亿阳网警 BOCO.SFW-5000 防火墙

技术白皮书

目录

1 概述 3

2 亿阳网警BOCO.SFW-5000 防火墙系统特点 4

3 亿阳网警BOCO.SFW-5000 防火墙具有的关键技术 6

4.1 网络处理器体系结构 6
4.2 防火墙策略快速查找算法 9
4.3 亿阳网警BOCO.SFW-5000 防火墙的透明模式 10
4.6 高可用性模式 14

4 亿阳网警BOCO.SFW-5000 防火墙的功能介绍 15

5.1 对象管理功能 15
5.2 基于状态检测的包过滤 15
5.3 地址转换与端口映射功能 16
5.3 网络时钟协议支持 16
5.5 规则导入导出功能 16
5.6 远程升级功能 16
5.7 虚拟系统功能 17
5.8 路由管理功能 17
5.9 SNMP协议支持 17
5.10 双机热备功能 17
5.11 抗攻击功能 18
5.12 系统状态显示功能 18
5.13 报警功能 18
5.14 安全审计功能 18
5.15 网络测试功能 18

5 亿阳网警BOCO.SFW-5000 防火墙的安全性分析 19

6 亿阳网警BOCO.SFW-5000 防火墙的参数指标 20

6.1 亿阳网警BOCO.SFW-5000 防火墙的物理参数 20
6.2 亿阳网警BOCO.SFW-5000 防火墙的性能指标 20

1 概述

互联网的增长正改变着我们做事的方式。我们已经生活在一个有线的世界里，人们需要随时随地地访问信息，这一需求也正推动着人们对安全的 Internet 连接和站点间通信及远程用户通信的需求。

两大技术趋势使得这一需求的实现成为可能。首先，由于DWDM（密集波分复用）技术的最新进展，网络核心的带宽已经可以满足用户方便快捷地上网需求，而且成本很低。其次，最新的宽带访问技术，如xDSL，有线调制解调器及千兆位以太网，已经普遍应用，在BtoB和BtoC交互中，丰富的多媒体内容和高带宽应用也已司空见惯了。

在这样一个高带宽的互联的环境中，访问控制对一个网络的安全而言是至关重要的。当前许多机构不再使用昂贵的租用线路，而选择较为便宜的、基于 IP 的公共网络基础设施。这样一来，网络安全就成为一个非常重要的问题。网络安全所关注的主要内容是：保护网络不被未经授权的人访问、不被拒绝服务 (DoS)或其他黑客行文所攻击，监视并控制公司员工上网的方式及所能访问的内容等。时至今日，人们在规划和部署网络时，网络安全还是一直被忽视的问题。事实上，约有 90%的网络还没有配置任何网络安全设备。造成这一状况的原因是，网络安全产品的复杂性以及用户对网络安全的定义的理解的不恰当。幸运的是，现在网络安全产品已经越来越贴近用户的需求，并且有越来越多的人意识到了网络安全的重要性，这使得网络安全策略的大范围普及成为可能。

提供这些安全功能的最基本工具是防火墙。和其它联网技术一样，防火墙设备在过去的十年里经历了剧烈的演变。九十年代早期的软件解决方案（如 Check point）对于当时流行的公共网络访问速度而言绰绰有余。九十年代后期，高速宽带互联成为主流，基于 ASIC（特定用途集成电路）的速度较快但灵活性不足的解决方案（如 Netscreen）开始兴起。如今，千兆位网络统治了局域网和城域网，而市场上的大部分防火墙解决方案只是对上一代解决方案作了一些增强，且被滥用得超出了它们的性能局限。因为组成千兆位端口的设备并不保证能提供千兆位的流量。千兆位网络使用

这种未达到千兆位性能的防火墙便产生了一个网络瓶颈，它限制了信息流量，从而也限制了营业收入。

新一代电信级安全网关已经研制出来了，它不仅提供了完全的千兆位防火墙，而且能适应高速演化的标准和技术。这就是业界最先进的基于网络处理器构架的防火墙亿阳网警 BOCO.SFW-5000，本白皮书将对其体系结构及功能特点进行详细阐述。

亿阳网警 BOCO.SFW-5000 防火墙结合了网络处理器硬件加速技术和最先进的并行处理技术，构造出目前市场上性能最高的防火墙产品。亿阳网警 BOCO.SFW-5000 防火墙的性能优于硬编码的 ASIC 解决方案，又拥有足够的灵活性，可以适应瞬息万变的网络安全标准及新的用户层协议需求。

