Netpower

安 · 全 · 信 赖

网威网络入侵检测系统

技术白皮书

北京中科网威信息技术有限公司

版权声明

本文档为阶段性更新文档，如有新版本改动，恕不另行通知。您欲取得最新的网威网络入侵检测系统资料，敬请访问中科网威公司网站：
http://www.netpower.com.cn
或联系：netpower@netpower.com.cn
5*8 小时技术热线： 010-82333399-168
7*24 小时支持热线：13601085408

北京中科网威信息技术有限公司
Beijing Netpower Technologies Inc.
北京市海淀区学院路 35 号世宁大厦 9 层（100083）
Rm903，Shining Building，35 Xueyuan Rd，Haidian，Beijing
电话（TEL）：86-10-82333399
传真（FAX）：86-10-82318600

目 录

一、系统简介

“网威”网络入侵检测系统是采用北京中科网威信息技术有限公司积累多年的安全产品开发经验，在充分调研国内外相关产品和精心准备的基础上独立开发的一款基于网络的实时入侵检测及响应系统。

“网威”系列产品在产品的检测能力、响应能力以及系统自身的保护能力等方面都进行了精心的设计。该系统作为防火墙的重要补充，与防火墙组成动态防御、预警系统，它能够监视 10M/100M/1000M 局域以太网上传输的所有网络数据信息，根据用户指定的保护目标及检测策略对网络上传输的数据进行深度分析，当可疑行为或攻击行为发生时立即产生警报，同时根据用户需要能采取多种响应措施，包括立即切断连接会话、重新配置防火墙、发送 SNMP Trap 消息、发送电子邮件等。

系统采用引擎/控制台结构，网络引擎（以专用硬件形式提供）部署于网络中各个关键点，通过网络和中央控制台（运行于 Windows 平台）交换信息。网络引擎软件部分运行于安全操作系统之上，负责网络数据的获取、分析、检测，对警报进行过滤和实时响应，并发送给控制台进行显示和记录；控制台负责警报信息的实时显示、记录、查阅等，并支持用户定制检测、响应策略和控制网络引擎。

二、主要功能

“网威”网络入侵检测系统具备一般网络入侵检测系统的主要功能，同时针对网络入侵检测系统面临的威胁和网络入侵检测系统发展方向开发出多项具有针对性的新功能，此外该系统对于国内外流行的防火墙（包括中科网威“网威”防火墙、天融信、CheckPoint、东软 NetEye、亿阳信通、联想等防火墙）提供互动接口，具有较完备的检测、响应、互动能力，是一款高效实用的入侵防范工具，它的具体功能如下：

2.1 引擎集中管理功能

管理员在中央控制台可以直接控制各个引擎的行为，包括启动、停止、添加、删除引擎，也可以查看、删除、查询引擎的实时警报，修改引擎的检测和响应策略。此外，在必要的时候用户还可以通过串口连接引擎主机，通过专用界面对引擎进行控制，包括启动、停止、查看/设置网络接口状态、查看引擎运行状态以及系统维护等。

2.2 策略管理功能

策略管理功能为用户提供了一个根据不同网络的安全需要，灵活配置安全策略的功能。网络管理员可以利用策略管理功能，轻松地针对特定的引擎定制策略，以满足不同的网络的安全要求。同时支持用户自定义规则，用户可定制自有网络的专有策略。网络管理员还可以通过“策略配置”菜单，方便地对已经制定的策略进行过滤策略，自定义策略，响应方式以及响应对象的修改。

同时，策略管理功能还向用户提供了入侵检测规则的扩充能力，网络管理员可以根据自己需要定制入侵检测规则，直接应用于网络引擎，很快实现网络管理员的安全意图。

2.3 实时入侵检测功能

能实时识别各种基于网络的攻击及其变形，包括 DOS 攻击、WEB 攻击、溢出攻击、后门探测等。检测攻击或者可疑行为是一般入侵检测系统的必要功能，但是大多存在着误报率和漏报率较高的问题，“网威”网络入侵检测系统使用深入的应用层协议分析技术和正

则表达式技术，极大的降低了误报率和漏报率，使得大量使用“安全扫描”类的黑客工具进行的变形攻击毫无效果，同时去除了干扰，减轻了检测引擎的工作压力，提高性能，更适用于大流量的网络环境。目前可以检测 29 大类，1800 余种攻击行为及其变形。

2.4 警报过滤功能

能根据定制的条件，过滤重复警报事件，减轻传输与响应的压力，同时还能保证警报信息不被遗漏。它能够明显缓解目前针对网络入侵检测系统的 DOS 攻击,使得系统能够高效稳定的工作。

通过报警插件的显示排序功能，可有效针对当前的警报状态，监控某些事件类型触发频率，通过查找攻击主机和被攻击主机，采取相关防护措施或补救手段。

2.5 实时响应功能

根据用户定义，警报事件在经过系统过滤后进行及时响应，包括实时切断连接会话、重新配置防火墙，彻底屏蔽攻击、给管理员发送电子邮件、发送 SNMP Trap 报警、控制台实时显示、数据库记录等等。

2.6 防火墙互动开放接口－OpenIDS

为了提高网络安全产品之间协同工作、动态防护的互操作性，中科网威提供了 IDS 与防火墙互动的开放接口—OpenIDS。通过 OpenIDS，可以根据设定好的阻断时间和阻断方式，通知防火墙，进行相应 IP 地址、协议端口的阻断。

OpenIDS 现提供两种接口方式：开发包和可运行的 Agent (目前支持 Linux)，不需要防火墙厂商进行二次开发。

目前可以和“网威”网络入侵检测系统实现互动的防火墙有包括：中科网威“网威”防火墙、联想“网御”防火墙、亿阳信通“网警”防火墙、东软“网眼”防火墙、CheckPoint FireWall-1 和天融信防火墙等。

2.7 报表统计和数据库维护功能

“网威”网络入侵检测系统提供了非常简便的入侵警报统计和报表工具。用户可以根据各种可选条件，例如：引发报警数据包的源 IP 地址、目的 IP 地址、源端口号、目的端口号、警报产生的时间、危险级别等等，使用单一条件或者复合条件进行查询。当警报信息数量大、信息来源广泛的时候，网络管理员可以很轻松的对警报信息进行分类，从而着重显示网络管理员所需要的信息。通过报表提供的统计模板统计相关报警事件的攻击次数及其趋势，确定事件等级及其采取相关措施，通过查阅事件安全建议采取防护措施。启动报表守护进程功能可达到报表统计资料的定期汇总和导出，使网络管理员的网络安全报告更直观、清晰。

控制台程序长时间工作后会产生大量的冗余信息，通过压缩数据库，可以使数据库变得更精简，使系统工作效率更高，更稳定。当数据库达到一定大小的时候，通过“网威”网络入侵检测系统的历史数据维护程序，网络管理员可以根据自己的需要导出某一个确切时间范围内的数据，进行备份。数据导入功能则可以将备份的数据导入程序数据库，来查看历史警报信息。另外，为了方便数据库的维护，通过设定数据库的导出条件，控制台可以定期导出符合条件的报警信息，进行备份。

