ICS 35.020
L 80

中华人民共和国国家标准

GB/T 25068.3—2010/ISO/IEC 18028-3:2005

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

Information technology—Security techniques—IT network security—Part 3:Securing communications between networks using security gateways

(ISO/IEC 18028-3:2005,IDT)

2010-09-02 发布　　2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB/T 25068 在《信息技术　安全技术　IT 网络安全》总标题下，拟由以下 5 个部分组成：

——第 1 部分：网络安全管理；

——第 2 部分：网络安全体系结构；

——第 3 部分：使用安全网关的网间通信安全保护；

——第 4 部分：远程接入的安全保护；

——第 5 部分：使用虚拟专用网的跨网通信安全保护。

本部分为 GB/T 25068 的第 3 部分。

本部分使用翻译法等同采用国际标准 ISO/IEC 18028-3:2005《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》(英文版)。根据 GB/T 1.1—2000 的规定，做了如下一些编辑性修改：

——第 2 章中增加了引用文件“ISO/IEC TR 15947”；

——在 3.6 中对“内容过滤”加以说明，并在 6.5 中补充了内容过滤的内容“关键字过滤”，为今后技术发展预留了空间；

——删除了第 4 章中缩略语 S/MIME 英文名称中的“protocol”，以与 GB/T 25068.4—2010 中 2.34定义的同一术语 S/MIME 统一。另外，增加了一些缩略语，增加的缩略语在所在页边的空白处用单竖线“|”标出。

本部分由全国信息安全标准化技术委员会(TC 260)提出并归口。

本部分起草单位：黑龙江省电子信息产品监督检验院、中国电子技术标准化研究所、哈尔滨工程大学、北京励方华业技术有限公司、山东省标准化研究院。

本部分主要起草人：王希忠、张国印、李健利、王向辉、黄俊强、马遥、方舟、王大萌、树彬、张清江、王智、许玉娜、刘亚东、邱意民、王运福。

引　言

通信和信息技术业界一直在寻找经济有效的全面安全解决方案。安全的网络应受到保护，免遭恶意和无意的攻击，并且应满足业务对信息和服务的保密性、完整性、可用性、抗抵赖、可核查性、真实性和可靠性的要求。保护网络安全对于适当维护计费或使用信息的准确性也是必要的。产品的安全保护能力对于全网的安全(包括应用和服务)是至关重要的。然而，当更多的产品被组合起来以提供整体解决方案时，互操作性的优劣将决定这种解决方案的成功与否。安全不仅是对每种产品或服务的关注，还必须以促进全面的端到端安全解决方案中各种安全能力交合的方式来开发。因此，GB/T 25068 的目的是为 IT 网络的管理、操作和使用及其互连等安全方面提供详细指南。组织中负责一般 IT 安全和特定 IT 网络安全的人员应能够调整 GB/T 25068 中的材料以满足他们的特定要求。GB/T 25068 的主要目标如下：

——GB/T 25068.1 定义和描述网络安全的相关概念，并提供网络安全管理指南——包括考虑如何识别和分析与通信相关的因素以确立网络安全要求，还介绍可能的控制领域和特定的技术领域(在 GB/T 25068 的后续部分中涉及)；

——GB/T 25068.2 定义一个标准的安全体系结构，它描述一个支持规划、设计和实施网络安全的一致框架；

——GB/T 25068.3 定义使用安全网关保护网络间信息流安全的技术；

——GB/T 25068.4 定义保护远程接入安全的技术；

——GB/T 25068.5 定义对使用虚拟专用网(VPN)建立的网络间连接进行安全保护的技术。

GB/T 25068.1 与涉及拥有、操作或使用网络的所有人员相关。除了对信息安全(IS)和/或网络安全及网络操作负有特定责任的，或对组织的全面安全规划和安全策略开发负有责任的管理者和管理员外，还包括高级管理者和其他非技术性管理者或用户。

GB/T 25068.2 与涉及规划、设计和实施网络安全体系结构方面的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

GB/T 25068.3 与涉及详细规划、设计和实施安全网关的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

GB/T 25068.4 与涉及详细规划、设计和实施远程接入安全的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

GB/T 25068.5 与涉及详细规划、设计和实施 VPN 安全的所有人员(例如 IT 网络管理者、管理员、工程师和 IT 网络安全主管)相关。

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

1　范围

GB/T 25068的本部分规定了各种安全网关技术、组件和各种类型的安全网关体系结构。它还提供安全网关的选择和配置指南。

尽管个人防火墙使用类似的技术,但因为它不作为安全网关使用,所以它不在本部分的范围之内。

本部分适用于技术和管理人员,例如IT管理者、系统管理员、网络管理员和IT安全人员。本部分提供的指南有助于用户正确地选择最能满足其安全要求的安全网关体系结构类型。

2　规范性引用文件

下列文件中的条款通过GB/T 25068的本部分的引用而成为本部分的条款。凡是注日期的引用文件,其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本部分,然而,鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件,其最新版本适用于本部分。

GB/T 25068.4　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(GB/T 25068.4—2010,ISO/IEC 18028-4:2005,IDT)

ISO/IEC TR 15947　信息技术　安全技术　IT入侵检测框架

3　术语和定义

下列术语和定义适用于本部分。

3.1

报警　alert

“即时”指示信息系统和网络可能受到攻击或因意外事件、故障或人为错误而处于危险之中。

3.2

攻击者　attacker

故意利用技术性和非技术性安全控制措施的脆弱性,以窃取或损害信息系统和网络,或者损害合法用户对信息系统和网络资源可用性的任何个人。

3.3

审计　audit

依照期望对事实进行的正规调查、正规检验或验证,以确认它们之间的符合性和一致性。

3.4

审计日志　audit logging

为了评审和分析以及持续监视而收集有关信息安全事态的数据。

3.5

非军事区　demilitarised zone;DMZ

插在网络之间作为“中立区”的安全主机或小型网络(也称为屏蔽子网或边界网络)。

注:它形成一个安全缓冲区。

3.6

过滤 filtering

根据指定的准则，接受或拒绝数据流通过网络的过程。

注：内容过滤是对网络内容进行监控，防止某些特定内容在网络上进行传输的技术，如关键字过滤。

3.7

防火墙 firewall

设置在网络环境之间的一种安全屏障。它由一台专用设备或若干组件和技术的组合组成。网络环境之间两个方向的所有通信流均通过防火墙，并且只有按照本地安全策略定义的、已授权的通信流才允许通过。

3.8

信息安全事件 information security incident

单独的或一系列有害或意外的信息安全事态，它们极有可能危害业务运作和威胁信息安全。

注：见 GB/Z 20985。

3.9

信息安全事件管理 information security incident management

响应和处理信息安全事态和事件的正规过程。

注：见 GB/Z 20985。

3.10

入侵 intrusion

对网络或连接到网络的系统的未授权访问，即对信息系统进行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对信息系统内资源的未授权使用。

3.11

入侵检测 intrusion detection

检测入侵的正规过程，其一般特征为采集如下知识：异常使用模式，以及已被利用的脆弱性的类型和利用方式（包括何时发生及如何发生）。

3.12

入侵检测系统 intrusion detection system；IDS

用于识别某一入侵已被尝试、正在发生或已经发生，并可能对 IT 系统和网络中的入侵做出响应的技术系统。

3.13

端口(1) port(1)

