中山大學 SUN YAT-SEN UNIVERSITY Google

Module II. Internet Security

Chapter 6
Firewall

Web Security: Theory & Applications

School of Software, Sun Yat-sen University

Outline

6.1 Introduction to Firewall

- What Is a Firewall
- Types of Firewall
- What Can a Firewall Do

6.2 Design Principles of Firewall

- Packet Filtering Firewall
- Packet Filtering Firewall Based on the state
- Application Proxy Firewall
- Bastion Host

Outline

6.3 Penetration of firewall

- Attack Packet Filtering Firewall
- Attack Stateful Inspection Firewall
- Attack Proxy

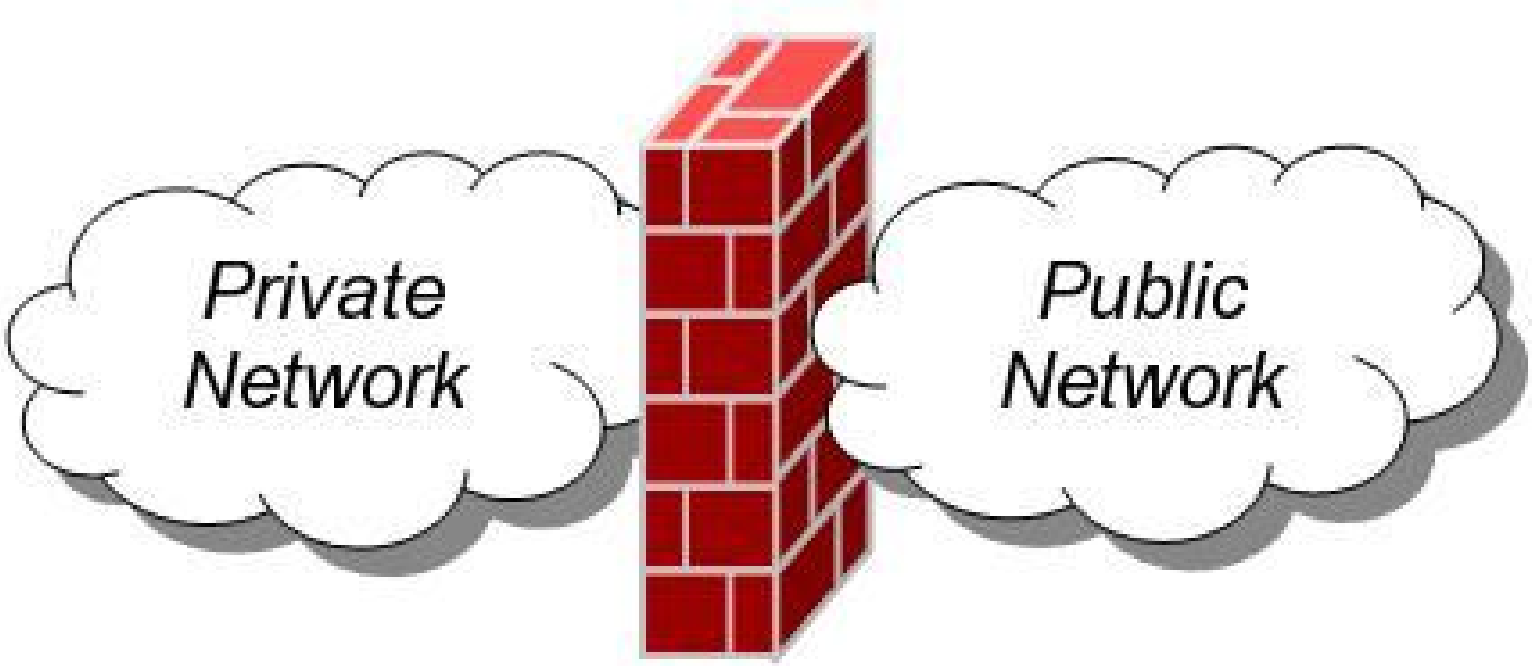
6.4 Firewall installation and Configuration

- Iptables

Outline

6.1 Introduction to Firewall

6.1.1 What Is a Firewall



6.1 Introduction to Firewall

6.1.2 Types of Firewall

- 1st gen: Packet Filters
- 2nd gen: Stateful Filters
- 3rd gen: Application Layer

6.1 Introduction to Firewall

- **Packet Filters**
  - ***IP Packet Filter Firewall*** is a firewall deciding 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.

6.1 Introduction to Firewall

- Packet filtering firewalls work mainly on the first three layers 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 to Firewall

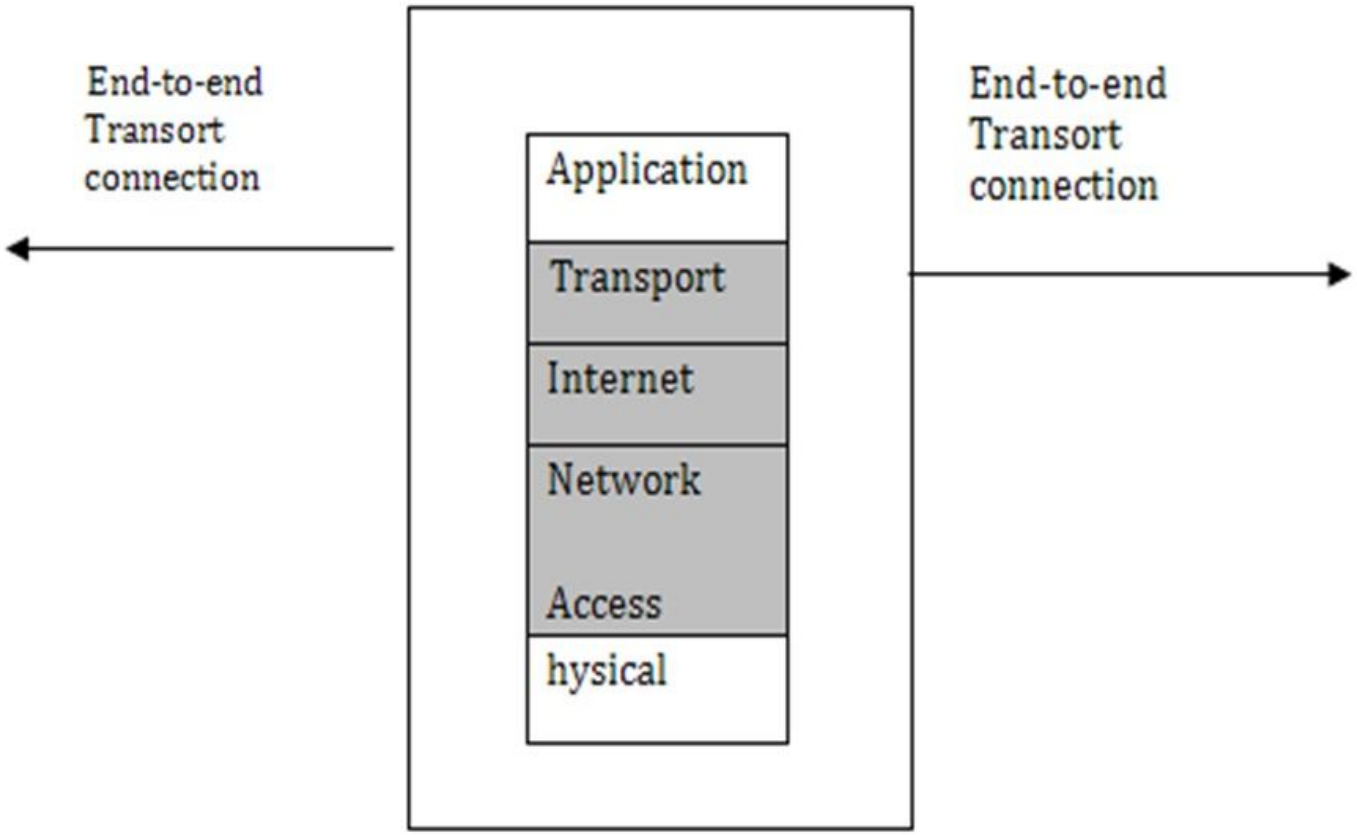
- Stateful Filters
  - ***Stateful filters*** introduce a technology of stateful inspection packet filtering.
  - These firewalls perform the work of their first-generation predecessors but operate up to layer 4 (transport layer) of the OSI model. This is achieved by retaining packets until enough are available to make a judgement about its state. Known as stateful packet inspection, it records all connections passing through it and determines 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 to Firewall

- **Application Layer**
  - ***Application layer filtering*** can "understand" 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).

