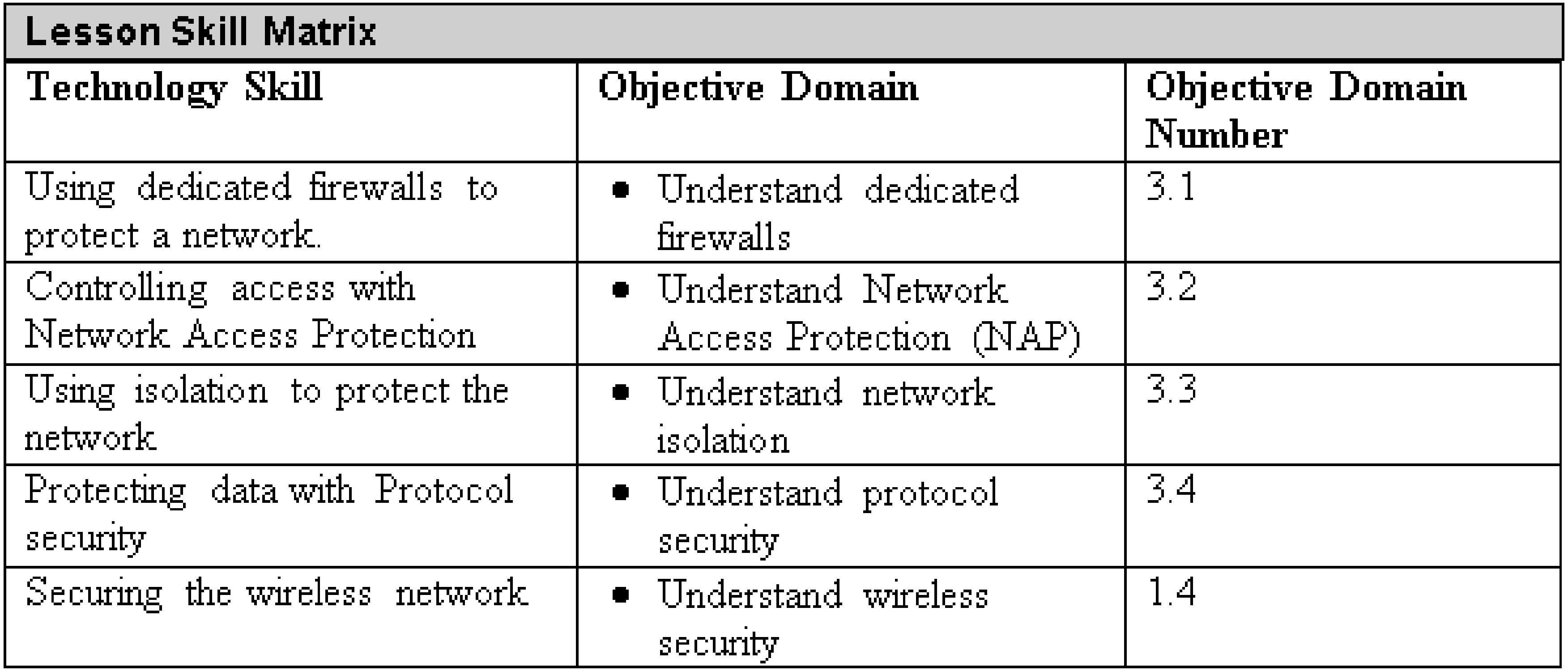
Understanding Network Security

Lesson 4

Objectives

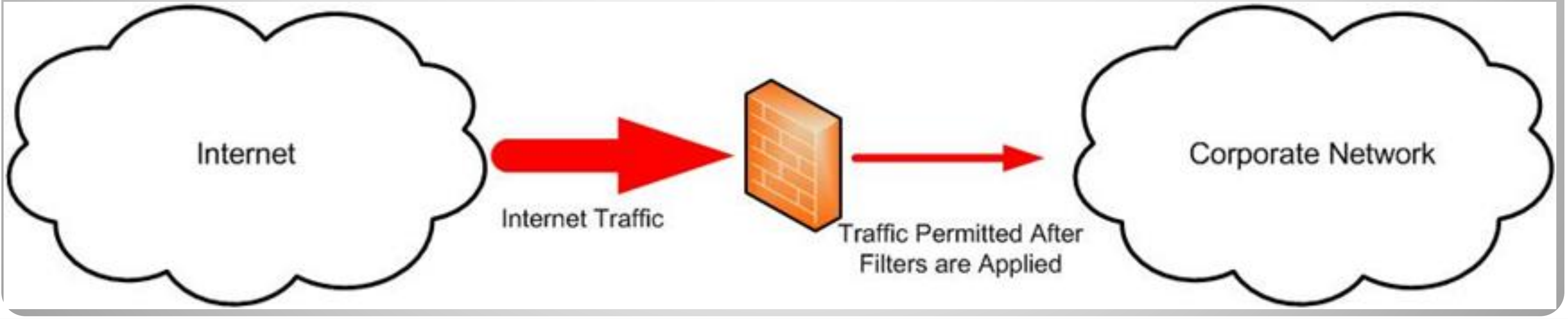


Lesson Skill Matrix

Technology Skill	Objective Domain	Objective Domain Number
Using dedicated firewalls to protect a network.	- Understand dedicated firewalls	3.1
Controlling access with Network Access Protection	- Understand Network Access Protection (NAP)	3.2
Using isolation to protect the network	- Understand network isolation	3.3
