(2020春季　课程编号：011184)

信息安全导论

第8章　网络与系统安全防护

中国科学技术大学 曾凡平

billzeng@ustc.edu.cn

课程回顾：第7章 网络与系统攻击技术

- 7.1 网络攻击概述
  - 网络攻击的概念，网络攻击的一般流程
- 7.2 网络探测
  - 网络踩点，网络扫描，常见的扫描工具
- 7.3 缓冲区溢出攻击
  - 缓冲区溢出的基本原理，缓冲区溢出的防范
- 7.4 拒绝服务攻击
  - 常见的拒绝服务攻击
  - 分布式拒绝服务攻击，拒绝服务攻击的防范
- 7.5 僵尸网络
- **7.6 缓冲区溢出漏洞的分析与利用**

第8章 网络与系统安全防护

8.1 防火墙技术

- 防火墙的概念、特性、技术，
- 自适应代理技术，防火墙的体系结构
- 防火墙的应用与发展

8.2 入侵检测技术

- 入侵检测概述，入侵检测系统分类
- 分布式入侵检测，入侵检测技术发展趋势

8.3 “蜜罐”技术

- 概念，分类，关键机制，部署结构

8.4 应急响应技术

- 应急响应的概念，应急响应策略
- 应急事件处理流程，应急响应技术及工具

第8章 网络与系统安全防护

- **安全防护是指为保护己方网络和系统正常工作，保护信息数据安全而采取的措施和行动。**
- 攻击和防护是矛和盾的关系。在建立安全防护体系时，必须走管理和技术相结合的道路。

- 安全防护的涉及面很宽，从**技术层面**上讲主要包括防火墙技术、入侵检测技术、“蜜罐”技术、应急响应技术。
- 此外，从**广义**上看，病毒防护技术、数据加密技术和认证技术也属于安全防护技术。

8.1 防火墙技术

- Internet在提供便利的同时，也使得外面的世界能够接触到本地网络并对其产生威胁。为了保护内部网络的安全，通常使用防火墙。
- 防火墙被嵌入在本地网络和Internet之间，从而建立受控制的连接并形成外部安全墙或者说是边界。这个边界的目的在于防止本地网络受到来自Internet的攻击，并在安全性将受到影响的地方形成阻塞点。

- **防火墙的定义：**防火墙是位于两个(或多个)网络之间**执行访问控制**的软件和硬件系统，它**根据访问控制规则**对进出网络的数据流进行过滤。

8.1.1 防火墙的概念

- 防火墙的本义是指古代人们房屋之间修建的一道墙，可以防止火灾发生时蔓延到别的房屋。在计算机网络安全领域，防火墙是一个由软件和硬件组合而成的、起过滤和封锁作用的计算机系统或者网络系统，它一般部署在本地网络（内部网）和外部网(通常是Internet)之间，内部网络被认为是安全和可信赖的，外部网络则是不安全和不可信赖的。
- **防火墙的作用是隔离风险区域（外部网络）与安全区域（内部网）的连接**，阻止不希望的或者未授权的通信进出内部网络，通过边界控制强化内部网络的安全，同时不会妨碍内部网对外部网络的访问。

防火墙的概念

- **网络防火墙隔离了内部网络和外部网络，在企业内部网和外部网(Internet)之间执行访问控制策略，以防止发生不可预测的、外界对内部网资源的非法访问或潜在的破坏性侵入。**
- 防火墙被设计成只运行专门用于访问控制软件的设备，而没有其他服务，具有相对较少的缺陷和安全漏洞。此外，防火墙改进了登录和监测功能，可以进行专用的管理。如果采用了防火墙，内部网中的计算机不再直接暴露给来自Internet的攻击。
- 因此，对整个内部网的主机的安全管理就变成了对防火墙的安全管理，使得安全管理更方便，易于控制。
- 防火墙是目前实现网络安全策略的最有效的工具之一，也是控制外部用户访问内部网的第一道关口。

8.1.2 防火墙的特性

一般而言，防火墙的设计目标有以下几个：

(1)**针对所有的通信**，无论是从内部到外部还是从外部到内部的，都必须经过防火墙。这一点可以通过阻塞所有未通过防火墙的对本地网络的访问来实现。

(2)**只有被授权的通信才能通过防火墙**，这些授权将在**安全策略**中规定。不同类型的防火墙实现不同的安全策略。

(3)**防火墙本身对于渗透攻击必须是免疫的**。这意味着必须使用运行安全操作系统的可信系统。

防火墙采用的4项常用技术

① **服务控制**：决定哪些Internet服务可以被访问，无论这些服务是从内而外还是从外而内。防火墙可以以IP地址和TCP端口为基础过滤通信；也可以提供代理软件，在服务请求通过防火墙时接收并解释它们；或者执行服务器软件的功能，比如邮件服务。

② **方向控制**：决定在哪些特定的方向上服务请求可以被发起并通过防火墙。

③ **用户控制**：根据用户正在试图访问的服务器，来控制其访问。这个技术特性主要应用于防火墙网络内部的用户（本地用户），也可以应用到来自外部用户的通信。后者要求某种形式的安全认证技术，如IPSec。

④ **行为控制**：控制一个具体的服务怎样被实现。例如，防火墙可以通过过滤邮件来清除垃圾邮件。它也可能只允许外部用户访问本地服务器的部分信息。

防火墙具有的典型功能

(1)访问控制功能。这是防火墙最基本和最重要的功能，通过禁止或允许特定用户访问特定资源，保护内部网络的资源和数据。防火墙定义了单一阻塞点，它使得未授权的用户无法进入网络，禁止潜在的、易受攻击的服务进入网络。

(2)内容控制功能。根据数据内容进行控制，比如过滤垃圾邮件、限制外部只能访问本地Web服务器的部分功能等。

(3)日志功能。防火墙需要完整地记录网络访问的情况，包括进出内部网的访问。一旦网络发生了入侵或者遭到破坏，可以对日志进行审计和查询，查明事实。

防火墙具有的典型功能

(4)集中管理功能。针对不同的网络情况和安全需要，指定不同的安全策略，在防火墙上集中实施，使用中还可能根据情况改变安全策略。防火墙应该是易于集中管理的，便于管理员方便地实施安全策略。

(5)自身安全和可用性。防火墙要保证自己的安全，不被非法侵入，保证正常的工作。如果防火墙被侵入，安全策略被破坏，则内部网络就变得不安全。防火墙要保证可用性，否则网络就会中断，内部网的计算机无法访问外部网的资源。

- 另外，防火墙可能还具有流量控制、网络地址转换(NAT)、虚拟专用网(VPN)等功能。

防火墙的局限性

(1)防火墙不能防御不经由防火墙的攻击。比如，如果允许从内部网络向外拨号，网络内部可能会有用户通过拨号连入Internet，形成与Internet的直接连接，从而绕过了防火墙，成为一个潜在的后门攻击渠道。

(2)防火墙不能防范来自内部的威胁。比如，某个私下里与网络外部攻击者联手的雇员，从内部网进行破坏活动，因为该通信没有经过防火墙，则防火墙无法阻止。

(3)防火墙不能防止病毒感染的程序和文件进出内部网。事实上，安装了防火墙的网络系统内部，运行着多种多样的操作系统和应用程序，想通过扫描所有进出网络的文件、电子邮件以及信息来检测病毒的方法是不实际的，也是不大可能实现的。这只能在每台主机上安装反病毒软件。

(4)防火墙不能防止数据驱动式的攻击。一些表面正常的数据通过电子邮件或者其他方式复制到内部主机上，一旦被执行就形成攻击。

8.1.3 防火墙的技术

根据不同的分类标准，可将防火墙分为不同的类型。

A. 从**工作原理**角度看，防火墙技术主要可分为**网络层防火墙技术和应用层防火墙**技术。这两个层次的防火墙技术的具体实现有包过滤防火墙、代理服务器防火墙、状态检测防火墙和自适应代理防火墙。

B. 根据实现防火墙的硬件**环境**不同，可将防火墙分为**基于路由器的防火墙和基于主机系统的防火墙**。包过滤防火墙和状态检测防火墙可以基于路由器，也可基于主机系统实现；而代理服务器防火墙只能基于主机系统实现。

C. 根据防火墙的**功能**不同，可将防火墙分为FTP防火墙、Telnet防火墙、E-mail防火墙、病毒防火墙、个人防火墙等各种专用防火墙。通常也将几种防火墙技术结合在一起使用以弥补各自的缺陷，增加系统的安全性能。

1．包过滤技术

- 网络层防火墙技术根据网络层和传输层的原则对传输的信息进行过滤。网络层技术的一个范例就是**包过滤(packet filtering)**技术。因此，利用包过滤技术在网络层实现的防火墙也叫包过滤防火墙。

1)包过滤原理

- 包过滤技术是最早的防火墙技术，工作在网络层。
- 这种防火墙的原理是将IP数据报的各种包头信息与防火墙内的规则进行比较，然后根据过滤规则有选择地阻止或允许数据包通过防火墙。常用的包头信息包括**源地址、目的地址、源端口、目的端口、协议类型等**。

包过滤防火墙的主要工作原理

- 包过滤防火墙要遵循的一条基本原则就是**“最小特权原则”**，即明确允许管理员希望通过的那些数据包，禁止其他的数据包。包过滤的核心技术是安全策略及过滤规则的设计。包过滤防火墙一般由路由器充当，要求路由器在完成路由选择和数据转发之外，同时具有包过滤功能。

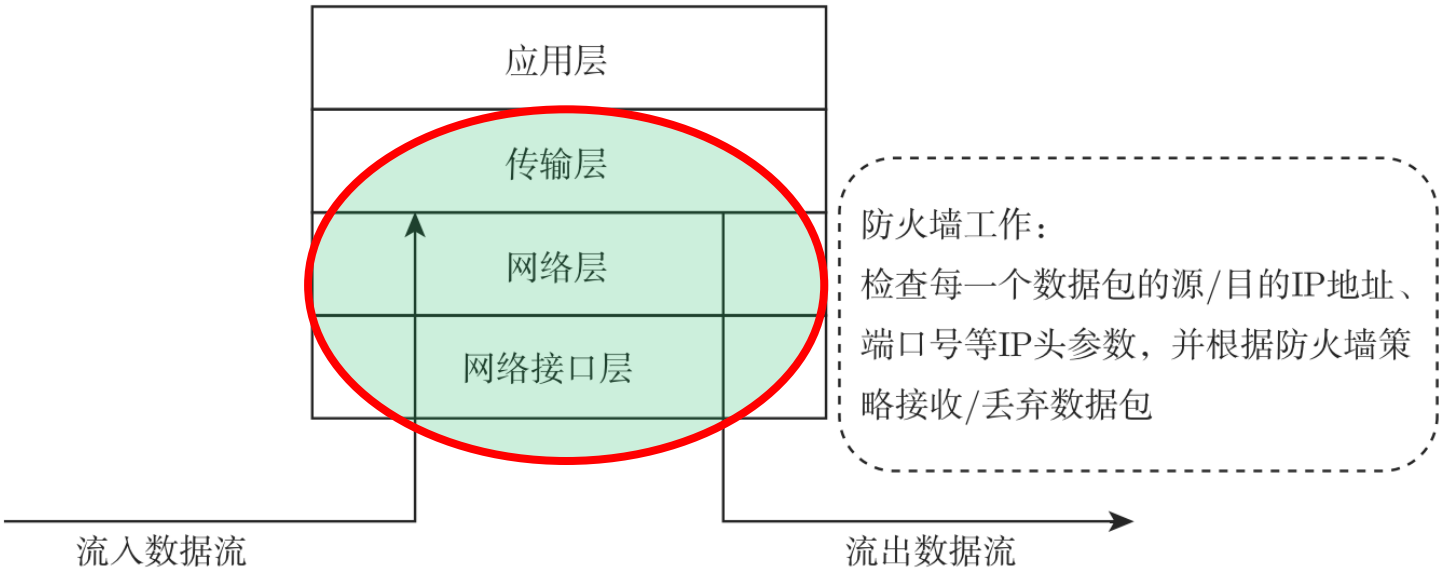


图8-1 包过滤防火墙

包过滤防火墙的具体实现

- 包过滤防火墙的具体实现是基于过滤规则的。建立这类防火墙包括如下步骤：建立安全策略，写出所允许和禁止的任务，将**安全策略**转化为一个**包过滤规则表**。过滤规则的设计主要依赖于数据包所提供的包头信息：源地址、目的地址、TCP/UDP源端口号、TCP/UDP目的端口号、标志位、用来传送数据包的协议等。由规则表和数据头内容的匹配情况来执行过滤操作。**如果有一条规则和数据包的状态匹配，就按照这条规则来执行过滤操作；如果没有一条规则匹配，就执行默认操作**。
- 默认的策略可能是：

① **默认值：丢弃**：那么所有没有被规定允许转发的数据包都将被丢弃。

② **默认值：转发**：那么所有没有被规定需要丢弃的数据包都将被转发。

包过滤规则表的例子

表8-1包过滤的实例

A	处理	内部主机	端口	外部主机	端口	说明
	阻塞	*	*	SPIGOT	*	这些人不被信任
	通过	OUR-GW	25	*	*	与内部主机的 SMTP 端口有连接
B	处理	内部主机	端口	外部主机	端口	说明
	阻塞	*	*	*	*	默认
C	处理	内部主机	端口	外部主机	端口	说明
	通过	*	*	*	25	与外部主机的 SMTP 端口有连接

