Chapter Three

Network Firewall Security

Network Security

Introduction

- In today's highly networked world, we can't talk of computer security without talking of network security
- Focus is on:
  - Internet and Intranet security (TCP/IP based networks)
  - Attacks that use security holes of the network protocol and their defenses
- Does not include attacks that use networks to perform some crime based on human weaknesses (such as scams)

Network Security/ Types of Attacks

Passive attacks

- Listen to the network and make use of the information without altering
  - Passive wiretapping attack
  - Traffic analysis
- Defense
  - Using switching tools rather than mere repeating hubs limits this possibility
  - Using cryptography;.

Network Security/ Types of Attacks

Active attacks

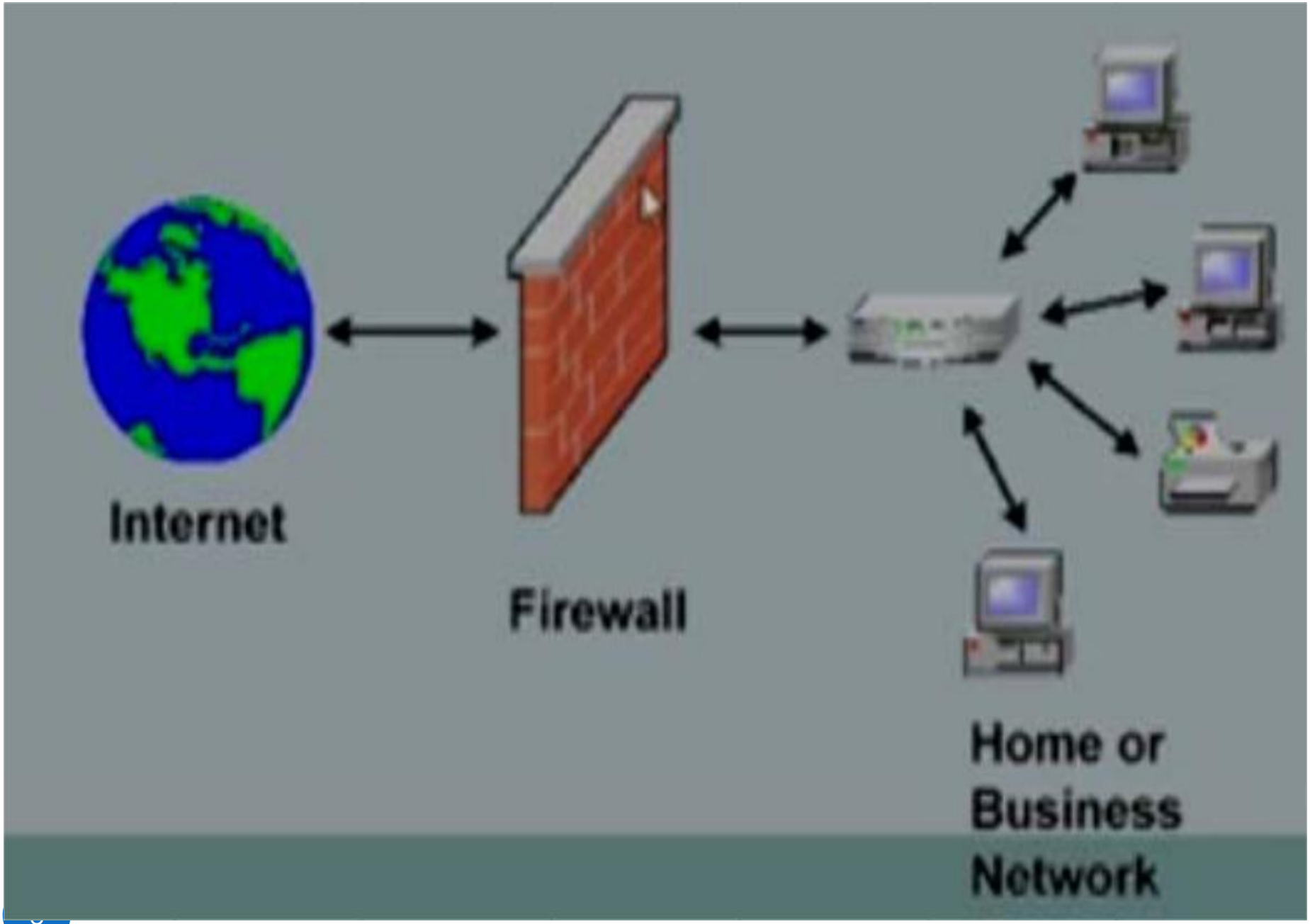
- An active attack threatens the integrity and availability of data being transmitted
  - The transmitted data is fully controlled by the intruder
  - The attacker can modify, extend, delete or play any data
- This is quite possible in TCP/IP since the frames and packets are not protected in terms of authenticity and integrity

- Denial of service or degrading of service attack
  - Prevention of authorized access to resources
  - Examples
    - E-mail bombing: flooding someone's mail store
    - Smurf attack: Sending a "ping" multicast or broadcast with a spoofed IP of a victim. The recipients will respond with a "pong" to the victim
    - There had been reports of incidences of distributed denial attacks against major sites such as Amazon, Yahoo, CNN and eBay

Firewalls

What is a Firewall?

