

第四章

防火墙工作原理及应用



第四章 防火墙工作原理及应 用



4.1 防火墙概念与分类



4.2 防火墙体系结构



4.3 防火墙选型与产品简介



绿盟科技下一代防火墙-NF NX3-G2000M

主要参数

设备类型	下一代防火墙
并发连接数	1000000
吞吐量	三层吞吐量2Gbps，七层吞吐量600M
网络端口	4GE，4SFP
控制端口	1MGT
VPN支持	IPSec/SSL/L2TP
入侵检测	4000+无重复签名，NSS Labs推荐，通过CVE兼容性认证，DDoS防护
管理	中文Web界面、SNMP v1/v2c/v3、syslog日志、集中管理、在线升级

没有帧丢失的情况下，设备能够接受的最大速率

交换机接口模块

2019-10-08
75家商家报价

[查询底价](#)

¥3.9万

2019-10-08
47家商家报价

[查询底价](#)

一般参数

电源	单电源：60W
外形设计	1U
适用环境	工作温度：0-40℃ 相对湿度：5%-95%（无凝结状态）
其他性能	Bypass：2路 传统防火墙：覆盖传统防火墙功能包括访问控制、NAT支持、路由协议、VLAN、STP、主主/主备双机热备 病毒防护：支持基于流引擎查毒技术，针对HTTP、FTP、SMTP、POP3等协议进行查杀 上网管理：P2P流量管控、应用流量控制、web网站过滤、恶意站点过滤、内容过滤管理 其他功能：云安全日志管理

旁路功能,让两个网络不通过网络安全设备的系统，直接物理导通

¥3340

2019-10-08
52家商家报价

¥7.9万

2019-10-08
3家商家报价

[查询底价](#)

*本信息来源于ZOL产品库



第四章 防火墙工作原理及应用

当网络涉及不同的信任级别时（例如内部网、Internet或者网络划分），要保证安全必须安装控制设备。此类控制设备几乎总是某种形式的防火墙。防火墙允许授权的数据通过，而拒绝未经授权的数据通信，并记录访问报告等。由于使用防火墙能增强内部网络的安全性，因此防火墙技术的研究已经成为网络信息安全技术的主导研究方向。本章将介绍防火墙的基本功能、工作原理、分类、体系结构、局限性以及典型防火墙产品。



4.1 防火墙概念与分类

网络防火墙是隔离内部网与Internet之间的一道防御系统，允许人们在内部网和开放的Internet之间通信。访问者必须首先穿越防火墙的安全防线，才能接触目标计算机，网络防火墙如图4.1所示。



网络防火墙

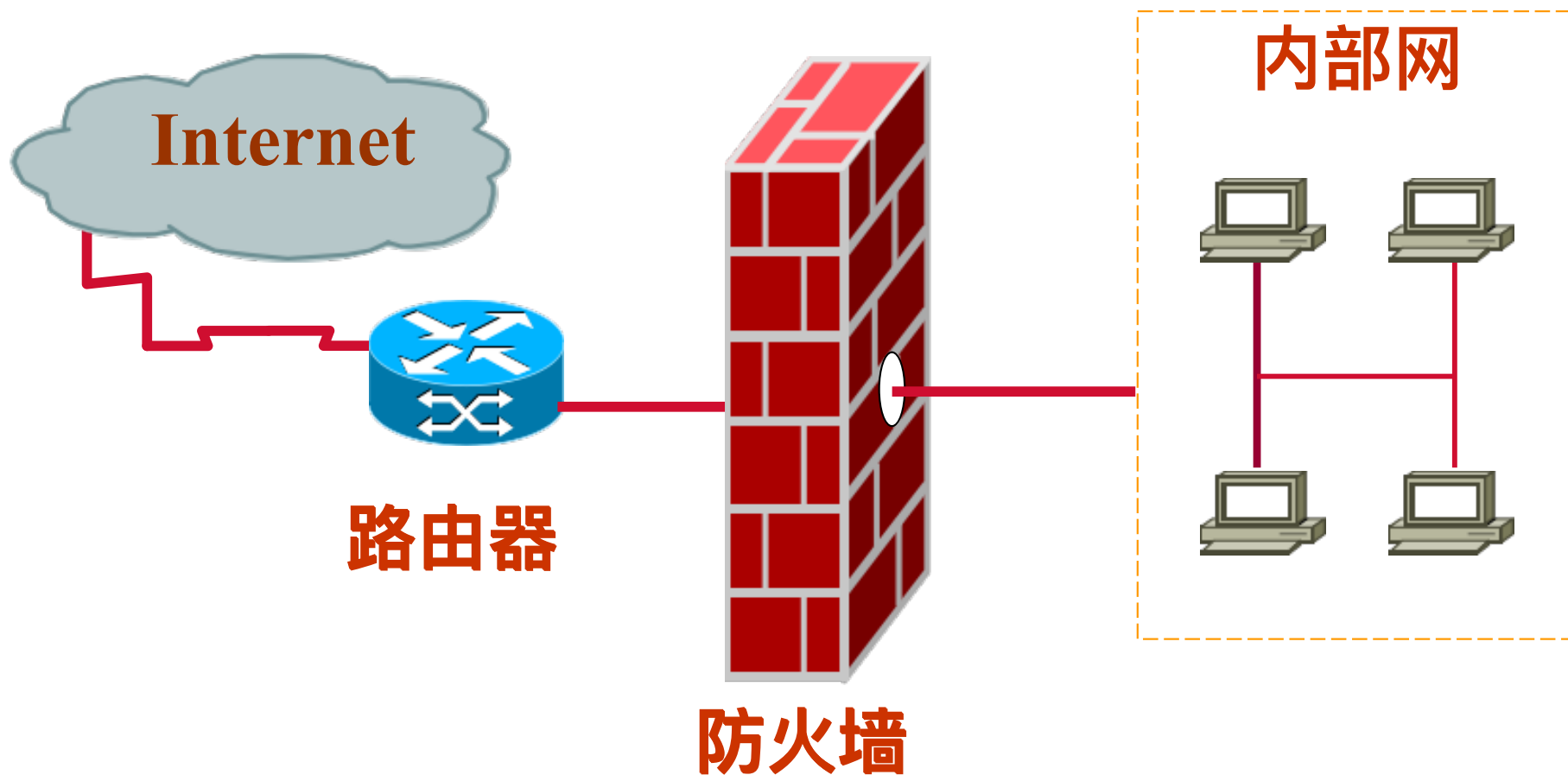


图4.1



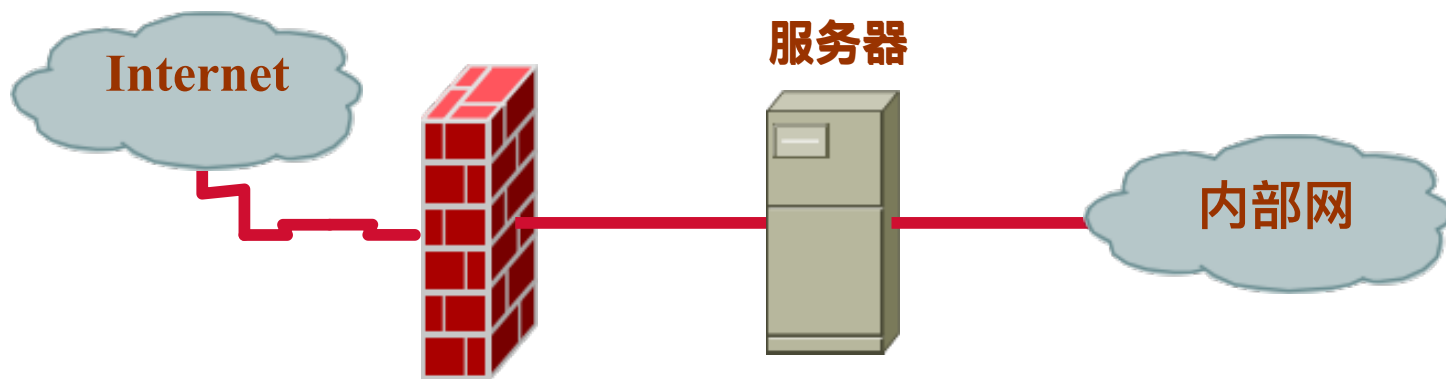
4.1.1 防火墙简介

在没有防火墙时，局域网内部的每个节点都暴露给Internet上的其它主机，此时内部网的安全性要由每个节点的坚固程度来决定，且安全性等同于其中最薄弱的节点。使用防火墙后，防火墙会将内部网的安全性统一到它自身，网络安全性在防火墙系统上得到加固，而不是分布在内部网的所有节点上。

防火墙把内部网与Internet隔离，仅让安全、核准了的信息进入，而阻止对内部网构成威胁的数据，它防止黑客更改、拷贝、毁坏重要信息；同时又不会妨碍人们对Internet的访问。



防火墙的工作原理



根据安全策略，从Internet到Intranet的流量受到阻塞



根据安全策略，从Internet来的特殊类型的流量可能被允许到达Intranet



根据安全策略，从Intranet到Internet的流量以及响应的返回流量允许通过防火墙。

图4.2



防火墙的基本功能

- 作为一个中心“遏制点”，将内部网的安全管理集中起来，所有的通信都经过防火墙；
- 只放行经过授权的网络流量，屏蔽非法请求，防止越权访问,并产生安全报警；
- 能经受得起对其自身的攻击。



防火墙的基本功能 (续)

防火墙能为管理人员提供对下列问题的答案：

- 什么人在使用网络？
- 他们什么时间，使用了什么网络资源？
- 他们连接了什么站点？
- 他们在网上做什么？
- 谁要上网,但是没有成功？



防火墙工作在osi参考模型上

OSI参考模型	防火墙技术
应用层	应用级网关
表示层	加密
会话层	电路级网关
传输层	包过滤
网络层	NAT
数据链路层	无
物理层	无



防火墙的发展史

- 第一代防火墙技术由附加在边界路由器上的访问控制表ACL (Access Control Table)构成，采用了包过滤技术。
- 第二代代理防火墙即电路层网关和应用层网关。
- 1994年，以色列的Check Point公司开发出了第一个基于动态包过滤技术的防火墙产品。
- 1998年，美国的网络联盟公司NAI (Network Associates Inc.)又推出了一种自适应代理技术。



防火墙的两大分类

- 尽管防火墙的发展经过了将近20年，但是按照防火墙对内外来往数据的处理方法，大致可以将防火墙分为两大体系：包过滤防火墙和代理防火墙。前者以Checkpoint防火墙和Cisco公司的PIX防火墙为代表，后者以NAI公司的Gauntlet防火墙为代表，表4.2为防火墙两大体系性能的比较。

防火墙 { 包过滤防火墙：工作在IP和TCP层
代理防火墙



防火墙两大体系性能的比较

	第一层 包过滤防火墙	应用层 代理防火墙
优点	<p>工作在IP和TCP层，所以处理包的速度快，效率高； 提供透明的服务，用户不用改变客户端程序</p> <p>检查的信息少</p>	<p>不允许数据包直接通过防火墙，避免了数据驱动式攻击的发生，安全性好；</p> <p>能生成各项记录。能灵活、完全地控制进出的流量和内容；</p> <p>能过滤数据内容。</p>



防火墙两大体系性能的比较 (续)

	包过滤防火墙	代理防火墙
缺点	<p>定义复杂，容易出现因配置不当带来的问题；</p> <p>允许数据包直接通过，容易造成数据驱动式攻击的潜在危险；</p> <p><u>不能彻底防止地址欺骗；</u></p> <p><u>包中只有来自哪台机器的信息</u></p> <p><u>不包含来自哪个用户的信息；</u></p> <p>不支持用户认证；</p> <p>不提供日志功能。</p>	<p>对于每项服务代理可能要求不同的服务器；</p> <p><u>速度较慢；</u></p> <p>对用户不透明，用户需要改变客户端程序；<u>711/p+协议本</u></p> <p>不能保证免受所有协议弱点的限制；<u>有名无实</u></p> <p>不能改进底层协议的安全性。</p>

因为只检查头部



防火墙的组成

- 防火墙既可以是一台路由器、一台PC或者一台主机，也可以是由多台主机构成的体系。应该将防火墙放置在网络的边界。网络边界是一个本地网络的整个边界，本地网络通过输入点和输出点与其它网络相连，这些连接点都应该装有防火墙，然而在网络边界内部也应该部署防火墙，以便为特定主机提供额外的、特殊的保护。



防火墙放置的位置

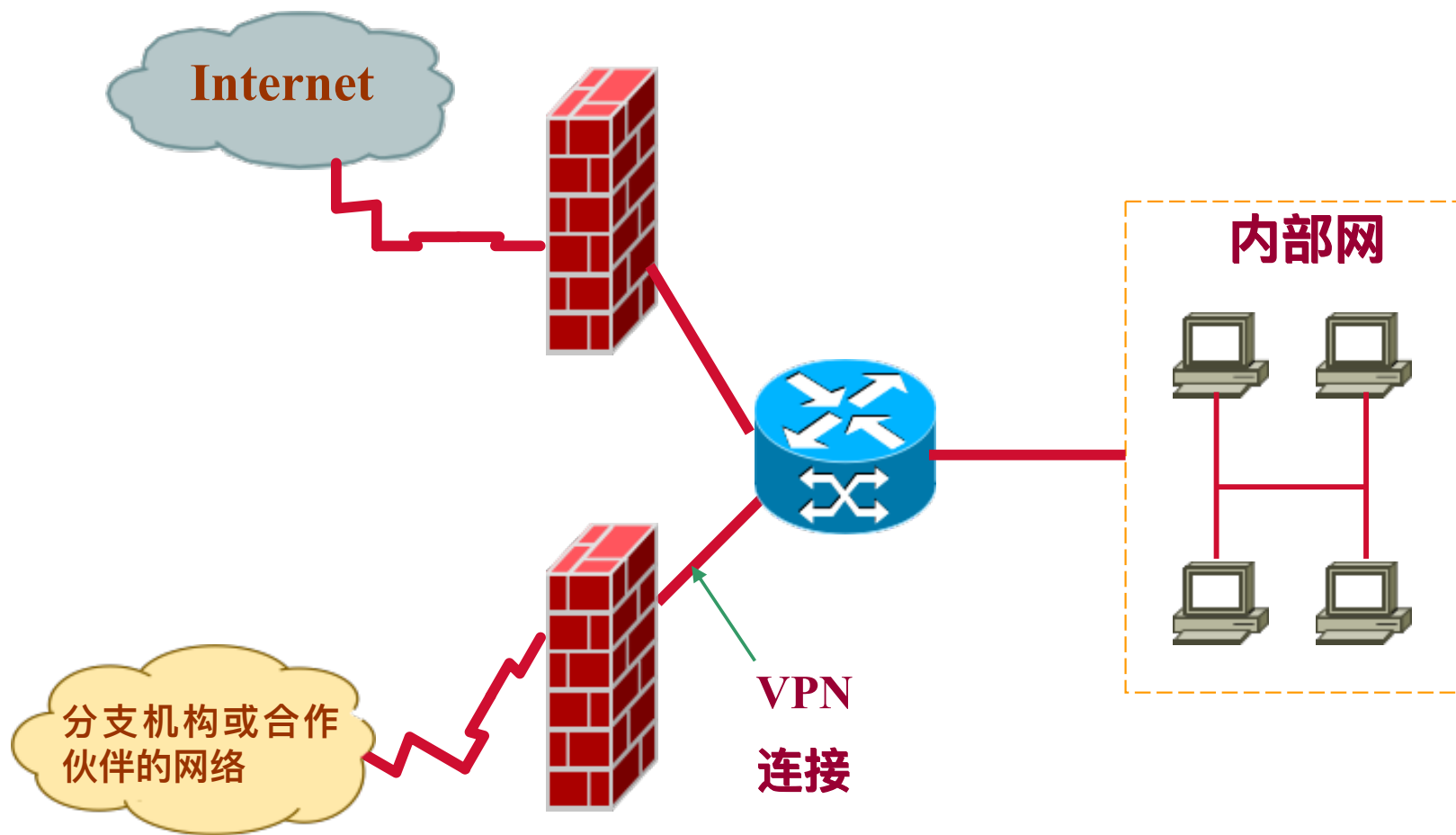


图 4.3



防火墙的分类

根据采用的技术不同,

- 包过滤防火墙
- 代理服务防火墙

按照应用对象的不同

- 企业级防火墙
- 个人防火墙

依据实现的方法不同

- 软件防火墙
- 硬件防火墙
- 专用防火墙



软件防火墙

- 防火墙运行于特定的计算机上，一般来说这台计算机就是整个网络的网关。软件防火墙像其它的软件产品一样需要先计算机上安装并做
好配置才可以使用。使用这类防火墙，需要网络管理人员对所工作的
操作系统平台比较熟悉



硬件防火墙

专用的硬件和OS

- 由PC硬件、通用操作系统和防火墙软件组成。在定制的PC硬件上，采用通用PC系统、Flash盘、网卡组成的硬件平台上运行Linux、FreeBSD、Solaris等经过最小化安全处理后的操作系统及集成的防火墙软件。特点是开发成本低、性能实用、稳定性和扩展性较好，价格也低廉。由于此类防火墙依赖操作系统内核，因此会受到操作系统本身安全性影响，处理速度也慢。



专用防火墙

- 采用特别优化设计的硬件体系结构，使用专用的操作系统，此类防火墙在稳定性和传输性能方面有着得天独厚的优势，速度快，处理能力强，性能高；由于使用专用操作系统，容易配置和管理，本身漏洞也比较少，但是扩展能力有限，价格也较高。由于专用防火墙系列化程度好，用户可根据应用环境选择合适的产品。



4.1.2 包过滤防火墙

- 包过滤(Packet Filter)是所有防火墙中最核心的功能，进行包过滤的标准是根据安全策略制定的。通常情况下靠网络管理员在防火墙设备的ACL中设定。与代理服务器相比，它的优势是不占用网络带宽来传输信息。
- 包过滤规则一般存放于路由器的ACL中。在ACL中定义了各种规则来表明是否同意或拒绝数据包的通过。
- 如果没有一条规则能匹配，防火墙就会使用默认规则，一般情况下，默认规则要求防火墙丢弃该包。包过滤的核心是安全策略即包过滤算法的设计。



