第 1 章

计算机网络安全与管理任务分析

任何一个实际运行的计算机网络系统，特别是较大型的企业网络系统，为保证其安全、可靠地运行，必须建立相应的网络安全与管理方案，以减少各种潜在网络安全风险和网络性能瓶颈对信息系统正常运行的影响。本书以一个典型的跨地区公司网络系统为例，按照实际网络工程项目过程，先分析其中所需解决的网络安全与管理问题，然后介绍解决这些问题所需的知识和技术，最后给出这些问题的相应的解决方案。

1.1 公司网络环境

1.1.1 企业网络应用概况

某大型新兴产业公司为提高生产效率，拟新建联通各地分公司的计算机网络。该公司的总公司及其直属 3 个分支机构在 A 市，并在 B 市和 C 市分别设有一个子公司和两个分支机构。总公司和分公司主要负责产品的研发和生产，设有管理部门、研发部门、市场部门、售后服务部门和生产部门。各分支机构主要负责产品销售和售前、售后服务，设有市场部门、售后服务部门和管理部门。

公司所建网络将主要承载公司内部 OA、邮件、FTP、远程教育等系统和面向公众提供服务的电子商务网站系统。受业务发展、系统性能等诸多方面因素影响，以上网络应用系统设计在总公司、分公司分别设有网络应用及数据库服务器，而在分支机构只设网络终端。

1.1.2 企业网络拓扑结构

全公司的网络拓扑结构如图 1-1 所示。总公司与分公司利用电信专线互联，而为节约线路成本，总/分公司与其下属分支机构通过宽带线路接入本地 Internet 实现互联。

总公司局域网的网络拓扑结构按照网络应用需求分为核心、汇聚、接入 3 层，图 1-2 为总公司局域网的网络拓扑结构示意图。为了保证系统的安全可靠性，在各交换机上使用了双冗余线路设计。

分公司在局域网结构、链路冗余等方面与总公司类似。但分支机构 B-1、C-1 网络规模较大，而分支机构 B-2、C-2 网络规模较小，分支机构的网络拓扑结构如图 1-3 所示。

