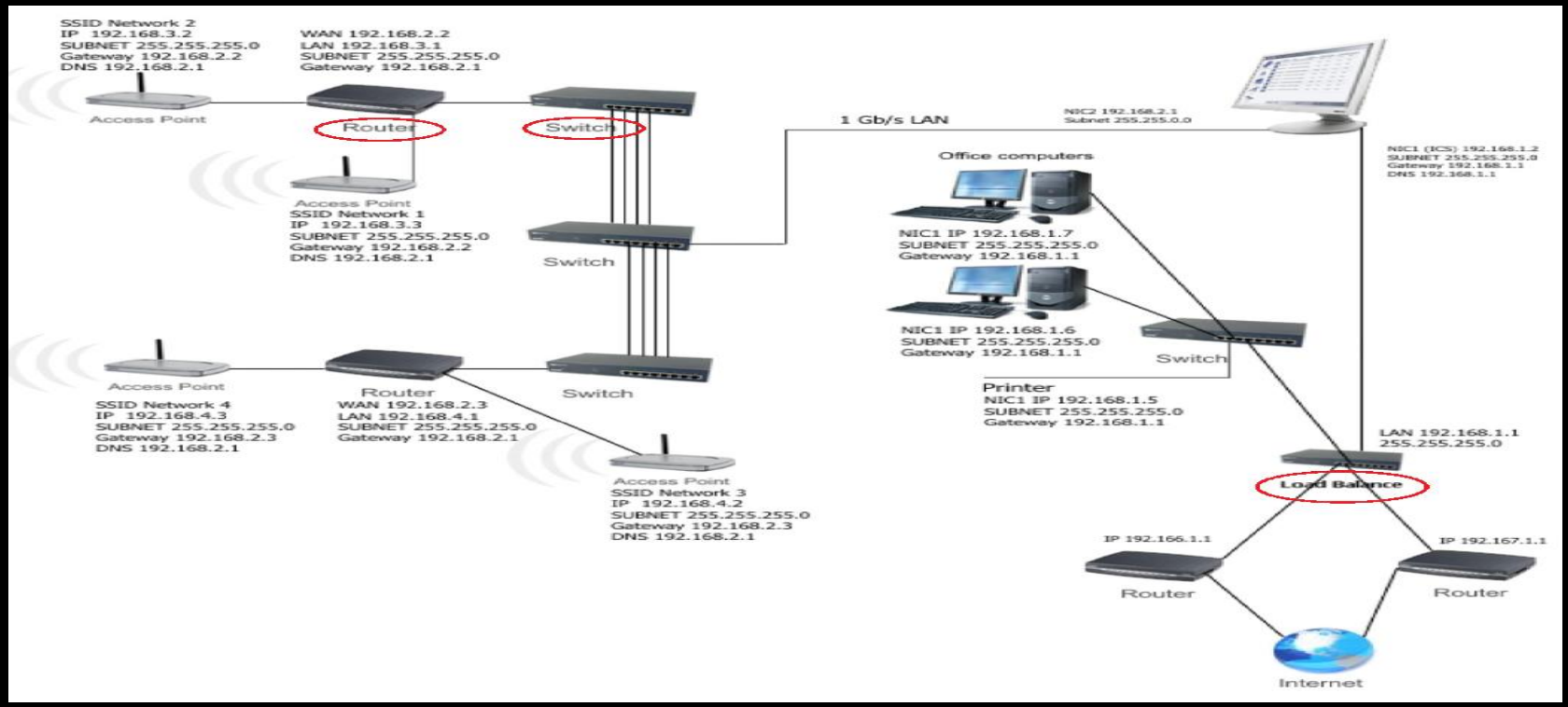
Info Security Technology

Topic 4
Network Security
(Firewalls)

Network Device Vulnerabilities

Network Device

- equipment that mediate data in a computer network.
- Includes hub, switch, router and load balancer.



Security Through Network Devices

- Not all applications designed, written with security in mind
  - Network must provide protection
- Networks with weak security invite attackers
- Aspects of building a secure network
  - Network devices
  - Network technologies
  - Design of the network itself

Standard Network Devices

- Security features found in network hardware
  - Provide basic level of security
- Open systems interconnection (OSI) model
  - Network devices classified based on function
  - Standards released in 1978, revised in 1983, still
    - used today
  - Illustrates:
    - How network device prepares data for delivery
    - How data is handled once received

Standard Network Devices (cont'd.)

- OSI model breaks networking steps into seven layers
  - Each layer has different networking tasks
  - Each layer cooperates with adjacent layers

Layer number	Layer name	Description	Function
Layer 7	Application Layer	The top layer, Application, provides the user interface to allow network services	Provides services for user applications
Layer 6	Presentation Layer	The Presentation Layer is concerned with how the data is represented and formatted for the user	Is used for translation, compression, and encryption
Layer 5	Session Layer	This layer has the responsibility of permitting the two parties on the network to hold ongoing communications across the network	Allows devices to establish and manage sessions
Layer 4	Transport Layer	The Transport Layer is responsible for ensuring that error-free data is given to the user	Provides connection establishment, management, and termination as well as acknowledgments and retransmissions
Layer 3	Network Layer	The Network Layer picks the route the packet is to take, and handles the addressing of the packets for delivery	Makes logical addressing, routing, fragmentation, and reassembly available
Layer 2	Data Link Layer	The Data Link Layer is responsible for dividing the data into packets; some additional duties of the Data Link Layer include error detection and correction (for example, if the data is not received properly, the Data Link Layer would request that it be retransmitted)	Performs physical addressing, data framing, error detection, and handling
Layer 1	Physical Layer	The job of this layer is to send the signal to the network or receive the signal from the network	Involved with encoding and signaling, data transmission, and reception

Table OSI reference model

Network Device Vulnerabilities

1. Hubs
   - Hub works on Physical Layer (Layer 1) of OSI model
   - Do not read data passing through them. Ignorant of data source and destination
   - A hub repeats all frames to all its attached network devices. Can pose security risk.
   - Protocol analyzers (eg wireshark) can be used by attackers to capture the network traffic on a hub to decode and analyze its content.

