COURSE TECHNOLOGY
CENGAGE Learning™

Lecture 4: *Firewall & Intrusion Prevention & Detection Systems*

Overview

- Identify common misconceptions about firewalls
- Explain why a firewall is dependent on an effective security policy
- Understand what a firewall does
- Describe the types of firewall protection
- Recognize the limitations of firewalls
- Firewalls and related technical controls are a fundamental security tool
- Overview of the issues involved in planning and designing firewalls
- Each individual firewall
  - Combination of software and hardware components

Firewalls Explained

- Firewall
  - Anything that can filter the transmission of packets of digital information
  - As they attempt to pass through an interface between networks
- Basic security functions:
  - Packet filtering.
    - A packet filter firewall analyzes network traffic at the network layer.
  - Application proxy.
    - An application level firewall evaluates network packets for valid data at the application layer before allowing a connection at the Application, presentation and session layers.

Misconceptions about Firewalls

- Software firewalls
  - – Permit authorized traffic to pass through while blocking unauthorized and unwanted traffic
  - – Need constant maintenance to keep up with the latest security threats
  - – Work best as part of a multilayered approach to network security

An Analogy: Office Tower Security Guard

- Firewall performs same types of functions as does a security guard at a checkpoint
  - – Monitors entry and exit points
  - – Scans for viruses and repairing infected files before they invade the network
  - – Can be configured to send out alert messages and notify staff of break-ins or if viruses are detected

Firewall Security Features

- Advanced security functions offered by some firewalls
  - Logging
  - VPN
  - Authentication
  - Shielding hosts inside the network so that attackers cannot identify them and use them as staging areas for sustained attacks
  - Caching data
  - Filtering content that is considered inappropriate

Firewall Network Perimeter Security

- Perimeter
  - Boundary between two zones of trust
  - Blurred by
    - Extranet
    - VPN
    - Mobile devices
- Benefit of locating firewall at the perimeter
  - Set up a checkpoint where you can block viruses and infected e-mail messages before they get inside

Firewall Network Perimeter Security (cont'd.)