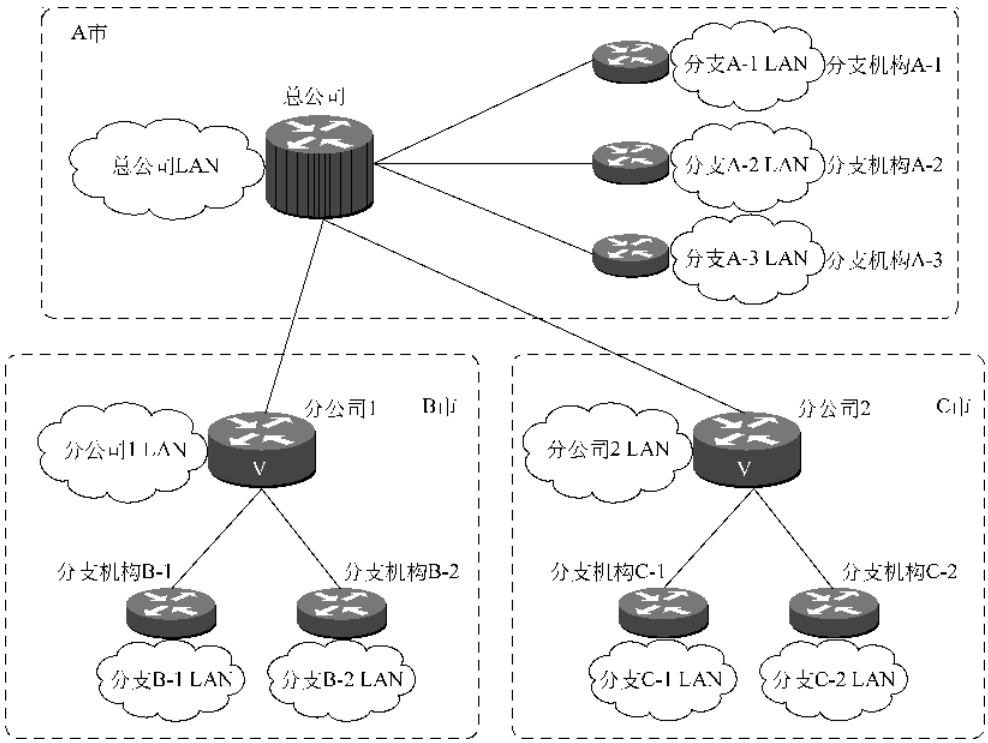

图 1-1　公司网络结构示意图

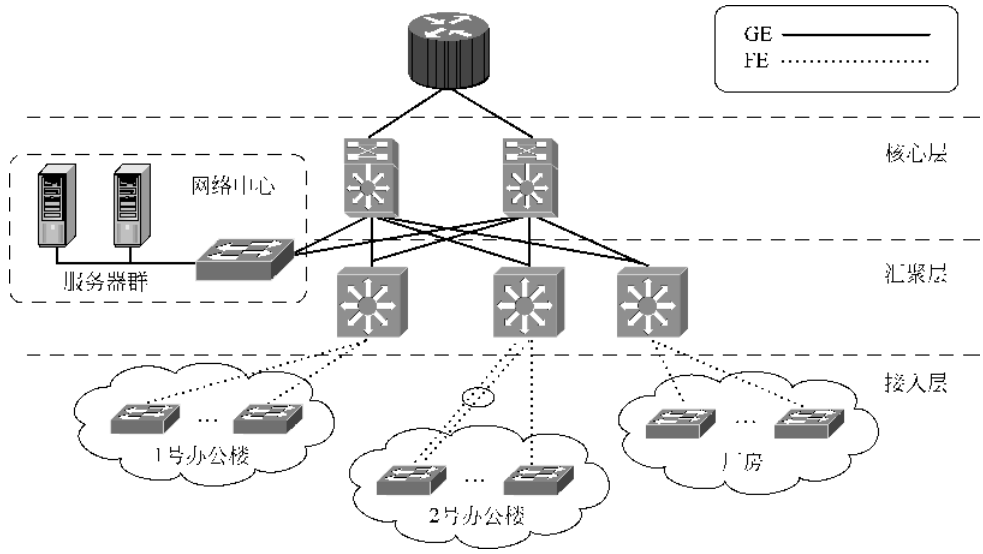

图 1-2　总公司网络拓扑结构图

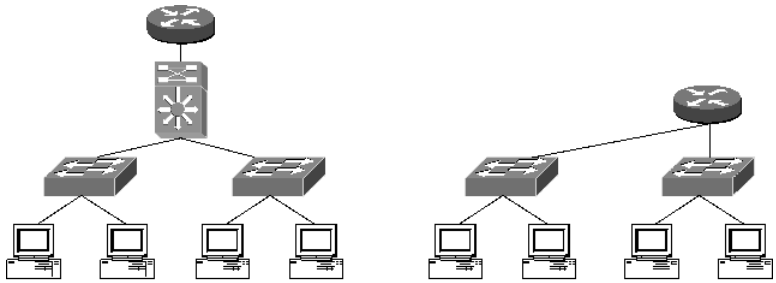

图 1-3　分支机构网络拓扑结构图

1.2　模拟公司网络安全及管理需求

1.2.1　模拟公司的网络安全管理需求

目前计算机网络面临着多方面的安全威胁，例如，物理安全威胁、网络通信威胁、网络服务威胁、网络管理威胁等，模拟公司网络也不能例外。本书将重点讨论如何解决网络通信安全威胁问题，其他方面的解决方法可参考本系列教材中的《计算机网络集成技术》和《网络操作系统》两书。

从模拟公司网络环境和业务需求分析可以发现，要保证该网络安全运行，需要解决以下网络安全问题。

（1）由于连接到 Internet，所以必须解决来自 Internet 的网络入侵和攻击问题。

（2）模拟公司与分支机构间使用 Internet 线路通信，必须解决通信数据安全问题。

（3）由于公司租用的 IP 地址有限，随着企业网络规模发展，必须解决公司网络中 IP 地址资源不足的问题。

（4）模拟公司网络不是单纯的生产网络，办公局域网的接入，使得网络管理人员必须面对局域网中各种潜在安全威胁，如病毒问题、非授权访问网络资源问题、非授权变更网络结构等。

