

网络卫士防火墙 猎豹系列 产品说明



天融信

北京市海淀区上地东路1号华控大厦 100085

电话: +8610-82776666

传真: +8610-82776677

服务热线: +8610-8008105119

<http://www.topsec.com.cn>

版权声明

本手册的所有内容，其版权属于北京天融信公司（以下简称天融信）所有，未经天融信许可，任何人不得仿制、拷贝、转译或任意引用。本手册没有任何形式的担保、立场倾向或其他暗示。

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，天融信及其员工恕不承担任何责任。本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不承担另行通知之义务。

版权所有 不得翻印© 1995-2007 天融信公司

商标声明

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

TopSEC®天融信

信息反馈

<http://www.topsec.com.cn>

目 录

1	可编程 ASIC 技术	1
1.1	ASIC 技术的发展	1
1.2	可编程 ASIC 技术特点	2
1.3	可编程 ASIC 在安全领域应用的必然	3
2	猎豹系列防火墙介绍	4
2.1	产品概述	4
2.2	产品特点	5
3	猎豹系列防火墙功能	7
4	运行环境与标准	10
5	典型应用	12
5.1	典型应用一：猎豹在大型网络中的应用	12
5.2	典型应用二：猎豹在千百兆混合网络中的应用	13
6	声明	13

1 可编程 ASIC 技术

在确定技术总体方案时，选择合适的硬件体系结构是非常重要的。如果硬件架构选择不当，就无法保证千兆线速防火墙必须具备的高性能、高灵活性和足够的稳定性。

目前实现千兆防火墙的硬件体系结构可以分为通用 CPU 架构、可编程 ASIC 架构和网络处理器架构三种，他们各自的特点分别如下：

➤ 通用 CPU 架构

通用 CPU 架构最常见的是基于 Intel X86 架构的防火墙，在百兆防火墙中 Intel X86 架构的硬件以其高灵活性和扩展性一直受到防火墙厂商的青睐；由于采用了 PCI 总线接口，Intel X86 架构的硬件虽然理论上能达到 2Gbps 的吞吐量甚至更高，但是在实际应用中，尤其是在小包情况下，远远达不到标称性能，通用 CPU 的处理能力也很有限。

➤ 可编程 ASIC 架构

可编程 ASIC (Application Specific Integrated Circuit, 专用集成电路) 技术是当前高端网络设备广泛采用的技术。由于采用了硬件转发模式、多总线技术、数据层面与控制层面分离等技术，可编程 ASIC 架构防火墙解决了带宽容量和性能不足的问题，稳定性也得到了很好的保证。

➤ 网络处理器架构

由于网络处理器所使用的微码编写有一定技术难度，难以实现产品的最优性能，因此网络处理器架构的防火墙产品难以占有大量的市场份额。

因此，采用可编程 ASIC 架构是目前千兆高端防火墙的主流技术。

1.1 ASIC 技术的发展

从概念上来讲，从有电路的一刻起，就开始了 ASIC (Application-Specific Integrated Circuit, 专用集成电路) 的开发与应用，ASIC 采用硬接线的固定模式，最早的 ASIC 确实是完全量身订造，并经过了数十年的发展，现在每年 ASIC 市场超过 90 亿美元。可编程芯片则从 70 年代初期开始起步，可编程逻辑装置 (Programmable Logic Device; PLD) 经历了 PLA、PAL、GAL、PEEL、EPLD、CPLD、SPLD、FPGA 等阶段，现在每年主流的 FPGA (Field Programmable Gate Array, 现场可编程门阵列) 市场超过 30 亿美元，FPGA 在小量应用或大量但低复杂度的应用中具有光明的前景。

当前自主研发芯片的网络 IT 设备大多采用了 ASIC 或者 FPGA 技术。厂商在考虑选用 ASIC 和 FPGA 时，硅芯片成本、NRE (非重复性工程设计, Non-Recurring Engineering)、封装和测试费用等是厂商考虑的主要因素。当设计要求具有极高的性能、极大的容量或