2.8 强大的策略模板管理功能

系统默认提供最大检测集模板、最小检测集模板、中强度检测集模板、标准检测集模板、Windows 检测集模板、Linux 检测集模板，共六种模板。并且支持用户自定义模板，允许用户将自己定义的模板和系统的模板进行导入导出操作。

2.9 提供大型数据库转换支持

控制台允许用户将警报的信息改用大型数据库来存取、管理，如 MS SQL Server 等。

2.10 策略库的在线升级、本地升级支持

系统支持在线远程升级策略库， 同时为不能接入互联网的用户提供升级文件，进行本地升级。策略库的升级可以保证入侵检测系统能检测最新出现的攻击。

2.11 协议分析还原功能

“网络协议分析监听系统”是网威网络入侵检测系统附带的安全工具之一。“网络协议分析监听系统”获取网络中的数据包，对所关心协议的数据进行进一步处理，在应用层进行还原，使用户能够轻松的监视网络中的各种异常行为。目前，“网络协议分析监听系统”支持的协议有 7 种：FTP、HTTP、SMTP、POP3、MSN、YAHOO Messager、Telnet。用户可以根据自己网络的特征，过滤一些自己不需要还原的协议，也可以同时对这 7 种协议进行还原；并且可以根据数据包的源地址、目的地址、方向进行过滤，增加了灵活性。

“网络协议分析监听系统”提供了友好的分析查询界面，在分析查询界面中可以实时的显示各个协议的还原内容，用户可以在分析查询界面中看到非常丰富的还原信息，如：时间、源地址、目的地址，除了这些基本的信息外，每种协议还提供了其特有的信息。下面分别介绍几种重要协议的还原内容。

HTTP：可以显示出时间、URL、模式(如：GET、POST)、主机、源地址、目的地址，双击该还原信息可以显示出整个网页的内容。

SMTP：可以显示出时间、发件人、发件 Email 地址、收件人、收件 Email 地址、主题、类型、尺寸，双击该还原信息可以显示出整个邮件的内容。

FTP：可以显示出时间、类型(如：GET、PUT)、源地址、目的地址、文件名、用户、口令。

2.12 流量统计

流量统计是网威网络入侵检测系统附带的安全工具之一。它通过抓取网络中的数据包，并通过用户设置的 IP 地址，对数据包进行过滤，然后将用户所关心的数据包进行统计，计算出网络中的数据流量，并对流量进行分类统计，使用户可以更为详细的了解网络中的流量变化，发现网络中的异常。

用户可以设置所要检测的 IP 地址，可以单一的添加，也可以指定一个 IP 范围进行添加。流量统计界面中会实时的显示出用户所关心的 IP 的流量信息，如果用户设置了端口，还可以显示出特定端口的流量。所有流量的数据均以数字和图形两种形式进行显示，在图形显示界面中我们可以根据协议类型、流量单位、流量方向查看不同的流量图形，并且可以在 3D 图形和平面图形间进行切换。

2.13 引擎状态监控

网威网络入侵检测系统控制台提供了查看引擎状态的功能，我们可以观察引擎当前各网卡的网络流量，CPU 使用率以及内存使用情况，这些信息均通过数字和图形两种方式进行显示，使用户查看更加直观方便。

三、主要特点

3.1 引擎稳定高效

网络引擎软件由三个部分组成：引擎管理、数据获取与检测、警报过滤与响应，保证了网络数据处理和警报处理相对独立，不致阻塞；引擎管理代码逻辑简单，能保证长时间稳定运行，同时保证其他两部分稳定工作，确保网络引擎整体 24 小时不间断工作。各个数据处理单元间采用多级缓冲设计，确保高带宽下数据不致丢失。

3.2 支持灵活的系统部署

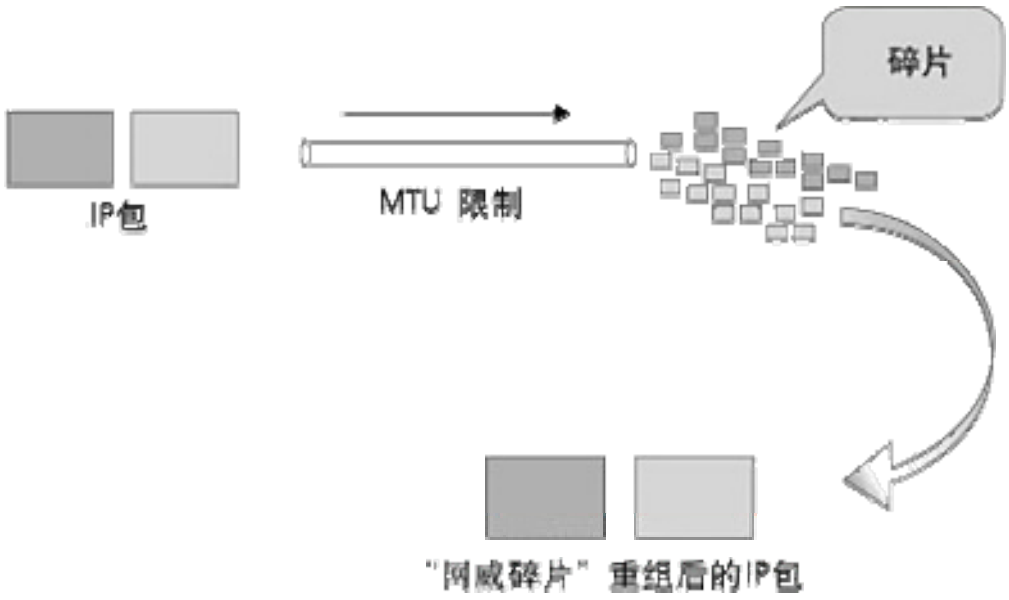
系统支持控制台同时作为客户端和服务器两种通讯模式（即同时从一个网络引擎拉数据和向另外一个引擎推数据），这使得网络引擎和控制台的部署可以满足复杂网络拓扑的实际需求。对于隐藏本地 IP 地址的多网段大型网络环境，可以把控制台置于内部网络，而把网络引擎部署到网络中的任意位置。此外，在骨干网实际带宽很高的情况下，用户可以根据地址、协议、应用类型等条件配置数据获取策略，同时部署多个网络引擎确保充分检测网络数据，使得保护对象更加明确具体，提高引擎运行效率。

3.3 更低的误报率和漏报率

系统采用领先的基于应用层协议分析的入侵检测技术，根据各种典型应用的具体协议对网络数据进行分析、检测，能够识别各种伪装或变形的攻击，极大的降低了漏报率和误报率。

在详细的协议分析的基础上，采用重组还原技术判断碎片攻击，很多黑客通过对 IP 包进行分片的方式来逃避 IDS 的检测：将一个完整的攻击请求分成几个步骤发出去，常规的网络入侵检测系统是根据每个单独的数据包进行匹配判断的，这样就不能检测到一个完整的攻击请求，从而造成漏报。“网威”网络入侵检测系统在每次匹配之前，先判断数据包是否为分片包，如果是，则根据协议规则先进行重组，使本次的请求还原到一个完整的数据包状态再进行检测。

