可以提供更多的NAT策略控制权。如：一对一的NAT、多对多NAT、一对多NAT，地址端口转换（PAT），及选择特定的源/目的地址进行NAT转换，使各种管理及支持变得更加便捷。对互联网来说，访问全部是来自于防火墙转换后的地址，并不认为是来自内部网的某个地址，能够有效的隐藏内部网络的拓扑结构等信息。同时内部网用户共享使用这些转换地址，自身使用保留IP 地址就可以正常访问公众网，有效的解决了全局IP 地址不足的问题。

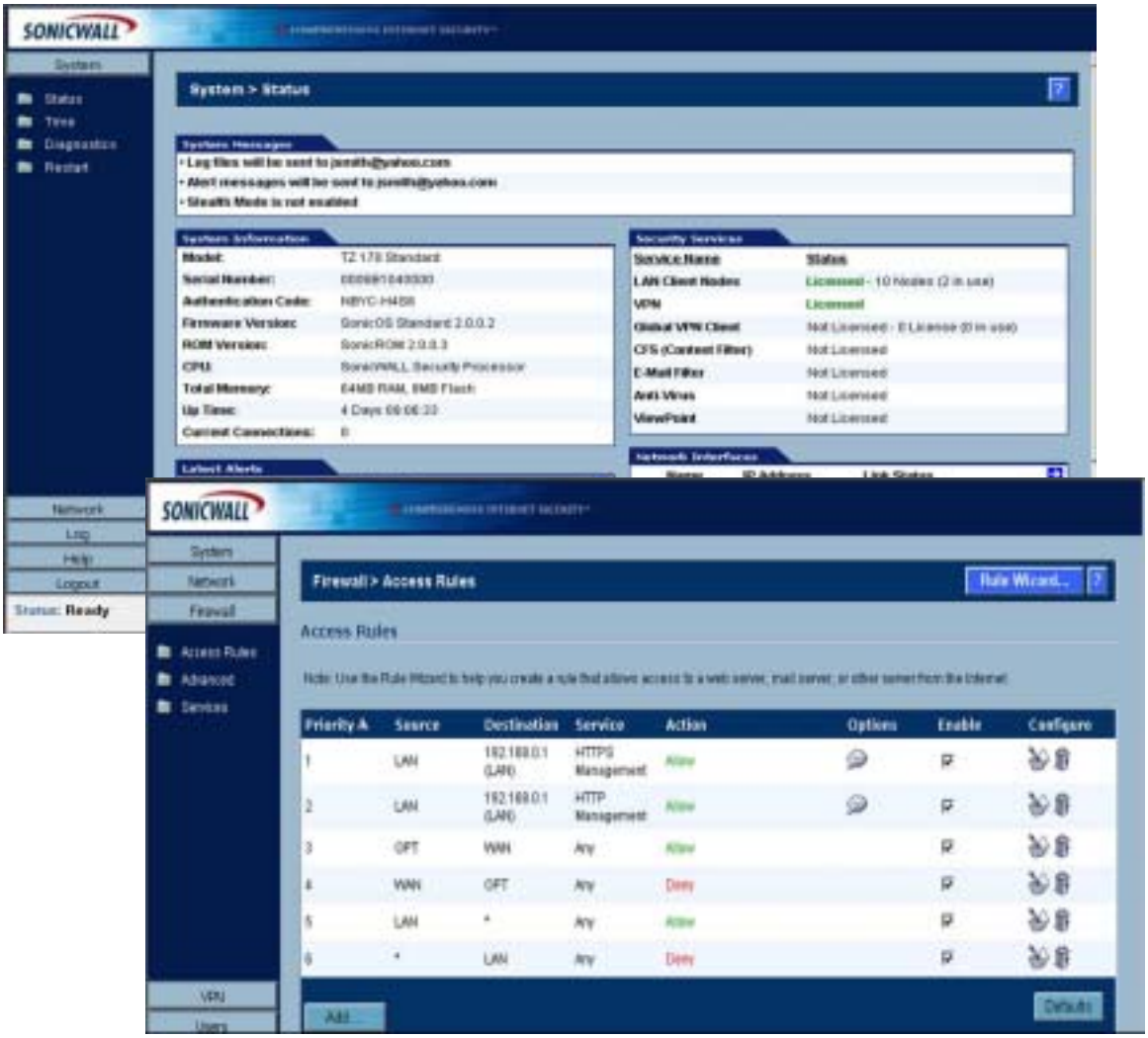
3.9 反向地址映射

目前国内越来越多的企业通过ADSL或Cable Modem接入Internet，是可以获得动态的真IP地址，在以前这种线路想提供Web 、FTP 服务等是不可能的，但现在结合防火墙的端口映射和动态域名（DDNS）就可以提供Web 、FTP 服务。SonicWALL 防火墙的反向地址转换来对目的地址进行转换。同样既可以解决全局IP 地址不足的问题，又能有效的隐藏内部服务器信息，对服务器进行保护。SonicWALL 防火墙提供端口映射和IP 映射两种反向地址转换方式，方便用户的部署。

3.10 面向对象可视化的规则编辑和管理工具

从本质上讲，防火墙仅仅是实现网络安全的工具，是否能起到对网络的保护作用，以及起到多大的作用在很大程度上取决于管理员是否能够正确地使用。传统的防火墙规则是通过命令行来设置的，如 Cisco 防火墙；另外其它防火墙的设置过于晦涩难懂，非专业人员很难配置，如 CheckPoint。特别是当规则数目稍多时，规则的含义和结果，以及其正确性的判断将变得十分困难。从而经常使防火墙成为网络故障的发源地，更严重的是一些故障隐患长期存在，难以发觉，而对入侵者大开方便之门。