1.2.2　模拟公司的网络管理需求

要保证模拟公司网络安全、可靠运行，必须对网络进行管理和维护。在网络管理过程中，需要解决以下问题。

（1）根据网络需求变化，使用工具对网络进行配置、调整。

（2）当网络发生故障时，能够发现、跟踪故障现象，记录故障状态信息，分析故障原因，解决网络故障。

（3）监控、记录网络性能变化；根据网络需求适当调整网络，以提高网络性能。

（4）监控、记录网络受到安全威胁的情况，检查网络可能存在的安全漏洞或隐患，并通过访问控制等手段对网络的薄弱环节进行改善。

1.3 网络安全及管理实验环境

本书将根据以上网络安全及管理方案基本设计思路，逐个解决模拟公司网络中的安全及管理方面的问题，介绍相关知识，提出解决方案，完成相应系统配置。在课程学习过程中，可在如图 1-4 所示实验环境中进行相应配置，测试网络安全及管理方案的可行性。

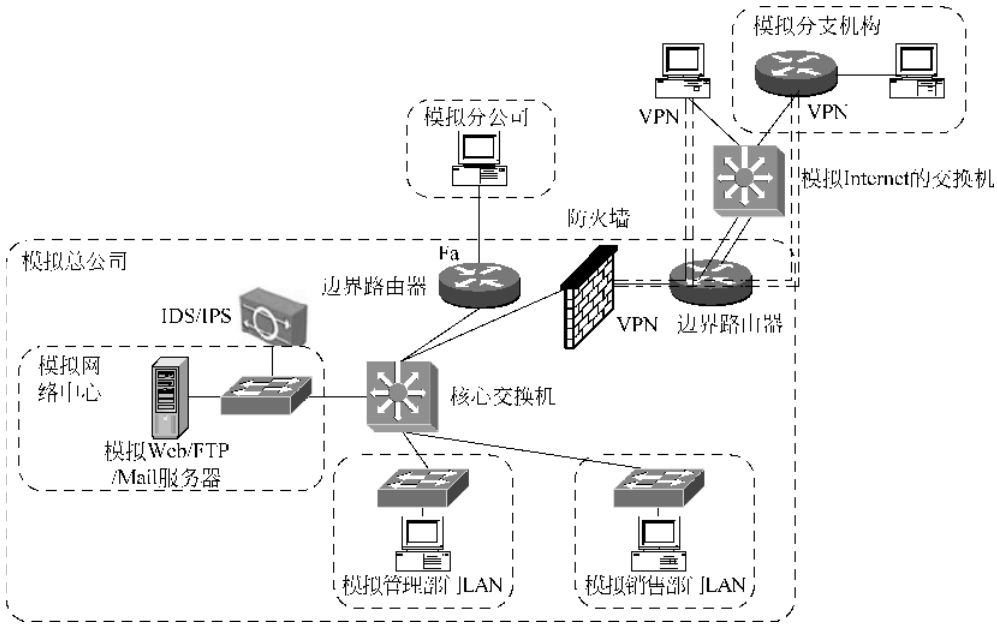

图 1-4 实验网络拓扑结构图

图 1-4 所示的实验网络拓扑可使用实际网络设备实现，也可使用模拟器软件实现。为便于实验，简化与网络安全、管理无关的内容，网络中广域网线路可使用以太网线路或串行口的背对背线路进行模拟；图中的 IDS/IPS 设备也可使用安装 IDS 软件的计算机模拟。

该模拟网络实验环境的硬件系统包括如下内容。

(1) 防火墙。

(2) IDS 设备(可选)。

(3) 路由器。

(4) 二层、三层交换机。

(5) PC。

该模拟网络实验环境的软件系统包括如下内容。

(1) Web、FTP、Mail 服务软件。

(2) IDS 软件。

(3) VPN 客户端软件。

(4) 网络管理软件，例如 PRTG 等。

(5) 网络攻击软件，例如 Smurf 等。

第 2 章

访问控制列表技术

本章任务：根据工程任务安全需求分析，解决网络边界访问控制配置问题。

必备知识：(1) 无状态访问控制列表技术。

(2) 有状态访问控制列表技术。

(3) 基于上下文的访问控制列表技术。

学习目标：利用访问控制列表技术完成模拟公司分支机构网络边界访问控制配置，防御外网攻击。

2.1 模拟公司分支机构网络边界安全任务分析

2.1.1 模拟公司分支机构网络边界安全风险分析

如图 2-1 所示，模拟公司各分支机构网络通过 Internet 与模拟公司其他网络相连，各分支机构网络内设有可 24 小时连接到 Internet 的邮件服务器，周一至周五使用端口 3000～3010 通过 Internet 连接总/分公司的应用服务器，24 小时可通过 Internet SSH 连接远程管理的网络设备。由于 Internet 的开放性，各分支机构网络面临以下安全风险。

