入侵检测系统概述

郭晓翔 2006-02-09 发表

入侵检测系统概述 - 入门篇

第1章入侵检测系统概述

网络发展到今天，规模已经超乎想象，可以说我们的生活已经离不开网络。而互联网的基础IP技术确并非完美，因此网络安全问题日益突出，这里不再赘言。魔高一尺、道高一丈，与此同时网络安全技术也在不断发展。

思考：我们能了解的网络安全问题有哪些？这些攻击方式是什么原理呢？

1、什么是入侵检测系统？很多人了解一些，很多人也可能不太了解。我们来先看看教科书中的关于入侵的定义，入侵是对信息系统的非授权访问及（或）未经许可在信息系统中进行操作,威胁计算机或网络的安全机制（包括机密性、完整性、可用性）的行为。入侵可能是来自互联网的攻击者对系统的非法访问，也可能是系统的授权用户对未授权的内容进行非法访问。

思考：任何违反安全策略规定的操作是否都可认为是入侵？

显然可以通俗的理解，入侵就是小偷入室盗窃的行为，是非法的。那么入侵检测就是对企图入侵、正在进行的入侵或已经发生的入侵进行识别的过程。入侵检测系统（英文简称IDS：Intrusion Detection System）是从多种计算机系统及网络中收集信息，再通过这些信息分析入侵特征的网络安全系统。

看完这个定义，问题也随之而来，入侵检测系统如何检测入侵行为？能否确保所有的攻击被检测到？检测到之后有何动作？是否仅仅只是检测？它和防火墙又有那些区别与联系？耐心看完下面的内容，这些疑问都会有个答案。

2、入侵检测系统的目标

根据以上的定义，我们可以看到，IDS的目标主要是：

对攻击的检测与诊断

IDS需要快速地鉴别并且分类一个攻击。在网络中引入IDS这个设备，在对网络进行保护的同时，也需要综合考虑这个设备如何尽可能地降低网络管理员的工作量和工作难度，这就使得诊断成为IDS的重要目标之一。

显然，IDS将对新出现的攻击手段无能为力。这一点很正常，这也是IDS的攻击特征描述库需要不断更新的原因。现在的基于协议异常行为分析的检测手段可以在一定程度上检测出未被定义的攻击。

100%准确的报告

虽然无法达到这个理想的目标，但是仍然要把它列在这里。

对于不准确的报告，可以分为两类：**误报**（False Positive）和**漏报**（False Negative）。太多的误报会激怒网络管理人员，从而对一些真正需要关注的报警不再关注，导致“狼来了”的结局；而太多的漏报会使得IDS形同虚设，被保护网络没有得到应该得到的保护。

所以，好的IDS应该致力于如何降低这两个名词在评估报告中的出现频率。

迅速的通告

从发现入侵到报告这个入侵，这中间存在着天然的时延。之所以称其为天然的，是因为：1、IDS需要一定的时间来判断是否出现了攻击；2、通告渠道本身有一定的延迟。好的IDS应该尽量降低这两个时间值，使得入侵在开始生效之前（也就是对系统的破坏发生之前）管理员可以得知这一情况从而做出反应。（对于IDS，这几乎是不可能的，这也正是IPS出现的重要原因之一。）

通告方式也是IDS需要考虑的重要指标之一，常用的方式有声光报警、电子邮件通报、短消息通报等，在不同的情况下酌情采用。

主动防御

既然IDS只能检测已经发生的攻击，那么一个很自然的想法是：有没有办法主动采取一些措施，降低攻击生效的可能性？有，而且这是IDS需要关注的焦点功能之一，他们包括：对被保护系统的缺陷分析（有哪些漏洞有可能被攻击）、对被保护系统对存在的缺陷的通告（告诉管理员）、对修复已知缺陷的建议（告诉管理员怎么做）和与网络中其他安全设备的配合（TCP复位和防火墙联动）等。

遗憾的是，以上手段并不是十分有效，尤其是最后一点中的防火墙联动，反而还存在着被攻击的安全隐患。（这些，也是促使IPS概念出现的重要原因。关于IPS在后续文章中会介绍）