- A firewall is a program or network devices that filters the information coming through the internet connection into your private network or computer system.
- Firewalls are often categorized as either network firewalls or host-based firewalls.
- **Network firewalls** filter traffic between two or more networks and run on network hardware.
- **Host-based firewalls** run on host computers and control network traffic in and out of those machines.


Internet
Firewall
Home or
Business
Network

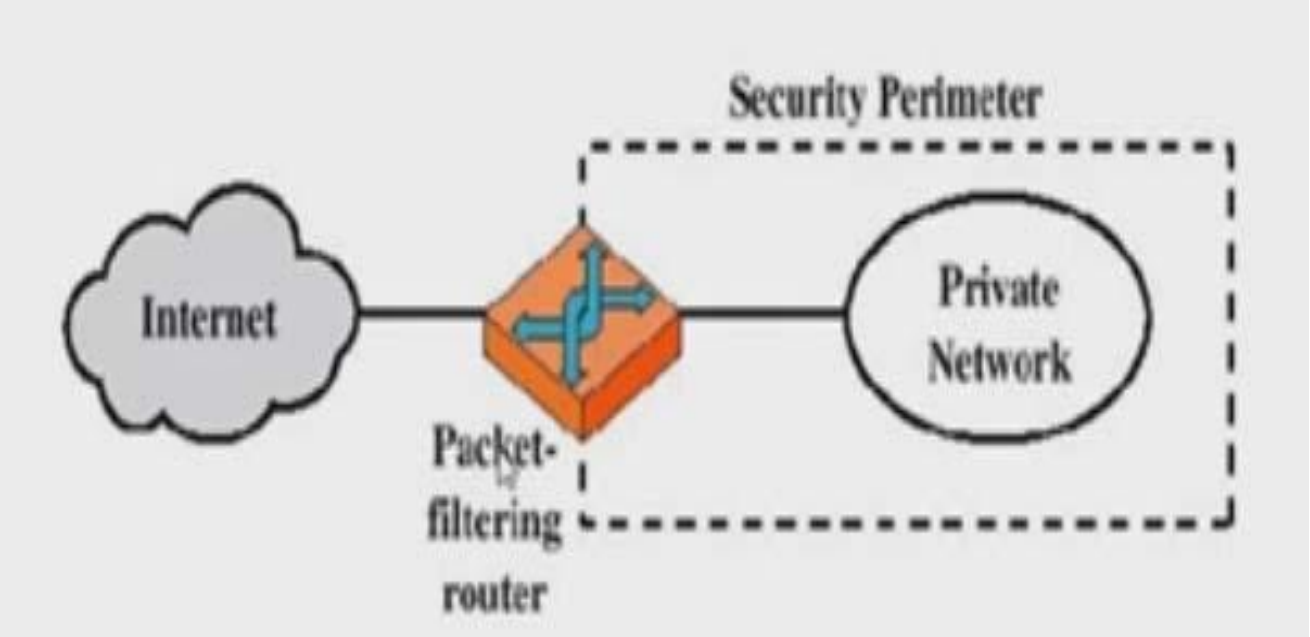
Types of Firewalls:

1. **Packet Filtering Router**
2. **Application Level Gateway**
3. **Circuit Level Gateway**

1. Packet Filtering Router

- Applies a set of rules to each incoming IP packets and then Allow or Drop the packets.
- Filter packets going in both directions.
- The packet filter is typically set up as a list of rules based on matches in the IP or TCP header.

