ICS 33.040.40;33.200
M54

YDN

通 信 技 术 规 定

YDN 140-2006

网络入侵检测系统技术要求

Technical Requirement for Network Intrusion Detection System

2006-07-04 发布　　2006-07-04 实施

中华人民共和国信息产业部 发布

目　次

前　言

本标准是网络入侵检测系统系列标准之一。该系列标准的名称预计如下：

1. 网络入侵检测系统技术要求
2. 网络入侵检测系统测试方法

本标准的附录A为资料性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院
北京启明星辰信息技术有限公司
华为技术有限公司

本标准起草人：落红卫　楚建梅　吴海民　苗福友　刘　册

引　言

网络入侵检测系统是指从IP网络的若干关键点收集信息并对其进行分析，从中发现网络中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定措施的系统。

网络入侵检测技术是网络动态安全的核心技术，相关设备和系统是整个安全防护体系的重要组成部分。目前，防火墙是静态安全防御技术，但对网络环境下日新月异的攻击手段缺乏主动的监测和响应。而网络入侵检测系统能对网络入侵事件和过程做出实时响应，其和防火墙并列为网络与信息安全的核心设备。

网络入侵检测系统技术要求

1 范围

本标准规定了网络入侵检测系统的系统结构、检测内容、响应方式、系统管理、日志审计、自身安全、性能指标和物理安全。

本标准适用于网络入侵检测系统及相关设备。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 4943-2001	信息技术设备的安全
GB/T 5271.8-2001	信息技术 词汇 第8部分：安全
GB 9254-1998	信息技术设备的无线电骚扰限值和测量方法
GB/T 17618-1998	信息技术设备抗扰限值和测量方法
GB/T 18336-2001	信息技术 安全技术 信息技术安全性评估准则

3 术语和定义

下列术语和定义适用于本标准。

报警 Alert

报警是指网络入侵检测系统在检测到入侵行为时，发布给具有系统管理角色实体的消息。

攻击 Attack

攻击是指任何危及计算机资源与网络资源完整性、机密性或可用性的行为。

自动响应 Automated Response

自动响应是指网络入侵检测系统在发现攻击后自发采取的保护行为。

躲避 Evasion

躲避是指入侵者发动攻击，而又不希望被发现而采取的行为。

漏报 False Negatives

漏报是指一个攻击事件未被网络入侵检测系统检测到而造成的错误。

误报　False Positives

误报是指系统把正常行为作为入侵攻击而进行报警，或者把一种周知的攻击错误报告为另一种攻击而导致系统错误响应。

防火墙　Firewall

在网络之间执行访问控制策略的一个或一组设备。

入侵　Intrusion

同“攻击”含义。

入侵检测　Intrusion Detection

入侵检测是对入侵行为的发觉。它从IP网络或计算机系统中的若干关键点收集信息并对其进行分析，从中发现是否有违反安全策略的行为或遭到入侵的迹象。

入侵检测系统　Intrusion Detection System (IDS)

进行入侵检测并依据既定的策略采取一定响应措施的软件与硬件的组合。

网络入侵检测系统　Network Intrusion Detecion System (NIDS)

使用IP网络数据包作为数据源的入侵检测系统。

策略　Policy

入侵检测系统的策略是指对于IP网络中的攻击事件采取何种响应方式和响应条件。多个策略构成策略集。

策略模板　Policy Template

入侵检测系统中的策略模板是策略集的表现形式，采用直观的名称对策略集进行区分。

规则　Rule

入侵检测规则包含了对网络中攻击事件进行评判的依据及对该事件采用的策略，多个规则构成规则集。

特征　Signature

入侵检测系统的特征是使入侵检测系统在攻击行为发生时触发事件的依据。多个特征可以构成特征库。

隐藏　Stealth

隐藏是指网络入侵检测系统在检测攻击时不为外界所见。

4 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	访问控制列表
CPU	Central Processing Unit	中央处理单元
DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
FTP	File Transfer Protocol	文件传输协议
HTTP	Hypertext Transfer Protocol	超文本传输协议
IP	Internet Protocal	互联网协议
POP3	Post Office Protocol: Version 3	邮局协议第3版
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
TCP	Transmission Control Protocol	传输控制协议

5 系统描述

网络入侵检测系统是指从IP网络的若干关键点收集信息并对其进行分析，从中发现网络中是否有违反安全策略的行为或遭到入侵的迹象，并依据既定的策略采取一定措施的软件与硬件的组合。按照功能划分，网络入侵检测系统至少要包括4个基本组件：事件产生器、事件分析器、响应单元和事件数据库。网络入侵检测系统的框架如图1所示。

