海信 FW3010PF 防火墙

技术白皮书

Hisense Packer Filter Firewall FW3010PF

北京海信数码科技有限公司

Beijing Hisense Digi-Tech Co., Ltd

注意

白皮书中的内容是海信防火墙 FW3010PF 系统的技术说明书。本材料的相关版权归北京海信数码科技有限公司所有。白皮书中的任何部分未经本公司许可，不得转印、影印或复印。

海信防火墙 FW3010PF
技术白皮书

本资料将定期更新，如欲获取最新相关信息，请访问北京海信数码网站，www.hisencyber.com，您的意见和建议请发送至：

电子信箱：marketing@hisencyber.com

北京海信数码科技有限公司

Beijing Hisense Digi-Tech Co., Ltd

北京市海淀区上地信息产业园信息路 11 号彩虹大厦 3 楼，100085

IRICO Building 3, No 11, Shangdi Xinxi Road, Hai dian District,

Beijing,China

电话(TEL)：010-62963695/96/97/98/99

传真（FAX）：010-62963700

htttp://www.hisencyber.com.

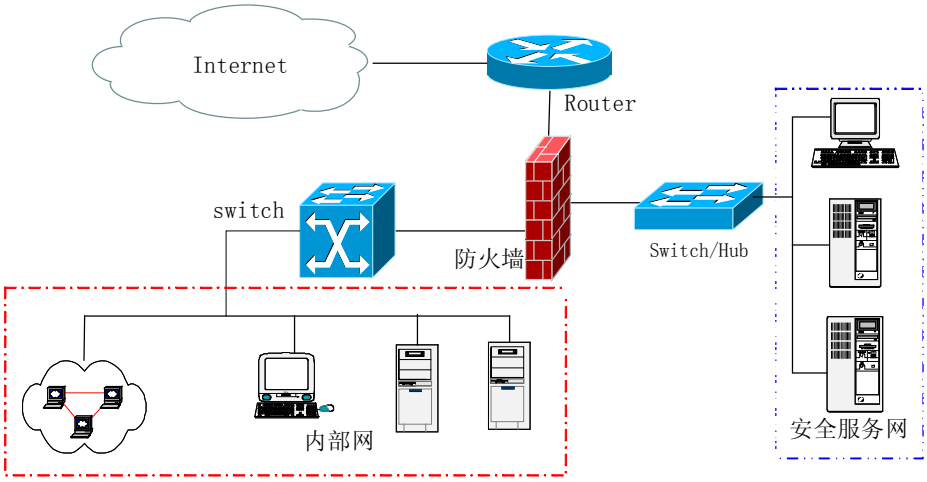
前　言

北京海信数码科技有限公司是海信集团在北京中关村注册的一家专业网络安全公司。北京海信数码科技有限公司自成立以来，在防火墙技术和产品上一直不断创新，所推出的“红狐”系列防火墙产品，遵循国家相关政策和标准开发生产的，完全自主版权的安全产品，它以先进的技术、强大的功能、优良的性能、高可靠性，赢得了遍布全国各地，涵盖政府、银行、证券、保险、税务、电信、电力等几千家用户的信任。

目　　录

第一章　防火墙简介

防火墙是一种广泛应用于因特网上的安全设备，主要作用是将内域网（Intranet）和因特网（Internet）“隔离”。网络管理员通过为防火墙设置适当的访问控制策略，来控制内部网与外部网之间的数据传输，以实现对内域网的安全保护。如图。



防火墙位置示意图

第二章　海信 FW3010PF 防火墙

1、系统的组成

1.1 产品概述

“红狐”防火墙基于 Linux 操作系统，具有系统管理、日志管理、安全策略、安全检测、网络计费、虚拟专网等多项强大的安全功能，弥补了传统包过滤防火墙的很多不足，可谓防火墙中的精品。

本产品易于安装和使用，网络性能和透明性好，拥有自行设计的友好全中文化 WWW 管理界面，通过直观、易用的界面来管理强大、复杂的系统功能。它还可根据系统管理者设定的安全规则（Security Rules）把守网络的大门，提供强大

的访问控制、身份认证、网络地址转换(Network Address Translation)、流量控制等功能。

1.2 系统组成

■ 海信FW3010防火墙（硬件）：是一个基于安全的操作系统平台的自主版权的高级通信保护控制系统

■ 管理软件（软件）： 是用来管理和配置防火墙的管理软件，由于海信防火墙采用基于WEB和通用串口管理，管理主机（管理防火墙的机器）只需具有IE浏览器或WINDOW系统下的超级终端软件。

