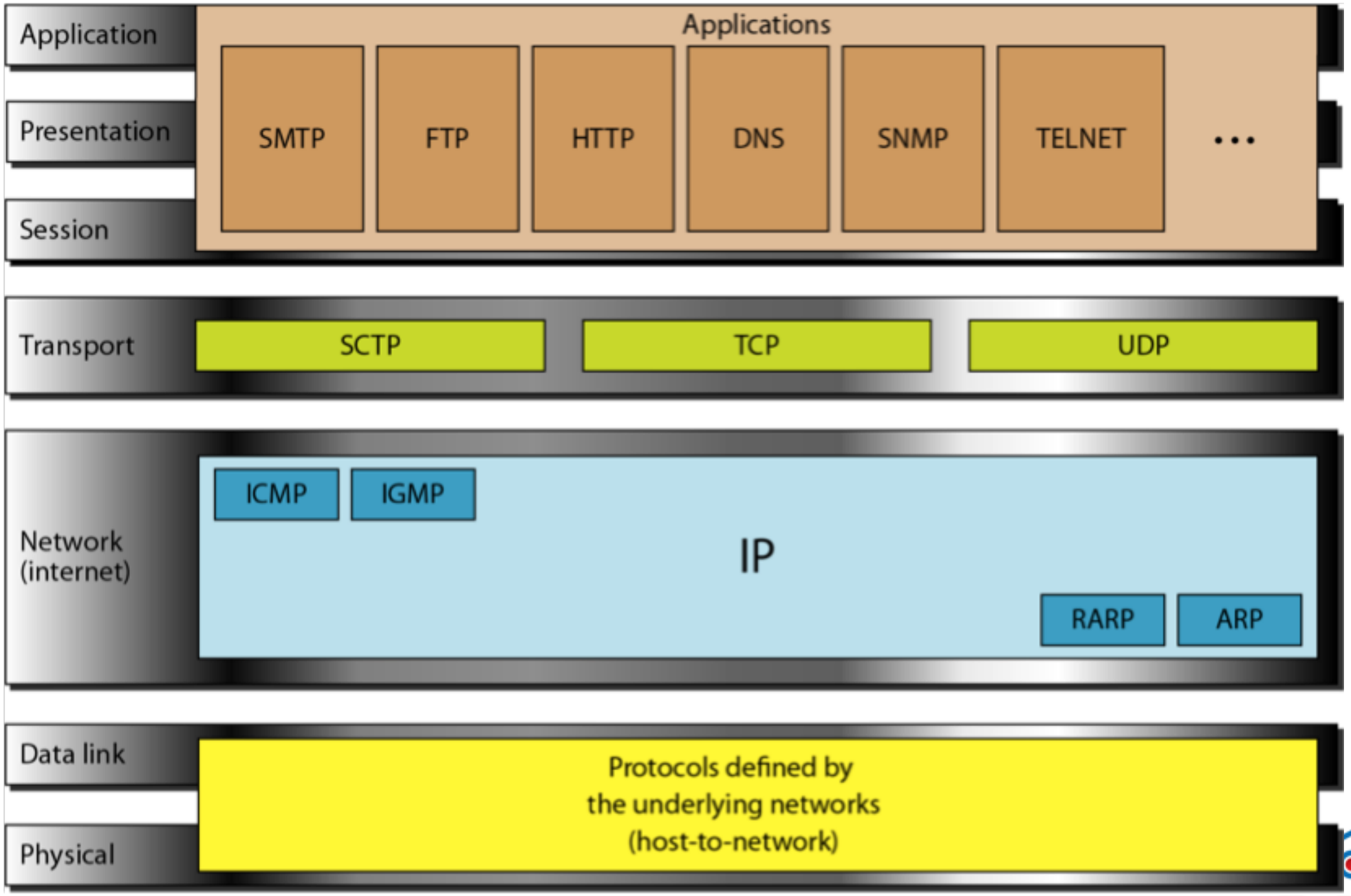
Network Security

Kitisak Jirawannakool

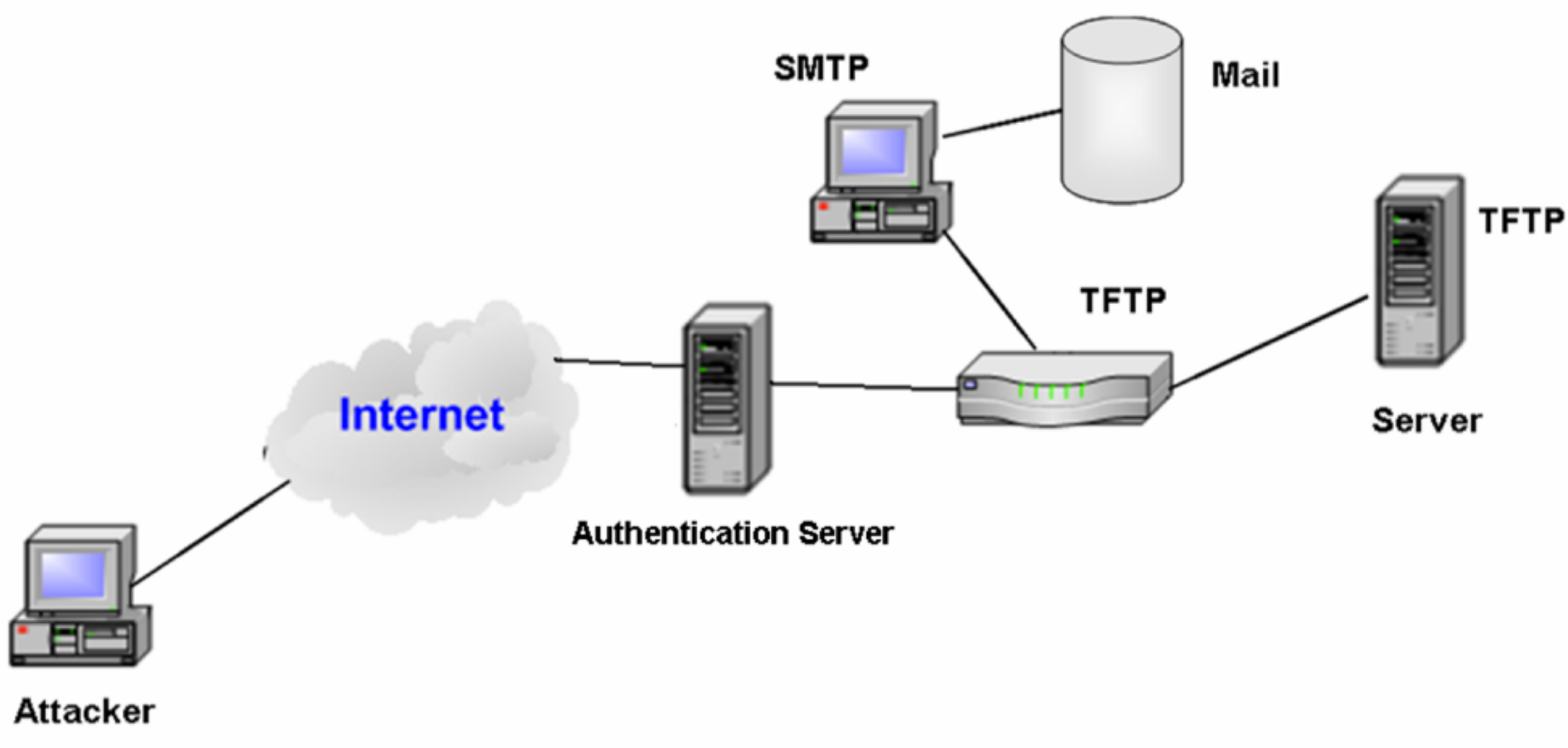
Electronics Government Agency
(public organisation)

A Brief History of the World

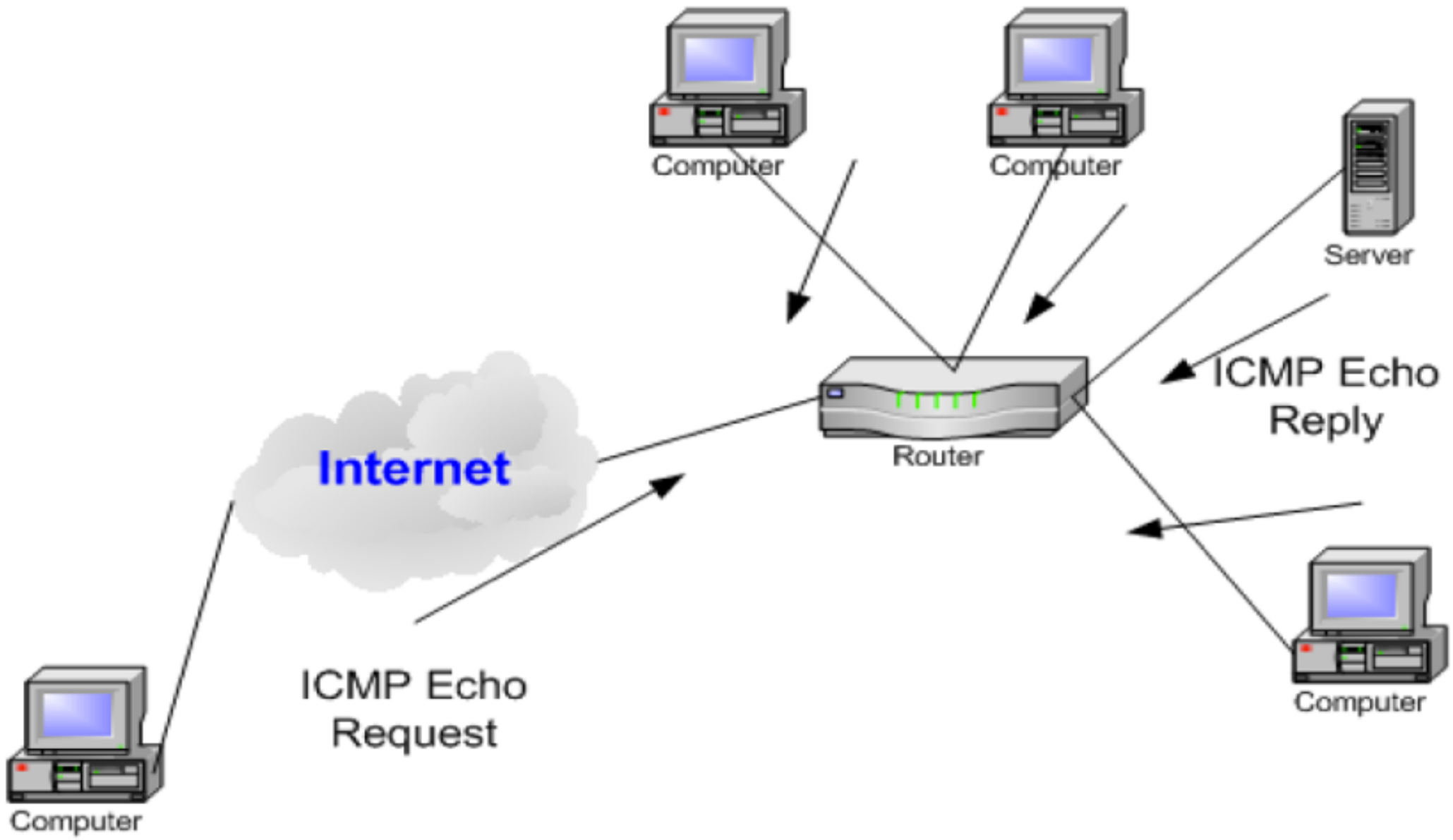
OSI Model vs TCP/IP suite



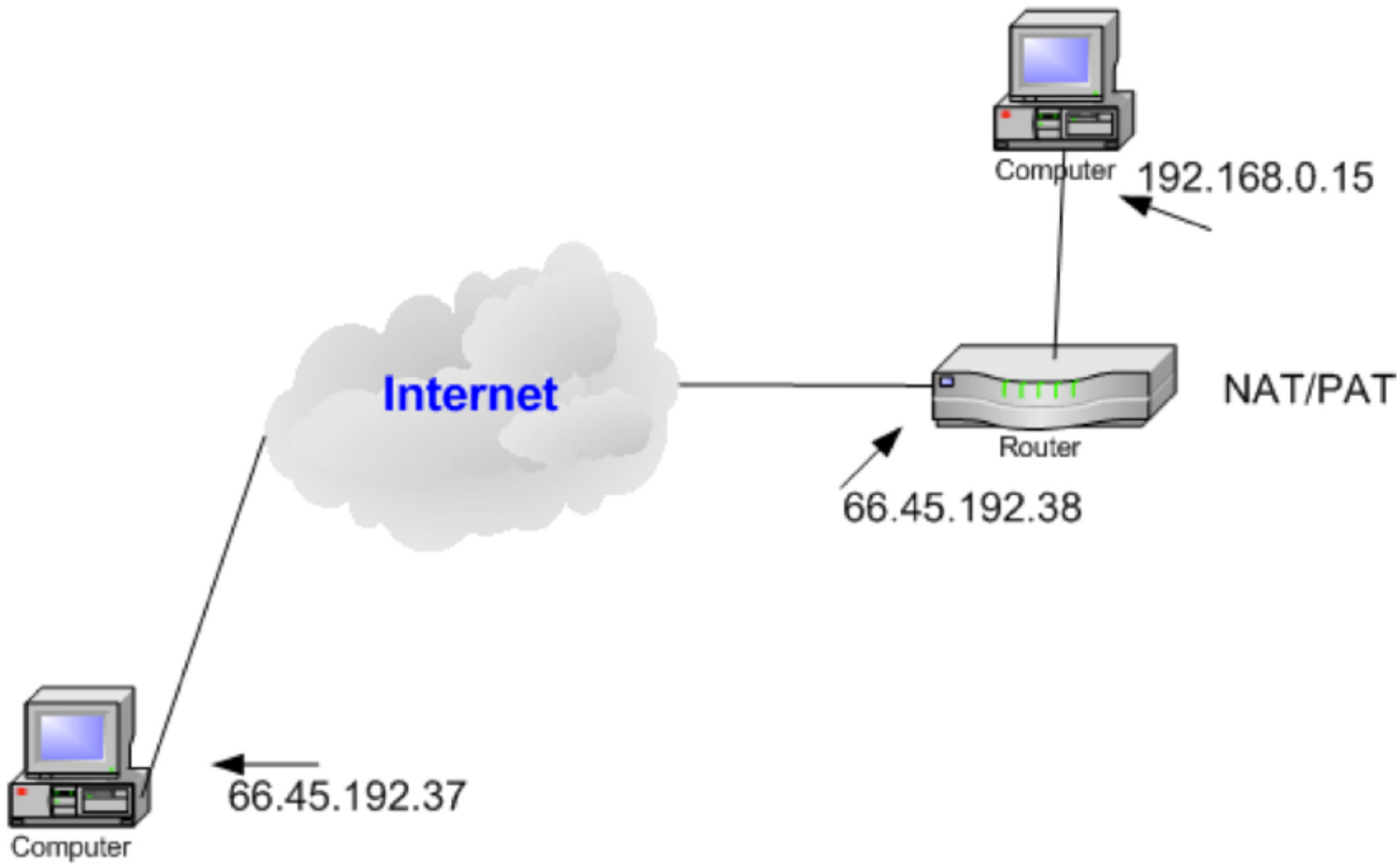
TFTP & SMTP


SMTP
Mail
TFTP
TFTP
Internet
Server
Authentication Server
Attacker

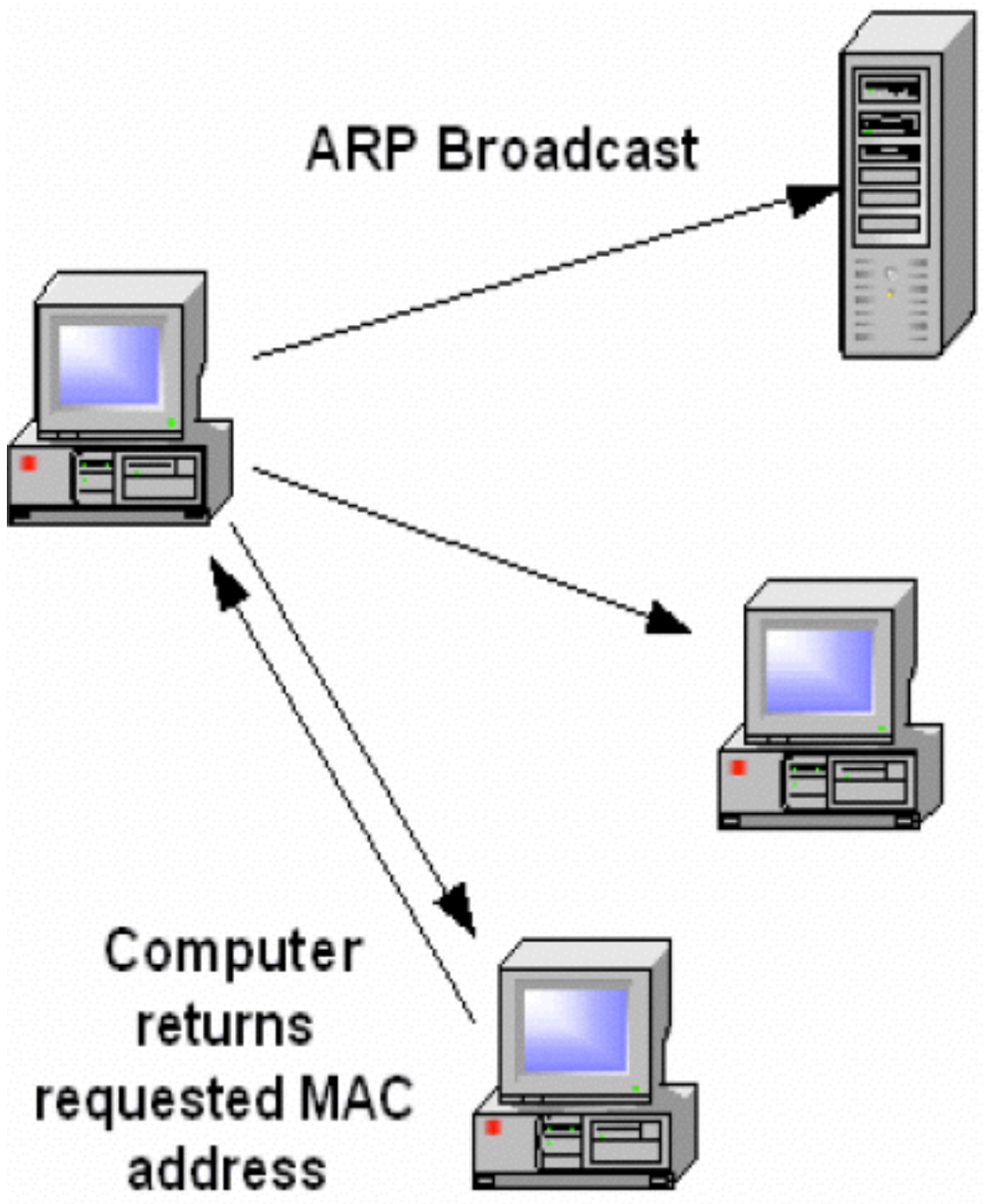
ICMP


Computer
Computer
Server
ICMP Echo
Reply
Router
Internet
Computer
ICMP Echo
Request
Computer