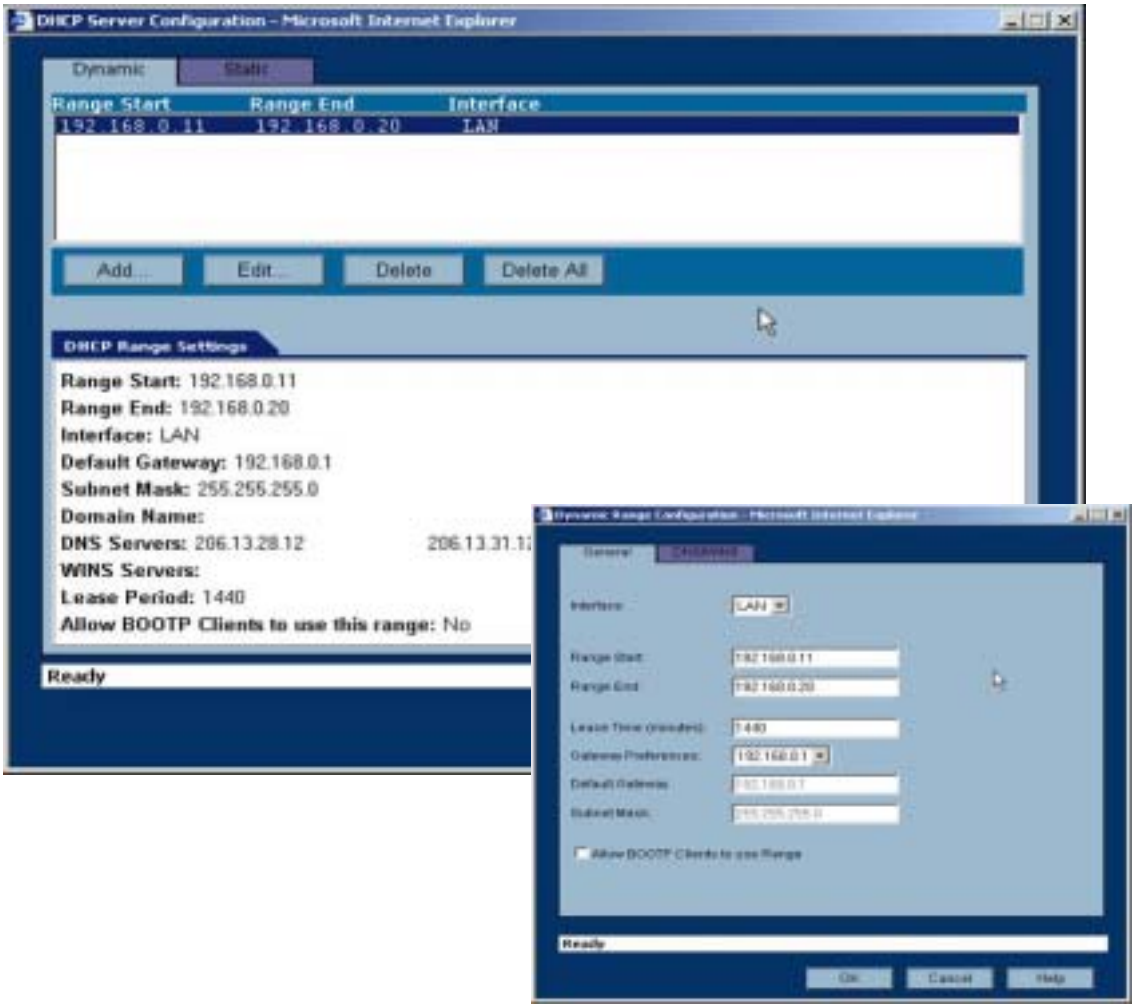
SonicWALL 防火墙对这种配置方式做了彻底的摈弃，提出了全新的可视化的管理和配置概念。SonicWALL 的管理工具提供了友好的 GUI 界面，可以在网络的逻辑图上的对象进行访问控制的配置。用户可以直接指定所期望的控制结果，而控制结果在图上一目了然，不需要根据规则进行控制结果的推断。添加安全规则时，SonicWALL 防火墙会根据自身的规则排序，也可自定义规则的顺序。



3.11 支持 DHCP 服务器

SonicWALL 既可作为 DHCP 服务器，也可作为 DHCP 用户端。当 SonicWALL 作为 DHCP 服务器时，它可以集中管理网络中的计算机的 TCP/IP 的设定，包括 IP 地址、DNS 地址和网关地址。

SonicWALL防火墙同样可以作为DHCP Server ， 防火墙可以为网络中计算机动态的分配IP地址，从而为企业的网络建设节约投资，同时方便网络的应用和IP地址的管理。



3.12 支持各种应用服务协议

互联网的应用是通过端口和协议（ICMP、TCP、UDP）起作用的。SonicWALL 支持各种应用服务协议，缺省服务协议包括HTTP、FTP、SMTP、POP3、DNS、PING和IKE等。如果还需要其它服务协议，可以增加已定义好的服务协议，包括NNTP、IRC、Telnet、Lotus Notes、PPTP、IPSec、 H232、 T120、Quicktime、Filemaker、RealAudio、HTTPS、Authentication、Gopher、IMAP3、Napstar、NetBios、 PC Anywhere、Syslog、Timbuktu、LPR等；或自定义服务协议。

3.13 提供带宽管理服务

在信息高速发展的今天，网络不仅仅只需要带宽，而且必须考虑网络流量高峰时

期重要数据优先传输。当信息拥塞造成瓶颈时，网络管理员必须有优先权数据队列机制，保证那些重要应用的数据比次重要应用数据获得更高的优先传输权。SonicWALL防火墙具有带宽管理功能，使网络可以支持重要任务或实时数据流
与较低优先级别的数据优先传输。SonicWALL防火墙通过定义防火墙安全规则的方式提供带宽管理，同时也可以对VPN进行带宽管理。从而保证重要数据的服务质量。总体来说，具有以下的特点：

- 带宽限制

可以通过防火墙的安全规则进行带宽限制，例如：限制某个用户对外访问最大带宽，或者访问某种服务的最大带宽。

- 带宽保证

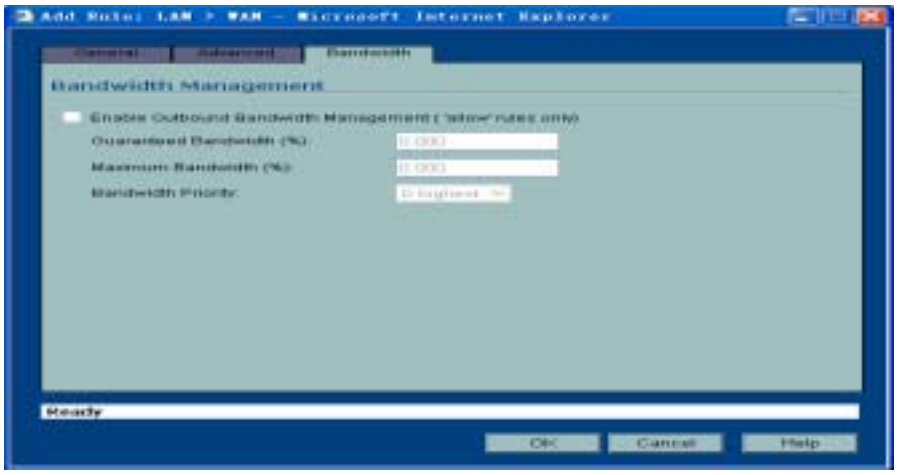
保证网络中重要服务或者重要用户的带宽不被其他服务或者用户占用，从而保证了重要数据优先通过网络。

- 优先级控制

SonicWALL 优先级控制分8个优先级（0-7），保障某用户的带宽或访问某种服务的最大带宽。

- 动态流量均衡

为了保证网络中的所有带宽都得到合理的应用，防火墙提供动态流量均衡功能。例如：假如某网络带宽为512k，设定主机A的最小带宽为128k，最大带宽为256k；主机B最小带宽为192k，最大带宽为256k，主机C最小带宽为128k，最大带宽为256k，先保证所有最小带宽，然后再根据优先级分配剩余的带宽，从而保证重要服务或者用户优先进行数据传。



3.14 虚拟专用网(VPN)