2 亿阳网警 BOCO.SFW-5000 防火墙系统特点

亿阳网警 BOCO.SFW-5000 防火墙是真正意义上的全线速千兆位防火墙，可为服务提供商和大型企业提供安全、快速、可靠的网络安全服务。亿阳网警 BOCO.SFW-5000 防火墙的特性如下：

基于 NPU 的全新硬件平台

采用业界最先进的网络处理器技术，是一款真正达到线速的千兆防火墙产品。它同时具有采用 ASIC 纯硬件解决方案的高性能与软件解决方案的快速升级能力。

真正千兆线速

亿阳网警 BOCO.SFW-5000 防火墙基于网络处理器硬件平台，采用的先进的报文快速转发算法和规则快速查找算法，使防火墙即使在转发小帧的情况下也能达到千兆的线速度。

支持多虚拟系统

利用虚拟系统技术使得单个亿阳网警 BOCO.SFW-5000 防火墙可以划分为多个逻辑上独立的防火墙，可以为客户提供独立的策略空间和管理空间。

丰富的协议支持

亿阳网警 BOCO.SFW-5000 系列防火墙支持多种数据链路层、网络层、应用层协议，可以适应各种用户网络环境。

强安全性

亿阳网警 BOCO．SFW－5000 防火墙提供了多种保护网络的安全措施，如果配置得当，可以保证用户网络的安全。

抗攻击能力强

亿阳网警 BOCO．SFW－5000 防火墙自身带有抗攻击模块，可以抵御各种拒绝服务攻击行为。

灵活的接入方式

亿阳网警 BOCO．SFW－5000 防火墙提供多种接入模型，可以以路由方式接入，也可以以桥方式透明接入，满足用户的各种网络环境的接入需求。

完整的冗余特性

- 双处理器结构，在任何一个处理器发生故障时，另一个都可以接管它的工作。
- 双热插拔式冗余电源、冗余热插拔散热风扇。
- 系统与策略配置的双备份，保证系统与策略的完整性
- 冗余式 GBIC 输入/输出端口(千兆光纤口)，在主接口发生物理链路上的故障时，能自动讯速切换到从接口上。

卓越的高可用性模式

为了获得最高的容错性能，我们可以将两台亿阳网警 BOCO.SFW-5000 防火墙配置为高可用性（HA）模式，当主防火墙出现系统故障，从防火墙能够快速的接管工作，