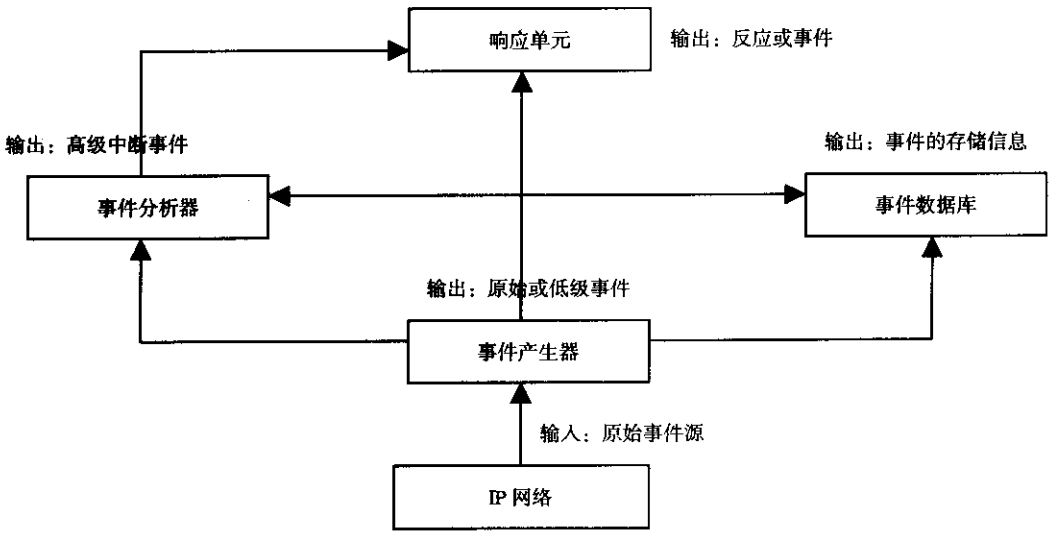

图 1 网络入侵检测系统的框架

4个组件的关系是：事件产生器的任务是通过监听所处的IP网络从而提取关心的事件并转化为一定格式以供其他组件使用；事件分析器接收这些事件，并且分析它们是否是入侵行为，结果依然转化为相应格式的事件；响应单元根据命令系统执行特定行为的事件做出相应响应；事件数据库存储事件以备将来使用。

在网络入侵检测系统框架中，事件产生器、事件分析器和响应单元通常以应用程序的形式出现，而事件数据库则往往以文件或数据流的形式出现。4个组件只是逻辑实体，它们以事件的形式进行数据交换。

以上4个组件是网络入侵检测系统最核心的部分，可以完成最基本的入侵检测功能。但是作为一个完整的网络入侵检测系统，系统管理组件和日志审计组件也是必不可少的。系统管理完成对系统的操作与配置，而日志审计是任何安全设备必须具备的功能。

5.1 事件产生器

对于网络入侵检测系统来说，事件产生器从系统所处的IP网络环境中收集事件，并将这些事件转换成一定格式以传送给其它组件。可以说，事件产生器是实时监视网络数据流并依据入侵检测规则产生事件的一种过滤器。

5.2 事件分析器

事件分析器分析从事件产生器收到的事件，并经过分析以后产生新的事件传送给其它组件。事件分析器既可以是一个特征检测工具，用于在一个事件序列中检查是否有已知的攻击特征；也可以是一个统计分析工具，检查现在的事件是否与以前某个事件来自同一个事件序列；此外，事件分析器还可以是一个相关器，观察事件之间的关系，将有联系的事件放到一起，以利于以后进一步分析。