ACL对数据包的过滤

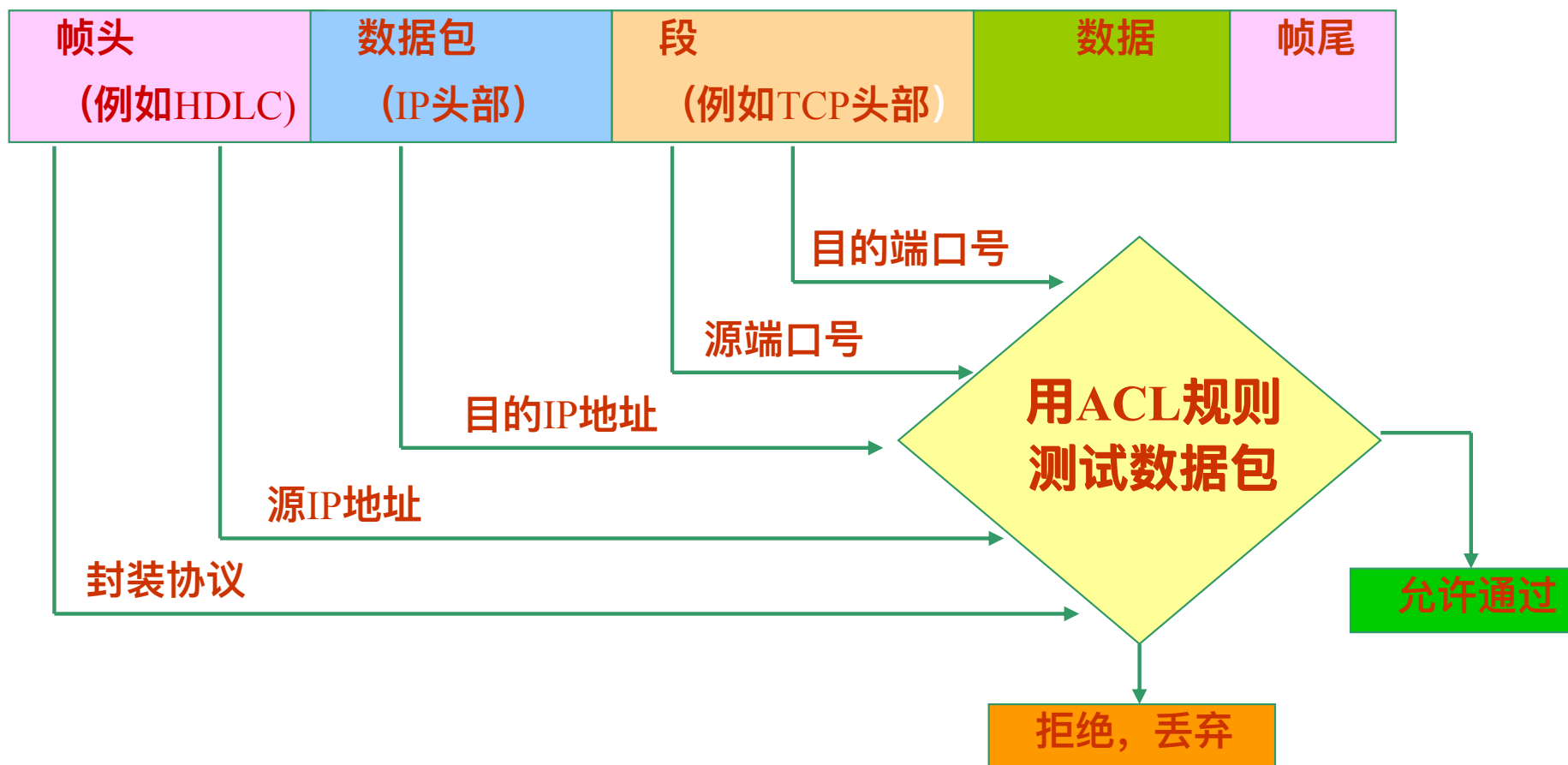


图4.4



ACL处理入数据包的过程

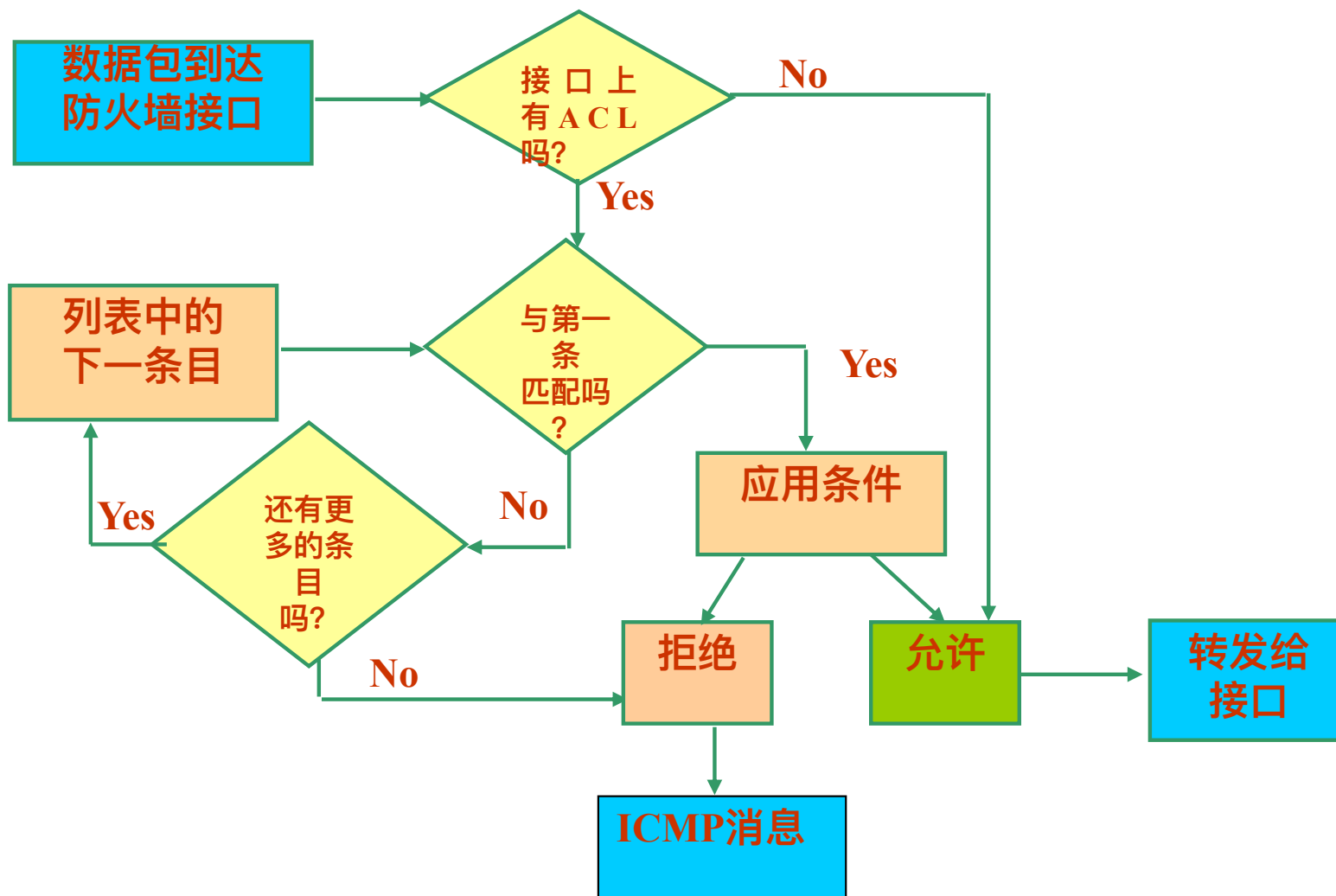


图4.5



无状态包过滤防火墙

- 无状态包过滤也叫静态包过滤或者无检查包过滤。防火墙在检查数据包报头时，不关心服务器和客户机之间的连接状态，只是根据定义好的过滤规则集来检查所有进出防火墙的数据包报头信息来允许或者拒绝数据包。



无状态包过滤防火墙的执行

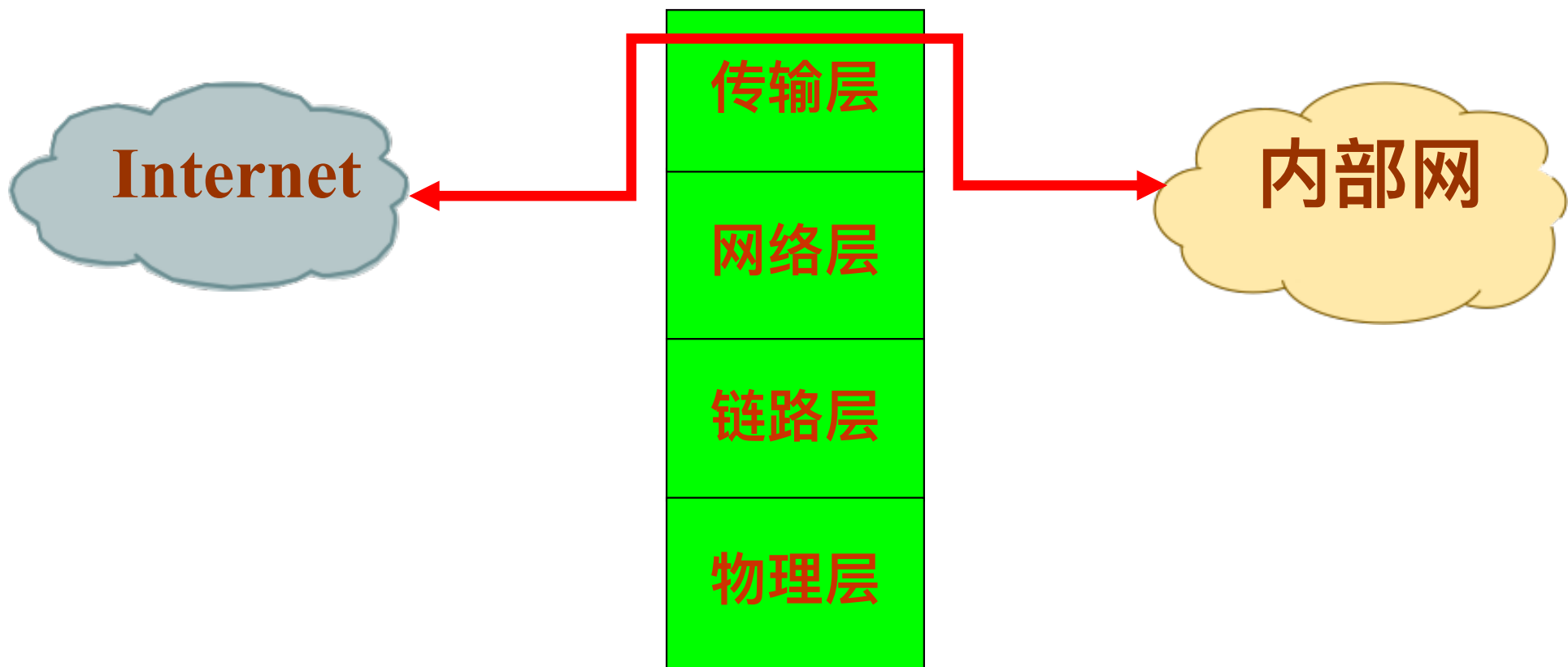


图4.6



无状态包过滤防火墙的优缺点

不能识别IP欺诈, 不能识别连接

- 无状态包过滤防火墙最大的好处是速度快、效率高，对流量的管理较出色；由于所有的通信必须通过防火墙，所以绕过是困难的；同时对用户和应用是透明的。
- 无状态包过滤防火墙的缺点也很明显：它允许外部网络直接连接到内部网络主机；只要数据包符合ACL规则都可以通过，因此它不能区分包的“好”与“坏”；它不能识别IP欺诈。它也不支持用户身份认证，不提供日志功能；虽然可以过滤端口，但是不能过滤服务。



IP欺骗

伪装内部主机 → 可识别

伪装外部主机 → 不可识别

- 当外部主机伪装内部主机的IP地址时，防火墙能够阻止这种类型的IP欺骗。
- 但是当外部主机伪装成可信的外部主机的IP地址时，防火墙却不能阻止它们。
- 由于无状态包过滤防火墙不能为挂起的通信维持一个记录，所以它就必须根据数据包的格式来判断该数据包是否属于先前所允许的对话。这就使其有受到IP欺诈的可能性，并且无法识别UDP数据包和ICMP包的状态。



无法过滤服务

- 对于一些比较新的多媒体应用在会话开始之前端口号是未知的。
- 例如，Web服务器默认端口为80，而计算机上又安装了RealPlayer，那么它会搜寻可以允许连接到RealAudio服务器的端口，而不管这个端口是否被其他协议所使用，RealPlayer正好是使用80端口而搜寻的。就这样无意中，RealPlayer就利用了Web服务器的端口。

RealPlayer 就用了 80 端口
但 80 端口没有被封锁



有状态包过滤防火墙

- 有状态包过滤也叫状态包检查SPI (State-fulPacket Inspection) 或者动态包过滤 (Dynamic packet filter), 后来发展成为包状态监测技术, 它是包过滤器和应用级网关的一种折衷方案。具有包过滤机制的速度和灵活, 也有应用级网关的应用层安全的优点。



SPI防火墙

不使用代理, 但检查数据部分

- 采用SPI技术的防火墙除了有一个过滤规则集外, 还要对通过它的每一个连接都进行跟踪, 汲取相关的通信和应用程序的状态信息, 形成一个当前连接的状态列表。列表中至少包括源和目的IP地址、源和目的端口号、TCP序列号信息, 以及与那个特定会话相关的每条TCP/UDP连接的附加标记。当一个会话经过防火墙时, SPI防火墙把数据包与状态表、规则集进行对比, 只允许与状态表和规则集匹配的项通过。

匹配规则集和状态列表

避免IP欺诈



SPI防火墙 (续)

- 在维护了一张状态表后，防火墙就可以利用更多的信息来决定是否允许数据包通过，大大降低了把数据包伪装成一个正在使用的连接的一部分的可能性。
- SPI防火墙能够对特定类型数据包的数据进行检测。如运行FTP协议的服务器和客户端程序有许多漏洞，其中一部分漏洞来源于不正确的请求或者不正确的命令。
- SPI防火墙不行使代理功能，即不在源主机和目的之间建立中转连接；也不提供与应用层网关相同程度的保护，而是仅在数据包的数据部分查找特定的字符串。