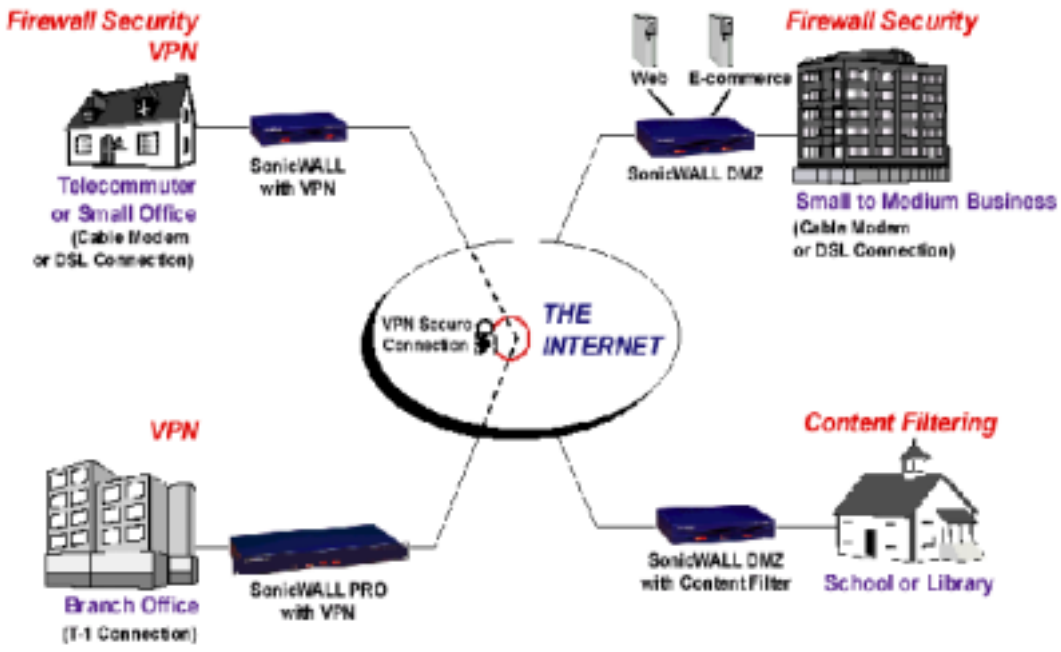
VPN（Virtual Private Networking 虚拟专用网）就是在公共网络基础上

（Internet）利用安全、认证、加密等技术建立企业的专用线路，也就是一个安全的网络隧道（TUNNEL）,在降低联网费用的同时确保信息的安全性、完整性和真实性。VPN 虚拟专网，是一个通过利用公用基础网络为企业各部门提供安全的互联网服务，它可以提供与昂贵的专线（DDN）类似的安全性，可靠性，可管理性和优先级别，可构筑于 IP 网络，帧中继网络和 ATM 网络上。

通过 VPN 功能， SonicWALL VPN 安全地将公司的各个办公地点、移动和远程办公者、商业伙伴连接在一起。 SonicWALL VPN 使用数据加密，使两个或更多的点或 LAN 之间通过 Internet 实现安全通信，而无需昂贵的专线。可通过 IP 地址或动态域名（DDNS）建立 VPN。

Sonicwall VPN采用**IPSec**协议标准，可与其他执行IPSec标准的VPN产品共同使用，如 AXENT RAPTOR、Check point的Firewall-1、CISCO PIX等。加密方法有56 位的DES、168位的3DES、56位的ARC4和最新的AES。

SonicWALL使用专属高效能 ASIC 加解密芯片有效地减轻CPU加解密负担，使VPN处理效能又达另一高峰,PRO 3060/4060的3DES 及 AES VPN 传输效率高达75M/190 Mbps。

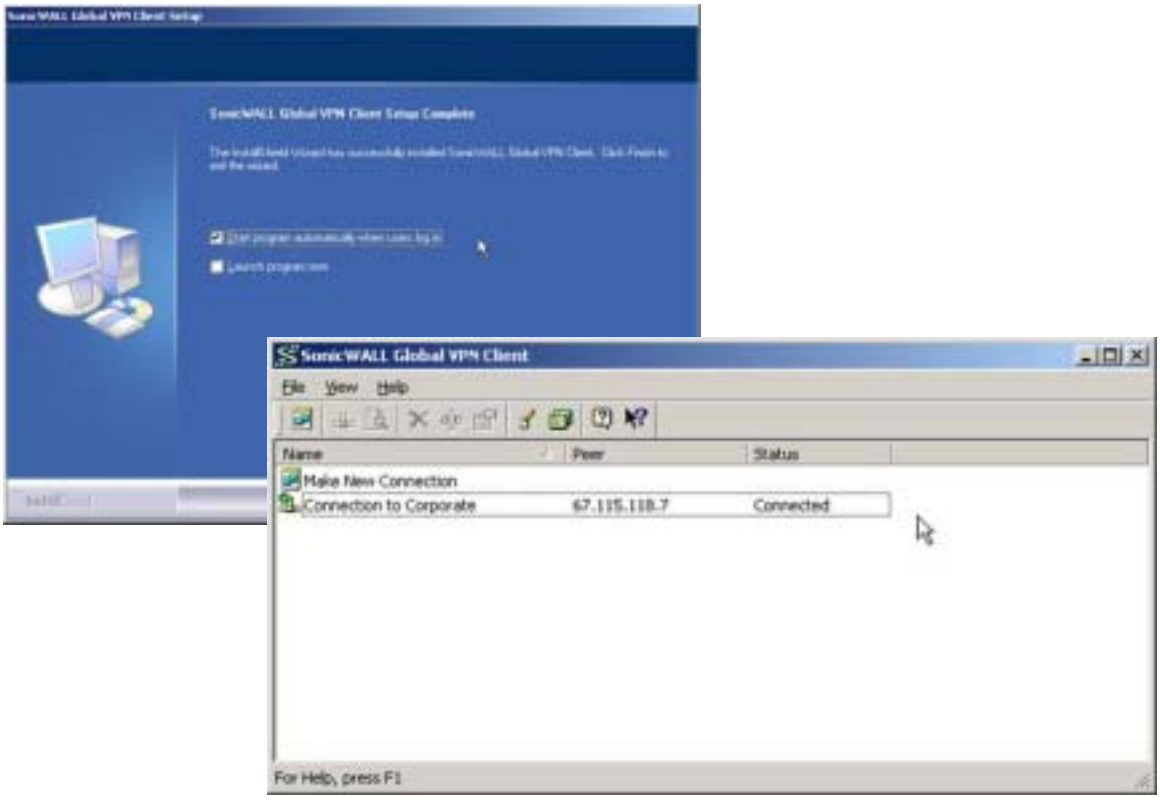


3.15 VPN 客户端（软件）

VPN 客户端视为用户创建全面的远程、移动用户接入解决方案。SonicWALL的Global VPN Client软件能够帮助移动工作者提高效率，使他们在任何地点、任何IP网

络环境中，都可以通过宽带、无线或是拨号上网的方式灵活、安全地接入到公司网络。移动用户只需键入一个主机名或IP地址，VPN的配置信息就会自动地从SonicWALL VPN 网关上下载并进行连接。此外，与目前一些不易安装和管理的VPN客户解决方案相比，Global VPN Client的自动策略提供功能还可以为终端用户提供更清晰的安装过程，从而减轻网管员的负担。

