Advanced Network Security

Firewall

Dr. Yaeghoobi

PhD. Computer Science & Engineering, Networking, India

dr.yaeghoobi@gmail.com

00 Security Policy

01 Firewall

02 Types of Firewalls

03 How Firewalls Work

04 Firewalls Features

Security Policy

00

Even paranoids have enemies.

—Anonymous

Picking a Security Policy

- A ***security policy*** is the **set of decisions** that, collectively, determines an organization’s posture toward security.
- A security policy **determines the limits of acceptable behavior**, and what the **response to violations should be**.
- Naturally, security policies will differ from organization to organization.
- Every organization should have one, if only to let it take action when unacceptable events occur.

Picking a Security Policy

- The first step, then, is to decide what is and is not permitted.
  - To some extent, this process is driven by the business or structural needs of the organization; thus, there might be an edict that bars personal use of corporate computers.
  - Some companies wish to restrict outgoing traffic, to guard against employees exporting valuable data.
  - Other aspects may be driven by technological considerations: a specific protocol, though undeniably useful, may not be used, because it cannot be administered securely.
  - Still others are concerned about employees importing software without proper permission: the company doesn’t want to be sued for infringing on someone else’s rights.
- Making such decisions is clearly an iterative process.

Stance

- **A key decision in the policy is the *stance* of the firewall design.**

- Firewalls are an important tool that can **minimize the danger**, while providing most—but not necessarily all—of the benefits of a network connection.

- But a paranoid stance is necessary for many sites when setting one up.

All programs are buggy

- **Theorem 1** *Large programs are even buggier than their size would indicate.*
- **Corollary 1.1** *A security-relevant program has security bugs.*
- **Theorem 2** *If you do not run a program, it does not matter whether or not it is buggy.*
- **Corollary 2.1** *If you do not run a program, it does not matter if it has security holes.*
- **Theorem 3** *Exposed machines should run as few programs as possible; the ones that are run should be as small as possible.*
- **Corollary 3.1 (Fundamental Theorem of Firewalls)** *Most hosts cannot meet our requirements: they run too many programs that are too large. Therefore, the only solution is to isolate them behind a firewall if you wish to run any programs at all.*

Security Policy Philosophies

- Flexibility
- Service-access
- Firewall Design
- Information
- Remote Access

Flexibility

- Ability to adapt or change the policy
- Flexible due to the following considerations:
  - Internet changes
  - Internet risks

- انعطاف پذیری
  - امکان انطباق یا تغییر خط مشی و قوانین
  - به دلیل ملاحظات زیر قابل انعطاف است:
    - تغییر اینترنت
    - خطرات اینترنت

Service Access

- Internal user issues
- Remote access policies
- External connections

- دسترسی به خدمات
  - مشکلات داخلی کاربر
  - قوانین دسترسی از راه دور
  - اتصالات خارج از سازمان

Firewall Design

- Permit any service unless it is expressly denied
- Deny any service unless it is expressly permitted
- طراحی فایروال
  - اجازه خدمات را بدهید مگر اینکه صریحاً رد شود
  - هرگونه خدمات را رد کنید مگر اینکه صریحاً مجاز باشد