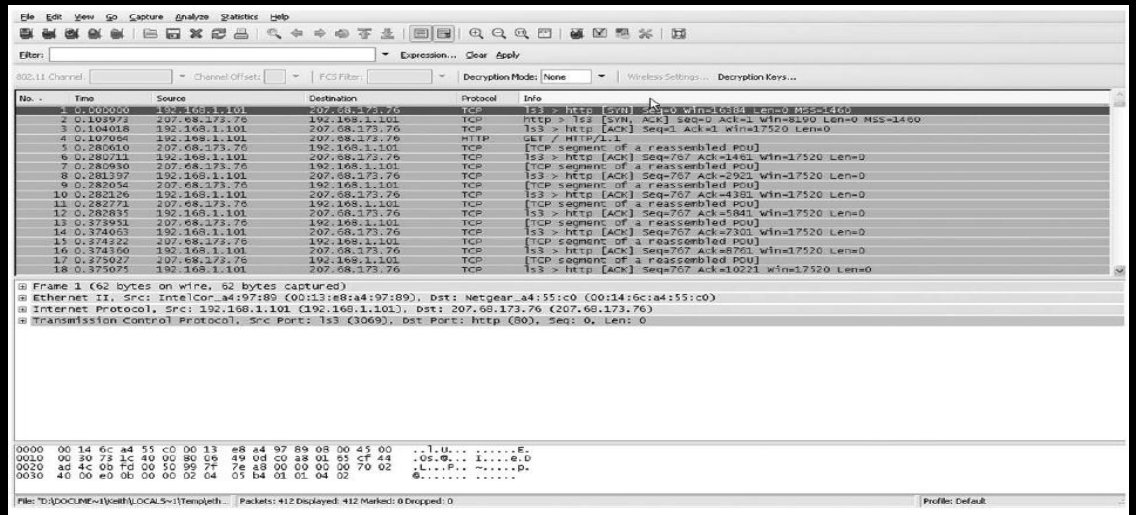


Figure 4-2 Protocol analyzer output

Network Device Vulnerabilities

2. Switches
   - Switch works on Data Link Layer (Layer 2) of OSI model
   - Determine which device is connected to each port. Use MAC address to identify devices
   - Can forward frames sent to that specific device or broadcast to all devices
   - Improves network performance and provide better security.
   - Allow administrator to monitor traffic in two ways
     - Use a switch with port mirroring
       - To redirect traffic that occurs on some or all ports to a designated monitoring port on the switch
     - Install a network tap (test access point)
       - A separate device that can be installed between two network devices, such as a switch, router, or firewall, to monitor traffic

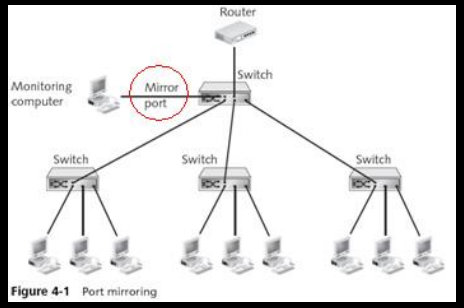


Figure 4-1 Port mirroring

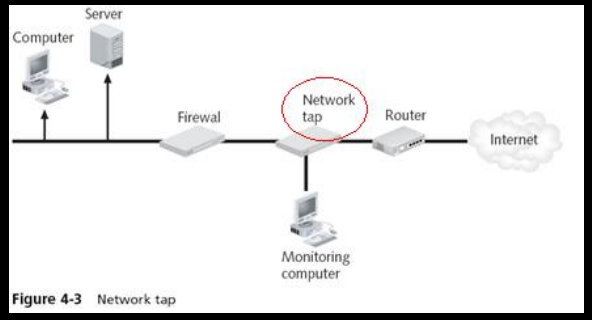


Figure 4-3 Network tap

Network Device Vulnerabilities

3. Routers
   - Forward packets across computer networks
   - Can be set to filter out specific types of network traffic

4. Load balancer
   - Help evenly distribute work across a network
   - Can stop attacks directed at a server or application
   - Can detect and prevent denial-of-service attacks
   - Some can deny attackers information about the network

Standard Network Devices (cont'd.)

- Advantages of load-balancing technology
  - Reduces probability of overloading a single server
  - Optimizes bandwidth of network computers
  - Reduces network downtime
- Load balancing is achieved through software or
- hardware device (load balancer)

Standard Network Devices (cont'd.)

- Security advantages of load balancing
  - Can stop attacks directed at a server or application
  - Can detect and prevent denial-of-service attacks
  - Some can deny attackers information about the network
    - Hide HTTP error pages
    - Remove server identification headers from HTTP responses

Apply Network Security Devices

- Network Security Devices include:
  - Firewalls
  - Intrusion detection systems (IDS)
  - Proxy servers
  - Honeypots
  - Internet content filters

Security Device: Firewall

- A **firewall** is a network device—hardware, software, or a combination.
  - Firewall can come as part of a router, a piece of software or an appliance box.
  - Can either accept or deny packet entry
  - Usually located outside network security perimeter

- It enforces a **security policy** across its connections.
- A security policy is a series of rules that define what traffic is permissible and what traffic is to be blocked or denied.
- A key to security policies for firewalls is the **principle of least access**.
  - Only allow the necessary access for a function, and block or deny all unneeded functionality.
- Security topology determines the network devices that are employed and their location.
  - A corporate connection to the Internet should pass through a firewall to block all unauthorized network traffic