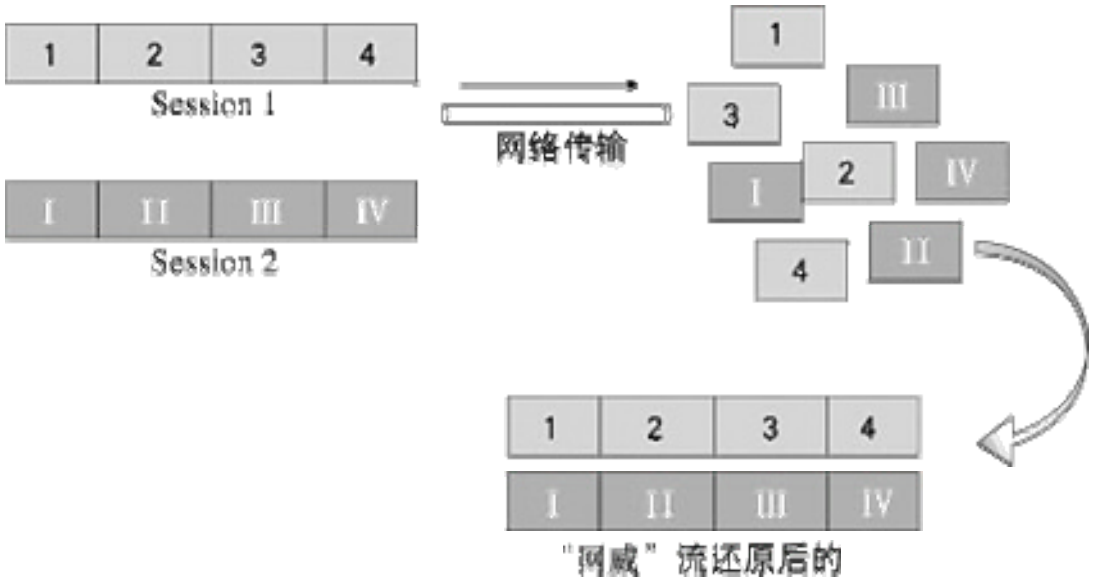
IP 数据包分片和重组过程如下图所示：图中两个 IP 数据包，在传输过程中，由于网络 MTU 的限制，会被分成不同的碎片进行传输；在“网威”入侵检测系统的引擎上会被还原为原始包，然后再进行匹配检测。



3-1 “网威”网络入侵检测系统碎片重组示意图

同时，对于基于连接数据记录每一次的会话，使那些上下文相关的入侵行为无处躲藏，即一次可疑行为的产生需要两个相关联的数据包共同来完成，常规的网络入侵检测系统只判断单一的数据包，从而会产生漏报。“网威”网络入侵检测系统会记录每一次会话的全过程，使检测数据范围更广，检测更严谨。

TCP 数据流还原过程如下图所示：图中分别描述两个连接的数据包：Session 1 和 Session 2，每个连接中都有多个数据包需要传递。数据在网络传输过程中，可能会按照不同的路由到达目的地，顺序有了很大变化。当到达“网威”入侵检测系统的引擎后，会经过流重组模块使其还原为原始数据流状态，即按照数据包的标志，重新组合为 Session 1 和 Session 2 的状态，然后在此基础上进行检测，进而提高检测的准确性。



3-2 “网威”网络入侵检测系统流还原示意图

此外，我们在应用层针对特殊服务做了特殊编码还原/协议分析处理，使一些 IDS 逃避攻击、特殊编码变形等攻击无处躲藏。

3.4 增强的抗攻击能力

系统能够防御针对 IDS 的拒绝服务攻击，采用的重复事件过滤技术和其他监控手段，使得对 IDS 的 DOS 攻击的冲击降到最低。同时对于网络中断等异常情况采用了智能控制技术，确保引擎稳定运行，警报不致丢失，当网络通讯恢复后能够及时显示。

3.5 系统自身安全性更强

网络引擎运行于安全操作系统并经过严格配置。网络引擎具备管理微内核，采用双网卡（获取数据网卡无 IP）工作方式，通讯支持认证和加密，确保系统的安全。

3.6 强大的攻击识别能力

具备更强的攻击识别能力，采用领先的基于应用层的协议分析入侵检测技术，根据各种典型应用的具体协议结果进行检测，能够识别各种伪装或变形的攻击。

3.7 千兆入侵检测

随着宽带网络的普及应用，千兆环境下的入侵检测已经日益受到重视。中科网威通过长期的技术积累，开发出能够运行于千兆网络环境下的千兆入侵检测系统。该系统通过对操作系统的调整、驱动优化和检测算法的优化，提高了检测的效率，完全能够满足千兆环境下的流量要求。

3.8 网络蠕虫防御版

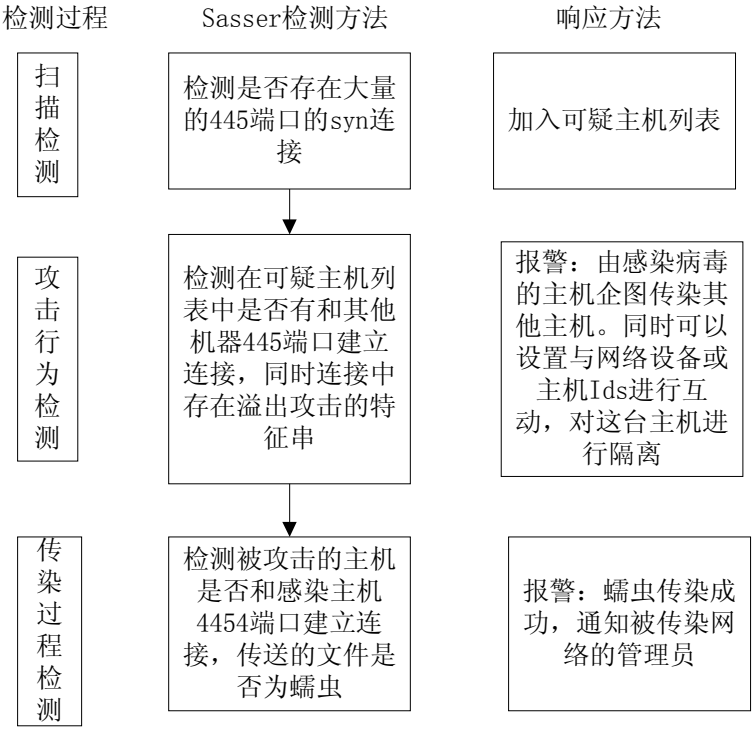
在当前的网络环境中，网络蠕虫带来的危害日益升高，仅 2003 年一年，网络蠕虫就给全世界造成了几百亿的损失。在安全领域，对网络蠕虫的发现和防御，也越来越被重视。中科网威通过多年在安全方面的积累，开发研制了入侵检测系统的一个分支，网络入侵检测-网络蠕虫防御版。

网络蠕虫防御版在网威原有的入侵检测系统基础上，加强了蠕虫的行为检测功能，同时利用异常检测技术对 0-Day 蠕虫进行预警。网络蠕虫防御版提供多种方法同网络设备和网络管理软件进行互动，起到阻止蠕虫传播的作用，同时便于网络管理员对网络蠕虫进行查杀。网络蠕虫防御版主要功能如下：

