

# 7 防火墙技术

2019年5月27日 10:02

## 1 包过滤技术

- [1.1 包过滤原理](#)
- [1.2 包过滤模型](#)
- [1.3 包过滤技术](#)
  - [1.3.1 配置访问控制列表](#)
  - [1.3.2 动态访问控制列表](#)
  - [1.3.3 状态包检查](#)
- [1.4 包过滤技术优缺点](#)

## 2 网络地址翻译技术

- [2.1 NAT技术原理](#)
- [2.2 NAT相关术语](#)
- [2.3 静态网络地址翻译技术](#)
- [2.4 动态网络地址翻译技术](#)
- [2.5 网络地址翻译技术实现负载均衡](#)
- [2.6 网络地址翻译技术处理网络地址交迭](#)
- [2.7 网络地址翻译技术缺点](#)

## 3 网络代理技术

- [3.1 应用层代理](#)
  - [3.1.1 应用层代理简介](#)
  - [3.1.2 应用层代理实现](#)
  - [3.1.3 代理服务程序](#)
  - [3.1.4 应用层代理优缺点分析](#)
- [3.2 电路级代理](#)
  - [3.2.1 电路级代理概述](#)
  - [3.2.2 电路级网关的工作原理](#)
  - [3.2.3 SOCKS代理技术](#)
  - [3.2.4 SOCKS代理的实现](#)

## 1 包过滤技术

- [1.1 包过滤原理](#)
- [1.2 包过滤模型](#)
- [1.3 包过滤技术](#)
  - [1.3.1 配置访问控制列表](#)
  - [1.3.2 动态访问控制列表](#)
  - [1.3.3 状态包检查](#)
- [1.4 包过滤技术优缺点](#)

### 1.1 包过滤原理

- 通过检测网络数据包的信息头决定是否将数据包发往目的地址，以达到对流入和流出网络的数据进行监测和限制的目的。
- 理论上，包过滤防火墙可以被配置为根据协议报头的任何数据域进行分析和过滤，但大多数过滤型防火墙只是针对性地分析最有用的数据域。

### 1.2 包过滤模型

- 包过滤防火墙的核心是包检查模块。
- 包检查模块深入到操作系统的内核，在操作系统或路由器转发包之前拦截所有的数据包。
- 在网关上安装包过滤防火墙之后，包过滤检查模块深入到系统的传输层（TCP）和网络层（IP）之间，在操作系统或路由器的TCP层对IP包处理以前对IP包进行处理。
- 实际应用中，数据链路层主要由网络适配器(NIC)进行实现，网络层是软件实现的第一层协议堆栈，所以防火墙位于软件层次的最底层。

数据链路层	目的物理地址	源物理地址	类型	数据
-------	--------	-------	----	----

## 网络层

版本	首部长度	服务类型	总长度			
标识		标志		分段偏移		
生存时间	协议		首部检验和			
源IP地址						
目的IP地址						
数据						

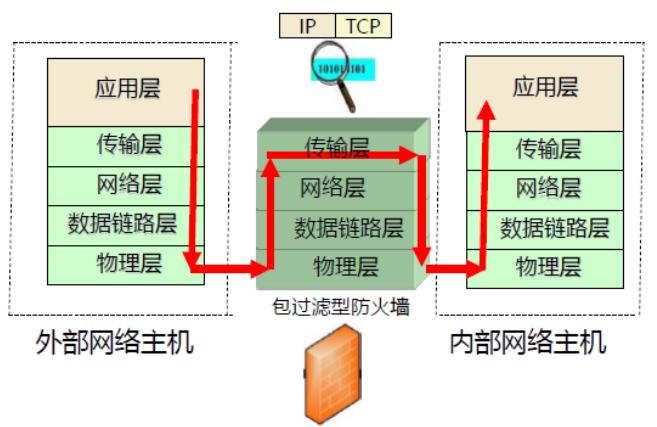
## 传输层

源端口号	目的端口号
顺序号	
确认序号	
首部 长度	保留
URG	A CK
RST	P SH
SYN	R SYN
FIN	F IN
窗口大小	
校验和	
紧急指针	
选项	
数据	

- 防火墙检查模块验证每个包是否符合过滤规则，不管是否符合过滤规则，防火墙一般都要记录数据包情况
  - 不符合规则的包进行报警或通知管理员
  - 对被过滤或丢弃的数据包，防火墙可以返回ICMP消息，这要取决于包过滤防火墙的策略

### 1.3 包过滤技术

- 数据包过滤功能的实现依赖于包过滤规则，有时也称之为访问控制列表。
- 只有满足访问控制列表的数据才被转发，其余数据则被从数据流中删除。
- 为了保证所有流入和流出的网络的数据包都被监控和检测，包过滤器必须被放在网络单点访问的位置。
- 包过滤技术虽然是防火墙技术的一部分，在实际应用中也往往和边界路由器集成使用。



- [1.3.1 配置访问控制列表](#)
- [1.3.2 动态访问控制列表](#)
- [1.3.3 状态包检查](#)