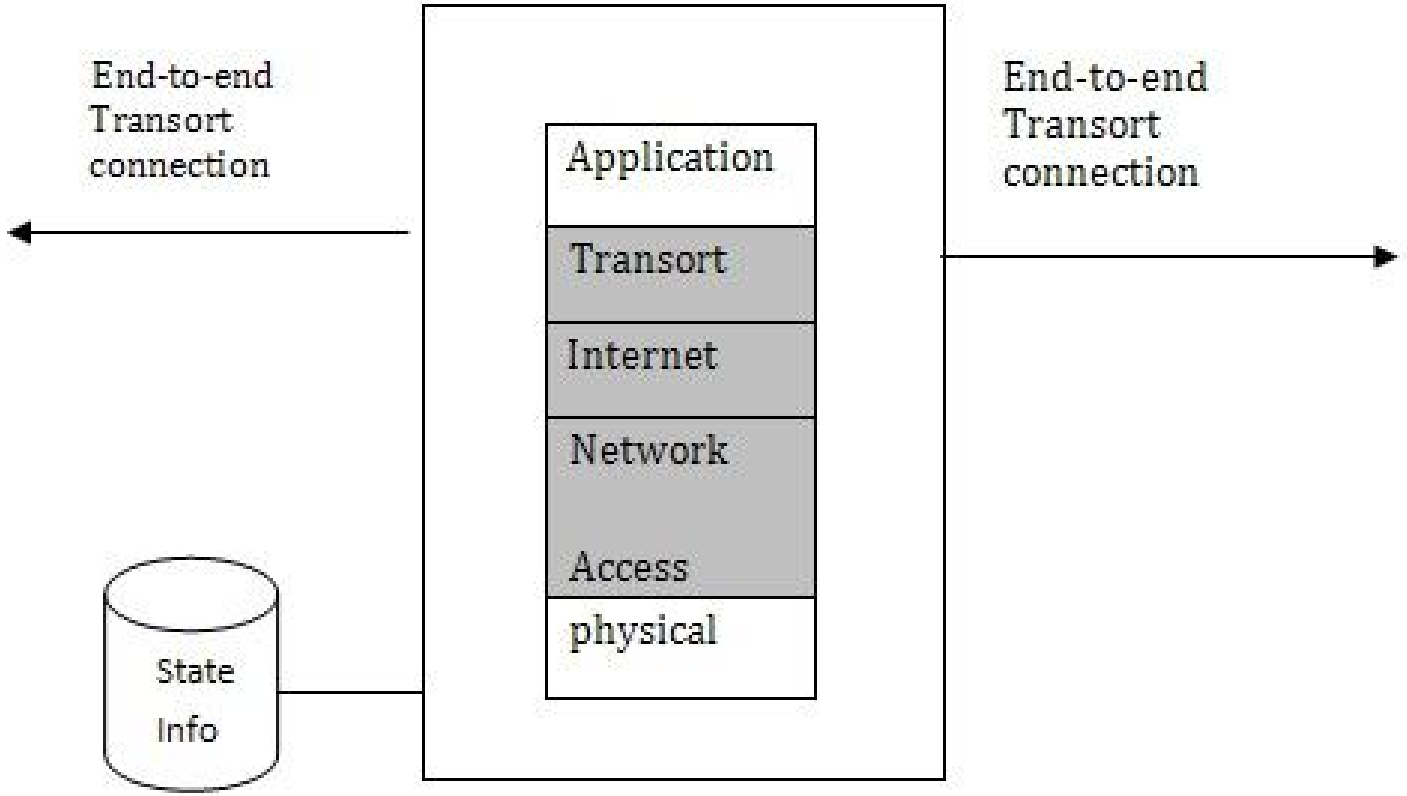
6.1 Introduction to Firewall

- **Packet Filtering Firewall**



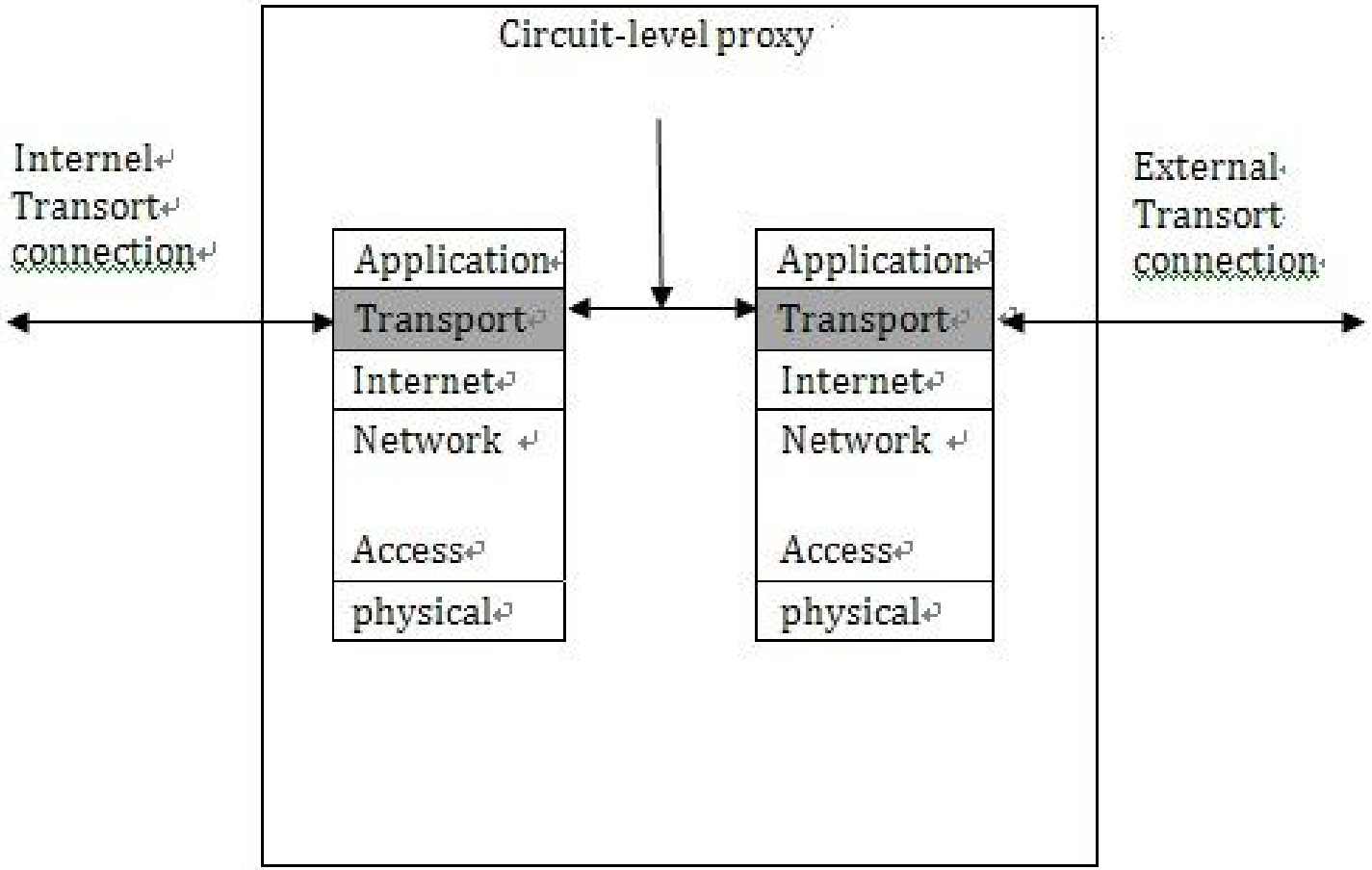
6.1 Introduction to Firewall

- **Stateful Inspection Firewall**



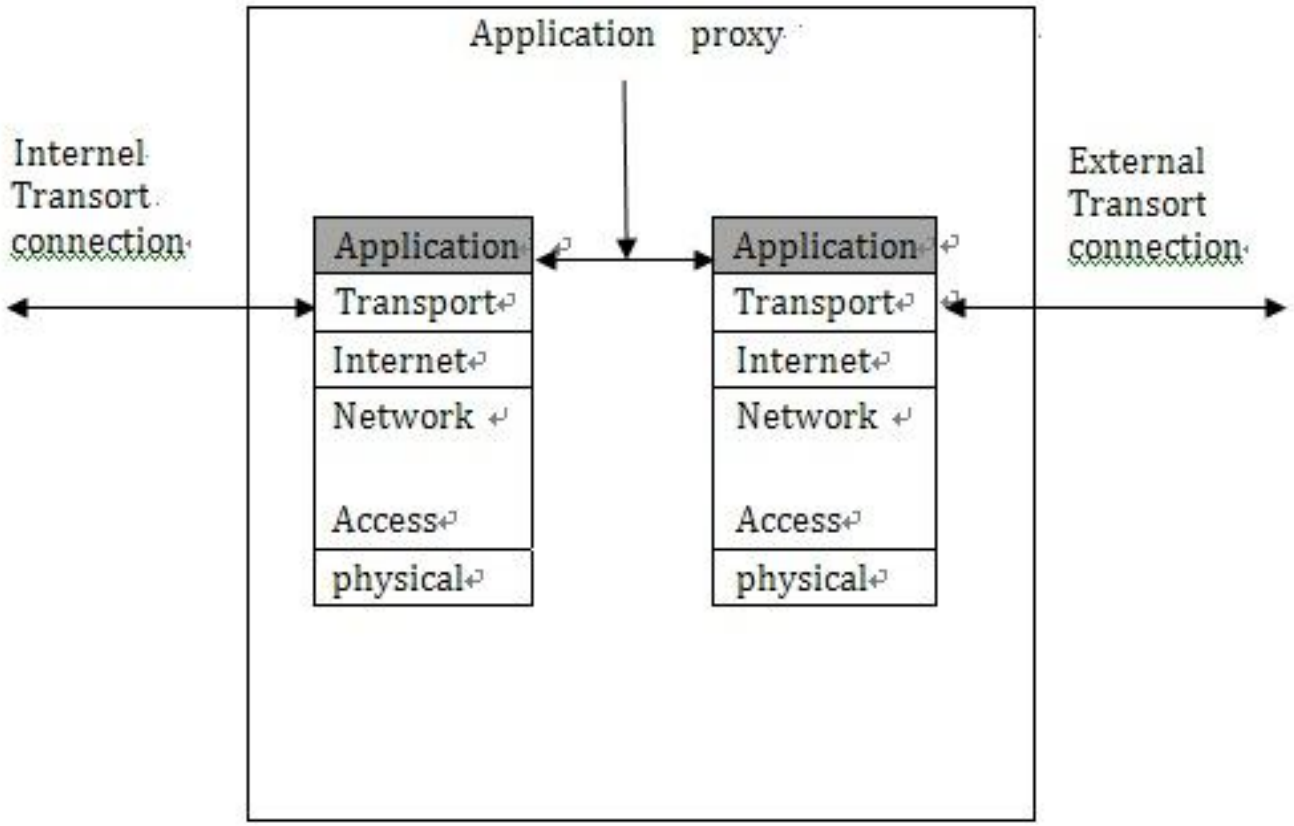
6.1 Introduction to Firewall

- **Circuit-Level Gateway**



6.1 Introduction to Firewall

- **Application-Level Gateway**



6.1 Introduction to Firewall

6.1.3 What Can a Firewall 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

6.1 Introduction to Firewall

- Protect resources
  - To 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
  - Alarm when a policy has been violated

Outline

6.1 Introduction to Firewall

6.2 Design Principles of Firewall

- Packet Filtering Firewall