连接的端点。

3.14

端口(2) port(2)

TCP 或 UDP 连接的〈互联网协议〉逻辑信道端点。

注：基于 TCP 或 UDP 的应用协议通常分配默认端口号，例如，HTTP 协议的端口 80。

3.15

隐私 privacy

每个人都享有的不公开处理他/她的私人和家庭生活、居所和通信的权利。

注：隐私不得受到当局干涉，而在依照法律，且对于国家安全、公共安全或国家经济稳定，或者对于防止动乱或犯罪、保护健康或道德，或者对于保护他人的权利和自由有必要时除外。

3.16

远程接入 remote access

从另一网络或从一个正在访问但非永久连接到网络的终端设备来访问网络资源的过程。

3.17

路由器 router

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

注：路由信息被保存在路由表中。

3.18

安全维 security dimension

为处理特定网络安全方面而设计的安全控制措施集。

注：安全维的详细描述见 GB/T 25068.2。

3.19

安全域 security domain

遵从于共同安全策略的资产和资源的集合。

3.20

安全网关 security gateway

网络之间或网络内子部分之间或不同安全域内的软件应用之间的连接点，旨在按照给定的安全策略保护网络。

注：安全网关不仅包括防火墙，而且还包括可提供访问控制和加密(可选)功能的路由器和交换机。

3.21

欺骗 spoofing

假冒成合法的资源或用户。

3.22

交换机 switch

利用内部交换机制来提供联网设备之间连通性的设备。

注 1：交换机不同于其他局域网互联设备(例如集线器)，其原因是交换机中使用的技术是在点对点的基础上建立连接。这就确保网络通信流只对有地址的网络设备可见，并使几个连接能够并存。

注 2：交换技术能在 OSI 参考模型(GB/T 9387.1)的第 2 层或第 3 层实现。

3.23

虚拟专用网 virtual private network

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。

4 缩略语

API	应用程序接口(Application Program Interface)
BGP	边界网关协议(Border Gateway Protocol)
DLL	动态链接库(Dynamic Link Library)
ICMP	互联网控制报文协议(Internet Control Message Protocol)
IDP	入侵检测防护(Intrusion Detection Prevention)
IT	信息技术(Information Technology)
NFS	网络文件传输(Network File Transfer)
NIS	网络信息系统(Network Information System)

NNTP	网络新闻传输协议(Network News Transfer Protocol)
NTP	网络时间协议(Network Time Protocol)
OSPF	开放式最短路径优先(Open Shortest Path First)
RIP	路由信息协议(Routing Information Protocol)
RPC	远程过程调用(Remote Procedure Call)
SHTTP	安全超文本传输协议(Secure Hypertext Transfer Protocol)
SOAP	简单对象访问协议(Simple Object Access Protocol)
S/MIME	安全多用途互联网邮件扩展(Secure Multipurpose Internet Mail Extensions)
SPAN	交换端口分析器(Switched Port Analyzer)
TCP-SYN	传输控制协议,同步(Transmission Control Protocol,SYNchronisation)
V.35	高速同步数据交换协议(high-speed synchronous data exchange protocol)
VLAN	虚拟局域网(Virtual Local Area Network)
VPN	虚拟专用网(Virtual Private Network)
WAIS	广域信息服务(Wide Area Information Service)
X.11	图形用户界面协议(graphical user interface protocol)
XML	可扩展置标语言(Extensible Mark-up Language)

5 安全要求

按照文档化的安全策略,安全网关的适当部署宜保护组织的内部系统,并安全地管理和控制通过它的通信流。

安全网关控制对网络(OSI模型第2、3和4层)或应用(OSI模型第4层至第7层)的访问。包含防火墙在内的安全网关实例用于保护:

- 内部组织网络免受来自互联网的威胁;
- 两个内部组织网络免受彼此之间的威胁;
- 内部组织网络免受来自外部组织网络的威胁。

安全网关用于满足以下安全要求:

- 分隔逻辑网络;
- 对逻辑网络之间流经信息提供限制和分析功能;
- 通过连接检测或所选应用上的代理操作来提供对出入组织网络的访问进行控制的手段;
- 提供可控可管的网络单一进入点;
- 强化组织对网络连接的安全策略;
- 提供日志的单一记录点;
- 提供网络地址转换以隐藏内部网络;
- 提供端口映射(包括动态端口开启)和应用级攻击检测与保护(包括内容过滤)。

6 安全网关技术

从简单的包过滤开始,安全网关中所使用的更多技术方法已逐渐发展到包括诸如应用代理和状态包检测之类的技术。此外,网络地址转换和内容过滤也在本章介绍,因为这些技术经常与安全网关结合使用。

6.1 包过滤

包过滤是指通过将每个入站包或出站包的包头信息与访问控制规则列表进行比较,确定阻止或放行网络通信流。这种过滤设备在每个包进入时单独查看其包头,并将源和目的的IP地址及端口与其规则库进行比较。如果其地址和端口信息是许可的,则该包进而直接穿越防火墙到达目的地。如果包未

通过该测试，它就被丢弃。

可以选择性地检查IP包，以确认2台主机或2个网络之间的数据流是否应允许通过。决定允许或拒绝这种数据流通过所依据的准则包括：

- IP源地址；
- IP目的地址；
- 协议(例如TCP、UDP、ICMP)；
- 源端口；
- 目的端口；
- 通信方向(入站、出站)。

包过滤网关速度快，是因为它运行在网络层和传输层，且仅对给定连接的有效性进行粗略的检查。

6.2 状态包检测

基于包过滤技术，状态包检测方法增加了更多的安全检查，以便模拟应用代理防火墙的安全检查。状态包检测防火墙在网络层截取入站包直到它具有足够的信息来对上层尝试连接的状态作出某种判定，而不是简单地单独查看每个入站包的地址。然后这些包在置于操作系统内核的专有检测模块中被检测。安全判定所需的状态相关信息在这种检测模块中被检验，并被保留在动态状态表中用于评测后续的连接尝试。被清理过的包便被转发到防火墙之内，允许内部系统和外部系统之间直接联系。

因为大多数检验发生在内核，所以状态包检测防火墙经常比应用代理防火墙快。尽管状态包检测方法已显著增强了简单包过滤防火墙的安全，但是，在需要将包收集到诸如URL或文件之类较大单元时，它不能对其进行安全检查。尽管如此，它必须在没有协议栈应用层信息的情况下能像应用代理那样做出安全决定。

具有状态检测功能的包过滤仍允许外部用户直接访问业务应用程序和系统，这些业务应用程序和系统很可能安装了配置不当、具有众所周知的安全脆弱性的操作系统。应用代理通过将对应用程序或计算机系统的访问限制在其代理自身内可识别任务的有限集内，来规避这些脆弱性。

6.3 应用代理

应用代理方法提供较高级的安全控制，因为它通过检验协议栈最高层的所有信息，对尝试连接提供应用级感知。因为应用代理服务在应用层是完全可见的，因此它能容易地预先看到每个尝试连接的各个细节，再实施相应的安全策略。应用代理服务的特点还包括内置的代理功能——在应用网关处终止客户端连接，并发起一个到受保护的内部网络的新连接。这种代理机制提供增强的安全，因为它将外部系统与内部系统相隔离，从而使得外部黑客更难以利用系统内部的脆弱性。

