目录

项目 7 防火墙基础安全业务实施 / 121

项目 8 防火墙安全策略业务实施 / 155

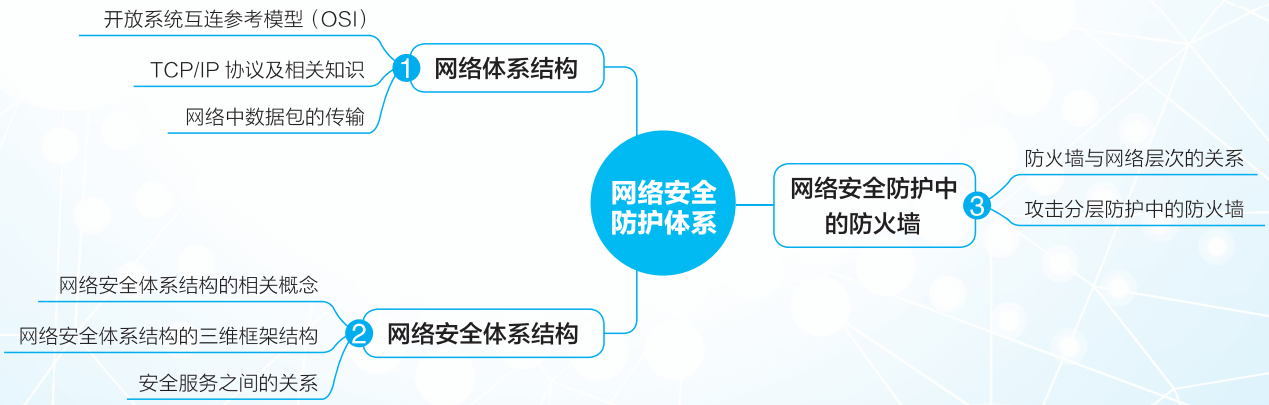
项目 9　NAT 安全策略业务实施 / 183

项目 1 网络安全防护体系

项目目标

1. 了解网络体系结构。
2. 了解网络安全框架。
3. 掌握网络安全防护中的防火墙。

知识导图



笔记

项目导入

随着计算机技术和通信技术的发展，计算机网络日益成为工业、农业和国防等方面的重要信息交换手段，渗透到社会生活的各个领域，网络安全问题逐渐突出。为了提高网络的整体安全水平，必须全方位地构建网络安全防护体系。网络安全体系是一项复杂的系统工程，需要把安全组织体系、安全技术体系和安全管理体系等手段进行有机融合，构建一体化的整体安全屏障。针对网络安全防护，本项目介绍了防火墙在网络安全防护中的地位和作用，帮助读者了解防火墙在整个网络信息安全防护中所处的位置。通过介绍两种重要的网络体系模型 OSI 和 TCP/IP 的基础知识、网络安全框架，帮助读者认识防火墙在网络安全防护中的基础性地位和作用。

任务 1.1 网络体系结构

子任务 1.1.1 开放系统互连参考模型（OSI）

OSI 网络模型分为七层：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。L1 代表 Layer 1，就是物理层；L2 是数据链路层；L3 是网络层。L2 也就是我们所说的接入层。OSI 参考模型如表 1-1 所示。

表 1-1　OSI 参考模型

7 层名称	数据格式	功能与连接方式	典型设备
应用层（Application）	—	网络服务与使用者应用程序间的一个接口	—
表示层（Presentation）	—	数据表示、数据安全、数据压缩	—
会话层（Session）	—	建立、管理和终止会话	—
传输层（Transport）	数据组织成数据段（Segment）	用一个寻址机制来标识一个特定的应用程序（端口号）	—
网络层（Network）	分割和重新组合数据包（Packet）	基于网络层地址（IP 地址）进行不同网络系统间的路径选择	路由器
数据链路层（Data Link）	将比特信息封装成数据帧（Frame）	通过使用接收系统的硬件地址或物理地址来寻址	网桥、交换机
物理层（Physical）	传输比特（bit）流	建立、维护和取消物理连接	网卡、中继器和集线器

1. 物理层

物理层（Physical Layer）规定通信设备的机械的、电气的、功能的和过程的特性，用以建立、维护和拆除物理链路连接。具体地讲，机械特性规定了网络连接时所需接插件的规格尺寸、引脚数量和排列情况等；电气特性规定了在物理连接上传输比特流时线路上信号电平的大小、阻抗匹配、传输速率、距离限制等；功能特性是指对各个信号先分配确切的信号含义，即定义了 DTE 和 DCE 之间各个线路的功能；过程特性定义了利用信号线进行比特流传输的一组操作规程，是指在物理连接的建立、维护、交换信息时，DTE 和

DCE 双方在各电路上的动作系列。在这一层，数据的单位称为比特（bit）。属于物理层定义的典型规范代表包括 EIA/TIA RS-232、EIA/TIA RS-449、V.35、RJ-45 等。

笔记

物理层为数据端设备提供传送数据的通路，数据通路可以是一个物理介质，也可以是多个物理介质连接而成。一次完整的数据传输，包括激活物理连接、传送数据、终止物理连接。所谓激活，就是不管有多少物理介质参与，都要在通信的两个数据终端设备间连接起来，形成一条通路。

物理层要形成适合数据传输需要的实体，为数据传送服务，一是要保证数据能在其上正确通过，二是要提供足够的带宽（带宽是指每秒内能通过的比特（bit）数），以减少信道上的拥塞。传输数据的方式能满足点到点、一点到多点、串行或并行、半双工或全双工、同步或异步传输的需要，并完成物理层的一些管理工作。

物理层的主要设备有中继器、集线器。

2. 数据链路层

数据链路层（Data Link Layer）在物理层提供比特流服务的基础上，建立相邻节点之间的数据链路，通过差错控制提供数据帧在信道上无差错地传输，并进行各电路上的动作系列。

数据链路层在不可靠的物理介质上提供可靠的传输。该层的作用包括物理地址寻址、数据的成帧、流量控制、数据的检错、重发等。在这一层，数据的单位称为帧（Frame）。数据链路层协议的代表包括 SDLC、HDLC、PPP、STP、帧中继等。

数据链路层是为网络层提供数据传送服务的，这种服务要依靠本层具备的功能来实现。数据链路层应具备如下功能：链路连接的建立、拆除、分离；帧定界和帧同步。数据链路层的数据传输单元是帧，协议不同，帧的长短和界面也有差别，但无论如何必须对帧进行界定。顺序控制，指对帧的收发顺序的控制、差错检测和恢复。还有链路标识、流量控制等。差错检测多用方阵码校验和循环码校验来检测信道上数据的误码，而帧丢失等用序号检测。各种错误的恢复则常靠反馈重发技术来完成。