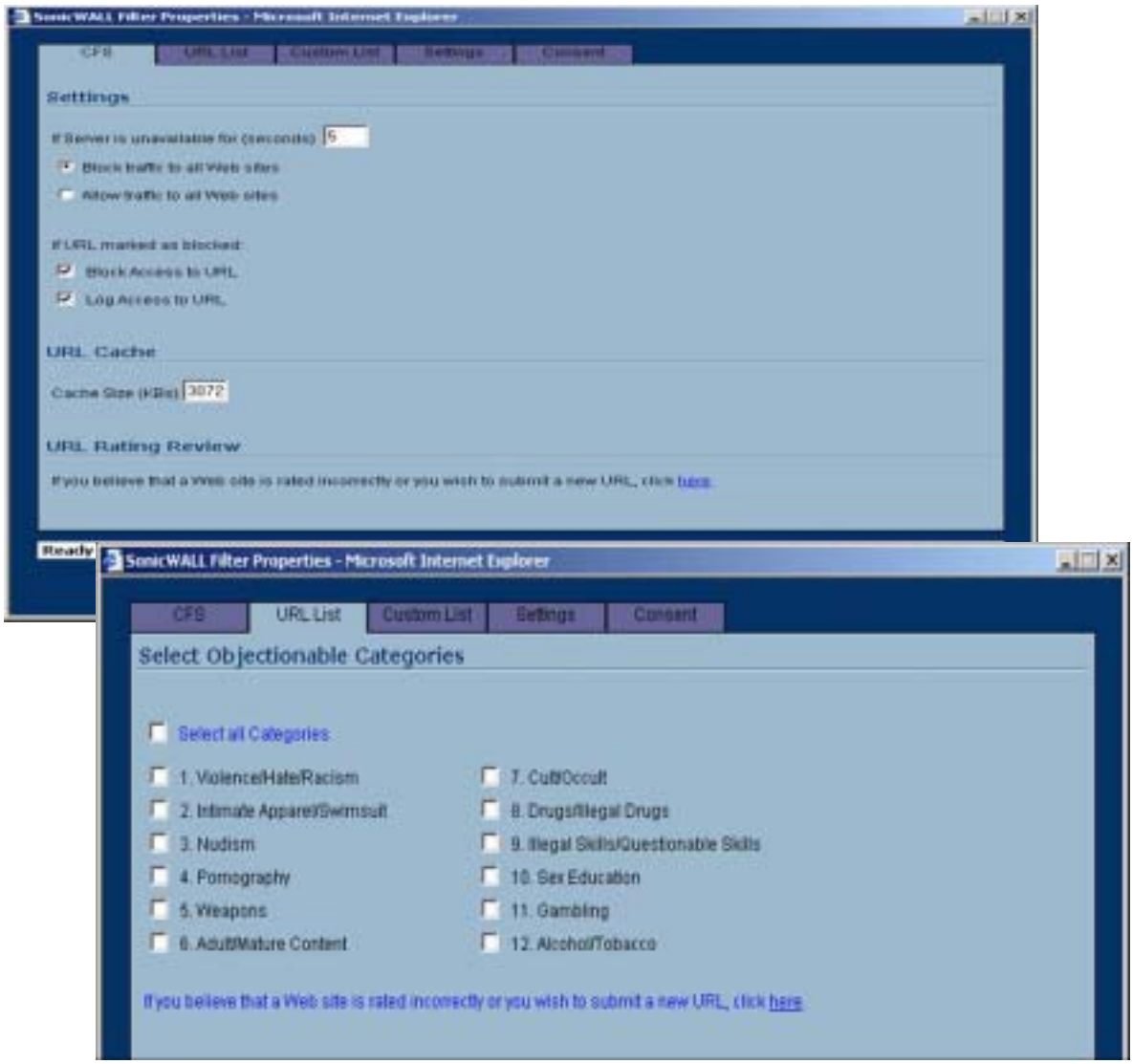
自动策略提供功能是SonicWALL的独创技术，IT管理员能够用它维护并更新群组的安全策略，以响应业务变化的需求，而无需对每一个终端用户的安全策略逐一进行手动调节。当用户尝试进入VPN 时，SonicWALL的网关会自动识别每一个用户，然后为他分配一个加密的安全策略。通过认证的用户能够使用最新的安全策略及时、安全地接入VPN，而未被认证的用户则会被阻挡在网络之外，SonicWALL这一独创的系统大大地减轻了管理员的工作量，减少了用户的配置错误，使SonicWALL解决方案成为有效创建群组VPN的首选方案。



3.16 内容过滤（选项）

随着连接在互联网上企业机构的不断增加，不适当Web内容也接踵而来。由于不良Web内容造成的威胁有越来越严重的趋势，企业对于功能更强大的Web内容过滤工具的需求也越来越迫切。为使企业Web应用集中于与业务相关的活动，各企业机构不

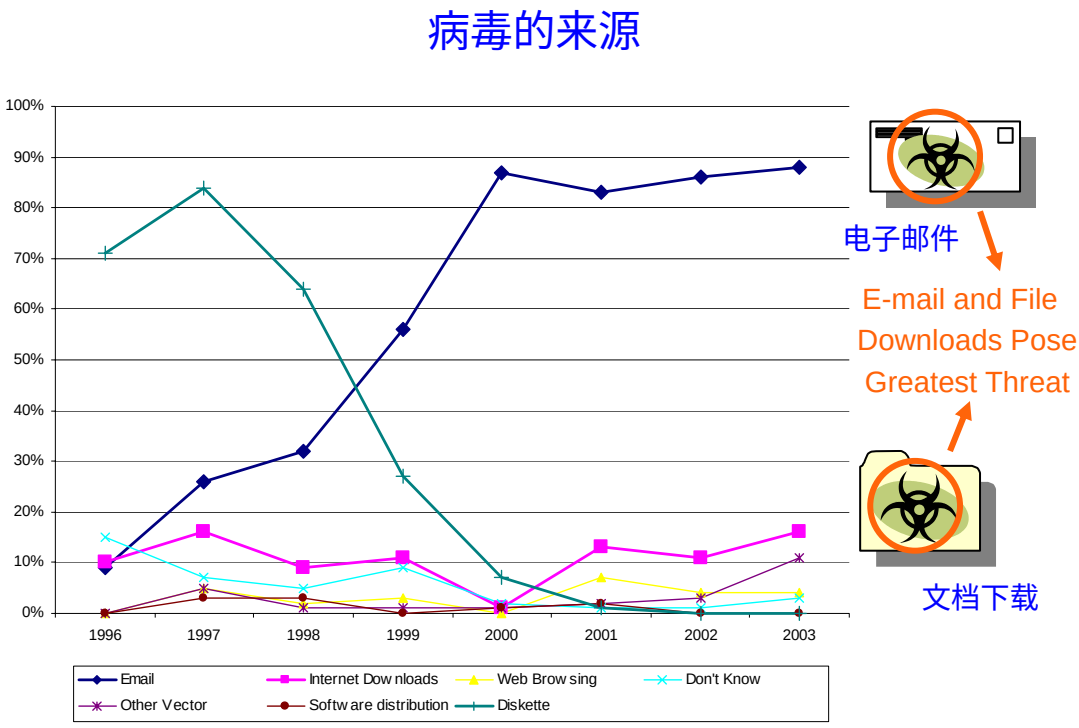
仅需要保护公司资产和保持高业务生产率，还必须提高网络性能，并减少因浏览不良内容而暴露企业保密内容的机会。SonicWALL 自带的自定义过滤功能是可以直接使用，包含禁止访问域、允许访问域和关键字。SonicWALL 防火墙把内容过滤作为可选项购买。SonicWALL内容过滤允许管理员设置访问类别和内容控制，限制访问带有色情、种族偏见、赌博等网站。也可给特定用户一个密码来绕过过滤器，给他们不受限制地访问Internet。另外SonicWALL 还可以Websense 和N2H2的内容过滤（Websense或N2H2需要单独购买）。



