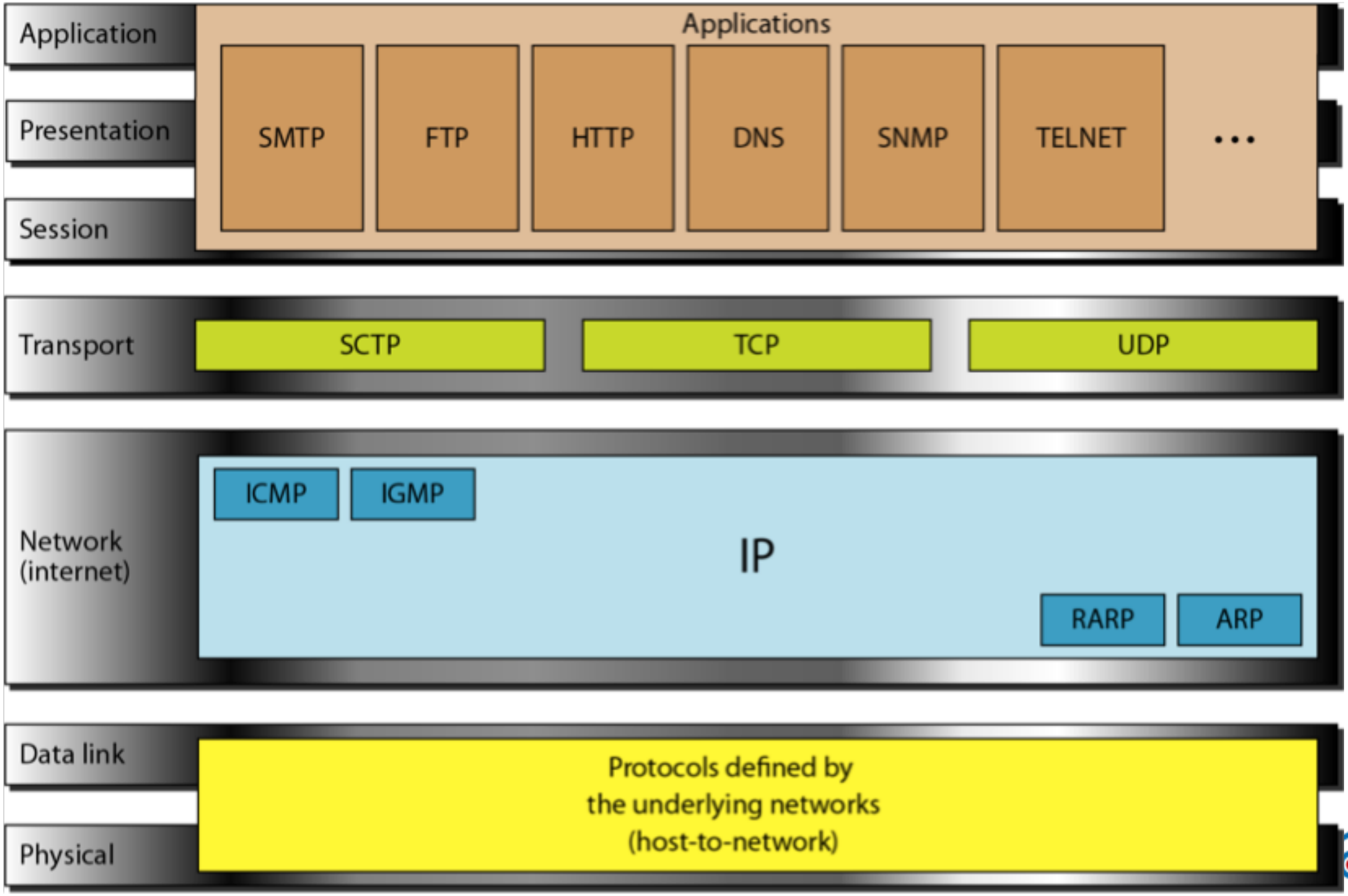
Network Security

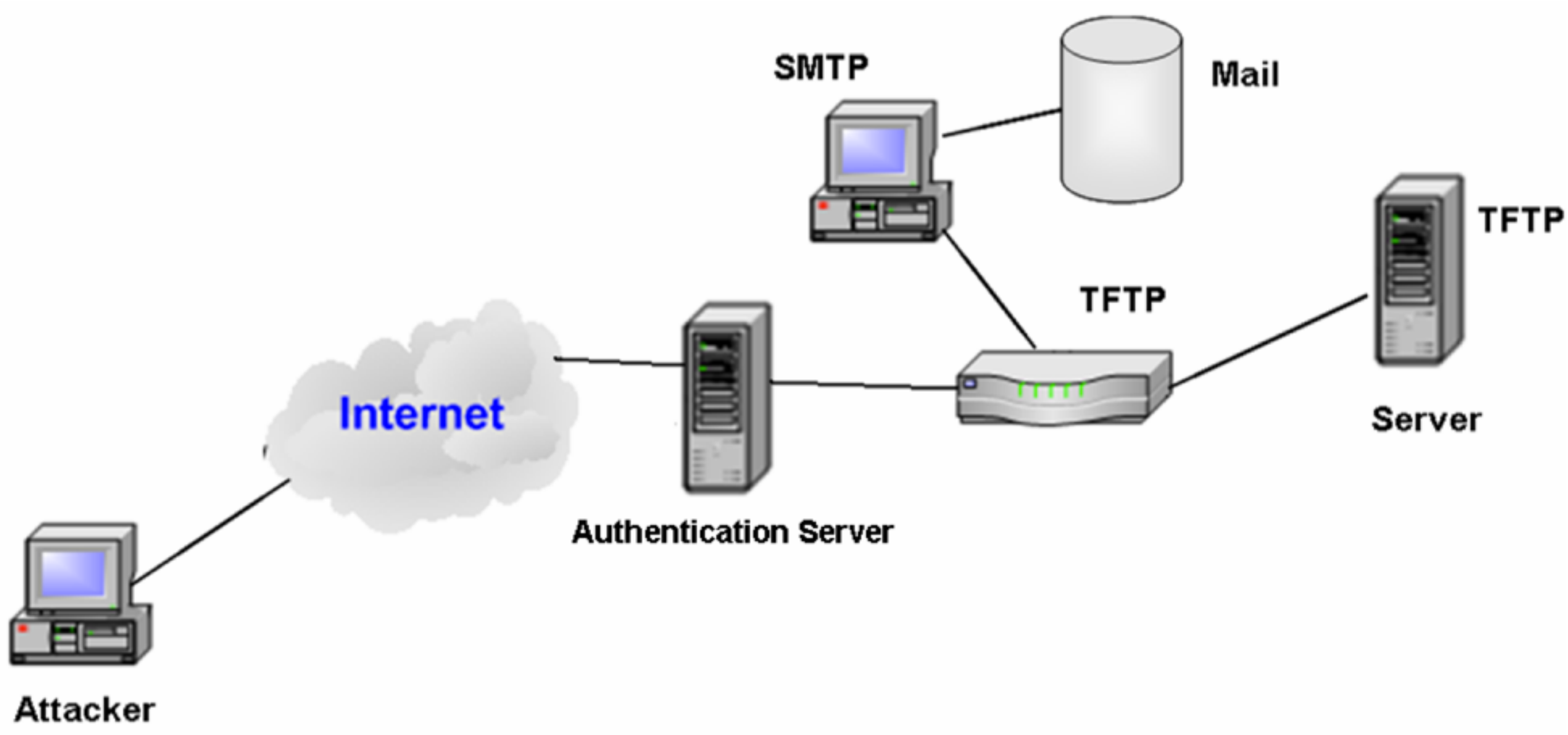
Kitisak Jirawannakool

Electronics Government Agency
(public organisation)