数据链路层主要设备有交换机、网桥。

3. 网络层

在计算机网络中进行通信的两个计算机之间可能会经过很多个数据链路，也可能还要经过很多通信子网。网络层（Network Layer）的任务就是选择合适的网间路由和交换节点，确保数据及时传送。网络层将数据链路层提供的帧组成数据包，包中封装有网络层包头，其中含有逻辑地址信息——源站点和目的站点地址的网络地址。

如果你在谈论一个 IP 地址，那么你是在处理第三层的问题，这是“数据包”问题，而不是第二层的“帧”。IP 是第三层问题的一部分，此外还有一些路由协议和地址解析协议（ARP）。有关路由的一切事项都在第三层处理。地址解析和路由是第三层的重要目的。网络层还可以实现拥塞控制、网际互联等功能。在这一层，数据的单位称为数据包（Packet）。网络层协议的代表包括 IP、IPX、OSPF 等。

网络层为建立网络连接和为上层提供服务，应具备的功能有：路由选择和中继；激活、终止网络连接；在一条数据链路上复用多条网络连接（多采取分时复用技术）；差错检测与恢复；排序和流量控制；服务选择；网络管理；网络层标准简介。

网络层主要设备有路由器。

笔记

4. 传输层

传输层（Transport Layer）的数据单元也称作数据包（Packet）。但是，当在谈论 TCP 等具体的协议时又有特殊的叫法。TCP 的数据单元称为段（Segment），而 UDP 协议的数据单元称为“数据报（Datagram）”。这个层负责获取全部信息，因此，它必须跟踪数据单元碎片、乱序到达的数据包和其他在传输过程中可能发生的危险。第四层为上层提供端到端（最终用户到最终用户）的透明的、可靠的数据传输服务。所谓透明的传输是指在通信过程中传输层对上层屏蔽了通信传输系统的具体细节。传输层协议的代表包括 TCP、UDP、SPX 等。传输层是两台计算机经过网络进行数据通信时第一个端到端的层次，具有缓冲作用。当网络层服务质量不能满足要求时，它将服务加以提高，以满足高层的要求；当网络层服务质量较好时，它只用很少的工作。传输层还可进行复用，即在一个网络连接上创建多个逻辑连接。传输层也称为运输层。传输层只存在于端开放系统中，是介于低三层通信子网系统和高三层之间的一层，但却是很重要的一层，因为它是源端到目的端对数据传送进行控制从低到高的最后一层。

有一个既成事实，即世界上各种通信子网在性能上存在着很大差异，例如电话交换网、分组交换网、公用数据交换网、局域网等通信子网都可互取，但它们提供的吞吐量、传输速率、数据延迟、通信费用各不相同。对于会话层来说，却要求有一个性能恒定的界面，传输层就承担了这一功能。它采用分流 / 合流、复用 / 介复用技术来调节上述通信子网的差异，使会话层感受不到它们之间的差别。

此外，传输层还要具备差错恢复、流量控制等功能，以此对会话层屏蔽通信子网在这些方面的细节与差异。传输层面对的数据对象已不是网络地址和主机地址，而是和会话层的界面端口。上述功能的最终目的是为会话提供可靠的、无误的数据传输。传输层的服务一般要经历传输连接建立阶段、数据传送阶段、传输连接释放阶段 3 个阶段才算完成一个完整的服务过程，而在数据传送阶段又分为一般数据传送和加速数据传送两种。传输层服务分成 5 种类型，基本可以满足对传送质量、传送速度、传送费用的各种不同需要。

5. 会话层

会话层（Session Layer）也可以称为会晤层或对话层，在会话层及以上的高层中，数据传送的单位不再另外命名，统称为报文。会话层不参与具体的传输，它提供包括访问验证和会话管理在内的建立和维护应用之间通信的机制，如服务器验证用户登录便是由会话层完成的。会话层提供的服务可使应用建立和维持会话，并能使会话获得同步。会话层使用校验点可使通信会话在通信失效时从校验点继续恢复通信。这种能力对于传送大的文件极为重要。会话层、表示层、应用层构成开放系统的高三层，面对应用进程提供分布处理、对话管理、信息表示、恢复最后的差错等。会话层同样要担负应用进程服务要求，而传输层不能完成的那部分工作，给传输层功能差距以弥补，主要的功能是对话管理、数据流同步和重新同步。要完成这些功能，需要由大量的服务单元功能组合，已经确定的功能单元已有几十种。

为给两个对等会话服务用户建立一个会话连接，应该做如下几项工作。

（1）将会话地址映射为运输地址。

（2）选择需要的运输服务质量参数（QoS）。

（3）对会话参数进行协商。

（4）识别各个会话连接。

（5）传送有限的透明用户数据。

数据传输阶段是在两个会话用户之间实现有组织的、同步的数据传输。用户数据单元为 SSDU，而协议数据单元为 SPDU。会话用户之间的数据传送过程是将 SSDU 转变成 SPDU 进行的。连接释放是通过“有序释放”“废弃”“有限量透明用户数据传送”等功能单元来释放会话连接的。会话层标准为了使会话连接建立阶段能进行功能协商，也为了便于其他国际标准参考和引用。会话层定义了 12 种功能单元。各个系统可根据自身情况和需要，以核心功能服务单元为基础，选配其他功能单元组成合理的会话服务子集。会话层的主要标准有“DIS8236：会话服务定义”和“DIS8237：会话协议规范”。

6. 表示层

表示层（Presentation Layer）主要解决用户信息的语法表示问题。它将欲交换的数据从适合于某一用户的抽象语法，转换为适合于 OSI 系统内部使用的传送语法，即提供格式化的表示和转换数据服务。数据的压缩和解压缩、加密和解密等工作都由表示层负责。例如图像格式的显示，就是由位于表示层的协议来支持。

7. 应用层

应用层（Application Layer）为操作系统或网络应用程序提供访问网络服务的接口。应用层协议的代表包括 Telnet、FTP、HTTP、SNMP 等。通过 OSI 各层，信息可以从一台计算机的软件应用程序传输到另一台计算机的应用程序上。例如，计算机 A 上的应用程序要将信息发送到计算机 B 的应用程序，则计算机 A 中的应用程序需要将信息先发送到其应用层（第七层），然后此层将信息发送到表示层（第六层），表示层将数据转送到会话层（第五层），如此继续，直至物理层（第一层）。在物理层，数据被放置在物理网络媒介中并被发送至计算机 B。计算机 B 的物理层接收来自物理媒介的数据，然后将信息向上发送至数据链路层，数据链路层再转送给网络层，依次继续，直到信息到达计算机 B 的应用层。最后，计算机 B 的应用层再将信息传送给应用程序接收端，从而完成通信过程。