已知蠕虫检测功能：目前的市场上的蠕虫检测产品对蠕虫的检测基本是针对蠕虫的特征码进行匹配。由于网络的复杂性，这种方法导致了大量的漏报和误报。

中科网威入侵检测网络蠕虫防御版使用编译技术结合虚拟机技术，创建了网威的脚本语言 NPDCL（网威检测控制语言）。根据当前流行的蠕虫的行为和蠕虫引发的网络异常情况，制定了针对蠕虫行为的检测脚本，可以准确地发现蠕虫及其相关变种。

就当前比较流行的震荡波蠕虫为例，它的传播可分为三个过程。第一步震荡波蠕虫按一定算法随机生成 IP 地址，进行扫描。如果发现对方主机开放 445 端口，第二步就是利用对方主机存在的漏洞进行溢出攻击，得到系统的 Root 权限。第三步从已感染主机的 4454 端口通过 FTP 服务下载到被感染主机并运行。在我们的检测过程中，当我们发现主机意图连接 445 端口时，我们记录这次连接的原 IP 地址，如果一个 IP 地址在一个时间段内，多次连接其他多台不同的主机时，我们进行统计，如果超过一定的域值，控制台显示可疑主机，并将主机加入到可疑主机列表。具体行为见下图：



这种根据蠕虫行为的检测，可以对蠕虫的各个阶段的行为产生不同的报警，为网络管理员提供不同的处理方法，可以最大限度的限制蠕虫传播。

0-Day 蠕虫预警功能：对 0-Day 蠕虫(未知蠕虫)的检测，是当前蠕虫检测产品面临的最大难题。中科网威通过多年的网络安全技术积累和对网络蠕虫的研究，总结了蠕虫在网络中传播所引起的网络异常。通过分析监控网络流量，服务，各种协议数据包等信息。发现网络中因蠕虫存在而引起的异常变化，从而发现网络中存在的未知蠕虫。

网威入侵检测蠕虫防御版通过对网络中的数据进行采集，分析，发现网络中的异常行为。如：某单独 IP 向多个不同 IP 的相同端口进行扫描，网络中存在大量的 TCP 不成功连接,短时间内向邮件服务器发送大量的信件，HTTP 服务器访问中出现危险的 URI，Windows 网络用户名和密码猜测，Windows 网络写共享访问，ARP 异常，ICMP 异常，HTTP 服务访问异常等。蠕虫防御版提供异常自定义功能，对一般用户提供异常策略配置向导。同时高级用户可以针对自身网络中的情况，使用 NPDCL 语言，进行网络异常的重新定义和扩展。

蠕虫防御功能：当蠕虫被发现时，中科网威入侵检测系统蠕虫防御版将会在尽量短的时间内对其进行响应。首先产生报警，通知管理员，并通过防火墙、路由器、或者 HIDS 的互动将感染了蠕虫的主机隔离；然后对蠕虫进行分析，进一步制定检测策略，尽早对整个系统存在的安全隐患进行修补。系统同时提供对蠕虫发现有帮助的工具和指导方法，有

助于用户发现和移除蠕虫。

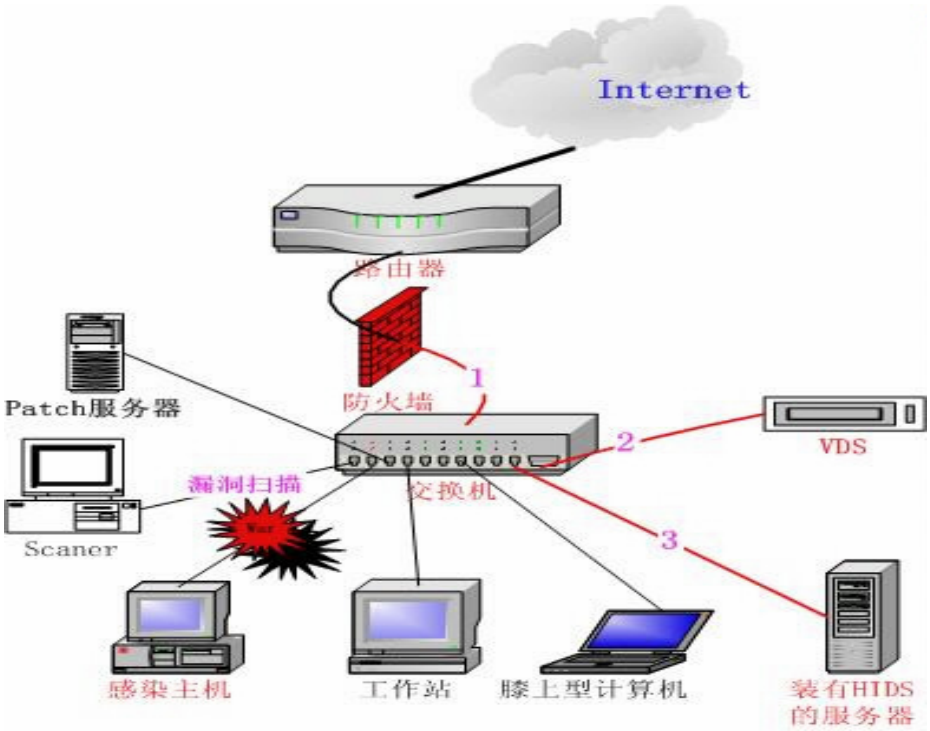


图 3-3 网威入侵检测系统蠕虫防御版的响应图

如图 3-3 所示，中科网威入侵检测系统蠕虫防御版发现感染了蠕虫的主机时，可以通过如下方式进行响应：

- 防火墙联动：通过控制防火墙的策略，对感染主机的对外访问数据进行控制，防止蠕虫对外部网络的主机进行感染。如果入侵检测系统蠕虫防御版发现外部网络存在的蠕虫对用户内部网络进行扫描和攻击，也通过和防火墙进行联动，防止外部网络的蠕虫传染内部网络的主机。
- 交换机联动：中科网威入侵检测系统蠕虫防御版支持和 CISCO 系列的交换机通过 SNMP 协议进行联动，当发现用户内部网络的主机被蠕虫感染时，可以切断感染主机同内部网络的其他主机的通讯，防止感染主机在内部网络的大肆传播，同时可以控制因为蠕虫发作而产生的大量的网络异常流量。为了适应用户的网络环境，我们还提供了 Telnet 配置网络设备的接口，系统可以和用户网络中任何支持 Telnet 管理的网络设备进行联动。
- 通知 HIDS：装有 HIDS 的服务器接收到蠕虫防御版传来的信息，对可疑主机的访问进行阻断，以阻止受感染主机对服务器进行感染，从而保护服务器上重要资源

免受损坏。

- 报警：产生报警，通知网络管理员。当管理员对蠕虫进行分析后，可以通过配置 Scanner 来对网络进行漏洞扫描，并通知存在漏洞的主机到 Patch 服务器下载相关的补丁进行漏洞修复，防治蠕虫进一步传播。

四、产品型号

根据不同的网络规模和性能要求,“网威”网络入侵检测系统提供了两个型号产品，分别为百兆和千兆网络环境设计。同时为了加强网络入侵检测在防范网络蠕虫方面的功能，还推出了蠕虫防御版。

