中山大學
SUN YAT-SEN UNIVERSITY

Module II. Internet Security

Chapter 6
Firewalls

Web Security: Theory & Applications

School of Data & Computer Science, Sun Yat-sen University

Outline

- **6.1 Introduction**
  - What Is a Firewall
  - Types of Firewalls
  - What Can a Firewall Do
  - Where to Deploy a Firewall
- **6.2 Packet Filtering Firewall**
  - What is Packet Filtering Firewall
  - How Packet Filtering Firewall Works
  - Advantages & Disadvantages
  - Attacking Packet Filtering Firewall
- **6.3 Stateful Inspection Firewall**
  - What is Stateful Inspection Firewall
  - How Stateful Inspection Firewall Works
  - Advantages & Disadvantages
  - Attacking Stateful Inspection Firewall

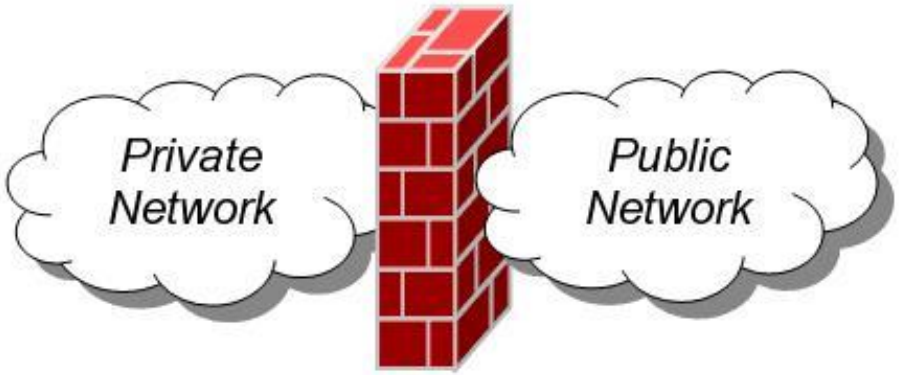
Outline

- **6.4 Application Proxy Firewall**
  - What is Proxy
  - Topological Graph of Proxy
  - Functions Offered by Proxy
  - Advantages & Disadvantage
  - Attacking Proxy
- **6.5 Bastion Host**
  - Topological Graph of Bastion Host
  - Design Principles of Bastion Host
  - Types of Bastion Host
  - Deployment of Bastion Host
- **6.6 Iptables**
  - What is Iptables
  - Architecture of Iptables
  - Command Formats
  - Examples
- **6.7 Conclusion**

6.1 Introduction

❑ Concept of Firewalls

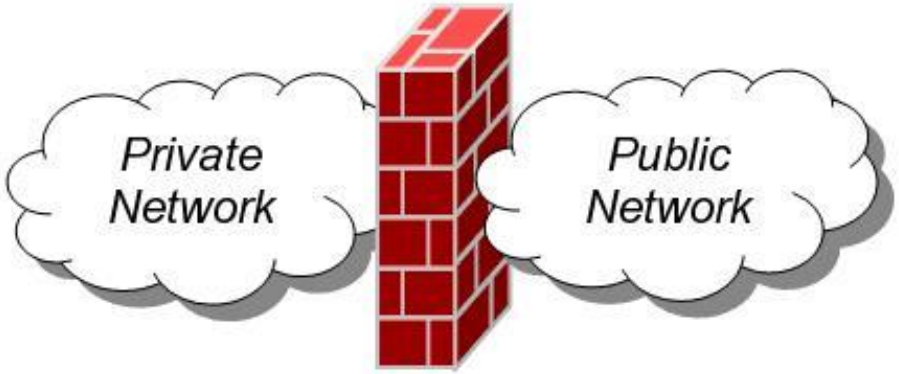
- A firewall is positioned to provide a protective barrier between an external, potentially untrusted source of traffic and an internal network.
  - ✧ A security administrator must decide on the location, on the selection, and on the number of firewalls needed.



6.1 Introduction

❑ Concept of Firewalls

- 防火墙是在两个网络之间实现访问控制的一个或一组软件或硬件系统。
  - ✧ 防火墙的最主要功能是屏蔽和允许指定的数据通信，功能的实现主要依靠一组访问控制策略，由访问控制策略决定通讯的合法性。



6.1 Introduction

❑ What a Firewall Can Do

- Manage and Control Network Traffic
  - ✧ Packet Inspection
  - ✧ Connections and State
  - ✧ Stateful Packet Inspection
- Act as an Intermediary
  - ✧ protect internal host from the risk of direct interaction
  - ✧ Insulate the protected host from threats by ensuring that an external host can never directly communicate with the protected host
- Protect Resources from threat
  - ✧ Protected resources should always be kept patched and up-to-date
- Record and Report on Events
  - ✧ Record all communications especially access policy violations through system log or proprietary logging format (专用日志格式)
  - ✧ Alarm when a policy has been violated

6.1 Introduction

❑ What a Firewall Can Do

- 管理控制网络数据流
  - ✧ 防火墙最基本的功能是控制在计算机网络中的不同信任程度区域间传送的数据流，阻止安全策略所禁止的通信，其最终目标是在不同信任程度的区域之间，通过实施安全策略提供受控连通性。
    - ◌ 典型的不同信任程度区域如互联网 (不可信任的区域) 和内部网络 (高信任度的区域) 。
  - ✧ 防火墙对流经它的网络通信进行扫描，尽量阻止对目标计算机的攻击。防火墙还可以关闭不使用的端口，禁止特定端口的流出通信，封锁特洛伊木马。它也可以禁止来自特殊站点的访问，从而防止来自不明入侵者的所有通信。

6.1 Introduction

❑ What a Firewall Can Do

- 阻塞不安全的服务和协议
  - ✧ 防火墙作为阻塞点、控制点，通过过滤不安全服务来降低风险，从而极大地提高一个内部网络的安全性。
    - ◌ 防火墙只允许经过精心选择的应用协议通过。例如防火墙可以禁止不安全的网络文件协议 NFS 协议进出网络，使得外部的攻击者无法利用这些脆弱的协议攻击内部网络。
    - ◌ 防火墙同时可以保护网络免受基于路由的攻击，如 IP 选项中的源路由攻击和 ICMP 重定向中的重定向路径。防火墙应该可以拒绝所有以上类型攻击的报文并通知防火墙管理员。

6.1 Introduction

❑ What a Firewall Can Do

- 强化网络安全策略
  - ✧ 通过以防火墙为中心的安全方案配置，能将所有安全软件 (如口令、加密、身份认证、审计等) 配置在防火墙上。与将网络安全问题分散到各个主机上分别解决相比，防火墙的集中安全管理更为经济高效。
    - ◌ 例如在网络访问时，一次一密口令系统和其它的身份认证系统不必分散在各个主机上，而可以集中在防火墙上。

6.1 Introduction

❑ What a Firewall Can Do

- 对网络存取和访问进行监控审计
  - ✧ 如果所有的访问都必须经过防火墙，那么防火墙可以建立日志记录这些访问，同时提供网络使用情况的统计数据。当发生可疑动作时，防火墙能进行适当的报警，并提供网络是否受到监测和攻击的详细信息。
    - ◌ 收集一个网络的使用和误用情况非常重要，可以据此了解防火墙是否能够抵挡攻击者的探测和攻击，并且判断防火墙的控制是否充足。
    - ◌ 网络使用情况统计对网络需求分析和威胁分析等也非常重要。

6.1 Introduction

❑ What a Firewall Can Do

- 保护内部信息
  - ✧ 利用防火墙对内部网络的划分，可实现对内部网重点网段的隔离，从而限制了局部的重点或敏感网络安全问题对全局网络造成的影响。防火墙同样可以阻塞有关内部网络中的 DNS 信息，保护内部主机的域名和 IP 地址的私密性。
    - ◌ 内部网络中一些不引人注意的细节可能包含了有关安全的线索，甚至因此而暴露了内部网络的某些安全漏洞。使用防火墙可以屏蔽那些透漏内部细节的服务 (如 Finger)。
      - Linux 的 Finger 命令显示了主机的所有用户的注册名、真名，最后登录时间和使用 shell 类型等。Finger 显示的信息非常容易被攻击者所获悉。攻击者可以知道一个系统使用的频繁程度，这个系统是否有用户正在连线上网，这个系统是否在被攻击时会引起注意等等。

6.1 Introduction

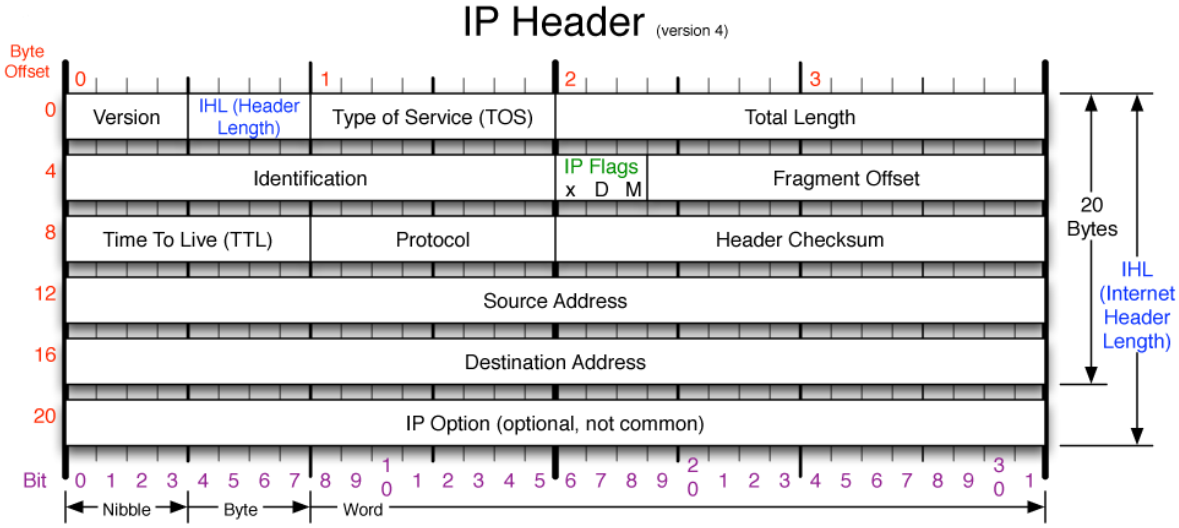
❑ Types of Firewalls

- 1st generation : Packet Filters
  - ✧ Packet Filtering Firewalls decide to forward or to drop a certain packet according to the information of the packet's head. Packet filters act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet filter's set of rules, the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source).
  - ✧ This type of packet filtering pays no attention to whether a packet is part of an existing stream of traffic (i.e. it stores no information on connection "state"). Instead, it filters each packet based only on information contained in the packet itself.
  - ✧ Packet filtering firewalls work mainly on the first three layers (Physical layer, Data Link layer and Network layer) of the OSI reference model, which means most of the work is done between the network and physical layers, with a little bit of peeking into the transport layer to figure out source and destination port numbers.

6.1 Introduction

❑ Types of Firewalls

- 1st generation : Packet Filters



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

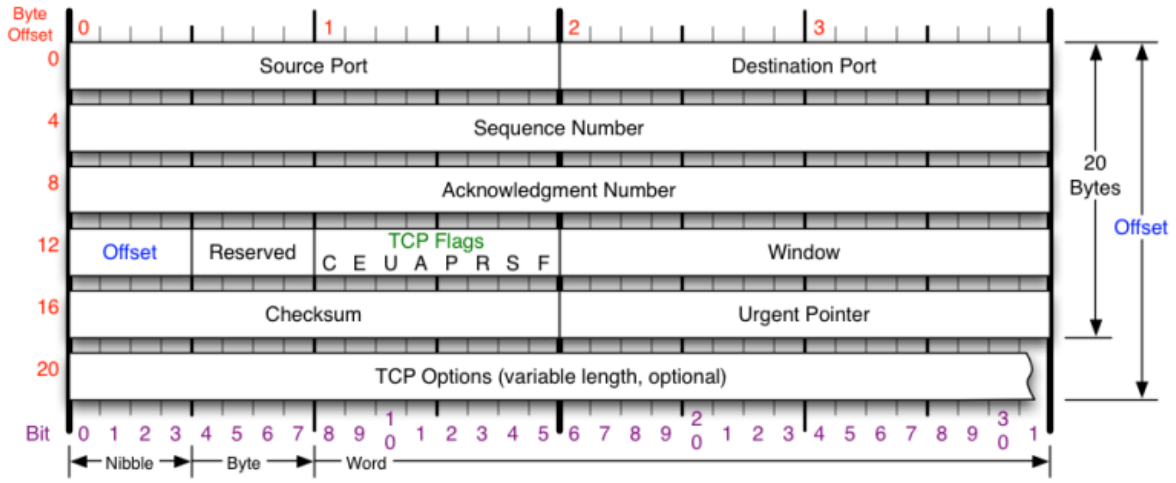
Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

6.1 Introduction

❑ Types of Firewalls

- 1st generation : Packet Filters

TCP Header



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

6.1 Introduction

❑ Types of Firewalls

- 2nd generation : Stateful Filters
  - ✧ Stateful filtering firewalls perform the work of their first-generation predecessors but operate up to transport layer of the OSI model. This is achieved by retaining enough packets to make a judgement about its state.
  - ✧ Known as stateful packet inspection, all connections passing through it are recorded to determine whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection. Though static rules are still used, these rules can now contain connection state as one of their test criteria.
    - ◌ Certain DoS attacks bombard the firewall with thousands of fake connection packets to overwhelm it by filling its connection state memory

6.1 Introduction

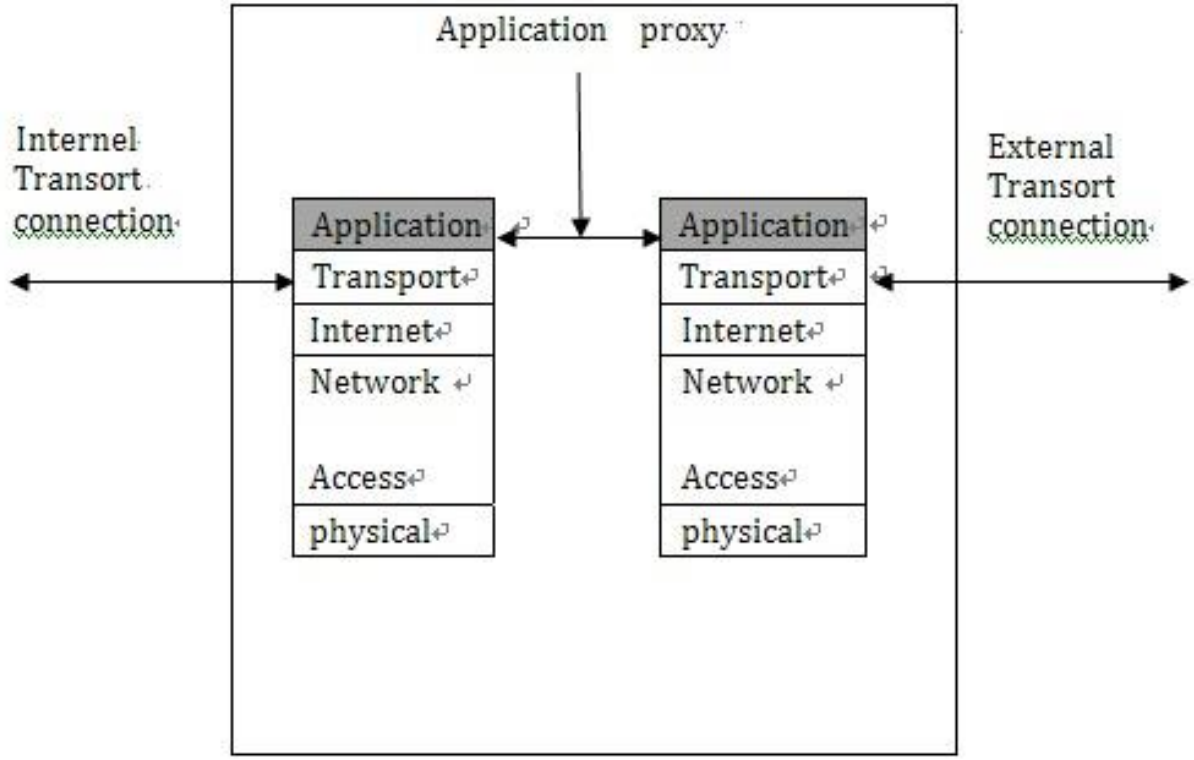
❑ Types of Firewalls

- 3rd generation : Application Layer Filters
  - ✧ Application layer filtering understands certain applications and protocols (such as File Transfer Protocol FTP, Domain Name System DNS, or Hypertext Transfer Protocol HTTP).
  - ✧ This is useful as it is able to detect if an unwanted protocol is attempting to bypass the firewall on an allowed port, or detect if a protocol is being abused in any harmful way.
  - ✧ The existing deep packet inspection functionality of modern firewalls can be shared by Intrusion Prevention Systems (IPS).