Continued…

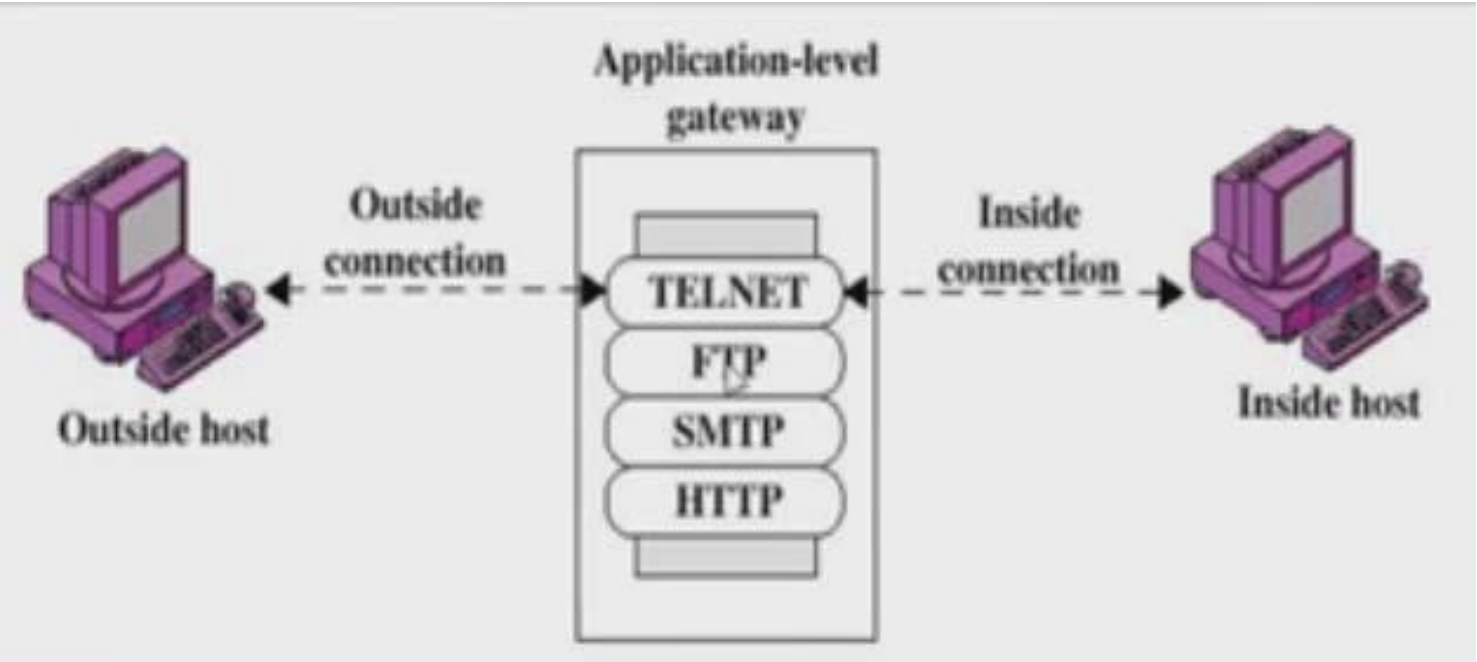

Security Perimeter
Internet
Private Network
Packet-filtering router

Application Level Gateway

Also called as proxy server.

Acts as a relay of application level traffic.

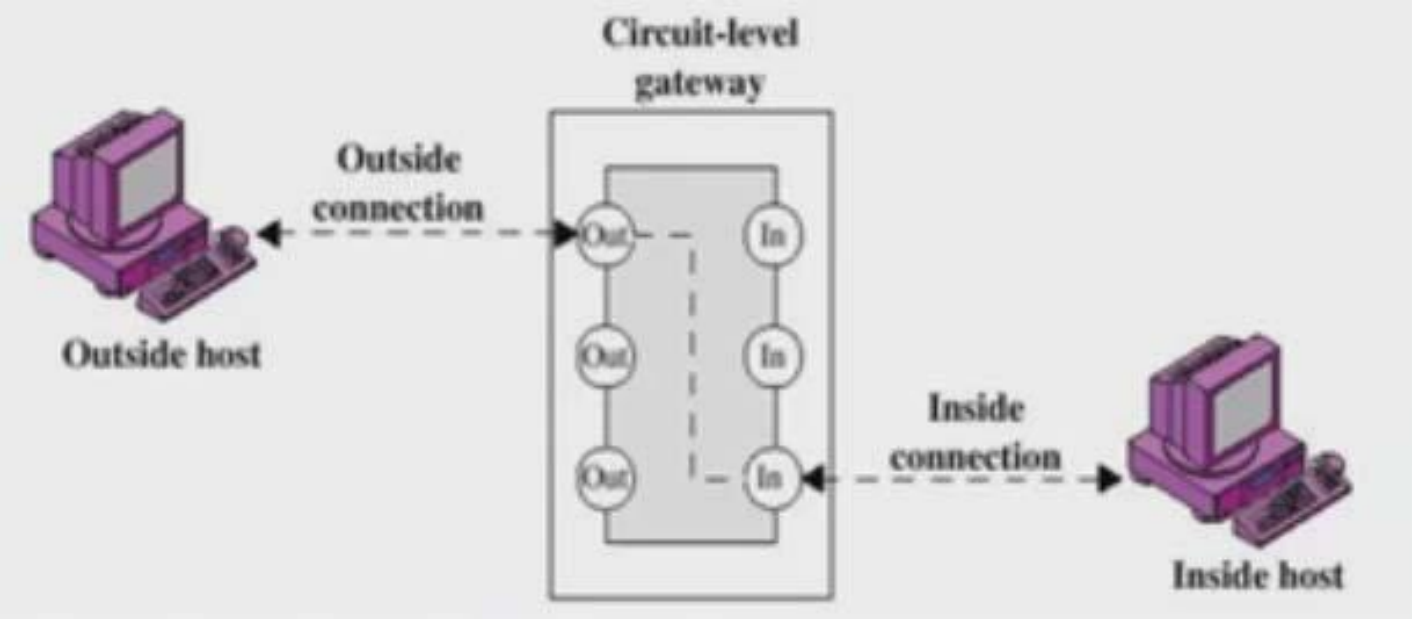
It is used to check the traffic levels.