使用应用代理的安全网关提供最强大的安全，其唯一的缺点是：增强的安全能对其性能有负面影响。而且，对于新的服务，常常要花费时间才能使代理对此服务可用。

6.4 网络地址转换(NAT)

网络地址转换(NAT)技术的特征之一是它能够“隐藏”防火墙环境之内的网络编址方案。通过网络地址转换，内部网络上一个系统的IP地址被映射到一个不同的、对应外部的、可路由的IP地址。防火墙之内的许多系统也有可能共享同一个外部IP地址。外部用户仍可通过向某些端口号上的内连接转发来访问防火墙之内的资源。

网络地址转换能在大多数网络设备(交换机、路由器以及堡垒主机或防火墙)上实施。

6.5 内容分析和过滤

具有应用级代理的安全网关也经常实施内容分析和过滤。内容过滤包括关键字过滤、抵御恶意代码(如病毒、蠕虫和特洛伊木马)以及那些能够损害网络、应用程序和数据的移动代码(如Java、JavaScript、ActiveX或任何其他可执行代码)。

由于大多数这种恶意代码是通过电子邮件或基于HTTP通信(例如从Web站点或FTP站点的下载)在互联网上散布的，所以应在安全网关和互联网的接口处启动保护。因此，病毒扫描器或更通用的

内容扫描器被加到了屏蔽子网或非军事区(DMZ)。在大多数的安装中,内容扫描器直接与具有网络接口的防火墙链接,以便基于 SMTP 的电子邮件通信流和基于 HTTP 的通信被传输到内容过滤扫描器中。

内容分析的主要技术如下:

- 基于特征码的扫描(搜索已知模式);
- 研究性的分析(分析功能代码和已知与恶意代码相关的行为);
- 沙箱技术(本质上是一个内容监视程序,它把可疑代码隔离在"沙箱"中)。

由于内容扫描与入侵检测(特别是基于网络的入侵检测)之间的差别很小,通过在防火墙设备上实施 IDS 代理还可使入侵检测系统(IDS)与防火墙相结合。见 ISO/IEC TR 15947:2002。

注:入侵检测系统的选择、部署和操作是 ISO/IEC 18043 的主题。

内容过滤技术也有一定的局限性。如果数据在传输层或应用层上被加密(例如 SSL/TLS 或 S/MIME),就不再可能进行内容筛选,除非在防火墙上将加密数据解密,然后再重新加密。注意,这可能造成诸如"中间人"攻击之类的安全威胁。

对内容扫描及过滤有一些法律限制,尤其是在有强数据保护法律要求之处。在这种情况下,只允许对恶意代码进行自动扫描,而不允许扫描电子邮件的具体内容,因为这将影响到发送方和接收方的隐私。

7 安全网关组件

本章综述按组件(例如交换机、路由器和防火墙)区分的 4 种不同类型的安全网关。

7.1 交换机

交换机用于将完全的网络带宽分配给每个物理端口来实现高速通信。通常交换机是第 2 层设备,被广泛用于分割局域网。此外,当实施 VLAN 技术时,交换机能提供子网隔离。

通过把访问控制列表(ACL)用到 OSI 模型第 2、3 和 4 层中,交换机和与其相连的节点之间的通信流能够得到控制。交换机提供的访问控制功能使其成为安全网关体系结构的有用组件,对于实施和构造任何屏蔽子网的各自非军事区也非常有用。

在安全网关环境中使用的交换机不宜直接连接到公共网络,这是由于存在各种威胁,例如,类似拒绝服务的这种攻击能导致外露的交换机向所连接的网络大量倾泻包。

7.2 路由器

路由器通常设计为通过支持多种网络协议来连接不同的网络,并优化通信主机间的网络通信流和路由。此外,路由器可用作安全网关的组件,因为它能够基于包过滤技术来过滤各类数据通信中的数据包。

利用这种包信息检查来控制网络通信流的路由器经常被称作屏蔽路由器(见 8.1.1)。路由器通常在 OSI 模型的第 3 层(网络层)工作,目前在该层只可能控制数据包的低级信息,而不对用户数据进行任何检查。

路由器能执行 NAT 和包过滤。

7.3 应用级网关

应用级网关是基于硬件和软件的一台或一套设备。应用级网关专门设计成限制 2 个独立网络之间的访问。

应用级网关的实施主要使用 2 种技术:

- 状态包检测;
- 应用代理。

也可能使用这些技术的组合和变体(例如电路级防火墙)。此外,能够通过应用级网关执行 NAT。

7.4 安全装置

仅以安全为目的、配置了加固的操作系统的网络设备(路由器、交换机、调制解调器等)被称作安全装置。这些设备可作为安全软件(防火墙、IDS/IDP、抗病毒保护等)的基础。

可在范围广泛的平台上,从最小的远端到大型的公司网络以及数据中心,提供安全装置以满足各种各样的安全需求。专用于保护远端或单个计算机的装置称作个人防火墙装置,尽管这些装置可能还包含其他的安全功能,例如抗病毒保护。

第6章中介绍的所有技术均能使用安全装置来实施。

8 安全网关体系结构

为了充分地保护内部网络以免暴露给来自外部网络(诸如互联网)的攻击,宜为安全网关选择一种有效的体系结构。

可考虑用2种不同的方法,即结构化方法和层次化方法,来创建安全网关。

结构化方法是基于网络设计原则和由互联网协议设置的安全选项。层次化方法涉及到安全域和域边界上实施的防护措施,这些防护措施与组织的安全策略中所定义的安全要求相一致。

下面讨论这2种方法。

8.1 结构化方法

在组织可能有的、不同的、特定安全需求的驱动下,结构化方法可通过4种不同的体系结构来实施。它们是:

- 包过滤防火墙;
- 双宿主网关;
- 屏蔽主机;
- 屏蔽子网。

这种保护应包括抵御恶意代码、病毒、骇客、拒绝服务攻击和其他未授权活动的防护措施。

8.1.1 包过滤防火墙体系结构

防火墙体系结构的最基本类型称作包过滤器。包过滤防火墙本质上是包含对系统地址和通信会话的访问控制功能的路由设备。它们经常被称作屏蔽路由器。在其最基本的形式中,包过滤器在OSI模型的第3层运行。见图1。