6.1 Introduction

❑ Types of Firewalls

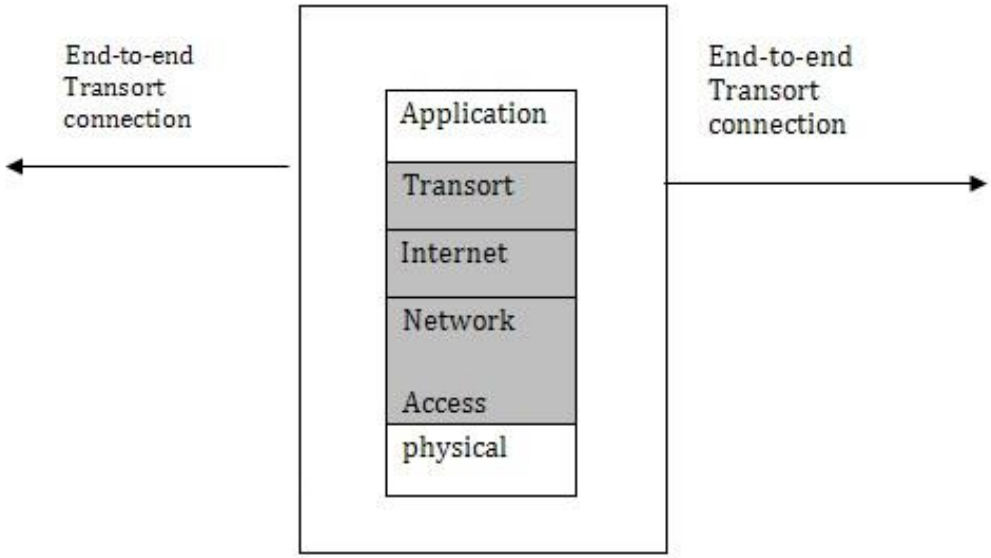
- 3rd generation: Application Layer Filters



6.1 Introduction

❑ Types of Firewalls

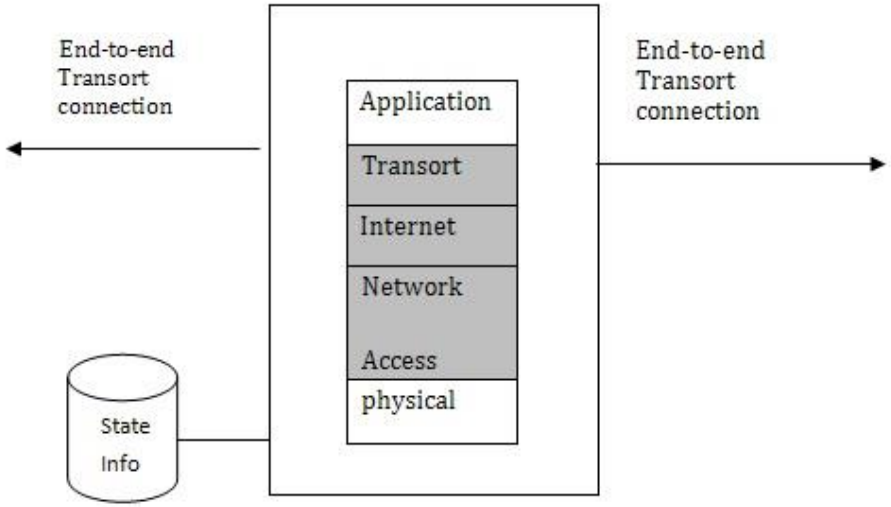
- 防火墙可以作如下三种类型的划分：
  - ✧ 包过滤防火墙 (网络级防火墙)
    - ◌ 包过滤防火墙 (或分组过滤防火墙) 工作在网络层以下，通过查看所流经的数据包的包头 (Header) 信息，决定丢弃或接受这个数据包，或者执行其它更复杂的动作。



6.1 Introduction

❑ Types of Firewalls

- 防火墙可以作如下三种类型的划分：
  - ✧ 状态检测防火墙
    - ◌ 主要工作在网络层，采用状态检测技术，是传统包过滤技术的功能扩展。状态检测防火墙在网络层使用一个检查引擎截获数据包并抽取出与应用层状态有关的信息，以此为依据决定对该连接是接受还是拒绝。



6.1 Introduction

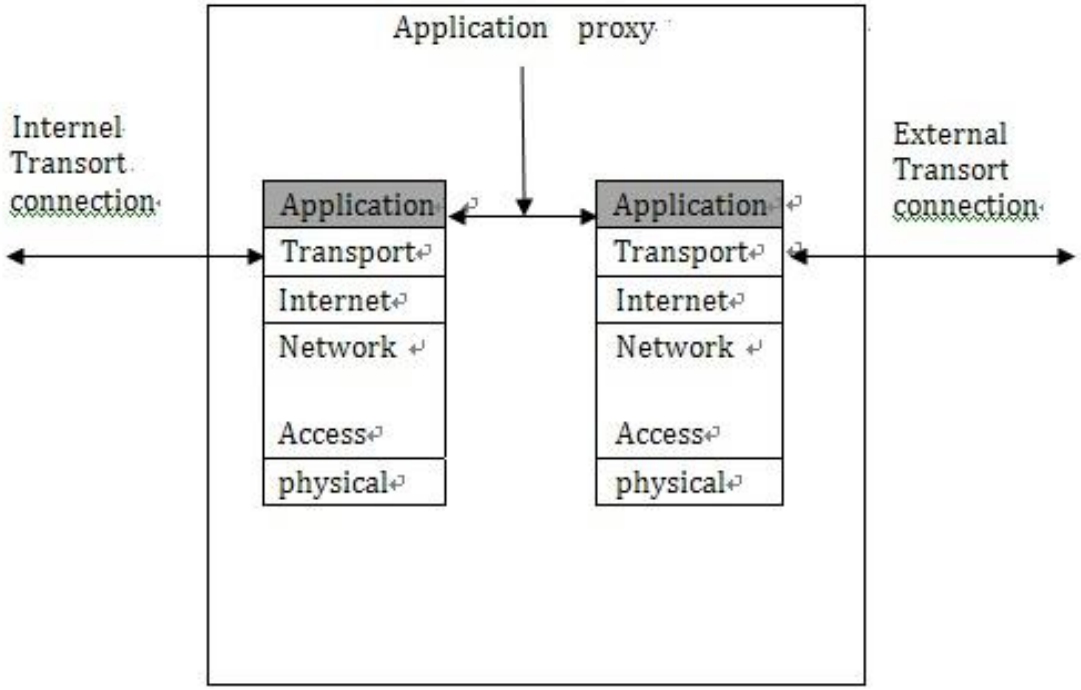
❑ Types of Firewalls

- 防火墙可以作如下三种类型的划分：
  - ✧ 应用层网关
    - ◌ 也称应用层防火墙或应用层代理防火墙。
    - ◌ 当用户希望从可信赖的网络连接到不被信赖的网络的服务(例如 Internet) 时，应用层网关代理服务器能有效地伪装成在因特网上的真实服务器，对请求作出评估，并决定允许或拒绝。
    - ◌ 应用级网关检查进出的数据包，通过网关复制传递数据，防止在受信任服务器和客户机与不受信任的主机间直接建立联系。应用级网关能够理解应用级上的协议，完成较为复杂的访问控制。但针对每一种协议需要相应的代理软件，效率不如网络级防火墙。用户在受信任的网络上通过防火墙访问 Internet 或 Intranet 时会存在延迟。

6.1 Introduction

❑ Types of Firewalls

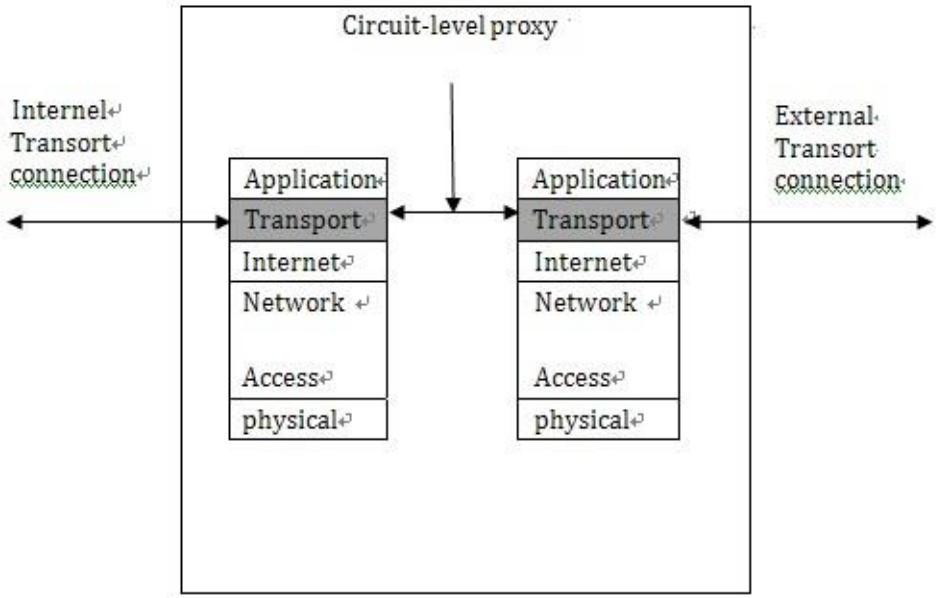
- 防火墙可以作如下三种类型的划分：
  - ✧ 应用层网关



6.1 Introduction

❑ Types of Firewalls

- 防火墙可以作如下三种类型的划分：
  - ✧ 电路级网关 Circuit-Level Gateway
    - ◌ 电路级网关与应用层网关结合用于监控受信任的客户或服务器与不受信任的主机间的 TCP 握手信息，并以此决定该会话 (session) 是否合法，例如代理服务器。



6.1 Introduction

❑ Types of Firewalls

- 防火墙技术的发展基于其实现方式，还可以划分为四个阶段：
  - ✧ 第1代：基于路由器的分组过滤防火墙。
    - ◌ 由于多数路由器中本身就包含有分组过滤功能，网络访问控制可通过路由控制来实现，从而使具有分组过滤功能的路由器成为第1代防火墙产品。
  - ✧ 第2代：应用层防火墙。
    - ◌ 应用层防火墙将分组过滤功能从路由器中独立出来，加上审计和告警功能，并针对用户需求提供模块化支持，是一类纯软件产品。
  - ✧ 第3代：建立在通用操作系统上的防火墙。
    - ◌ 第3代防火墙建立在通用操作系统 (如 Linux) 上，包括分组过滤和代理功能，获得广泛应用。这一类防火墙可以由纯软件实现，也可以由硬件方式实现。
  - ✧ 第4代：建立在安全操作系统上的防火墙。

6.1 Introduction

❑ Where to Deploy a Firewall

- It is common to base a firewall on a
  - ✧ Stand-alone machine running a common operating system, such as UNIX or Linux.
  - ✧ Or be implemented as a software module in a router or LAN switch.
- In consideration of where to base them, we have three kind of firewalls
  - ✧ Bastion Host
  - ✧ Host-Based Firewall
  - ✧ Personal Firewall

6.1 Introduction

❑ Where to Deploy a Firewall

- Bastion Host (堡垒主机)
  - ✧ A bastion host is a computers on a network, specifically designed and configured to withstand attacks
    - ◌ It's identified by the firewall admin as a critical strong point in the network's security
  - ✧ The firewalls (application-level or circuit-level gateways) and routers can be considered bastion hosts.
  - ✧ Other types of bastion hosts include web, mail, DNS, and FTP servers.

6.1 Introduction

❑ Where to Deploy a Firewall

- Bastion Host
  - ✧ Securing Bastion Hosts
    - ◌ Each bastion host fulfills a specific role, all unnecessary services, protocols, programs, and network ports are disabled or removed.
    - ◌ Bastion hosts do not share authentication services with trusted hosts within the network so that if a bastion is compromised the intruder will still not have 'the keys to the castle.'
    - ◌ A bastion host is hardened to limit potential methods of attack. The specific steps to harden a particular bastion host depend upon the intended role of that host as well as the operating system and software that it will be running.
    - ◌ All unnecessary TCP and UDP ports will be disabled.

6.1 Introduction

❑ Where to Deploy a Firewall

- Bastion Host
  - ✧ Securing Bastion Hosts
    - ◌ All non-critical services will be removed.
    - ◌ As many utilities and system configuration tools as is practical will also be removed.
    - ◌ All appropriate service packs, hot fixes, and patches should be installed.
    - ◌ Logging of all security related events need to be enabled and steps need to be taken to ensure the integrity of the logs so that a successful intruder is unable to erase evidence of their visit.
    - ◌ Any local user account and password databases should be encrypted if possible.

6.1 Introduction

❑ Where to Deploy a Firewall

- Host-Based Firewall
  - ✧ A host-based firewall filters and restricts the flow of packets. It is a software module used to secure a server.
    - ◌ Such modules are available in many operating systems or can be provided as an add-on package.
  - ✧ Advantages of using Host-Based Firewalls
    - ◌ Filtering rules can be tailored (量身定做) to the host environment.
      - Specific corporate security policies for servers can be implemented, with different filters for servers used for different application.

6.1 Introduction

❑ Where to Deploy a Firewall

- Host-Based Firewall
  - ✧ Advantages of using Host-Based Firewalls
    - ◌ Protection is provided independent of topology. Thus both internal and external attacks must pass through the firewall.
    - ◌ Used in conjunction with stand-alone firewalls (bastion host).
      - The host-based firewall provides an additional layer of protection. A new type of server can be added to the network, with its own firewall, without the necessity of altering the network firewall configuration.

6.1 Introduction

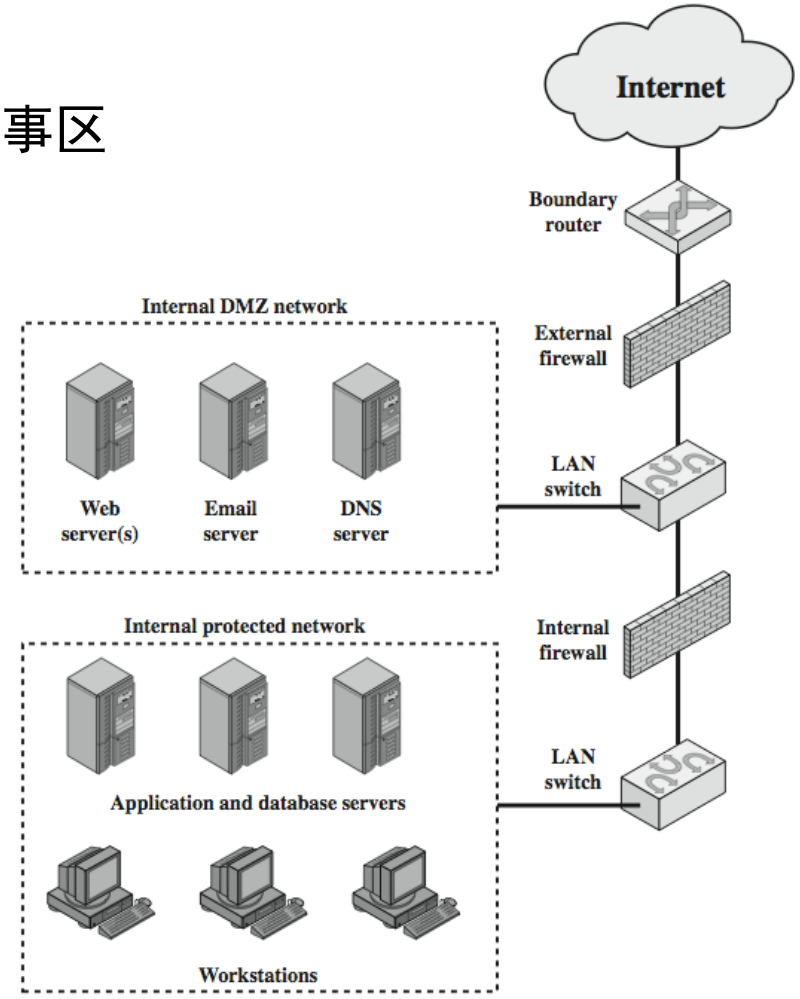
❑ Where to Deploy a Firewall

- Personal Firewall
  - ✧ Controls traffic between PC/workstation and Internet or enterprise network
  - ✧ A software module on personal computer
  - ✧ Or in home/office DSL/cable/ISP router
  - ✧ Typically much less complex than other firewall types
  - ✧ Primary role to deny unauthorized remote access to the computer
  - ✧ Monitor outgoing activity for malware
  - ✧ *Example.*
    - ◌ Windows Firewall

6.1 Introduction

❑ Where to Deploy a Firewall

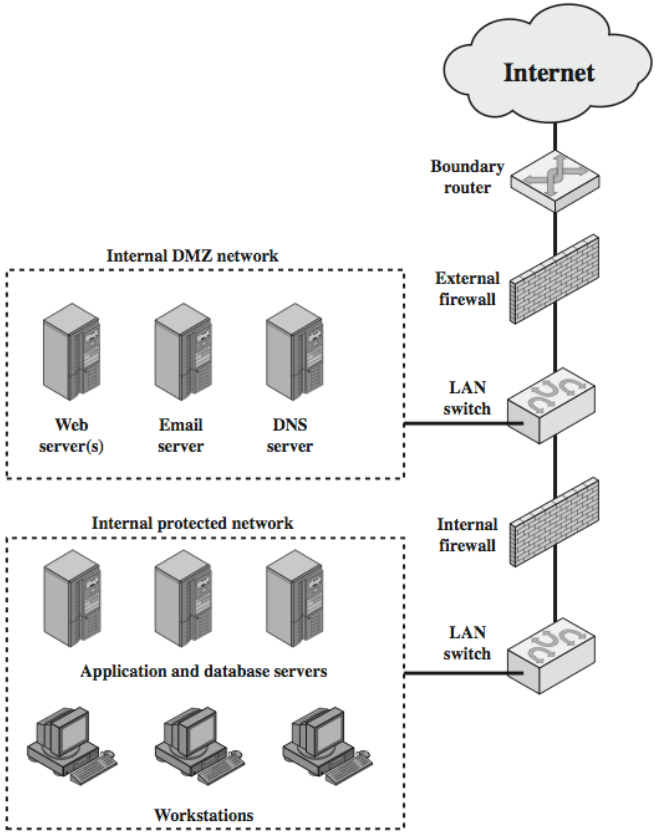
- DMZ Network
  - ✧ DMZ - De Militarized Zone, 非军事区
  - ✧ Systems that are externally accessible but needs some protection allocated in DMZ networks.