Information Concerns

- E-MAIL
- Web browsing

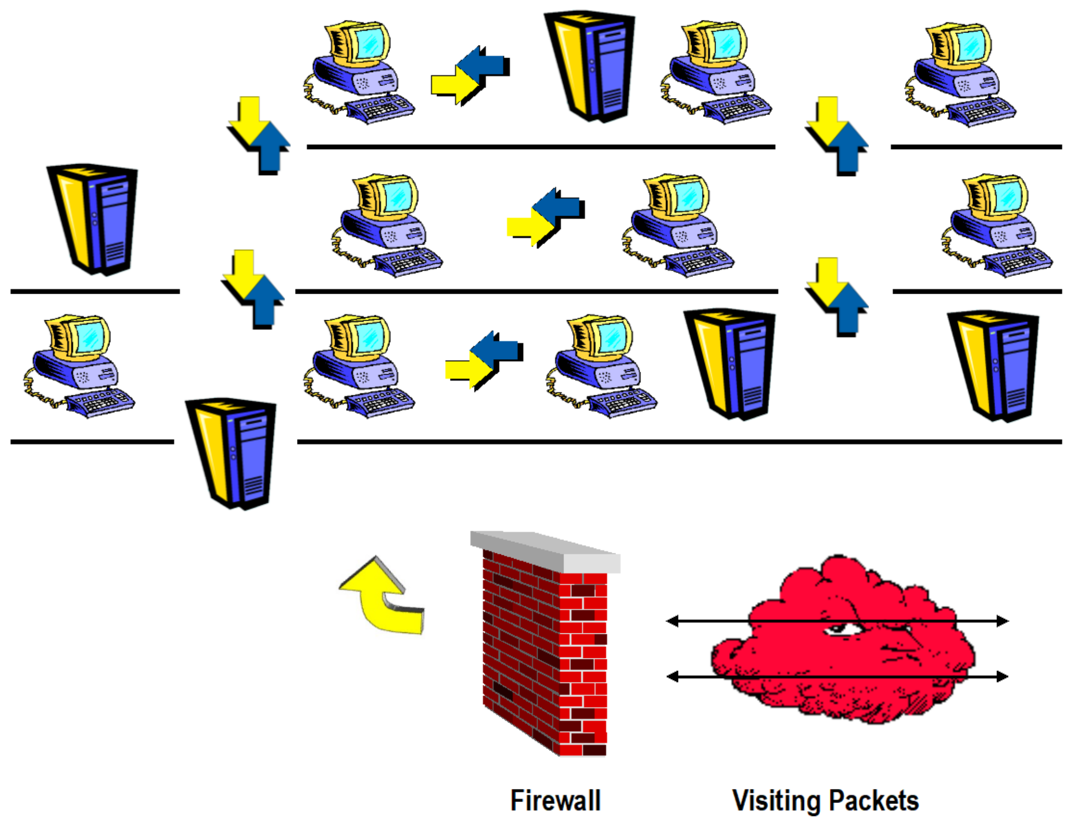
- نگرانی‌های اطلاعاتی

Remote Access

- A user’s dial-out capability might become an intruder dial-up threat
- Outside users must be forced to pass through the advanced authentication features of the firewall

- دسترسی از راه دور
- کاربران خارج از سازمان باید مجبور شوند از ویژگیهای پیشرفته احراز هویت فایروال عبور کنند

Securing a Network



Firewall

01

Firewall Location

- Placed at the entrance to an organization’s intranet
- Placed inside an internal network
- Placed between Remote Access Server (RAS) and internal network
- It is the check point for communication to an outside network

Network Packet

- Contains all the information required to route it to the final destination
- Contains the information to deliver it to the correct application on the destination system
- Requires five specific pieces of information for routing

Division of IP Address

- **Network -** similar to a zip code, the primary information used by routers to deliver the packet to the correct LAN

- **Host -** similar to a letter address, directs the packet to the correct host on the LAN

Network Session

- The **total data sent** between an initial request and the completion of that request
- Evident at the user or application level of the protocol stack

- کل داده های ارسال شده بین یک درخواست اولیه و تکمیل آن درخواست
- در سطح کاربر یا برنامه پروتکل مشهود است

Standard Firewall Services

- Access Control کنترل دسترسی
- Authentication احراز هویت
- Activity Logging فعالیت ورود به سیستم
- Other Firewall Services سایر خدمات فایروال

Access Control

- Allows the firewall to **consider the network interface** where the packet enters
- **Prevents or limits IP spoofing**
- “Don’t talk to me unless I talk to you first”
- به دیوار آتش اجازه می دهد تا رابط شبکه را که بسته در آن وارد می شود در نظر بگیرد
- جلوگیری و محدود کردن جعل IP

Authentication

- Standards have usually relied on passwords or smartcards or token
- No based on IP address but user level
- استاندارد ها معمولاً به رمزهای عبور یا کارتهای هوشمند یا نشانه ها اعتماد کرده اند
- نه بر اساس آدرس IPبلکه در سطح کاربر

Activity Logging

- Allows the firewall to **record information** concerning all successful and failed session attempts
- Referred to as an **audit log**
- به دیوار آتش اجازه می دهد تا اطلاعات مربوط به همه تلاش های موفق و ناموفق جلسه را ضبط کند
- به عنوان یک گزارش حسابرسی

Other Firewall Services

- Proxy Applications
- Virus Scanning
- Address Mapping
- Virtual Private Networks (VPN)

Firewall Administration Interfaces

- Text-file based administration مدیریت مبتنی بر فایل متنی
  - **Popular in routers and homegrown firewalls**
  - Interface of choice for **UNIX administrators**
  - **Easier to make errors**
- Text-menu based administration مدیریت مبتنی بر متن
  - **Reduces likelihood of errors**
  - **Less** flexibility of control
  - **Limited visual feedback** to changes made
- GUI-based administration
  - **Most prominent**
  - **Easier to use**
  - **Less prone to errors**