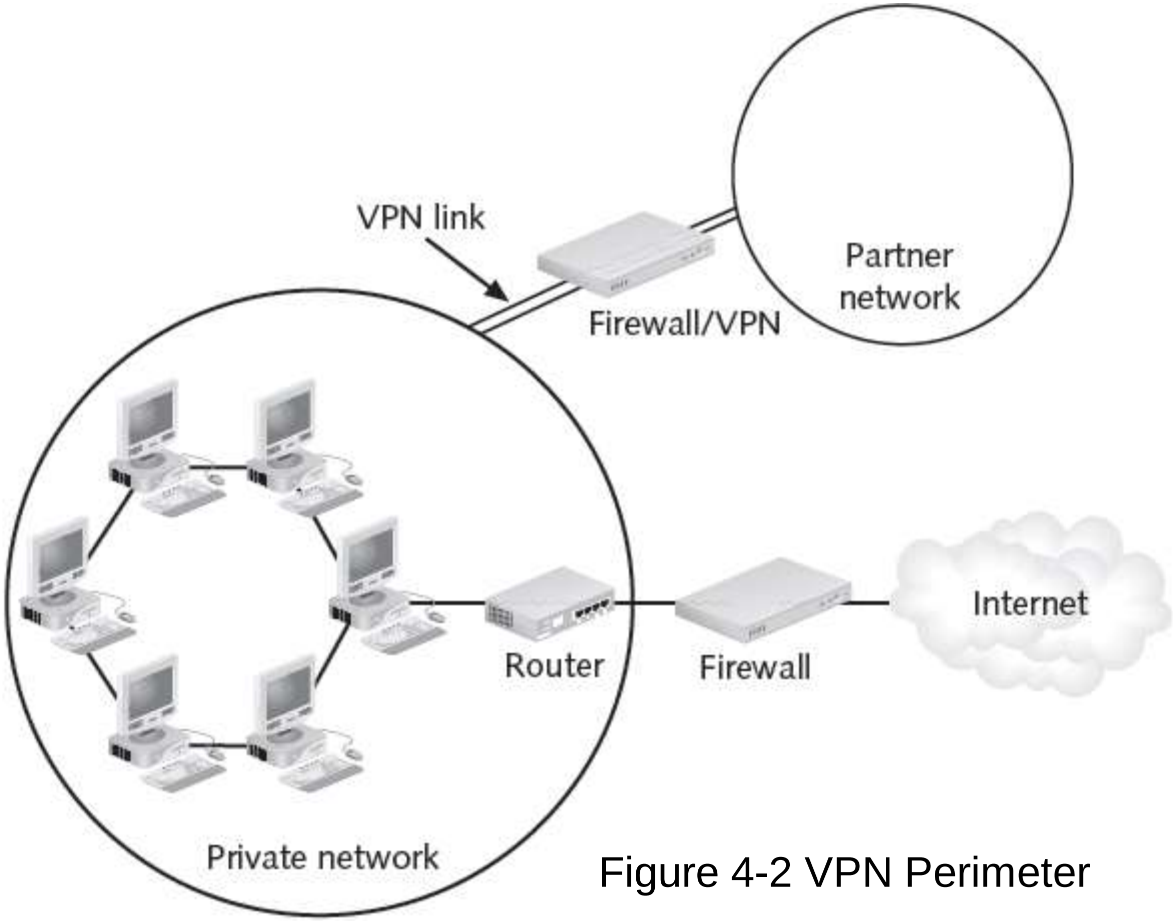


Figure 4-2 VPN Perimeter

@ Cengage Learning 2012

Firewall Components

- Packet filter
- Proxy server
- Authentication system
- Software that perform Network or Port Address Translation (NAT or PAT)
- Bastion host
  - Has only the bare essentials
  - See Figure 4-3

Firewall Components (cont'd.)

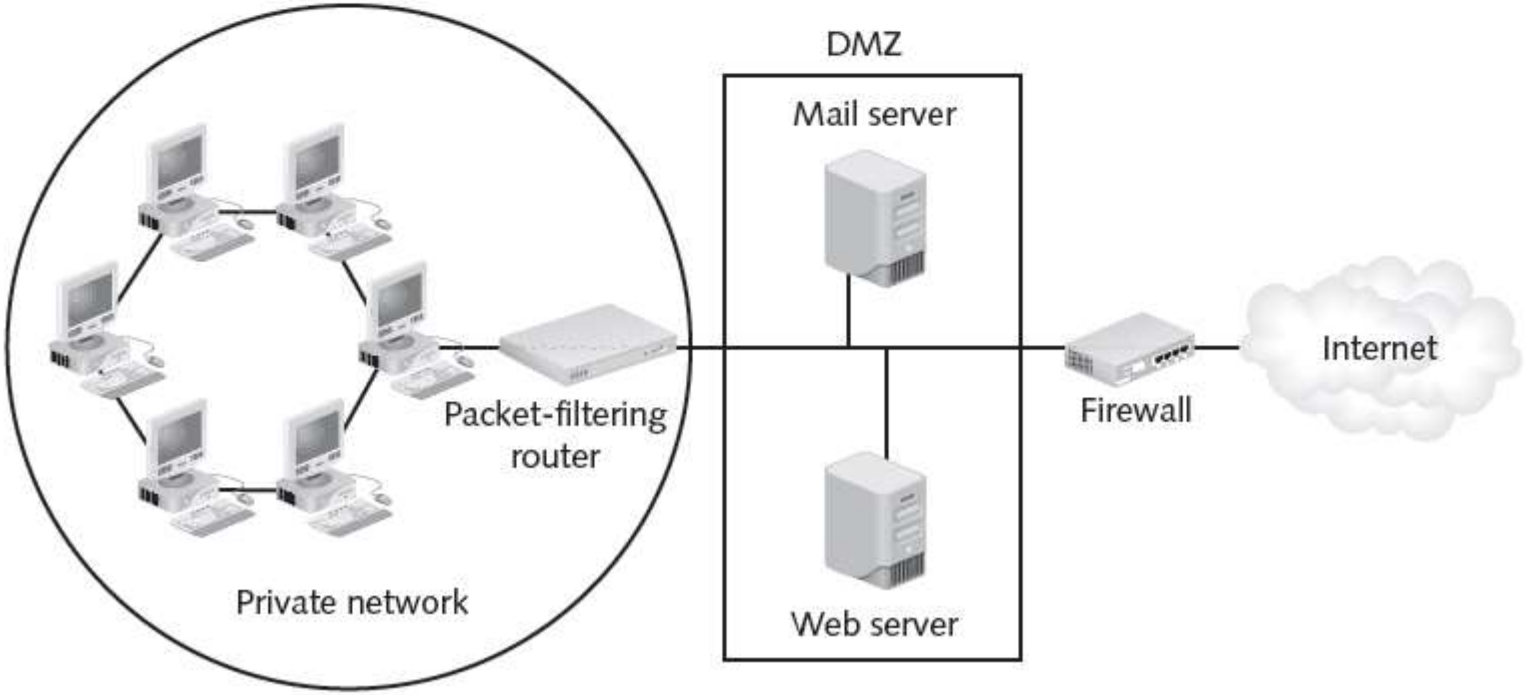


Figure 4-3 DMZ Networks

@ Cengage Learning 2012

Firewall Security Tasks

- Restricting access from outside the network
  - Regulate which packets of information can enter the network
  - Firewall that does packet filtering protects networks from port scanning attacks
- Restricting unauthorized access from inside the network
  - Prevent damage from malicious and careless employees

Technical Details
Ports

- Ports
  - Allow many network services to share a single network address
- Socket
  - Combination of a sender’s full address and receiver’s address
- Port numbers come in two flavors:
  - Well-known ports: number 1023 or below
  - Ephemeral ports: number from 1024 to 65535

Firewall Security Tasks (cont’d.)

