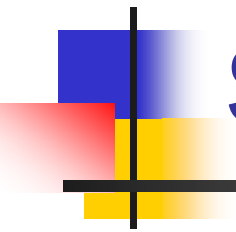


INTRUSION DETECTION SYSTEMS and Network Security

Intrusion Detection System IDS

- A layered network security approach starts with :
  - A well – secured system which starts with:
    - Up-to-date application and OS patches
    - Well-chosen passwords
    - Minimum number of services running
    - Restricted access to available services
  - On top of that, we can add layers of protective measures such as :
    - Antivirus products
    - Firewalls
    - Sniffers
    - IDSs

Intrusion Detection System IDS

- Similar to a burglar alarm in physical world
- Main purpose:
  - To identify suspicious or malicious activity
  - Note activity that deviates from normal behavior .
  - Catalog or classify the activity
  - And if possible, respond to the activity

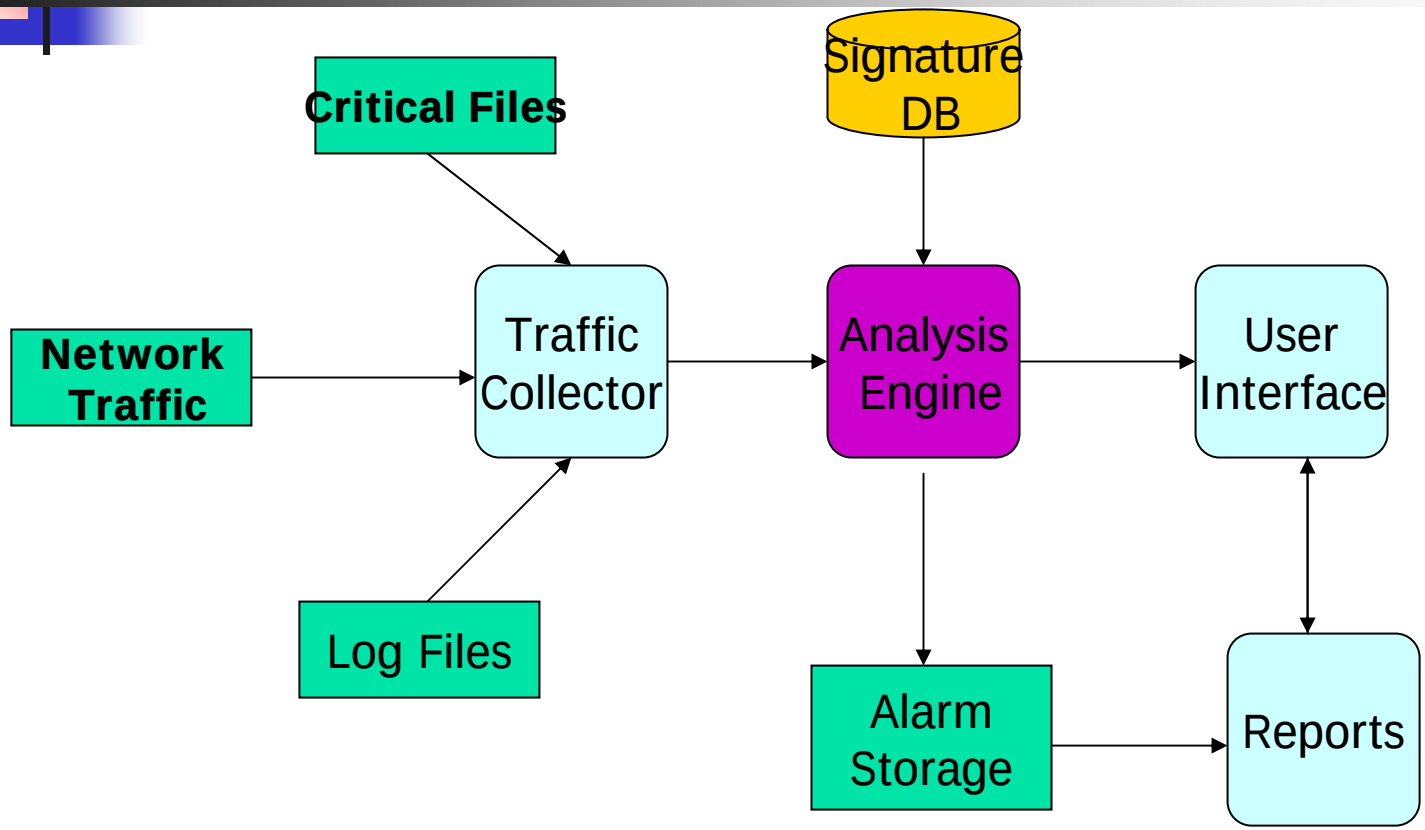
Brief History of IDS

- Originated in DOD (like the Internet)
- Anderson in 1980 published a paper on that topic
- 1986 IDES (Intrusion Detection Expert system) paper
- 1987 Denning published the ID Model paper
- 1989 the first commercial IDS product “Stalker” was introduced
- 1995 the first network-based IDS

Two main Categories of IDSs

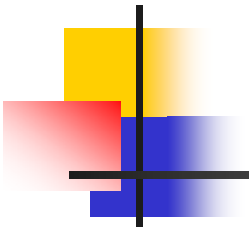
- Host-based IDSs
  - Examines activity on an individual system such as a PC, web server or mail server.
- Network-Based IDSs
  - Examines activity on the network itself.

Typical Logical Components of an IDS



Logical Components of IDS

- Traffic Collector : when host-based this includes:
  - Log files
  - Audit logs
  - Traffic coming in and going out (sniffer)
- Analysis Engine : this is the brains of the IDS
- Signature DB : collection of patterns and definitions of known suspicious or malicious activity
- User Interface and Reporting



IDS Tuning

- Most IDSs may be “tuned” to fit a particular environment.
- E.g.
  - Certain signatures can be turned off
  - The severity of the alarm can be adjusted
  - Exclude certain patterns of activity from specific hosts

Intrusion-Detection Systems

- Devices that establish and maintain network security
- Active IDS (or reactive IDS) performs a specific function when it senses an attack, such as dropping packets or tracing the attack back to a source
  - Installed on the server or, in some instances, on all computers on the network
- Passive IDS sends information about what happened, but does not take action