最低的功耗时，标准单元 ASIC 很可能仍将是首选的技术，只要产量和价格能满足业务的需要。

然而，最新的统计显示，大约 80% 的 ASIC 从来没有达到 50 万片以上的投产量。目前，中等设计复杂度大约是 120 万门 (80 万逻辑单元和 40 万储存单元)。尽管 FPGA 供货商并不承认，但最大型的 FPGA 仍必须突破 100 万逻辑闸的门坎。结果，越来越多的 ASIC 用户正寻求可行的替代方案。这些趋势说明，不论 ASIC 还是 FPGA 都不能有效满足某些设计需要，而且这样的设计变得越来越多，FPGA 与标准单元 ASIC 之间存在巨大的市场空白。

传统的 ASIC 和 FPGA 设计方法，都能够满足网络 IT 设备部份需要，但随着应用的多样化，这两种技术也都暴露了一些大缺陷：

1) 虽然 ASIC 一旦投产，就能提供良好的性价比，但 ASIC 设计、工具和光罩的巨额成本令大多数公司望而却步。严格的 ASIC 设计流程和硬联机的实现方式不能提供相应的灵活性，因而无法及时抓住稍纵即逝或新兴的市场机会。缺乏灵活性还导致可升级能力较弱，因为诸如通讯基础设备等许多应用的关键需求之一是具备现场可升级能力。

2) FPGA 能解决上市时间以及 ASIC 缺乏灵活性的问题，并能避免在工具上的前端高额投资以及 NRE 费用。然而，高昂的 FPGA 单片成本限制了它们在成本感应型应用中的使用。高功耗、低性能以及有限容量等技术因素使 FPGA 在很多应用中显得不切实际或缺乏经济上的可行性。

日益缩短的产品生命周期以及不断提高的性能和容量需求迫使产品开发商采用创新的 IC 技术，以满足这些市场需求。为解决传统设计方法的缺陷，特别是弥补 FPGA 和高端 ASIC 之间的需求间隔，从 2002 年开始众多厂商先后提出并开发了可编程 ASIC (Programmable ASIC)，可编程 ASIC 融合了 FPGA 和 ASIC 的优点，克服了它们的缺陷。

1.2 可编程 ASIC 技术特点

可编程 ASIC 是将多个电路迭层 (Layer) 的 ASIC，将其中数层的电路改成 FPGA 的形态 (允许变动、调整电路)，并保留几层为原有的传统 ASIC 形态 (不允许再行调整电路)。如此，可编程 ASIC 的价位成本、变更弹性、设计周期、效能、用电等各种特性，皆能介于 ASIC 与 FPGA 之间。这种电路结构、特性上采复合、混种的设计正好填补了今日 ASIC 与 FPGA 所难兼顾的市场需求。

可编程 ASIC 的设计如图所示，在七层的电路迭层，其中三层允许可程序化调整 (类似 FPGA)，其它层仍为传统 ASIC 的固定光罩制成。

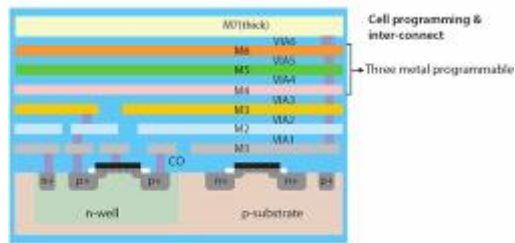


图 1-1 可编程 ASIC 的七层迭层电路

由于可编程 ASIC 的设计不同于以往的 ASIC，也不同于以往的 FPGA，鉴于可编程 ASIC 的技术优势，众多全球性大公司参与其中，很多知名的开发厂商都提供了相应工具，形成了一个完整的可编程 ASIC 的产业链。

在可编程 ASIC 中固定的或低风险的设计功能——例如防火墙系统的路由、交换、以及报文队列等，可以用传统 ASIC 电路实现，而高风险模块和需要现场可升级能力的功能可以被置于可编程的电路层中实现。这种方案能提供类似 FPGA 的设计流程和灵活性，同时达到类似 ASIC 的性能、功耗和成本。

传统 ASIC 在 TAT (Turn-Around Time; 设计、验证、修正微调的周期往返时间) 周期时间上需时 50 多个星期，而改用可编程 ASIC 可缩短至 18—20 个星期，大大加速芯片产品及时上市的时间。同时基于可编程 ASIC 的产品的 NRE 费用接近 FPGA。