- Limiting employee access to external hosts
  - Provide precise control of how employees inside the network use external resources
  - Act as a proxy server
- Protecting critical resources
  - Protect from varied types of attacks
- Protecting against hacking
  - Attacks can also have tangible organization-wide impact

Firewall Security Tasks (cont’d.)

- Providing centralization
  - Centralizes security for the organization it protects
- Enabling documentation
  - Provide information to the network administrator in the form of log files
- Providing for authentication
  - Users with registered usernames and passwords are recognized by the server and allowed to enter
- Contributing to a VPN
  - Connects two companies’ networks over the Internet

Types of Firewall Protection

- Firewalls work in different ways
- Seven-layer OSI networking model
  - See Figure 4-5

Types of Firewall Protection

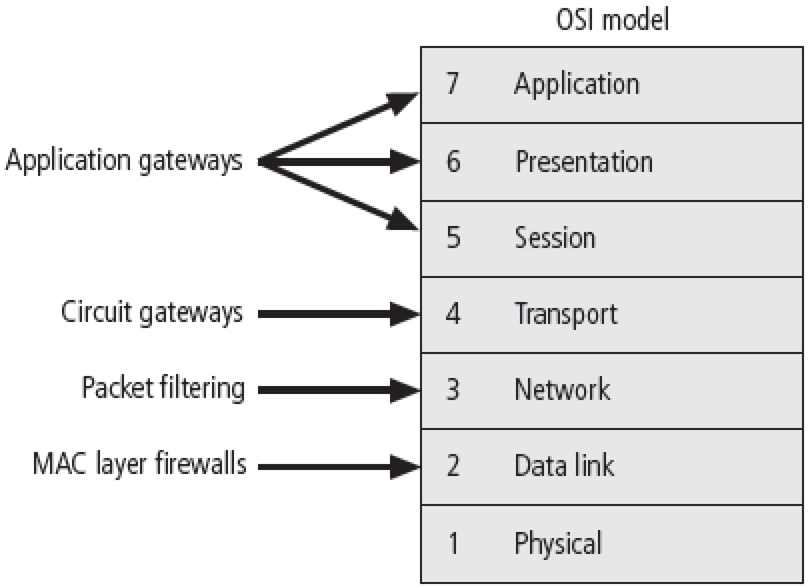


Figure 4-5 Firewalls in the OSI Model

@ Cengage Learning 2012

Packet Filtering

- Packet
  - Sometimes called a datagram
  - Basic element of network data
  - Contains two types of information: header and data
- Packet-filtering firewall
  - Functions at the IP level
  - Determines whether to drop a packet or forward it to the next network connection based on the rules programmed into the firewall

Packet Filtering (cont’d.)

- Filtering firewalls
  - Inspect packets at the network layer (Layer 3) of the OSI model
  - When device finds a packet that violates a rule, it stops the packet from traveling from one network to another
  - Based on a combination of the following:
    - IP source and destination address
    - Direction (inbound or outbound)
    - TCP or UDP (User Datagram Protocol) source and destination port

Packet Filtering (cont'd.)

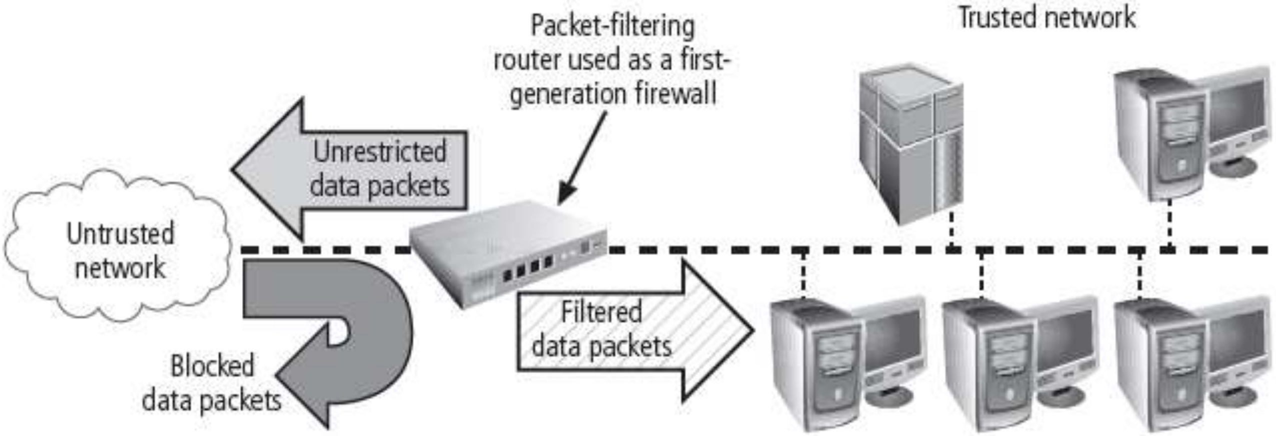

Packet-filtering router used as a first-generation firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

Figure 4-9 Packet Filtering Router

@ Cengage Learning 2012

Packet Filtering (cont'd.)