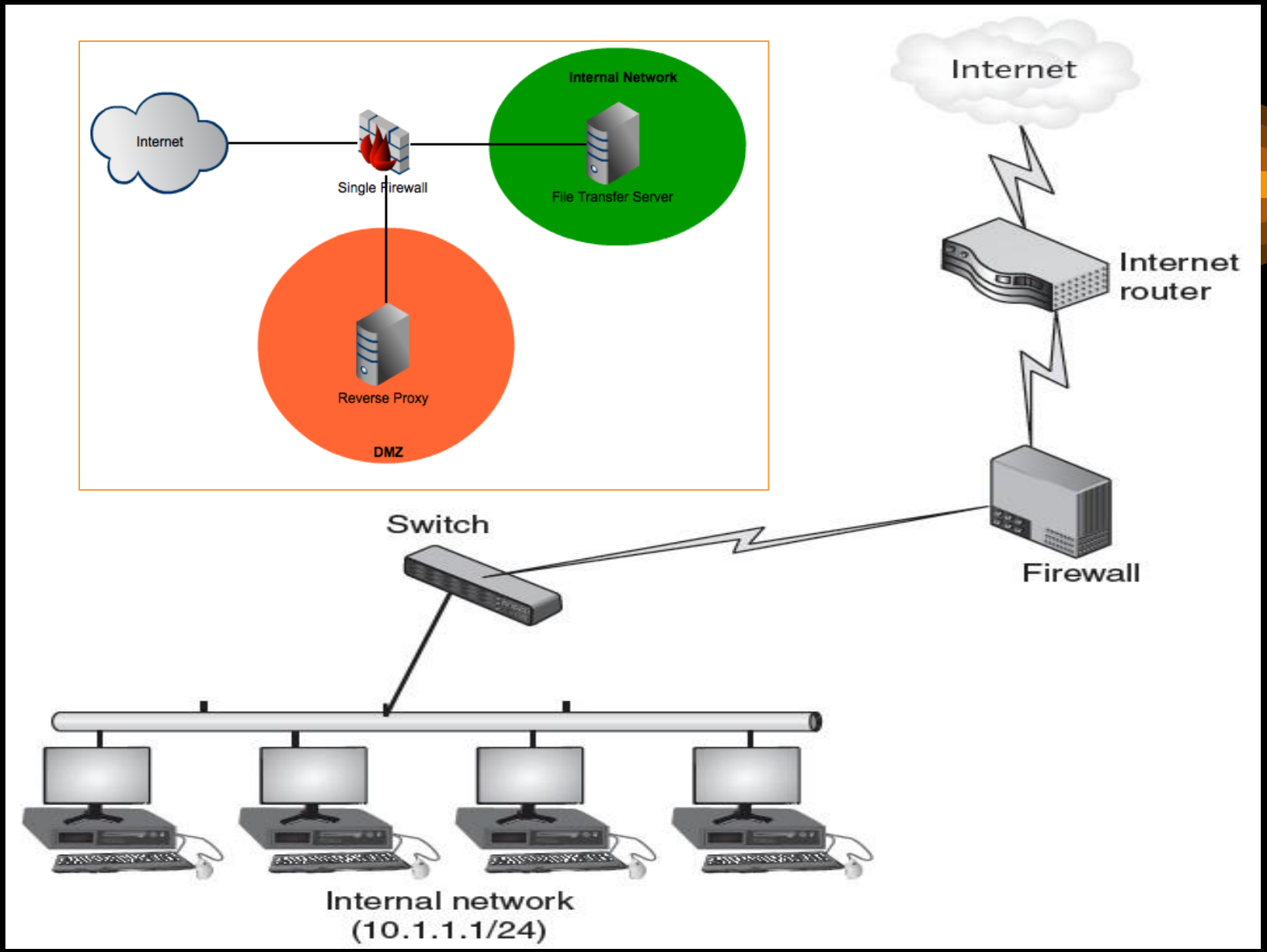


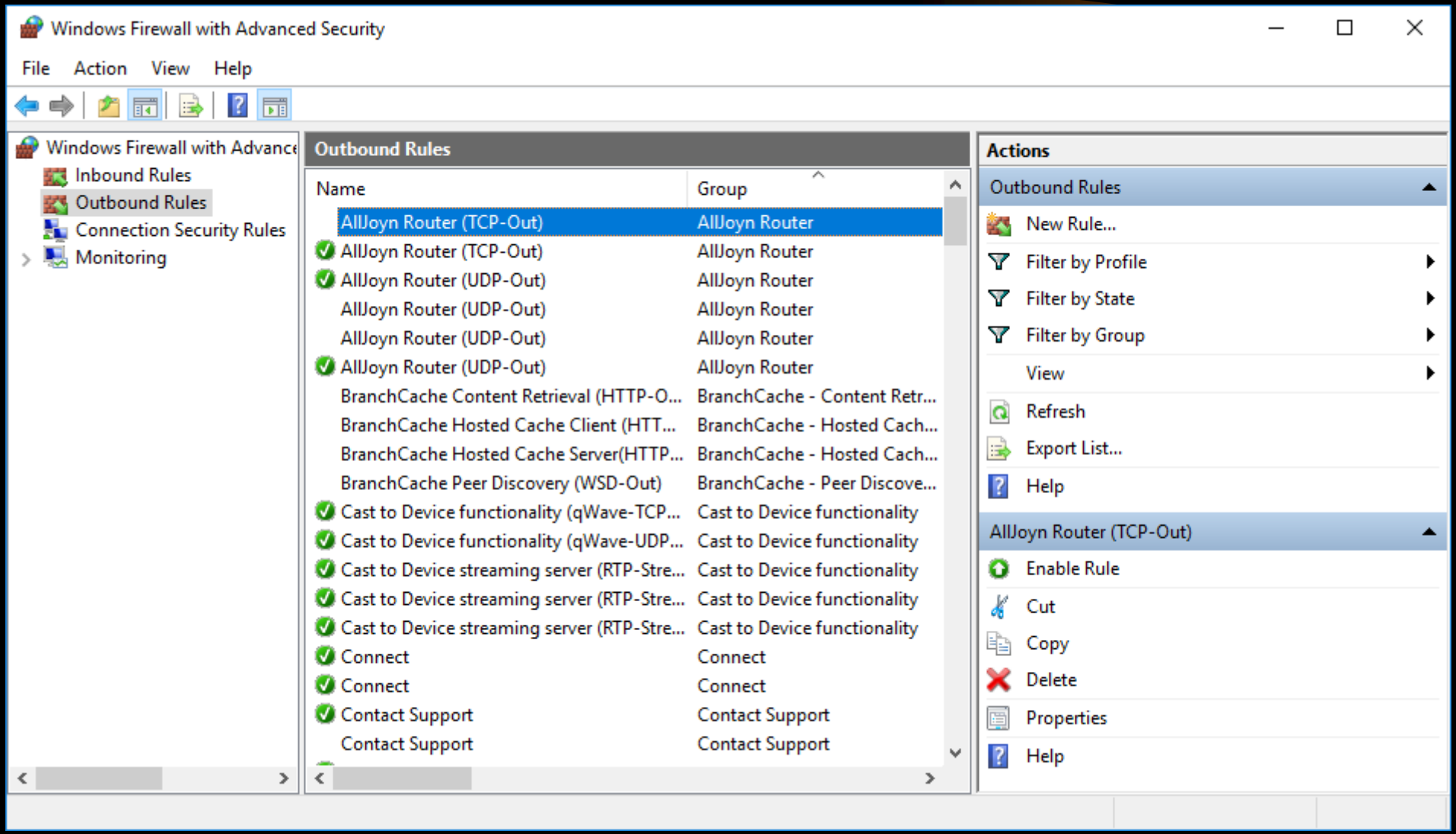
Figure Firewall location

Network Security Hardware (cont'd.)