6.1 Introduction

❑ Where to Deploy a Firewall

- A DMZ Network Configuration
  - ✧ The External Firewall
    - ◌ access control and protection for the DMZ systems
    - ◌ basic level of protection for the remainder of the enterprise network
  - ✧ The Internal Firewall
    - ◌ adds more stringent (严格/苛刻) filtering capability to protect enterprise servers and workstations from external attack
    - ◌ it protects the remainder of the network from attacks launched from DMZ systems, and protects DMZ systems from attack by internal hosts.



6.1 Introduction

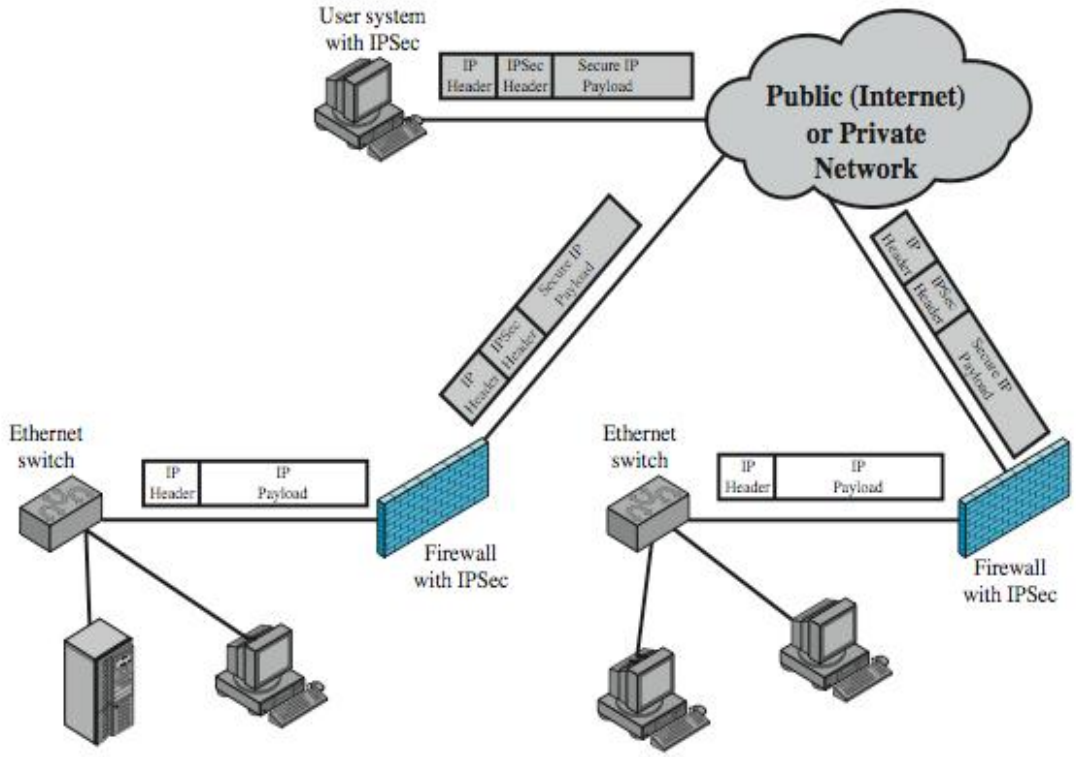
❑ Where to Deploy a Firewall

- VPN Network
  - ✧ If IPSec is implemented, VPN traffic passing through the firewall in both directions is encrypted.
    - ◌ In this case, the firewall is unable to perform its filtering function or other security functions, such as access control, logging, or scanning for viruses.
  - ✧ IPSec could be implemented in the boundary router, outside the firewall. However, this router device is likely to be less secure than the firewall and thus less desirable as an IPSec platform.

6.1 Introduction

❑ Where to Deploy a Firewall

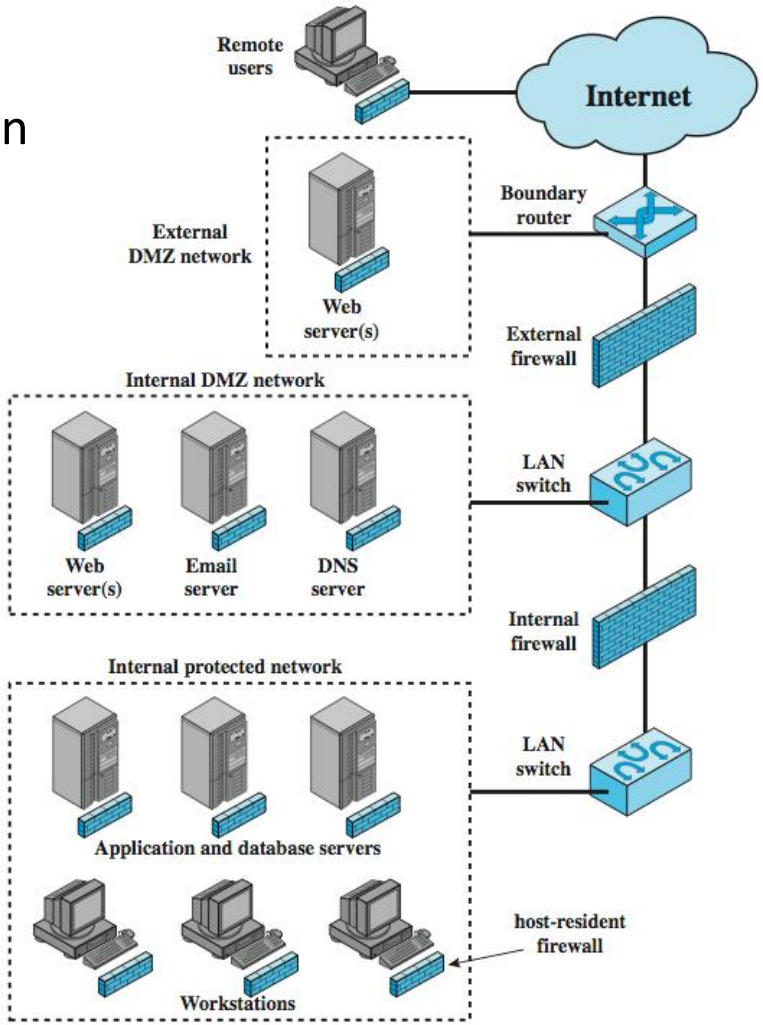
- VPN Network
  - ✧ A VPN Network configuration



6.1 Introduction

❑ Where to Deploy a Firewall

- Distributed Firewalls
  - ✧ A distributed firewall configuration involves
    - ○ stand-alone firewall devices
    - ○ host-based firewalls
  - ✧ Used by some large businesses and government organizations.



6.2 Packet Filtering Firewall

6.2 Packet Filtering Firewall

- What is Packet Filtering Firewall
- How Packet Filtering Firewall Works
- Advantages & Disadvantages
- Attacking Packet Filtering Firewall

6.2 Packet Filtering Firewall

❑ What is Packet Filtering Firewall

- Packet Filtering Firewall allows the packet which match the established rule set to pass and deny the packet which violate the established rule set, at the same time, it will record log message, alarm the administrator when a policy has been violated.
- 包过滤防火墙是最基本的防火墙，通常工作在 OSI 的三层及三层以下，可控的内容主要包括报文的源地址、报文的目标地址、服务类型，以及第二层数据链路层可控的 MAC 地址等。除此以外，随着包过滤防火墙的发展，部分 OSI 四层的内容也被包括进来，如报文的源端口和目的端口。
- 包过滤技术允许符合安全过滤规则 (基于组织或机构预先制定的网络安全策略所定义) 的数据包通过，拒绝那些不符合安全过滤规则的的数据包通过，并且执行预先定义的操作，如记录过滤信息、发送报警信息给管理人员等。

6.2 Packet Filtering Firewall

❑ What is Packet Filtering Firewall

- What to Filter
  - ✧ IP address filtering
  - ✧ TCP/UDP's port filtering
  - ✧ ACK filtering
  - ✧ UDP packet filtering

6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- A packet filter has a set of rules with accept or deny actions, based on the information contained in the packet itself.
  - ✧ IP packet header
  - ✧ TCP packet header
- Using different field in the head of the packet to filter, include the packet‘s source and destination address, its protocol, port number, and so on.
- When the packet filter receives a packet of information, the filter compares the packet to your pre-configured rule set.
- At the first match, the packet filter either accepts or denies the packet of information.

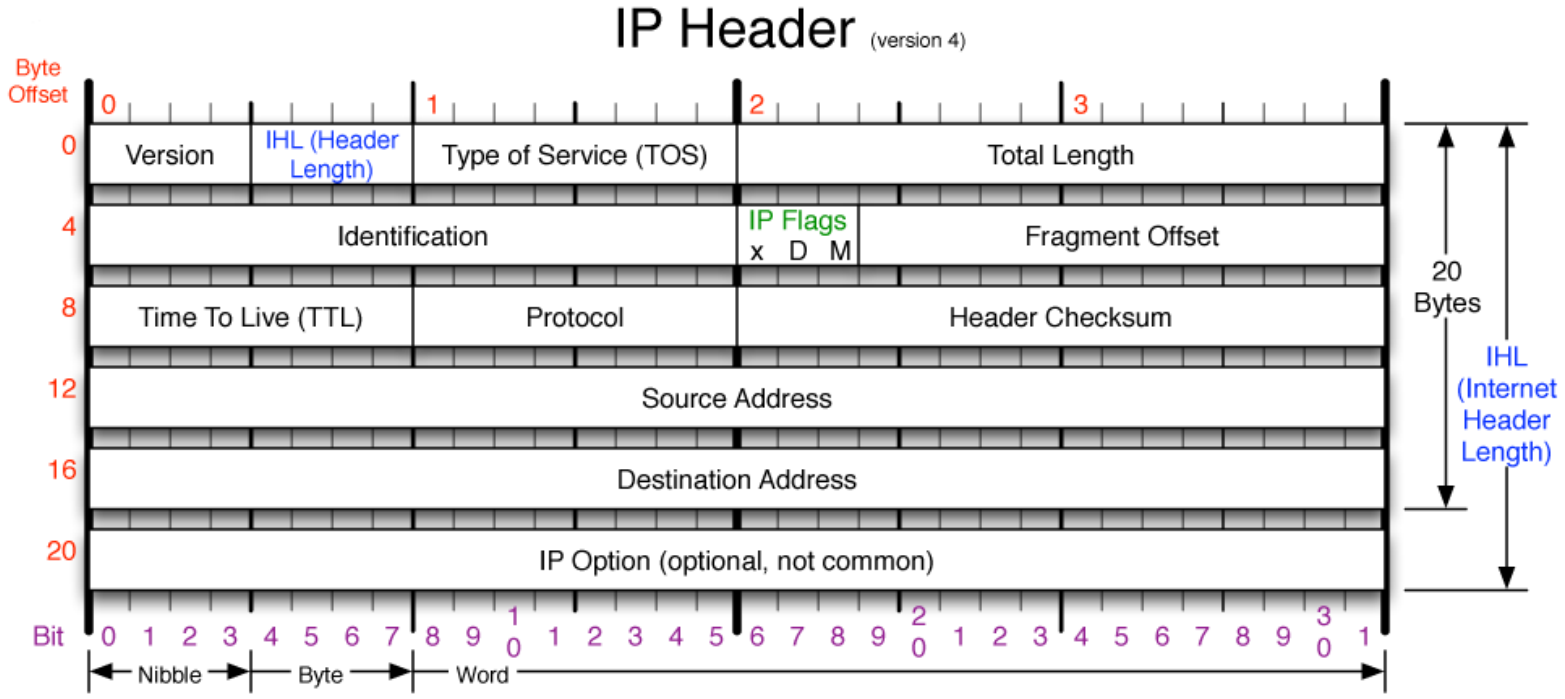
6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- 包过滤技术分析数据包的包头的各个字段，包括源 IP 地址、目的 IP 地址、数据载荷协议类型、IP 选项、源端口、目的端口、TCP 选项以及数据包传递的方向等信息。根据这些字段的内容，包过滤以安全过滤规则为评判标准，来确定是否允许数据包通过。
- 安全过滤规则是包过滤技术的核心，直接体现网络安全策略。安全过滤规则集是一个访问控制列表，该表的每一条记录都明确定义了对符合该记录条件的数据包所要执行的动作：允许或拒绝通过，其中的条件是对上述数据包包头的各个字段内容的限定。

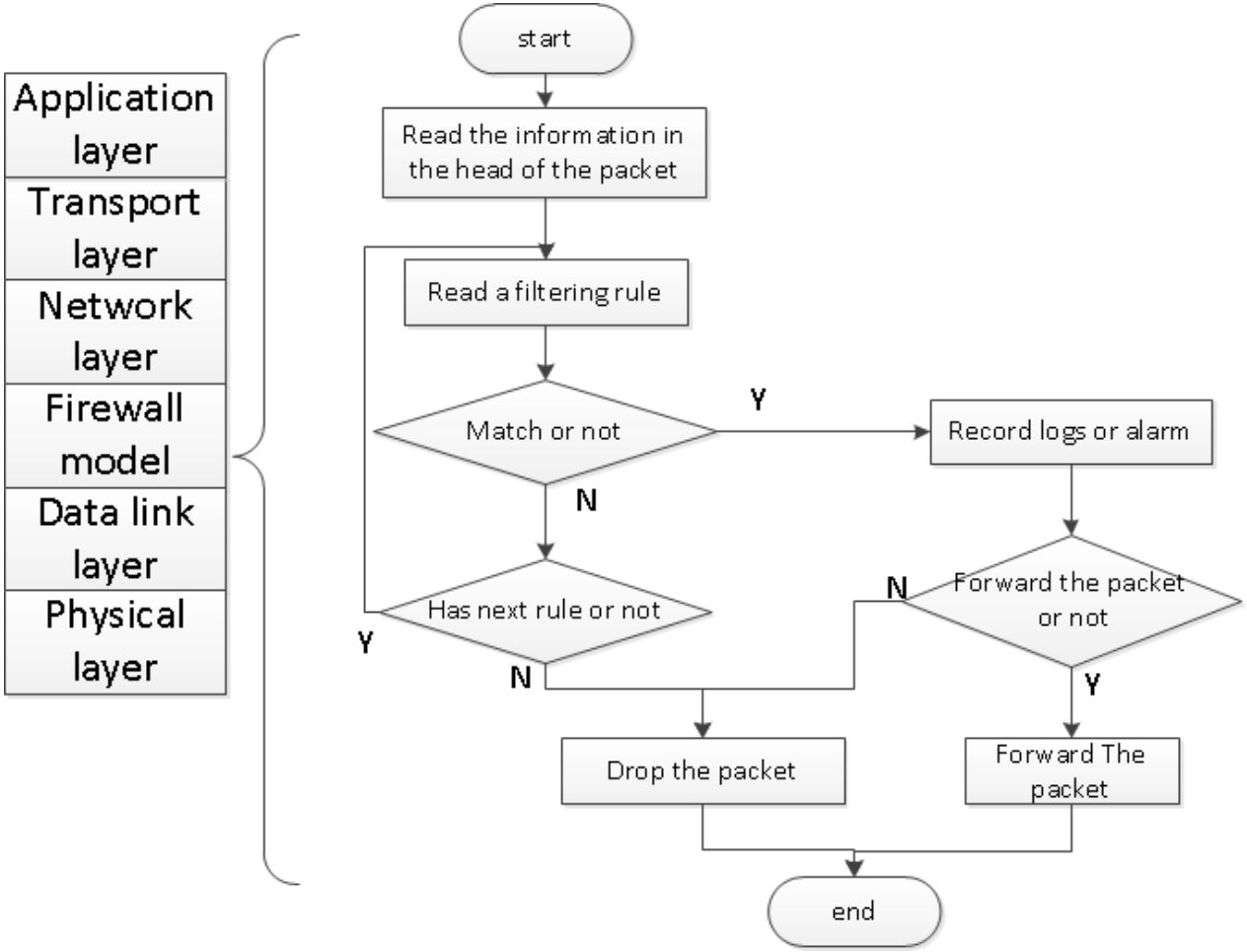
6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works



