ICS 35.040
L 80

中华人民共和国国家标准

GB/T 28454—2020
代替 GB/T 28454—2012

信息技术　安全技术　入侵检测和防御系统（IDPS）的选择、部署和操作

Information technology—Security techniques—Selection, deployment and operation of intrusion detection and prevention systems (IDPS)

(ISO/IEC 27039:2015,MOD)

2020-04-28 发布　　2020-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 28454—2012《信息技术　安全技术　入侵检测系统的选择、部署和操作》。与 GB/T 28454—2012 相比，主要技术变化如下：

——修改了入侵检测系统 IDS 为入侵检测和防御系统(IDPS)，将入侵防御系统 IPS 纳入标准范围；

——修改了标准范围，增加标准适用对象(见第 1 章，2012 年版的第 1 章)；

——修改了部分术语和定义，包括“攻击”“拒绝服务攻击”“非军事区”“入侵者”“入侵”“路由器”“交换机”“特洛伊木马”“攻击特征”“防火墙”“主机”“入侵检测系统”“入侵防御系统”“在线升级”“探测器”“测试接入点”，增加了部分术语和定义，包括“分布式拒绝服务攻击”“入侵检测和防御系统”“病毒”“虚拟专用网”“脆弱性”(见第 3 章，2012 年版的第3 章)；

——增加了部分缩略语，包括 AIDPS、DMZ、DDoS、DoS、IDPS、I/O、IODEF、HIDPS、SIEM、VPN，删除缩略语 NIDS、SIM(见第 4 章，2012 年版的第 4 章)；

——删除背景中关于 IDPS 基础知识的介绍(见第 5 章，2012 年版的第 5 章)；

——因增加入侵防御系统，修改“当组织对 IDS 产品有安全等级方面的要求时，见 GB/T 20275”为“当对 IDPS 产品有安全等级方面的要求时，见 GB/T 20275 和 GB/T 28451。”(见 7.3.1，2012 年版的 7.2)；

——增加云计算环境中 IDPS 选择考虑事项(见 7.4.1、7.4.2、7.4.3、7.4.5)和云环境下 IDPS 部署方式、多层级组织中 IDPS 部署方式等(见 8.1)；

——“能力的确认”修改为“能力的验证”(见 7.4.5，2012 年版的 7.3.5)；

——修改 SIEM 功能，增加了事态关联、事态过滤、事态聚合(见 7.5.6，2012 年版的 7.4.6)；

——删除响应中关于 IDS 和 IPS 介绍的相关内容(见 9.5.2)。

本标准使用重新起草法修改采用 ISO/IEC 27039:2015《信息技术　安全技术　入侵检测和防御系统(IDPS)的选择、部署和操作》。

本标准与 ISO/IEC 27039:2015 相比，在结构上增加了第 2 章“规范性引用文件”和第 4 章“缩略语”，将 7.3.1 和 7.3.2 的内容进行调序。

本标准与 ISO/IEC 27039:2015 的技术性差异及其原因如下：

——增加了第 2 章“规范性引用文件”和第 4 章“缩略语”，主要保持与 GB/T 28454—2012 的延续性；

——删除第 3 章背景中关于 IDPS 基础知识的介绍(见第 5 章)，因该内容在附录 A 中有详细介绍；

——增加了“当对 IDPS 产品有安全等级方面的要求时，见 GB/T 20275 和 GB/T 28451”，这主要是考虑对 IDPS 产品安全等级保护要求(见 7.3.1)；

——删除 7.5.2 关于 IDS 和 IPS 的相关内容(见 9.5.2)，因标准将入侵防御系统 IPS 纳入本标准范围，标准对象界定为入侵检测和防御系统 IDPS，故无需再单独介绍；

——增加了云计算环境中 IDPS 选择考虑事项(见 7.4.1、7.4.2、7.4.3、7.4.5)以及云环境下 IDPS 部署、多层级组织中 IDPS 部署，主要是因为目前云计算环境中 IDPS 部署也需要考虑相关事项，但国际标准并未考虑此部分内容(见 8.1)。

本标准做了下列编辑性修改：

——删除 3.8 的注。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东省标准化研究院、中国网络安全审查技术与认证中心、陕西省网络与信息安全测评中心、北京天融信网络安全技术有限公司、山东崇弘信息技术有限公司、成都秦川物联网科技股份有限公司。

本标准主要起草人:王曙光、王庆升、王凤娇、魏军、公伟、张斌、来永钧、杨帆、杨锐、雷晓峰、邵泽华、樊华、朱琳、高瑞、杨向东、杨斌、权亚强、路征、陈慧勤、刘勘伪、于秀彦、胡鑫磊、王栋、潘海燕、李红胜。

本标准所代替标准的历次版本发布情况为:

——GB/T 28454—2012。

引　言

组织在选择、部署入侵检测和防御系统(IDPS)之前，不仅需要知道入侵事件(针对网络、系统或应用)是否发生、何时发生以及如何发生，也需要知道入侵事件利用了何种脆弱性，为防止类似入侵事件发生，未来需要采取何种防护措施或风险处置手段(即风险缓解、风险保留、风险规避、风险分担)。组织需识别并避免基于网络的入侵。从20世纪90年代中期开始，组织为了满足上述需求开始使用入侵检测和防御系统(IDPS)。随着IDPS产品的不断发展，其应用领域不断扩大，满足了组织对入侵检测和防御能力持续增长的需求。

为了使IDPS效益最大化，需要由经过培训、经验丰富的人员精心策划及实施IDPS的选择、部署和操作过程。通过上述过程，使IDPS成为组织预防入侵的重要安全工具(在组织ICT基础设施中作为重要安全设施)，帮助组织截获入侵信息。

本标准提供了有效选择、部署和操作IDPS的指南，以及有关IDPS的基础知识。同时本标准还适用于需要外包其IDPS服务的相关组织。关于外包服务级别协议的相关信息参见ISO/IEC 20000的IT服务管理(ITSM)过程。

本标准主要用于帮助组织实现如下目标：

a) 满足GB/T 22080的下列要求：

——应实施过程和控制以便能快速检测和响应安全事件；

——应执行监视、评审过程以及控制以便识别企图的安全危害和既成的安全事件。

b) 实现控制以满足GB/T 22081的下列安全目标：

——能够检测未授权的信息处理活动；

——监视系统并记录信息安全事态，使用操作者日志和默认日志以确保能够识别信息系统问题；

——满足所有适用于监视和记录活动的相关法律要求；

——将系统监视用于检查已实施控制的有效性，以验证访问策略模型是否符合需求。

对满足上述要求而言，部署IDPS并非唯一、完善的解决方案。此外，本标准并不作为诸如信息安全管理体系(ISMS)认证、IDPS服务或产品认证等合格评定的准则。

信息技术　安全技术　入侵检测和防御系统（IDPS）的选择、部署和操作

1　范围

本标准给出了组织部署入侵检测和防御系统（IDPS）的指南。本标准详细说明了 IDPS 的选择、部署和操作。同时本标准给出了形成这些指南的背景信息。

本标准适用于准备部署入侵检测和防御系统（IDPS）的组织。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 18336（所有部分）　信息技术　安全技术　信息技术安全评估准则[ISO/IEC 15408（所有部分）]

GB/T 20275　信息安全技术　网络入侵检测系统技术要求和测试评价方法

GB/T 20985.1—2017　信息技术　安全技术　信息安全事件管理　第 1 部分：事件管理原理（ISO/IEC 27035-1：2006，IDT）

GB/T 25068.2　信息技术　安全技术　IT 网络安全　第 2 部分：网络安全体系结构（ISO/IEC 18028-2：2006，IDT）

GB/T 28451　信息安全技术　网络型入侵防御产品技术要求和测试评价方法

GB/T 29246—2017　信息技术　安全技术　信息安全管理体系　概述和词汇（ISO/IEC 27000：2016，IDT）

3　术语和定义

GB/T 29246—2017 界定的以及下列术语和定义适用于本文件。

3.1

攻击　attack

企图破坏、泄露、篡改、损伤、窃取、未授权访问或未授权使用资产的行为。

[GB/T 29246—2017，定义 2.3]

3.2

攻击特征　attack signature

执行某种攻击的计算机活动系列或其变体，通常通过检查网络流量或主机日志加以确定，IDPS 也依其来发现已经发生的攻击。

注：这也可称为一个攻击模式。

3.3

证明　attestation

公钥加密而产生的变量，可使 IDPS 软件程序和设备鉴别其远程方的身份。

注：见 3.23 远程证明。

3.4

网桥 bridge

将位于 OSI 2 层的局域网连接到采用相同协议的另一局域网的网络设备。

3.5

密码散列值 cryptographic hash value

分配给一个文件并在后期用来测试这个文件的数学值，以验证包含在文件中的数据没有被恶意更改。

3.6

拒绝服务攻击 denial-of-service attack；DoS

未授权访问系统资源或者延迟系统操作和功能。

3.7

分布式拒绝服务攻击 distributed denial-of-service attack；DDoS

通过洪水攻击带宽或目标系统的资源，破坏多个系统的方式来未授权访问系统资源或者延迟系统操作和功能，导致授权用户失去可用性。

3.8

非军事区 demilitarized zone；DMZ

位于边界路由器和外部防火墙之间的逻辑或者物理网络空间。

3.9

（脆弱性）利用 （vulnerability） exploit

已明确定义的利用脆弱性破坏信息系统安全的一种方式。

3.10

防火墙 firewall

设置在网络环境之间的一类屏障。

注：它可以是一台专用设备，也可以是若干部件和技术的组合。网络环境间所有通信都要流经防火墙，只允许按照本地安全策略定义的、已授权的通信通过。

3.11

误报 false positive

没有攻击时 IDPS 有报警的情况。

3.12

漏报 false negative

攻击发生时 IDPS 没有报警的情况。

3.13

蜜罐 honeypot

用来欺骗、扰乱和引开攻击者的诱饵系统，促使攻击者把时间花在某些信息上，这些信息看起来有价值，实际上是虚假的，对合法用户没有任何价值。

3.14

主机 host

基于 TCP/IP 协议网络（如 Internet），可设定地址的系统或计算机。

3.15

入侵者 intruder

针对目标主机、站点、网络或组织，正在或已经进行入侵或攻击的个体。

3.16

入侵 intrusion

对某一网络或联网系统的未授权访问，即对某一信息系统的有意或无意的未授权访问，包括针对信

息系统的恶意活动或者信息系统内资源的未授权使用。

3.17

入侵检测　intrusion detection

检测入侵的正式过程。该过程一般特征为采集如下知识:反常的使用模式、被利用的脆弱性及其类型、利用的方式,以及何时发生和如何发生。

3.18

入侵检测系统　intrusion detection system:IDS

在信息系统和网络中,一种用于辨识某些已经尝试、正在发生或已经发生的入侵行为,并可对其做出响应的技术系统。

3.19

入侵防御系统　intrusion prevention system:IPS

特别设计用来提供主动响应能力的入侵检测系统的变体。

3.20

入侵检测和防御系统　intrusion detection and prevention system:IDPS

为了防范恶意活动而监视系统的入侵检测系统 IDS 和入侵防御系统 IPS 的软件应用或设备,IDS 仅能对发现的这些活动予以报警,而 IPS 则有能力阻止某些检测到的入侵。

注:如果需要防范攻击,IPS 将主动部署在网络中。如果部署在被动模式下,它将不能提供上述功能,其有效功能仅能像常规 IDS 那样提供报警。

3.21

渗透　penetration

绕过系统安全机制、未经授权的行为。

3.22

在线升级　provisioning

为信息技术(IT)设备安装正确软件、执行安全策略及加载配置数据的过程。

3.23

远程证明　remote attestation

使用数字证书来确保 IDPS 的身份及其软件和硬件配置,并安全地将信息传输到可信操作中心的过程。

3.24

响应　response

事件响应或入侵响应　incident response or intrusion response

当攻击或入侵发生时,为了保护和恢复信息系统正常运行的条件以及存储在其中的信息而采取的行动。

3.25

路由器　router

通过基于路由协议机制和算法选择路径或路由,建立和控制不同网络之间数据流的网络设备。

注 1:其自身可基于不同的网络协议。

注 2:路由信息存储在路由表内。

3.26

服务器　server

为其他计算机提供服务的计算机系统或程序。

3.27

服务级别协议　service level agreement:SLA

规定技术支持或业务性能目标的合同,包括服务提供方提供给其客户的性能以及对失败结果的

测量。

3.28

传感器　sensor

从被观察的信息系统或网络中，通过感知、监测等收集事态数据的一种 IDPS 部件或代理。

注：也称为监视器。

3.29

子网　subnet

在某一网络中，共享某一公共地址成分的部分。

3.30

交换机　switch

在联网的设备之间，一种借助内部交换机制来提供连通性的设备。其交换技术通常在 OSI 参考模型的 2 层或 3 层实现。

注：交换机不同于其他局域网互联设备(例如，集线器)，原因是交换机中使用的技术是以点对点为基础建立连接。确保了网络通信量只对有地址的网络设备可见，并使几个连接能够并存。

3.31

测试接入点　test access points；TAP

典型的被动设备，不会在网络信息包中加装任何负载；当它们使数据收集接口在网络中不可见时，也能提高安全级别，在这里交换机仍然可保持端口的 2 层信息。

注：TAP 也给出了多端口的功能，这样在不丧失 IDPS 能力的情况下，可以调试网络问题。

3.32

特洛伊木马　Trojan horse

一种伪装成良性应用软件的恶意程序。

3.33

病毒　virus

一种带有不良意图的恶意软件，可直接或间接地对用户和(或)用户系统造成潜在伤害。

3.34

虚拟专用网　virtual private network；VPN

利用物理网络的系统资源而构建的限制性使用的逻辑计算机网络，例如，使用加密技术和/或虚拟网络的隧道链接来跨越真实网络。

[GB/T 25068.3—2010，定义 3.23]