Protecting data with Protocol security	- Understand protocol security	3.4
Securing the wireless network	- Understand wireless security	1.4

Firewall

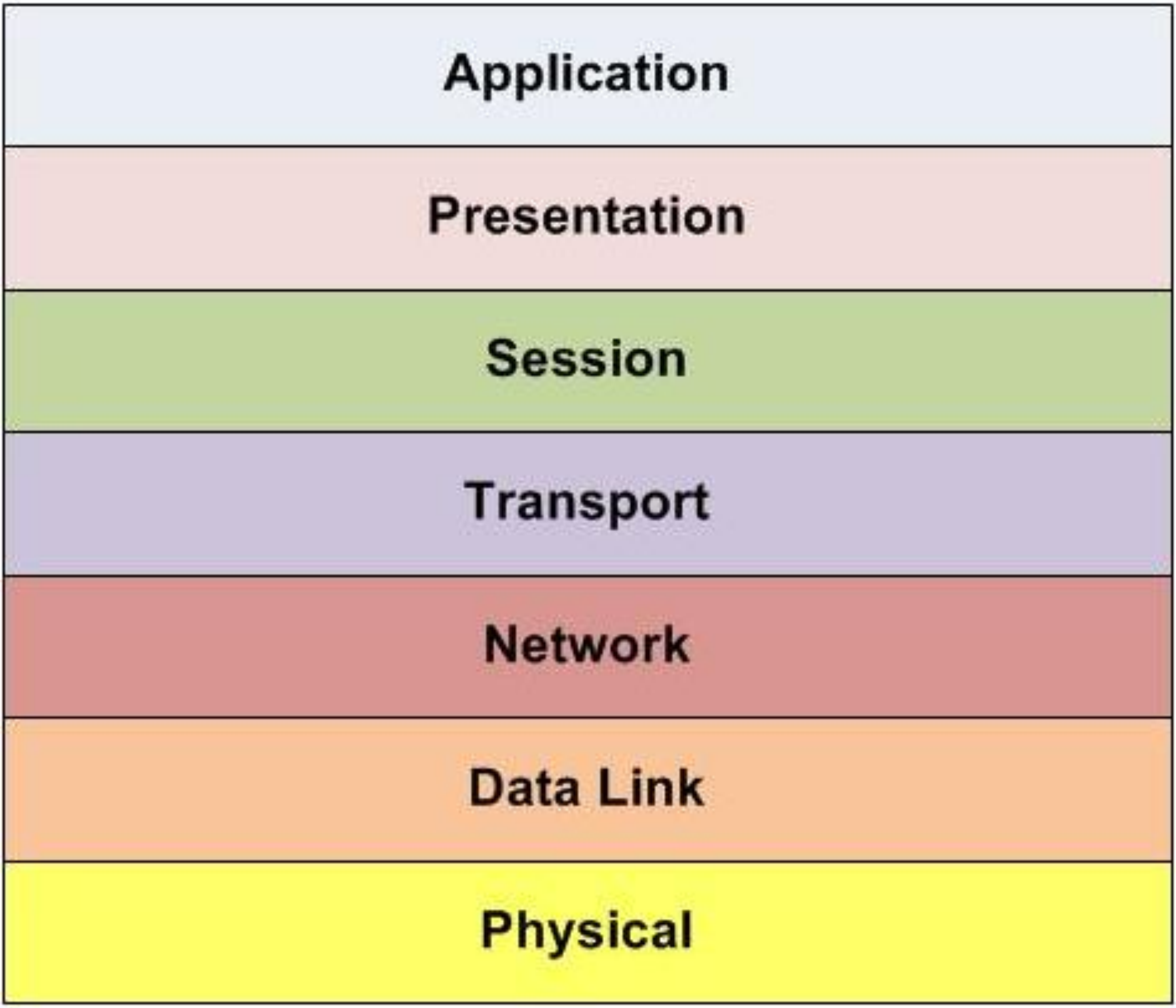
- Firewalls remain the foundation of network security technologies.
- A firewall is a system that is designed to protect a computer or a computer network from network-based attacks.
- A firewall does this by filtering the data packets traversing the network.