SPI防火墙的处理过程

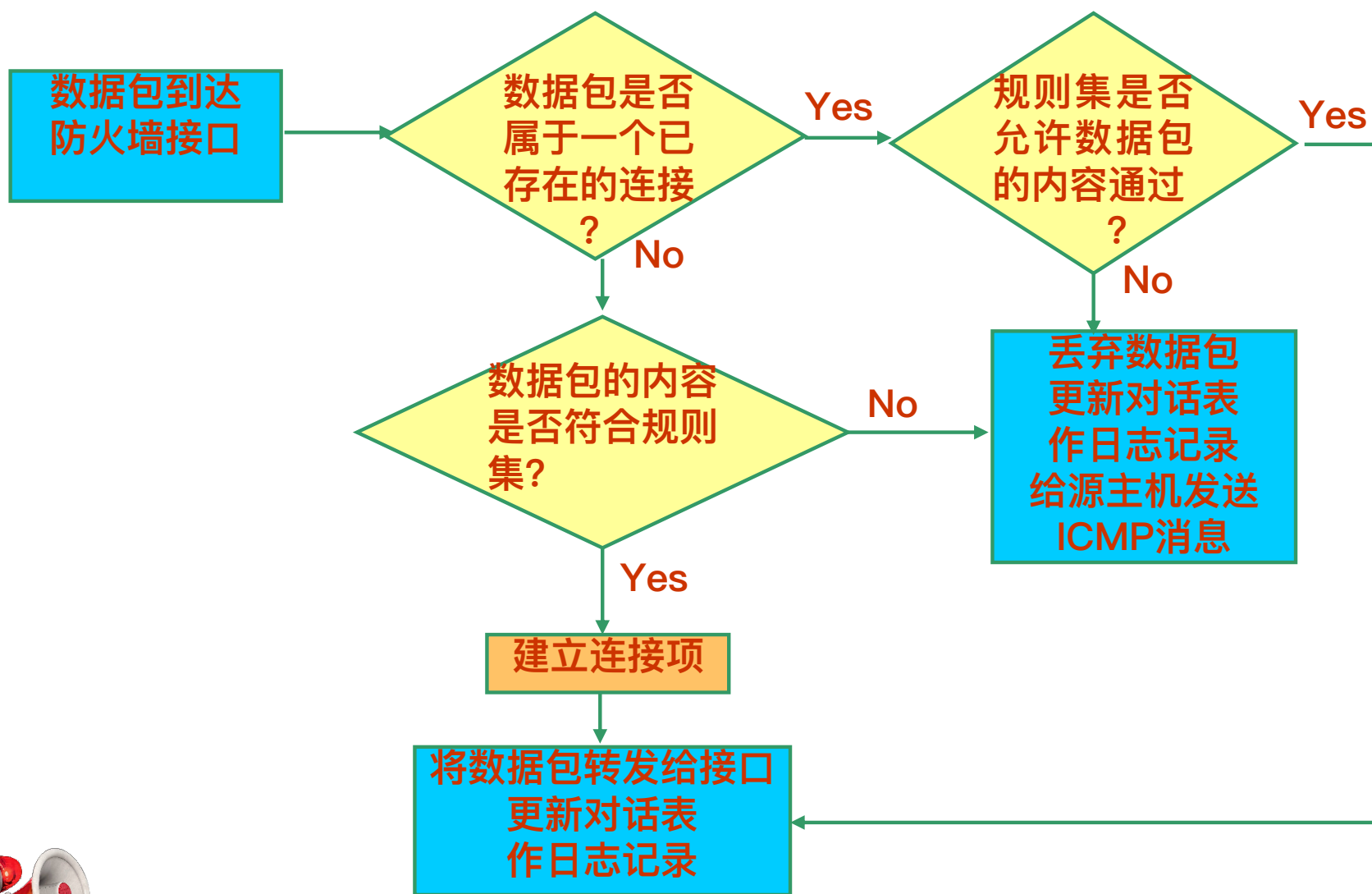


图 4.7



主机A发出连接请求通过SPI防火墙

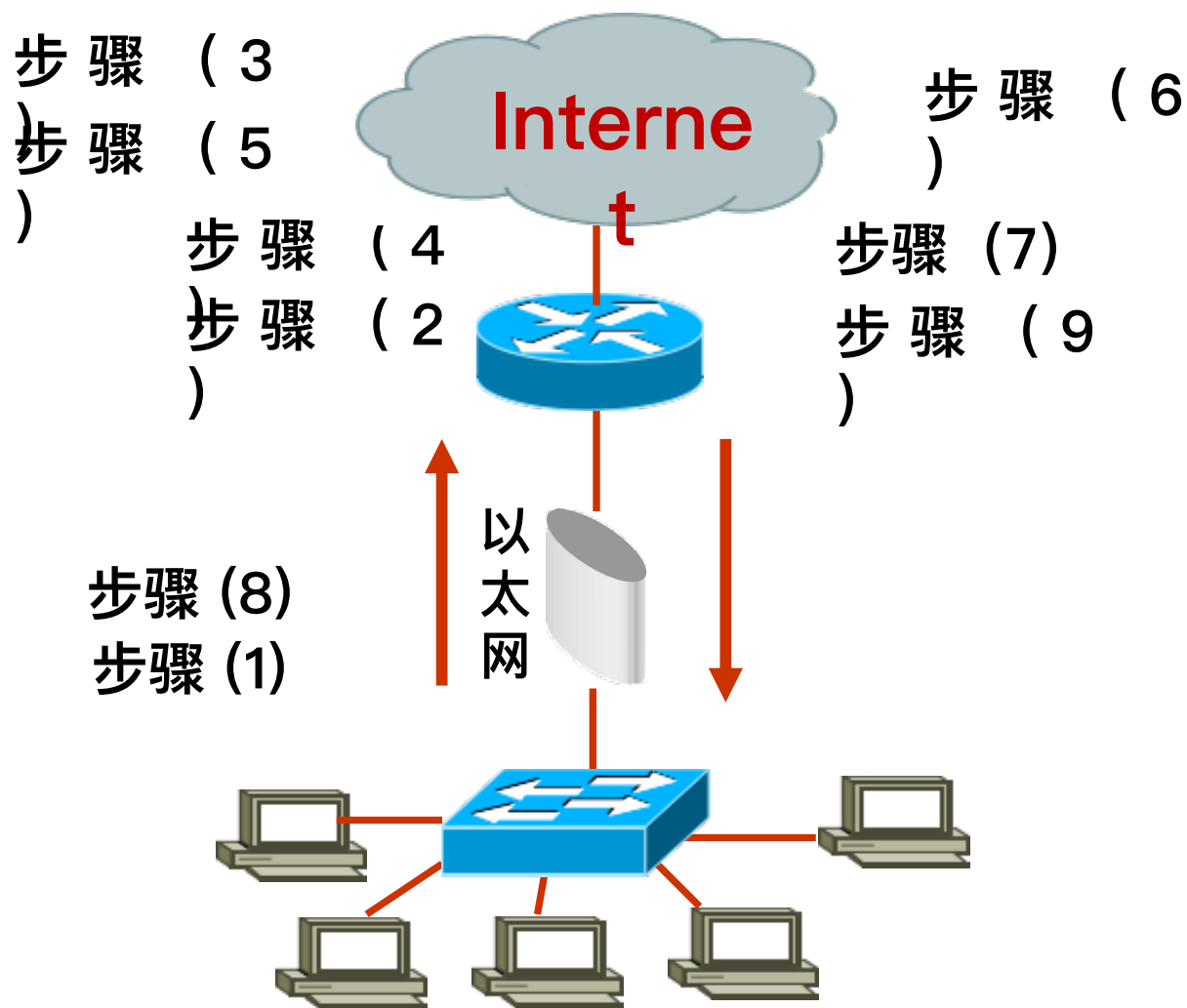


图4.8



举 例

- 例1主机A试图访问www.sohu.com，它必须通过路由器，而该路由器被配置成SPI防火墙，下面是主机A发出连接请求的工作过程，见图4.8。
 - 1) A发出连接请求到 www.sohu.com；
 - 2) 请求到达路由器，路由器检查状态表；
 - 3) 如果有连接存在，且状态表正常，允许数据包通过；
 - 4) 如果无连接存在，创建状态项,将请求与防火墙规则集进行比较；
 - 5) 如果规则允许内部主机可以访问TCP/80。则允许数据包通过；
 - 6) 数据包被Web服务器接收；
 - 7) SYN/ACK信息回到路由器，路由器检查状态表；
 - 8) 状态表正确，允许数据包通过，数据包到达最先发出请求的计算机；
 - 9) 如果规则不允许内部主机访问TCP/80。则禁止数据包通过，路由器发送ICMP消息。



SPI防火墙的优缺点

- 优点：具有识别带有欺骗性源IP地址包的能力；检查的层面能够从网络层至应用层；具有详细记录通过的每个包的信息的能力，其中包括应用程序对包的请求，连接的持续时间，内部和外部系统所做的连接请求等。
- 缺点：所有这些记录、测试和分析工作可能会造成网络连接的某种迟滞，特别是在同时有许多连接激活的时候，或者是有大量的过滤网络通信的规则存在时。但是，硬件速度越快，这个问题就越不易察觉。



4.1.3 代理服务防火墙

- 最初，代理服务器将常用的页面存储在缓冲区中，以便提高网络通信的速度。后来代理服务器逐渐发展为能够提供强大安全功能的一种技术。代理能在应用层实现防火墙功能，代理技术针对每一个特定应用都有一个程序，通过代理可以实现比包过滤更严格的安全策略。

包过滤技术只在运输层和网络层

→ 应用级网关



代理服务器原理

代理服务器（Proxy Server）防火墙是基于软件的。运行在内部用户和外部主机之间，并且在它们之间转发数据，它像真的墙一样挡在内部网和Internet之间。从外面来的访问者只能看到代理服务器但看不见任何内部资源；而内部客户根本感觉不到代理服务器的存在，他们可以自由访问外部站点。代理可以提供极好的访问控制、登录能力以及地址转换功能，对进出防火墙的信息进行记录，便于管理员监视和管理系统。



主机A发出连接请求通过 代理服务器防火墙

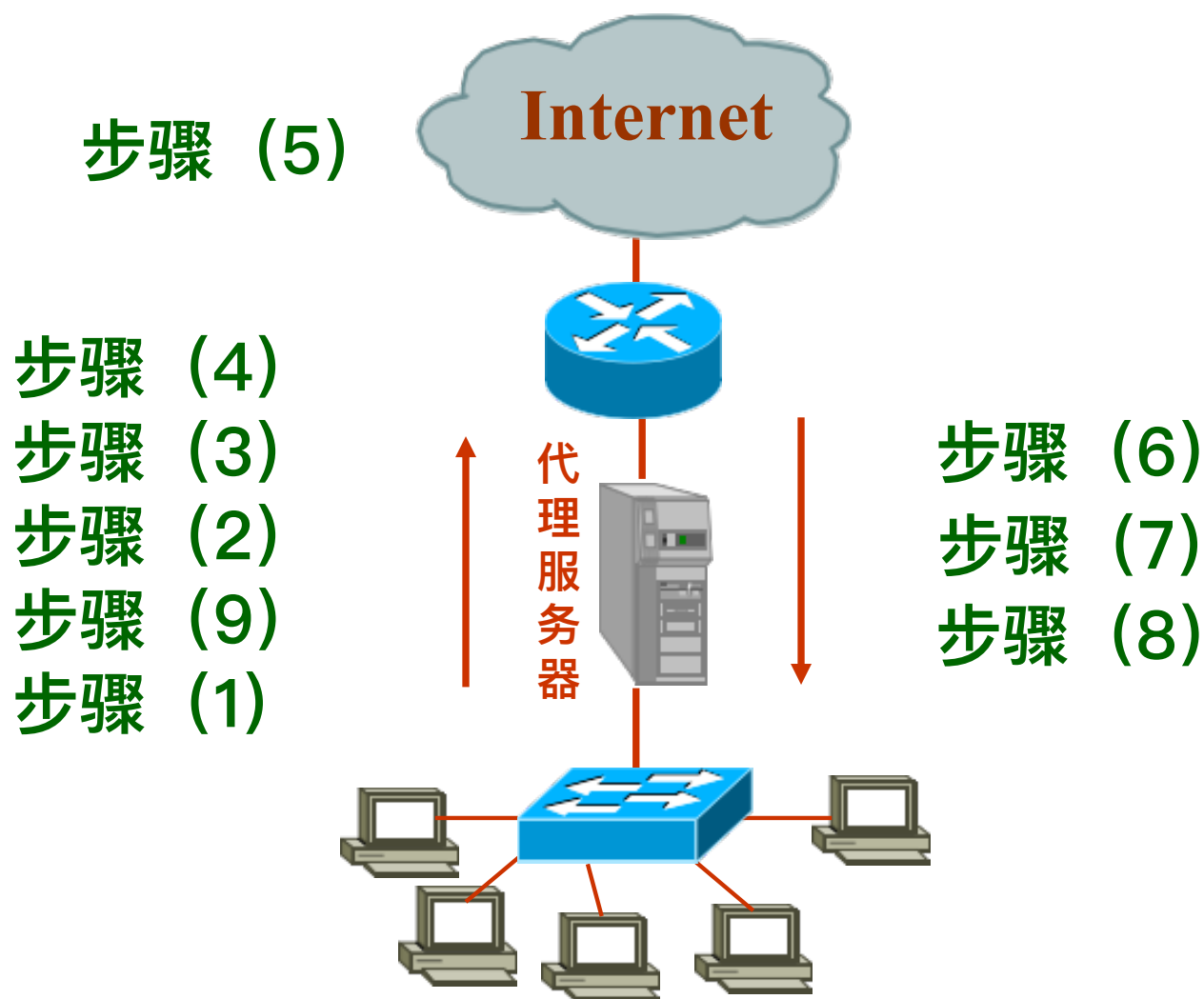


图4.9



举 例

例2主机A试图访问 `www.sohu.com` ，它通过代理服务器到达网关。下面是主机A发出连接请求的工作过程

主机发出访问
Web 网站的请
求；

如果不允许该请
求发出，代理服
务器拒绝请求，
发送ICMP消息
给源主机；

代理服务器将数
据包发给目的计
算机，数据包显
示源IP地址来自
代理服务器；

请求到达代理服
务器，代理服务
器检查防火墙规
则集，检查数据
包报头信息和数
据；

如果允许该请求
发出，代理服务
器修改源IP地址，
创建数据包；



举例 (续)

返回的数据包又被发送到代理服务器。服务器再次根据防火墙规则集检查数据包报头信息和数据；

如果允许该数据包进入内部网，代理服务器将它发给最先发出请求的计算机；

如果不允许该数据包进入内部网，代理服务器丢弃该数据包，发送ICMP消息；

数据包到达最先发出请求的计算机，此时数据包显示来自外部主机而不是代理服务器。



对内透明

代理服务器和包过滤的比较

代理服务器对整个IP包的数据进行扫描，因此它比包过滤器提供更详细的日志文件。

如果数据包和包过滤规则匹配，就允许数据包通过防火墙，而代理服务器要用新的源IP地址重建数据包，这样对外隐藏了内部用户。

使用代理服务器，意味着在Internet上必须有一个服务器，且内部主机不能直接与外部主机相连。带有恶意攻击的外部数据包也就不能到达内部主机。

对网络通信而言，如果包过滤器由于某种原因不能工作，可能出现的结果是所有的数据包都能到达内部网；而如果代理服务器由于某种原因不能工作，整个网络通信将被终止。



电路级网关

- 电路级网关不允许TCP端到端的连接，而是要建立两个连接。其中一个连接是网关到内部主机，另一个是网关到外部主机。一旦两个连接被建立，网关只简单地进行数据中转，即它只在内部连接和外部连接之间来回**拷贝字节**，并将**源IP地址转换为自己的地址**，使得外界认为是网关和目的地址在进行连接，电路级网关防火墙如图4.10所示。由于电路级网关在会话建立连接后不对所传输的内容作进一步的分析，因此安全性稍低。

电路级网关，仅进行数据的中转



电路级网关防火墙

电路级网关

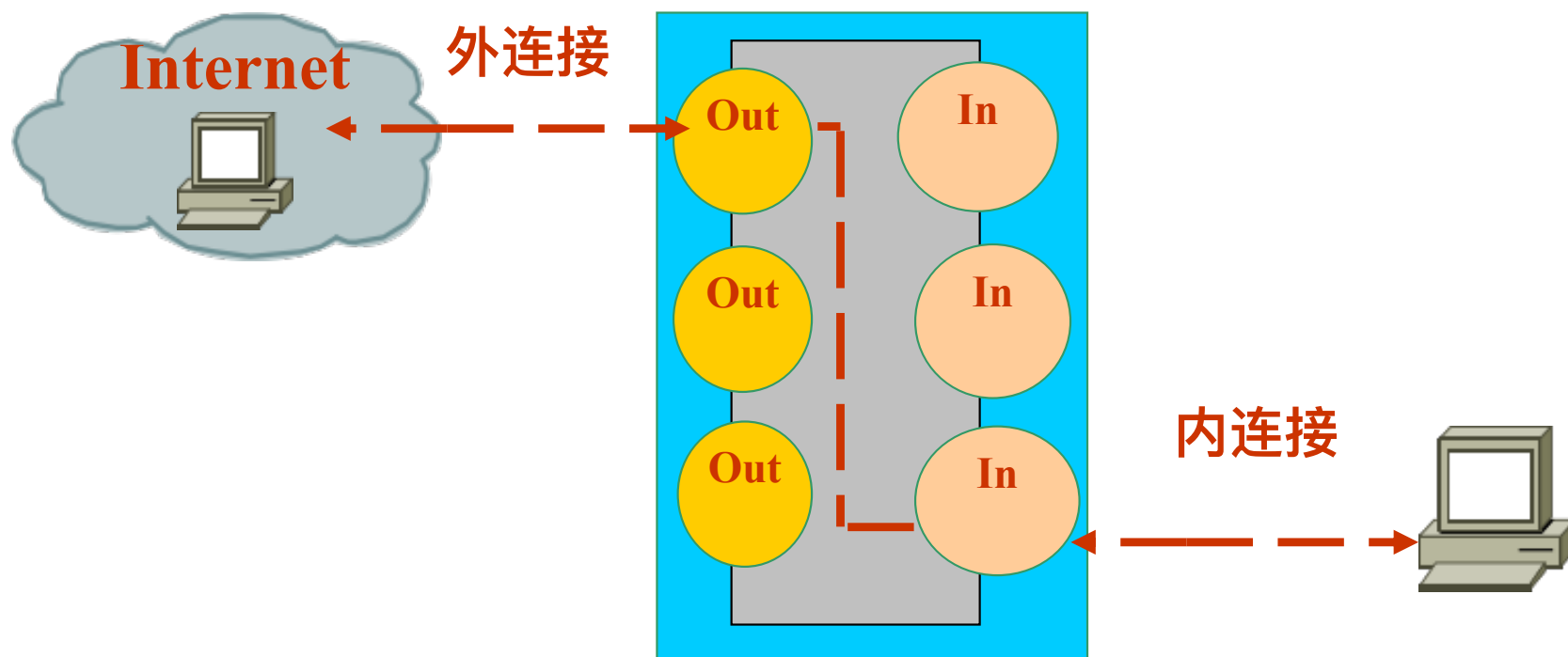


图4.10



举 例

例3主机A试图访问 www.sohu.com，它要通过一个电路级网关。下面是主机A发出连接请求的工作过程。

主机发出访问Web站点的请求；

该主机上的客户端应用程序将请求发送到电路级网关的内部接口；

如果需要身份验证，网关会提示用户进行身份验证；

如果规则集允许进行连接，网关向目的URL发出DNS请求，接着 将自己的IP地址作为源IP地址，与目的IP地址建立一个连接；

如果规则集不允许进行连接，网关将拒绝访问站点的请求，并发送ICMP消息给源主机；

如果用户的身份验证通过，网关将目的URL与防火墙规则集进行比较，该规则集包括允许或者禁止的URL列表；

网关接收到Web站点的应答后，将转发该应答给最先发出请求的计算机。

不看数据包



电路级网关的优缺点

电路级网关的优点是提供网络地址转换NAT（Network Address Translation），在使用内部网络地址机制时为网络管理员实现安全提供了很大的灵活性；和基于包过滤防火墙一样的规则，具有包过滤防火墙提供的所有优点。

电路级网关的缺点是不能很好地区分好包与坏包、易受IP欺骗类的攻击；需要修改应用程序和执行程序；要求终端用户通过身份认证。



应用级网关

代理服务、应用级网关、应用程序代理这些术语指的都是同一种保护方式。

应用级网关主要工作在应用层。它检查进出的数据包，如图4.11所示，通过自身（网关）复制传递数据，防止在内部网主机与internet主机间直接建立联系。

它能够理解应用层上的协议，能够作复杂一些的访问控制，并做精细的注册和审核。



基本工作过程

当客户机需要使用服务器上的数据时，首先将数据**请求**发给代理服务器，代理服务器再根据这一请求向服务器**索取数据**，然后再由代理服务器将数据传输给客户机。由于外部系统与内部服务器之间没有直接的数据通道，外部的恶意侵害也就很难伤害到内部网。



基本工作过程 (续)

在应用级网关中，每一种协议都需要相应的代理软件，常用的代理服务软件有如HTTP、SMTP、FTP、Telnet等，但是对于新开发的应用，尚没有相应的代理服务。有些应用级网关还存储Internet上的那些被频繁使用的页面。当用户请求的页面在服务器缓存中存在时，服务器将检查所缓存的页面是否是最新的版本（即该页面是否已更新），如果是最新版本，则直接提交给用户，否则，到真正的服务器上请求最新的页面，然后再转发给用户。