具体检测内容参见第6章。

5.3 事件数据库

事件数据库用来临时存储事件，以备系统需要的时候使用。

5.4 响应单元

响应单元处理收到的事件，并依据策略采取相应的反应措施。

具体响应方式参见第7章。

5.5 系统管理

负责网络入侵检测系统的管理，主要包括角色管理、设备管理、规则管理和升级管理。

具体内容参见第8章。

5.6 日志审计

系统应该提供详细日志记录及查询统计功能，日志审计至少包括两部分：操作日志审计和入侵检测日志审计。

具体内容参见第9章。

6 检测内容

网络入侵检测系统的主要功能包括以下几方面内容。

6.1 协议分析

可以对基于TCP/IP的各种协议（如HTTP、FTP、TELNET、SMTP和POP3等）进行分析、解码，并提取特征信息。网络入侵检测系统至少可以识别如下信息：

- 协议主体
- 协议客体
- 协议类型
- 协议内容

6.2 攻击识别

网络攻击一般分为以下5类：信息探测类、拒绝服务类、蠕虫病毒类、权限获取类和可疑网络活动类。

信息探测类：搜集对计算机和网络信息的攻击尝试行为，包括端口扫描、漏洞扫描等。

拒绝服务类：破坏计算机和网络资源可用性的攻击行为，包括各种DoS、DDoS攻击等。

蠕虫病毒类：通过病毒进行的攻击行为，包括蠕虫（即网络病毒）、邮件病毒等。

权限获取类：非法获取更高权限的攻击行为，包括后门攻击、木马攻击和缓冲区溢出攻击等。

可疑网络活动类：不确定，但有可能是攻击的行为，或者用户自定义的网络违规行为。

网络入侵检测系统在协议分析的基础上，结合攻击特征模式匹配和异常统计等技术，应能检测出以上种类中的若干种攻击行为。

6.3 躲避识别

躲避是指入侵者发动攻击，而又不希望被发现而采取的行为，而躲避识别则是为了对抗网络入侵者的各种躲避行为。为识别躲避行为，网络入侵检测系统应具备如下功能：

- IP碎片重组：对所监视的网络中的IP碎片包重组后进行分析，防止碎片欺骗。
- TCP流重组：对所监视的网络中乱序的TCP流重新排序，从而对完整的网络对话进行分析。

7 响应方式

7.1 响应方式分类

在检测到入侵攻击后，网络入侵检测系统的响应单元主要有两类响应方式：被动响应方式和主动响应方式。被动响应方式是系统在检测出入侵攻击后只是产生报警和日志通知具有系统管理角色的实体，具体处理工作由此实体完成；主动响应方式是系统在检测出入侵攻击后可以自动对目标系统或者相应网络设备做出修改制止入侵行为。

网络入侵检测系统的响应单元应具备以下主动响应方式和被动响应方式中的一种或者多种。

7.2 被动响应方式

7.2.1 报警功能

当系统检测到入侵事件产生时，响应单元应将报警信息以邮件、SNMP Trap、声光告警、焦点窗口等形式中的一种或者几种提交具有系统管理角色的实体。报警信息至少应包括以下内容：

- 事件主体
- 事件客体
- 发生时间
- 事件类型
- 事件内容
- 事件级别

7.2.2 生成日志

当系统检测到入侵事件产生时，响应单元应将入侵事件记录到日志中，日志记录应至少包括以下字段：

- 事件主体
- 事件客体
- 发生时间
- 事件类型
- 事件内容

- 事件级别

7.2.3 自定义被动响应

为了满足实际需求，系统还可以提供具有系统管理角色的实体以自定义的被动响应方式来响应入侵事件。

7.3 主动响应方式

7.3.1 联动响应

系统可以通过相应的控制方式和其它网络设备（如路由器、交换机等）或安全系统（如防火墙、漏洞扫描系统等）进行联动。

与网络设备联动是指系统发现了入侵事件后，通知指定的网络设备（如路由器、交换机等），利用网络设备自身的命令（如ACL控制命令）来修改访问控制策略，对入侵行为进行主动响应，如阻断。

与安全系统联动是指系统发现了入侵事件后，通知指定的安全系统（如防火墙等），由安全系统执行一些安全措施，对入侵行为进行主动响应。如通知防火墙修改当前访问控制策略以对攻击行为进行阻断。

为保证联动安全性，系统应提供与其它网络设备或安全系统之间的身份认证，联动消息也应采取措施保证机密性和完整性。

7.3.2 实时切断会话连接

当系统检测到入侵事件后，响应单元可以通过发送特定的阻断信息来实现阻断当前连接。系统应至少支持通过发送TCP Reset报文来切断特定的TCP会话连接。

7.3.3 自定义的响应程序

为了满足实际需求，系统还可以提供具有系统管理角色的实体以自定义的主动响应方式来响应入侵事件。

8 系统管理

网络入侵检测系统的系统管理应包括以下几个部分：角色管理、设备管理、规则管理和升级管理。

8.1 角色管理

网络入侵检测系统需要采用不同的角色进行管理。网络入侵检测系统应提供三种不同管理角色：用户管理角色、系统管理角色和审计管理角色。

- 用户管理角色：可以生成、删除系统管理角色的账号，调整系统管理角色对应账号的具体操作权限，但用户管理角色不能调整自身和审计管理角色的权限；
- 系统管理角色：具有对IDS的管理权限，如：配置入侵检测规则、查看入侵检测日志、报警响应等权限，但无用户管理和用户系统操作日志审计功能；
- 审计管理角色：仅具有对系统操作日志的查看、备份、删除的权限，并可以进行可选的用户审计配置、审计日志的完整性检查及登陆失败处理。