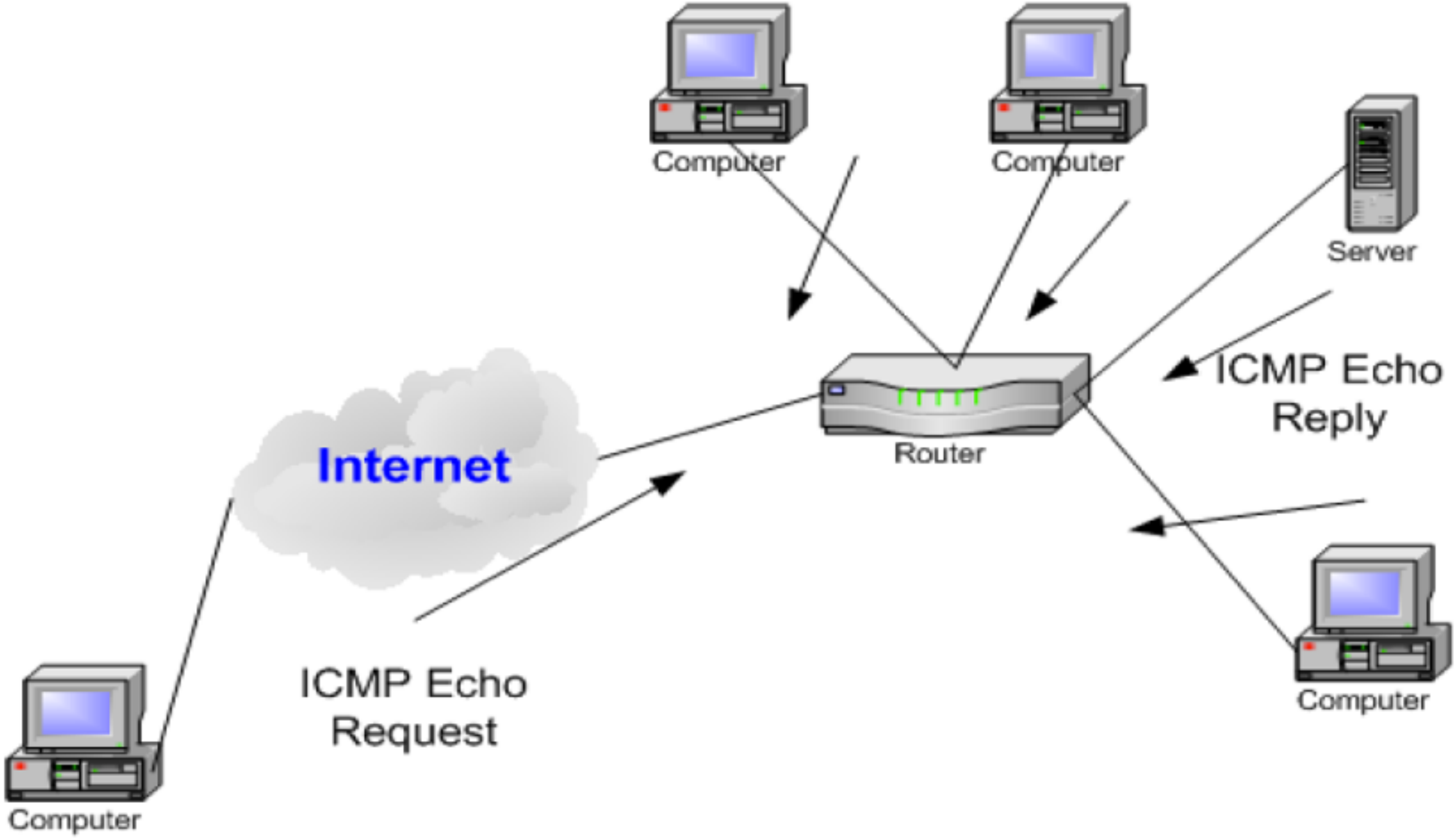
OSI Model vs TCP/IP suite



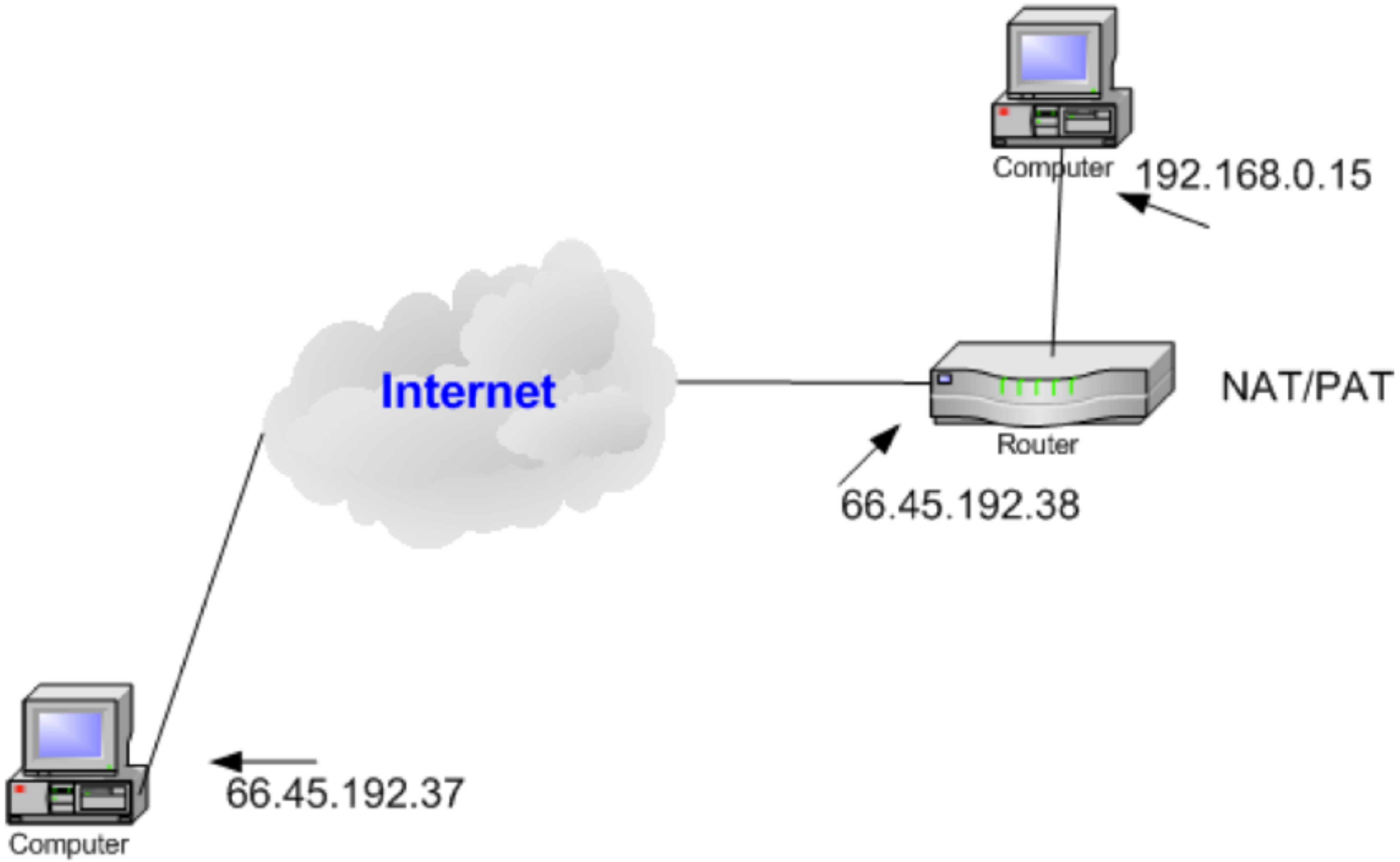
TFTP & SMTP


SMTP
Mail
TFTP
TFTP
Server
Internet
Authentication Server
Attacker

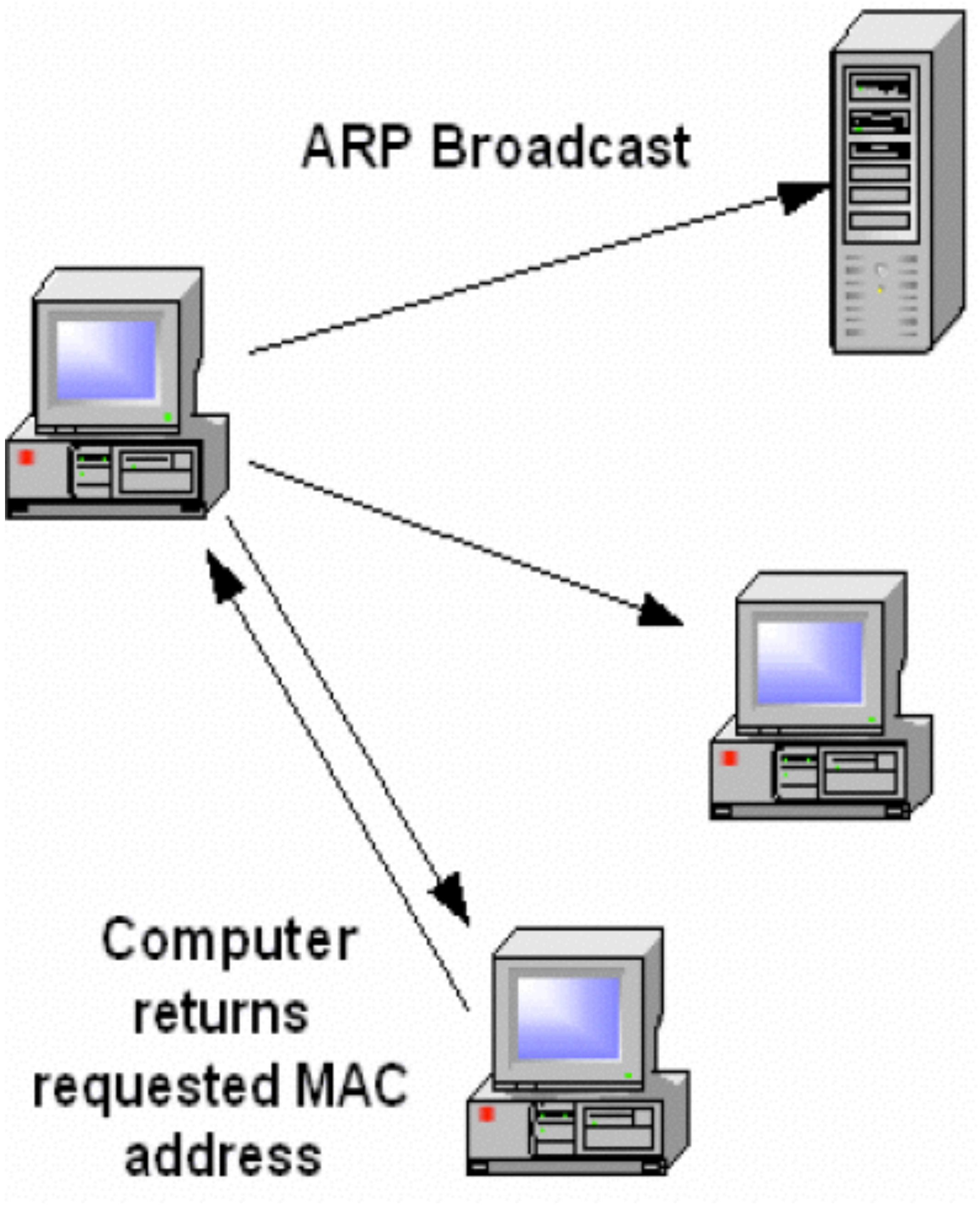
ICMP


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

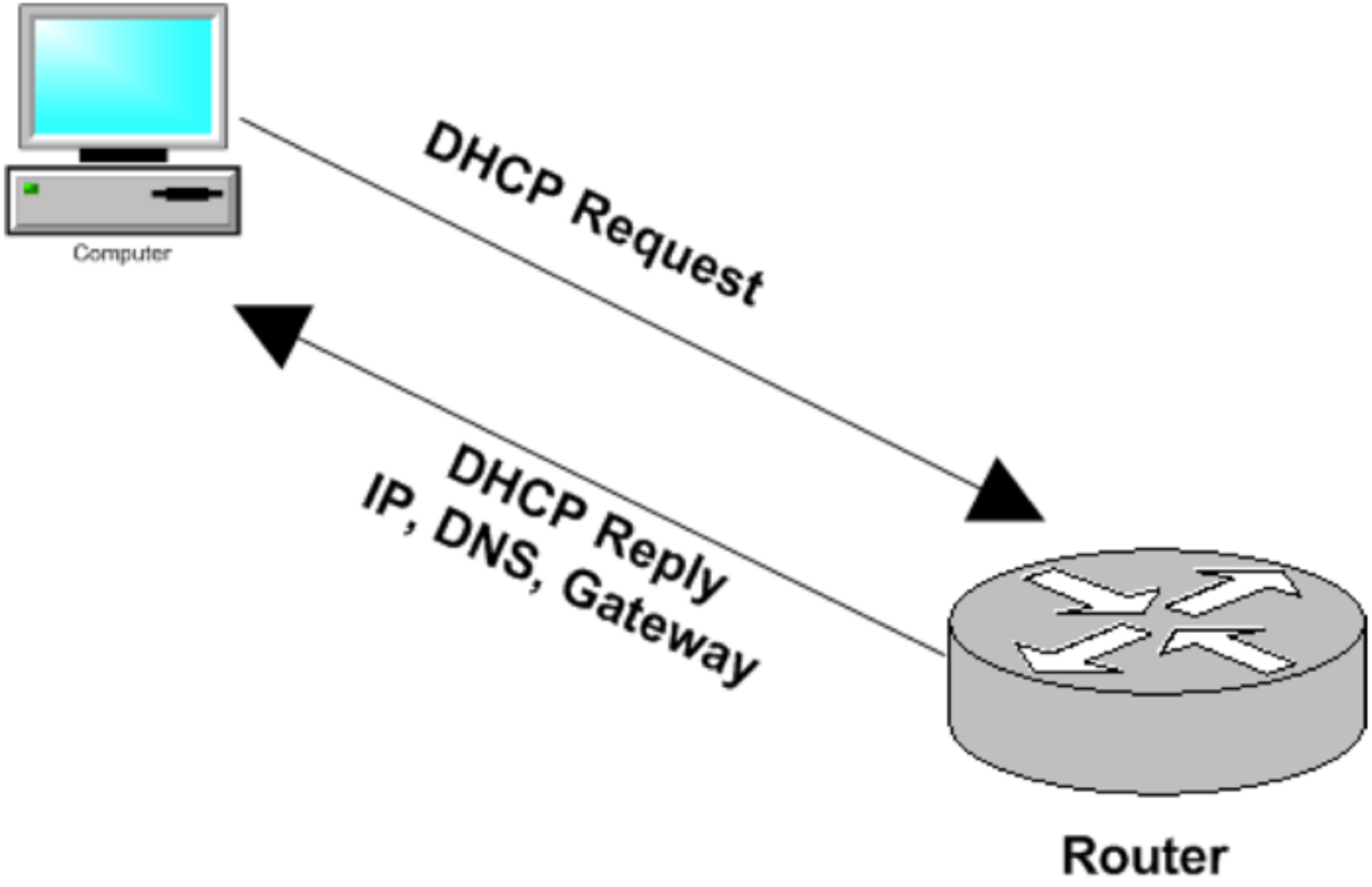
NAT/PAT


Computer
192.168.0.15
Internet
NAT/PAT
Router
66.45.192.38
66.45.192.37
Computer

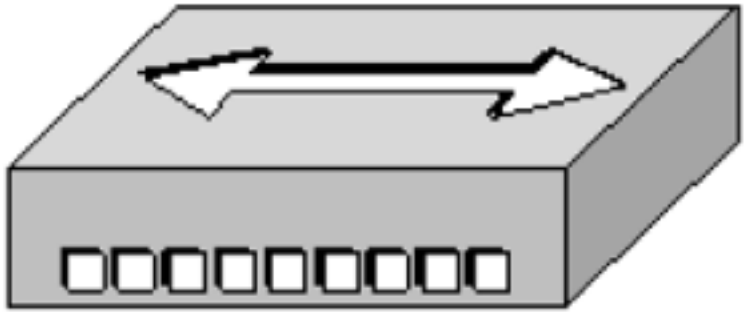
ARP/RARP



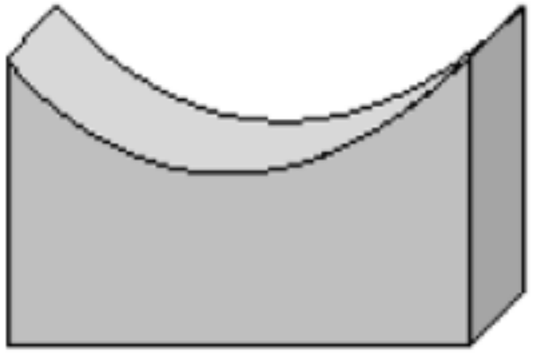
DHCP



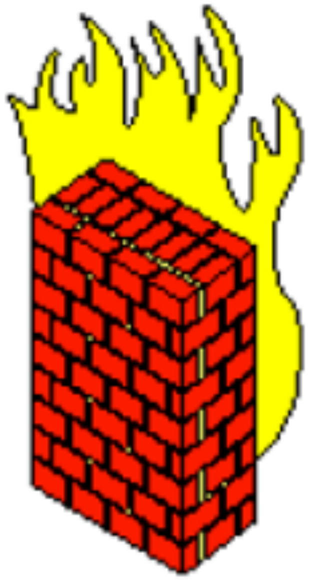
Network Connection Devices



Hub



Bridge



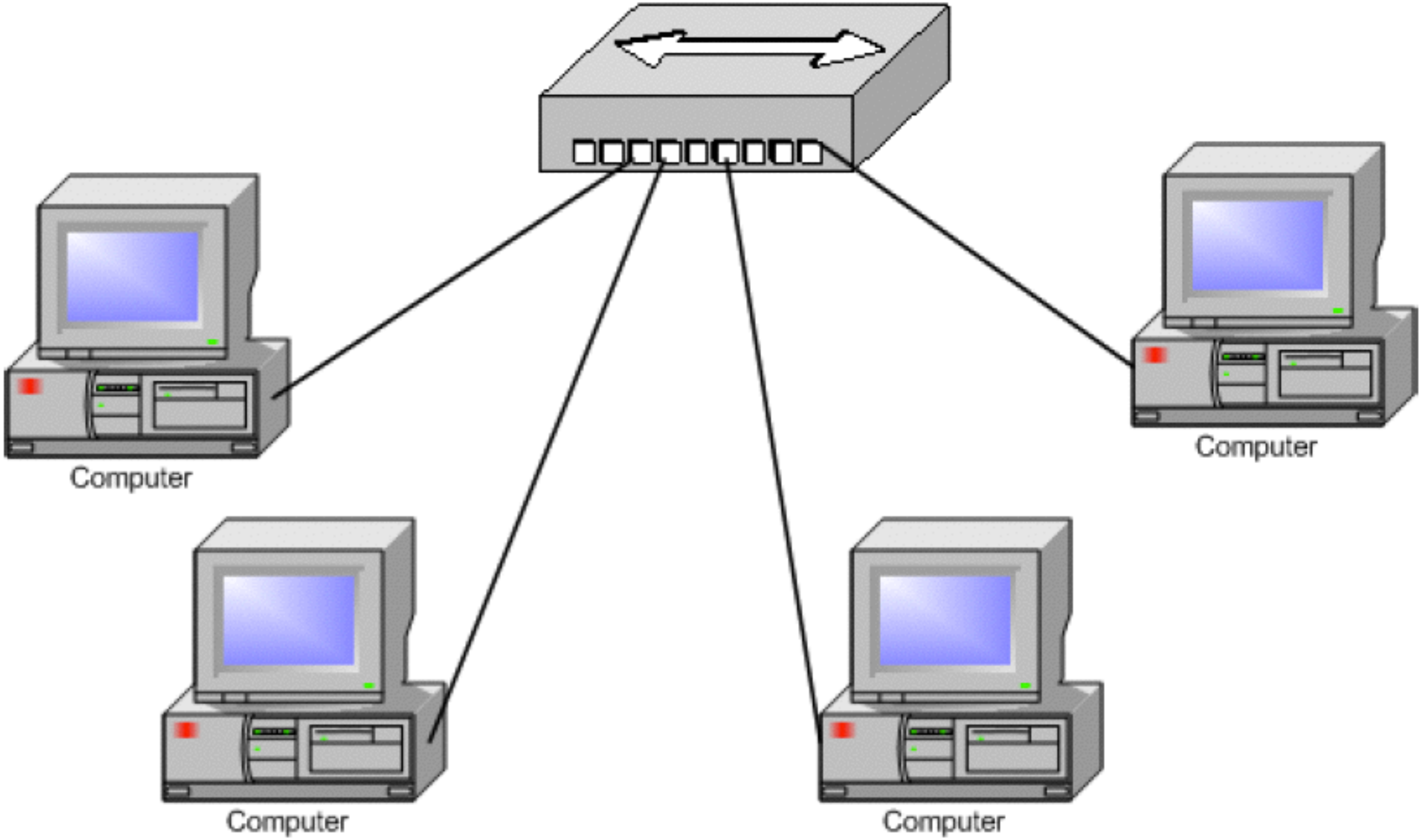
Firewall

Switch

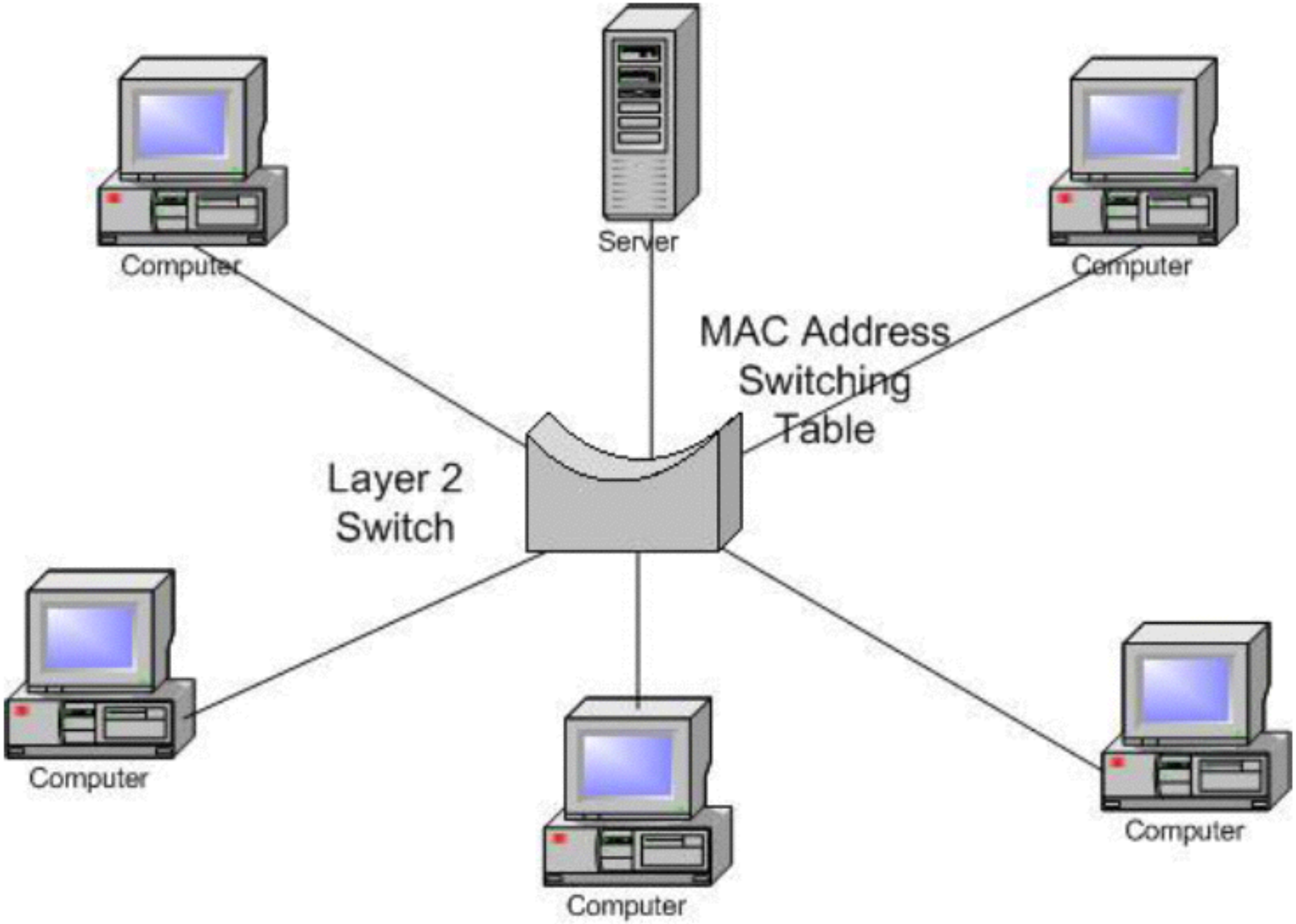
Router