应用级网关防火墙

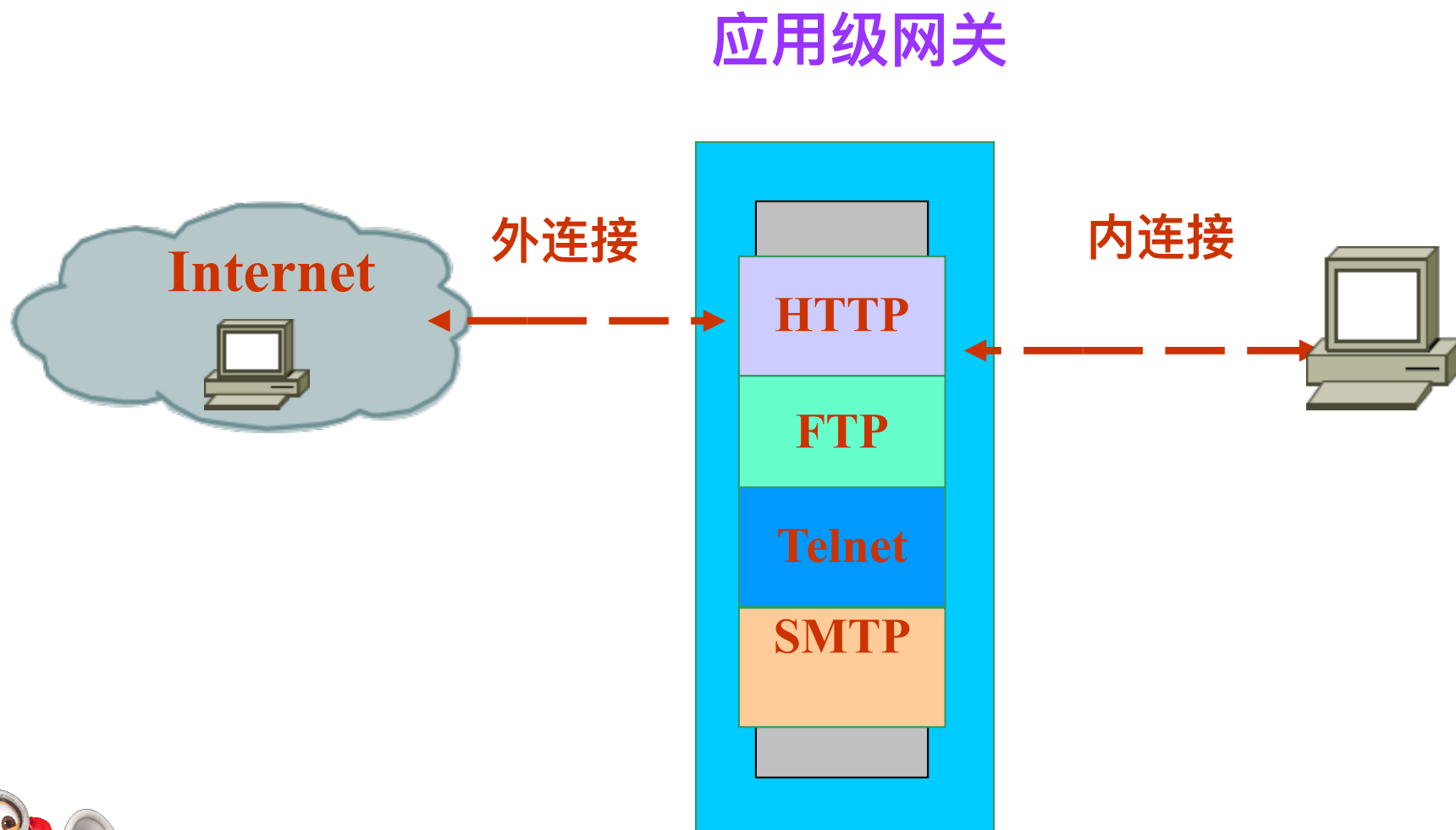


图4.11



举 例

- 例4 一个Telnet服务器允许远程管理员对其执行某些特定的操作。该Telnet网关对Internet可见，但是隐藏了其真实主机名，以便不受信任的网络不能识别它的真实身份，连接它的过程如图4.12。
- 应用级网关一般由双宿主主机或者多宿主主机（在主机至少插有两块网卡）担任。在本例中，应用级网关有两块网卡，一块用于连接受保护的内部网，一块连接Internet.



远程连接应用级网关

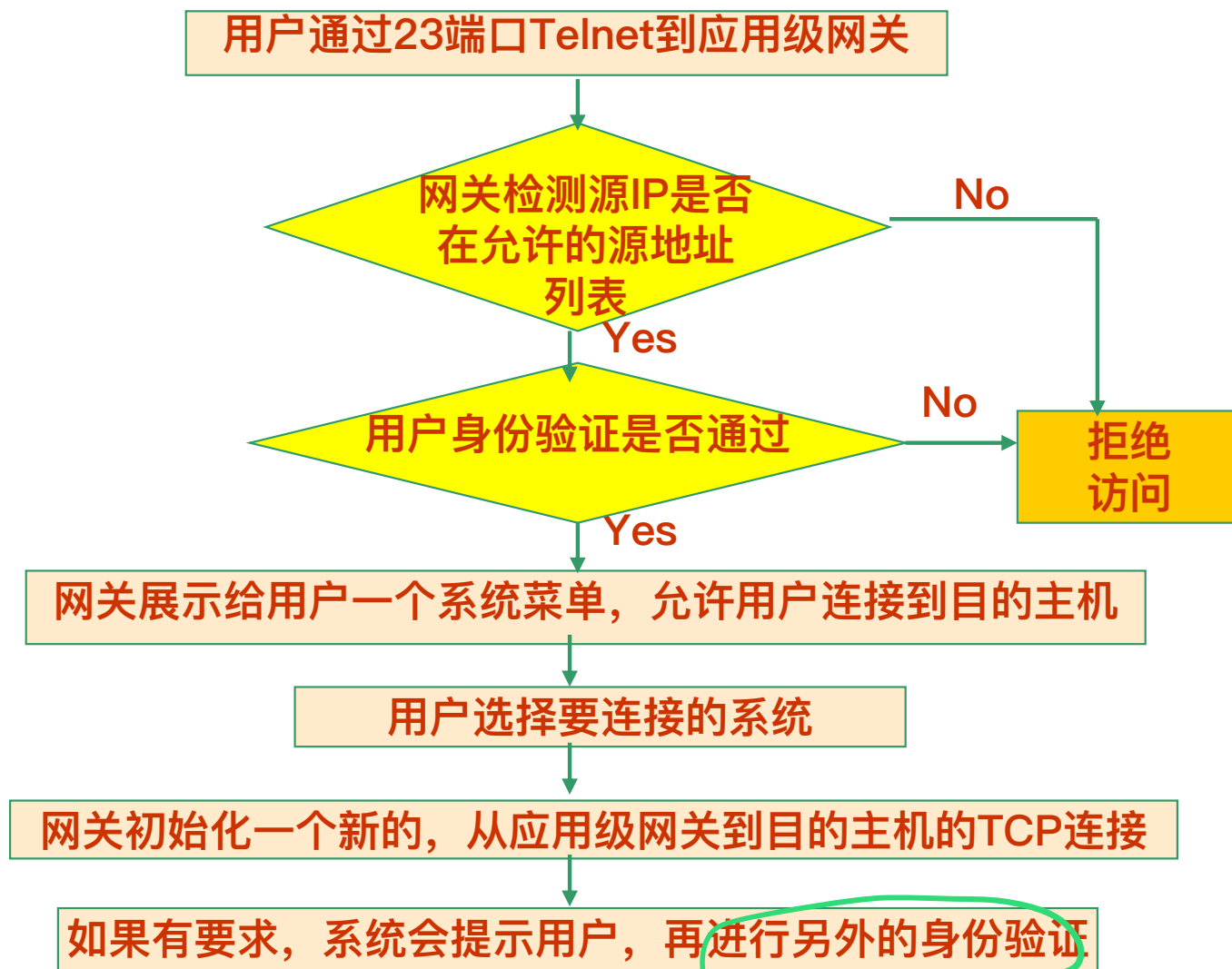



图4.12


应用级操作



应用级网关的优缺点



应用级网关的优点是能够有效地实现防火墙内外计算机系统的隔离，安全性好，还可用于实施较强的数据流监控、过滤、记录和报告等功能。



缺点是实现麻烦，对于那些为了使用代理服务器而修改自己应用的终端用户来说，这种选择缺乏透明度。

另外由于代理服务器必须采用操作系统服务来执行代理过程，所以它通常是建立在操作系统之上的，由此带来的问题是增加了开销、降低了性能，而且由于通用操作系统是众所周知的，所以该操作系统容易被攻击的漏洞也是公开的。



自适应代理防火墙

虽然应用代理防火墙具有很好的安全性，但速度不尽如人意。自适应代理技术（Adaptive proxy）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度等优点，组成这种类型防火墙的基本要素有两个：自适应代理服务器（Adaptive Proxy Server）与动态包过滤器。在自适应代理防火墙中，初始的安全检查仍在应用层中进行，保证实现传统防火墙的最大安全性；而一旦可信任身份得到认证，建立了安全通道，随后的数据包就可重新定向到网络层。这使得它在毫不损失安全性的基础上将代理服务器防火墙的性能提高10倍以上。

仅检查IP



4.1.4 复合防火墙

由于防火墙所处的优越位置（内部网与Internet的分界点），在实际应用中除了基本的过滤和访问控制外，防火墙又添加了NAT、VPN、IDS、AAA、QoS、加密、内容过滤、防病毒、路由管理、网络监视等功能。刚开始这些功能都是由另外的设备提供，这些设备在网络中的位置处于串行或者并行。

目前通常的解决办法是将这些特性合并到防火墙中，当整合了这些功能的防火墙正常运转时，网络连接既安全可靠，又效率高。



网络地址转换

11

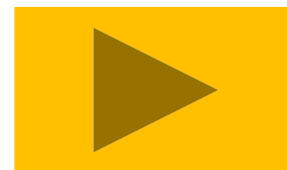
网络地址转换NAT（Network Address Translation），是一种将一个IP地址域映射到另一个IP地址域的技术，从而为终端主机提供透明路由。NAT常用于私有地址域与公用地址域的转换以解决IP地址匮乏问题。在防火墙上实现NAT后，可以隐藏受保护网络的内部拓扑结构，在一定程度上提高网络的安全性。它可以在边界路由器、包过滤防火墙以及代理服务防火墙上实现。

由内网到外网



虚拟专用网络

虚拟专用网络VPN (Virtual Private Network), 是在公共网络中建立专用网络, 数据通过安全的“加密通道”在公网中传播。目前, VPN的安全保证主要是通过防火墙技术、路由器配以隧道技术、加密协议和安全密钥来实现的, 用于公司总部和分支机构、合作伙伴之间以及移动办公用户通过公网进行通信, 并且达到安全的目的。



入侵检测系统

防火墙为第一层
第二层防线

入侵检测系统IDS (Intrusion Detection System) ，是主动保护自己免受攻击的一种网络安全技术。它要对侵入计算机网络和主机的行为进行发现并进行一定的阻止。通常IDS安装在计算机网络或计算机系统的若干关键点，进行网络和系统的信息收集和分析，从中发现网络或系统中是否有违反安全策略的行为和攻击的迹象。它扩展了系统管理员的安全管理能力（包括安全审计、监视、攻击识别和响应），提高了信息安全基础结构的完整性。



认证、授权、审计

认证、授权、审计AAA (Authentication, Authorization, Accounting), Cisco系统表述集中式身份验证服务器三大主要功能的术语，它是网络安全策略的一个组成部分。

认证：确认远端访问用户的身份，判断访问者是否为合法的网络用户。

授权：对用户进行认证后，授权服务将决定该用户可以访问哪些资源，允许该用户执行哪些操作。

审计：为统计、计费 and 审计目的记录用户使用网络服务中的所有操作，包括使用的服务类型、起始时间、数据流量等信息。



服务质量

服务质量QoS (Quality of Service)，是网络的一种安全机制。拥有QoS的网络是一种智能网络，它可以对网络上传输的视音频流等对实时性要求较高的数据提供优先服务，从而保证较低的延迟。如果不实施QoS，IP电话、电视会议及关键任务数据等应用只能作为“尽力而为”业务传输，这将导致在网络拥塞时话音和视频的不稳定性。



其 它

防火墙还应包含先进的鉴别措施，如信息的保密性保护、信息的完整性校验，以及授权管理技术等。网络管理安全越完善，体系架构就越复杂。管理网络的多台安全设备，还需要集中的网管。



4.1.5 个人防火墙

个人版防火墙是安装在PC 机系统里的一段“代码墙”把你的电脑和Internet分隔开。它检查到达防火墙两端的所有数据包，无论是进入还是发出，从而决定该拦截这个包还是将其放行。也就是说：在不妨碍你正常上网浏览的同时，阻止Internet上的其他用户对你的计算机进行的非法访问。

一个好的个人版防火墙必须是低的系统资源消耗，高的处理效率，具有简单易懂的设置界面，具有灵活而有效的规则设定。



4.2 防火墙体系结构

防火墙是保护网络安全的一个很好的选择，**设置防火墙、选择合适的防火墙并配置它**，是用好防火墙的三大关键任务。如何设置它，应该将它放到什么位置。在网络设计时要考虑网络安全问题，所以应该考虑网络安全拓扑内容。关注网络安全拓扑设计对阻止网络攻击大有帮助。并且能够使不同设备的安全特性得到最有效的使用。



4.2.1. 堡垒主机

“堡垒”一词来源于中世纪，指城堡中特别加固的部分，用于发现和抵御攻击者的进攻。

在网络中堡垒主机是经过加固，安装了防火墙软件的计算机。它对外界提供一些必要的服务，也可以被内部用户访问。通常它只提供~~一种服务~~，因为提供的服务越多，导致的安全隐患的可能性也就越大。

它应该位于非军事区DMZ（Demilitarized Zone），也称为停火区或者周边网络。如果堡垒主机提供~~代理服务~~，它会知道自己将要为哪些应用提供代理。