3.35

脆弱性　vulnerability

可能被一个或多个威胁利用的资产或控制的弱点。

[GB/T 29246—2017，定义 2.89]

4　缩略语

下列缩略语适用于本文件。

AIDPS：基于应用的 IDPS(Application-based IDPS)

API：应用程序编程接口(Application Programming Interface)

ARP：地址解析协议(Address Resolution Protocol)

CGI：通用网关接口(Common Gateway Interface)

CPU：中央处理器(Central Processing Unit)

DMZ:非军事区(Demilitarized Zone)
DNS:域名系统(Domain Name System)
DDoS:分布式拒绝服务(Distributed Denial of Service)
DoS:拒绝服务(Denial of Service)
ICMP:网际控制报文协议(Internet Control Message Protocol)
IDS:入侵检测系统(Intrusion Detection System)
IDPS:入侵检测和防御系统(Intrusion Detection and Prevention Systems)
I/O:输入/输出(Input/Output)
IODEF:事件对象描述交换格式(Incident Object Description Exchange Format)
IP:网际协议(Internet Protocol)
IPS:入侵防御系统(Intrusion Prevention System)
ISIRT:信息安全事件响应团队(Information Security Incident Response Team)
IT:信息技术(Information Technology)
HIDS:基于主机的 IDS(Host-based IDS)
HIDPS:基于主机的 IDPS(Host-based IDPS)
HIPS:基于主机的 IPS(Host-based IPS)
HTTP:超文本传送协议(Hypertext Transfer Protocol)
MAC:媒体访问控制(Media Access Control)
MIB:管理信息库(Management Information Base)
NIDPS:基于网络的 IDPS(Network-based IDPS)
NIPS:基于网络的 IPS(Network-based IPS)
NOC:网络运行中心(Network Operations Center)
OSI:开放系统互连(Open System Interconnection)
RID:实时网络防御(Real-time Intern-network Defense)
ROI:投资回报率(Return On Investment)
SIEM:安全信息和事态管理(Security Information Event Management)
SMS:短消息系统(Short Message System)
SLA:服务级别协议(Service Level Agreement)
SMTP:简单邮件传送协议(Simple Mail Transfer Protocol)
SNMP:简单网络管理协议(Simple Network Management Protocol)
SPAN:交换机端口分析器(Switch Port Analyzer)
TAP:测试接入点(Test Access Points)
TCP:传输控制协议(Transport Control Protocol)
UDP:用户数据报协议(User Datagram Protocol)
VPN:虚拟专用网络(Virtual Private Network)

5 背景

部署入侵检测和防御系统(IDPS)的目的是监视、检测和记录不适当、不正确、可疑或异常的活动,当检测到这些活动时,IDPS 会发出报警信号和(或)自动响应。IT 安全人员负责评估这些报警信号和相关日志并做出恰当的响应。因此,当需要对组织信息系统的入侵进行检测并给出响应时,可以考虑部署 IDPS。此时,既可通过直接获取 IDPS 软硬件产品的方式部署 IDPS,也可通过向 IDPS 服务提供商外包 IDPS 业务的方式部署 IDPS。

目前，可供选择的 IDPS 产品和服务众多，有付费的商业产品也有免费开源的。不同的 IDPS 产品和服务采用不同的技术和方法。此外，IDPS 并不是“即插即用”的，需要专业人员进行安装部署，因此当准备部署 IDPS 时，相关人员需要熟悉本标准提供的指南和相关信息。

关于 IDPS 的基础知识参见附录 A。

6 总则

综合考虑 IDPS 的功能和局限性(参见附录 A)，组织可把基于主机的方法(包括应用监视)和基于网络的方法结合起来，以应对各种潜在入侵。根据每类 IDPS 的优缺点，将其结合起来，能更好地处理安全事态以及提供报警分析。

不同 IDPS 技术的结合主要依赖于 IDPS 报警管理系统中关联模块的可用性。人工关联 HIDPS 和 NIDPS 报警信息无任何优点，却会导致操作人员超负荷工作，其结果比从一种 IDPS 中选取最合适的输出方式效果更差。

在组织内选择、部署和操作 IDPS 的过程如图 1 所示，第 7 章～第 9 章将详细描述本过程中的关键步骤。

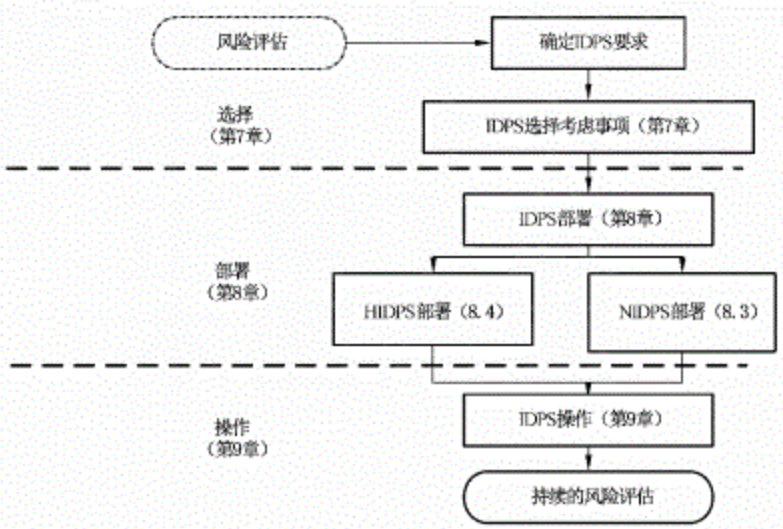

图 1 IDPS 的选择、部署和操作

7 选择

7.1 简介

可供选择的 IDPS 产品种类很多，既包含免费产品(可在低成本主机上部署)，也包含较为昂贵的商用收费产品(需要最新的硬件支持)。由于可供选择的 IDPS 产品较多，因此需要综合考虑组织需求选择最符合要求的产品。另外，不同 IDPS 产品会存在兼容性问题，同一组织使用不同 IDPS 产品(由于组织的兼并以及广泛的地理分布问题，不得不使用不同的 IDPS 产品)时的还需要关注不同 IDPS 的集成问题。

供应商提供的 IDPS 说明书给出了 IDPS 可以检测到的攻击类型，但在大流量网络中却无法描述 IDPS 如何较好地检测出入侵，无法给出部署、操作和维护 IDPS 的难度，因为在对组织网络流量缺乏了解前提下，也无法准确描述 IDPS 如何有效地避免漏报和误报。同时，还需要根据组织自身要求，独立地评估 IDPS 的主动响应和被动响应的能力(此时，主要考虑深度数据包检测和重组的需要，而不考虑

网络性能和成本)。因此,仅依赖供应商提供的 IDPS 说明书来了解 IDPS 的能力是远远不够的,需根据组织自身需要选择 IDPS 产品。

GB/T 18336 可用于 IDPS 第三方评价。此时,不同于 IDPS 说明书,"安全目标"文件可更准确可靠地描述 IDPS 性能,其将作为选择 IDPS 的重要考虑因素。

IDPS 选择过程中需要重点关注 7.2～7.7 的相关要素。

7.2 信息安全风险评估

选择 IDPS 之前,首先需要实施信息安全风险评估,在考虑相关因素(诸如信息系统使用信息的性质、需要如何保护这些信息、使用的通信系统类型以及其他操作和环境的因素)基础上,识别针对组织信息系统(可能存在脆弱性)的攻击和入侵(威胁)。然后根据组织信息安全目标,针对这些潜在威胁,识别出可以有效降低风险的低成本控制。这些控制可作为选择 IDPS 的基础。

注:信息安全风险评估和管理是 GB/T 22080 的主题。

IDPS 安装完成并开始运行后,需要根据系统操作的变更和威胁环境的变化,持续实施风险管理过程,以便周期性地评审控制的有效性。

7.3 主机或网络 IDPS

7.3.1 概述

IDPS 的部署需要基于组织信息安全风险评估和资产保护优先级,同时选择 IDPS 时需要研究 IDPS 监视事态最有效的方法,即选择 NIDPS 和 HIDPS 共同部署:首先分阶段部署 NIDPS(因为 NIDPS 安装和维护通常最简单),然后在关键服务器上部署 HIDPS。

每种选择方式都有其优缺点。例如,将 IDPS 部署在外部防火墙之外时,由于外部防火墙能有效阻止大量需要扫描的报警事态,因此 IDPS 不需要对大部分报警事态进行深入分析。

当对 IDPS 产品有安全等级方面的要求时,按照 GB/T 20275 和 GB/T 28451 执行。

7.3.2 基于网络的 IDPS(NIDPS)

当部署 NIDPS 时,将传感器主要放置在如下位置:

——外部防火墙之内;

——外部防火墙之外;

——主要的骨干网络上;

——关键子网上。

7.3.3 基于主机的 IDPS(HIDPS)

当选择 HIDPS 时,需识别目标主机,同时由于其部署成本较高,因此需根据目标主机风险分析结果和成本效益(对主机进行优先级排序),优先在关键主机上部署 HIDPS。当 HIDPS 部署的主机数量较大时,需要考虑部署具备集中管理和报告功能的 IDPS。

7.4 考虑事项

7.4.1 系统环境

在信息安全风险评估的基础上,首先确定需要保护的资产优先级,然后记录并综合考虑如下系统环境信息,在此基础上选择定制合适的 IDPS:

——网络拓扑图,详细说明主机数量和位置、网络入口以及与外部网络连接点等;

——网络管理系统的描述;

——每个主机的操作系统；
——网络设备(如路由器、网桥和交换机)的数量和类型；
——服务器和拨号线路的数量和类型；
——网络服务器的描述，包括类型、配置、应用软件和正在运行的版本；
——与外部网络的连接，包括标称带宽和支持协议；
——与引入连接路径不同的数据返回路径，即不对称数据流。
当系统部署于云计算平台之上时，还需要考虑收集以下系统环境信息：
——云计算平台的外部边界和内部关键边界；
——云计算平台所使用的虚拟化平台软件信息，包括软件名称、配置、版本等。

7.4.2 安全保护机制

在记录系统环境信息之后，识别已安装的安全保护机制，包括：
——非军事区(DMZ)；
——防火墙和过滤路由器的数量、类型和位置；
——身份鉴别服务器；
——数据和通信链路加密；
——反恶意软件或反病毒包；
——访问控制产品；
——专业的安全硬件，如加密硬件；
——虚拟专用网络(VPNs)；
——其他已安装的安全机制；
——当系统部署在云计算平台上时，云平台多租户之间互访限制及攻击防护。

7.4.3 IDPS 安全策略

在记录系统环境和通用的安全环境信息基础上，制定 IDPS 的安全策略，主要考虑如下因素：
——要监视的信息资产类型；
——未成功打开或未成功关闭时，采取的策略；
——需要的 IDPS 的类型；
——IDPS 部署的位置；
——需要检测的攻击的类型；
——需要记录的信息的类型；
——响应或报警的类型；
——系统环境为云环境时，采用的流量引入 IDPS 方式、产品形态、部署模式。
IDPS 安全策略体现了组织购买 IDPS 的目标，这是从 IDPS 获取收益的开始。
为了详细说明 IDPS 安全策略目的和目标，需首先识别内部和外部风险，在此基础上，可将 IDPS 安全策略定义为一组 IDPS 产生报警的规则。
需要组织依据对 IDPS 系统在保密性、完整性、可用性、抗抵赖性(上述四个为标准安全目标)、隐私、责任保护、易管理性等方面的管理目标需求，对 IDPS 安全策略进行评审(需提供针对 IDPS 需求的模版)。
当 IDPS 检测到安全策略违规时，需确定 IDPS 的响应策略。当对信息安全策略违规进行响应时，需对 IDPS 进行配置，并要求操作人员了解响应策略，以便正确处理 IDPS 报警。例如，可请求执法机构开展调查以帮助解决安全事件，并将相关信息(包括 IDPS 日志)移交执法机构，以获取证据。
安全事件管理相关的其他信息可见 GB/T 20985.1—2017。

7.4.4 性能

选择 IDPS 时，还需要考虑性能因素，至少需包括：

——IDPS 需要处理的带宽的大小；

——在给定带宽下，误报率的最大范围；

——能否为选择高速 IDPS 提供正当理由，或者中速或低速的 IDPS 能否满足需要；

——由于 IDPS 性能局限性，错过潜在入侵的后果；

——当深度包检测和重组发生时，对 IDPS 性能的影响。

组织需避免以下两类 IDPS 的产生：在大多数环境中，IDPS 会错过或者漏掉可能是攻击的一部分流量包；某些时候，随着带宽和(或)网络流量的增加，IDPS 不能再有效和持续地检测入侵(可持续性主要是在给定的可用带宽范围内持续检测攻击的能力)。

结合负载均衡和调整优化可以提高 IDPS 效率和性能。例如：

——需要组织网络及其脆弱性的相关知识：通过信息安全风险评估过程明确需要保护的网络资产(每个网络都是不同的)，这些资产与哪些攻击特征的调整优化有关。

——当 IDPS 用于处理有限数量的网络流量和服务时，其性能会更好。例如，从事电子商务的企业需要监视所有 HTTP 流量并需要调整优化 IDPS，以便查找仅与 web 流量相关的攻击特征。