OSI Model

- The OSI model is a conceptual model, created by the International Organization for Standardization (ISO) in 1978 and revised in 1984, to describe a network architecture that allows data to be passed between computer systems.
- While never fully utilized as model for a protocol, the OSI model is the standard for discussing how networking works.

OSI Model



Application

Presentation

Session

Transport

Network

Data Link

Physical

OSI Model

- **Physical Layer (Layer 1) -** Define the physical characteristics of the network, including Media, hardware and topology
- **Data-Link Layer (Layer 2) -** Connects the data layer to the physical layer so that the data can be transmitted across the network. The data link layer handles error detection, error correction and hardware addressing.
  - The data link layer is broken into two sub-layers, the Media Access Control (MAC) sub-layer and the Logical Link Control (LLC) sub-layer.

OSI Model

- **Network Layer (Layer 3) -** Primarily responsible for routing.
- **Transport Layer (Layer 4)** - Provides the mechanisms for carrying data across the network. It uses three main mechanisms: segmentation, service addressing and error checking.

OSI Model

- **Session Layer (Layer 5) -** Responsible for data synchronization between the applications on the two devices. The session layer establishes, maintains, and breaks sessions between devices.
- **Presentation Layer (Layer 6) -** The presentation layer converts application layer data into a format that permits the data to be transmitted across the network.

OSI Model

- **Application Layer (Layer 7) -** Takes data from the user and passes the data to the lower layers of the OSI model for transport. Responses are passed up through the layers and are displayed back to the user.

Packet Filtering

- Packet filtering firewall is considered the first generation firewall
- A packet filtering firewall inspects the data packets as they attempt to traverse the firewall, and based on the rules that have been defined on the firewall, the firewall allows or denies each packet.
- Routers have the ability to do some rudimentary packet filtering, such as permitting all outbound traffic while denying all inbound traffic, or blocking specific protocols from passing through the router, like telnet or ftp.

Packet Filtering

- When you are configuring a packet filtering firewall rule, you will generally use one (or more) of the following TCP/IP attributes:
  - Source IP addresses
  - Destination IP addresses
  - IP protocol (telnet, ftp, http, https, etc.)
  - Source TCP and UDP ports (for example, the http protocol runs on TCP port 80)
  - Destination TCP and UDP ports
  - The inbound firewall network interface
  - The outbound firewall network interface

Circuit-Level Firewalls

- Circuit-level firewalls are typically considered a second generation firewall technology.
- They work in a very similar fashion as packet-filtering firewalls, but they operate at the transport and session layers of the OSI model.
- Instead of analyzing each individual packet, a circuit-level firewall monitors TCP/IP sessions, by monitoring the TCP handshaking between packets to validate the session.
- Traffic is filtered based on specified session rules and may be restricted to authorized computers only.