Wireless Access Point

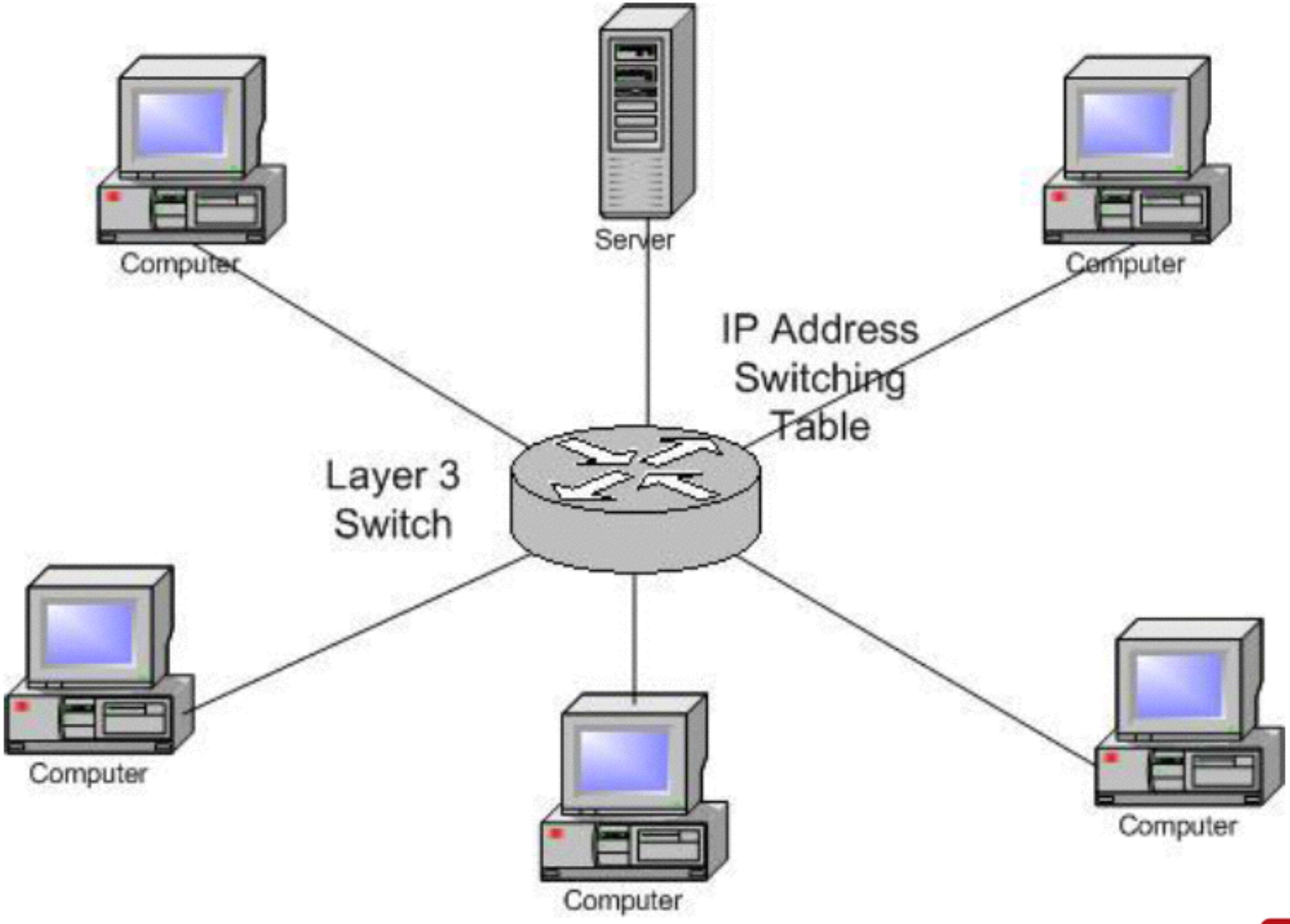
Hub Operation



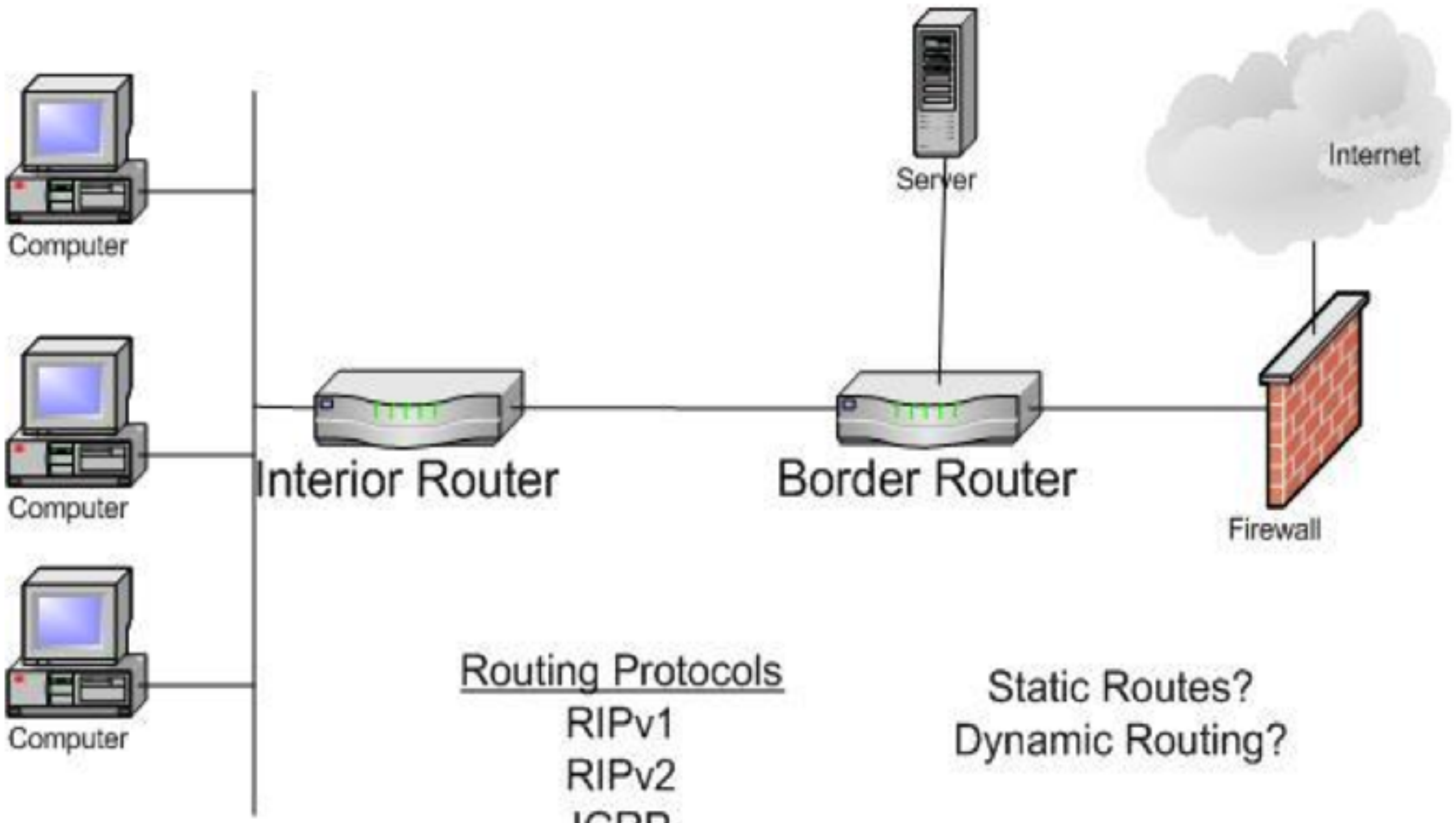
Layer 2 Switch Operation



Layer 3 Switch Operation



Router & Routing Protocols



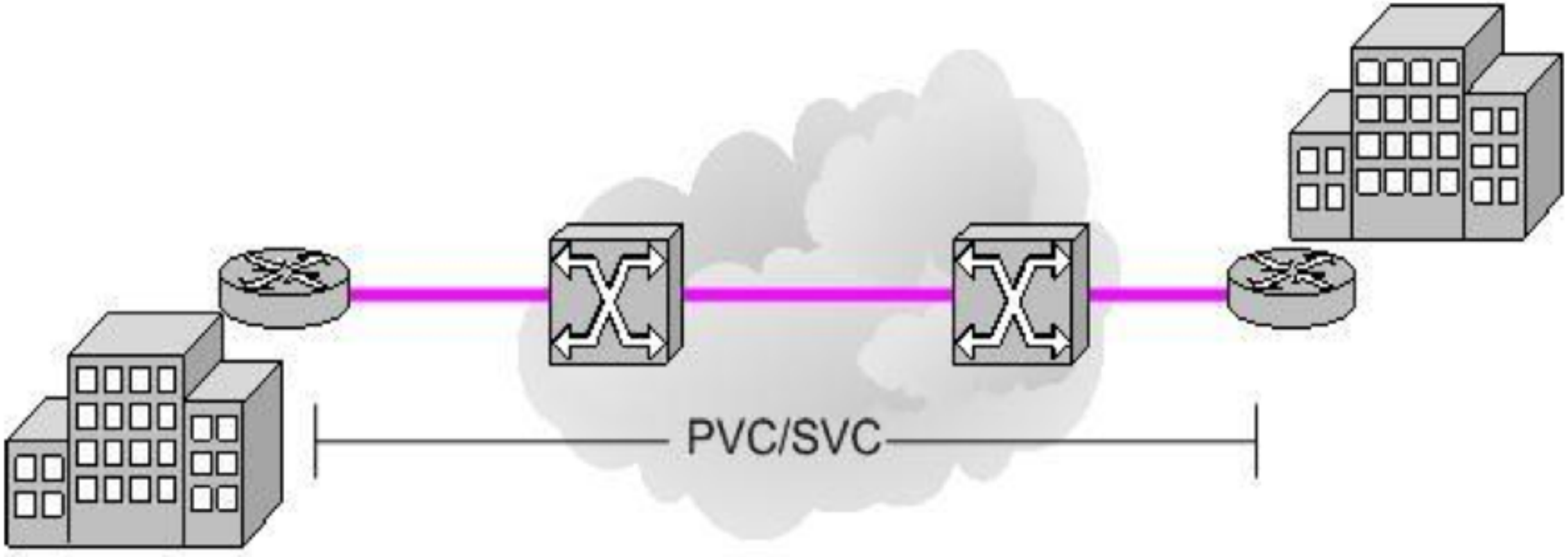
<u>Routing Protocols</u>

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

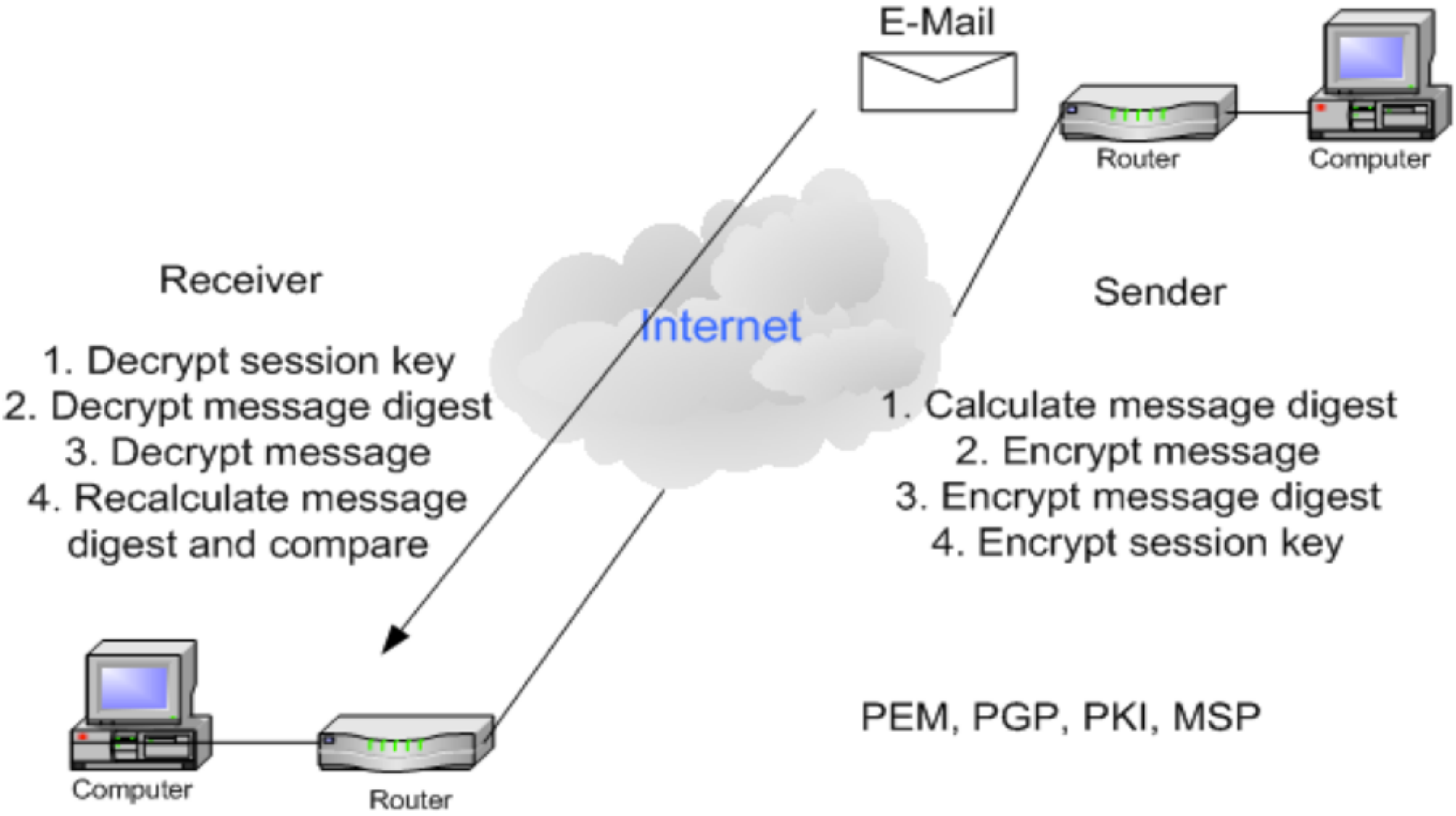
SMDS

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



Receiver

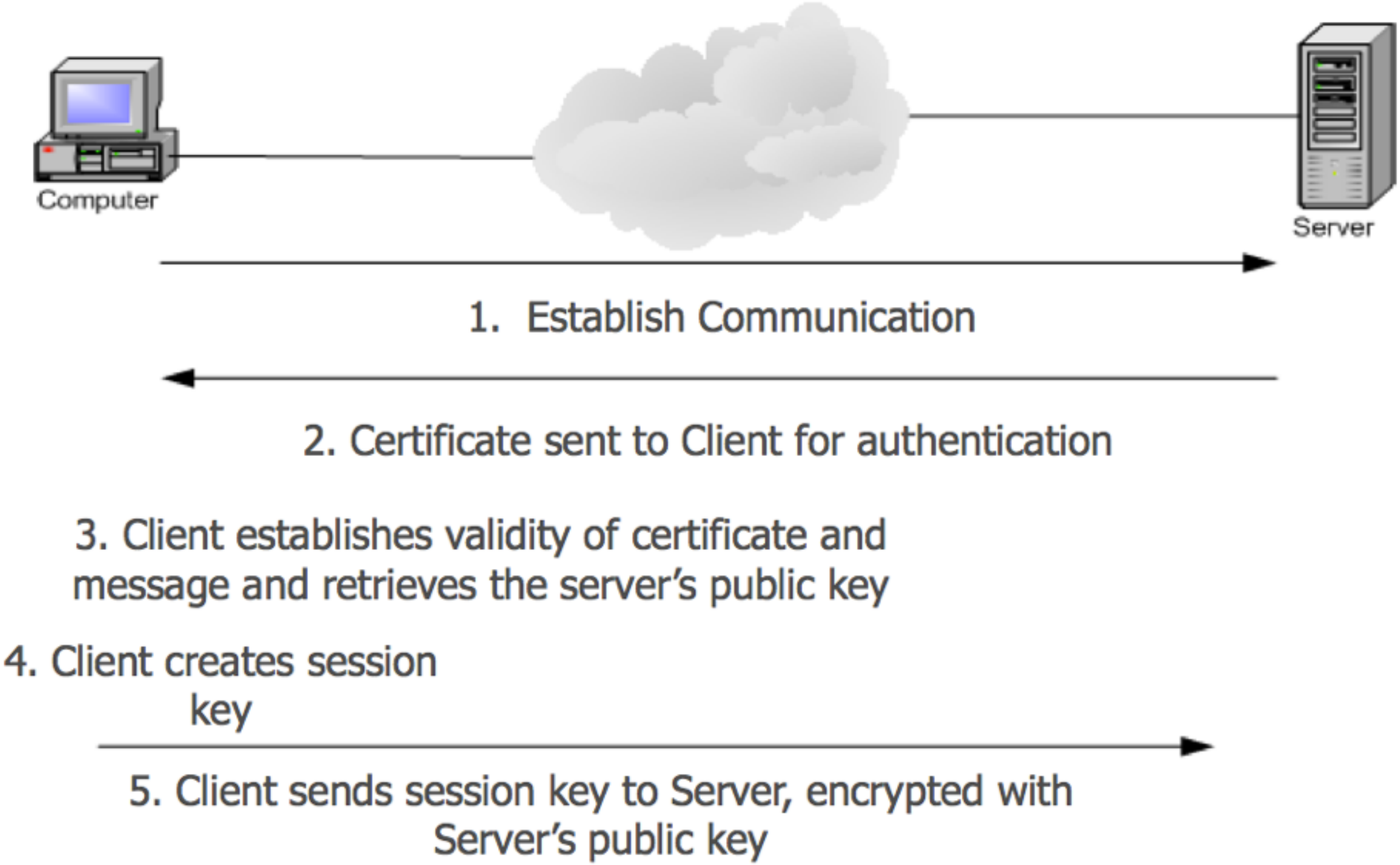
1. Decrypt session key
2. Decrypt message digest
3. Decrypt message
4. Recalculate message digest and compare

Sender

1. Calculate message digest
2. Encrypt message
3. Encrypt message digest
4. Encrypt session key

PEM, PGP, PKI, MSP

Secure Socket Layer (SSL)