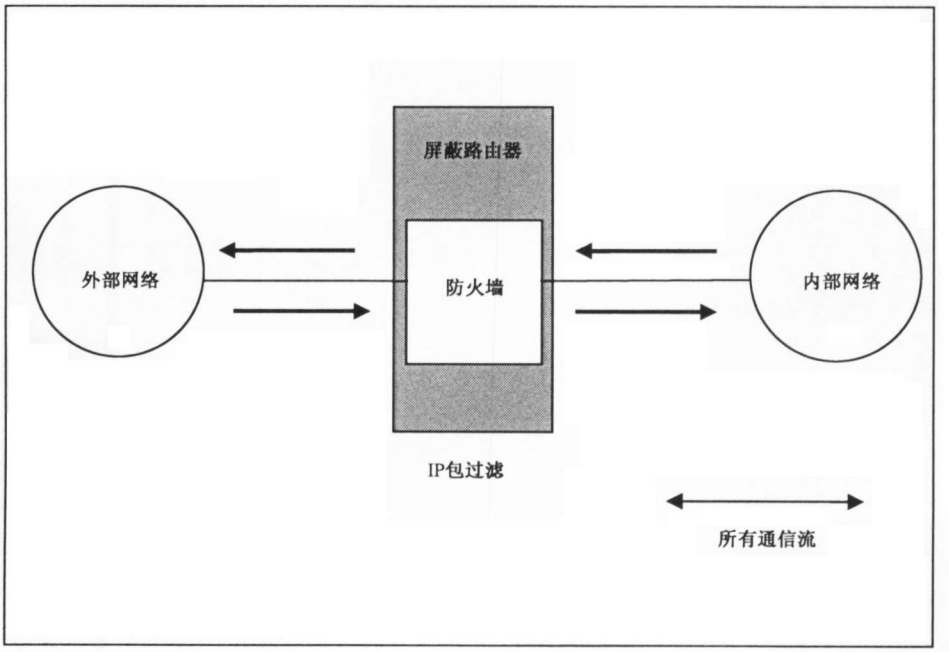

图1 包过滤防火墙/屏蔽路由器

包过滤防火墙的访问控制功能由一套统称为规则集的指令控制。这些指令提供网络访问控制并能够基于,例如包的源地址、包的目的地址、通信流类型、第4层通信会话的一些特征(诸如会话的源端口与目的端口)以及(有时)包来自路由器的哪个接口和包的目的地是哪个接口的信息。

包过滤防火墙有2个主要优点:快速和灵活。由于包过滤器通常不检验OSI模型第3层以上的数据,所以它们能够非常快地运行。这种简单性允许包过滤防火墙可作为外部路由器部署在屏蔽主机或屏蔽子网前面。这样放置的原因是其具有阻止拒绝服务攻击以及相关攻击的能力。

因为屏蔽路由器不检验上层(第5层至第7层)数据,所以不能防止那些利用与应用相关的脆弱性或功能的攻击。由于防火墙可利用的信息有限,所以包过滤防火墙中的日志功能也是有限的。由于访问控制判定中使用大量的变量,因此易受到由不当配置导致的安全违规的影响。

8.1.2 双宿主网关体系结构

双宿主网关由一个具有A和B 2个网络接口的主机系统构成(见图2),并且关闭了主机的IP转发功能。因此,来自一个网络(例如互联网)的IP包不能按某一路线直接发送到其他网络(例如内部网络)。内部网络的系统能够与双宿主主机通信,外部网络上处于防火墙之外的系统也能与双宿主主机通信,但这些系统彼此之间不能直接通信。

如果这种主机配备了若干网卡,例如,与互联网上的几个互联网服务提供商分别连接,或与内部网络上的不同服务器(诸如电子邮件服务器或日志服务器)连接,其配置就有多个变体。在这种情况下,它被称作多宿主网关。

作为选择方案,可在与外部网络连接处放置一个路由器,以通过网络包的过滤来提供额外保护。双宿主网关阻止外部网络与被保护站点之间的所有直接IP通信流。服务和访问由防火墙上的应用级代理服务提供。

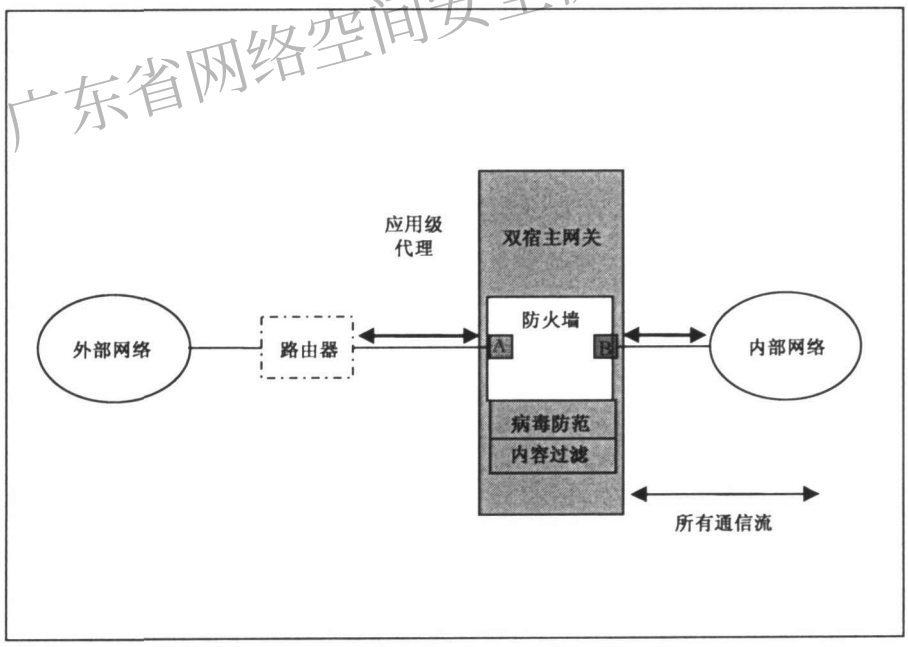

图2 双宿主网关

双宿主网关代表一种更合规的安全网关类型,因为它对外部网络的系统隐藏内部IP地址,并提供可与入侵检测系统(IDS)联合使用的日志功能以检测可能的入侵者活动。这种网关只允许存在相应代理的服务通过,这种有限的灵活性对于某些站点来说可能是一个缺点。在这种情况下若增加一个路由器以建立一个可信的通信作为安全网关的旁路,就能解决这个问题。用于防火墙的主机系统的安全对整体保护来说是至关重要的,因为如果防火墙受到损害,那么入侵者就可能获得对内部系统的访问。

8.1.3 屏蔽主机体系结构

屏蔽主机体系结构将包过滤路由器与使用应用代理的堡垒主机结合在一起。堡垒主机被置于路由器的受保护子网一侧(见图3)。在这种体系结构中,主要的安全保护由包过滤路由器提供,例如,防止人们绕过代理服务器建立与内部网络的直接连接。

屏蔽路由器上的包过滤按如下方式设置:堡垒主机是外部网络的主机能打开连接到的唯一系统。作为应用级防火墙的这种堡垒主机由依据站点的策略放行或阻止服务的代理服务构成。路由器自动过滤危险的协议以防止其到达防火墙及站点系统。