Application-Level Firewall

- Application-level firewalls (also known as proxy servers) work by performing a deep inspection of application data as it traverses the firewall.
- Rules are set based by analyzing client requests and application responses, then enforcing correct application behavior.
- Application-level firewalls can block malicious activity, log user activity, provide content filtering and even protect against spam and viruses.

Stateful Firewall

- Stateful multi-level firewalls are designed to provide the best features of both packet filtering and application-level firewalls.
- Stateful inspection also determines whether or not a packet is part of an existing session and that information can be used to determine whether to permit or deny a packet.

Host versus Network Firewalls

- There are two basic types of software firewall:
  - ***Host firewall:*** A software firewall is a firewall application installed on a host, used to protect the host from network-based attacks.
    - Host firewalls are also known as ***personal firewalls***.
  - ***Network firewall***: The other type of software firewall is a firewall application installed on a server used to protect network segments from other network segments.

Network Access Protection

- ***Network Access Protection (NAP)*** is solution that allows administrators a more powerful way to control access to network resources.
- These controls are based on a client computer’s identity and whether the computer complies with the configured network governance policies.
- These components require health state validation and if the computer is not compliant, they enforce limited network access using the Network Policy Server (NPS) which is a component in Windows Server 2008.

Network Access Protection

- NAP has three distinct components:
  - **Health State Validation**: In order to validate the health state of a computer, the administrator defines health requirement policies. Then when the computer tries to connect to the network, system health agents (SHAs) and system health validators (SHVs) validate the computer’s configuration against the health requirement policy.

Network Access Protection

- **Health Policy Compliance:** Administrators can enforce compliance with health requirement policies by configuring NAP to automatically update noncompliant computers with missing software updates or configuration changes.
- **Limited Access Mode:** The final component that NAP provides to protect the network is Limited Access Mode. This mode permits administrators to protect their networks by limiting the access of noncompliant computers.

Network Access Protection

- The NPS also allows the Windows Server 2008 host to act as the health policy server, enforcing limited access in the following ways:
  - IPsec Enforcement
  - 802.1x Enforcement
  - VPN Enforcement
  - DHCP Enforcement

Virtual LANs (VLANS)

- Virtual LANs (VLANs) were developed as an alternate solution to deploying multiple routers.
- VLANs are logical network segments used to create separate broadcast domains, but still allow the devices on the VLANs to communicate at Layer 2, without requiring a router.
- VLANs are created by switches, and traffic between VLANs is switched, not routed, which creates a much faster network connection, as there is no need for a routing protocol to be involved.
- Even though the hosts are logically separated, the traffic between the hosts is switched directly as if the hosts were on the same LAN segment.

Virtual LANs (VLANS)

- VLANs provide a number of benefits over a routed network, including:
  - Higher performance on medium or large LANs due to reduced broadcast traffic
  - Organizing devices on the network for easier management.
  - Providing additional security because devices can be put on their own VLAN.

Routing

- Routing takes one step up the OSI model from the VLAN – and takes place at Layer 3.
- Routing is the process of forwarding a packet based on the packet's destination address.
- At each step in the route a packet takes across the network a decision has to be made about where the packet is to be forwarded.
- To make these decisions, the IP layer consults a routing table stored in the memory of the routing device.

Routing Protocols

- Routing protocols are based either on a distance vector or link state algorithm.
- Path selection involves apply a routing metric to multiple routes, in order to select the best route.
- Some of the metrics used are bandwidth, network delay, hop count, path cost, load, reliability, and communication costs.
- The hop count is the number of routers traversed by a packet between its source and destination.