#### 1.3.1 配置访问控制列表

- 本质上，一个包过滤防火墙由：
  - 一个脏端口：连接Internet，来自Internet和流向Internet的数据流都由此端口通过。
  - 一个净端口：连接内部网络，防火墙一般认为内部网络完全可信，网络安全威胁来自网络外部。
  - 一组访问控制规则组成
- 数据包过滤规则，只有满足访问控制列表的数据包才被转发，其余数据包则被从数据流中删除。访问控制列表的配置有两种方式：
  - 限制策略。接受受信任的IP包，拒绝其他所有IP包。
  - 宽松策略。拒绝不受信任的IP包，接受其他所有IP包。





方向	类型	源地址	目的地址	源端口	目的端口	动作
inside	tcp	*	123.4.5.6	any	21	permit
inside	tcp	*	123.4.6.7	any	80	permit
inside	udp	129.6.1.2	123.4.5.8	any	161	permit
*	*	*	*	*	*	deny

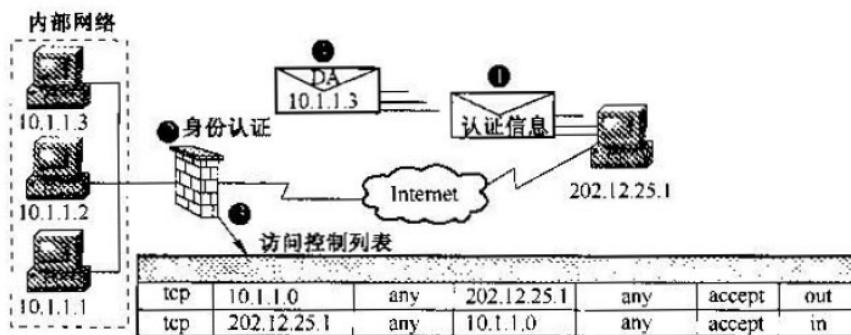
### 访问控制列表实例

顺序	协议	源地址	目的地址	源端口	目的端口	方向	行为
1	TCP	192.168.10.11	*.*.*.*	any	80	out	deny
2	TCP	192.168.10.*	*.*.*.*	any	80	out	accept
3	TCP	*.*.*.*	202.106.185.236	any	80	out	accept
4	TCP	192.168.10.*	202.106.185.236	any	80	out	deny
5	TCP	192.168.10.*	*.*.*.*	any	21	out	accept
6	TCP	192.168.10.*	202.106.185.236	any	21	out	accept
7	TCP	*.*.*.*	*.*.*.*	any	any	out	deny
8	UDP	192.168.10.*	202.106.185.236	any	53	out	accept
9	UDP	*.*.*.*	202.106.185.236	any	53	out	accept
10	UDP	*.*.*.*	*.*.*.*	any	any	out	deny

### 访问控制列表中规则出现的顺序至关重要

#### 1.3.2 动态访问控制列表

- 动态包过滤技术是指配置动态访问控制列表
  - 实现指定用户的IP数据流临时通过防火墙，进行会话连接，从而实现对数据包的动态过滤。
  - 当动态访问控制列表被触发后，动态访问控制列表重新配置接口上已有的访问控制列表，允许指定用户访问指定IP地址。
  - 在会话结束后，将接口配置恢复到原来的状态。
- 动态包过滤技术一般结合身份认证机制实现。
  - 例如，用户首先发起一个到防火墙的标准Telnet会话时，防火墙进行身份验证。
  - 如果用户通过身份验证，则激活动态访问控制列表，在防火墙开放一个数据通道，此时，用户可以暂时通过防火墙访问内部网络目标主机。



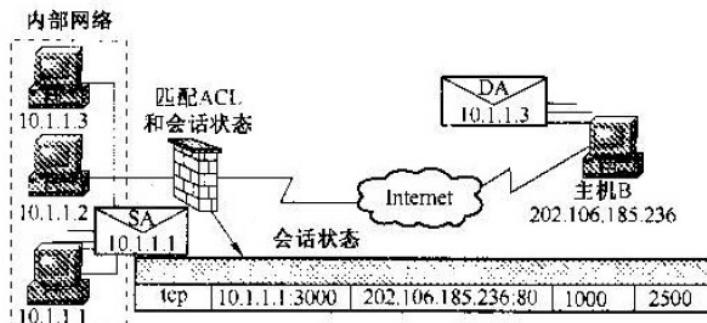
- 过程：

- 用户发起一个到防火墙的Telnet会话。
- 防火墙接收到Telnet数据包分组后，打开Telnet会话，提示用户输入认证信息并对用户身份进行验证。
- 通过身份认证后，用户退出Telnet会话，防火墙访问控制列表内创建一个临时条目。该临时条目可限制用户临时访问的网络范围。
- 用户通过防火墙交换数据。
- 超过预定超时时间（Timeout）后，防火墙将删除这个临时访问控制列表规则，系统管理员也可手动删除。