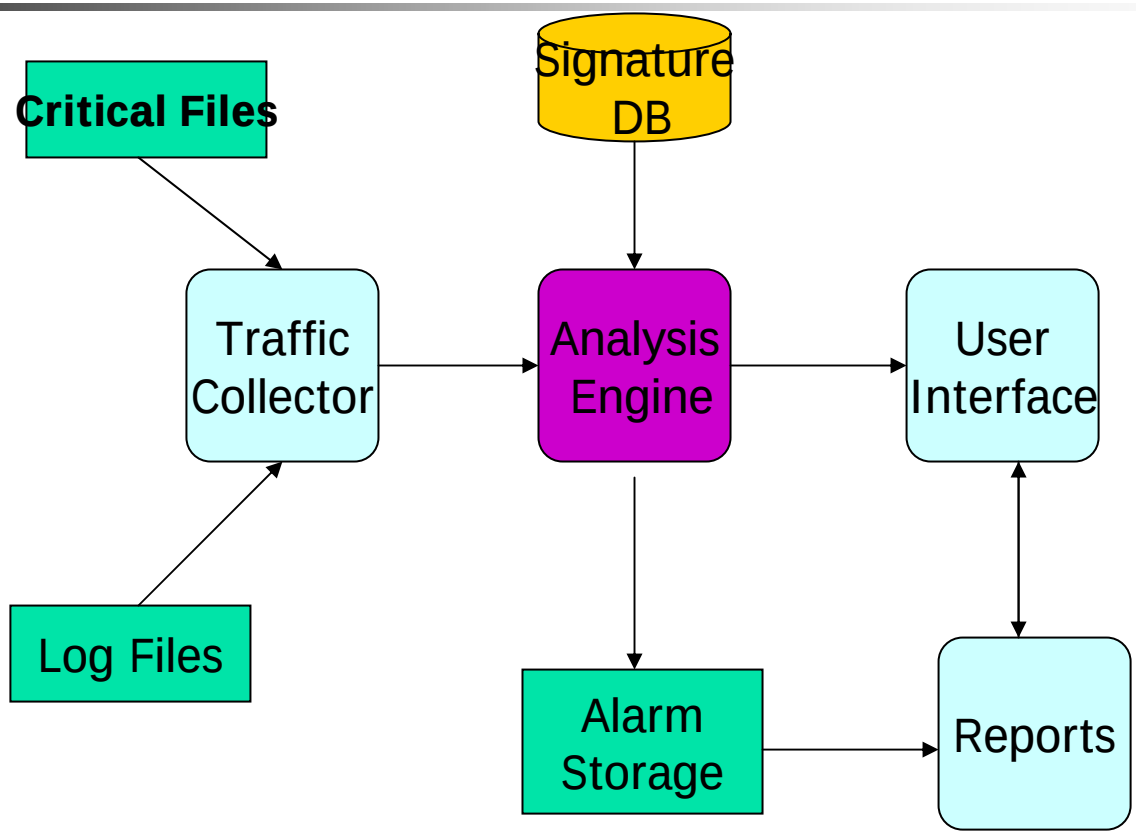
Intrusion-Detection Systems (IDSs) (cont.)

- Host-based IDS monitors critical operating system files and computer's processor activity and memory; scans event logs for signs of suspicious activity
- Network-based IDS monitors all network traffic instead of only the activity on a computer
  - Typically located just behind the firewall
- Other IDS systems are based on behavior:
  - Watch network activity and report abnormal behavior
  - Result in many false alarms

Host-Based IDSs (HIDS)

- HIDS is a system that examines log files, audit trails, and network traffic coming into or leaving a specific host.
- HIDS can operate in:
  - Real time
  - Batch mode looking for activity on a periodic basis

Typical Logical Components of HIDS

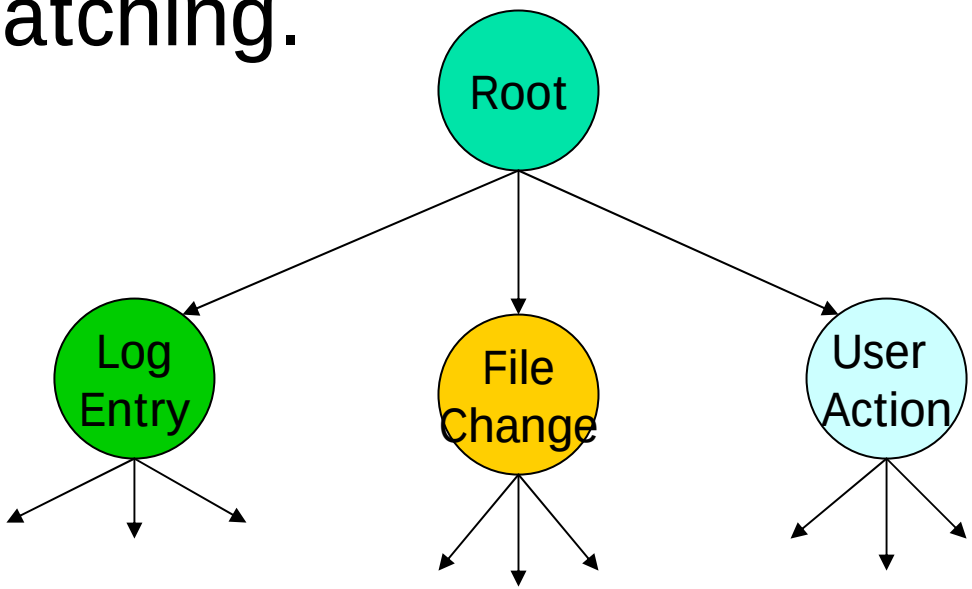


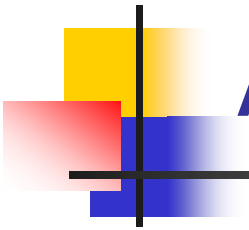
Host-Based IDSs

- Within the log files, the IDS is looking for activities that typify hostile actions or misuse such as:
  - Logins at odd hours
  - Login authentication failures
  - Adding new user accounts
  - Modification or access of critical system files
  - Modification or removal of binary files (exe's)
  - Starting or stopping processes
  - Privilege escalation
  - Use of certain programs

The Analysis Engine

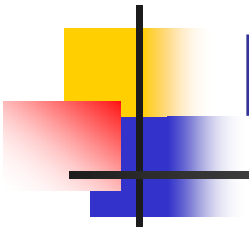
- Most IDSs include a decision tree in the analysis engine to expedite pattern matching.