IDS and IPS

- Two other security technologies available to secure networks are ***intrusion detection systems (IDS)*** and ***intrusion prevention systems (IPS)***.
- An IDS is a solution designed to detect unauthorized user activities, attacks, and network compromises.
- An intrusion prevention system (IPS) is very similar to an IDS, except that in addition to detecting and alerting, an IPS can also take action to prevent to breach from occurring.

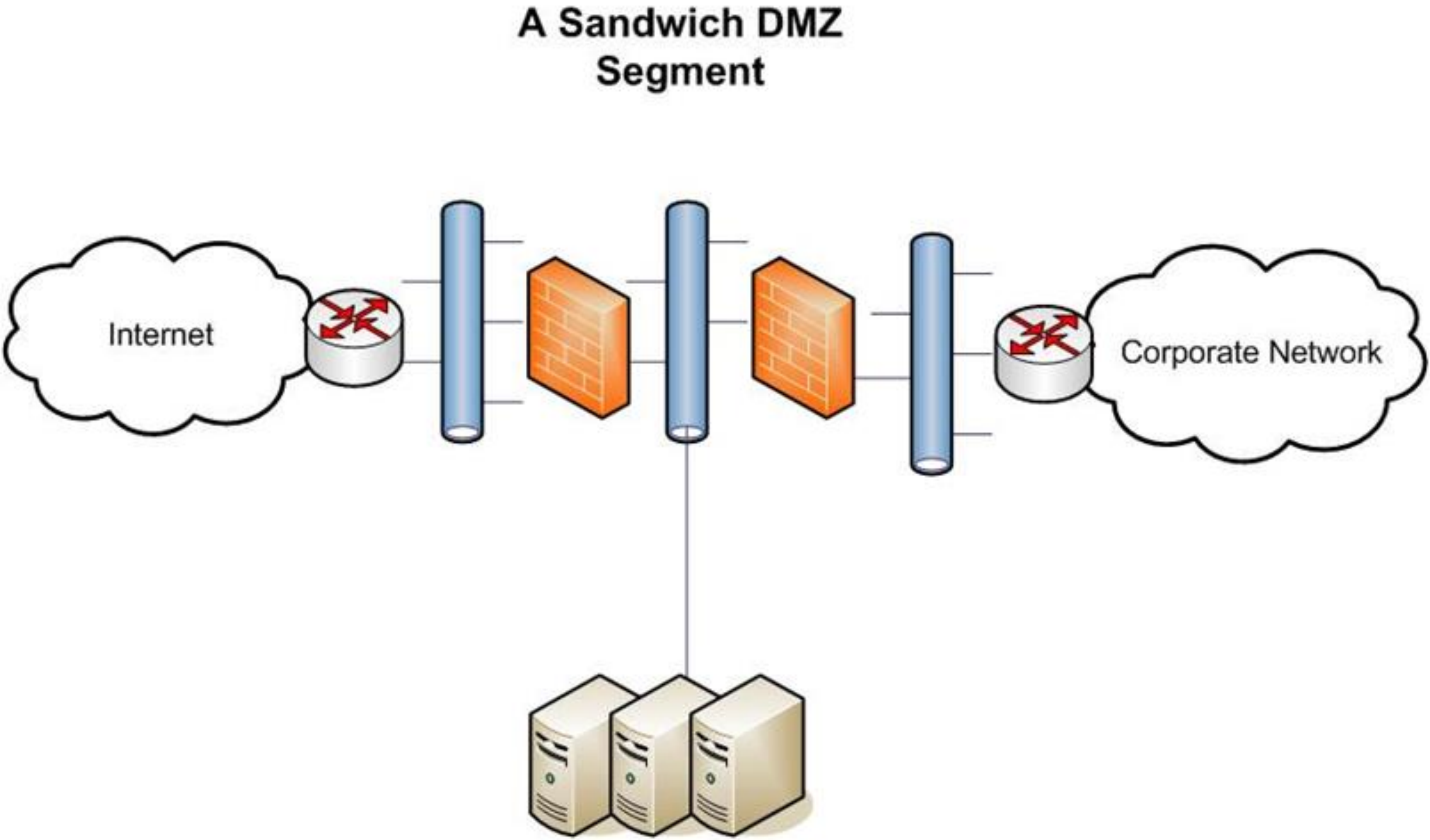
Honeypots

- A ***honeypot*** is a trap for hackers. A honey pot is designed to distract hackers from real targets, detect new vulnerabilities and exploits, and learn about the identity of attackers.
- A ***honey net*** is just a collection of honeypots used to present an attacker an even more realistic attack environment.
- A padded cell is a system that waits for an IDS to detect an attacker and then transfers the attacker to a special host where they cannot do any damage to the production environment.