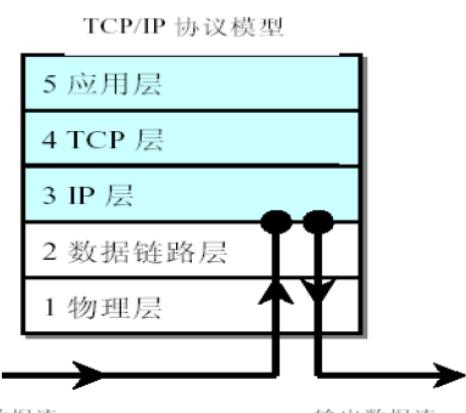
#### 1.3.3 状态包检查

- 状态包检查技术又称为反射访问控制列表技术。

- SPI (StatefulPacketInspection) 技术能够动态建立访问控制列表条目。
- 在这些临时条目中不仅包含必要的包过滤信息，还包含了网络会话的状态信息。
- 这些临时条目在新会话开始（如内部主机向外部主机发起连接请求）时创建，并在会话结束时被删除。
- SPI包过滤技术维护网络中的会话连接信息。
  - 防火墙检查每一个通过的数据包，看这些数据包是否属于一个已经建立的通过防火墙的会话的延续，或者能否通过预设定包过滤规则集的检查。
  - SPI包过滤技术拒绝除设计允许和已经在状态表中的连接之外的所有连接。
- 状态检测包过滤协议描述：
  - 当一个内部主机与一个外部主机建立连接时，首先发送一个TCP SYN包或 UDP 数据包，包含目的IP、目的端口号、源IP和源端口号。
  - 当内部主机发送的数据包通过状态检查包过滤防火墙时，防火墙将在它的状态表中建立一条状态信息规则，源IP：源端口号 $\leftrightarrow$ 目的IP：目的端口号，然后将数据包发送到外部网络上。
  - 外部主机返回请求响应时，防火墙从状态表中查找是否存在相应规则。
  - 如果寻找到匹配的状态信息，就允许该数据包通过；否则，数据包就被丢弃。
  - 当会话关闭数据包经过防火墙（通过查看TCP数据包FIN位进行判断），或者在一段延迟（通常是几分钟）之后，防火墙将相应的状态信息规则从状态表中删除。以保证放弃的连接不会在状态表中留下漏洞。
- 会话结束的判定和临时条目的删除：
  - 对于TCP会话：
    - 检测到两组FIN位被设置的TCP分组后，临时条目一般将在几秒钟内被删除。
    - 在检测到RST位被设置的TCP分组后，临时条目将被立即删除（在会话中的两组FIN位被置位的TCP分组表示会话即将结束，几秒钟的时间可以使得会话能完美地结束，设置了RST位的TCP分组表示会话突然关闭）。
    - 在超时时间段内，如果没有检测到和特定会话相关的数据分组，临时条目也将被删除。
  - 对于UDP和其他协议，会话结束的判定方法不同于TCP。原因在于这些协议被认为是无连接（Sessionless）服务，在它们的数据分组内没有会话跟踪信息。
  - 因此，通常在超时时间段内没有检测到此UDP会话的任何相关数据分组时，便认为UDP会话结束了。



状态检查访问控制列表原理图



状态包检查防火墙工作示意图

## 1.4 包过滤技术优缺点

- 优点：
  - 包过滤防火墙是两个网络之间访问的惟一途径，防火墙可对每个传入和传出网络的数据包实行低水平控制。
  - 每个IP包的字段都被检查，如源地址、目的地址、协议、端口等。防火墙将基于这些信息应用过滤规则。
  - 防火墙可以识别、丢弃带欺骗性源IP地址的包。
  - 包过滤通常被包含在路由器中，不需要额外的系统来处理。
- 缺点：
  - 访问控制列表的配置和维护困难。
  - 包过滤防火墙难以详细了解主机之间的会话关系，容易受到欺骗。
  - 基于网络层和传输层实现的包过滤防火墙难以实现对应用层服务的过滤。

## 2 网络地址翻译技术

- NAT (NetworkAddressTranslation, 网络地址翻译) 的最初设计目的是用来增加私有组织的可用地址空间和解决将现有的私有TCP/IP网络连接到互联网上的IP地址编号问题。
- 互联网网络号分配机构 (IANA, InternetAssignedNumbersAuthority) 规定了私有IP地址空间
  - [2.1 NAT技术原理](#)
  - [2.2 NAT相关术语](#)
  - [2.3 静态网络地址翻译技术](#)
  - [2.4 动态网络地址翻译技术](#)
  - [2.5 网络地址翻译技术实现负载均衡](#)
  - [2.6 网络地址翻译技术处理网络地址交迭](#)
  - [2.7 网络地址翻译技术缺点](#)

私有IP地址空间分配表

类型	地址空间
A类	10.0.0.0至10.255.255.255
B类	172.16.0.0至172.31.255.255
C类	192.168.0.0至192.168.255.255