3、入侵检测系统的分类

下表描述了IDS的分类：

按照系统在网络中所处的位置	基于主机（Host-based IDS, HIDS）
	基于网络（Network-based IDS, NIDS）
	混合型（Hybrid IDS）
按照系统采用的检测方法	基于攻击特征分析（Signature-based IDS）
	基于协议异常分析（Anomaly-based IDS）
	混合型（Stateful-Signature-based/Hybrid IDS）

下面一一简介：

基于主机（Host-based IDS, HIDS）
HIDS的概念起源于一种最初为大型的多用户分时操作系统设计的保护软件，这种软件主要用来协助管理员发现用户之间的互相侵扰。后来，随着主机入侵事件的频频发生，人们发现可以使用同样的原理保护整个系统，继而出现了为特定操作系统制作的入侵保护软件。
顾名思义，HIDS是一种软件系统，这种软件运行在被保护的主机（也就是说特定的操作系统）上，与操作系统和应用程序紧密耦合。HIDS主要基于对系统漏洞的扫描和系统日志的审计工作，现在也有一些实时的入侵检测软件。
有一种观点是：HIDS是无用的。因为HIDS可以完成的事情，NIDS完全可以完成。其实，HIDS是对NIDS的有益补充，因为NIDS无法完成一些与操作系统依赖性非常强的检测，所以，HIDS和NIDS是一个完整的入侵检测方案的不可或缺的三个组成部分中的两个（另外一个是管理系统）。
HIDS的优点在于：它可以获得关于用户级活动的最详细的数据，一旦HIDS驻留的系统被攻击，作为被攻击系统的一部分，它可以提供关于攻击的详细资料，从而保证对该种攻击的分析效果；另外，HIDS只需要处理本机数据，相对于NIDS，不需要进行海量运算，从而对系统性能的要求不是很高；HIDS是对操作系统、文件系统、应用程序进行系统的检测的理想选择。
HIDS也不可避免地具有缺点：攻击发生后，被攻击系统所存留的信息不能保证百分之百可靠，甚至HIDS本身都有可能被攻击；依赖于特定的应用程序和操作系统，跨系统移植代价高；HIDS随着被保护系统的崩溃而崩溃，无法有效抵御“ping to death”一类的攻击；因为需要运行在每个被保护系统上，所以部署代价高，维护代价高。

基于网络（Network-based IDS, NIDS）
网络系统的大规模普及是促使NIDS出现的根本原因，现在，NIDS已经成为现在IDS研究的主导方向。
NIDS的基本工作原理是使用专门的设备，利用该设备的工作于混杂模式的以太网接口，来监听并分析所连接的广播式网络里的流量，以期发现问题。NIDS的分析方法主要有攻击特征分析和协议异常分析两种，但是这两种检测方法并不是互斥的，而是相辅相成的。其实，现在的IDS都是利用这二者的有机结合来提高系统的性能和准确度的。
以下是NIDS的优点：集中的特点使得NIDS较HIDS来说，易于部署，易于维护；以抽象数据的方式分析网络中的流量，可以有效抵御DoS、ping to death一类的攻击；针对标准的TCP/IP协议检测，从而具备良好的操作系统无关性；有可能使得NIDS对外在攻击和被保护系统（网络）透明，从而避免对NIDS的攻击（方法是：不为工作于混杂模式的监听接口设置IP地址，从而使得基于TCP/IP的攻击无法影响NIDS。）。
NIDS的缺点在于：因为网络拥塞等原因，有可能遗漏对某些分组的检测；针对网络内的所有流量检测，无法针对用户级的流量检测；对于某些攻击，无法明确地判定被攻击的目的系统（某些攻击只针对Windows系统，而对Solaris系统无效，NIDS仍然会报警）；需要了解所有的细节，实现复杂度高。