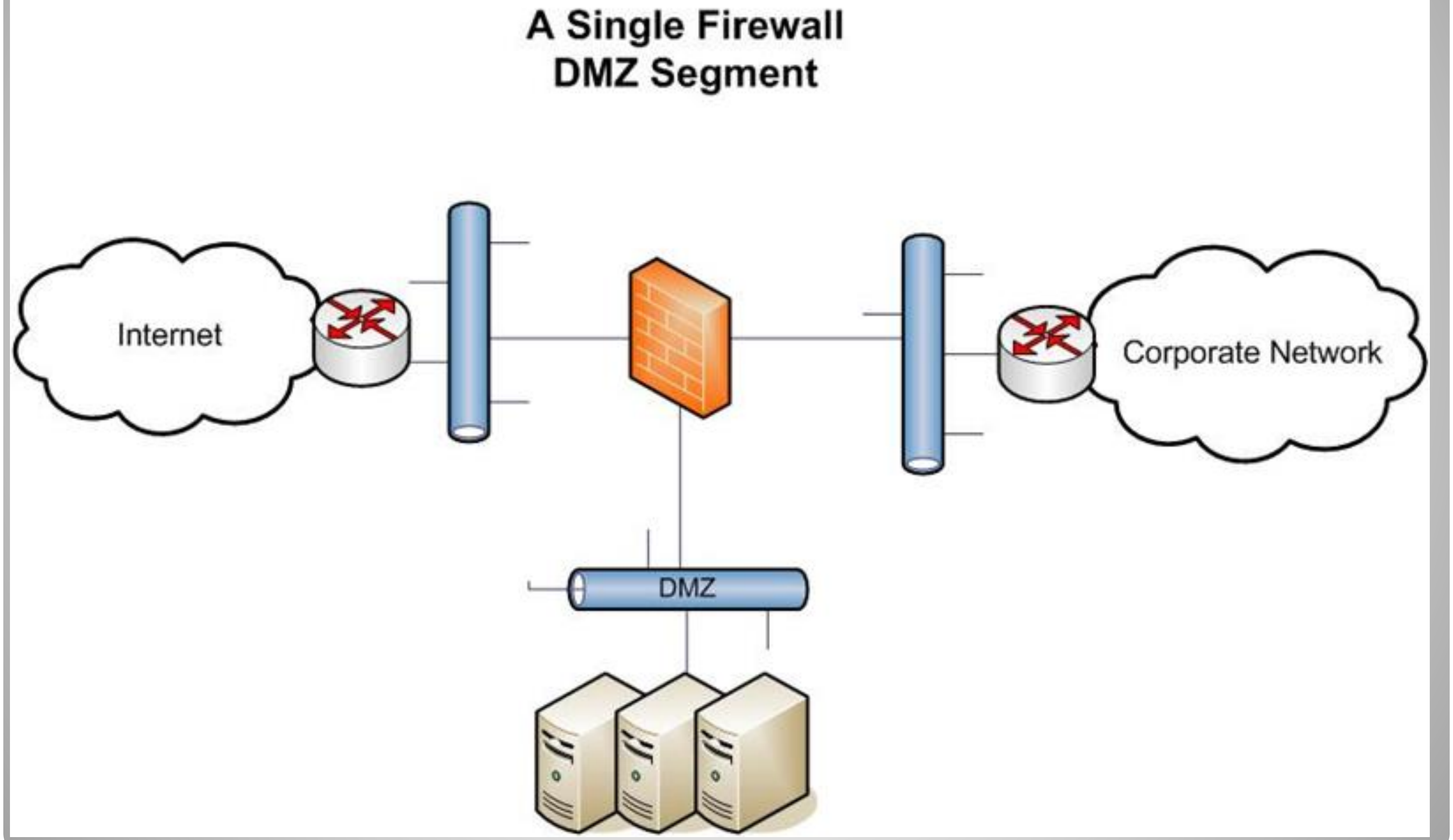
DMZ

- In computer networking, a **DMZ** (short for demilitarized zone) is a firewall configuration used to secure hosts on a network segment.
- In most DMZs, the hosts on the DMZ are connected behind a firewall which is connected to a public network like the Internet.
- Another common configuration is to have the firewall connected to an extranet, with connections to customers, vendors or business partners. DMZ’s are designed to provide access to systems without jeopardizing the internal network.

Sandwich DMZ Segment



