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

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

- 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

- 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。

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。

(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。

(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

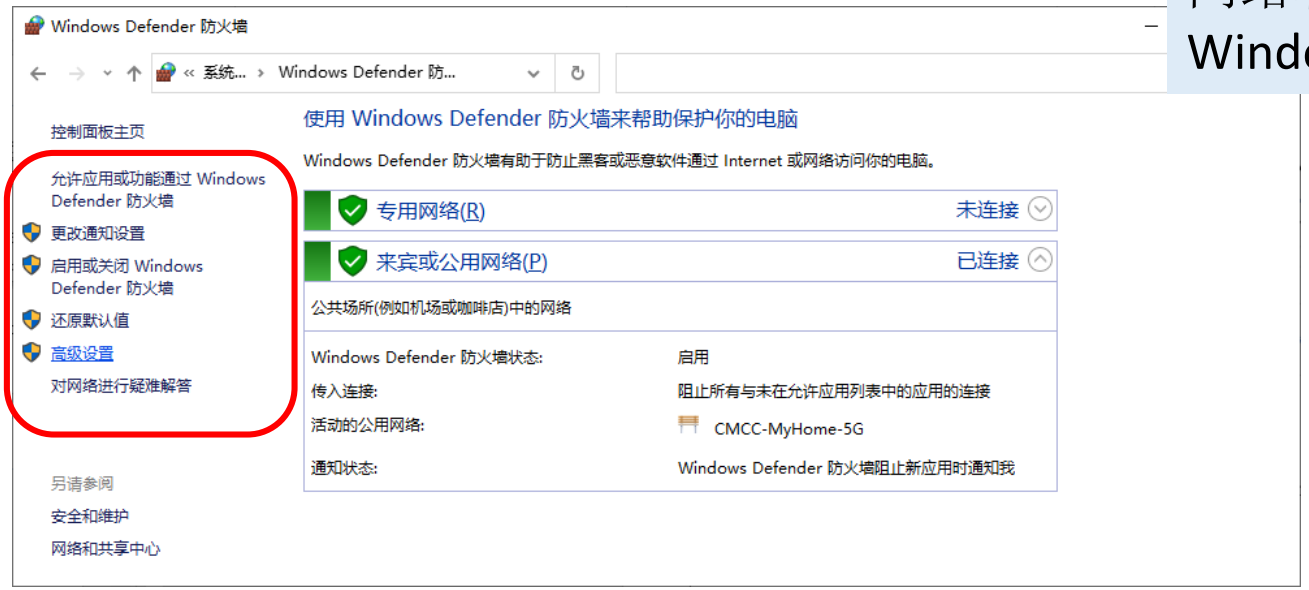
(1)防火墙不能防御不经由防火墙的攻击。

(2)防火墙不能防范来自内部的威胁。

(3)防火墙不能防止病毒感染的程序和文件进出内部网。

(4)防火墙不能防止数据驱动式的攻击。

防火墙实例：Windows10防火墙



控制面板→
网络和Internet→
网络和共享中心→
Windows Defender 防火墙

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。

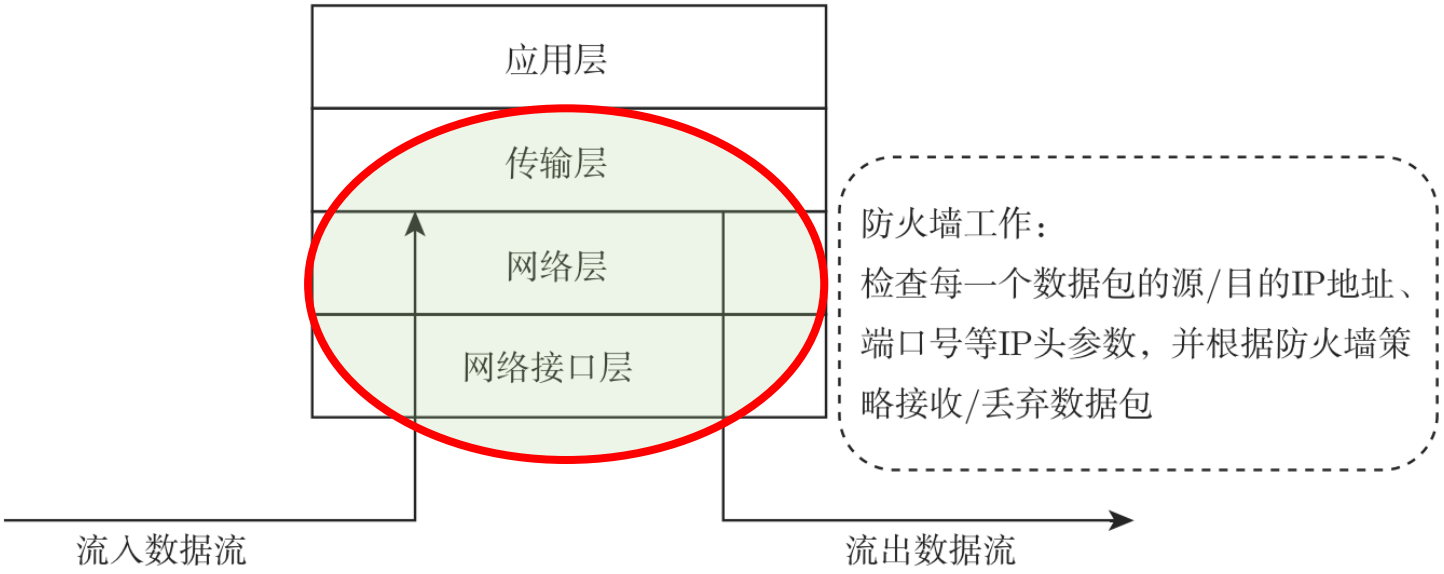


图8-1 包过滤防火墙

包过滤防火墙的具体实现

1. **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。
2. **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**。