4.1 百兆网络入侵检测系统

适用于 10/100M 网络类型，结构简单，配置方便。

网络引擎：以专用硬件直接提供。

产品配置：

硬件规格：

材料：采用工业级的 CPU 主机板，高强度钢壳结构

尺寸（长×宽×高）：460mm×430mm×44mm

重量：9.5 千克

工作温度：5~50℃

工作湿度：10~95%·40℃，非浓缩

外设接口：

一个 Console 口

三个 10/100Base-TX 接口（可扩展到八个）

一个 220V/50HZ 电源插座

一个电源开关

处理器：Intel Pentium III 处理器

内存：256MB（可扩充）

电源：输出功率：250 瓦特（最大）

控制台：软件

软件环境：

中文版 Windows NT、Windows2000 或更高的版本

正确配置的 TCP/IP 网络，要求安装运行用户具备管理员权限。

硬件环境：

PII 300 或更高主频的 PC 计算机

128MB 或更高容量的内存

2GB 以上空余硬盘空间

4.2 千兆网络入侵检测系统

高配置、高性能、易用方便，适用于需要进行大量数据处理和交换的网络环境。

网络引擎：以专用硬件直接提供。

产品配置：

硬件规格：

材料：采用工业级主机板，高强度钢壳结构

尺寸（长×宽×高）：460mm×430mm×86mm

重量：16.5 千克

工作温度：5~50℃

工作湿度：10~95%·40℃，非浓缩

外设接口：

一个 Console 口

两个千兆接口（铜缆或单模、多模光纤）（可扩展到四个）

两个 10/100Base-TX 接口（可扩展到八个）

220V/50HZ 热备份双电源

一个电源开关

处理器：双 CPU，Intel Pentium III 处理器

内存：512MB（可扩充）

电源：输出功率：250 瓦特（最大）

控制台：软件

软件环境：

中文版 Windows NT、Windows2000 或更高的版本

正确配置的 TCP/IP 网络，要求安装运行用户具备管理员权限。

硬件环境：

PII 300 或更高主频的 PC 计算机

128MB 或更高容量的内存

2GB 以上空余硬盘空间

4.3 蠕虫防御版

提供对网络中蠕虫的发现和防御功能，通过异常检测和行为特征检测的方法对蠕虫进行准确的监测。

网络引擎：以专用硬件直接提供。

产品配置：

硬件规格：

材料：采用工业级主机板，高强度钢壳结构

尺寸（长×宽×高）：460mm×430mm×86mm

重量：16.5 千克

工作温度：5~50℃

工作湿度：10~95%·40℃，非浓缩

外设接口：

一个 Console

两个 10/100Base-TX 接口（可扩展到八个）

220V/50HZ 热备份双电源

一个电源开关

处理器：双 CPU，Intel Pentium III 处理器

内存：512MB（可扩充）

电源：输出功率：250 瓦特（最大）

控制台：软件

软件环境：

中文版 Windows NT、Windows2000 或更高的版本

正确配置的 TCP/IP 网络，要求安装运行用户具备管理员权限。

硬件环境：

PII 300 或更高主频的 PC 计算机

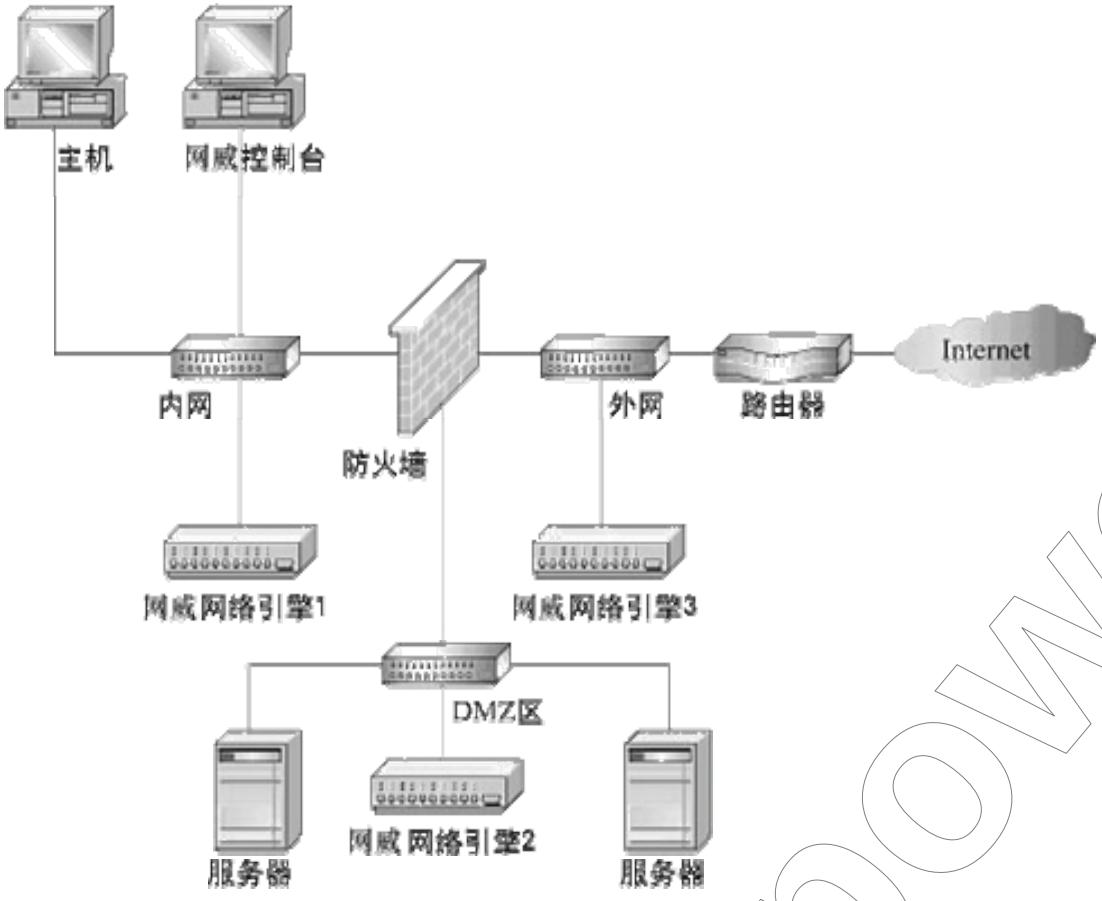
128MB 或更高容量的内存

2GB 以上空余硬盘空间

五、应用实例

5.1 单一内网环境

这个应用方案中， 在一个典型的网络环境中部署了三个网络引擎。DMZ 区和外网中的网络引擎以被动方式运行（即控制台主机主动发起连接从中“拉”数据），而网络引擎 1 既可以配置为主动方式，也可以配置为被动方式。控制台主机可以同时监控位于三个不同区域网络引擎的状态并处理传送回来的实时信息。