OSI 的七层运用各种各样的控制信息来和其他计算机系统的对应层进行通信。这些控制信息包含特殊的请求和说明，它们在对应的 OSI 层间进行交换。每一层数据的头和尾是两个携带控制信息的基本形式。

对于从上一层传送下来的数据，附加在前面的控制信息称为头，附加在后面的控制信息称为尾。然而，在对来自上一层数据增加协议头和协议尾，对一个 OSI 层来说并不是必需的。当数据在各层间传送时，每一层都可以在数据上增加头和尾，而这些数据已经包含了上一层增加的头和尾。协议头包含了有关层与层间的通信信息。头、尾以及数据是相关联的概念，它们取决于分析信息单元的协议层。例如，传输层头包含了只有传输层可以看到的信息，传输层下面的其他层只将此头作为数据的一部分传递。对于网络层，一个信息单元由第三层的头和数据组成。对于数据链路层，经网络层向下传递的所有信息，即第三层头和数据都被看作是数据。换句话说，在给定的某一 OSI 层，信息单元的数据部分包含来自所有上层的头和尾以及数据，这称之为封装。例如，如果计算机 A 要将应用程序中的某数据发送至计算机 B，数据首先传送至应用层。 计算机 A 的应用层通过在数据上添加协议头来和计算机 B 的应用层通信，所形成的信息单元包含协议头、数据，可能还有协议尾，被发送至表示层，表示层再添加为计算机 B 的表示层所理解的控制信息的协议头。信息单元的大小随着每一层协议头和协议尾的添加而增加，这些协议头和协议尾包含了计算机 B 的对应层要使用的控制信息。在物理层，整个信息单元通过网络介质传输。计算

笔记

笔记

机 B 中的物理层收到信息单元并将其传送至数据链路层；然后计算机 B 中的数据链路层读取计算机 A 的数据链路层添加的协议头中的控制信息；然后去除协议头和协议尾，剩余部分被传送至网络层。每一层执行相同的动作：从对应层读取协议头和协议尾，并去除，再将剩余信息发送至上一层。应用层执行完这些动作后，数据就被传送至计算机 B 中的应用程序，这些数据和计算机 A 的应用程序所发送的完全相同 。一个 OSI 层与另一层之间的通信是利用第二层提供的服务完成的。相邻层提供的服务帮助一 OSI 层与另一计算机系统的对应层进行通信。一个 OSI 模型的特定层通常是与另外三个 OSI 层联系：与之直接相邻的上一层和下一层，还有目标联网计算机系统的对应层。例如，计算机 A 的数据链路层应与其网络层、物理层以及计算机 B 的数据链路层进行通信。

子任务 1.1.2 TCP/IP 协议及相关知识

OSI 的七层协议体系结构虽然概念清楚，但是复杂又不适用。TCP/IP 协议得到了全世界的承认，成为 Internet 使用的参考模型。

计算机网络系统在网络操作系统和 TCP/IP 协议的支持下，位于不同主机内的操作系统进程可以像在一个单机系统中一样互相通信，只不过通信时延稍大一些而已。

TCP/IP 协议族可以看作是一组不同层的集合，每一层负责一个具体任务，各层联合工作实现整个网络通信。每一层与其上层或下层都有一个明确定义的接口来具体说明希望处理的数据。

一般将 TCP/IP 协议族分为 4 个功能层：应用层、传输层、网络层和网络接口层。这 4 层概括了相对于 OSI 参考模型中的七层。

1. 端口

端口将应用进程与 IP 网络相关联，是应用进程的地址标识。一个端口是一个 16 位号码。端口分为公用和临时两种。

公用端口：属于标准服务器，由权威机构 IANA 统一分配，从 1~1023。

临时端口：用于客户，从 1024~65535。

2. 套接字

为了使得多主机多进程通信时不至于发生混乱，必须把端口号主机的 IP 地址结合起来使用，称为插口或套接字（Socket）。由于主机的 IP 地址是唯一的，这样目的主机就可以区分收到的数据报的源端机了。

套接字包括 IP 地址（32 位）和端口号（16 位），共 48 位。例如（124.33.13.55，200）和（126.45.21.51，25）就是一对套接字。在整个 Internet 中，在传输层上进行通信的一对套接字都必须是唯一的。

3. TCP 连接的建立

第一次握手：客户端 TCP 首先给服务器端 TCP 发送一个特殊的 TCP 数据段。该数据段不包含应用层数据，并将头部中的 SYN 位设置为 1，所以该数据段称为 SYN 数据段。另外，客户选择一个初始序列号 SEQ，设 SEQ = x 并将这个编号放到初始的 TCP SYN 数据段的序列号字段中。该数据段被封装到一个 IP 数据报中，并发送给服务器。

第二次握手：一旦装有 TCP SYN 数据段的 IP 数据报到达了服务器主机，服务器将从该数据报中提取出 TCP SYN 数据段，给该连接分配 TCP 缓冲区和变量，并给客户 TCP

发送一个允许连接的数据段。这个允许连接的数据段也不包含任何应用层数据。但是，它的头部中装载着 3 个重要信息。首先，SYN 被设置为 1；其次，TCP 数据段头部的确认字段被设置为 x+1；最后服务器选择自己的初始顺序号，SEQ=y，并将该值放到 TCP 数据段头部的序列号字段中。

笔记

第三次握手：在接收到允许连接数据段之后，客户也会给连接分配缓冲区和变量。客户端主机还会给服务器发送另一个数据段，对服务器的允许连接数据段给出确认。TCP 协议中连接建立的过程如图 1-1 所示。