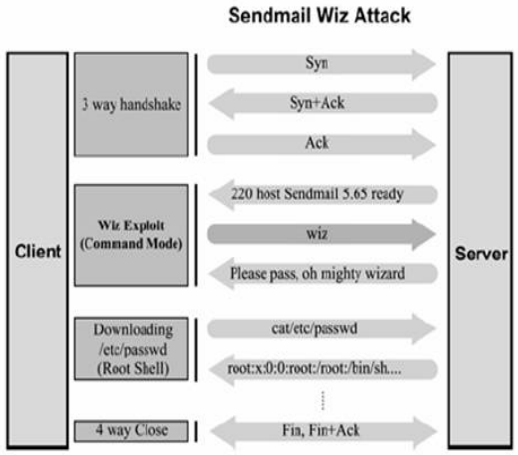
混合型（Hybrid IDS）
混合型IDS可以从两个方面讨论。
第一种是从被保护主机系统的角度来看待：在系统的IP层进行基于三层的检测，在应用层进行基于应用（操作系统）的检测，从而达到综合检测的目的。
第二种是从被保护网络系统的角度来看：在被保护网络中部署NIDS来监听所有进入该网络的流量，在网络中的重点保护对象（如文件服务器）上再部署HIDS来检测进入该主机的流量。

基于攻击特征分析（Signature-based IDS）
顾名思义，具备该种检测方法的IDS具备详细的关于各种攻击的特征知识库，其原始思想很朴素：对网络中的流量进行特征匹配，如果匹配成功，说明有入侵企图。根据其工作原理可以看出，检测效率是具备该种检测方法的IDS的关键点，解决效率问题的方法包含基于状态的特征分析和正则表达式分析两种。另外，如何应对攻击特征的变种（使用unicode，一个攻击特征可以表示为多种形态，IDS需要跟踪所有的这些可能的形态。）也是一个需要注意的问题。
一般地来说，在这种设备的开发团队背后，需要有一个强大的支撑团队来跟踪网络安全、操作系统漏洞、甚至病毒等方面的最新动态，以便实时更新特征库。事实上，这样一个团队对于一个IDS供应商来说是不可或缺的。
该种IDS的优点显而易见：原理简单，易于实现；可以发现与协议操作无关的攻击。但是，其缺点也同样显而易见：效率是个严重的问题；系统的特征知识库需要动态更新；无法有效检测攻击的变种；无法抵御新的攻击；需要管理员随时跟踪网络安全动态。

基于协议异常分析（Anomaly-based IDS）
开放网络协议运作的高度规范性是该种检测方法的基础。任何协议都具备高度规范的操作流程，例如在A发生之前B不允许发生，或者C发生的时候不应该有特定的操作发生。这样，就为NIDS提供了一种新的检测手段。
该检测方法主要监听网络中运行的通信协议的状态，以期发现与协议中定义的规则相悖的操作/异常状态，从而发现可能存在的入侵。典型的此类攻击包括：Buffer overflow、FTP Bounce、TCP SYN Flooding、SMTP Wiz等。
优点：可以在一定程度上发现新的或者未知的攻击，并且可以发现对已知攻击的变种；缺点：无法发

现不依赖于协议状态的攻击。

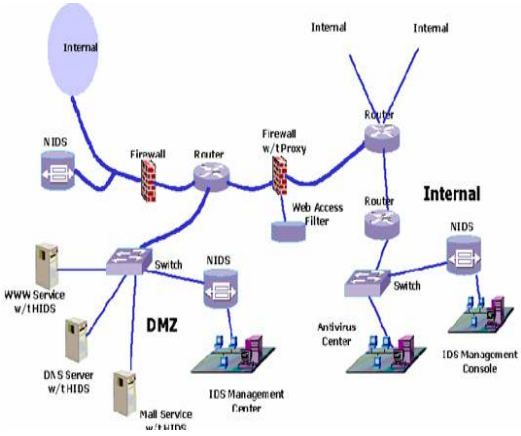
混合型（Stateful-Signature-based/Hybrid IDS）
从以上可以看出，每一种检测方法在有其所长的同时也都有其所短。既然采用一种单纯的方法无法面面俱到，那么综合了多种检测方法的NIDS的也就理所当然地出现了。事实上，这种综合了多种检测方法的NIDS正是现在NIDS的主流方向，NetScreen、Cisco、ISS、NFR等的NIDS设备全部是基于这种思想设计、开发的。需要说明的是，这种综合是有机的结合，并不是简单地在一个盒子中放置两个漏斗。这样才能在综合的同时进一步提高性能。
下面的例子，生动地说明了这个问题：