1.3 可编程 ASIC 在安全领域应用的必然

现在网络的速度越来越快，防火墙应用越来越丰富，网络应用越来越向实时交互发展，新的业务层出不穷，从而要求的性能越来越高，从 100M 到 1000M 到 10G，实时性越来越向电路级靠拢，对新的应用、解决新威胁也要求安全设备在几个月得到响应。在高端安全可编程 ASIC 中把成熟的功能单元 ASIC 化，如内存控制、IP、MAC、交换、路由、3DES/DES/MD5/SHA1、模式匹配等，而把不成熟或会变化的功能置于 FPGA 形态电路层，如 H323 支持。通过这样的设计与实现，减少了 NRE，降低了单芯片的成本，加快了开发，同时确保了高速与低时延。

从芯片的角度探讨安全技术，已经成为国际性公司展现实力的最普遍形式之一，特别是在专用芯片领域，一大批公司试图通过完全的自身研发，从而得到专属芯片技术。在高端的产品，无论是交换机、路由器还是安全设备，最大的技术区分还是集中在芯片上。对安全技术，更面临着工作稳定性和自身安全性的挑战。

2 猎豹系列防火墙介绍

2.1 产品概述

网络卫士防火墙系统猎豹产品，是天融信公司在多年网络安全产品开发与实践经验的基础上开发的，基于可编程 ASIC 为核心芯片的新一代防火墙。

猎豹继承了天融信公司十年来在安全产品研发中的积累的多项成果，以自主知识产权的网络安全操作系统 TOS（Topsec Operating System）为系统平台，采用开放性的系统架构及模块化的设计思想，充分体现了天融信公司在长期的产品开发和市场推广过程中对于用户需求的深刻理解。

同时，猎豹采用了天融信自主研发的新一代可编程 ASIC 芯片——TopASIC™，它天融信公司投资数千万元，历时三年，在多年芯片开发实践基础上的研发成果，TopASIC™ 既具有高可靠性、高扩展性，为系统提供了灵活的升级能力，同时又能确保防火墙的千兆、百兆端口在各种应用下达到线速转发，为防火墙构建了一个高性价比的安全平台。

猎豹是网络卫士防火墙系列的中高端产品，适用于性能要求较高的网络环境，是天融信为政府、金融、能源、教育等行业及大中型企业客户量身打造的高性能防火墙产品。



图 2-1 猎豹 I 系列产品外观图



图 2-2 猎豹 II 系列产品外观图

2.2 产品特点

● 自主知识产权的安全芯片

猎豹的核心芯片—TopASIC™，是天融信在多年芯片开发的经验积累下，在上一代芯片开发的基础上完成的，从而确保该芯片在继承了原有技术优势的同时，技术的稳定性好。TopASIC™的成功开发和应用，使天融信跻身于少数拥有芯片级核心技术自主知识产权的国际安全厂商的行列。

● 高集成度高稳定性的芯片

猎豹借鉴了业内芯片 SoC(System on Chip)技术，芯片内置硬件防火墙单元、7层数据分析单元、VPN 加密单元、硬件路由交换单元、快速报文缓存、MAC 等众多硬件芯片单元，使得防火墙全部业务功能都在安全芯片系统内完成。高度集成化确保产品具有低功耗、高性能、高稳定、长寿命的特点。

● 灵活的双引擎构架

猎豹的核心构架采用高性能管理 CPU 与可编程 ASIC 技术相结合的方式，将系统的控制平面与数据平面分开，大大降低了控制平面与数据平面间的数据流量。ASIC 硬件芯片负责数据业务的处理转发；高性能管理 CPU 处理器提供系统的管理控制功能，它具有强大运算能力的优势可以大大提高系统的自身抗攻击能力，以及保证在高强度攻击下的系统自身管理效率。

● 真正的线速性能

内置的专用硬件加速芯片，保证系统从小包 64 字节到 1518 字节的数据处理，从简单功能到复杂网络应用组合，都可以达到 100%的线速转发。加之天融信自主 TAPF (TopASIC Packet Fashpath)报文转发技术，报文转发延迟比传统防火墙降低了数十倍。具体表现为：

- 各种业务条件下的线速转发。例如当启动 NAT、各种防火墙策略后，系统性能不变。
- 系统大容量。最高 5Gbps 总转发容量。保证猎豹千兆端口的线速转发。
- 低延迟。借助报文快速处理 TAPT 等技术，使得报文转发延迟相对 X86 或者 NP 构架防火墙有数十倍的降低，最低可以小于 3us。