(2)**包过滤用户对用户透明**。

(3)**过滤路由器速度快、效率高**。

(4)**技术通用、廉价、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**。

(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**。

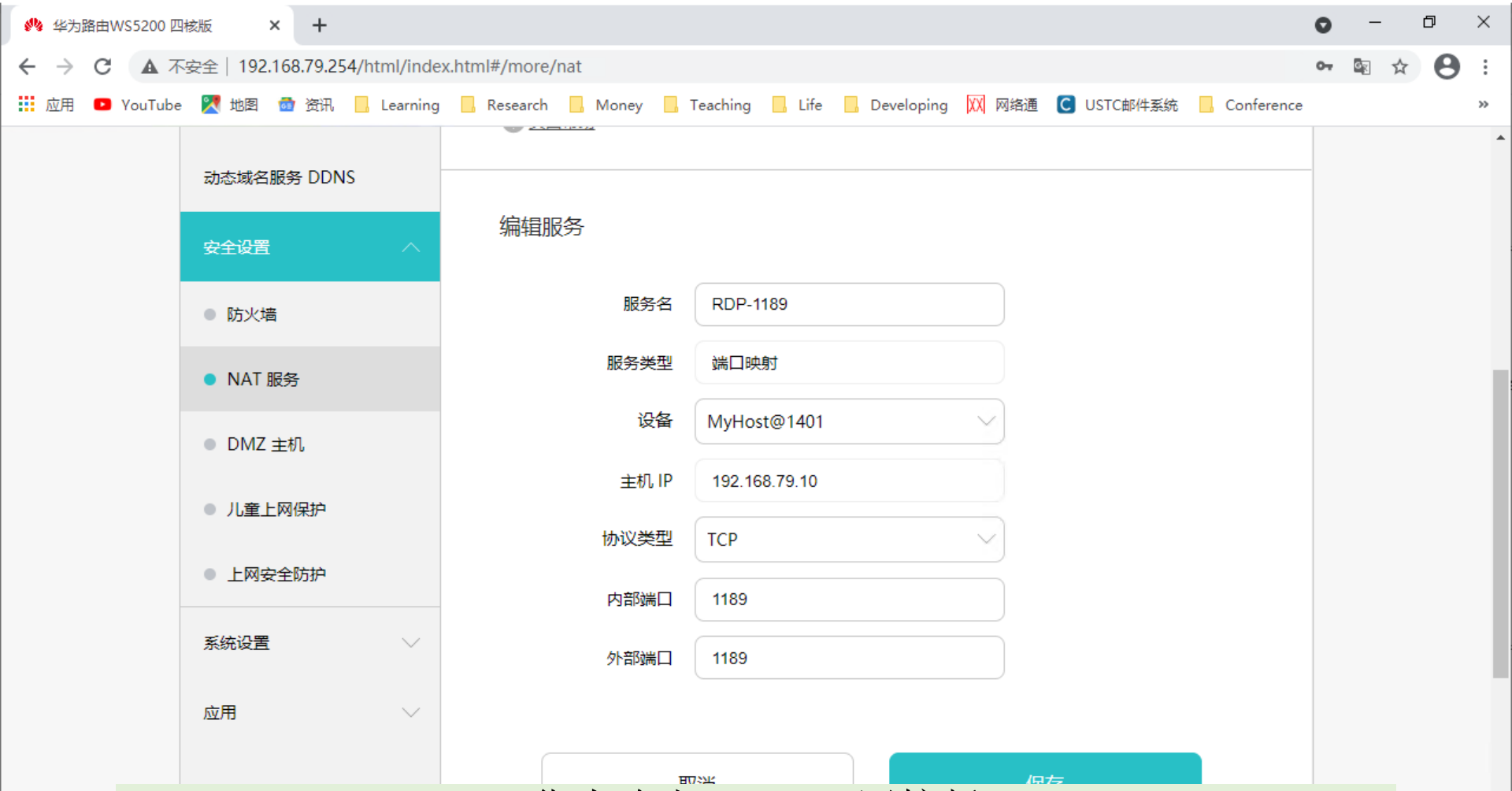
(3)**无法执行某些安全策略**。

(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。

包过滤防火墙的实例：无线路由器的防火墙



华为路由WS5200 四核版

- 端口开放的功能通过NAT提供，比如本实验室的主页：http://cybersecurity.ustc.edu.cn/

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

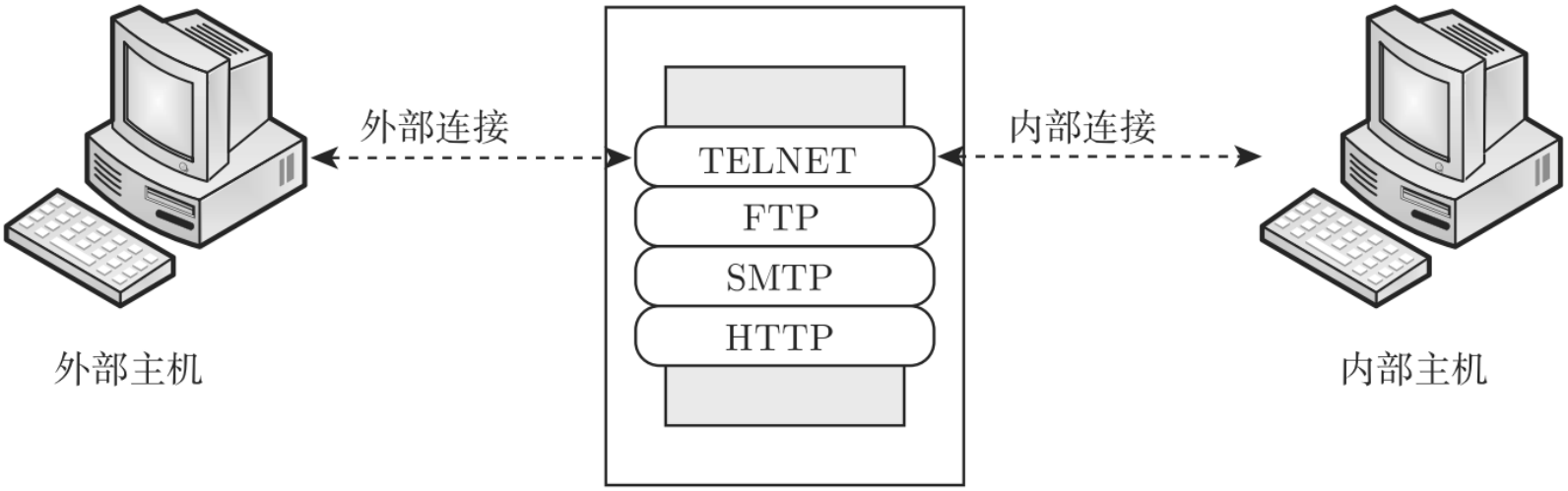


图8-2 代理服务技术

- 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。
- 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。

(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。

2)代理服务器的实现

(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。

实例：Web代理服务器

五大开源 Web 代理服务器横评

https://linux.cn/article-7119-1.html

Squid : http://www.squid-cache.org/

Privoxy : http://www.privoxy.org/

Varnish : https://www.varnish-cache.org/

Polipo : http://www.pps.univ-paris-diderot.fr/~jch/software/polipo/

Tinyproxy : https://banu.com/tinyproxy/

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。

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**。
- 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。
- 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。

8.1.5 防火墙的体系结构

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。

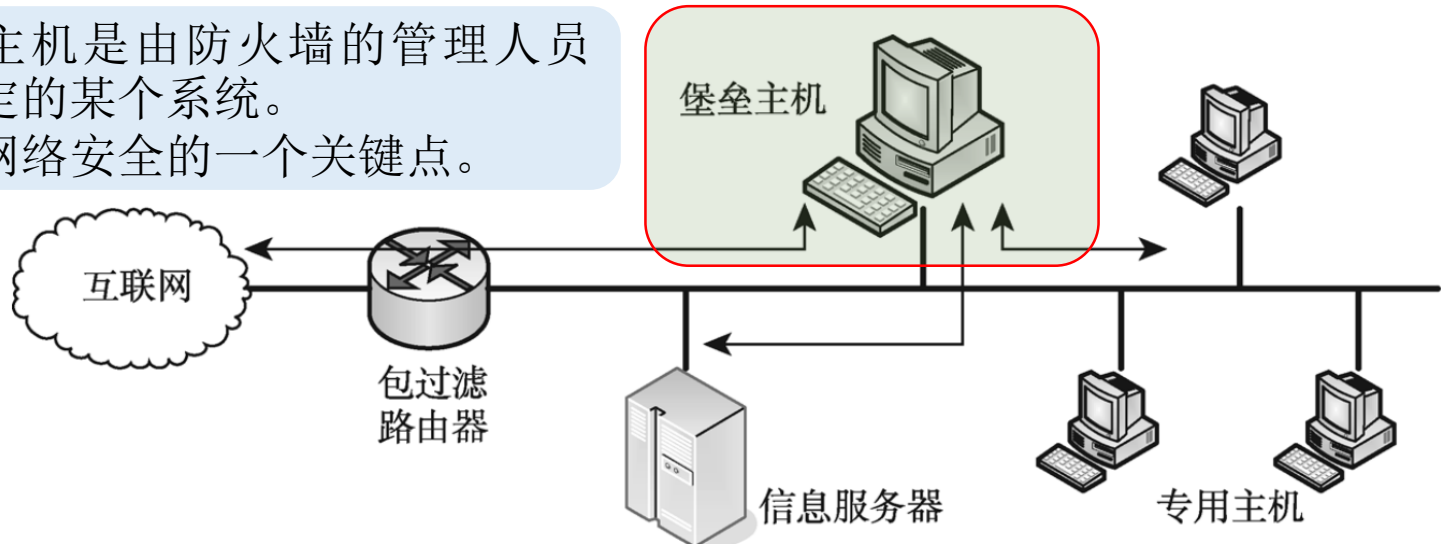


图8-3(a)

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）

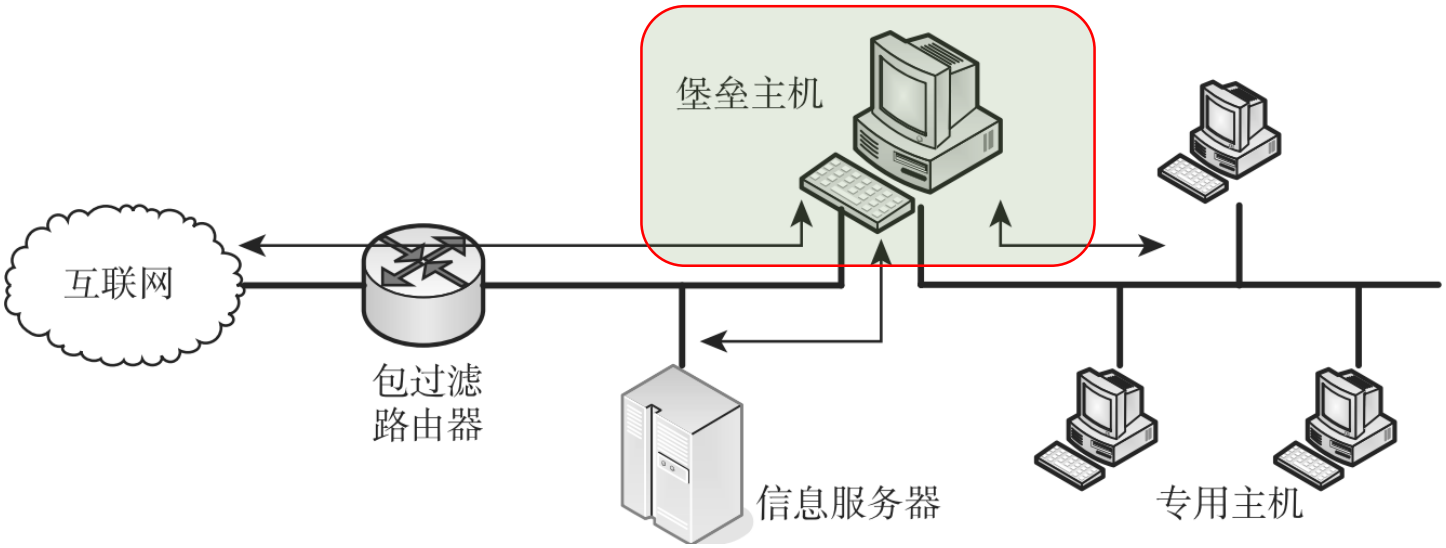
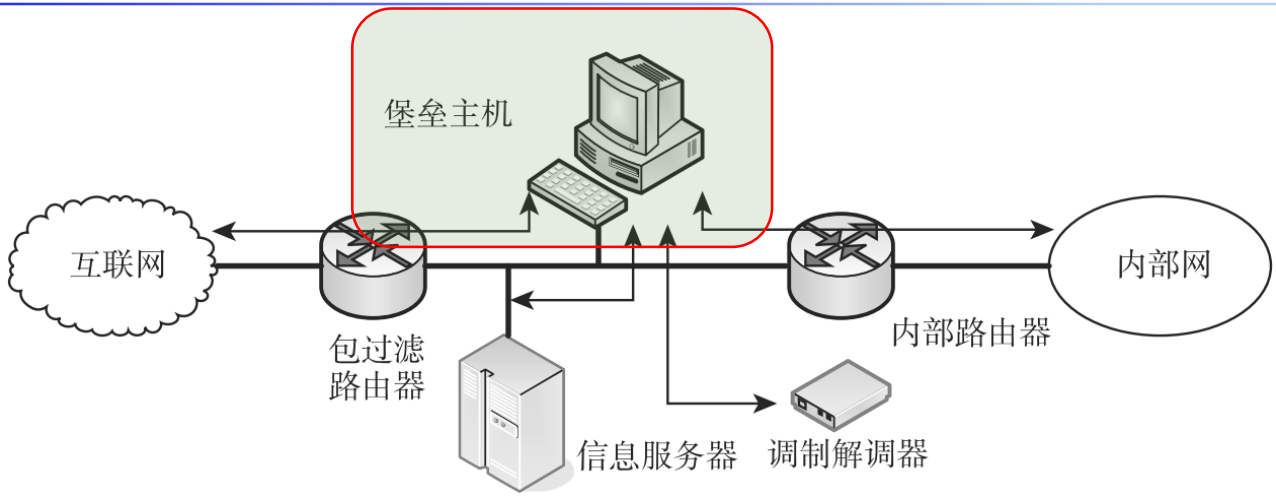


图8-3(b)

- 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**双宿堡垒主机结构**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

8-3(c)

- 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

- 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

(2)双重DNS

(3)虚拟专用网络(VPN)