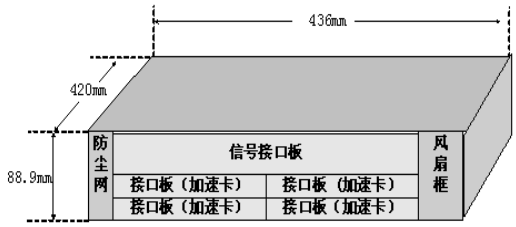
Sendmail Wiz攻击是发生在TCP传输阶段的一种试图获取目标系统的root操作权限的攻击。对于只具备简单的攻击特征匹配功能的NIDS，不得不对一次TCP通信的所有阶段进行特征匹配；而对于具备了TCP协议分析功能和攻击特征匹配功能的NIDS来说，只会在TCP传输阶段去做匹配操作。所以，显而易见，后一种NIDS的性能要优于第一种很多。这只是一个简单的例子，而经过对现有协议和针对这些协议的攻击的分析，在实际的网络流量中有将近60%存在类似的规律。

风险分析
网络安全
安全策略
系统防护
实时监测
实时响应
灾难恢复
第2章关于IDS 200

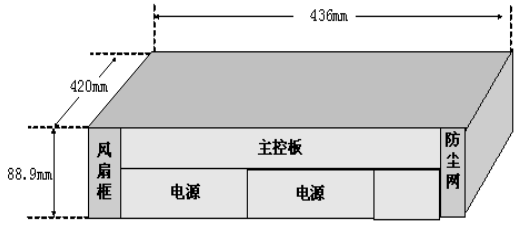
上面一章我们详细介绍了入侵检测系统的一般概念，下面简单一下介绍我司产品IDS 200，内部版本号为9011V100R001，定位为网络入侵检测系统产品，工作在SNIFFER模式下，通过路由器或交换机的监听口对被保护网络进行“监听”，如果发现有攻击发生或有可疑的网络活动就报警和记日志。
思考：IDS 200的报警方式有哪些？检测到攻击的动作就是报警和记日志？
IDS 200的网络位置



如图所示，IDS 200可用在网络中NIDS位置，代替NIDS。通过连接到hub、router或switch的监听接口，IDS 200可以监听所有进入内部网络的流量，从而达到入侵检测的目的。
思考：网络中的流量如何进入IDS，需要镜像吗？
***2*、IDS 200的硬件结构图**



IDS 200系列机箱结构图（前视图）



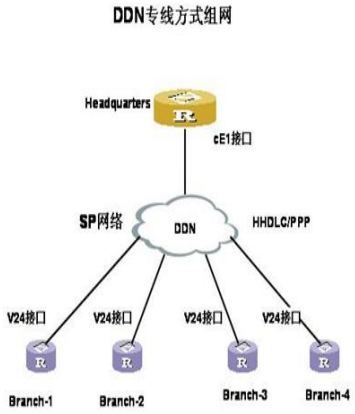
IDS 200系列机箱结构图（后视图）

IDS 200系列产品为横插板形式，前后的视图分别如上图所示。除了主控板之外，其它模块均为可带电插拔。其中电源模块、风扇框和防尘网为后插拔式，接口卡、加速卡和信号接口板为前插拔式。

3、关于本产品的其他内容，且听下回分解。

常见广域网组网技术分析（作者：肖春喜）

cE1方式



E-载波是国际电信联盟-电信标准部ITU-T（International Telecommunication Union-Telecommunication Standardization Sector）建议的一种数字通信体系，开始于2048kbit/s的E-1，应用于北美以外地区。

E1属于ITU-T建议的数字通信体系，信号速率为2048kbit/s。

E1/CE1接口是指可通道化的E1，即Channelized E1，它有两种工作方式：E1工作方式（clear channel）和CE1工作方式（channelized）。

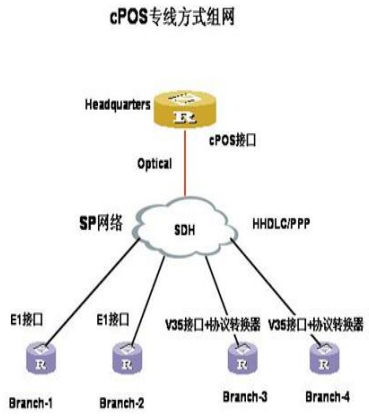
l当工作在E1方式时，它相当于一个不分时隙、数据带宽为2.048M的接口，其逻辑特性与同步串口相同，支持PPP、帧中继等链路层协议，支持IP网络协议。

l当工作在CE1方式时，它在物理上分为32个时隙，对应编号为0～31。其中的31个时隙可以被任意地分成若干组（时隙0用于传送帧同步信号，不能被捆绑），每组时隙捆绑以后作为一个接口（channel-set）使用，其逻辑特性与同步串口相同，支持PPP、HDLC、FR、LAPB和X.25等链路层协议，支持IP等网络协议。