Circuit Level Gateway

- Standalone Software.
- Sets up two TCP connections.
- The gateways typically relays TCP segments from one connection to the other without examining the contents (simply it will send).
- The Security functions consists of determining which connections will be allowed

Continued...


Circuit-level
gateway
Outside
connection
Out
In
Out
In
Out
In
Outside host
Inside
connection
Inside host

The Role of Firewalls

- A firewall is a term used for a "barrier" between a network of machines and users that operate under a common security policy and generally trust each other and the outside world.

There are two basic reasons for using a firewall at present:

- to save money in concentrating your security on a small number of components
- to simplify the architecture of a system by restricting access only to machines that trust each other.

Advantages of Firewalls

- Concentration of security all modified software and logging is located on the firewall system as opposed to being distributed many hosts.
- **Protocol Filtering**, where the firewalls filters protocols and services that are either not necessary or that cannot be adequately secured from exploitation.
- **Information Hiding,** in which a firewall can "hide" names of internal systems (or) electronic mail addresses, thereby revealing less information to outside hosts.
- **Application Gateways,** where the firewalls requires inside or outside users to connect first to the firewall before connecting further, thereby filtering the protocol.

Continued...

Disadvantages of Firewalls

- The most obvious being that certain types of network access may be hampered or even blocked for some hosts, including telnet, ftp, NFS etc.
- A second disadvantages with a firewall system is that it concentrates security in one spot as opposed to distributing it among systems, thus a compromised of the firewall could be disastrous to other less protected systems on the subnet.
  Example: If someone attacks the security guard, the organization face more risks.

Internet Security Architecture

Designing an Appropriate Network

- There are invariably numerous requirements and expectations placed upon a network, such as meeting and exceeding the organization's availability and performance requirements, providing a platform that is conducive for securing sensitive network assets, and enabling effective and secure links to other networks.
- On top of that, the overall network design must provide the ability to grow and support future network requirements.

Continued...

- Common steps for obtaining such information include meeting with project stakeholders, application and system owners, developers, management, and users.
- It is important to understand their expectations and needs with regard to performance, security, availability, budget, and the overall importance of the new project.
- Adequately understanding these elements will ensure that project goals are met, and that appropriate network performance and security controls are included in the design.
- One of the most common problems encountered in a network implementation is unmet expectations resulting from a difference of assumptions. That's why expectations should be broken down into mutually observable (and measureable) facts as much as possible, so the security designers ensure that there is explicit agreement with any functional proposals clearly understood and agreed.

Performance

- The legacy Cisco Hierarchical Internetworking model, which most network engineers are intimately familiar with, is a common design implemented in large-scale networks today, although many new types of purposed designs have been developed that support emerging technologies like class fabrics, lossless Ethernet, layer two bridging with trill or IEEE 802.1aq, and other data center–centric technologies.
- The three-tier hierarchy still applies to campus networks, but no longer to data centers. This is a "legacy" model socialized by Cisco, but even Cisco has newer thinking for datacenters. Networks are becoming much more specialized, and the security thinking for different types of networks is significantly different.
- The Cisco three-tier model is derived from the Public Switched Telephone Network (PSTN) model, which is in use for much of the world's telephone infrastructure.

Continued...

- The Cisco Hierarchical Internetworking model, depicted in Figure 13-1, uses three main layers commonly referred to as the core, distribution, and access layers:
- **Core layer** Forms the network backbone and is focused on moving data as fast as possible between distribution layers. Because performance is the core layer's primary focus, it should not be used to perform CPU-intensive operations such as filtering, compressing, encrypting, or translating network addresses for traffic.
- **Distribution layer** Sits between the core and the access layer. This layer is used to aggregate access-layer traffic for transmission into and out of the core.
- **Access layer** Composed of the user networking connections. Filtering, compressing, encrypting, and address-translating operations should be performed at the access and distribution layers.

Continued...