并能保留主防火墙上的所有会话信息，平滑的切换技术充分保证了用户网络的畅通。

3 亿阳网警 BOCO.SFW-5000 防火墙具有的关键技术

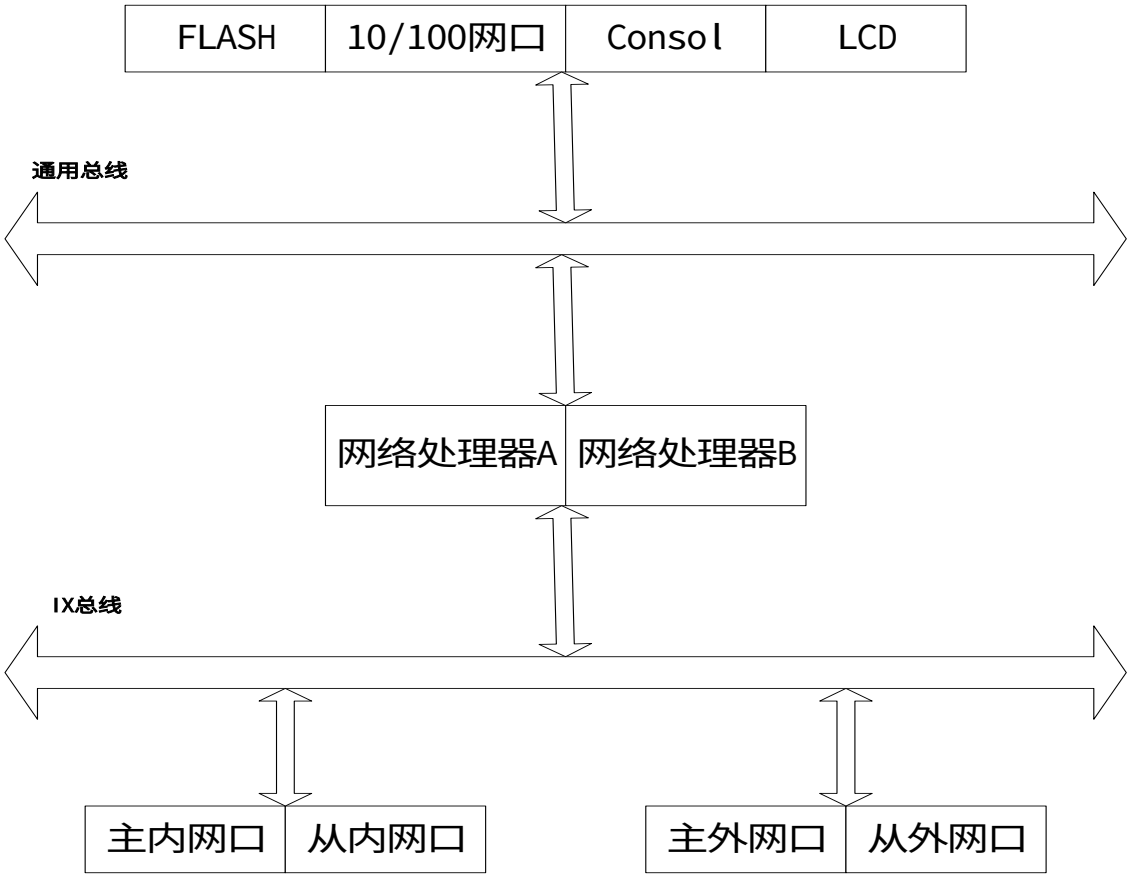
4.1 网络处理器体系结构

亿阳网警 BOCO.SFW-5000 防火墙的基础是并行网络处理器平台。该体系结构包括：用于数据包处理的高性能 Intel 网络处理器，用于网络处理与其他设备通信的专用总线以及千兆网接口等其它硬件。这些处理器通过高性能的 IXP 和 PCI 总线、嵌入式固件操作系统和独创的安全策略查找算法连在一起，致力于为平台提供完全的千兆位信息流量。

亿阳网警 BOCO.SFW-5000 防火墙提供无阻塞、全双工的千兆位防火墙性能，并能过滤 DoS 攻击，使网络免受攻击。该体系结构的带宽可扩展至 10 GB。

亿阳网警 BOCO.SFW-5000 防火墙提供了两个千兆位以太网链路(另有两个备用)，每一个可以与内部网络和外部网络相连。亿阳网警 BOCO.SFW-5000 防火墙硬件结构简图如图 1 所示。

图 1—亿阳网警 BOCO.SFW-5000 防火墙硬件结构简图



网络处理器

九十年代后期，ASIC(面向应用的集成电路)被应用于有状态数据包检查及加密/解密任务。网络安全处理速度成数量级的提高，可以跟得上最新的公共网络带宽增长。基于 ASIC 的解决方案把以前只能在软件中执行的算法的核心部分提取出来，把这些计算和操作“ 烧制 ”到专用的电路里。这样的硬件可以快速地执行定义好的操作，但缺少基于软件的解决方案的灵活性和“ 易于重编程性 ”。如果发现了新的“ bug ”,或需要增强特性/性能，我们就必须通过重新设计 ASIC 来进行必要的改动，这不仅费时，而且代价高昂。ASIC 代表了一种折衷策略：以耗时的设计和验证周期，以及高昂的“ 构建 ”费用，来换取执行特定操作集的高速度。如果能大批量生产 ASIC 并且在使用过程中不进行设计修改的话，那么基于 ASIC 的解决方案无疑是非常划算的。

在基于软件的解决方案(最为灵活)和基于 ASIC 的解决方案(最佳性能)之间的这种差别一直被认为是应验了一句俗话“ 鱼与熊掌不可兼得 ”，显然无论哪一种方案都不够完美。就在那个时候，一种新型的设计工具，网络处理器问世了。

网络处理器(NP)不同于 Pentium 之类的“ 经典的 ”中央处理单元(CPU)。从以 CPU 为中心的角度来看，Pentium 的体系结构为了普通数据处理而进行了优化，而网络处理器的体系结构围绕着处理数据包流和对这些数据包执行的操作进行了优化。

为了执行各种各样的任务，并且能维持高性能，NPU 通常要包含多个可编程处理元件。例如亿阳网警 BOCO.SFW-5000 防火墙中使用的 Intel IXP-1200 就包含了一个 Strong Arm®处理器和六个“ 微引擎 ”(micro engine)，每个引擎都可进行编程来处理四个轻量级进程，即所谓的“ 线程 ”。一般情况下，每个引擎被分派一个特定的重复性任务。数据以管道的方式在各处理器间传递、处理，这样，每个处理元件只执行一份工作，这和汽车装配线上的工位很相似。等到数据包完成了管道之旅的时候，它就已经被标记上了特征标记(接受和拒绝)，也有可能被修改(添加或删除 VLAN 标记、NAT 等)。