4.2.1. 堡垒主机

地域

华南地区 华东地区 华北地区 西南地区

广州 上海 南京 北京

不同地域云产品之间内网不互通，创建成功后不支持切换地域

可用区

北京一区 北京二区 北京三区

网络类型

私有网络 基础网络

规格

基础版S0 基础版S1 基础版S2

购买时长

1个月 2个月 3个月 6个月

☒ 账户余额足够时，实例到期后按月自动续费

当前配置

地域 北京

可用区 北京一区

网络 基础网络

子网

规格 旗舰版S1

购买时长 1个月

堡垒机参数

节点数 2000节点授权

并发数 2000

CPU 4核

内存 16G

公网带宽 16M

弹性硬盘 2T

地域

华南地区 华东地区 华北地区 西南地区

广州 上海 南京 北京 成都 重庆

不同地域云产品之间内网不互通，创建成功后不支持切换地域

可用区

北京一区 北京二区

网络类型

私有网络 基础网络

规格

基础版S0 基础版S1

购买时长

1个月 2个月

☒ 账户余额足够时，实例到期后按月自动续费

当前配置

地域 北京

可用区 北京一区

网络 基础网络

子网

规格 旗舰版S1

购买时长 1个月

堡垒机参数

节点数 2000节点授权

并发数 2000

CPU 4核

内存 16G

公网带宽 16M

弹性硬盘 2T

地域

华南地区 华东地区 华北地区 西南地区

广州 上海 南京 北京 成都 重庆

不同地域云产品之间内网不互通，创建成功后不支持切换地域

可用区

北京一区 北京二区 北京三区 北京四区 北京五区

网络类型

私有网络 基础网络

规格

基础版S0 基础版S1 基础版S2 企业版S1 企业版S2 旗舰版S1 旗舰版S2

购买时长

1个月 2个月 3个月 6个月 1年 2年 3年

☒ 账户余额足够时，实例到期后按月自动续费

当前配置

地域 北京

可用区 北京一区

网络 基础网络

子网

规格 旗舰版S1

购买时长 1个月

堡垒机参数

节点数 2000节点授权

并发数 2000

CPU 4核

内存 16G

公网带宽 16M

弹性硬盘 2T

总费用: 堡垒机费用
1,500.00 元 4,500.00元

立即支付

总费用: 堡垒机费用
5,500.00 元 9,500.00元

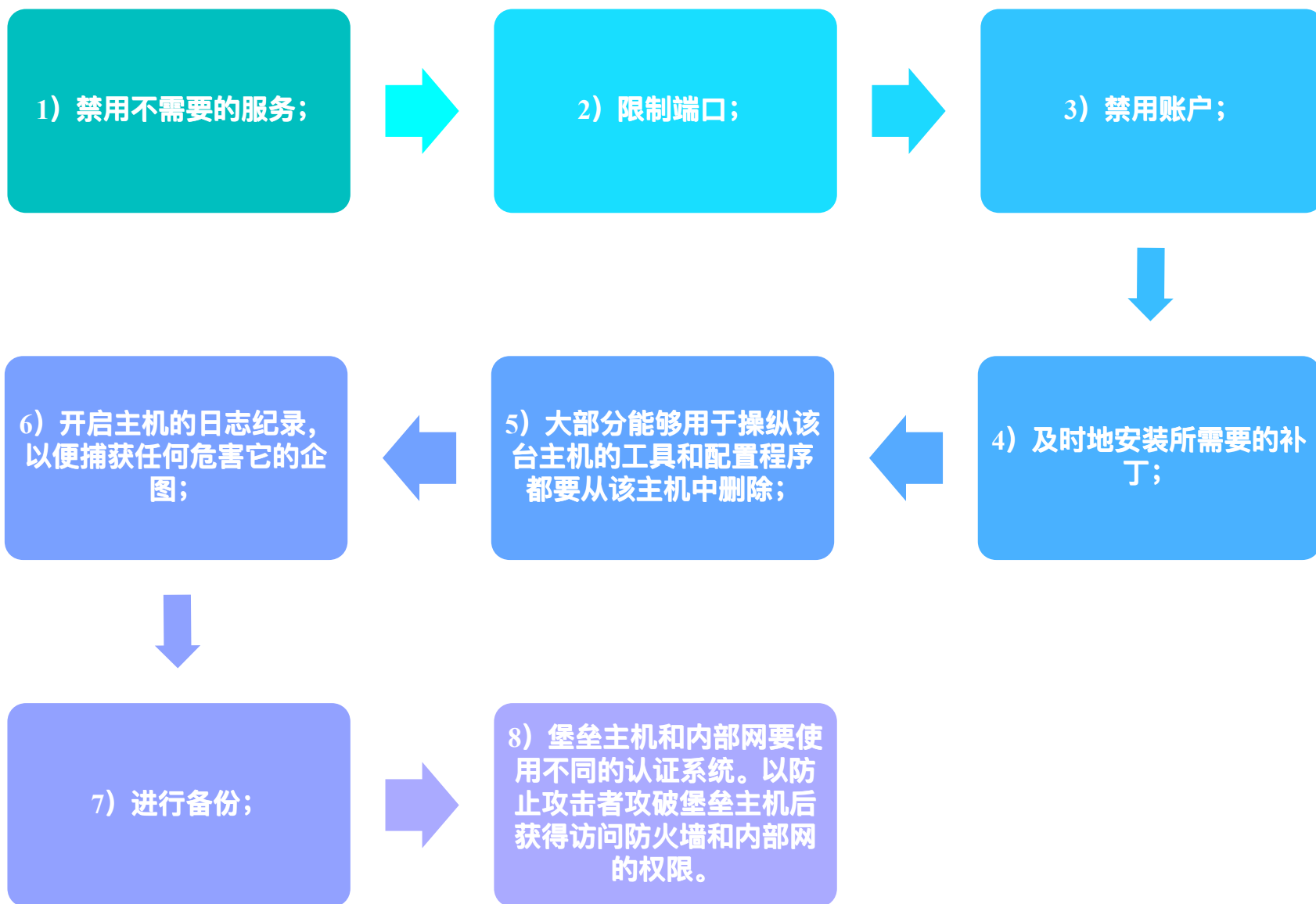
立即支付

总费用: 堡垒机费用 CVM费用 ⑦
9,500.00 元 9,500.00元 2,025.50 元 2,025.50元

立即支付

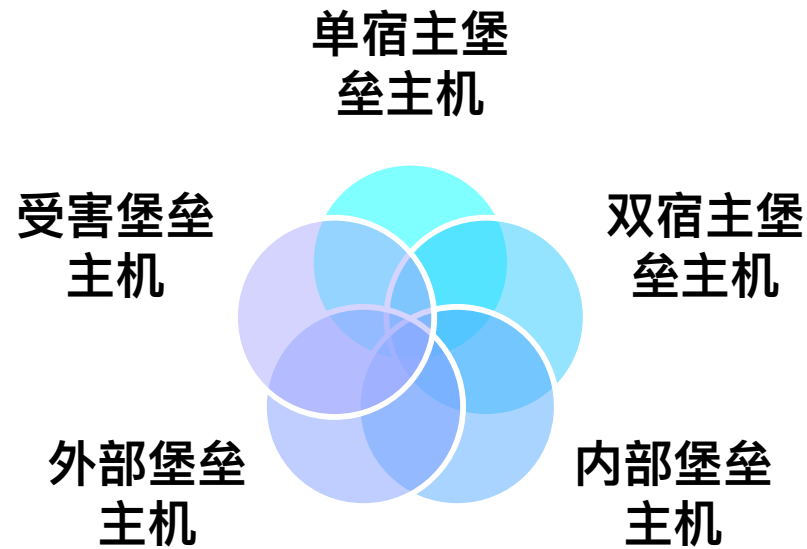


配置堡垒主机

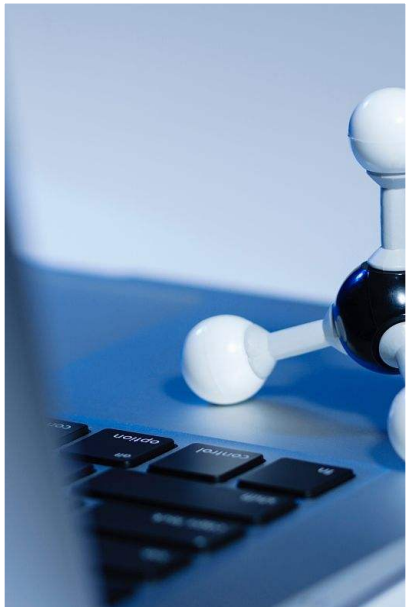


堡垒主机的配置类型

宿主机网卡的数量



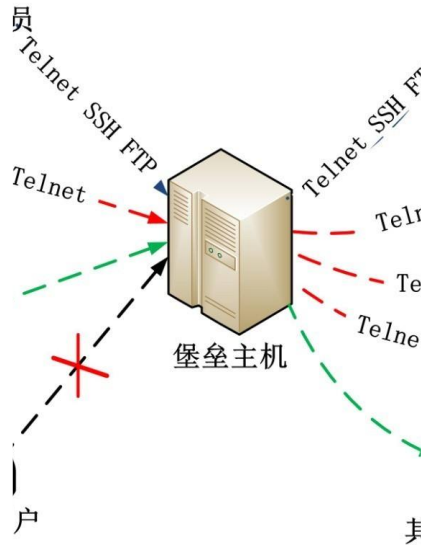
单宿主堡垒主机



有一块网卡的堡垒主机做防火墙，通常用于应用级网关防火墙。将外部路由器配置成所有进来的数据均发送到堡垒主机上，同时将全部内部客户端配置成所有出去的数据都发送到这台堡垒主机上。堡垒主机以安全方针作为依据检验这些数据。它的主要缺点是可以配置路由器使信息直接进入内部网络，而完全绕过堡垒主机；内部用户也可以配置他们的主机，绕过堡垒主机把信息直接发送到路由器上。



双宿主堡垒主机



有两块网卡的堡垒主机做防火墙，两块网卡各自与内外部网络相连。但是内外部网络之间不能直接通信，内外部网络之间的数据流被双宿主机完全切断。它采用主机取代路由器执行安全控制功能。可以通过运行代理软件或者让用户直接注册到其上来提供网络控制。当一个黑客若要访问内部网络时，他必须首先攻破双宿主堡垒主机，这使得网络管理员有时间阻止对入侵做出反应。



内部堡垒主机

堡垒主机与内部网通信，以便转发从外部网获得的信息。这类堡垒主机启用了较多的服务，并开放了较多的端口以便满足应用程序的需要。

转发外部网请求



外部堡垒主机

暴露在外网

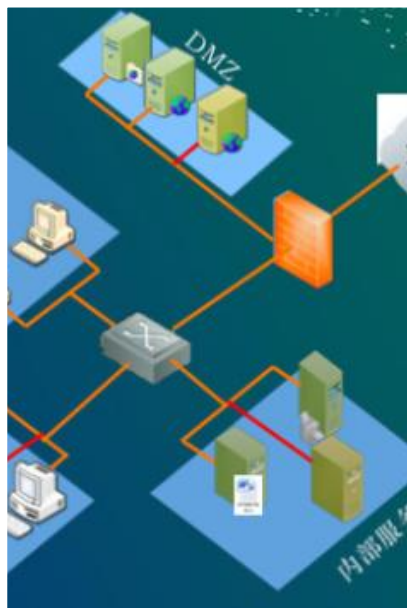
不转发外部请求，自己处理请求

堡垒主机为Internet 提供公共服务，它不向内部网转发任何请求，而是自己处理请求。它只提供非常有限的服务，并且只开放有限的端口来满足这类服务。它需要更多的防御和保护，并应切断对内部网的任何访问。



受害堡垒主机

蜜罐



该堡垒主机是故意向攻击者暴露的目标，也被称作蜜罐（honeypot）或者陷阱。设置它的主要目的是引诱不法者的攻击，让黑客误以为已经成功侵入网络，并且让黑客继续“为所欲为”，以便赢得时间跟踪他们。该堡垒主机只包含最起码的最小服务配置以便运行相应的程序。



4.2.2. 非军事区

在现代网络安全设计中用到的最关键的思想之一是按照**功能**或者**部门**将网络分割成**网段**。不同的网段对安全有着不同的需要。

以太网是一个广播的网络，网络上的任何机器都有可能查看到这个网络上的所有通信。如果黑客侵入网络，可以容易地截获所有通信。为了配置和管理方便，**内部网需要向外提供服务的服务器往往放在一个单独的网段，这个网段便是DMZ**。DMZ在内部网之外，具有一个与内部网不同的网络号，连接到防火墙，提供公共服务。

↓
往往把数据置于堡垒主机上



创建DMZ的方法

创建DMZ的方法有很多，怎样创建它依赖于网络的安全需要，也依赖于对它的预算约束。创建DMZ的常用方法如下

三接口
使用一个三脚防火墙

将DMZ置于防火墙之外，公网和防火墙之间

将DMZ置于防火墙之外，但不在公网和防火墙之间的通道上

两个防火墙，一个DMZ

“脏”DMZ



使用一个三脚防火墙

使用一个有三个接口的防火墙（三宿主防火墙）创建隔离区，如图4.12所示，每个隔离区成为这个防火墙接口的一员。防火墙提供区之间的隔离，也提供了DMZ的安全。



DMZ在三脚防火墙中 (续)

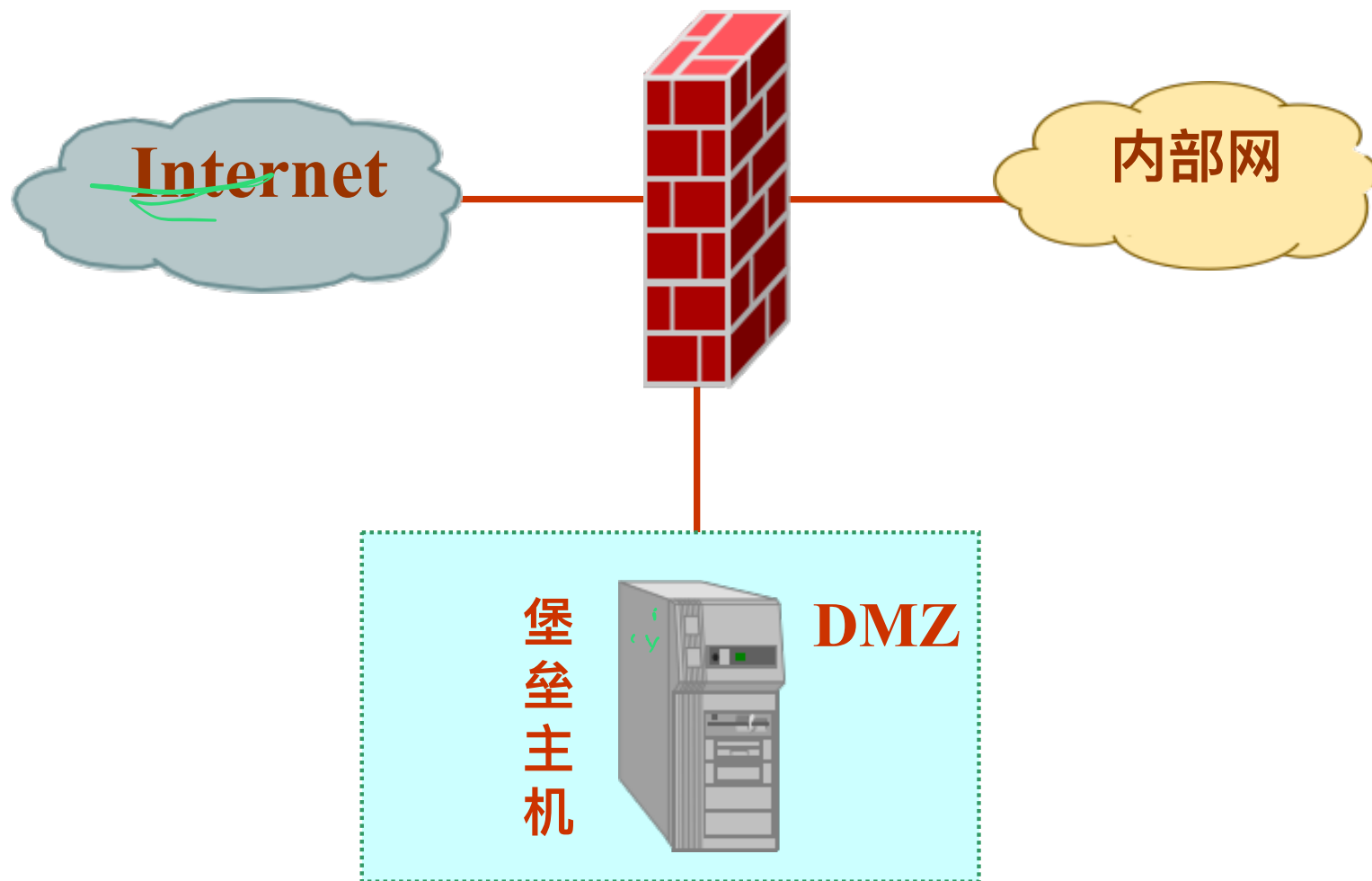


图4.12



DMZ置于防火墙之外 公网和防火墙之间

需要通过防火墙的流量首先通过DMZ。缺点是DMZ暴露在公共面一侧，因此不推荐使用这种配置，如图4.13所示。



DMZ置于防火墙之外 公网和防火墙之间 (续)

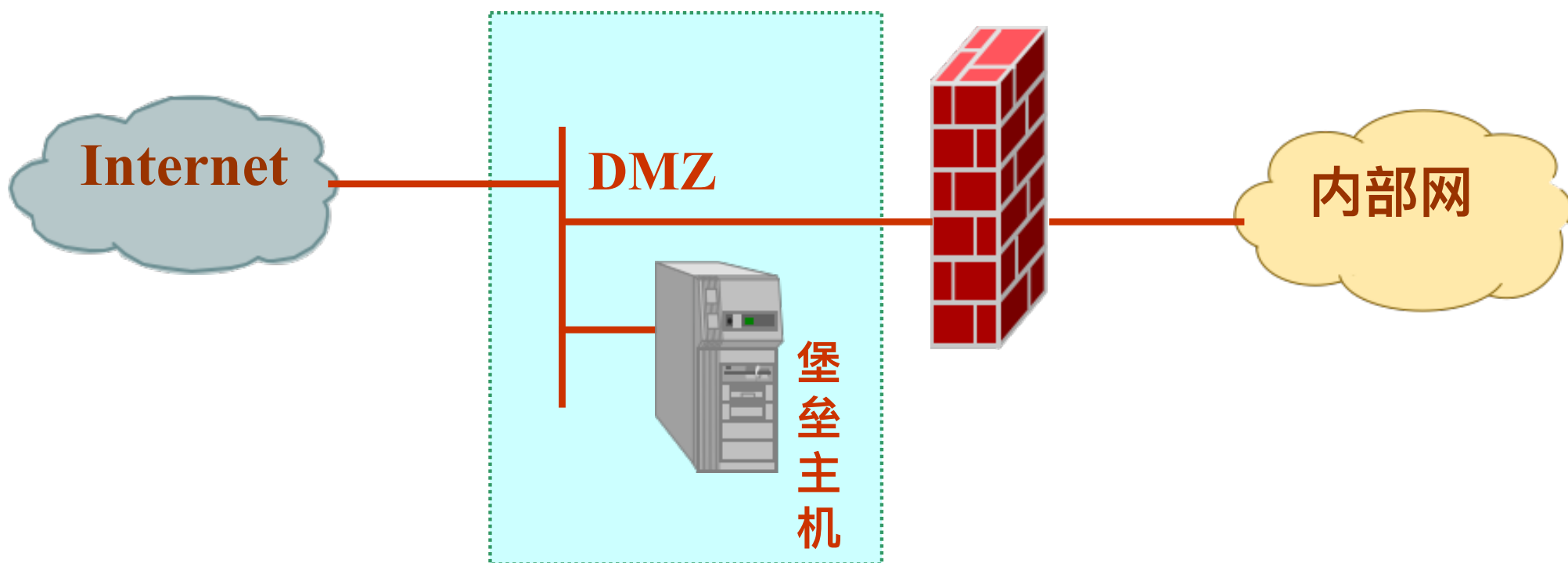


图4.13



DMZ置于防火墙之外 不在公网和防火墙之间的通道上

DMZ位于边缘路由器的一个接口，没有与防火墙直接相连，如图4.14所示，从DMZ到防火墙形成一个隔离层。在这种配置中**路由器**能够用于拒绝所有从DMZ子网到防火墙所在的子网的访问，当位于DMZ子网的主机受到危害，并且攻击者开始使用这个主机对网络发动进一步攻击时，增加的隔离层能够帮助延缓对防火墙的攻击进度。



DMZ置于防火墙之外 不在公网和防火墙之间的通道上 (续)