- Firewall actions on a packet
  - Allow (let packet pass through)
  - Block (drop packet)
  - Prompt (ask what action to take)
- Rule-based firewall settings
  - Set of individual instructions to control actions
  - default deny all OR allow all
- Settings-based firewall
  - Allows administrator to create parameters

Rule description	Explanation	Filtering
Source address = any	The source IP address is that of the Web server on the Internet	Because the IP address of a Web server cannot be known in advance, this rule allows a packet coming from anywhere to enter the network
Destination address = internal IP address	The destination address is the IP address of the computer on the internal network where the packet is being sent	This rule allows packets directed to this internal computer to pass through, but blocks packets that do not have the correct destination address
Port = 80	Indicates which port is open to accept packets	No other ports are open unless indicated

Table Rule for Web page transmission


Windows Firewall with Advanced Security
File Action View Help
Windows Firewall with Advance
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Outbound Rules
Name
Group
AllJoyn Router (TCP-Out) AllJoyn Router
AllJoyn Router (TCP-Out) AllJoyn Router
AllJoyn Router (UDP-Out) AllJoyn Router
AllJoyn Router (UDP-Out) AllJoyn Router
AllJoyn Router (UDP-Out) AllJoyn Router
AllJoyn Router (UDP-Out) AllJoyn Router
BranchCache Content Retrieval (HTTP-O... BranchCache - Content Retr...
BranchCache Hosted Cache Client (HTT... BranchCache - Hosted Cach...
BranchCache Hosted Cache Server(HTTP... BranchCache - Hosted Cach...
BranchCache Peer Discovery (WSD-Out) BranchCache - Peer Discove...
Cast to Device functionality (qWave-TCP... Cast to Device functionality
Cast to Device functionality (qWave-UDP... Cast to Device functionality
Cast to Device streaming server (RTP-Stre... Cast to Device functionality
Cast to Device streaming server (RTP-Stre... Cast to Device functionality
Cast to Device streaming server (RTP-Stre... Cast to Device functionality
Connect Connect
Connect Connect
Contact Support Contact Support
Contact Support Contact Support
Actions
Outbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
AllJoyn Router (TCP-Out)
Enable Rule
Cut
Copy
Delete
Properties
Help

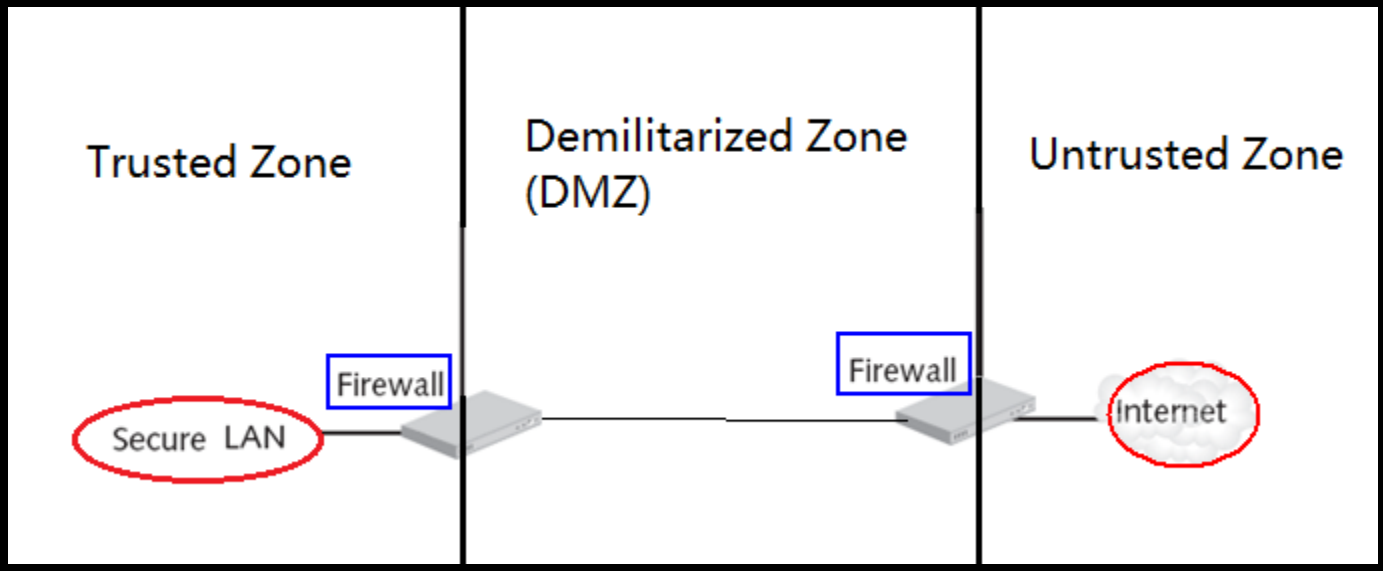
Secure Network Design: DMZ

- Demilitarized Zone (DMZ)
  - A separate network that sits outside the secure network perimeter
  - Outside users can access the DMZ but cannot enter the secure network

DMZ Security Zones – North Korea

Secure Network Design: DMZ

- The three zones
  - Untrusted Zone (The Internet)
  - Demilitarized Zone (DMZ)
  - Trusted Zone (Internal Network)