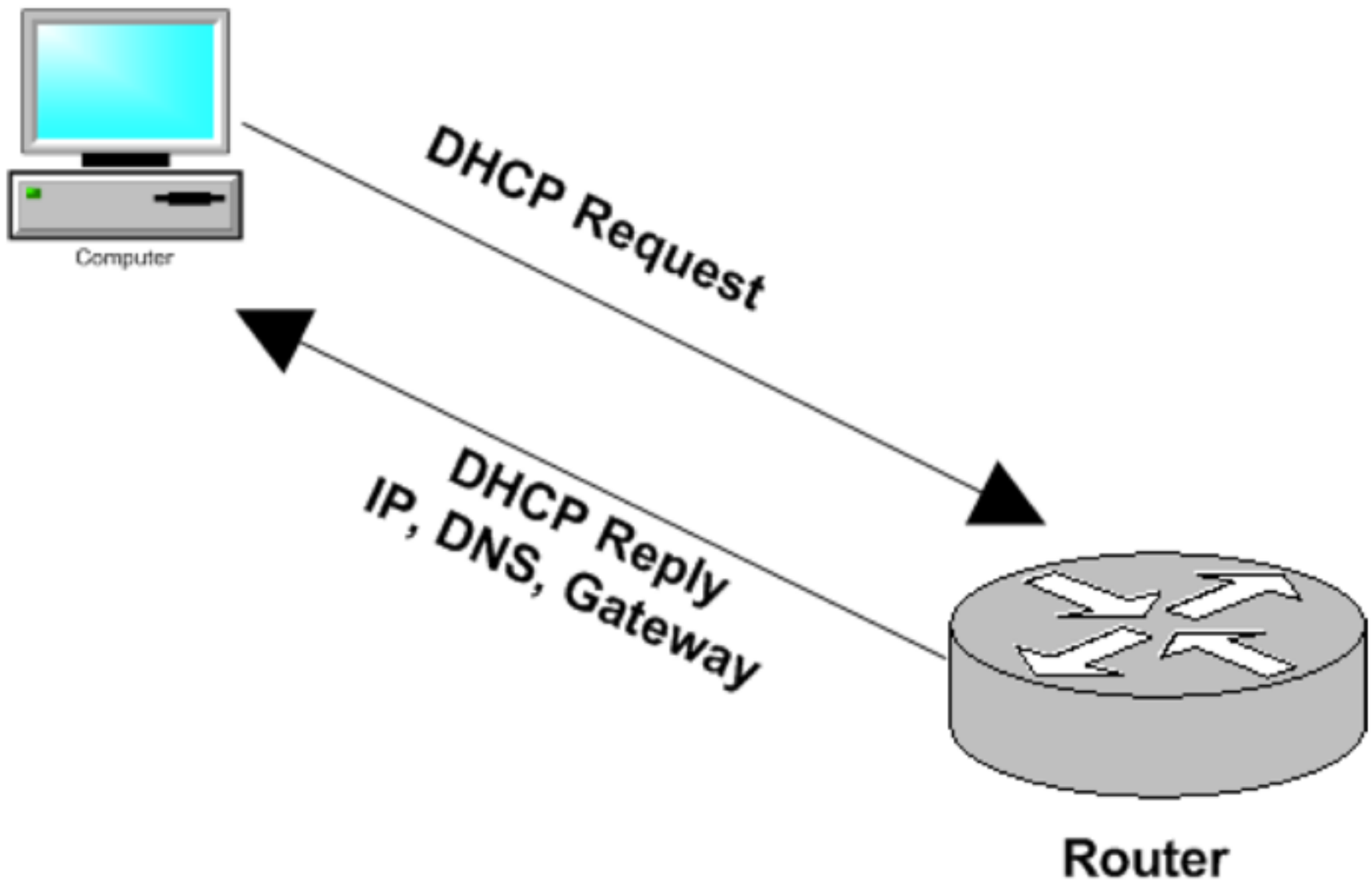
NAT/PAT


Computer
192.168.0.15
Internet
NAT/PAT
Router
66.45.192.38
66.45.192.37
Computer

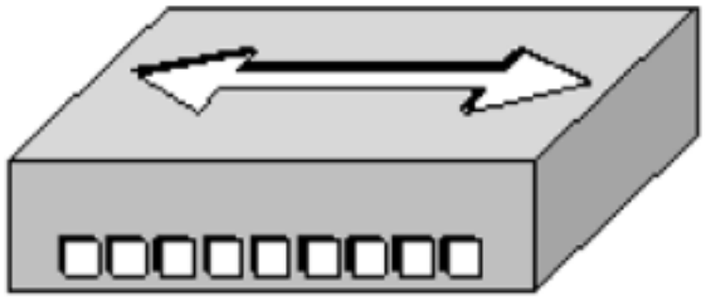
ARP/RARP



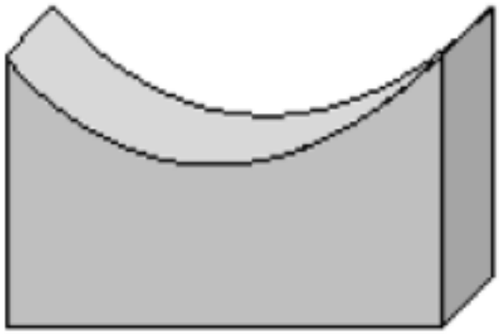
DHCP



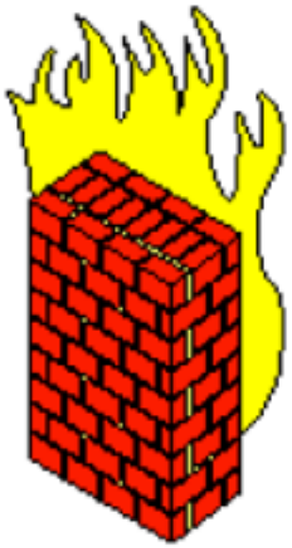
Network Connection Devices



Hub



Bridge



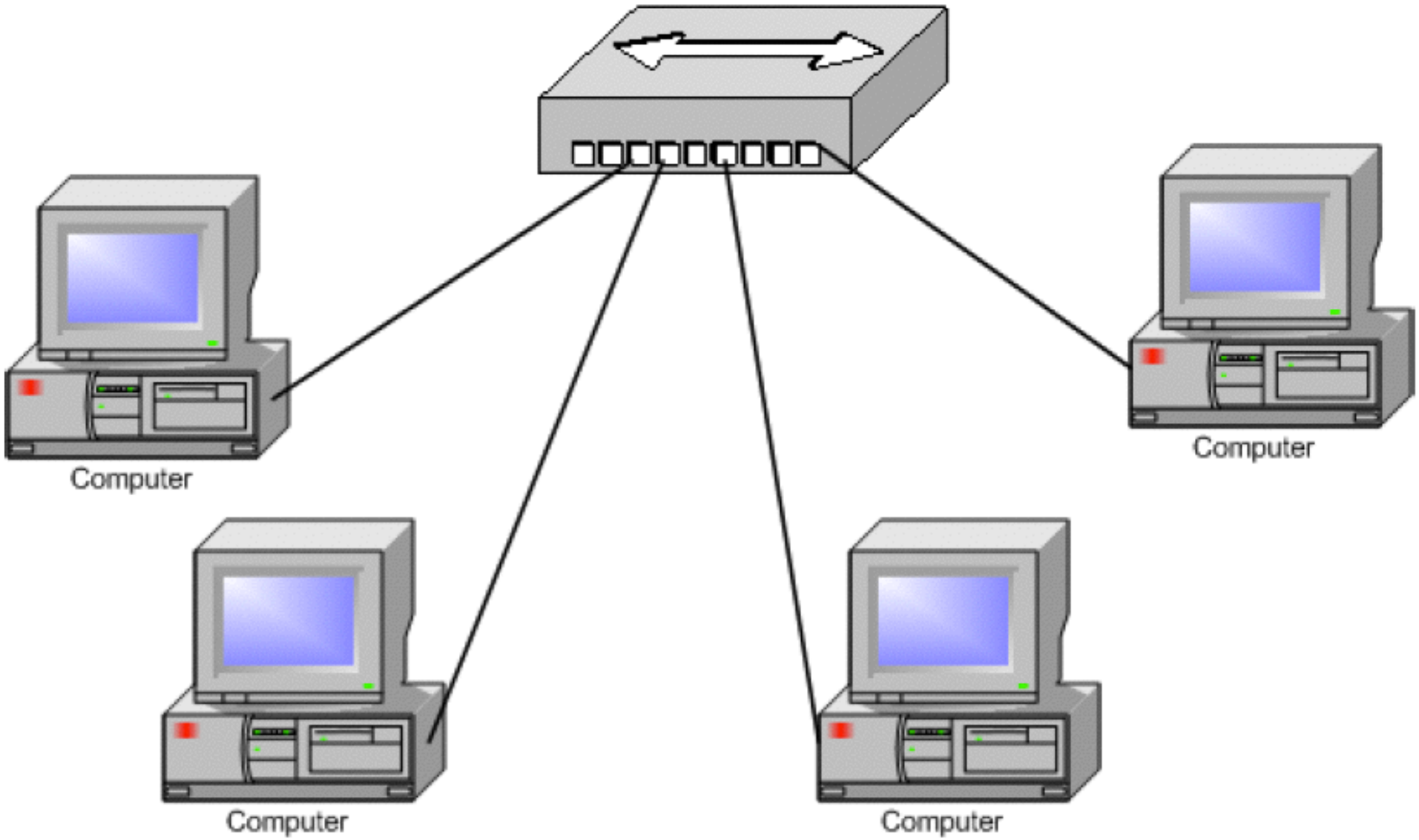
Firewall

Switch

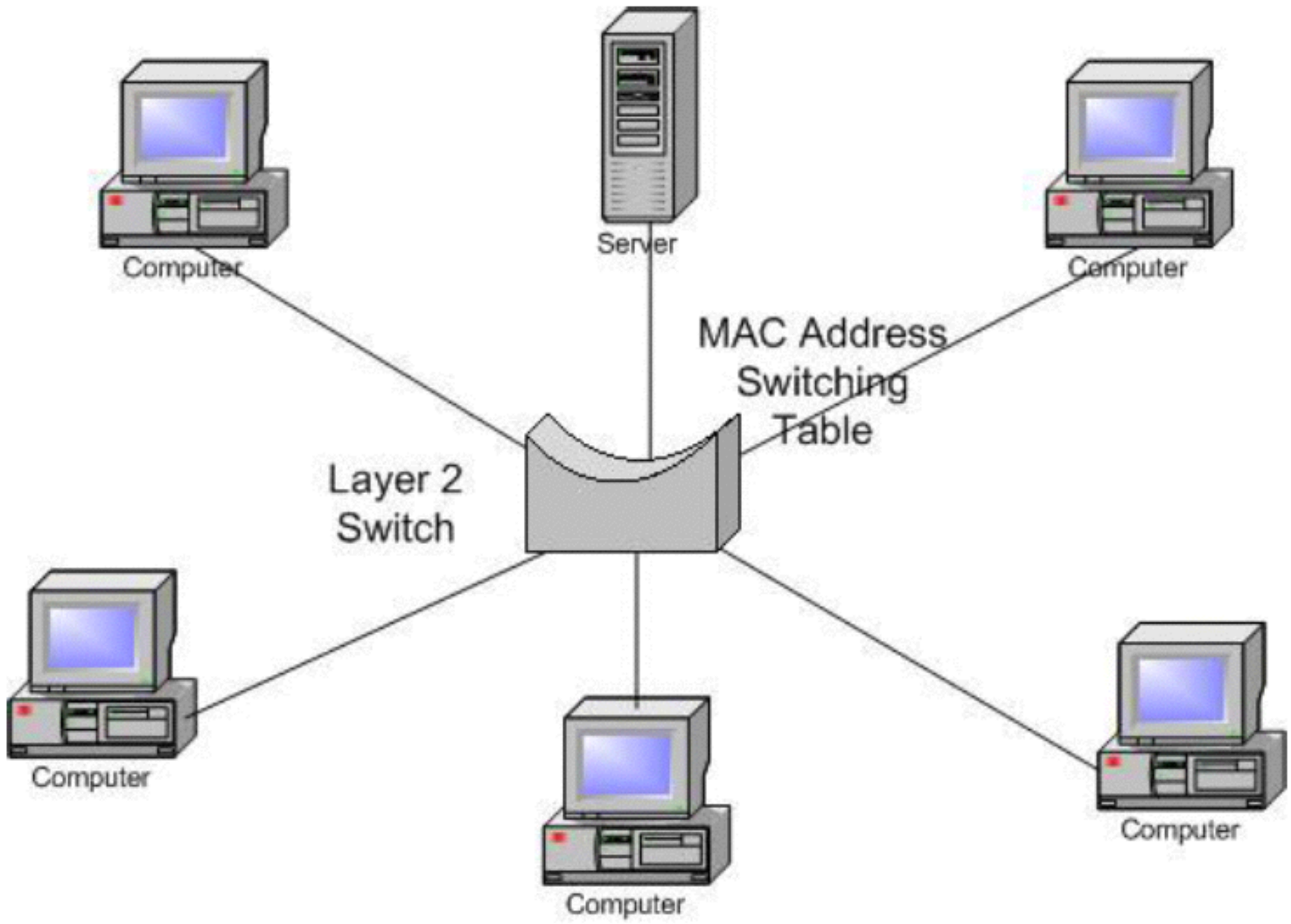
Router

Wireless Access Point

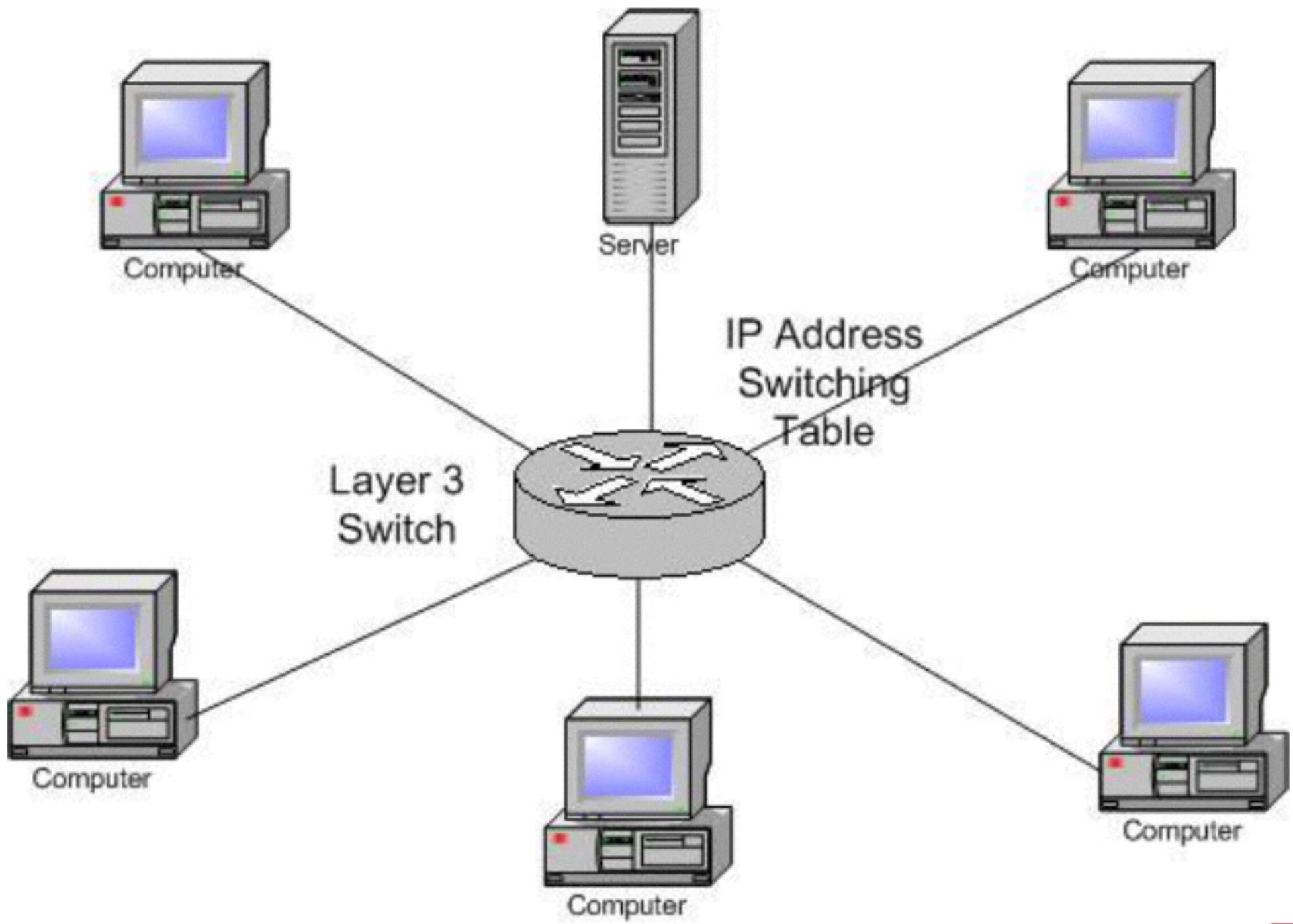
Hub Operation



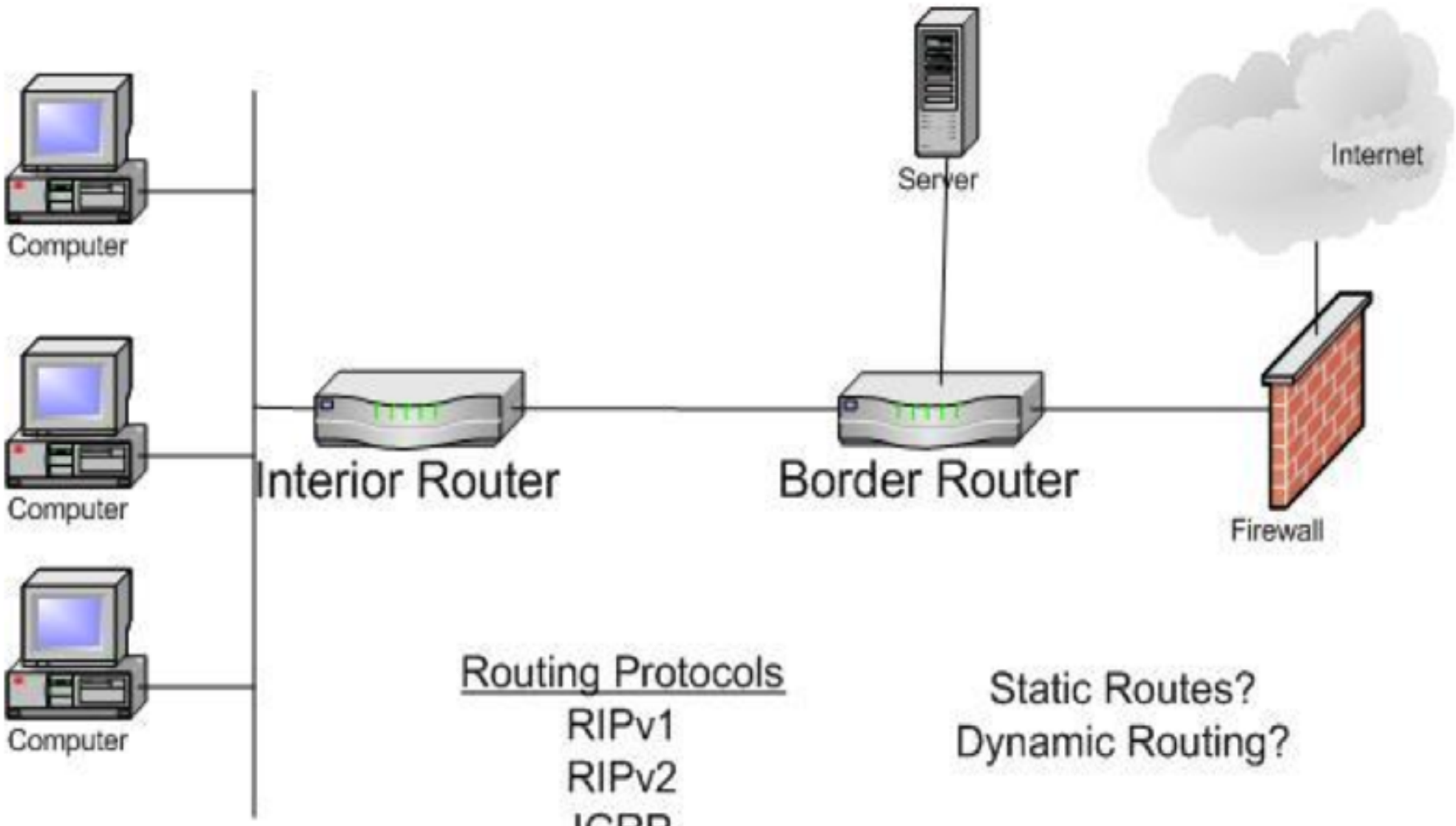
Layer 2 Switch Operation



Layer 3 Switch Operation



Router & Routing Protocols

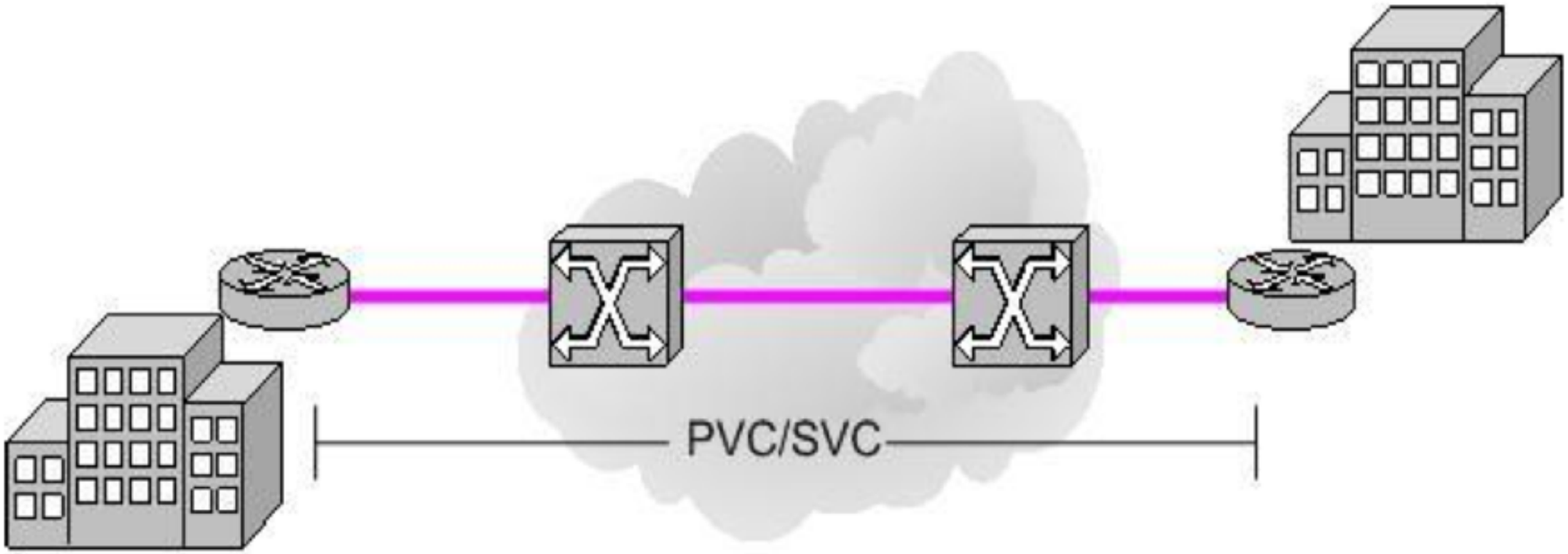


Routing Protocols
RIPv1
RIPv2
IGRP
EIGRP
BGP
OSPF

Static Routes?
Dynamic Routing?

