具有主动防御功能的 Intranet 网络安全研究①

Research of Intranet security for Proactive Defence

文光斌　（深圳职业技术学院计算中心 518055）

摘要：从提高 Intranet 网络的安全出发，提出了具有主动防御功能的 Intranet 网的概念，并就主动防御 Intranet 网的组成、工作原理、工作过程及实现方法进行了阐述，最后，对主动防御网的关键部件及技术进行了探讨。

关键词：主动防御　网络安全　协处理 Agent　入侵检测

1　引言

随着计算机技术和通信技术的发展，Intranet（企业内部网）网络结构体系变得越来越庞大，网络协议变得越来越复杂，黑客和病毒对网络的攻击越来越频繁，入侵手段变化无常，形态各异。Intranet 网络的安全问题日渐突出，变得更加重要。但目前对 Intranet 网络安全都采取的是“被动防御”技术，即发现网络受到了攻击，才采取打补丁、关端口和用防火墙或用防毒软件杀毒，这往往是网络已造成了损失，进行事后补救，而并不能使网络具备主动防御的能力和鲁棒性（Robust）。黑客和病毒对网络的攻击往往会采用一些新方法和手段，使得网络在未知攻击的情况下不能做出任何反应，而导致重大损失，因此研究 Intranet 网络的主动防御技术具有重要的现实意义。

2　主动防御网络的基本原理及工作过程

2.1　主动防御 Intranet 网的概念

主动防御网络如同具有免疫能力的人体，能够主动防御网络病毒、黑客的侵害。也就是说在未知的攻击来到时，网络已经具备了抵抗攻击的能力。主动防御网络的关键就是要使路由器具有主动过滤攻击包的能力，按照 ISO 制定的网络七层参考模型，路由器是工作在第三层，即网络层；而根据 TCP/IP 协议模型，路由器是工作在 IP 层。但为了协同工作，路由器除了支持基本的 IP 协议外，还支持其它辅助协议，如：TCP 协议、ICMP 协议、SNMP 协议、TELNET 协议、HTTP 协议等。黑客和病毒正是利用了这些辅助协议对路由器和网络进行攻击的，耗尽其资源，使路由器和网络瘫痪。如果针对不同的协议采取不同的防范措施，只会使防范变得越来越复杂，如果是纯粹关掉这些协议或端口，不但因噎废食使许多网络功能不能使用，而且也不符合“主动防御”的思想。

根据网络协议的工作原理可知，路由器的所有辅助协议都是基于 IP 协议的，即工作在 IP 协议之上，而路由器是工作在 IP 层的。所有进入路由器的 IP 包根据其目的地址可分为两类：一类是目的地址指向其它网络主机的 IP 包，这里称为“转发 IP 包”；一类是目的地址指向本路由器的 IP 包，这里称为“终点 IP 包”。

对转发 IP 包路由器会根据策略进行转发或丢弃，不会耗费太多的资源，对内网也没有威胁。即使当这类 IP 包太多，网络出现拥塞时，路由器也会根据排队的原则简单的丢弃一些 IP 包，路由器不会出现异常。因此“转发 IP 包”相对路由器来说是一般正常的 IP 包，对路由器和 Intranet 来说都是安全的。

路由器对终点 IP 包的处理会根据策略丢弃或传给高层协议处理。高层协议通常会根据这些 IP 包的请求，为其分配相应的内存，并阻塞某些端口，还有可能带有病毒的 IP 包被路由器转发到了 Intranet 网，且复杂的协议很可能会隐藏一些潜在的漏洞。因此这类 IP 包是对路由器和网络潜在威胁最大的 IP 包，攻击和入侵的 IP 包往往隐藏在这类路由器认为正确的 IP 包中。从目前路由器和网络受到的攻击来看，大都属于此类 IP 包，如：ICMP 攻击、TELNET 远程攻击、HTTP 远程攻击、广播风暴及蠕虫病毒等。

① 基金号：2005 年深圳市科技计划资助课题（编号：05KJce019

通过上面对路由器攻击方式的分析，以及在 IP 层对 IP 数据包的分类，对路由器防攻击的研究应集中在对终点 IP 包的处理上，而且应采取主动防御的策略来提高路由器和网络的抗攻击能力，这样不会由于未知的攻击而出现不可预测的后果。