1. Establish Communication

2. Certificate sent to Client for authentication

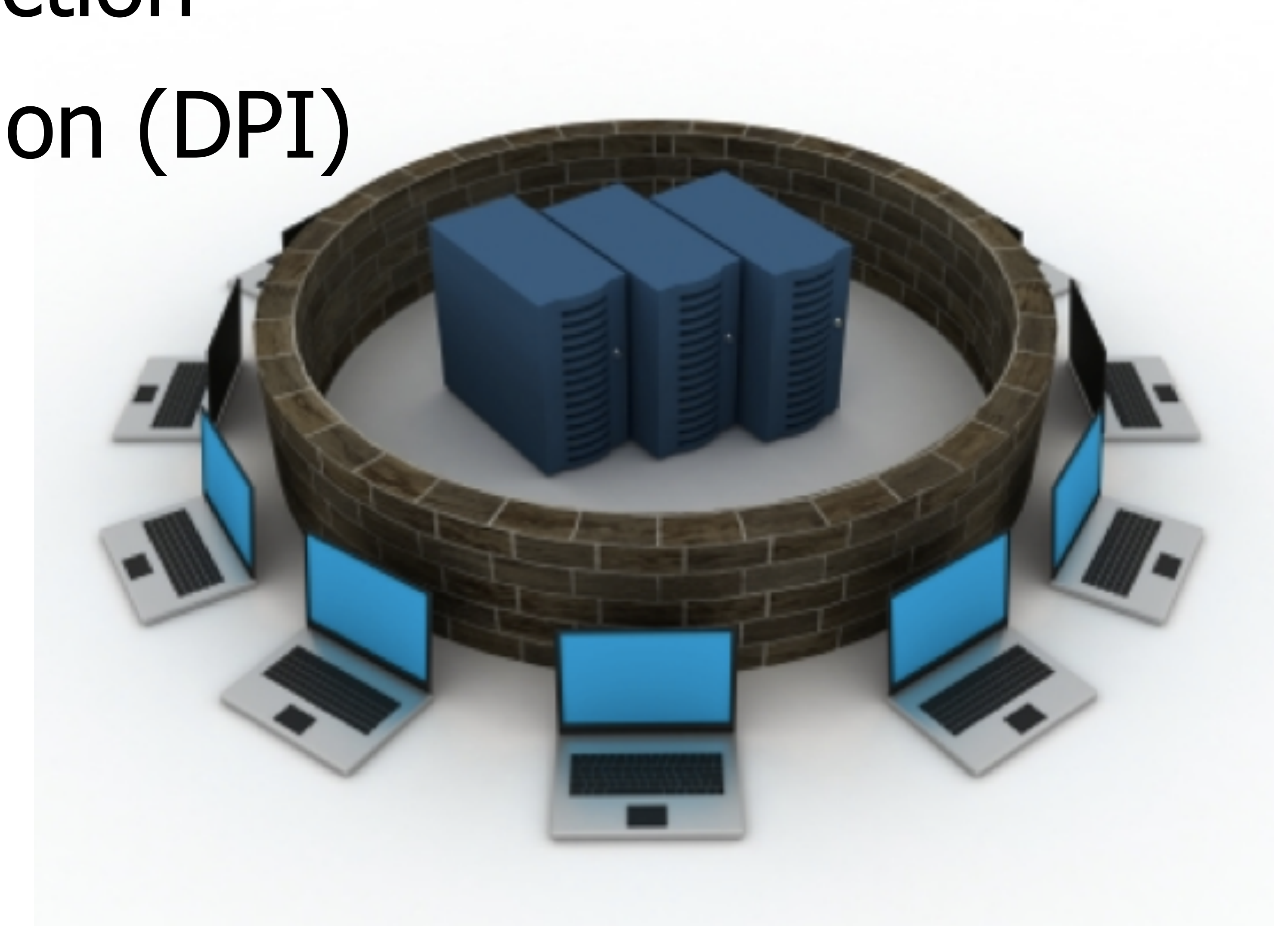
3. Client establishes validity of certificate and message and retrieves the server's public key

4. Client creates session key

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

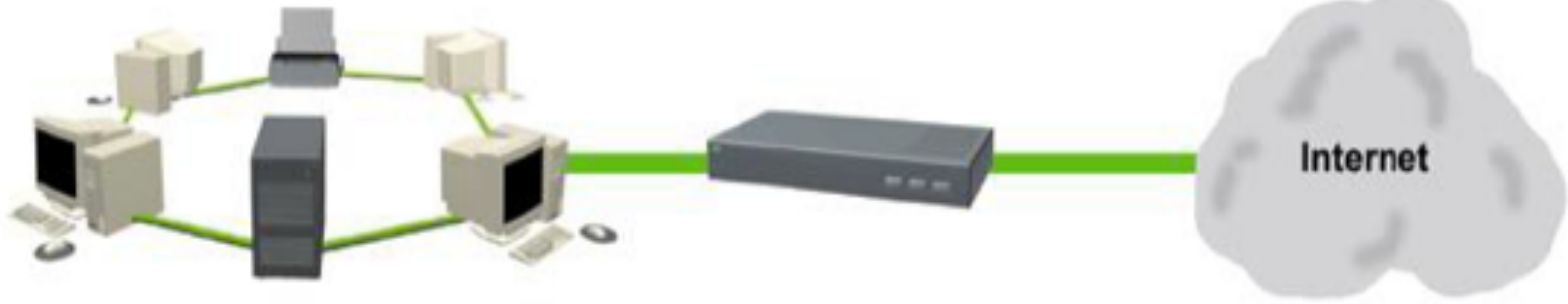
Firewall

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

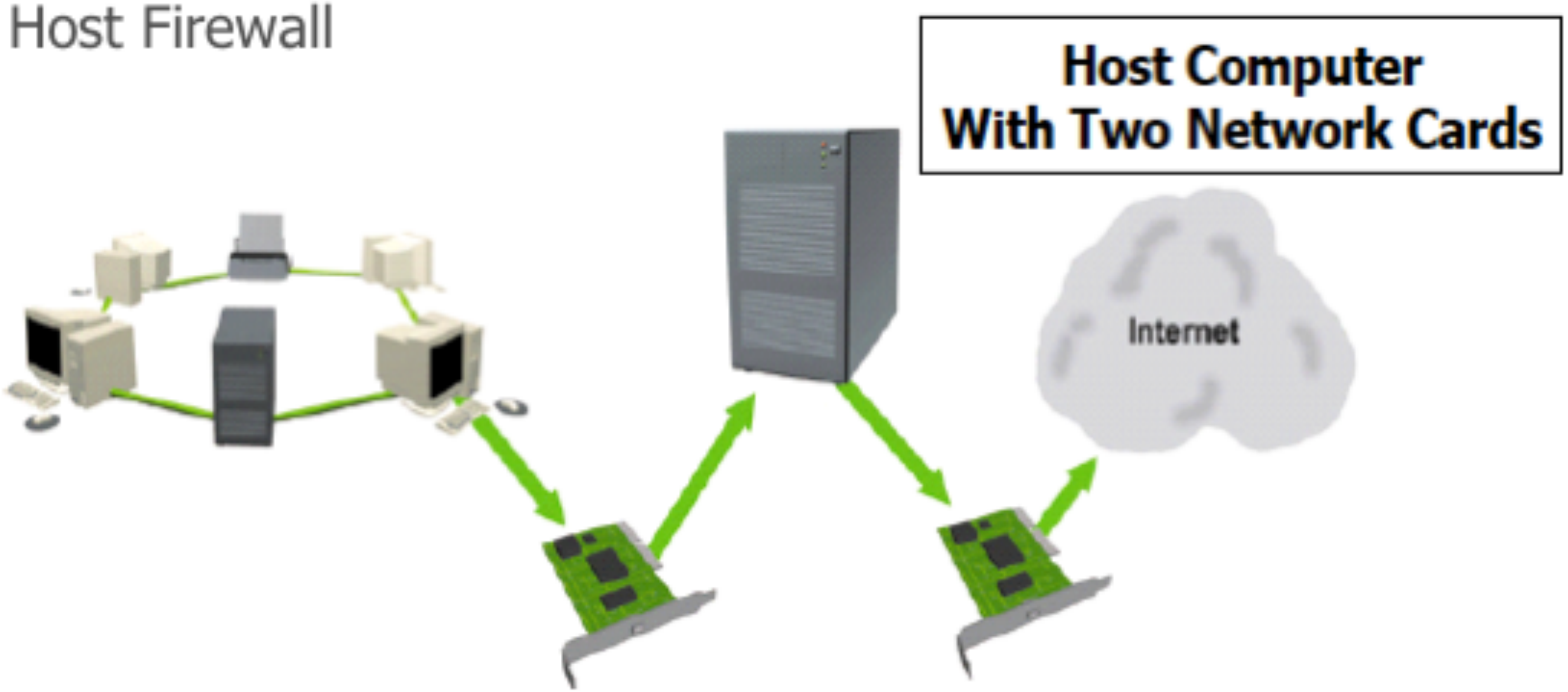


Firewall Configuration

- Boundary Packet Filtering Router

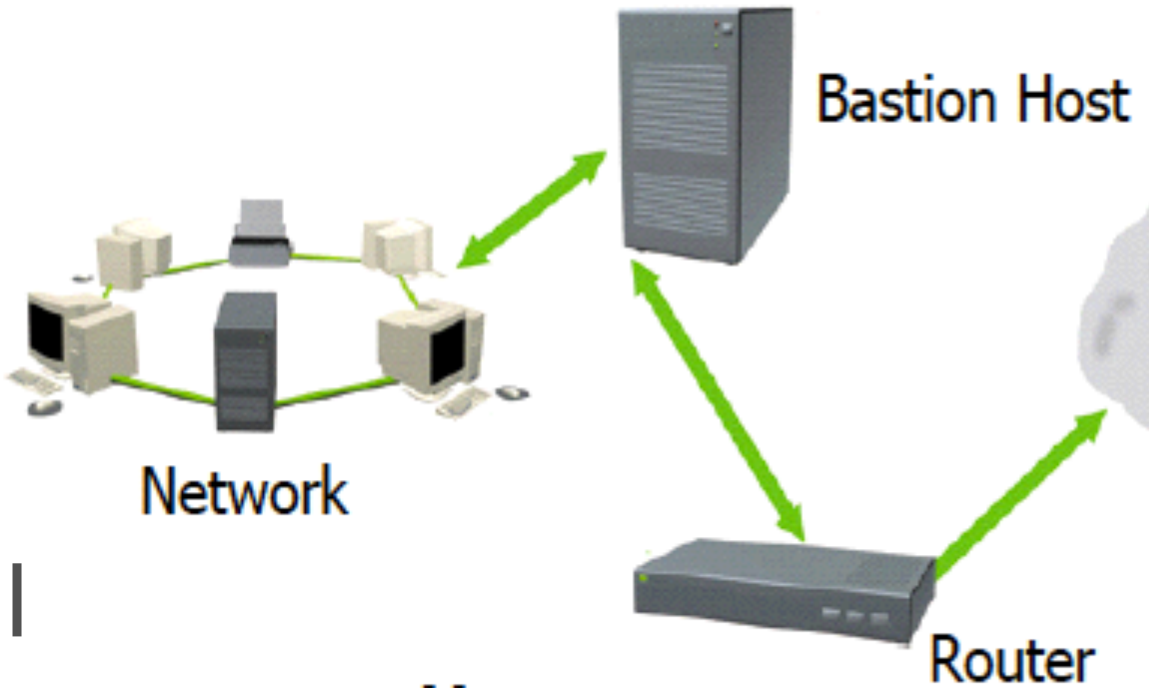


- Dual Homed Host Firewall

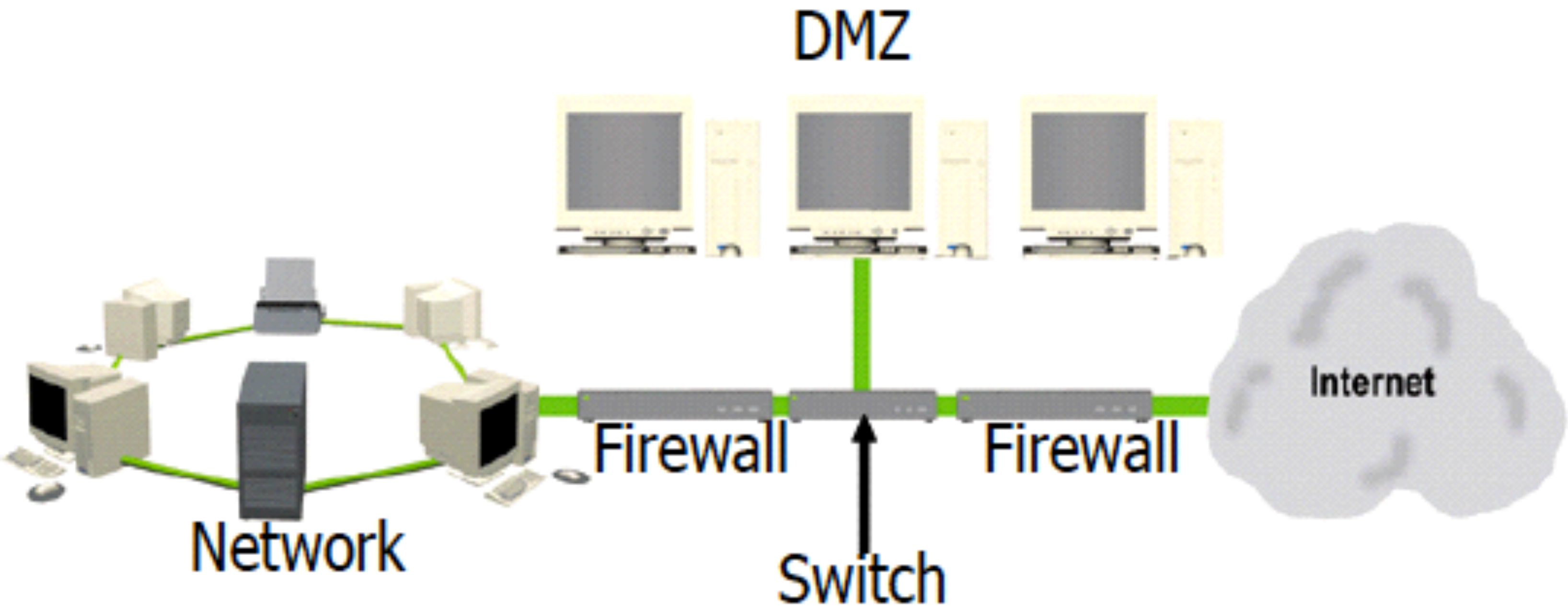


Firewall Configuration

- Screened-Host Firewall



- Screened Subnet Firewall



IDS Component

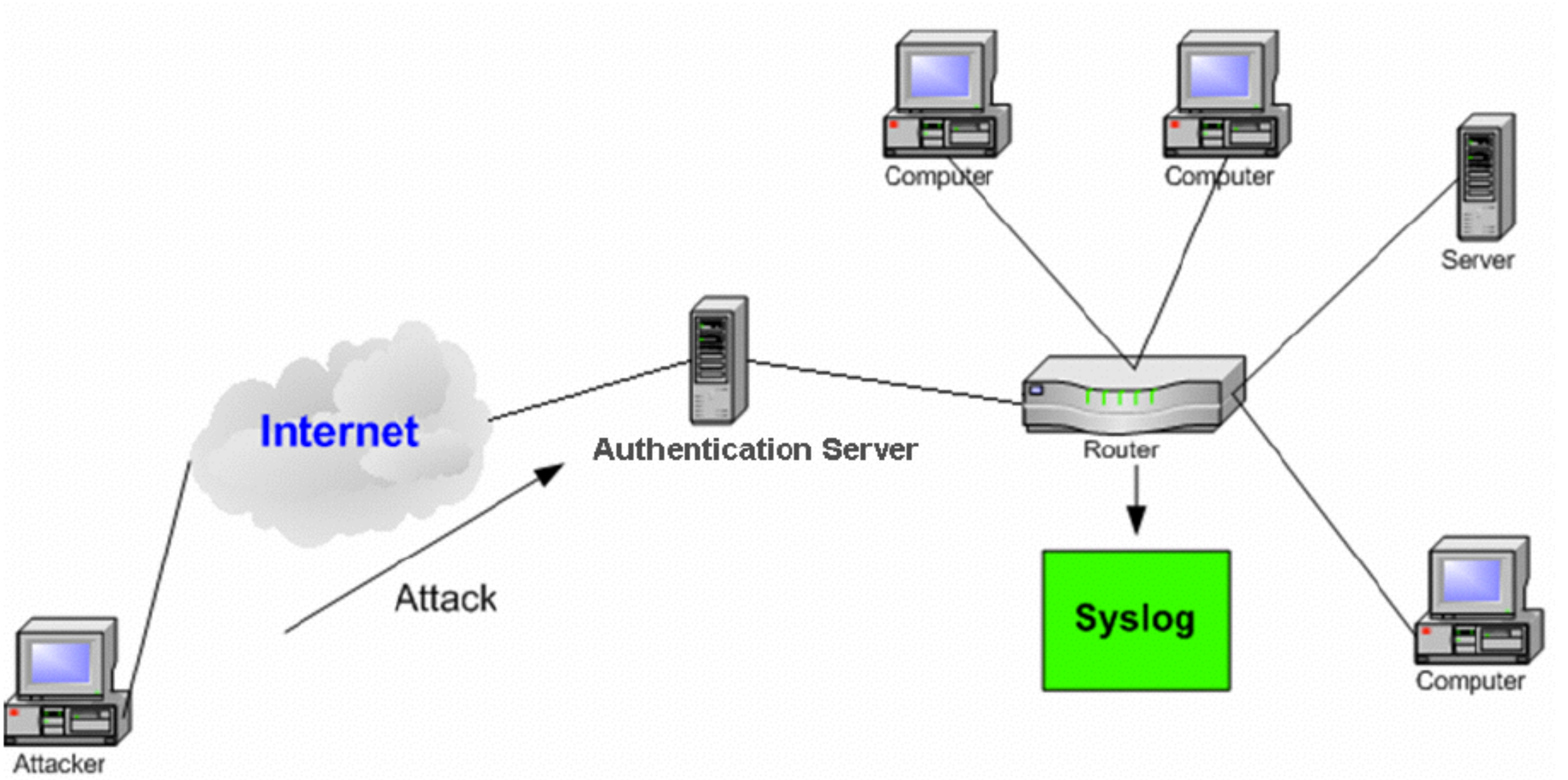
Traffic collector:

- 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.