从外部网络到堡垒主机的应用通信流得到路由;来自外部站点的所有其他通信流被拒绝。路由器拒绝任何源自内部网络的应用通信流,除非它来自堡垒主机。

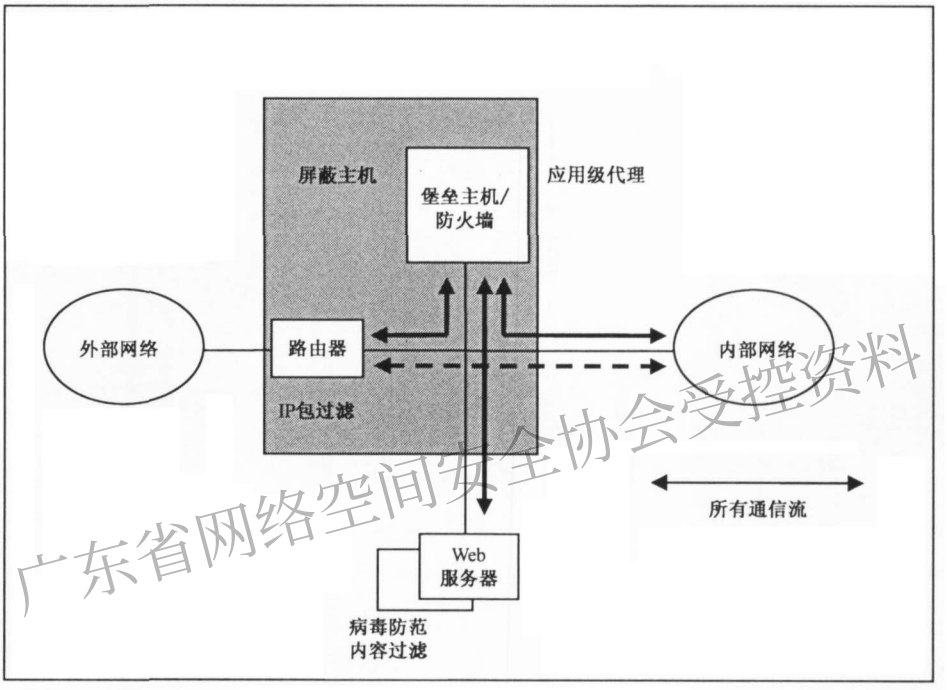

图3 屏蔽主机

这种体系结构更灵活,因为这种堡垒主机只需要一个网络接口,不要求在堡垒主机和路由器之间有一个独立子网。此外,路由器能够放行可信服务"绕过"堡垒主机直接到达内部系统。

因为这种灵活性更易于违反已确立的安全策略,所以被认为整体不太安全。这种体系结构的主要缺点是:如果攻击者设法闯入到堡垒主机,那么在堡垒主机与内部网络之间便无任何网络安全可言。路由器也会出现单点故障,如果路由器受到损害,攻击者就可利用整个网络;另一个缺点是用户具有两个系统,需谨慎地加以配置。这种路由器的包过滤规则可能相当复杂并且难以维护。

8.1.4 屏蔽子网体系结构

屏蔽子网体系结构是双宿主网关和屏蔽主机体系结构的一种变体(见图4)。它在屏蔽主机体系结构中增加了一个额外的保护层,即增加边界网络以把内部网络和外部网络(如互联网)进一步分隔开。

创建一个内部屏蔽子网要用到2个路由器。这种子网有时被称作非军事区(DMZ)或边界网络。可在其中放置堡垒主机或应用级防火墙,然而,也可以在里面放置Web服务器、电子邮件服务器或DNS服务器以及其他需要谨慎控制访问的系统。外部路由器限制外部网络对屏蔽子网内特定系统的访问(例如,将电子邮件通信流从互联网站点按某一路线发送到电子邮件服务器),并阻止从不宜发起连接的系统至外部网络的所有其他通信流(例如,NFS挂载到外部系统)。内部路由器根据现有规则放行进/出屏蔽子网系统的通信流(例如,将电子邮件通信流从站点系统按某一路线发送到电子邮件服务器,反之亦然)。

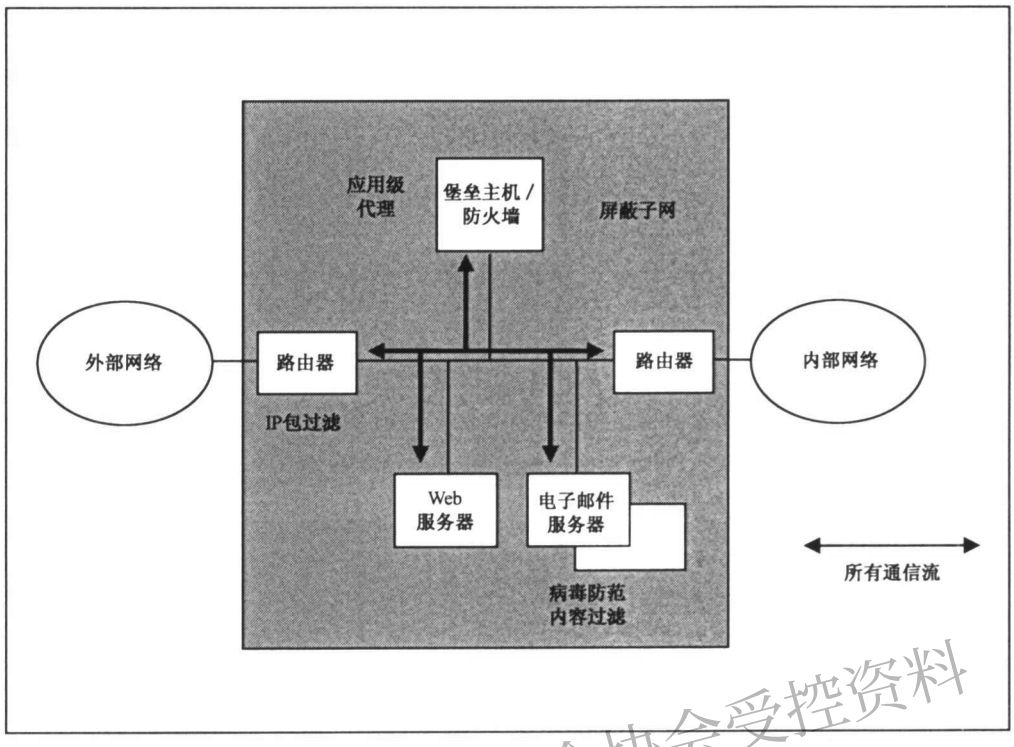

图 4 屏蔽子网

从外部网络不能直接到达任何内部系统，反之亦然。这一点对于双宿主网关(也经常包括多宿主网关)来说是重要的。对于屏蔽子网体系结构来说，没有绝对必要像双宿主系统那样实现应用级网关各自的堡垒主机。

屏蔽子网体系结构可能更适用于具有大通信流的站点或需要极高速通信流的站点。

8.2 层次化方法

保护层次由涵盖安全要求的安全域的不同安全维组成。例如，操作系统的口令提示就是用于访问控制的保护层次。如果外部用户在这种保护层次上用有效 ID 和口令适当鉴别，外部用户就能访问这种安全域。如果这种鉴别机制强壮到足以满足该访问鉴别要求，它就能被实现来保护该域免受未授权访问。

保护层次的要求能够用安全域中关键数据和服务的保密性、完整性、可用性、可核查性、真实性和可靠性来表示。保护层次能包含以下安全控制措施：

- 鉴别；
- 包过滤；
- 入侵检测；
- 日志。

保护层次能分别在不同设备上实施，如果可能，也能被组合在一个或多个设备中。这一点是结构化方法和层次化方法的互补之处。例如，若能把所有层次置于同一设备中，就可形成包过滤或双宿主的网关体系结构。

这种方法通过在需要的地方实现多个保护层次，并提供足够的安全控制措施以满足受保护安全域的安全要求，来创建纵深防御。

8.2.1 单层次和多层次安全网关体系结构

单层次体系结构是最简单的层次化方法。它能适用于只满足一种安全要求的情况，例如，访问安全域之前的用户鉴别。典型的方案是，所实施的路由器只执行一项安全任务——用户鉴别(见图 5)。