- Stateless packet-filtering firewalls
  - Ignores the state of the connection between the internal computer and the external computer
- Stateful packet-filtering firewalls
  - Examination of the data contained in a packet and the state of the connection between the internal and the external computer
  - State table
    - Kept in a memory location called the cache.
  - Can leave the system vulnerable to a DoS or DDoS attack

Packet Filtering (cont’d.)

- Packet-filtering rules
  - Depends on the establishment of rules
- Must have a basic understanding of how some of the various protocols that make up the Internet function
  - Internet Control Message Protocol (ICMP)
  - User Datagram Protocol (UDP)
  - TCP filtering
  - IP filtering

PAT and NAT

- Each computer on a network is assigned an IP address
- Port Address Translation (PAT) and Network Address Translation (NAT)
  - Make internal network addresses invisible to outside computers
  - Function as an outbound network-level proxy

PAT and NAT (cont'd.)

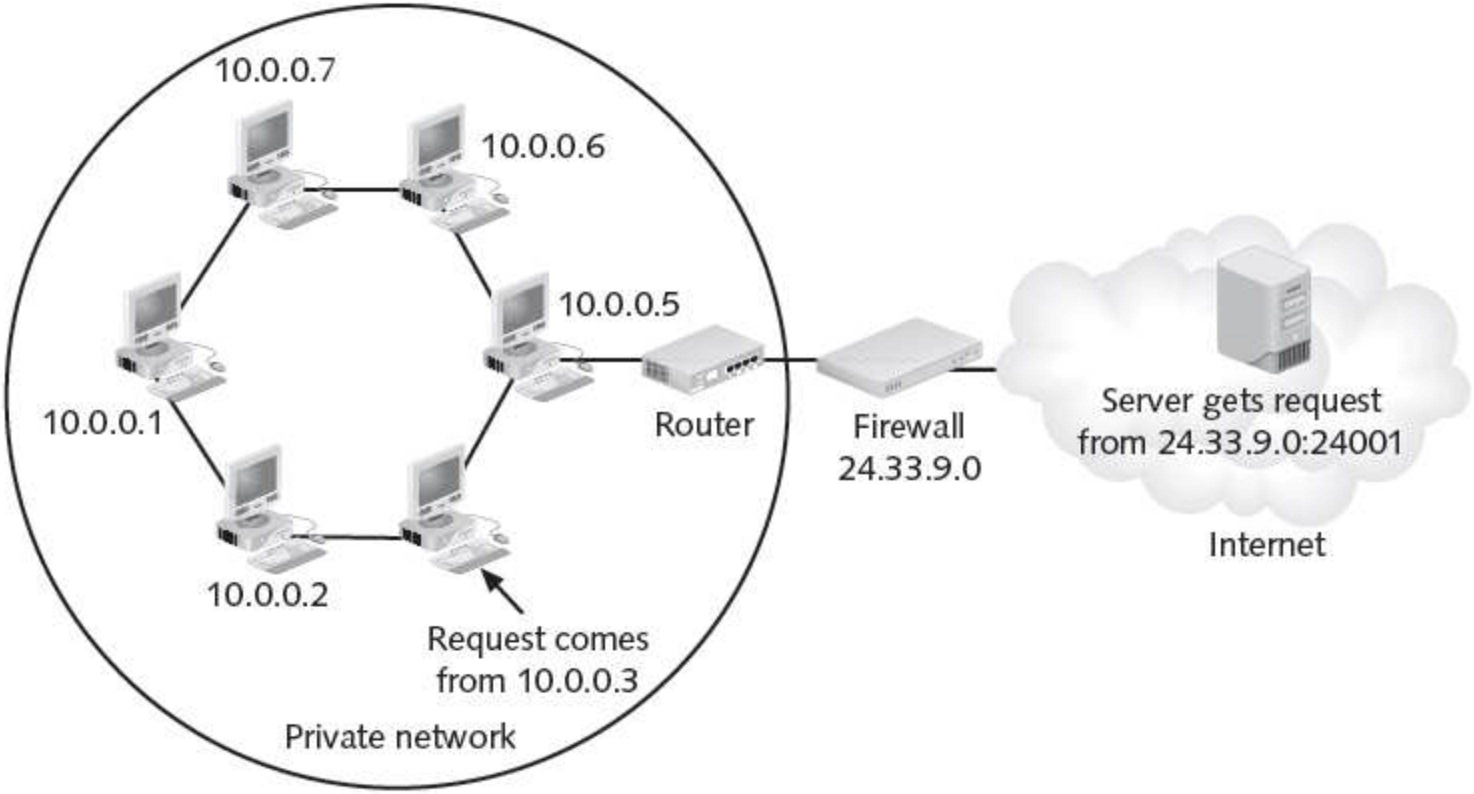


Figure 4-11 Port Address Translation (PAT)

@ Cengage Learning 2012

Application Layer Gateways

- Work at the Application layer
- Control the way applications inside the network access external networks by setting up proxy services
- Minimize the effect of viruses, worms, Trojan horses, and other malware
- Run special software that enable them to act as a proxy for a specific service request

Application Layer Gateways (cont’d.)