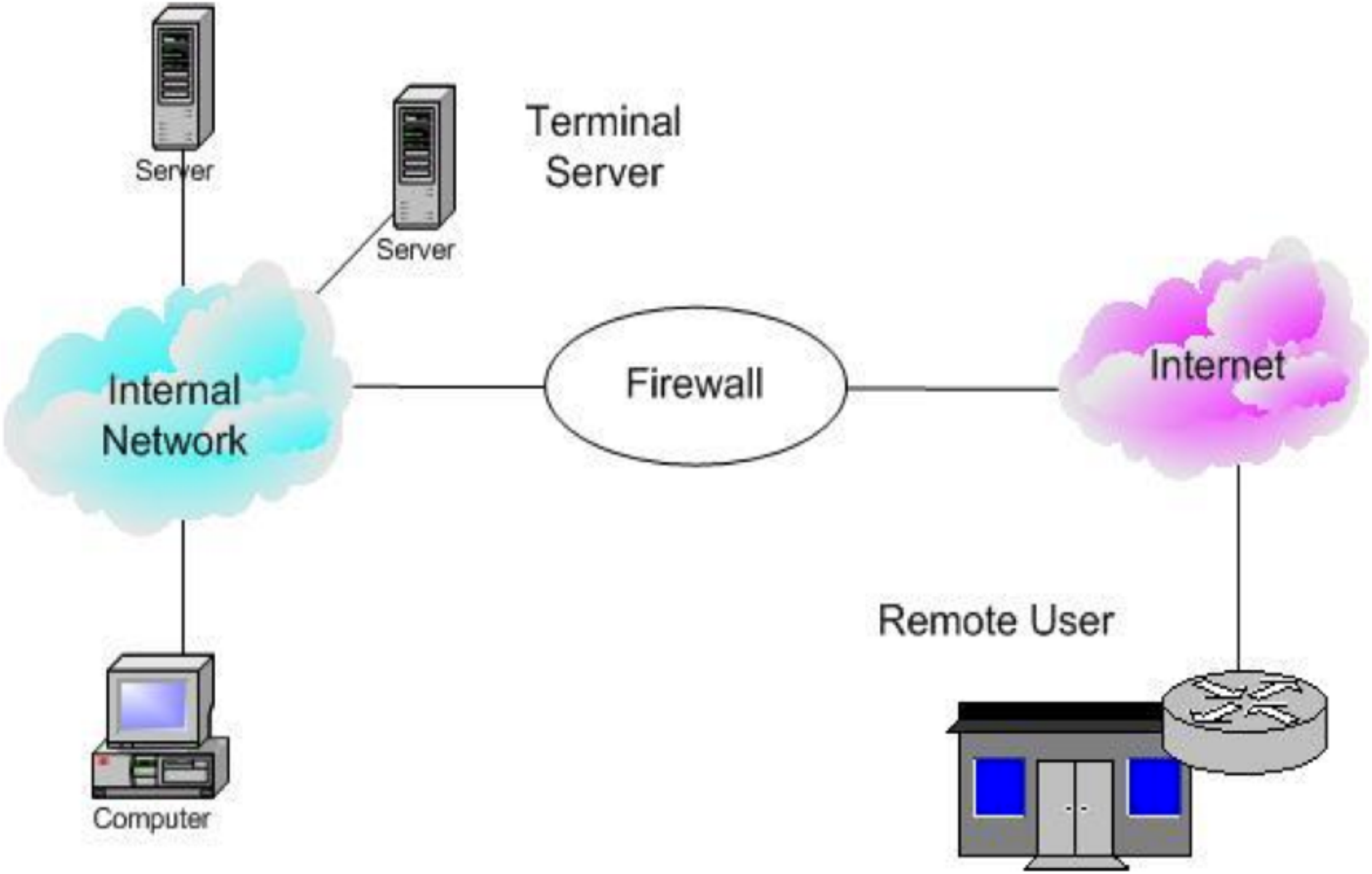
IDS Component

- 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.

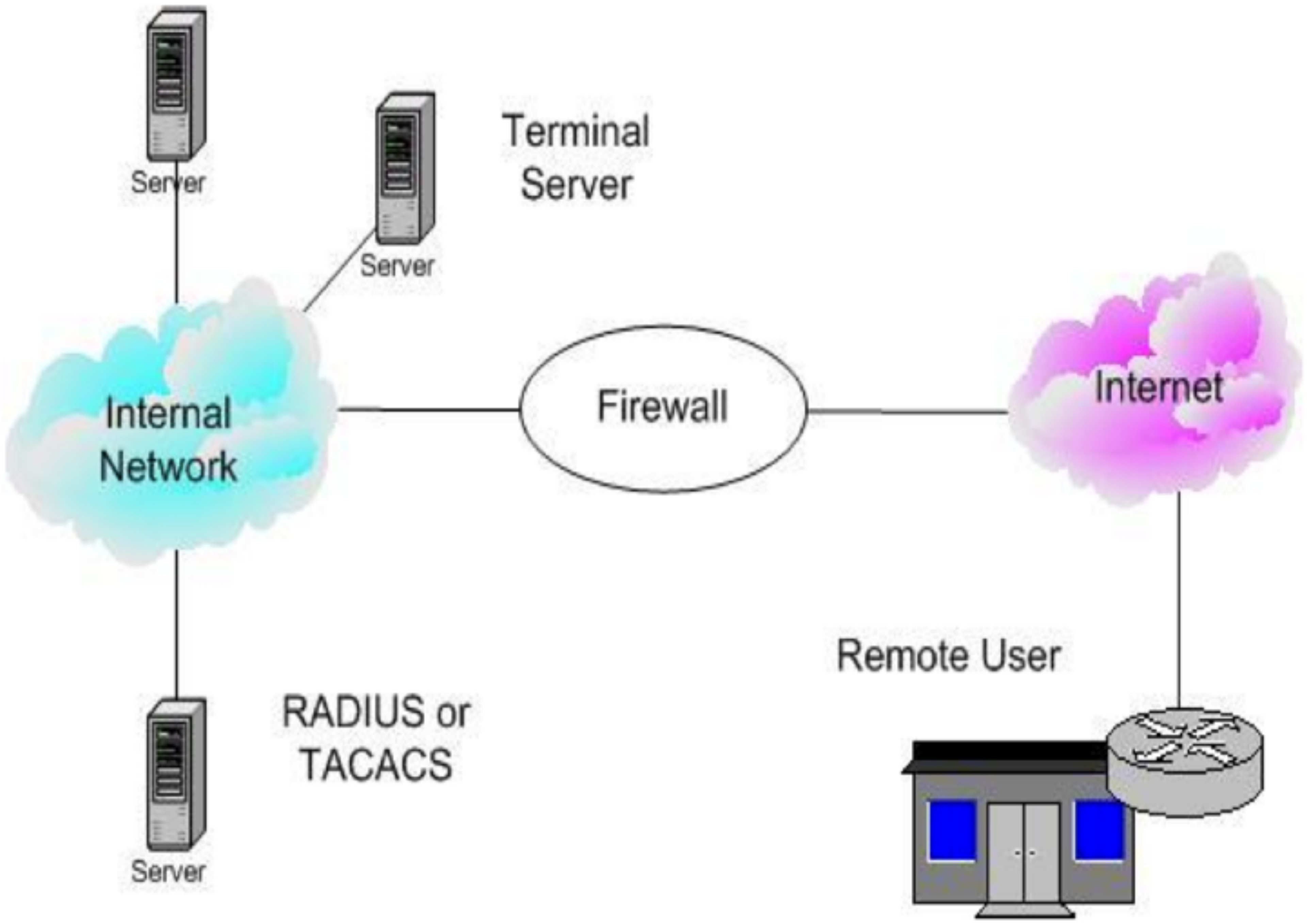
Syslog


Computer
Computer
Server
Internet
Authentication Server
Router
Attack
Syslog
Computer
Attacker

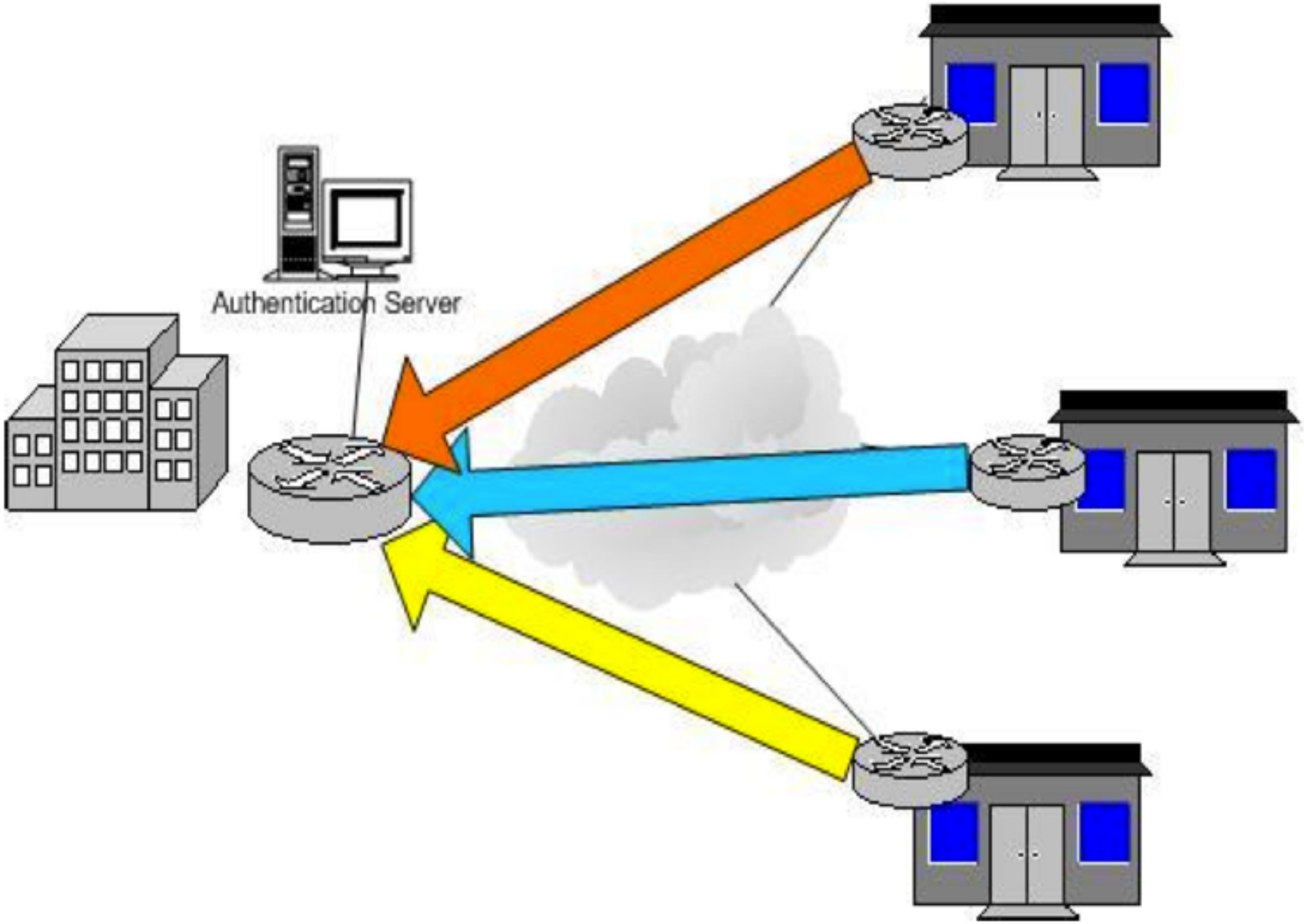
Remote Access Server



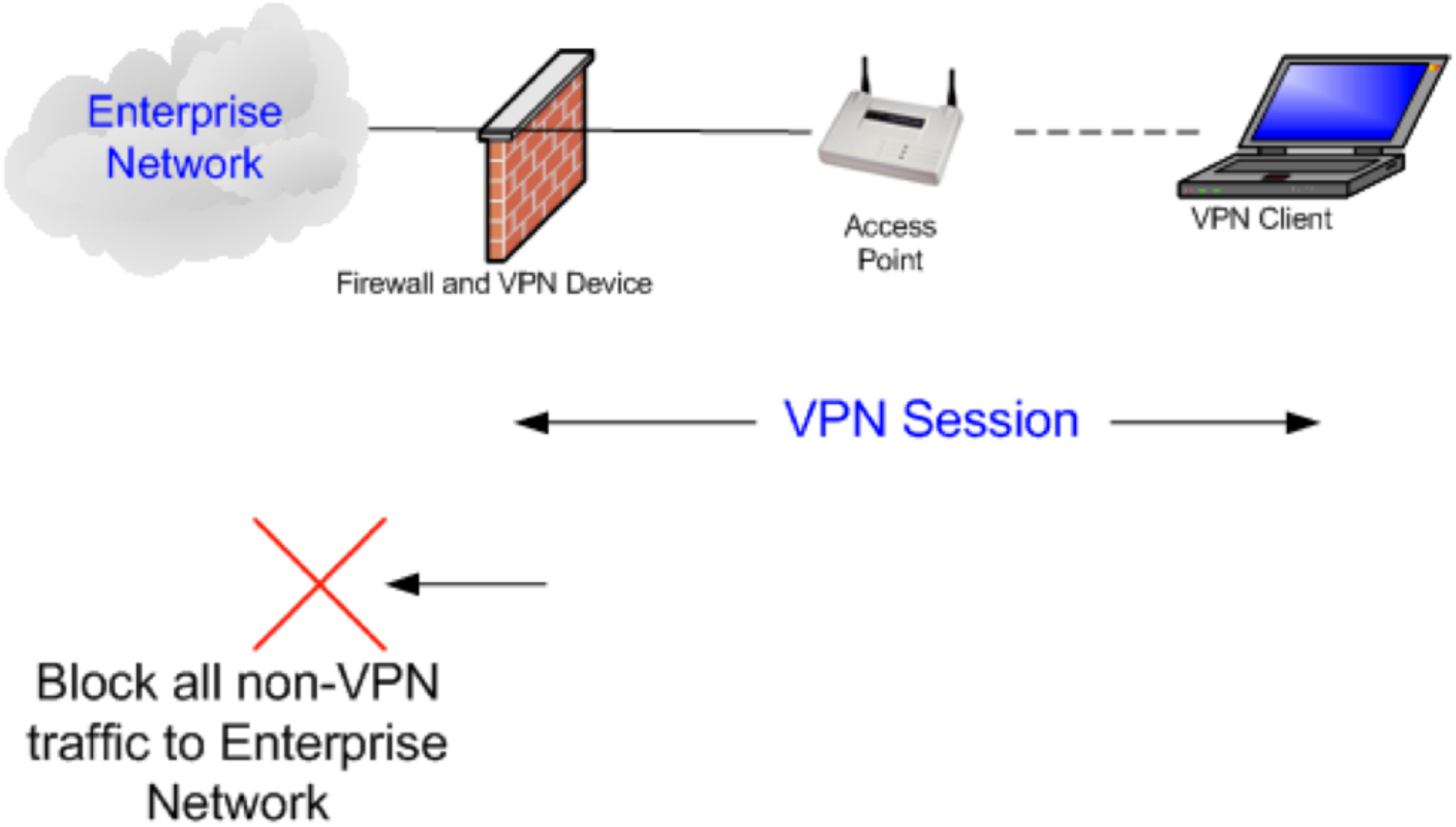
Identification & Authentication Remote Users