Secure Network Design: DMZ

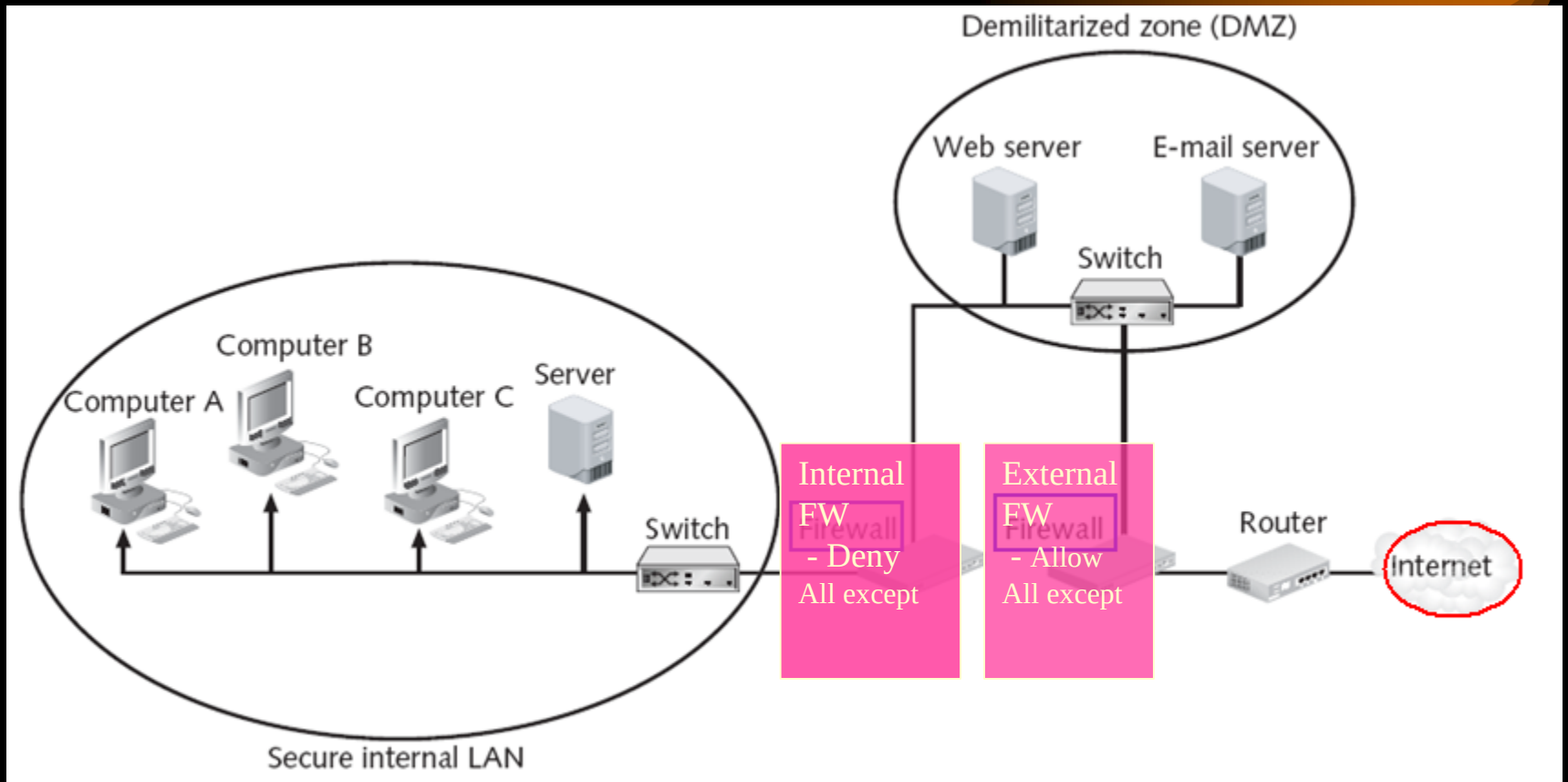


Figure 5-5 Demilitarized zone (DMZ) with two firewalls

Secure Network Design: DMZ

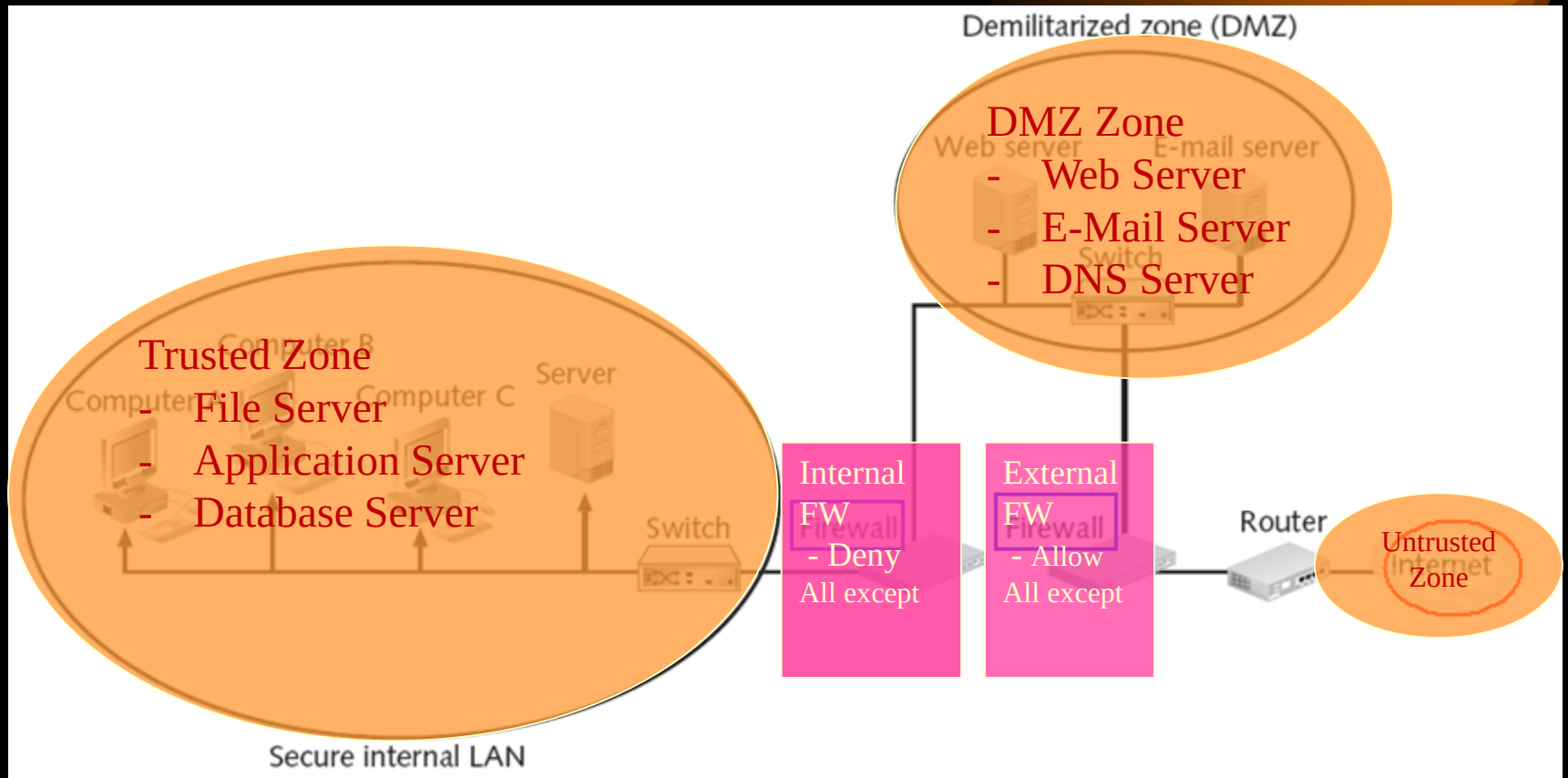


Figure 5-5 Demilitarized zone (DMZ) with two firewalls

How does Firewalls Work?