3.17 网关防病毒（选项）

随着 Internet 的飞速发展，我们的工作和日常生活越来越以来于网络。随着网络的发展，病毒的传播也具备了越来越依赖于网络传播的特点。据国际计算机安全委员会（ICSA）统计，企业用户感染的病毒中，有超过 20%的病毒与从 Internet 上下载文

件有关。此外还有 87%的病毒是通过电子邮件附件进入企业网络的。Internet 大大加快了病毒在世界范围内的传播速度并使很多公司陷于瘫痪。因此，在企业的网关设置防病毒系统，防止通过 Internet 传播的病毒进入企业网内部并对企业网络造成危害就成了刻不容缓的工作了。如下图：



Source: ICSA Labs Virus Prevalence Survey 2003

防火墙集成防病毒功能，即网关防病毒，与平常常见的基于主机的传统防病毒有很大的不同。传统的防病毒软件通常是在类似 fopen()这样的文件操作函数中形成一个文件流时，使用预设地病毒特征数值与流中的值进行匹配，从而确认该文件是否含有已知的病毒特征。而在网关环境中，根本就不存在一个“ 文件 ”的概念，有的只是分属于不知那里来的那个文件的成千上万的 IP 包，因此，网关防病毒需要完全不同的防病毒引擎。

网关防病毒同样是基于特征字符串匹配。固然可以直接在防火墙过滤内核中匹配每个 IP 包的内容是否包含指定的 ASII 字符串，但这样很不可靠，因为许多文件在以太网传输过程中是分成许多 IP 包的，如果特征码刚好在分割界限上，这种字符串匹配就无能为力，因此，就要求防火墙使用 IP 碎片重组技术，即必须由防火墙内核辟出一个新的缓冲区重组 IP 包，然后再继续转发。另外，全面匹配每个 IP 包的每一段

内容，对防火墙的通量性能危害极大，性能的损害可以达千倍以上。正是由于这个原因，使用这种方式进行防火墙的防病毒对性能的损害的极大的，防火墙变慢不足为奇。也正是由于这个原因，使用这种方法是不可能达到传统的杀毒作用，在防火墙上，只能是查毒，一旦发现，就把该 IP 或该会话丢弃，显然，这时涉及的文件也不会有用，因此，防火墙的操作就是把文件丢弃，也即一般用户在防火墙上看到的病毒文件的“被丢弃”。

为了解决以上这些情况,SonicWALL 公司为 TZ170 系列和 PRO 系列安全设备开发了可伸缩的高速的网关防病毒和入侵防护方案. SonicWALL 的网关防病毒和入侵防护对病毒, 蠕虫,木马和应用漏洞采取智能的实时的安全防护.采用灵活的高性能的深度包检测架构, SonicWALL 的网关防病毒和入侵防护服务无论在网络核心还是在网络边缘都能对各种各样的动态威胁有效阻断,诸如病毒,蠕虫,木马,软件漏洞如缓冲区溢出,同时还能防范对等应用和及时消息应用,后门程序以及其他恶意代码.

这项独特的解决方案采用高性能的深度包检测引擎直接在安全网关上匹配全面的签名库,对网页下载,邮件传输及压缩文件的潜在威胁进行安全防护. 因为威胁层出不穷不可预测,签名库必须不断更新以尽最大可能对不断出现的威胁采取最有效的防护. 新的签名来自 SonicWALL 的 SonicAlert 工作组和第三方资源. SonicWALL 的网关防病毒和入侵防护不仅防护来自外部的威胁,还对来自内部的威胁采取防护措施.

主要功能和优点.

- 实时的网关病毒扫描. SonicWALL 的网关防病毒和入侵防护通过时时地扫描非压缩及压缩文件,对文件病毒和恶意代码采取防范,隔离病毒,蠕虫,木马及其它 Internet 威胁.
- 强大的入侵防护. SonicWALL 的网关防病毒和入侵防护通过扫描数据包的内容对诸多基于网络的应用层威胁采取防护措施,诸如防范蠕虫,木马和应用漏洞 (如缓冲区溢出), 同时还能防范对等应用和及时消息应用,后门程序以及其他恶意代码.
- 集成深度包检测引擎. SonicWALL 的网关防病毒和入侵防护采用高性能的深度包检测引擎,利用并行搜索算法,检测到应用层,提供传统的全状态检测防火墙所不能达到的功能,对应用层,Web,邮件攻击采取防护措施.并行搜索算法极大降低了由此带来的对防火墙性能的影响.

- 无比的伸缩性和高性能. SonicWALL 的网关防病毒和入侵防护是业界第一个采用逐个包扫描引擎的解决方案,它的独特之处在于它对传输的文件大小和同时下载的文件的数目没有限制,实现无比的灵活性和高性能.
- 安全域之间数据扫描. SonicWALL 的网关防病毒和入侵防护提供另外一层的安全防护,即不仅在各个内部安全域与 Internet 之间安全扫描,在各个内部安全域之间也进行安全扫描.
- 全面的签名库. SonicWALL 的网关防病毒和入侵防护采用一个非常全面的签名库,包含成千上万个签名(IPS:1900+,GAV:24000+),来检测并防护病毒,蠕虫,应用漏洞以及及时消息和对等应用的使用.
- 应用控制. SonicWALL 的网关防病毒和入侵防护可以监视并管理及时消息和对等应用文件共享程序的使用,关闭潜在的后门,确保网络的安全.节省网络带宽的同时提高工作效率.