● 高稳定性和高处理能力

专用芯片技术是当前高端网络设备广泛采用的技术。由于采用了硬件转发模式、多总线技术、数据层面与控制层面分离等技术，专用芯片架构防火墙解决了带宽容量和性能不足的问题，稳定性也得到了很好的保证。

通过对用户需求的深入了解，对关键功能的处理流程进行大量的优化工作，使得关键处理部分以简单而固定的方式实现，从而固化到硬件。通过把指令或计算逻辑固化到硬件中，可以获得很高的处理速度，因而能够很好地满足网络安全设备对处理能力、性能及稳定性的要求。

● 自主产权的安全操作系统平台

猎豹采用自主知识产权的安全软件操作系统——TOS (Topsec Operating System)，既提高了产品性能，又提高了产品的灵活性、高效性和安全性。具有高安全性、高可靠性、高实时性、高扩展性及多体系结构平台适应性的特点。TOS 操作系统的应用使猎豹产品继承了天融信在安全领域多年积累的经验，确保了原有产品解决方案的稳定性和功能特点。

3 猎豹系列防火墙功能

功能类别	功能项	功能描述
基本功能	芯片功能	<ul style="list-style-type: none"> ◇ 灵活速度共存：融合了 NP 可编程、传统 ASIC 高性能特点。比 NP 性能更高更稳定，编程更简单；比传统 ASIC 更加灵活。 ◇ ASIC 两级独立缓存。ASIC 系统内部 256Kbps 的 SRAM 一级缓存，以及高达 256M 的 ASIC 独立专用存储空间（二级 catch 缓存），保证所有网络处理和表项都在 ASIC 内部快速执行，并保证表项的扩充能力，这也是产品拥有高性能的重要保证。 ◇ 系统集成化。将众多处理功能芯片（MAC、SRAM、VPN 加密单元、NAT 加速单元、FW 功能单元等）集于 ASIC 一身，确保系统的低功耗，高性能，高稳定，长寿命。 ◇ 低报文延迟。采用 TAPF（TopASIC Packet FastPath，ASIC 报文快速路径），和其他 ASIC 对比，是降低报文延迟的关键技术。
工作模式	网络接入	<ul style="list-style-type: none"> ◇ 透明，路由，混合。
	虚拟系统	<ul style="list-style-type: none"> ◇ 支持路由(包括 NAT)和透明模式下的虚拟系统。 ◇ 每个虚拟系统都提供独立的策略管理（包括 NAT、包过滤、以及访问控制策略）。
网络安全性	内容过滤	<ul style="list-style-type: none"> ◇ 采用完全内容检测（Complete Content Inspection）技术。 ◇ 支持基于流、数据包、透明代理的过滤方式。 ◇ 支持对 HTTP、SMTP、POP3、FTP 等协议的深度内容过滤。 ◇ 支持 URL 过滤。 ◇ 支持对移动代码如 Java applet、Active-X、VBScript、Java script 的过滤。 ◇ 支持对邮件的收发邮件地址、文件名、文件类型过滤。 ◇ 支持对邮件主题、正文、收发件人、附件名、附件内容等关键字匹配过滤。 ◇ 支持 MSN, QQ, Skype 等 Instant Messenger 通信，并可以对于这些应用进行登陆限制。 ◇ 可限制 BT, eMule, eDonkey 等 P2P 应用。 ◇ 可屏蔽受保护主机/服务器系统信息，如替换服务器（FTP、SMTP、POP3、telnet,HTTP）的 BANNER 信息。
	包过滤	<ul style="list-style-type: none"> ◇ 基于状态检测的动态包过滤。 ◇ 基于源/目的 IP 地址、MAC 地址、端口和协议、时间、用户的访问控制。 ◇ 支持基于用户的 PPTP 的访问控制。 ◇ 支持报文合法性检查。 ◇ 动态端口支持协议：H.323、SIP、FTP、RTSP、SQL*NET、MMS、RPC、TFTP、PPTP。 ◇ 可实现 IP/MAC 绑定。
	防御攻击	<ul style="list-style-type: none"> ◇ 非法报文攻击：land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspooof。 ◇ 统计型报文攻击：Synflood、Icmpflood、Udpflood、Portscan、ipsweep。 ◇ Topsec 联动：可与支持 TOPSEC 协议的 IDS 设备联动，以提高入侵检测效率。 ◇ 端口阻断：可以根据数据包的来源和数据包的特征进行阻断设置。 ◇ SYN 代理：对来自定义区域的 Syn Flood 攻击行为进行阻断过滤。 ◇ CC 攻击：可通过设置端口和阈值阻断 CC 攻击。 ◇ 可记录攻击日志和报警。