### 2.1 NAT技术原理

- 私有IP地址只能在内部网络使用，不能在互联网主干网上使用。
- 网络地址翻译技术通过地址映射保证使用私有IP地址的内部主机或网络能够连接到公用网络。
- 这个连接要通过一个运行NAT软件的路由器（称为NAT网关），NAT网关被安放在网络末端区域（内部网络和外部网络之间的边界点上）。
- NAT网关在源自内部网络的数据包发送到外部网络之前把数据包的源地址转换为全球统一可寻址的IP地址。
- 在源自外部网络的数据包进入内部网络之前把数据包的源地址转换为内部网络私有IP地址。
- NAT技术中，通信通常由内部网络发起。
- 网络地址翻译技术并非为防火墙而设计，它在解决IP地址短缺的同时提供了内部主机地址隐藏功能，使其成为防火墙实现中经常采用的核心技术之一。

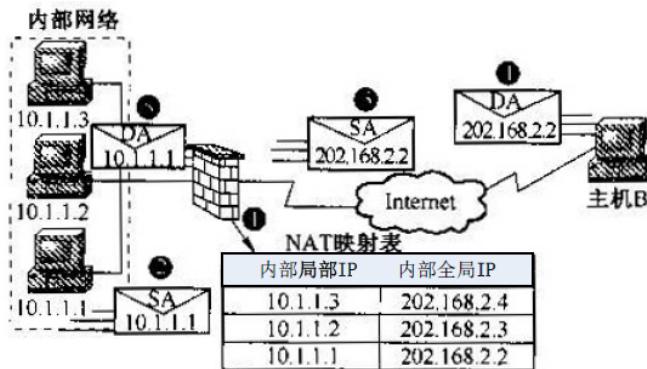
### 2.2 NAT相关术语

- 内部局部地址 (InsideLocalAddress)
  - 在内部网络中使用，标识内部网络的主机。内部网络分配给主机的私用IP地址。
- 内部全局地址 (InsideGlobalAddress)
  - 在外部网络中使用，标识内部网络的主机。一般是由互联网服务提供商 (ISP) 提供的一个合法IP地址。
  - 在互联网中代表一个虚拟的主机。
  - 这个虚拟主机对应了内部网络中一个或多个内部局部IP地址。
- 外部全局地址 (OutsideGlobalAddress)

- 在外部网络中使用，标识外部网络的主机。一般是由互联网服务提供商（ISP）提供的一个合法IP地址，该地址是从全球统可寻址的地址空间中分配的。
- 外部局部地址（OutsideLocalAddress）
  - 在内部网络中使用，标识外部网络的主机。外部网络的主机表现在内部网络的IP地址。这一地址是从内部可寻址的地址空间中分配的，是从私有IP地址空间中分配的。

### 2.3 静态网络地址翻译技术

- NAT网关只对内部网络和外部网络之间传输的数据包进行转换。
- 如果网络地址翻译技术完全依赖于人工指定内部局部地址和内部全局地址之间的映射关系来运行，称为静态网络地址翻译技术。

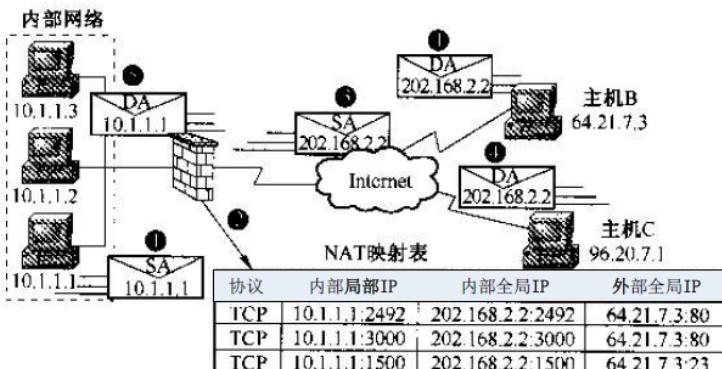


静态网络地址翻译地址转换原理图

- 静态网络地址翻译协议描述：
  - 在防火墙手工建立静态NAT映射表。
  - 网络内部主机建立一条到外部主机的会话连接。主机10111发送数据包到主机B。
  - 防火墙从内部网络接收到一个数据包时，检查NAT映射表：
    - 如果已为该地址配置了静态地址转换，防火墙使用内部全局地址，并转发该数据包。防火墙使用20216822来替换内部局部地址10111；
    - 否则，防火墙不对内部地址进行任何转换，直接将数据包进行转发或丢弃。
  - 外部主机收到数据包后进行应答。主机B将收到来自20216822的数据包（已经过NAT转换），并进行应答。
  - 当防火墙接收到来自外部网络的数据包时，防火墙检查NAT映射表：如果NAT映射表中存在匹配项，则使用内部局部地址替换数据包的目的IP地址，并将数据包转发到内部网络主机。防火墙使用10111替换20216822并进行转发；如果NAT映射表中不存在匹配项，则拒绝数据包。
- 对于每个数据包，防火墙都将执行第b步到第e步的操作。