通过基于 NPU 的设计获得高性能的关键是：确保由合适的处理元件在合适的时间处理合适的信息。这意味着在设计的过程中，要十分仔细地设计存储器高速缓存。由于亿阳网警 BOCO.SFW-5000 防火墙旨在为大型用户群提供服务，所以有必要配置相应规模的资源容量。亿阳网警 BOCO.SFW-5000 防火墙 NPU 的内存资源可以实现 500,000 以上并发会话的会话信息和状态信息的本地储存。用于策略查找(处理每个数据包都要执行的关键步骤)的内存资源足以保存数千条策略，这使得亿阳网警 BOCO.SFW-5000 防火墙可在数千条策略的负荷下维持峰值全线速性能。

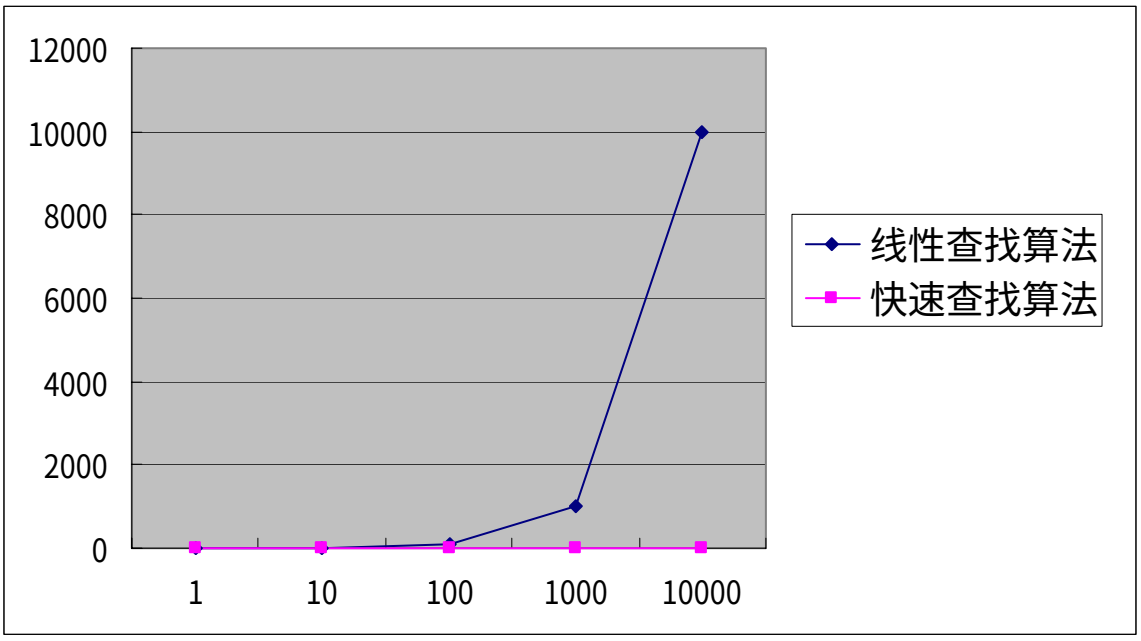
4.2 防火墙策略快速查找算法

亿阳网警 BOCO.SFW-5000 防火墙采用了先进的防火墙策略快速查找算法。传统的防火墙策略，即访问控制列表(ACL)，基于规则集合 (如源与目的地地址、协议、服务类型)及其它选项(如时间表等)来决定防火墙的行为。这样一来，防火墙引擎就必须顺序地搜索策略列表，来查找相匹配的策略。

随着安全策略数量的增加，防火墙性能就要大大降低。虽然采用更快的处理器或定制的 ASIC 可以减轻问题的影响，但到目前为止，仍然没有一个彻底的解决性能瓶颈的方案。

亿阳网警 BOCO.SFW-5000 防火墙采用的防火墙策略快速查找算法有效的降低了策略搜索的计算复杂度。图 2 显示了对于同样数目的策略，采用传统的线性搜索算法的设备上所需的查找次数与采用快速查找算法的亿阳网警 BOCO.SFW-5000 防火墙所需查找次数的比较，对比效果是明显的。

图 2—线性搜索与快速策略查找算法在不同数目规则下计算量的比较



此外，亿阳网警 BOCO.SFW-5000 防火墙还实现了动态会话缓存，这进一步提高了策略搜索速度。在整合了多网络处理器体系结构的固有高性能、专用系统总线、防火墙策略快速查找算法及动态会话缓存之后，亿阳网警 BOCO.SFW-5000 防火墙可以在加载数千条安全策略的情况下达到高达 1 千兆位全双工信息流量(一秒钟可以处理 2,960,000 多数据包)。