Types of Firewalls

02

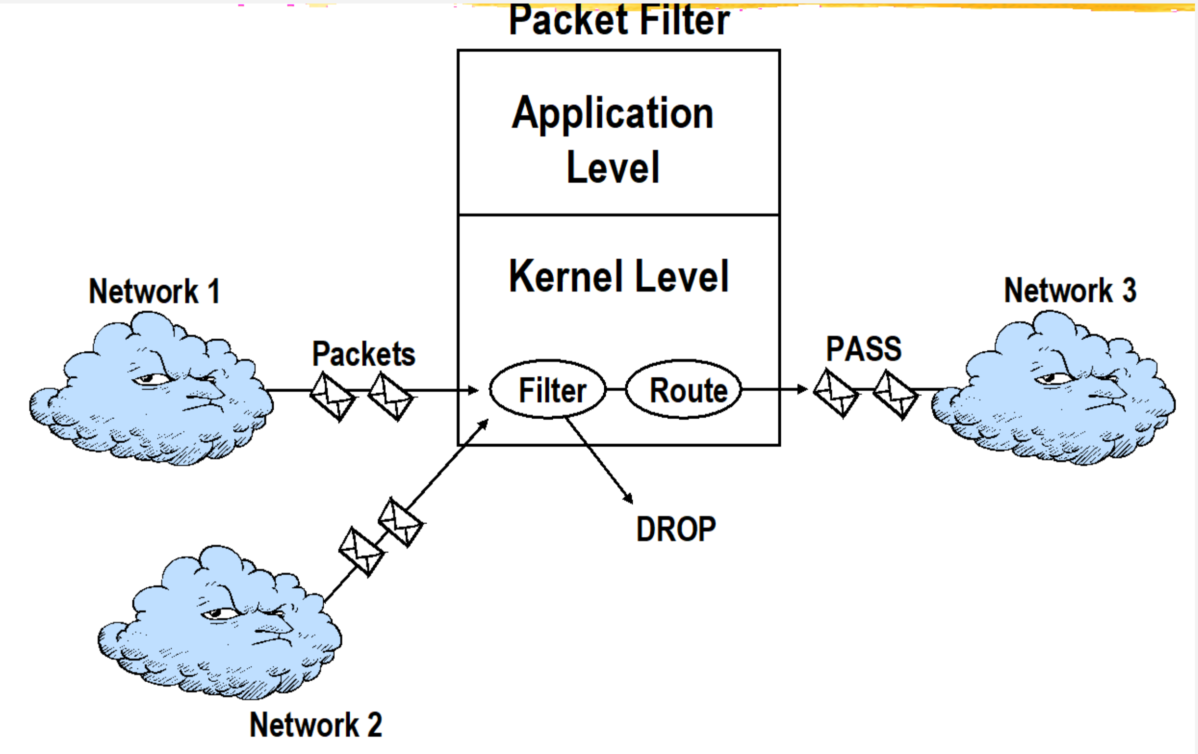
Basic Types of Firewalls

- Packet Filter
- Application-Level Gateway
- Stateful Inspection

Packet Filter Firewall

- Referred to as **filtering routers** with a set of simple rules
- Determines whether **a packet should pass based on the source and destination information within the packet**
- Process is performed at the **kernel level**
- **Less secure** than application-level gateway firewalls

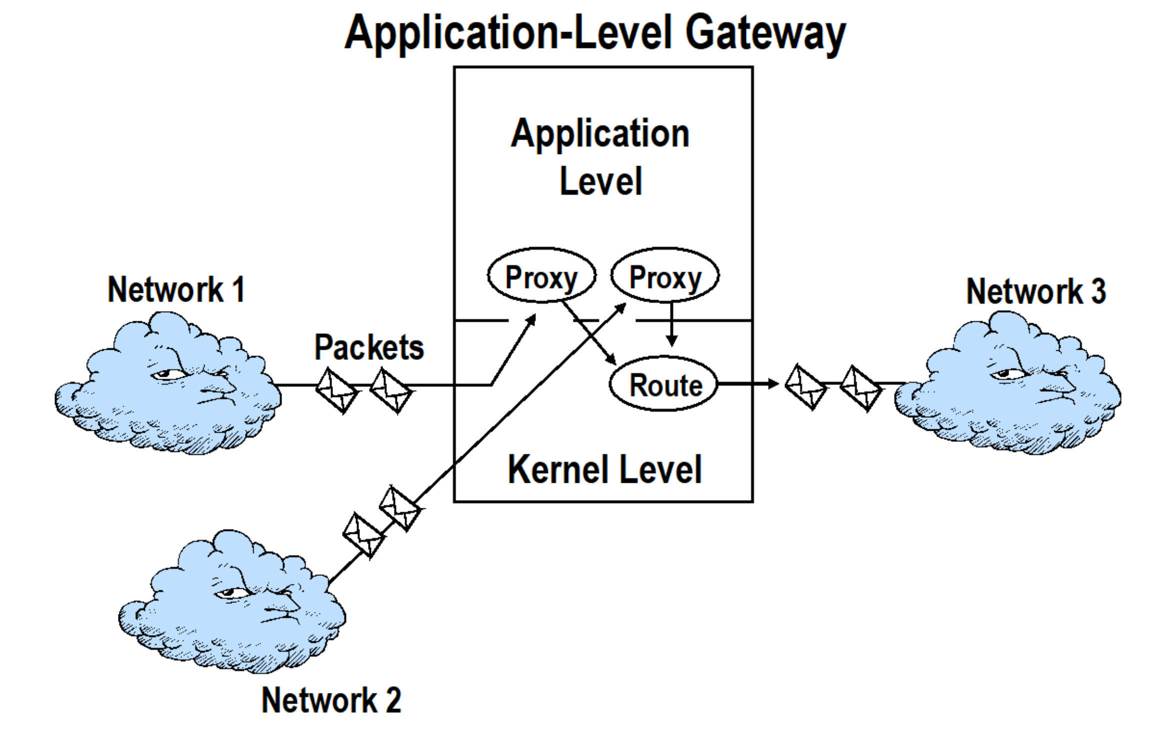
Packet Filter Firewall



Application-level Gateway Firewall

- **Does not allow packets to pass directly between networks**
- **Original connections are made to a proxy** on the firewall
- Requires a **separate application** for each network service
  - TELNET
  - FTP
  - E-mail
  - WWW