- Packet Filtering Firewall Based on the State
- Application Proxy Firewall
- Bastion Host

6.3 Penetration of firewall

6.4 Firewall installation and Configuration

Google

6.2 Design Principles of Firewall

6.2.1 Packet Filtering Firewall

- What is Packet Filtering Firewall
- How Packet Filtering Firewall Works
- What to Filter
- Advantages
- Disadvantages

6.2 Design Principles of Firewall

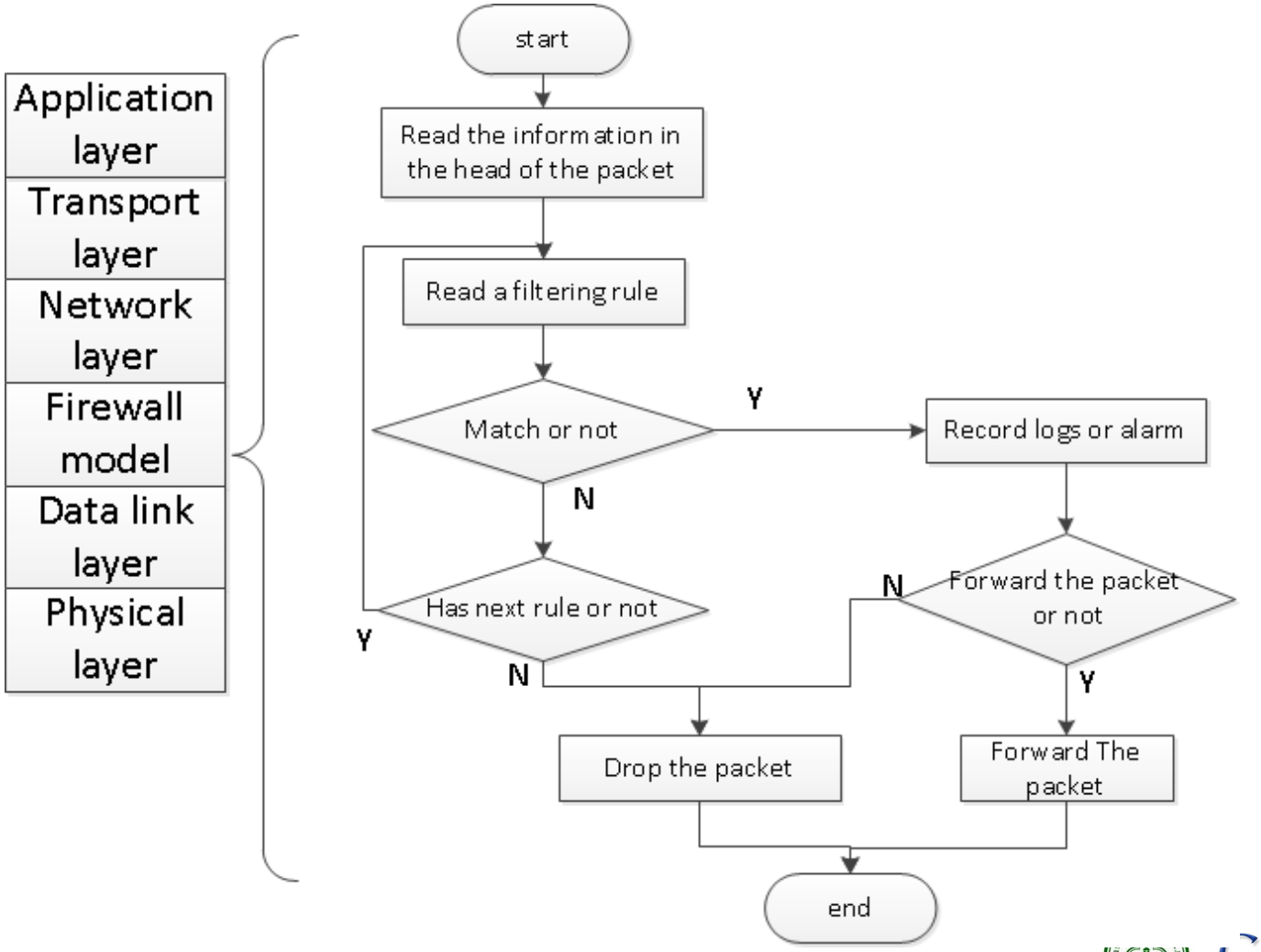
- **What is Packet Filtering Firewall**
  - Packet Filtering Firewall allow the packet which match the established rule set to pass and deny the packet which violate the established rule set, at the same time, it will record log message, alarm the administrator when a policy has been violated.