- Primary disadvantage
  - Designed for a specific protocol
  - Cannot easily be reconfigured to protect against attacks on other protocols
- Valuable security benefit
  - Can be configured to allow or deny (both actions can be taken as a result of filtering) specific content, such as viruses and executables

Offline
“X” Marks the Spot

- Letter “x” used in two ways
  - 10.10.x.x, where the “x” indicates a value in the range of 0 to 254 that can be assigned by the user organization
  - Represent “any” value, but in a different location
    - Any address that meets the defined portion of the address

Technical Details
Fresh Hot CIDR

- “CIDR”
  - Classless Inter-Domain Routing
- CIDR Mask
  - Mitigate the inefficiencies in the way IP addresses used to be organized and assigned
- Assigns addresses using the demarcation between network address and host address
- Slash (/) and number following the slash
  - Indicate where the boundary between network address and host address is located

Firewall Categories

- “Processing mode”
  - How the firewall examines the network traffic that it is trying to filter
- “Generation”
  - Level of technology a firewall has
  - Later generations being more complex and more recently developed
- “Structure”
  - Kind of structure for which the firewalls are intended

Processing Mode

- Five major processing-mode categories for firewalls:
  - Packet-filtering firewalls, application gateways, circuit gateways, MAC layer firewalls, and hybrids
  - Most are hybrids
- Packet-filtering firewalls
  - Three kinds of packet-filtering firewalls:
    - Static filtering, dynamic filtering, and stateful inspection

Processing Mode (cont’d.)

- Application gateways
  - Frequently installed on a dedicated computer,
  - Separate from the filtering router
  - Commonly used in conjunction with a filtering router
- Circuit gateways
  - Operates at the transport layer
  - Connections are authorized based on addresses

Processing Mode (cont'd.)

- MAC layer firewalls
  - Operate at the media access control sublayer of the data link layer
  - Consider specific host computer's identity
- Hybrid firewalls
  - Combine the elements of various types of firewalls

Firewall Generations

- First-generation firewalls
  - Static packet-filtering firewalls
- Second-generation firewalls
  - Application-level firewalls or proxy servers
- Third-generation firewalls
  - Stateful inspection firewalls
- Fourth-generation firewalls
  - Also known as dynamic packet-filtering firewalls
  - Allow only a particular packet with a particular source, destination, and port address to enter

Firewall Generations (cont'd.)

- Fifth-generation firewalls
  - Kernel proxies
  - Works under Windows NT Executive
    - Kernel of Windows NT

Firewall Structures

- Commercial-grade firewall appliances
  - Stand-alone, self-contained combinations of computing hardware and software
  - Have many of the features of a general-purpose computer
  - With the addition of firmware-based instructions
    - Increase reliability and performance
    - Minimize the likelihood of being compromised

Firewall Structures (cont'd.)

- Commercial-grade firewall systems
  - Consists of application software that is configured for the firewall application
  - Runs on a general-purpose computer
- Full-featured, commercial-grade firewall packages
  - Check Point Power-1
  - Cisco ASA
  - Microsoft Internet Security & Acceleration Server
  - McAfee Firewall Enterprise (Sidewinder)

Firewall Structures (cont'd.)

- Small office/home office (SOHO) firewall appliances
  - Most effective methods of improving computing security in the SOHO setting
  - Serves first as a stateful firewall
  - Enables inside-to-outside access
  - Can be configured to allow limited TCP/IP port forwarding and/or screened subnet capabilities

Firewall Structures (cont’d.)

- Broadband router devices
  - Can function as packet-filtering firewalls
  - Enhanced to combine the features of wireless access points (WAPs) as well as small stackable LAN switches in a single device
- Provide more than simple NAT services
  - Include packet filtering, port filtering, and simple intrusion detection systems
  - Restrict access to specific MAC addresses

Firewall Structures (cont’d.)