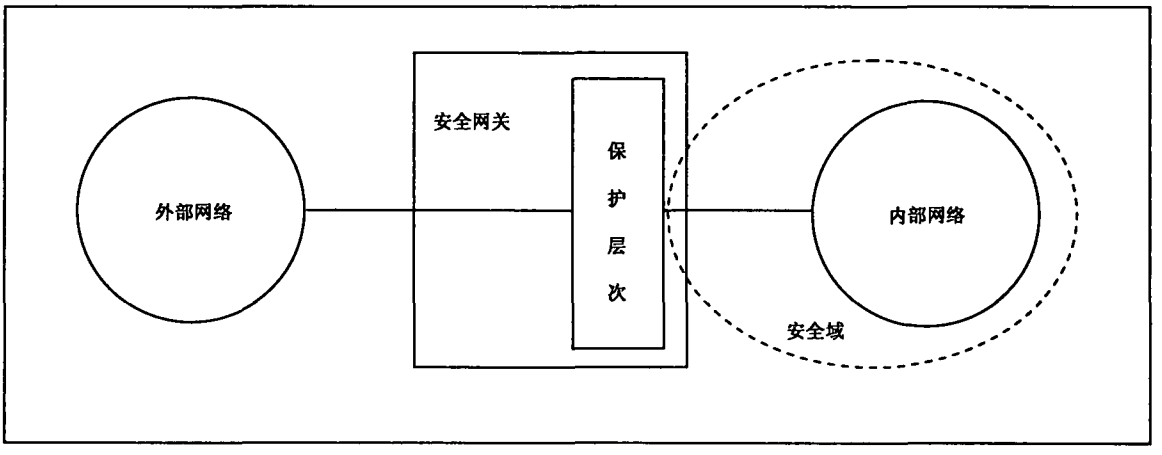

图 5 单层次安全网关

通常安全域宜满足更多的安全要求，并且安全网关也变得更复杂，例如，允许一组规定的协议并在访问安全域之前执行鉴别。在这种情况下需要 2 个安全层次——包过滤层次和鉴别层次(见图 6)。2 个层次均能由执行包过滤和鉴别的路由器实施。

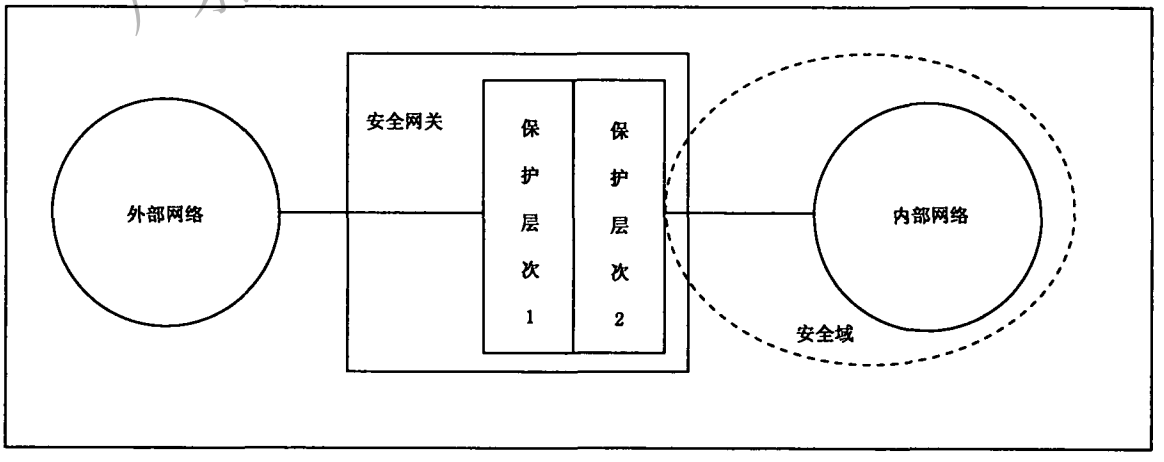

图 6 多层次安全网关

大多数组织的网络中都有不止一个安全域。如果组织中有另一个具有相似安全要求的域，那么安全网关就可能同时保护这两个域。在这种情况下，就能够形成一个非军事区(DMZ)或边界网络。如果第一个域的安全策略允许其通信流通过第二个域，则这种 DMZ 就类似于屏蔽子网体系结构中的 DMZ(见图 7)。