- Firewalls enforce established security policies through **mechanisms**, including:
  - Network Address Translation (NAT)
  - Basic packet filtering
  - Stateful packet filtering
  - Application layer proxies

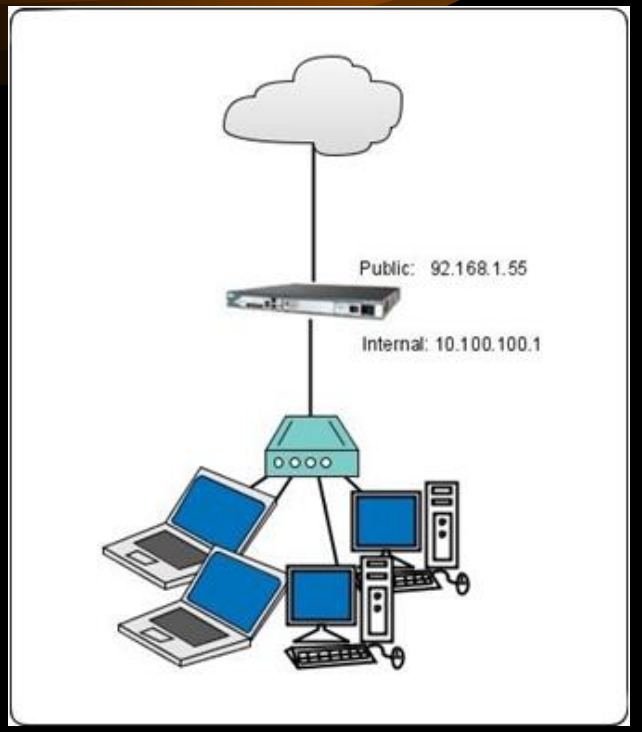
NAT and the Firewall

- **Network Address Translation (NAT)** allows masking of significant amounts of information from outside the network.

- It allows an outside entity to communicate with an entity inside the firewall without knowing its address.

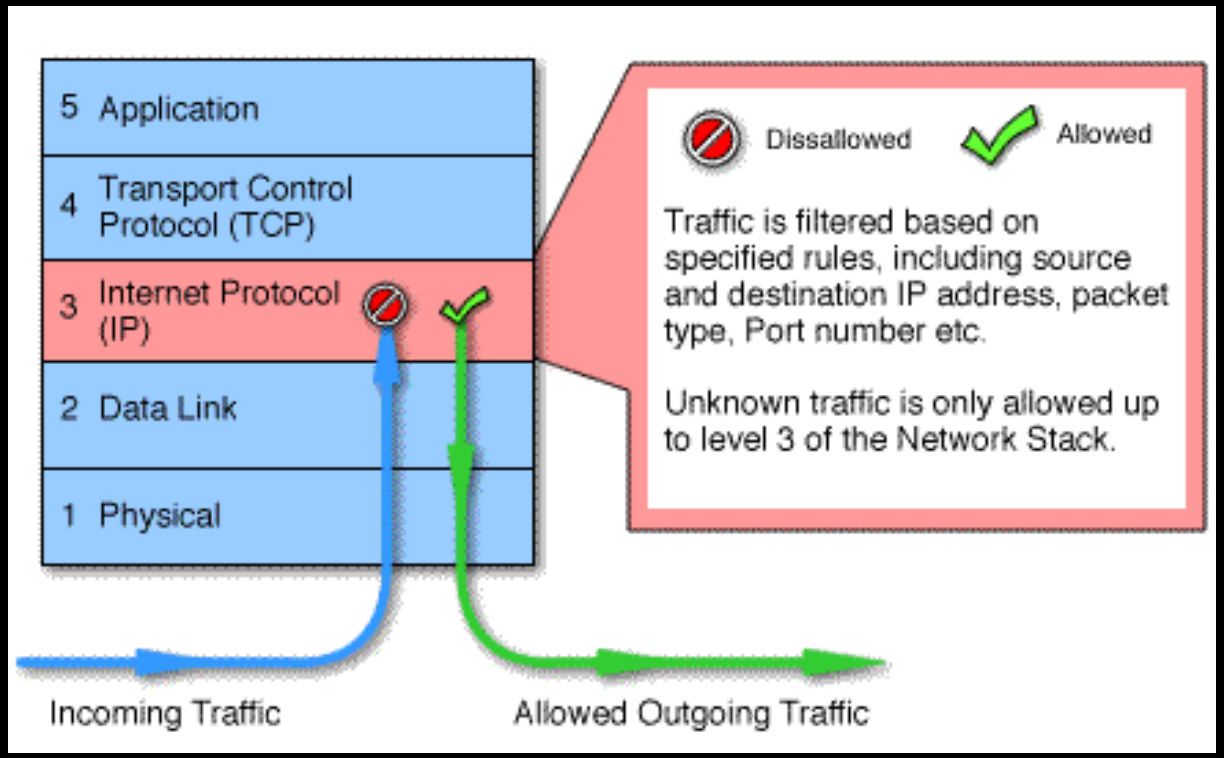
Secure Network Technologies

- Network Address Translation (NAT)
  - Hides the IP addresses of network devices from attackers
  - Private addresses
    - IP addresses not assigned to any specific user or organization
    - Function as regular IP addresses on an internal network
    - Non-routable addresses
  - NAT removes the private IP address from the sender's packet
  - When a packet is returned to NAT, the process is reversed
  - An attacker who captures the packet on the Internet cannot determine the actual IP address of the sender
  - Port address translation (PAT)
    - A variation of NAT
    - Each packet is given the same IP address but a different TCP port number



Packet Filters

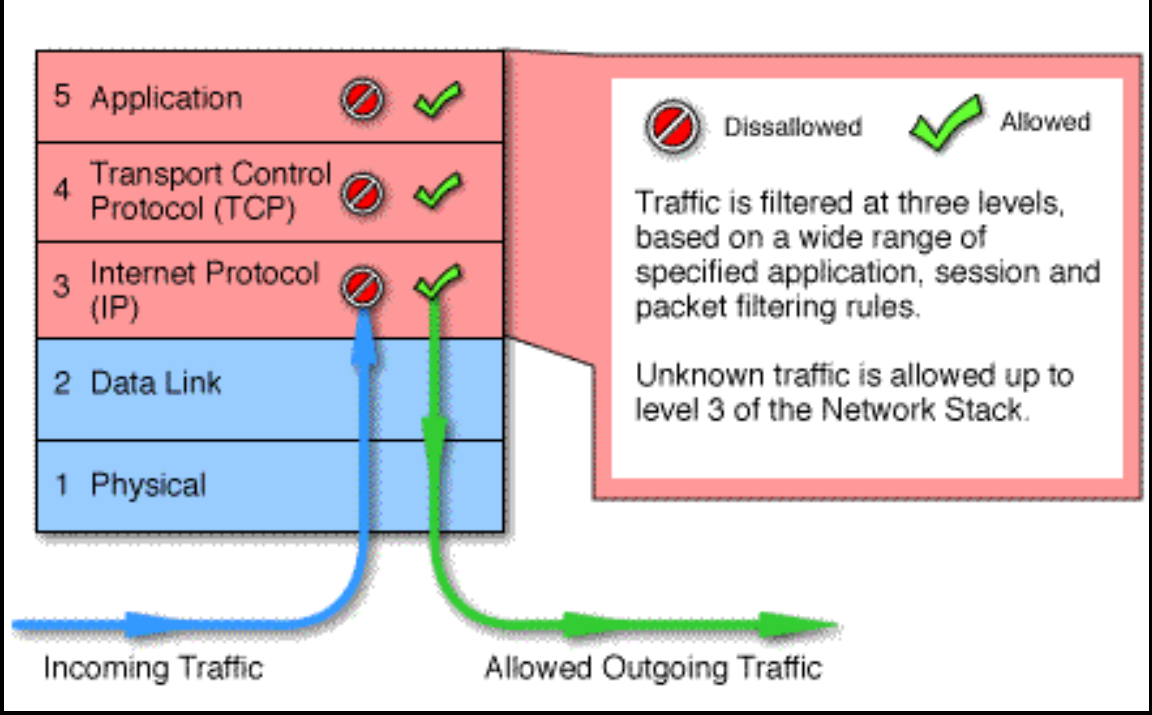
- **Basic packet filtering** involves examining packets, their protocols and destinations, and checking that information against the security policy.