Advantages of HIDS

- They can be very OS-specific and have more have more detailed signatures
- They can reduce false positive rates
- They can examine data after it has been decrypted
- They can be very application specific
- They can determine whether or not an alarm may impact that specific system



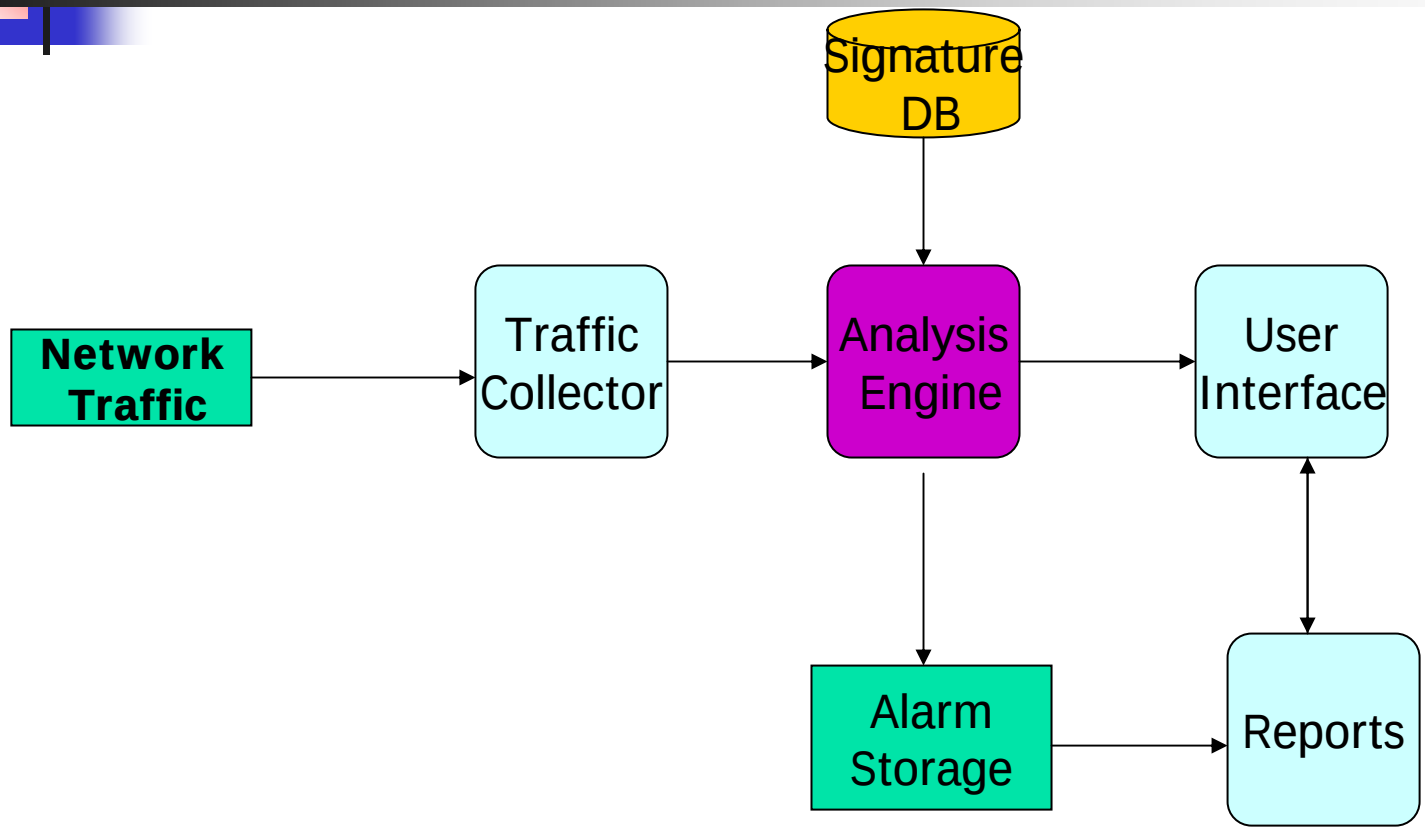
Disadvantages of HIDS

- The IDSs must have a process on every system to be watched
- High cost of ownership and maintenance
- Uses local system resources
- Has very focused view and cannot relate to activity around it
- If logged locally, could be compromised or disabled

Network-Based IDSs (NIDS)

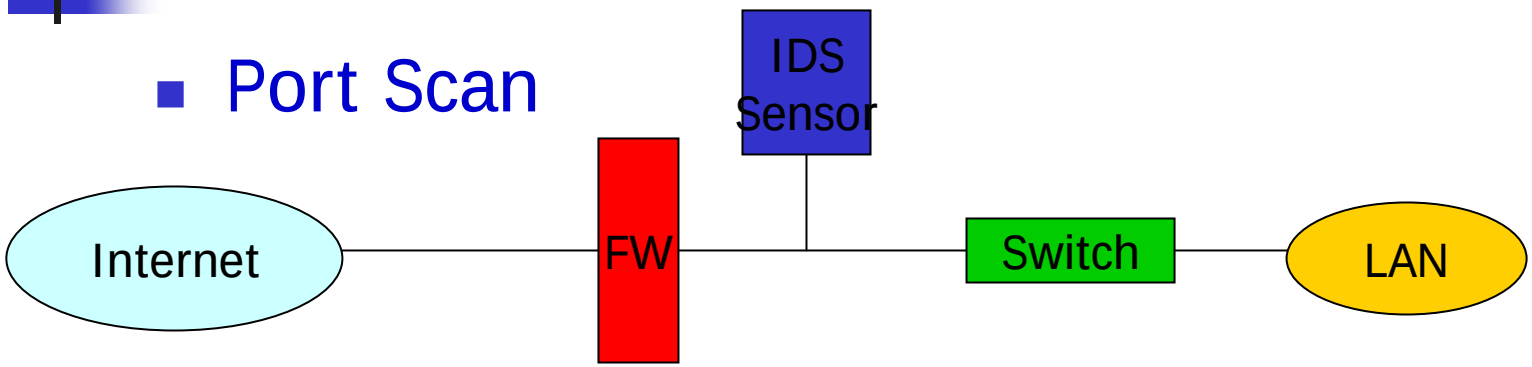
- Integrated well into the concept of “Perimeter Security”
- The network traffic collector behaves as a network traffic sniffer (attaches itself to a NIC in promiscuous mode)
- The patterns and signatures being matched are *far more complicated* than Host-based signatures
- *The NIDS signatures DB is usually much larger than HIDS DB; and the signatures themselves are much larger*

Typical Logical Components of NIDS



Examples on the Operation of NIDS

- Port Scan



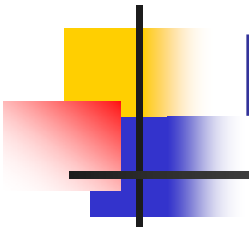
  - The pattern of attempting to connect to different services on different systems will be noticed. The IDS compares that pattern to the signatures database, and finds that it matches the Port Scanning signature, and it will generate an alarm.
- Ping of Death : IDS looks for ICMP packets that are above a certain size.