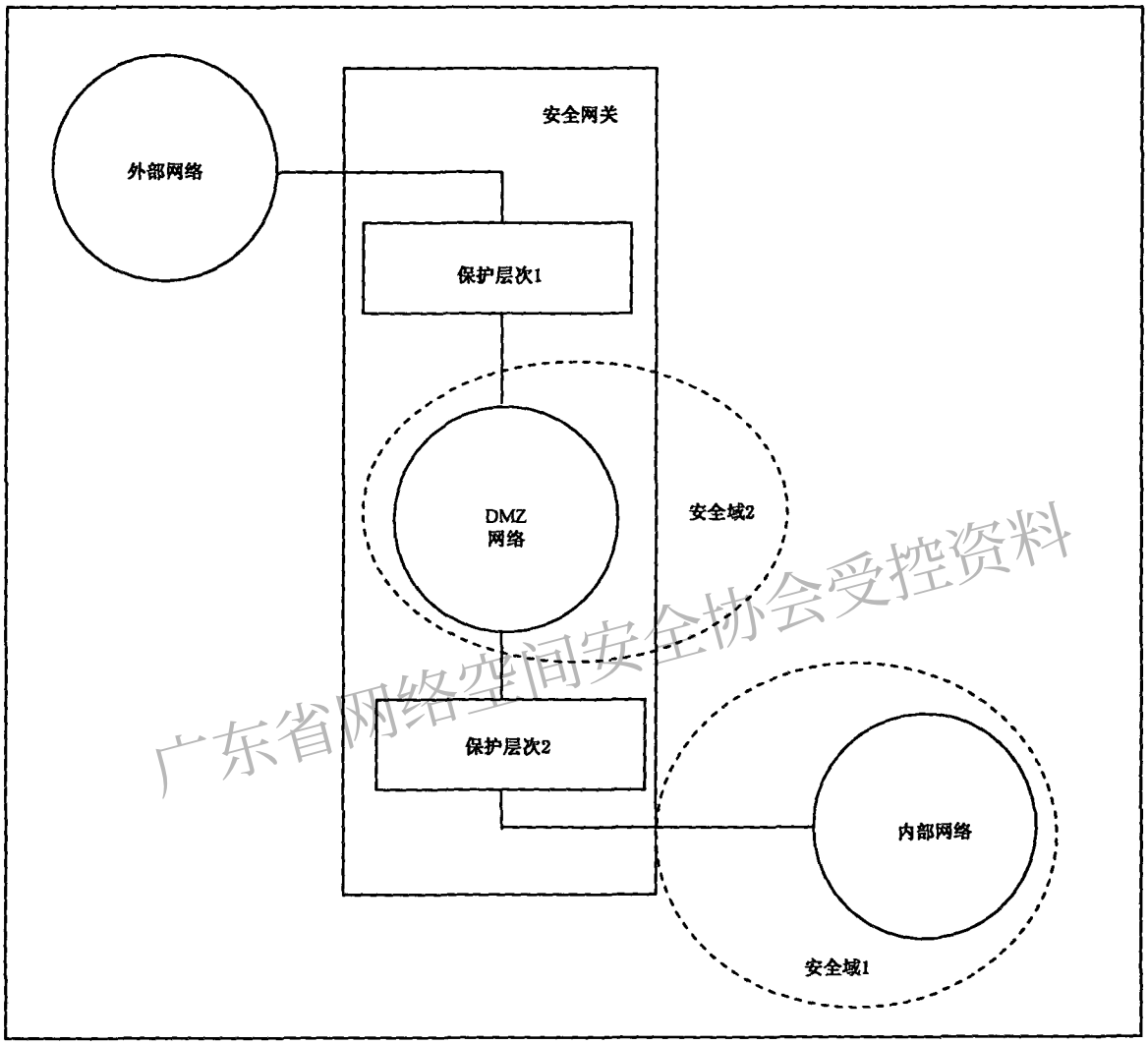

图 7　多层次安全网关中的 DMZ

如果第一个域的安全策略不允许其通信流通过其他任何域，并且外部层次能为第二个域提供独立的连接，那么这种 DMZ 称作服务向 DMZ(见图 8)。

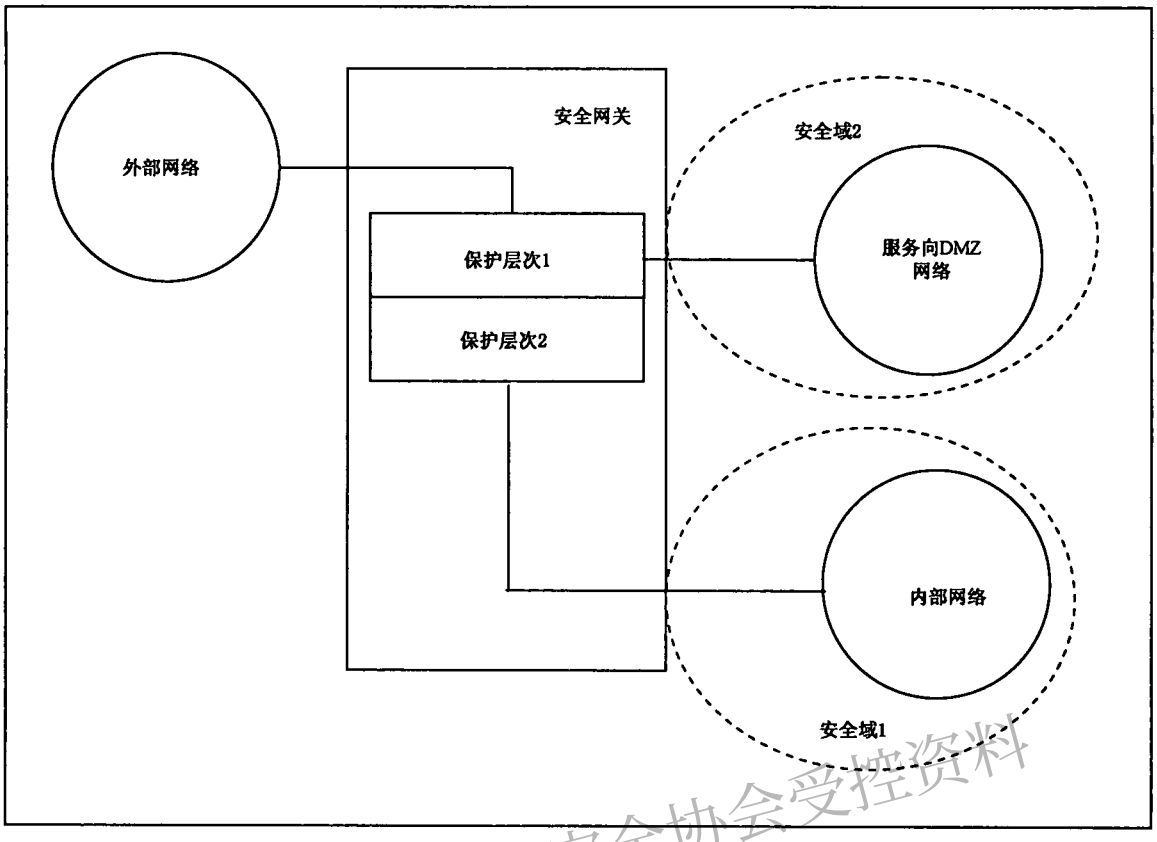

图 8 多层次安全网关中的服务向 DMZ

9 选择和配置指南

为了确保满足第 5 章中概述的要求，选择和配置安全网关的结构化方法是必要的。本章为这一过程给出了一些指南，尤其是在以下领域：

- 安全网关体系结构和适当组件的选择；
- 硬件和软件平台的选择；
- 配置；
- 安全特点和设置；
- 常规管理；
- 日志；
- 文档化；
- 审计；
- 培训/教育。

作为一般指南，应遵循以下 4 项原则：

- 注意所有可能的威胁，特别是内部威胁；
- 注意人的因素，例如，在常规管理和教育方面；
- 尽可能保持其简单，尽管更高的安全要求通常也意味着更复杂的体系结构；
- 使用组件或设备的指定功能和配置。

9.1 安全网关体系结构和适当组件的选择

应基于对安全网关的业务及安全要求（见第 5 章），来选择和调整适当的安全网关体系结构（可能的安全网关体系结构的综述见第 8 章）。

注：网络安全管理是 GB/T 25068.1 的主题。

一旦定义了体系结构，就需要进一步规定这种体系结构的每个组件以及评价这些组件的功能。有关可能的组件的综述见第7章，而所提供功能的详细描述见第6章。

以下章条提供一些有关选择适当体系结构及其正确组件的进一步指南。

9.2 硬件和软件平台

在选择硬件平台时，应特别考虑其性能、效率、可靠性和适用性。例如，如果一个硬件平台只具有以太网接口但却需要V.35上的帧中继，那么这种平台是不可用的。

其次，应查看这种硬件设备的操作系统。为了安全起见，宜使用加固的操作系统。另外还建议针对已知的脆弱性对其进行检查。也需要根据软件平台的性能和可靠性对其进行验证，例如，具有10BaseT以太网接口的路由器不能提供千兆比特的吞吐量。

9.3 配置

在安全网关网络设备的配置过程中，应考虑以下推荐设置：

- 屏蔽子网体系结构中各自非军事区的交换网络；
- 路由器与安全网关之间的静态路由；
- 源路由信息不宜被接受；
- 应在安全网关上只安装(“平台加固”)操作所绝对必要的软件/程序；
- 对于包过滤情况下的规则定义，有定义所有未明确允许的包将被禁止的过滤规则的可能性；
- 确保端口未默认为被激活；
- 确保SPAN端口未被激活，除非需要使用入侵检测系统；
- 确保口令在设备接口处被实施；
- 拒绝RIP报文“Loose-source-routing(松散源路由)”；
- 适当的网络地址转换功能；
- 安全网关的透明操作；
- 安全网关的访问控制(识别、鉴别)；
- 在安全网关崩溃的情况下，宜仍可能执行管理任务；
- 针对操作系统的平台加固。