——恰当地负载均衡配置能使基于特征的 IDPS 运行地更快更彻底，因为基于特征的 IDPS 不需要遍历所有攻击特征的数据库，只需要遍历优化后更小的攻击特征数据库。

在 IDPS 的部署中，负载均衡可用来分割可用带宽，但该措施会产生诸如附加成本、管理开销、流量同步失效、重复报警和漏报等问题。在当前的技术条件下，IDPS 与负载均衡的成本效益比可能是最低的。

7.4.5 能力的验证

仅依靠供应商提供的有关 IDPS 能力的信息通常是不够充分的。因此，选择 IDPS 时，可以要求供应商附加说明，或者给出适用于组织具体环境及安全目标的 IDPS 适用性示范。具体而言，可以要求 IDPS 供应商[大部分 IDPS 供应商具有调整其 IDPS 产品(针对目标网络扩容)的经验，部分供应商在威胁环境中可以支持新协议标准，在平台类型和变更等方面积累了相关经验]提供如下信息对 IDPS 能力进行验证：

——在特定环境中，IDPS 的适用性该做何种假设；

——为验证 IDPS 能力而执行的测试的详细资料；

——对 IDPS 操作人员该做何种假设；

——提供的 IDPS 接口(例如，物理接口、通信协议、与关联引擎交互的报告格式等)；

——报警输出机制或格式，以及它们是否有据可查[例如，格式、系统日志消息或简单网络管理协议(SNMP)消息的管理信息库(MIB)]；

——IDPS 接口是否可以配置快捷键、配置可定制报警功能以及配置自定义攻击特征；

——动态配置 IDPS 时，能够提供的特征是否都有据可查；

——产品能否适应信息系统的发展和变化；

——IDPS 产品能否适应不断扩大、日益多样化的网络；

——IDPS 是否具备自动防故障和故障排除能力，以及这些能力如何与网络链路层上的相同能力集成；

——IDPS 是否为报警使用专用网络，或者报警与监视是否使用相同的网络进行传输；

——在质量保证、脆弱性响应和产品性能记录方面，供应商的信誉如何；

——当部署于云计算环境时，IDPS 在云计算平台中的适用性该做何种假设。

7.4.6 成本

IDPS 成本除了购买 IDPS 软硬件花费的实际成本，其附加成本包括：运行 IDPS 软件系统的购置成本、安装和配置 IDPS 的成本、人员培训和维护成本等，其中最大的成本是管理系统和分析结果的人员成本。目前，测量 IDPS 成本常用的方法是投资回报率(ROI)或成本效益分析。ROI 主要基于管理入侵时节省的成本来计算。成本效益分析主要是要确保购买和操作 IDPS 的成本要与处理报警所需的人员成本以及由于误报和不恰当响应(如由于无法确定信息系统哪部分遭到损害而重装信息系统)导致的间接成本相互平衡。

运行 IDPS 的好处主要包括：

——可以识别有缺陷的或错误配置的设备；

——提供验证配置；

——提供系统使用的统计信息。

选择 IDPS 时，需要考虑 IDPS 的总成本，因此需要分析组织内部署 IDPS 的花费，主要从如下方面确定：

——购买 IDPS 的初始预算；

——IDPS 的运行时间(如 7×24 h 或者更少时间)；

——处理、分析和报告 IDPS 输出需要的基础设施及其成本；

——按照安全策略配置的 IDPS 所需人员和资源，操作、维护、更新和监视 IDPS 输出以及响应报警所需的人员和资源，如无相关人员和资源，如何实现相关功能；

——IDPS 培训的成本；

——IDPS 部署的范围(如 HIDPS 保护主机的数量)。

可以通过向远程管理的 IDPS 服务外包商外包 IDPS 监视和维护功能来降低日常管理成本，从而降低相关成本。

从 IDPS 提供的功能来看，响应是 IDPS 部署中成本最高的部分，主要涉及确定响应方式、建立响应队伍、开发与部署响应策略以及培训和演练。

7.4.7 更新

7.4.7.1 总则

由于多数 IDPS 基于攻击特征，因此 IDPS 的价值相当于针对事件分析的攻击特征数据库。由于不断发现新的攻击和脆弱性，因此，需持续更新 IDPS 攻击特征数据库。故选择 IDPS 时组织至少需考虑如下方面：

——更新的及时性；

——内部分发的有效性；

——更新实施；

——攻击特征更新后对系统影响。

7.4.7.2 基于特征的 IDPS 更新的及时性

只有维护好攻击特征，才可以有效检测出已知攻击。为确保攻击特征更新的及时性，选择 IDPS 时需考虑如下方面：

——当发现漏洞时，IDPS 供应商发布攻击特征更新信息的速度；

——通知程序的可靠性；

——攻击特征更新信息的真实性和完整性；

——如果需要自定义攻击特征，是否具备足够可用的技术；

——为了立即响应高风险脆弱性或持续攻击，是否可写入或者接收自定义攻击特征。

7.4.7.3 内部分发的有效性和更新实施

攻击特征更新后，需要向所有相关系统快速分发并实施具体更新。此时需及时修改攻击特征的更新资料，以便包括特定站点的 IP 地址、端口等。因此选择 IDPS 时，在网络可信边界需注意如下方面：

——在手动分发时，管理员或用户能否在可接受的时间范围内实施攻击特征更新；

——能否测量自动分发和安装过程的有效性；

——是否具备可有效跟踪攻击特征更新的机制。

7.4.7.4 系统影响

为将攻击特征更新对系统性能的影响最小化，在选择 IDPS 时需注意如下方面：

——攻击特征的更新是否影响重要服务或应用的性能；

——能否选择性关注攻击特征的更新，以避免冲突影响服务或应用的性能。

7.4.8 报警策略

IDPS 的配置和操作主要基于设定的监视策略。选择 IDPS 时，在报警策略方面需要考虑兼容现有信息基础设施的报警方法，诸如电子邮件、网页、短信系统(SMS)、SNMP 事态以及自动阻止攻击源等。

当 IDPS 数据用于取证(包括内部举证)时，需要依据法律法规的要求来处理、管理、应用或提交 IDPS 数据。

7.4.9 身份管理

7.4.9.1 总则

选择 IDPS 时，还需要考虑 IDPS 身份管理(用于保护 IDPS 数据和身份交换的安全、可控)，关键是 IDPS 远程证明和在线升级需要借助可信第三方作为权威机构(类似于公钥基础设施中的权威机构)来进行。此外，IDPS 身份管理对无缝、安全、可控的 IDPS 数据和企业网络信任边界的 IDPS 身份交换也很重要。

7.4.9.2 远程证明

IDPS 包含的代码可达数百万行，可能被攻击者插入恶意软件，从而控制 IDPS 的输出。针对此问题，可以通过远程证明(在无人发出指令的情况下)，基于发起访问请求的访问者身份，对 IDPS 软件和硬件的访问控制进行严格的鉴别。

在 IDPS 硬件中，远程证明主要通过产生加密证书或者散列值来验证硬件设备的身份或者在设备上运行软件的身份。其中，散列值(表示身份最简单的形式)可区分不同软件、设备并发现软件的变更，加密证书可提供给 IDPS 用户请求的远程方，还可用于校验远程方(即 IDPS 正在使用预期的和未被改动的软件)。当 IDPS 软件有改动时，生成的加密证书中 IDPS 的编码也会改变。

远程证明的目的是检测 IDPS 软件的未授权变更(例如，如果攻击者已经替换或者修改了一个 IDPS 应用或者操作系统的一部分，远程服务或其他软件将无法认可它们)。因此，远程方(如网络运行中心 NOC)检测到被病毒或者木马破坏的 IDPS 软件时，要采取相应措施，并远程通知与此 IDPS 相关联的其他 IDPS(此 IDPS 受到了损害)，并且在此 IDPS 恢复功能前，避免其发送相关信息。

因此，IDPS 需要借助远程证明实现如下功能：

——向远程方证明或报告其状态、配置或其他重要信息；

——评估 IDPS 的健壮性以及执行大量 IDPS 配置和更新操作的能力；
——远程测试 IDPS 完整性；
——汇总 IDPS 证明报告以提供网络防御状态的态势评估，作为整个网络态势评估的重要组成部分。

7.4.9.3 在线升级

当远程证明检测到 IDPS 存在问题时，可通过在线升级（业界已采纳术语“在线升级”，涵盖了为 IT 设备（也包括 IDPS）安装正确软件、执行安全策略及加载配置数据的过程）解决。这主要通过远程方向 IDPS 推送已鉴别配置、软件更新和补丁等来完成。在线升级尤其是攻击特征的更新应尽可能的远程处理，这样既可节约人员成本，又可及时地缓解问题。为行之有效，IDPS 在线升级需要从远程方进行推送，由 IDPS 安全地拉入即由 IDPS 安全、自动地从供应商网站上远程查找并下载已鉴别的更新。

7.5 补充 IDPS 的工具

7.5.1 总则

对于检测入侵并减轻入侵引起的损害而言，IDPS 并不是唯一、完善的解决方案。因此，选择 IDPS 时，还需要借助一些设备和工具以加强和补充 IDPS 的能力，主要包括：

——文件完整性检查器；
——防火墙或安全网关；
——蜜罐；
——网络管理工具；
——安全信息和事态管理（SIEM）工具；
——病毒（内容）保护工具；
——脆弱性评估工具。

7.5.2 文件完整性检查器

文件完整性检查器是辅助 IDPS 的另一类安全工具，其利用关键文件与对象的信息摘要或者加密校验码，与参考值相比较，来标记文件的差异或变化。由于攻击者可能修改系统文件，因此目前主要在攻击的三个阶段使用加密校验码：第一阶段，攻击者修改了作为攻击目标的系统文件（例如，放置木马）；第二阶段，攻击者试图在系统内留下后门，以便随后能重新进入；最后阶段，攻击者试图掩盖痕迹，使系统责任人可能意识不到攻击。

选择文件完整性检查器时，需要考虑其优缺点。

优点：

——可以确定厂商提供的 bug 补丁或其他期望变更是否已经运用于系统二进制文件；
——允许对攻击痕迹进行快速可靠的判断，特别是对已被攻击的系统进行取证检查时；
——攻击者经常修改或者替换系统文件，并利用技术手段保留系统管理员例行检查的文件属性；而使用此工具能检测到对文件的任何变更或修改；
——可识别对数据文件的修改。

缺点：

——在分析期间，可能要求关闭信息系统或者至少是关闭被检查的系统。

7.5.3 防火墙

防火墙（见 GB/T 25068.2）主要用于限制网络间的访问。简单的防火墙是基于组织可访问的源 IP

地址、目的 IP 地址和端口号来过滤网络流量[例如，组织只接受来自电子邮件服务器(端口号 25)或者 web 服务器(端口号 80)的流量]。然而，应用级防火墙使用应用协议信息可提供更复杂的过滤方式。当防火墙位于封闭区域时，它能减少 NIDPS 需要检查的流量。

当被阻止的流量试图通过防火墙时，与 NIDPS 相比，大多数防火墙在监视网络信息内容和发起报警方面较为受限，而 NIDPS 专门用来检查网络包，检测其中合法和非法流量的构成，并在检测其中存在恶意内容时发出报警。同时，当需要时，NIDPS 报警也能用来改变防火墙的过滤参数。

当在防火墙内侧部署 NIDPS 时，适当配置的防火墙会大大减少由 NIDPS 检查数据包的数量。此类 NIDPS 配置可极大提高 NIDPS 的准确性。因为在控制传入流量的同时，能消除由扫描活动导致的 Internet 背景噪声。

7.5.4 蜜罐

蜜罐是诱骗系统的专业术语，用来欺骗、分散、转移并引诱攻击者在看似有价值的信息上花费时间，但这些信息实际上是捏造的，对合法用户来说毫无价值。蜜罐的主要目的是收集对组织有威胁的信息，并引诱入侵者远离关键系统。

蜜罐不是一个操作系统，而是能引诱攻击者保持足够在线时间的信息系统，以评估攻击者的意图、技能水平和操作方法。

分析蜜罐中入侵者的活动可以使组织更好地理解系统受到的威胁和其脆弱性，从而改进 IDPS 的操作，为推进组织 IDPS 的策略、攻击特征数据库以及整体方法(此方法是 IDPS 避免受到已知攻击威胁的最佳实践)的发展提供帮助。

蜜罐使用前，需寻求法律顾问的指导。鉴于蜜罐是一种诱捕技术，需要确定蜜罐及其数据的合法性。

选择蜜罐时，需要考虑其优缺点。

优点：

——将攻击者转移到他们不能破坏的目标系统；

——蜜罐不管理已授权的活动，因此蜜罐捕捉到的所有活动均是可疑的；

——管理员有更多时间决定如何应对攻击者；

——能够更加容易、广泛地监视攻击者活动，监视结果可用来优化威胁模型、提升保护系统的能力；

——可以有效捕捉在网络上进行窥探的内部人员。

缺点：

——使用此设备的合法性尚不确定；

——一旦进入诱捕系统，攻击者可能发动更具破坏性的攻击；

——为了使用这些系统，管理员和安全管理者需具备较多的专业知识。

7.5.5 网络管理工具

网络管理工具利用探测技术来监视网络设备的可用性和性能，通过收集网络部件和拓扑信息，来进行网络基础设施配置和管理。

网络管理工具主要与 IDPS 报警相关联，帮助 IDPS 操作者恰当地处理报警并评价他们对于所监视系统的影响。

7.5.6 安全信息事态管理(SIEM)工具

SIEM 工具主要用来整合来自 IDPS、防火墙、嗅探器等的信息(收集相关信息并减少过载信息)，并将整合后的信息发送给管理平台和报警控制平台，使得分析者可以管理和利用这些海量信息。同时，SIEM 通过关联分析(使无数小的单个数据包和多个数据源在雷达控制下长时间关联)收集的数据可大