	AAA 服务	<ul style="list-style-type: none"> ◇ 支持使用一次性口令认证 (OTP)、本地认证、双因子认证 (SecurID) 以及数字证书 (CA) 等常用的安全认证方式。 ◇ 支持 RADIUS、TACACS/TACACS+、LDAP、域认证等安全认证方式。 ◇ 支持 Session 认证、HTTP 会话认证。 ◇ 支持认证保活功能。 ◇ 可将认证用户信息加密存放在本地数据库。
	NAT	<ul style="list-style-type: none"> ◇ 支持双向 NAT。 ◇ 支持动态地址转换和静态地址转换。 ◇ 支持多对一、一对多和一对一等多种方式的地址转换。 ◇ 支持虚拟服务器功能。
网络适应性	路由	<ul style="list-style-type: none"> ◇ 支持静态路由、动态路由。 ◇ 支持基于源/目的地址、接口、Metric 的策略路由。 ◇ 支持单臂路由，可通过单臂模式接入网络，并提供路由转发功能。 ◇ 支持 Vlan 路由，能够在不同的 VLAN 虚接口间实现路由功能。 ◇ 支持 RIP、OSPF 等路由协议。
	组播	<ul style="list-style-type: none"> ◇ 支持 IGMP 组播协议。 ◇ 支持 IGMP SNOOPING。 ◇ 可有效地实现视频会议等多媒体应用。
	VLAN	<ul style="list-style-type: none"> ◇ 可与交换机的 Trunk 接口对接，并且能够实现 Vlan 间通过安全设备传播路由。 ◇ 支持 802.1Q，能进行封装和解封。 ◇ 支持 ISL，能进行 ISL 的封装和解封。 ◇ 在同一个 Vlan 内能进行二层交换。
	生成树	<ul style="list-style-type: none"> ◇ 支持 802.1D 生成树协议。
	ARP	<ul style="list-style-type: none"> ◇ 支持 ARP 代理、ARP 学习。 ◇ 可设置静态 ARP。
	非 IP 协议	<ul style="list-style-type: none"> ◇ 支持对非 IP 协议 IPX/NetBEUI 的传输与控制。
	DHCP	<ul style="list-style-type: none"> ◇ 支持 DHCP Client、DHCP Relay、DHCP Server。
	接入	<ul style="list-style-type: none"> ◇ 支持 ADSL 等宽带接入。 ◇ 支持 PPPOE 拨号接入。
VPN	其它	<ul style="list-style-type: none"> ◇ 支持网络时钟协议 SNTP，可以自动根据 NTP 服务器的时钟调整本机时间。 ◇ 支持 IPX、NetBEUI 等非 IP 协议。
	PKI	<ul style="list-style-type: none"> ◇ 支持基于标准 IKE 协商的 VPN 通信隧道。 ◇ 支持多种 IKE 认证方式，如预共享密钥、数字证书，支持扩展认证。 ◇ 支持 IKE 扩展认证，如 Radius 认证等。 ◇ 支持 OCSP 在线证书认证协议
	接入扩展	<ul style="list-style-type: none"> ◇ 可允许远程用户通过 L2TP 接入，建立 L2TP 隧道访问内部网络。 ◇ 可允许远程用户通过 PPTP 接入，建立 PPTP 隧道访问内部网络。
	移动用户	<ul style="list-style-type: none"> ◇ 支持基于时间的移动用户访问权限控制。 ◇ 支持 windows98\windows me\windows 2000 和 Windows XP 操作系统用户。
	解决方案	<ul style="list-style-type: none"> ◇ 支持网关到网关、远程移动用户到网关的 VPN 隧道。 ◇ 在具有 SCM 的解决方案中，支持灵活的移动用户到移动用户的隧道。 ◇ 可以和密码机产品，远程客户端产品及 VPN 安全管理系统 (SCM) 共同组成完整的 VPN 解决方案。
	算法	<ul style="list-style-type: none"> ◇ 支持 3DES、DES、国密办等加密算法。 ◇ 支持标准 MD5、SHA-1 认证算法。
	工作模式	<ul style="list-style-type: none"> ◇ 支持 HUB-SPOKE 方式。 ◇ 支持网状连接方式。 ◇ 支持分级的树状连接方式。