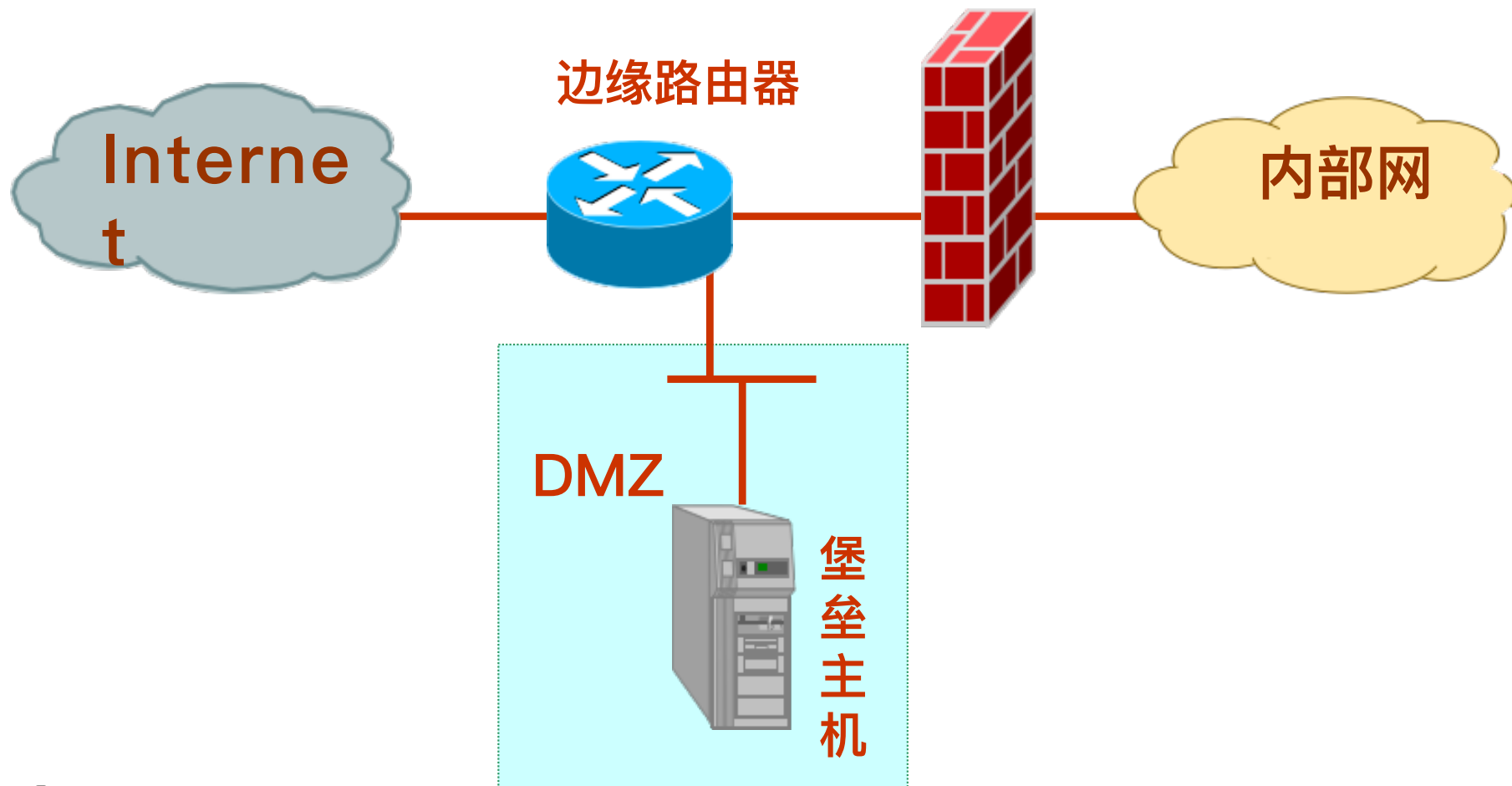


图4.14



两个防火墙，一个DMZ

- DMZ由两个防火墙来保护如图4.15。防火墙①监控DMZ到Internet之间的通信，防火墙②监控DMZ到内部网之间的通信。防火墙②相当于一个备份设备,可以作为故障切换防火墙，当防火墙①工作失败时，它可以立即工作。
- 由于防火墙①使得DMZ获得相当多的安全，但它的缺点是需要从Internet访问到内部网时，所有流量必须**通过DMZ**，所有从内部网到Internet的访问流量也都要**经过DMZ**，当一个DMZ设备被攻陷后，攻击者会阻截或者攻击这个流量。解决的办法是在两个防火墙之间的设备上使用VLAN。它的另一个缺点是需要**使用两个防火墙**，增加了设备的成本。



两个防火墙，一个DMZ (续)

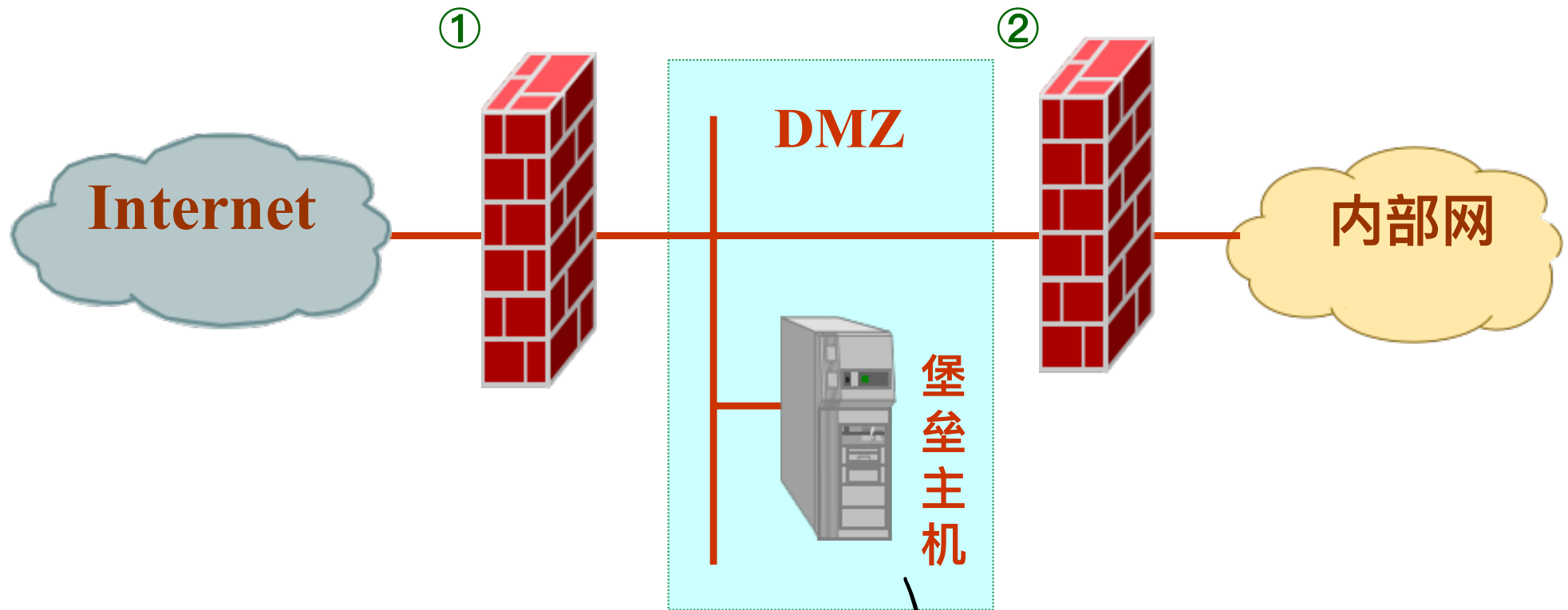


图4.15

被攻陷后有危险



“脏”DMZ

用一个边界路由器在不安全的Internet 与准安全的DMZ之间建立一个分界线，即产生一个“脏”DMZ，见图4.16。在这里**边界路由器**是担当第一道防线的普通路由器，内置的ACL用来实现由网络安全策略所定义的包过滤规则，以便可以对堡垒主机提供一个部分受保护的环境。专用的防火墙提供第二道防线，更好的保护内部网资源。



“脏”DMZ (续)

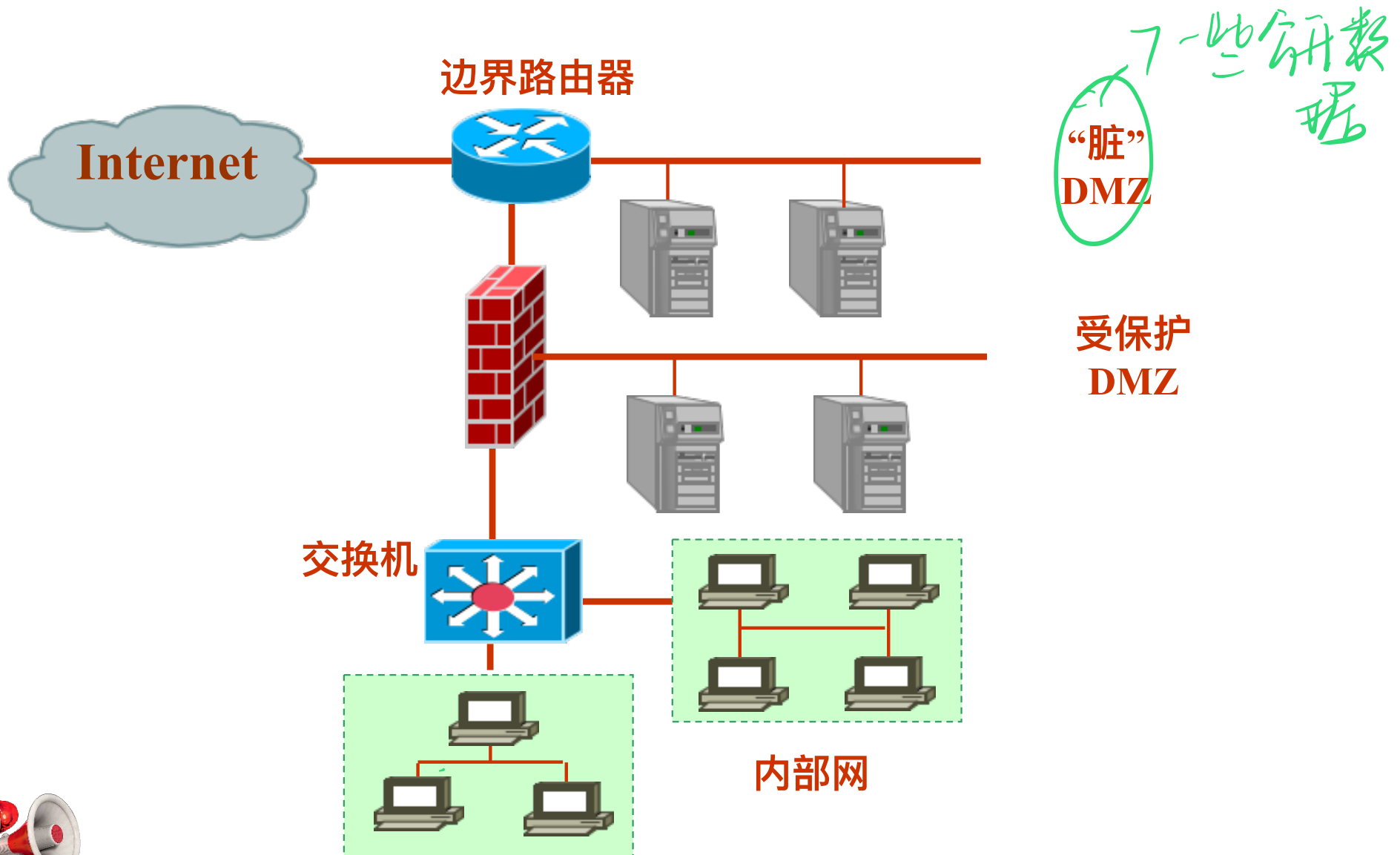


图4.16



4.2.3. 屏蔽路由器

- **屏蔽路由器(Screening Router)**是在Internet和内部网之间放置一个路由器，使之执行**包过滤功能**，这是最简单的防火墙。屏蔽路由器可以由路由器实现。它作为内外连接的唯一通道，要求所有的数据包都必须在此通过检查。在路由器上安装包过滤软件，实现包过滤功能。图4.17显示了它的拓扑结构，虽然它并不昂贵，但仍能提供重要的保护。
- 屏蔽路由器体系结构也称**筛选路由器体系结构**，最大优点是架构简单且硬件成本较低，由于路由器提供非常有限的服务，所以保卫路由器比保卫主机较易实现。



屏蔽路由器防火墙

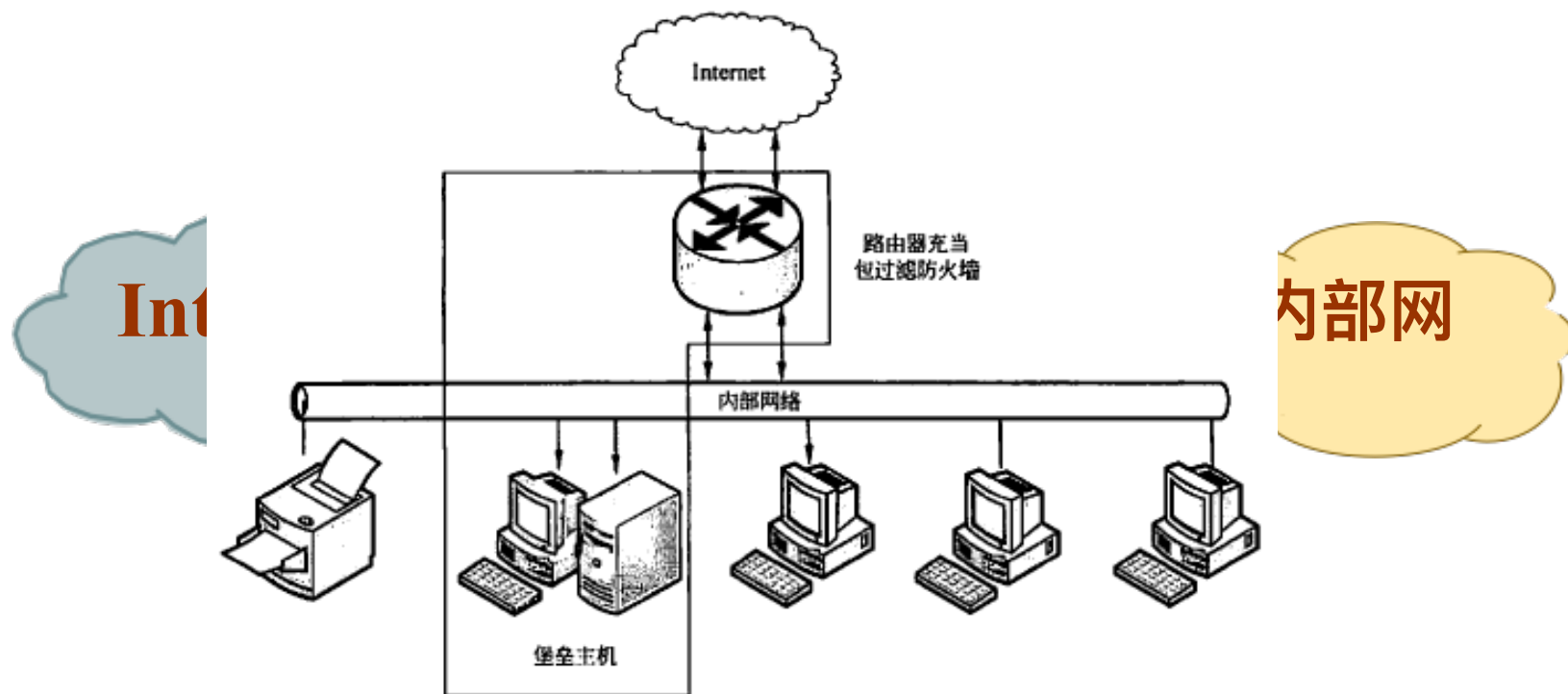


图4.17



屏蔽路由器的缺点

屏蔽路由器仅依靠包过滤规则过滤数据包，一旦有任何错误的配置，将会导致不期望的流量通过或者拒绝一些可接受的流量；

只有一个单独的设备保护网络，如果一个黑客损害到这个路由器，他将能访问到内部网中的任何资源；

屏蔽路由器不能隐藏内部网的配置，任何能访问屏蔽路由器的人都能轻松地看到内部网的布局 and 结构；

屏蔽路由器没有较好的监视和日志功能、没有报警功能，缺乏用户级身份认证，如果一个安全侵犯事件发生，对于这种潜在的威胁它不能通知网络管理员。



4.2.4 双宿主主机体系结构

用一台装有两块网卡的堡垒主机做防火墙，两块网卡各自与内部网和Internet相连，如图4.18。堡垒主机上运行防火墙软件，可以转发应用程序，提供服务等。内、外部网之间的通信必须经过堡垒主机。在这种体系结构中必须禁用路由选择功能，这样防火墙两边的网络才可以只与双宿主主机通信，而两系统不能直接通信。

双宿主只有一条路径信息



双宿主主机体系结构

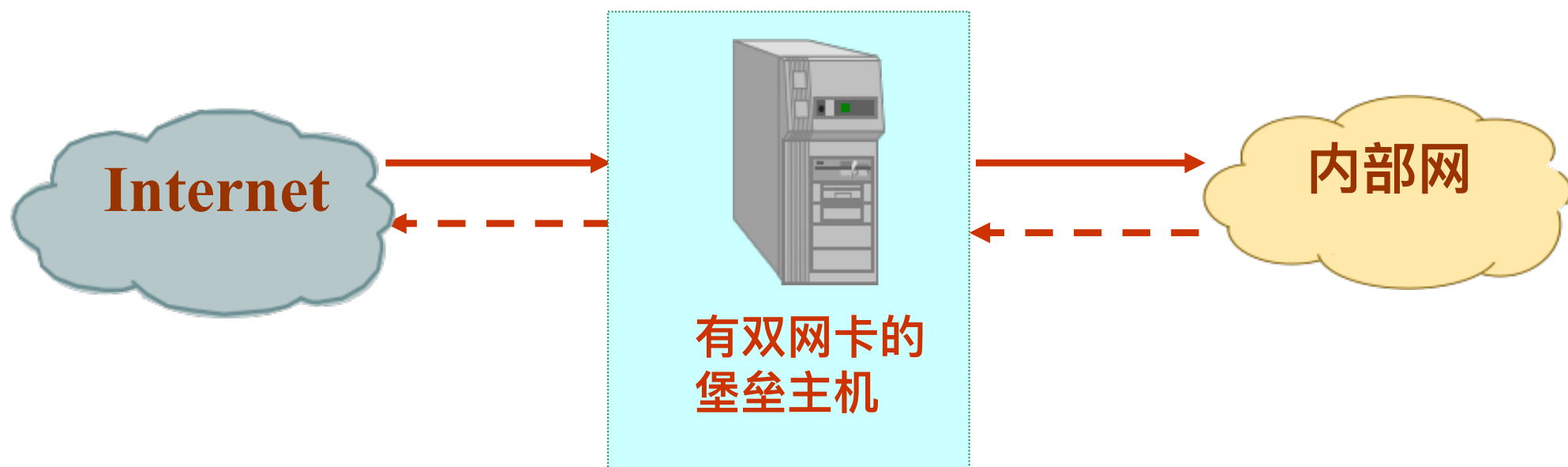


图4.18



优缺点

- 双宿主主机体系结构优于屏蔽路由器的地方是：堡垒主机的系统软件可用于**维护系统日志**、硬件拷贝日志或远程管理日志。这对于日后的检查很有用。但这不能帮助网络管理者确认内部网中哪些主机可能已被黑客入侵。
- 双宿主主机体系结构的一个致命弱点是：一旦入侵者侵入堡垒主机并使其**只具有路由功能**，则任何网上用户均可以随便访问内部网。