■ 审计管理器（软件）：是一个可运行于Windows98、Windows2000系统下，用于对海信防火墙FW3010PF提供的远程日志信息进行可视化审计的管理软件。

1.3 硬件配置

- **接口数量（标配）**
  a. 2 个 10/100/1000Base-TX 接口（可扩展、光口和电口可选）
  b. 2 个 10/100Base-TX 接口（可扩展）
  b. 一个 CONSOLE 口
- **接口规范**
  a. 网络接口：10/100/1000BaseTX
  b. CONSOLE 口： RS232C，DTE，9600-8-N-1
- **电气性能**
  a. 电源：AC 220V 50HZ， 80W（最大）
  b. 环境规范：
  c. 运行温度：0-- 45 摄氏度
  d. 非运行温度：-20 --65 摄氏度

1.4 结构特性

本机采用了全新式结构设计，机内部件合理紧凑；在结构设计和大功率器件的布局方面充分考虑了风冷设计，使机壳内各个部件的散热问题得到了解决。除了具有技术上的许多创新和突破之外，它还在物理安全性上做了许多考虑，增加了防盗锁和防拆螺钉等。

2、产品型号说明

产品名称	功能描述	功能实现
FW3010PF-1000-3E1U-S	S 标准配置	
FW3010PF-2000-3E1U-S	S1000+C+I+R+U+T	
FW3010PF-4000-4E1U	S2000+复合型模块	
海信网络计费系统	可选模块	C
海信安全检测系统	可选模块	I
扩展接口	可选模块	E
高级路由管理模块	可选模块	R
多接入模块	可选模块	M
VLAN 模块	可选模块	L
流量控制模块	可选模块	T
双机热备模块	可选模块	H
IDS 联动模块	可选模块	U
VPN 模块	可选模块	V
身份认证模块	可选模块	O

注意：

1、 标准配置包括：串口控制+NAT+系统管理+安全策略+日志管理+透明网桥/路由/NAT 复用。

2、 在购买防火墙时，如果没有购买可选模块，则该防火墙将不具有可选模块对应的功能。

3、 复合性模块包括各种透明代理及其代理下的各种内容过滤、访问控制等功能。

第三章　海信防火墙 FW3010PF 系统特点

高安全性

专用的高性能的安全操作系统，专为防火墙、VPN 等安全应用设计开发，最大程度地确保了系统自身的安全性和高性能。

高可靠性

海信FW3010PF系列防火墙产品，采用工业控制级硬件平台，结构合理，工艺精细，最大程度地保证了稳定可靠和高效安全。

高性能

精简的操作系统，专用硬件及先进的核心处理机制的完美结合，实现高吞吐量、高带宽的安全检测，确保安全的同时，保证正常的网络应用。

高适用性

采用混合工作模式，方便接入，不影响原有网络结构。

支持众多应用协议，保证正常的网络应用。

管理方便、安全

支持本地和远程多种管理方式，管理简单，快捷。

支持远程日志功能，便于日志管理。

高度集成、灵活扩展

模块化结构，多接口设计，满足了从单一用户部署到包括多个客户的大型互联网数据中心的广泛需求。

可以灵活地与 VPN、IDS 等其他安全产品有机集成、协同工作，从而构建更强、更快、更方便的安全防御体系。

第四章　海信防火墙 FW3010PF 技术特点

4.1 一体化的软硬件设计

系统与硬件紧密结合，发挥硬件最高效能，提高系统自身安全性。

4.2 高容错电源设计

系统可采用真正容错、热插拔电源。支持双电源。

4.3 高性能的系统核心

专门为 TCP/IP 及 Firewall 而设计，能大大提升系统性能。

4.4 多接口结构体系

海信防火墙具有三个或三个以上的物理上相互独立的网络接口，是一种典型的多接口体系结构。使用物理上相互独立的网络接口，将受控网络从物理上隔离开来，提高了安全保护的能力，同时方便网络的互连和接入。海信防火墙最多可以支持到 12 个物理接口，并且在每个物理接口上还可以配置多达 256 个虚拟接口，可以满足任何规模用户网络环境的需求。