### 2.4 动态网络地址翻译技术

- 如果NAT映射表由防火墙动态建立，对网络管理员和用户透明，则称之为动态网络地址翻译技术。
- 网络地址翻译技术允许将多个内部IP地址映射成为一个外部IP地址
- 从本质上讲，网络地址映射并不是简单的IP地址之间的映射，而是网络套接字映射，网络套接字由IP地址和端口号共同组成。
- 这种方法在节省了大量网络IP地址的同时隐藏了内部网络拓扑结构

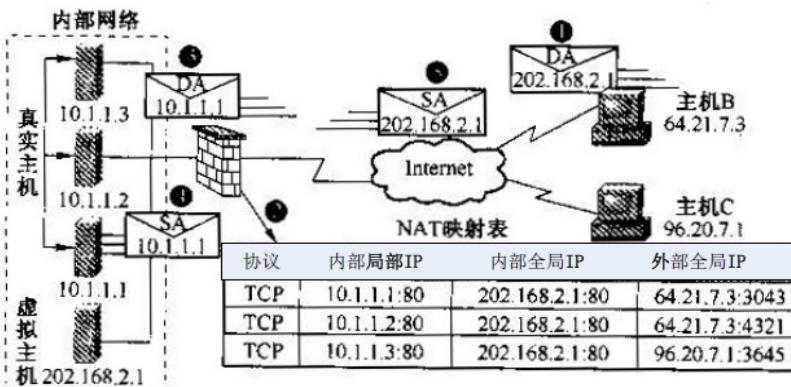


动态网络地址翻译地址转换原理图

- 动态网络地址翻译协议描述:
  - a. 网络内部主机建立到外部主机的会话连接。主机10.1.1.1访问外部主机B:64.21.7.3。
  - b. 防火墙接收到来自某内部主机的数据包时检查NAT映射表：如果还没有为该内部主机建立地址转换映射项，防火墙会决定对该地址进行转换。
    - 防火墙收到来自10.1.1.1的第一个数据包时，建立：10.1.1.1:2492---202.168.2.2:2492，并记录会话状态。如果已经有地址转换映射存在，那么防火墙将使用该记录进行地址转换，并记录会话状态信息。
  - c. 防火墙进行地址转换后转发数据包。
  - d. 外部主机收到访问信息，并进行应答。
  - e. 当防火墙接收到来自外部网络的数据包时，检查NAT映射表查询匹配项：如果NAT映射表中存在地址映射和会话状态匹配的选项，则转发数据包；否则，拒绝数据包。
- 对于每个数据包，防火墙都将执行第b步到第e步的操作。

## 2.5 网络地址翻译技术实现负载均衡

- 对于外部网络访问内部网络服务器的数据流，可以为其配置一种目的地址转换的动态形式。
- 当建立好恰当的映射方案后，与NAT映射表相匹配的目的地址会被内部局部地址集中的一个地址所代替。
- 这种地址转换是以连接为单位按循环方式(round-robin)进行的，只有当建立一个由外部发起到内部的新连接时才执行。
- 所有非TCP的数据流不进行转换（除非设置了其它转换方式）。



网络地址翻译实现TCP负载均衡原理图

- 网络地址翻译技术实现TCP负载均衡原理描述：
  - a. 外部主机建立到内部服务器的会话连接。外部主机B建立到内部网络虚拟WWW服务器202.168.2.1:80的一个会话连接
  - b. 防火墙从主机10.1.1.1接收到这个连接请求，为其建立一个新的地址转换映射，为该内部全局IP地址202.168.2.1分配一个真实内部主机地址（例如，10.1.1.1）。
  - c. 防火墙用所选的真实内部主机地址替换原目的地址，并转发该数据包。
  - d. 内部主机10.1.1.1接收到该数据包，并做出应答。
  - e. 防火墙接收到应答数据包，用内部局部地址及端口号和外部地址及端口号从NAT映射表中查找出对应的虚拟主机地址和端口号。然后将源地址转换成虚拟主机地址，并转发该数据包。
    - 对于下一个连接请求，边界路由器将为其分配另一个内部局部地址，例如，10.1.1.2

## 2.6 网络地址翻译技术处理网络地址交迭

- 网络地址翻译技术也可用于解决内部网络地址与外部网络地址交迭的情况。当两个公司要进行合并，但双方各自使用的内部网络地址有重叠时就会发生这种问题。

## 2.7 网络地址翻译技术缺点

- 一些应用层协议的工作特点导致了它们无法使用网络地址翻译技术
- 当端口改变时，有些协议不能正确执行它们的功能。例如，对于数据包的数据域部分含有源或、和目的IP地址的TCP/UDP数据流，Cisco IOS NAT不支持：
  - 路由表更新协议
  - DNS区域传输协议