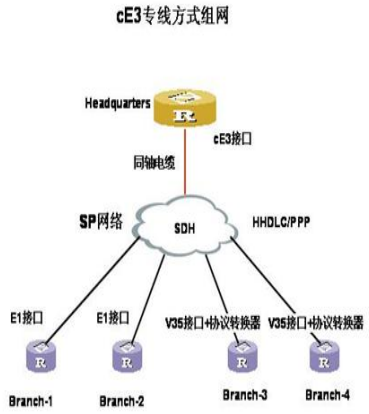
在CE1工作方式下，它在物理上分为32个时隙，对应编号为0～31，其中时隙0用于传送帧同步信号。对其余的31个时隙有两种使用方法：用作CE1接口或PRI接口。

这种是早期的组网，中心采用一台带有CE1模块的路由器，分枝机构采用V24串口，中心将一个E1（其实少了一个时隙，只有31个）拆分成64K，分别连接下面节点，由SP负责信道的对应，可以两个和多个信道对应同一分枝，采用链路捆绑技术MP来实现，而总部和分枝在单链路时，多用HDLC或是PPP的链路层协议，而捆绑比用PPP。此技术现在应用在网点或边远的乡村，适合业务量不大的应用，如农信联的柜面业务以及银行储蓄网点的应用。

cPOS技术



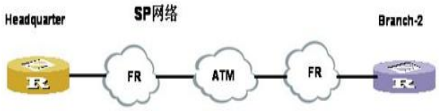
在同步数字系列SDH（Synchronous Digital Hierarchy）中，采用同步复用方式和灵活的映射结构，可以从SDH信号中直接分插出低速的支路信号，而不需要使用大量的复接/分接设备，从而能够减少信号损耗和设备投资。
当把SDH信号看成由低速信号复用而成时，这些低速支路信号就称为通道。CPOS，即通道化的POS接口。它充分利用了SDH体制的特点，提供对带宽精细划分的能力，可减少组网中对路由器低速物理端口的数量要求，增强路由器的低速端口汇聚能力，并提高路由器的专线接入能力。
这种组网，现在比较普遍总部采用cPOS方式，实际是将一个155M带宽的cPOS拆分成63个2M的E1线路或是84个1.54M的T1线路（中国大陆不使用），在接入分支机构时，中心采用cPOS的模块，通过光纤接入SP网络，由SP负责将拆分出的63个2M去对应每一个分支节点，分支节点用带E1模块的路由器或是V35串口＋协议转换器联入SP网络。单链路时，链路层协议可用HDLC/PPP,也可做捆绑，将多个2M捆绑使用。适合有多个分支机构的大型企业网组网，尤其是全国的网。
同时，也有将2.5G的cPOS拆分成16个155M的POS,不过企业网比较少见。
cE3技术



E3与E1同属于ITU-T的数字载波体系，数据传输速率为34368kbit/s，线路编解码方式采用HDB3。
类似于E1/CE1，E3/CE3接口也有两种工作模式：
当工作在E3方式时，它相当于一个不分时隙，数据带宽为34.368M的接口。
当工作在CE3方式时，它可以复用/解复用16路E1信号，E3到E1的复用符合ITU-T G.751和G.742规范。每个E1又可以分为32个时隙，对应编号为0～31，其中1～31时隙可任意捆绑为N×64kbit/s的逻辑通道（时隙0用于传送帧同步信号，不能被捆绑）。因此，CE3支持通道化到E1和通道化到64kbit/s。
组网和cPOS类似，不过只能拆分出16个2M，也支持将2M拆分成64K。