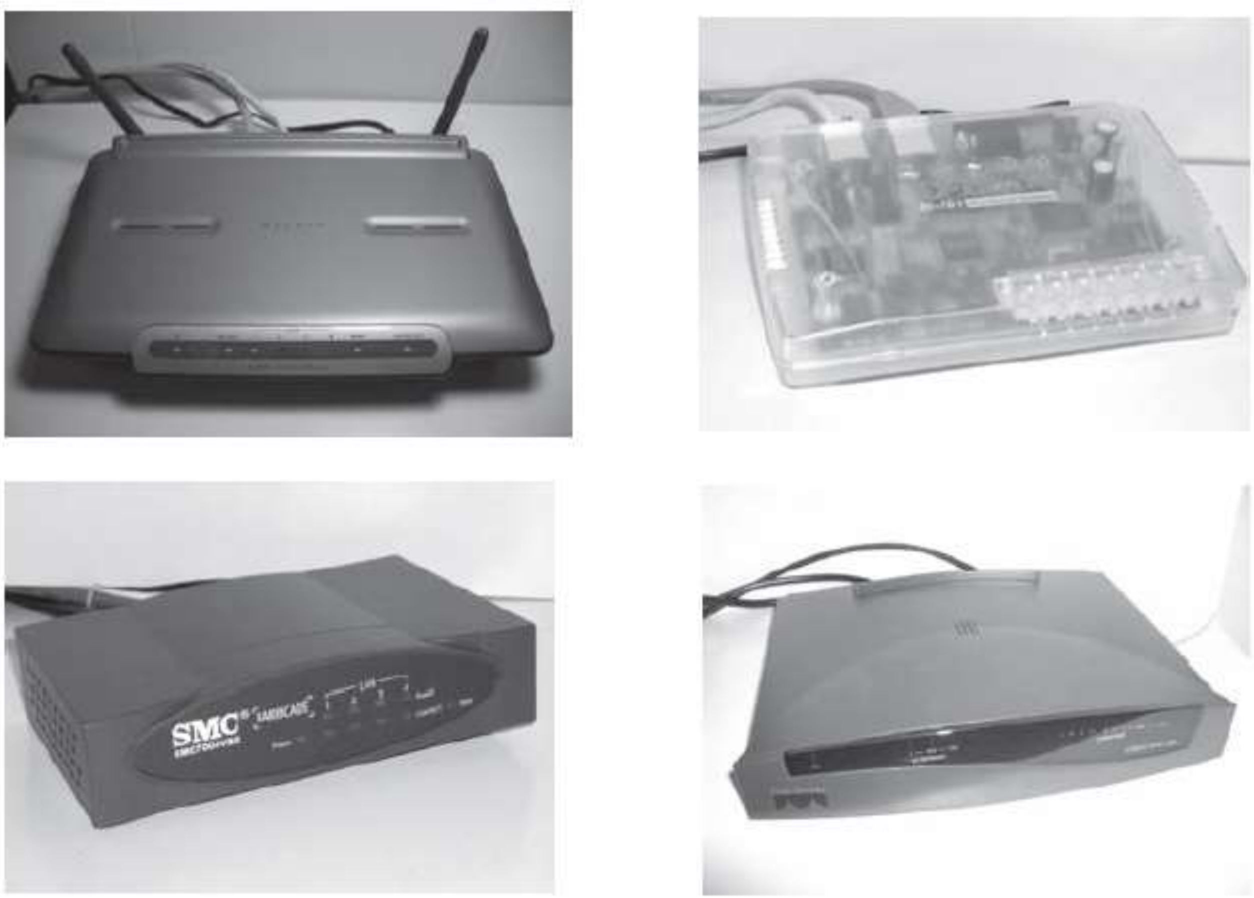


Figure 4-12 Example SOHO Firewalls

@ Cengage Learning 2012

Firewall Structures (cont’d.)

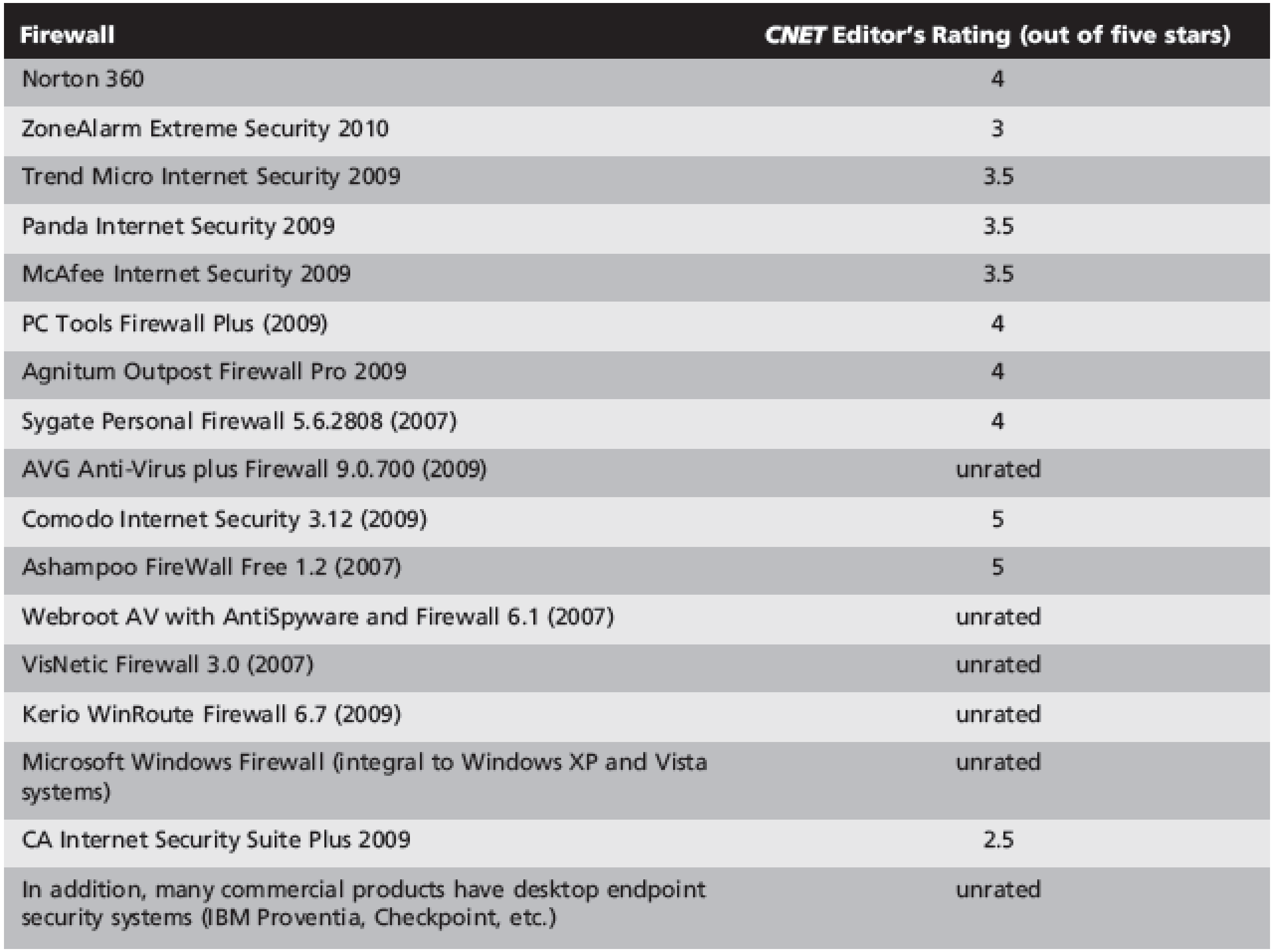
- Software firewalls
  - Many of the firewalls in Table 4-4 provide free versions of their software
  - Not fully functional
  - “You get what you pay for”