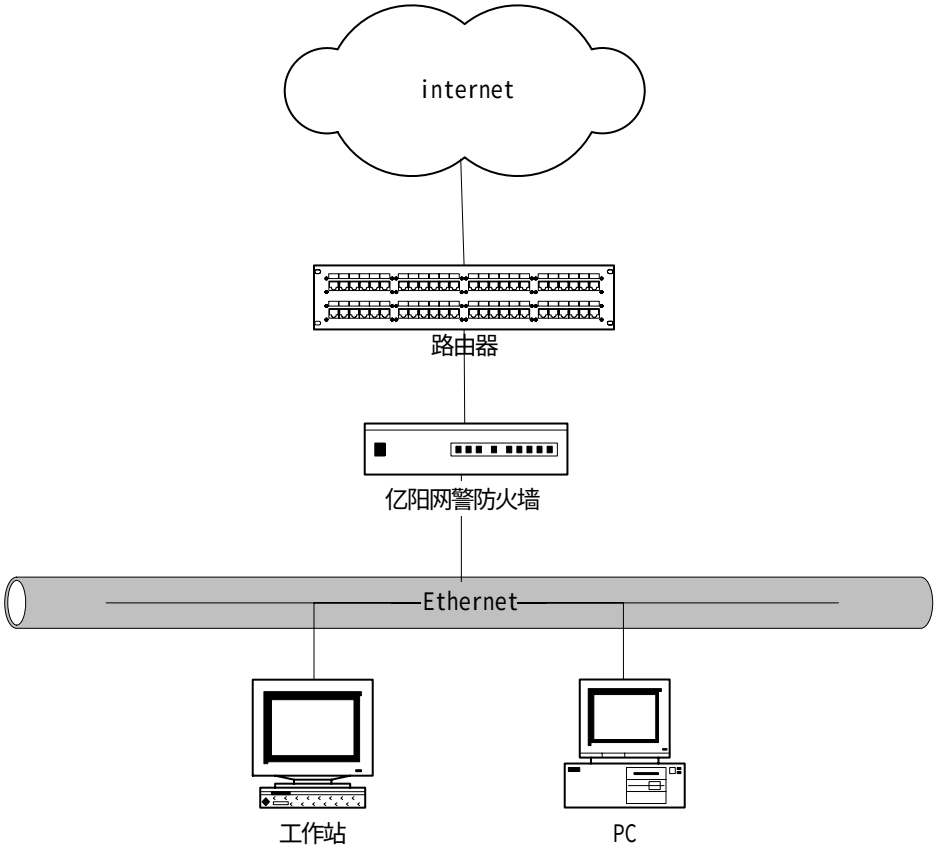
4.3 亿阳网警 BOCO.SFW-5000 防火墙的透明模式

透明模式提供了无须中断现有的网络地址或服务而无缝地接入防火墙并提供安全性的能力。

在透明模式下，亿阳网警 BOCO.SFW-5000 防火墙处于互联网网关路由器和内部网络之间。网络信息流通过亿阳网警 BOCO.SFW-5000 防火墙的外部端口从路由器进入亿阳网警 BOCO.SFW-5000 防火墙，检查通过后，再通过它的内部端口传送给内部网，无须重新映射子网。即使添加了新的虚拟防火墙，IT 管理员也不必重新配置现有网络的任何 IP 地址。

图 3 显示了亿阳网警 BOCO.SFW-5000 防火墙在路由器和内部网之间的位置。防火墙与路由器的内部网口以及内部主机属于同一网络。管理员通过受保护的内部管理端口管理亿阳网警 BOCO.SFW-5000 防火墙，而亿阳网警 BOCO.SFW-5000 防火墙背后的所有主机都受到了保护。