Route Authentication?

Wide Area Networking



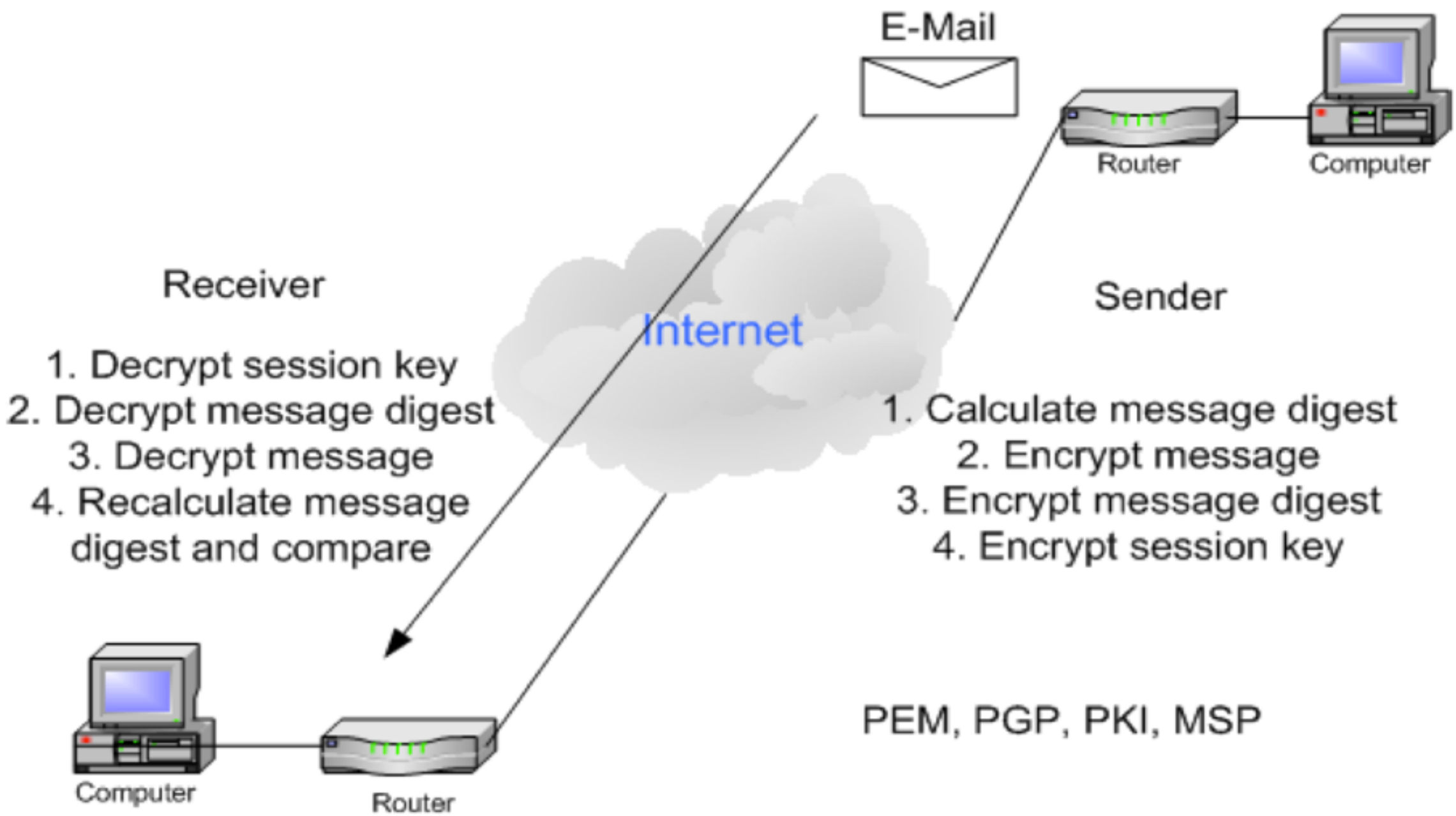
Circuit Switched
POTS
ISDN

Packet Switched
X.25
Frame Relay
SMDS
ATM

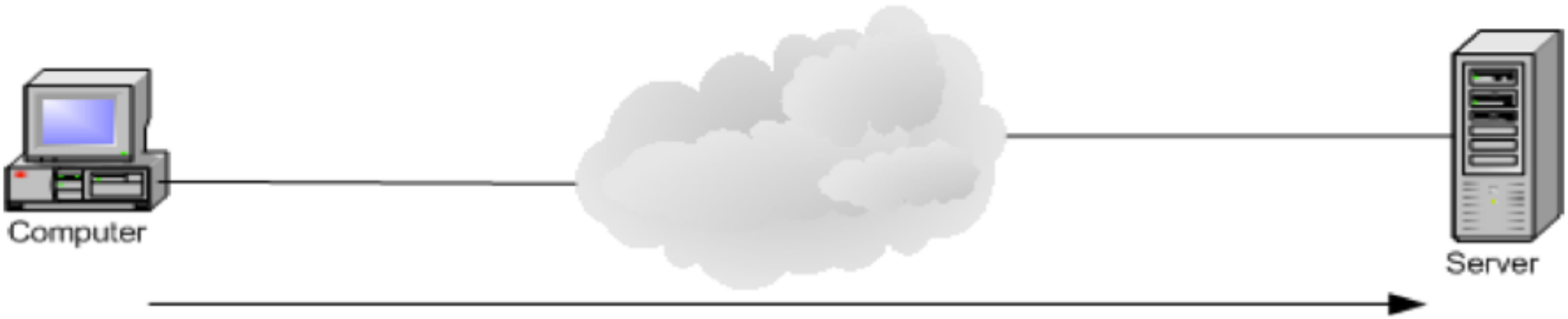
Security Strategy

- For many years, protection was equated with prevention
- How well people with the prevention, still many could find ways around safeguards
- Thus, most practical model includes 2 more factors, detect & response

Application Layer Security



Secure Socket Layer (SSL)



1. Establish Communication

2. Certificate sent to Client for authentication

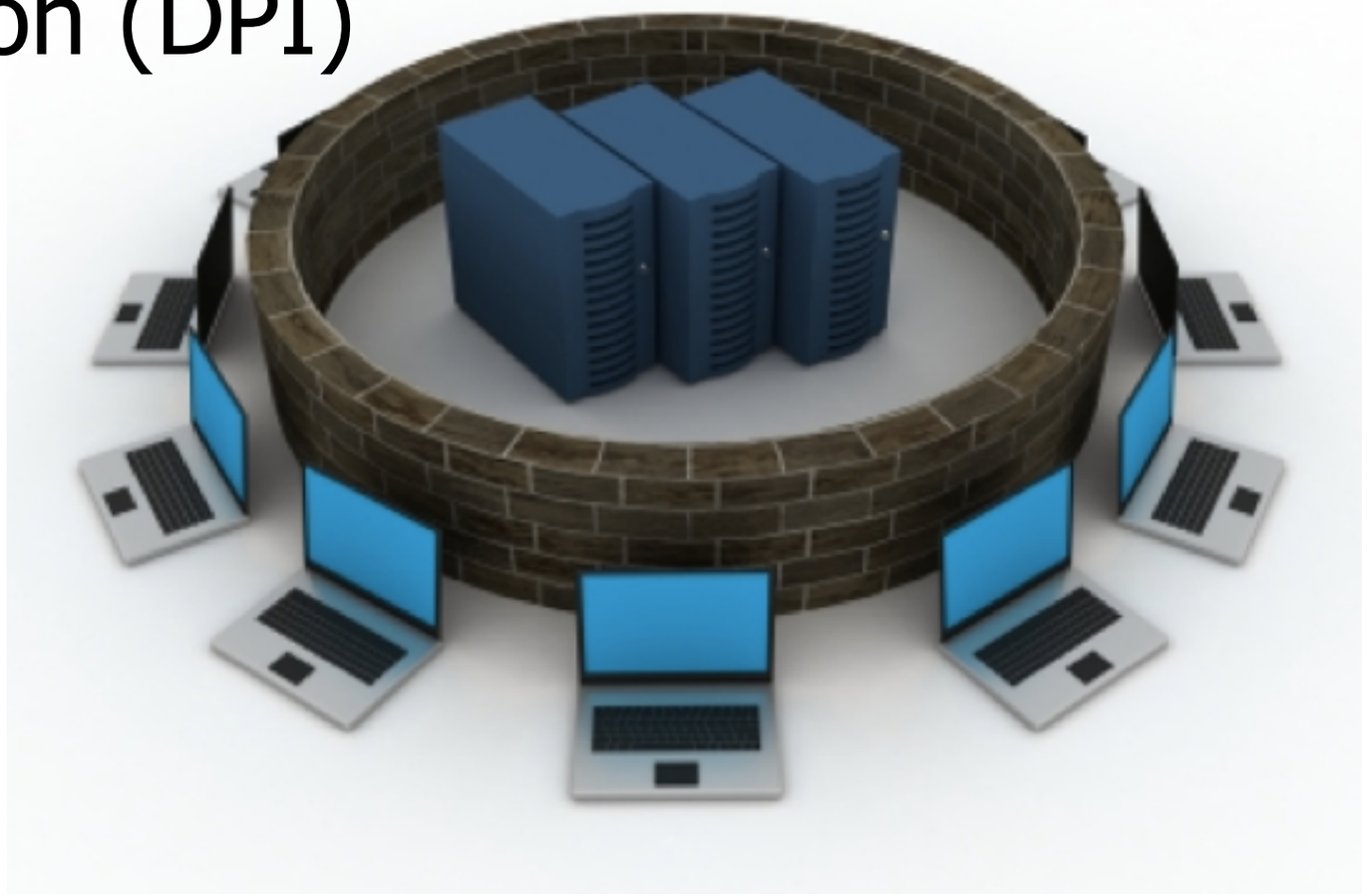
3. Client establishes validity of certificate and message and retrieves the server's public key

4. Client creates session key

5. Client sends session key to Server, encrypted with Server's public key

Firewall

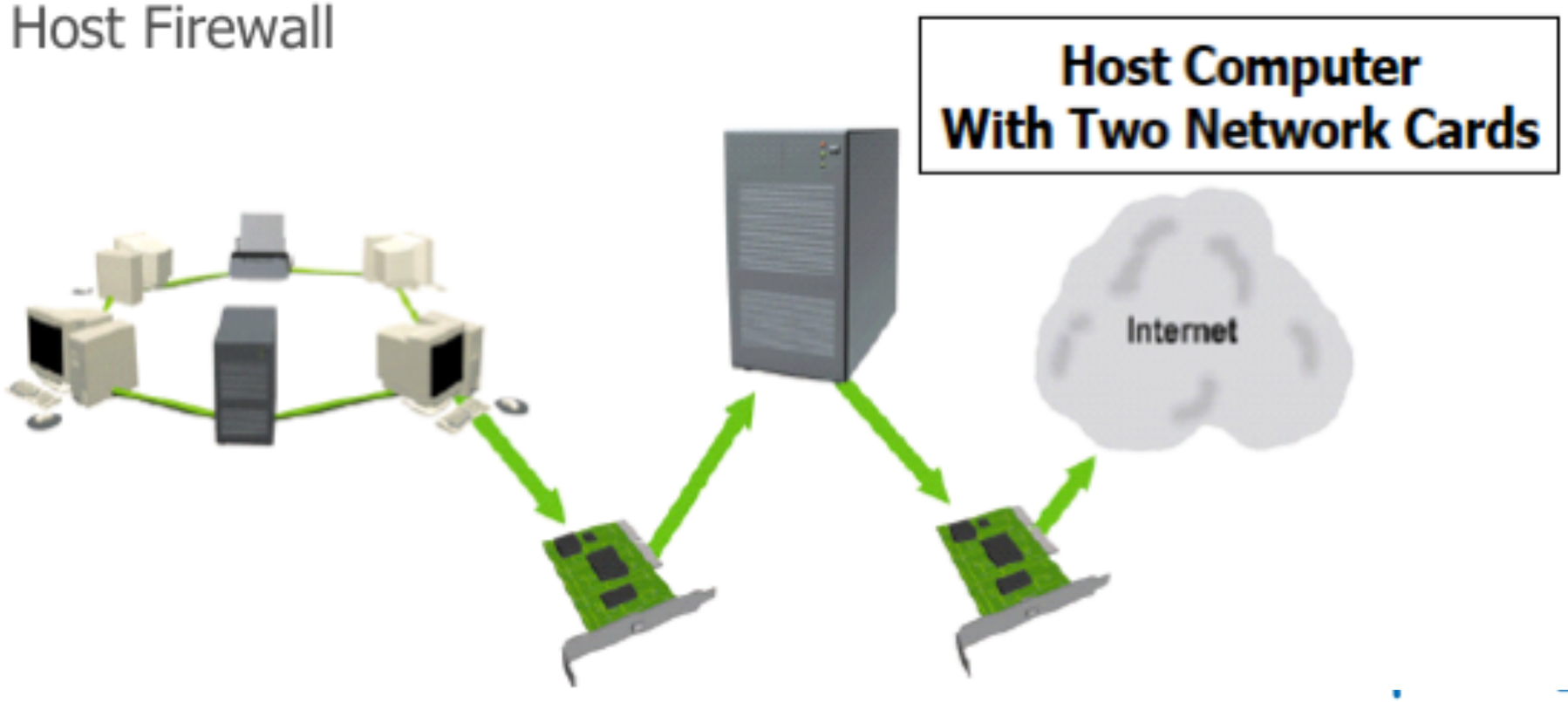
- Various types of Firewall
- Packet filtering
- Stateful packet inspection
- Deep Packet Inspection (DPI)
- Application proxy
- Circuit proxy