6.2 Design Principles of 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
  - 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 Design Principles of Firewall

- **How Packet Filtering Firewall Works**



6.2 Design Principles of Firewall

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

6.2 Design Principles of Firewall

- **Advantages**
  - High speed
  - Transparent for the users

6.2 Design Principles of 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 Design Principles of Firewall

6.2.2 Stateful Inspection Firewall

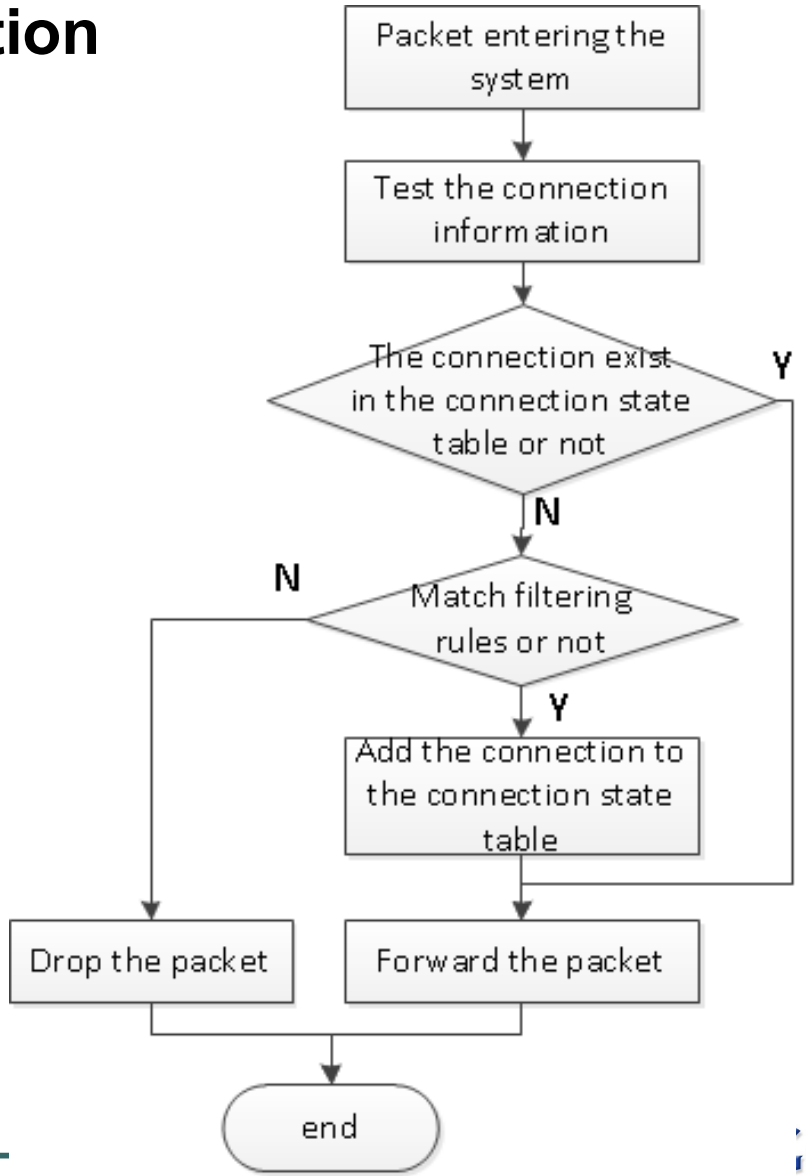
- What is Stateful Inspection Firewall
- How Stateful Inspection Firewall Works
- Advantages
- Disadvantages

6.2 Design Principles of Firewall

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

6.2 Design Principles of Firewall

- **How Stateful Inspection Firewall Works**



6.2 Design Principles of Firewall

- **Advantages**
  - **Safer than** static packet filtering
  - Better performance than static packet filtering
- **Disadvantages**
  - Security is not high enough due to fewer checks on packet data
  - More detections demand higher performance of the firewall

6.2 Design Principles of Firewall

6.2.3 Application Layer Gateway (ALG, or Proxy Server)

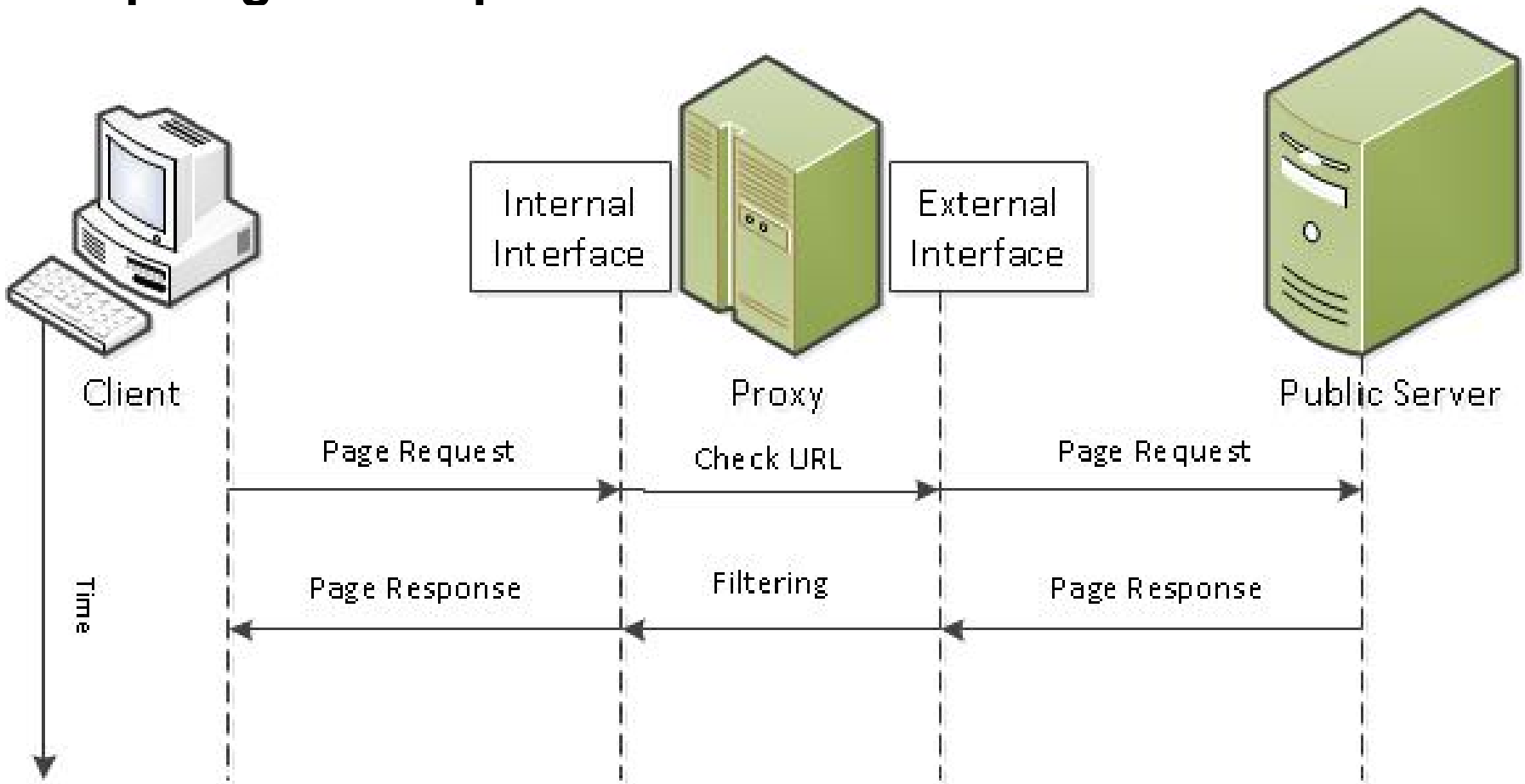
- What is Proxy
- Topological Graph of Proxy
- Function Offered By Proxy
- Advantages
- Disadvantage