- A：允许进入防火墙内部的邮件通过（端口25专门供SMTP进入内部使用），但是只能发往一台特定的网关主机，从特定的外部主机SPIGOT发来的邮件将被阻塞。
- B：默认策略。实际应用中，所有的规则表都把默认策略当作最后的规则。
- C：这个规则表规定内部的每一台主机都可以向外部发送邮件。一个目的端口为25的TCP包将被路由到目的机器上的SMTP服务器。

2) 包过滤防火墙的优点

(1) 一个过滤器能协助保护整个网络。如果仅有一个包过滤路由器连接内部与外部网路，不论内部网络的大小和内部拓扑结构如何，通过该路由器进行数据包过滤，就可在网络安全保护上取得较好的效果。

(2)包过滤用户对用户透明。数据包过滤不要求任何自定义软件或客户机配置，也不要求用户任何特殊的训练或操作。

(3)过滤路由器速度快、效率高。过滤路由器只检查包头相应的字段，一般不查看数据包的内容，而且某些核心部分是由专用硬件实现的，故其转发速度快、效率较高。

(4)技术通用、廉价、有效。大多数路由器都提供包过滤功能，不用再增加更多的硬件和软件，因此其价格低廉，能很大程度地满足企业的安全要求，其应用行之有效。

- 此外，包过滤防火墙还易于安装、使用和维护。

3)包过滤防火墙的缺点

(1)**安全性较差**。防火墙过滤的只有网络层和传输层的有限消息，因而各种安全要求不可能充分满足。

(2)由于防火墙可用的信息有限，它所提供的**日志功能也十分有限**。

(3)**无法执行某些安全策略**。包过滤路由器上的信息不能完全满足人们对安全策略的需求。

(4)这种防火墙通常**容易受到利用TCP/IP规定和协议栈漏洞的攻击**，例如网络层地址欺骗。

(5)在这种防火墙做出安全控制决定时，**起作用的只是少数几个因素**，包过滤器防火墙对由于不恰当的设置而导致的安全威胁显得十分脆弱。

- 在实际应用中，**很少把这种包过滤技术作为单独的解决方案**，而是把它与其他防火墙技术组合在一起使用。

2．代理服务技术

1)代理服务技术原理

- 代理服务器防火墙又称**应用层网关、应用层防火墙**，它工作在OSI模型的应用层，掌握着应用系统中可用作安全决策的全部信息。
- 代理服务技术的核心是运行于防火墙主机上的代理服务器程序，这些代理服务器程序直接对特定的应用层进行服务。
- 代理服务器防火墙**完全阻隔了网络通信流**，通过对每种应用服务编制专门的代理服务程序，实现监视和控制应用层通信流的作用。从内部网用户发出的数据包经过这样的防火墙处理后，就像是源于防火墙外部网卡一样，从而可以达到隐藏内部网结构的作用。
- 其技术原理如图8-2所示。

代理服务技术

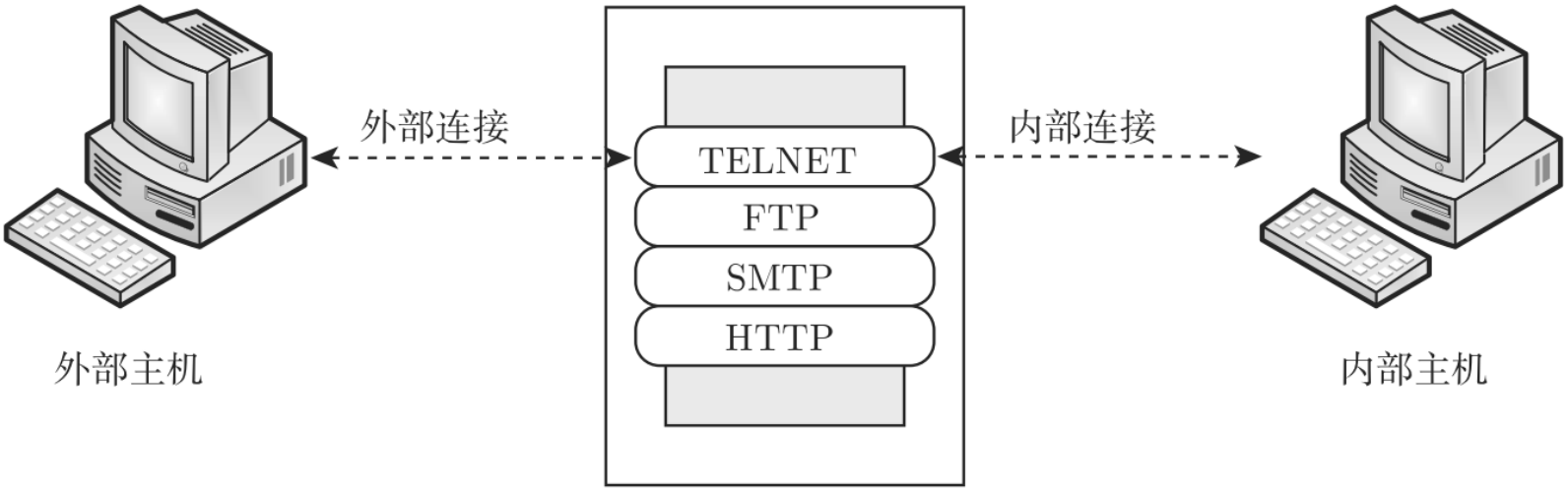


图8-2 代理服务技术

- 代理服务器通常运行在两个网络之间，在某种意义上，可以把这种防火墙看作一个翻译器，由它负责外部网络和内部网络之间的通信。
- 代理服务技术能够记录通过它的一些信息，如什么用户在什么时间访问过什么站点等，这些信息可以帮助网络管理员识别网络间谍。
- 代理服务可以实现用户认证、详细日志、审计跟踪和数据加密等功能，并实现对具体协议及应用的过滤，如阻塞JavaScript。

2)代理服务器的实现

(1)应用代理服务器

- **应用代理服务器可以在网络应用层提供授权检查及代理服务功能**。当外部某台主机试图访问受保护的内部网时，它必须先在防火墙上经过身份认证。通过身份认证后，防火墙运行一个专门程序，把外部主机与内部主机连接。在这个过程中，防火墙可以限制用户访问的主机、访问时间及访问方式。同样，受保护的内部网络用户访问外部网时也需要先登录到防火墙上，通过验证后才可使用Telent或FTP等有效命令。
- **应用代理服务器的优点是既可以隐藏内部IP地址，也可以给单个用户授权**。即使攻击者盗用了一个合法的IP地址，他也要通过严格的身份认证。但是这种认证使得应用网关不透明，用户每次连接都要受到“盘问”，这会给用户带来许多不便。而且这种代理技术需要为每个应用网关编写专门的程序。

(2)回路级代理服务器

- 回路级代理服务器也称**一般代理服务器**，它**适用于多个协议**，但不解释应用协议中的命令就建立连接回路。回路级代理服务器通常要求修改过的用户程序。
- 套接字服务器(sockets server)就是回路级代理服务器。套接字(sockets)是一种网络应用层的国际标准。当受保护的网络客户机需要与外部网交互信息时，在防火墙上的套接字服务器检查客户的UserID、IP源地址和IP目的地址，经过确认后，套接字服务器才与外部服务器建立连接。对用户来说，受保护的内部网与外部网的信息交换是透明的，感觉不到防火墙的存在，那是因为因特网用户不需要登录到防火墙。

(3)智能代理服务器

- 如果一个代理服务器不仅能处理转发请求，同时还能够做其他许多事情，这种代理服务器称为智能代理服务器。智能代理服务器可提供比其他方式更好的日志和访问控制能力。一个专用的应用代理服务器很容易升级到智能代理服务器，而回路级代理服务器则比较困难。

(4)邮件转发服务器

- 当防火墙采用相应技术使得外部网络只知道防火墙的IP地址和域名时，从外部网络发来的邮件就只能发送到防火墙上。这时防火墙对邮件进行检查，只有当发送邮件的源主机是被允许的，防火墙才对邮件的目的地址进行转换，送到内部的邮件服务器，由其进行转发。

3)代理服务器防火墙的特点

(1)**安全性好**。安全性好是代理服务技术突出的特点。

(2)易于配置。

(3)能生成各项记录。代理生成的日志和记录对于流量分析、安全检验是十分重要的。

(4)能完全控制进出的流量和内容。

(5)**能过滤数据内容**。可以把一些过滤规则应用于代理，让它在高层实现过滤功能，例如，文本过滤、图像过滤、预防病毒和扫描病毒等。

(6)能为用户提供透明的加密机制。

(7)**可以方便地与其他安全技术合成**。目前安全问题解决方案很多，如验证(authentication)、授权(authorization)、账号(accouting)数据加密、安全协议(SSL)等。如果把代理与这些技术联合使用，将大大增强网络的安全性。

代理服务技术也有它的缺点

(1)**速度较慢**。

(2)**对用户不透明**。

(3)对于不同服务器代理可能要求不同的服务器，可能需要为每项协议设置一个不同的代理服务器。选择、安装和配置所有这些不同的服务器是一项较繁重的工作。

(4)通常要求对客户或者过程进行限制。除了一些为代理而设置的服务，代理服务器要求对客户或过程进行限制，每一种限制都有不足之处，人们无法经常按他们自己的步骤使用快捷可用的方式。由于这些限制，代理应用就不能像非代理应用运行得那样好，它们往往可能曲解协议的说明。

(5)代理不能改进底层协议的安全性。

3．状态检测技术

1)状态检测技术的工作原理

- **状态检测(stateful inspection)技术**由CheckPoint率先提出，又称**动态包过滤技术**。
- 状态检测技术是一项新的防火墙技术。这种技术具有非常好的安全特性，它使用一个在网关上实行的网络安全策略的软件模块，称为**检测引擎**。
- 检测引擎在不影响网络正常运行的前提下，采取抽取有关数据的方法对网络通信各层实时监测。**检测引擎将抽取的状态信息动态地保存起来作为以后执行安全策略的参考**。
- 检测引擎维护一个**动态的状态信息表**并对后续的数据包进行检查，一旦发现任何连接的参数有意外的变化，连接就被终止。

状态检测技术的工作原理

- **状态检测技术监视和跟踪每一个有效连接的状态，并根据这些信息决定网络数据包是否能通过防火墙**。它在协议底层截取数据包，然后分析这些数据包，并将当前数据包和状态信息与前一时刻的数据包和状态信息进行比较，从而得到该数据包的控制信息，来达到保护网络安全的目的。
- 检测引擎支持多种协议和应用程序，并可以很容易地实现应用和服务的扩充。
- 与前两种防火墙不同，当用户访问请求到达网关的操作系统前，状态监视器要收集有关数据进行分析，结合网络配置和安全规定做出接纳或拒绝、身份认证、警报处理等动作。一旦某个访问违反了安全规定，该访问就会被拒绝，并报告有关状态，做日志记录。

状态检测技术的工作原理

- 状态检测技术试图跟踪通过防火墙的网络连接和包，这样它就可以使用一组附加的标准，以确定是否允许和拒绝通信。状态检测防火墙是在使用了基本包防火墙的通信上应用一些技术来做到这一点的。为了跟踪包的状态，状态检测防火墙不仅跟踪包中包含的信息，还要记录有用的信息以帮助识别包。
- 状态检测技术可检测无连接状态的远程过程调用(RPC)和用户数据包(UDP)之类的端口信息，而包过滤和代理服务技术都不支持此类应用。状态检测防火墙无疑是非常坚固的，但它会降低网络的速度，而且配置也比较复杂。好在有关防火墙厂商已经注意到这一问题，如CheckPoint公司的防火墙产品Firewall-1，所有的安全策略规则都是通过面向对象的图形用户界面(GUI)定义的，因此可以简化配置过程。

表8-2状态检测防火墙的状态表实例

源地址	源端口	目的地址	目的端口	连接状态
192.168.1.100	1030	210.9.88.29	80	已建立
192.168.1.102	1031	216.32.42.123	80	已建立
192.168.1.101	1033	173.66.32.122	25	已建立
192.168.1.106	1035	177.231.32.12	79	已建立
223.43.21.231	1990	192.168.1.6	80	已建立
219.22.123.32	2112	192.168.1.6	80	已建立
210.99.212.18	3321	192.168.1.6	80	已建立
24.102.32.23	1025	192.168.1.6	80	已建立
223.212.21.2	1046	192.168.1.6	80	已建立

2)通过状态检测防火墙数据包的类型

(1) TCP包：

当建立起一个TCP连接时，通过的第一个包被标有包的SYN标志。通常，防火墙丢弃所有外部的链接企图，除非已经建立起某条特定规则来处理它们。对内部到外部的主机连接，防火墙注明连接包，允许通过影响两个系统之间的包，直接到连接结束为止。在这种方式下，传入的包只有在它响应一个已建立的连接时，才会允许通过。

(2) UDP包：UDP包比TCP包简单，因为它们不包含任何连接或序列信息，只包含源地址、目的地址、检验和携带的数据。这些简单的信息使得防火墙很难确定包的合法性，因为没有打开的连接可利用，以测试传入的包是否应被允许通过。但如果防火墙跟踪包的状态，就可以确定其合法性。对传入的包，若它使用的地址和UDP包携带的协议与传出的连接请求匹配，该包就被允许通过。