大减少漏报的数量。

SIEM 工具也可用于处理从 IDPS 获得的数据，其主要功能包括：

——收集和维护与安全相关的不同数据源的事态数据，可能包含来自一个或多个 IDPS 的数据、来自网络设备与主机的日志文件以及来自反病毒工具的事件数据；

——进一步处理所收集的数据，特别是提供进一步的事态关联、事态过滤和事态聚合；

——事态关联：通过建立安全和非安全相关事态的情景来检测非模式相关的安全漏洞；

——事态过滤：通过基于相关性的关联来降低报警级别(例如，IDPS 报警和安全补丁级别)；

——事态聚合：通过收集和归一化基于源、目的、时间戳和事态描述等的事态，来降低 IDPS 报警溢出；

——为报告相关报警提供简单易用的界面，为基于收集数据的报警进行深层次分析提供帮助。

SIEM 主要目标是自动区别高威胁报警以及不相关或者没有威胁的误报。当策划引入 SIEM 工具时，需将其作为重要的任务，对 SIEM 进行正确地配置。当 SIEM 与 IDPS 配合使用时，能提供更多有价值的信息，从而触发诸如事件管理这样进一步的处理过程和活动，但 SIEM 配置需要高水平的专业知识和大量的工作。

7.5.7 病毒(内容)保护工具

病毒(内容)保护工具可通过对特定流量和病毒来源信息的交叉分析，提供附加数据来对 IDPS 进行补充。

7.5.8 脆弱性评估工具

脆弱性评估是风险评估、安全审计(符合性检查)和监视策略的重要组成部分。其通过查找脆弱性，采取纠正措施来减少入侵者利用脆弱性入侵的机会。因此使用脆弱性评估能极大地减少 IDPS 查找攻击的数量。

与执行攻击脚本不同，脆弱性评估重点在于评估给定主机对给定脆弱性的暴露程度。因此，IDPS 检测脆弱性评估活动失效并不表示 IDPS 不能检测攻击。相反的，IDPS 对脆弱性评估活动的检测并不意味着相同的 IDPS 也可以准确地检测到攻击。

脆弱性评估工具主要用来测试网络主机对损害的敏感度。其与 IDPS 结合使用，为检查 IDPS 在攻击检测和攻击应对方面的有效性提供了好的方法。脆弱性评估工具可分为基于主机或基于网络两类。其中，基于主机的脆弱性工具通过查询数据源、配置细节和其他状态信息，来评估信息系统的安全，其允许访问目标主机，通过远程连接在目标主机上运行。基于网络的脆弱性工具用来扫描与网络服务相关联主机的脆弱性。脆弱性评估需要由管理者批准以后才能进行。使用脆弱性评估工具是对 IDPS 的补充而不是替代。

选择脆弱性评估工具时，需要考虑其优缺点。

优点：

——脆弱性评估工具为记录信息系统的安全状态提供了有效的方法，它可以重建安全基线以便在系统变更后回退；

——定期使用脆弱性评估工具能够可靠识别信息系统的变更；

——最大的优点是帮助识别脆弱性；

——允许将已知脆弱性与攻击数据相匹配，以确定攻击是否成功。

缺点：

——基于主机的脆弱性评估工具在建立、管理和维护方面通常比基于网络的工具更加昂贵；

——基于网络的脆弱性评估工具是与平台无关的，因此不如基于主机的工具更有针对性；

——脆弱性评估消耗资源(可能是不切实际的，也可能是以降低系统或网络性能为代价，或者在规

定日期和时间限制下运行）；

——在许多情况下，脆弱性评估是周期性（周、月或随机的）活动，可能不能及时检测出安全事件；

——和 IDPS 一样，脆弱性评估工具易受到误报或漏报的影响，需要仔细分析；

——重复地脆弱性评估会使基于异常的 IDPS 忽视真正的攻击；

——需要更新攻击特征；

——基于主机的脆弱性评估工具无法检测网络中的未授权系统。

基于网络脆弱性评估需要限定在目标系统中，由于收集数据是敏感信息（易被入侵者利用入侵信息系统），因此需要注意保护敏感信息和数据的隐私。

7.6 可伸缩性

在选择 IDPS 时，还需要考虑其可伸缩性。许多 IDPS 在带宽提高后，性能却会降低（在数据传输速率较低时 IDPS 性能较好），导致数据包丢失进而误报（当没有攻击时产生了报警）和漏报（当攻击产生时没有产生报警）显著增加，因此此类 IDPS 不适用于大规模或者广域分布式的企业网络环境。

可伸缩性主要适用于 NIDPS 部署以及需要高性能主机设备的 HIDPS。

7.7 技术支持

IDPS 不是“即插即用”的，因此 IDPS 需要供应商提供技术支持和维护。部分供应商会在 IDPS 安装和配置过程中提供技术支持；也有部分供应商仅通过电话和电子邮件等远程方式提供技术支持，由员工进行 IDPS 的安装和配置。

IDPS 技术支持主要通过组织与供应商的合同规定，并结合具体实际进行实施。供应商要结合组织的具体需求，协助组织调优或调试 IDPS，以符合组织的实际需求（无论此需求是监视定制系统或原有系统，还是以定制的协议或格式报告 IDPS 结果）。

因此，选择 IDPS 时，还需要考虑 IDPS 供应商可提供的技术支持，通过合同形式明确技术支持联系方式（如电子邮件、电话、在线聊天、基于 web 的报告、远程监视或响应服务）、主要技术支持服务、响应时间等，以支持事件处理或其他敏感时期的需要。

7.8 培训

仅通过技术不足以检测或防御系统入侵，还需要考虑配备有资质的技术人员评估、选择、安装、操作和维护 IDPS。针对于此，可将 IDPS 操作外包给安全管理服务商，这样就无须招聘、雇佣、留住满足 IDPS 职责要求的有经验的专业人员，但会有培训方面的问题和风险（例如，即使 IDPS 的大部分功能选择外包，也需要向员工培训关于 IDPS 的知识和 IDPS 的操作，否则将失去对 IDPS 的控制）。为降低此类风险，可考虑通过培训方式使负责监督 IDPS 外包操作的员工熟悉 IDPS 操作和规程，实现 IDPS 的最佳应用。相关培训可从 IDPS 产品供应商处获得，并作为 IDPS 购买成本的一部分。

当培训不是 IDPS 服务供应商所提供的服务的一部分时，组织需要额外增加操作人员培训的相关预算。此类培训需要持续提供，以便应对人员更替、IDPS 及其环境的变更等情况。

8 部署

8.1 总则

根据本标准前面的内容，可通过如下方式实现 NIDPS 或 HIDPS 的部署：

——基于风险评估，进行需求分析；

——选择 IDPS 部署策略；

——识别与网络基础设施、策略以及资源级别相一致的解决方案；

——进行 IDPS 维护和操作培训；

——制定培训和演练规程以处理和响应 IDPS 报警。

根据两种主要 IDPS 的优缺点，可考虑 NIDPS 和 HIDPS 的结合，以保护整个组织范围内的网络。

当在云计算环境中进行 IDPS 部署时，主要包括两种方式：

——基于服务器内部部署虚拟 IDPS，利用虚拟平台软件开放的 API 接口，在虚拟机流量进入虚拟交换机之前，将流量引入到虚拟 IDPS 中，从而判断虚拟机直接流量交换是否存在漏洞攻击；

——基于重定向的方式部署 IDPS，将虚拟机中的网络流量引入到外部物理交换机中，利用重定向技术将流量引入到硬件 IDPS 中，从而进行深度报文检测和安全策略配置。

当在多层级组织中部署 IDPS 时，需要考虑的方面包括：

——分级管理权限：需要限定上下级之间的权限划分，明确对跨级权限的限制；

——策略管理：部分 IDPS 策略更改后同级不同 IDPS 之间的策略如何同步更新，下级策略修改更新后，上级 IDPS 如何统计和管理最新策略，针对需要集中升级的策略，或部分分支需要升级的策略如何统一分配；

——日志信息上传管理：各级设备的版本、设备健康监视信息、规则库更新信息、日志报警信息的获取；

——日志、报表分析：如何对日志，报表进行分级、分类分析，保证既能详细了解数据全面的有效分析结果，又不会泄露其他组织的内部保密数据；

——数据传输加密问题：不同层级间数据传输的通道应该做加密处理，防止信息外泄。

当在多层级组织中进行 IDPS 部署和操作时，主要通过如下方式：

——建立管理框架来启动和控制多层组织内 IDPS 的部署和操作：

- 设立 IPDS 部署和操作的责任部门，由其制定的统一的管理机制，对本组织其他与 IDPS 系统部署和操作相关的各垂直管理的业务部门进行管理和协调。
- 设立 IPDS 部署和操作的责任人。
- 各部门部署和操作 IDPS 时，责任部门有相关要求的，应该符合责任部门的要求。责任部门无相关要求的，可符合部门自身的要求。
- 同一部门中，由上级对下级的 IDPS 的部署和操作进行管理，通过责任部门与其他部门进行协调。

——实施统一的信息安全事件响应程序，包括跨部门的事件处理团队。

——遵循最小权限原则。

8.2 分阶段部署

IDPS 的部署可分阶段进行，从而使操作人员在进行过程中不断增加经验，确定不同阶段需要的监视和维护资源（资源需求变化范围较广，主要取决于组织的信息系统和安全环境）。

在分阶段部署中，建议首先从 NIDPS（其安装和维护最简单）部署开始，然后部署 HIDPS 以保护关键服务器。此外，可使用脆弱性评估工具定期测试 IDPS 和其他的安全机制，以便恰当地运行、配置 IDPS。

8.3 NIDPS 部署

8.3.1 总则

与 HIDPS 一样，经过培训的操作人员需在可控环境中使用经过测试的 NIDPS。在全面部署 NIDPS 前，需在不同位置试验 NIDPS 传感器，详见图 2。同时在部署传感器时，还需要平衡部署及持续运行的成本与需要的实际保护级别之间的关系。

当在高速网络环境中时，需注意 IP 数据包的丢包率，避免因丢包率过高导致严重增加模式不匹配的数量进而导致的误报和漏报的增加。为防止上述情况发生，可采用具有较高捕获率的网络接口卡或减少数据丢包率的相关技术。

当 NIDPS 用于网络监视时(特别是使用交换机或 TAP 时)，需考虑数据捕获方法，建议使用物理隔离的交换机，而不是 VLAN 或者核心交换上类似的技术。此时，交换机仅允许单个 SPAN 端口在给定的时间运行，从而防止 CPU 使用率过高(SPAN 端口本身会增加交换机 CPU 使用率，但可通过阻止数据复制降低 CPU 使用率)。

当 SPAN 端口用于网络调试时，IDPS 变成非功能性的，因此需向 NIDPS 开放此端口。此时，可考虑使用网络 TAP(特别是结合上行和下行流量的汇聚 TAP)，在不给网络包增加任何负载(因其是被动设备)情况下，提高安全级别(交换机保持端口的二层信息，数据接口对网络不可见)，保持 IDPS 能力(因为 TAP 提供多端口)并完成网络调试。

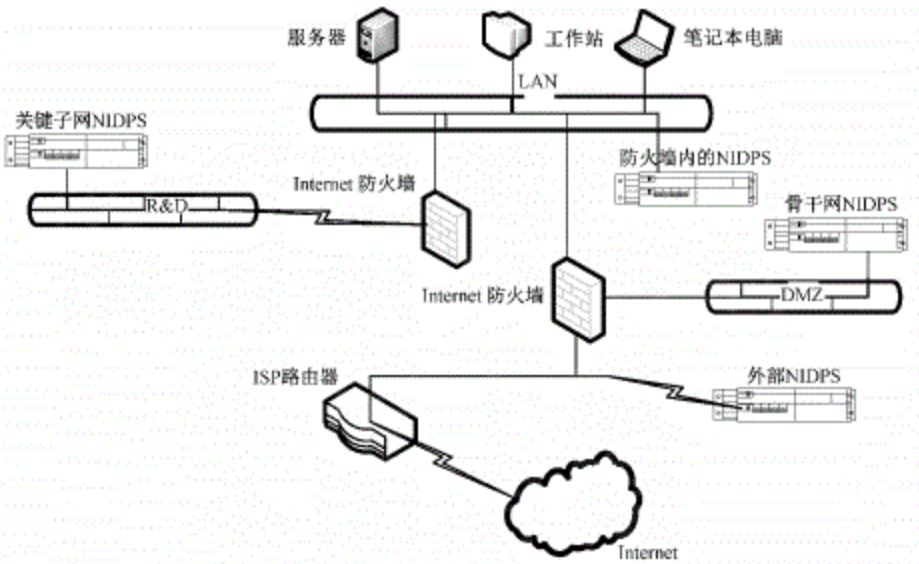

图 2　典型 NIDPS 位置

8.3.2　位于 Internet 防火墙内的 NIDPS

优点：

——识别源于外部网络、已经渗入防护边界的攻击；

——帮助检测防火墙配置策略上的错误；

——监视针对 DMZ 中系统的攻击；

——通过配置检测源于内部、针对外部目标的攻击。

缺点：

——由于其接近外部网络，不能作为强保护；

——不能监视防火墙阻止(过滤掉)的攻击。

8.3.3　位于 Internet 防火墙外的 NIDPS

优点：

——允许对源于外部网络的攻击的数量和类型进行管理；

——可发现未被防火墙阻止(过滤掉)的攻击；

——可减轻拒绝服务攻击的影响；

——与位于外部防火墙内部的 IDPS 一起使用时，IDPS 配置能评估防火墙的有效性。

缺点：

——当传感器位于网络安全边界之外时，会受到攻击，因此需要一个加固的隐形设备；

——在此位置上产生了大量数据，使得分析已收集的 IDPS 数据的难度增加；

——IDPS 传感器和管理控制台之间的交互可能需要在防火墙打开额外的端口，导致可从外部访问管理控制台。

8.3.4 位于重要骨干网络上的 NIDPS

优点：

——监视大量的网络流量，因此更易发现攻击；

——在拒绝服务攻击对关键子网造成破坏之前，可阻止这些攻击；

——在安全边界内部，检测授权用户的未授权活动。

缺点：

——捕获和存储敏感或机密数据的风险；

——IDPS 需要处理大量数据；

——检测不到不通过骨干网络的攻击；

——识别不到子网上主机对主机的攻击。

8.3.5 位于关键子网上的 NIDPS

优点：

——监视针对关键系统、服务和资源的攻击；

——允许将有限的资源集中到最有价值的网络资产上。

缺点：

——子网间相互关联的安全事态问题；

——如果未通过专用网络传输报警，IDPS 流量会增加关键子网的网络负载；

——如果配置不当，IDPS 可能捕获和存储敏感信息，并以非指定的方式访问这些信息。

8.4 HIDPS 部署

HIDPS 操作部署之前，操作人员需熟悉其特性和功能。HIDPS 能否发挥作用，主要取决于操作人员依据网络拓扑、脆弱性以及相关细节等内容区分真假报警的能力(随着时间推移，操作人员操作经验不断增加，从而可识别 IDPS 相关正常活动)。同时，鉴于 HIDPS 监视的不持续性，需建立检查 HIDPS 输出的时间表。HIDPS 的操作模式需降低 HIDPS 遭受攻击时的损害。