Application-level Gateway Firewall



Stateful Packet Filtering

- Ensures the **highest level** of firewall security by performing the following functions:

1. Accessing, analysing and utilizing communication information
2. Communication-derived state
3. Application-derived state
4. Information Manipulation

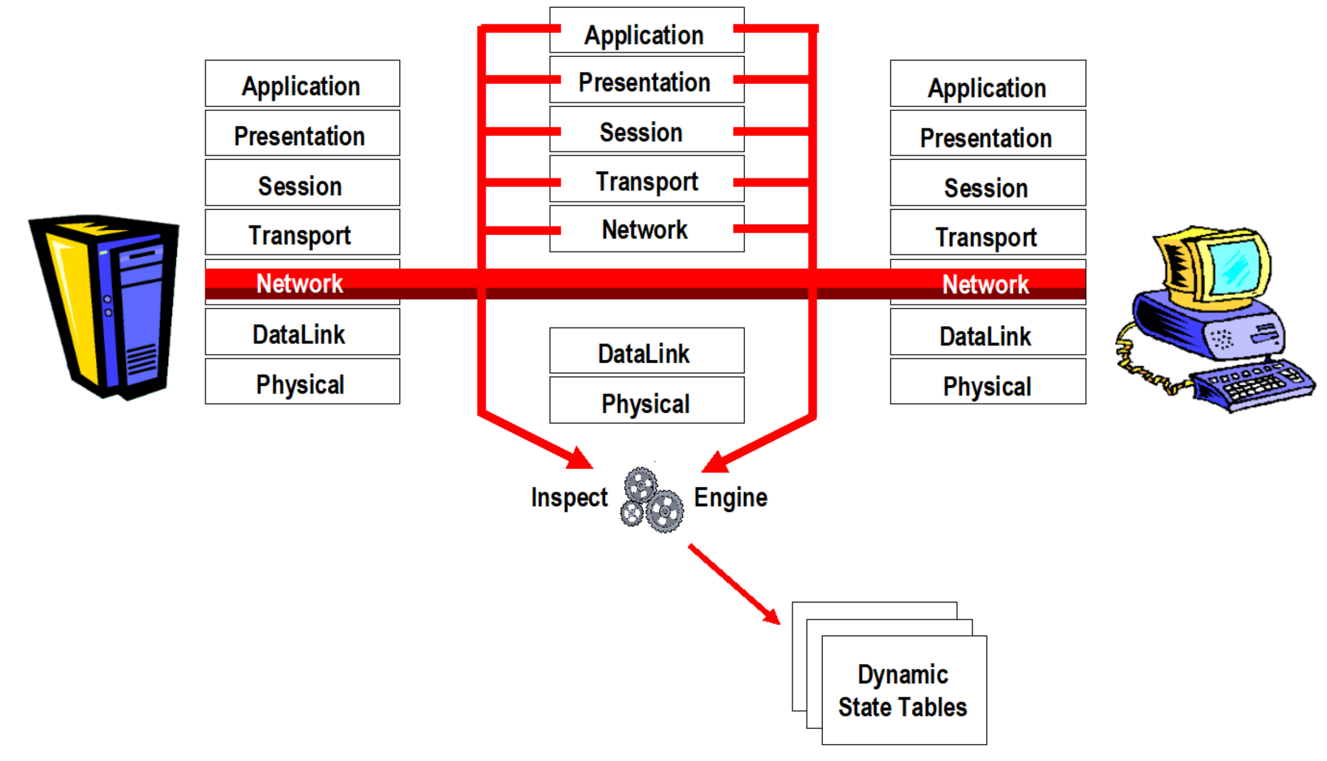
Stateful Packet Filtering …

- Communication information
  - **Information from all seven layers of the packet**
- Communication-derived state
  - State information derived from **previous communications**

Stateful Packet Filtering …

- Application-derived state
  - State information derived from **other applications**
- Information manipulation
  - Evaluation of flexible expressions based on the following:
    - communication information
    - communication-derived state
    - application-derived state

Stateful Packet Filtering



Comparison of Firewall Architecture

Firewall Capability	Packet Filters	Application Level Gateways	Stateful Inspection
Communication information	Partial	Partial	Yes
Communication-derived state	No	Partial	Yes
Application-derived state	No	Yes	Yes
Information manipulation	Partial	Yes	Yes