图 3—以透明模式保护内部网


internet
路由器
亿阳网警防火墙
Ethernet
工作站
PC

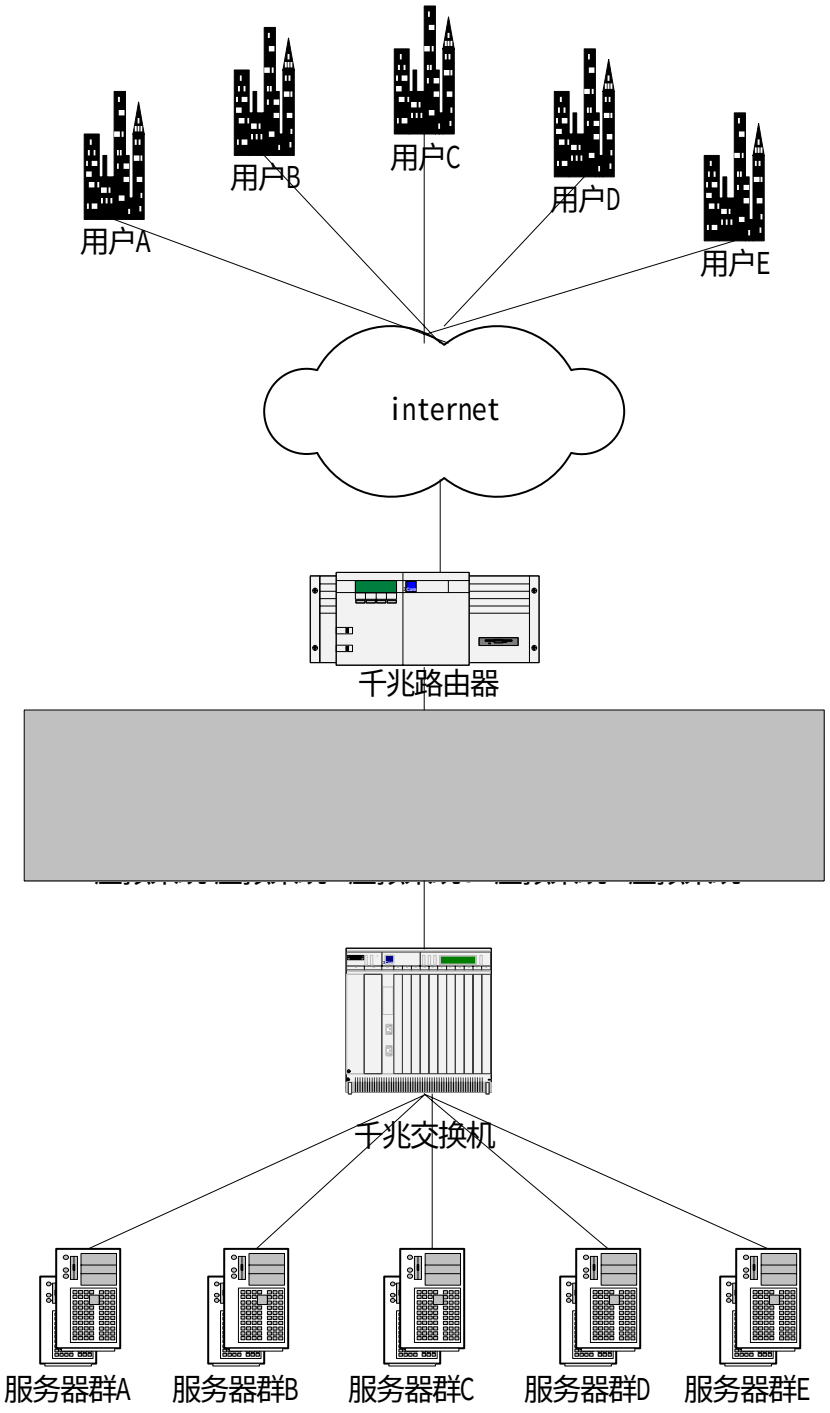
4.2 亿阳网警 BOCO.SFW-5000 防火墙的虚拟系统

亿阳网警BOCO.SFW-5000防火墙提供了多达50个独立的安全域，即虚拟系统，足以满足托管安全服务提供商及拥有多个部门和分部的企业的需求。虚拟系统可以使用户在一个防火墙设备中配置了多个逻辑上独立的防火墙。它为用户群提供了独立的安全支持，我们可以通过一个给定的 VLAN 编号或一个已配置好的 IP 地址序列来配置管理逻辑的防火墙。这样一来，就可以可供多个独立的实体（每一实体都有专门定义的、独立的及私有的安全需求）共享。

亿阳网警 BOCO.SFW-5000 防火墙为每一个用户群都提供了一个独立的、支持他们的私有虚拟系统的管理接口。在浏览器的地址栏中输入虚拟系统各自的 IP 地址，就可以管理该用户群的虚拟系统的各项参数及配置。

虚拟系统可以配置为透明模式或 NAT/路由模式。根据配置，来自公共 Internet 的信息将被导向由 IP 目的地址或 VLAN 编号所决定的相应的虚拟系统。对于从私有网络传送到公共网络的信息，根据数据包的源 IP 地址或 VLAN 编号，启用相应的虚拟防火墙策略。

图 4— 亿阳网警 BOCO.SFW-5000 防火墙在共享环境中保护客户服务器群：



具有多个虚拟系统的亿阳网警防火墙

4.5 冗余及可靠性

亿阳网警 BOCO.SFW-5000 防火墙是为服务提供商和大型企业无中断网络环境设计的。在亿阳网警 BOCO.SFW-5000 防火墙中，实现了部件级冗余设计。亿阳网警 BOCO.SFW-5000 防火墙的底层配置是双处理器结构，在任何一个处理器发生故障时，另一个都可以接管它的工作。亿阳网警 BOCO.SFW-5000 防火墙还融合了双热插拔电源、冗余热插拔风扇单元、及直流电源选项，确保为用户提供目前同类产品中最好的服务质量。亿阳网警 BOCO.SFW-5000 防火墙还可以设置为高可用性模式：亿阳网警 BOCO.SFW-5000 防火墙的其它特性还有：