Network-Based IDSs

- They look for hostile activities that typify hostile actions or misuse such as:
  - Denial of service attacks
  - Port scans or sweeps
  - Malicious content in the data payload of a packet
  - Vulnerability scanning
  - Trojans, viruses, or worms
  - Tunneling
  - Brute force attacks

Advantages of NIDS

- It takes fewer systems to provide IDS coverage
- Deployment, maintenance, and upgrade costs are usually lower
- NIDS has visibility into network traffiv and can correlate attacks among multiple systems.

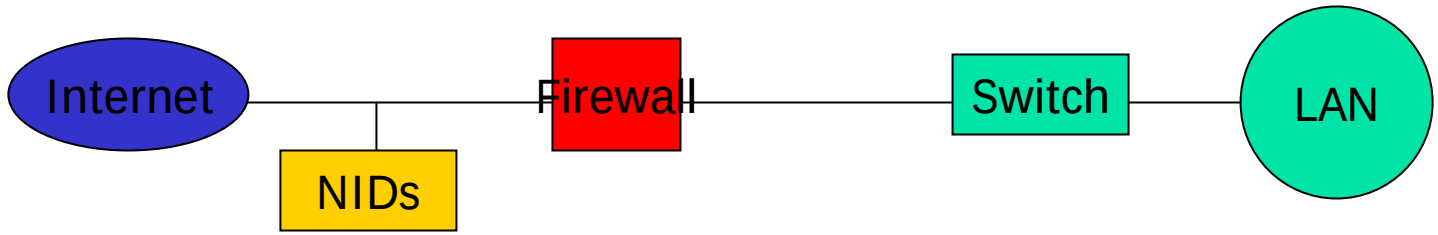


Disadvantages of NIDS

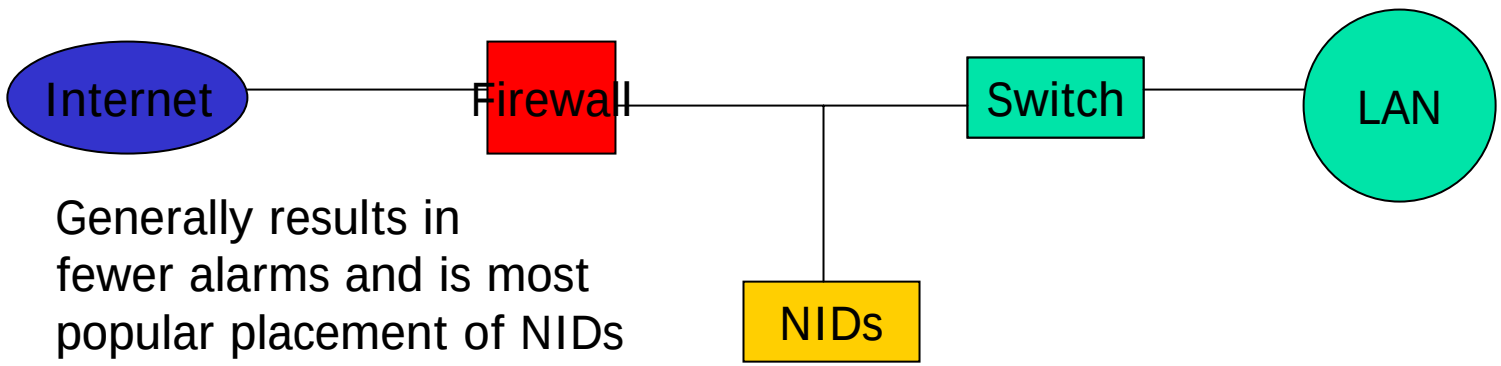
- Ineffective when traffic is encrypted
- It cannot see traffic that does not cross it (i.e. the link it is on)
- It must be able to handle high volumes of traffic. (Data rates used to be 10Mbps , now rates are 100Mbps)
- It doesn’t know about the activity on the hosts.

Positioning NIDs

- NIDs sensor placed in front of Firewall



- NIDs sensor placed behind Firewall



Generally results in fewer alarms and is most popular placement of NIDs

IDS Products

Product	Vendor
Cisco IDS	CISCO
SecureNet, SecureHost	Intrusion Inc.
eTrust	Computer Associates
RealSecure	Internet Security Services
Snort	Snort (Free open source)

IDS Models

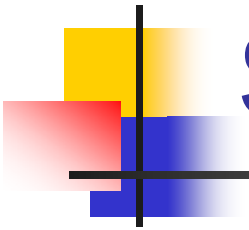
- IDSs are often classified according to the detection model they use:
  - Anomaly detection model . This is the more complicated type. In this model the IDs must know what “normal” behavior on the host or network being protected really is. Once the normal behavior baseline is established, the IDS can then go to work identifying deviations from this norm, which are further scrutinized to determine if that activity is malicious.
  - A misuse detection model is the simpler and more popular model. The IDS looks for activity that violates specific policies.