How Firewalls Work

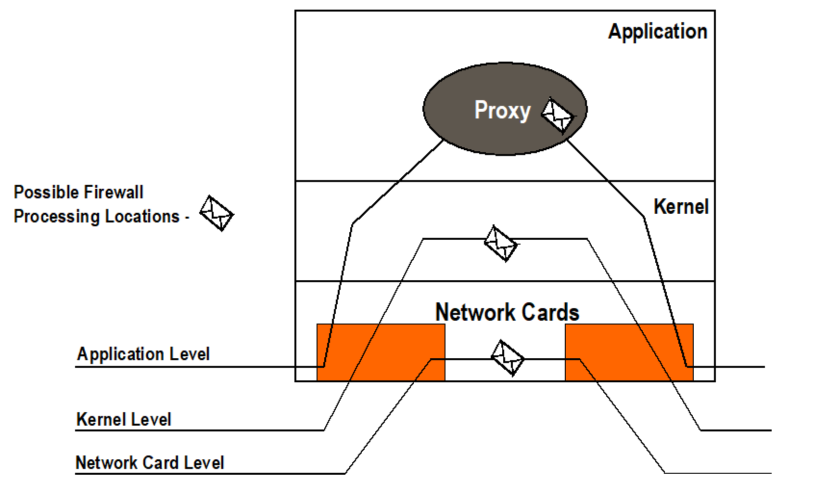
03

Objectives

- Identify the packet processing locations on a firewall
- Describe packet filtering and its limitations
- Describe proxy applications and their limitations
- Identify user authentication
- Describe firewall auditing

Packet Processing Locations

- Application Level
    - Proxy services
- Kernel Level
    - Routers and host-based packet filters
- Network Interface Card (NIC) Level

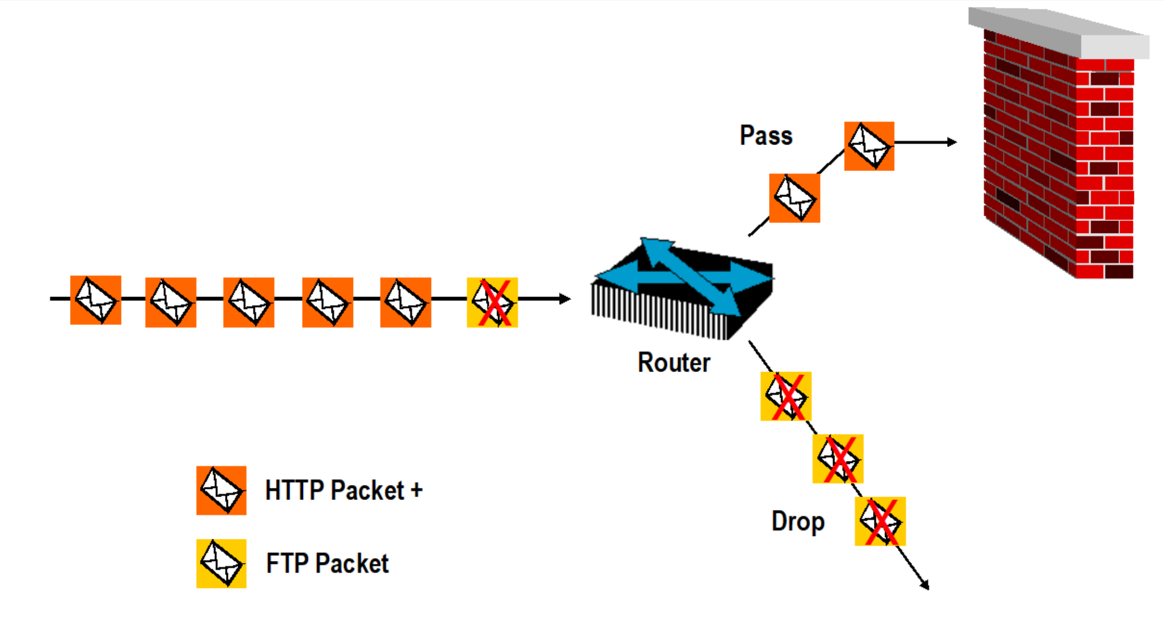


Packet Filtering

- May occur at **any one of the processing locations**
- Most often supported at the **NIC or kernel level**
- Passes or drops packet based on source and destination **IP addressing**

Field	**Purpose**
Source IP address	Host address of sender
Destination IP address	Host address of service provider
Upper level protocol	Different protocols offer different services
TCP source port number	A random number greater than 1024
TCP destination port number	Indicates service such as Telnet or HTTP

HTTP Filtering



Example of Rule List

Rule Number	Source Address	Destination Address	Protocol	Source port Number	Action
1	10.56.2.99	*	*	*	Drop
2	10.56.*	10.122.*	TCP	*	Pass
3	10.122.*	10.56.*	TCP	23	Pass
4	*	10.56.*	TCP	*	Pass
5	*	*	*	*	Drop