- BOOTP (BootstrapProtocol) , 引导程序协议
- Talk和Ntalk协议
- SNMP
- NetShow协议等
- 静态和动态网络地址映射安全问题
  - 静态网络地址翻译技术在一对一的基础上替换端口信息，虽然可以屏蔽内部网络的拓扑结构，但对内部主机并未提供额外的保护功能，非法数据包可以像有效连接请求一样被翻译
  - 动态网络地址翻译技术在内部主机建立穿越防火墙的网络连接之前，相应的NAT映射并不存在。网络外部主机根本没有到达内部主机的路径，因此网络内部主机完全被屏蔽，不可能受到攻击。而对于内部网络攻击，NAT不存在任何安全保护
- 对内部主机的引诱和特洛伊木马攻击
  - 动态网络地址映射可以使得黑客难以了解网络内部结构，但是无法阻止内部用户主动连接黑客主机。
  - 如果内部主机被引诱连接到一个恶意外部主机上，或者连接到一个已被黑客安装了木马的外部主机上，内部主机将完全暴露，就像没有防火墙一样容易被攻击。
- 状态表超时问题
  - 当内部主机向外部主机发送连接请求时，动态网络地址翻译映射表内容动态生成。
  - NAT映射表条目有一个生存的周期
    - 当连接中断时，映射条目删除
    - 经过一个超时值后自动清除。

### 3 网络代理技术

- 代理 (Proxy) 只为单个或少数主机提供因特网访问服务，而不允许所有的主机均能为用户提供此类服务。只有具有访问因特网能力的主机才可以作为那些无权访问因特网的主机的代理，使其可以完成因特网访问工作。
- [3.1 应用层代理](#)
  - [3.1.1 应用层代理简介](#)
  - [3.1.2 应用层代理实现](#)
  - [3.1.3 代理服务程序](#)
  - [3.1.4 应用层代理优缺点分析](#)
- [3.2 电路级代理](#)
  - [3.2.1 电路级代理概述](#)
  - [3.2.2 电路级网关的工作原理](#)
  - [3.2.3 SOCKS代理技术](#)
  - [3.2.4 SOCKS代理的实现](#)

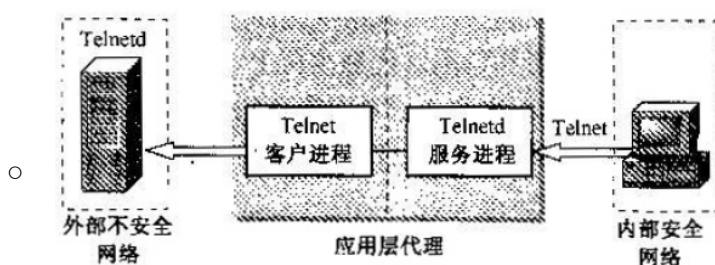
#### 3.1 应用层代理

##### 3.1.1 应用层代理简介

- 应用层代理技术针对每一个特定应用进行实现，在应用层实现网络数据流保护功能。代理的主要特点是具有状态性。代理能够提供部分与传输有关的状态，能完全提供与应用相关的状态部分传输信息，代理也能够处理和管理信息。

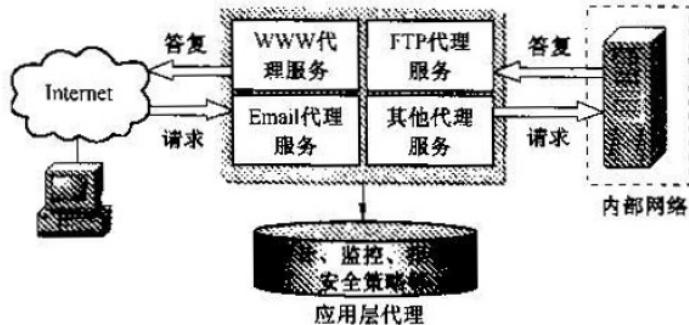


- 下图显示了内部网的一个telnet客户通过代理访问外部网的一个telnet服务器的情况



Telnet代理服务（服务器一端）

- 如图所示，应用层代理服务器起到了内部网络向外部网络申请服务时的中间转接作用。
- 应用层代理服务实际上分为一个客户代理和一个服务器代理，telnetd是一个telnet的服务器守护进程，它侦听来到telnet连接。
- 当一个连接到来之后，它首先要进行相应的身份认证，并根据安全策略来决定是否中转连接。
- 当决定转发的时候，应用层代理服务器上的telnet客户进程向真正的telnet服务器返回由代理服务器转发给telnet客户机的数据。
- 对外部网来说，外部网所见到的只是代理服务器，因为它收到的请求都来自代理服务器，对内部网来说，客户机所能直接访问的只是代理服务器。

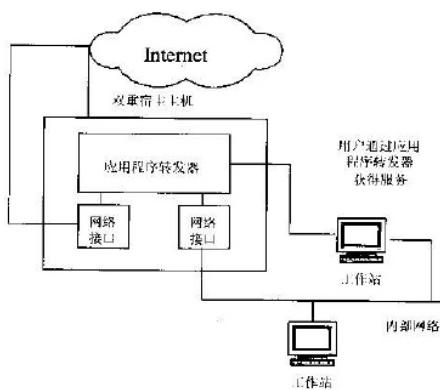


#### Internet客户通过应用层代理访问内部网络主机

- 如图所示，外部网络主机通过应用层代理访问内部网络主机，内部网络主机只接受应用层代理提出的服务请求，拒绝外部网络节点的直接请求。
- 应用层代理接受外部网络节点提出的服务请求过程为：
- 它对该用户的身份进行验证，若为合法用户，则把该请求转发给某个真正的内部网络主机（真正的服务提供者）。
- 整个服务过程中，应用代理一直监控用户的操作，并对每一个操作进行记录。一旦发现用户非法操作，就可以干涉，若为不合法的用户，则拒绝访问。