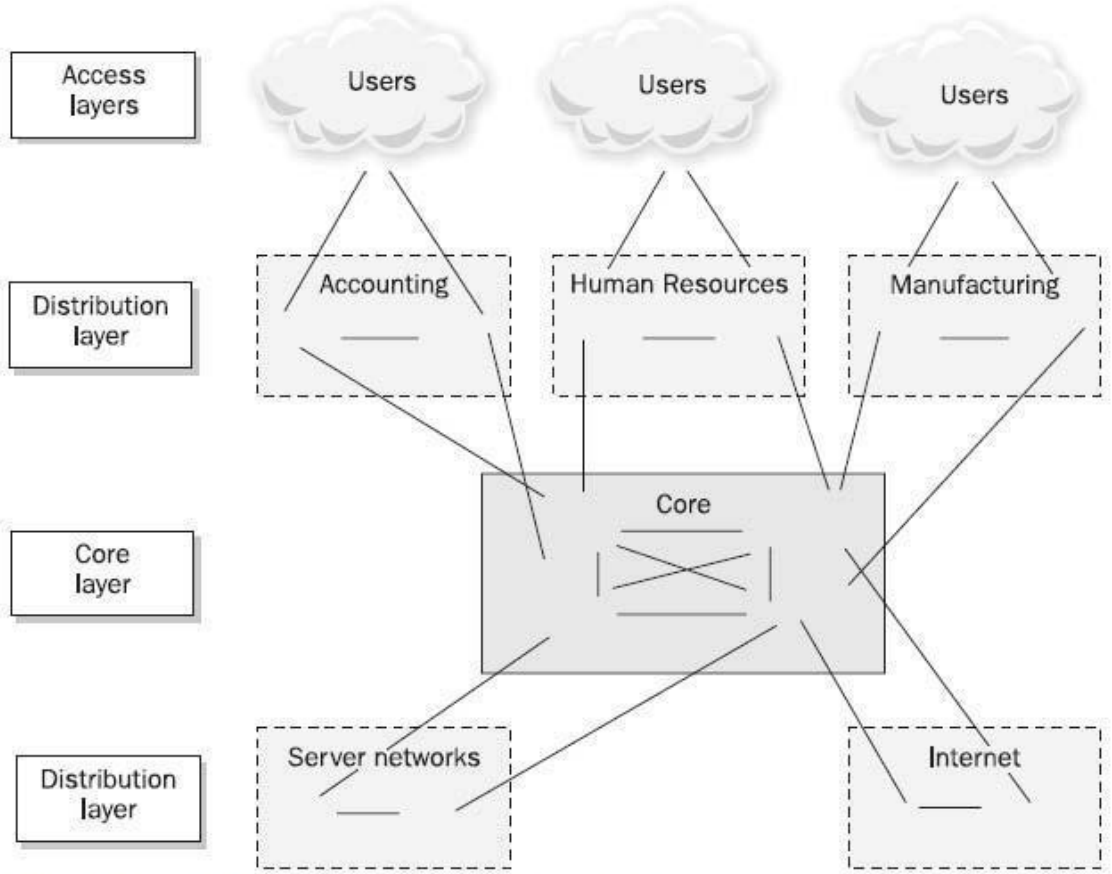


Figure 13-1 The Cisco Hierarchical Internetworking model

Continued...

- The Cisco model is highly scalable. As the network grows, additional distribution and access layers can be added seamlessly.
- As the need for faster connections and more bandwidth arises, the core and distribution equipment can be upgraded as required.
- This model also assists corporations in achieving higher levels of availability by allowing for the implementation of redundant hardware at the distribution and core layers. And because the network is highly segmented, a single network failure at the access or distribution layers does not affect the entire network.

Internal Security Practices

- Organizations that deploy firewalls strictly around the perimeter of their network leave themselves vulnerable to internally initiated attacks, which are statistically the most common threats today.

Continued...

- Internal controls, such as firewalls and early detection systems (IDS, IPS, and SIEM), should be located at strategic points within the internal network to provide additional security for particularly sensitive resources such as research networks, repositories containing intellectual property, and human resource and payroll databases.
- Dedicated internal firewalls, as well as the ability to place access control lists on internal network devices, can slow the spread of a virus. Figure 13-4 depicts a network utilizing internal firewalls.

Continued...

- When designing internal network zones, if there is no reason for two particular networks to communicate, explicitly configure the network to block traffic between those networks, and log any attempts that hosts make to communicate between them.
- With modern VoIP networks, this can be a challenge as VoIP streams are typically endpoint to endpoint, but consider only allowing the traffic you know to be legitimate between any two networks.
- A common technique used by hackers is to target an area of the network that is less secure, and then work their way in slowly via "jumping" from one part of the network to another.
- If all of the internal networks are wide open, there is little hope of detecting, much less preventing, this type of threat vector

Continued...