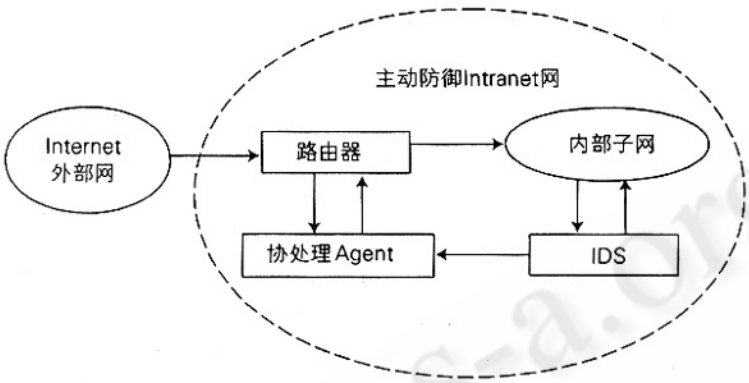

图 1　主动防御 Intranet 网功能图

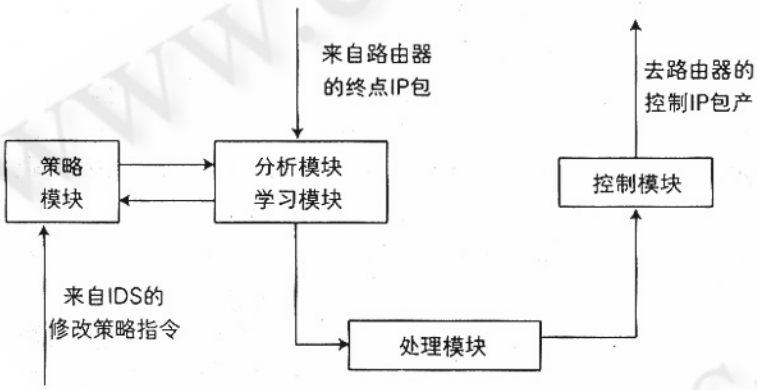

图 2　协处理 Agent 的功能模块及组成

2.2 主动防御 Intranet 网的工作原理及工作过程

为了使路由器具有主动防御的能力，可以引入一个“协处理 Agent”来协助路由器完成 IP 包的处理功能，并对路由器进行控制，实施主动防御。同时在 Intranet 网内部建立 IDS(Intrusion Detection System，入侵检测系统)。对企业内网发起的攻击若攻破了协处理 Agent 控制的路由器的第一道关卡，可以依靠入侵检测系统阻断和发现攻击的行为，同时通过与协处理 Agent 的互动，自动修改协处理 Agent 策略设置上的漏洞和不足，阻挡攻击的继续进入。路由器、协处理 Agent、IDS 和网络的结构关系如图 1 所示，图中箭头所示方向为 IP 包的传输方向。路由器、协处理 Agent、IDS 内部子网共同组成了主动防御 Intranet 网。

主动防御 Intranet 网的工程过程是：当路由器收到来自外部网络或内部子网的 IP 包时，若是转发 IP 包则根据路由器的策略进行转发或丢弃；若是终点 IP 包，则会根据策略丢弃或转交协处理 Agent 进行处理。协处理 Agent 在处理这些 IP 包时会进行分析和判断，是正常 IP 包交由路由器转发，攻击 IP 包则控制路由器丢弃。当出现新的攻击方法和病毒时，协处理 Agent 可能没有防御这些攻击的策略，带有攻击性质的 IP 包被转发到内部子网，此时 IDS 能立即检测到这些攻击包，马上反馈协处理 Agent，自动修改协处理 Agent 的策略，使协处理 Agent 及时控制路由器丢弃这些攻击包，避免网络和路由受到进一步的攻击。

3　主动防御网络的关键部件及技术

3.1 协处理 Agent 的组成及工作过程

协处理 Agent 是由策略模块、分析模块、学习模块、处理模块及控制模块组成，如图 2 所示。

协处理 Agent 的工作流程如图 2 所示，当收到来自路由器的终点 IP 包时，分析模块会根据策略模块提供的策略对 IP 包进行分析，判断是否为恶意的包还是有用的包。学习模块在分析模块的配合下进行学习，动态改变策略模块的策略。同时策略模块还受到来自 IDS 的修改策略指令的控制，实时修改策略模块的策略。然后处理模块会根据分析模块的结果对 IP 包进行处理，处理结果交给控制模块，由控制模块对路由器发出控制指令，使路由器做到丢弃攻击 IP 包，转发正常 IP 包。

设立协处理 Agent 的优点：

(1) 器免受来自终点 IP 包攻击。当攻击发生时，遭受攻击的是协处理 Agent，而非路由器。

(2) 协处理 Agent 的处理程序可以不受路由器的功能的干扰和限制而进行合理的设计，使其具有很强的分析、判断和学习能力，对合理的 IP 包做出响应，对非法的 IP 包做出限制，协助路由器工作，使路由器更具智能性。

(3) 协处理 Agent 与路由器分开，在增强路由器的抗攻击能力的同时，并不增加路由器的负担。并且可以在不用多改变路由器的基础上，实现从原路由器到抗攻击路由器的升级。