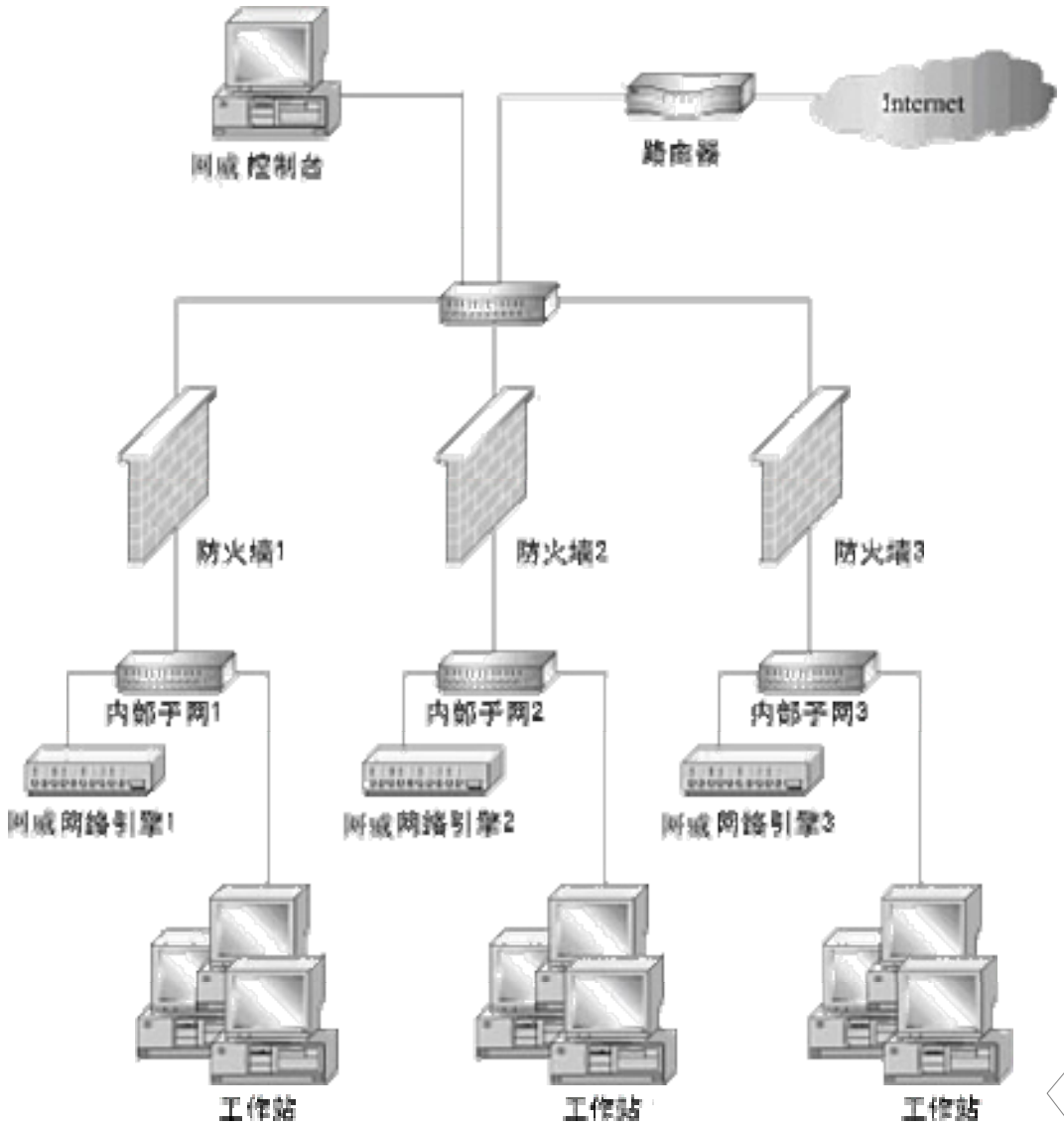


5－1“网威”网络入侵检测系统单一内网环境部署示意图

5.2 多内网环境

这个应用方案中，每个内部子网通过单独的防火墙与外网连接，控制台主机位于公开

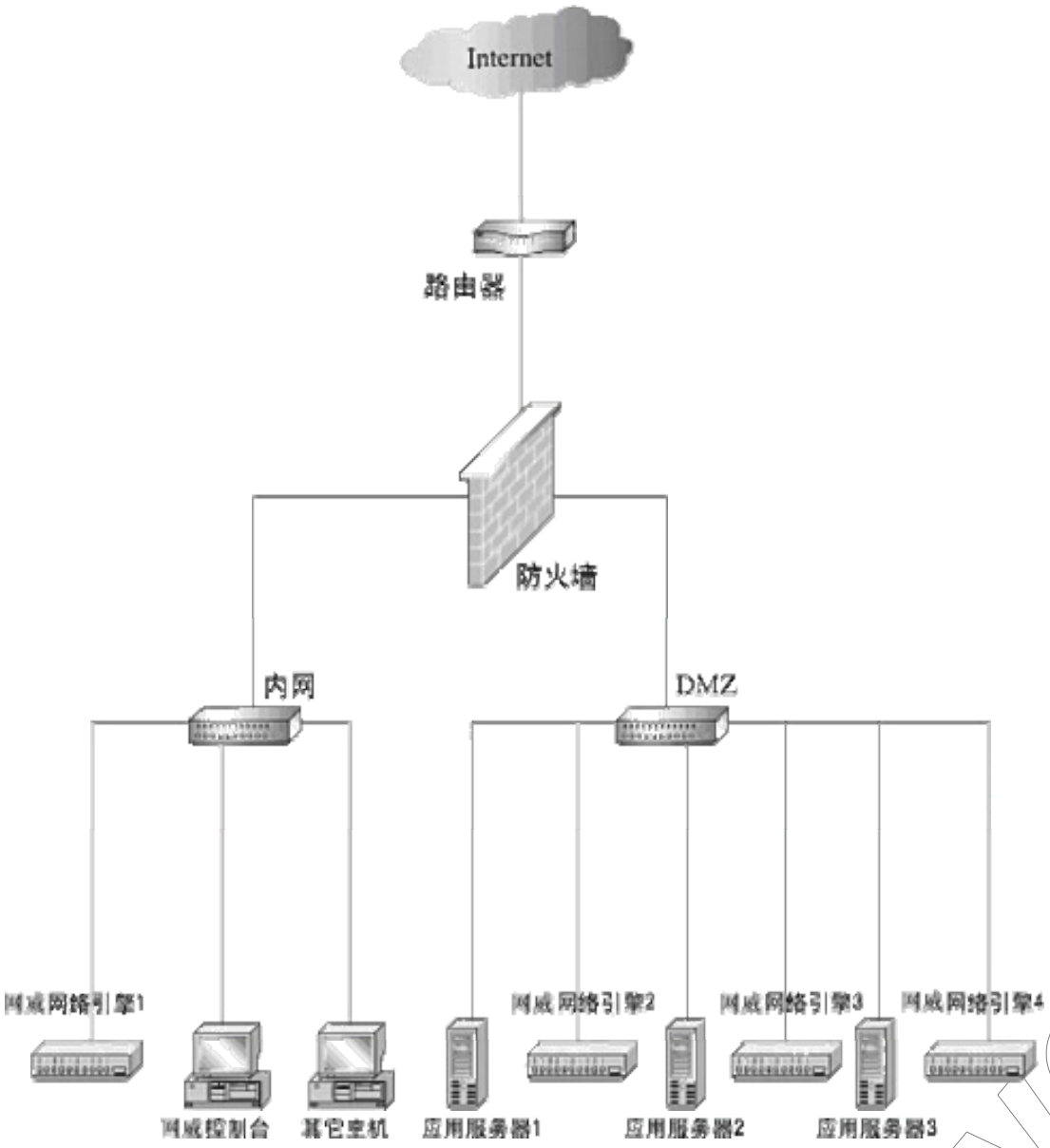
网段，它可以监控位于各个内网的网络引擎。



5－2“网威”网络入侵检测系统多内网环境部署示意图

5.3 重点监控

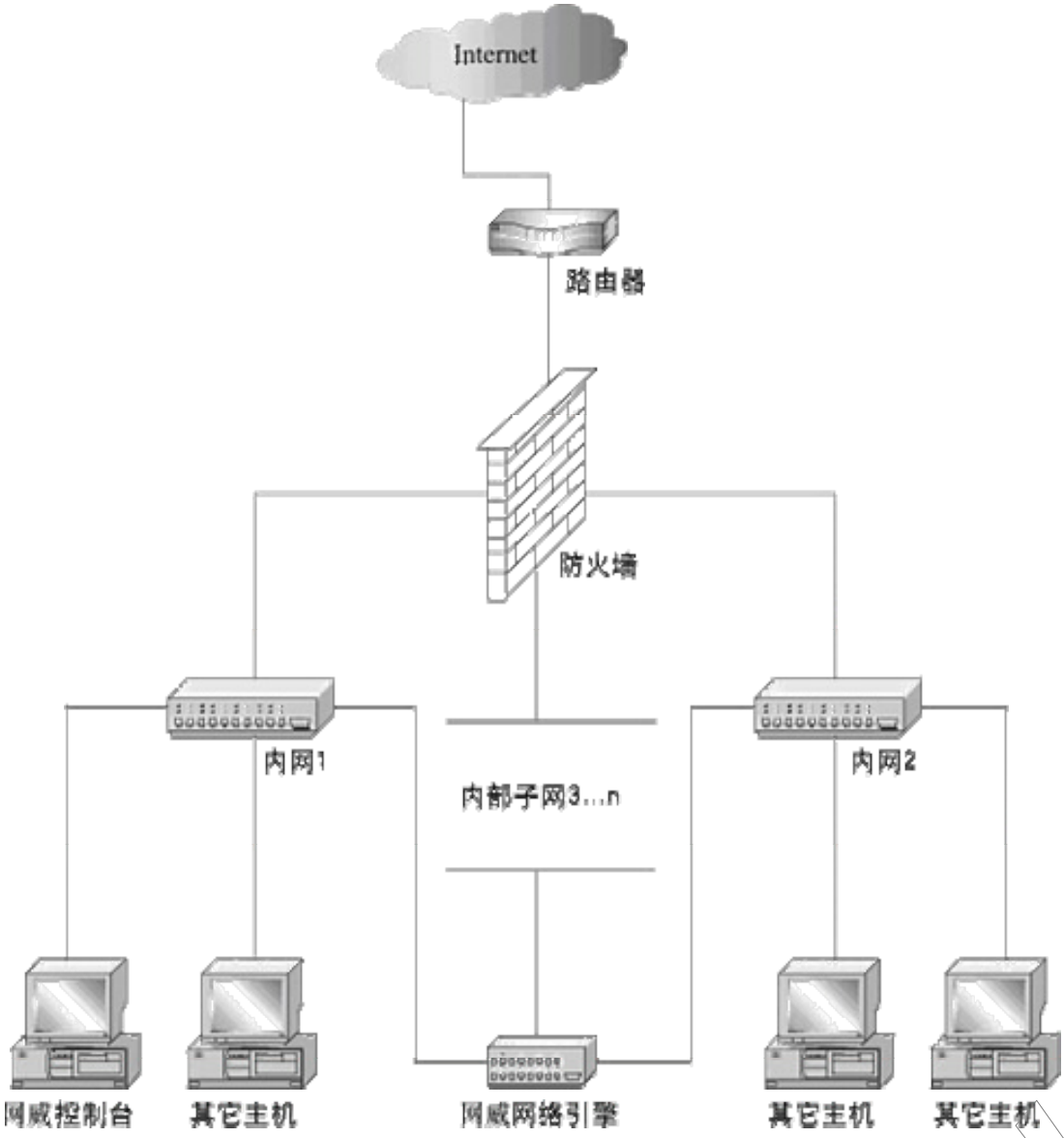
这个应用方案中，在 DMZ 区中通过分接器给每个关键应用服务器连接一个专门的网络引擎，以保证对关键主机的重点监控，这样既可以加强监测的针对性引擎，同时也便于过滤策略和检测策略的定制。