Network Monitoring and Diagnostic Devices

- SNMP (Simple Network Management Protocol) enables network administrators to:
  - Monitor network performance
  - Find and solve network problems
  - Plan for network growth
- Managed device:
  - Network device that contains an SNMP agent
  - Collects and stores management information and makes it available to SNMP

Designing Network Topologies

- Topology: physical layout of the network devices, how they are interconnected, and how they communicate
- Essential to establishing its security
- Although network topologies can be modified for security reasons, the network still must reflect the needs of the organization and users



Security Zones

- One of the keys to mapping the topology of a network is to separate secure users from outsiders through:
  - Demilitarized Zones (DMZs)
  - Intranets
  - Extranets

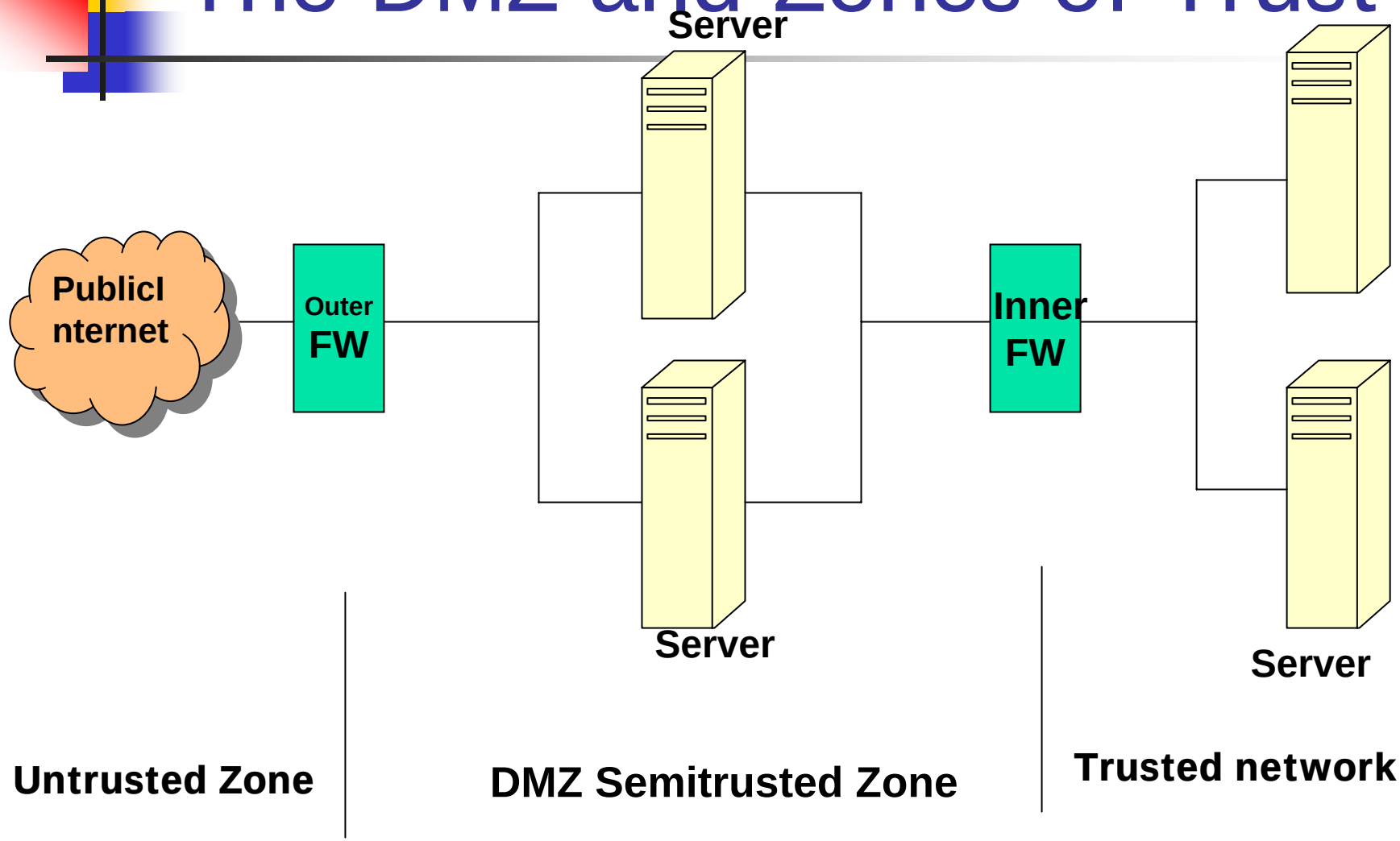
Demilitarized Zone (DMZ)

- A DMZ in a computer network is used in the same way as in a military environment...the ground separating two opposing forces.
- It acts as a buffer zone between the Internet, where no controls exist, and the inner secure network.
- To demarcate the zones and enforce separation, a firewall is placed on each side of the DMZ.
- The area between these firewalls is accessible from either the inner, secure, network or the Internet.
- The firewalls are specifically designed to prevent access across the DMZ directly, from the Internet to the inner network.

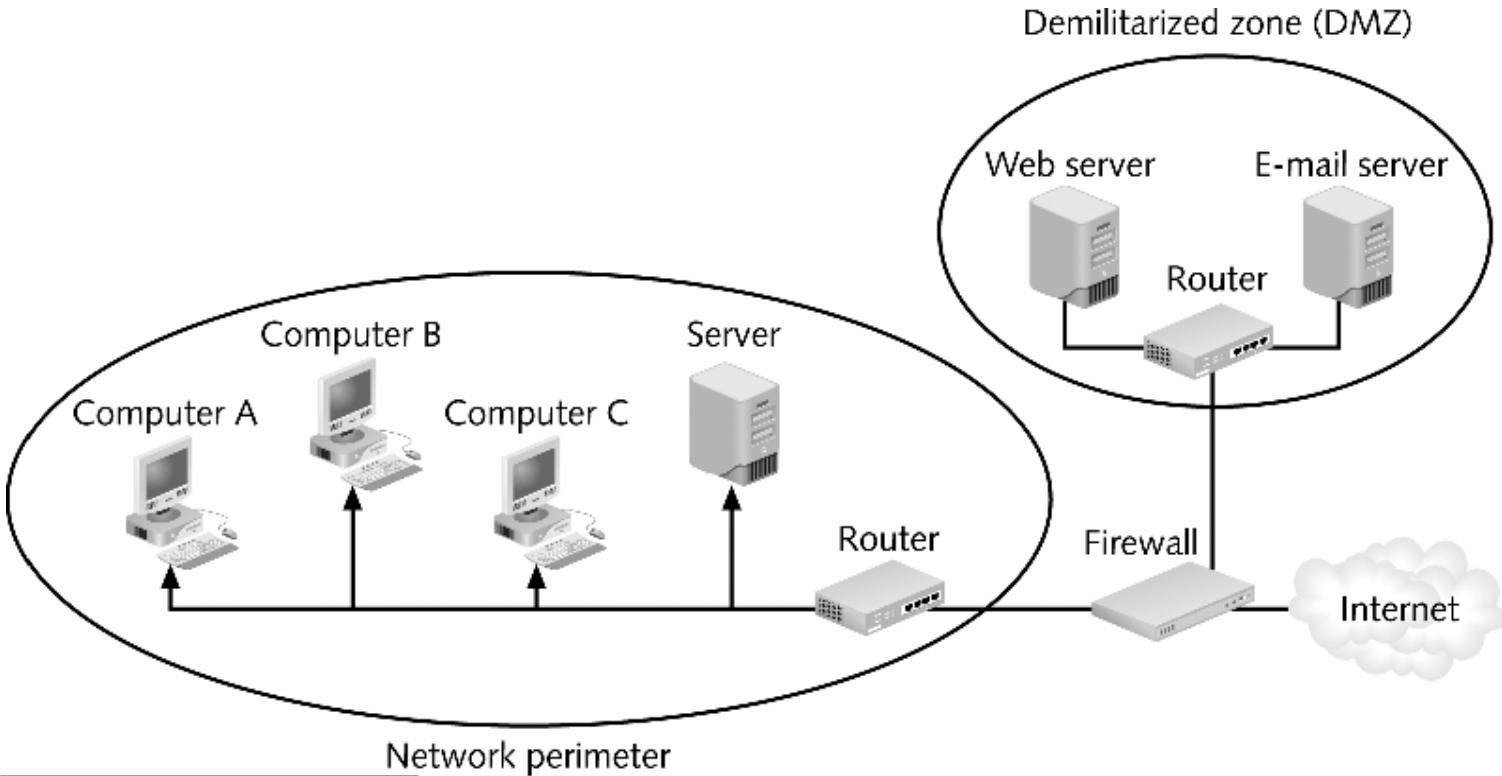
Demilitarized Zones (DMZs)