HIDPS 全面部署需从关键服务器开始(由于每台主机上 IDPS 都需安装和配置，故在组织内所有主机上安装 HIDPS 既昂贵又耗时。因此组织首先在关键服务器上安装 HIDPS)。这降低了整体部署成本，并使得缺乏经验人员将精力集中在最重要资产产生的报警上。当这一部分 HIDPS 操作常规化后，基于成本、时间、信息安全风险评估结果等，可在更多主机上安装 HIDPS。此时，需部署具备集中管理和报告功能的 HIDPS，从而降低对 HIDPS 报警予以管理的复杂度。同时，HIDPS 大量部署时，也可考虑向安全服务供应商外包其 HIDPS 操作和维护。

8.5 防护和保护 IDPS 信息安全

IDPS 存储的数据与组织信息基础设施内的攻击和可疑活动有关，是安全敏感的，因此可采取如下控制对其保护：

——使用校验码确认存储数据的完整性；

——对存储的 IDPS 数据进行加密；
——适当配置数据库，如使用访问控制机制；
——包括备份程序在内的数据库维护技术；
——对运行 IDPS 数据库的系统进行充分加固以抵抗渗透；
——连接 IDPS 到以太网集线器或者交换机的嗅探(只接收)电缆；
——实现单独的 IDPS 管理网络线路。
——定期对 IDPS 和连接系统进行脆弱性评估和渗透测试。

日志需存储在独立的日志主机上，而非本地计算机上。需避免未授权修改或删除 IDPS 日志、配置、攻击特征和 IDPS 传感器及收集器之间交换的信息。

因 IDPS 日志中包含敏感或隐私相关信息，因此在 IDPS 日志存储和传输中需加以保护。同时，负责分析信息(主要来自 IDPS 传感器或收集器)的相关人员也需要注意保护这些信息。

9 操作

9.1 总则

在 IDPS 操作之前，需要：
——建立过程、规程和机制，确保脆弱性管理过程包含 IDPS；
——准备与 GB/T 20985.1—2017 相一致的事件管理过程；
——当 IDPS 产生报警时，规定需采取的行动；
——识别自动化及半自动化响应的条件，以及如何能监视这种类型的响应结果以确保执行安全且恰当的操作；
——明确法律方面需要考虑的事项。

9.2 IDPS 调优

IDPS 部署后，需要确定 IDPS 的报警功能、以及何时如何使用这些功能，并确保这些功能可常规调整。

IDPS 报警功能通常可配置，且有多种报警方式(包括电子邮件、短信系统、网页、网络管理协议陷阱，以及攻击源的自动阻止)，组织需要详细了解并清楚其安装、其行为特性等内容后，才可开始对其进行操作。

如前所述，借助于 SIEM 技术，IDPS 可更好的对事态进行优先级排序并减少 IDPS 报警(例如，将脆弱性评估数据和系统补丁级别与 IDPS 报警配置进行比较)。在这种情况下，借助于网络发现工具和流量分析器可进一步提高 IDPS 的价值，并对报警规则进行调整优化。

组织可根据实际情况，来决定是否延迟启用整套报警功能。通常经过试验使得操作要求和报警可能性达到最佳平衡后，才可定制报警规则和响应功能(从而启用整套报警功能)。同时也可根据实际情况确定哪些功能是不必要的、哪些功能对组织更有帮助、哪些功能最有利于组织。当 IDPS 报警和响应采取自动响应时(特别是允许 IDPS 指示防火墙阻止已发现的攻击源流量时)，需要防止被攻击者利用以造成拒绝合法用户的访问即拒绝服务攻击(因为此类响应原为半自动模式，由人员决定是否对攻击进行响应)。

9.3 IDPS 脆弱性

为防止攻击者在了解已知脆弱性情况下，尝试利用 IDPS 已知的脆弱性(如以不安全方式安装启用 IDPS 传感器、发送未加密的日志文件、有限的访问控制、缺乏对日志文件的完整性检查等)，使 IDPS 失去能力或提供错误信息，需以安全的方式安装启用 IDPS 传感器和控制台，并处理好 IDPS 的潜在脆

弱性。

9.4 处理 IDPS 报警

9.4.1 总则

IDPS 通常会产生大量报警，需要对其全面分析，以区分其中有价值的报警和无价值的报警。报警信息主要包含检测到的攻击的简明摘要，主要包括：

——检测到攻击的时间或日期；
——检测到攻击的传感器 IP 地址；
——供应商特定的攻击名称；
——标准的攻击名称(如果存在)；
——源和目的 IP 地址；
——源和目的端口号；
——攻击利用的网络协议。

此外，一些 IDPS 提供了所利用攻击方法的通用详细信息，其允许操作人员评估攻击的严重程度，主要包含：

——攻击的描述；
——攻击的严重性等级；
——由攻击造成的损失类型；
——攻击利用的脆弱性类型；
——易受到攻击的软件的类型列表及版本号列表；
——相关补丁列表；
——可公开通报的参考信息，内含攻击或脆弱性的详细信息。

9.4.2 信息安全事件响应团队(ISIRT)

组织内部需配备信息安全事件响应团队(ISIRT)，以响应报警。ISIRT 需规划建立安全事件(如病毒、系统的内部误用及其他类型的攻击)处理的相关规程，主要给出发生信息安全事件时要采取的行动，并为人员培训建立时间表，就信息事件处理过程中人员的职责进行培训。安全事件报告和处理的更多信息见 GB/T 20985.1—2017。

9.4.3 外包

安全服务供应商除了提供 IDPS 产品外，还提供 IDPS 托管服务，包括提供咨询服务及提供运行中心管理服务。许多组织选择将一些支持类服务(如安全服务)托管给服务供应商，从而不必培训和保留具备专业技能的人员。当组织将其 IDPS 服务托管给安全服务商时，需确定经济上是否可行，以及安全服务商在保持机密性的同时是否提供适当的支持。与 IDPS 安全服务供应商合作需注意如下内容：

——提供何种保密协议；
——IDPS 监视人员具备的资格；
——监督人员具备的资格；
——服务提供商和组织内部安全人员之间的联络和沟通安排；
——供应商是否可以提供紧急响应服务，以补充组织的能力；
——供应商是否提供取证调查服务；
——供应商是否提供服务级别协议(SLA)；
——哪些报告可供选择，它们是否能根据组织的需求定制；

——是否能为组织定制检测策略，或者是否必须使用供应商预设的检测策略；
——为了执行这些协议，采取的技术措施；
——服务提供方人员采取的安全审查程序。
服务级别协议 SLA 主要包括：
——定期(如每日、每周等)报告的内容；
——响应时间的指标；
——发生攻击时的通报机制(如电子邮件、呼叫器、短消息系统、多媒体系统、电话等)；
——事件追踪和管理程序；
——保密和非公开协议。
优点：
——同等花费下，相对组织自己提供服务，托管安全服务提供方可提供更高级别的安全；
——通常花费更少的成本，可更快、更有效地实现 7×24 h 能力；
——由于许多托管安全服务提供方可访问来自不同客户的信息，他们能够更好的处理可疑活动并识别攻击；
——减少将有效 IDPS 规程集成在一起所需要的时间，以及重复所有实施细节所需的时间；
——无需对员工提供最新 IDPS 工具和能力的持续专业培训(尽管需要了解 IDPS 能力)。
缺点：
——需监视和审计外包方，使其符合安全要求、限制和策略；
——可能向第三方暴露敏感信息；
——如果实施不当可能会比内部支持成本更高；
——能剥夺对敏感数据的控制。

9.5 响应选项

9.5.1 原则

IDPS 支持范围广泛的响应，其可分为主动响应、被动响应。

9.5.2 主动响应

主动响应(具有主动响应功能的入侵检测系统 IDS 也称为入侵防御系统 IPS)包括检测到攻击时 IDPS 自动采取的行动，其进一步分为：
——收集可疑攻击的附加信息；
——变更系统环境，以阻止攻击；
——在报警之后不需人为参与，会采取预防措施，主动拒绝通信和(或)终止通信会话。

9.5.3 被动反应

被动响应向操作人员或者预先指定的位置提供信息，然后 IDPS 操作人员根据所提供信息来采取后续行动。被动响应有如下形式：
——报警和通知，通常以屏幕提示、弹出窗口、寻呼机信息或手机信息的形式；
——配置 SNMP 陷阱，以响应中央管理控制台。

9.6 法律方面的考虑事项

9.6.1 总则

系统收集的信息可能包含敏感资料、个人信息或刑事调查证据，因而需负责任地保存或处理并符合

相关法律法规的要求。同时，需要确保员工意识到这方面的职责。本条主要给出了 IDPS 相关的法律方面考虑事项。

9.6.2 隐私权

IDPS 操作过程中需要收集个人信息，并监视员工的活动，因此需要遵守隐私权和适用的法律法规。组织需要制定、实施策略，以确保 IDPS 的使用符合相关隐私权和适用的法律法规的要求。

9.6.3 其他法律和方针的考虑事项

IDPS 的实施和操作还需要符合其他的法律法规的要求以及部署 IDPS 组织的方针要求等。实施和操作 IDPS 时，需要评审和处理法律、法规和组织方针要求。法律和法规方面的其他问题在 GB/T 20985.1—2017 中进一步讨论。

9.6.4 取证

IDPS 日志可用于取证。组织需理解相关的取证要求，并针对存储和处理 IDPS 日志实施相关控制以确保这些信息能用于取证，同时还需要关于 IDPS 系统和过程的文档信息以用于取证和提供证据。

附 录 A
（资料性附录）
入侵检测和防御系统（IDPS）：框架及需要考虑的问题

A.1 入侵检测和防御的介绍

尽管信息系统的脆弱性易被无意或有意的利用、受到入侵和攻击，但是由于业务的需求，组织仍然会使用信息系统并将其连接到因特网和其他网络上。因而需要保护这些信息系统。

随着技术的不断发展，获取信息的便利性也在不断提高，新的脆弱性也随之出现。与此同时，利用这些脆弱性的攻击也在不断发展。入侵者也在不断提高入侵技术。随着计算机知识、攻击脚本和各种工具的普及，实施攻击所必需的技术门槛越来越低。因此，攻击的不确定性和攻击所产生的危害越来越大。

保护信息系统的第一层防御是利用物理、管理和技术控制，主要包括鉴别与认证、物理和逻辑访问控制、审计以及加密机制（参见 GB/T 22081—2016）。但从经济方面考虑不可能总是能够完全保护每一个信息系统、服务和网络。比如对于全球使用、没有地理界限、内部和外部差别不明显的网络，很难实施访问控制机制。员工与商业合作伙伴越来越依赖远程访问，已无法通过边界防御保护网络。需要进行动态、复杂的网络配置，为员工提供访问 IT 系统和服务的多路访问点。此时，需要第二层防御即利用入侵检测和防御系统（IDPS），迅速有效的发现和响应入侵。同时，还可通过 IDPS 的反馈完善有关信息系统脆弱性的知识，帮助提高组织信息安全整体水平。

组织可通过购买 IDPS 软件和（或）硬件产品，或通过向 IDPS 服务提供商外包 IDPS 功能等方式部署 IDPS。需要说明的是，IDPS 不是一个“即插即用”设备，需要有效部署才能发挥作用，因此需要了解 IDPS 的相关知识。

像其他控制一样，需要通过信息安全风险评估来证明 IDPS 部署的有效性，并将其融入信息安全管理过程。另外，当已部署 IDPS 的信息系统遭受攻击时（即入侵者或攻击者窃听并修改了其中的信息），需识别并证明相关保护措施（如 IDPS）的必要性。需要根据系统或服务安全策略选择适当的保护措施管理入侵风险，包括：