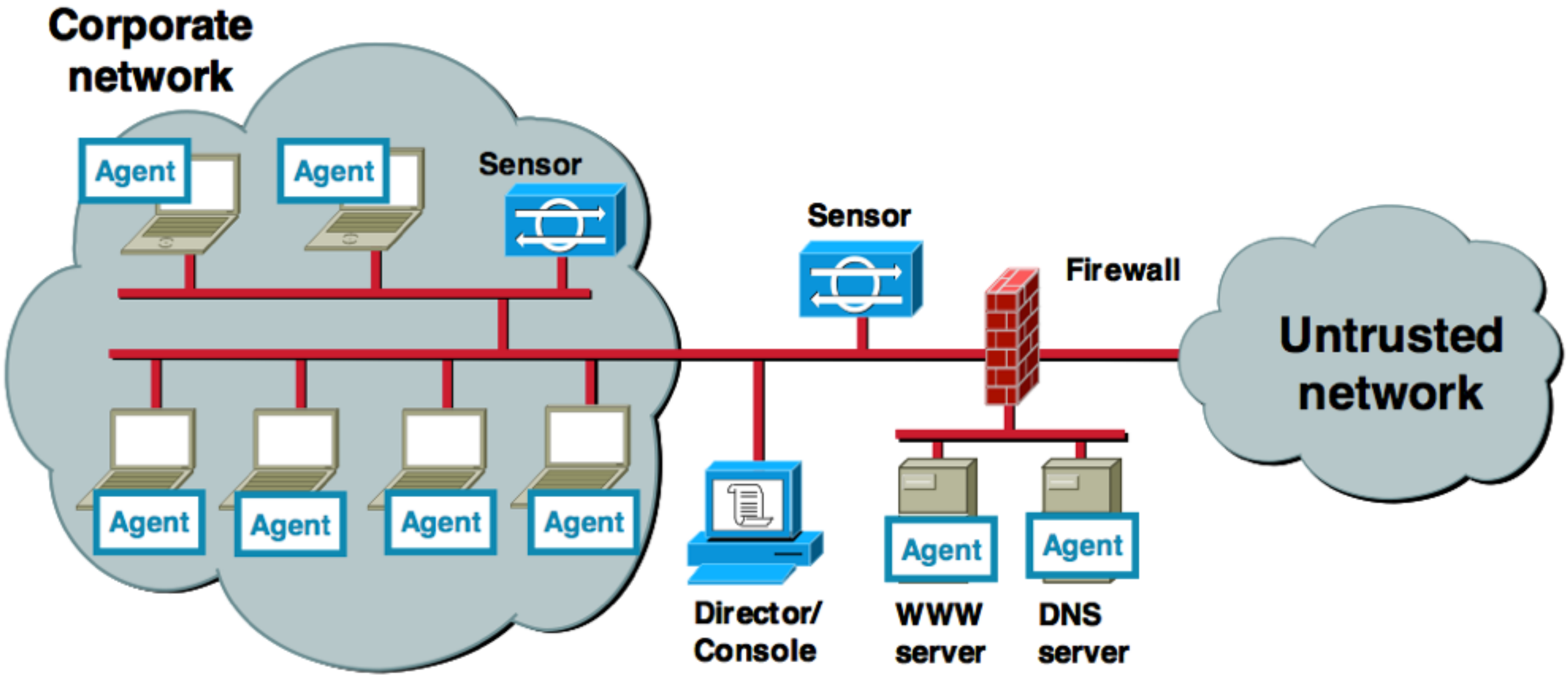
VPN Concentrators



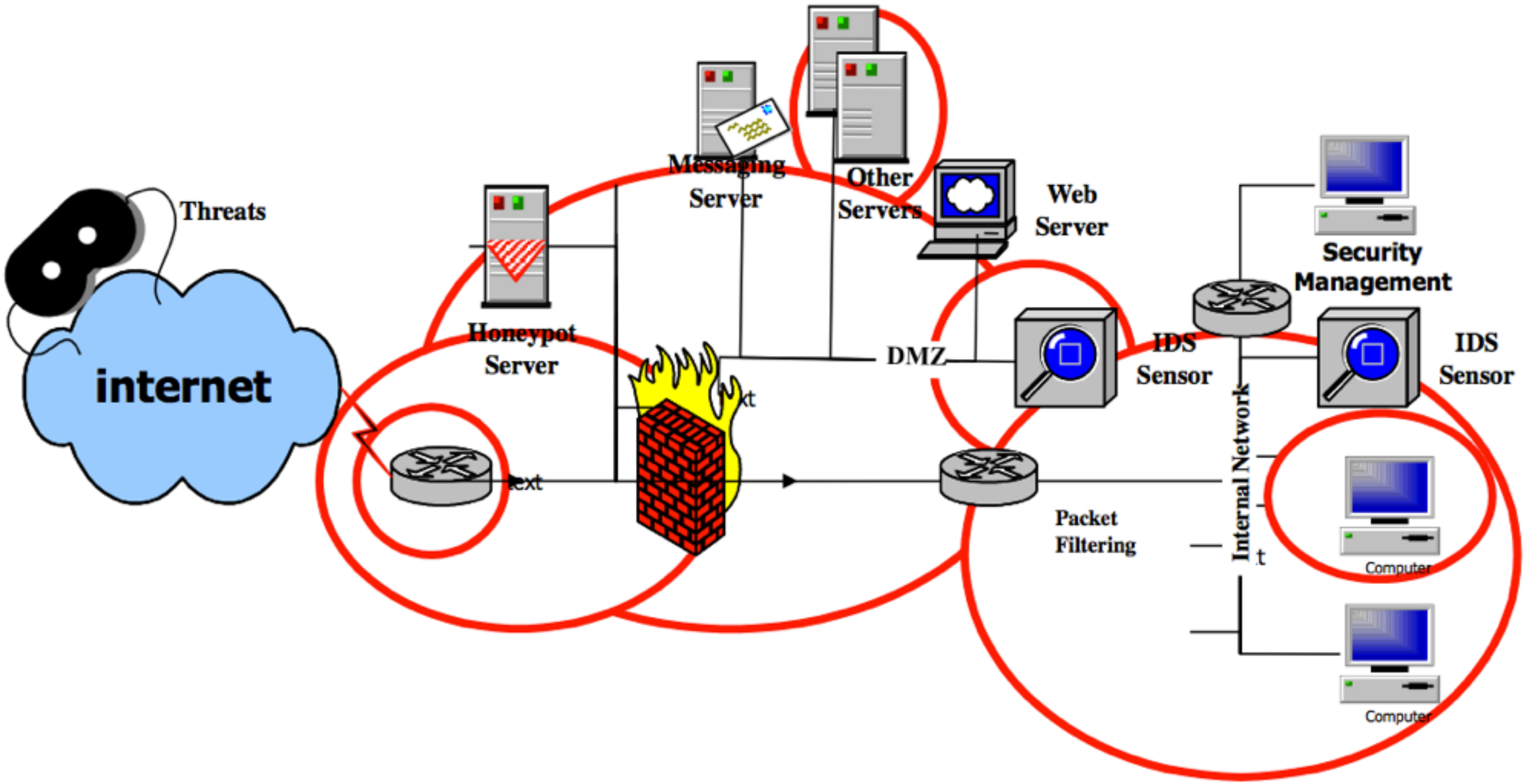
Virtual Private Network (VPN)



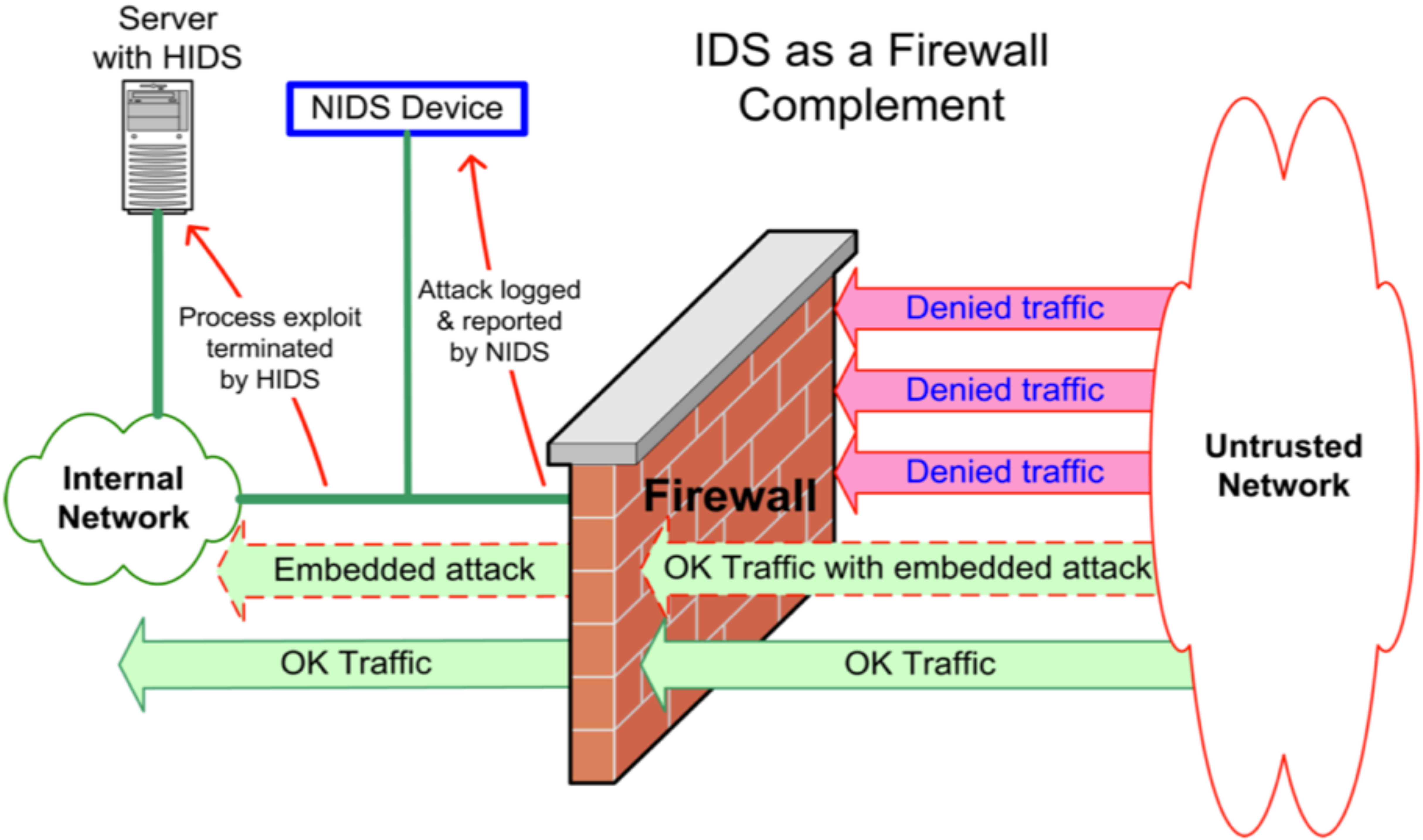
AV Layered Defense-in-Depth



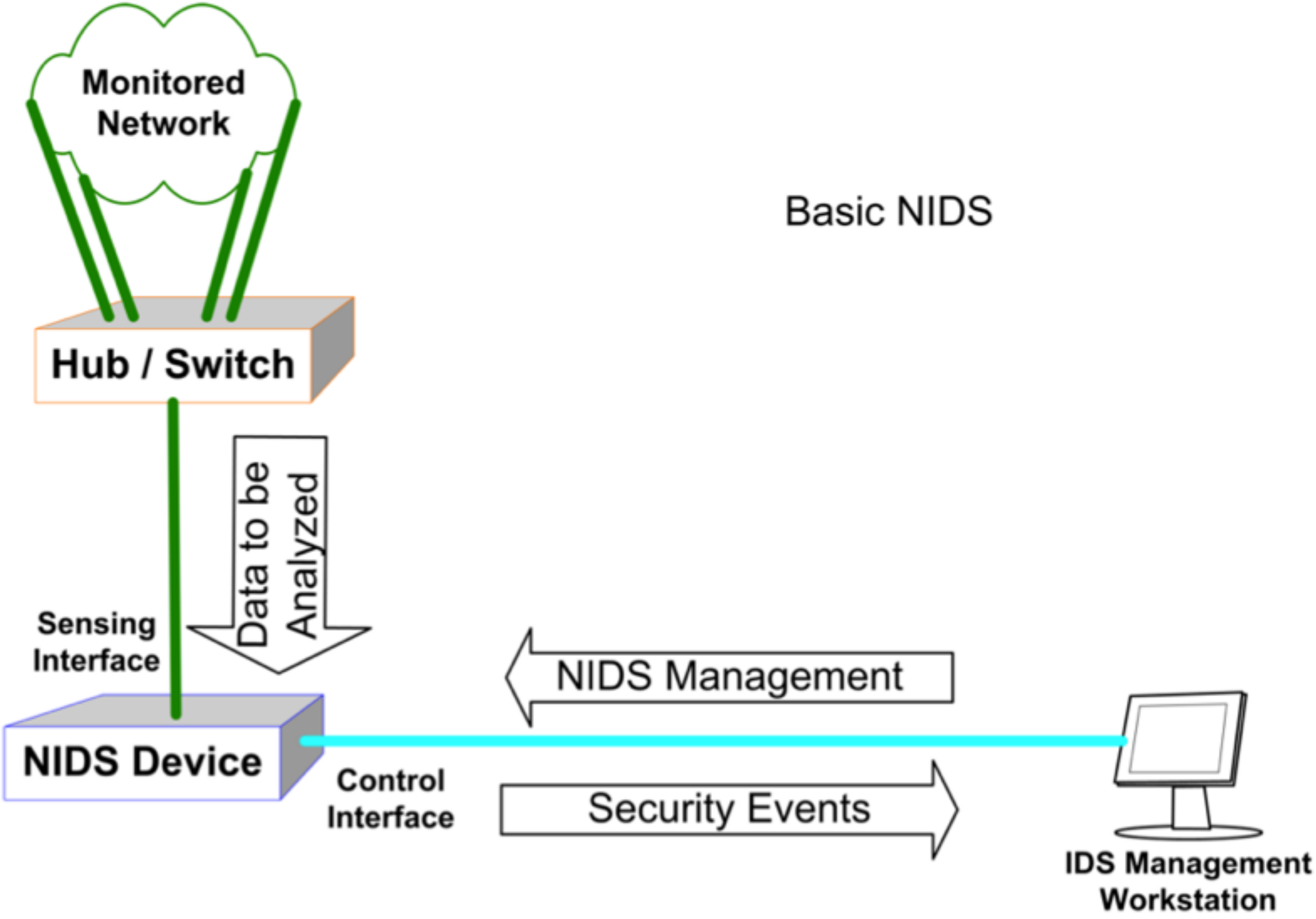
Multiple Zones of Defense & Defense-in-Depth



IDS as Firewall Complement

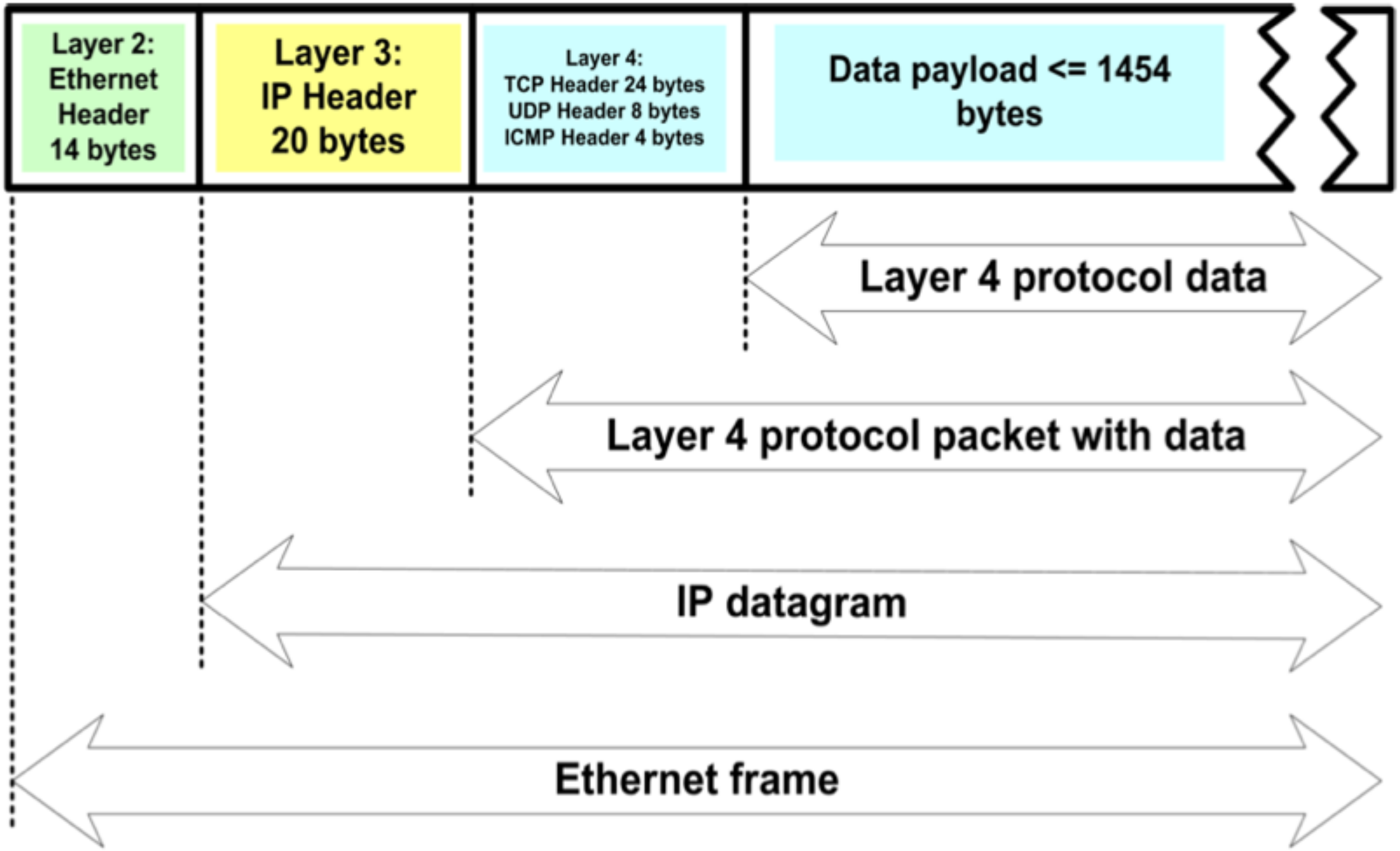


Network IDS (NIDS)