6.2 Design Principles of Firewall

- What is Proxy
  - Responsible for the communication between external network and internal network
  - When the users intend to communicate, they do not communicate directly, proxy will help forwarding instead

6.2 Design Principles of Firewall

- **Topological Graph**



6.2 Design Principles of Firewall

- **Topological Graph**

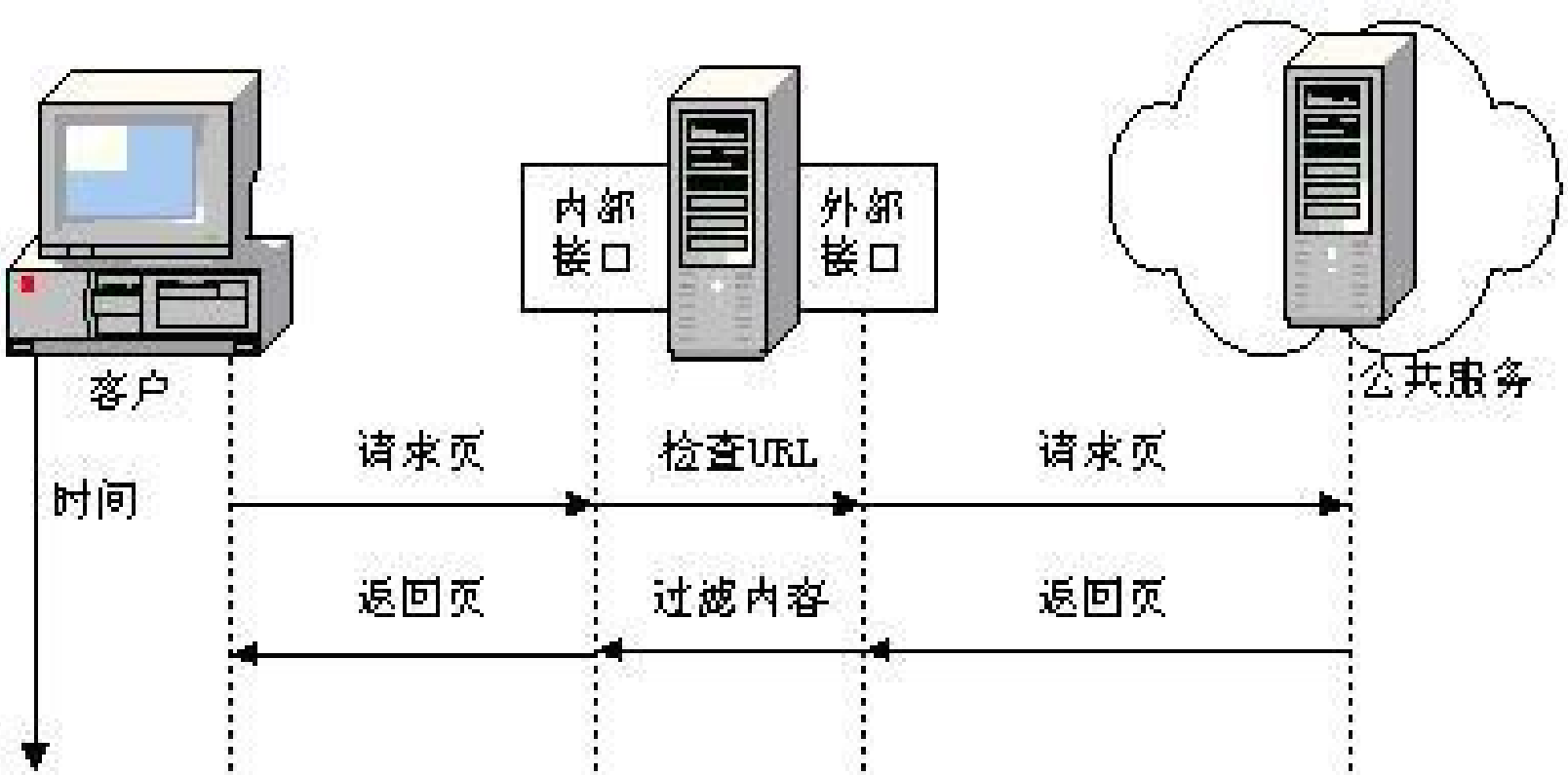


图8.4 一个服务代理

6.2 Design Principles of Firewall

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

6.2 Design Principles of Firewall

- **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

6.2 Design Principles of Firewall

- **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 firewall
- **Example:** H3C SecPath F1000-A-EI

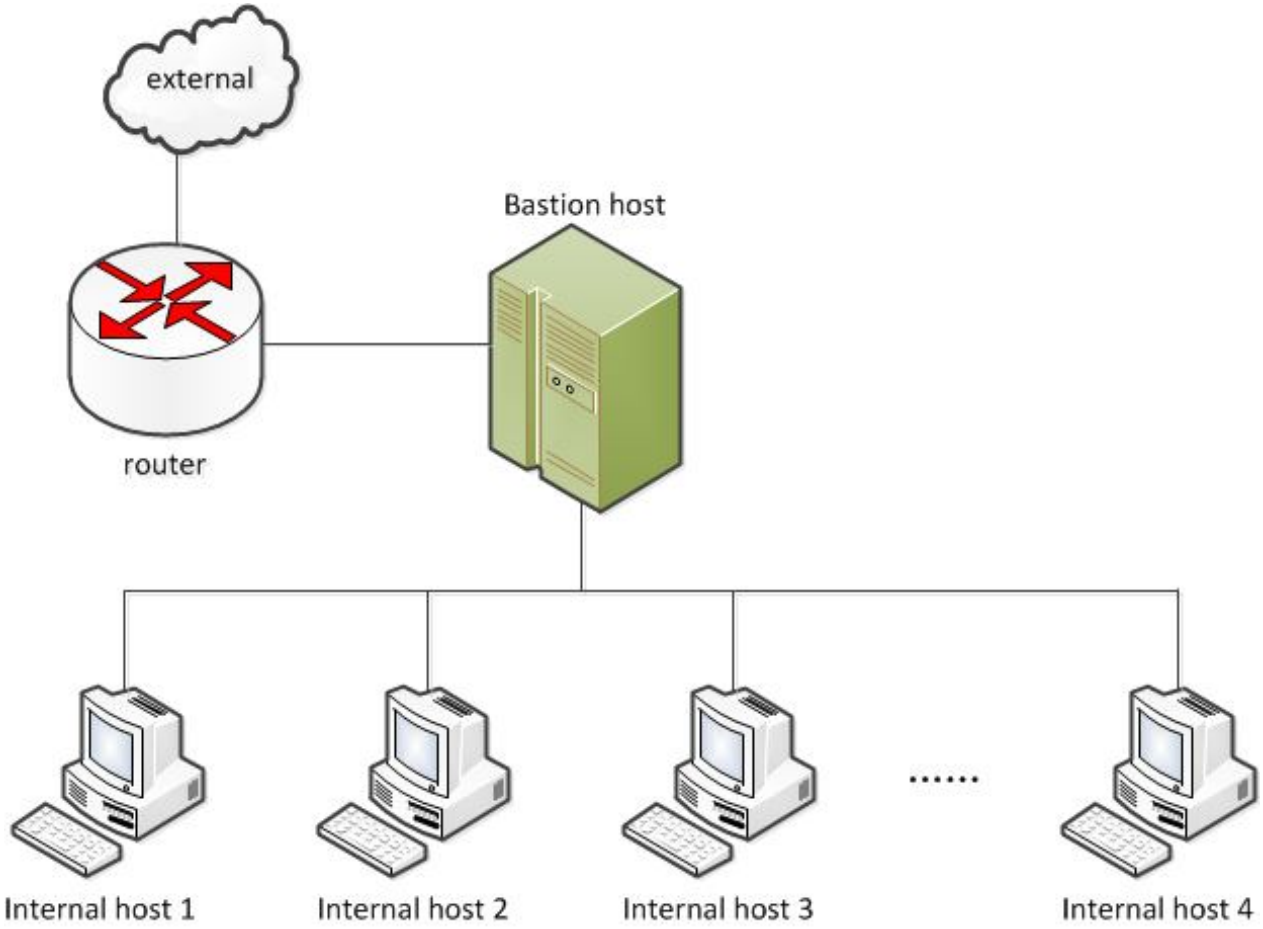
6.2 Design Principles of Firewall

6.2.4 Bastion Host

- Topological Graph
- Design Principles of Bastion Host
- Type of Bastion Host
- Physical Placement of Bastion Host