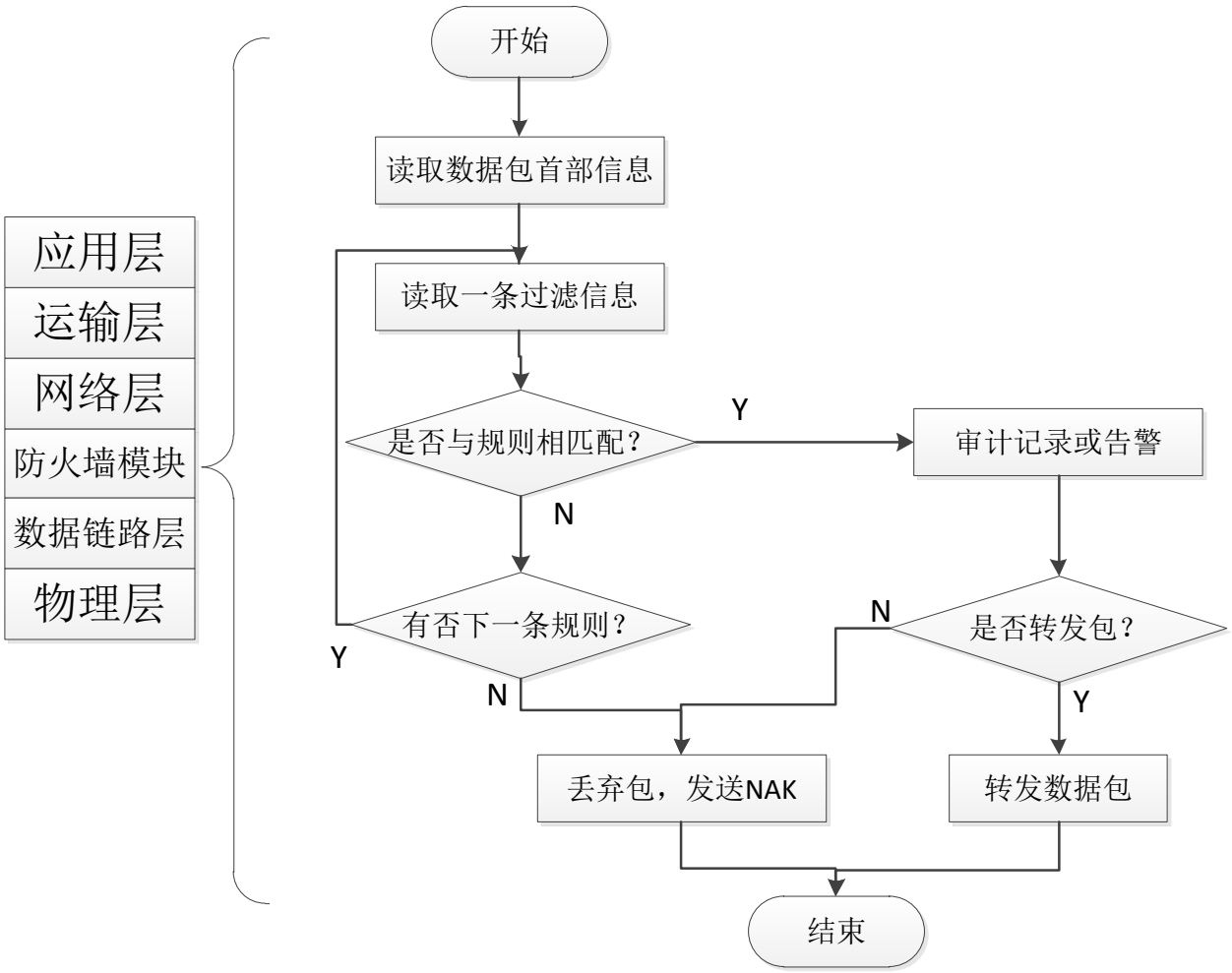
6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works



6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works



6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- 实现包过滤技术的防火墙模块在系统协议栈的网络层之前拦截数据包，它工作在系统协议栈的网络层之下，数据链路层之上。
- 实现包过滤技术的防火墙模块检测数据包的包头部分，按照访问控制列表的顺序，将包头各个字段的内容与安全过滤规则进行逐条对比，直到找到一条相符的安全过滤规则为止，接着按照安全过滤规则的定义执行相应动作。如果没有相符的安全过滤规则，就执行防火墙默认的安全过滤规则。

6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- 针对 IP 的过滤：
  - ✧ 查看每个 IP 数据包包头，将包头数据与规则集比较，转发规则集允许的数据包，拒绝规则集不允许的数据包。
    - ◌ 针对源 IP 地址过滤：只允许受信任的主机访问网络资源，拒绝一切不可信的主机访问。
    - ◌ 针对目的 IP 地址过滤：将所有源 IP 不是内联网络，而目的 IP 恰巧落在内联网络的数据包拒绝。
- 针对 ICMP 的过滤：
  - ✧ 阻止存在泄漏用户网络敏感信息的危险的 ICMP 数据包进出网络，拒绝所有可能被攻击者利用的、对用户网络进行破坏的 ICMP 数据包。

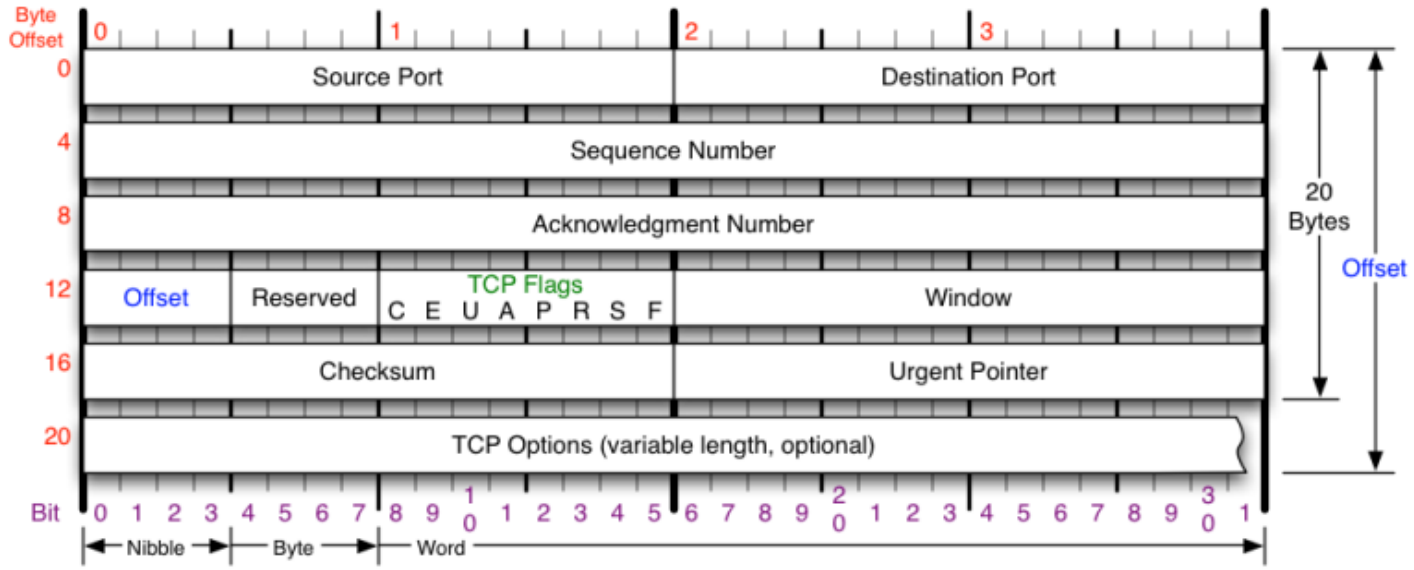
6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- 针对 TCP 的过滤：
  - ✧ 设定对源端口或目的端口的过滤，也称为端口过滤或协议过滤。例如拒绝内部主机到外部服务器的80端口的连接，就可以实现禁止内部用户访问外部网站。
  - ✧ 两个网络节点之间如果存在基于 TCP 的通信，那么存在着至少一个会话。会话总是从连接建立阶段开始的，而 TCP 的连接建立过程就是3 次握手的过程。注意到除了上述连接建立的过程之外，会话过程的 Syn 位 (TCP Flags 的 S 位) 始终为0。因此针对 TCP Flags 的标志位过滤，拒绝 SYN 位为1的一类报文，就可以阻断 TCP 通信连接的建立。

6.2 Packet Filtering Firewall

- TCP Header



TCP Flags

C E U A P R S F

Congestion Window
C 0x80 Reduced (CWR)
E 0x40 ECN Echo (ECE)
U 0x20 Urgent
A 0x10 Ack
P 0x08 Push
R 0x04 Reset
S 0x02 Syn
F 0x01 Fin

Congestion Notification

ECN (Explicit Congestion Notification). See RFC 3168 for full details, valid states below.

Packet State	DSB	ECN bits
Syn	0 0	1 1
Syn-Ack	0 0	0 1
Ack	0 1	0 0
No Congestion	0 1	0 0
No Congestion	1 0	0 0
Congestion	1 1	0 0
Receiver Response	1 1	0 1
Sender Response	1 1	1 1

TCP Options

0 End of Options List
1 No Operation (NOP, Pad)
2 Maximum segment size
3 Window Scale
4 Selective ACK ok
8 Timestamp

Checksum

Checksum of entire TCP segment and pseudo header (parts of IP header)

Offset

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

RFC 793

Please refer to RFC 793 for the complete Transmission Control Protocol (TCP) Specification.

6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- 针对 TCP 的过滤：
  - ✧ TCP Header
    - ◌ URG: 紧急指针位，1-有紧急数据需要优先传递
    - ◌ ACK: 确认位
    - ◌ PSH: 紧急位，1-发送方马上发送该分段，接收方尽快将报文交给应用层，不做队列处理
    - ◌ RST: 重置位，1-本数据包不属于任何一个连接；0-本数据包传给自己
    - ◌ SYN: 请求位，1-发起连接
    - ◌ FIN: 完成位，1-断开连接

6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- 针对 TCP 的过滤：
  - ✧ 例如：假设连接的发起者是 *Alice*，接收者是 *Bob*，过程如下：
    - ① *Alice* 向 *Bob* 发出连接请求报文，其 SYN 位为1，而包括 ACK 位在内的其他标志位为0。该报文携带了*Alice* 自行选择的一个通信初始序号；
    - ② *Bob* 接受该连接请求，向 *Alice* 返回一个连接应答报文，其 SYN 位为1，ACK 位为1。该报文不但携带对 *Alice* 通信初始序号的确认信息（加1），而且携带 *Bob* 自行选择的另一个通信初始序号。如果 *Bob* 拒绝该连接请求，则返回的报文 RST 位置1；
    - ③ *Alice* 向 *Bob* 返回一个应答报文，其 ACK 位为1。该报文对 *Bob* 自行选择的通信初始序号进行确认，返回该值加1作为希望接收的下一个报文的序号。

6.2 Packet Filtering Firewall

❑ How Packet Filtering Firewall Works

- 针对 UDP 的过滤：
  - ✧ 阻断某个端口，除非要求 UDP 传输。
    - ◌ UDP 与 TCP 采用的是不同的服务策略。TCP 是面向连接的，相邻报文之间具有明显的关系，数据流内部也具有较强的相关性，因此过滤规则的制定相对比较容易；UDP 基于无连接的服务，一个 UDP 用户数据包报文中携带了到达目的地所需的全部信息，不需要返回任何的确认，报文之间的关系很难确定，因此很难制定相应的过滤规则。

6.2 Packet Filtering Firewall

❑ Advantages

- High speed
  - ✧ 这是因为包过滤防火墙只检查数据包的包头，而对数据包所携带的内容没有任何形式的检查。
- Transparent to users
  - ✧ 包过滤防火墙对用户是透明的，无需在用户端进行任何配置。

6.2 Packet Filtering Firewall

- **Disadvantages**
  - Can not filter the packet according the containing of the packet
  - Only offer brief log messages
  - Every port that may be used must be open to the external network, which increase the risk of attack
  - Very difficult to configure ACL (Access Control List)

6.2 Packet Filtering Firewall

❑ Disadvantages

- 包过滤防火墙无法对数据包及上层的内容进行核查，因此无法阻止内容未能通过审核的数据包。
- 所有有可能用到的端口都必须静态放开，对外界暴露，从而极大的增加了被攻击的可能性。对某个端口的开放意味着相应端口对应的服务所能够提供的全部功能都被放开，即使通过防火墙的数据包有攻击性，也无法进行控制和阻断。
  - ✧ 例如 UNIX 下的危险的 rpc 服务，它们工作在高端口，针对这些服务的攻击程序在互联网上异常流行。
  - ✧ 例如针对微软 IIS 漏洞的 Unicode 攻击使用的是防火墙所允许的80端口，而包过滤防火墙无法对数据包内容进行审查。未打相应补丁的提供 web 服务的系统，即使在包过滤防火墙的屏障之后，也会被攻击者轻松取得超级用户权限。

6.2 Packet Filtering Firewall

❑ Disadvantages

- 包过滤防火墙工作在较低层次，防火墙本身所能接触到的信息较少，无法提供描述事件细节的日志系统，生成的日志常常只是包括数据包捕获时间、三层的 IP 地址、四层的端口等原始信息。
  - ✧ 例如：某日志记录了11月23日14点13分防火墙阻止了一个数据包，其源 ip 地址x.x.x.x，端口4131，目的 ip 地址y.y.y.y，目的端口3389，包头20字节，净荷长度28。防火墙不会理会这个数据包内容，而这对安全管理员而言恰是至为关键的。因为即使一个非常优秀的系统管理员，一旦陷入大量的通过/屏蔽的原始数据包信息中，往往也难以理清头绪，当发生安全事件时会给管理员的安全审计带来很大的困难。
- 对于复杂的网络结构，管理员难以配置合适的 ACL (Access Control List)。
  - ✧ 当网络发展到一定规模时，ACL 出错几乎是必然的。

6.2 Packet Filtering Firewall

❑ Attacking Packet Filtering Firewall

- 包过滤防火墙在网络层截获网络数据包，获得数据包的源 IP 地址、目的 IP 地址、TCP/UDP 源端口、TCP/UDP 目的端口等信息，根据防火墙的规则表检测攻击行为。
- 包过滤防火墙以一个个单独的数据包来匹配规则。
  - ✧ 但是对同一个 TCP 连接，其数据包是前后关联的 (发包顺序：syn 包 → 数据包 → fin 包，数据包的前后序列号也是相关的)。如果割裂这些关系，单独过滤数据包，很容易被精心构造的攻击数据包欺骗 (例如 Nmap 的扫描攻击) 。
- 包过滤防火墙很容易受到的攻击：
  - ✧ IP 地址欺骗 IP Address Spoofing Attack
  - ✧ 拒绝服务 Denial-of-service Attack
  - ✧ 碎片攻击 Tiny Fragment Attack
  - ✧ 木马攻击 Trojan Attack

6.2 Packet Filtering Firewall

❑ Attacking Packet Filtering Firewall

- IP Address Spoofing Attack
  - ✧ IP 地址欺骗修改数据包的源、目的地址和端口，模仿一些合法的数据包来骗过防火墙的检测。
    - ◌ 例如：外部攻击者将他的数据报源地址改为内部网络地址，获得防火墙的放行。
    - ◌ 防火墙结合接口、地址进行匹配可以防范这类攻击。
  - ✧ 数据包穿透防火墙以后主机的响应包回复给了伪装的地址，攻击者无法获得响应包，无法与防火墙后的主机建立通信。
- Denial-of-Service Attack
  - ✧ 简单的包过滤防火墙不能跟踪 TCP 的状态，很容易受到拒绝服务攻击。受到 DoS 攻击的防火墙一直处于繁忙状态，规则选择不当的话有可能被绕过。