4. TCP 连接的释放

第一次握手：由进行数据通信的任意一方提出要求释放连接的请求报文段。

第二次握手：接收端收到此请求后，会发送确认报文段，同时当接收端的所有数据也都已经发送完毕后，接收端会向发送端发送一个带有其自己序号的报文段。

第三次握手：发送端收到接收端的要求释放连接的报文段后，发送反向确认。TCP 连接的释放过程如图 1-2 所示。

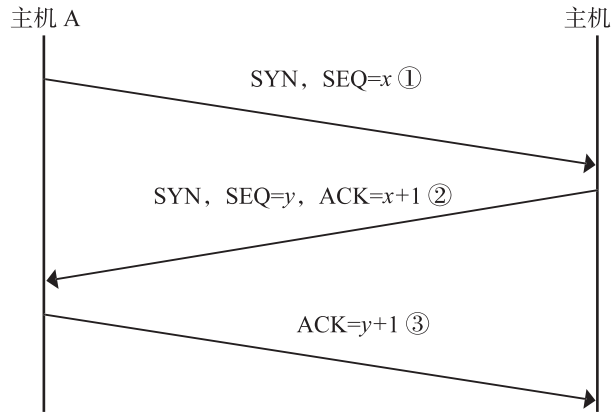


图 1-1　TCP 协议中连接建立的过程

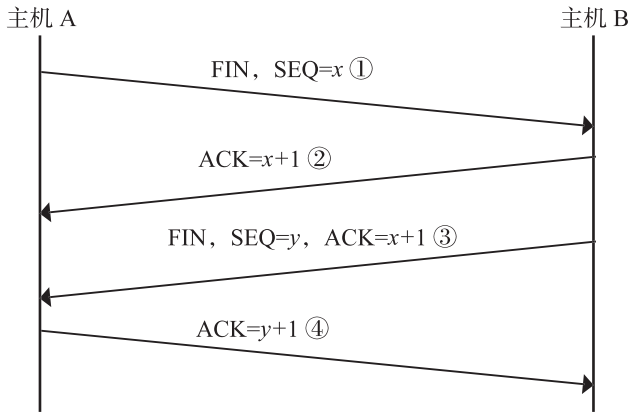


图 1-2　TCP 连接的释放过程

图 1-3 所示为 TCP 数据报文结构，图 1-4 所示为 UDP 报文结构。

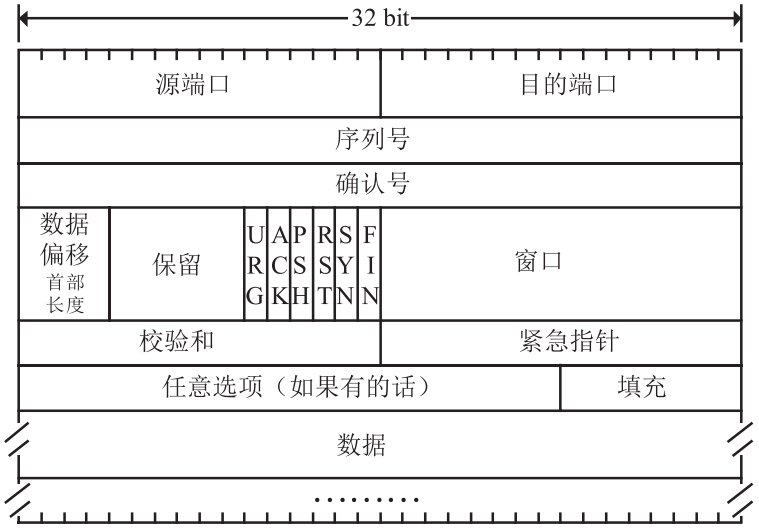


图 1-3　TCP 数据报文结构

笔记

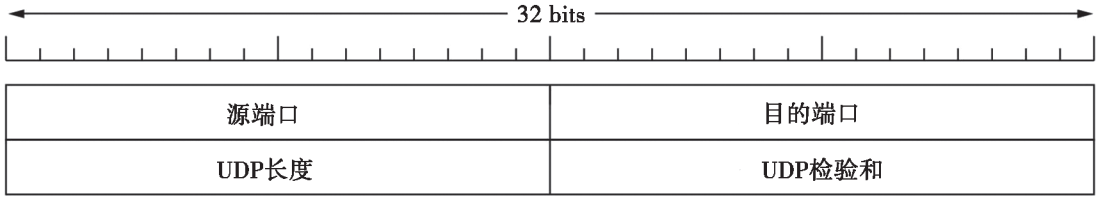


图 1-4　UDP 报文结构

5. IPv6

IPv4 的不足主要有以下几点：

（1）基本耗尽，这是当前最棘手的问题 。

（2）路由表越来越大。

（3）功能不足，缺少对多媒体信息传输的支持。

（4）缺少对安全的支持。

（5）缺少对主机漫游的支持。

针对 IPv4 的不足，引入了 IPv6，其主要有以下几点改进：

（1）更大的地址空间：128 位。

（2）灵活的首部格式：用一系列固定格式的扩展首部取代了 IPv4 中可变长度的选项字段。

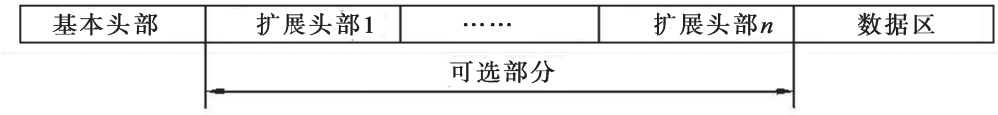
（3）简化了协议：如取消了首部的校验和字段，分段只能在源端进行。

（4）允许对网络资源的预分配，支持实时图像等要求，保证一定的带宽和时延的应用。

（5）允许协议继续演变，增加新的功能。

IPv6 数据包格式如图 1-5 所示。

❖ **基本头部和扩展头部**



❖ **基本头部格式**

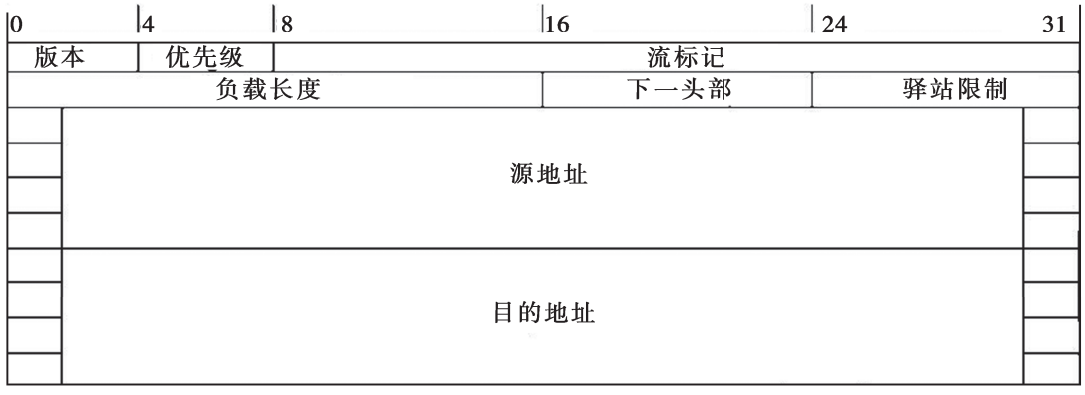


图 1-5　IPv6 数据包格式

6. 域名

为了使用和记忆方便，Internet 还采用了域名管理系统（Domain Name System，

DNS）。在 IP 地址之外，网上的计算机还有另一种表示法：域名，它是由代表一定意义的英文单词的缩写构成，如图 1-6 所示。

笔记