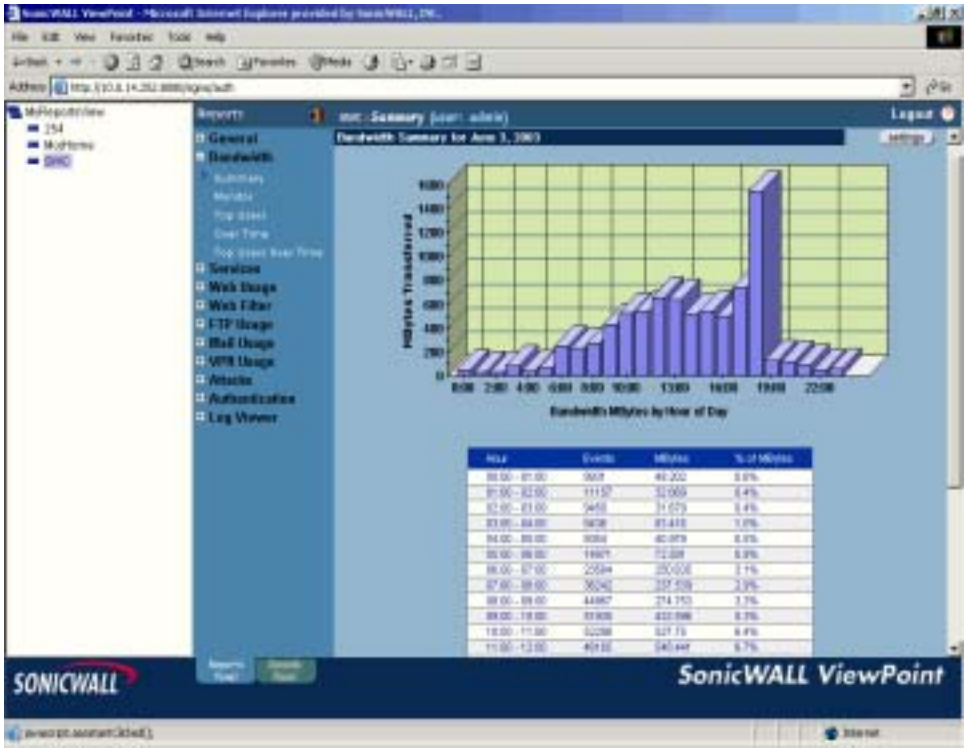
简化部署和管理. SonicWALL 的网关防病毒和入侵防护允许管理员在各个安全域之间创建全局安全策略,按组管理不同优先级别的攻击,简化分布式网络环境的部署和管理.

3.18 监测、报告软件ViewPoint（选项）

对商业机构来说，他们不但要保护网络资源，同时还要确保员工的工作效率，因此网络活动的监测与报告功能极其重要。SonicWALL ViewPoint 2.0报告软件帮助网管员追踪网络活动和事件，甄别可疑的网络流通情况， 并判断员工是否滥用网络资源。ViewPoint 2.0中的风险评估工具可以帮助网管员确保公司网络安全并防止攻击。这种时实时的网络活动报告用于帮助网管员甄别不恰当或无效的网络资源应用。

SonicWALL ViewPoint 2.0具备网络安全的监测能力，并可提供实时及历史的图表报告。这些报告能够总结网络中全部SonicWALL 网络安全产品的活动情况，而且涵盖多种网络活动，包括个人或群体使用某一类型或某一组防火墙产品的情况，以及防火墙遭受攻击的类型与时间等等。这一灵活、随需定制的报告界面能够显示员工经常访问的网站地址、网络使用者、应用软件及带宽分配情况。

另外， SonicWALL公司的ViewPoint 2.0软件可与Web服务器、syslog服务器及数据库集成，进行轻松地配置、使用与维护。其并发连接部分允许多名网管员登录，查看防火墙活动报告以监测本地区的安全响应。



3.19 全球管理系统（SonicWALL Global Management System ）（选项）

众所周知，分布式网络通常包括：公司总部、远程及分支机构、远程工作者和移动工作者。目前，网络环境日趋分布，越来越多的员工需要从远程点接入到公司网络。GMS 2.5 可以完全满足这一需求，它具有管理 SonicWALL 全球 VPN 客户端的功能，可以帮助网管员经济有效地管理远程工作者或移动工作者，让他们随时随地、安全地接入公司网络。

另一方面，随着员工们对移动办公需求的增多，无线网络也呈现出快速增长的趋势。SonicWALL GMS 2.5 与 SOHO TZW 一起帮助网管员在无线局域网中执行严格的接入及加密安全策略，从而带来了一个新的网络架构，这样就可以像在有线网络中一样进行管理和控制。

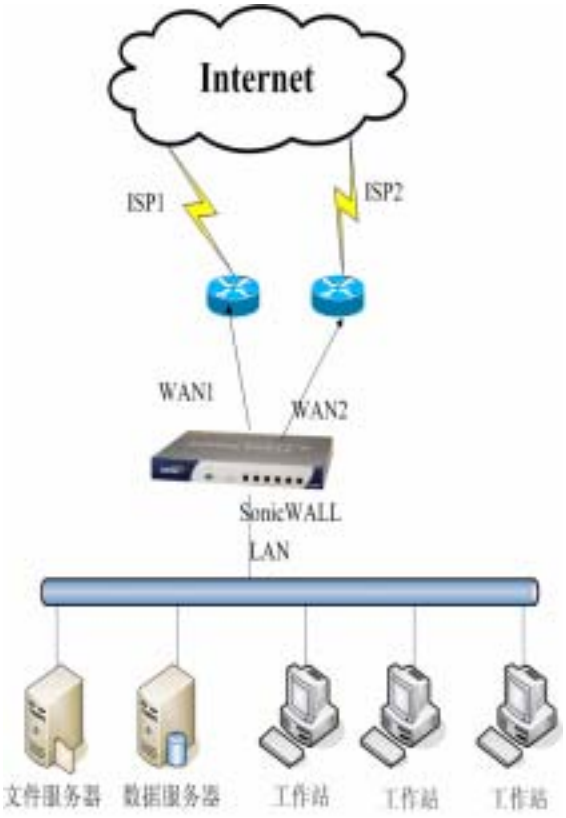
SonicWALL GMS 2.5 版本能够监测并管理上千台 SonicWALL 网络安全产品和客户端，并允许商业机构和服务提供商的网管员配置防火墙和其他 SonicWALL 服务，其中包括虚拟专用网（VPN）、防病毒、无线安全和网页内容过滤。网管员能够通过加密的 VPN 通道从中心为个体、群组或全球范围远程设置安全策略。

3.20 支持双机热备

为了保证网络的高可用性与高可靠性，SonicWALL防火墙提供了双机热备份功能，即在同一个网络节点使用两个配置相同的防火墙。正常情况下主防火墙处于工作状态，另一个处于备份状态，当工作状态的系统出现故障时，备份状态的防火墙自动切换到工作状态，并保证网络的正常使用。要保护网络的安全，防火墙本身首先要安全。即使防火墙没被黑客攻击，也会由于电力，原器件老化，异常死机等特殊原因发生故障，万一故障发生，网络的安全就无法保证。对于需要高度可靠性的用户，一定要选用有双机热备技术的防火墙。SonicWALL防火墙的双机热备功能可以使防火墙备用主机在极短时间完成整个切换过程，切换过程不需要人为操作和除两个防火墙以外的其他系统的参与。SonicWALL 第四代只有 PRO 2040 、PRO 3060和PRO 4060 的增强版才支持双机热备。