1. 恶意用户对分支网络进行的勘测攻击

勘测攻击是一种对网络进行扫描或窃听，试图获得网络拓扑、网络中主机或网络设备运行应用软件情况的攻击方式，它往往是恶意用户对网络实施攻击的前奏。勘测攻击的两种常见类型是扫描和窃听。

常见扫描攻击包括 IP 地址扫描和端口扫描。通过 ping 网络的直接广播地址或者 ping 网络中每个 IP 地址，恶意用户就可以对网络实施 IP 地址扫描；而一些常用端口扫描工具，也可以通过测试是否可以与网络中主机建立各类服务连接来探测主机上打开的网络服务端口情况。

勘测攻击的另一种类型是窃听攻击。恶意用户可以通过各类嗅探、监听软件，从网络流量中窃取用户账户等信息。但此类攻击一般只能在本地网络中实施。恶意用户往往通过先攻陷网络内部一台主机，然后在这台主机上运行嗅探、监听软件，来进行此类攻击。

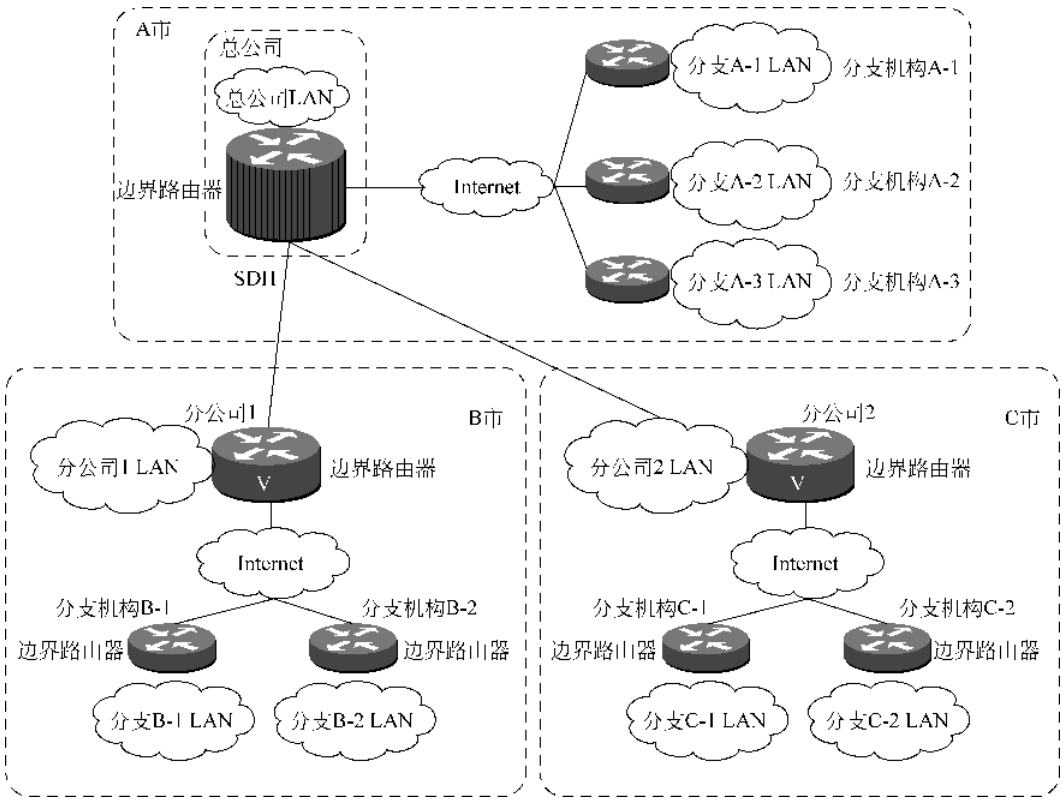

图 2-1 模拟公司网络间连接拓扑示意图

2. 恶意用户对分支网络进行的访问攻击

访问攻击常见类型包括未授权访问攻击、数据操纵攻击、会话攻击等。

(1) 未授权攻击是指通过口令暴力破解、社会工程学窃取口令等试图获得访问网络权利的攻击方式。

(2) 数据操纵攻击是指对网络服务提供的数据内容进行修改,例如改变网页内容,嵌入非法插件、Java 小程序等。

(3) 会话攻击是指在会话层实施的网络攻击,主要类型包括会话欺骗攻击、会话重放攻击、会话劫持攻击。