6.2 Packet Filtering Firewall

❑ Attacking Packet Filtering Firewall

- Tiny Fragment Attack
  - ✧ 在 IP 的分片包中，所有的分片包用一个分片偏移字段标志分片包的顺序，但是，只有第一个分片包含有 TCP 端口号的信息。当 IP 分片包通过包过滤防火墙时，防火墙只根据第一个分片包的 TCP端口信息判断是否允许通过，对该分片包的其他后续分片不作检测，让它们直接通过。
  - ✧ 攻击者可以通过先发送第一个合法的 IP 分片，通过防火墙的检测，封装了恶意数据的后续分片包可以穿透防火墙，直接到达内部网络主机，从而威胁网络和主机的安全。

6.2 Packet Filtering Firewall

❑ Attacking Packet Filtering Firewall

- Trojan Attack
  - ✧ 对于传统的包过滤防火墙，木马几乎是最有效的攻击手段。包过滤防火墙一般只过滤低端口 (1-1024)，高端口因为一些服务需要必须打开，因此无法过滤。预先植入的木马会在高端口打开等待。
  - ✧ 木马穿透的前提是攻击者利用内部网络主机开放的服务漏洞在被攻击的主机上植入并运行木马程序，因此攻击具有一定的局限性。

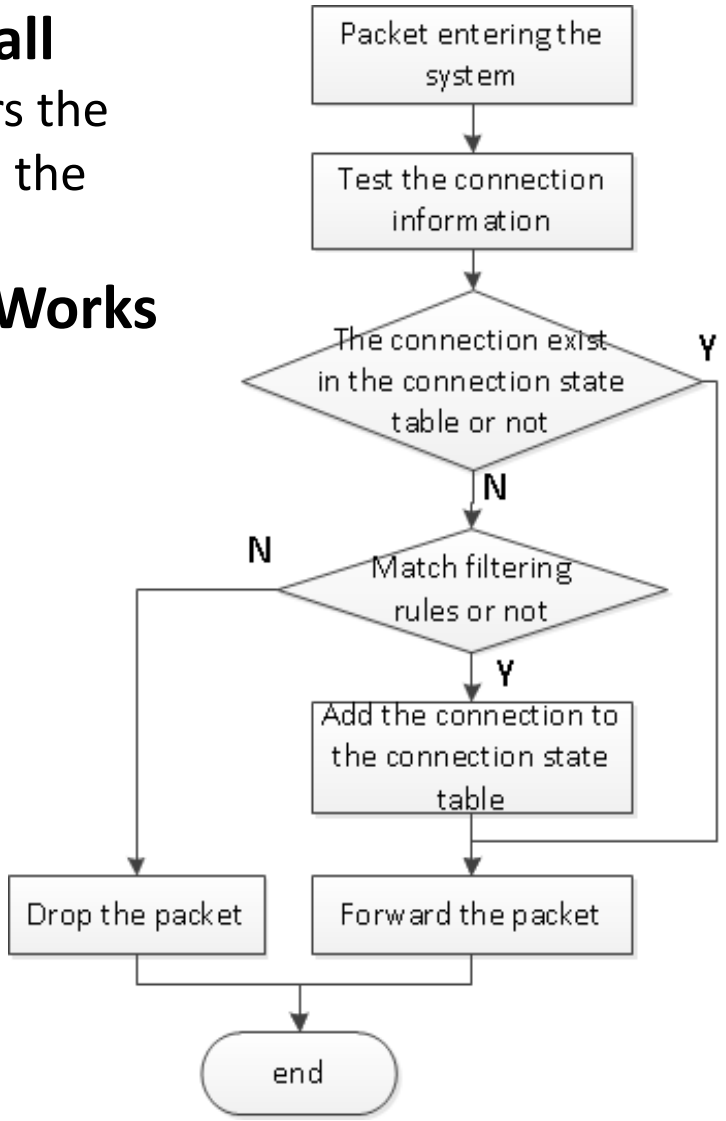
6.3 Stateful Inspection Firewall

6.3 Stateful Inspection Firewall

- What is Stateful Inspection Firewall
- How Stateful Inspection Firewall Works
- Advantages & Disadvantages
- Attacking Stateful Inspection Firewall

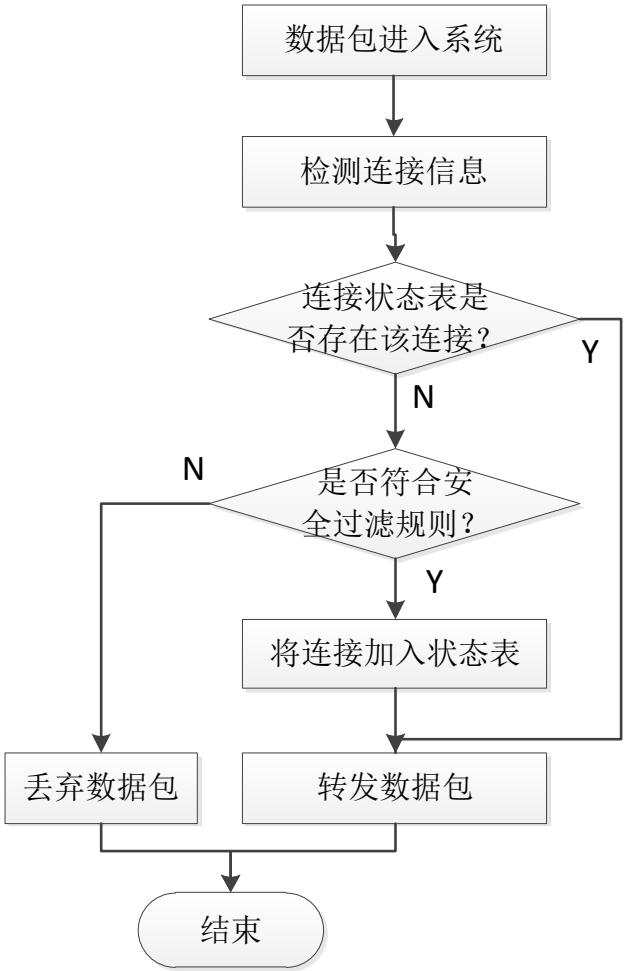
6.3 Stateful Inspection Firewall

- **What is Stateful Inspection Firewall**
  - A stateful inspection firewall monitors the state of the connection and compiles the information in a state table.
- **How Stateful Inspection Firewall Works**



6.3 Stateful Inspection Firewall

❑ How Stateful Inspection Firewall Works



6.3 Stateful Inspection Firewall

❑ How Stateful Inspection Firewall Works

- 当一个连接的初始数据报文到达执行状态检测的防火墙时，首先检查该报文是否符合安全过滤规则的规定。如果该报文与规定相符合，则将该连接的信息记录下来并自动添加一条允许该连接通过的过滤规则，然后向目的地转发该报文。以后凡是属于该连接的数据，防火墙一律予以放行，包括从内向外的和从外向内的双向数据流。在通信结束、释放该连接以后防火墙将自动删除关于该连接的过滤规则。动态过滤规则存储在连接状态表中并由防火墙维护。状态检查技术主要在网络层和传输层工作。
  - ✧ 为了防止无效的表项长期保存在状态表中，对状态表中的表项需要设置超时参数。

6.3 Stateful Inspection Firewall

❑ Advantages

- Safer than static packet filtering
  - ✧ 与包过滤技术相比，安全性得到改善，状态检测机制可以区分连接的发起方和接收方，可以通过状态分析阻断更多的复杂的攻击行为，也可以通过分析打开相应端口。
    - ◌ 而不是对端口处理“一刀切”
- Better performance than static packet filtering
  - ✧ 与包过滤技术相比，提升了防火墙的性能。状态检测机制只对连接的初始报文进行详细的检查，后续报文不作检查可以快速通过。

6.3 Stateful Inspection Firewall

❑ Disadvantages

- Security is not high enough due to fewer checks on packet data
  - ✧ 主要工作在网络层和传输层，对报文的数据部分检查很少，安全性能还不够高。
- More detections demand higher performance of the firewall
  - ✧ 对初始报文的检测内容相对增多，对防火墙的响应速度提出更高要求。

6.3 Stateful Inspection Firewall

❑ Attacking Stateful Inspection Firewall

- 状态检测防火墙工作于网络层，判断允许还是禁止数据流的依据也是源 IP 地址、目的 IP 地址、源端口、目的端口和通讯协议等。不同的是，状态检测防火墙是基于会话信息，而不是数据包的信息做出决策。状态检测防火墙在发起连接时就判断并登记了连接的状态信息 (包括 Source IP, Source Port, Destination IP, Destination Port 以及其它选项)，后续的属于同一个连接状态的数据包可以直接通过。一些攻击数据包由于不具备已经登记的相应状态信息而被拒绝。
- 动态规则技术
  - ✧ 状态检测过程中采用动态规则技术可以解决高端口开放问题。防火墙常规地过滤内部网络的所有端口 (1-65535)，外部攻击者难于发现入侵的切入点。为了不影响正常的服务，一旦检测到服务必须开放高端口时 (如 ftp 协议、irc - internet relay chat 等)，防火墙动态添加一条规则，打开相应的高端口。服务完成后，防火墙将这条规则删除，既保障安全，又不影响正常服务。

6.3 Stateful Inspection Firewall

❑ Attacking Stateful Inspection Firewall

- Protocol Tunneling
  - ✧ 协议隧道的攻击思想类似于 VPN 的实现原理，攻击者将一些恶意的攻击数据包隐藏在一些协议分组的头部，穿透防火墙对内部网络进行攻击。许多简单允许 ICMP 回射请求、ICMP 回射应答和 UDP 分组通过的防火墙容易受到 ICMP 和 UDP 协议隧道的攻击。
  - ✧ 由于许多防火墙允许 ICMP 和 UDP 分组自由出入，因此攻击者的恶意数据可以附带在正常的分组，绕过防火墙的认证，顺利地到达攻击目标主机。

6.3 Stateful Inspection Firewall

❑ Attacking Stateful Inspection Firewall

- Protocol Tunneling
  - ✧ 例：Loki 攻击。
    - ◌ Loki 作为一个验证工具发布于1996年的 Phrak，Loki 攻击使用 ICMP 协议进行通信。安装在内部主机上的 Loki 将数据放在 ICMP 头信息后面，使用 ICMP 回叫网络外的黑客。管理员看到的只是发出的新 ping 流量，而黑客事实上已经建立了隐秘通道。
    - ◌ 实际攻击中，攻击者首先设法在内部网络的一个系统上安装 lokid 服务端，攻击者通过 loki 客户端将希望远程执行的攻击命令嵌入 ICMP 或 UDP 包头部，再发送给内部网络服务端 lokid，由它执行其中的命令，并以同样的方式返回结果。

6.3 Stateful Inspection Firewall

❑ Attacking Stateful Inspection Firewall

- Trojan Rebound
  - ✧ 针对状态检测防火墙仍然可以使用木马进行穿透。反弹木马是对付这种防火墙的最有效的方法之一。攻击者在内部网络安装的反弹木马定时地连接外部攻击者控制的主机，由于连接是从内部发起的，防火墙不能区分木马的连接，而都认为是一个合法的连接，因此可以实现穿透。
  - ✧ 这种攻击的局限是：攻击者必须事先在内部网络安装这个木马程序。

6.4 Application Layer Gateway

6.4 Application Layer Gateway (ALG, or Proxy Server)

- What is Proxy
- Topological Graph of Proxy
- Functions Offered By Proxy
- Advantages & Disadvantage
- Attacking Proxy

6.4 Application Layer Gateway

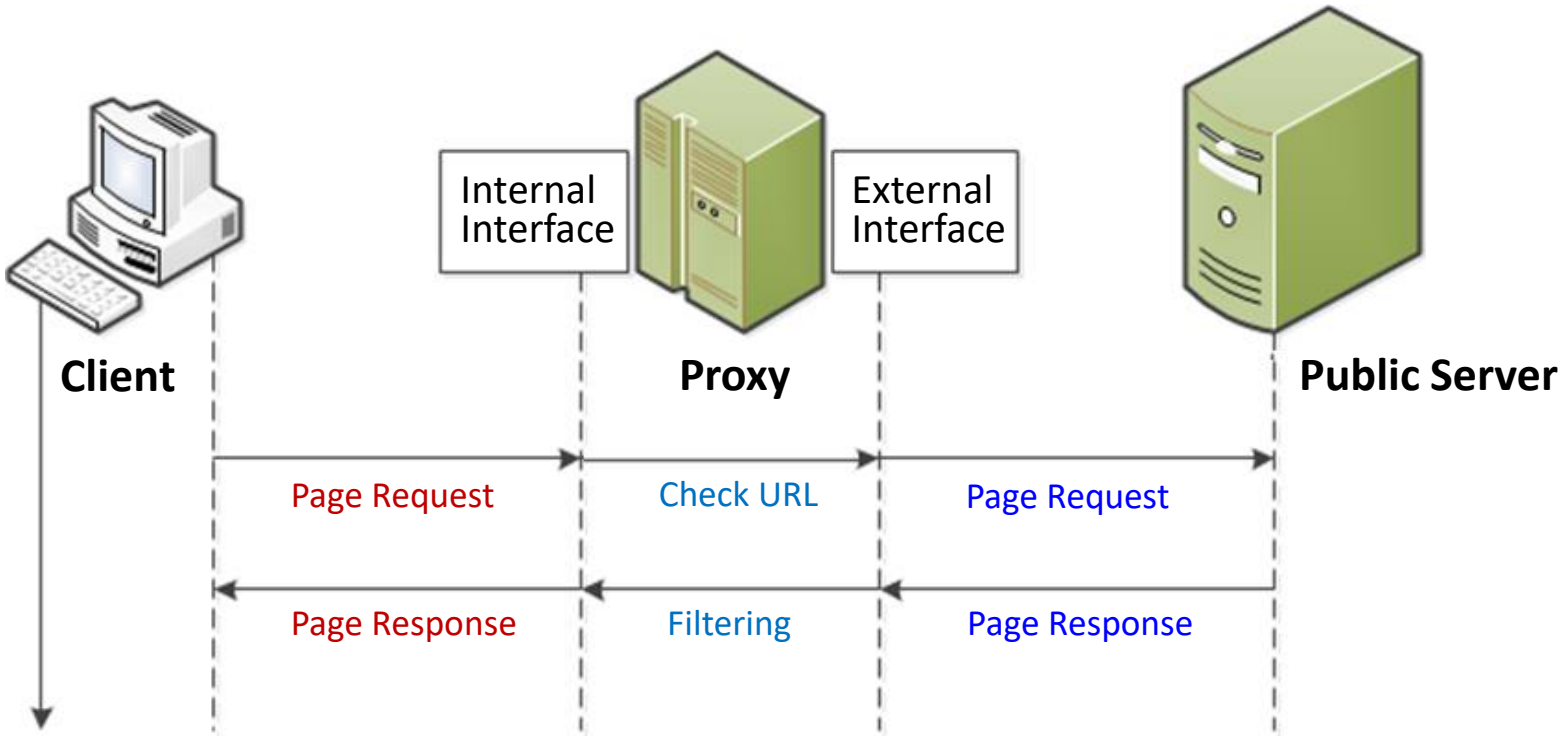
What is Proxy

- 应用层网关防火墙也叫应用层代理，它作为中介实现外部网络和内部网络之间的通讯。防火墙两端的用户的网络通讯由应用层代理负责转发。代理将截获所有的通讯数据，如果连接符合预定的访问控制规则，则由代理将通信内容转发给目标系统。目标系统的回应发送给代理，再由代理将回应数据转发给相应的客户机。网络连接通过中介实现，可以有效避免被保护的真实的网络设备受到恶意侵害。

6.4 Application Layer Gateway

❑ What is Proxy

- Topological Graph and Sequence Chart of Proxy



6.4 Application Layer Gateway

- **Functions Offered by Proxy**
  - Authentication mechanism
  - Content Filtering
  - Mature Log

6.4 Application Layer Gateway

❑ Functions Offered by Proxy

- ALG 工作在高层，能够理解应用层的协议，因而可以提供前面两种防火墙所无法提供的诸多特别的功能，能够进行一些复杂的访问控制，主要包括：
  - ✧ 认证机制。例如使用一些常见的用户和密码认证。
  - ✧ 内容过滤。例如 ALG 能够发现 Unicode 攻击，并对攻击进行阻断。
    - ◌ 此外，还能对常见的使用80端口的 Java Applet、JavaScript、ActiveX、电子邮件的 MIME (Multipurpose Internet Mail Extensions) 类型等应用的内容进行过滤。
  - ✧ 成熟的日志。突破了 OSI 四层的限制，日志记录详尽。比如：记录进入防火墙的数据包中有关应用层的命令，表现在上例中就是 Unicode 攻击的执行命令。