3)状态检测技术的特点和应用

- **状态检测技术结合了包过滤技术和代理服务技术的特点**。与包过滤技术一样，它对用户透明，能够在OSI网络层上通过IP地址和端口号过滤进出的数据包；与代理服务技术一样，它可以在OSI应用层上检查数据包内容，查看这些内容是否符合安全规则。
- **状态检测技术克服了包过滤技术和代理服务技术的局限性**，能根据协议、端口及源地址、目的地址的具体情况决定数据包是否通过。对于每个安全策略允许的请求，状态检测技术启动相应的进程，可快速地确认符合授权标准的数据包，使得运行速度加快。
- **状态检测技术的缺点是状态检测可能造成网络连接的某种迟滞**，但运行速度越快，这个问题就越不易察觉。
- 状态检测防火墙已经在国内外得到广泛应用。目前市场上流行的防火墙大多属于状态检测防火墙。

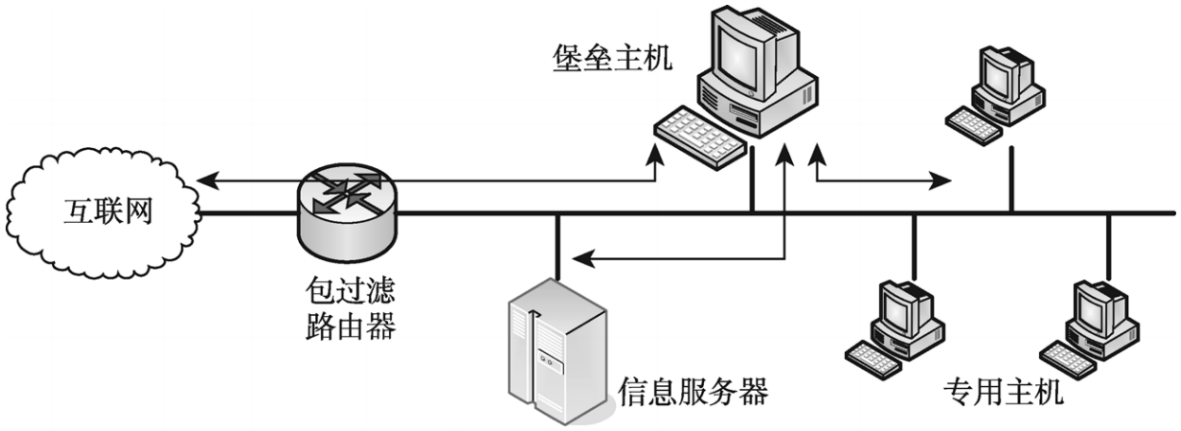
8.1.4 自适应代理技术

- **自适应代理(adaptive proxy)**防火墙技术，本质上也属于代理服务技术，但它也结合了动态包过滤（状态检测）技术。
- 自适应代理技术是最近在商业应用防火墙中实现的一种革命性的技术。
- 组成这类防火墙的基本要素有两个，即自适应代理服务器和动态包过滤器。
- **自适应代理防火墙结合了代理服务器防火墙的安全性和包过滤防火墙的高速等优点**，在保证安全性的基础上将代理服务器防火墙的性能提高十倍以上。

自适应代理技术的实现

- 在自适应代理服务与动态包过滤器之间存在一个控制通道。在对防火墙进行配置时，用户仅仅将需要的服务类型、安全级别等信息通过相应代理的管理界面进行设置就可以了。
- 然后，自适应代理就可以根据用户的配置信息，决定是使用相应代理服务从应用层代理请求，还是使用动态包过滤器从网络层转发包。如果是后者，它将动态地通知包过滤器增减过滤规则，满足用户对速度和安全的双重要求。

8.1.5 防火墙的体系结构



(a) 屏蔽主机防火墙(单宿堡垒主机)

- 堡垒主机是由防火墙的管理人员所指定的某个系统，它是网络安全的一个关键点。

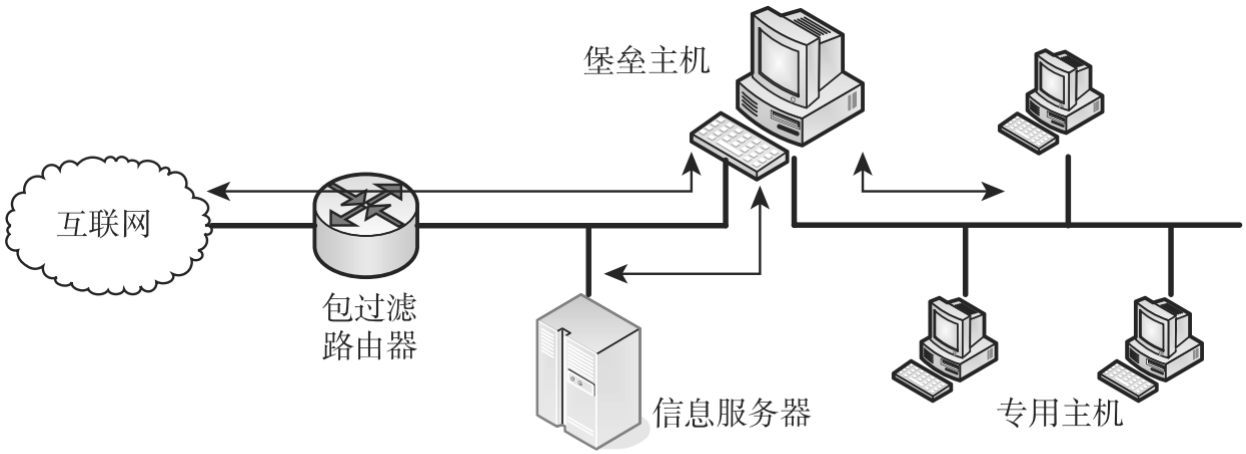
1)屏蔽主机防火墙（单宿堡垒主机）

- 堡垒主机是外部网主机能连接到的唯一的内部网上的系统，任何外部系统要访问内部网的资源都必须先连接到这台主机(图8-3(a))。路由器按照如下方式配置。

(1)对来自Internet的通信，只允许发往堡垒主机的IP包通过。

(2)对来自网络内部的通信，只允许经过了堡垒主机的IP包通过。

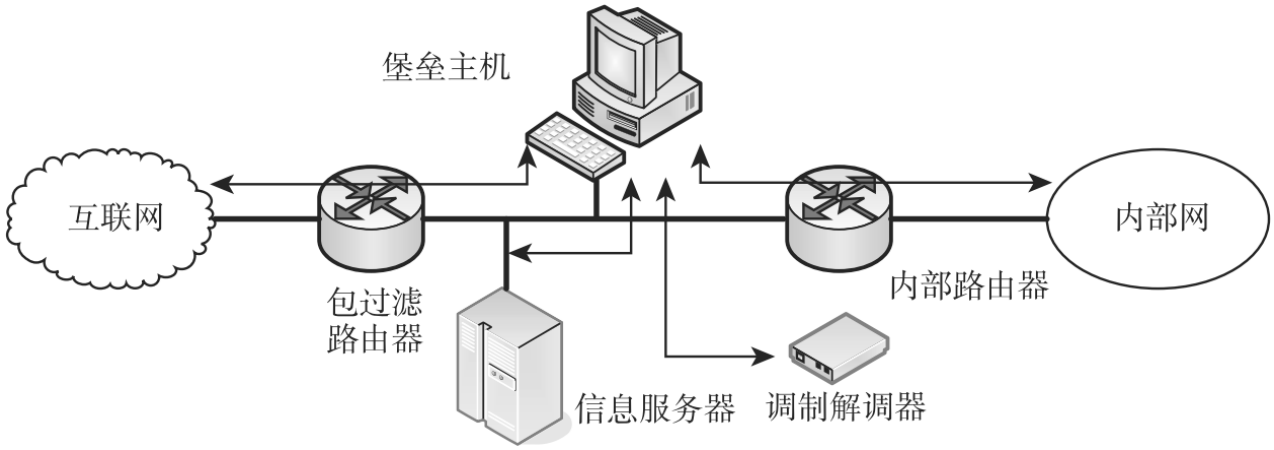
2)屏蔽主机防火墙（双宿堡垒主机）



(b) 屏蔽主机防火墙(双宿堡垒主机)

- 在单宿堡垒主机体系中，如果包过滤路由器被攻破，那么通信就可以越过路由器在 Internet和内部网络的其他主机之间直接进行。**屏蔽主机防火墙双堡垒主机结构**在物理上防止了这种安全漏洞的产生(图8-3(b))。双宿堡垒主机具有至少两个网络接口，外部网络和内部网络都能与堡垒主机通信，但是不能直接通信，它们之间的通信必须经过双宿堡垒主机的过滤和控制。

3)屏蔽子网防火墙



(c) 屏蔽子网防火墙

- 如图8-3(c)所示，屏蔽子网防火墙是我们所探讨的配置里最为安全的一种。
- 在这种配置中，使用了两个包过滤路由器，一个在堡垒主机和Internet之间，称为外部屏蔽路由器；另一个在堡垒主机和内部网络之间，称为内部屏蔽路由器。每一个路由器都被配置为只和堡垒主机交换流量。

8.1.6 防火墙的应用与发展

1.防火墙的应用

- **选用防火墙首先要明确哪些数据是必须保护的**，这些数据的被侵入会导致什么样的后果，以及网络不同区域需要什么等级的安全级别。不管采用原始设计还是使用现成的防火墙产品，对于防火墙的安全标准，首先需根据安全级别确定；其次，选用防火墙必须与网络接口匹配，要防止可以预料到的各种威胁。防火墙可以是软件模块或硬件模块，并能集成于网桥、网关或路由器等设备之中。
- **选用防火墙时要注意防火墙自身的安全性。**

- 防火墙的选用也要考虑用户的安全策略中的特殊需求，比如：

(1) **IP地址转换**。进行IP地址转换有两个好处：一是隐藏内部网络真正的IP地址，可以使黑客无法直接攻击内部网络，这也是强调防火墙自身安全性的主要原因；二是可以让内部用户使用保留的IP地址，这对许多IP不足的企业是有益的。

(2)**双重DNS**。当内部网络使用没有注册的IP地址或防火墙进行IP转换时，DNS也必须经过转换。因为同一个主机的内部IP与给予外界的IP将会不同，有的防火墙会提供双重DNS，有的则必须在不同主机上各安装一个DNS。

(3)**虚拟专用网络(VPN)**。VPN可以在防火墙与防火墙或移动的客户机间对所有网络传输的内容加密，建立一个虚拟通道，让两者感觉是在同一个网络上，可以安全且不受拘束地相互存取。

(4)**病毒扫描功能**。大部分防火墙都可以与防病毒系统搭配以实现病毒扫描功能，有的防火墙则可以直接集成病毒扫描功能。差别只是病毒扫描工作是由防火墙完成，或是由另一台专用的计算机完成。

(5)**特殊控制需求**。有时候企业会有特别的控制需求，如限制特定使用者发送Email，FPT只能下载文档而不能上传文档，限制同时上网人数、使用时间等，防火墙需要依需求不同而定。

2.防火墙技术的发展

1)智能化

- 防火墙将从目前的静态防御策略向具备人工智能的智能化方向发展。未来智能化的防火墙应能实现以下功能。

(1)自动识别并防御各种黑客攻击手法及其相应变种攻击手法。

(2)在网络出口发生异常时自动调整与外网的连接端口。

(3)根据信息流量自动分配、调整网络信息流量及协同多台物理设备工作。

(4)自动检测防火墙本身的故障并能自动修复。

(5)具备自主学习能力并能制定识别与防御方法。

防火墙技术的发展

2)高速度

- 随着网络传输速率的不断提高，防火墙必须在响应速度和报文转发速度方面做相应的升级，这样才不至于成为网络的瓶颈。

3)分布式并行结构

- 分布式并行处理的防火墙是防火墙的另一发展趋势，在这种概念下，将有多台物理防火墙协同工作，共同组成一个强大的、具备并行处理能力和负载均衡能力的逻辑防火墙。

4)多功能

(1)在保密性方面，将继续发展高保密性的安全协议用于建立VPN，基于防火墙的VPN在较长一段时间内将继续成为用户使用的主流。

(2)在过滤方面，将从目前的地址、服务、URL、文本、关键字过滤发展到对CGI、ActiveX、 Java等Web应用的过滤，并将逐渐具备病毒过滤的功能。

(3)在服务方面，将在目前透明应用的基础上完善其性能，并将具备针对大多数网络通信协议的代理服务功能。

(4)在管理方面，将从子网和内部网络的管理方式向基于专用通道和安全通道的远程集中管理方式发展，管理端口的安全性将是其重点考虑内容。用户费用统计、多种媒体的远程警报及友好的图形化管理界面将成为防火墙的基本功能板块。

(5)在安全方面，对网络攻击的检测、拦截及告警功能将继续是防火墙最重要的性能指标。

5)专业化

- 单向防火墙、电子邮件防火墙、FTP防火墙等针对特定服务的专业化防火墙将作为一种产品门类出现。

未来防火墙的发展思路

① 防火墙将从目前对子网或内部网管理的方式向远程上网集中管理方式发展；过滤深度不断加强，从目前的地址、服务过滤，发展到URL(页面)过滤、关键字过滤和对ActiveX、Java等的过滤，并逐渐有病毒清除功能。

② 利用防火墙建立VPN是较长一段时间内用户使用的主流，IP的加密需求越来越强，安全协议的开发是一大热点；对网络攻击的检测和告警将成为防火墙的重要功能。

③ 此外，网络的防火墙产品还将把网络前沿技术，如Web页面超高速缓存、虚拟网络和带宽管理等与其自身结合起来。

8.2 入侵检测技术

- 传统的安全防护技术包括防火墙、杀毒软件、加密软件等，也称为“被动防护”技术，难于及时应对日趋复杂多样的攻击工具与手法带来的挑战。
- **入侵检测**是一种从更深层次上进行**“主动”网络安全防御**的措施。它不仅可以通过监测网络实现对内部攻击、外部入侵和误操作的实时保护，有效地弥补防火墙的不足，而且能结合其他网络安全产品，对网络安全进行全方位的保护，具有**主动性和实时性**的特点。
- 目前，入侵检测的相关研究已成为网络安全领域的热点课题，基于人工智能的入侵检测成为了主流。