Firewall Configuration

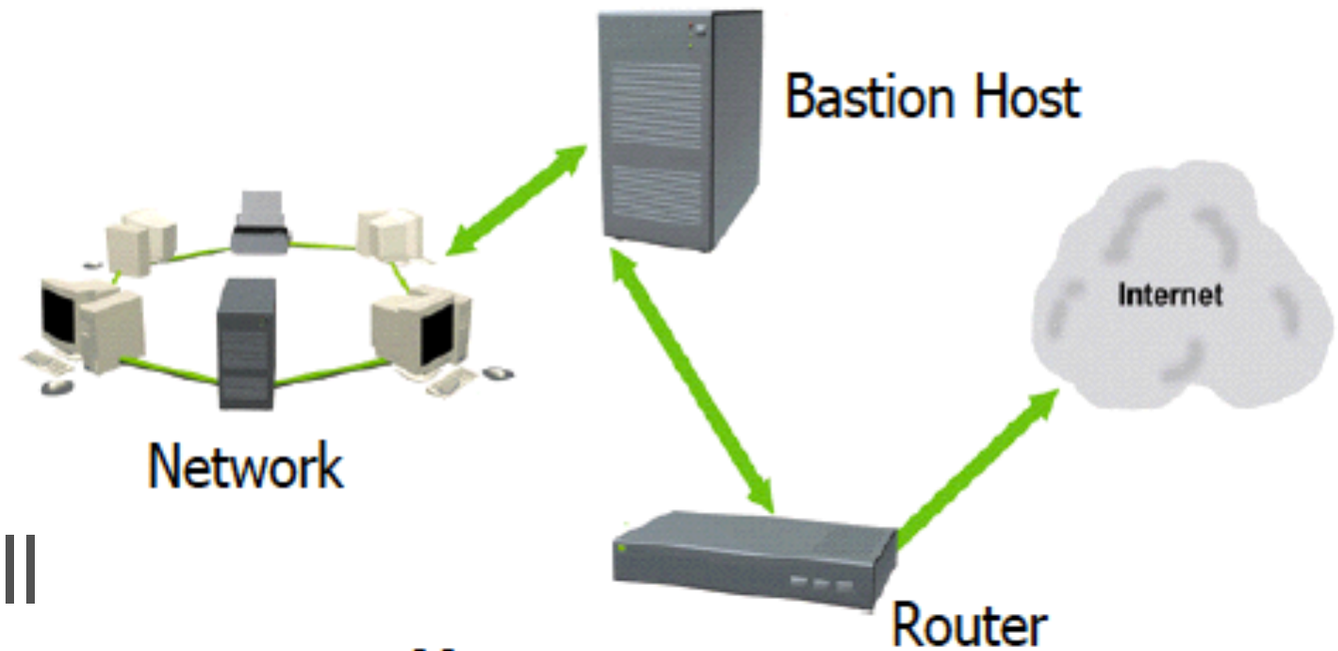
- Boundary Packet Filtering Router

- Dual Homed Host Firewall

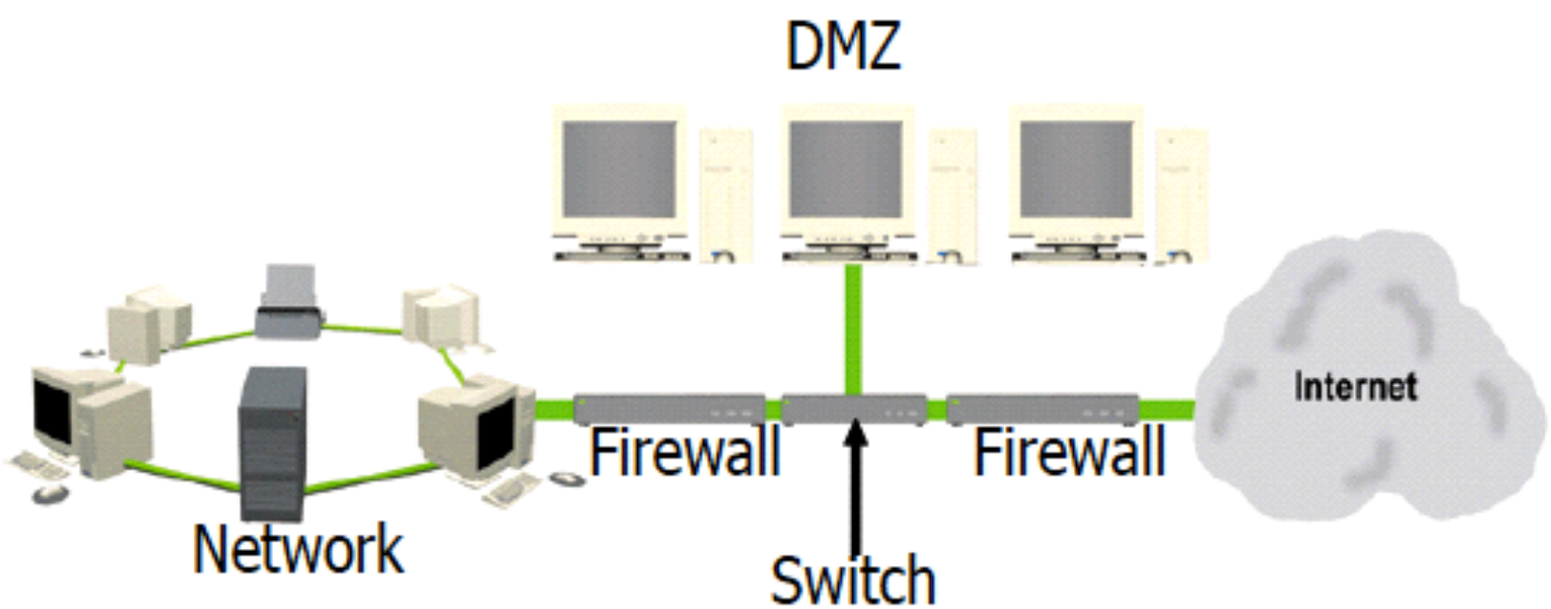


Firewall Configuration

- Screened-Host Firewall



- Screened Subnet Firewall



IDS Component

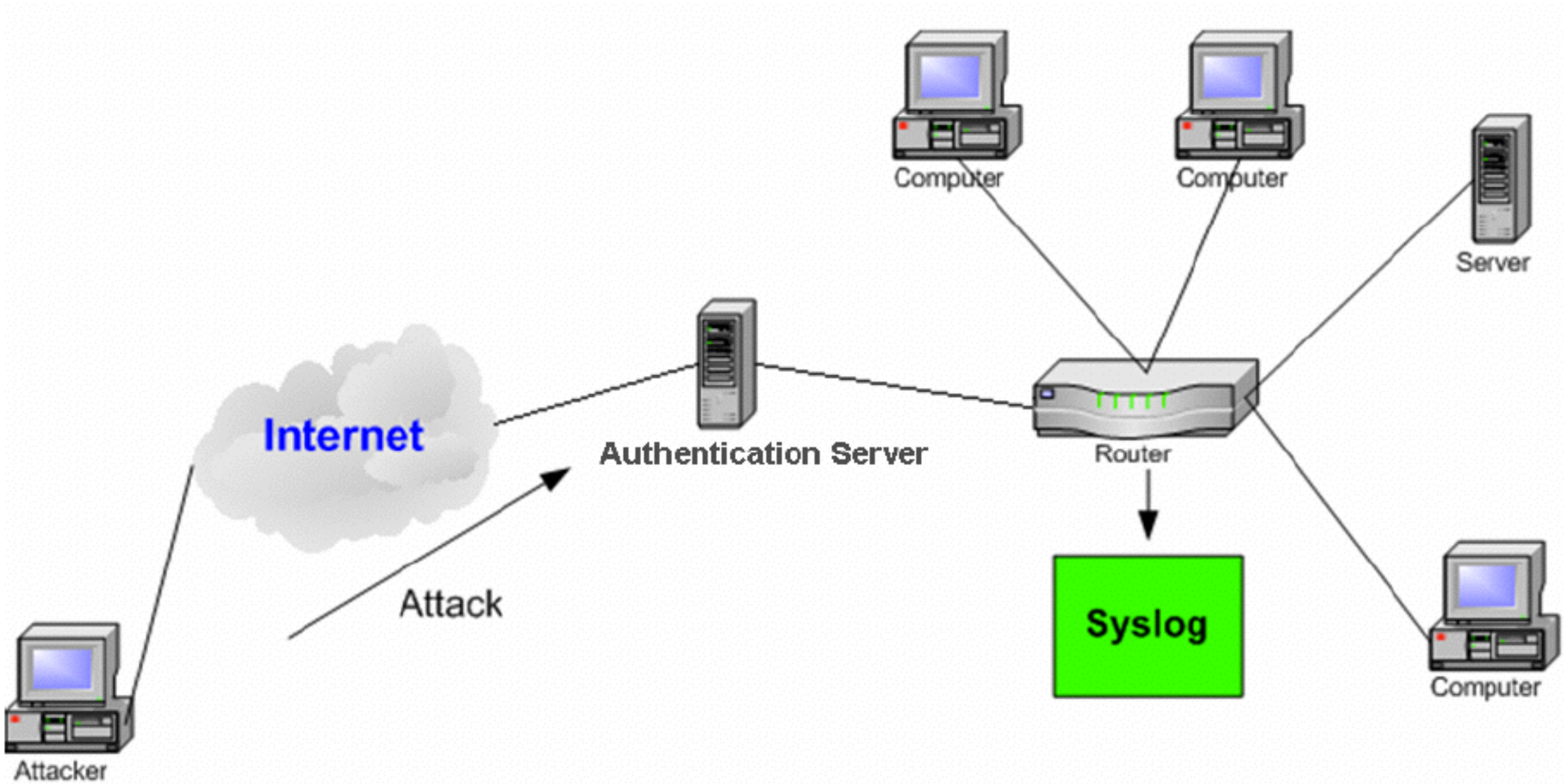
Traffic collector:

- collects information for the IDS to examine.
- host-based IDS
  - this could be log files, audit logs, or traffic coming to or leaving a specific system.
- network-based IDS
  - typically a mechanism for copying traffic off the network link—basically functioning as a sniffer.

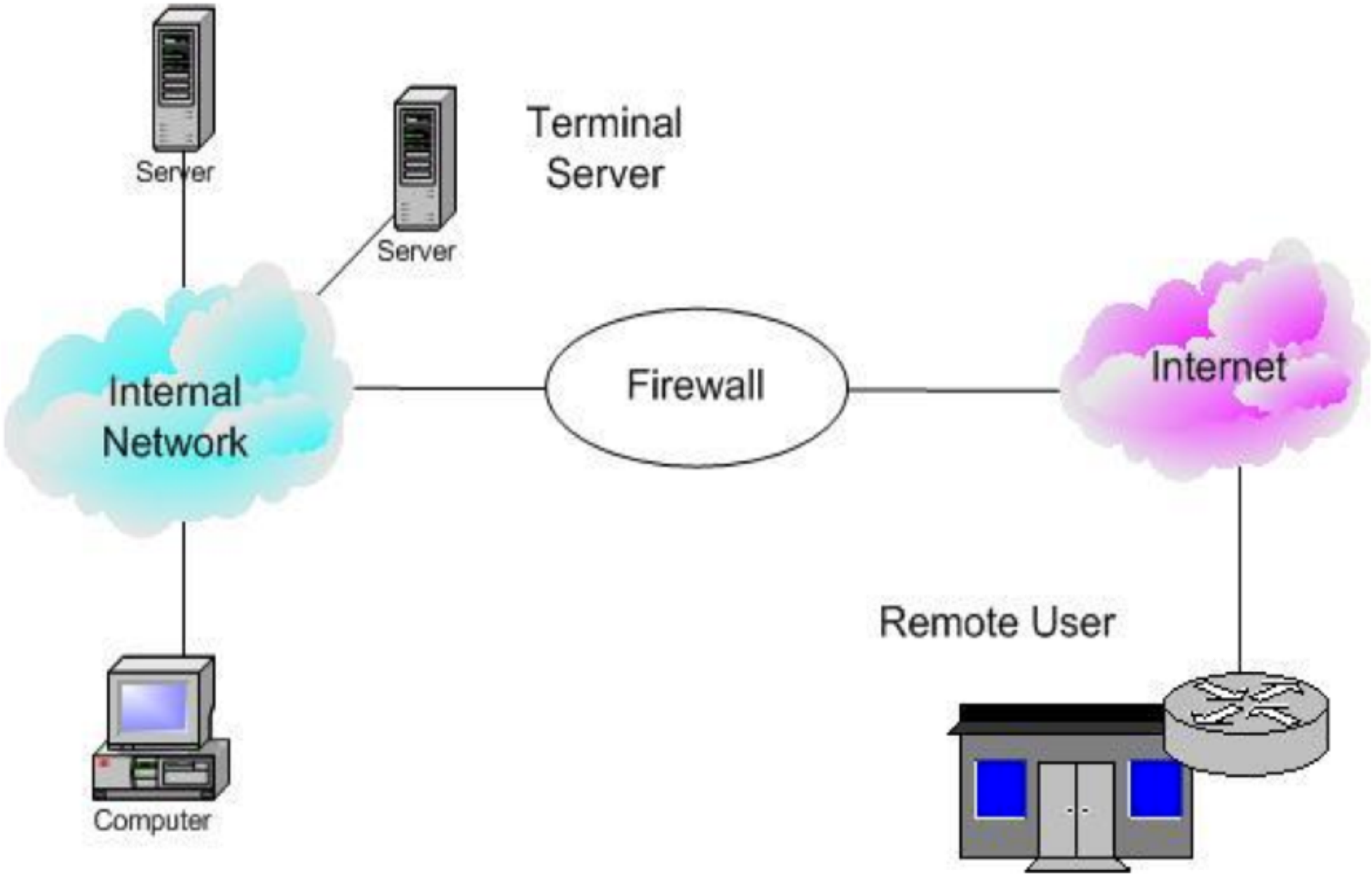
IDS Component

- Analysis engine:
  - Examines the collected information and compares it to known patterns of suspicious or malicious activity stored in the signature database.
- Signature database:
  - A collection of patterns and definitions of known suspicious or malicious activity.
- User interface and reporting:
  - The component that interfaces with the human element, providing alerts when appropriate and giving the user a means to interact with and operate the IDS.

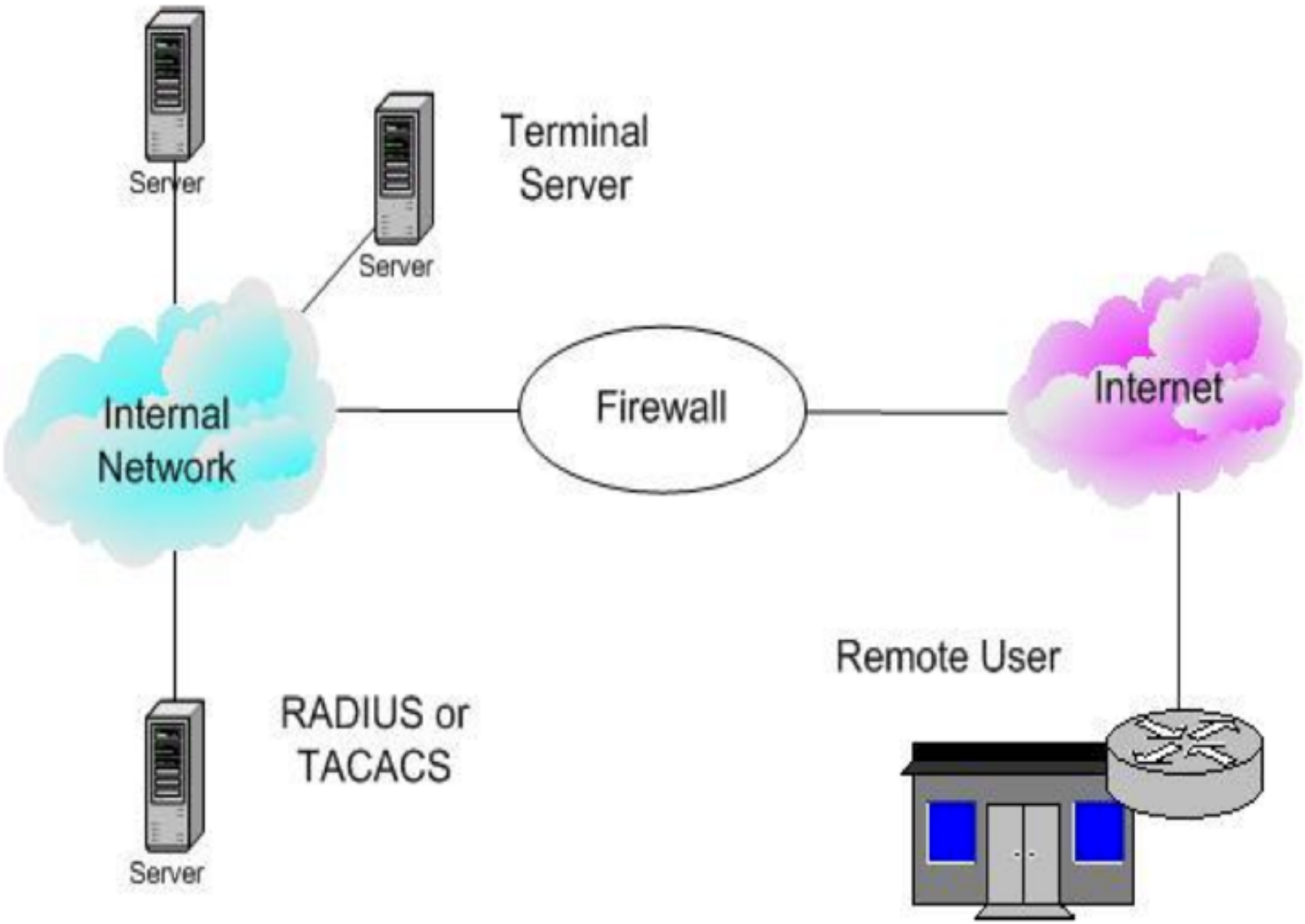
Syslog


Computer
Computer
Server
Internet
Authentication Server
Router
Attack
Syslog
Computer
Attacker

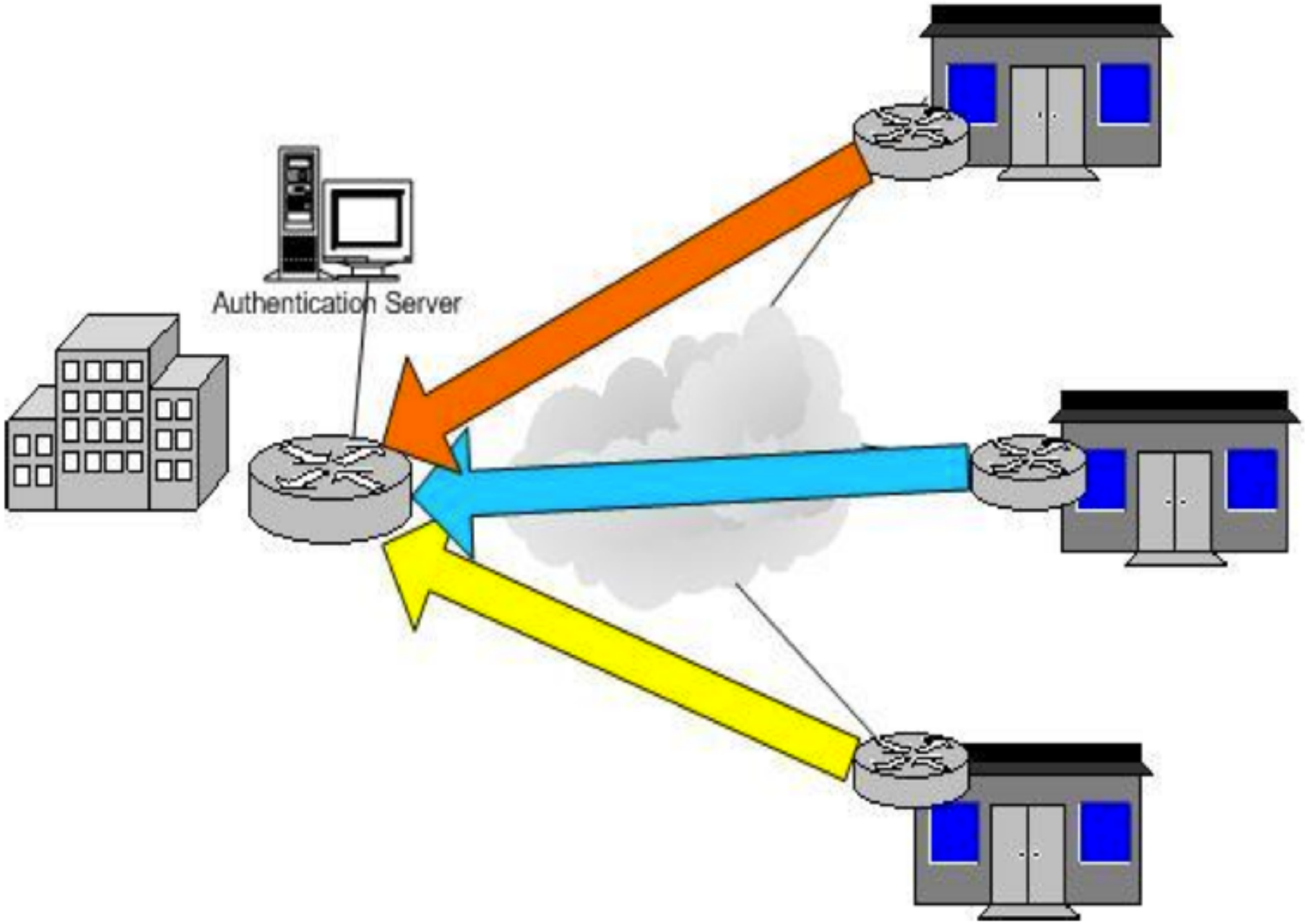
Remote Access Server



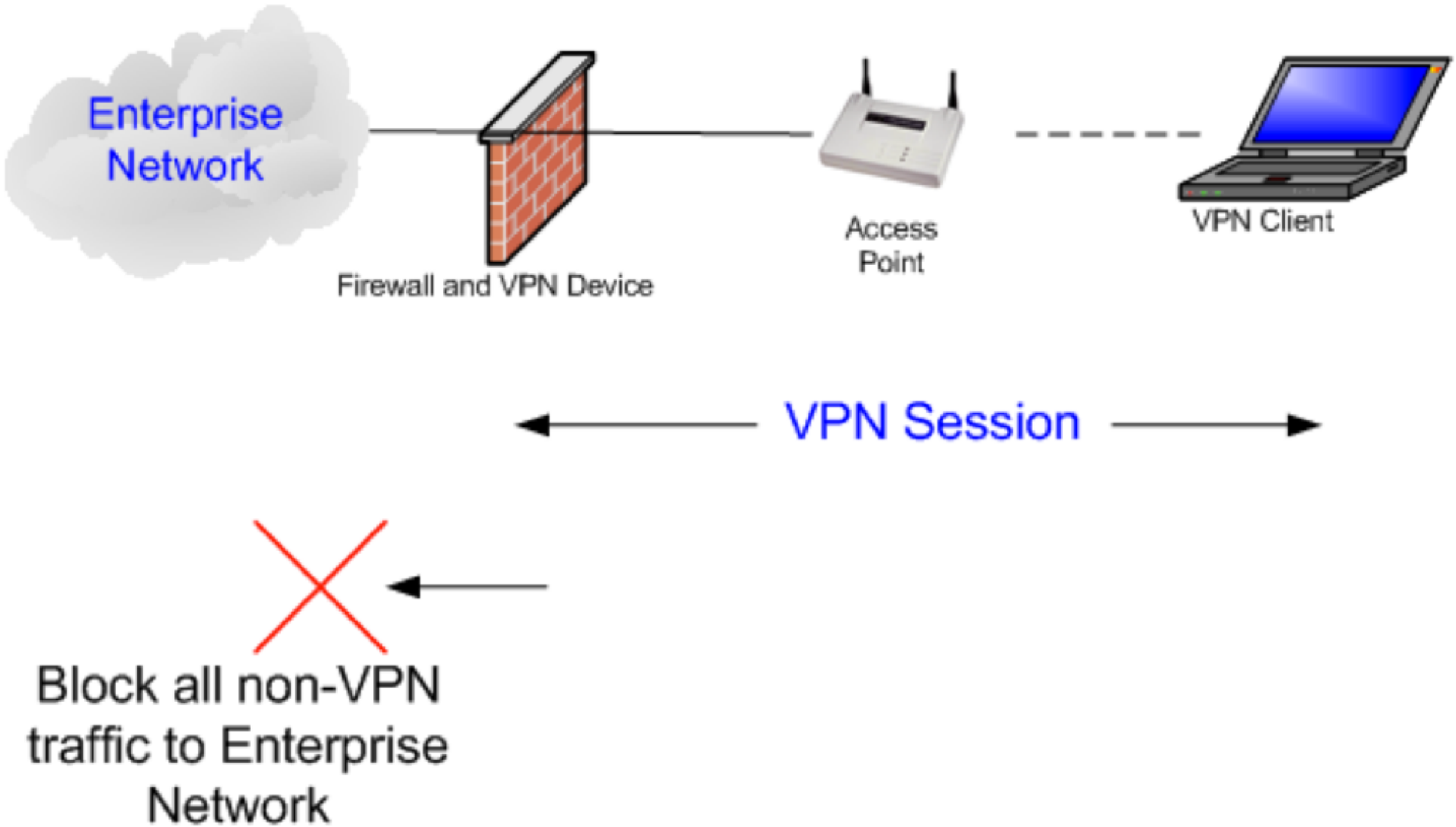
Identification & Authentication Remote Users