4.2.5 主机过滤体系结构

- 在双宿主主机体系结构防火墙中没有使用路由器。而**主机过滤体系结构防火墙（Screened Host Firewall）**则使用一个路由器把内部网和外部网隔离，路由器充当内部网和外部网之间的接口，主机过滤体系结构如图4.19所示。
- 主机过滤体系结构也称作**屏蔽主机体系结构**或者**筛选主机体系结构**。在这种体系结构中利用一个执行**数据包过滤**的路由器连接外部网，在其上设立过滤规则用于防止人们绕过代理服务器直接相连。同时将一个堡垒主机安装在内部网，并使这个堡垒主机成为从**外部网唯一可直接到达的主机**，这样确保了内部网不受未被授权的外部用户的攻击。



主机过滤体系结构

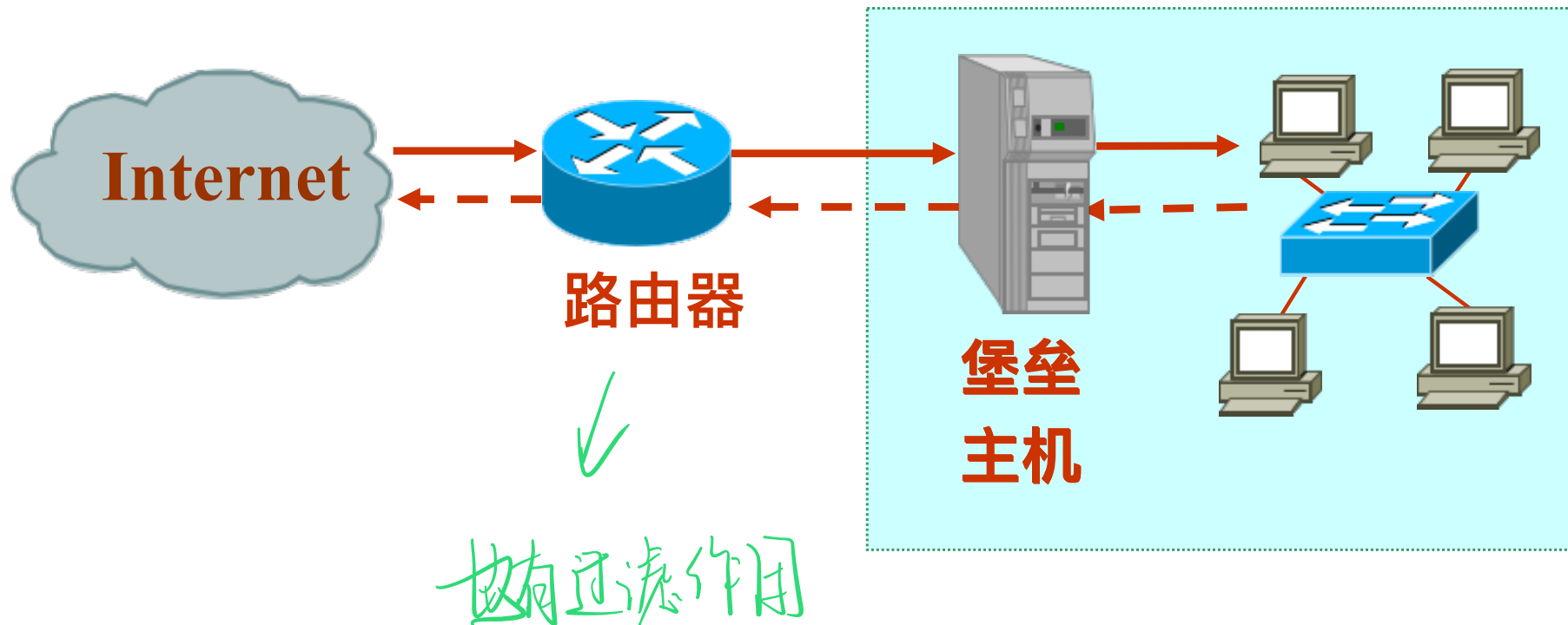


图4.19



主机过滤体系结构 (续)

- 路由器执行的数据包过滤可以允许内部主机为特定服务打开到Internet的连接或者拒绝所有从内部主机到Internet 连接的尝试，应该**强制内部主机通过堡垒主机发送它们的连接请求**。
- 应该将**代理服务器安装在防火墙后面**。防火墙应该有一个和Internet的接口，可以对在它后面的代理服务器起到保护作用。这种保护是关键性的，因为当代理服务器被黑客攻破时，代理服务器会误以为黑客是内部客户机，而允许其通过代理服务器，这样将会对受保护的**网络造成灾难性的后果**。

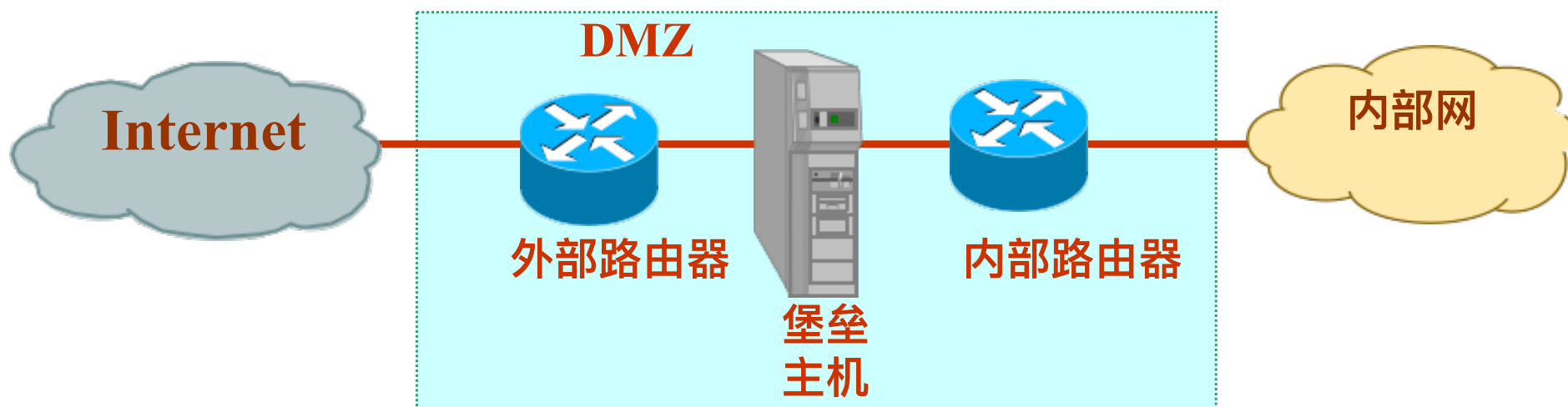


4.2.6 子网过滤体系结构

- 子网过滤体系结构也称为被**屏蔽子网体系结构**或者**筛选子网体系结构**。它用两台**包过滤路由器**建立一个DMZ，用这一DMZ将内部网和外部网分开，简单的子网过滤体系结构如图4.20所示。
- 在这种体系结构中两个包过滤路由器放在DMZ的两端，构成一个内部网和外部网均可访问的被屏蔽子网，但**禁止信息直接穿过被屏蔽子网**进行通信。在被屏蔽子网中**堡垒主机作为唯一的可访问点**，该点作为应用级网关代理。



最简单的子网过滤体系结构



两层路由器，中间夹一个堡垒主机

图4.20



子网过滤体系结构 (续)

为了侵入这种类型的网络，黑客必须先攻破外部路由器，即使他设法侵入堡垒主机，仍然必须通过内部路由器，才能进入内部网。在该体系结构中，因为堡垒主机不直接与内部网的主机交互使用，所以内部网中两个主机间的通信不会通过堡垒主机，即使黑客侵入堡垒主机，他也只能看到从Internet 和一些内部主机到堡垒主机的通信以及返回的通信，而看不到内部网络主机之间的通信。所以**DMZ为内部网增加了安全级别**。



内部路由器

内部路由器也称作**阻塞路由器**、**扼流路由器**。它的任务是**保护内部网使之免受来自Internet和DMZ的侵犯**，并承担防火墙数据包过滤的任务。它允许从内部网到Internet的有选择的出站服务。为了减少堡垒主机受侵袭的数量，要限制堡垒主机给内部网提供的服务。



外部路由器

外部路由器也称作**访问路由器**，保护DMZ和内部网使之免受来自Internet的侵犯。它几乎允许任何通信从DMZ出站，并且通常只执行非常少的数据包过滤；但它要阻止**从Internet上任何伪造源地址进来的数据包**，这样的数据包自称来自内部的网络，但实际上是来自Internet。



4.2.7 组合体系结构

建造防火墙时，一般很少采用单一的技术，通常采用解决不同问题的多种技术的组合。

- 1) 多堡垒主机
- 2) 合并内部路由器与外部路由器
- 3) 合并堡垒主机与外部路由器
- 4) 合并堡垒主机与内部路由器
- 5) 使用多台外部路由器
- 6) 使用多个周边网络