对于所有权限的管理角色，都要有详细的登录记录和操作记录，以备参看。

8.2 设备管理

系统中具有系统管理角色的实体可以查看网络入侵检测系统的网络接口状态、组件的工作状态、当前的日志文件大小、CPU占用率、内存占用率、存储器占用率以及软硬件版本信息。

具有系统管理角色的实体可以配置以上网络入侵检测系统组件的参数以及状态；设置管理接口的通讯参数；启动或者停止系统运行。

具体具有系统管理角色的实体所对应的管理权限可以由具有用户管理角色的实体来设置。

8.3 规则管理

系统应提供多种定制缺省策略模板，具有系统管理角色的实体可以根据自己的网络情况选择模板或编辑定制策略模板。

具有系统管理角色的实体可以查询当前策略配置；并可以根据需要增加、删除与修改入侵检测规则；对系统内置的入侵规则，用户可以根据需要进行修改。

网络入侵检测系统应尽可能多地为具有系统管理角色的实体提供灵活的入侵规则定制功能，使之可根据自身网络环境及需求对已有规则进行选择，或根据自己的认识定义特征，从而产生新的规则，并确定这些规则的响应方式，使之能够对系统的检测内容和响应方式做到灵活的控制。

网络入侵检测系统应能导入导出入侵检测规则。

8.4 升级管理

网络入侵检测系统应支持系统升级管理，以对抗新的攻击方式和系统漏洞。升级应包括系统软件的升级和对入侵特征库升级两部分。升级方式既要支持手工升级方式，也要支持自动升级方式。

9 日志审计

网络入侵检测系统应包括入侵检测日志和系统操作日志。

9.1 入侵检测日志

针对每一个攻击事件，入侵检测日志都要记录其详细的信息，应包括如下字段：

- 事件主体
- 事件客体
- 发生时间
- 事件类型
- 事件内容
- 事件级别

其中，事件级别建议参考SYS-LOG的日志输出信息格式和代码，采用通用的8个级别，具体见下表。

序　号	等　级	描　述
0	LOG_EMERG	紧急事件
1	LOG_ALERT	重要事件
2	LOG_CRIT	关键事件
3	LOG_ERR	普通事件
4	LOG_WARNING	警告事件
5	LOG_NOTICE	需注意事件
6	LOG_INFO	提示事件
7	LOG_DEBUG	调试信息

9.2 系统操作日志

针对系统的所有登录以及操作事件，系统都要有详细的记录，应包括如下字段：

- 操作者
- 操作时间

- 操作内容
- 是否成功

9.3 审计功能

日志数据的存储时间应能够满足用户的要求，统计数据最低存储时间不低于一个月，原始数据最低存储时间不低于一个星期。

日志数据可以以文件或者数据库的形式存储于磁带、磁盘等永久性存储介质中，而且需支持日志的转储和备份。当系统内的日志数据超过预定义的域值时，系统应及时通知进行外部备份；

具有系统管理角色的实体可以查询和审阅入侵检测日志。

网络入侵检测系统应严格保护系统操作日志，只有具有审计管理角色的实体可以查询和审阅全部系统操作日志，并可以在确认后删除日志数据。

10 自身安全

和其它系统一样，网络入侵检测系统也可能存在安全漏洞。若对该系统攻击成功，则会导致其工作失灵。因此网络入侵检测系统首先要保证自身的安全。具体要求如下：

10.1 系统安全

系统除了管理端口可以配置有效IP地址以外，其它端口都不设IP地址。

系统不允许启用任何Internet 服务（远程管理除外）。

网络入侵检测系统各组件之间需要通过网络进行通信时，应能对各组件间的通信进行加密。

10.2 管理安全

角色管理（具体内容参见第8.1节）。

系统应具备严格的访问控制机制，一般采用身份认证形式确保具有管理角色的实体的身份，非授权人员不能管理检测系统。

具有管理角色的实体在一定时限内失败的登录次数超过设定限值，系统应阻止该实体进一步的登录或在设定时间内无法登录。

具有管理角色的实体在设定时间内没有任何操作，则自动退出。如要进行其它操作，必须重新登录。

对于远程管理应采用加密信道对传输信息进行处理，保证数据机密性和完整性。

系统必须严格按照操作日志格式记录所有的登录与操作事件。

11 性能指标

网络入侵检测系统的指标主要包括3类：准确性指标、效率指标和系统指标。

11.1 准确性指标

准确性指标在很大程度上取决于测试时采用的样本集和测试环境。样本集和测试环境不同，准确性也不相同。因此，本标准对检测率、误报率和漏报率的准确性数值不作统一规范，只作为重要的性能指标供比较。