Source: http://www.vicomsoft.com/knowledge/reference/firewalls1.html

Stateful Packet Filtering

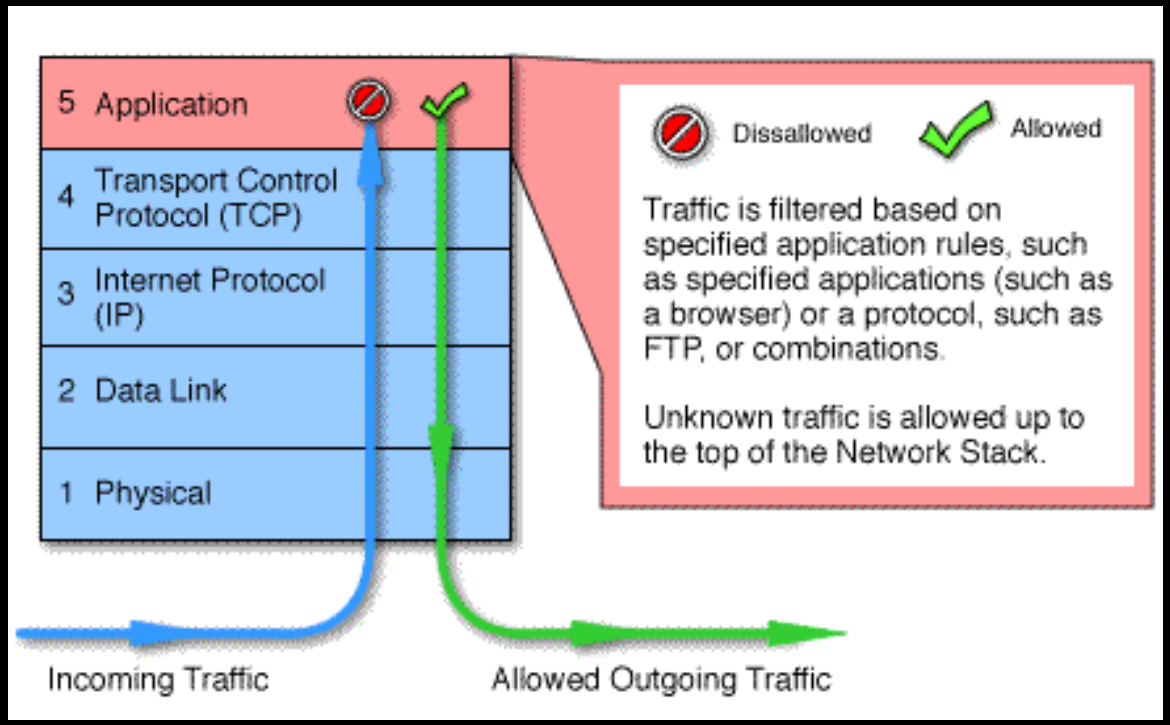
- If a packet arrives from outside the network with no record of its being requested, the firewall will block access by dropping it.
- **Stateful monitoring** enables a system to determine which sets of communications are permissible and which should be blocked.



Source: http://www.vicomsoft.com/knowledge/reference/firewalls1.html

Application Layer Firewalls

- Some high-security firewalls also employ **application layer proxies** through which packets are not allowed to traverse the firewall, but data instead flows up to an application that in turn decides what to do with it.



Source: http://www.vicomsoft.com/knowledge/reference/firewalls1.html

Application Layer Firewalls

- Web application firewall
  - Looks deeply into packets that carry HTTP traffic
    - Web browsers
    - FTP
    - Telnet
  - Can block specific sites or specific known attacks
  - Can block XSS and SQL injection attacks

Application Layer Firewalls

- Proxies
  - Devices that substitute for primary devices
- Proxy server
  - Computer or application that intercepts and processes user requests
  - If a previous request has been fulfilled:
    - Copy of the Web page may reside in proxy server's cache
  - If not, proxy server requests item from external Web server using its own IP address