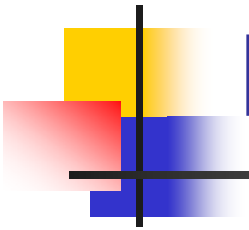
- Separate networks that sit outside the secure network perimeter
- Outside users can access the DMZ, but cannot enter the secure network
- For extra security, some networks use a DMZ with two firewalls
- The types of servers that should be located in the DMZ include:
  - Web servers
  - E-mail servers
  - Remote access servers
  - FTP servers

The DMZ and Zones of Trust



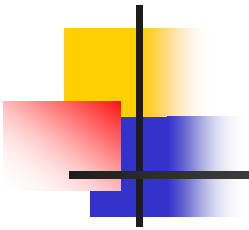
Demilitarized Zones (DMZs) (cont.)





DMZ

- Special attention should be paid to the security settings of network devices placed in the DMZ, and they should be considered to be compromised to unauthorized use.
- The machines in the DMZ should have *hardened operating systems* (machines with some locked up functionality to preserve security)
- Many types of servers belong to this area, including web servers that are serving content to Internet users, as well as remote access servers, and external e-mail servers.
- In general any server accessed from the outside, untrusted Internet zone needs to be in the DMZ.
- All other servers like domain name servers, database servers, application servers should not be accessible from the outside. Also the routers and switches that connect these machines together.



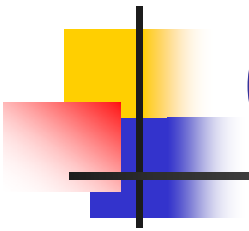
Intranets

- Networks that use the same protocols as the public Internet, but are only accessible to trusted inside users
- Disadvantage is that it does not allow remote trusted users access to information

Extranets

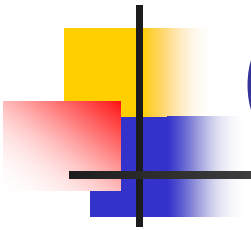
- Sometimes called a cross between the Internet and an intranet
- Accessible to users that are not trusted internal users, but trusted external users
- Not accessible to the general public, but allows vendors and business partners to access a company Web site

Network Address Translation (NAT)

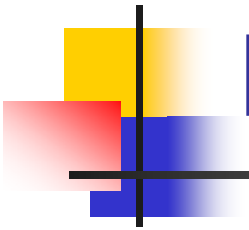


- “You cannot attack what you do not see” is the philosophy behind Network Address Translation (NAT) systems
- Hides the IP addresses of network devices from attackers
- Computers are assigned special IP addresses (known as private addresses)

Network Address Translation (NAT) (cont.)



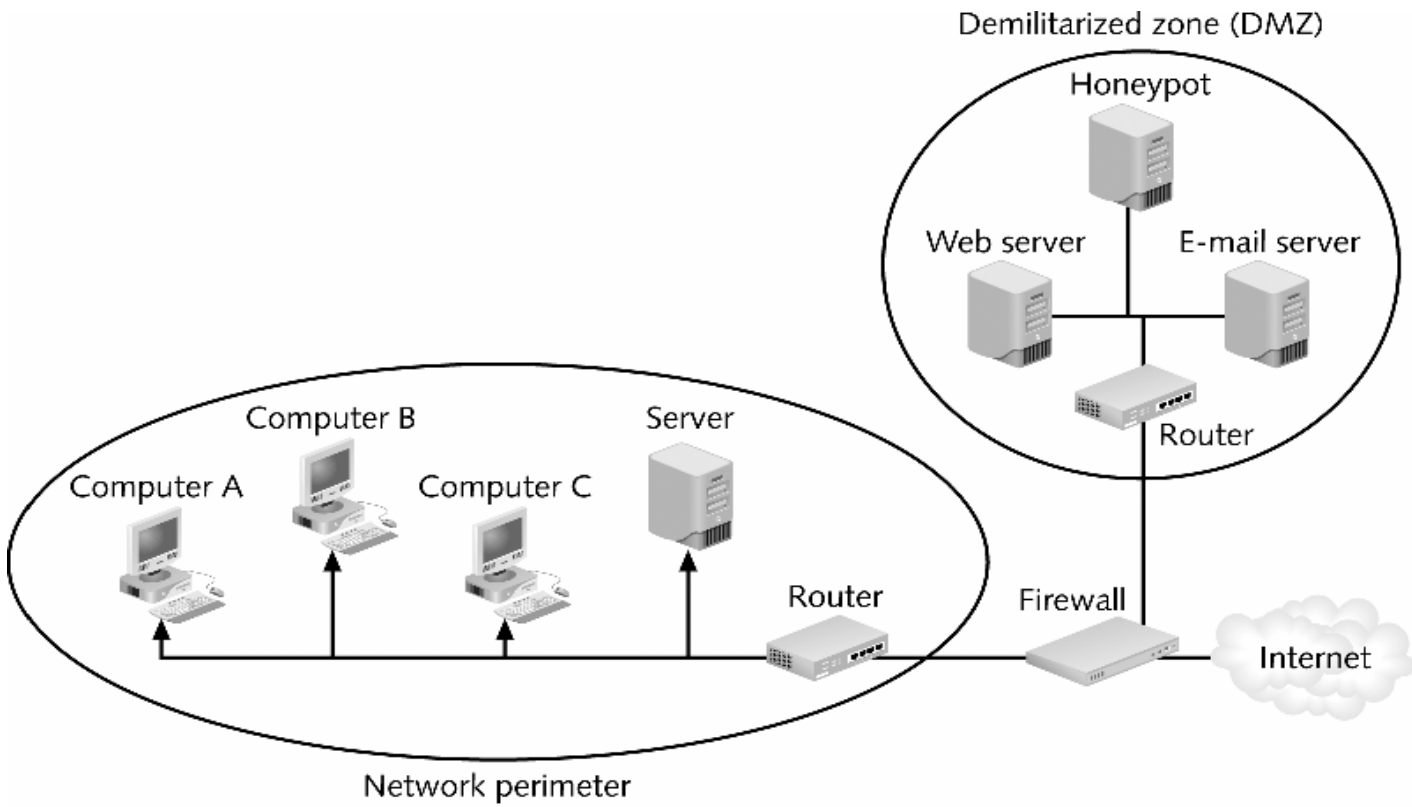
- These IP addresses are not assigned to any specific user or organization; anyone can use them on their own private internal network
- Port address translation (PAT) is a variation of NAT
- Each packet is given the same IP address, but a different TCP port number