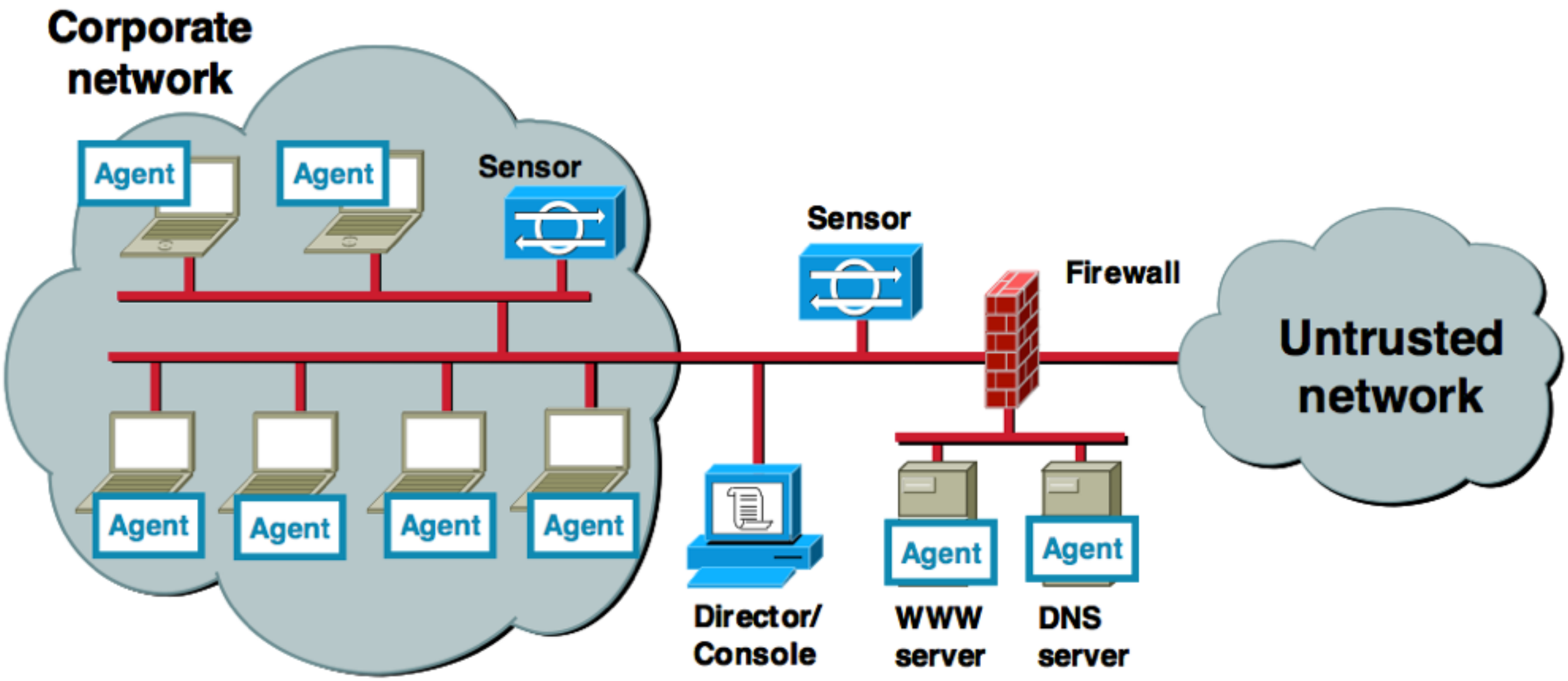
VPN Concentrators



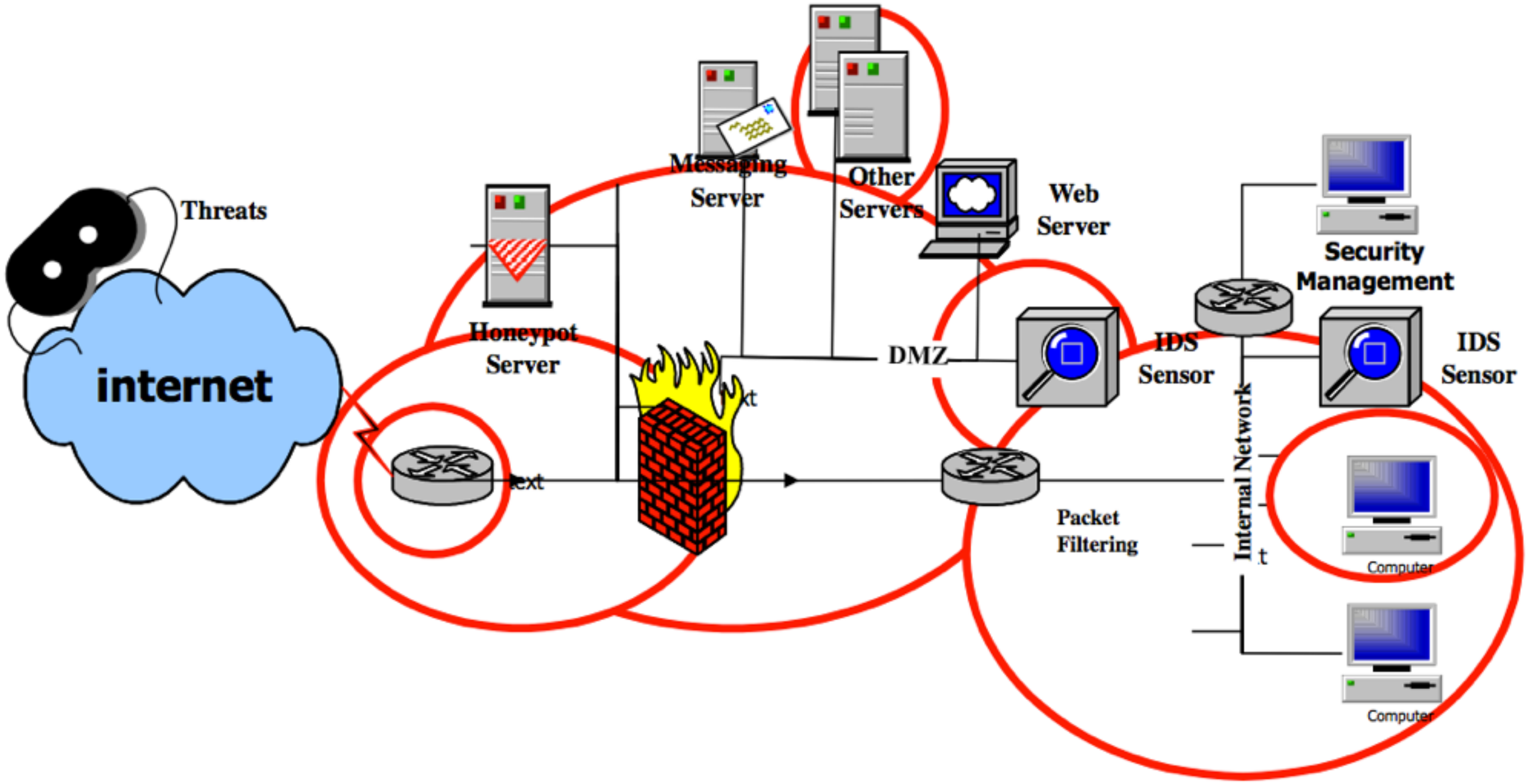
Virtual Private Network (VPN)



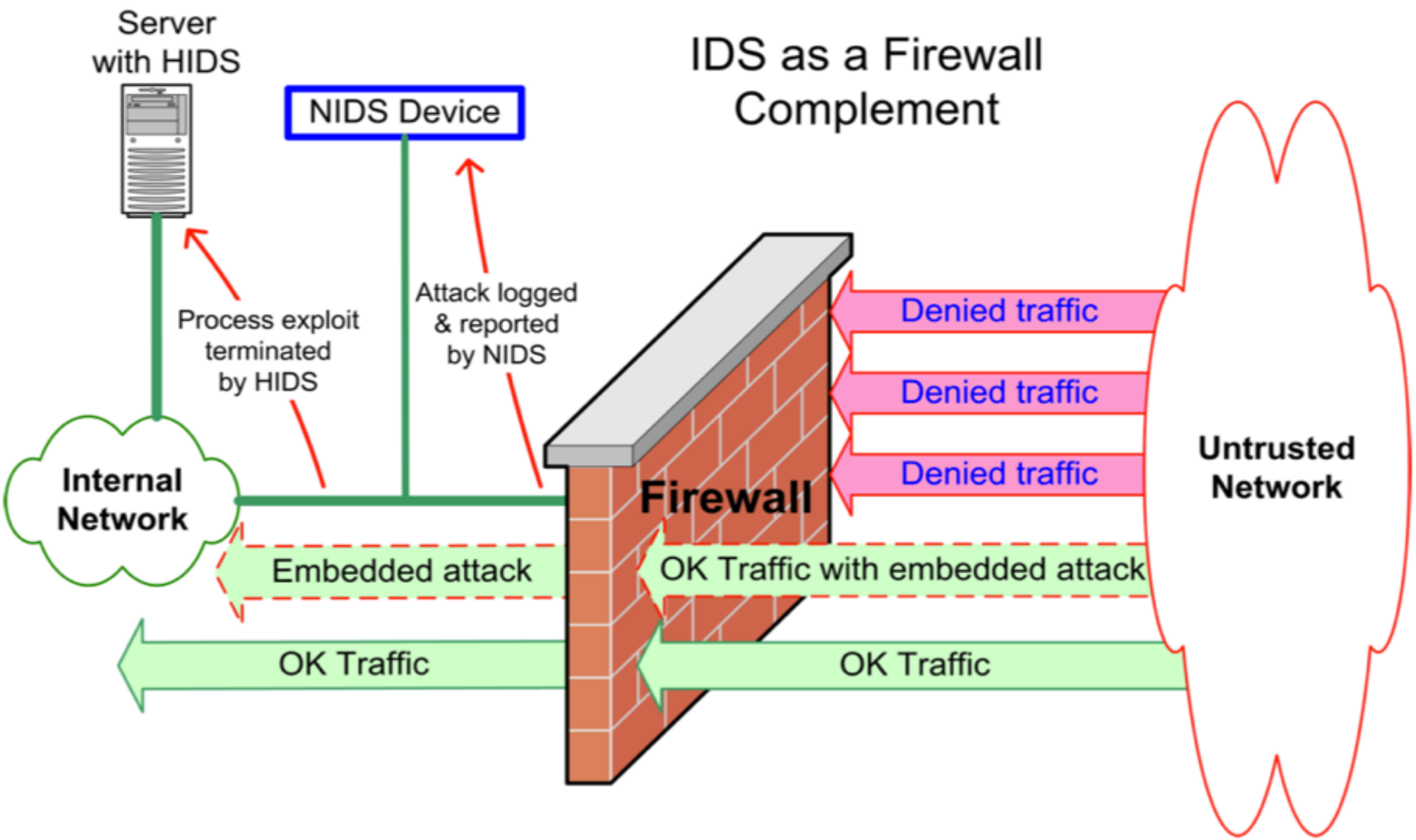
AV Layered Defense-in-Depth



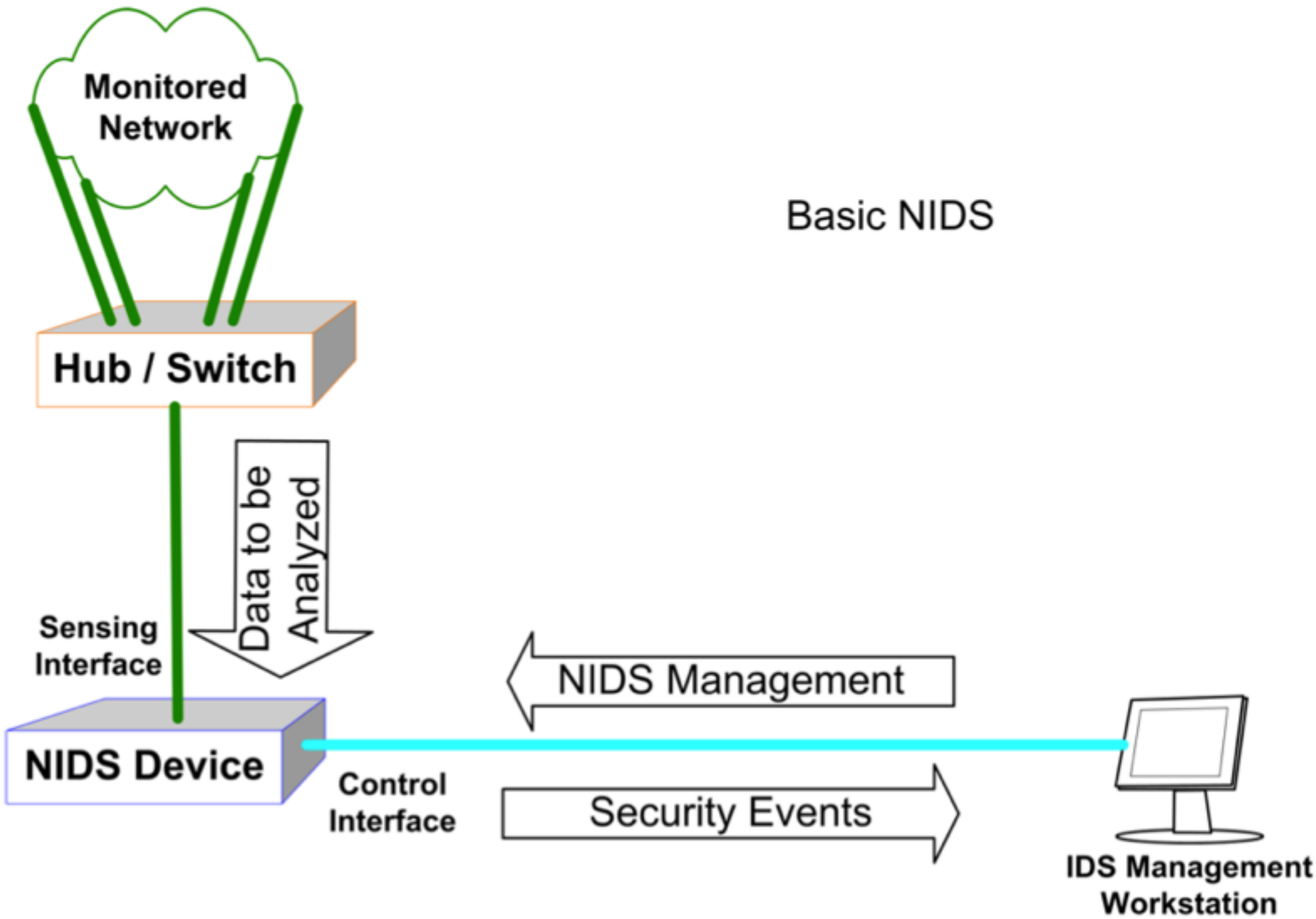
Multiple Zones of Defense & Defense-in-Depth



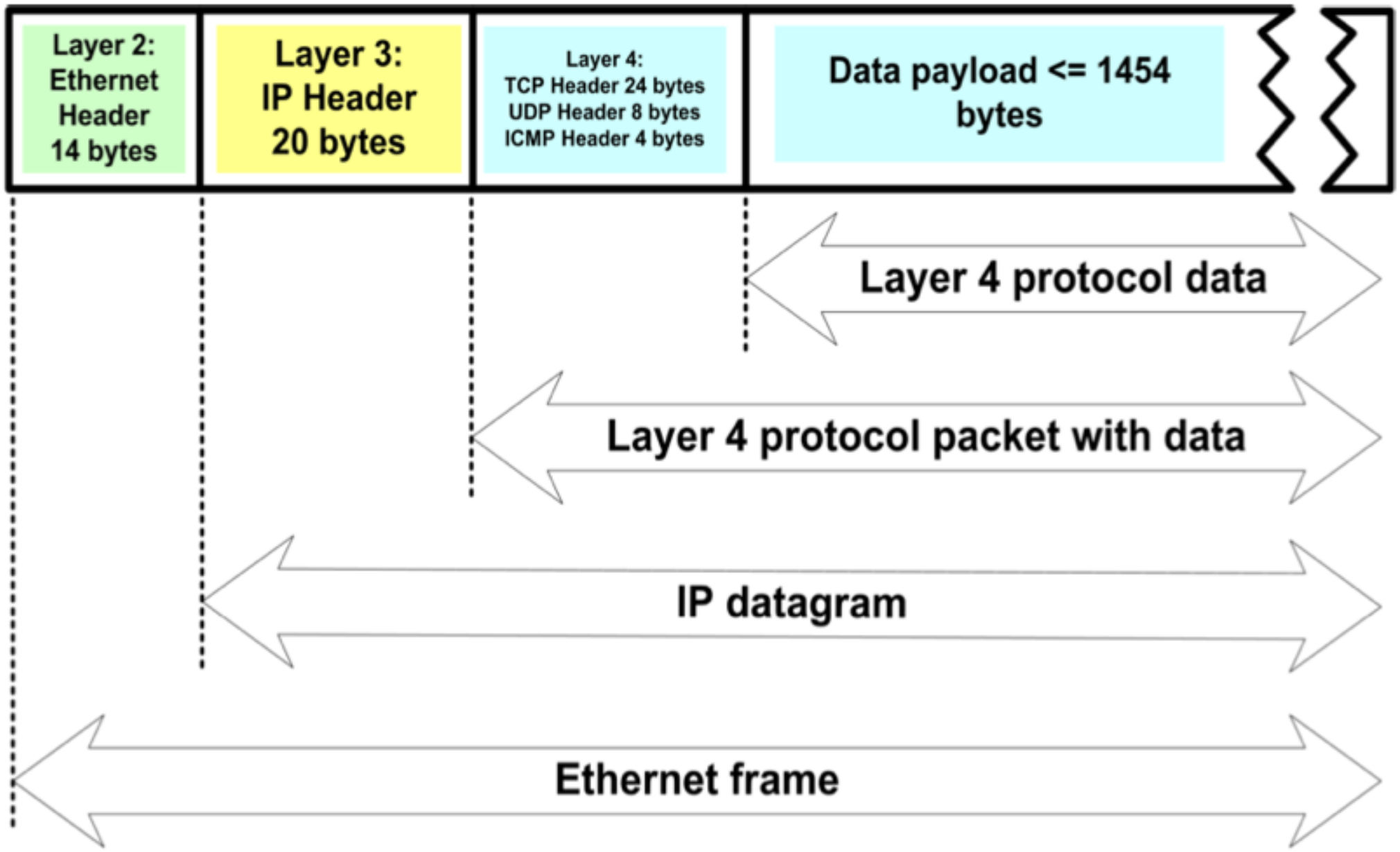
IDS as Firewall Complement



Network IDS (NIDS)