4．5 透明网桥

海信防火墙支持透明接入。将海信防火墙配置为透明工作模式，无需更改用户网络的拓扑结构就能接入用户网络中，用户网络中的主机也无需更改任何网络配置就能通过防火墙进行访问（当然是要在防火墙规则允许的情况下）。透明接入极大的方便了防火墙的接入，同时并不降低网络的安全性。

4．6 基于状态的包过滤

海信防火墙可以基于连接的状态进行数据包过滤，极大地提高了系统的性能。

4．7 多级过滤

海信防火墙可以基于数据包的源地址、目的地址、源端口、目标端口、协议标志位等进行过滤，提高了系统的防护能力。

4．8 强大的 NAT 能力

网络地址转换对 Internet 隐藏内部地址，防止内部地址公开。这一功能可以克服 IP 寻址方式的诸多限制，完善内部寻址模式。把未注册的 IP 地址映射成合法地址，就可以对 Internet 进行访问。海信防火墙支持源地址转换和目标地址转换，并支持端口影射。

4．9 SSN 服务区

海信防火墙支持安全服务器网络（SSN——Security Server Network），将提供信息访问服务的服务器安装于该网络区域内，与内、外网络从物理上隔离开来，并提供专门的安全保护。SSN 概念有别于传统的所谓 DMZ 停火区模式，它是一种更为积极的安全防护理念：一般情况下，SSN 主机不允许主动向内、外网发起连接请求，只允许向内、外网回应其请求数据包；外网用户也只能访问 SSN 上的主机，不能访问内部网主机。即 SSN 与外部网之间受防火墙保护，同时 SSN 与内部网之间也受防火墙保护，即使 SSN 受破坏，内部网络仍处于防火墙保护之下。

4．10 基于规则的带宽管理

海信防火墙的带宽管理粒度细致，方便灵活。海信防火墙能够指定进行带宽

管理的网络接口，支持多达 8 级。可以灵活地根据 IP 地址限制其使用的带宽。

4．11 内置入侵检测

海信防火墙内置简单入侵检测系统，能够检测对防火墙常用的攻击方式。

4．12 双机热备

为了保证网络的高可用性与高可靠性，海信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。正常情况下一个处于工作状态，为主防火墙，另一个处于备份状态，为从防火墙。当主防火墙发生意外 down 机、网络故障、硬件故障等情况时，主从防火墙自动切换工作状态，从防火墙代替主防火墙正常工作，从而保证了网络的正常使用。切换过程不需要人为操作和其他系统的参与，切换时间可以以秒计算。

4．13 支持 SSL WEB 管理

为了便于管理员的管理，海信防火墙除了支持本地管理以外，还提供基于 Web 方式的管理。

为了保证远程管理的安全性，海信 FW3010PF 防火墙不论是对管理员还是管理过程都采取了一系列安全措施。为了防止远程管理过程被监听和修改，采用基于 SSL 的 Web 方式管理，将管理主机和防火墙之间的通讯进行加密以保证安全。管理主机不需要安装专门的管理软件，只需通常的浏览器软件，就可以在不同操作系统平台对防火墙进行配置和管理。

4．13 系统备份

海信防火墙提供简单方便的配置文件管理，管理员可通过 Web 界面进行配置文件的备份、下载、删除、恢复和上载。用户可以随时手工备份防火墙的配置文件，可以将备份结果下载到本地管理主机中保存，也可以将备份上载回防火墙进行恢复还原。

4．14 IP 与 MAC 地址绑定

MAC 是用户使用网卡的标识字串，共 6 字节，是网卡在出厂时由生产厂家设定的全球唯一的标识符，可以唯一的标识一个内部用户的物理地址，IP 与 MAC 捆绑防止防火墙管理的内网域内主机的 IP 地址被另一台机器盗用。也就是说，如果要保护的主机与防火墙直接相连，可以将此机器的 IP 物理与网卡地址捆绑，

这样其他内部机器就不可能使用这个 IP 通过防火墙访问外部网络。

4.15 透明代理

提供对常用高层应用服务（HTTP、FTP、SMTP、POP3、NNTP）的透明代理。用户不需要在自己的主机上作任何的有关代理服务器的设置，只需管理员在防火墙上配置相关的规则，用户通过防火墙进行的上述应用访问就会由防火墙进行代理，这些配置对用户来说完全是透明的，极大的方便了用户使用代理。