	其它功能	<ul style="list-style-type: none"> ◇ 支持 Cleaned VPN，能对隧道内数据进行病毒查杀和内容过滤。 ◇ 支持网络邻居（利用 WINS）。 ◇ 支持隧道内的 QoS。 ◇ 支持隧道的 NAT 穿越。 ◇ 支持对隧道内明文的访问控制。 ◇ 可同时支持明密传输。
安全管理	用户认证	<ul style="list-style-type: none"> ◇ 支持使用一次性口令认证（OTP）、本地认证、双因子认证（SecurID）以及数字证书（CA）等常用的安全认证方式。 ◇ 支持使用第三方认证，如 RADIUS、TACACS/TACACS+、LDAP、域认证等安全认证方式。 ◇ 支持 Session 认证、HTTP 会话认证。 ◇ 支持认证保活功能。 ◇ 可将认证用户信息加密存放在本地数据库。
	日志	<ul style="list-style-type: none"> ◇ 支持 Welf、Syslog 等多种日志格式的输出。 ◇ 支持通过第三方软件来查看日志。 ◇ 支持日志分级。 ◇ 支持对接收到的日志进行缓冲存储。 ◇ 支持安全审计系统（TA-L），获得更详尽的日志分析和审计功能。 ◇ TA-L 除接受防火墙日志外还能接受交换机、路由器、操作系统、应用系统和其他安全产品的日志进行联合分析。 ◇ 可对日志进行加密传输。
	监控	<ul style="list-style-type: none"> ◇ 支持网络接口、CPU 利用率、内存使用率、操作系统状况、网络状况、硬件系统、进程、进程内存、加密卡状况的监测。 ◇ 可根据配置文件进行错误恢复。
	报警	<ul style="list-style-type: none"> ◇ 内置了“管理”、“系统”、“安全”、“策略”、“通信”、“硬件”、“容错”、“测试”等多种触发报警的事件类。 ◇ 支持邮件、NETBIOS、声音、SNMP、控制台等多种组合报警方式。
带宽管理	QoS 流量整形	<ul style="list-style-type: none"> ◇ QOS 带宽管理。 ◇ 根据 IP、协议、网络接口、时间定义带宽分配策略。 ◇ 支持最小保证带宽和最大限制带宽。 ◇ 支持分层的带宽管理。
	优先级	<ul style="list-style-type: none"> ◇ 支持 8 级优先级控制。
高可用性	双机热备	<ul style="list-style-type: none"> ◇ 支持双机热备（Active-Active，与 Active-Standby 两种模式）。 ◇ 支持系统故障切换，包括主设备抢状态开关功能，控制主设备是否在设备恢复正常情况时抢回主设备状态。 ◇ 支持 VPN 网关的双机热备功能。
	负载均衡	<ul style="list-style-type: none"> ◇ 支持轮询、加权轮叫、最少连接、加权最少链接等多种服务器负载均衡方式。 ◇ 支持生成树协议，实现链路负载均衡。
	其它功能	<ul style="list-style-type: none"> ◇ 支持链路备份功能。 ◇ 支持双系统引导。 ◇ 支持 Watchdog 功能。
配置管理	配置方式	<ul style="list-style-type: none"> ◇ 支持 WEB 图形配置、命令行配置。 ◇ 支持本地配置、远程配置。 ◇ 支持基于 SSH、SSL 的安全配置。
	命令行	<ul style="list-style-type: none"> ◇ 支持配置命令分级保护。 ◇ 支持中英文。 ◇ 支持命令超时、历史命令、命令补齐、命令帮助、命令错误提示等功能。
	SNMP	<ul style="list-style-type: none"> ◇ 支持 SNMP 的 v1、v2、v2c、v3 版本。 ◇ 与当前通用的网络管理平台兼容，如 HP Openview 等。
	系统升级	<ul style="list-style-type: none"> ◇ 支持双系统升级。 ◇ 支持远程维护和系统升级。 ◇ 支持 TFTP 升级。