5—3“网威”网络入侵检测系统重点监控部署示意图

5.4 多网段监控

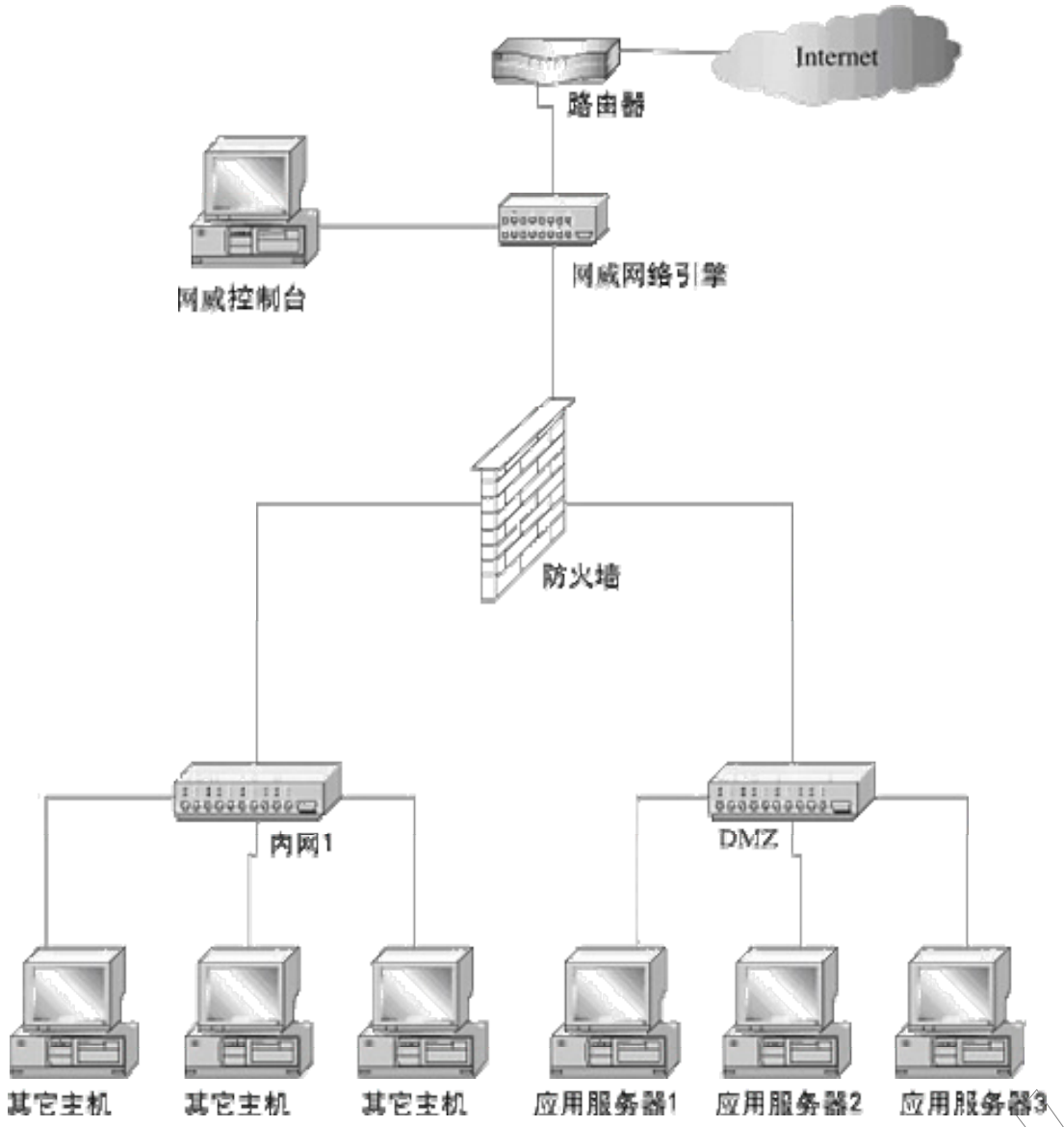
网络中划分多个网段时，通常每个网段需要配置一个入侵检测引擎，这样带来的问题是成本相对较高。对于网络流量不是很高，同时又划分多个网段的网络中，“网威”网络入侵检测系统提供了一个引擎同时监控多个网段的功能。这个应用方案中，通过一个入侵检测引擎可以同时监听 2-7 个网段，可以监控内部网内 2-7 个节点内的所有主机，减少引擎个数，利于管理，方便设定策略；降低网络部署成本。