——减少入侵发生的机会；

——有效检测和响应可能发生的入侵。

当组织考虑部署 IDPS 时，需了解：

——针对信息系统和（或）网络的入侵和攻击类型；

——本标准提及的 IDPS 通用模型。

A.2 入侵和攻击的类型

A.2.1 简介

信息系统的入侵者和攻击者主要是利用信息系统和（或）网络缺陷（包括配置缺陷、实施缺陷和概念缺陷）以及异常的用户行为。

具体来说，入侵者和攻击者首先利用脆弱性入侵信息系统，然后获取其处理或存储的信息，从而损害信息系统和信息的机密性、完整性和可用性。通过入侵和攻击，入侵者和攻击者获得了大量有价值信息，并将其利用到其他入侵和攻击中。此外，不仅要防范外部入侵者和攻击者，还要防范内部人员实施

入侵和攻击(例如,信息系统授权用户试图获得未授权的额外特权)。借助入侵和攻击可进行:

——信息收集,攻击者试图获取目标信息系统的详细信息;

——试图获得未授权系统特权、资源或数据;

——损害系统,可使用系统资源实施进一步攻击;

——信息泄露,入侵者试图用非授权手段使用受保护信息(如密码、信用卡数据);

——拒绝服务(DoS)攻击,攻击者试图使目标信息系统服务变得迟缓,或者使其服务中止。

从入侵和攻击的脆弱点来说,入侵和攻击可分为:

——基于主机的(入侵);

——基于网络的(入侵);

——基于组合方法的(入侵)。

A.2.2 基于主机的入侵

基于主机的入侵,通常会引入恶意代码(例如,利用木马、蠕虫或病毒的攻击),这类入侵性活动主要发生在:

——应用层(SMTP、DNS)(如伪造电子邮件、垃圾邮件、缓冲区溢出攻击、竞争状态攻击、中间人攻击);

——鉴别系统(如利用窃听或密码猜测的攻击);

——基于 Web 的服务(如针对 CGI、ActiveX 或 JavaScript 的攻击);

——系统可用性(如拒绝服务攻击);

——操作系统;

——网络和应用管理系统(如 SNMP 攻击)。

A.2.3 基于网络的入侵

基于网络的入侵通常发生在:

——物理层和数据链路层通信协议以及实现它们的系统(如 ARP 欺骗、MAC 地址克隆);

——网络层和传输层通信协议(IP、ICMP、UDP、TCP)以及实现它们的系统(如 IP 欺骗攻击、IP 碎片攻击、同步洪泛攻击、异常 TCP 报头信息攻击)。

A.3 入侵检测和防御过程的通用模型

A.3.1 简介

由软硬件组成的 IDPS 通过自动监视、收集和分析信息系统或网络中的可疑事态来发现入侵。入侵检测和防御的通用模型主要包括的功能有:原始数据来源、事态检测、分析、数据存储和响应。这些功能可以由单独的组件实现,也可作为更大系统一部分的软件包来实现。图 A.1 给出了这些功能之间相互关联的方式。

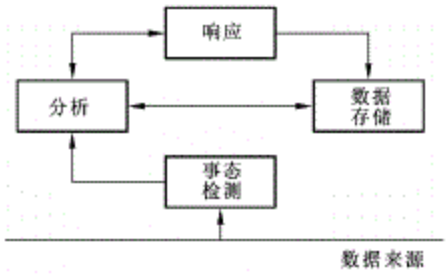

图 A.1　入侵检测和防御的通用模型

A.3.2　数据来源

入侵检测和防御过程的成功依赖于入侵信息的数据来源，主要包括：

——来自不同系统资源的审计数据：审计数据记录包含了消息和状态信息，其范围涵盖了从高层次的抽象数据到显示事态流时间顺序的详细数据。审计数据主要来源于操作系统日志文件(包括由操作系统产生的系统事态日志和活动日志，如审计痕迹或日志)或文件系统、网络服务、访问尝试等记录信息的应用。

——操作系统系统资源的分配：系统监视的参数(例如，CPU 工作负载、内存利用率、系统资源短缺、I/O 速率、活跃的网络连接数等)。

——网络管理日志：网络管理日志主要提供网络设备的健康程度信息、状态信息和设备状态转换信息。

——网络流量：网络流量提供了与安全相关的参数(比如源地址、目的地址、源端口、目的端口等)。此外还需收集通信协议的不同选项(如 IP 和 TCP 状态标记，表示源路由或连接的尝试与确认)。数据收集前几乎不会受到攻击，因此可依据 OSI 模型在低层次上收集原始数据[如果仅在 OSI 模型高层次(例如，一个代理服务器上)上收集原始数据，那么底层的信息将会丢失]。

——其他的数据来源：包括防火墙、交换机、路由器以及 IDPS 特定的传感器或监视代理。

原始数据来源可分为两类：来自主机的数据和来自网络的数据。根据 IDPS 位置的不同，其也可同样分为两类：基于主机的 IDPS 和基于网络的 IDPS。基于主机的 IDPS 能检查审计数据和其他来自主机或应用的数据。基于网络的 IDPS 能检查网络管理日志，以及来自防火墙、交换机、路由器和 IDPS 传感器代理的数据。

A.3.3　事态检测

事态检测的目的是为了检测和提供安全相关的事态数据，以用于分析。

检测到的事态可以是简单事态(包括正常操作过程中发生的攻击或事件)，也可以是复杂事态(由简单事态的组合组成，这些事态极有可能表示特定攻击)。然而，事态和事态数据无法直接作为入侵的证据。

事态检测可通过 IDPS 的监视组件实现。根据要检测的事态数据的来源不同，IDPS 的监视组件可安装在网络设备上(如路由器、网桥、防火墙)，或特定的计算机上(如应用服务器、数据库服务器)。

由于事态检测过程将产生大量的事态数据，因此事态检测的频率会影响 IDPS 整体的有效性。这也适用于下面的分析过程。

A.3.4　分析

A.3.4.1　简介

分析功能的目的是为了分析并处理由事态检测提供的事态数据，以发现正在尝试的、正在发生的或

已经发生的入侵。

除了检测到的事态数据，分析还可以利用的信息或数据来源包括：

——先前分析的结果数据和存储的数据；

——从个体或系统如何表现的知识（如执行的已知任务和完成的已授权活动）中产生的信息或数据；

——从个体或系统不被期望如何表现的知识（如已知攻击或已知损害行为）中产生的信息或数据；

——其他相关信息或数据，如可疑攻击源站点、个体或攻击者位置。

有两种通用的分析方法：基于误用的方法（也称作基于知识的方法）和基于异常的方法（也称作基于行为的方法）。

A.3.4.2 基于误用的方法

A.3.4.2.1 总则

基于误用的方法主要以已知攻击和未授权活动的知识积累为基础，对检测到的事态数据进行分析，从而寻找出攻击证据。

具体来说，此方法首先将信息系统的已知攻击以及先前被认为是恶意的或入侵性的行为和活动，建模、编码为特定的攻击特征，然后系统地扫描信息系统以发现这些攻击特征。由于已知攻击的模式或已知攻击的细微变化被称作特征，因此基于误用的 IDPS 有时称作基于特征的 IDPS。

在 IDPS 商用产品中，（最常见的）基于特征的攻击检测技术通常将与攻击或未授权活动相一致的每个事态模式建模和编码为一个独立的攻击特征。然而，也存在一些更复杂的系统允许使用单一的攻击特征来检测一组已知攻击和未授权活动。

需要注意的是，基于误用的方法是基于如下假设，即事态数据与攻击特征不匹配时不代表有入侵或攻击。由于某些入侵和攻击在攻击特征建模时还是未知的，因此不匹配的数据仍然可能包含入侵或攻击的证据。

目前，基于误用的分析广泛使用的方法有攻击特征分析、专家系统、状态转换分析。

A.3.4.2.2 攻击特征分析

此方法是入侵检测和防御中最常见的方法，主要基于如下假设，即信息系统中安全相关的行为都将能产生相应的审计日志。

入侵场景可转换为审计日志序列或特征数据，因此可从计算机操作系统、应用、防火墙、交换机、路由器、特定 IDPS 传感器或监视器以及网络数据流等产生的数据中发现攻击特征或审计日志序列。协议分析作为攻击特征分析的一种方法，主要利用确定的通信协议结构分析数据包、帧和连接等元素。

攻击特征分析首先分析、收集或制定已知攻击的语义描述、攻击特征，然后将其保存在数据库中。对日志进行审计时，当发现与预定义的入侵攻击特征相匹配的特定序列或攻击特征时，就表示有入侵企图。

此方法能用于有阈值（单位时间内发生事件的比例、数量或是其他的测量指标）或没有阈值的情况。如果未定义阈值，当识别出一个攻击特征时即产生报警。如果定义了阈值，会在攻击特征数量超过阈值时才产生报警。

此方法的缺点主要是需要不断地更新攻击特征，以便发现新的脆弱性和攻击。

A.3.4.2.3 专家系统

基于误用的方法的专家系统包含了描述入侵的规则。而基于异常的方法的专家系统生成一系列规则，根据给定时间段内用户行为记录，统计用户的使用行为。所有规则都需要不断更新以适应新的入侵

或新的使用模式。

本方法主要将经过审计的事态转换为表达其语义的事实，输入专家系统，利用这些规则和事实得出结论，以检测可疑入侵或不一致的行为。

A.3.4.2.4 状态转换分析

该方法将带有一系列目标和转换的入侵表示成为状态转换图。借助状态转换图中与状态相关的布尔声明进行分析。

A.3.4.3 基于异常的方法

A.3.4.3.1 总则

基于异常的方法根据以往对正常系统行为的观察或者预先定义的配置文件(一个预先确定的事态模式，通常与一系列的事态相关，存储在数据库中用于对比)，从预期或预测的常规行为中发现异常行为。

需要注意的是，基于异常的方法基于如下假设，即事态数据与攻击特征不匹配时，代表有入侵或攻击。由于某些正常的证据或已授权行为在攻击特征建模时还是未知的，因此不匹配的数据仍然可能包含正常的证据或已授权行为。

目前，广泛使用的基于异常的分析方法有识别异常行为、专家系统、统计方法和神经网络。

A.3.4.3.2 识别异常行为

此方法主要匹配用户的正常活动模式，而攻击特征分析则匹配用户的异常活动模式。

此方法通过一系列的任务(这些任务由用户通过使用非统计技术在系统上执行，其表现为用户期望的或授权的活动模式，如访问特定文件或文件类型)对用户正常的或已授权的行为进行建模，并将审计中发现的个人行为与预期的或授权的模式相比较，当行为模式与预期的或授权的模式不同时，将产生报警。

A.3.4.3.3 专家系统

参见 A.3.4.2.3。

A.3.4.3.4 统计方法

在基于异常的入侵检测方法中，最常用的是统计方法。

本方法通过随时间采样的多个变量来测量用户行为或系统行为，并将其存储在配置文件中。当前配置文件定期与已存储的配置文件合并，并随着用户行为的变化(如每次会话的登录和退出时间、资源利用的持续时间，以及在会话或给定的时间内消耗的处理器内存磁盘资源量)而更新。

配置文件可以由不同类型的测量组成，主要包括：

——活动强度测量；

——审计记录分发测量；

——分类测量(如登录的相对频率)；

——计数测量(如特定用户的 CPU 或 I/O 的数值)。

异常行为主要通过检查当前配置文件和存储的配置文件来确定，即阈值是否超出了变量的标准偏差。

A.3.4.3.5 神经网络

神经网络是一种算法，用来学习输入—输出向量的关系并从中发现普遍规则，以获得新的输入—输

出向量。对入侵检测和防御来说，神经网络主要用于学习系统内角色(如用户、后台程序)的行为。使用神经网络的优势在于神经网络能够较为简单的表示变量之间的非线性关系，还能够自学习和再训练。

A.3.4.4 结合方法

基于误用和基于异常的方法可以结合使用，以便利用彼此的优点。混合方式的 IDPS 部署允许基于已知攻击特征和未经确认的模式(如特定用户登录尝试的次数)来检测入侵。

此外检测入侵的其他方式或方法正在探索研究中。例如，Petri 网的应用研究和计算机免疫学的研究。

A.3.4.5 分析频率

A.3.4.5.1 总则

原始数据(如审计痕迹或日志)通常是连续产生的，但它们可能不会全部用于事态检测处理或事态分析。因此，分析的频率可分为：

——连续的；

——周期性的；

——特定条件下的。

A.3.4.5.2 连续的或接近实时的

此种情况下，事态检测不断查找出现的特定数据、情况或活动并提供事态数据，分析也持续不断的进行。

此时，需要注意在检测到并且报告入侵之前，入侵已经完成的情况。由于事态发生时间与检测并报告它的时间之间存在时间差，因此导致了入侵开始和侵入目标系统之间存在时间差(这主要取决于事态数据来源、检测方法或入侵性质等相关信息)。

A.3.4.5.3 定期或批量处理

将原始数据和检测到的事态数据放置到存储介质时，可选择定期或在合适的时间检测分析这些数据。例如，可在 IT 系统负荷较低时(如晚上或通过一个辅助的旁路子系统)，对事态数据进行检测和分析。

A.3.4.5.4 仅在特定条件下发起

取证分析是一种仅在特定条件下(如发生大范围的攻击，且引起了严重破坏)才发起的分析，需集中力量对攻击相关方面和产生的后果进行全面分析，主要用于法律诉讼，因此需要遵循相关的证据规则。