(4)病毒扫描功能

(5)特殊控制需求

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。

防火墙技术的发展

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。

(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。

(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。

防火墙技术的发展

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。

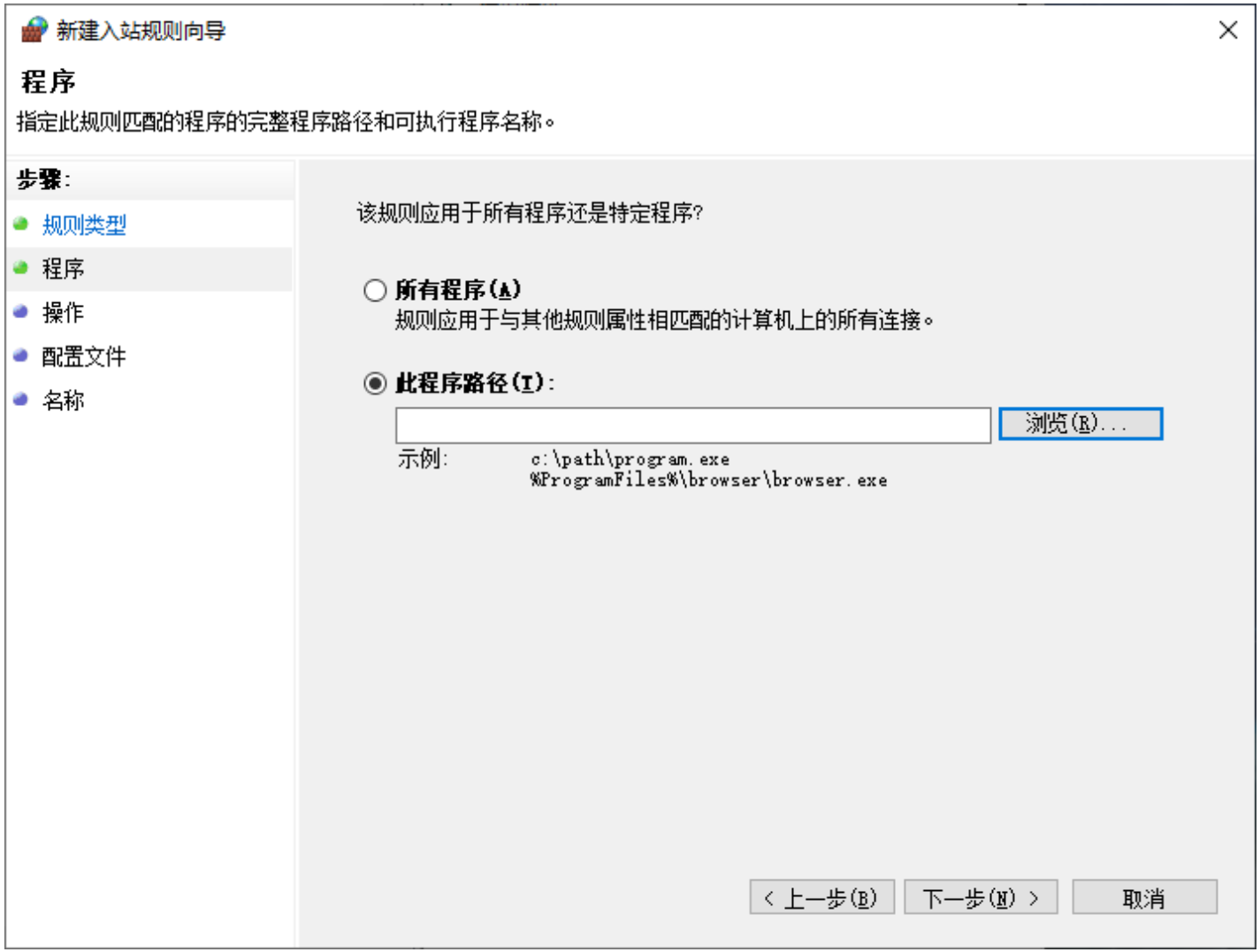
未来防火墙的发展思路

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，并逐渐有病毒清除功能。

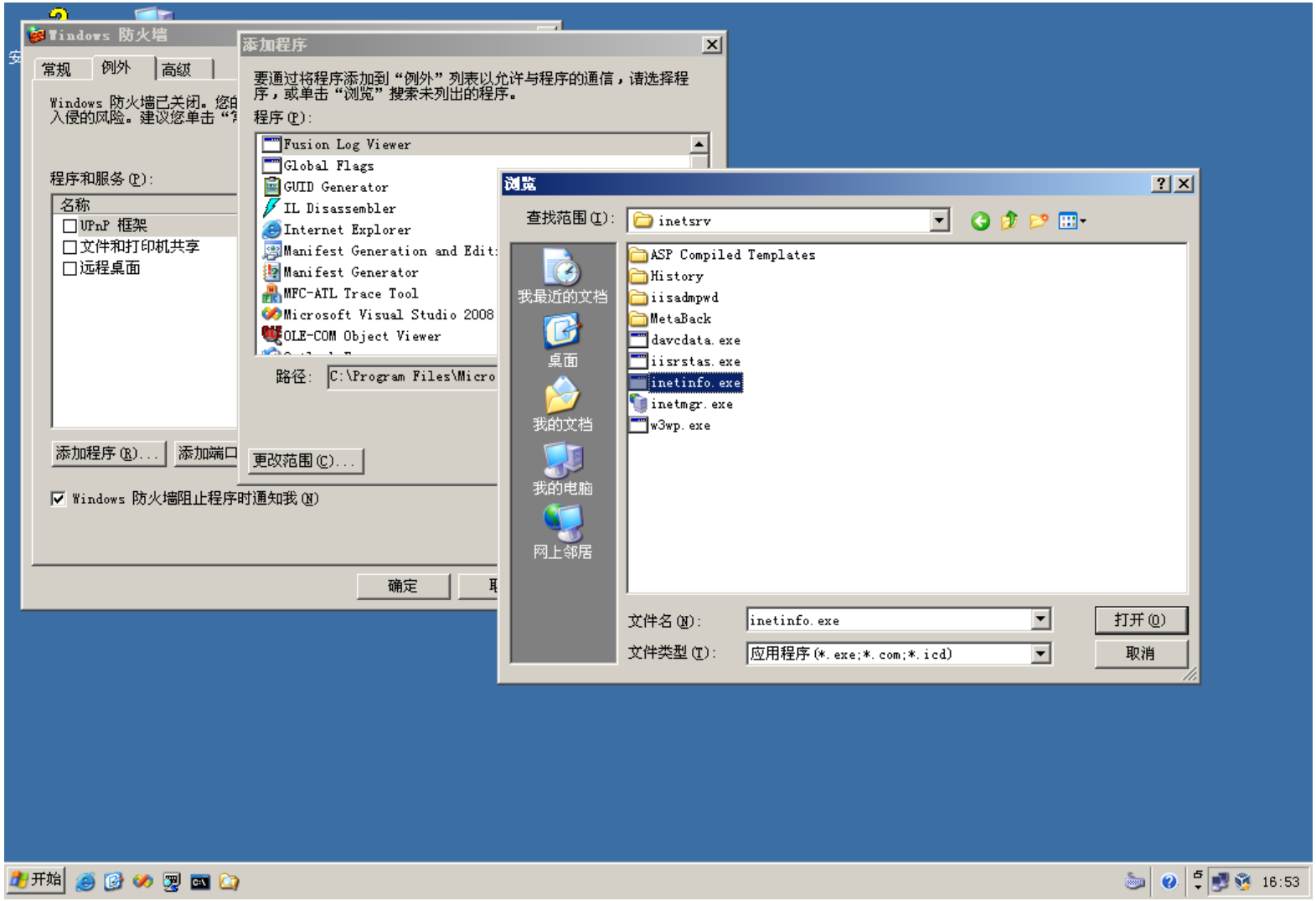
② 利用防火墙建立VPN是较长一段时间内用户使用的主流；对网络攻击的检测和告警将成为防火墙的重要功能。

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。

防火墙实例：Windows10基于程序的过滤



防火墙实例：Windows 2003基于程序的过滤



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研究的主流。

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。

1．入侵检测的概念

- **入侵**就是试图破坏网络及信息系统机密性、完整性和可用性等安全属性的行为。入侵方式一般有：
  (1)未授权的用户访问系统资源；
  (2)已经授权的用户企图获得更高权限，或者是已经授权的用户滥用所给定的权限等。

- **入侵检测的概念：入侵检测是监测计算机网络和系统、发现违反安全策略事件的过程。**

- 美国国家安全通信委员会(NSTAC)下属的入侵检测小组(IDSG)在1997年给出的关于“入侵检测”(Intrusion Detection)的定义是：**入侵检测是对企图入侵、正在进行的入侵或已经发生的入侵行为进行识别的过程。**

“入侵检测”的另3种常见的定义

(1)检测对计算机系统的非授权访问。

(2)对系统的运行状态进行监视，发现各种攻击企图、攻击行为或攻击结果，以保证系统资源的保密性、完整性和可用性。

(3)**识别**针对计算机系统和网络系统、或广义上的信息系统的**非法攻击**，包括检测外部非法入侵者的恶意攻击或探测，以及内部合法用户越权使用系统资源的非法行为。