#### 3.1.2 应用层代理实现

1. 应用层代理往往通过一台双宿主机或堡垒主机实现。
2. 应用层代理允许用户访问，但不允许用户注册到应用层代理主机上
  - 防火墙系统的安全就会受到威胁。因为入侵者可能会利用这些帐号阻挠或破坏防火墙有效性的操作。
  - 如入侵者获取防火墙的管理员权限，安装特洛伊木马来截取口令、修改防火墙的安全配置文件等。
3. 应用层代理一般只向单个或部分主机提供网络服务，而不是向所有主机。具有访问能力的主机可作为那些没有访问权限的主机的代理而形成多层代理模式。
4. 代理服务器工作在应用层，因此可以提供应用层服务控制，起到外部网络与内部网络进行通信时的中间转接、监控、限制和审计等作用。



#### 通过应用程序转发器工作的双重宿主主机

- 对于Internet服务如电子邮件等，双重宿主主机的工作方式本质上就是存储转发。

#### 3.1.3 代理服务程序

- 对于一些服务，可以容易或自动提供代理，这些服务可以通过对正常服务器的配置来设置代理。但对大多数代理服务来说，要求有合适的代理服务器软件，需要针对不同服务的代理功能开发不同的代理服务程序。在客户端可以有不同的方法。
- 定制客户软件

- 软件必须知道当用户提出请求时怎样与代理服务器进行联系并且告诉代理服务器如何与真实服务器联系。
- 定制的客户软件一般只适用于特定的平台。很少有客户程序支持任何形式的代理系统。
- 有时可以修改客户程序支持代理服务器，但这需要有客户程序的源程序，并具有重新编译能力。修改客户程序也不能使代理做到对用户透明。
- 定制客户过程
  - 用户使用标准的客户软件与代理服务器连接，并通知代理服务器与真实服务器相连，以此来代替与真实服务器的直接连接。
  - 使用定制客户过程进行代理时，要求标准客户软件的用户遵守定制的过程。用户通知客户软件与代理服务器连接，还需通知代理服务器与哪台主机相连接。用户需要说明每个协议的具体步骤。例如：用户想从匿名服务器ftpgetfilenet上下载一个文件，则需要：
    - 使用FTP客户软件与代理服务器进行连接；
    - 输入用户名，并指定要连接的真实服务器名。

### 3.1.4 应用层代理优缺点分析

- 应用层代理的主要优点.应用层代理工作在应用层，和包过滤技术相比能够实现对网络数据包更加细粒度的监测、审计和控制，主要表现在：
  - 有能力支持可靠的用户认证并提供详细的注册信息；
  - 用于应用层的过滤规则，相对于包过滤路由器来说更容易配置和测试；
  - 应用层代理工作在客户机和真实服务器之间可以完全控制网络会话，可提供详细的日志和安全审计功能；
  - 提供代理服务的防火墙可以被配置成唯一的可被外部看见的主机，这样可以隐藏内部网的IP地址，保护内部主机免受外部主机的进攻；
  - 通过代理访问Internet可以解决合法的IP地址不够的问题。Internet所见到只是代理服务器的地址，内部IP可以通过代理访问Internet。
- 应用层代理的缺点.应用层代理可以在一定程度上有效地实现对内部网络的保护，但是依然存在一定的局限性：
  - 有限的连接性：代理服务器一般具有解释应用层命令的功能，如解释FTP命令、Telnet命令等，那么这种代理服务器就只能用于某一种服务。因此，可能需要提供多种不同的代理服务器，如FTP代理服务器，Telnet代理服务器等，所以能提供的服务和可伸缩性有限；
  - 技术有限：应用层代理很难为RPC、Talk和其他一些基于通用协议族的服务提供代理；
  - 应用层实现的防火墙会造成明显的性能下降；
  - 每个应用程序都必须有一个代理服务程序来进行安全控制，每一种应用升级时，相应代理服务程序也要升级，维护相对复杂；
  - 应用层代理要求用户改变自己的行为，或在访问代理服务器的每个系统上安装特殊的软件。
    - 比如，通过应用层代理Telnet的访问，可能要求用户通过两步而不是一步来建立连接。
    - 特殊的端系统软件可以让用户在Telnet命令中指定目标主机而不是应用层代理来使应用层代理透明。
- 应用层代理对操作系统和应用层的漏洞是脆弱的，不能有效检查底层的信息，传统的代理也很少是透明的。
- 从历史发展的观点来说，应用层代理应适应Internet通用用途和需要。
- Internet的环境在不断动态变化，新的协议、服务和应用在不断出现，代理应该能够处理Internet上各种类型的传输，满足新的商业需求，胜任用户对网络高带宽和安全性的需要。