6.4 Application Layer Gateway

❑ Advantages

- Accelerate the network by its Cache
- Prevent any detection to internal network
- Filtering the content of the packet effectively
- Reduce direct attack to internal network
- No IP Address Spoofing Attack
- Mature Log

6.4 Application Layer Gateway

❑ Advantages

- 提供高速缓存
  - ✧ 由于大部分信息都可以重复使用，当对同一个信息有重复请求时，可以从缓存获取信息而不必再次进行网络连接，提高了网络性能。
- 屏蔽内联网络
  - ✧ 代理服务器禁止内联网络与外联网络的直接连接，阻止对内联网络的探测活动，减少了内部主机受到直接攻击的危险。
- 连接基于服务
  - ✧ 代理服务器不是基于物理连接的，代理防火墙不易受到 IP 地址欺骗的攻击。
- 规则简单
  - ✧ 代理防火墙的过滤规则比包过滤防火墙的过滤规则更简单。

6.4 Application Layer Gateway

- **Advantages**
  - 代理服务建立在应用层上
    - ✧ 代理服务可以提供各种身份认证手段，加强服务的安全性。
    - ✧ 代理服务可以有效地过滤内容。
    - ✧ 代理服务可以提供详细的日志记录，有助于进行细致的日志分析与审计。

6.4 Application Layer Gateway

❑ Disadvantages

- A special service must have a special proxy
- Too much access delay when proxy server is busy
- Opaque (not transparent) for the users
- Slower than Packet Filtering

6.4 Application Layer Gateway

❑ Disadvantages

- 代理服务程序很多都是专用的，不能很好地适应网络服务和协议的不断发展；
- 在访问数据流量较大时，代理技术会增加访问的延迟，影响系统的性能；
- 应用层网关需要用户改变自己的行为模式，不能够实现用户的透明访问；
- 应用层代理还不能完全支持所有的协议；
- 代理系统对操作系统有明显的依赖性，必须基于某个特定的系统及其协议；
- 相对于包过滤技术来说，代理技术执行的速度较慢。

6.4 Application Layer Gateway

❑ Example

- 华为 ALG 防火墙：H3C SecPath F1000-A-EI
- Ref: 05-NAT配置指导-ALG.pdf

6.4 Application Layer Gateway

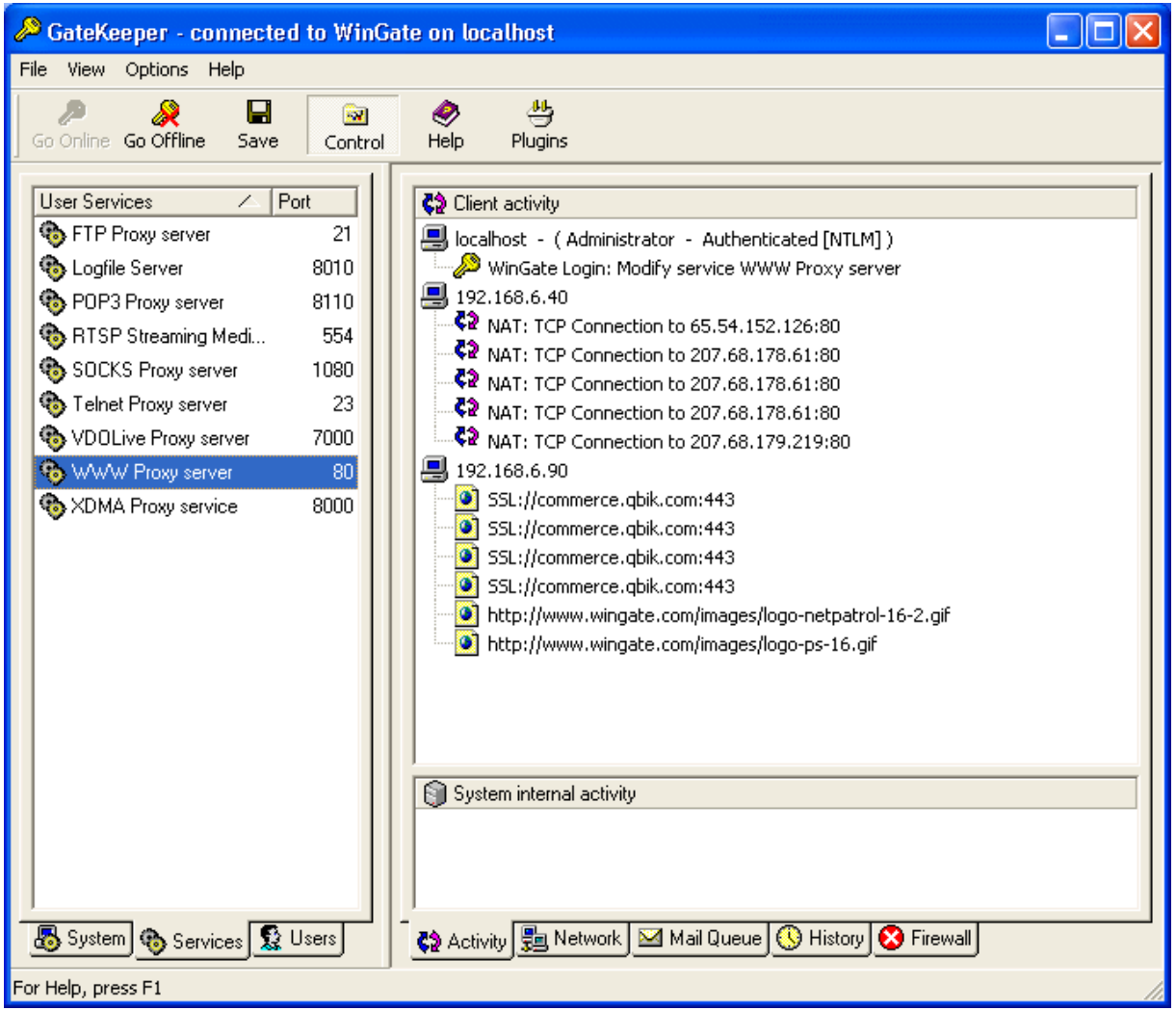
❑ Attacking Proxy

- 代理是运行在应用层的防火墙。对于每一个连接请求，代理需要启动两个连接，一个是客户到代理，另一个是代理到目的服务器。代理的实现基本上也是根据规则施行过滤。
- 例：WinGate
  - ✧ WinGate 是应用广泛的一种代理防火墙软件，内部用户可以通过一台安装有 WinGate 的主机访问外部网络。黑客经常利用其安全漏洞获得 WinGate 的非授权 Web、Socks 和 Telnet 的访问，从而伪装成 WinGate 主机身份对下一个攻击目标发动攻击。这种攻击通常难于被跟踪和记录。
  - ✧ http://www.wingate.com/

6.4 Application Layer Gateway

❑ Attacking Proxy

- 例：WinGate



6.4 Application Layer Gateway

❑ Attacking Proxy

- 例：WinGate - 非授权 Web 访问漏洞
  - ✧ 早期的 WinGate 版本在误配置情况下，允许外部主机完全匿名访问因特网。因此，外部攻击者可以利用 WinGate 主机对 Web 服务器发动各种 Web 攻击 (如 CGI 的漏洞攻击等)。同时由于 Web 攻击的所有报文都从 TCP 80端口穿过，很难追踪到攻击者的来源。
  - ✧ 检测 WinGate 主机是否有非授权 Web 访问安全漏洞的方法：
    - ① 以一个不会被过滤掉的连接 (譬如拨号连接) 连接到因特网上；
    - ② 把浏览器的代理服务器地址指向待测试的 WinGate 主机。
    - ◌ 如果浏览器能够访问因特网，则 WinGate 主机存在着非授权 Web 访问漏洞。

6.4 Application Layer Gateway

❑ Attacking Proxy

- 例：WinGate - 非授权 Socks 访问漏洞
  - ✧ 在 WinGate 的缺省配置中，Socks 代理 (1080端口) 同样存在安全漏洞。与打开的 Web 代理 (80端口) 一样，外部攻击者可以利用 Socks 代理访问因特网。
  - ✧ 要防止攻击 WinGate 的这个安全脆弱点，管理员可以限制特定服务的捆绑。例如在多宿主 (multi homed) 系统上，执行以下步骤以限定如何提供代理服务。
    - ① 选择 Socks 或 WWW Proxy Server 属性；
    - ② 选择 Bindings 标签；
    - ③ 按下 Connections Will Be Accepted On The Following Interface Only 按钮，并指定本 WinGate 服务器的内部接口。

6.4 Application Layer Gateway

❑ Attacking Proxy

- 例：WinGate - 非授权 Telnet 访问漏洞
  - ✧ 非授权 Telnet 访问是 WinGate 最具威胁的安全漏洞。通过连接到一个误配置的 WinGate 服务器的 Telnet 服务，攻击者可以使用别人的主机隐藏自己的踪迹，随意地发动攻击。
  - ✧ 检测 WinGate 主机是否有非授权 Telnet 访问安全漏洞的方法：

① 使用 telnet 尝试连接到一台 WinGate 服务器

```
[root@happy/tmp]#telnet 172.29.11.191
Trying 172.29.11.191....
Connected to 172.29.11.191.
Escape character is '^]'.
Wingate>10.50.21.5
```

② 如果得到如上的响应文本，则输入待连接的 IP；如果看到了该新系统的登录提示符，则该服务器是脆弱的

```
Connected to host 10.50.21.5...Connected
Sun OS 5.6
Login:
```

6.4 Application Layer Gateway

❑ Attacking Proxy

- 例：WinGate - 非授权 Telnet 访问漏洞
  - ✧ 防止这种安全脆弱点的方法和防止非授权 Socks 访问的方法类似，在 WinGate 中限制特定服务的捆绑可以解决这个问题。在多宿主 (multi homed) 上的系统管理员可以通过执行以下步骤来完成：

    ① 选择 Telnet Sever 属性；

    ② 选择 Bindings 标签；

    ③ 按下 Connections Will Be Accepted On The Following Interface Only 按钮，并指定本 WinGate 服务器的内部接口。

6.5 Bastion Host

6.5 Bastion Host

- Topological Graph of Bastion Host
- Design Principles of Bastion Host
- Type of Bastion Host
- Deployment of Bastion Host

6.5 Bastion Host

❑ Bastion Host

- 堡垒主机是一种被强化的专门用于网络防御的计算机。它被用作进入内部网络的一个检查点，在上面集中解决整个网络的安全问题，而简化对其它主机的安全考虑。
  - ✧ 堡垒主机是网络中最容易受到侵害的主机，对其自我保护能力需要仔细设计和配置，将它遭到外网攻击成功的风险性减至最低。
- 传统应用的堡垒主机
  - ✧ 堡垒主机作为安全但可公开访问的计算机 (例如用作 Web 服 务器、DNS 服务器或 FTP 服务器等)，通常部署于外围网络 (也称为 DMZ、网络隔离区域或屏蔽子网) 面向公众的一侧。这类堡垒主机不受防火墙的保护，完全暴露在外网攻击威胁中。
  - ✧ 将必须开放的服务部署在堡垒主机而不是内部网络，可以换取内部网络的安全。

6.5 Bastion Host

❑ Bastion Host

- 安全堡垒主机
  - ✧ 安全堡垒主机设法吸引入侵者的注意力，耗费其攻击内部网络主机的时间并且使追踪入侵企图变得更加容易。一些场景下安全堡垒主机被当作做牺牲品 (sacrificial host / victim machine) 来换取内部网络的安全。
  - ✧ 安全堡垒主机的配置与常规主机有明显的差别，它只提供极少的必要的服务，其它不必要的服务、协议、程序和网络接口都被禁用或删除。每台堡垒主机通常被配置为只承担一个特定角色以减少其自身的安全漏洞。另外一些可以提高堡垒主机自身安全性的手段包括：采用安全操作系统、采取必要的身份认证和严格的权限控制技术等。

6.5 Bastion Host

❑ Entrance Control Host

- 进入控制堡垒主机 (Entrance Control Host) 被部署在外部网络和企业内部网络之间，提供对内部网络特定资源的安全访问控制。这类堡垒主机本身不提供网络层的路由功能，因此可以过滤对内部网络的非授权访问。
  - ✧ 访问内部网络特定资源的前提是必须先登录到进入控制堡垒主机上。
  - ✧ 进入控制堡垒主机是进入内部网络的一个集中检查点和控制点，因此很容易将整个网络的安全问题集中在自身解决，为内部网络其他主机的安全提供一道安全屏障。
  - ✧ SSL VPN 可以视为进入控制堡垒主机的一个成功应用。

6.5 Bastion Host

❑ Internal Control Host

- 内控堡垒主机 (Internal Control Host) 融合了系统运维管理和安全性，采用协议代理的方式接管终端计算机对网络和服务器的访问。
- 内控堡垒主机扮演着看门者的工作，所有对网络设备和服务器的请求都要通过内控堡垒主机实现。因此内控堡垒机能够拦截非法访问和恶意攻击、对不合法命令进行命令阻断，以及过滤所有对目标设备的非法访问行为。
- 内控堡垒主机的主要功能
  - ✧ 单点登录功能
  - ✧ 帐号管理功能
  - ✧ 身份认证功能
  - ✧ 资源授权功能
  - ✧ 访问控制功能
  - ✧ 操作审计功能

6.5 Bastion Host

❑ Internal Control Host

- 单点登录功能
  - ✧ 内控堡垒主机提供了基于 B/S 的单点登录系统，用户一次成功登录系统后，可以无需认证访问包括被授权的多种基于 B/S 和 C/S 的应用系统。
  - ✧ 单点登录为具有多帐号的用户提供了方便快捷的访问途经，用户无需记忆多种登录的用户 ID 和口令。通过向用户和客户提供对其个性化资源的快捷访问提高系统的生产效率。同时，系统自身的强认证能力提高了用户认证环节的安全性。
  - ✧ 单点登录可以实现与用户授权管理的无缝连接，通过对用户、角色、行为和资源的授权，增加对资源的保护和对用户行为的监控以及审计。

6.5 Bastion Host

❑ Internal Control Host

- 帐号管理功能
  - ✧ 帐号集中管理包含对所有服务器和网络设备帐号的集中管理。帐号和资源的集中管理是集中授权、认证和审计的基础。
  - ✧ 帐号集中管理可以完成对帐号整个生命周期的监 控和管理，降低企业管理大量用户帐号的难度和工作量。帐号的统一管理还能够发现帐号中存在的安全隐患，制定统一、标准的用户帐号安全策略。
  - ✧ 通过帐号集中管理，可以将帐号与具体的自然人相关联，实现多级的用户管理和细粒度的用户授权，还可以实现针对自然人的行为审计，以满足审计的需要。

6.5 Bastion Host

❑ Internal Control Host

- 身份认证功能
  - ✧ 内控堡垒主机为用户提供统一的认证接口。
  - ✧ 采用统一的认证接口不但便于对用户认证的管理，而且能够采用更加安全的认证模式，提高认证的安全性和可靠性。
  - ✧ 统一身份认证机制提供静态密码、Windows NT 域、Windows Kerberos、双因素、一次性口令和生物特征等多种认证方式。系统具有灵活的定制接口，可以方便的与其它第三方认证服务器进行结合。

6.5 Bastion Host

❑ Internal Control Host

- 资源授权功能
  - ✧ 内控堡垒主机系统提供统一的界面，将用户、用户角色、用户行为以及资源作为授权对象进行授权，以达到对权限的细粒度控制，最大限度保护用户资源的安全。
  - ✧ 通过集中访问授权和访问控制，系统可以对用户通过 B/S、C/S 对服务器主机、网络设备的访问进行审计和阻断。系统不但能够实现对用户访问资源的角色控制这类基于应用边界的粗粒度授权，对某些应用还可以限制用户的操作，以及实现对用户进行操作时间控制这类应用内部的细粒度授权。

6.5 Bastion Host

❑ Internal Control Host

- 访问控制功能
  - ✧ 内控堡垒主机系统能够提供细粒度的访问控制，最大限度保护用户资源的安全。
  - ✧ 细粒度的命令策略是命令的集合，可以是一组可执行命令，也可以是一组非可执行的命令，该命令集合用来分配给具体的用户，限制其系统行为，管理员会根据其自身的角色为其指定相应的控制策略来限定用户。
  - ✧ 访问控制策略是保护系统安全性的重要环节，制定良好的访问策略能够更好的提高系统的安全性。