11.1.1 检测率

检测率是指被监视网络在受到入侵攻击时，系统能够正确报警的概率。通常利用已知入侵攻击的实验数据集合来测试系统的检测率。

检测率=入侵报警的数量/入侵攻击的数量

11.1.2 误报率

误报率是指系统把正常行为作为入侵攻击而进行报警的概率和把一种周知的攻击错误报告为另一种攻击的概率。

误报率=错误报警数量/（总体正常行为样本数量+总体攻击样本数量）

11.1.3 漏报率

漏报率是指被检测网络受到入侵攻击时，系统不能正确报警的概率。通常利用已知入侵攻击的实验数据集合来测试系统的漏报率。

漏报率=不能报警的数量/入侵攻击的数量

11.2 效率指标

效率指标根据用户系统的实际需求，以保证检测质量为准；同时取决于不同的设备级别，如百兆比网络入侵检测系统和千兆比网络入侵检测系统。这里不做强制性的量化规定或建议。与准确性指标一样，只作为重要的性能指标供比较。

11.2.1 最大处理能力

指网络入侵检测系统在检测率下系统没有漏警的最大处理能力。目的是验证系统在检测率下能够正常报警的最大流量。最大处理能力应该达到接口标称速率的80%。

11.2.2 每秒并发 TCP 会话数

网络入侵检测系统每秒最大可以增加的TCP连接数。

11.2.3 最大并发 TCP 会话数

网络入侵检测系统最大可以同时支持的TCP连接数。

11.3 系统指标

11.3.1 最大规则数

系统允许具有系统管理角色的实体配置的入侵检测规则条目的最大数。

11.3.2 平均无故障间隔

系统无故障连续工作的平均时间间隔。

12 物理安全

网络入侵检测系统设备的安全特性，应符合GB 4943-2001《信息技术设备的安全》的相关规定。

系统设备的电磁兼容性，应符合GB 9254-1998 《信息技术设备的无线电骚扰限值和测量方法》和GB/T 17618-1998 《信息技术设备抗扰限值和测量方法》的相关规定。

附 录 A
（资料性附录）
事件分类

原始事件：由事件产生器产生可以直接判断或由事件产生器产生专门供事件分析器统计分析判断的事件，一般是针对 TCP/IP 协议中传输层以及传输层以下的事件。原始事件在事件数据库没有缺省对应关系，也不需要进入事件数据库，除非用户自己定义该类事件。例如：对于限制 IP 地址和端口的检测规则，只要事件产生器检测到包含有相应 IP 地址和端口的原始事件（即 IP 数据包）就可以判断为攻击并交予响应单元响应；对于基于传输层或传输层以下的 DOS 攻击，一般在事件分析器有一个统计计数器（对于 TCP 层还有状态记录和维护），在单位时间内相应原始事件计数达到限制域值即可判断为攻击，形成高级中断事件并交予响应单元响应。

低级事件：由事件产生器产生可以直接判断，或者需要事件分析器进行高级分析判断，或者需要临时存储在事件数据库以便事件分析器分析判断的事件，一般是针对 TCP/IP 协议中传输层以上的事件。低级事件在事件数据库有缺省对应关系，可以临时存储在事件数据库中供事件分析器进行高级分析判断。例如：对于协议（比如：Telnet、HTTP 等）有限制的检测规则，只要事件产生器检测到相应限制的事件就可以判断为攻击并交予响应单元响应；对于网络应用的口令猜测或者利用多个会话完成一次攻击的行为，就必须统计或关联多个低级事件。只要符合相应的关联或统计规则就可以判断为攻击，形成高级中断事件并交予响应单元响应。

高级中断事件：由事件分析器对采集到原始事件、低级事件进行统计分析或关联分析判断后输出的事件，可交付响应单元做相应响应。

参考文献

The Common Intrusion Detection Framework Architecture　通用入侵检测框架结构