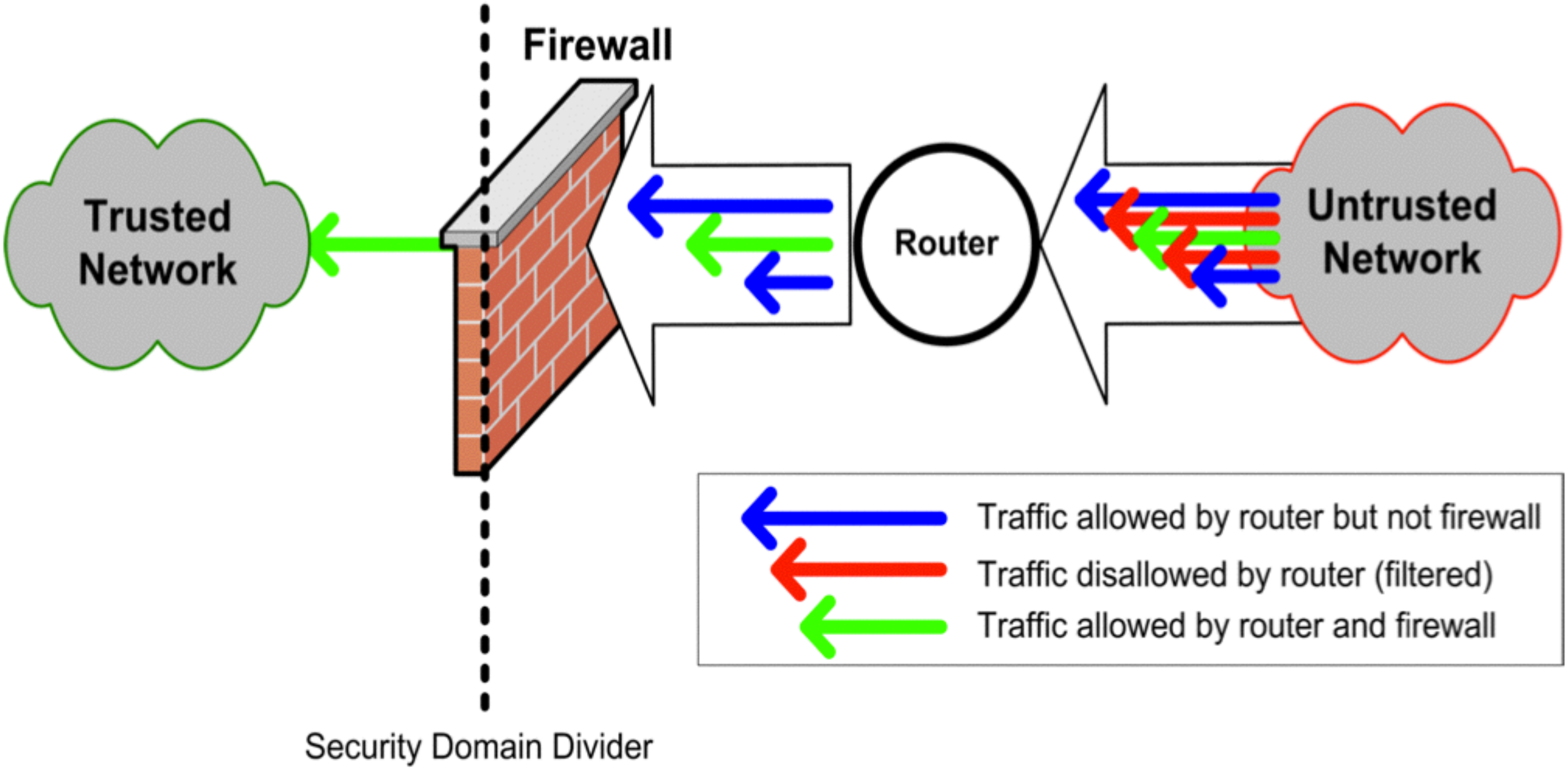
Basic NIDS

NIDS Operation

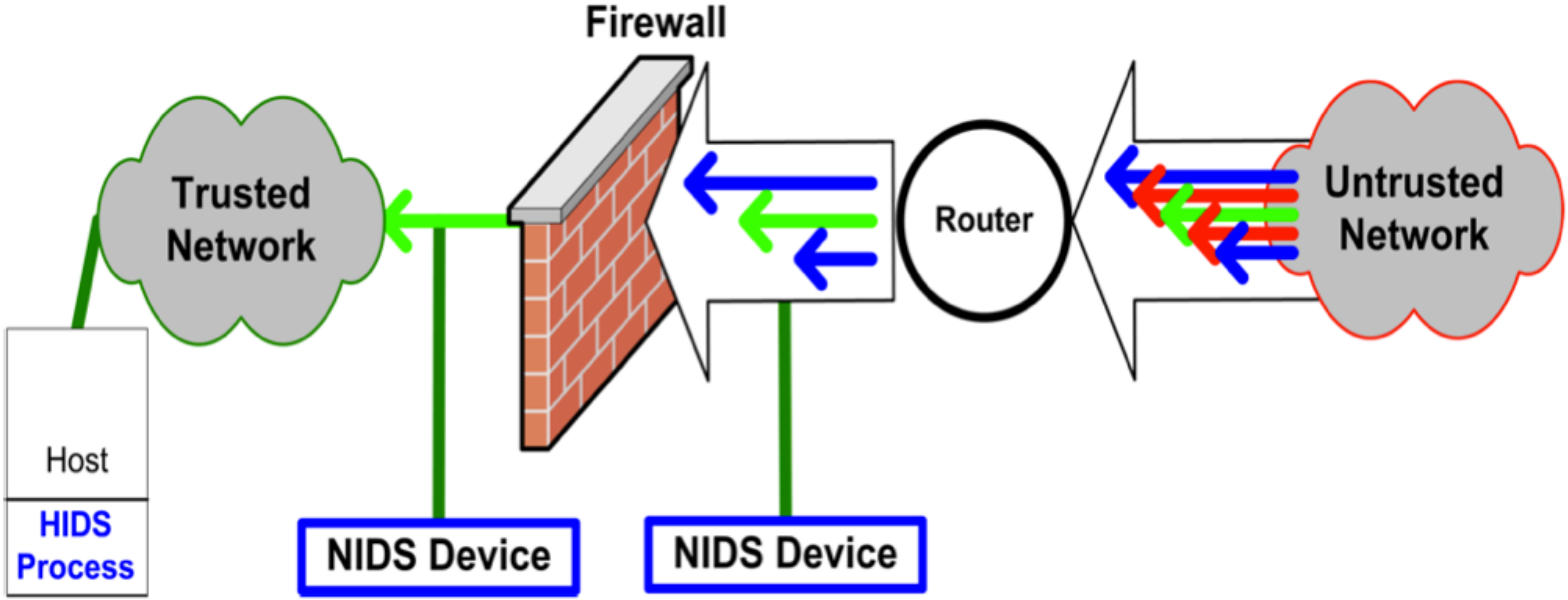


IP datagram framed for an Ethernet network

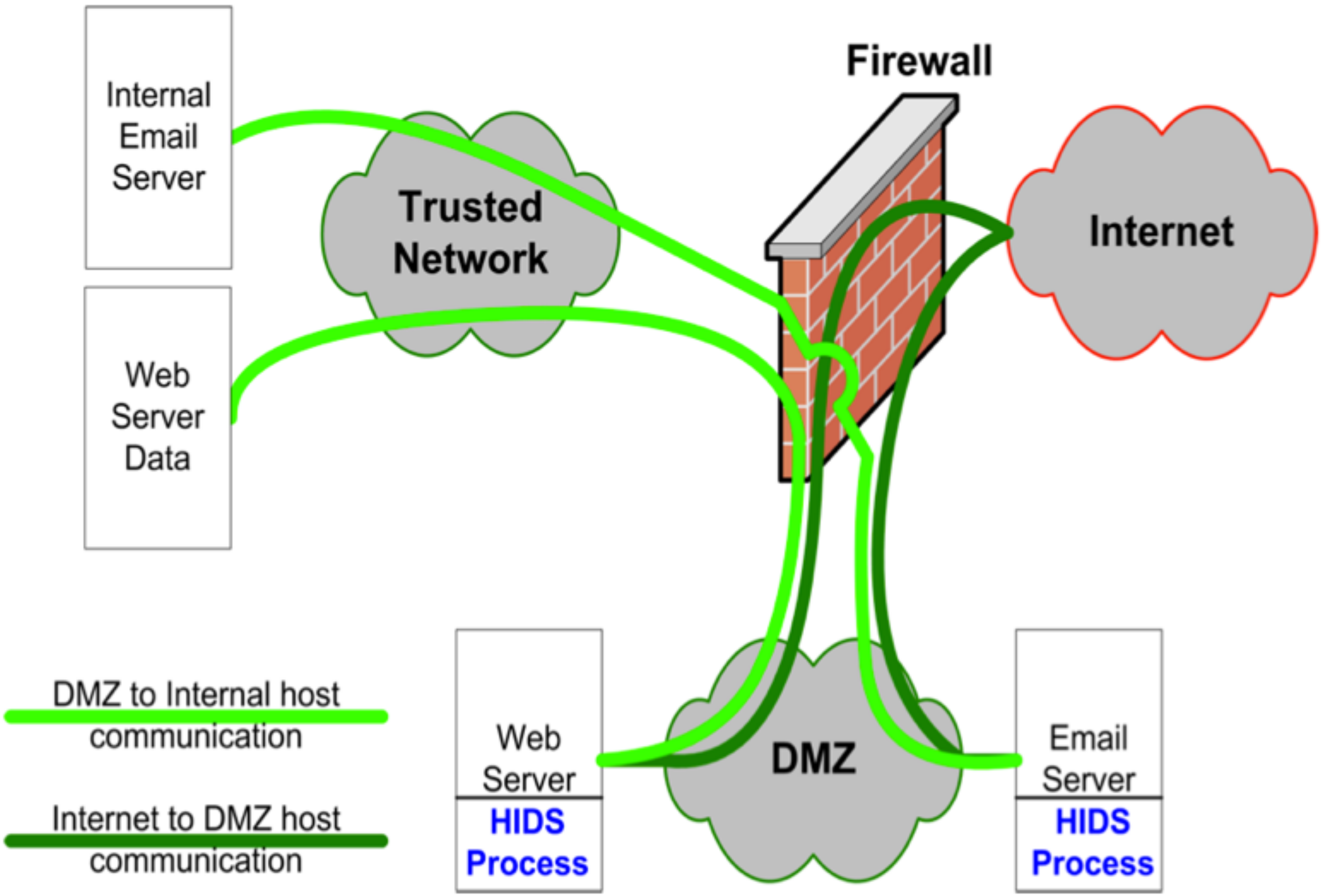
Layered Defense - Network Access Control


Firewall
Trusted Network
Router
Untrusted Network
Traffic allowed by router but not firewall
Traffic disallowed by router (filtered)
Traffic allowed by router and firewall
Security Domain Divider

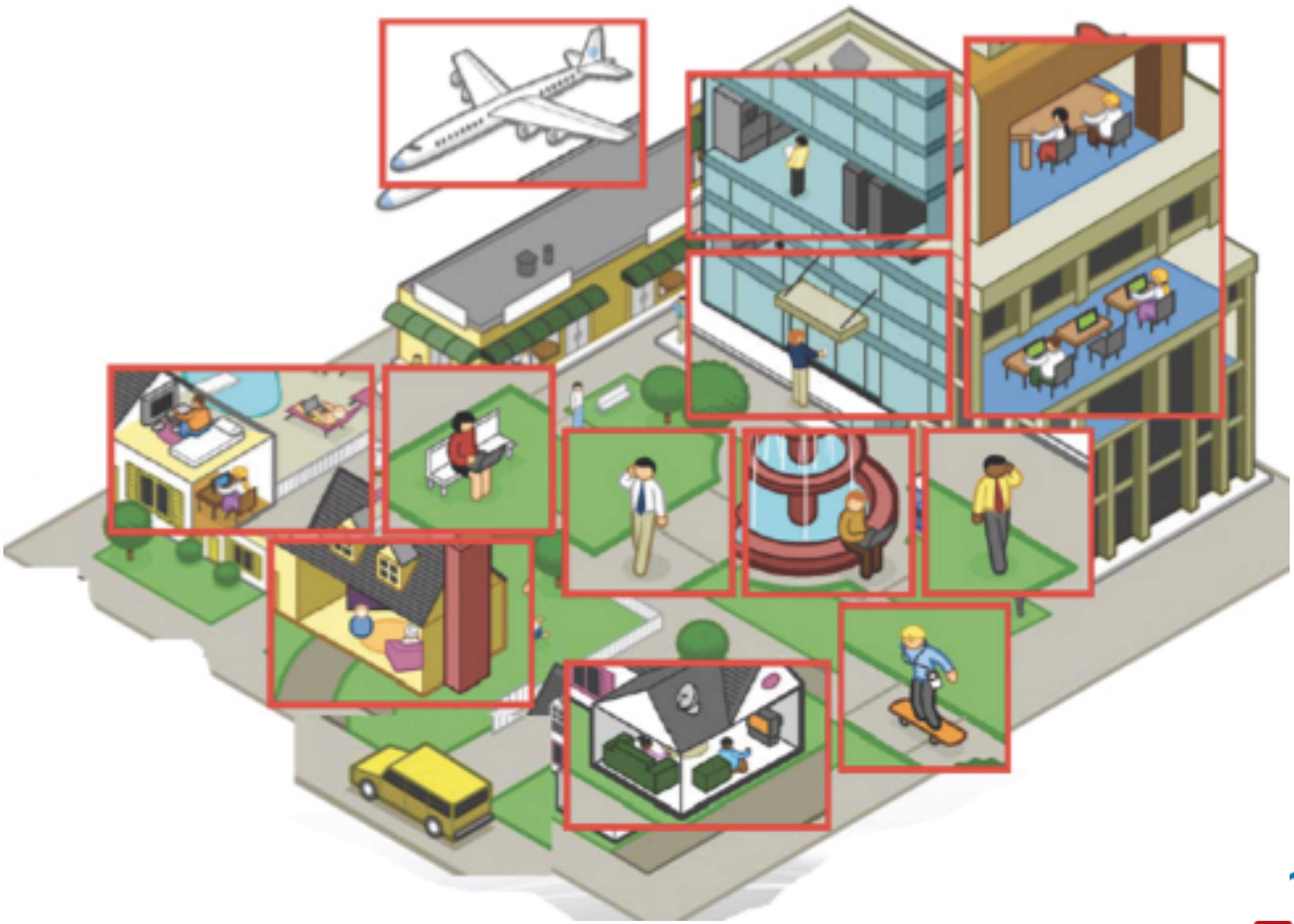
Control Check - Intrusion Detection



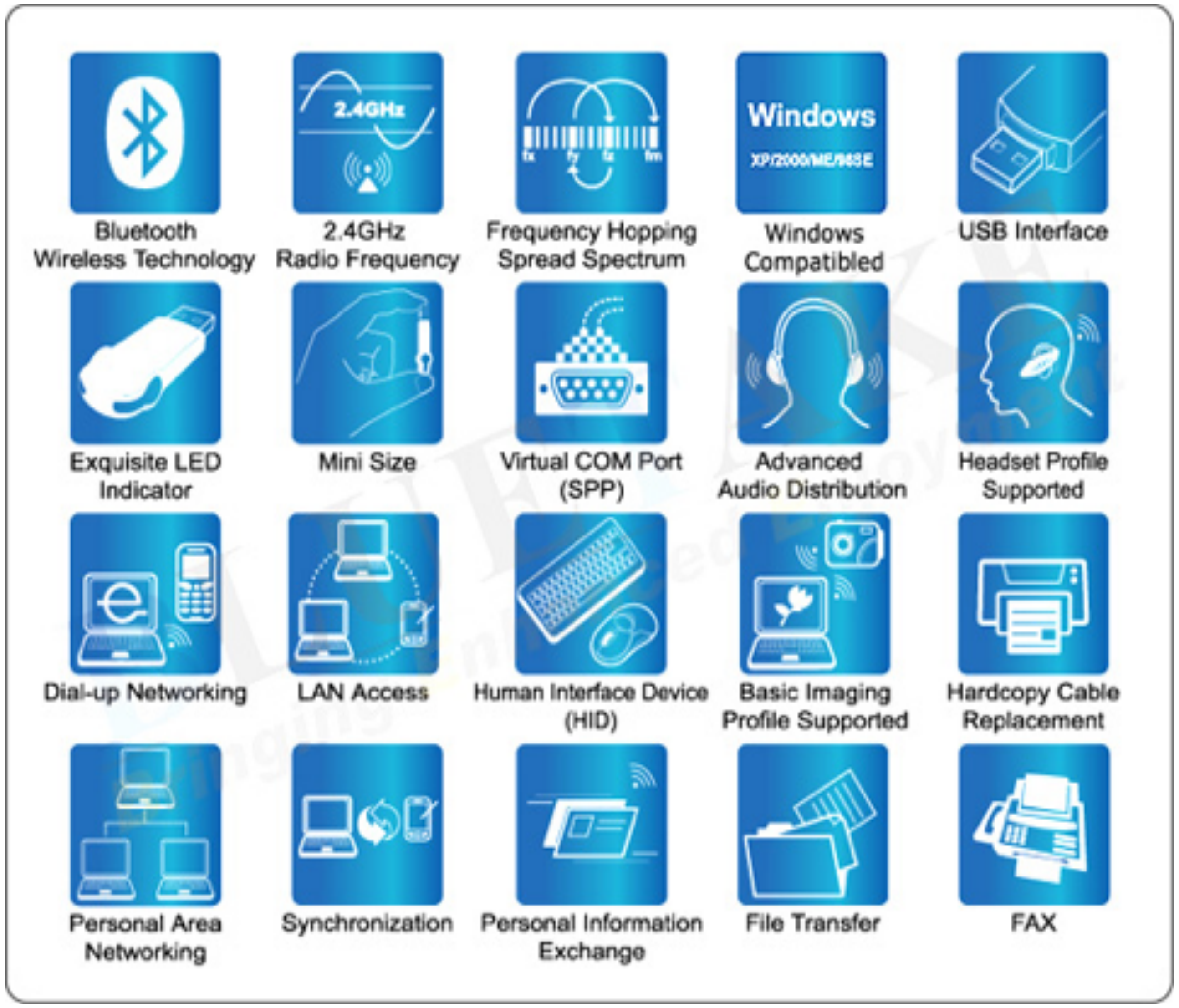
Host Isolation



Wireless Technologies



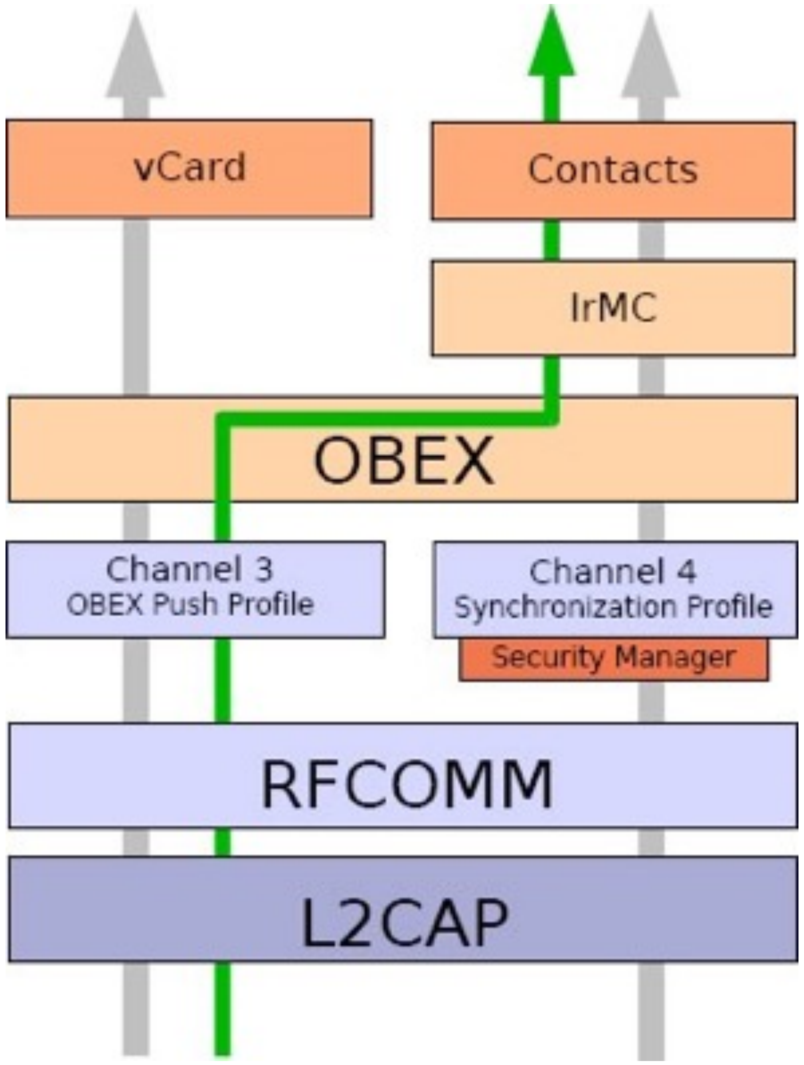
Bluetooth (IEEE 802.15)