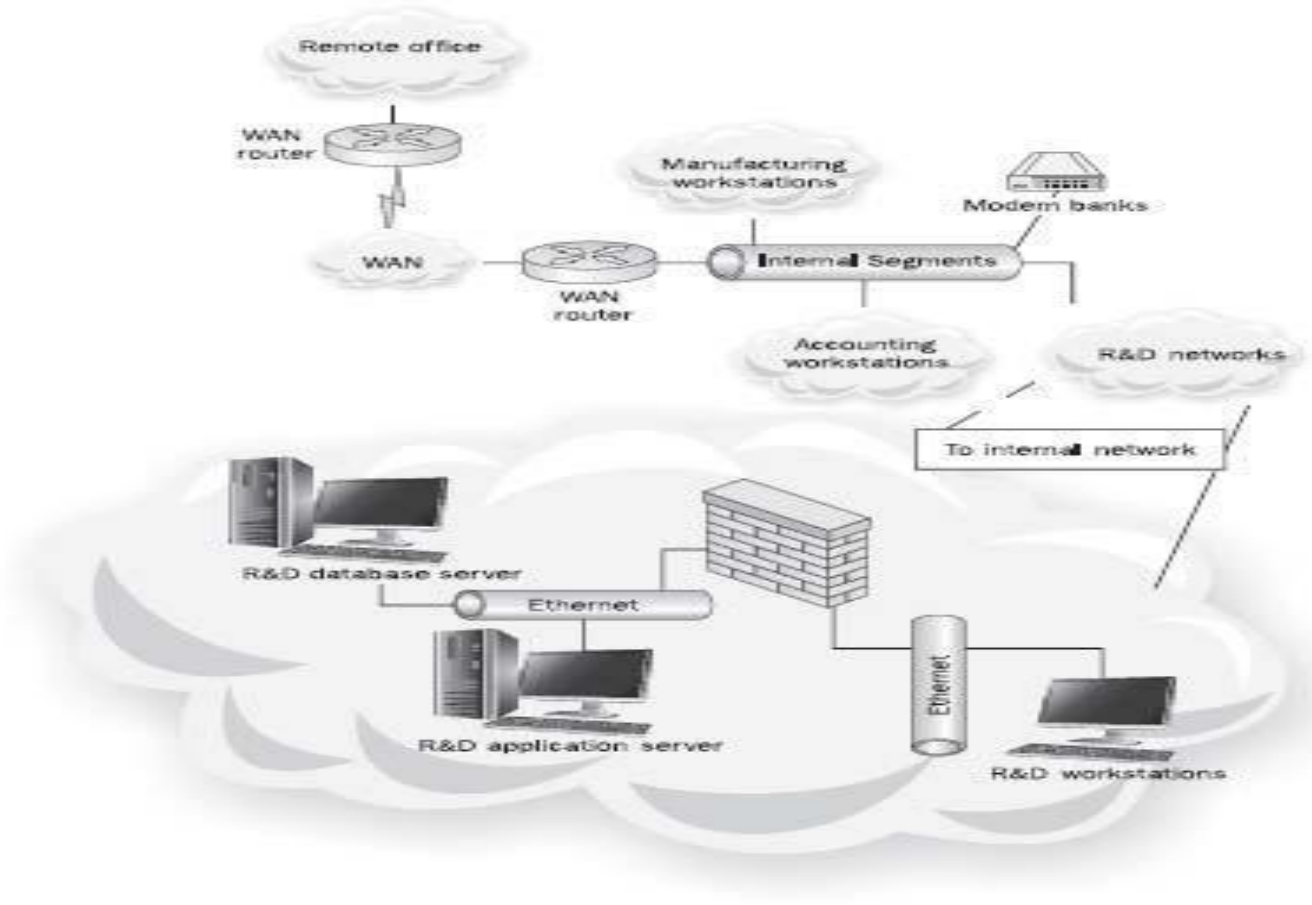


Figure 13-4 Internal firewalls can be used to increase internal security.

Continued...