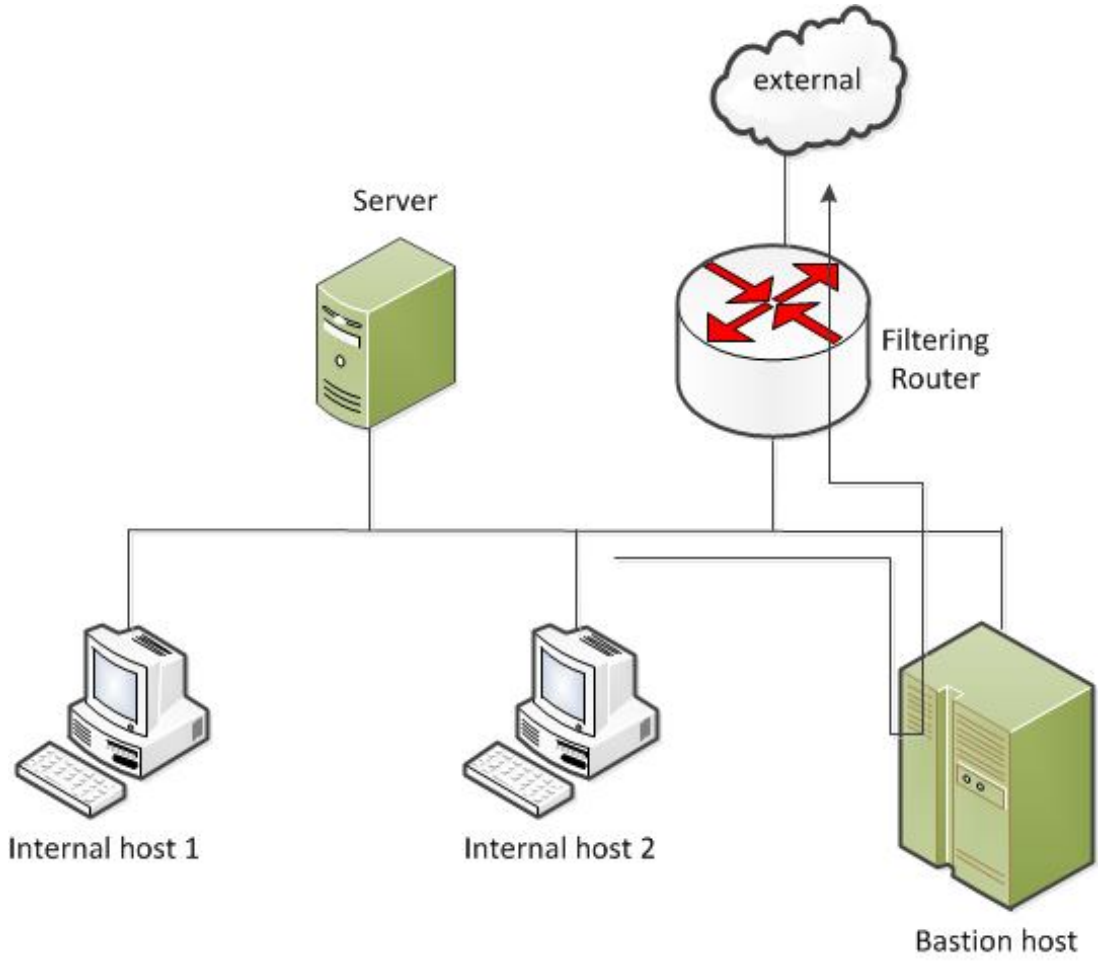
6.2 Design Principles of Firewall

- **Topological Graph**



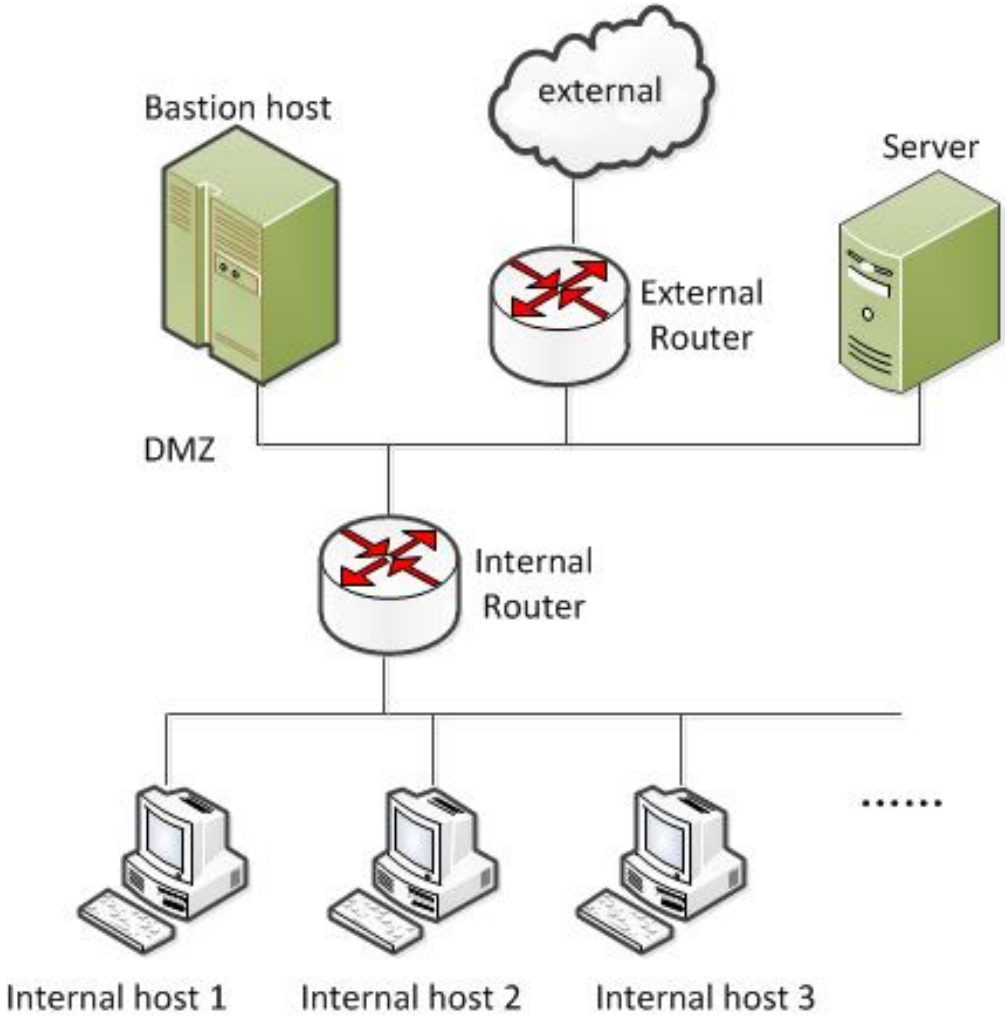
6.2 Design Principles of Firewall

- **Physical placement of bastion host**



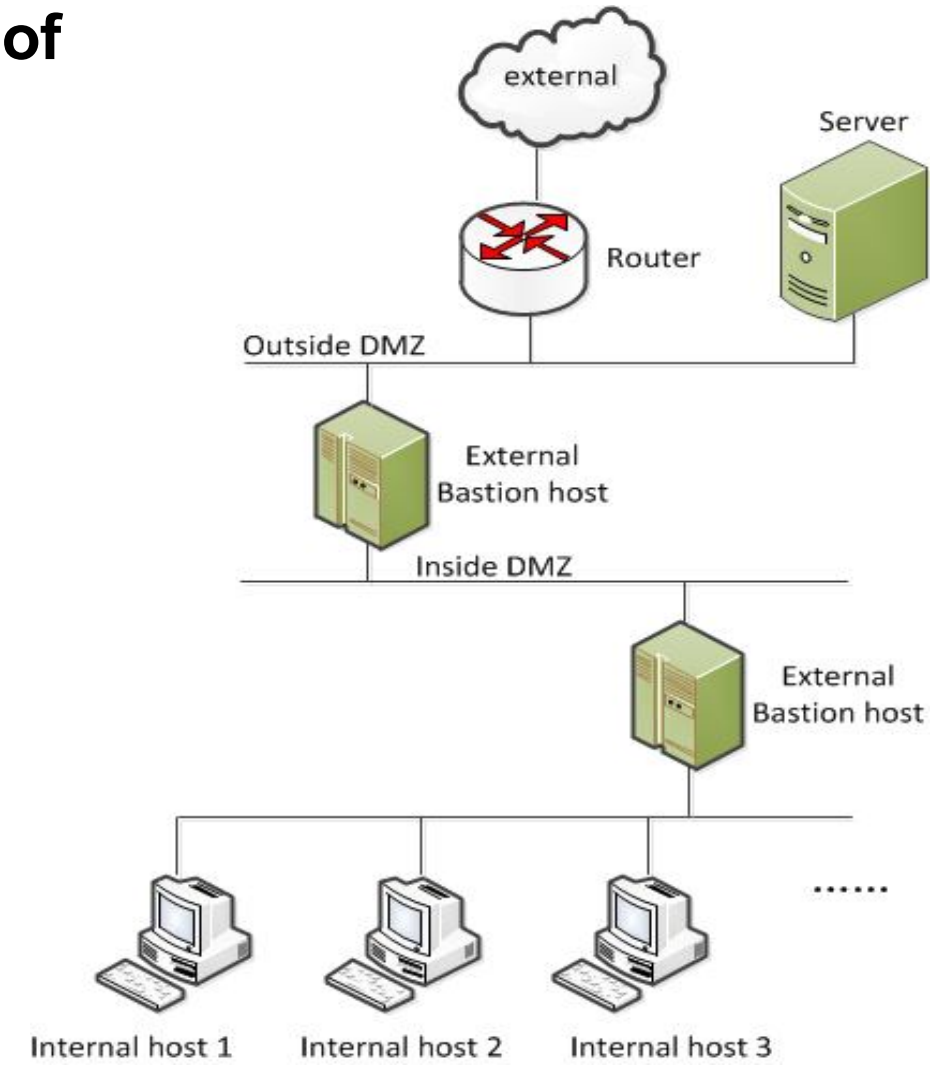
6.2 Design Principles of Firewall

- **Physical placement of bastion host**



6.2 Design Principles of Firewall

- **Physical placement of bastion host**



Outline

6.1 Introduction to Firewall

6.2 Design Principles of Firewall

6.3 Penetration of firewall

- Attacking Packet Filtering Firewall
- Attacking Stateful Inspection Firewall
- Attacking Proxy