A.3.5 数据存储

数据存储的目的是存储安全相关信息，并用于后续的分析和报告中。

存储的数据主要包括：

——已检测到的事态数据和其他的必要数据；

——分析的结果，包括已检测到的入侵和可疑事态(后续用于可疑事态分析)；

——收集已知攻击和正常行为的配置文件；

——安全报警响起时，收集和保存的详细原始数据(作为证据，如为了可追溯性)。

需要提供数据保留和数据保护策略，用于处理各种后续事项，如完成分析、数据取证、证据保存，以及防止对安全相关信息的窃听。

A.3.6 响应

响应的目的是为了向相关人员(如系统管理员、安全负责人)提供合适的分析结果。这些结果通常以图形用户界面的形式呈现,并可通过邮件、短信、电话等方式通知相关人员,以便升级和组织对报警的响应。

被动响应仅限于在控制台产生报警,而主动响应(具有主动响应功能的 IDS 也称为 IPS)还能针对入侵提供适当的对策,以限制入侵或将其影响降到最低,相关对策主要包括:

——重新配置被入侵的系统;

——锁定入侵的账户;

——封锁会话协议。

响应提供的信息主要帮助评估入侵的严重程度,并决定所采取的对策。此时需要确保评估得到的入侵严重程度及所采取的对策要与组织的信息安全策略和程序相一致。

GB/T 22081—2016 第 13 章给出了相关的对策,包括信息安全事态的报告、从安全漏洞中恢复、纠正系统故障的职责和程序。此外,GB/T 20985.1—2017 也提供了关于信息安全事件管理的相关信息。

A.4 IDPS 类型

A.4.1 简介

按照检测方法的不同,IDPS 可分为三类:基于特征的 IDPS、基于异常的 IDPS、状态协议分析 IDPS。通常,实际使用的 IDPS 会包含多种检测方法(无论是单一的或集成的),以提供更广泛和更准确的检测。检测方法分类如下:

基于特征的检测,将观察到的事态与已知的威胁特征相比较来识别事件,其主要用于检测已知威胁,但无法检测未知威胁、已知威胁的变种以及包含多个事态的攻击(原因是无法跟踪和了解复杂通信的状态)。

基于异常的检测,将观察到的事态与已确定的正常活动进行比较,以识别与正常活动的偏差。该方法首先形成配置文件(通过一段时间内的监视典型活动特征形成),后将当前活动的特征与配置文件进行比较。此方法主要用于检测未知的威胁,但因配置文件的问题(可能无意中包含恶意活动,也可能由于其不够复杂不足以完全反映真实世界的计算活动)易产生误报。

状态协议分析,将观察到的事态与预先设定的配置文件(定义状态协议的相关活动)进行比较,以识别与配置文件的偏差。该方法与基于异常的检测(使用主机或特定网络配置文件)的区别主要是利用供应商提供的通用配置文件(该配置文件规定了特定协议可如何使用和不可如何使用),其主要用于检测其他方法无法检测到的攻击,但存在无法完全准确定义状态协议模型、耗费资源以及无法检测到未违反通用行为特征的攻击等问题。

按照数据来源的不同,IDPS 可分为基于主机的 IDPS(HIDPS)和基于网络的 IDPS(NIDPS),此外还包括基于应用的 IDPS(AIDPS),它是 HIDPS 的特殊类型并且具有与 HIDPS 相似的特性。

IDPS 的功能主要包括:

——监视和分析系统事态和用户行为;

——识别与已知攻击相匹配的系统事态模式;

——识别与正常活动不同的活动模式;

——检测到攻击时,通过合理的方式通知相关人员;

——检查安全策略的执行情况;

——允许非安全专家执行安全监视;

——增加发现安全风险和抵御攻击者的能力;

——识别其他安全设备无法预防的问题；
——协调其他安全设备(如防火墙)处理事态；
——验证、列举并描述对信息系统的网络威胁；
——提供有关入侵的有用信息，以支持进行事件处理、损害评估、系统恢复和法律诉讼。

IDPS 的局限性主要包括：

——无法检测新的攻击以及已有攻击的变体(主要针对基于特征的 IDPS，不适用于基于异常的 IDPS)；
——难以过滤信息源的错误和噪声；
——难以有效的处理交换网络；
——不适用于范围较大网络或分布式网络；
——难以根据 IDPS 输出确定入侵者的物理和(或)虚拟位置；
——难以用网络管理系统来整合不同的 IDPS 产品；
——无法弥补安全策略和安全机制(如防火墙、身份证明和鉴别、链路加密、访问控制机制和病毒的检测与清除)的缺陷或缺失；
——无法对特定类型的攻击进行检测、报告或快速响应；
——尽管有能力识别，但无法减缓 DoS 攻击；
——没有人为干预，无法对攻击进行详细分析；
——无法弥补安全战略、策略或安全架构的重大缺陷；
——无法弥补网络协议的安全缺陷；
——其输出通常包含误报和漏报，需耗费大量的时间和资源来解决；
——可能作为攻击序列的一部分而被禁用；
——可能被攻击者利用来产生误报，以分散对主要攻击的注意力；
——可能产生大量的审计信息，需占用系统额外的本地存储；
——基于 IDPS 报警的自动拦截可能引起安全性和可用性问题；
——需要掌握先进的技术和系统知识，才能有效地使用 IDPS。

A.4.2 基于网络的 IDPS(NIDPS)

NIDPS 主要监视网络中发送给主机系统的流量，其由一系列单用途传感器或位于网络中不同位置的主机组成。这些单元首先对流量进行分析，然后将分析结果汇总到中央管理控制台，以此来监视网络流量。传感器作为 IDPS 的专用部件，应加强对其保护。同时，为使攻击者难以感知传感器的存在并确定其位置，大部分传感器对网络层之上是不可见的(即运行在“隐身”模式下)。

目前，通过提供可以入侵(如 DoS)信息，NIDPS 可以达到实时或近实时的检测和响应，而 HIDPS 的响应时间与间隔频率有关。

除了 IDPS 通用功能外，NIDPS 特有的功能包括：

——在“隐身模式”下操作，并将传感器对更高级别的网络协议(通常第 3 层及以上)隐藏；
——使用单一的传感器监视同一网络段上多个主机的流量；
——识别影响多主机的分布式攻击。

NIDPS 特有的局限性包括：

——无法很好地处理加密网络通信；
——需要比 HIDPS 更大的带宽和更快的处理能力(因为 NIDPS 的性能容量与部署性能最大化的网络段的流量是一致的)；
——NIDPS 的许多功能需要特殊的技术设置才能在现有交换网络中使用(如网络传感器，它需要连接到映射所有其他端口数据的网络交换机特定端口)；

——由于解码应用层协议(如 HTTP、SMTP)的有关问题,一些 NIDPS 可能在处理网络层(IP)或传输层(TCP/UDP)分段数据包攻击时存在问题;

——通常无法监测攻击是否成功。

A.4.3 基于主机的 IDPS(HIDPS)

HIDPS 位于一台计算机内并为其提供保护,其可检查计算机操作系统日志数据(如审计痕迹/日志)、本地数据、操作系统或应用日志数据等,以此分析相关应用程序发生的事态。

操作系统审计日志由操作系统内核产生,其比系统日志详细,但系统日志比其简短更易于理解。

需注意,当 HIDPS 旨在支持 IDPS 集中管理和报告时,可通过一个控制台管理多台主机。HIDPS 生成消息的格式需与网络管理系统相兼容。

与 NIDPS 不同,HIDPS 能监测到攻击企图(因为它能直接访问和监视攻击针对的数据文件和系统进程),例如,HIDPS 可检测来自关键任务服务器键盘的攻击。

除了 IDPS 通用功能外,HIDPS 特有的功能包括:

——将用户身份与可疑活动关联起来;

——观察并追踪用户行为的变化;

——建立系统安全状态的基线,并跟踪基线的变化;

——管理操作系统审计机制、日志机制和生成的数据;

——当数据以加密或者非加密形式传输和存储时,提供应用层的日志记录和监视;

——监测攻击引起的数据篡改;

——监视处于高速网络和加密网络中的系统;

——检测 NIDPS 无法发现的攻击。

HIDPS 特有的局限性包括:

——某些 DoS 攻击会使 HIDPS 失效;

——HIDPS 将占用大量主机资源,包括主机审计日志所需的数据存储;

——由于需要安装的 HIDPS 数量较大(至少每台主机按照一个 HIDPS),安装和维护过程较为复杂;

——由于主机通常可通过更高的网络层分配地址,因此无法在“隐身模式”下使用;

——无法识别针对其他主机或网络的攻击。

A.5 架构

在不同的架构中,IDPS 可通过不同方式来实现。

在具有小规模网络的组织中,通常选择单个 IDPS 来满足入侵检测和防御的要求,以保护相关系统。

在具有较大规模且复杂网络的组织中,通常需多个 IDPS 来满足入侵检测和防御的要求(单个 IDPS 可能不足以或不能够满足入侵检测和防御的要求),每个定制的 IDPS 保护不同的子系统或组件。为了能有效检测攻击(攻击可针对子系统或组件,也可针对子系统或组件的配置,而非子系统或组件本身的脆弱性),需要关联和分析来自不同 IDPS 的事态数据。

为了有效实现 IDPS 架构的目标即高效和有效地实现入侵检测和防御,IDPS 架构需重点关注:

——多个 IDPS 相互连接和关联的方式;

——架构中任务的集中或分发。

分层入侵检测和防御架构的示例如图 A.2 所示。

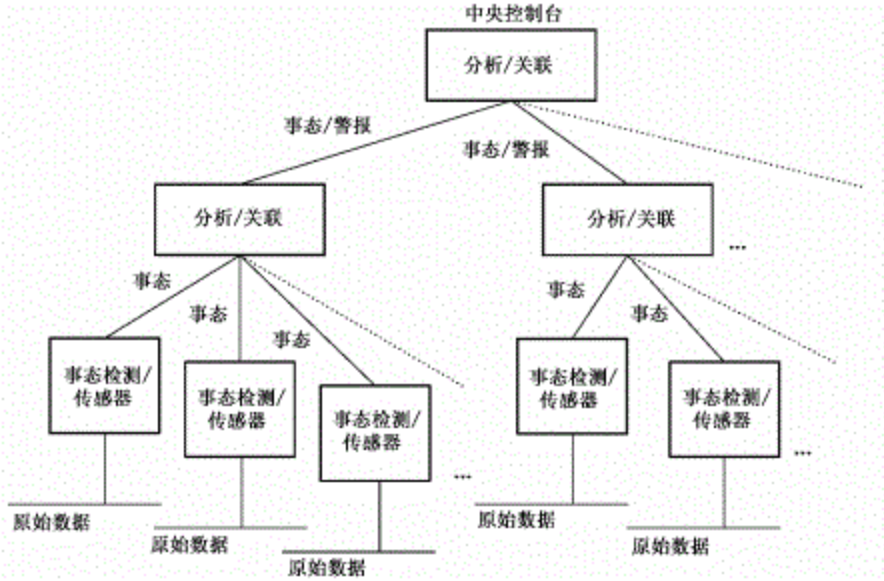

图 A.2　分层入侵检测和防御架构

在图 A.2 中，将低层级的分析和关联组件的输出汇总后，输入更高层级的组件中进行更高层级的分析和关联。参考其他多层应用程序基础设施，可在多个位置执行所需的相关功能。

与分层架构不同，集中式架构将收集的原始数据发送到单个组件进行分析和关联。此方法设计简单，但可扩展性差，只适用于小规模网络中。

更多可扩展的架构如下：尽早减少原始数据，在分散的组件中执行某些 IDPS 任务后，将相关事态传输到下一层组件，形成组件链，以此类推，最终仅将相关事态或报警传递到核心部件。此类架构中间将涉及一些非常复杂的任务（例如，此类可扩展架构就需要配置过滤器以及相关的分析和关联组件，并通过攻击指示找到到达核心部件的方法，从而发出报警）。

A.6　IDPS 的管理

A.6.1　简介

IDPS 的有效管理有助于组织有效和高效的部署网络基础设施。为使 IDPS 有效运行，需注意 A.6.2中 IDPS 管理的各个方面。

A.6.2　配置管理

A.6.2.1　总则

配置管理用以控制、识别、收集来自 IDPS 各组成部分的数据并向 IDPS 提供数据。未达到入侵检测和防御的目的，其主要包括检测功能的配置管理和响应功能的配置管理。

A.6.2.2　检测功能

检测功能的配置管理包括为事态和事态序列违反安全策略设置标准、描述误用模式和正常用户行为。

A.6.2.3　响应功能

响应功能的配置管理主要是安全报警时系统采取的措施，包括控制各种响应机制（如声音报警、管

理员和安全人员通知以及会话终止)。为防止 IDPS 未授权的响应和对虚假入侵的响应(可能会产生比未安装 IDPS 更大的损害,主要取决于已配置的响应),避免造成较大损失,需采取相关措施保护 IDPS。响应管理需与组织的事件管理方案相一致。

A.6.2.4 安全服务管理

安全服务管理主要是管理 IDPS 的安全服务,包含控制用户证书、机密性、完整性和访问控制服务。主要根据用户证书来设定用户对 IDPS 的访问(包括对配置参数、审计日志以及与安全事态相关信息的访问)权限。

A.6.2.5 与其他管理系统的集成

IDPS 管理不可孤立的去进行,需要融入到组织的 IT 环境中,与其他管理如网络管理、系统管理和安全管理结合起来使用[如通过与网络管理、系统管理和(或)安全管理系统的安全接口,或与其他管理系统集成成为管理系统不可或缺的一部分]。此时,需实施部分检测功能(如访问日志)和部分响应功能,以便更好的与其他管理相结合。