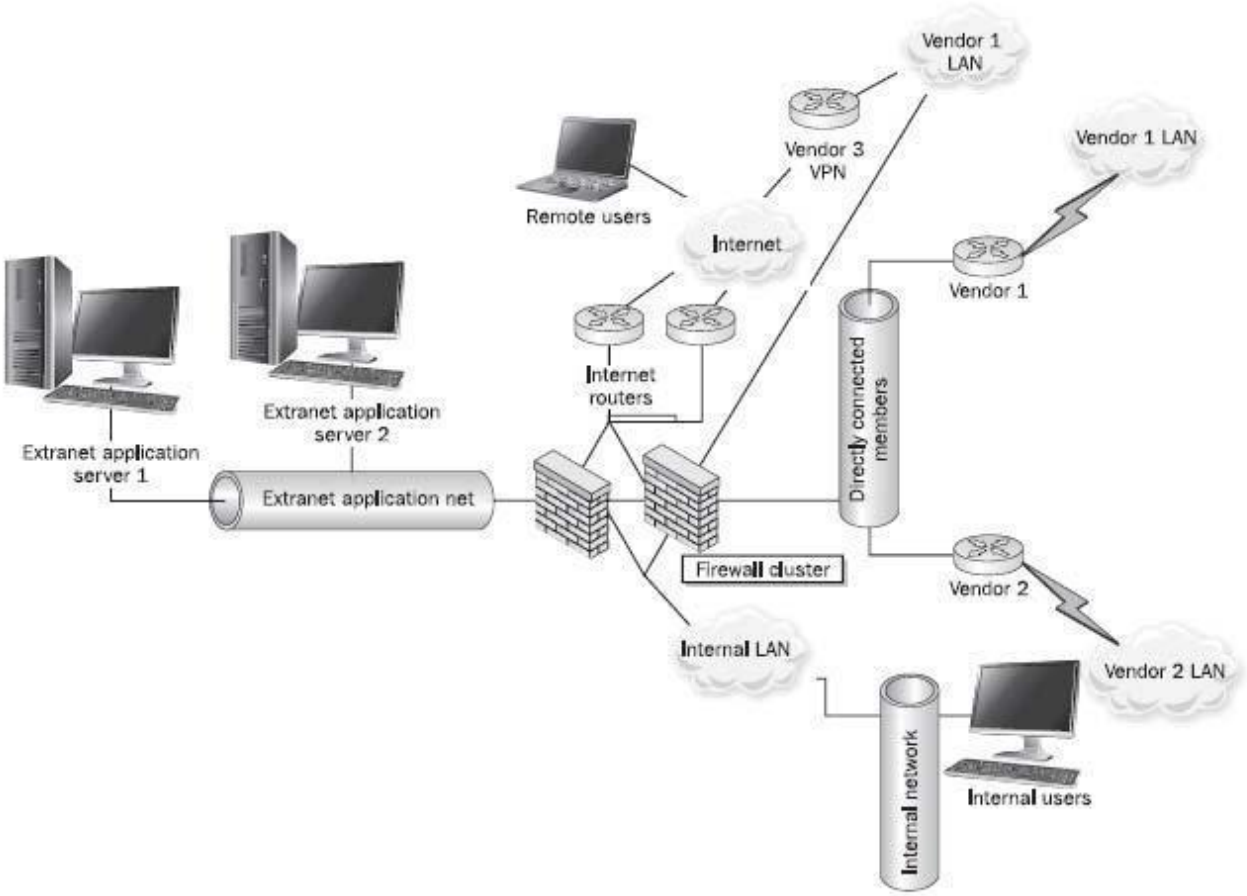


Figure 13-5 A possible extranet design

IPv4 and IPv6 Security

IP Security Overview

- The Internet community has developed application-specific security mechanisms in a number of areas, including electronic mail (S/MIME, PGP), client/server(Kerberos), Web access (SSL), and others. However, users have some security concerns that cut across protocol layers.
- For example, an enterprise can run a secure, private TCP/IP network by disallowing links to untrusted sites, encrypting packets that leave the premises, and authenticating packets that enter the premises.
- By implementing security at the IP level, an organization can ensure secure networking not only for applications that have security mechanisms but also for the many security-ignorant applications

Continued...

- In response to these issues, the Internet Architecture Board (IAB) included authentication and encryption as necessary security features in the next-generation IP, which has been issued as IPv6. Fortunately, these security capabilities were designed to be usable both with the current IPv4 and the future IPv6. This means that vendors can begin offering these features now, and many vendors do now have some IPsec capability in their products.
- IP-level security encompasses three functional areas: authentication, confidentiality, and key management.
- The **authentication mechanism** assures that a received packet was, in fact, transmitted by the party identified as the source in the packet header. In addition, this mechanism assures that the packet has not been altered in-transit

Continued...

- The **confidentiality facility** enables communicating nodes to encrypt messages to prevent eavesdropping by third parties.
- The **key management facility** is concerned with the secure exchange of keys. The current version of IPsec, known asIPsecv3, encompasses authentication and confidentiality. Key management is provided by the Internet Key Exchange standard, IKEv2.

Overview of IP security (IPsec)

- Internet Protocol Security (IPsec) is a network protocol, that authenticates and encrypts the packets of data sent over a network.
- IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session.

Continued...

- IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).
- Internet Protocol security (IPsec) uses cryptographic security services to protect communications over Internet Protocol (IP) networks.
- IPsec supports network-level peer authentication, data-origin authentication, data integrity, and data confidentiality (encryption), and replay protection.

Continued...