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

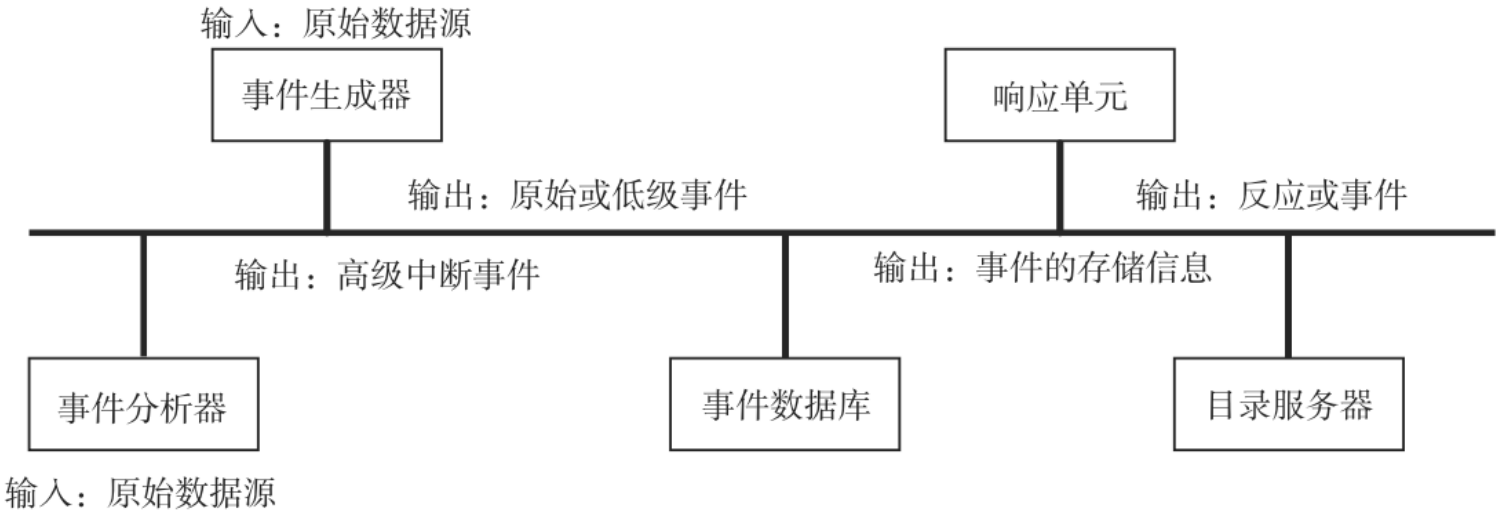
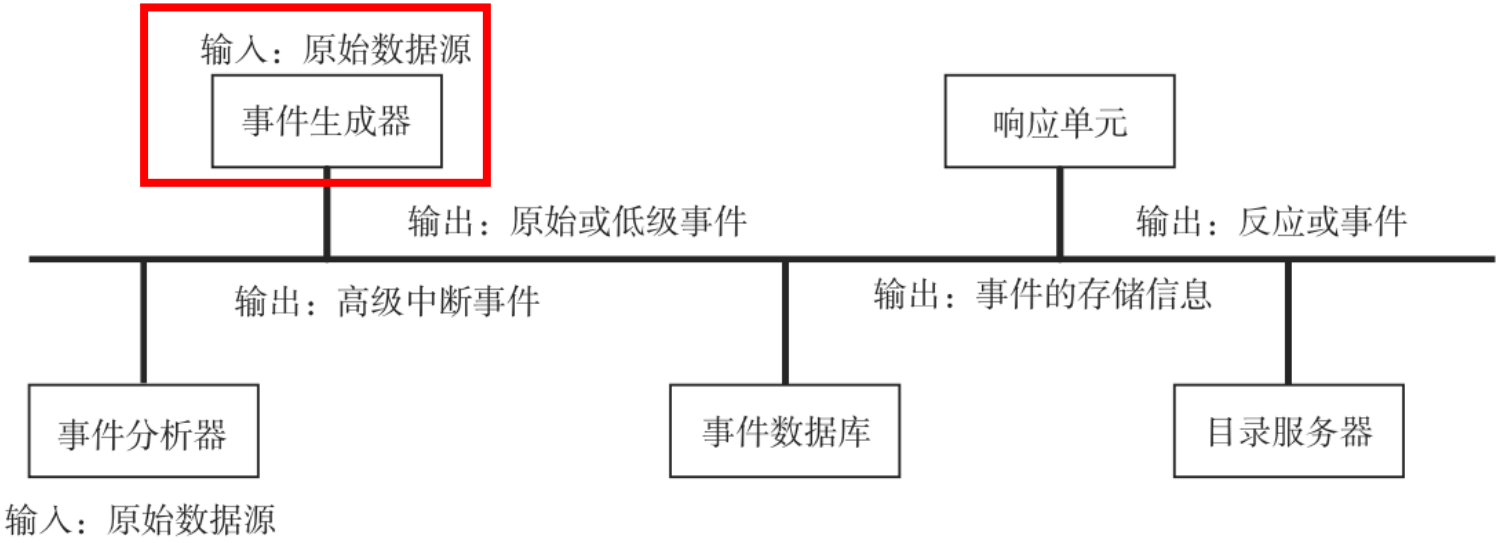