Honeypots

- Computers located in a DMZ loaded with software and data files that appear to be authentic
- Usually a machine dedicated to this purpose
- Intended to trap or trick attackers
- Provides early warning of attacks
- Two-fold purpose:
  - To direct attacker's attention away from real servers on the network
  - To examine techniques used by attackers

Honeypots (cont.)

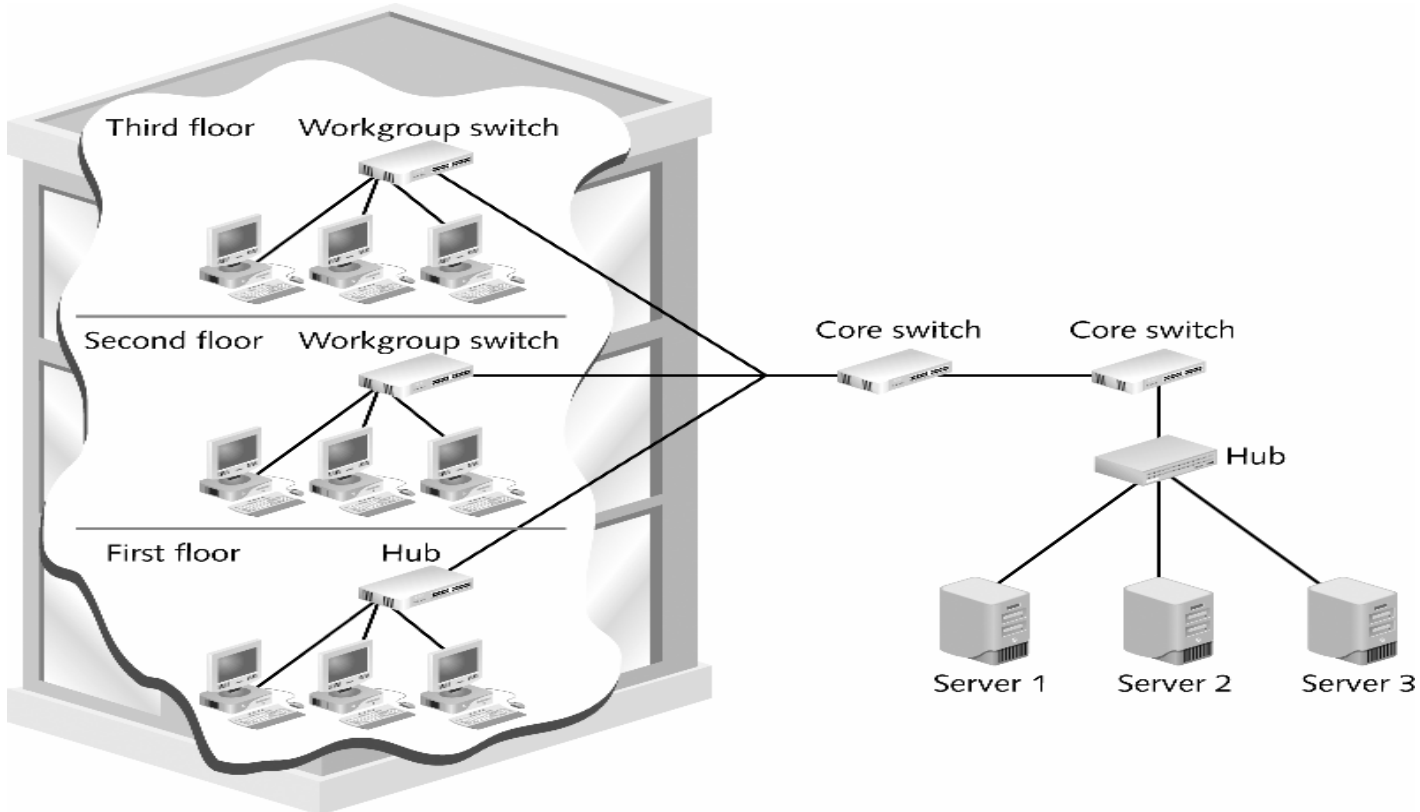


Honeypots

Virtual LANs (VLANs)

- Segment a network with switches to divide the network into a hierarchy
- Core switches reside at the top of the hierarchy and carry traffic between switches
- Workgroup switches are connected directly to the devices on the network
- Core switches must work faster than workgroup switches because core switches must handle the traffic of several workgroup switches

Virtual LANs (VLANs) (cont.)