8.2.1 入侵检测概述

1. 入侵检测的概念

- 入侵检测是指在计算机网络或计算机系统中的**若干关键点收集信息并对收集到的信息进行分析**，从而判断网络或系统中是否有违反安全策略的行为和被攻击的迹象。它**是对入侵行为的发觉**。
- 入侵检测作为安全技术，其**主要目的**在于：第一，识别入侵者；第二，识别入侵行为；第三，检测和监视已成功的安全突破；第四，为对抗入侵及时提供重要信息，阻止事件的发生和事态的扩大。
- 所以说，入侵检测对建立一个安全系统来说是非常必要的，它可以弥补传统安全保护措施的不足。

2．入侵检测过程

- 入侵检测的**典型过程**是：信息收集、信息（数据）预处理、数据的检测分析、根据安全策略做出响应。有的还包括检测效果的评估。

① **信息收集**是指从网络或系统的**关键点**得到原始数据，这里的数据包括原始的网络数据包、系统的审计日志、应用程序日志等原始信息；

② **数据预处理**是指对收集到的数据进行预处理，将其转化为检测器所需要的格式，也包括对冗余信息的去除，即数据简约；

③ **数据的检测分析**是指利用各种算法建立检测器模型，并对输入的数据进行分析以判断入侵行为的发生与否。入侵检测的效果如何将直接取决于检测算法的好坏。

④ **响应**是指产生检测报告，通知管理员，断开网络连接，或更改防火墙的配置等积极的防御措施。

审计记录的两种方法

- 入侵检测的一个基本工具是审计记录。用户活动的记录应作为入侵检测系统的输入。两种方法：

(1)原始审计记录：几乎所有的多用户操作系统都有收集用户活动信息的审计软件。使用这些信息的好处是不需要再额外使用收集软件。其缺点是审计记录可能没有包含所需的信息，或者信息没有以方便的形式保存。

(2)检测专用的审计记录：使用的收集工具可以只记录入侵检测系统所需要的审计记录。此方法的优点在于提供商的软件可适用于不同的系统。缺点是一台机器要运行两个审计包管理软件，需要额外的开销。

每个审计记录包含的域

(1)主体：行为的发起者。主体通常是终端用户，也可是充当用户或用户组的进程。所有活动都来自主体发出的命令。主体分为不同的访问类别，类别之间可以重叠。

(2)动作：主体对一个对象的操作或联合一个对象完成的操作。如登录、读、I/O操作和执行。

(3)客体：行为的接收者。客体包括文件、程序、消息、记录、终端、打印机、用户或程序创建的结构。当一个客体是一个活动的接收者时，则主体也可看成是客体，比如电子邮件。客体可根据类型分类，客体的粒度可根据客体类型和环境发生变化。

(4)异常条件：若返回时有异常，则标识出该异常情况。

(5)资源使用：指大量元素(资源使用的数量)的列表。

(6)时间戳：当动作发生时用来标识的唯一的时间日期戳。

3．入侵检测系统

- 入侵检测系统(intrusion detection system，IDS)是完成入侵检测功能的软件、硬件的组合。
- IETF定义了一个IDS的**通用入侵检测模型（CIDF）**，如图8-4所示

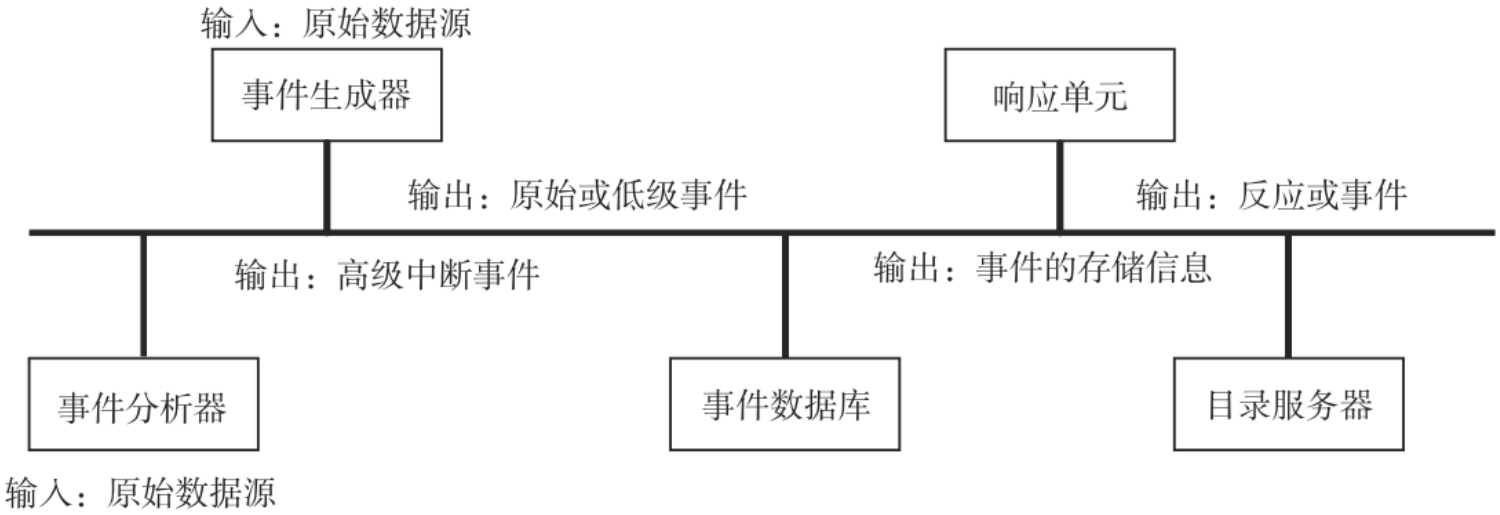
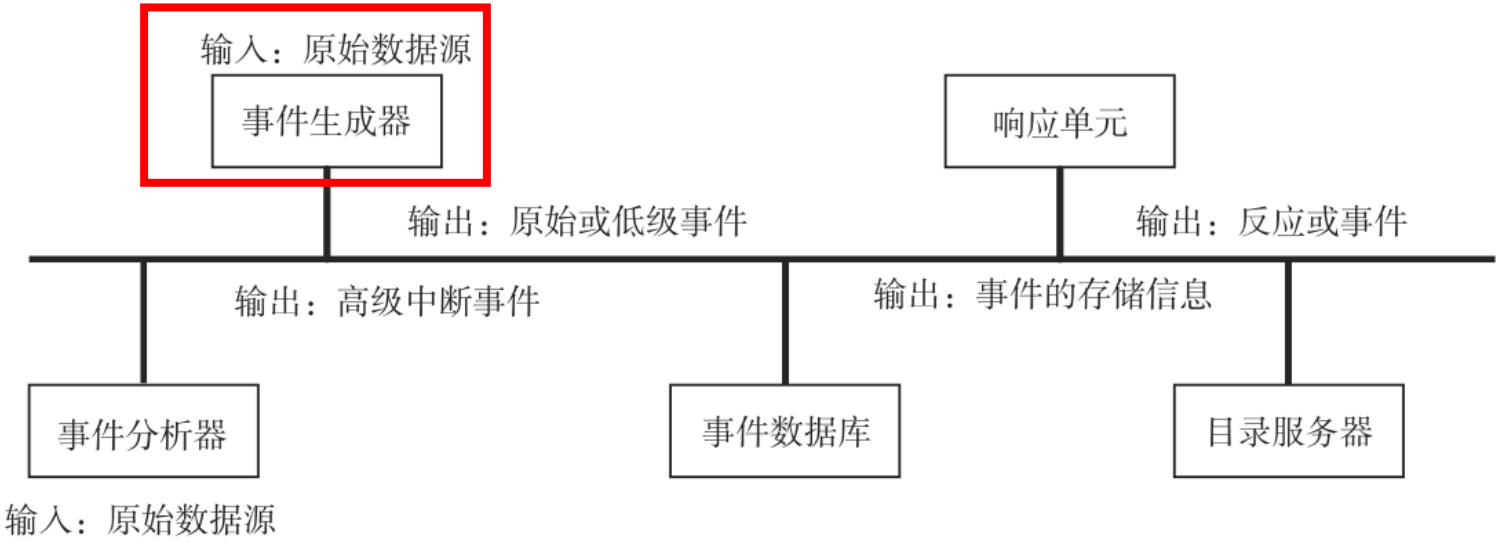