Firewall Structures (cont’d.)

- Free firewall tools on the Internet
  - Most of the free firewall software also run on a free operating system
  - Convenience, simplicity, and unbeatable price
- Netfilter
  - Firewall software that comes with the Linux 2.4 kernel
  - Powerful solution for stateless and stateful packet filtering, NAT, and packet processing

Firewall Structures (cont'd.)

- Software vs. hardware: the SOHO firewall debate
  - Hardware device
    - If the attacker manages to crash the firewall system
      - Computer and information are still safely behind the now-disabled connection
    - Assigned a nonroutable IP address
    - Virtually impossible to reach from the outside
  - Software device
    - Can be disabled and allow free network access



Firewall	*CNET* Editor's Rating (out of five stars)
Norton 360	4
ZoneAlarm Extreme Security 2010	3
Trend Micro Internet Security 2009	3.5
Panda Internet Security 2009	3.5
McAfee Internet Security 2009	3.5
PC Tools Firewall Plus (2009)	4
Agnitum Outpost Firewall Pro 2009	4
Sygate Personal Firewall 5.6.2808 (2007)	4
AVG Anti-Virus plus Firewall 9.0.700 (2009)	unrated
Comodo Internet Security 3.12 (2009)	5
Ashampoo FireWall Free 1.2 (2007)	5
Webroot AV with AntiSpyware and Firewall 6.1 (2007)	unrated
VisNetic Firewall 3.0 (2007)	unrated
Kerio WinRoute Firewall 6.7 (2009)	unrated
Microsoft Windows Firewall (integral to Windows XP and Vista systems)	unrated
CA Internet Security Suite Plus 2009	2.5
In addition, many commercial products have desktop endpoint security systems (IBM Proventia, Checkpoint, etc.)	unrated

Table 4-4 Common Software Firewalls As Rated by CNET (www.cnet.com)

Firewall Architectures

- Packet-filtering routers
  - Can be configured to reject packets that the organization does not allow into the network
- Screened host firewalls
  - Combine the packet-filtering router with a separate, dedicated firewall
    - Application proxy server

Firewall Architectures (cont'd.)