9.4 安全特点和设置

应用代理至少应能够做到：

- 支持主要的互联网服务(HTTP、FTP、Telnet、SMTP、NNTP)；
- 支持更多的互联网服务；
- 支持通用代理(针对新的协议或服务)；
- HTTP代理应能够正确处理SHTTP；
- 拒绝BGP报文“notification(通知)”(例如通过通用代理)；
- 支持动态路由协议；
- 支持Web服务(例如SOAP/XML)；
- 支持成套的企业应用系统或其他业务应用系统的代理；
- 可以允许、拒绝或丢弃连接或包。

包过滤设备至少应能够做到：

- 通过动态包过滤器的适当保护来支持NFS、NIS、RPC、RIP、OSPF、DNS、WAIS服务；
- 支持基于如下信息的包过滤：
  - ——IP的源和目的地址；
  - ——源和目的端口(针对TCP、UDP)；
  - ——连接方向(向内、向外)；
- 保持过滤规则的内在一致；

- 分别为每个网络接口过滤包；
- 若需要设备集群，则支持组播包；
- 由安全网关保持过滤规则的顺序；
- 检测拒绝服务攻击(例如 TCP-SYN 洪泛)；
- 防止对 TCP 序号的猜测；
- 限制 IP 包分段的长度，并定义最小分段偏移量；
- 重组 IP 包；
- 过滤 ICMP 报文“destination unreachable(目标不可达)”和“redirect(重定向)”；
- 抵抗“ping-of-death”攻击(一种拒绝服务攻击)；
- 防止 IP 欺骗，即，若内部 IP 地址来自互联网就加以拒绝；
- 将 FTP 命令的使用与特定访问权限相结合；
- 使得环境信息被存储，例如，检查动态分配的端口号；
- 过滤其他网络客体(域、组、VPN 客体，等等)；
- 防止会话劫持。

建议检查其他繁杂的特点或设置，例如：

- 基于日志信息[或通过入侵检测传感器(若已安装)]发现入侵时报警。
- 应注意的是，使用 SOAP 通信机制的应用程序能够不被发现地通过状态检测和应用代理防火墙。这就给予避开应用代理和其他防火墙策略的企图以可乘之机。需要特别关注基于 SOAP 的应用需要经过安全网关的连接的情况。例如，通过(在允许编写适当的 XML 过滤器程序的 XML 防火墙中)实施与应用相关的 XML 内容过滤器，和/或通过执行只在被端到端 VPN 保护情况下才允许基于 SOAP 的应用通过安全网关进行通信的强制策略，一些基于 SOAP 的应用才能得到保护。

9.5 常规管理

常规管理过程是维持适当安全级别的任务中最敏感的任务之一。应主要考虑的安全网关特点如下：

- 安全网关管理员的识别和鉴别；
- 常规管理任务的可信赖通信路径(例如控制台、加密通信、分隔的网络)；
- 只有在强鉴别和加密条件下才允许的远程常规管理；
- 在部署多个安全网关的情况下集中常规管理的可能性；
- 安全网关所使用的程序和文件的完整性测试；
- 来自安全网关的报警日志应能够发送到外部主机；
- 通过任何便利的安全信道(例如电子邮件)向管理员报警；
- 低耗费的常规管理。

9.6 日志

当需要跟踪数据流时，例如，灾难恢复、法律调查等，记录日志过程非常重要：

- 记录日志的能力(用户身份识别、IP 的源和目的地址、端口号、时间、日期)。此处的要点是，存储的信息越多，事件处理得越好。
- 与 NTP 服务器同步的能力，以获取精确的日期和时间。
- 日志文件的保护，以抵御恶意更改。

9.7 文档化

现场保存网络文档对于安全网关的有效管理是必要的。至少应具有：

- 电子形式的文档(具有图表)；
- 与安全网关相关的过程(批准过程、评审过程)文档；

- 访问指南文档(允许访问的服务和应用);
- 过滤规则和所用代理的文档;
- 针对安全网关环境的业务连续性规划/灾难恢复的文档。

文档应定期评审。

9.8 审计

安全网关应支持审计工具来验证日志文档,同时维持诸如保密性、完整性、可用性、鉴别、可核查性和抗抵赖等信息安全的基本概念。

9.9 培训和教育

- 安全网关应拥有足够的文档和支持资料以便安装和实施,从而确保对网络和系统的充分保护;
- 为操作和维护人员编制培训资料;
- 应定期培训安全网关的操作和维护人员,以确保他们保持足够的知识和能力水平。

9.10 其他

建议检查能影响整体安全级别的其他系统和设备,例如:

- 所有远程接入连接宜由安全网关保护。更多有关信息见 GB/T 25068.4。
- 抗病毒检查。
- 可执行代码的过滤,诸如 Java、JavaScript、MIME、ActiveX;即使包含在 FTP 数据传输中。
- 虚拟专用网(VPN)环境中安全网关的使用。

注:使用虚拟专用网的通信安全保护是 GB/T 25068.5 的主题。

- 第三方的内容安全产品的集成:

安全网关体系结构经常集成包含对文件或互联网通信流(例如 SMTP、FTP、HTTP)进行病毒或恶意代码扫描和检查的内容安全解决方案。一方面,有些方法是使用分隔开的网关服务器,对经过服务器的互联网通信流或特定的互联网服务进行病毒或恶意代码扫描,并防止危险代码进入内部网络。另一方面,有些解决方案是通过 DLL 或 API 技术,将内容检查功能更紧密的集成到防火墙产品中。

内容安全方法也经常包括 URL 的检查或筛选。

- 入侵检测系统(IDS)的集成:

在安全网关环境中,入侵检测系统被置于非军事区。防火墙系统以及重要的应用服务器都属于这种受入侵检测系统传感器监控的系统。

更多有关信息见 ISO/IEC TR 15947:2002。

注:入侵检测系统的选择、部署和操作是 ISO/IEC 18043 的主题。

参 考 文 献

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall, Bonn 1997

[2] Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI Firewall Studie II, Bonn 2001

[3] Chapman, D. Brent, Zwicky, Elizabeth D.: Building Internet Firewalls, Cambridge 2000 (O'Reilly)

[4] Cheswick, William R.; Bellovin, Steven M.: Firewall and Internet Security. Repelling the Wily Hacker. Reading, a. o. 1994 (Addison-Wesley)

[5] Ellermann, Uwe: Firewalls. Isolations-und Audittechniken zum Schutz von lokalen Computer-Netzen. Berlin 1994 (DFN-Bericht Nr. 76)

[6] Siyan, Karanjit; Hare, Chris: Internet Firewalls and Network Security. Indianapolis 1995 (New Riders Publishing)

[7] Wack, John; Cutler, Ken; Pole, Jamie: Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology, 2001 (National Institute of Standard and Technology (NIST) Special Publication 800-41)

[8] GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则(ISO/IEC 27002:2005, IDT)

[9] ISO/IEC 18028-2:2006 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

[10] GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理指南(ISO/IEC 18044:2004, MOD)

[11] GB/T 22080—2008 信息技术 安全技术 信息安全管理体系 要求(ISO/IEC 27001:2005, IDT)

中华人民共和国
国家标准
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
GB/T 25068.3—2010/ISO/IEC 18028-3:2005
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1.5 字数 40千字
2011年1月第一版 2011年1月第一次印刷
*
书号:155066·1-40818 定价 24.00元

GB/T 25068.3-2010