图8-4 IDS体系结构

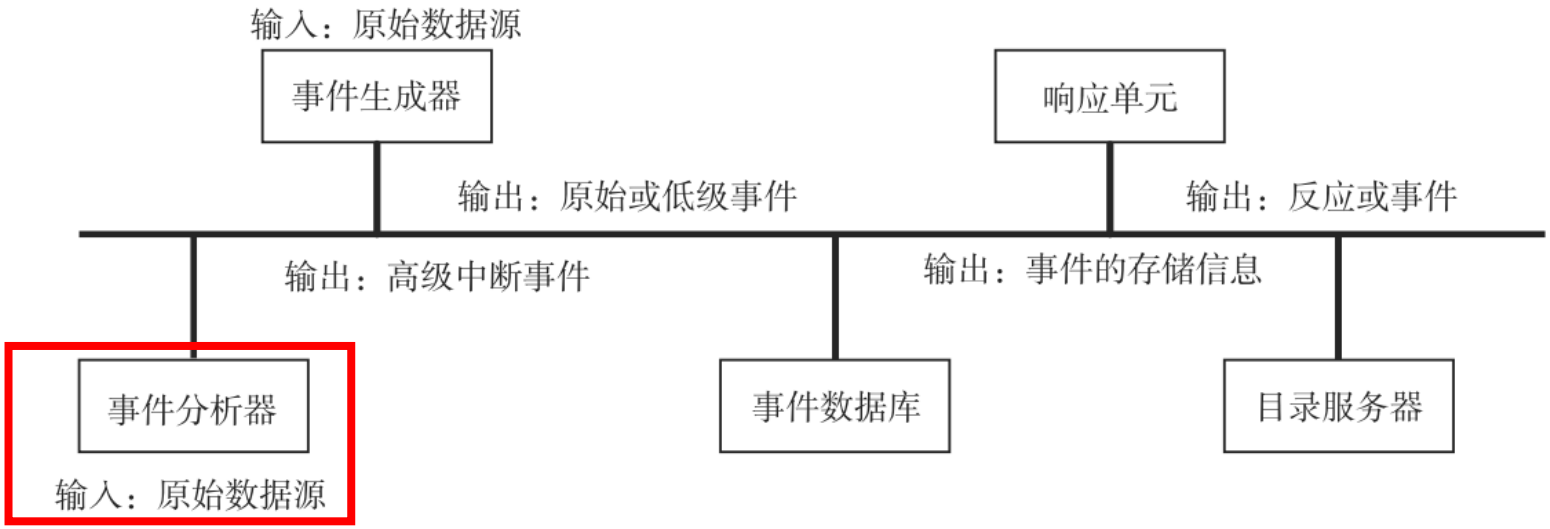
(1)事件生成器



(1)事件生成器：它是采集和过滤事件数据的程序或模块。

- 负责收集原始数据，对数据流、日志文件等进行追踪，然后将搜集到的原始数据转换成事件，并向系统的其他部分提供此事件。

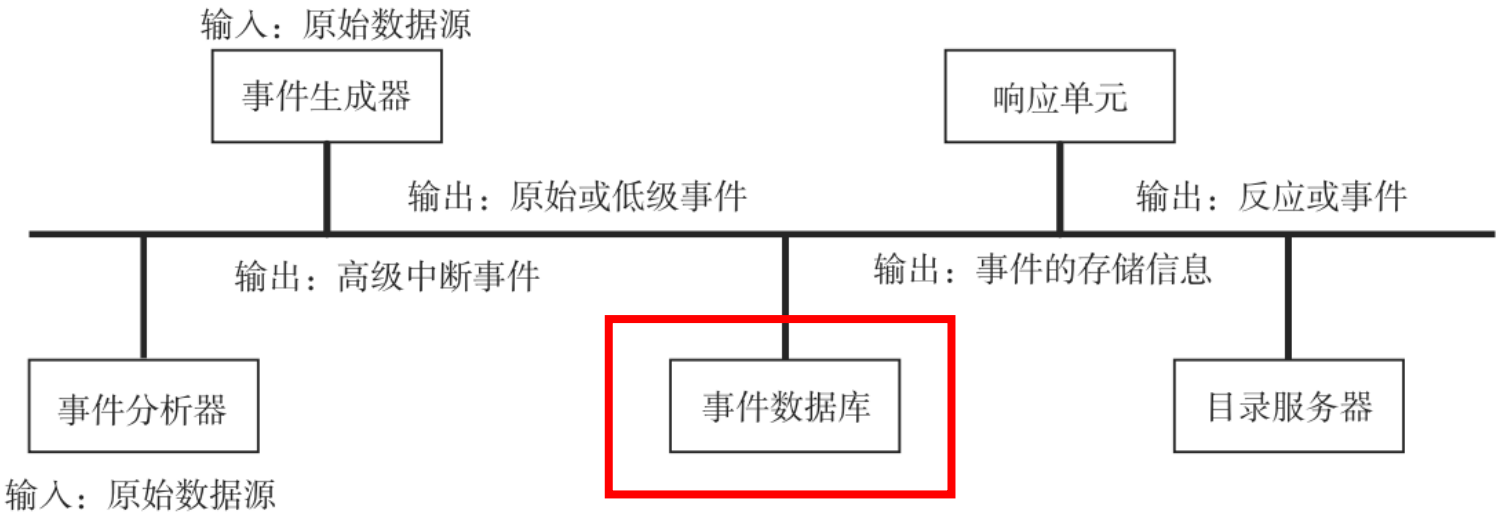
(2)事件分析器



(2)事件分析器：事件分析器是分析事件数据和任何CIDF组件传送给它的各种数据。

- 例如将输入的事件进行分析，检测是否有入侵的迹象，或描述对入侵响应的响应数据，都可以发送给事件分析器进行分析。

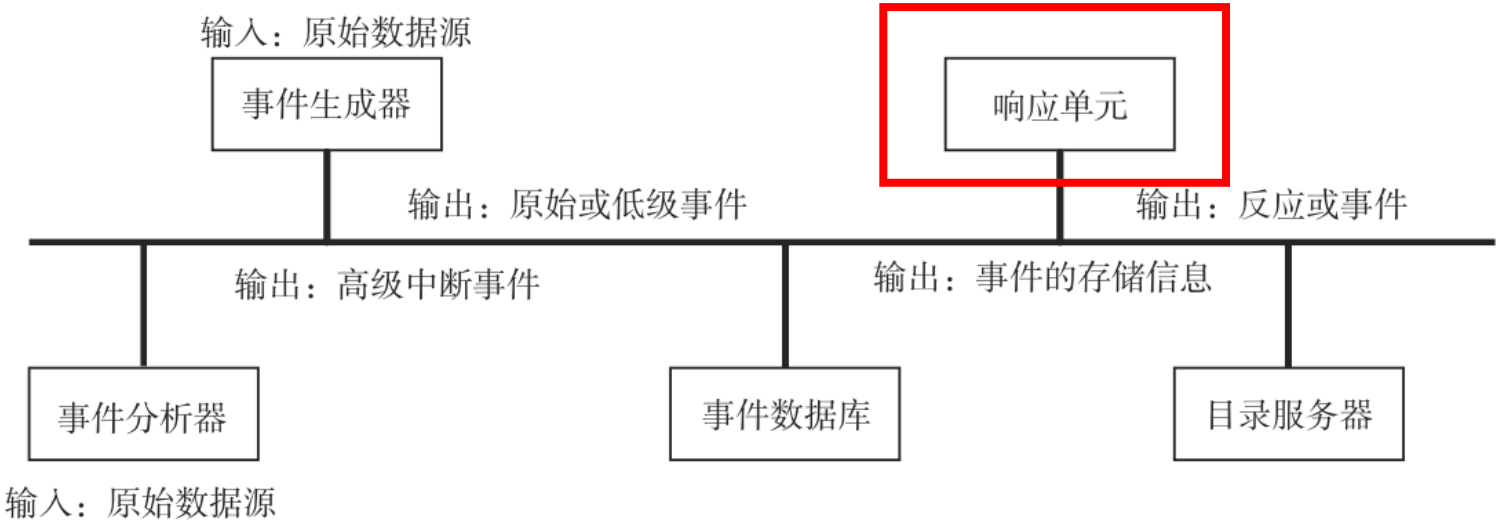
(3)事件数据库



(3)事件数据库：负责存放各种原始数据或已加工过的数据。

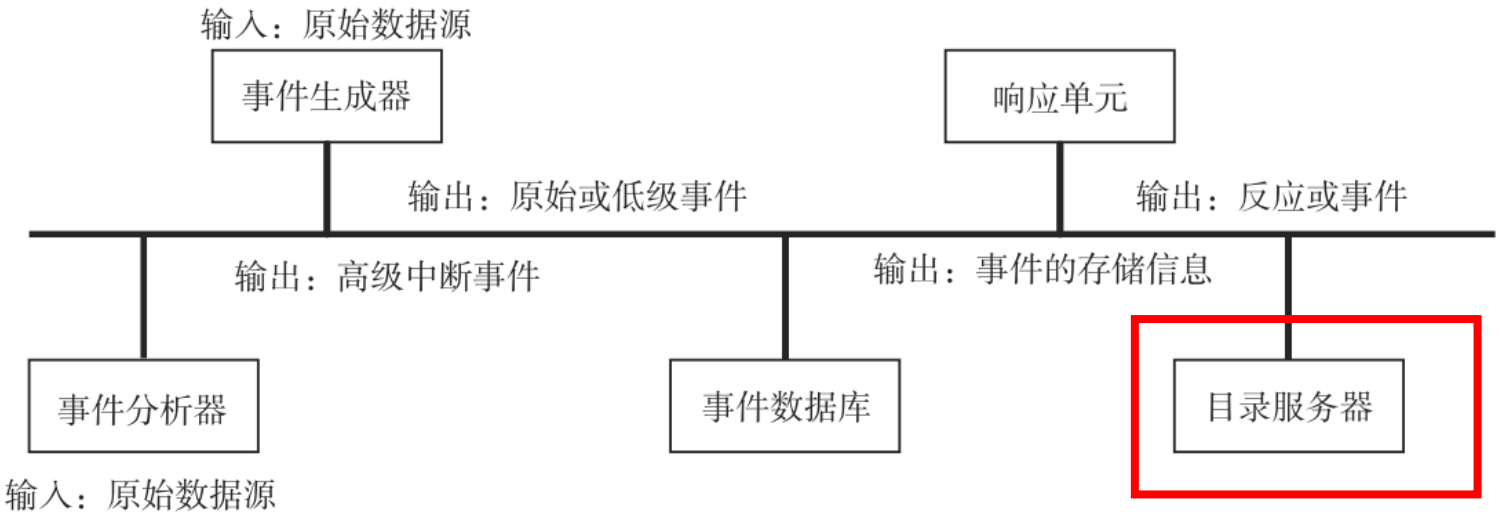
- 它从事件生成器或事件分析器接收数据并进行保存，它可以是复杂的数据库，也可以是简单的文本。

(4)响应单元



(4)响应单元：是针对分析组件所产生的分析结果，根据响应策略采取相应的行为，发出命令响应攻击。

(5)目录服务器



(5)目录服务器：目录服务器用于各组件定位其他组件，以及控制其他组件传递的数据并认证其他组件的使用，以防止入侵检测系统本身受到攻击。

- 目录服务器组件可以管理和发布密钥，提供组件信息和用户组件的功能接口。

入侵检测系统的主要功能

(1)监测并分析用户和系统的活动。

(2)核查系统配置与漏洞。

(3)识别已知的攻击行为并报警。

(4)统计并分析异常行为。

(5)对操作系统进行日志管理，并识别违反安全策略的用户活动。

8.2.2入侵检测系统分类

1. 基于检测对象的分类

1)基于主机的入侵检测系统

- (host-based IDS，**HIDS**)开始并兴盛于20世纪80年代，其检测对象是**主机系统和本地用户**。
- 检测原理是在每一个需要保护的主机上运行一个代理程序，根据主机的审计数据和系统的日志发现可疑事件，检测系统可以运行在被检测的主机上，从而实现监控。

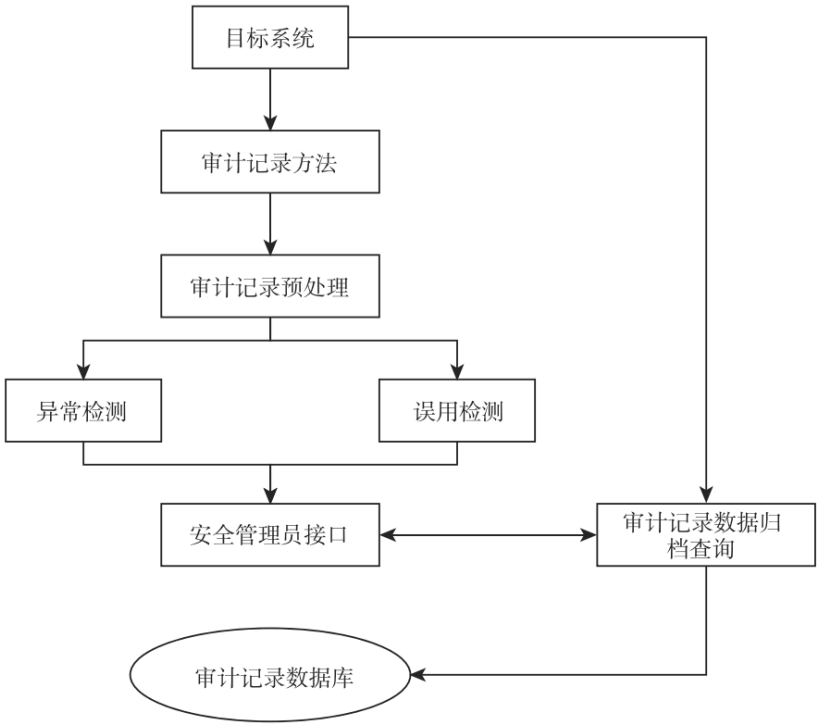


图8-5 基于主机的入侵检测系统

基于主机的入侵检测系统的优缺点

(1)能确定攻击是否成功。基于主机的IDS使用含有已发生的事件信息，根据该事件信息能准确判断攻击是否成功，因而基于主机的IDS误报率较小。

(2)监控更为细致。基于主机的IDS监控目标明确。它可以很容易地监控一些在网络中无法发现的活动，如敏感文件、目录、程序或端口的存取。

(3)配置灵活。用户可根据自己的实际情况对主机进行个性化的配置。

(4)适应于加密和交换的环境。由于基于主机的IDS是安装在监控主机上的，故不会受加密和交换的影响。

(5)对网络流量不敏感。基于主机的IDS不会因为网络流量的增加而放弃对网络的监控。

HIDS的缺点：

(1)由于它通常作为用户进程运行，依赖于操作系统底层的支持，与系统的体系结构有关，所以它无法了解发生在下层协议的入侵活动。

(2)由于HIDS要驻留在受控主机中，对整个网络的拓扑结构认识有限，根本监测不到网络上的情况，只能为单机提供安全防护。

(3)基于主机的入侵检测系统必须配置在每一台需要保护的主机上，占用一定的主机资源，使服务器产生额外的开销。

(4)缺乏对平台的支持，可移植性差。

2)基于网络的入侵检测系统

- **基于网络的入侵检测系统(network-based IDS，NIDS)**通过监听网络中的**分组数据包**来获得分析攻击的数据源，分析可疑现象。
- 它通常使用报文的模式匹配或模式匹配序列来定义规则，检测时将监听到的报文与规则进行比较，根据比较的结果来判断是否有非正常的网络行为。通常情况下是利用混杂模式的网卡来捕获网络数据包。

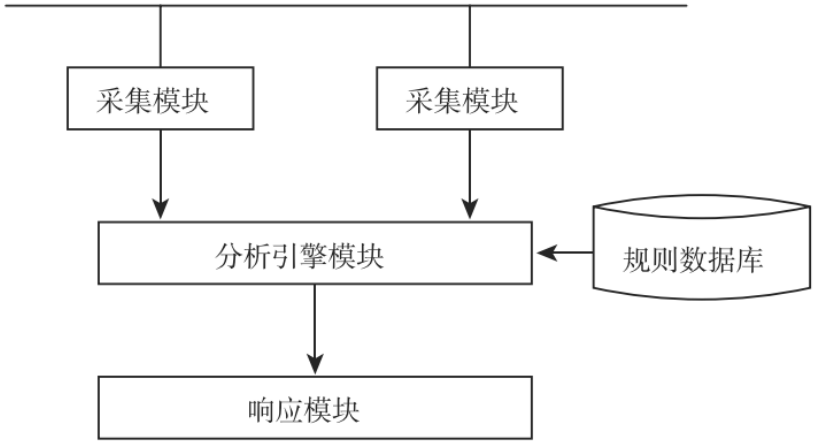


图8-6 基于网络的入侵检测系统

基于网络的入侵检测系统的优缺点

(1)监测速度快。基于网络的IDS能在微秒或秒级发现问题。

(2)能够检测到HIDS无法检测的入侵。

(3)入侵对象不容易销毁证据。被截取的数据不仅包括入侵的方法，还包括可以定位入侵对象的信息。

(4)检测和响应的实时性强。一旦发现入侵行为就立即终止攻击。

(5)与操作系统无关性。由于基于网络的IDS是配置在网络上对资源进行安全监控，因此，它具有与操作系统无关的特性。

缺点：

(1) NIDS无法采集高速网络中的所有数据包。

(2)缺乏终端系统对待定数据包的处理方法等信息，使得从原始的数据包中重构应用层信息很困难，因此，NIDS难以检测发生在应用层的攻击。

(3) NIDS对以加密传输方式进行的入侵无能为力。

(4) NIDS只检查它直接连接网段的通信，并且精确度较差，在交换式网络环境下难以配置，防入侵欺骗的能力较差。

3)混合式入侵检测系统

- NIDS和HIDS都有不足之处，单纯使用一类系统会造成主动防御体系的不全面。由于两者各有其自身的优点和缺陷，有些能力是不能互相替代的，而且两者的优缺点是互补的，如果将这两类系统结合起来部署在网络内，则会构成一套完整立体的主动防御体系。
- **综合了网络和主机两种结构特点的IDS**，既可以发现网络中的攻击信息，也可以从系统日志中发现异常状况，这就是混合式入侵检测系统。它主要综合了基于网络和基于主机入侵检测系统两种结构的特点，既可以利用来自网络的数据，也可以利用来自计算机主机的数据信息。
- 采用混合分布式入侵检测系统可以联合使用基于主机和基于网络这两种不同的检测方式，有很好的操作性，能够达到更好的检测效果。