6.4 Firewall installation and Configuration

6.3 Penetration of Firewall

6.3.1 Attacking Packet Filtering Firewall

- IP Address Spoofing Attack
- Denial-of-service Attack
- Tiny Fragment Attack
- Trojan Attack

6.3 Penetration of Firewall

6.3.2 Attacking Stateful Inspection Firewall

- Protocol Tunneling
- Trojans Rebound

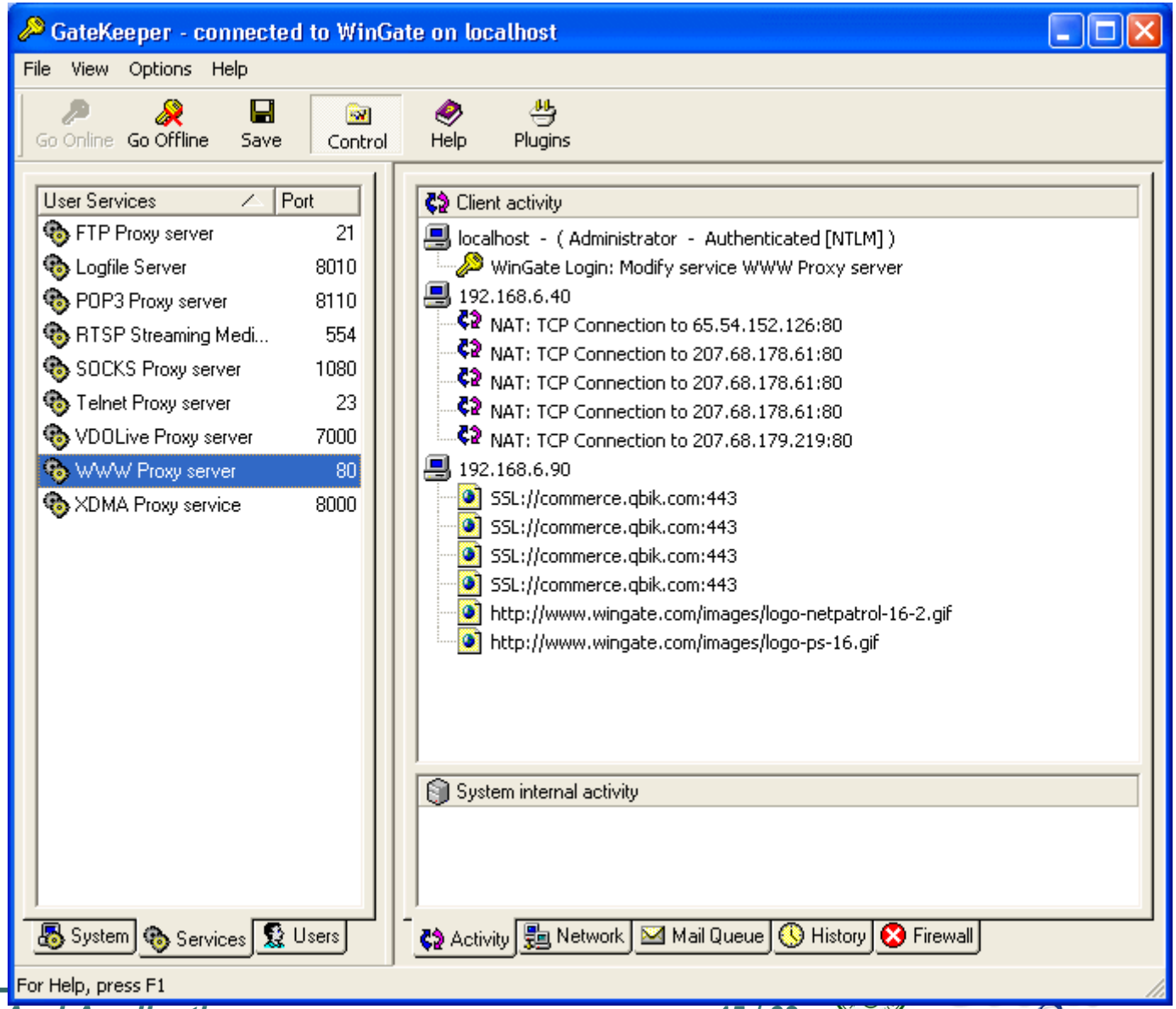
6.3 Penetration of Firewall

6.3.3 Attacking Proxy

- Unauthorized Web Access
- Unauthorized Socks Access
- Unauthorized Telnet Access

6.3 Penetration of Firewall

- WinGate



6.3 Penetration of Firewall

- **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.