## 3.2 电路级代理

- [3.2.1 电路级代理概述](#)
- [3.2.2 电路级网关的工作原理](#)
- [3.2.3 SOCKS代理技术](#)
- [3.2.4 SOCKS代理的实现](#)

### 3.2.1 电路级代理概述

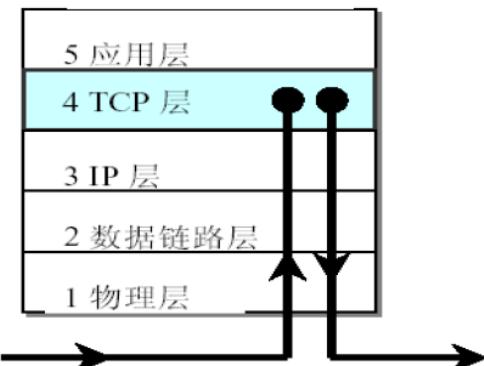
- 应用层代理为特定的服务（如FTP,Telnet等）提供代理服务，它不但转发流量而且对应用层协议做出解释。电路级代理（通常也称为电路级网关或回路级代理）也是一种代理，但只是建立起一个回路，对数据包只起转发的作用。

- 电路级网关是一个通用代理服务器，它工作于OSI互联模型的会话层或是TCP/IP协议的TCP层。

### 3.2.2 电路级网关的工作原理

- 电路级网关依赖于TCP连接，并不进行任何附加的包处理或过滤
- 数据包被提交给应用层来处理。
- 电路级网关只是在两个通信终点之间转接数据包，将简单的字节来回复制。
- 连接起源于防火墙，隐藏了受保护网络的有关信息。
- 电路级网关对外像一个代理，而对内则是一个过滤路由器，这种代理的优点是它可以对各种不同的协议提供服务。
- 一个简单的电路级网关仅传输TCP的数据段，增强的电路级网关还应该具有认证功能。

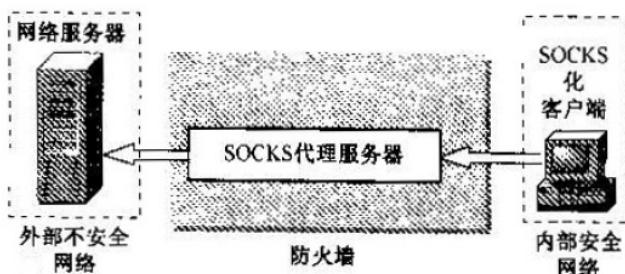
TCP/IP 协议模型



电路级网关防火墙示意图

### 3.2.3 SOCKS代理技术

- SOCKS协议是一个电路级网关的标准，于1991年由Koblas等提出，IETF也建立了SOCKS标准。SOCKS协议可以通过中继TCP数据包实现功能强大的电路级网关防火墙，而对应用层不需要作任何改变。



SOCKS防火墙工作原理图

- SOCKS防火墙工作原理：
  - 当内部网络用户需要申请外部网络节点的应用服务时：
    - 客户建立一个与SOCKS代理服务器的连接（例如连接SOCKS代理服务器的1080端口）
    - 把包括应用服务器地址、端口号和认证信息的访问请求发给SOCKS代理服务器，SOCKS代理服务器根据其配置的安全策略验证该请求的有效性，然后建立与目标的合适连接，这种方式对用户来讲是完全透明的。
  - SOCKS代理可以使那些运行在防火墙后面的主机充分地访问Internet而无须直接与外部主机建立连接；
  - 可以实现管理员明确地控制一个组织内部如何与Internet通信
  - 可以实现在特定的主机上提供特定的服务；
  - 可以禁止对Internet上的某些主机的访问，可以实现详细的日志记录。
  - 代理主要由两部分组成：
    - SOCKS服务端程序。直接同Internet和内部网络通信的程序；
    - SOCKS客户端程序。经过修改的Internet客户程序。它将使运行客户程序的主机同运行服务程序的主机通信，而不是直接与Internet通信。

### 3.2.4 SOCKS代理的实现

- SOCKS客户程序替换了UNIX中的一些套接字函数，如connect(), getsocketname(), bind(), listen()和select()。可以通过在Makefile文件中增加了一些宏定义FLAGS，然后编译，达到在应用程序中链入SOCKS库函数的目的。

- 当一个经SOCKS修改的客户程序连接到Internet上时，SOCKS库中的子程序就截获这个连接，并连接到运行SOCKS代理服务器的主机上，而不是的Internet。当连接建立后，SOCKS客户程序发送如下信息：版本号、连接请求命令、客户端的端口号、发起连接的用户名等
- SOCKS代理服务进程将检查访问控制表，判断应该接受还是拒绝这个连接。
- 如果连接被接受，SOCKS服务进程将打开一个与远程主机的连接，然后在这两主机间传递信息。
- 如果连接被拒，SOCKS服务进程就断开连接。