2．基于检测技术的分类

- 根据入侵检测技术，可分为异常检测和误用检测两类。

1)异常检测

- 异常检测也称之为**基于行为的检测**，来源于这样的思想：任何一种入侵行为都能由于其偏离正常或者所期望的系统和用户的活动规律而被检测出来。
- 异常检测通常首先从用户的正常或者合法活动模式中收集一组数据，这一组数据集被视为“正常调用”。若用户偏离了正常调用模式，则会认为是入侵而报警，即任何不符合以往活动规律的行为都将被视为入侵行为。

异常检测的模型

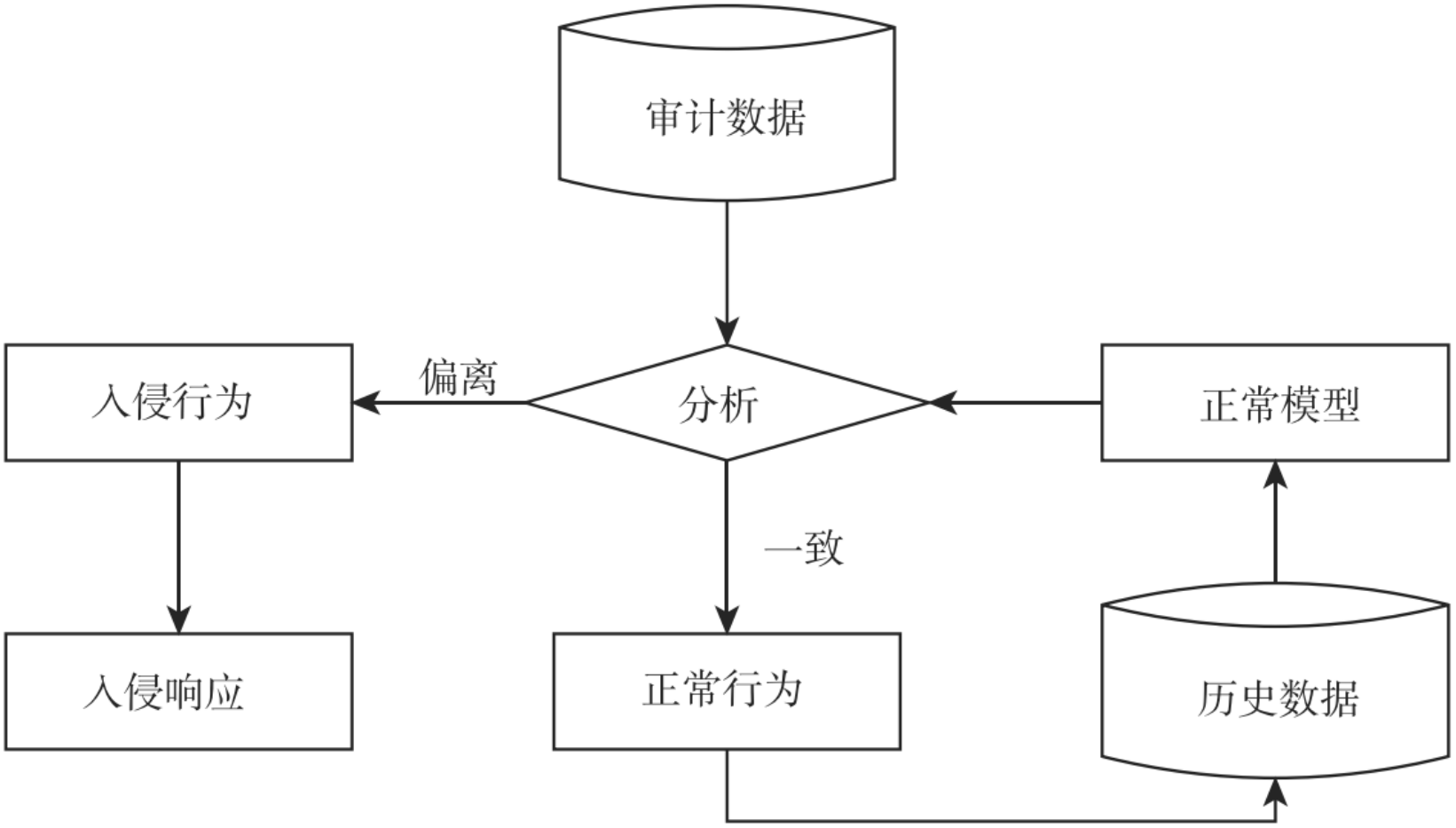


图8-7 异常检测的模型

优缺点

- 异常检测方法的优点是：
- 第一，正常使用行为是被准确定义的，检测的准确率高；
- 第二，能够发现任何企图发掘、试探系统最新和未知漏洞的行为，同时在某种程度上，它较少依赖于特定的操作系统环境。

- 异常检测的缺点是：第一，必须枚举所有的正常使用规则，否则会导致有些正常使用的行为会被误认为是入侵行为，即有误报产生；
- 第二，在检测时，某个行为是否属于正常，通常不能做简单的匹配，而要利用统计方法进行模糊匹配，在实现上有一定的难度。

2)误用检测

- 误用检测又称之为**特征检测**，建立在对过去各种已知网络入侵方法和系统缺陷知识的积累之上。入侵检测系统中存储着一系列已知的入侵行为描述，当某个系统的调用与一个已知的入侵行为相匹配时，则认为是入侵行为。
- 误用检测是直接对入侵行为进行特征化描述，其**主要优点**有：依据具体特征库进行判断，检测过程简单，检测效率高，针对已知入侵的检测精度高，可以依据检测到的不同攻击类型采取不同的措施。**缺点**有：对具体系统依赖性太强，可移植性较差，维护工作量大，同时无法检测到未知的攻击。

误用检测的模型

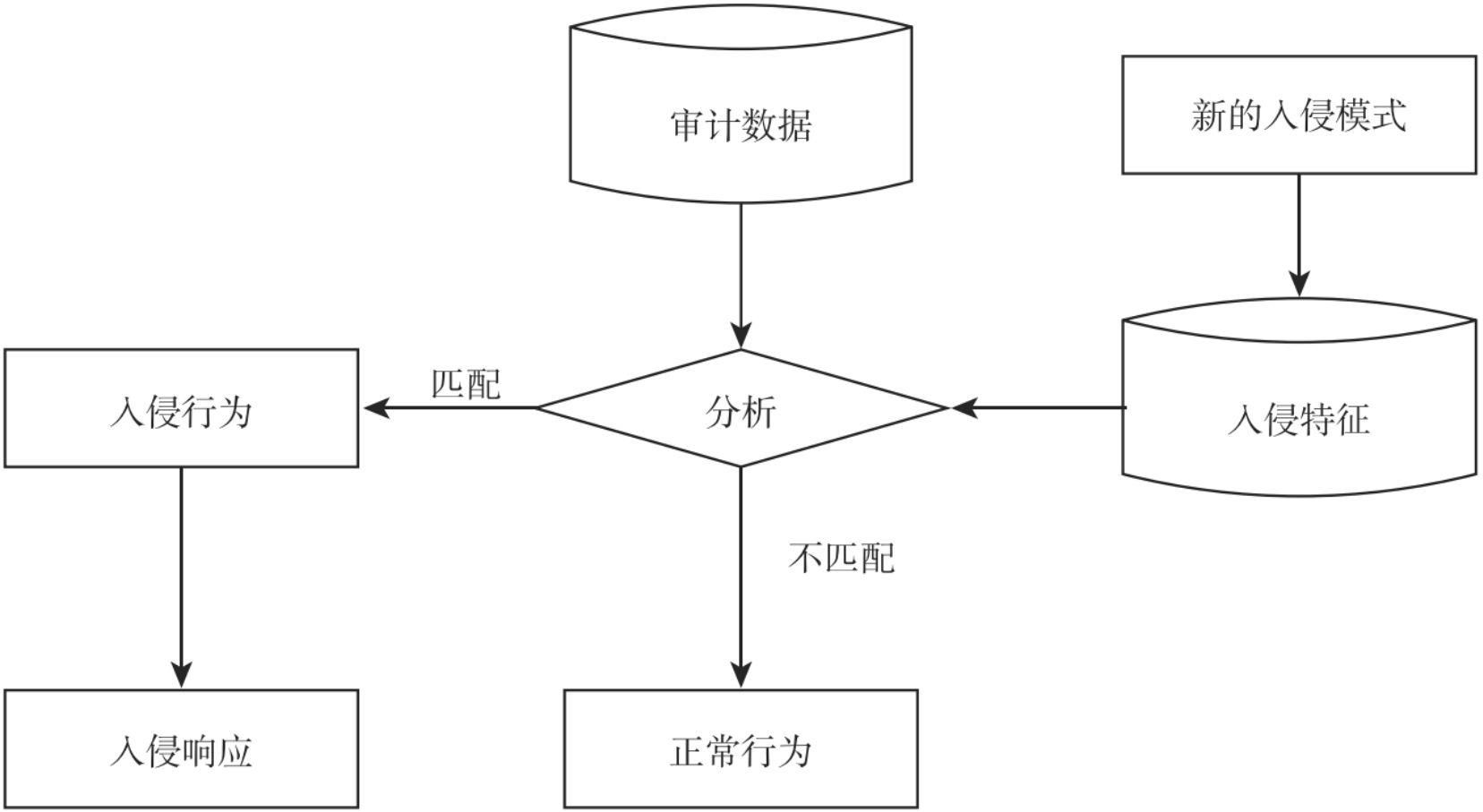


图8-8 误用检测的模型

3．基于工作方式的分类

- 根据工作方式，可分为离线检测系统和在线检测系统。

1)离线检测系统

- 离线检测系统是**非实时工作**的系统，它在事后分析审计事件，从中检查入侵活动。事后入侵检测由网络管理人员进行，他们具有网络安全的专业知识，根据计算机系统对用户操作所做的历史审计记录判断是否存在入侵行为，如果有就断开连接，并记录入侵证据和进行数据恢复。
- 事后入侵检测是管理员定期或不定期进行的，不具有实时性。

2)在线检测系统

- 在线检测系统是**实时联机的检测**系统，它包含对实时网络数据包分析和实时主机审计分析。
- 实时入侵检测在网络连接过程中进行，系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型等对用户当前的操作进行判断，一旦发现入侵迹象，立即断开入侵者与主机的连接，并搜集证据和实施数据恢复。这个检测过程是不断循环进行的。

8.2.3 分布式入侵检测

- 为应对复杂多变的大型分布式网络，分布式入侵检测系统(**distributed IDS，DIDS**)应运而生。它采用多个代理在网络各部分分别进行入侵检测，各检测单元协作完成检测任务，并还能在更高层次上进行结构扩展，以适应网络规模的扩大。通过网络入侵检测系统的共同合作，可获得更有效的防卫。
- **分布式入侵检测系统的各个模块分布在网络中不同的计算机设备上**。一般来说，**分布性主要体现在数据收集模块**上，如果网络环境比较复杂、数据量比较大，那么**数据分析模块**也会分布在网络的不同计算机设备上，通常是按照层次性的原则进行组织。分布式入侵检测系统根据各组件间的关系还可细分为**层次式DIDS和协作式DIDS**。

- 在**层次式DIDS**中，定义了若干个分等级的监测区域，每一个区域有一个专门负责分析数据的IDS，每一级IDS只负责所监测区域的数据分析，然后将结果传送给上一级IDS。层次式DIDS通过分层分析很好地解决了集中式IDS的不可扩展的问题，但同时也存在下列问题：当网络的拓扑结构改变时，区域分析结果的汇总机制也需要做相应的调整；一旦位于最高层的IDS受到攻击后，其他那些从网络多路发起的协同攻击就容易逃过检测，造成漏检。
- **协作式DIDS**将中央检测服务器的任务分配给若干个互相合作的基于主机的IDS，这些IDS不分等级，各司其职，负责监控本地主机的某些活动，所有的IDS并发执行并相互协作。协作式IDS的特点就在于它的各个节点都是平等的，一个局部IDS的失效不会导致整个系统的瘫痪，也不会导致协同攻击检测的失败。因而，系统的可扩展性、安全性都得到了显著的提高。但同时它的维护成本却很高，并且增加了所监控主机的工作负荷，如通信机制、审计开销、踪迹分析等。而且，主机之间的通信、审计以及审计数据分析机制的优劣直接影响了协作式入侵检测系统的效率。