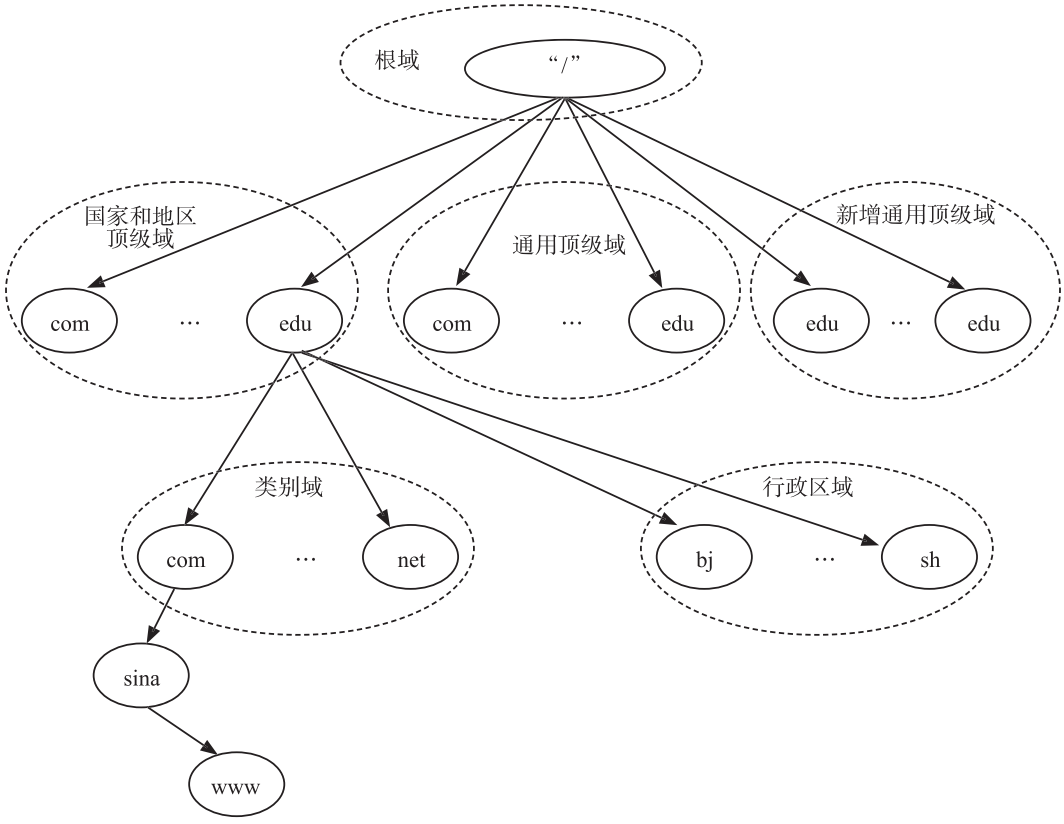


图 1-6　域名举例

域名是一种按一定规律书写的、用户容易理解、容易记忆的 Internet 地址。Internet 上一台主机的主机名是由它所属的各级域的域名和分配给该主机的名字共同构成的。书写的时候，顶级域名放在最右面，各级名字之间有“.”隔开。域名是有层次的。 Internet 主机域名的一般格式为：四级域名 . 三级域名 . 二级域名 . 顶级域名（并不一定分四级），如 www.sina.com.cn。顶级域名的划分采用了两种模式：地理模式、组织模式。互联网的域名空间如图 1-7 所示。

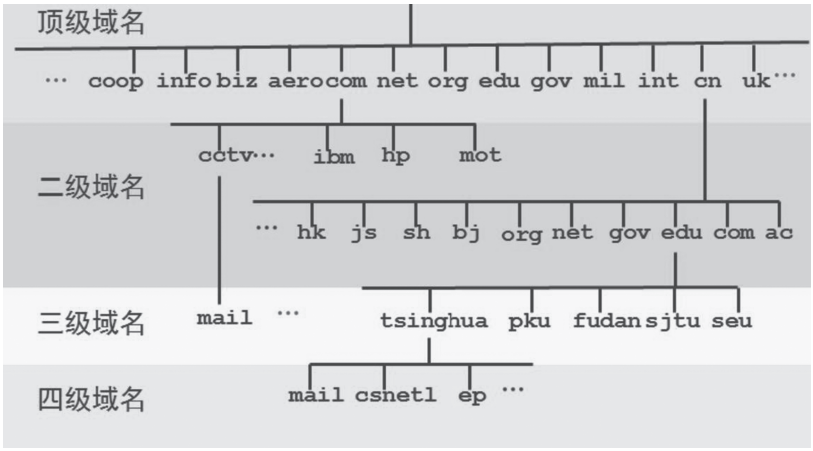


图 1-7　互联网的域名空间

笔记

（1）地理模式。顶级域名表示国家，次级域名表示该网络的属性，如表 1-2 所示。

表 1-2　域名的地理模式

顶级域名	所表示的国家或地区	顶级域名	所表示的国家或地区	顶级域名	表示的国家或地区
au	澳大利亚	ca	加拿大	ch	瑞士
cn	中国	cu	古巴	de	德国
dk	丹麦	es	西班牙	fr	法国
hk	中国香港	in	印度	it	意大利
jp	日本	mo	中国澳门	se	瑞典
sg	新加坡	tw	中国台湾	us	美国

（2）组织模式。在组织模式中，顶级域名表示该网络的属性，如表 1-3 所示。

表 1-3　域名的组织模式

顶级域名	表示的网络属性	顶级域名	表示的网络属性	顶级域名	表示的网络属性
com	营利的商业实体	mil	军事机构或组织	store	商场
edu	教育机构或设施	net	网络资源或组织	wb	和 WWW 有关的实体
gov	非军事性政府或组织	org	非营利性组织机构	arts	文化娱乐
int	国际性机构	firm	商业或公司	arc	消遣性娱乐

知识拓展

常见七类机构性顶级域名举例

COM（商业机构）：www.tom.com。
EDU（教育机构）：www.xidian.edu.cn；www.pku.edu.cn。
INT（国际机构）：www.who.int。
GOV（政府机构）：www.whitehouse.gov；www.gov.cn。
MIL（军事机构）：www.army.mil ；www.navy.mil。
NET（网络机构）：www.263.net。
ORG（社会团体、组织）：www.chinaembassycanada.org。