A.6.2.6 管理操作的安全

A.6.2.6.1 总则

为防止入侵者访问 IDPS 的信息或控制 IDPS 的资源,需要保护 IDPS 管理操作的安全,主要包括管理服务的鉴别、完整性、机密性和可用性。

需要根据所要求的高安全级别安全策略(与其他管理系统所要求的安全策略相比较)对拥有 IDPS 管理特权的系统进行配置。同时需注意 HIDPS 的管理特权漏洞:

——HIDPS 传感器拥有的主机操作系统特权漏洞,可产生更为严重的安全漏洞并损害运行 IDPS 代理的主机;

——HIDPS 的管理特权安全漏洞(易被忽略),在监视主机上执行攻击响应选项。

需保持对事态检测器和传感器的持续监视,以确保事态检测器和传感器的正确操作和运行(事态检测器将来自传感器的信息发送到检测分析部分),不会导致误报(如错误的安全感应)或漏报(如传感器失效,中央系统未发现此故障故中央系统将不会向中央管理员发送报警)等情况的发生。

A.6.2.6.2 鉴别

在进行管理操作之前,需对管理实体(可能是用户或系统实体)进行识别和鉴别。

A.6.2.6.3 完整性

需保护管理操作以避免完整性攻击。不可以未授权方式插入、删除或更改管理操作。

A.6.2.6.4 机密性

需保护管理操作以避免机密性攻击。不可以未授权方式推测管理操作的意图。

A.6.2.6.5 可用性

管理服务的可用性不可受相关攻击(针对网络基础设施、IDPS 或监视目标)的影响。例如,当发生拒绝服务攻击时,即使 IDPS 发生故障,也可对 IDPS 进行管理。IDPS 及其管理需纳入业务连续性管理。

A.6.3 管理模型

在包含大量 IDPS 部件的分布式环境中，IDPS 部件的有效控制和管理对实现入侵检测和防御的至关重要。图 A.3 提供了一个实现分层管理模型的示例，该模型主要适用于具有较大规模网络的组织。此模型主要缺点在于集中控制会导致单点失效（某些环境中可能无法接受）。同时，其也向攻击者提供了一个单一的攻击点，使得攻击者可延迟 IDPS 对攻击的检测，并阻止 IDPS 响应。

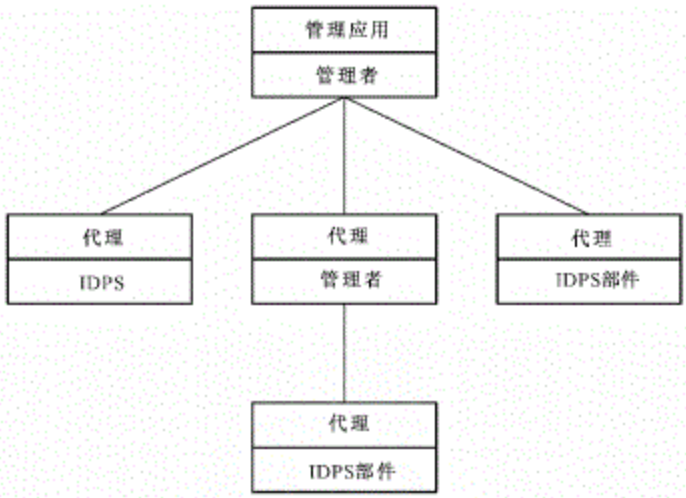

图 A.3 入侵检测管理模型

在分层模型中除了使用一对多，还可使用如下管理关系集合：

——多对多：多个管理控制台能管理多个分布式代理；

——一对一：一个管理控制台能管理一个代理。

A.7 实施和部署问题

A.7.1 简介

所有的 IDPS 不尽相同，因此当决定部署 IDPS 时，需考虑如下方面的因素：效率、功能、人员以及其他事项等。同时需根据自身的 IT 风险管理要求和安全策略，对已部署 IDPS 进行评价。

A.7.2 效率

部署 IDPS 时，效率是需要考虑的要素之一。评价 IDPS 效率的相关指标有：

——准确性：当 IDPS 把活动误认为攻击（如误报）或者 IDPS 把攻击误认为合法的活动（如漏报）时，就会出现误差。具体来说，准确性主要通过 IDPS 误报和漏报的数量与事态总数的比率来表示，其是重要的安全策略参数，表示分析执行情况的偏差。

——性能：主要是指收集、存储和处理审计事态的速度，只有性能较好时 IDPS 才可做到的实时检测。但需注意，IDPS 本身也会增加网络的负载。

——全面性：当 IDPS 无法检测到攻击时就会出现不全面性。具体的，全面性主要通过 IDPS 可检测攻击的种类多少表示，因为无法列出所有攻击，所以此项指标比其他几项指标难以评估。

——容错性：主要是指 IDPS 自身抵抗攻击尤其是拒绝服务攻击的能力。IDPS 运行于商用操作系统或硬件之上，因此易受到攻击。

——及时性：主要是指 IDPS 分发分析报告的速度，及时性越好，IDPS 响应速度就越快，从而使安

全负责人可在遭受重大损害前做出响应，并阻止攻击者破坏数据、数据源或 IDPS。

A.7.3 功能

功能是部署 IDPS 时另一个需要考虑的要素，主要包括：

——在加密或交换环境中使用：HIDPS 主要部署在主机上，可以避免在加密和交换环境中部署 NIDPS 面临的挑战，从而较好的适应加密和交换环境。

——检测攻击：NIDPS 在攻击发生时通过提供数据来检测恶意和可疑的攻击（如拒绝服务攻击），并实时检测以提供更快速的通知和响应。其主要检测基于主机未发现的相关攻击（如基于 IP 的拒绝服务攻击和分段包攻击，其仅可通过查找包头识别）。

——综合分析基于主机和基于网络的数据：IDPS 通过集成主机和网络组件，可综合利用基于主机和网络的数据源。正如 8.1 中的讨论，NIDPS 和 HIDPS 各自有其优缺点，可以相互补充。因此，基于主机的和基于网络的入侵检测和防御技术可结合起来分析，以增强信息系统防御。

A.7.4 IDPS 部署和操作人员

目前，IDPS 功能先进，其子系统与 IT 系统、服务和网络可以较好的集成在一起，但 IDPS 大部分的功能仍需要由接受过培训、了解相关知识[包括入侵检测与防御、IT 安全（包括网络安全）以及信息技术（包括网络拓扑结构和配置）]的人员手动完成。这些人员需具备如下能力：

——定制 IDPS，以便能够检测到与已部署 IDPS 的 IT 环境相关的事态；

——当 IDPS 报警时，解释 IDPS 要表达的内容；

——制定策略和程序，以响应 IDPS 报警；

——修复导致入侵成功的漏洞。

这些需要由人员手动完成的操作不在供应商 IDPS 安装范围内，但属于入侵检测和防御过程不可或缺的一部分。

分析模块主要对传感器收集的数据进行分析，以发现未授权活动、可疑活动或相关事态迹象（这些迹象表明正在探测/扫描网络、入侵已经发生或攻击正在进行）。其需要借助人工输入、人工配置、人机交互、人工对输出进行分析及解释、对 IDPS 调优等人工活动基础上，才能执行自动化部分。

IDPS 恰当配置后，通过分析相关数据可获悉网络中发生的入侵行为，此时需要人机交互（而非只是拒收相关数据包），由有经验的相关人员判断 IDPS 输出是否为误报（合法的活动被归为入侵）或漏报（入侵活动被识别为非入侵）。

响应主要包括自动化响应和手动响应。鉴于目前 IDPS 自动响应的缺乏（目前多数 IDPS 根据报警严重性对报警分类，却未给出报警发生后如何响应）、操作人员对手动响应的经验和知识不足（可能是新员工经验不足，也可能是由于入侵种类过多，经验知识丰富人员也无法识别所有入侵）、事态的快速发展，需在自动化响应基础上，为操作人员提供针对特定类型 IDPS 报警的响应指南，借助于手动响应对 IDPS 报警快速响应。

通过匹配已知漏洞的有效载荷模式或通过匹配恶意字节码特征，IDPS 可用于检测“零日漏洞”，此时，人员需告知供应商，让其了解未知的新漏洞，并采取相应控制措施。

A.7.5 实施中其他考虑事项

考虑实施、操作、集成和选择 IDPS 时，需要考虑的其他因素包括：

——用户接口。

——网络传感器的布局，即网络传感器需灵活放置以支持检测和响应策略（如检测攻击的外部防火墙）。

——系统故障容错，主要考虑系统完整性和防范可能的攻击，从而提高安全性和可用性。同时，建

议将 IDPS 传感器、监视器和管理者之间的通信放在与监视网络无关的独立网络中进行。

——IDPS 的保证。

——易用性即容易使用。

——IDPS 的可测量性。

——与其他安全产品的互操作性。

——供应商支持的级别和质量。

——管理：IDPS 不是“即插即用”设备，需技术人员对 IDPS 输出分析和解释。

——硬件和软件需求。

——文档。

——成本：除软件、硬件和安装成本之外，还包括教育、培训、操作和维护的成本。

A.8 入侵检测问题

A.8.1 入侵检测和隐私

当使用 IDPS 时，需要关注隐私问题。在识别或检测网络流量和操作系统审计日志的同时，查找包含恶意和可疑内容的攻击特征或特定模式。

IDPS 收集的网络流量或事态数据中，包含许多个人相关的数据，如硬件地址或 IP 地址。因此 IDPS 可用作监视用户及其行为(包括监视内部入侵者即内部员工，但需注意影响)。

使用 IDPS 时需考虑涉及隐私权问题的三个原则：

——入侵检测与防御必须以保护数据或系统为目的；

——数据(网络数据包、审计日志)收集必须以满足保护为目的；

——需制定并应用个人隐私保护(用于 IDPS 数据收集)相关策略。

第一个原则意味着入侵检测与防御不需要用作监督员工行为的工具。

第二个原则指出 IDPS 仅可收集和分析对识别攻击有必要的数据。将事态数据与 IDPS 攻击特征对比后，需删除不再需要的数据或未显示攻击迹象的数据，并通过安全的方式存储显示攻击迹象的数据。然而，在某些情况下，相关事态数据不可直接删除，需对其存档以便后续进行相关工作(诸如追溯攻击者或取证分析等)。显示攻击迹象的数据需加强分析，以获取其与攻击的关联性。所有相关数据都需要加强保护，尤其注重隐私保护。所采取的保护措施需与安全策略相一致。

数据按照安全策略要求存储一段时间后需安全地销毁，以保护所有相关方的隐私。这既为取证和法律调查预留了时间，也避免了隐私的泄露(如系统将来遭受未授权访问，但不会泄露敏感数据)。

第三个原则意味着需要依据隐私策略和适用于个人信息保护的相关法律，保护和管理个人信息。

A.8.2 入侵数据的共享

入侵数据和 IDPS 使用经验的共享对 IDPS 所有使用组织都是非常有用的，可帮助相关使用组织对入侵的早期进行预警、了解新型入侵的信息以及改进其 IDPS 操作。

目前，入侵公共知识的重要性已不言而喻，为有效利用与共享入侵公共知识，净化入侵的信息来源和 IDPS 的使用信息(即使信息匿名)，可在收集相关匿名知识和信息的基础上，参与合作构建入侵数据库，用于：

——整合有关脆弱性配置、入侵类型和如何利用这些配置等相关信息；

——处理关于入侵样本的信息，以便在先决条件、影响、踪迹、困难、补救措施等方面对入侵类型做出正确的说明；

——存储不同入侵类型的数据，共享不同入侵类型之间的差异；

——确保支持新的入侵描述的结构化格式；

——当发现新的脆弱性时，更新规则和(或)变更参数；

——提取需要的信息自动生成新规则(如签名、参数等)，以检测新的入侵。

IDPS 数据库类似于现代病毒检测系统(其通常可基于网络自动更新)。

入侵数据库不同于入侵事件数据库，前者主要存储入侵公共知识，后者存储有关攻击案例证据。

GB/T 32920—2016 列出了共享事件信息需考虑的事项。

参 考 文 献

[1] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2013,IDT)

[2] GB/T 22081—2016 信息技术 安全技术 信息安全控制实践指南(ISO/IEC 27002:2013,IDT)

[3] GB/T 25068.1—2012 信息技术 安全技术 IT 网络安全 第 1 部分:网络安全管理(ISO/IEC 18028-1:2006,IDT)

[4] GB/T 25068.3—2010 信息技术 安全技术 IT 网络安全 第 3 部分:使用安全网关的网间通信安全保护(ISO/IEC 18028-3:2005,IDT)

[5] GB/T 25068.4—2010 信息技术 安全技术 IT 网络安全 第 4 部分:远程接入的安全保护(ISO/IEC 18028-4:2005,IDT)

[6] GB/T 32920—2016 信息技术 安全技术 行业间和组织间通信的信息安全管理(ISO/IEC 27010:2012,IDT)

[7] ISO/IEC 15408(所有部分) 信息技术 安全技术 信息技术安全性评估准则

[8] ISO/IEC 18028-5 信息技术 安全技术 IT 网络安全 第 5 部份:使用虚拟专用网的跨网通信安全保护

[9] ISO/IEC 20000(所有部分) 信息技术 服务管理

[10] ISO/IEC 27001 信息技术 安全技术 信息安全管理体系 要求

[11] ISO/IEC 27002 信息技术 安全技术 信息安全控制实践指南

[12] ISO/IEC 27033-1:2009 信息技术 安全技术 网络安全 第 1 部分:概述和概念

[13] ISO/IEC 27033-2:2012 信息技术 安全技术 网络安全 第 2 部分:网络安全设计和实施指南

[14] ISO/IEC 27035:2011 信息技术 安全技术 信息安全事件管理