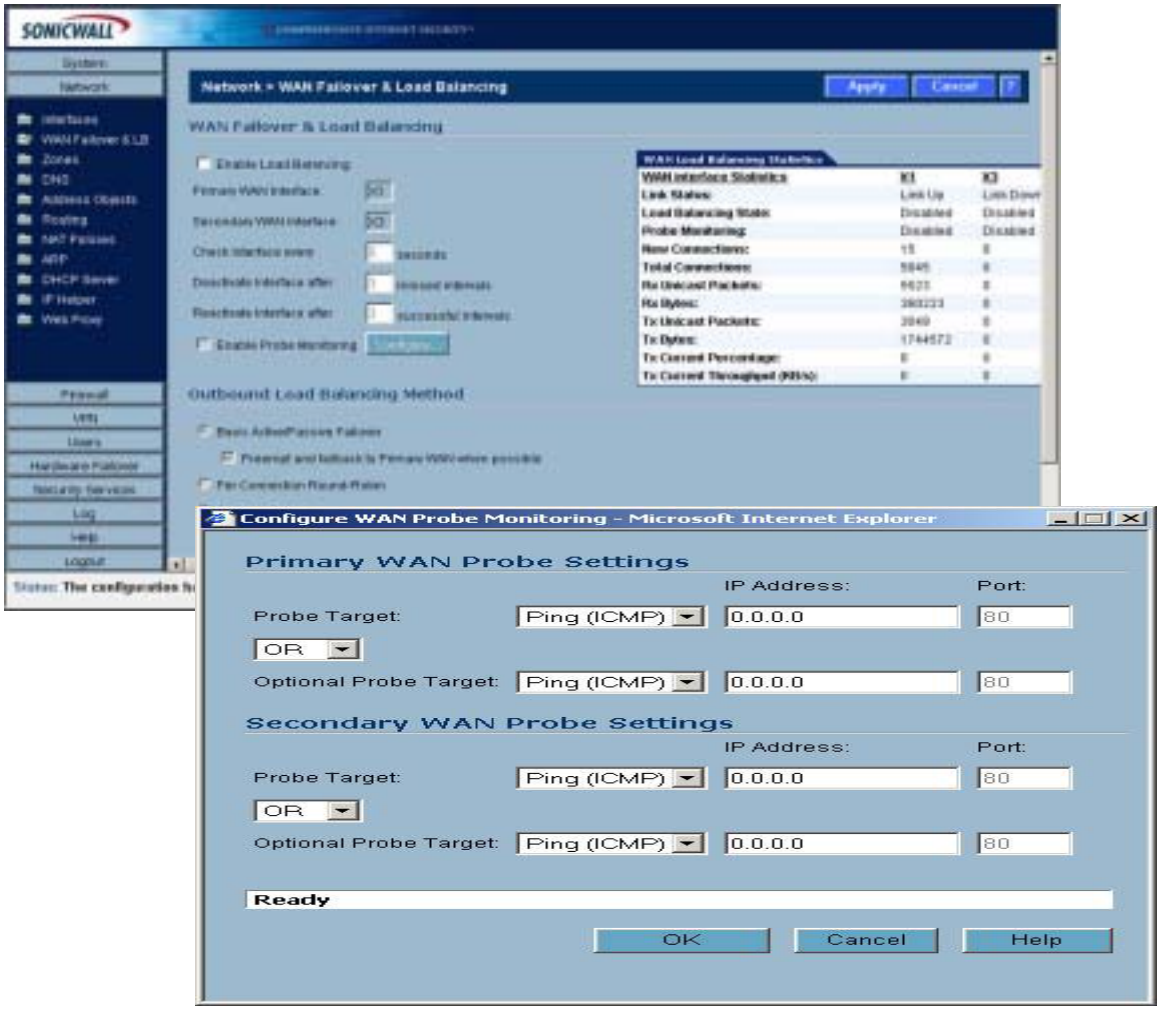
3.21 ISP Failover & Load balancing – 链路备份及负载均衡

随着计算机技术的发展，互联网已经成为最大的公共数据网络，在全球范围内实现并促进了个人通信和商业通信。互联网和企业网络上传输的数据流量每天都以指数级的速度迅速增长。越来越多的通信都通过电子邮件进行；移动员工、远程办公人员和分支机构都利用互联网来从远程连接他们的企业网络；而在互联网上通过 WWW 方式完成的商业贸易现在已经成为企业收入的重要组成部分。随着互联网的应用越来越多，带宽成为互联网应用的瓶颈，很多公司增加连接互联网的带宽，但如果在专线增加带宽，费用昂贵。所以很多用户会增加一条宽频线路。



SonicWALL 第四代产品增强版提供并且可自定义多达两个 WAN 口，支持两条 ISP 互联网接入线路，并提供线路备份及负载均衡，更大的优化网络接入的安全性，经济、有效的保证企业实时在线。ISP Failover 支持“ active-passive ” 线路备份架构；load balancing 支持 “ active-active ”均衡负载架构；

利用 SonicWALL 第四代产品增强版多端口特性，更有效地防止重要的企业资源受到威胁，所有接口都支持防火墙拒绝服务和攻击的防御功能，保证不受内部和外来的的威胁。



3.22 Intrusion Prevention Service (IPS)

SonicWALL Intrusion Prevention Service (IPS)能有效的侦测阻止网络入侵攻击; 如 Nimda、 Code Red…等蠕虫病毒; 软件安全漏洞如 IIS 未更新; 木马及 Spyware 间谍程序。 SonicWALL IPS 可实时扫描 50 种以上通讯协议， 包含 P2P 如 eDonkey、 eMule…等造成网络拥塞与非法软件; 非法 Video 文档共享传送及网上聊天如 MSN、ICQ… 等实时通讯管理， SonicWALL 采用自行研发的 Deep Packet Inspection Engine – 快速深层封包扫瞄引擎， 在不需要费时重组 TCP 封包， 即可顺畅并行一次完成并对入侵或危险网络封包， 从而根据危害级别进行阻挡。 SonicWALL 公司透过安全技术中心主机不断自动更新内建于每部启用 IPS 功能 Firewall 的 Signature Database – 目前这个网络危机数据库支持高达 1700 状态特征码。管理者可设定只要启用侦测或直接阻挡， 经由敏感度微调设定可减少误判情形。 配合 SonicWALL Security Zone 网络区域规划的分区隔离安全政策设定， 防止日益严重的网络蠕虫病毒入侵与扩散□

SonicWALL IPS 支持全系列 SonicWALL TZ170、PRO 2040、 PRO 3060 及 PRO 4060 防火墙，原有用户可经由购买升级服务将 防火墙/ VPN 提升为内建高效能 IDS/IPS 入侵防御网关器。 其价格竞争优势可让用户全面布建 IPS 功能于总部 Firewall 与一般较被忽视的外点各个分支机构对外之 Internet 联机之 VPN 安全网关内， 经由集中控管的 GMS 安全政策控管系统， 防止由外点感染蠕虫病毒或入侵事件再由 VPN 联机而全面扩散的危机。