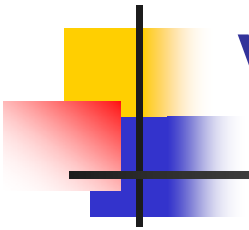
VLAN

Virtual LANs (VLANs) (cont.)

- Segment a network by grouping similar users together
- Instead of segmenting by user, you can segment a network by separating devices into logical groups (known as creating a VLAN)

Virtual Private Networks VPN

- VPN is a technology that is gaining popularity among large organizations that use the global Internet both both intera- and interorganization communication, but require privacy in their communications.
- VPN uses IPsec in the tunnel mode to provide authentication, integrity, and privacy.

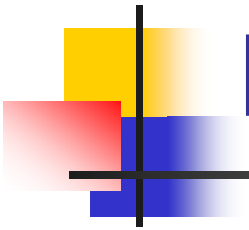


VPN

- Takes advantage of using the public Internet as if it were a private network
- Allow the public Internet to be used privately
- Prior to VPNs, organizations were forced to lease expensive data connections from private carriers so employees could remotely connect to the organization’s network (Private Networks)

VPN (cont.)

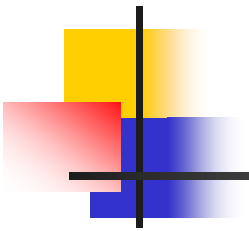
- What if a company has more than one office?
- And they are far apart?
  - Like on the opposite coasts of the US
- How can you have a secure cooperation between them?



Leased Line Solution

- Lease private lines from some telephone company
- The phone company ensures that your lines cannot be tapped
  - To the extent you trust in phone company security
- Can be expensive and limiting

Another Solution via the Internet



- Communicate via the Internet
  - Getting full connectivity, bandwidth, reliability, etc..
  - At a lower price, too
- But how do you keep the traffic secure?
- Use IPsec in the Tunneling mode

VPNs (cont.)

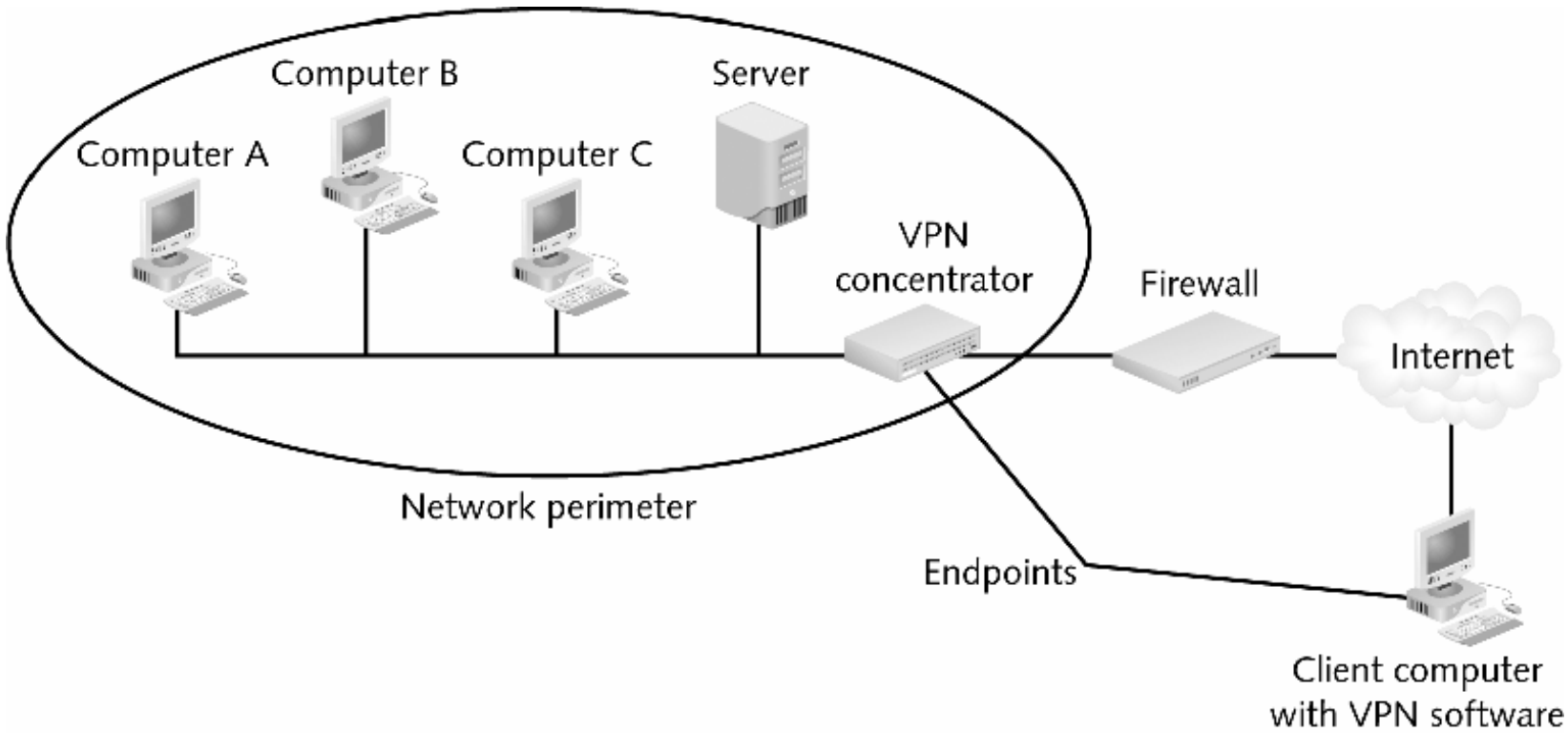
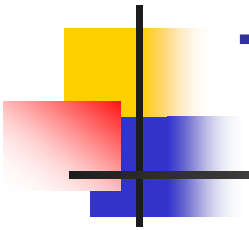


Figure Virtual private network



Tunneling

- To guarantee privacy and other security measures for an organization, VPN uses IPsec in the tunnel mode.
- In this mode, each datagram destined for private use in the organization is encapsulated in another datagram.
- To use IPsec in ***tunneling,*** the VPNs need two sets of addresses.
- The public network is responsible for carrying the packet from R1 to R2. Outsiders cannot decipher the contents of the packet or the source or destination addresses.
- Deciphering takes place at R2, which finds the destination address of the packet and delivers it.

Addressing In a VPN