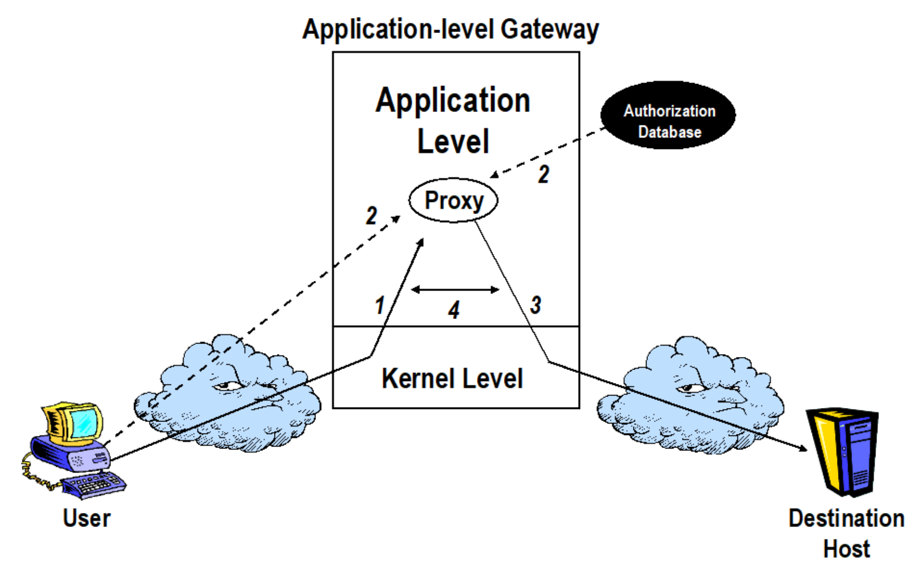
Example Packets and Resulting Actions

Source Address	Destination Address	Protocol	Source port Number	Destinatio n port Number	Match Rule #	Action
10.56.2.98	10.122.6.11	TCP	23567	23 (Telnet)	2	Pass
10.56.2.99	10.122.6.11	TCP	6723	23 (Telnet)	1	Drop
10.56.2.98	10.122.6.11	other	23568	23 (Telnet)	5	Drop
10.122.34.9	10.56.2.98	TCP	23	98455	3	Pass
10.122.23.1	10.56.2.5	TCP	1543	25 (mail)	4	Pass

- **Limitations of Packet Filtering**
  - Some rules could leave open doors to the network
  - Difficult to determine examine exactly what the rules permit

Proxy Applications

- Applications on proxy gateways that act on behalf of the user requesting service through the firewall



Connection Process

1. User first **establishes a connection to the proxy application** on the firewall
2. The **proxy** application **gathers information** concerning the connection and the requesting user
3. This **information** is used to determine whether the **request should be permitted** - if approved, the proxy creates another connection from the firewall to the intended destination
4. **The proxy shuttles the user data from one connection to the other**

Proxy Challenges

- Initial connection must go through the proxy application on the firewall, not to the intended destination
- **Proxy application must obtain the IP address of the intended destination**

Proxy Connections

- Direct Connection
- Modified Client
- Invisible Proxy

Direct Connection

- Connect directly to the firewall proxy using the address of the firewall and the port number of the proxy
- با استفاده از آدرس فایروال و شماره پورت پروکسی مستقیماً به پروکسی فایروال وصل شوید
- **Least preferred method**

- Requires two addresses for each connection:
  - Address of firewall
  - Address of the intended destination

Modified Client

- Applications are executed client-side, at the user’s computer
- برنامه ها توسط کاربر در کامپیوتر کاربر اجرا می شوند

- **Effective and transparent**

- The need to have a **modified client application** for each network service is a significant drawback

Invisible Proxy

- No need to modify client applications
- Users don’t have to direct their communication to the firewall
- Packets are automatically redirected to an awaiting proxy as they enter the firewall

- بدون نیاز به اصلاح برنامه های hvfv;
- کاربران لازم نیست ارتباط خود را به دیوار آتش هدایت کنند
- بسته ها به محض ورود به دیوار آتش به طور خودکار به پروکسی هدایت می شوند

Proxy Limitations

- New applications must be developed for each supported service

User Authentication

- Three traditional methods for verifying someone’s identity:
  - “Something known” - a password
  - “Something possessed” - a key to a lock, or a smartcard
  - “Something embodied” - fingerprint or retinal scan

Activity Logging

- Information provided by log files:
  - Time and date of session start
  - Time and date of session end
  - Source host address
  - Destination host address
  - Protocol
  - Destination Port
  - Action taken - accepted or denied
  - User name - if authentication used

Audit Information

- **Administrators may review the logs to look for suspicious activities:**
  - Repeated failed connection attempts
  - Flood of allowed connection attempts going to the same host
  - Connections made at odd hours
  - Multiple failed authentication attempts

Firewalls Features

04

Basic Access Control

- Access Rules and Lists
- Host Spoofing Controls

Access Rules and Lists

- **Host-Based**
  - Describes the sets of services allowed for each host or network
    - مجموعه خدمات مجاز برای هر میزبان یا شبکه را توصیف می کند
- **Service-Based**
  - Identifies the sets of hosts or networks that may use each service
    - مجموعه هاست یا شبکه هايي که ممکن است از هر سرویس استفاده کنند را مشخص می کند

Host Spoofing Controls

- **Reducing** the threat of spoofing IP addresses:
  - Restriction of the “source routing option” allows a host to control the route taken to return to the source host address
  - Control by network interface also reduces the threat

- محدود کردن "گزینه مسیریابی مبدأ" به میزبان اجازه می دهد تا مسیر برگشتی را کنترل کند
- همچنین کنترل توسط رابط شبکه، تهدید را کاهش می دهد