① 会话欺骗攻击是指通信会话中假冒其他 IP 地址的攻击行为,如图 2-2 所示。据统计,大约 65%的会话欺骗攻击使用 bogon 地址(即未被分配的地址),包括保留地址、私有 IP 地址等; 另外恶意用户常假冒内网合法主机发动会话欺骗攻击。

② 会话重放攻击是指通过监听网络中某台主机的数据报文信息,然后伪造数据报文发送给该主机的攻击行为。例如,恶意用户可以监听用户在线交易信息,然后伺机发送假冒信息给用户,误导用户登录假冒在线交易、网上银行网站。会话重放攻击如图 2-3 所示。

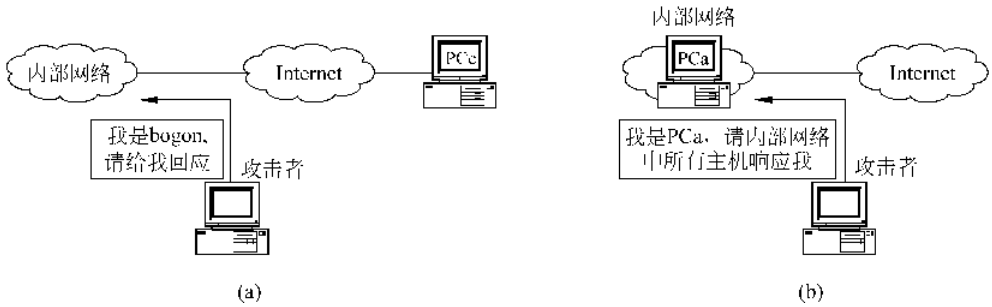

图 2-2　会话欺骗攻击示意图

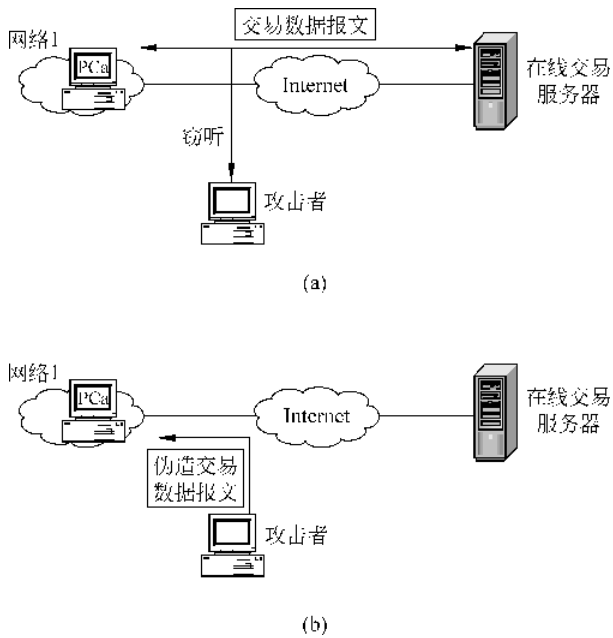

图 2-3　会话重放攻击示意图

③ 会话劫持攻击是指恶意用户拦截网络中会话信息，假扮通信双方发送虚假信息的攻击行为，如图 2-4 所示。

3. 恶意用户对分支网络进行的 DoS 攻击

恶意用户通过向网络中的网络设备、主机发送大量消耗、占用其资源的流量，使得网络、网络设备、主机无法进行正常通信的攻击行为，称为 DoS(Deny of Service)攻击。

TCP SYN 洪水攻击是一种利用 TCP 协议安全漏洞进行的 DoS 攻击，恶意用户利用 TCP 连接建立过程中“三次握手”的安全漏洞，向被攻击者发送大量连接建立请求，由于 TCP 协议需要等待接收到后续响应报文才能完成连接建立过程，大量连接建立请求会导致被攻击者大量资源被占用，无法进行正常通信。