Single Firewall DMZ Segment



Network Address Translation (NAT)

- Network Address Translation (NAT) is a technique used to modify the network address information of a host while traffic is traversing a router or firewall.
- This technique is used to hide the network information of a private network while allowing traffic to be transferred across a public network like the Internet.
- NAT was the resulting workaround solution for preserving the number of IP addresses used on the Internet.

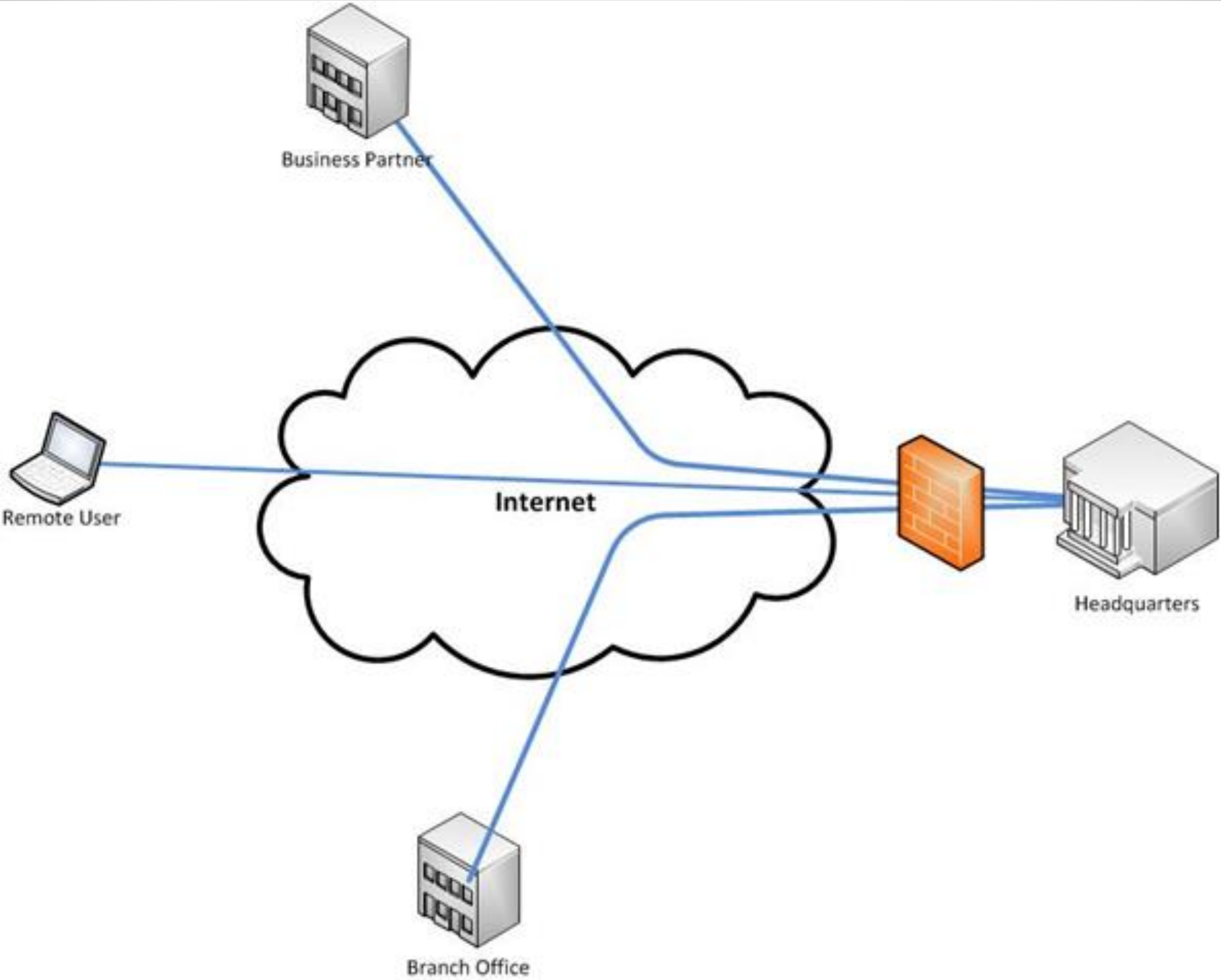
Network Address Translation (NAT)