Supported Services

- Domain Name System (DNS)
  - DNS servers **share information**
  - **An attacker** could possible **redefine the address** of a trusted host within a network to an address outside the network
- Finger
  - Used to find out **logins, user names, and information** concerning a users previous login
- File Transfer Protocol (FTP)
  - A separate network connection is usually made from the destination host back to the original FTP connection
  - Most FTP servers supports a PASV **(passive mode)** capability allowing the connection **to originate from the client rather than the server**

Supported Services …

- Internet Control Messaging Protocol (ICMP)
  - Used to **send error or test messages between systems**
  - “PING” uses ICMP to **send echo requests** to see if a host is reachable
- Internet Relay Chat (IRC)
  - Using IRC, a **user can contact an IRC server** and join an Internet conversation
  - Threats associated with IRC are of a “social engineering” nature - **an attacker may contact a user through IRC and convince them to compromise their network**

Supported Services …

- Network News Transfer Protocol (NNTP)
  - **Allows users to access newsgroups to read**
- Network File System (NFS)
  - Allows users to **share file systems** with other users
  - **Little security and vulnerable to attacks**
- Network Time Protocol (NTP)
  - A service used to **synchronize clocks** between computers and networks

Supported Services …

- rlogin
  - Developed at the University of California at Berkeley
  - Used for **remote access** between **local systems**, but not recommended for use across the Internet because of **lack of proper authentication capability**

- TELNET
  - Standard remote login protocol application
  - Provides a **character-based connection between two systems**

Remote/Central Administration

- Firewalls in multiple geographic locations should be administered by a single group within the company

- With central administration the administrator configures the firewalls from a central database they all share

Actions Taken From Alarms

- Recording the action in a log or alarm file
- Sending e-mail to an administrator
- Displaying a message on the firewall console
- Sending an SNMP alarm to a network manager system
- Activating and sending a message to an administrator’s pager
- Running a specialized application or script file from the firewall

Firewall Integrity

- **Dual-Host Firewalls**
  - Splitting the functions of a firewall between two hosts to force attackers to break into two systems for a successful attack
  - فایروال های دو میزبان
  - تقسیم کارکردهای فایروال بین دو میزبان برای مجبور کردن مهاجمین برای حمله موفقیت آمیز به دو سیستم

Firewall Integrity...

- **Integrity Scanner**
  - An application on the firewall that continually scans the firewall for any unauthorized changes to files, file size, or devices
  - برنامه ای در فایروال که دائماً فایروال را برای هرگونه تغییر غیرمجاز در پرونده ها ، اندازه پرونده یا دستگاه ها اسکن می کند

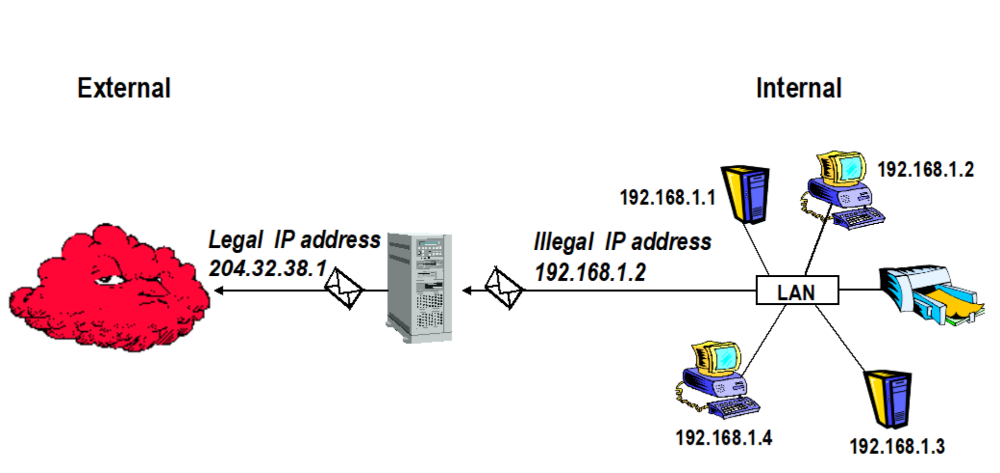
- **Invisibility**
  - A firewall that can’t be seen is difficult to attack
  - حمله به فایروالی که دیده نمی شود ، دشوار است

Special Features

- Address Mapping
- Day and Time Restrictions
- Load Control
- Tunneling
- Virtual Private Networks (VPN)
- Hacker Traps