	报文调试	<ul style="list-style-type: none"> ◇ 提供强大的报文调试功能，可以帮助网络管理员或安全管理员发现、调试和解决问题。 ◇ 支持发送虚拟报文。
	配置恢复	<ul style="list-style-type: none"> ◇ 可以进行配置文件的备份、下载、删除、恢复和上载。
	时钟调整	<ul style="list-style-type: none"> ◇ 支持网络时钟协议 SNTP，可自动根据 NTP 服务器时钟调整本机时间。

4 运行环境与标准

猎豹 I 系列电源：

电压：AC90-260V ±10%

频率：50/60HZ

冗余：不支持

猎豹 II 系列电源：

电压：AC100-240V ±10%

频率：50/60HZ

冗余：支持

环境：

运行温度：-5° C ~ +45° C

非运行温度：-20° C ~ +70° C

相对湿度：5%-95%RH，非冷凝

国家标准：

GB/T18336-2001

GB/T18019-1999

GB/T18020-1999

参考的安全规范及标准(相对参考)：

UL 1950

EN 41003

AS/NZS 3260

AS/NZS 3548 Class A

CSA Class A

FCC Class A

EN 60555-2

VCCI (ClassII)

抗干扰性：

IEC 1000 4 2 (ES0)

IEC 1000 4 3 (辐射敏感性)

IEC 1000 4 4 (电快速瞬变)

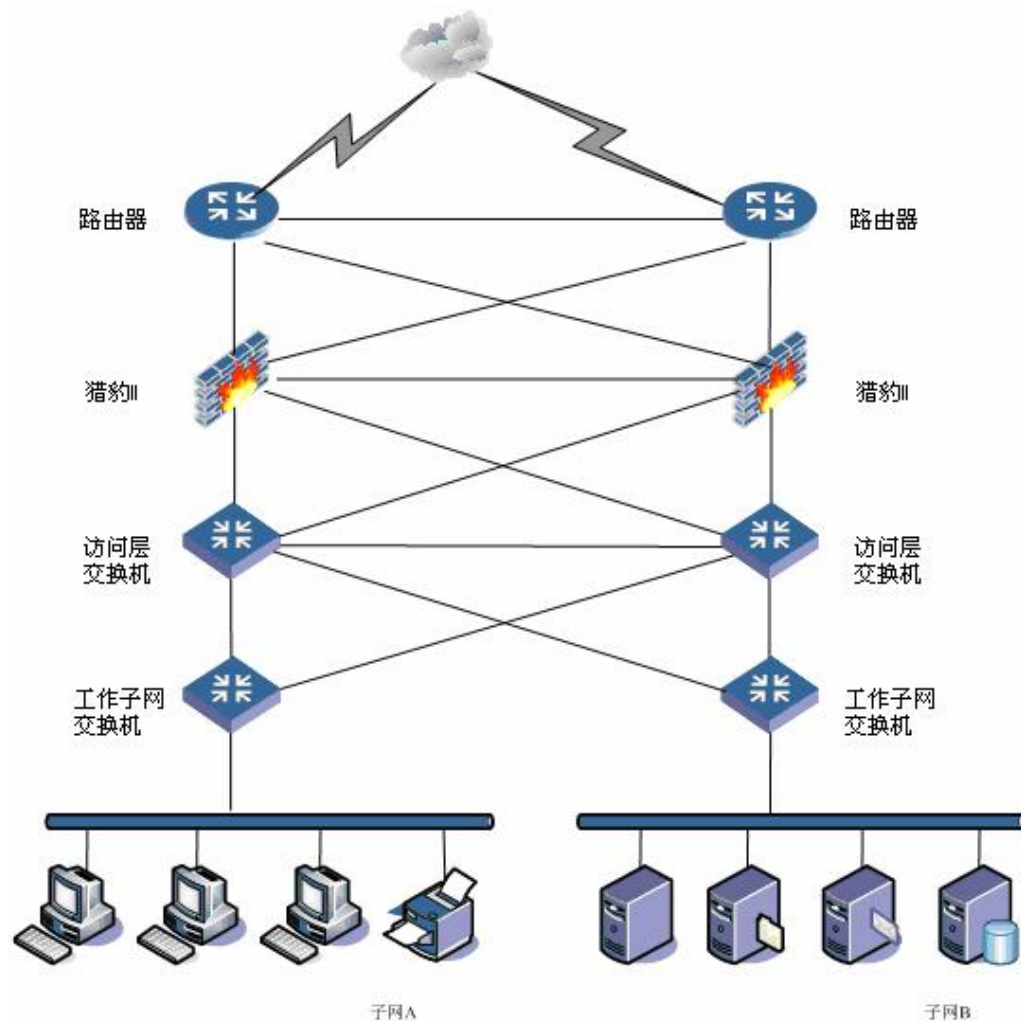
IEC 1000 4 5 (电源)