4.16 用户认证机制

海信 FW3010PF 防火墙支持用户认证机制，极大地提高了访问控制的安全性和方便性。

4.17 三权分立机制

海信 FW3010PF 防火墙在设计时充分考虑了防火墙本身的安全性，使得在同一时刻，只能有一位防火墙的管理员来对防火墙进行管理，同时将管理员的账号和 IP 地址捆绑，在管理员登录防火墙系统时对其账号、密码、IP 地址进行全面检查，从根本上保证了防火墙系统的安全性。

防火墙的管理员分为超级管理员、系统管理员、安全策略员、日志审计员。

第五章 海信防火墙 FW3010PF 系统功能

5.1 强大的抗攻击能力

可以抵抗 IP 地址欺骗攻击、源路由攻击、IP 碎片攻击、DOS/DDOS 攻击及其它多种拒绝服务攻击等。

5.2 丰富的包过滤功能

“红狐”包过滤功能是根据信息包的源地址、目标地址、端口号、协议类型、协议选项等多种内容进行定义的，端口可以是一个、多个或某一规定的范围，支持对多种 IP 协议，包括 TCP、UDP、ICMP 以及其它 IP 协议进行过滤。尤其是可以针对 MAC 号进行过滤；可以对通信连接状态进行跟踪。

5.3 透明网桥功能

透明网桥功能可以使海信防火墙适应不同复杂情况的网络拓扑结构。当海信 FW3010PF 防火墙工作在透明网桥模式下时，防火墙的工作状态类似一个网桥，但却可以安全地保障整个内部网络的安全。透明网桥的最大优点就是客户不需更改网络拓扑结构和原有网络设备及工作站的配置。

5.4 路由管理功能

海信防火墙的路由管理功能也是为了满足复杂网络拓扑结构应用防火墙的需求。通过防火墙的路由管理模块，为通过防火墙的数据报选择不同的路径，以保持网络的连同性。该模块的典型应用是当整个内部网络有两个或多个外出口的情况。

5.5 流量控制功能

网络带宽是另一种重要的网络资源，一个网络环境其出口带宽是有限的，防火墙可以建立一套对带宽的管理机制，能够对不同的外出访问占用的带宽进行统一的分配。可以针对具体的通信（按照源地址）对网络带宽进行分配，使得某一类的访问所占用的带宽不能超过管理员为其分配的额度，从而不至于影响其它类的访问的正常进行。

海信 FW3010PF 防火墙具有粒度细致、方便灵活的带宽管理功能。管理员指定进行带宽管理的网络接口及该接口的带宽上限后，进行带宽级别的定义。海信 FW3010PF 防火墙支持多达 8 级，管理员可以选定级别数，然后定义每个级别的带宽比例。

5.6 双机热备功能

双机热备是海信 FW3010PF 防火墙高可靠性的一种处理方式。双机热备功能必须有两台防火墙协助工作完成，一台作为主防火墙，另一台作为备份防火墙，两台防火墙通过串口连接，互相实时监测，当主防火墙发生故障时，备份防火墙自动接管主防火墙，避免整个网络通信发生中断。

5.6 SSN 安全服务区

海信防火墙的安全服务器网络体系能够对用户网络及服务器提供充分的保护。管理员将需要单独保护的服务器连接到 SSN 接口上，与内部网络和外部网络从物理上隔离开来，即能使 SSN 与外部网络之间受防火墙保护，同时 SSN 与内部网络之间也受防火墙保护，即使 SSN 受破坏，内部网络仍处于防火墙保护之下。

5.7 支持多种标准服务

系统支持几十种通信协议和几百种应用服务，包括 WWW、FTP、POP3、数据库服务、多媒体服务、Microsoft 网络服务等。用户不必担心使用了防火墙后出现某些服务失效的副作用。

5.8 针对性的防御措施

针对特定的攻击，本系统设有对应的防御措施。常见的 TCP/IP Denial-Of-Service Attack、IP Spoof 和其它具有潜在危害的网络弱点都可以由本系统保护。

5.9 美观易用的界面

系统设有基于 WWW 的管理界面，管理员可以通过由 HTML、Java applet 组成的图形界面对系统进行管理。把复杂繁多的系统功能设置变为直观易用的 WWW 界面，大大提高了系统的可用性。