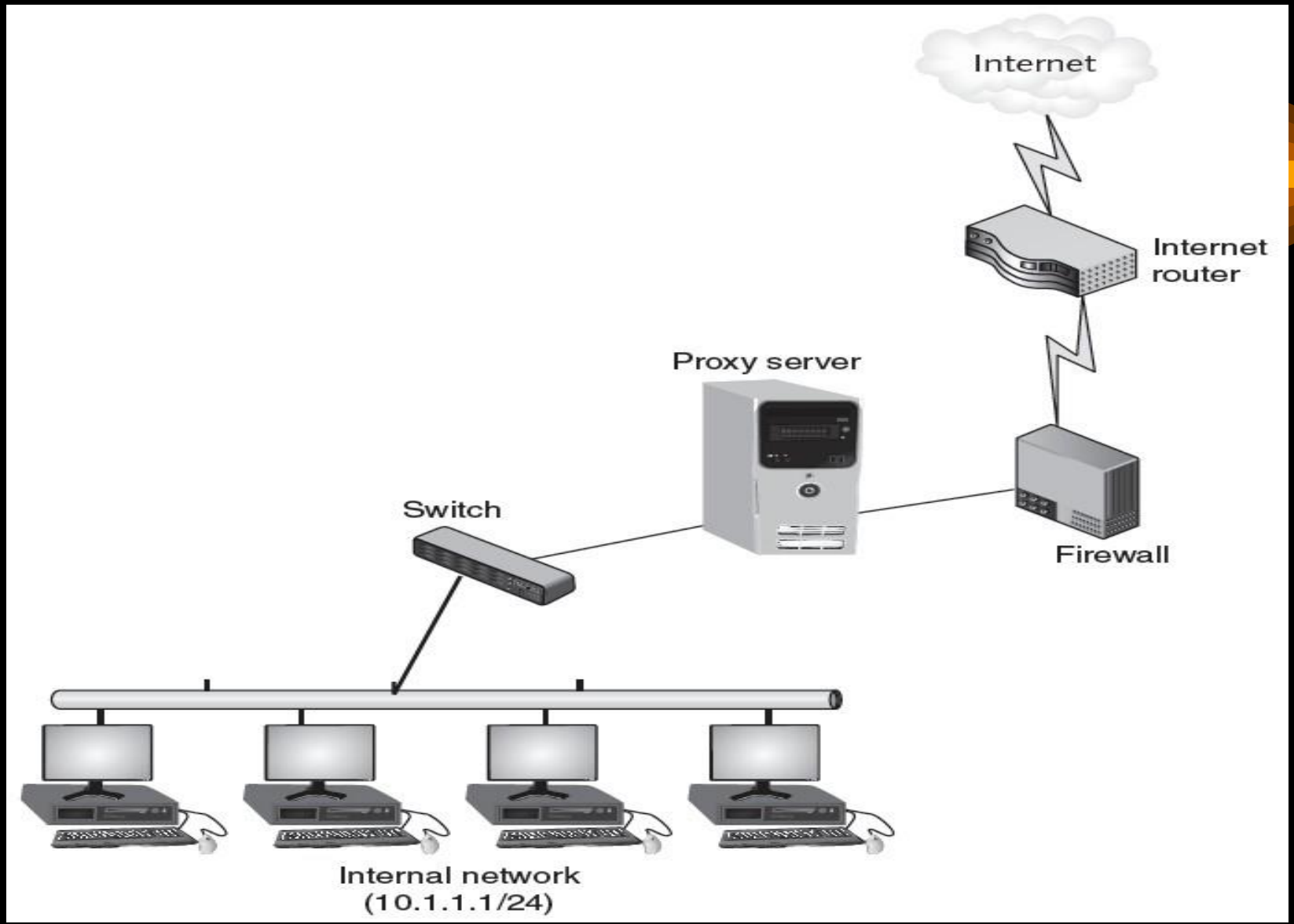


Figure Proxy server

Figure Configuring access to proxy servers

Application Layer Firewalls

- Proxy server advantages
  - Increased speed (requests served from the cache)
  - Reduced costs (cache reduces bandwidth required)
  - Improved management
    - Block specific Web pages or sites
  - Stronger security
    - Intercept malware
    - Hide client system's IP address from the open Internet

Application Layer Firewalls

- Reverse proxy
  - Does not serve clients
  - Routes incoming requests to correct server
  - Reverse proxy's IP address is visible to outside
  - users
    - Internal server's IP address hidden

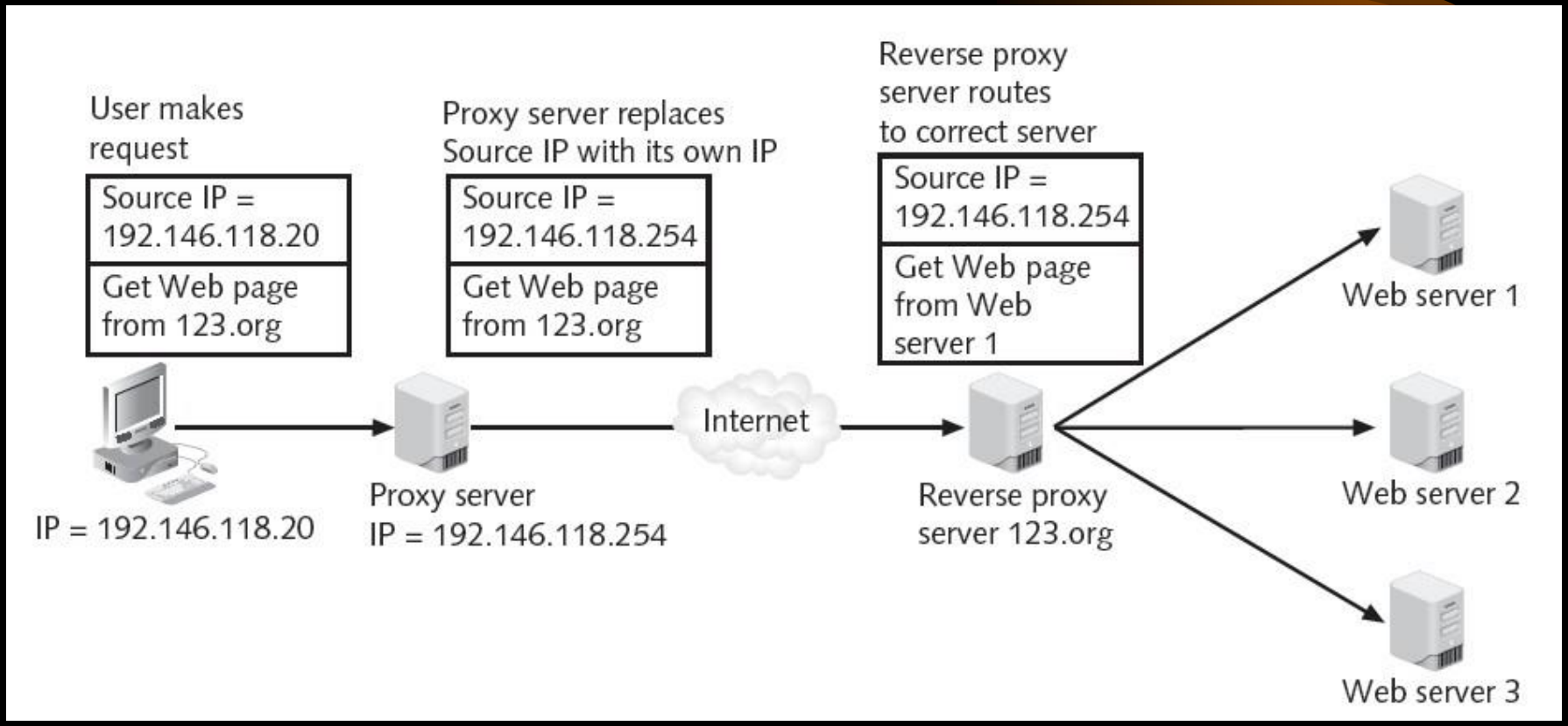


Figure Reverse proxy