Outline

6.4 Firewall Installation and Configuration

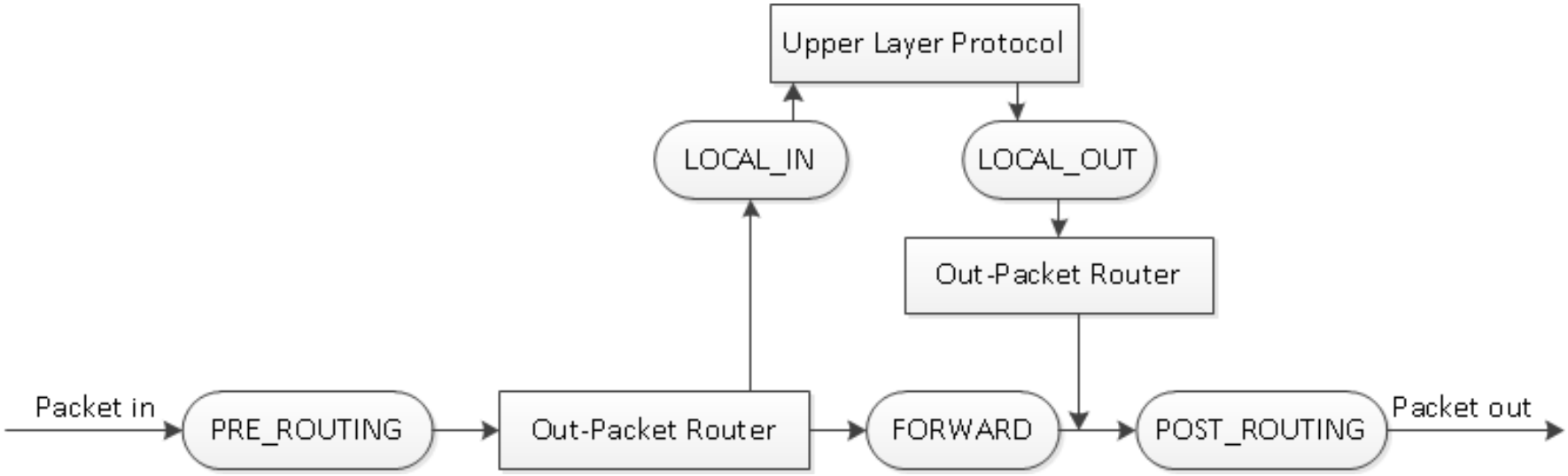
- **Security on Linux - Iptables**
  - What is Iptables
  - Architecture of Iptables
  - Command Format
  - Examples

6.4 Firewall Installation and Configuration

- **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** in the Linux 2.4 and later version of linux.

6.4 Firewall Installation and Configuration

- **Architecture of Iptables**



6.4 Firewall Installation and Configuration

- **Command Format**

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

6.4 Firewall Installation and Configuration

- **Command Format –** command

-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

6.4 Firewall Installation and Configuration

- **Command Format –** Rule

-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

6.4 Firewall Installation and Configuration

- **Command Format –** Target_Action

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

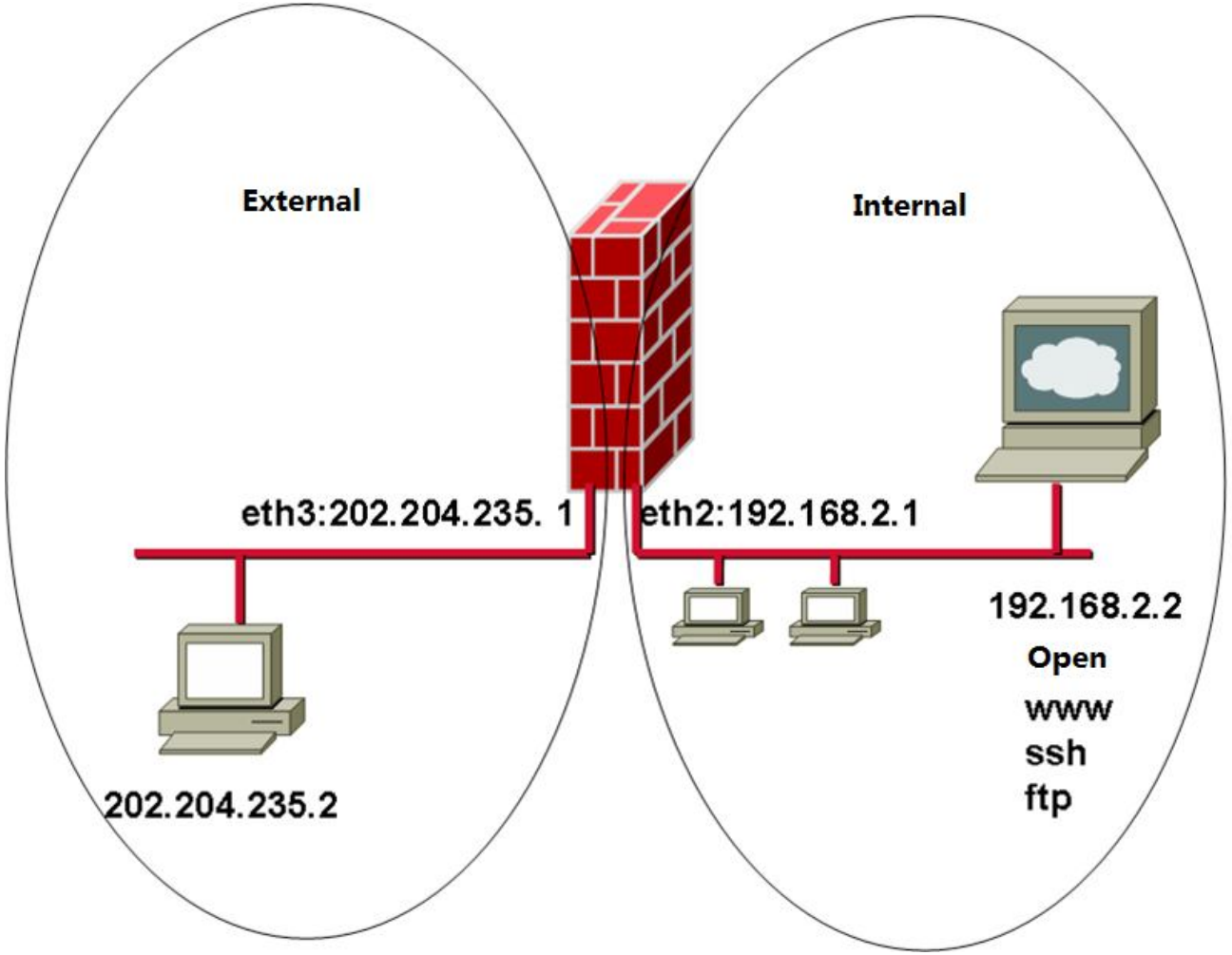
6.4 Firewall Installation and Configuration

- **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**

6.4 Firewall Installation and Configuration

- **Examples –** Gateway Firewall



6.4 Firewall Installation and Configuration

- **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

6.4 Firewall Installation and Configuration

- **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

6.4 Firewall Installation and Configuration

- **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

6.4 Firewall Installation and Configuration

- **Practice:**
  1. Understand IPTABLES
  2. Try to install and configurate IPTABLES.

References

1. Wikipedia Firewall (computing)
   http://en.wikipedia.org/wiki/Firewall_(computing)
2. Wes Noonan, Ido Dubrawsky, Firewall Fundamentals
3. Hui Yan, Wei Wang, Yupeng Ning, Principle and Technology of Firewall
4. Technology of Building Boston Host
   http://www.bitscn.com/netpro/firewall/200704/101642.html
5. D. Brent Chapman & Elizabeth D. Zwicky Building Internet Firewalls
   http://sjoel.home.xs4all.nl/the-networking-cd-bookshelf/firewall/index.htm
6. Several Common Technology Used By Hacker To Attack Firewall
   http://it.rising.com.cn/newSite/Channels/Safety/SafetyResourse/Safe_Foundation/200503/01-093018524.htm

References

7. The Vulnerability and Defect of Firewall
   http://www.xinfengit.com/201001/14101948.html
8. Tianfeng Lin. A Guide to Setting Up a Server.
9. Difference Between Hardware Firewall and Software Firewall
   http://www.differencebetween.net/technology/difference-between-hardware-firewall-and-software-firewall/
10. WinGate:
    http://www.wingate.com/products/wingate/index.php
11. Greg Hoglund,James Butler, Rootkits: Subverting the Windows kernel, Pearson Education Inc, 2006
12. Michael Gregg,Stephen Watkins, Hack the Stack, Syngress, 2006

Thank you!