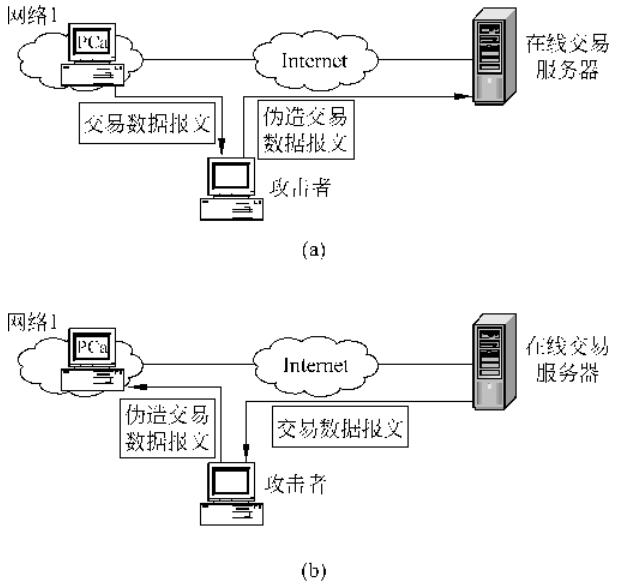

图 2-4 会话劫持攻击示意图

Smurf 攻击是一种利用 ICMP 报文洪水进行的 DoS 攻击。恶意用户可假冒被攻击主机向某网络广播地址发送 ICMP echo 报文，由于每个目的网络主机都向被攻击主机返回 ICMP reply 报文，所以会导致被攻击主机 CPU 和网络带宽被大量占用而不能再正常提供服务。

4. 恶意用户对分支网络进行的 DDoS 攻击

DDoS(Distributed Denial of Service)攻击即分布式拒绝服务攻击，是从多个源头发动 DoS 攻击的攻击方式。恶意用户往往先通过其他手段攻陷若干防御薄弱的主机，在其上安装可以远程控制的攻击程序，使其成为“肉机”，然后再控制这些“肉机”向网络上的合法服务器发动 DoS 攻击。由于发出 DoS 攻击洪水的“肉机”位置比较分散，因此极大增加了防御该类攻击的难度。例如 TFN、TFN2K、Trinoo、特洛伊木马等。

目前防范 DoS 攻击和 DDoS 攻击的手段主要有两种：控制流量大小、禁止来自 Internet 可能对内部网络造成攻击的流量。

例如，可以通过限制来自 Internet 的 ICMP 报文进入内部网络来防范 Smurf；也通过限制 Internet 对内部网络主机的主动 TCP 连接，来防范 TCP SYN 等。

虽然 DDoS 攻击比 DoS 攻击更难防御，但大部分 DDoS 程序都有各自通信特征的特点。例如，DDoS 程序 TFN 使用 ICMP echo-reply 消息来传递“攻击指令”；DDoS 程序 Trinoo 使用比较固定的端口，如 TCP 和 UDP 的 1524、27444、27665、31335 进行通信；DDoS 程序 Trinity 使用 IRC 通信来传送攻击命令；特洛伊木马使用一些特定端口通信。

因此，如果内部网络不需要提供以上端口的网络服务，就可以在网络边界上过滤以上特定端口的流量，从而减少遭遇网络攻击的风险。

2.1.2　模拟公司分支机构网络边界安全配置方案

在边界路由器上配置访问控制列表是保护内部网络防御以上安全风险的主要手段之一。但并不是所有路由器都支持高级访问控制列表技术，因此根据模拟公司各分支机构实际配置情况，对于使用中高端路由器的分支机构可以选用方案 1 来配置边界路由器，而使用低端路由器的分支机构可以选用方案 2 来配置边界路由器。

方案 1

(1) 在网络边界上配置基于上下文的访问控制列表 CBAC(Context-based Access Control)，过滤来自 Internet 到内网主机或服务器的所有 ICMP echo 报文，来防御利用 ping 进行的扫描攻击。

(2) 在网络边界上配置标准访问控制列表，过滤所有来自 Internet 的源地址为 bogon 地址或内网地址的访问，防御 IP 欺骗攻击。

(3) 在网络边界上配置基于上下文的访问控制列表，防范 DoS 攻击。

- 限制来自 Internet 的 ICMP 报文进入内部网络，以防范 Smurf。
- 限制 Internet 对分支机构网络主机的主动 TCP 连接、UDP 连接，来防范 TCP SYN 等。