图8-4 IDS体系结构

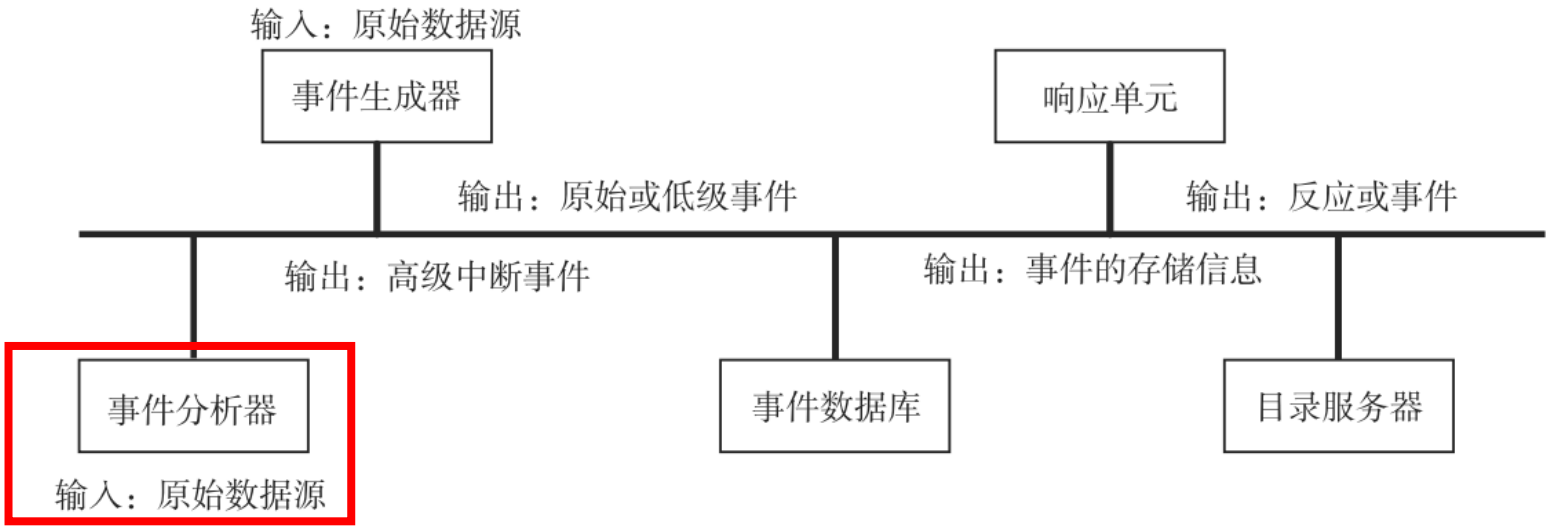
(1)事件生成器



(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。

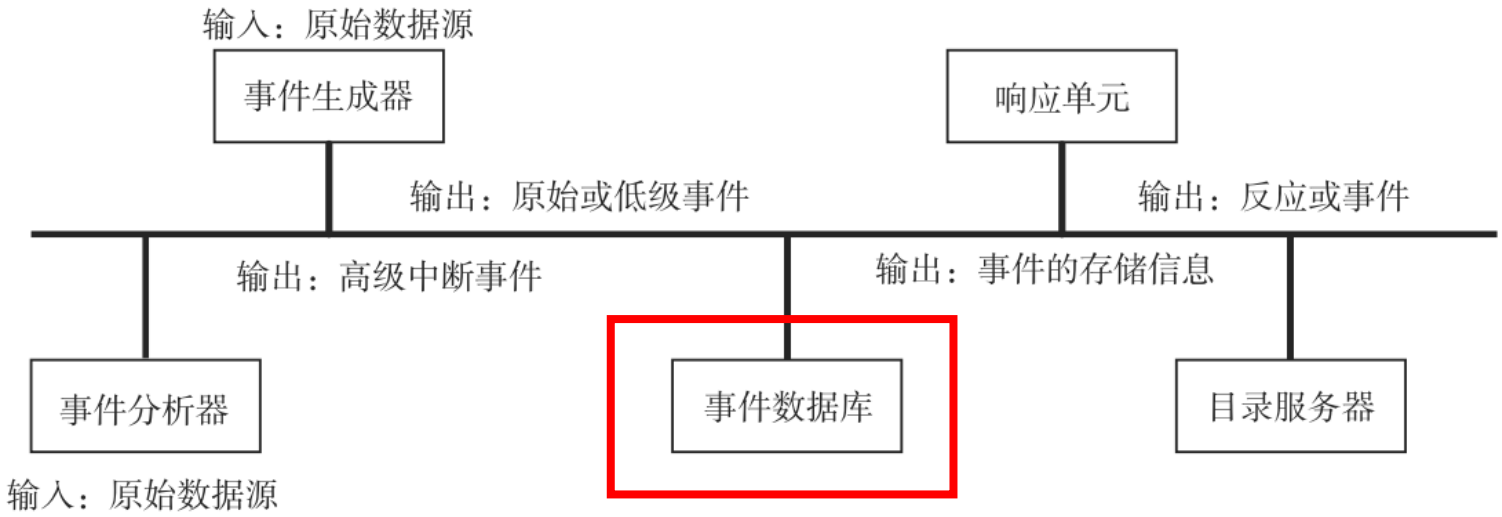
(2)事件分析器



(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。

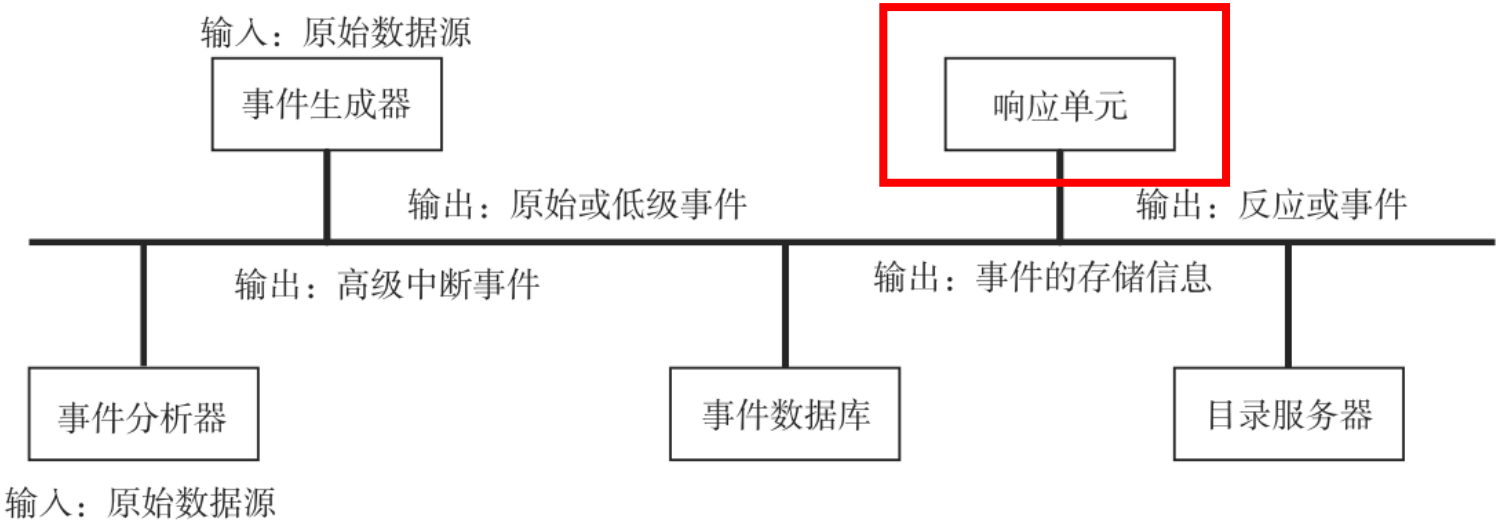
(3)事件数据库



(3)事件数据库：负责存放各种原始数据或已加工过的数据。

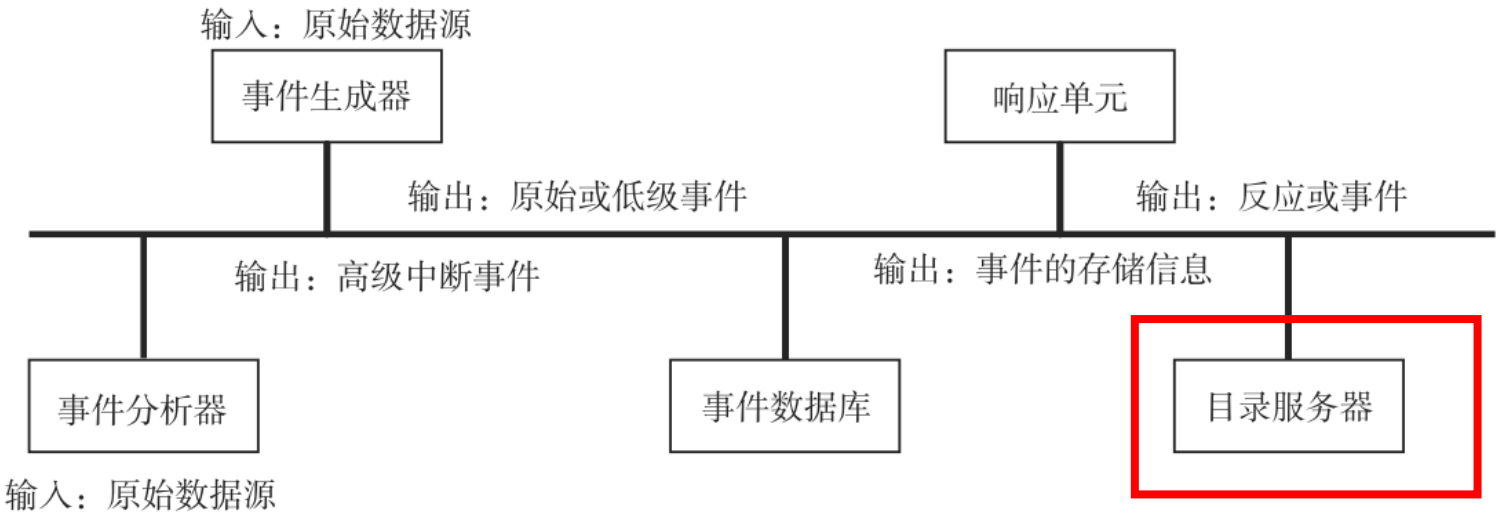
- 它从事件生成器或事件分析器接收数据并进行保存，它可以是复杂的数据库，也可以是简单的文本。