典型的分布式入侵检测系统结构

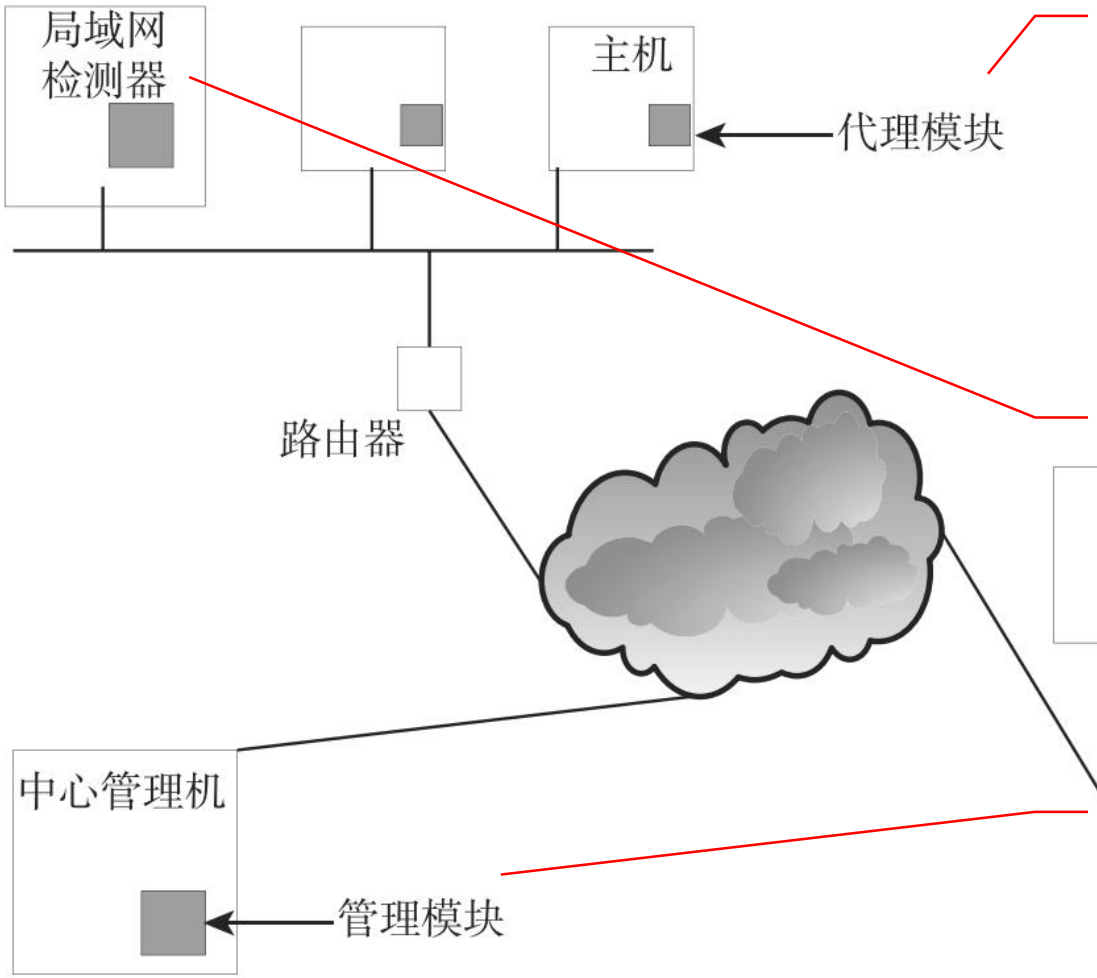


图8-9 分布式入侵检测系统的典型结

(1)**主机代理模块**：审计收集模块作为后台进程运行在监测系统上。它的作用是收集有关主机安全事件的数据，并将这些数据传至中心管理员。

(2)**局域网监视代理模块**：其运作方式与主机代理模块相同。但它还分析局域网的流量，将结果报告给中心管理员。

(3)**中心管理员模块**：接收局域网监视模块和主机代理模块送来的报告，分析报告，并对其进行综合处理用以判断是否存在入侵。

8.2.4 入侵检测技术发展趋势

入侵检测系统目前主要存在以下几个问题：

(1)高速网络下的误报率和漏报率。基于网络的入侵检测系统是通过截获网络上的数据包来进行分析和匹配，从而判断是否存在攻击行为。其匹配过程需要占用大量的时间和系统资源，如果检测速度落后于网络的传输速度，就会导致入侵检测系统漏掉其中部分数据包，从而导致误报和漏报。

(2)入侵检测产品和其他网络安全产品结合的问题。在大型的网络中，入侵检测系统如何与其他网络安全产品之间交换信息，共同协作来发现并阻止攻击，关系到整个系统的安全问题。目前的入侵检测系统尚不具备这方面的能力。

(3)入侵检测系统的功能相对单一。随着攻击手段的不断增加，入侵行为逐渐复杂化，而目前的大多数入侵检测系统只能对某一类型的攻击做出反应。比如，基于网络的入侵检测系统无法检测出本地的攻击；而基于主机的入侵检测系统同样无法检测出网络的攻击。

(4)入侵检测系统本身存在的问题。基于网络的入侵检测系统对加密的数据流以及交换网络下的数据流不能进行检测。另外，入侵检测系统缺少自我保护机制，本身的构件容易受到攻击。

入侵检测的研究重点

- **(1)分布式入侵检测**。分布式入侵检测系统主要面向大型网络和异构系统，它采用分布式结构，可以对多种信息进行协同处理和分析，与单一架构的入侵检测系统相比具有更强的检测能力。
- **(2)智能入侵检测**。智能入侵检测方法在现阶段主要包括机器学习、神经网络、数据挖掘等方法。国内外已经开展了各种智能技术（方法）在入侵检测中的应用研究，研究的主要目的是降低检测系统的虚警和漏报概率，提高系统的自学习能力和实时性。从目前的一些研究成果看，基于智能技术的入侵检测方法具有许多传统检测方法所没有的优点，有良好的发展潜力。

入侵检测的研究重点

- **(3)高效的模式匹配算法**。对目前广泛应用的基于误用检测方法的入侵检测系统，模式匹配算法在很大程度上影响着系统的检测速度。随着入侵方式的多样化和复杂化，检测系统存储的入侵模式越来越多，对入侵模式定义的复杂程度也越来越高，因而迫切需要研究和使用高效的模式匹配算法。
- **(4)基于协议分析的入侵检测**。对网络型入侵检测系统而言，如果其检测速度跟不上网络数据的传输速度，检测系统就会漏掉其中的部分数据包，从而导致漏报而影响系统的准确性和有效性。大部分现有的网络型入侵检测系统只有几十兆的检测速度，而百兆甚至千兆网络的大量应用，对系统的检测速度提出了更高的要求。基于协议分析的入侵检测所需的计算量相对较少，可以利用网络协议的高度规则性快速探测攻击的存在，即使在高负载的网络上也不容易产生丢包现象。

入侵检测的研究重点

- **(5)与操作系统的结合**。目前入侵检测系统的普遍缺陷是与操作系统结合不紧密，这会导致很多不便。例如，很难确定黑客攻击系统到了什么程度，不知道黑客拥有了系统哪个级别的权限，黑客是否控制了一个系统等。与操作系统的紧密结合可以提升入侵检测系统对攻击，特别是比较隐蔽的、新出现的攻击的检测能力。
- **(6)入侵检测系统之间以及入侵检测系统和其他安全组件之间的互动性研究**。在大型网络中，网络的不同部分可能使用了多种入侵检测系统，甚至还有防火墙、漏洞扫描等其他类别的安全设备，这些入侵检测系统之间以及IDS和其他安全组件之间的互动，有利于共同协作，减少误报，并更有效地发现攻击、做出响应、阻止攻击。

入侵检测的研究重点

- **(7)入侵检测系统自身安全性的研究**。入侵检测系统是个安全产品，自身安全极为重要。因此，越来越多的入侵检测产品采用强身份认证、黑洞式接入、限制用户权限等方法，免除自身安全问题。

- **(8)入侵检测系统的标准化**。到目前为止，尚没有一个关于入侵检测系统的正式的国际标准出现，这种情况不利于入侵检测系统的应用与发展。国际上有一些组织正在做这方面的研究工作。入侵检测系统的标准化工作应该主要包括：大型分布式入侵检测系统的体系结构、入侵特征的描述（数据格式）、入侵检测系统内部的通信协议和数据交换协议、各个部件间的互动协议和接口标准等。

8.3.1 蜜罐的概念

- 蜜罐是防御方为了改变网络攻防博弈不对称局面而引入的一种主动防御技术，本质上是一种没有任何产品价值的安全资源，其价值体现在被探测、攻击或者攻陷的时候。
- 蜜罐技术**本质上**是一种**对攻击方进行欺骗**的技术，通过布置一些作为诱饵的主机、网络服务或者信息（蜜罐），诱使攻击方对它们实施攻击，从而可以对攻击行为进行捕获和分析，了解攻击方所使用的工具与方法，推测攻击意图和动机，能够让防御方清晰地了解他们所面对的安全威胁，并通过技术和管理手段来增强实际系统的安全防护能力。

- **蜜网(honeynet)又可称为诱捕网络**，是由若干个能收集和交换信息的蜜罐构成的一个网络体系架构。与蜜罐不同的是，它融入了数据捕获、数据分析和数据控制等元素，使得安全研究人员能够方便地追踪入侵到各个蜜罐中的攻击者并对他们的攻击行为进行控制和分析，了解网络系统的安全威胁。蜜网是为了解决早期蜜罐交互程度低、捕获攻击信息有限且类型单一、较容易被攻击者识别等问题。
- 从20世纪80年代末蜜罐技术在网络安全管理实践活动中诞生以来，得到了长足发展与广泛应用。针对不同类型的网络安全威胁形态，出现了丰富多样的蜜罐软件工具。为适应更大范围的安全威胁监测的需求，逐步从中发展出**蜜网、分布式蜜罐、分布式蜜网和蜜场(honeyfarm)**等技术概念。在安全威胁监测研究与实际网络安全管理实践中，大量应用于网络入侵、恶意代码检测、恶意代码样本捕获、攻击特征提取、取证分析和僵尸网络追踪等问题。

8.3.2 蜜罐技术的分类

1. 按系统功能分类

- 根据系统的功能，蜜罐可以分为产品型蜜罐和研究型蜜罐两类。

2. 按系统交互活动级别分类

- 根据系统允许与黑客交互活动的级别，蜜罐可分为低交互蜜罐与高交互蜜罐。

3. 按服务实现方式分类

- 为了欺骗攻击者，蜜罐需要提供与真实的主机相似的操作系统和服务。根据服务实现方式将蜜罐系统分为真实蜜罐和虚拟蜜罐。

4. 按服务提供方式分类

- 根据服务提供方式将蜜罐分为服务端蜜罐和客户端蜜罐。

8.3.3 蜜罐技术关键机制

- 核心机制是蜜罐技术达成对攻击方进行诱骗与监测的必需组件。
- **(1)欺骗环境构建机制**。构造出对攻击方具有诱骗性的安全资源，吸引攻击方对其进行探测、攻击与利用。
- **(2)威胁数据捕获机制**。对诱捕到的安全威胁进行日志记录，尽可能全面地获取各种类型的安全威胁原始数据，如网络连接记录、原始数据包、系统行为数据、恶意代码样本等。
- **(3)威胁数据分析机制**。在捕获的安全威胁原始数据的基础上，分析追溯安全威胁的类型与根源，并对安全威胁态势进行感知。

辅助机制

- 辅助机制则是对蜜罐技术其他扩展需求的归纳，主要包括以下方面：
- **(1)安全风险控制机制**。确保部署的蜜罐系统不被攻击方恶意利用去攻击互联网和业务网络，让部署方规避道德甚至法律风险。
- **(2)配置与管理机制**。使得部署方可以便捷地对蜜罐系统进行定制与维护。
- **(3)反蜜罐技术对抗机制**。目标是提升蜜罐系统的诱骗效果，避免被具有较高技术水平的攻击方利用反蜜罐技术而识别。