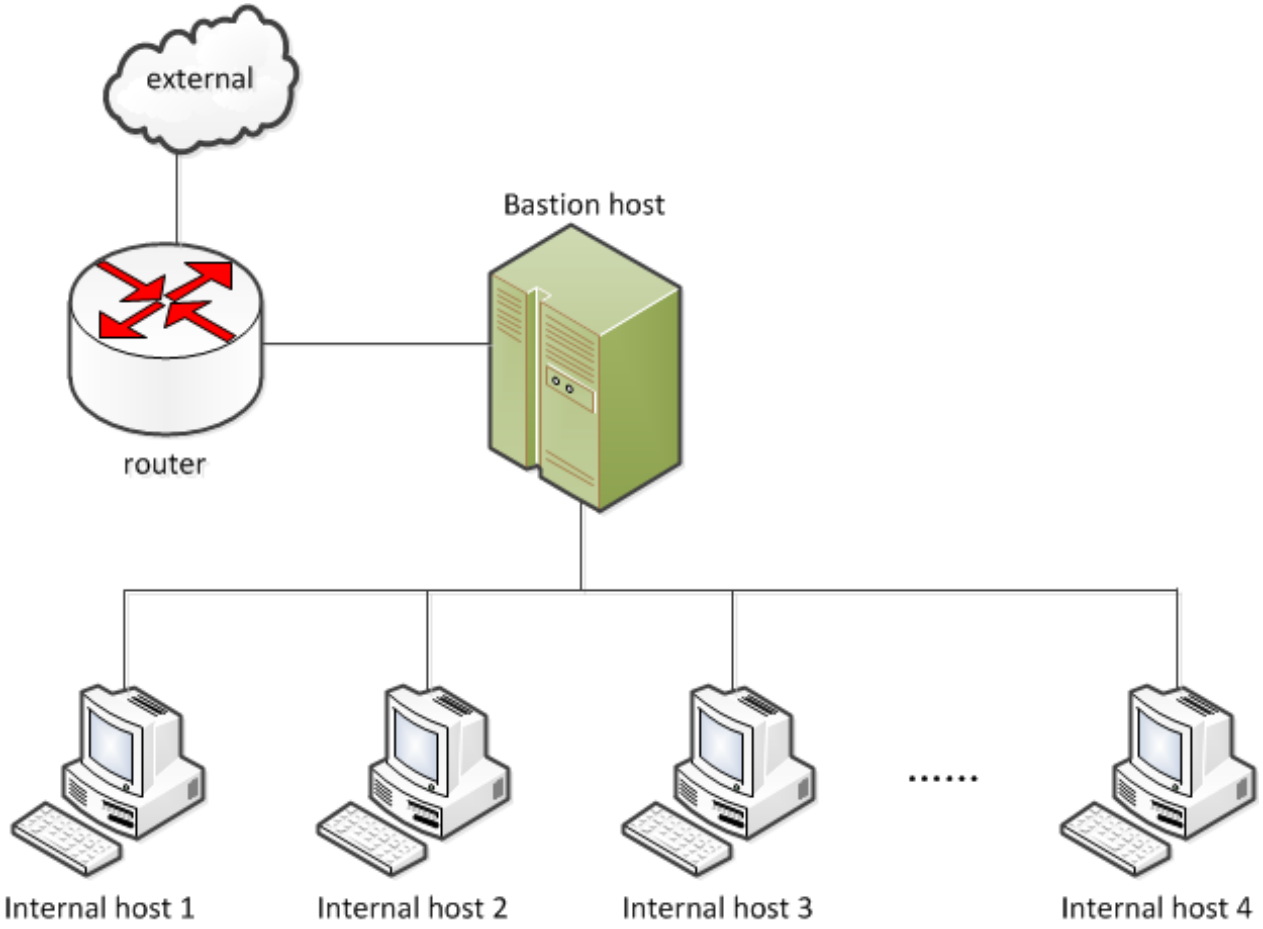
6.5 Bastion Host

❑ Internal Control Host

- 操作审计功能
  - ✧ 操作审计管理主要审计人员的帐号使用情况 (登录、资源访问) 、资源使用情况等。
  - ✧ 各个服务器主机、网络设备的访问日志记录采用统一的帐号、资源进行标识，操作审计能更好地对帐号的完整使用过程进行追踪。内控堡垒主机系统通过系统自身的用户认证系统、用户授权系统，以及访问控制机制等详细记录整个会话过程中用户的全部行为日志，还可以将产生的日志记录转交给第三方产品进行分析。
- 在这些主干功能构筑的安全体系下，内控堡垒机可以较好地实现系统用户管理、内网操作审计、网络设备管理和黑客行为防范四大功能。

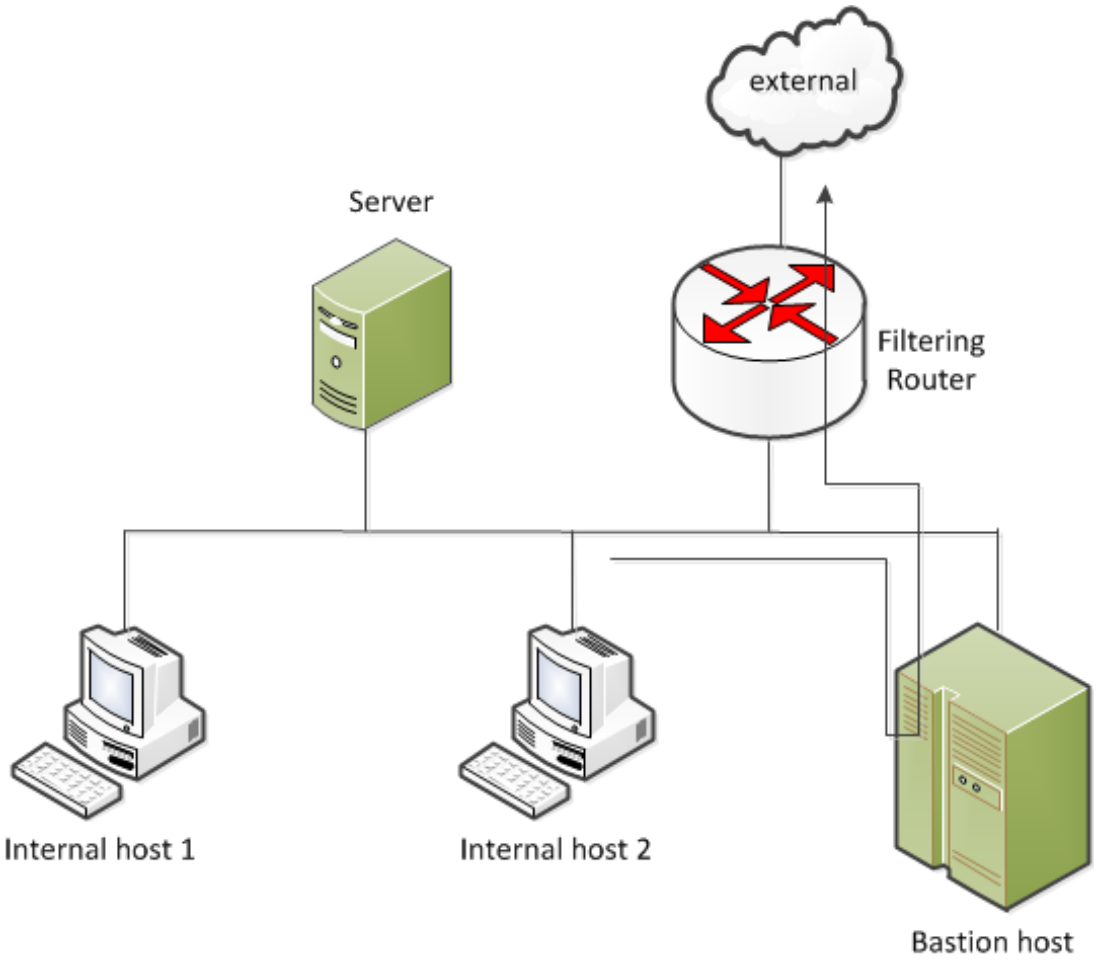
6.5 Bastion Host

❑ Deployment of Bastion Host



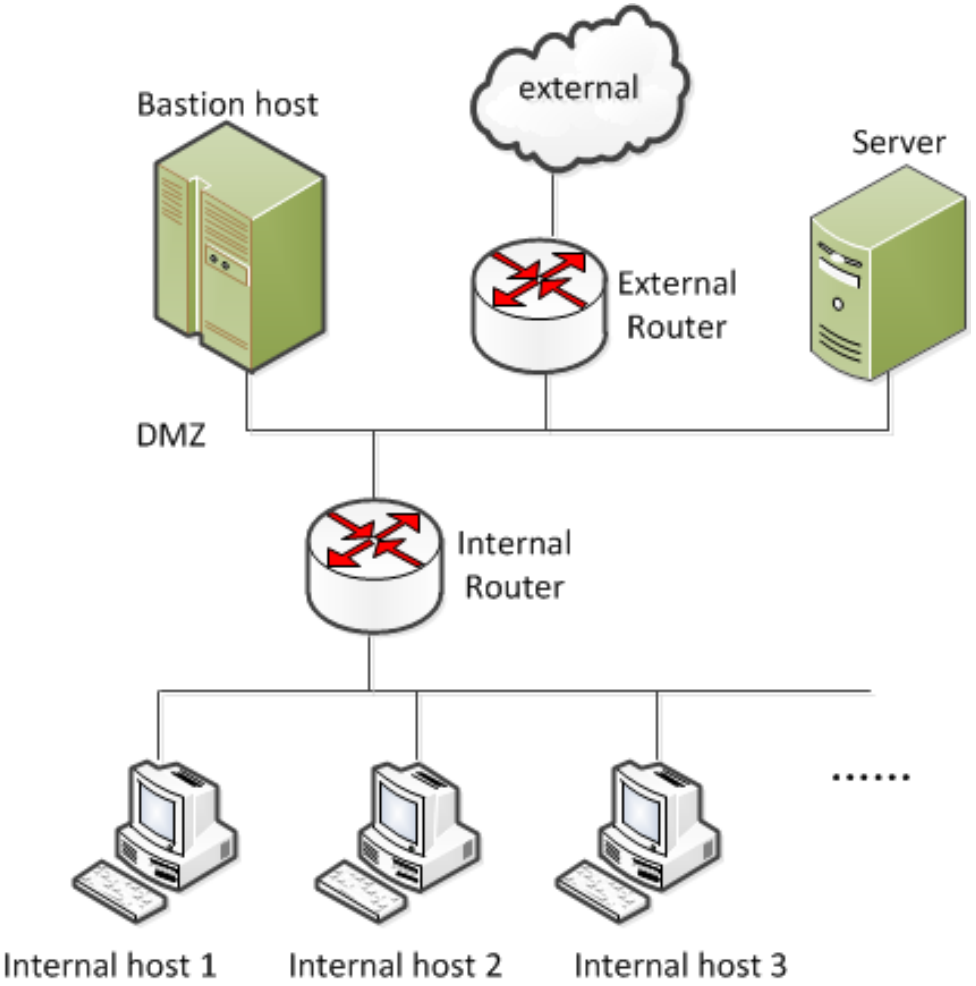
6.5 Bastion Host

❑ Deployment of Bastion Host



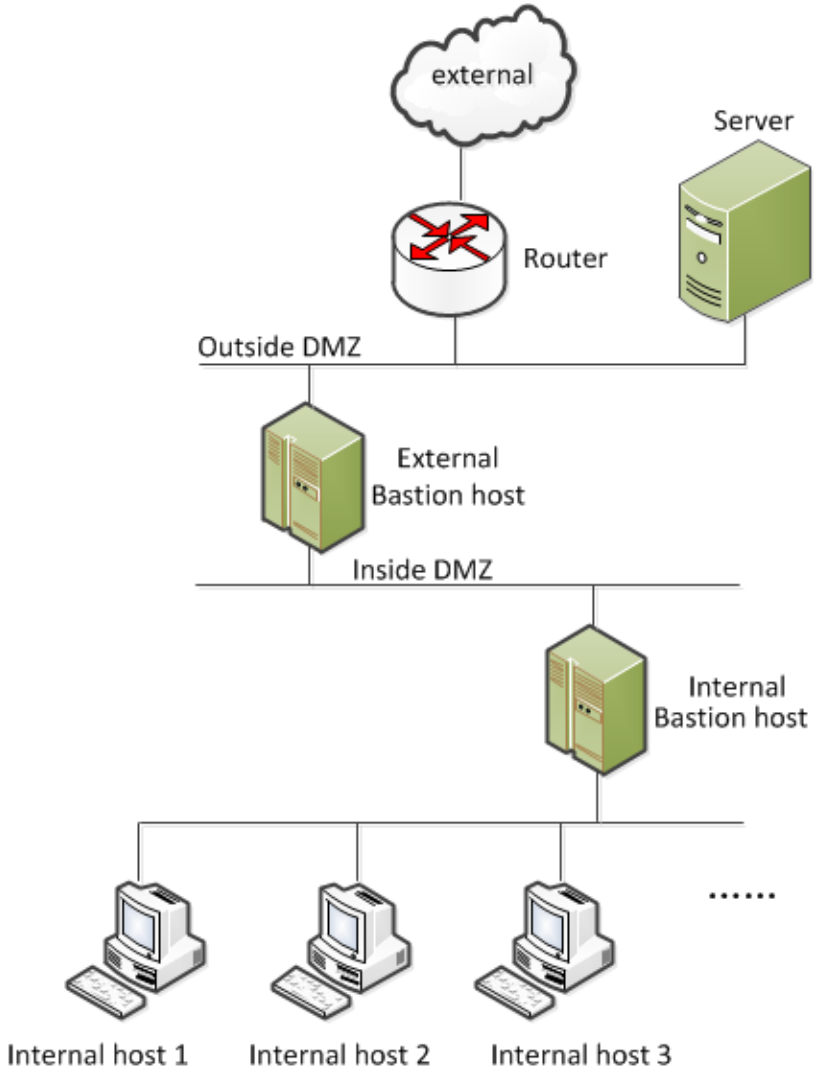
6.5 Bastion Host

❑ Deployment of Bastion Host



6.5 Bastion Host

❑ Deployment of Bastion Host



6.5 Bastion Host

❑ Deployment of Bastion Host

- 堡垒主机的物理部署
  - ✧ 物理位置安全
    - ○ 如果可以物理接触堡垒主机，入侵者就可能有很多我们无法控制的办法来攻破堡垒主机。
    - ○ 堡垒主机提供了许多内部网与外部公网的功能性连接，如果它被破坏或被盗用，那么整个网内的站点与外部网就会脱离或完全中断。
    - ○ 其他的机房安全规则。
  - ✧ 网络位置安全
    - ○ 堡垒主机应当部署在没有重要的或机密信息流的网络上，最好部署在一个单独的网络上，以尽量降低堡垒主机被意外侵入情况下的信息泄露风险。

6.6 Security on Linux - Iptables

6.6 Iptables

- What is Iptables
- Architecture of Iptables
- Command Format
- Examples
- Practice

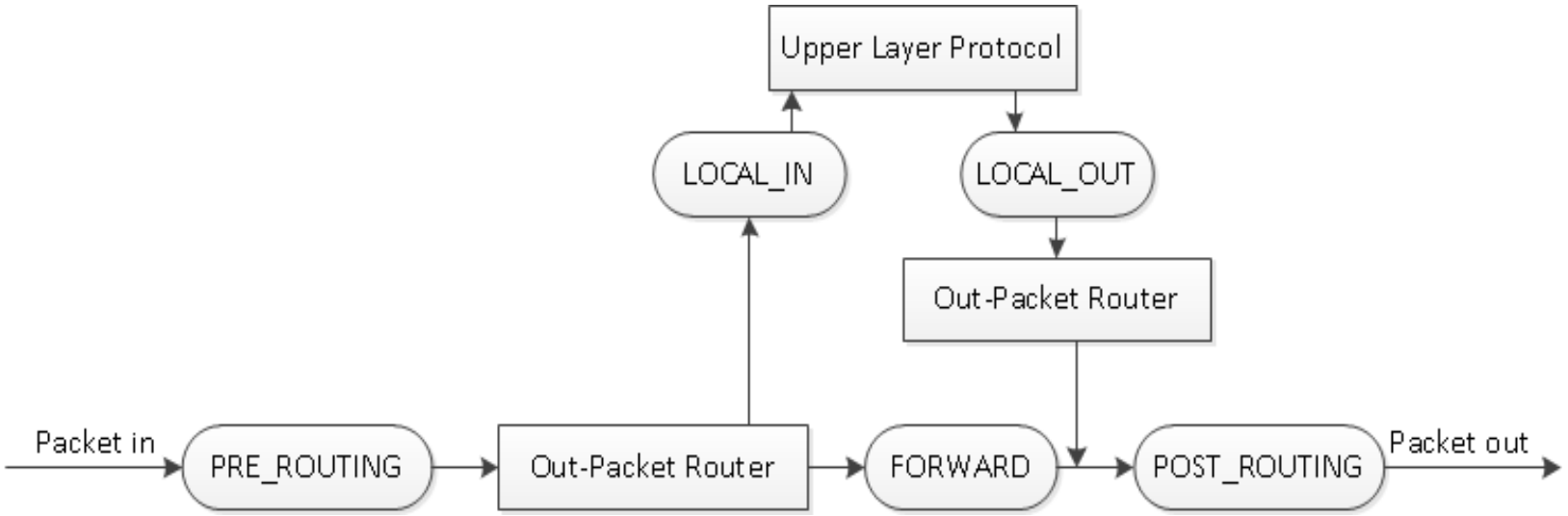
6.6 Security on Linux - Iptables

❑ What is Iptables

- Iptables is a generic table structure that defines rules and commands as part of the netfilter framework that facilitates *Network Address Translation* (NAT), *packet filtering*, and *packet mangling* (分组重整) in the Linux 2.4 and later version of Linux.