(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。

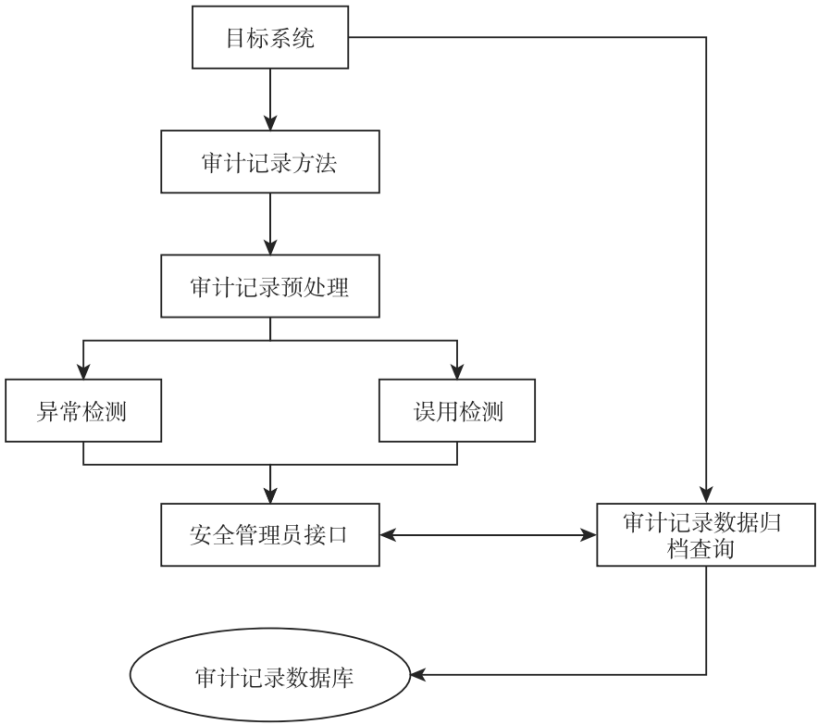


图8-5 基于主机的入侵检测系统

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。

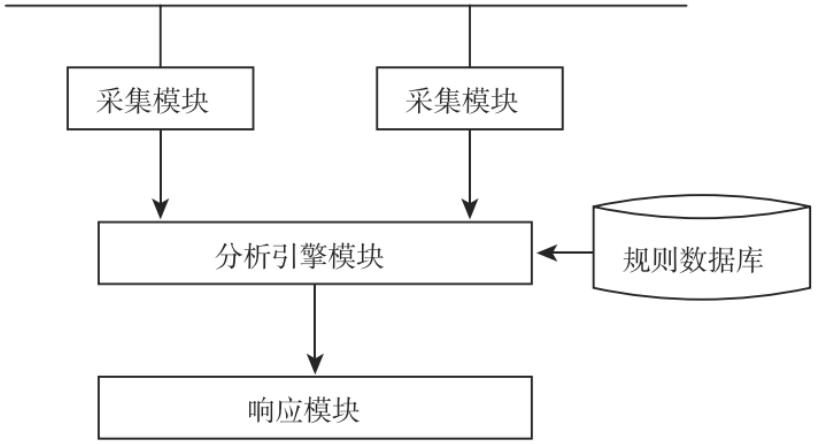


图8-6 基于网络的入侵检测系统

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

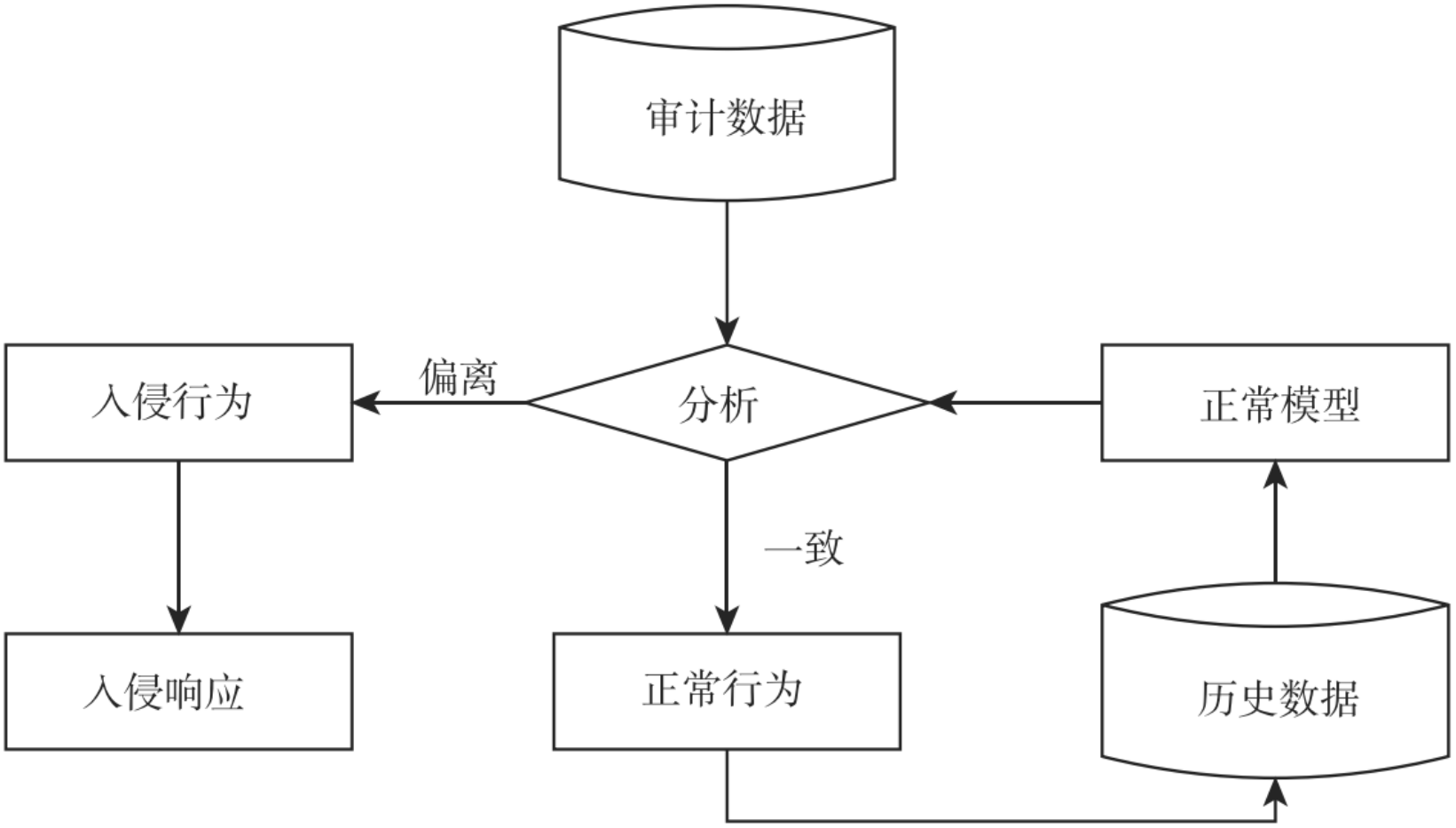


图8-7 异常检测的模型

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

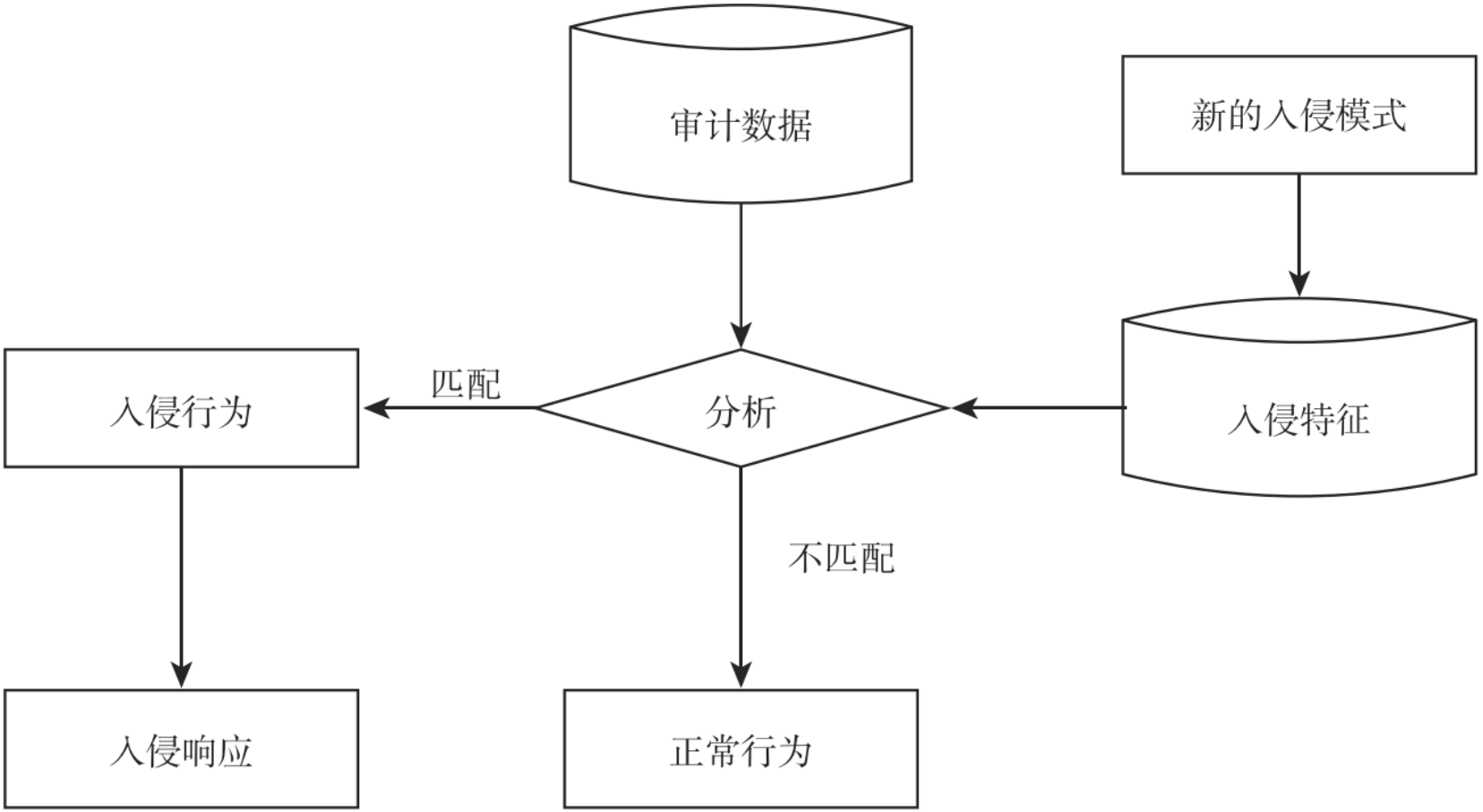


图8-8 误用检测的模型

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

- **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**。

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。

- **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。

典型的分布式入侵检测系统结构

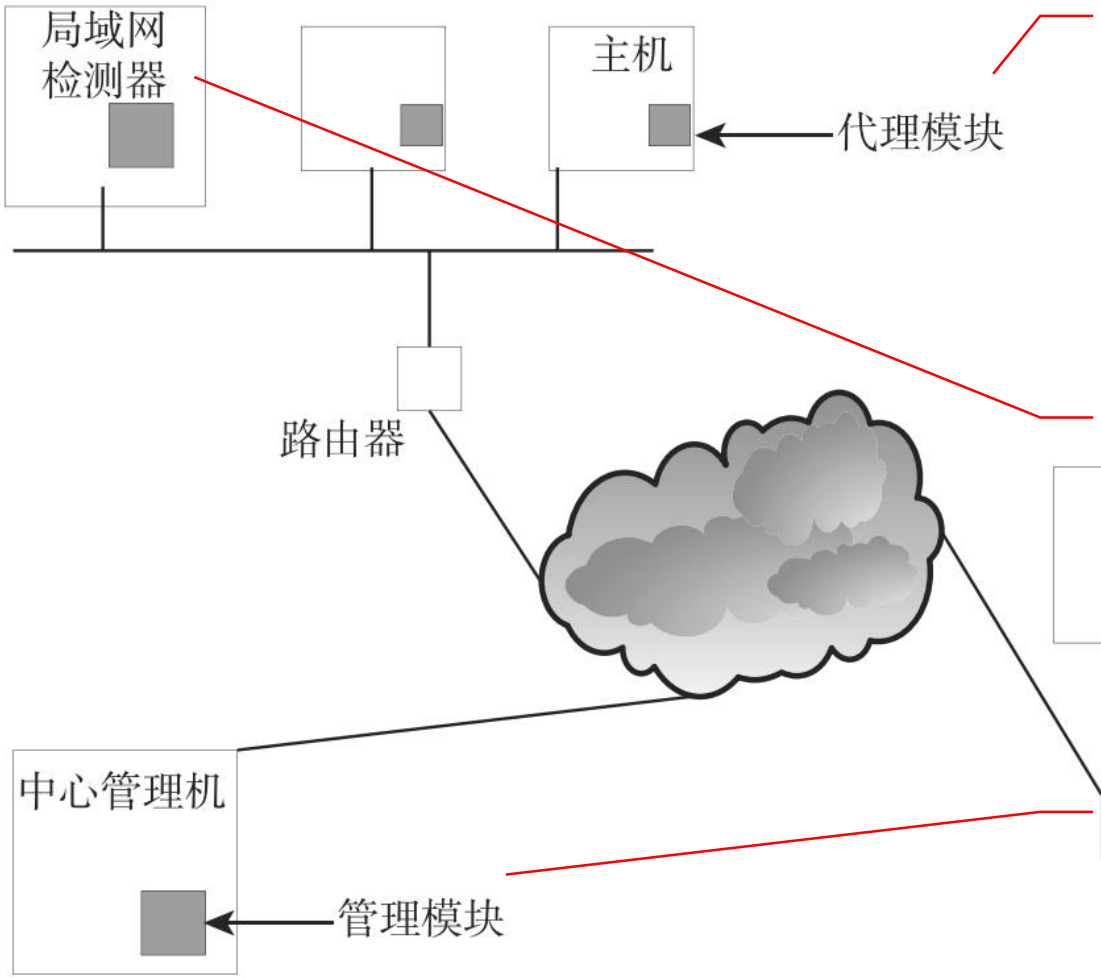


图8-9 分布式入侵检测系统的典型结

(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

(2)入侵检测产品和其他网络安全产品结合的问题

(3)入侵检测系统的功能相对单一

(4)入侵检测系统本身存在的问题

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。
- 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。

基于Snort部署IDS

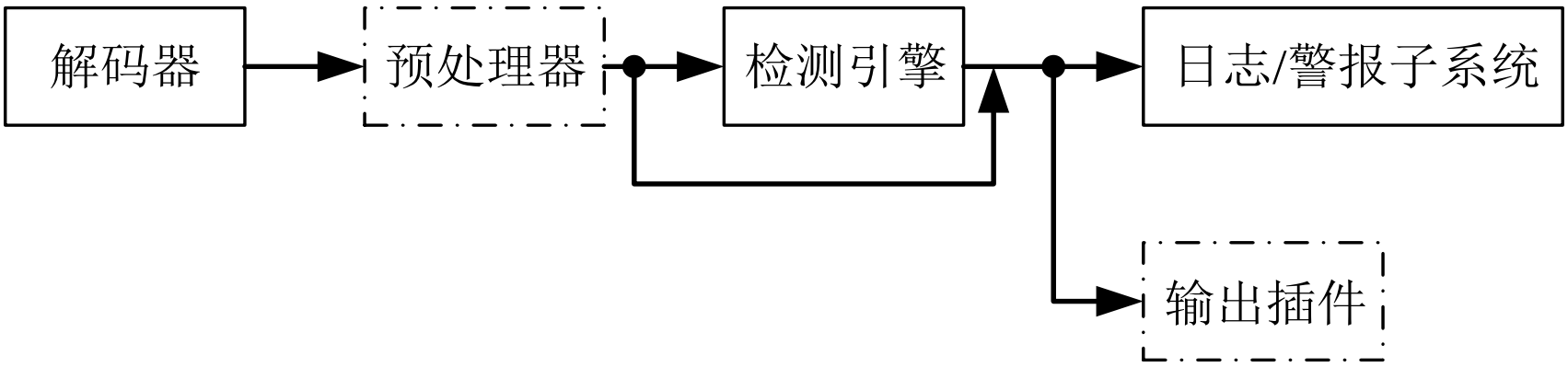
- 在网络中部署IDS时，可以使用多个NIDS和HIDS，这要根据网络的实际情况和自己的需求而定。图6-6是一个典型的IDS的部署图。
- Snort是一个免费的网络入侵检测系统，它是用C语言编写的开源软件。其作者**Martin Roesch**在设计之初，只打算实现一个数据包嗅探器，之后又在其中加入了基于特征分析的功能，从此Snort开始向入侵检测系统演变。
- 现在的Snort已经发展得非常强大，拥有核心开发团队和官方站点(https://www.snort.org/)。
  ① Copyright c 1998-2003 **Martin Roesch**
  ② Copyright c 2001-2003 Chris Green
  ③ Copyright c 2003-2013 Sourcefire, Inc.
  ④ Copyright c 2014-2020 **Cisco and/or its affiliates**. All rights reserved.