5.10 多层登录权限设置

系统支持多层登录权限，管理人员可以灵活设置权限。

5.11 统计计费功能

系统提供的统计接口，可以对经过防火墙的访问节点地址进行记录，经统计分析得出各节点的访问量，计费信息。

5.12 安全检测与实时报警功能

系统对受到的攻击设有完备的记录功能，但系统检测到危险信息时，系统可以根据管理员的设置发出警告。

5.13 完备的日志处理功能

防火墙每天都要进行大量的日志，当日志占有系统资源过大时，将影响系统

的性能。海信“红狐”防火墙有强大的日志处理功能，可以远程记录；也可以本地记录；还可以对日志占有系统资源的比例进行设定。

5.14 实时系统状态检测

通过实时观察系统的运行进程、通行连接情况等，来了解整个系统的运行状况以及系统的各种网络连接状况，从而可以根据系统的情况做出相应的调整。

5.15 黑名单

黑名单是不允许通过防火墙的一个地址列表。例如，如果把一个 INTERNET 地址列入黑名单，则所有的内部网络用户不能再访问该 IP 地址的主机；如果把一个内部网络的一个 IP 地址列入黑名单，则具有该 IP 地址的主机不能再通过防火墙访问外部网络。

5.16 用户组管理

管理员可以以组的形式管理整个网络用户，简化工作。

5.17 网络地址转换—NAT

网络地址转换是防火墙的又一项重要功能。海信 FW3010PF 防火墙的网络地址转换功能丰富强大，包括正向的网络地址转换和反向的地址映射两大类。

国际互联网 Internet 采用 IP 地址进行网际互联和通信，能够与 Internet 上的其它主机通信的主机接口必须有一个唯一的 IP 地址。目前使用的 IP 地址长度为 32 位，地址总数是有限的，而局域网内部主机间的通信并不需要用一个全世界唯一的地址，因此 IP 地址中指定了一批保留地址，这些地址不用申请就可以用于任何一个局域网的内部通信，使得这些地址可以复用。但保留地址不能在 Internet 上路由，使用保留地址不能与 Internet 上其它使用全局地址的主机通信，因此要在局域网与 Internet 之间做网络地址转换（NAT）才能实现通信。海信 FW3010PF 防火墙为用户提供的 NAT 功能能够很好的实现这种转换。海信 FW3010PF 防火墙提供两种配置 NAT 地址的方式：SNAT 和 DNAT。

SNAT 按照管理员制定的规则将内部网用户的访问转换为固定的 NAT 地址(防火墙外口地址)。

一个单位的网络可能要对 Internet 提供一定的服务，比如 Web 访问和文件下载等等。而由于分配到的全局 IP 地址很少或是出于安全的考虑等等，提供这些服务的服务器并没有配置全局 IP 地址而是配置的保留 IP 地址,要使 Internet 上的主机能访问到这些服务，就必须使用海信防火墙的 DNAT 转换功能。使用了 DNAT 地址转换后，外部网络访问海信防火墙的一个接口地址（通常是外口全局 IP 地址），由防火墙将访问转到真正的内部服务器上，实现该全局地址到服务器真实地址的映射，从而使内部服务器能对外提供服务。海信防火墙的 DNAT 地址转换包括端口映射和地址（IP）映射两种。

海信防火墙的端口映射将防火墙外部接口的某个端口映射到内部服务器的服务端口。端口映射实现了一个 IP 地址对应多个服务器的一对多映射。目前海信防火墙完善的支持 TCP 的端口映射

海信防火墙的地址映射将防火墙外部接口的某个地址映射到内部服务器的服务地址。地址映射实现的一个 IP 地址对一个 IP 地址的一对一映射，并且支持 TCP、UDP 协议的映射。