6.6 Security on Linux - Iptables

❑ Architecture of Iptables



6.6 Security on Linux - Iptables

❑ Command Format

iptables [-t table_name] <command> [Chain_name] [Rule_No.] [Rule] [-j Target_Action]

6.6 Security on Linux - Iptables

❑ Command Format

- Commands

-A <Chain_name> <Rule>	Add Rule
-D <Chain_name> <Rule>	Delete Rule
-D <Chain_name> <Rule No.>	
-R <Chain_name> <Rule No.> <Rule>	Replace Rule
-I <Chain_name> [Rule No.] <Rule>	Insert Rule
-L [Chain_name]	List Rule
-F [Chain_name]	Delete All Rule in Chain
-N <Chain_name>	New Chain
-X [Chain_name]	Delete Chain
-P <Chain_name> <Target>	Default Rule
-E <Old Chain_name> <New Chain_name>	Rename Chain

6.6 Security on Linux - Iptables

❑ Command Format

- Rules

-p <Protocol Type>	Specify Upper Protocol
-s <IP Address/Mask>	Specify Source IP ADD
-d <IP Address/Mask>	Specify Destination IP ADD
-i <Port>	Specify Input Network Interface
-o <Port>	Specify Output Network Interface

6.6 Security on Linux - Iptables

❑ Command Format

- Target_Actions

  -j ACCEPT
  -j REJECT
  -j DROP
  -j REDIRECT
  -j LOG
  -j <Chain_name>

6.6 Security on Linux - Iptables

❑ Examples

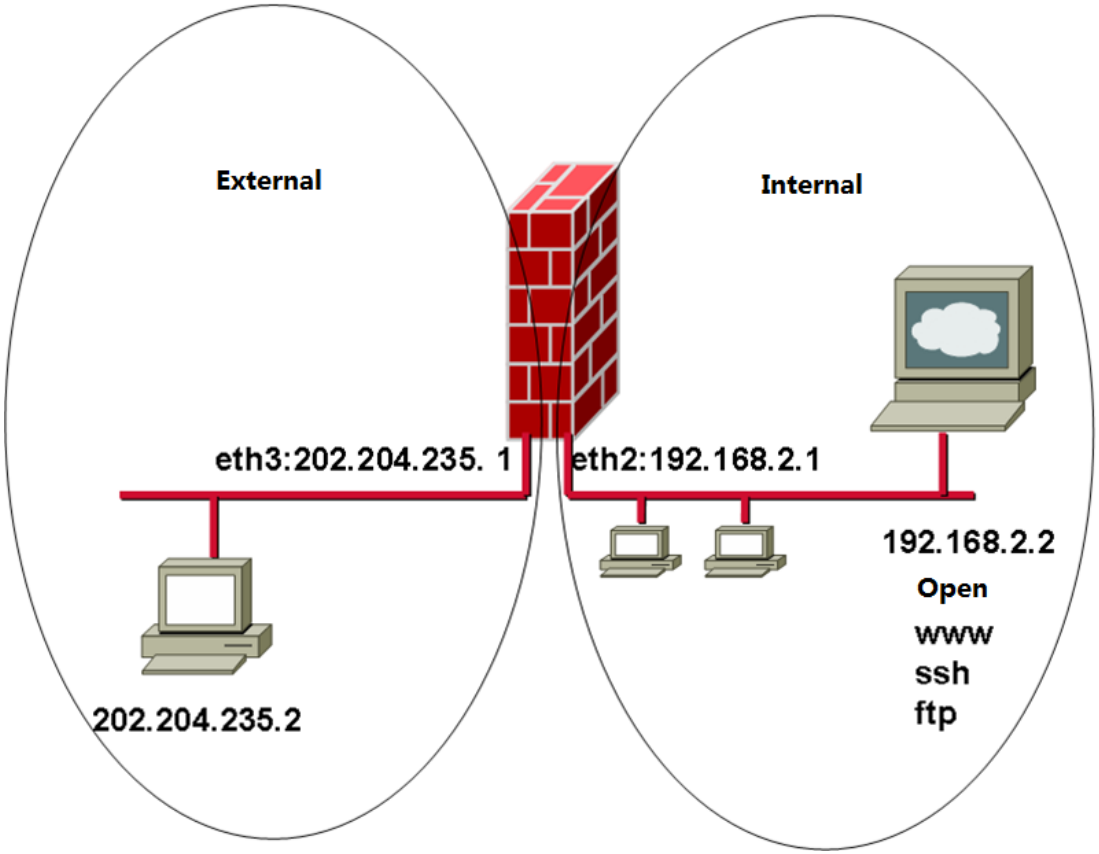
- Host Firewall

```
iptables -N MYCHAIN
iptables -A MYCHAIN -p tcp --dport 80 -j ACCEPT
iptables -A MYCHAIN -j RETURN
iptables -P INPUT DROP
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -j MYCHAIN
iptables -A INPUT -p tcp --dport 22 -j LOG --log-prefix "<--my GO ON--
>"
iptables -A OUTPUT DROP
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
iptables -L
```

6.6 Security on Linux - Iptables

❑ Examples

- Gateway Firewall



6.6 Security on Linux - Iptables

❑ Examples

- Gateway Firewall

```
iptables -F
iptables -F -t nat
iptables -F -t mangle
iptables -P FORWARD DROP
iptables -A FORWARD -i eth3 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth2 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -i eth3 -p tcp --dport 21 -j ACCEPT
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A FORWARD -p tcp --dport 22 -j ACCEPT
```

6.6 Security on Linux - Iptables

❑ Examples

- NAT (SNAT)

```
iptables -F
iptables -t nat -F
iptables -P  FORWARD ACCEPT
iptables -A  FORWARD -i eth3 -d 192.168.2.0/24 -p tcp --syn -j DROP
iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth3 -j SNAT --to-
source 202.204.235.100
```

6.6 Security on Linux - Iptables

❑ Examples

- NAT (DNAT)

```
iptables -F
iptables -t nat -F
iptables -t nat -A PREROUTING -i eth3 -d 192.168.2.0/24 -p tcp --syn -j
DROP
iptables -t nat -A PREROUTING -i eth3 -p tcp --dport 80  -j DNAT --to
192.168.2.2:80
iptables -t nat -A PREROUTING -i eth3 -p tcp --dport 21  -j DNAT --to
192.168.2.2:21
iptables -t nat -A PREROUTING -i eth3 -p tcp --dport 22  -j DNAT --to
192.168.2.2:22
iptables -P FORWARD DROP
```

6.6 Security on Linux - Iptables

- **Practice**
  1. Understand IPTABLES.
  2. Try to install and configure IPTABLES on your Linux.

6.7 Conclusion

❑ Conclusion

- 黑客对防火墙攻击的技术和手法越来越多样化和智能化。就黑客攻击防火墙的过程，可以将攻击分为三类：

(1) 对防火墙的探测攻击。探测在目标网络上安装的防火墙系统类型，发现防火墙系统允许的服务。

(2) 采取地址欺骗、TCP 序号攻击等手法绕过防火墙的认证机制，从而对防火墙和内部网络进行破坏。

(3) 寻找、利用防火墙系统实现和设计上的安全漏洞，有针对性地发动攻击。这种攻击难度比较大，但破坏性很强。

6.7 Conclusion

❑ Conclusion

- 防火墙的局限性：
  - (1) 不能防范不经过防火墙的攻击
  - (2) 不能解决来自内部网络的攻击和安全问题
  - (3) 不能防止策略配置不当或错误配置引起的安全威胁
  - (4) 不能防止可接触的人为或自然的破坏
  - (5) 不能防止利用标准网络协议中的缺陷进行的攻击
  - (6) 不能防止利用服务器系统漏洞所进行的攻击 (比如黑客通过防火墙准许的访问端口对该服务器的漏洞进行攻击)
  - (7) 不能防止受病毒感染的文件的传输 (不具备查杀病毒的功能)
  - (8) 不能防止数据驱动式的攻击 (当有些表面看来无害的数据邮寄或拷贝到内部网的主机上并被执行时，可能会发生数据驱动式的攻击)
  - (9) 不能防止内部的泄密行为
  - (10) 不能防止本身的安全漏洞的威胁

6.7 Conclusion

❑ Conclusion

- 防火墙的脆弱性：
  - (1) 防火墙的操作系统可能存在漏洞
  - (2) 防火墙的硬件可能失效
  - (3) 防火墙软件可能存在漏洞
  - (4) 无法解决 TCP/IP 等协议的漏洞
    - 防火墙本身基于 TCP/IP 等协议实现，无法解决协议漏洞。
  - (5) 无法区分恶意命令和善意命令
  - (6) 无法区分恶意流量和善意流量
  - (7) 安全性与多功能相互制约 (多功能与安全原则背道而驰)
  - (8) 安全性与速度相互制约
  - (9) 多功能与速度相互制约
  - (10) 无法保证准许服务的安全性
    - 防火墙准许某项服务，却不能保证该服务的安全性。
    - 准许服务的安全性问题必须由应用安全来解决。

6.7 Conclusion

❑ Conclusion

- 硬件防火墙和软件防火墙
  - ✧ 硬件防火墙
    - ○ 硬件防火墙通过硬件和软件的组合来达到隔离内外部网络的目的，采用专用的硬件设备，集成生产厂商的专用防火墙软件。硬件防火墙本身是单一任务设计，内置操作系统针对网络防护进行充分优化，与纯软件防火墙相比具备较高的抗攻击能力
    - ○ 从功能上看，硬件防火墙内建安全软件，使用专属或强化的操作系统，管理方便，更换容易，软硬件搭配较固定
    - ○ 硬件防火墙具有较高执行效率，解决了防火墙效率、性能之间的矛盾，可以达到线性
    - ○ 厂牌：华为、Juniper、Cisco、Fortinet、Sonicwall 等。

6.7 Conclusion

❑ Conclusion

- 硬件防火墙和软件防火墙
  - ✧ 软件防火墙
    - ◌ 软件防火墙通过纯软件的的方式实现隔离内外部网络的目的，其优点是定制灵活，升级快捷。但是软件防火墙在遇到密集 DoS 攻击的时候，所能承受的攻击强度远远低于硬件防火墙。软件防火墙比较适合于攻击频度不是很高的网络环境。
    - ◌ 软件防火墙一般基于某个操作系统平台开发，直接在计算机上进行软件的安装和配置。由于客户平台的多样性，软件防火墙需要支持多操作系统 (如Unix、Linux、SCO-Unix、Windows 等)，代码量大、安装成本高、售后支持成本高、运行效率较低。
    - ◌ Linux 和 Windows 的软件防火墙

6.7 Conclusion

❑ Conclusion

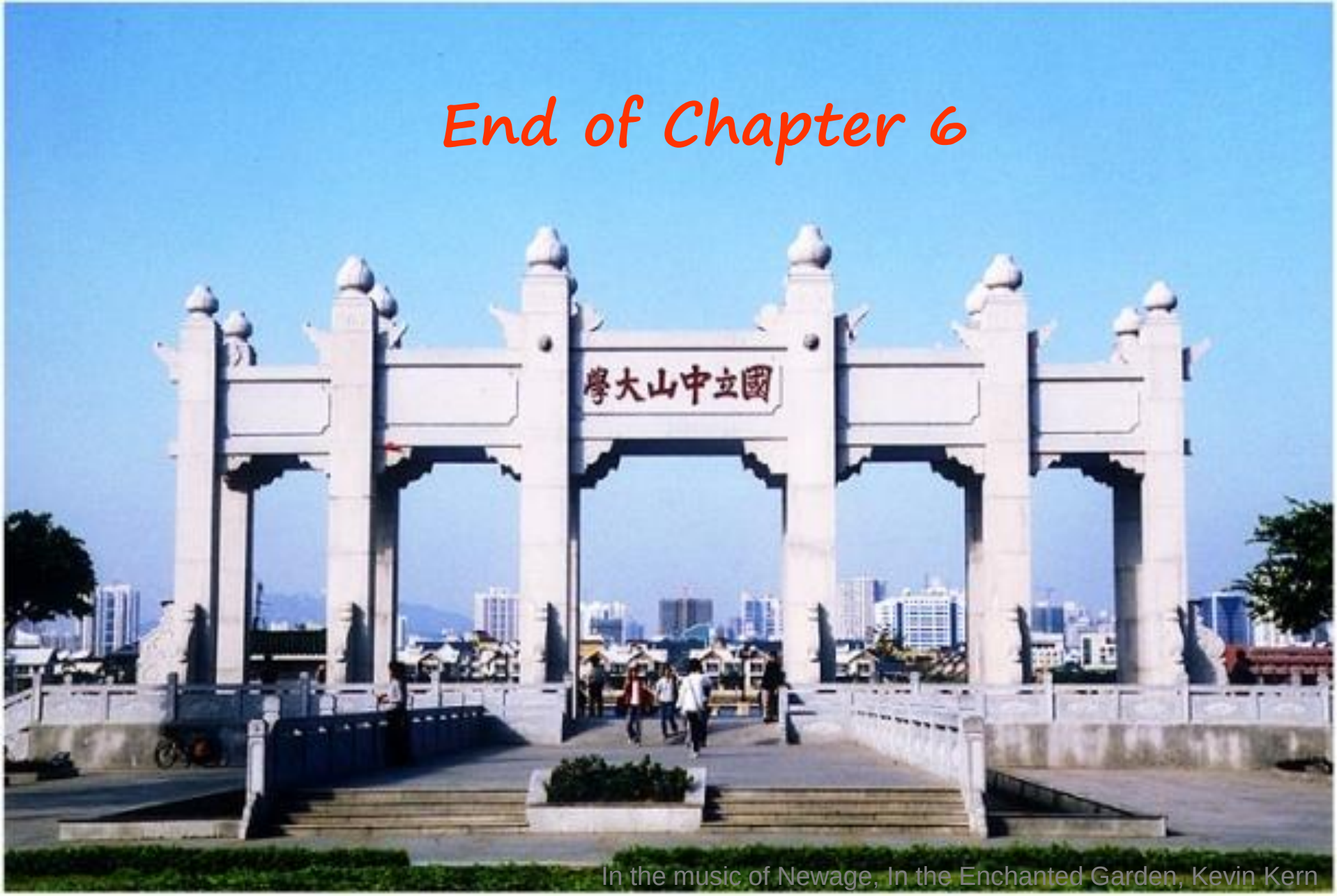
- Hardware Firewall vs Software Firewall
  - ✧ Hardware firewalls are specifically built within hardware devices like routers whereas software firewalls are software programs installed on computers.
  - ✧ Hardware firewalls protect a whole network while software firewalls protect individual computers on which they are installed.
  - ✧ By default, hardware firewalls filter web packets while software firewalls may not filter web packets unless web traffic filtering controls are enabled.
  - ✧ A hardware firewall can be configured to use a proxy service for filtering packets while a software firewall does not use a proxy service to filter.

6.7 Conclusion

❑ Conclusion

- 硬件防火墙对软件防火墙的比较优势
  - ✧ 性能优势
    - ◌ 性能对防火墙至关重要，它决定了每秒钟通过防火墙的数据流量 (Bps)。硬件防火墙流量从几十M到几百M不等，还有达到千兆甚至达到G级，这是软件防火墙难以达到的。
  - ✧ 主机 CPU 占用率的优势
    - ◌ 硬件防火墙不占用主机 CPU 资源。软件防火墙则不同，如果出于节约成本的考虑将防火墙软件安装在提供服务的主机上，当数据流量较大时，对主机 CPU 的高占用率有可能对主机的计算能力造成很大影响。
  - ✧ 售后支持
    - ◌ 硬件防火墙厂家对其防火墙产品通常能够提供方便的跟踪服务，而软件防火墙的用户能得到这种机会的相对较少。

End of Chapter 6



In the music of Newage, In the Enchanted Garden, Kevin Kern