子任务 1.1.3　网络中数据包的传输

地址转换协议（Address Resolution Protocol，ARP）可当作底层协议，用于 IP 地址到物理地址的转换。在以太网中，所有对 IP 的访问最终都转化为对网卡 MAC 地址的访问。如果主机 A 的 ARP 列表中到主机 B 的 IP 地址与 MAC 地址对应不正确，由 A 发往 B 的数据包就会发向错误的 MAC 地址，当然无法顺利到达 B，结果是 A 与 B 根本不能进行通信。

笔记

1. A、B 在同一网段数据包传递

假设有两台计算机分别命名为 A 和 B，A 需要向 B 发送数据的话，A 主机首先把目标设备 B 的 IP 地址与自己的子网掩码进行“与”操作，以判断目标设备与自己是否位于同一网段内。如果目标设备在同一网段内，并且 A 没有获得与目标设备 B 的 IP 地址相对应的 MAC 地址信息，则源设备（A）以第二层广播的形式（目标 MAC 地址为全 1）发送 ARP 请求报文，在 ARP 请求报文中包含了源设备（A）与目标设备（B）的 IP 地址。同一网段中的所有其他设备都可以收到并分析这个 ARP 请求报文，如果某设备发现报文中的目标 IP 地址与自己的 IP 地址相同，则它向源设备发回 ARP 响应报文，通过该报文使源设备获得目标设备的 MAC 地址信息。为了减少广播量，网络设备通过 ARP 表在缓存中保存 IP 与 MAC 地址的映射信息。在一次 ARP 的请求与响应过程中，通信双方都把对方的 MAC 地址与 IP 地址的对应关系保存在各自的 ARP 表中，以在后续的通信中使用。ARP 表使用老化机制，删除在一段时间内没有使用过的 IP 与 MAC 地址的映射关系。一个最基本的网络拓扑结构如图 1-8 所示。

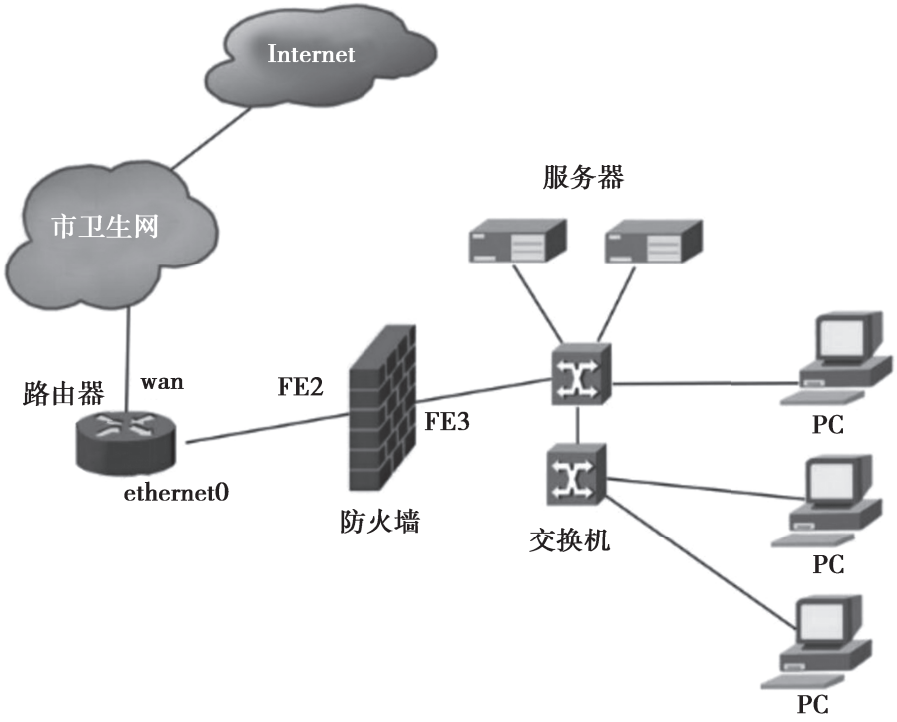


图 1-8　基本网络拓扑结构

如果中间要经过交换机的话，根据交换机的原理，它是直接将数据发送到相应端口，那么就必须保有一个数据库，包含所有端口所连网卡的 MAC 地址。它通过分析以太网（Ethernet）包的包头信息（其中包含源 MAC 地址、目标 MAC 地址、信息的长度等信息），取得目标 B 的 MAC 地址后，查找交换机中存储的地址对照表（MAC 地址对应的端口），确认具有此 MAC 地址的网卡连接在哪个端口上，然后将数据包发送到这个对应的端口，也就相应地发送到目标主机 B 上。这样一来，即使某台主机盗用了这个 IP 地址，但由于它没有这个 MAC 地址，因此也不会收到数据包。

2. A、B 在不同网段数据包传递

假设网络中要从主机 PC-A 发送数据包到 PC-C 主机中，如图 1-9 所示。

笔记

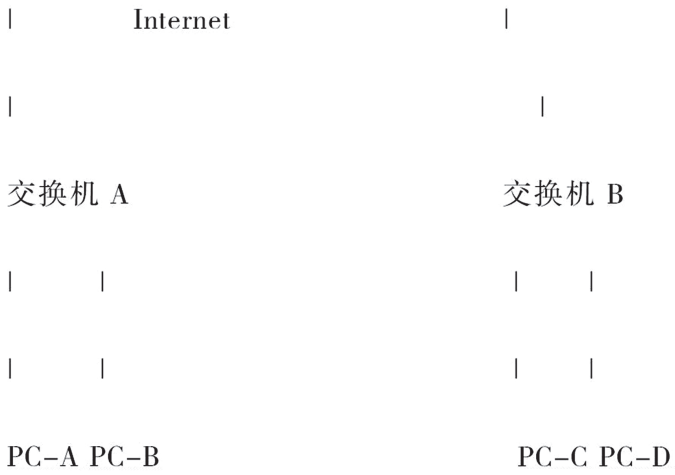


图 1-9　在不同网段数据包传递

PC-A 并不需要获取远程主机（PC-C）的 MAC 地址，而是把 IP 分组发向缺省网关，由网关 IP 分组完成转发过程。如果源主机（PC-A）没有缺省网关 MAC 地址的缓存记录，则它会通过 ARP 协议获取网关的 MAC 地址，因此在 A 的 ARP 表中只观察到网关的 MAC 地址记录，而观察不到远程主机的 MAC 地址。在以太网（Ethernet）中，一个网络设备要和另一个网络设备进行直接通信，除了知道目标设备的网络层逻辑地址（如 IP 地址）外，还要知道目标设备的第二层物理地址（MAC 地址）。ARP 协议的基本功能就是通过目标设备的 IP 地址，查询目标设备的 MAC 地址，以保证通信的顺利进行。数据包在网络中的发送是一个及其复杂的过程，图 1-9 只是一种很简单的情况，中间没有过多的中间节点，其实现实中只会比这个更复杂，但是大致的原理是一致的。