8.3.4 蜜罐部署结构

1.蜜网

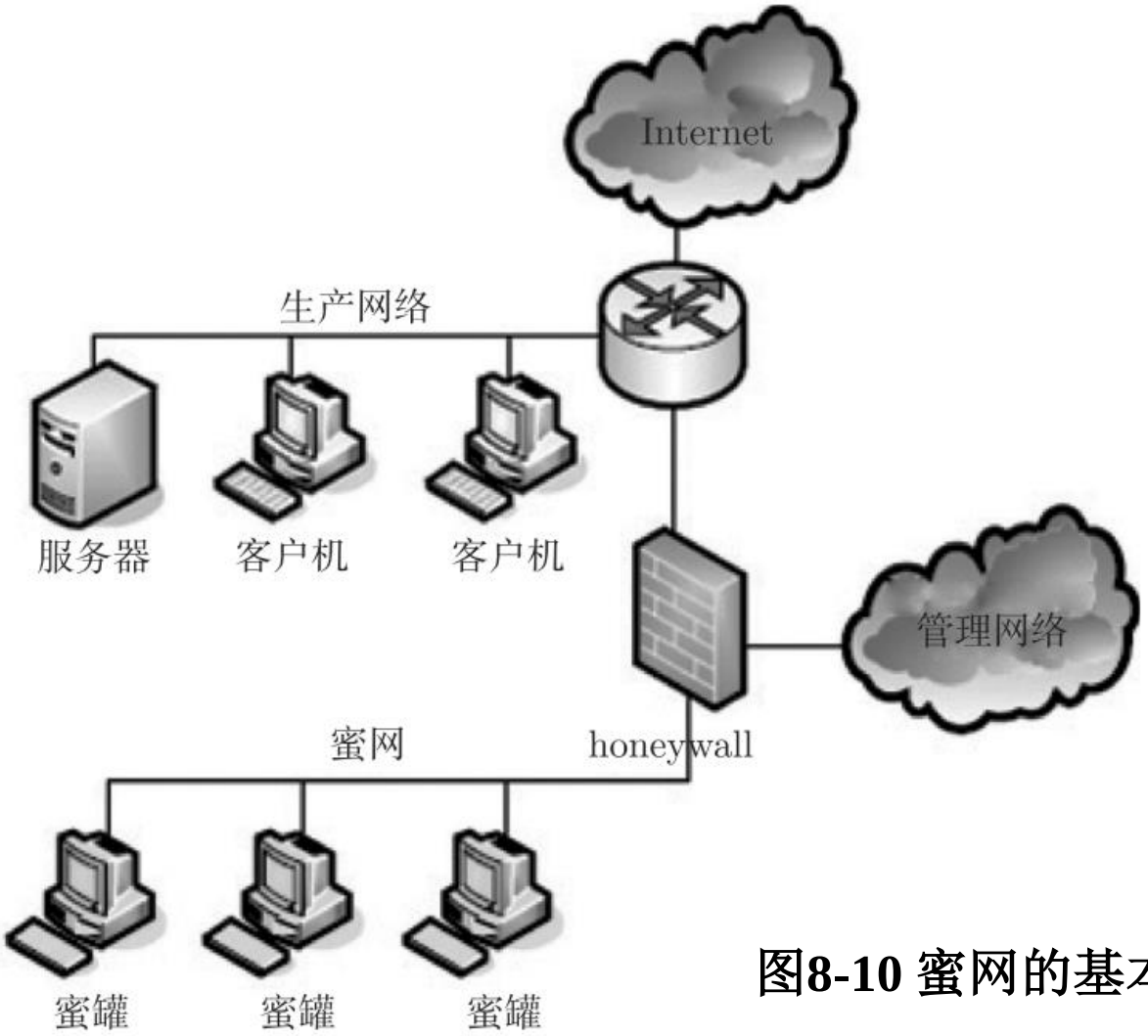


图8-10 蜜网的基本结构

2. 蜜场

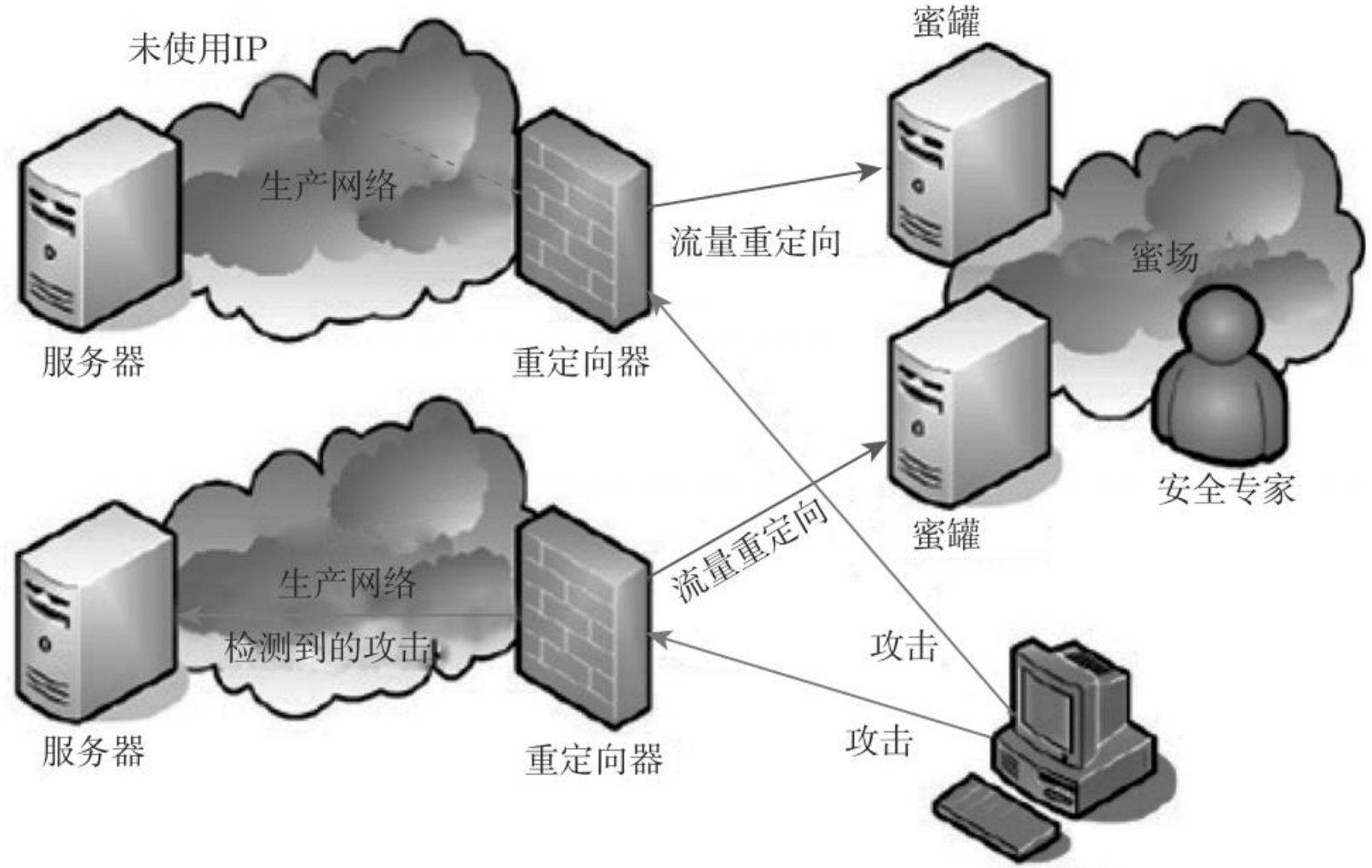


图8-11 蜜场技术概念图示

8.4.1 应急响应的概念

- 在常见的安全保障模型中，有一个很著名的**PDRR模型**，分别代表信息系统安全保障的主要操作环节：“防护”(protection)，“检测”(detection)，“响应”(response)和“恢复”(recovery)，**“响应”**是其中一个非常重要的环节。

1.为什么需要应急响应?

- 网络与信息系统面临诸多威胁，安全防护技术不能保证系统100%的安全，为此，需要做好出现安全问题之后的应急响应措施。
- 由于安全事件的突发性、复杂性与专业性，在组织体系以及协调机制方面都存在很多不和谐、不规范的问题。为了有备无患，需要建立计算机安全事件的快速响应机制，“计算机安全应急响应组(CSIRT)”便应运而生。

2．什么是应急响应

- **应急响应**就是**对国内外发生的有关计算机安全的事件进行实时响应与分析，提出解决方案和应急对策，保证计算机信息系统和网络免遭破坏**。
- 计算机安全应急响应组(**Computer Security Incident Response Team，CSIRT**)是一种服务组织，其职责就是接受、分析、响应有关计算机安全报告和活动，其服务对象通常为一个固定实体，例如，一个企业、政府或教育机构、一个地区或者国家、一个研究网络、一个付费的客户等。
- 计算机安全应急响应组可以是固定的或临时的。前者把履行应急响应作为主要工作，后者在需要时召集起来以响应一个计算机安全事件。有时**响应(response)**这个词也用**处理(handling)**来代替。

- 每一个CSIRT必须明确定义哪些事件是他们认为的计算机安全事件，通常定义为任何真实的或者可疑的，与计算机系统或计算机网络的安全相关的敌对事件，或者任何违反明显的或者隐含的安全策略的行为。这些行为指的是潜在地威胁计算机系统安全的网络或者主机的活动，可能包括以下方面：

(1)试图（不管成功与否）获得对系统或其数据的未授权访问。

(2)意外的破坏或者拒绝服务。

(3)未授权地使用系统处理或者存储数据。

(4)在所有者不知情、未指示或不同意情况下，改变系统硬件、固件和软件特征。

- 从广义上说，由于全世界的CSIRT服务于不同的对象，所以CSIRT以各种不同方式存在，其类型包括以下几种：

(1)内部CSIRT：为其所在的组织或机构提供应急响应服务。

(2)国家CSIRT：为其所在的国家提供应急响应服务，例如，中国计算机网络应急技术处理协调中心CNCERT。

(3)协调中心CC(coordination centers)：协调和推动各种不同的CSIRT之间的应急响应工作。

(4)分析中心AC(analysis centers)：专注于综合各种来源的数据以决定应急响应的趋势和类型，其提供的信息用来帮助预报未来的活动或者提供某些行为的早期报警。

(5)卖方团队(vendor teams)：处理他们自己的软件、硬件产品的漏洞报告，采用开发补丁、进行补救或提出缓解的办法。

(6)应急响应提供商(incident response providers)：为其他机构提供付费的应急处理服务。

8.4.2 应急响应策略

- 应急响应策略(CSIRT policies)是指导CSIRT正确、有效运作的主要原则。
- 按照策略的作用范围，一般可以把策略分为以下几种：

(1)全局策略，人员培训策略、道德规范策略、运行评价策略等。

(2)服务特定策略，反病毒策略、电子邮件策略、口令保护策略、远程访问策略、风险评估策略、服务器安全策略、路由器安全策略、VPN安全策略、无线通信策略、信息保密策略、审计漏洞扫描策略等。

(3)基础策略，操作代码策略、信息分类策略、信息披露策略、媒体策略、安全策略、人为过失策略等。

8.4.3 应急事件处理流程

- 目前各国的CSIRT主要提供以下几种基本服务。

1)安全事件的热线响应，包括：

- (1)检查入侵来源。完成入侵的取证工作，用于将来的法律诉讼。
- (2)恢复系统正常工作。
- (3)事故分析。避免类似安全事件再次发生。
- (4)发布安全警报、安全公告、安全建议。只有出现严重的安全问题时，CSIRT才发布安全警报，一般的安全问题则以安全公告的形式发布。
- (5)咨询。解决用户安全方面的求助。
- (6)风险评估。CSIRT定期对特定的网络和系统进行风险评估，以便及时地发现网络和系统存在的安全隐患。
- (7)安全教育培训。为企业或者机构进行安全意识、安全知识、安全技能等的培训。
- (8)协助其他组织成立自己的CSIRT，建立网络应急与救援队伍。

2) 应急响应的主要阶段

(1)准备阶段：在事件真正发生之前应该为事件响应做好准备，这一阶段十分重要。准备阶段的主要工作包括建立合理的防御／控制措施、建立适当的策略和程序、获得必要的资源和组建响应队伍等。

(2)检测阶段：检测阶段要做出初步的动作和响应。根据获得的初步材料和分析结果，估计事件的范围和发展势态，制定进一步的响应战略，并且保留可能用于司法程序的证据。

(3)抑制阶段：抑制的目的是限制攻击的范围。抑制措施十分重要，因为太多的安全事件可能迅速失控。典型的例子就是具有蠕虫特征的恶意代码的感染。可能的抑制策略一般包括：关闭所有的系统；从网络上断开相关系统；修改防火墙和路由器的过滤规则；封锁或删除被攻破的登录账号；提高系统或网络行为的监控级别；设置陷阱；关闭服务；反击攻击者的系统等。

(4)根除阶段：在事件被抑制之后，通过对有关恶意代码或行为的分析结果，找出事件根源并彻底清除。对于单机上的事件，可以根据对操作系统平台的具体检查，进行根除操作就可以了。但是，对于大规模爆发的带有蠕虫性质的恶意程序，要根除各个主机上的恶意代码，是十分艰巨的任务。很多案例表明，众多的用户并没有真正关注他们的主机是否已经遭受入侵，有的甚至持续相当长的时间，任由感染蠕虫的主机在网络中不断地搜索和攻击别的目标。造成这种现象的重要原因是，各网络之间缺乏有效的协调，或者是在一些商业网络中，网络管理员对接入到网络中的子网和用户没有足够的管理权限。

(5)恢复阶段：恢复阶段的目标是把所有被攻破的系统和网络设备彻底还原到它们正常的运行状态。恢复工作应该十分小心，避免出现误操作导致数据的丢失。另外，恢复工作中如果涉及机密数据，需要额外遵照机密系统的恢复要求。对承担不同恢复任务的单位，要有不同的担保。如果攻击者获得了超级用户的访问权，一次完整的恢复应该强制性地修改所有的口令。

(6)报告和追踪阶段：这是最后一个阶段，但却是绝对不能够忽略的重要阶段。这个阶段的目标是回顾并整理发生事件的各种相关信息，尽可能地把所有情况记录到文档中。这些记录的内容，不仅对有关部门的其他处理工作具有重要意义，而且对将来应急工作的开展也是非常重要的积累。

8.4.4 应急响应技术及工具

1)应急响应技术

✓应急响应的技术包括漏洞检测技术、监听技术、日志分析技术、路由控制技术、反向追踪技术等，有些技术是其独有的，有的技术与取证技术相同。

2)支持CSIRT日常运作的工具和技术

(1)执行CSIRT运作流程：事件跟踪和报告；事件分类和归档；通信。

(2)提供安全远程访问：远程网络访问；远程拨号访问；安全隧道。

(3)前置工具，支持审计/检测漏洞/预防事件：网络审计；主机审计；软件审计；网络监控；网络入侵检测。

3)支持事件调查

(1)证据收集工具：检查存储媒体；检查系统。

(2)证据调查工具：分析证据；校验同一性。

(3)证据处理工具。

(4)系统恢复。

第8章作业

- 作业

  2．为了提供安全，防火墙采用了哪些常用技术？

  6．一个典型的入侵检测系统包括哪些实体？分别具有什么功能？

  7．异常检测和误用检测的基本思想有哪些不同？

  9．蜜罐的功能是什么？

  11.什么是应急响应？其主要功能是什么？

- 实践（自己研究，不考核）
  - 熟悉Linux防火墙的配置命令iptables的使用。
  - 熟悉开源入侵检测snort（https://www.snort.org/）的使用。