5.18 系统提供有丰富的诊断和管理工具

提供有详细的统计和状态信息，让用户可以方便的了解防火墙的运行状态和性能；

支持各种网络管理系统；

支持当前配置保存。

5.19 良好的安全性

由于采用了专用安全操作系统，自身的安全性更高。

采用完善的状态检测技术，对网络地址、端口号或协议类型进行严密检查。

配置方式下的多级口令检查。

5.20 字符串过滤

海信防火墙可以对指定的字符串进行过滤。

5.21 IDS 动态策略

海信防火墙可以和海信 IDS（入侵检测系统）进行连动，当 IDS 检测到入侵时，IDS 发送信息给防火墙，防火墙动态形成控制策略，对入侵主机进行封堵。

5.22 时间限制

为了支持安全规则的灵活性，对每条安全策略，可以限制生效时间段，比如在星期二的 10：00 到 18：00 某条规则生效。

5.23 多种服务代理

海信 FW3010PF 防火墙支持 HTTP、FTP、POP3、SMTP 等多种服务的透明代理，从应用层上进行策略控制；可以对 HTTP 协议的 URL 关键字和脚本程序（JavaScript、JavaApplet、VBScript 和 ActiveX 等）进行过滤。

5.24 智能内容过滤功能

海信 FW3010PF 防火墙 http 代理提供内容过滤，可以帮助管理员完成对用户 IP 地址、URL、字符串、字符串组合、文件扩展名的过滤，同时具有很强的可扩展性。

海信 FW3010PF 防火墙 SMTP 代理提供内容过滤，可以帮助管理员完成对邮件来源、邮件目的地址、邮件标题、邮件内容、邮件附件的过滤，很大程度的保护了网络的安全性。

5.25 防端口扫描

海信 FW3010PF 防火墙内置了防端口扫描的模块，防止外部用户对本地用户的恶意攻击。

5.26 混合模式(透明网关)

在传统的透明网桥模式下，用户访问外网要么具有大量的公共 IP 地址，要么架设代理服务器。这两种条件无论哪一个在现代的网络规划设计中都不是最好的解决方案。

海信防火墙工作在混合模式下，提供透明网关的功能，可以很好的解决这个问题：用户既可以使用网桥的不改动网络拓扑、管理方面的优点，又可以利用地址转化功能，解决客户 IP 地址缺乏、多个外网接入的难题。

5.27 DHCP 功能

DHCP 的全称是动态主机配置协议(Dynamic Host Configuration Protocol)，由 IETF（Internet 网络工程师任务小组）设计，详尽的协议内容在 RFC 文档

rfc2131 和 rfc1541 里。目的就是为了减轻 TCP/IP 网络的规划、管理和维护的负担，解决 IP 地址空间缺乏问题。运行 DHCP 的服务器把 TCP/IP 网络设置集中起来，动态处理工作站 IP 地址的配置，用 DHCP 租约和预置的 IP 地址相联系，DHCP 租约提供了自动在 TCP/IP 网络上安全地分配和租用 IP 地址的机制，实现 IP 地址的集中式管理，基本上不需要网络管理人员的人为干预。而且，DHCP 本身被设计成 BOOTP（自举协议）的扩展，支持需要网络配置信息的无盘工作站，对需要固定 IP 的系统也提供了相应支持。

海信 HB 防火墙既可以做 DHCP 客户又可以做 DHCP 服务器。

DHCP 客户：防火墙每个接口都可以工作在这种模式下，可以动态的从网络上 DHCP 服务器上获得地址，适用于使用 DHCP 服务器统一管理 IP 地址的网络环境。

DHCP 服务器：DHCP 服务器可以启动在防火墙任意一个物理接口上，为与其相连的子网动态分配 IP 地址及相关信息，如网关、广播地址、DNS 等等，可以通过使用防火墙的 DHCP 服务功能，节约购置专门的 DHCP 服务器的资金。

5.28 支持 ADSL

ADSL(Asymmetric Digital Subscriber Line)，中文名字叫非对称数字用户线路，当在电话线两端分别放置ADSL MODEM时，在这段电话线上便产生了三个信息通道： 一个速率为 1.5Mbps-9Mbps的高速下行通道，用于用户下载信息； 一个速率为 16Kbps-1Mbps的中速双工通道，用于用户上传输出信息； 一个普通的老式电话服务通道，用于普通电话服务。这三个通道可以同时工作,传输距离达3KM---5KM。

非数字用户线路(ADSL)与以往调制解调技术的主要区别在于其上下行速率是非对称的，即上下行速率不等，ADSL技术的高下行速率和相对而言较慢的上行速率非常适于做Internet浏览使用。由于接入成本相对较低，却可以获得较高的带宽，ADSL宽带接入日益普及。

目前ADSL接入分为两种方式，一种是动态获取IP地址，就是用户没有固定的IP地址，在使用ADSL拨号软件时动态获得一个IP地址；另一种是固定IP地址，即用户在申请ADSL服务时，服务商提供给用户固定的IP地址、网关、DNS等等。