（1）PC-A 要发送数据包到 PC-C 的话，如果 PC-A 没有 PC-C 的 IP 地址，则 PC-A 首先要发出一个 DNS 的请求，路由器 A 或者 DNS 解析服务器会给 PC-A 回应 PC-C 的 IP 地址，这样 PC-A 关于数据包第三层的 IP 地址信息就全了。源 IP 地址：PC-A，目的 IP 地址：PC-C。

（2）接下来 PC-A 要知道如何到达 PC-C，然后，PC-A 会发送一个 ARP 的地址解析请求，发送这个地址解析请求，不是为了获得目标主机 PC-C 的 MAC 地址，而是把请求发送到了路由器 A 中，然后路由器 A 中的 MAC 地址会发送给源主机 PC-A，这样 PC-A 的数据包的第二层信息也全了。源 MAC 地址：PC-A 的 MAC 地址，目标 MAC 地址：路由器 A 的 MAC 地址。

（3）然后数据会到达交换机 A，交换机 A 看到数据包的第二层目标 MAC 地址，是去往路由器 A 的，就把数据包发送到路由器 A，路由器 A 收到数据包，首先查看数据包的第三层 IP 目的地址，如果在自己的路由表中有去往 PC-C 的路由，说明这是一个可路由的数据包。

（4）然后路由器进行 IP 重组和分组的过程。首先更换此数据包的第二层包头信息，路由器 PC-A 到达 PC-C 要经过一个广域网，在这里会封装很多广域网相关的协议，其作用也是为了找下一阶段的信息。同时对第二层和第三层的数据包重校验。把数据经过 Internet 发送出去。最后经过很多的节点发送到目标主机 PC-C 中。现在我们想一个问题，PC-A 和 PC-C 的 MAC 地址如果是相同的话，会不会影响正常的通信呢？答案是不会影响的，因为这两个主机所处的局域网被广域网分隔开了，通过对发包过程的分析可以看出

来，不会有任何的问题。而如果在同一个局域网中的话，那么就会产生通信的混乱。当数据发送到交换机时，这时的端口信息会有两个相同的 MAC 地址，而这时数据会发送到两个主机上，这样信息就会混乱。因此这也是保证 MAC 地址唯一性的一个理由。

笔记

任务 1.2　网络安全体系结构

子任务 1.2.1 网络安全体系结构的相关概念

网络协议是通信双方共同遵守的规则和约定的集合。网络协议包括以下三个要素。

（1）语法规定了信息的结构和格式。

（2）语义表明信息要表达的内容。

（3）同步规则涉及双方的交互关系和事件顺序。

整个计算机网络的实现体现为协议的实现。为了保证网络的各个功能的相对独立性，以及便于实现和维护，通常将协议划分为多个子协议，并且让这些协议保持一种层次结构。子协议的集合通常称为协议族。

无论是面对面还是通过网络进行的所有通信都要遵守预先确定的规则，即协议。这些协议由会话的特性决定。在日常的个人通信中，通过一种介质（如电话线）通信时采用的规则不一定与使用另一种介质（如邮寄信件）时的协议相同。网络中不同主机之间的成功通信需要在许多不同协议之间进行交互。执行某种通信功能所需的一组内在相关协议称为协议簇。这些协议通过加载到各台主机和网络设备中的软件和硬件执行。网络协议簇说明了以下过程。

（1）消息的格式或结构。

（2）网络设备共享通往其他网络的通道信息的方法。

（3）设备之间传送错误消息和系统消息的方式与时间。

（4）数据传输会话的建立和终止。

组成协议簇的许多协议通常都要参考其他广泛采用的协议或行业标准。标准是指已经受到网络行业认可并经过电气电子工程师协会（IEEE）或 Internet 工程任务组（IETF）之类标准化组织批准的流程或协议。 在协议的开发和实现过程中使用标准可以确保来自不同制造商的产品协同工作，从而获得有效的通信。如果某家制造商没有严格遵守协议，其设备或软件可能就无法与其他制造商生产的产品成功通信。

知识拓展

常用网络协议、服务及网络命令

常用网络协议：IP、TCP、UDP。

常用网络服务：活动目录、WWW 服务、电子邮件 、Telnet、FTP、DNS。

常用网络命令：ping 命令、at 命令、netstat 命令、tracert 命令、net 命令、ftp 命令、nbtstat 命令、telnet 命令。

笔记

子任务 1.2.2 网络安全体系结构的三维框架结构

计算机网络安全体系的框架结构对于体系的建设以及实行都有着极其重要的意义。然而框架的构建如果仅仅从一个角度出发，是难以完成的，需从较为全面的角度来考虑。我们从协议层次、安全服务、实体单元三个方面，全面地分析考虑体系框架的建立，其三维框架结构如图 1-10 所示。

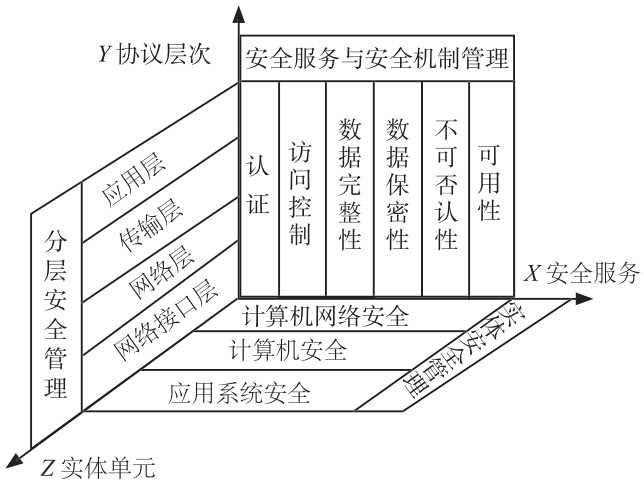


图 1-10　计算机网络安全体系的三维框架结构

子任务 1.2.3 安全服务之间的关系

信息安全服务是指适应整个安全管理的需要，为企业、政府提供全面或部分信息安全解决方案的服务。信息安全服务提供包含从高端的全面安全体系到细节的技术解决措施。

信息安全服务主要组成部分包括安全咨询、安全风险评估、安全加固服务、渗透测试服务、安全教育培训。

（1）安全咨询服务的发展趋势将向行业化的方向发展，针对性更强，咨询服务内容更细，具体会体现在政府、银行、企业等几个重点领域。咨询服务的内容将以行业特点为核心，从技术、运维、管理、策略等方面提供具有针对性的安全技术与管理咨询服务。