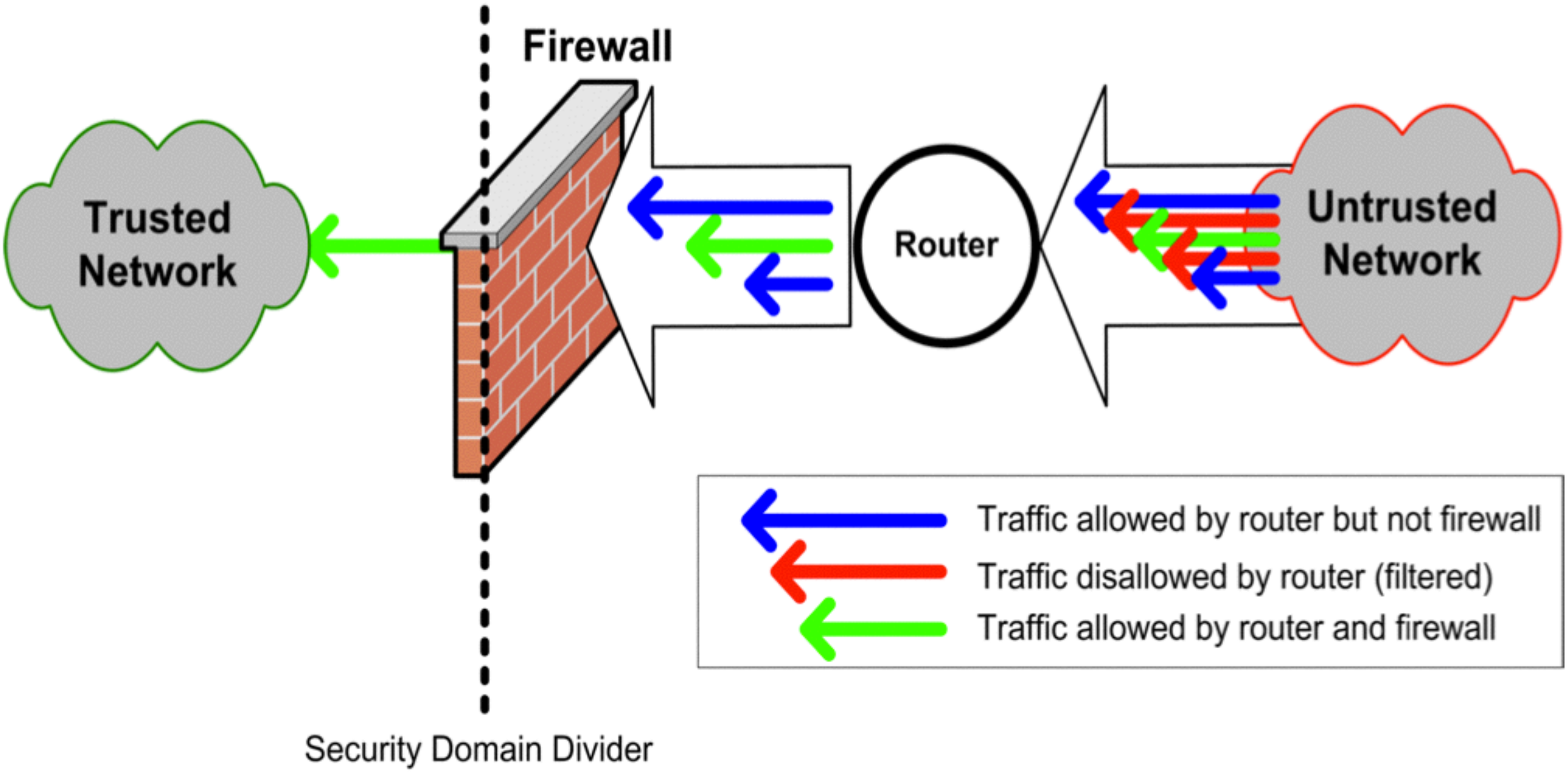


NIDS Operation

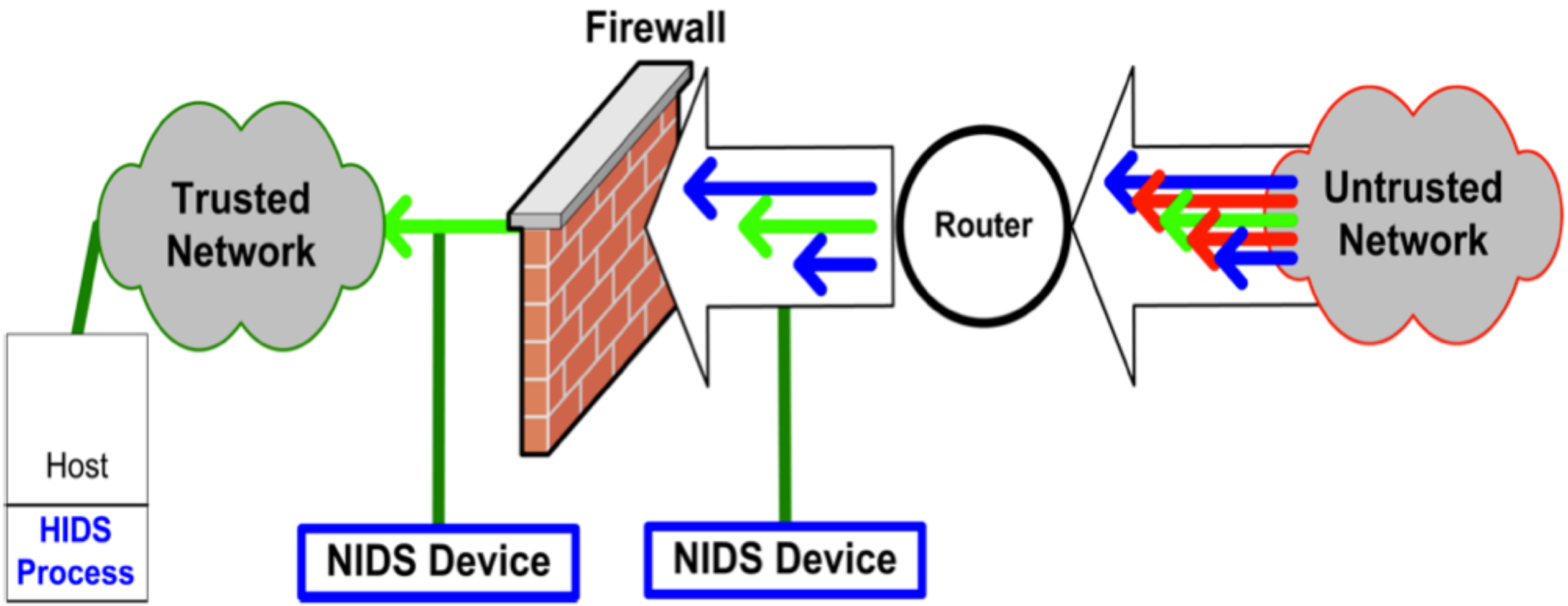


IP datagram framed for an Ethernet network

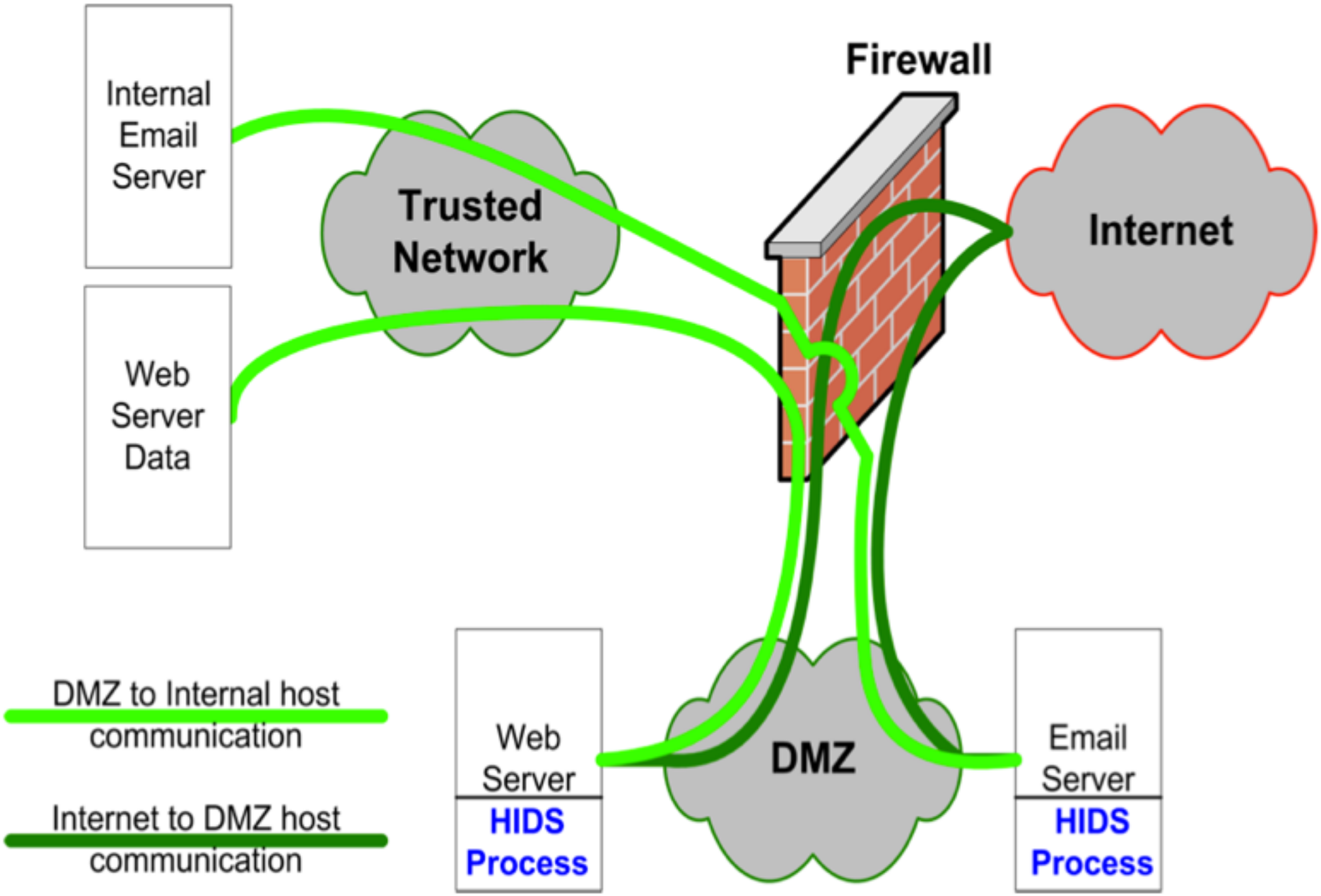
Layered Defense - Network Access Control



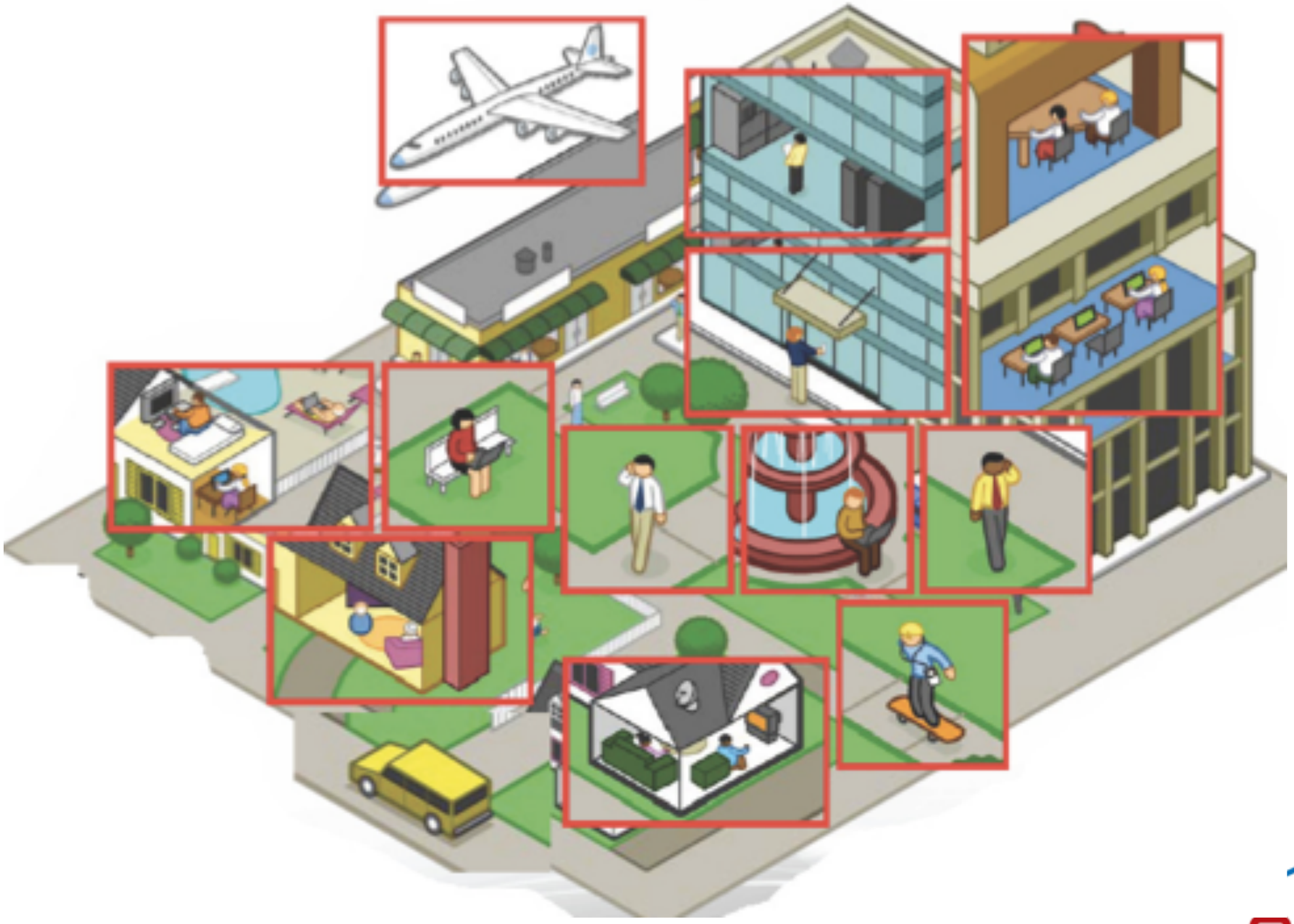
Control Check - Intrusion Detection



Host Isolation



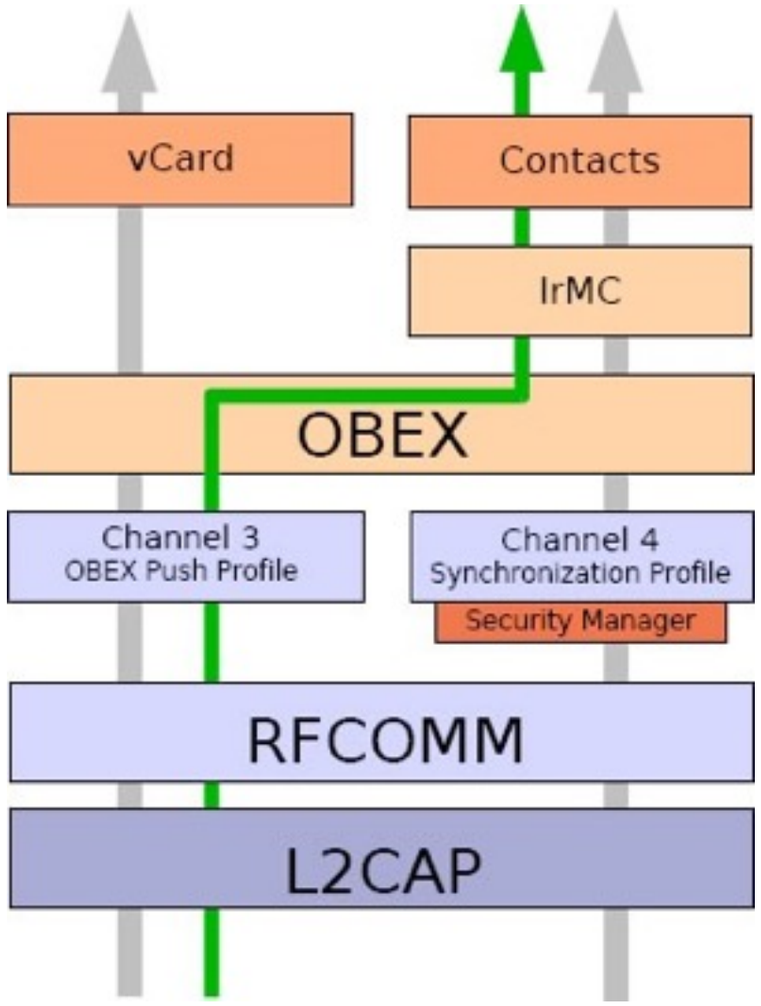
Wireless Technologies



Bluetooth (IEEE 802.15)

Bluetooth Threats & Security Issues

- Less security policies & implementation
  - Third party software providers
  - Security default configuration



BlueBug™ BlueSnarf™ BlueSmack™ BlueDump™

BlueBump™ BlueSnarf++™ Bluetooone™

Wireless LAN (IEEE 802.11)

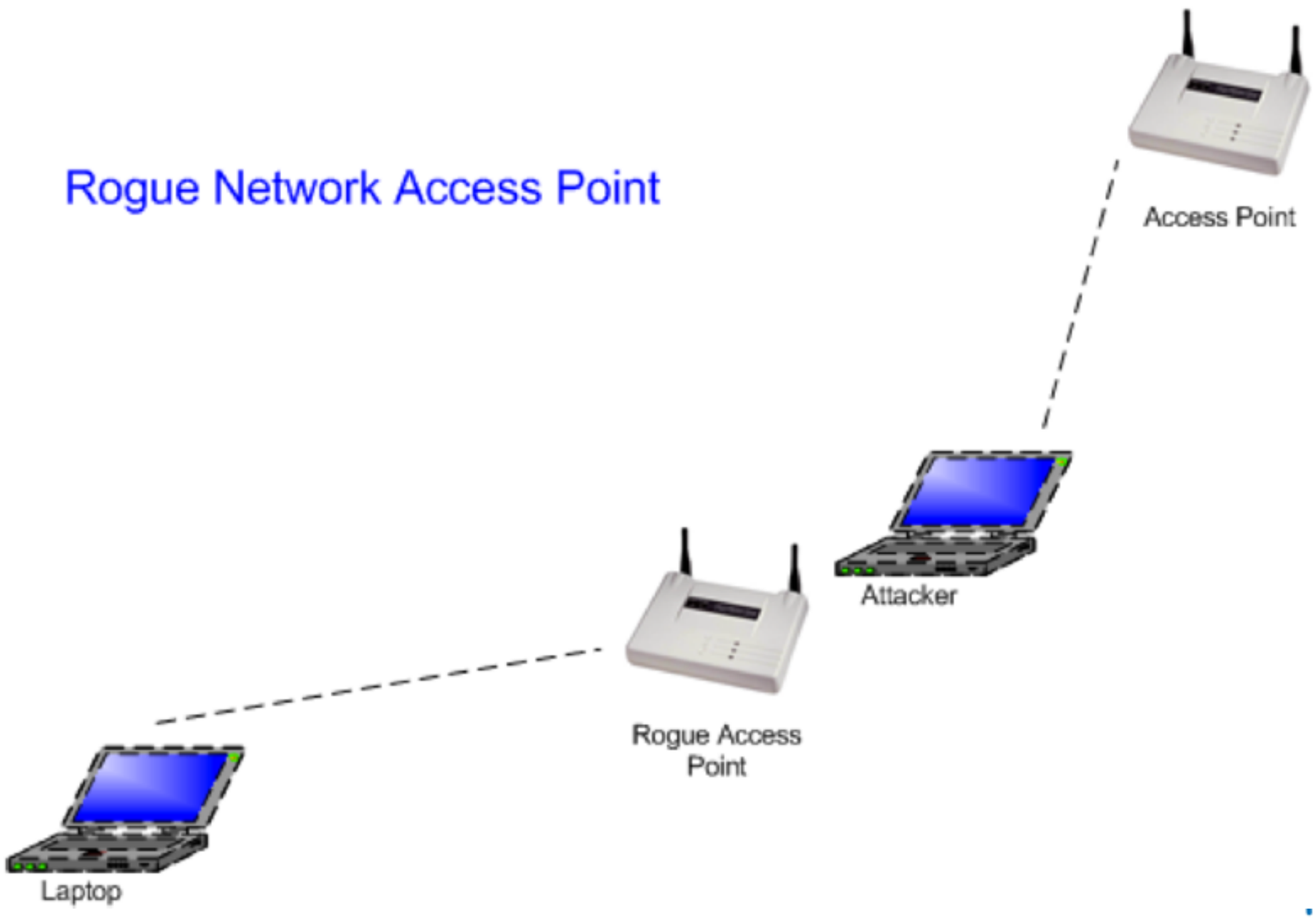
Wireless Standard	802.11b		802.11a		802.11g	
Popularity		Widely adopted. Readily available everywhere.		New technology.		New technology with rapid growth expected.
Speed	11 Mbps	Up to 11Mbps (note: cable modem service typically averages no more than 4 to 5Mbps).	54 Mbps	Up to 54Mbps (5X greater than 802.11b).	54 Mbps	Up to 54Mbps (5X greater than 802.11b).
Relative Cost	$	Inexpensive.	$$$	Relatively more expensive.	$$	Relatively inexpensive.
Frequency	2.4 GHz	More crowded 2.4GHz band. Some conflict may occur with other 2.4GHz devices like cordless phones, microwave ovens, etc.	5 GHz	Uncrowded 5GHz band can coexist with 2.4 GHz networks without interference.	2.4 GHz	More crowded 2.4GHz band. Some conflict may occur with other 2.4GHz devices like cordless phones, microwave ovens, etc.
Range	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.	25-75	Shorter range than 802.11b & 802.11g. Typically 25 to 75 feet indoors.	100-150	Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.
Public Access		The number of public "hotspots" is growing rapidly, allowing wireless connectivity in many airports, hotels, college campuses, public areas, and restaurants.	X	None at this time.		Compatible with current 802.11b hotspots (at 11Mbps). Also, it is expected that most 802.11b hotspots will quickly convert to 802.11g.
Compatibility	OK 802.11b	Widest adoption.	OK 802.11a	Incompatible with 802.11b or 802.11g.	OK 802.11b 802.11g	Interoperates with 802.11b networks (at 11Mpbs). Incompatible with 802.11a.