- 冗余式 GBIC 输入/输出端口，在主接口发生物理链路上的故障时，能自动切换到从接口上。
- 可热插拔风扇盘
- 确保系统可靠性的 RAID-1 磁盘镜像，如果其中一个磁盘出现问题，可从另一个磁盘起动系统，并保持所有配置不变。

4.6 高可用性模式

为了获得最高的容错性能，我们可以把亿阳网警 BOCO.SFW-5000 防火墙配置为冗余的、高可用性（HA）模式。在高可用性模式下，在两个亿阳网警 BOCO.SFW-5000 防火墙设备之间由一条专用网线和管理口来广播“心跳”，确保在系统或网络出了故障时能够及时发现并进行快速恢复。请注意，对于相邻的路由器而言，亿阳网警 BOCO.SFW-5000 防火墙是透明的。

在 HA 模式下，两台亿阳网警 BOCO.SFW-5000 防火墙以镜像方式运行，但在任何时间，只有一台亿阳网警 BOCO.SFW-5000 防火墙处理活动的网络报文。一旦

相邻设备出了故障，备用设备将继续处理网络报文（它一直被系统所同步，因此保持了会话信息）。

如果在备用设备被激活的过程中发生了“ 心跳 ”的丢失，工作的亿阳网警 BOCO.SFW-5000 防火墙就会给系统管理员发送报警 email，指示可能由于备用亿阳网警 BOCO.SFW-5000 防火墙系统故障或连接故障导致了“ 心跳 ”的丢失。如果工作的系统发生了“ 心跳 ”的丢失，备用亿阳网警 BOCO.SFW-5000 防火墙就假定活动的亿阳网警 BOCO.SFW-5000 防火墙发生了系统故障，而激活自身。新的处于激活状态的亿阳网警 BOCO.SFW-5000 防火墙将恢复所有会话（在“ 心跳 ”故障发生之前，会话已经从工作的亿阳网警 BOCO.SFW-5000 防火墙映射到了备用亿阳网警 BOCO.SFW-5000 防火墙），从而保证了无缝故障恢复。

4 亿阳网警 BOCO.SFW-5000 防火墙的功能介绍

亿阳网警 BOCO.SFW-5000 防火墙具有如下功能：

5.1 对象管理功能

对象化管理封装了防火墙的底层控制对象，使防火墙策略保持稳定。亿阳网警 BOCO．SFW－5000 防火墙对防火墙管理控制对象进行对象化管理，对象层的引入使防火墙策略对易变的底层控制对象保持稳定。

5.2 基于状态检测的包过滤

- 对 IP 包进行的过滤控制，控制项可以基于源 IP 地址、目的 IP 地址、协议类型（ICMP、TCP、UDP）、源 TCP/UDP 端口、目的 TCP/UDP 端口、TCP

报文标志、IP 分组选项域、ICMP 报文类型域和代码域、包通信的日期和时间（包括起始时间、终止时间、星期、日）等有效组合；

- 支持全状态检测包过滤技术；
- 支持对所有过滤的包进行日志记录；

5.3 地址转换与端口映射功能

NAT 将内部网中的私有 IP 地址转换为可以在外部网络（比如 Internet）上传输的合法 IP 地址。进入内部网络的报文会转换回可以在内部网络中传输的地址。它通过对外部网络隐藏内部 IP 地址的方式来提高网络私密性。

NAT 模式包括多个变化形态，包括动态 NAT、动态 PAT、反向 PAT 和 BiNAT，亿阳网警 BOCO.SFW-5000 防火墙支持所有形态。

5.3 网络时钟协议支持

网络时钟协议(NTP)运行管理员使亿阳网警 BOCO.SFW-5000 防火墙和标准 Internet 时钟服务器进行同步。

5.5 规则导入导出功能

规则的导出功能可以实现防火墙策略配置信息的异地备份。规则的导入功能将保存的安全策略复制到异常或新的防火墙上，这极大的方便了用户对安全策略的配置和管理。

5.6 远程升级功能

用户可以从亿阳集团网站（www.boco.com.cn）下载亿阳安全提供的防火墙升级

文件，并通过管理主机远程的对防火墙进行在线升级。利用此功能，用户可以随时更新亿阳网警防火墙系统的软件，及时拥有亿阳为您提供的各种新的安全功能。

5.7 虚拟系统功能

虚拟系统使一个防火墙设备可以配置多个逻辑上独立的防火墙。虚拟系统为用户群提供安全支持，而我们可以通过一个给定的 VLAN 编号或一个已配置好的 IP 地址序列来区分每一个虚拟系统。亿阳网警 BOCO.SFW-5000 防火墙提供了多达 50 个独立的虚拟系统。