（2）安全风险评估服务是一项以安全性评估和改进为目标的咨询服务。通过对客户信息系统的安全调查，识别信息系统的关键资产、面临的威胁以及存在的脆弱性，量化分析客户信息系统中存在的安全风险，为客户提供风险控制及安全性改进的建议，并协助客户实施各项风险控制措施，以管理信息系统中存在的各种安全风险，如图 1-11 所示。

风险评估服务内容包括设施安全性评估、网络安全性评估、平台安全性评估、数据安全性评估、应用安全性评估、安全管理评估、综合的风险评估。

笔记

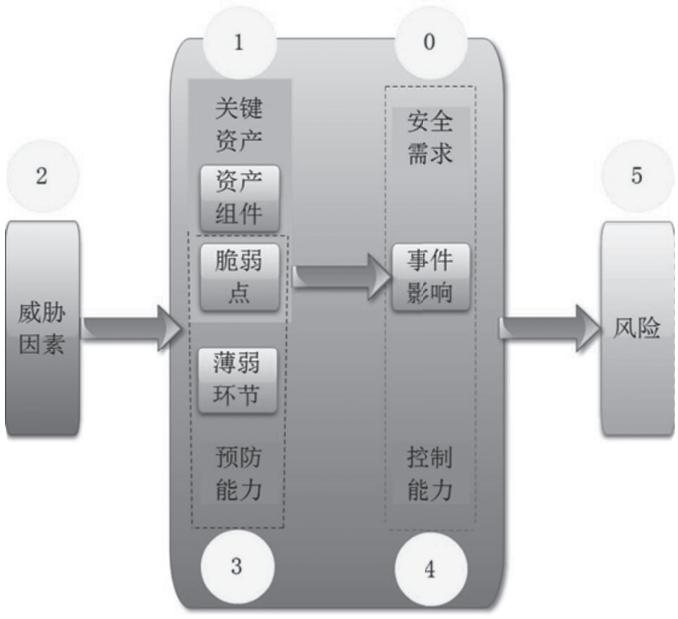


图 1-11　安全评估模型与方法

知识拓展

人工评估

人工评估内容包括系统补丁、系统账号、文件系统、网络及服务、系统配置文件、NFS 或其他文件系统共享、审计及日志、后门、入侵痕迹检测、分析；利用渗透测试技术，通过用户信息收集（包括用户名、密码长度、登录时间等），密码破解（猜测用户密码），溢出攻击（利用现有的弱点尝试获得主机的权限），网络信息收集（包括网络设备、拓扑结构的收集），最大限度地模拟网络在实际环境中对攻击的防御能力。

（3）安全加固。各种业务能否安全、稳定地运转取决于两点：一是最矮木板的高度，二是各块木板之间是否存在缝隙。安全加固是对信息系统中的主机系统（包括运行的软件系统）与网络设备的脆弱性进行分析并修补。安全加固包括了对主机系统的身份鉴别与认证、访问控制和审计跟踪策略的增强。安全加固的目标是解决目标系统在安全评估中发现的技术性安全问题，对系统性能进行优化配置，杜绝系统配置不当而出现的弱点。

知识拓展

安全加固的风险回避

安全加固的风险回避之加固时间安排：

①加固实施时间尽量安排在晚上或系统空闲时进行。

②加固实施时间可以在系统调优时进行，这样减少对系统的变更。

③如果两台或多台主机采用了高可用性措施（HA），如双机热备、集群、负载均衡，则可先加固一部分（或备机），待加固确认正常后，再加固另外一部分（主备方式的情况，先把主备关系切换）。

安全加固的风险回避之备份控制：加固前采取有效的备份措施。

安全加固的风险回避之备份控制人员安排：保证业务厂商联系畅通。

安全加固的风险回避之修补加固原则：不能影响目标系统所承载的业务运行；不能影响目标系统的自身性能；不能影响与目标系统以及与之相关的其他系统的安全性，也不能造成性能的明显下降。

笔记

（4）渗透测试服务是一种非常专业的安全服务，通过完全模拟黑客可能使用的漏洞发现技术和攻击技术，对目标系统的安全做深入的探测，发现系统最脆弱的环节。渗透测试能够让管理人员直观地知道自己网络所面临的问题。

（5）安全教育培训是企业安全管理的一项重要内容。通过安全知识教育和技能培训，使职工增强安全意识，熟悉和掌握有关的安全生产法律、法规、标准和安全生产知识和专业技术技能，熟悉本岗位安全职责，提高安全素质和自我防护能力，控制和减少违章行为，做到安全生产。

任务 1.3 网络安全防护中的防火墙

子任务 1.3.1 防火墙与网络层次的关系

防火墙可以工作在 TCP/IP 模型中的各层。

防火墙的主要工作在于实现访问控制策略，且所有防火墙均依赖于对 TCP/IP 各层协议所产生的信息流进行检查。一般说来，防火墙越是工作在协议的上层，其能够检查的信息就越多，也就能够获得更多的信息用于安全决策，因而检查的网络行为就可以越细致深入，提供的安全防护等级就越高。

子任务 1.3.2 攻击分层防护中的防火墙

作为网络安全的第一道防线，使用防火墙可以识别并阻挡许多黑客攻击行为。

1. 攻击发生过程中的防范

入侵检测系统（Intrusion Detection System，IDS）相对于传统意义的防火墙是一种主动防御系统，入侵检测作为安全的一道屏障，可以在一定程度上预防和检测来自系统内、外部的入侵。防火墙正在与 IDS、主机防护等安全设备融合，共同进行攻击发生过程中的防范。

2. 攻击发生后的应对

防火墙、IDS 等都提供详细的数据记录功能，可以对所有误操作的危险动作和蓄意攻击行为保留详尽的记录。这样可以在黑客攻击后通过这些记录来分析黑客的攻击方式，弥补系统漏洞，防止再次遭受攻击，并可进行黑客追踪和查找责任人。此外，应急响应、灾难备份与恢复和安全管理等，都是网络攻击发生后的常用应对方法。