海信 HB 防火墙早期仅支持固定 IP 的接入方式，为了响应动态获取 IP 接入

ADSL 的增多市场需求，目前海信 HB 防火墙也提供了对动态 IP ADSL 接入的支持，更好的为中小企业的网络安全提供保障。

5.29 智能阻断功能

网络安全系统的构建不是简单的安全产品的叠加，系统防御已从简单的静态防御向动态防御发展，动态防御的一个重要表现就是不同内型的安全设备协同工作，动态联动，对发现的攻击行为进行实时的适应性配置修改，使得系统防御能力在实际应用中自动适应性提高。

入侵侦测系统是收集各种信息，由内置的专家系统进行分析，发现其中潜在的攻击行为的一种网络安全设备。根据分析的信息的不同，入侵侦测系统分为基于网络的入侵侦测系统和基于主机的入侵侦测系统。网络入侵侦测系统（NIDS）捕获分析网络中的所有报文，发现其中的攻击企图，根据事先制定的策略通知管理员或自行采取保护措施。

海信防火墙提供了轻便型入侵监测系统，管理员可以启动海信防火墙自带的入侵监测系统，监测、监视本地网络，同时可以启动防火墙的智能阻断安全模块，当入侵监测系统发现有攻击行为时，防火墙的智能阻断模块根据管理员的设置，拦截网络攻击行为，从而保护本地网络免收攻击。如果攻击事件一直持续，防火墙对此攻击的拦截时间会持续增加。在攻击事件发生后的一定时间以后，智能阻断模块会自动解除来源于攻击方的请求，同时检测到的攻击事件。