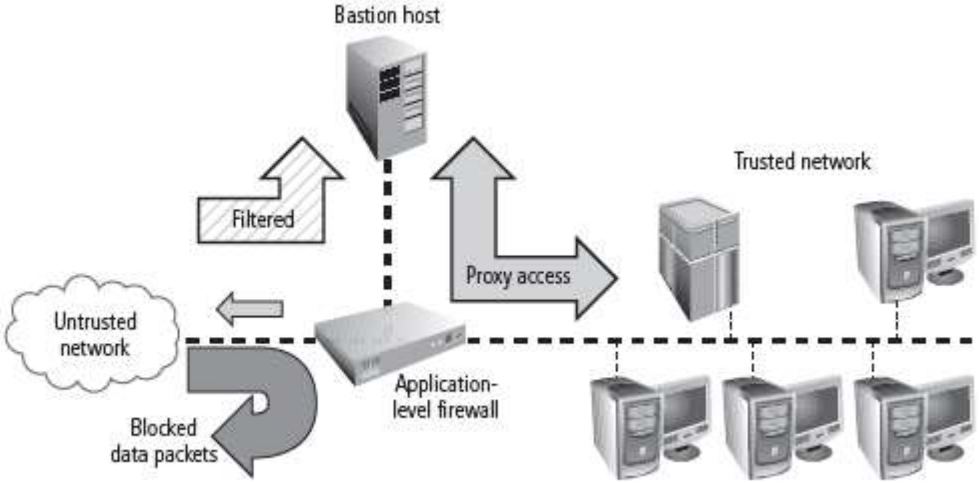


Figure 4-17 Screened Host Architecture

@ Cengage Learning 2012

Firewall Architectures (cont’d.)

- Dual-homed host firewalls
  - Bastion host contains two NICs rather than one
  - One NIC is connected to the external network
  - One is connected to the internal network
  - All traffic must physically go through the firewall to move between the internal and external networks

Firewall Architectures (cont’d.)

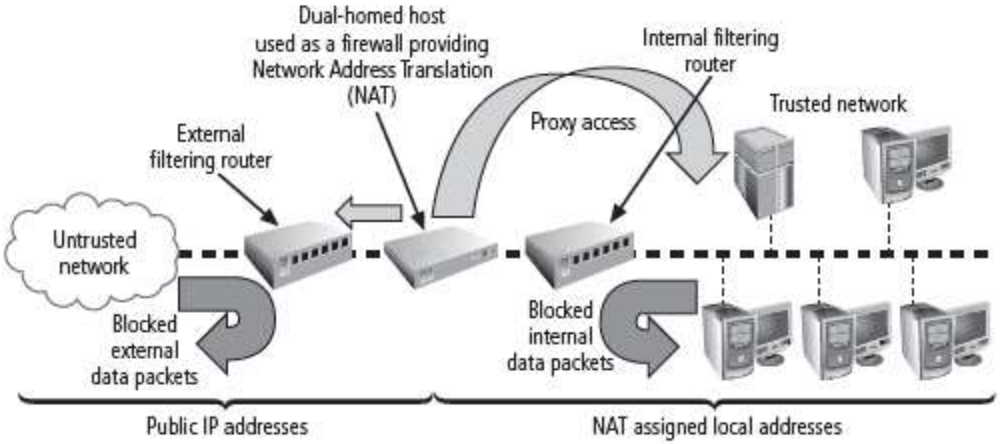

Dual-homed host used as a firewall providing Network Address Translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT assigned local addresses

Figure 4-18 Dual-Homed Host

@ Cengage Learning 2012

Firewall Architectures (cont’d.)

- Screened subnet firewalls (with DMZ)
  - Dominant architecture used today
  - Subnet firewall consisting of two or more internal bastion hosts behind a packet-filtering router
  - Each host protecting the trusted network
  - Many variants of the screened subnet architecture

Firewall Architectures (cont'd.)

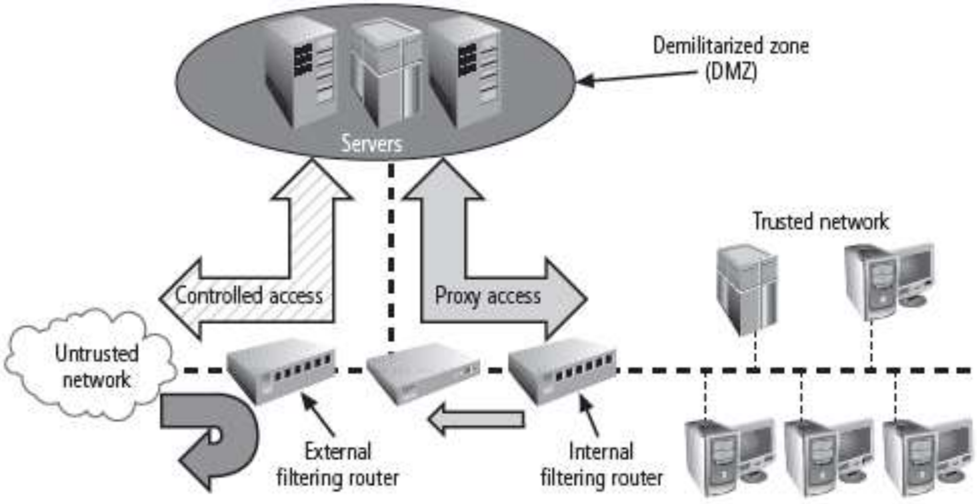


Figure 4-19 Screened Subnet

@ Cengage Learning 2012

Limitations Of Firewalls

- Cannot be expected to do everything
- Should not be the only form of protection for a network

Summary

- Firewall filters the transmission of packets of digital information
  - As they attempt to pass through a network boundary
- Packet filtering
  - Key function of any firewall
- Application layer gateways
  - Control the way applications inside the network access external networks
- Firewalls can be categorized by:
  - Processing mode, generation, or structure