Securing Wireless LAN

How do you secure this network?

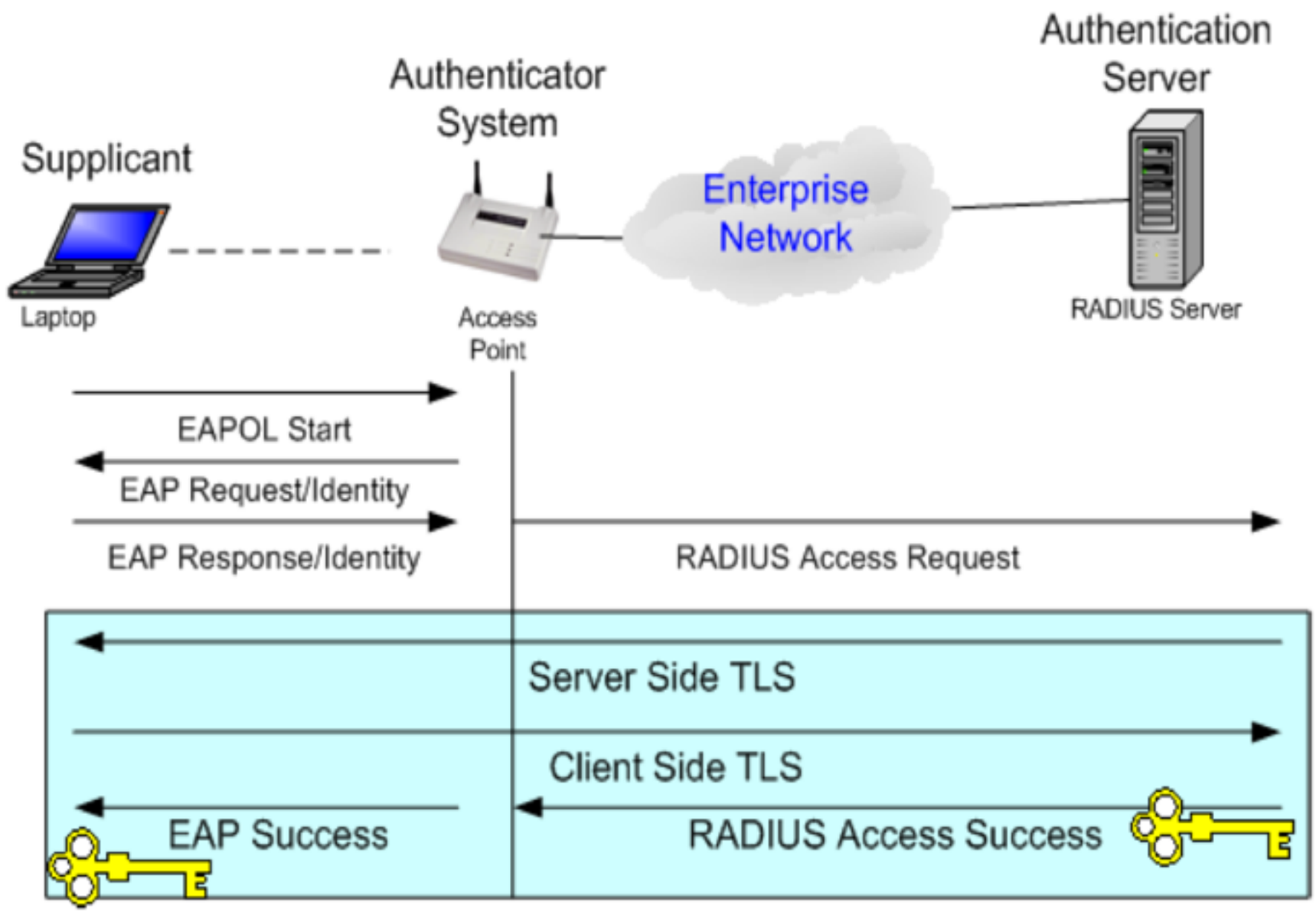
MAC Address Filtering
Authentication
RADIUS Servers
WEP Keys
VPN
Firewall

Rouge Access Point & Evil-twin Attack



IEEE 802.1x Standard

- Defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE802 which also know as EAPOL



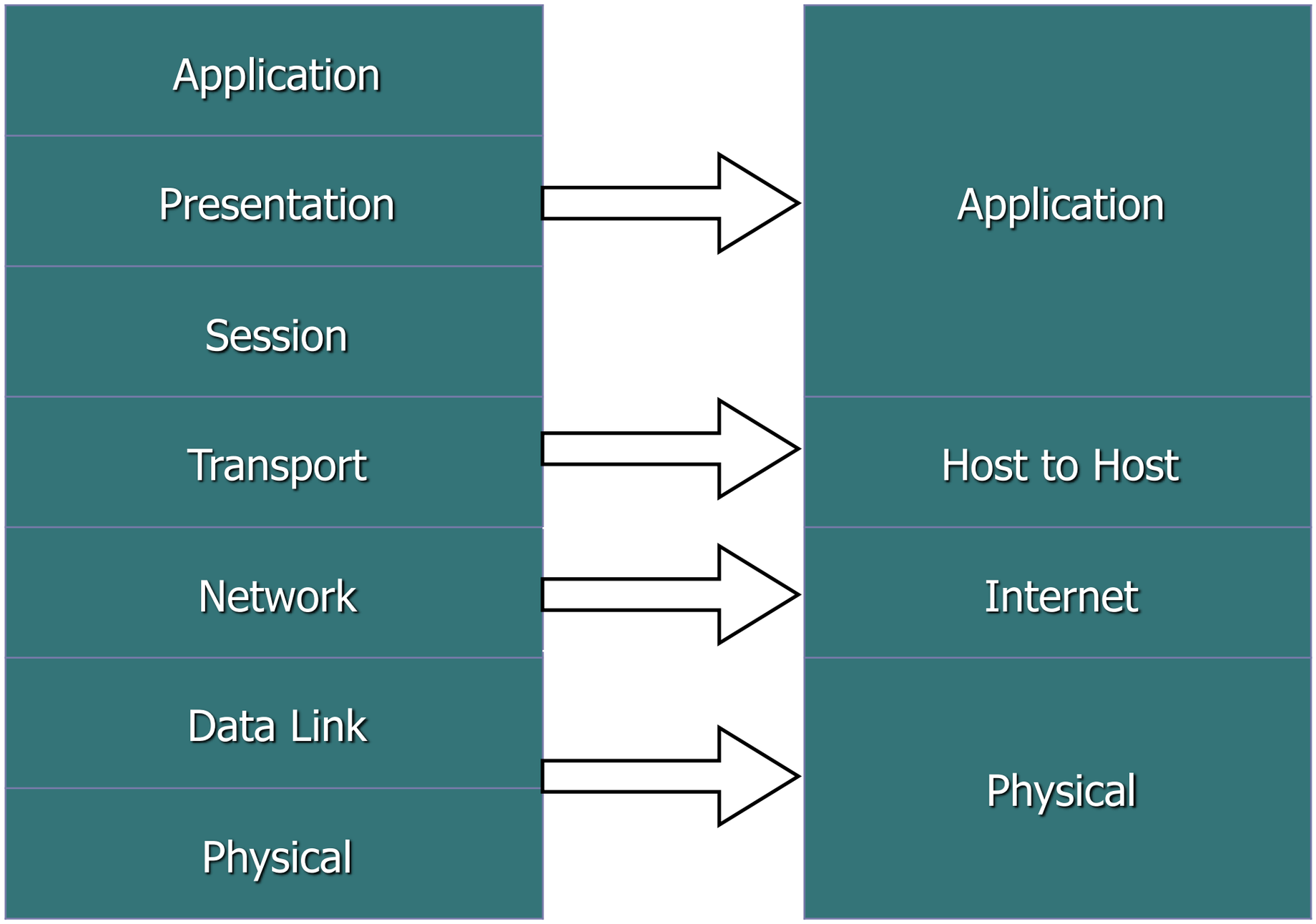
TCP/IP Fundamentals

A quick and easy way to understand TCP/IP v4.

Objectives

- Review the OSI & DoD Models
- Review TCP, UDP, & ICMP Protocols & Packet Structures
- Learn about Packet Communication Processes
- TCP/IP Commands on Linux
- Open Discussion

OSI and TCP/IP Models



IP Addressing

- Dotted Decimal
  - 192.168.20.59
- Binary
  - 11000000.10101000.00010100.00111011
- Decimal
  - 3232240699
- Hexadecimal
  - 0xC0.0xA8.0x14.0x3B

Ports and Services

- A port is a memory address space
  - Ports are numbered between 0 and 65535
  - UDP and TCP have separate spaces from 1 - 65535
  - 0 is reserved and used only in IPv6
  - Traffic on port 0 is never a good sign
- Each port may be assigned a specific service
  - Services wait and "listen" for specific requests
  - Ports from 1 - 1024 are reserved for specific services
  - Services using ports 1 - 1024 can only be assigned by root (see the list in Linux under directory /etc/services)
  - The requests are delivered to the service in the form of packets
- http://www.iana.org/assignments/port-numbers
- http://www.bekkoame.ne.jp/~s_ita/port/port1-99.html
  - IANA list with known exploits listed with port services

Popular Ports and Services

21	FTP	UDP	TCP
22	SSH	UDP	TCP
23	TELNET	UDP	TCP
25	SMTP	UDP	TCP
53	DNS	UDP	TCP
80	HTTP		TCP
110	POP		TCP
161	SNMP	UDP	TCP
162	SNMP TRAPS	UDP	TCP

How does this help us?

- Services are Identified by their responses
- All services exist in one of three states:
  - open - responds with SYN/ACK, Connect(), or in some cases, nothing as opposed to a RST
  - closed - responds with RST
  - filtered - no response because the router or firewall will not allow for any response (only possible when using TCP Connect or SYN scans)
- Remember, the only GOOD service is a filtered service. (Except when there is a Business Justification for it)

IP Protocols

- IP – Network Addressing Protocol
- TCP
- UDP
- ICMP
- Routing Protocols
  - BGP,OPSF, etc.
- Others
  - GRE, ISAKMP, IPSEC

TCP vs. UDP

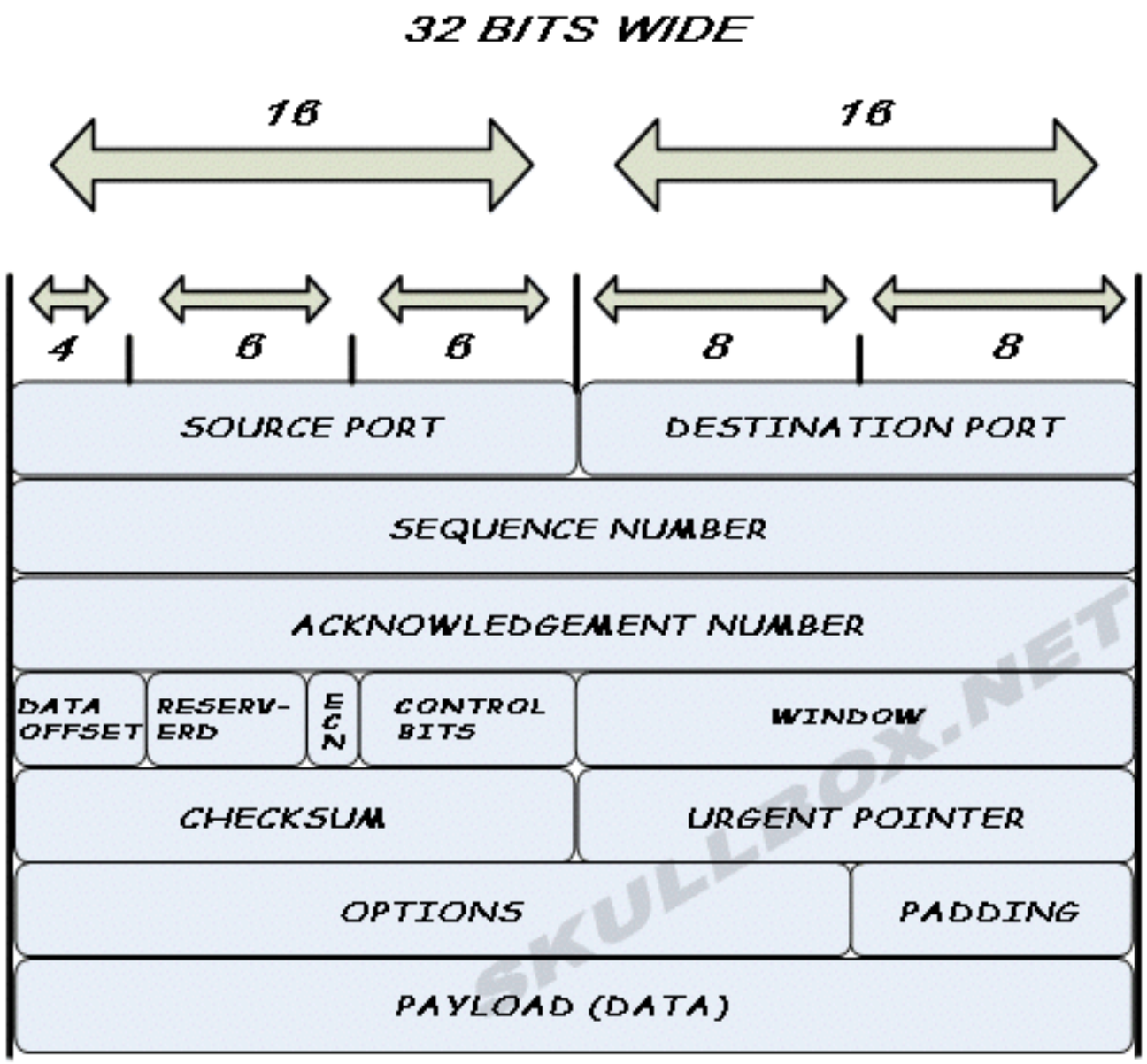
TCP

- Connection-Oriented
- Three Way Handshake
- Reliability more important than speed

UDP

- Connectionless
- No Handshake
- Speed more important than Reliability

The TCP Packet



Thanks to
Skullbox.net

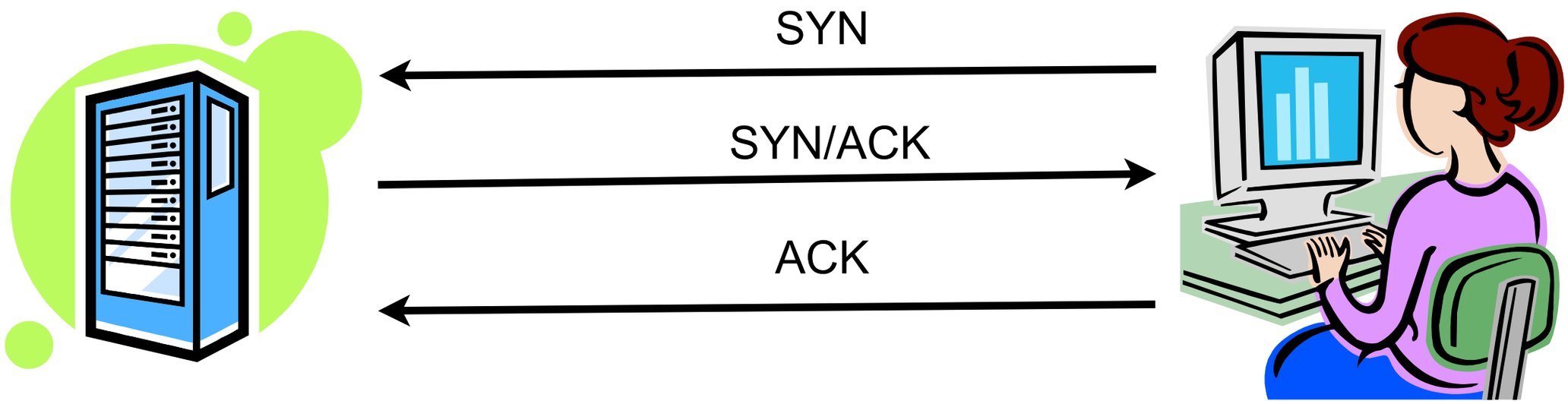
Flags

- SYN – New connection
- ACK – Acknowledging a connection or packet arrival.
- URG – Urgent Data
- PSH – Push the Data Thru (Don’t buffer)
- FIN – Finish the connection (Goodbye)
- RST – Reset (I didn’t want to talk to them anyway! [slam!])

The TCP Three Way Handshake

1. The Sending Host sends a SYN packet to the Receiving host. (Phone Rings)
2. The Receiving host response with a SYN-ACK. (Hello?)
3. The Sending Host then responds with an ACK. (HI!!)
4. The Connection is now up.

The TCP Three Way Handshake



Hacker's Use of TCP

- Hackers will mangle packets to confuse target systems.
- A confused system can give up information, provide access or even stop responding.
- Some of the common Tricks:
  - Setting no flags or all flags
  - Attempt to connect using the handshake but not complete it. This will provide a fast way to enumerate ports.
  - Setting strange combos of Flags may reveal what OS we are dealing with. (Fingerprinting)
  - Send a packet with the ACK flag set can get past some simple firewall systems.

TCP Scans

Name of Scan	Flags Set During Scan
SYN Scan	S
FIN Scan	F
Null Scan	Nothing
Xmas Scan	UPF
SYN-FIN Scan	SF
Nmap Fingerprint Attempt	UPSF

SYN Scan

If Port is Open

SYN →

← SYN/ACK

RST →

If Port is Closed

SYN →

← RST

No need to send back a RST

FIN Scan

If Port is Open

FIN →

No Answer

If Port is Closed

FIN →

← RST

No need to send back a RST

Nmap XMAS Scan

If Port is Open

URG/PSH/FIN →

No Answer

If Port is Closed

URG/PSH/FIN →

← RST

No need to send back a RST

Null Scan

If Port is Open

No Flags Sent

No Answer

If Port is Closed

No Flags Sent

RST

No need to send back a RST

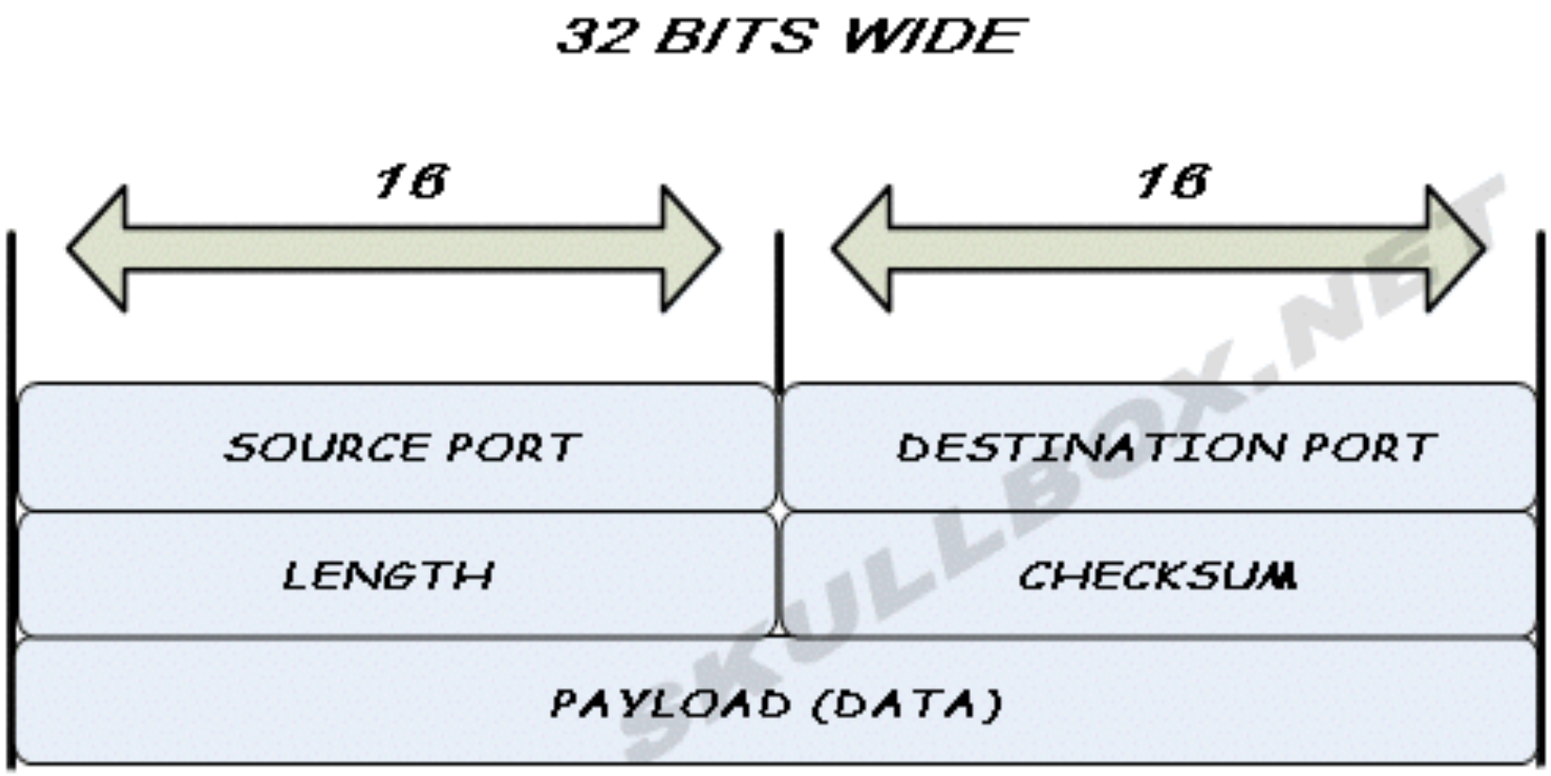
TCP Scan Comparison

Type of Scan (Flags Set)	Port is Open	Port is Closed
SYN -S	SYN/ACK	RST
FIN - F	(NOTHING)	RST
XMAS - UPF	(NOTHING)	RST
NULL – (None)	(NOTHING)	RST

The UDP Packet

- The sending host send the UDP packet
- The receiving host checks to see if the port is open and the protocol matches
- YES – Service action begins (sometimes not visible)
- NO – ICMP Type 3 error message is sent to the Sending Host.