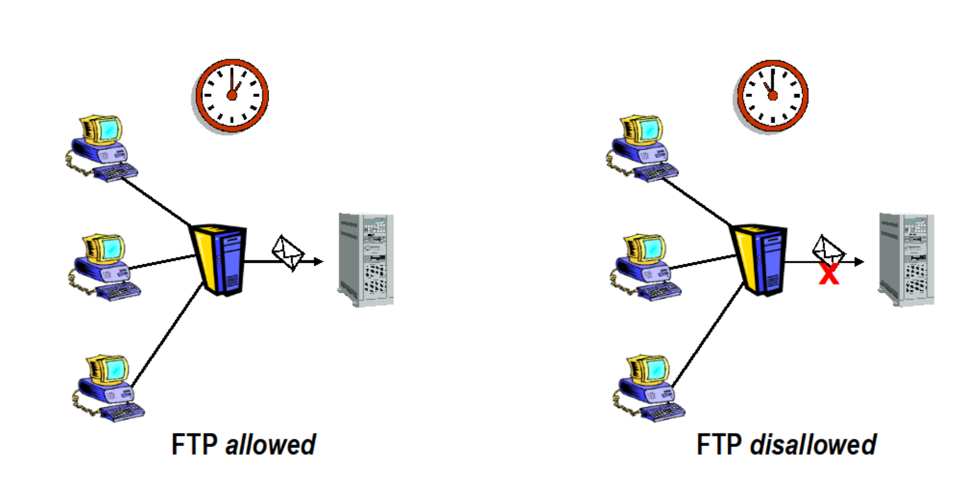
Address Mapping

- Most organizations have **invalid or illegal IP addressing internally**
- **Firewalls can map illegal addresses internally to legal addresses** as packets leave the network



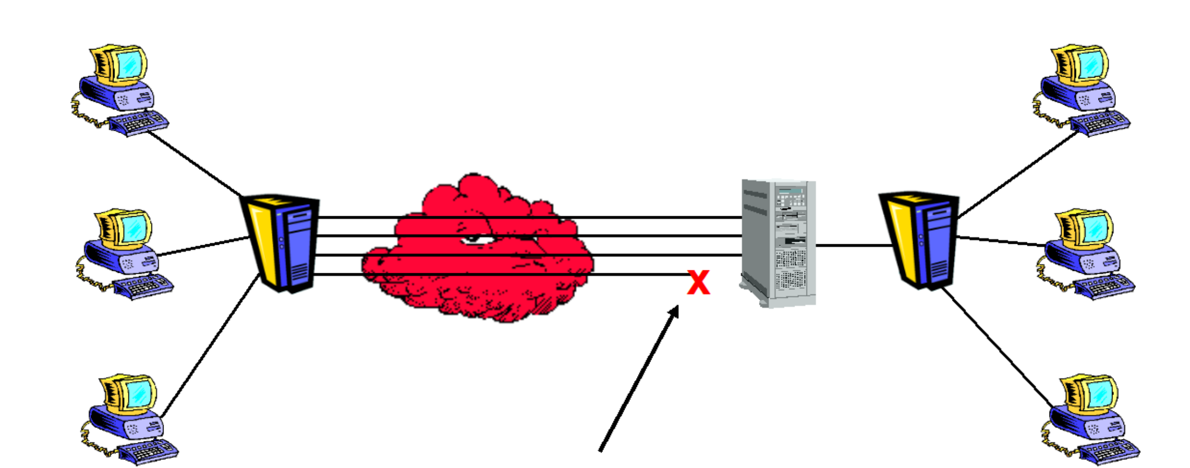
Day and Time Restrictions

- Security policies can be set to **restrict** certain network access based on **day and time**



Load Control

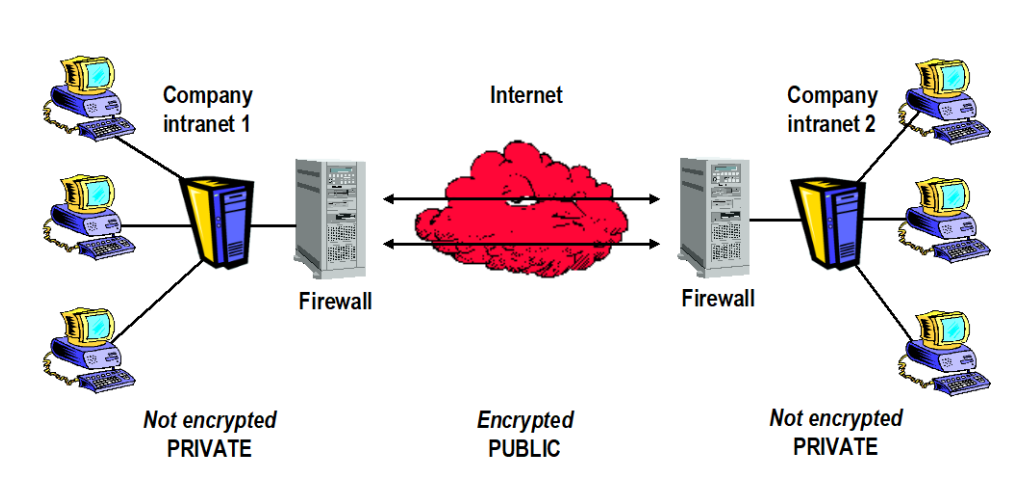
- **Limits the number of simultaneous connections permitted to a host**
- Helps protect **against flooding attacks**



Limiting the number of simultaneous connections

Virtual Private Networks (VPN)

- **Enables encryption** all or selected communication between two or more sites
- **Requires cooperating firewalls** to encrypt and decrypt packets as they are sent and received



Hacker Traps

- Sometimes referred to as **“lures and traps” or “honey pots”**
- Intruders think they have succeeded in breaking into the network when in reality they have been redirected to a “safe” place on the network

Thanks for your Attention.