5—4“网威”网络入侵检测系统多网段监控部署示意图

5.5 透明模式

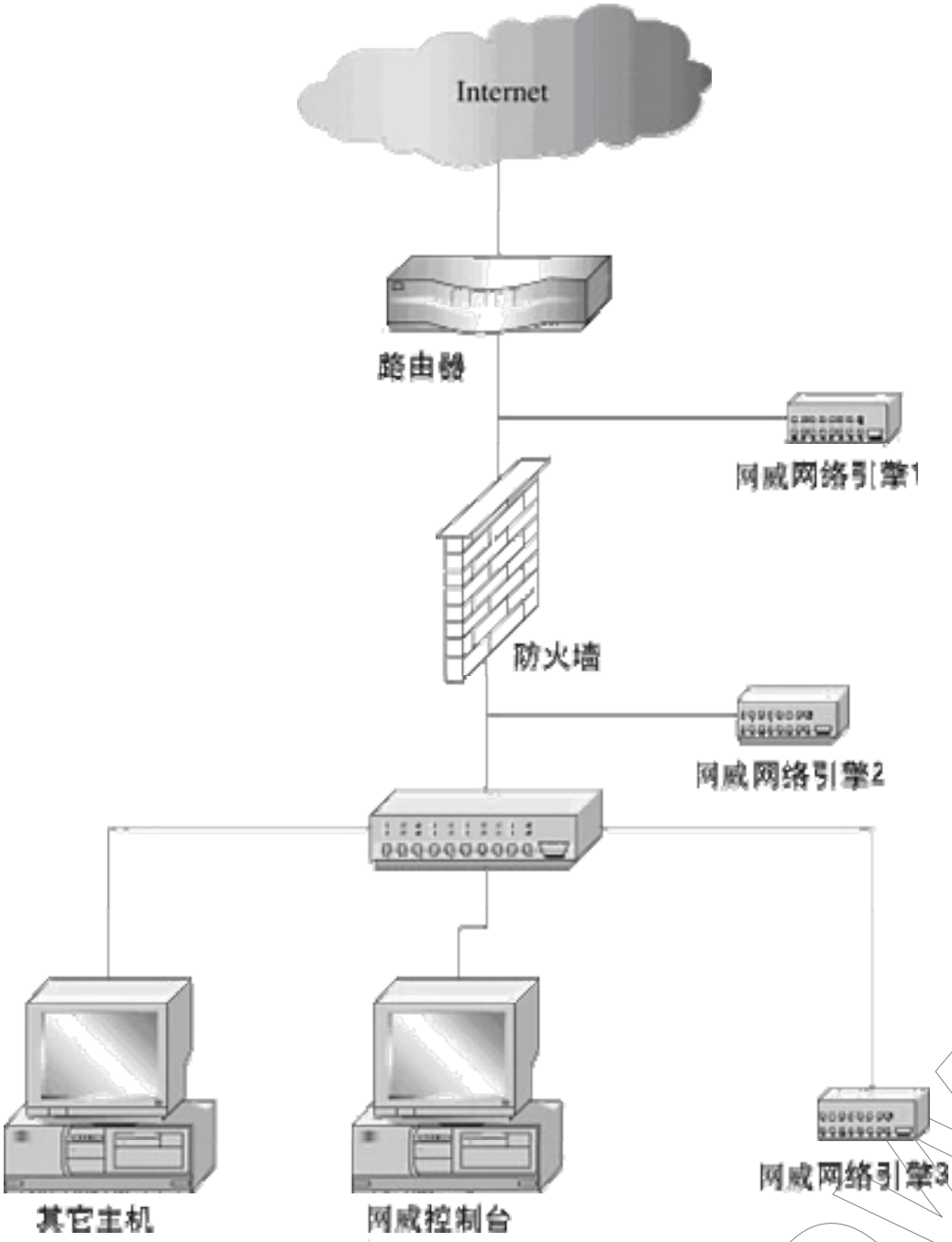
通常入侵检测是以混杂模式工作来监听网络上的数据包，在一些特殊的网络环境中这样会受到一些限制。“网威”入侵检测引擎工作能够在网桥模式下，这样，路由器与防火墙之间不需要再接出一个 HUB 或交换机用于接入引擎，部署方便简洁。



5—5“网威”网络入侵检测系统透明模式部署示意图

5.6 网络分级监控

这个应用方案中，“网威”网络引擎 1 检测从外部网来的攻击；“网威”网络引擎 2 检测经过防火墙的攻击，“网威”网络引擎 3 检测内部网的攻击及异常行为。



5－6“网威”网络入侵检测系统网络分级监控部署示意图

中科网威总部设在北京，在上海设有控股子公司，在广州、深圳等地设有分公司，在各省市设有办事处。

北京总部:

地址：北京市海淀区学院路 35 号世宁大厦 9 层

电话：010-82333399 传真：010-82318600 邮编：100083

E-mail: netpower@netpower.com.cn

上海:

地址：上海浦东峨山路 91 弄 28 号 9 楼（陆家嘴软件园）

电话：021-50895141 传真：021-50895141 邮编：200127

深圳:

地址： 深圳市电子科技大厦 B 座 2190 室

电话：0755-83127099 传真：0755-83127099 邮编：518049

广州:

地址：广州市天河区体育西路 133 号天河大厦 3813 室

电话：020-38869946 传真：020-38861159 邮编：510620