5.30 双接入

支持多线路接入方式（比如同时接入电信和联通），并在多线路之间进行负载均衡；实时监测线路健康状况，从而自动取消/恢复线路的通信。

第六章 海信 FW3010PF 防火墙性能指标

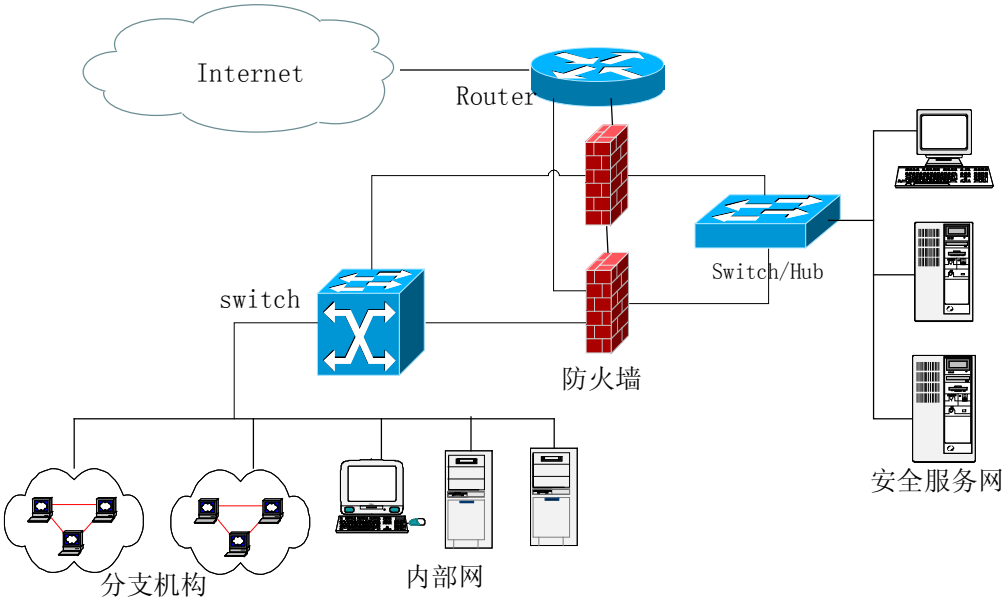
MTBF:>=80000 小时

最大（同时）并发连接数：100 万

设计性能：>920Mbps

第七章 海信 FW3010PF 防火墙典型应用

海信防火墙典型应用示例：



海信防火墙典型应用示例图

1、远程安全管理：基于SSL的Web方式管理，通信都是加密的，保证了远程管理的安全性。

2、对内部网的内部地址进行NAT地址转换。NAT既可以节省IP，又可以防止来自外部的探测。

3、需要对外提供服务的服务器如HTTP server、E-mail server、FTP server，放在SSN区，进行物理隔离。

4、对有限的出口带宽进行带宽管理。

5、支持双机热备。一般来说，出厂时，防火墙为单机模式，在上图的网络中，去掉一台防火墙，防火墙就只能在单机模式下工作。为了防止防火墙因为某种原因不能正常 工作，采用双机接入方式，一台为主防火墙，一台为从防火墙，正常工作时，主防火墙起作用，当主防火墙网络出现问题（如网线断掉、网卡坏掉等）时，从防火墙就会接替主防火墙的工作。

第八章 海信防火墙虚拟专网（VPN）特点

8.1 特点

1） 密钥管理系统，使用 IKE 协议进行会话密钥的自动协商，所有的 VPN 连接隔一段时间会自动的更换密钥。IKE 协议使用共享密钥进行认证，将管理的复杂程度降低到最小。

2） 支持的加密算法为 DES 三重加密算法，目前还无法破解。

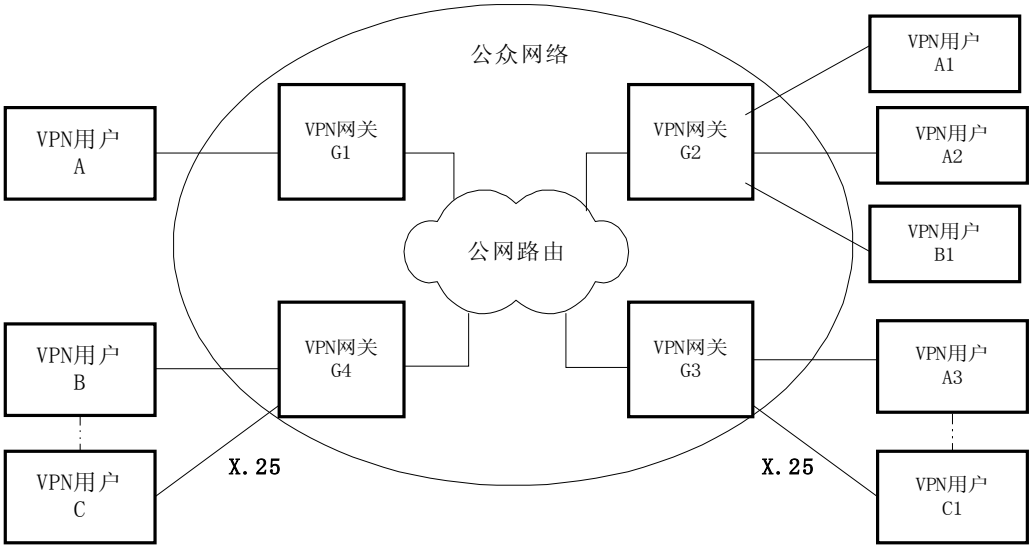
3） 支持的认证算法为 MD5 或 SHA，可为 AH 或 ESP 协议所使用，确认了对话双方的身份，有效防止了使用身份伪装的主动攻击。

4） 使用 WEB 中文管理界面，更易于管理。

5） 只需要在网关上进行配置，终端用户无需知道连接的细节。

6） 海信防火墙可选模块。

8.2 专网的逻辑连接示意图



在 VPN 用户 A 与 B 之间建立 VPN 连接，只需要在 VPN 网关 G1 和 G4 上进行设置，使用户 A 与用户 B 的子网建立 VPN 连接，对用户 A 与 B 则完全透明。假设 A 的 IP 地址为 10.0.0.4/24，B 的 IP 地址为 192.168.2.4/24，G1 的 IP 地址为 10.0.0.1，G2 的 IP 地址为 192.168.2.1，那么只需要在网关 G1 和 G2 上设置 A 与 B 所在子网的 IP 地址，网关 G1 和 G2 的 IP 地址，网关 G1 和 G2 进行认证

的公有密钥，一共五个参数即可。而且只需设置一次，从此在网关 G1 和网关 G2 之间就可以自动协商加密和认证的方法，而且以后在用户 A 或用户 B 所在的子网中添加计算机时，不需作任何改动，新添加的计算机即可使用 VPN 连接。体现了“红狐”防火墙使用简单、管理和维护开销低的特点。