The IPsec suite is an open standard. IPsec uses the following protocols to perform various functions:

- **Authentication Headers** (AH) provides connectionless data integrity and data origin authentication for IP datagrams and provides protection against replay attacks.
- **Encapsulating Security Payloads** (ESP) provides confidentiality, data-origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic-flow confidentiality.
- **Security Associations (SA)** provides the bundle of algorithms and data that provide the parameters necessary for AH and/or ESP operations. The Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for authentication and key exchange

APPLICATIONS OF IPSEC

- IPsec provides the capability to secure communications across a LAN, across private and public WANs, and across the Internet. Examples of its use include the following:
- Secure branch office connectivity over the Internet: A company can build a secure virtual private network over the Internet or over a public WAN. This enables a business to rely heavily on the Internet and reduce its need for private networks, saving costs and network management overhead.
- Secure remote access over the Internet: An end user whose system is equipped with IP security protocols can make a local call to an Internet service provider and gain secure access to a company network. This reduces the cost of toll charges for traveling employees and telecommuters.

Continued...

- Establishing extranet and intranet connectivity with partners: IPsec can be used to secure communication with other organizations, ensuring authentication and confidentiality and providing a key exchange mechanism.
- Enhancing electronic commerce security: Even though some Web and electronic commerce applications have built-in security protocols, the use of IPsec enhances that security

HOST Security

Authentication

- Authentication is the process of reliably verifying the identity of someone (or something). There are lots of examples of authentication in human interaction.

1. we recognize each others' faces when we meet.

2. we recognize each others' voices on the telephone.

3. we are authenticated by the customs official who checks us against the picture on our passport.

4. A guard might authenticate you by comparing you with the picture on your badge.

5. A mail order company might accept as authentication the fact that you know the expiration date on your credit card

Continued...

Creating a good quality password policy

- The security provided by a password system depends on the passwords being kept secret at all times. Thus, a password is vulnerable to compromise whenever it is used, stored, or even known.
- A password must be initially assigned to a user when enrolled on the system.
- A user's password must be changed periodically.
- The system must maintain a “password database”.
- Users must remember their passwords.
- Users must enter their passwords into the system at authentication time.
- Employees may not disclose their passwords to anyone. This includes administrators and IT managers.

Continued...

- **Authentication Identification** Sometimes also require that the computer verify its identity with the users, based on three methods:
- what you know (eg., passwords)
- what you have (eg., keycards)
- what you are (eg., biometric information) Verification
- Validation of information supplied against a table of possible values based on users claimed identity, Verify identity based on your physical characteristics, known as biometrics.

Continued...

Characteristics used include:

- **Signature**
- **Fingerprint, hand geometry**
- **face or body profile**
- **Speech, retina pattern**
- How authentication is done depends on capabilities of entity being authenticated.

Two most important capabilities:

- ability to store a high-quality key.
- ability to perform cryptographic operations

Continued…

High Quality Authentication

- Secret
- Chosen from large space
- Computationally infeasible to guess

Computer vs. Person

- Computer has both.
- Person has neither

Continued...

Types of Authentication

1. **Password-based authentication**

- Authenticating oneself by showing a secret password to the remote peer (and to the network).
- Always vulnerable to eavesdropping attack. Usually protection: limit frequency of incorrect password entries.

2. **Address-based authentication**

- Authenticating oneself by using a physically-secured terminal/computer. Conceptually similar to password-based authentication.

Continued...

3. **Cryptography-based authentication**

- Authenticating oneself by showing evidence of a secret key to the remote peer (and to the network) but without exposing the secret to the peer (or to the network).Secret key can be obtained from a password.

Problems with Passwords

- Eavesdropping
- On-line guessing of password
- Off-line cracking
- Security of password file

Continued...

1. **Eavesdropping**

- Passwords must be uttered to be used.
- Most people don't watch.
- But they are not the people you are worried about.
- Wiretapping is a more sophisticated problem.
- If the password is sent from across a network then eavesdropping is possible.
- For example, a traditional telnet connection is unsecured – no cryptography. so an attacker who can eavesdrop, eg., on the port in use, simply gets to see the password

2. Trojan Horses

- A Trojan horse is a useful, or apparently useful, program, which also performs unwanted/harmful functions.
- If a user can be induced to run a Trojan horse which mimics the log in program then the Trojan can capture the user's password.
- The password can then be sent to the author of the Trojan

3. On-Line Guessing

- I can impersonate you if I can guess your password.
- Some systems enforce easily guessable passwords (not really a good idea, but some do it – would be better to disallow).
- Some people use easily guessable passwords.
- With enough guesses even obscure passwords can be guessed.
- Executing users who get their password wrong would probably be unacceptable.
- Can make sure that guesses have to be typed

Continued...

4. Locking Accounts

- Can lock accounts after too many failed attempts.
- But then easy for someone to deny access.
- Can cut-off connection after a number of failed attempts and require it to be re-established.
- Can have system response be very slow.

5. Off Line Password Guessing

- Passwords more vulnerable if off-line guessing possible.
- Off line attack - an intruder captures a quantity that is derived from password.
- Attacker then takes their time trying to compute password

Thank You!