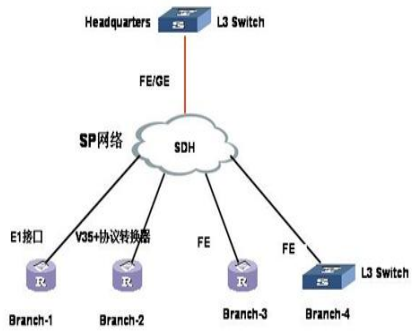
POS/ATM方式

POS（Packet Over SONET/SDH，SONET/SDH上的分组）是一种应用在城域网及广域网中的技术，它具有支持分组数据，如IP分组的优点。
POS将长度可变的数据包直接映射进SONET同步载荷中，使用SONET物理层传输标准，提供了一种高速、可靠、点到点的数据连接。
异步传输模式ATM（Asynchronous Transfer Mode）技术是一种主干网络技术，被设计用来传输语音、视频、及数据信息。由于它的灵活性以及对多媒体业务的支持，被认为是实现宽带通信的核心技术。
ATM物理层位于ATM协议参考模型的最低层。它涉及具体的传输介质，但其功能并不依赖于其所用的传输机制和速率。主要完成在高层与传输介质之间传送有效的信元和相应的定时信号。
上图的组网适合两个机构直间的高速线路连接，而ATM在此处的应用主要是IPoA方式，完全是将ATM作为了链路层，地位等同于FR，PPP。而线路带宽SP可根据用户的需求进行调整。普通情况下POS从155M到2.5G不等。ATM从155M到622M。也有应用户需要SP可以提供低于上述速率的带宽。
FR技术



帧中继（Frame Relay）是在X.25技术基础之上发展起来的一种快速分组交换技术。相对于X.25协议，帧中继只完成链路层核心的功能，更为简单高效。
帧中继网提供了用户设备（如路由器和主机等）之间进行数据通信的能力，用户设备被称作数据终端设备（DTE）；为用户设备提供接入的设备，属于网络设备，被称为数据电路终接设备（DCE）。帧中继网络可以是公用网络、私有网络、也可以是数据设备之间直接连接构成的网络。
帧中继的网络一般给用户提供的带宽可以从64K - 2M不等，由SP负责维护PVC链路，接入方式采用串口或是E1接口均可，费用比较低廉，适合企业机构互联，同时总部也在一个物理接口上建立多个子接口，与多个分支机构相连。有部分SP会做两次转换，利用FR - ATM - FR的转换，利用现有的ATM资源。
MSTP技术

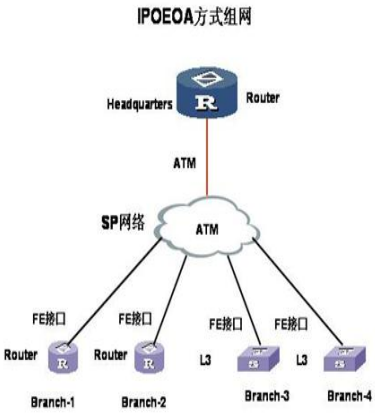
MSTP方式组网



这种技术比较新，是对传输技术的改进。原来的传输设备要求用户两端的协议类型一致，这样对多点接入单点时，用CPOS技术成本太高，用一对一的E1方式，用户端管理不方便，采用MSTP技术，传输设备分担了用户的工作，组网模式如上：总部用一台L3交换机（用L2的也行，但从实际组网来看，后面还是得有三层设备），接入SP的传输网络时，可用一根FE/GE（采用TRUNK方式），或是多根FE/GE,但要求发出的以太网报文要带有VLAN头，传输设备读取VLAN中的VLAN ID号，将其与对应的E1信道连接，这样分支机构接入时采用简单的E1接入，而总部网络设备投资减小，管理方便，费用低廉，接入方式简便。分支节点除了用路由器方式外，还可用L3，不过连接是两头是带VLAN的以太网报文，中间经过了SDH传输设备。

IPOEOA技术

IPOEOA方式组网



这种接入方式方便了分支机构，总部的投资大了一点。实现如下，总部通过155M的ATM，创建多个PVC，而每个PVC的带宽通过service class可配置，如vbr-nrt, vbr-rt, cbr等，带宽有2M，4M，10M等等，由SP提供。对分支机构来看，只要三层设备（路由器或是交换机）提供以太口，速率由SP控制，中心的ATM配置成了IPOEOA方式，每个Virtual-Ethernet接口对应一个分支机构的以太口。也很方便的接入了分支用户，但总部投资ATM模块，支持IPOEOA功能。