5.8 路由管理功能

用户可以根据目的 IP 地址、掩 码、网络接口来定制防火墙的路由表。

5.9 SNMP 协议支持

NMP 选项允许 SNMP 管理员请求和接收表明网络状态的网络级消息。亿阳网警 BOCO.SFW-5000 防火墙可以配置为一个 SNMP 代理。在当前时间，亿阳网警 BOCO.SFW-5000 防火墙仅支持 SNMP 陷阱。

5.10 双机热备功能

实现了主从式双机热备功能，配置友好方便，对防火墙失效状态判断准确全面可靠，从机接管切换快，切换时不丢失当前的会话，真正做到无缝切换。

5.11 抗攻击功能

亿阳网警 BOCO.SFW-5000 防火墙可保护网络使其不会被未授权的用户访问，还可以防止网络级的攻击。WinNuke、ICMP Smurf、Fraggle、SYN Flood、Ping of Death、Teardrop、IP spoofing、IP 源路由、Land 和 UDP Flood 这些攻击行为都可以在到达网络之前被检测到并可以被阻止；还可以检测端口扫描和地址扫描等攻击行为。

5.12 系统状态显示功能

亿阳网警 BOCO.SFW-5000 防火墙具有硬件/系统状态页面，这样管理员就可以快速的确定可能影响亿阳网警 BOCO.SFW-5000 防火墙性能和可靠性的问题，还可以显示关键系统参数。

5.13 报警功能

可以发送报警邮件给一列指定的收件人。当指定的事件发生时， 亿阳网警 BOCO.SFW-5000 防火墙会把通知发送给那些所列出的收件人。

5.14 安全审计功能

从安全的角度讲，日志主要是起抗抵赖的作用，即防火墙记录了用户的网络使用情况，如果有人对网络进行了攻击或是有窃密的行为，事后我们有据可查。

5.15 网络测试功能

支持 Ping,Traceroute,DNS lookup 等网络测试工具。

5 亿阳网警 BOCO.SFW-5000 防火墙的安全性分析

目前，常见的黑客攻击手段主要有以下几类：利用守护进程的漏洞，利用远程过程调用的漏洞，拒绝服务，代理服务，IP 欺骗，网络端口扫描，SNMP 漏洞，系统信息搜集，缓冲区溢出等。

在对 BOCO.SFW-5000 防火墙进行的抗攻击性实验中，使用了北京北方计算机中心研制的网络安全性分析系统 Internet Security Explorer 3.0 和 Linux 下的 Nessus 共享软件对 BOCO.SFW-5000 防火墙进行了扫描和攻击实验。实验进行的项目及得到的测试结果如下表所示：

测试项目	测试结果	测试项目	测试结果
邮件服务	通过	网管协议	通过
强力攻击	通过	WINDOWSNT 服务	通过
守护进程	通过	NT 用户组/网络配置	通过
远程过程调用	通过	网络共享/DOCM	通过
网络文件系统	通过	NT 安全配置与审计	通过
拒绝服务	通过	WINDOWSNT 安全区	通过
NETBIOS 及其它	通过	文件传输协议	通过
WINDOWS 用户及其	通过	网络端口扫描	通过
WINDOWS NT 注册	通过	NT 信息搜集	通过
WINDOWS NT 口令	通过	系统信息搜集	通过
代理/域名服务系统	通过	特洛伊和后门程序检测	通过
WWW,HTTP,CGI	通过	FIREWALL	通过

IP 欺骗	通过	浏览器	通过

6 亿阳网警 BOCO.SFW-5000 防火墙的参数指标

6.1 亿阳网警 BOCO.SFW-5000 防火墙的物理参数

输入电压：220V

有效功率：200W

网络接口：千兆网络接口 4 个（两两备份）

百兆网络接口 2 个(用于管理和双击热备份)

配置用 Console 口：RS232。

正常工作温度：-5~50ºC

6.2 亿阳网警 BOCO.SFW-5000 防火墙的性能指标

双向吞吐率：64 字节帧长的条件下为线速的 80%(800Mbps/sec)。128 以上字节帧长的条件下均达到或接近线速的 100%。

时延：16μs

丢包率：0。

最大会话连接数：100 万

虚拟防火墙数目：50 个(可扩充)