Bluetooth Wireless Technology
2.4GHz
2.4GHz Radio Frequency
Frequency Hopping Spread Spectrum
Windows XP/2000/ME/98SE
Windows Compatibled
USB Interface
Exquisite LED Indicator
Mini Size
Virtual COM Port (SPP)
Advanced Audio Distribution
Headset Profile Supported
Dial-up Networking
LAN Access
Human Interface Device (HID)
Basic Imaging Profile Supported
Hardcopy Cable Replacement
Personal Area Networking
Synchronization
Personal Information Exchange
File Transfer
FAX

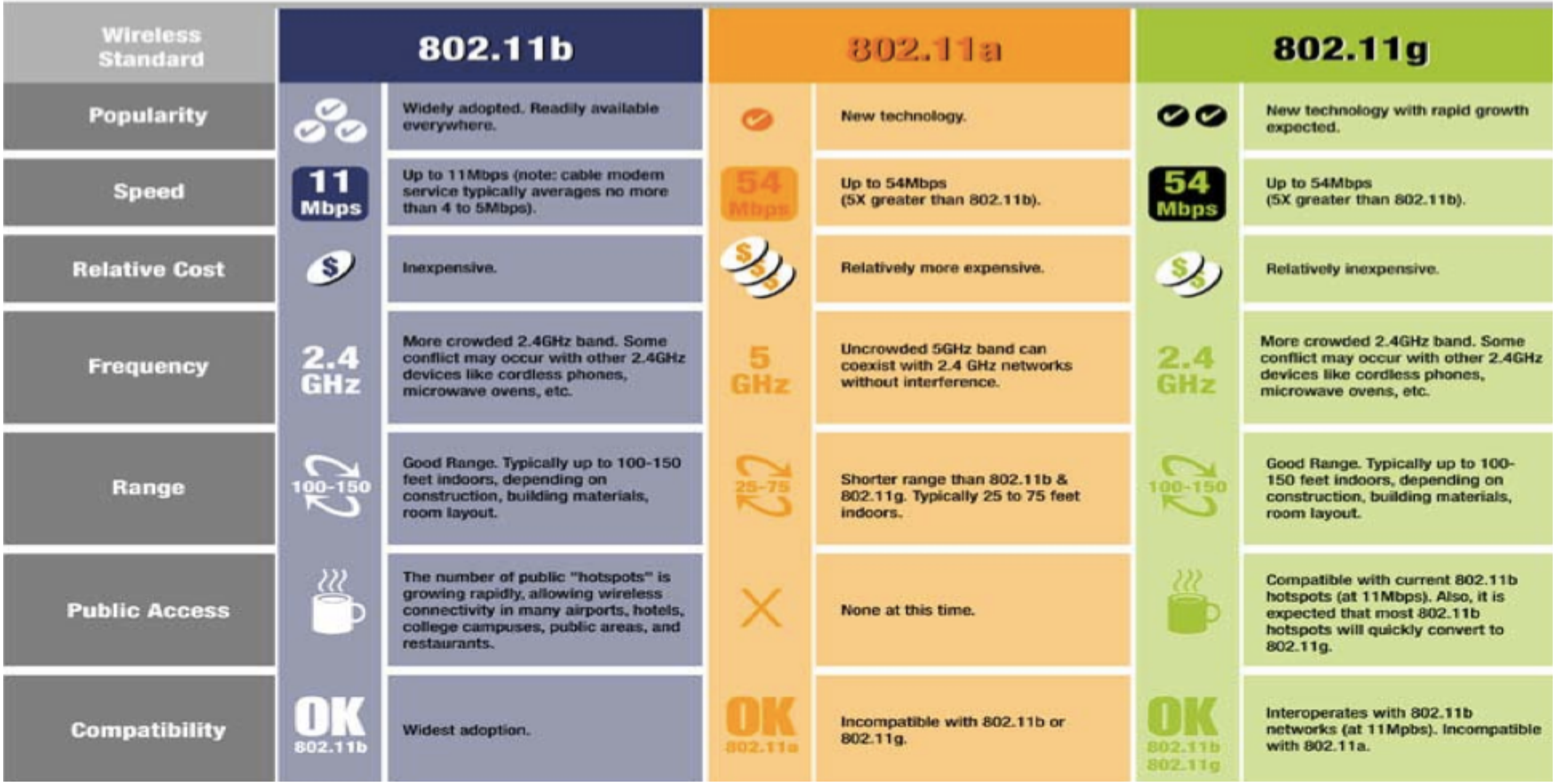
Bluetooth®

Bluetooth Threats & Security Issues

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

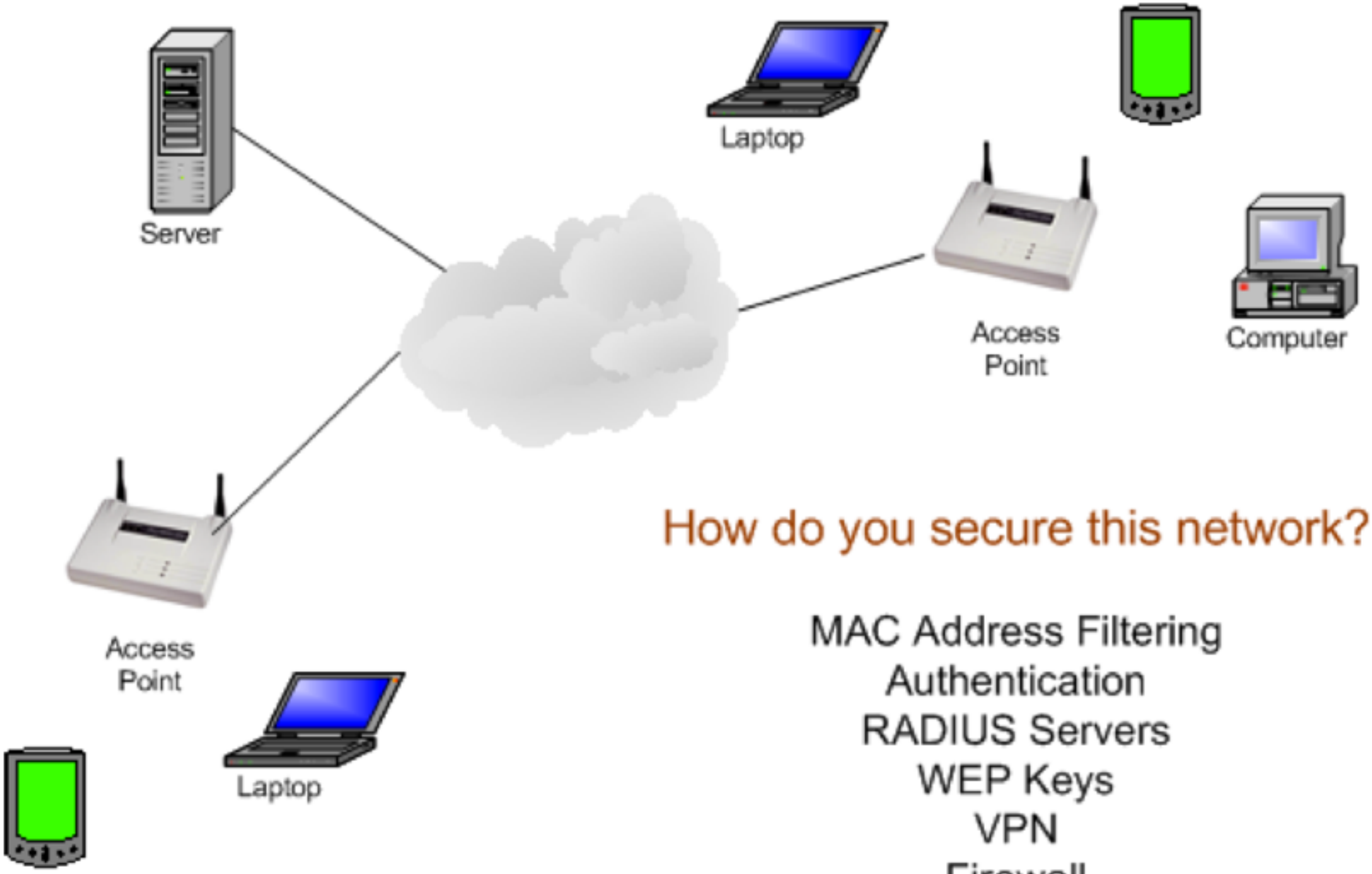


Wireless LAN (IEEE 802.11)



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.	✗	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.

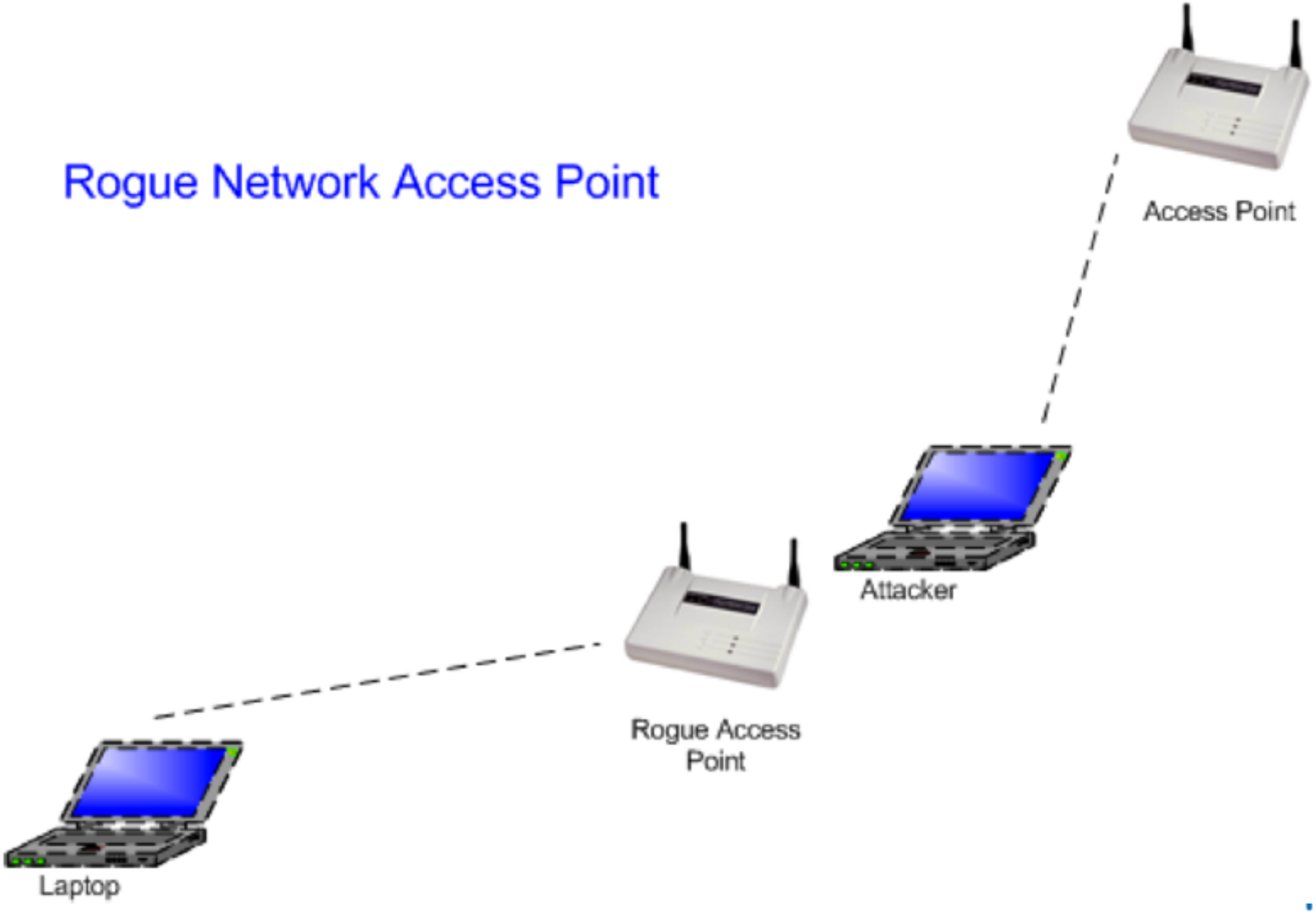
Securing Wireless LAN



How do you secure this network?

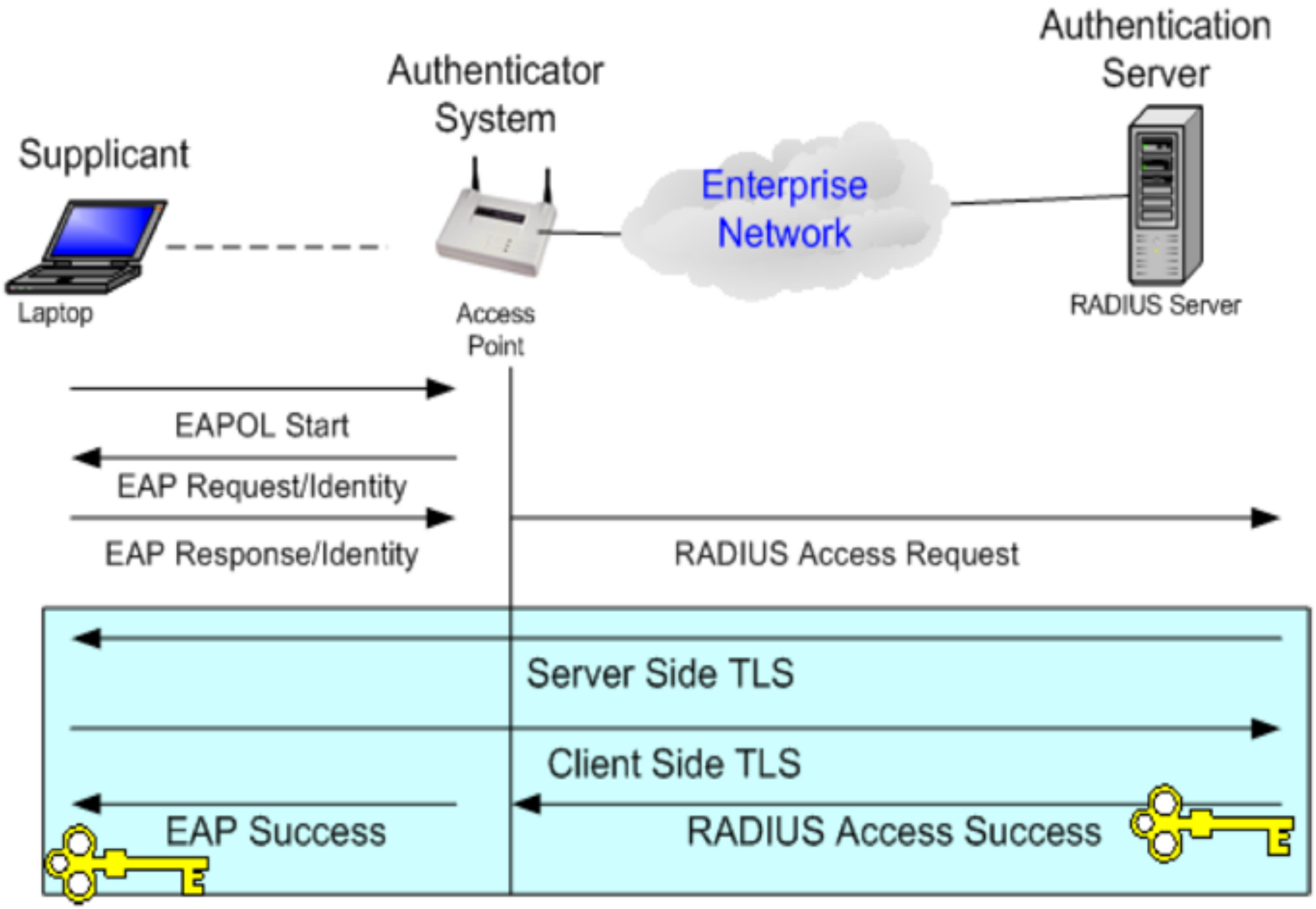
MAC Address Filtering
Authentication
RADIUS Servers
WEP Keys
VPN
Firewall

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



Q&A