第四章 防火墙的管理

4.1 基于对象名称过滤

SonicWALL防火墙访问控制规则基于对象名称或者IP地址两种方式进行过滤，标准版软件是通过IP地址方式进行过滤，增强版是通过对象名称方式进行过滤。可以将单个地址、一段网络、IP地址的范围、组设置为一个对象名称。这样配置出的规则具有很强的可读性，非常便于阅读。同一对象名称可以同时在不同规则中使用，提高了配置管理员的效率；名称可以被修改和编辑，只要不删除名称，规则本身可以不必修改，提高了配置的灵活性。当用户的某个地址发生了变化，只需在对象名称定义选项中做出相应的调整不需对规则作任何变化，从而减少了规则的变动，减轻了网管人员的工作量（因为针对与此地址的规则可能有多条）。

4.2 组策略管理

SonicWALL防火墙增强版在配置规则时候可以对多个具有相同属性的名称归为一

个组（例如：IP地址、用户、服务、时间表等），在设置规则的时候可以基于组进行规则设置，通过组的概念可以减少防火墙的规则数量。并且在多台防火墙管理时，通过在全局模式下组策略定义可以将这些定义的组应用到多台防火墙中，简化了管理员的管理工作。

4.3 多层组策略管理

SonicWALL 第四代产品增强版定义对象名称和组的数量都是有限的，其实所有产品都是有限的。SonicWALL 在高端产品如 PRO 3060 & 4060 的增强版是支持多层组，就是把所建立的组再重新组合成新的组。最多支持10层。

4.4 预定义服务

为了方便管理和使用，SonicWALL防火墙预定义100多个常用服务。配置规则时可以针对这些服务进行定义，不需要网管人员具有非常高的网络知识便可以轻松配置。同时还可以自定义服务协议。

4.5 远程管理

SonicWALL 第四代产品都支持远程管理，通过 https 、VPN 客户端和全球管理系统进行远程管理。和其他产品不同，SonicWALL 防火墙的远程管理功能出厂设置是关闭的，有需要时才打开。特别是 https 的远程管理虽然通过 SSL 的加密，还是有可能给黑客猜测用户名和密码的可能性。而且 SonicWALL 的管理可以指定某 IP 地址的计算机来管理。建议客户最好把 https 远程管理功能关闭，有需要才打开。

4.6 集中远程管理

通过SonicWALL全球管理系统（SonicWALL Global Management System ，SGMS）可以集中管理所有属于自己的SonicWALL 防火墙。SonicWALL 全球管理系统可以对无限台SonicWALL 防火墙进行统一的、集中的管理，方便用户在一台管理计算机上对所有SonicWALL 防火墙的远程管理。并且可以定义全局的服务、对象名称，提供对所有防火墙策略修改、上传、下载功能。这样具有共性的设置在全局配置中统一设置，每台防火墙只需定义个性的配置就可以了，从而减少规则数量、简化管理。并且所有的管理都是通过VPN 技术，保证了远程管理的安全性。当然要对需要远程的SonicWALL 防火墙进行配置才能进行管理。而且被远程管理的SonicWALL 防火墙还可以通过本地管理，只要控制用户名和密码就可以控制管理的安全性。而且并需要所有的SonicWALL 防火墙产品都有固定IP地址，如ADSL的用户是没有问题。

4.7 支持SNMP 协议

SonicWALL 防火墙支持 SNMP 协议,可通过通用的网管软件(例如 :Open View、Net View、Vmonitor 等) 对防火墙的运行状况进行监控。为了避免由于 SNMP 本身的安全性上的缺陷而导致防火墙本身的安全性受到威胁，系统仅允许网管系统查询信息，而不允许改变防火墙的配置。同时 SonicWALL 防火墙的 SNMP 是需要配置才起作用，从而保障了防火墙管理的安全性。

第五章 SonicWALL 防火墙性能

作为影响网络性能的瓶颈，防火墙性能是用户在选购时必须重点考察的指标。一般的衡量指标主要包括最大吞吐量、延迟、转送速率、丢包率、缓冲能力以及访问控制规则对防火墙性能的影响。

5.1 吞吐量

吞吐量是指防火墙在不丢包的情况下能够达到的最大包转发速率，通常将它作为衡量防火墙性能的最重要的指标。随着Internet 的日益普及，内部网用户访问 Internet 的需求在不断增加，一些企业也需要对外提供诸如WWW 页面浏览、FTP 文件传输、DNS 域名解析等服务，这些因素会导致网络流量的急剧增加，而防火墙作为内外网之间的唯一数据通道，如果吞吐量太小，就会成为网络瓶颈，给整个网络的传输效率带来负面影响。

5.2 延时

现在网络的应用种类非常复杂，许多应用对延迟非常敏感（例如：音频、视频等），而网络中加入防火墙必然会增加传输延迟，所以较低的延迟对防火墙来说也是不可或缺的。

5.3 并发连接数

并发连接数也是衡量防火墙性能的一个重要指标。最大并发连接数指的是防火墙能够同时处理的点对点连接的最大数目。它反映了防火墙设备对多个连接的访问控制能力和连接状态跟踪能力，以及防火墙对业务信息流的处理能力。这个参数的大小会直接影响到防火墙所能支持的最大信息点数。

5.4 平均无故障时间

平均无故障时间（MTBF）是指系统平均能够正常运行多长时间，才发生一次故障。系统的可靠性越高，平均无故障时间越长。这也是用户在选择产品的重要依据之一。

SonicWALL 第四代产品性能参数表

	TZ 170	PRO 2040	PRO 3060	PRO 4060
最大并发连接数	6,000	32,000	128,000	500,000
吞吐量	90 Mbps	200+ Mbps	300+ Mbps	300+ Mbps
VPN 吞吐量	30+ Mbps	50 Mbps	75 Mbps	195 Mbps
最大防火墙策略数	标准版：100 增强版：250	1,000	5,000	10,000
静态路由数	128	192	256	512
Site to Site 通道数	10 用户：2 25/无限用户：10	50	500	3,000
最大 VPN 客户端连接数	10 用户：5 25/无限用户：50	100	500	3,000

SonicWall 国内成功案例

金融证券：

深圳工商银行、湖南泰阳证券、香港工商银行、国际信托投资有限公司、万联证券

教育系统：

清华大学、天津军事交通学院、西北纺织学院、深圳福田电教中心

交通能源：

辽宁省交通厅高速公路局、广深铁路股份有限公司、华能集团

政府机关：

唐山市政府、辽宁省本溪市工商局

电信系统：

江苏移动、江苏铁通、佛山市惠通信息技术公司、广东省电信实业集团、中山数据通信局、东莞市路路通数码科技公司

电力系统：

广西容县电力公司、河南省电力公司、安徽电力二厂

企业：

盐田国际、日本川崎汽船、美能达上海公司、林德叉车 、金龙客车、上好佳（中国）有限公司、上海汽车工业集团销售总公司、马鞍山钢铁集团、大连小野田水泥厂、上海爱恩国际集团、大连友兰集团、大连金信集团、亿腾房地产、韩伟集团、万恒地产