UDP Packet Structure



Thanks to Skullbox.net for use of the graphics. For more info on TCP/IP checkout this informative site.

Scanning UDP Protocols

- Scanning UDP can be Frustrating.
  - A UDP packet that reaches a server port which is open replies with nothing
  - A UDP packet that reaches a server port which is closed replies with an ICMP type 3 message that the service is not reachable
  - A UDP packet that gets lost or dropped on the way to the server port (it happens) returns no response
  - A UDP packet that reaches a server port which is open and the protocol matches, replies with service
  - A UDP packet that reaches a server port which is closed and the firewall is configured to disallow ICMP replies, returns nothing or may return a packet which says this is not allowed by the administrator
- So Why scan UDP?
  - It is a nice place to hide for attackers
  - Most companies do not worry about UDP ports

The ICMP Packet

- Connectionless Protocol
  - Used for finding the best route across a network or the Internet
  - Influences routers
  - Used for error control messages
- Process
  - The sending computer sends an ICMP packet to a system
  - The receiving computer evaluates what service the packet is requesting and sends the proper response
  - NOTE: Sometimes the service action is not visible
  - If the service request is not allowed, a message is returned

ICMP Packet Structure

- Type
- Code
- Checksum
- Data

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             unused                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Internet Header + 64 bits of Original Data Datagram      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

ICMP Packet Types

Type	Description	Family
0	Echo Reply	Query (Reply)
3	Destination Unreachable	Error
4	Source Quench	Error
5	Redirect	Error
8	Echo Request	Query (Request)
9	Router Advertisment	Query (Reply)
10	Router Solicitation	Query (Request)
11	Time Exceeded	Error
12	Parameter Problem	Error
13	Timestamp Request	Query (Request)
14	Timestamp Reply	Query (Reply)

ICMP Packet Codes

- Type 3 Destination Unreachable [RFC792]
- Codes
  - 0 Net Unreachable
  - 1 Host Unreachable
  - 2 Protocol Unreachable
  - 3 Port Unreachable
  - 4 Fragmentation Needed and Don't Fragment was Set
  - 5 Source Route Failed
  - 6 Destination Network Unknown
  - 7 Destination Host Unknown
  - 9 Communication with Destination Network is Administratively Prohibited
  - 10 Communication with Destination Host is Administratively Prohibited

- http://www.faqs.org/rfcs/rfc792.html

Linux Networking Commands

- Ifconfig
- Dhclient
- Ping
- Traceroute

ifconfig

- Command line configuration for interfaces
- ifconfig –i eth0 address 192.168.1.1 netmask 255.255.255.0

dhclient

- Easy command used to configure your interface for use with DHCP.
- dhclient eth0
- Next run ifconfig to view the interface configuration.

Other Commands

- Ping – Detect if another host is reachable
- Traceroute – Determine the path to another host
- Dig – Utility for checking DNS resolution

Other Fun Networking Utils

- Nmap – Network Port Scanner
- Nessus – De Facto Standard in Network Vulnerability Scanning.
- Wireshark – (a.k.a Ethereal) Network Sniffer
- Many other tools!

One Last Note

- A big part of using TCP/IP is subnetting.
- The best way to learn is to practice!
- Many books and Online sources for learning how to Subnet.

Network Monitoring

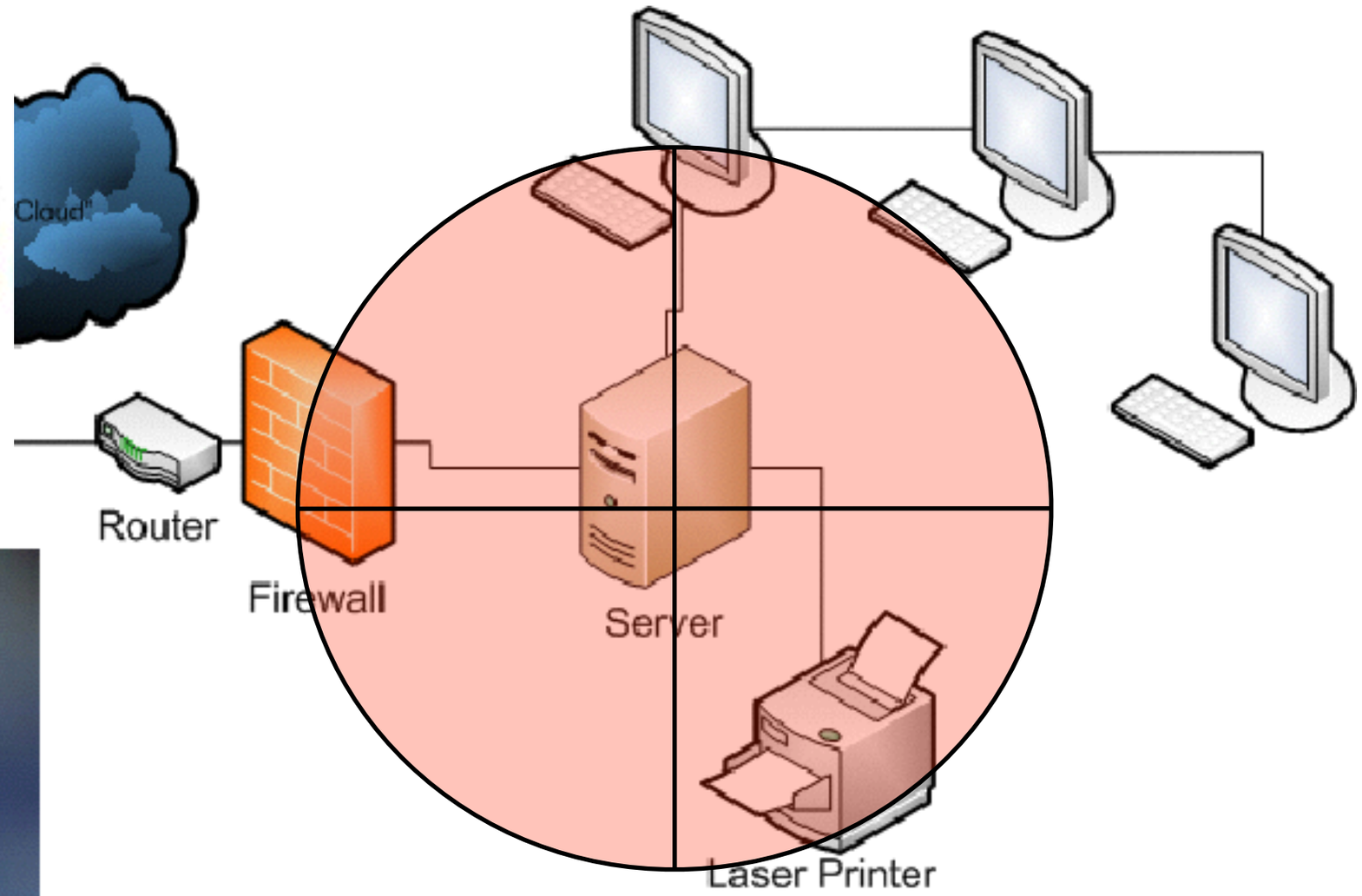
Kitisak Jirawannakool

Electronics Government Agency
(public organisation)

Agenda

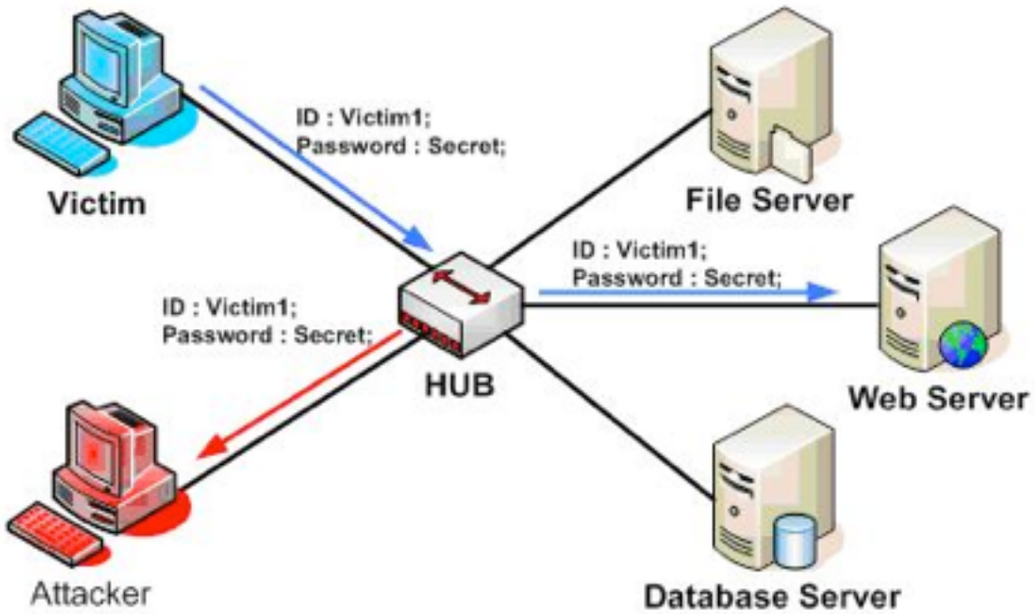
- What is Network monitoring?
- Why we need?

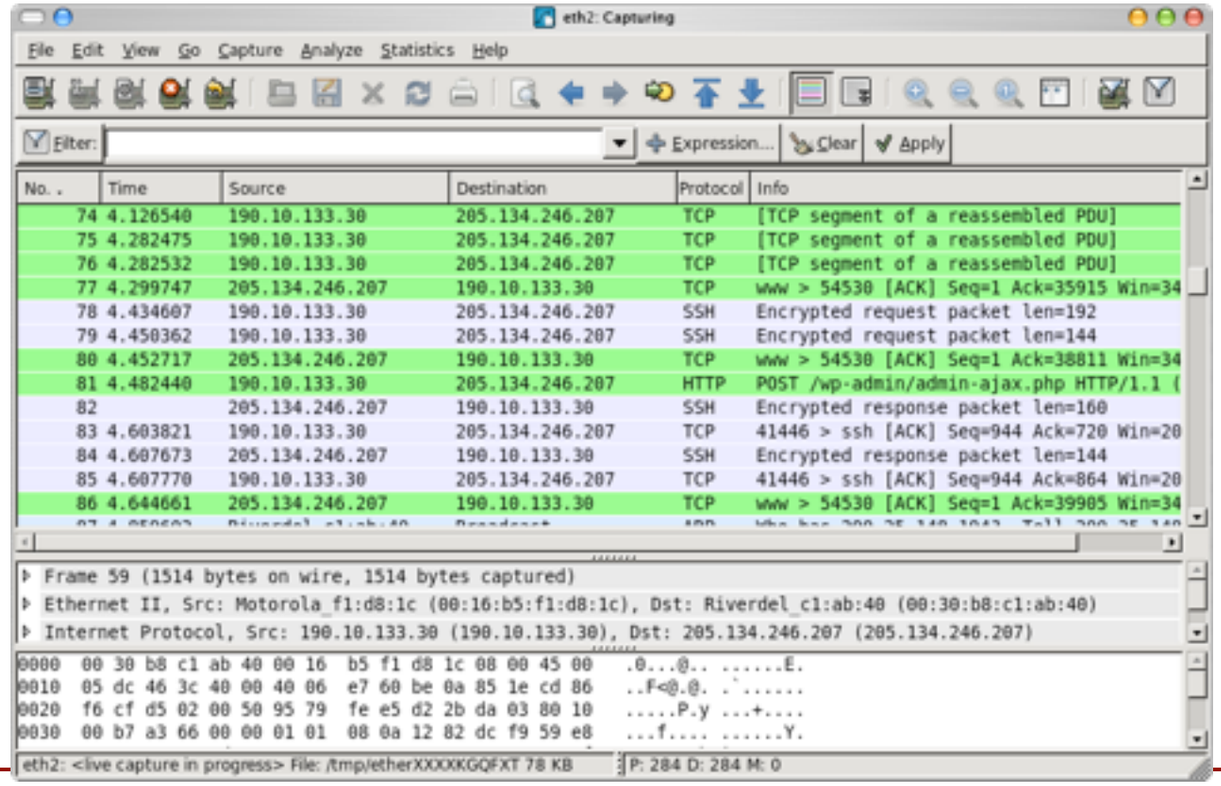
What is Network Monitoring?



Eavesdropping

Network Eavesdropping





Why we monitor?

- Network Capacity Design
  - Do we have to purchase ADSL or Lease line?
- Performance Monitoring
  - Fast enough? Too Slow?
  - Packet losses?
- Maintain Security
  - Malware (Bot, Key logger)
  - Insider threat (Policy violation)

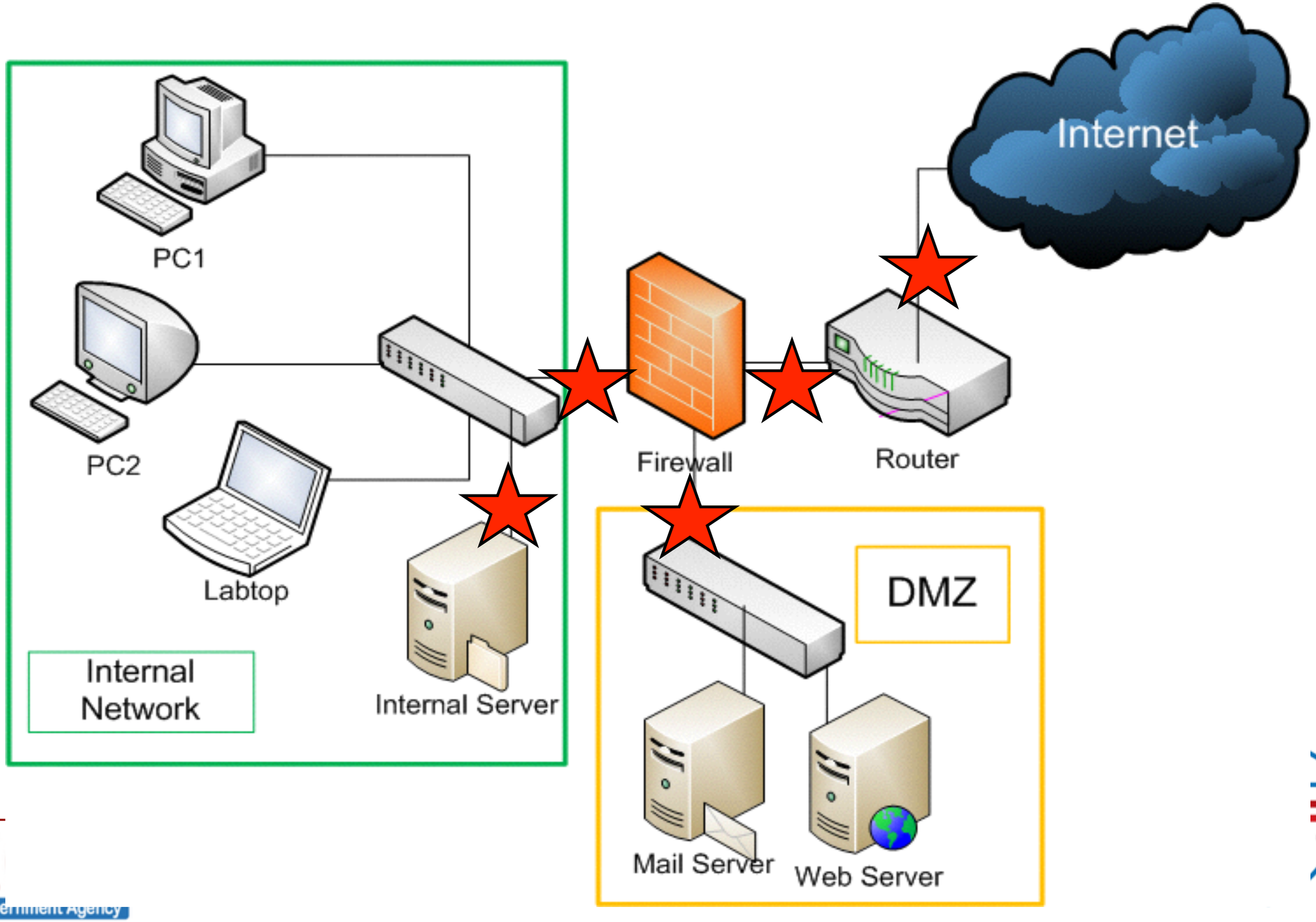
Network Monitoring methods

- Intrusion Detection: Intrusion detection monitors local area networks for unauthorized access by hackers.
- Packet Sniffing: A packet sniffer is a program that inspects every packet of information that passes through the network.
- Vulnerability Scanning: A vulnerability scanner will periodically scan the network for vulnerabilities and weaknesses which open up the potential for an exploit.
- Firewall Monitoring: Firewalls monitor the traffic that is coming in and out of the network.
- Penetration Testing: Penetration testing is carried out by IT professionals by using methods that hackers use to breach a network

How to monitor the network?

- Using monitoring agent
  - software/tools
  - port mirroring on network switch or router
    - aggregate all traffic that are processed by a network switch into one single port.
  - use shared hub
    - Shared hub is more expensive than a switching hub!!!
  - network tap
    - Can be installed without modifying your network design.

Where to monitor?



Where to monitor?

- Out side of Firewall
  - To understand what is going on the side of "THE INTERNET".
  - Research purpose.
  - Since it's a chaotic world, you will see too many suspicious flow.
- DMZ
  - To understand threat by external attack
- Local network
  - Monitor traffic within your corporate network
  - Prevent information leakage

What we can't do with network monitor?

- Monitor Encrypted traffic SSL, IPSec, SSH, HTTPS, and other
- Active protection
  - Network monitoring is Not for protect, not for filter, just watching what's in and out
  - Network monitoring system may not send any packet
- Monitor Huge traffic
  - Difficult to monitor everything because of tons of traffic
- Finding Targeted Attacks

Legal and Privacy

- We should be sure if network monitoring is clear to do by aspect of
  - Legal
    - Checking only in your country is enough ?
    - Any branches in other countries…
  - Privacy
    - Full traffic monitoring may contain privacy data
      - E-mail contents
      - Web history
      - Password

Legal and Privacy

- Organizational Policy
  - Advertise that you are monitoring network
  - For users

- Ethic
  - Some cases, we can monitor neighborhood wireless traffic…
  - Is hotel wireless/network

Challenges

- Network baselines
- Topology, locating the problem
- Visualization at scale
- Knowledge management
- Privacy
- Mixing and matching record types

Questions?