(4) 在协处理 Agent 技术比较成熟和稳定后,协处理 Agent 和路由器可以集成为一体,这样在协处理 Agent 和路由器之间会具有更高的传输速度和更好的安全性。

3.2 具有主动防御功能的路由器的工作原理

一般路由器的组成如图 3 所示。

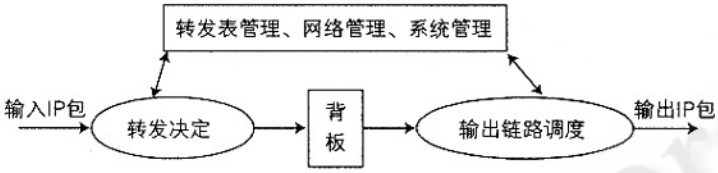

图 3　一般路由器的组成

其工作过程是:当数据 IP 包到达路由器时,它首先在转发表中查找它的目的地址,决定是否转发。若找到目的地址,就在数据包的前部添加下一跳的 MAC 地址,IP 数据包头的 TTL(Time to live)域开始减数据,并计算新的校验和(checksum),然后传给背板。数据包通过背板转发到它的输出端口。输出链路调度的作用是当数据包抵达输出端口时,使它按顺序等待以便传送到输出链路上。大多数路由器中。输出端口保持先到先服务队列,按数据包抵达的次序进行传送。更先进的路由器可将数据包分成不同的流量队列和优先级,并精心安排每个数据包的离开时间以满足服务质量的要求。

从上面的分析可以看出,只要协处理 Agent 的控制 IP 包去控制输入到转发决定的 IP 包,使它分成转发 IP 包和终点 IP 包,转发 IP 包照常转发,而终点 IP 包必须经过协处理 Agent 的处理决定是否转发,没有攻击性的包就转发,有攻击性的包就丢弃,从而达到主动防御之目的。具体实现方法见图 4。

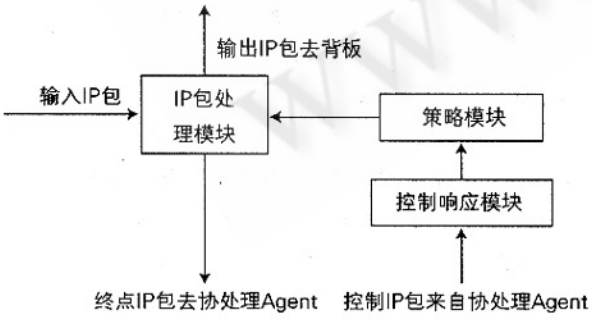

图 4　主动防御路由器原理示意图

输入的 IP 包经过 IP 包处理模块,在策略模块的控制下分为转发 IP 包和终点 IP 包,转发 IP 包直接输出,而终点 IP 包送到协处理 Agent 进行分析处理。协处理 Agent 输出的控制 IP 包送到控制响应模块,控制响应模块对策略模块的策略进行调整,如果终点 IP 包不是攻击和病毒 IP 包,IP 包处理模块就输出到路由器的背板,如果终点 IP 包包含有攻击或病毒信息,IP 包处理模块就丢弃此 IP 包。从而实现主动防御的目的。

3.3 入侵检测系统(IDS, Intrusion Detection System)

IDS 是用来识别针对计算机系统和网络系统的非法攻击,检测外界非法入侵者的恶意攻击或试探的。它由探测器(Sensor)、分析器(Analyzer)和用户接口(User Interface)三部分组成。

探测器主要负责收集数据。探测器的输入数据流包括任何可能包含入侵行为线索的系统数据,比如说网络数据包、日志文件和系统调用记录等。探测器将这些数据收集起来,然后发送到分析器进行处理。

分析器又可称为检测引擎,它负责从一个或多个探测器处接受信息,并通过分析来确定是否发生了入侵活动。分析器组件的输出为标识入侵行为是否发生的指示信号,该指示信号中还可能包括相关的证据信息。另外,分析器组件还能够提供关于可能的反应措施的相关信息。

用户接口使得用户易于观察系统的输出信号,并对系统行为进行控制。在这里要输出一个控制信号给协处理 Agent,以修改协处理 Agent 的策略。因此用户接口又可称为控制器。

4 结束语

本文提出了具有主动防御功能的 Intranet 网的设计思想和解决方案,它克服了被动防御的弱点,对黑客和病毒的攻击采取主动的防御,将来一定有美好的发展前景和巨大的市场潜力。

参考文献

1 黎连业、张维、向东明,路由器及其应用技术,[M]北京 清华大学出版社,2004。
2 唐正军,网络入侵检测系统的设计与实现,[M]北京 电子工业出版社,2002。
3 朱蕾、张勇、白英彩,基于 IPSec 的安全路由器设计与实现,[J]计算机工程,2001. 6。