(4) 在网络边界上配置扩展访问控制列表，防范使用特定协议消息、特定端口的 DDoS 攻击。

- 阻塞 ICMP echo-reply 消息，以抵御 TFN 攻击。
- 禁止 TCP 和 UDP 1524、27444、27665、16660、65000、31335 端口的流量，以防御 Trinoo 等 DDoS 攻击。
- 禁止 TCP 端口 6665～6669 的 IRC 流量以防御 Trinity 攻击。
- 禁止常见特洛伊木马使用的特定端口。

方案 2

对于那些不支持 CBAC 功能的路由器，配置反射访问控制列表作为替补方案。

(1) 在网络边界上配置反射访问控制列表，过滤来自 Internet 到内网主机或服务器的所有 ICMP echo 报文，来防御利用 ping 进行的扫描攻击。

(2) 在网络边界上配置标准访问控制列表，过滤所有来自 Internet 的源地址为 bogon 地址或内网地址的访问，防御 IP 欺骗攻击。

(3) 在网络边界上配置基于上下文的访问控制列表，防范 DoS 攻击。

- 限制来自 Internet 的 ICMP 报文进入内部网络，以防范 Smurf。
- 限制 Internet 对分支机构网络主机的主动 TCP 连接、UDP 连接，来防范 TCP SYN 等。

(4) 在网络边界上配置扩展访问控制列表，防范使用特定协议消息、特定端口的 DDoS 攻击。

- 阻塞 ICMP echo-reply 消息，以抵御 TFN 攻击。
- 禁止 TCP 和 UDP 1524、27444、27665、16660、65000、31335 端口的流量，以防御 Trinoo 等 DDoS 攻击。
- 禁止 TCP 端口 6665～6669 的 IRC 流量以防御 Trinity 攻击。

- 禁止常见特洛伊木马使用的特定端口。

方案 1 和方案 2 中提及的 bogon 地址，可以检索 http://www.cymru.com/Documents/bogon-dd.html 网页获得；常见木马端口可从 http://www.neohapsis.com/neolabs/neo-ports/neo-ports.html 获得。表 2-1 显示了截至 2009 年 8 月 Internet 上的 bogon 地址。

表 2-1 bogon 地址示例

网络地址	子网掩码	网络地址	子网掩码
0.0.0.0	254.0.0.0	100.0.0.0	252.0.0.0
2.0.0.0	255.0.0.0	104.0.0.0	252.0.0.0
5.0.0.0	255.0.0.0	127.0.0.0	255.0.0.0
10.0.0.0	255.0.0.0	169.254.0.0	255.255.0.0
14.0.0.0	255.0.0.0	172.16.0.0	255.240.0.0
23.0.0.0	255.0.0.0	176.0.0.0	254.0.0.0
27.0.0.0	255.0.0.0	179.0.0.0	255.0.0.0
31.0.0.0	255.0.0.0	181.0.0.0	255.0.0.0
36.0.0.0	254.0.0.0	185.0.0.0	255.0.0.0
39.0.0.0	255.0.0.0	192.0.2.0	255.255.255.0
42.0.0.0	255.0.0.0	192.168.0.0	255.255.0.0
46.0.0.0	255.0.0.0	198.18.0.0	255.254.0.0
49.0.0.0	255.0.0.0	223.0.0.0	255.0.0.0
50.0.0.0	255.0.0.0	224.0.0.0	224.0.0.0

2.2 访问控制列表的基础知识

2.2.1 访问控制列表的概念

访问控制列表(Access Control List，ACL)是一种过滤工具，普遍用于各种网络设备(路由器、交换机、防火墙等)中。

ACL 工作的基本原理如下。

- 定义一个访问控制列表，该访问控制列表包含一组过滤条件。
- 在网络设备接口、线路上，应用该访问控制列表对“进/出”该接口的流量进行过滤。

一个访问控制列表中包含一组命令(或称过滤条目、访问控制语句)，每条命令典型结构为：

permit | **deny** 匹配条件

即“允许”(permit)或“拒绝”(deny)符合“匹配条件”的流量通过网络设备接口。

其中“匹配条件”部分可以包含多种信息。

- 源地址或目的地址(可以是 IP、MAC 等)。
- 第 2 层协议信息，例如以太网帧类型。