IEC 1000 3 2 (谐波)

5 典型应用

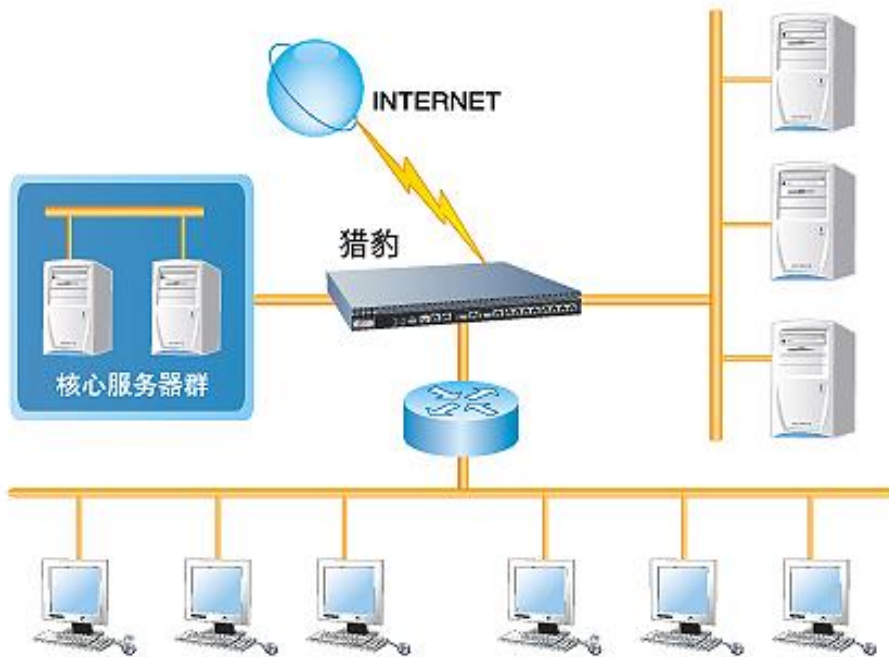
5.1 典型应用一：猎豹在大型网络中的应用

猎豹 II 防火墙可以应用于各行业大型千兆网络中。猎豹 II 最大可以提供 10 个千兆接口，其中包含 4 个 Combo 口，可以灵活适应光口/电口接入。借助于强大的 HA 功能，猎豹 II 能够采取下面的全交叉冗余接入模式，满足大型千兆网络对高可用性的需求。



5.2 典型应用二：猎豹在千百兆混合网络中的应用

猎豹 I 防火墙可以灵活应用于千百兆混合网络环境中。猎豹 I 对外提供一个 100M 出口，或者利用策略路由等功能提供多个 100M 出口链路；猎豹 I 对内最大可以提供两个千兆接口，分别用于高速交换内网和大容量服务器 DMZ 区的安全防护；另外对于内部网络的普通服务器或者部分子网，可以提供多条 100M 链路实现安全防护和隔离。



6 声明

1. 本手册所提到的产品规格及资讯仅供参考，有关内容可能会随时更新，天融信恕不另行通知。
2. 本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，此可能产生的差异为正常现象，产品功能和性能请以产品说明书为准。
3. 本手册中没有任何关于其他同类产品的对比或比较，天融信也不对其他同类产品表达意见，如引起相关纠纷应属于自行推测或误会，天融信对此没有任何立场。
4. 本手册中提到的信息为正常公开的信息，若因本手册或其所提到的任何信息引起了他人直接或间接的资料流失、利益损失，天融信及其员工不承担任何责任。