有两个堡垒主机的子网过滤体系结构

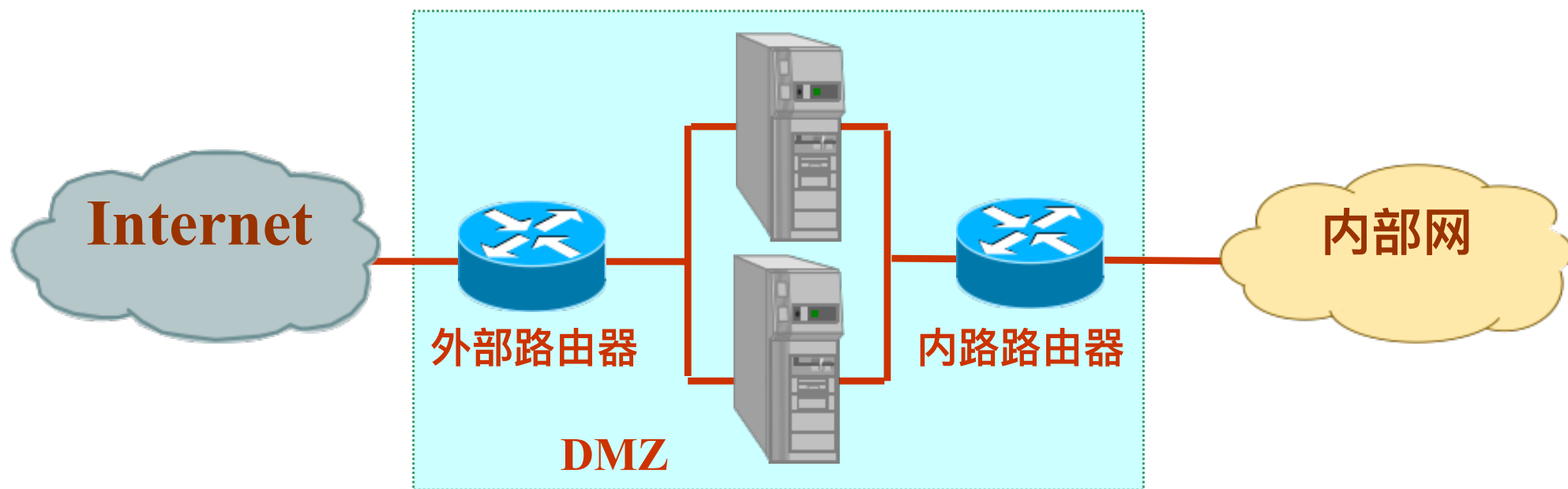


图4.21



单个路由器的子网过滤体系结构

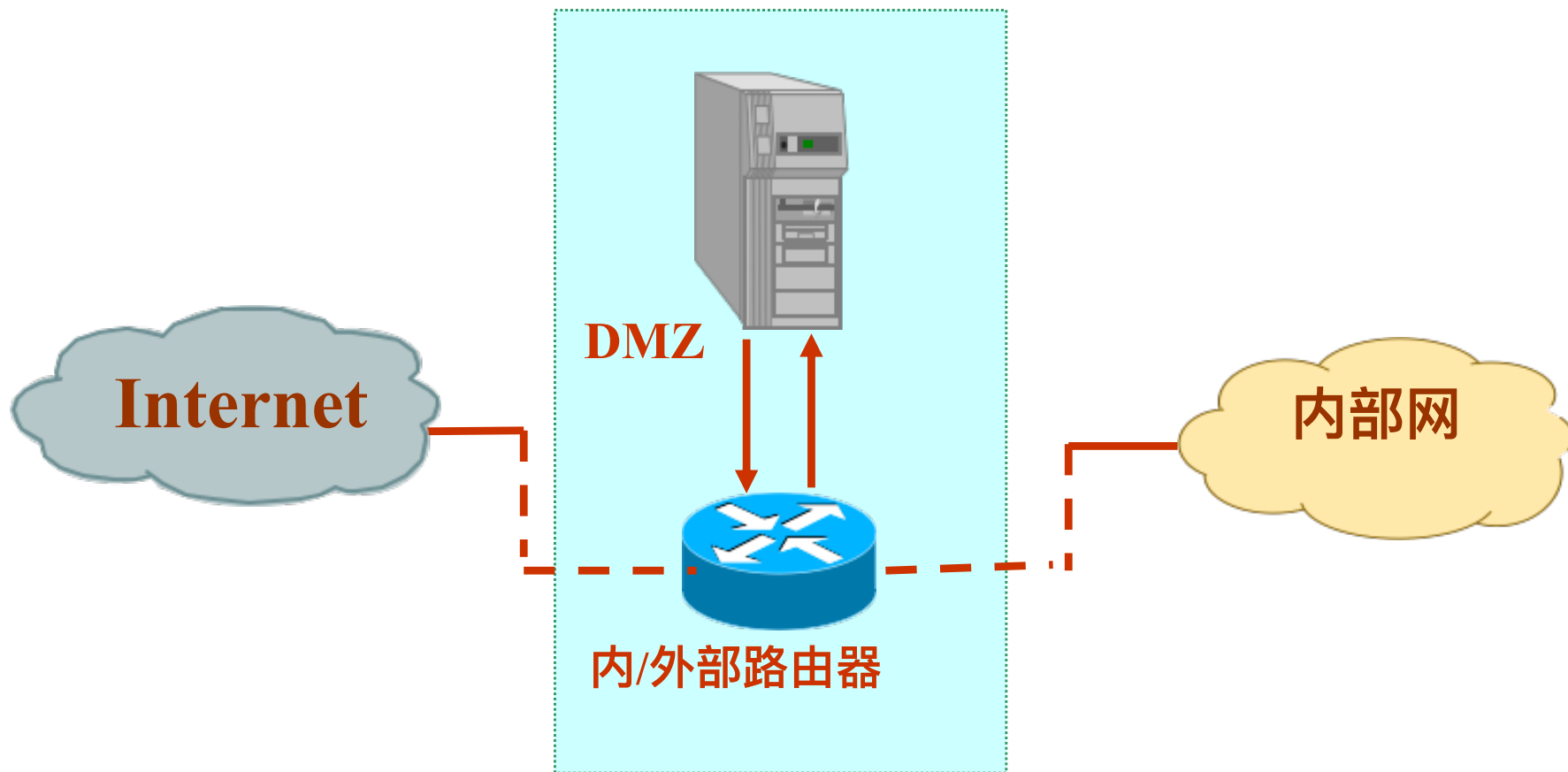


图4.22



堡垒主机充当外部路由器



图4.23



堡垒主机充当内部路由器

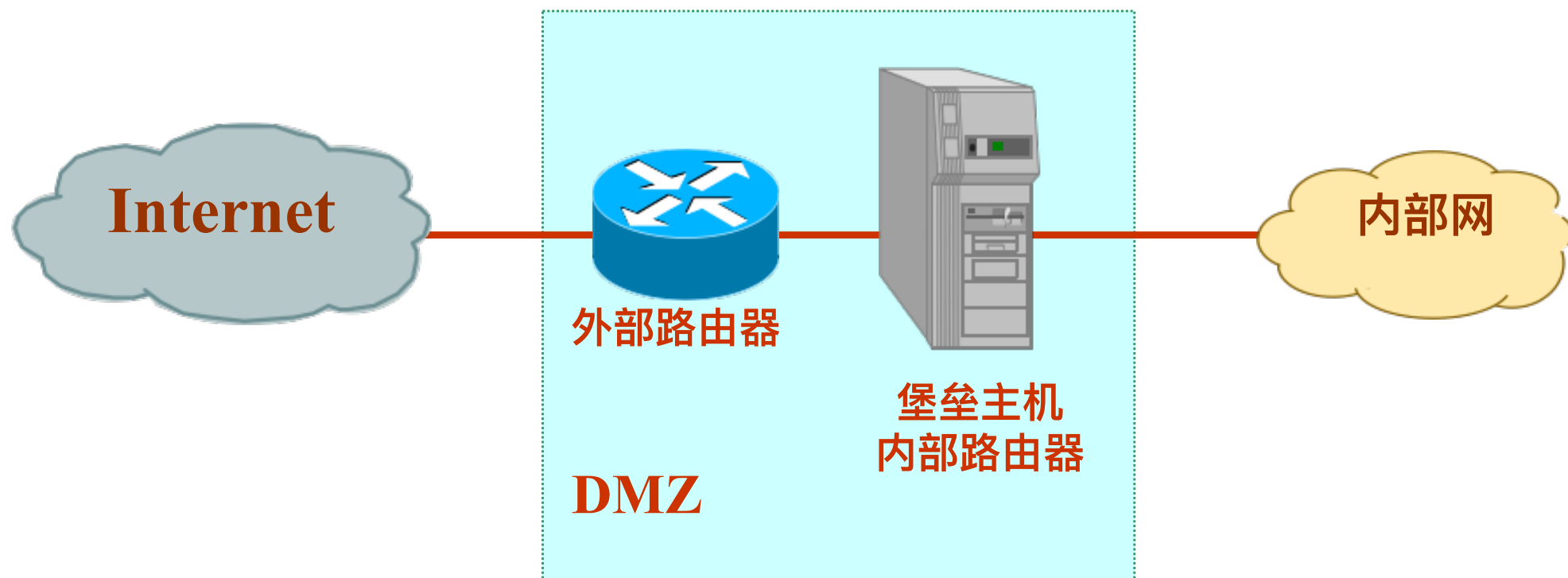


图4.24



多台外部路由器的子网过滤体系结构

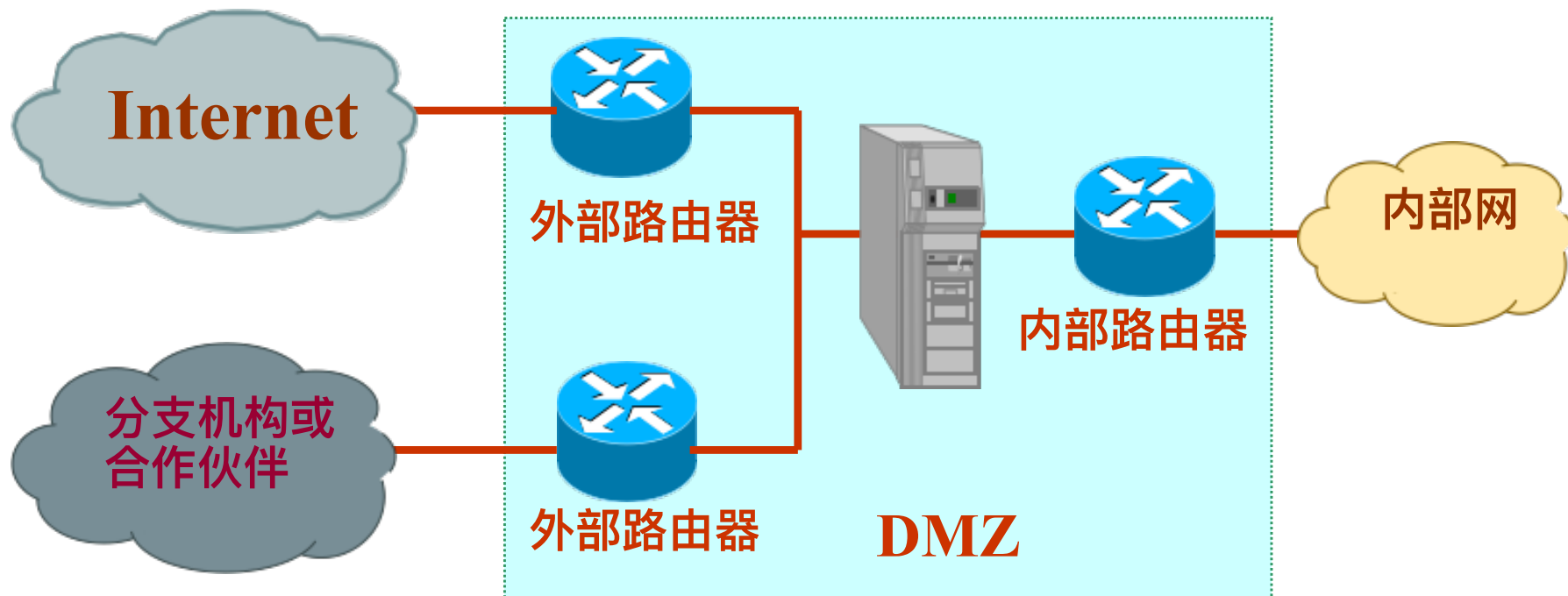


图4.25



有两个DMZ的子网过滤体系结构

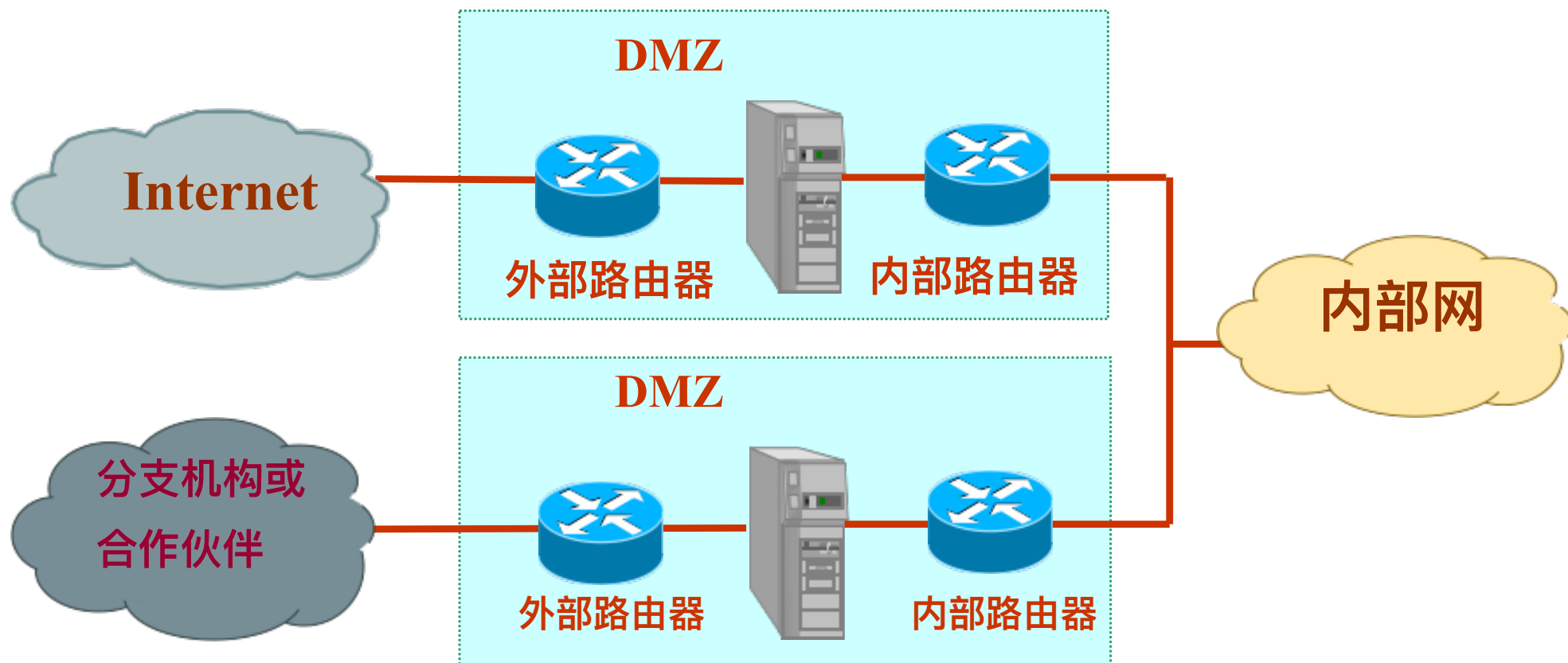


图4.26



4.3 防火墙选型与产品简介

- 防火墙技术发展到现在，其争的焦点主要是在以下四个方面：
- 防火墙的管理——网络安全的关键
- 防火墙的功能——防火墙应用的基础
- 防火墙的性能——提高网络传输效率的条件
- 防火墙的抗攻击能力——网络安全的保证



4.3.1 防火墙的局限性

- 1) 不能防范不经过防火墙的攻击
- 2) 不能防止来自内部变节者或不经心的用户带来的威胁；也不能解决进入防火墙的数据带来的所有安全问题
- 3) 只能按照对其配置的规则进行有效的工作
- 4) 不能防止感染了病毒的软件或文件的传输
- 5) 不能修复脆弱的管理措施或者设计有问题的安全策略
- 6) 可以阻断攻击，但不能消灭攻击源
- 7) 不能抵抗最新的未设置策略的攻击漏洞
- 8) 在某些流量大、并发请求多的情况下，很容易导致拥塞，成为整个网络的瓶颈
- 9) 防火墙对服务器合法开放的端口的攻击大多无法阻止
- 10) 防火墙本身也会出现问题 and 受到攻击



4.3.2 开发防火墙安全策略

一个有效的防火墙依赖于一个明确的、清楚的、全面的安全策略。在设计安全系统时，首先应该考虑的是安全策略而不是防火墙。

安全策略建立了全方位的防御体系来保护机构的信息资源。所有可能受到网络攻击的地方都必须以同样的安全级别加以保护。

国际标准化组织ISO (International Standardization Organization) 和国际电工委员会IEC (International Engineering Consortium) 颁布的ISO17799是一套常用的策略及指导过程，

从 <http://www.iso17799software.com> 可以获得。



安全策略 (续)

安装一个防火墙最困难的部分不是处理硬件和软件，

而是如何向周围的人解释你想施加的那些限制。

- 安全性和复杂性成反比
- 安全性和可用性成反比
- 对网络威胁要详加分析，真实的威胁、可能的威胁和假想的威胁，还有已知与未知的威胁
- 安全策略并不是一成不变的
- 安全是投资，不是消费，安全投资需要得到企业或组织领导的大力支持



4.3.3 防火墙选型原则

- 市场上防火墙的售价极为悬殊，从数万元到数十万元，甚至到百万元不等。由于用户数量不同，用户安全要求不同，功能要求不同，因此防火墙的价格也不尽相同。
- 网络吞吐量、丢包率、延迟、连接数等都是重要的技术指标。质量好的防火墙能够有效地控制通信，为不同级别、不同需求的用户提供不同的控制策略。
- 控制策略的有效性、多样性、级别目标清晰性以及制定难易程度都直接反映出防火墙控制策略的质量。



4.3.4 典型防火墙简介

- Checkpoint
FireWall-1
- Cisco PIX Firewall
- 东软NetEye



Checkpoint FireWall-1

- CheckPoint软件技术有限公司成立于1993年，该公司是Internet安全领域的全球领先企业。Check Point已经成为防火墙软件的代名词，它推出并持有专利的**状态监测技术**是网络安全性技术的事实标准。
- Check Point的成名部分原因归功于它的安全性开放式平台OPSEC（Open Platform for Security）。OPSEC联盟成立于1997年。
- FireWall-1 是Check Point网络安全性产品线中最重要的产品，也是业界领先的企业级安全性套件。它集成了**访问控制、用户认证、NAT、VPN、内容安全性、审计和报告**等特性。



FireWall-1的基本模块

- 状态检测模块 (Inspection Module) : 提供访问控制、客户机认证、会话认证、NAT和审计功能;
- 防火墙模块 (FireWall Module) : 包含一个状态检测模块, 另外提供用户认证、内容安全和多防火墙同步功能;
- 管理模块 (Management Module) : 对一个或多个安全策略执行点 (安装了FireWall-1的某个模块, 如状态检测模块、防火墙模块或路由器安全管理模块等的系统) 提供集中的、图形化的安全管理功能, 一个管理模块可以控制多达50个单独的FireWall-1。



Cisco PIX Firewall

1984年成立于斯坦福大学的思科系统公司，Cisco公司（Cisco Systems, Inc.）是全球领先的互联网设备供应商。1995年思科兼并了一个利用状态检测为计算机网络提供安全保障的生产即插即用的硬件设备厂商NTI（Network Translations, Inc.）。6年后，PIX成为防火墙市场的领导者。



Cisco PIX Firewall (续)

- 保密互连交换PIX (Private Internet Exchange) 的作用是防止外部网非授权用户访问内部网。多数PIX都可以有选择地保护一个或多个DMZ。内部网、外部网和DMZ之间的连接由PIX Firewall控制。
- PIX保护网络的方法如图4.28所示。在这种体系结构中，PIX 将形成受保护网络和不受保护网络之间的边界，受保护网络和不受保护网络之间的所有流量都通过PIX实现安全性。PIX也可以用在内部网中，以便隔离或保护某组内部计算系统和用户。



PIX 防火墙的使用

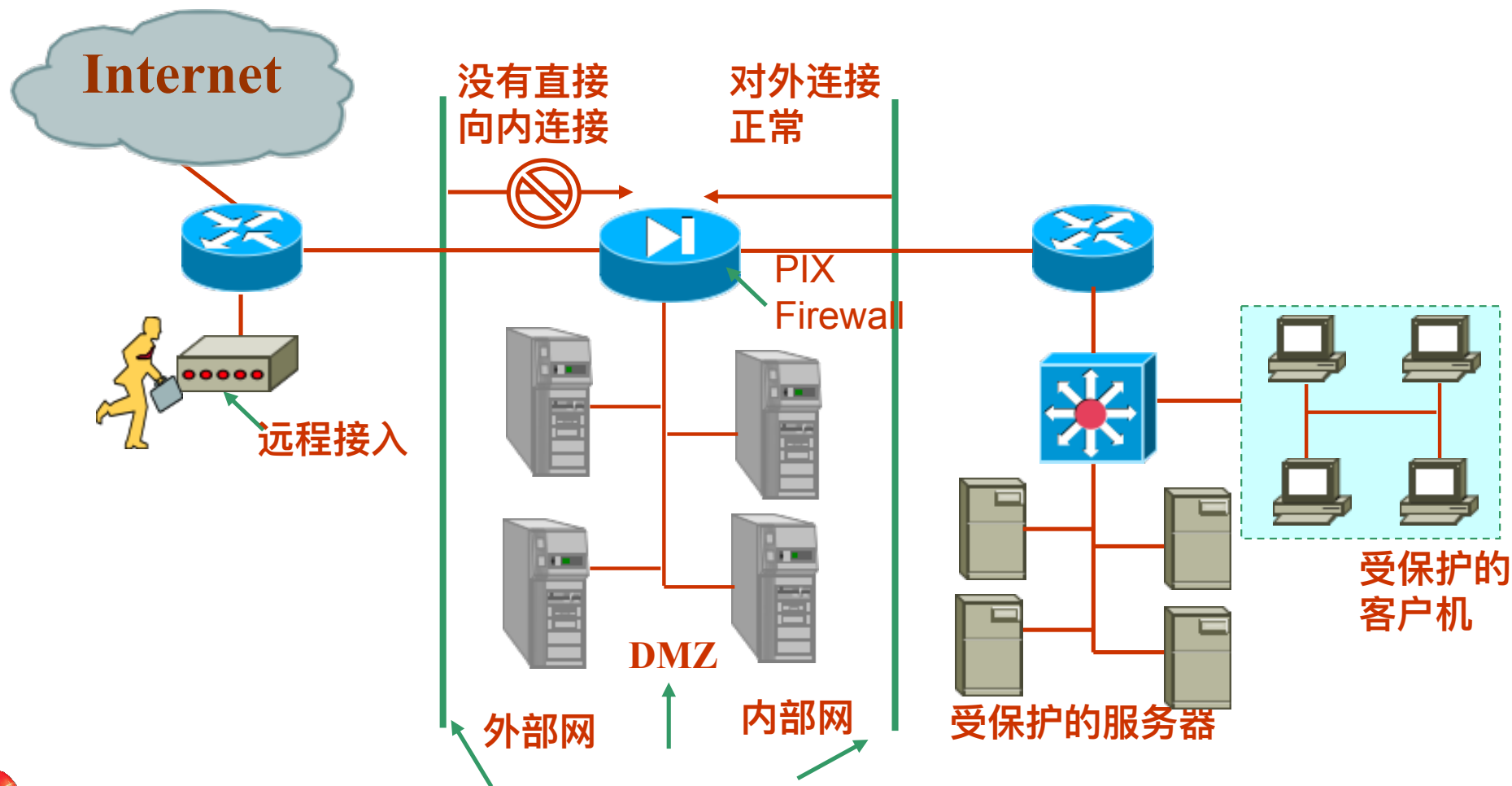


图4.28



自适应安全算法ASA

- PIX的核心是基于自适应安全算法ASA (Adaptive Security Algorithm) 的一种保护机制，它将内部主机的地址映射为外部地址，拒绝未经允许的包入境，实现了动态，静态地址映射，从而有效地屏蔽了内部网络拓扑结构。通过管道技术，出境访问列表，有效地控制内、外部各资源的访问。
- ASA是一种状态安全方法。每个向内传输的包都将按照自适应安全算法和内存中的连接状态信息进行检查。ASA一直处于操作状态，监控返回的包，目的是保证这些包的有效性。



ASA遵守以下规则

- 如果没有连接和状态，任何包都不能穿越PIX；
- 如果没有ACL的特殊定义，向外连接或状态都是允许的；
- 如果没有特殊定义，向内连接或状态是不允许的；
- 如果没有特殊定义，所有ICMP包都将被拒绝。
- 违反上述规则的所有企图都将失败，而且将把相应信息发送至系统日志。



东软NetEye

于1991年在东北大学创立的东软集团是中国领先的软件与解决方案提供商。东软NetEye 防火墙基于专门的硬件平台，使用专有的ASIC芯片和专有的操作系统，基于状态包过滤的“流过滤”体系结构。围绕流过滤平台，东软构建了网络安全响应小组、应用升级包开发小组、网络安全实验室，不仅带给用户高性能的应用层保护，还包括新应用的及时支持，特殊应用的定制开发，安全攻击事件的及时响应等。



4.4 本章知识点小结

1. 防火墙采用不同的技术

- (1) 包过滤防火墙：所有防火墙设备中最核心的功能。
- (2) 代理服务防火墙：针对特定的网络应用服务协议过滤。
- (3) 复合防火墙：在防火墙添加了NAT、VPN、IDS、AAA、QoS等功能。

2. 防火墙采用不同的实现方法

- (1) 软件防火墙：防火墙软件运行于特定的计算机上。
- (2) 软硬一体化防火墙：由PC硬件加通用操作系统加防火墙软件组成。
- (3) 硬件防火墙：采用经过优化设计的硬件体系结构和专用的操作系统。



小 结 (续)

3. 防火墙产品应用于不同对象

- (1) 企业级防火墙：要满足网络吞吐量、丢包率、延迟、连接数等技术指标。
- (2) 个人防火墙：安装在PC 机系统里的一段“代码墙”。

4. 防火墙体系结构

- (1) DMZ：一个可由公共访问的服务器网络，内部网和外部网之间的缓冲区。
- (2) 堡垒主机：放置在DMZ中,提供公共服务的设备。
- (3) 屏蔽路由器：在路由器上安装包过滤功能的最简单的防火墙。
- (4) 双宿主主机体系结构：用一台装有两块网卡的堡垒主机做防火墙。
- (5) 主机过滤体系结构:包过滤路由器连接外部网，堡垒主机安装在内部网。
- (6) 子网过滤体系结构：在内外网之间建立DMZ，包过滤路由器将DMZ、内、外部网分开。



小结 (续)

5.防火墙的选型

- (1) 防火墙具有局限性。
- (2) 仔细构建防火墙的安全策略。
- (3) 根据网络规模和安全策略选择合适的防火墙产品。

6.典型防火墙

- (1) checkpoint FireWall-1: 防火墙软件的代名词。
- (2) Cisco PIX Firewall 具有自己的硬件体系结构和专用的操作系统。
- (3) 东软NetEye。