关于Snort

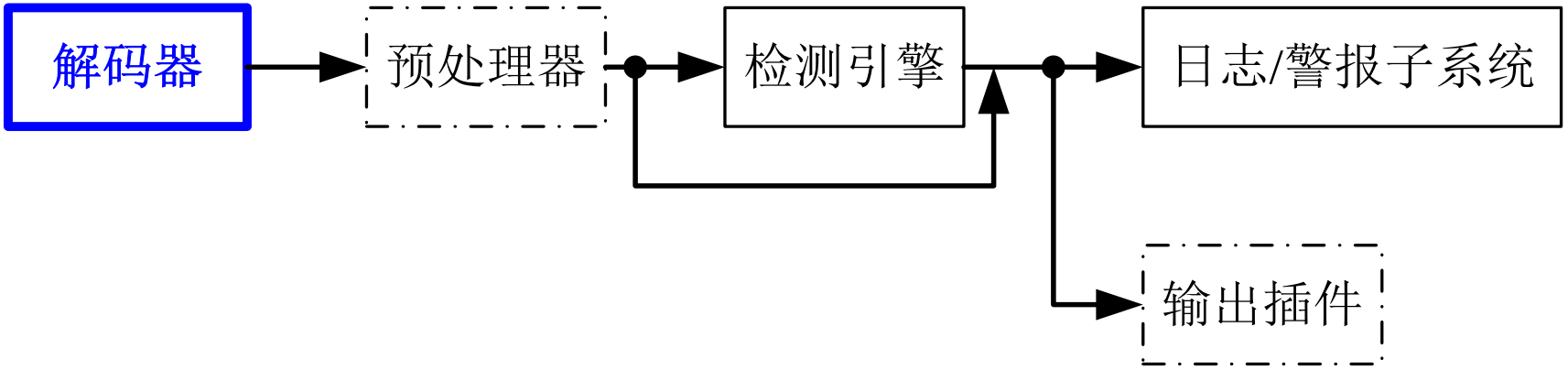
- Snort是一个基于**libpcap**的**轻量级**网络入侵检测系统。
- 它对系统的配置要求比较低，可支持多种操作平台，包括Linux、Windows、Solaris和FreeBSD等。
- 在各种NIDS产品中，Snort是其中最好的之一。不仅因为它是免费的，还因为它本身提供了如下各种强大的功能：
  (1) 基于规则的检测引擎。
  (2)良好的可扩展性。可以使用预处理器和输出插件来对Snort的功能进行扩展。
  (3)灵活简单的规则描述语言。只要用户掌握了基本的TCP、IP知识，就可以编写自己的规则。
  (4)除了用作入侵检测系统，还可以用作嗅探器和包记录器。

Snort的组成

- 一个基于Snort的网络入侵检测系统由以下5个部分组成：
- 解码器；预处理器；检测引擎；输出插件；日志/警报子系统

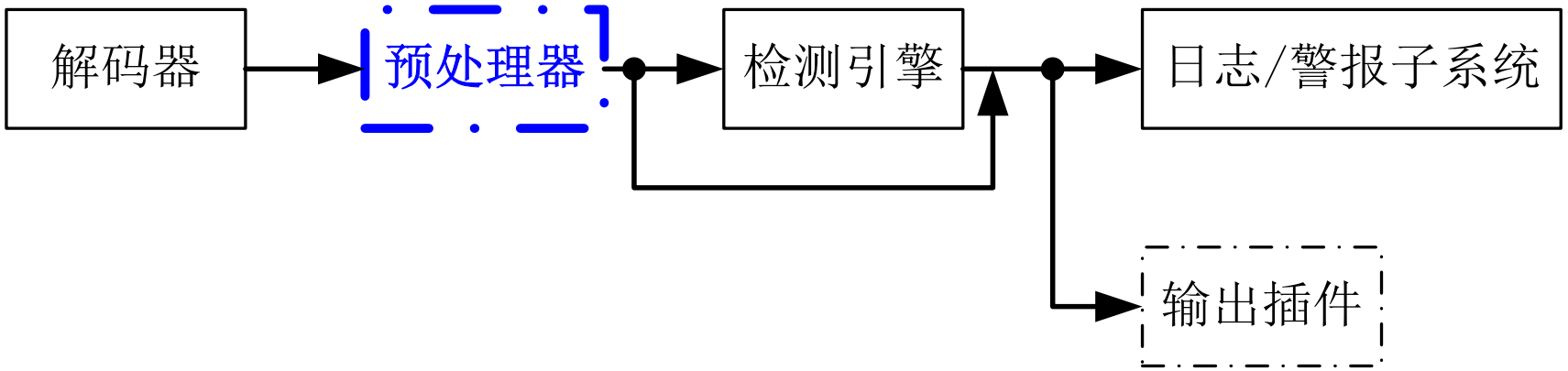


Snort的结构



1.解码器

- 通过libpcap获得网络数据包之后，数据将通过一序列的解码器。
- 首先填写链路级协议的包结构，然后解码为后续处理所需的信息，如TCP或UDP端口之类的信息。获取的信息将被送往预处理器。
- 解码器支持多种类型的网络接口，包括Ethernet、SLIP、PPP等。

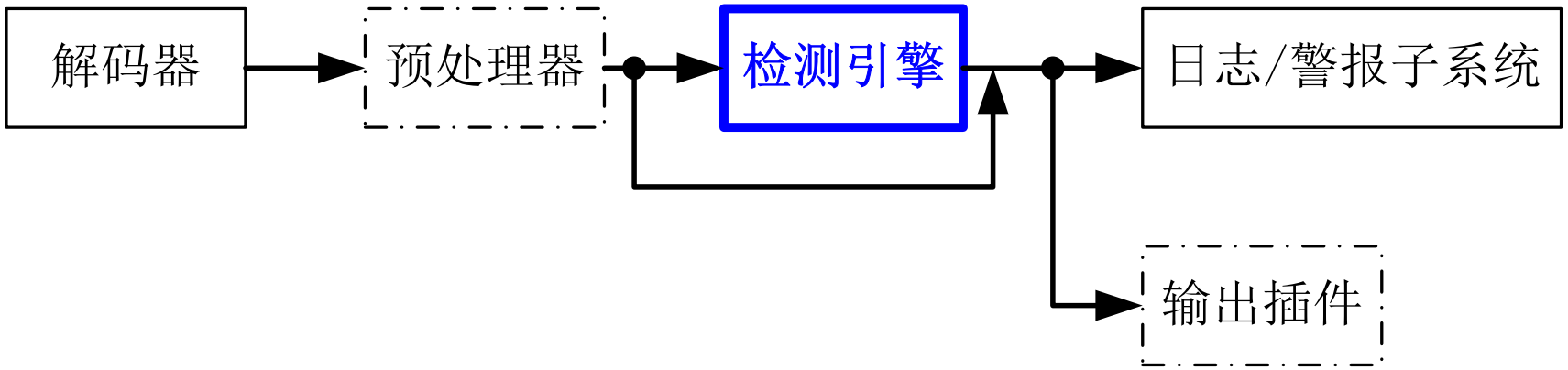


2.预处理器

- Snort主要采用基于规则的方式对数据包进行检测，这种方式因匹配速度快而受到欢迎。
- 但对于Snort来说，超越基于规则匹配的检测机制是必要的。比如说，仅依赖规则匹配无法检测出协议异常。这些额外的检测机制在Snort中是通过**预处理器**来实现的，它工作在检测引擎之前，解码器之后。

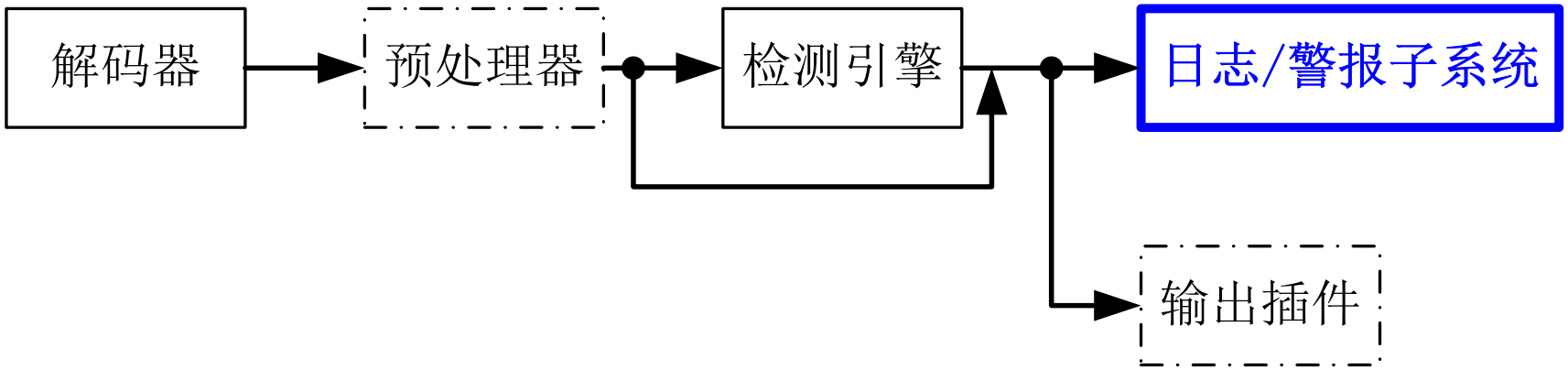
Snort的预处理器

- Snort中包含了三类**预处理器**，分别实现不同的功能：
  - **包重组**。这类预处理器的代表有stream4和frag2。它们将多个数据包中的数据进行组合，构成一个新的待检测包，然后将这个包交给检测引擎或其他预处理器。
  - **协议解码**。为了方便检测引擎方便地处理数据，这类预处理器对Telnet，HTTP和RPC等协议进行解析，并使用统一规范的格式对其进行表述。
  - **异常检测**。用来检测无法用一般规则发现的攻击和协议异常。与前面两种预处理器相比，异常检测预处理器更侧重于报警功能。



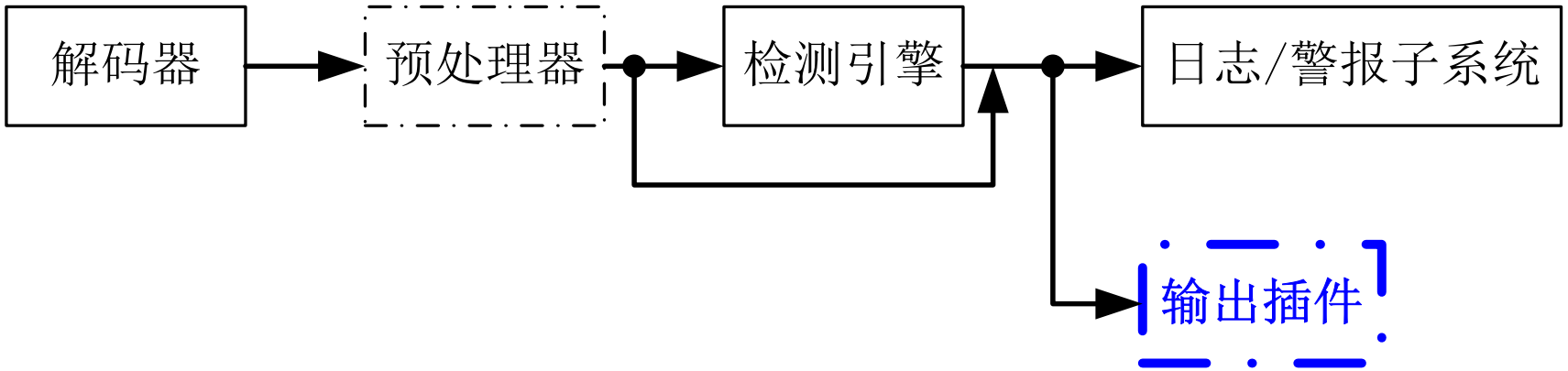
3.检测引擎

- 该子系统是Snort工作在入侵检测模式下的核心部分，它使用基于规则匹配的方式来检测每个数据包。一旦发现数据包的特征符合某个规则定义，则触发相应的处理操作。



4.日志/警报子系统

- 规则中定义了数据包的处理方式，包括alter(报警)、log(日志记录)和pass(忽略)等，但具体的alter和log操作则是由日志/警报子系统完成的。日志子系统将解码得到的信息以ASCII码的格式或以tcpdump的格式记录下来，警报子系统将报警信息发送到syslog、socket或数据库中。



5.输出插件

- 输出插件用来格式化警报信息，使得管理员可以按照公司环境来配置容易理解、使用和查看的报警和日志方法。例如，某公司使用MySQL来存储公司和客户的信息，他们的报表系统是基于MySQL之上的，那么，对于该公司来说，把入侵检测的日志和报警信息保存在MySQL中就显得非常有用。Snort有大量的插件来支持不同的格式，包括数据库、XML、Syslog等格式，从而允许以更加灵活的格式和表现形式将报警及日志信息呈现给管理员。

Snort的工作流程

1. 首先，Snort利用libpcap进行抓包。
2. 之后，由解码器将捕获的数据包信息填入包结构体，并将其送到各式各样的预处理器中。
3. 检测和响应：
   A. 对于那些用于检测入侵的预处理器来说，一旦发现了入侵行为，将直接调用输出插件或者日志、警报子系统进行输出；
   B. 对于那些用于包重组和协议解码的预处理器来说，它们会将处理后的信息送往检测引擎，由检测引擎对数据包的特征及内容进行检查，一旦检测到与已知规则匹配的数据包，或者利用输出插件进行输出，或者利用日志、警报子系统进行报警和记录。

Snort的安装、配置与使用

- 请从官方网站www.snort.org下载用户手册。
  - 截至2022-04-07，snort的最新版本为3.1.27.0

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)

- **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，蜜网融入了数据捕获、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。
- 蜜罐和蜜网技术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

- 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

- 蜜罐技术的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，包括：

(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。

蜜罐技术的辅助机制

- 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) 反蜜罐技术的对抗机制

- 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。
- 包括：1)欺骗环境构建机制；2)威胁数据捕获机制；3)威胁数据分析机制；4)反蜜罐技术的对抗机制。

8.3.4 蜜罐部署结构

1.蜜网

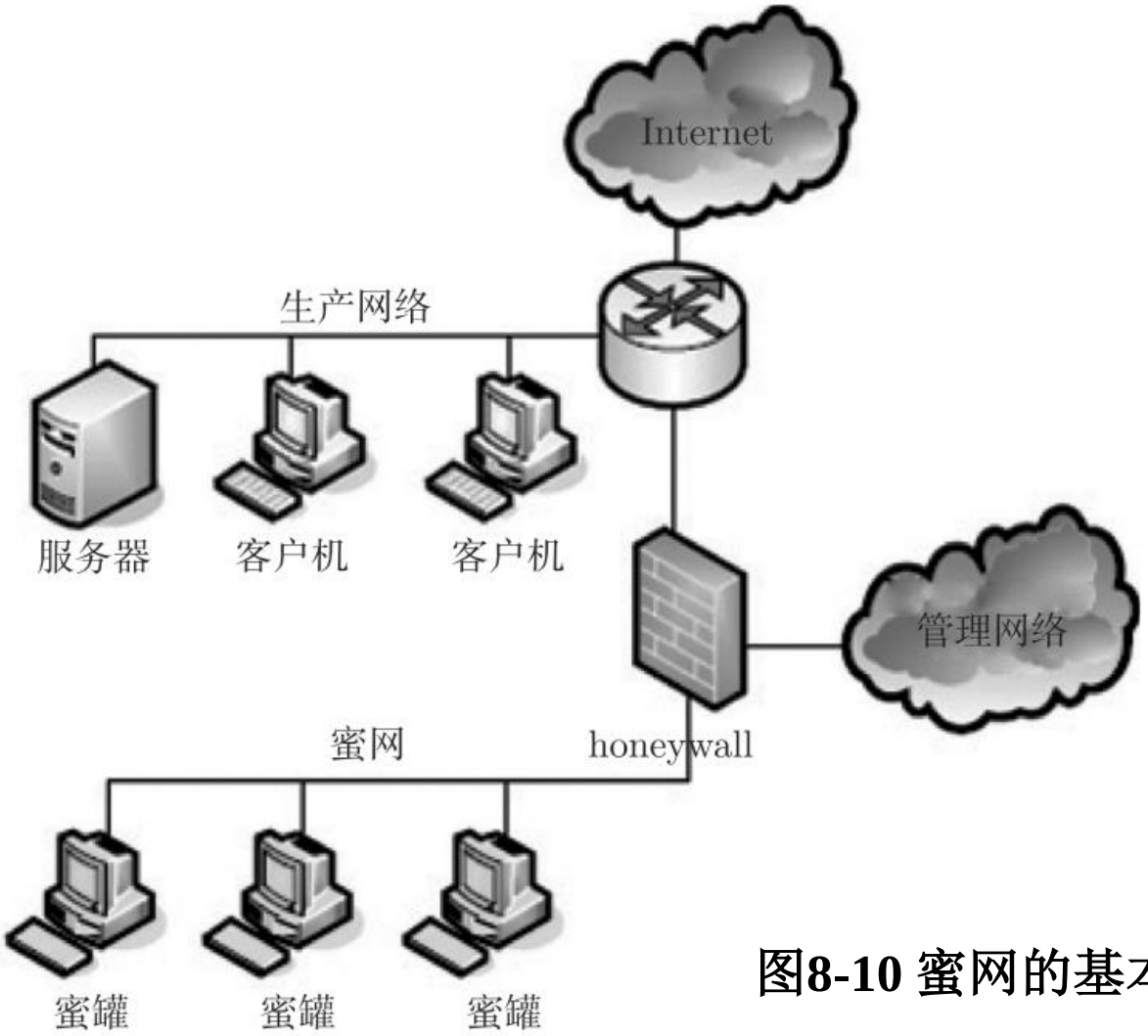


图8-10 蜜网的基本结构

2. 蜜场

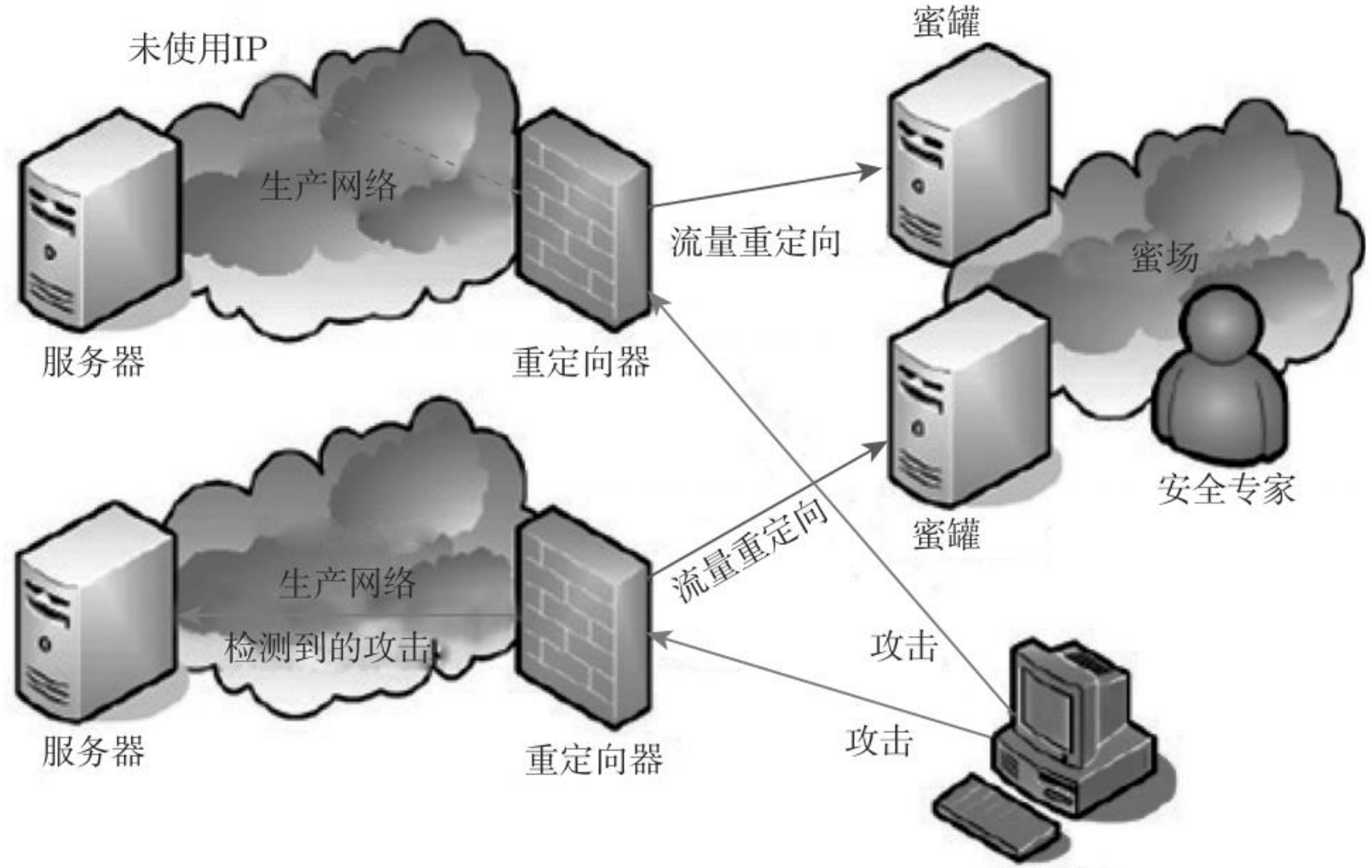


图8-11 蜜场技术概念图示

谢谢！