- Static NAT – Static NAT maps an unregistered IP address on the private network to a registered IP address on the public network, using a one-to-one basis. conjunction with DMZ or extranet networks.
- Dynamic NAT – Dynamic NAT maps an unregistered IP address on the private network to a registered IP address that is selected by the routing device providing the NAT service from a pool of registered IP addresses.

VPN

- VPN (Virtual Private Network) is a technology that uses encrypted tunnels to create secure connections across public networks like the Internet.
- VPNs are commonly used by remote employees for access to the internal network, to create secure network to network connections for branch offices or business partner connections, or even to create secure host to host connections for additional security and isolation on an internal network.
- VPNs utilize encryption and authentication to provide confidentiality, integrity, and privacy protection for data.

VPN


Business Partner
Remote User
Internet
Headquarters
Branch Office

IPsec

- Internet Protocol Security (IPsec) is a standards-based protocol suite designed specifically for securing Internet Protocol (IP) communications.
  - It is also a component of IPv6, the next generation of the IP protocol. IPsec authenticates and encrypts each IP packet in an IP data stream.
- IPsec has protocols that can be used to establish mutual authentication and cryptographic keys negotiation during a session. IPsec operates at the Network Layer of the OSI model.

SSL

- One of the key VPN protocols used today is SSL / TLS, which is the main alternative to IPsec for implementing a VPN solution.
- While this protocol is widely used to secure websites, it has since been formalized in the IETF standard known as Transport Layer Security (TLS).
- The SSL/TLS protocol provides a method for secure client/server communications across a network and prevents eavesdropping and tampering with data in transit. SSL/TLS also provides endpoint authentication and communications confidentiality through the use of encryption.

Secure Shell (SSH)

- The Secure Shell (SSH) Protocol is a protocol for secure remote login and other secure network services over the network.
- SSH can be used for a number of applications across multiple platforms including UNIX, Microsoft Windows, Apple Mac and Linux.

Tunneling

- Tunneling is defined as the encapsulation of one network protocol within another.
- Tunneling can be used to route an unsupported protocol across a network, or to securely route traffic across an insecure network.
- VPN’s uses a form of tunneling when data is encapsulated in the IPsec protocol.
- Examples include PPTP and L2TP with IPsec.

DNSSEC

- ***DNS Security Extensions (DNSSEC)*** adds security provisions to DNS so that computers can verify that they have been directed to proper servers.
- DNSSEC provides authentication and integrity checking on DNS lookups ensuring that outgoing Internet traffic is always sent to the correct server.
- This removes the issues of forged DNS data, because there is no way to forge the appropriate authentication.
- This not only addresses the issue of website redirection, but also addresses some challenges associated with spam and the use of faked mail domains.

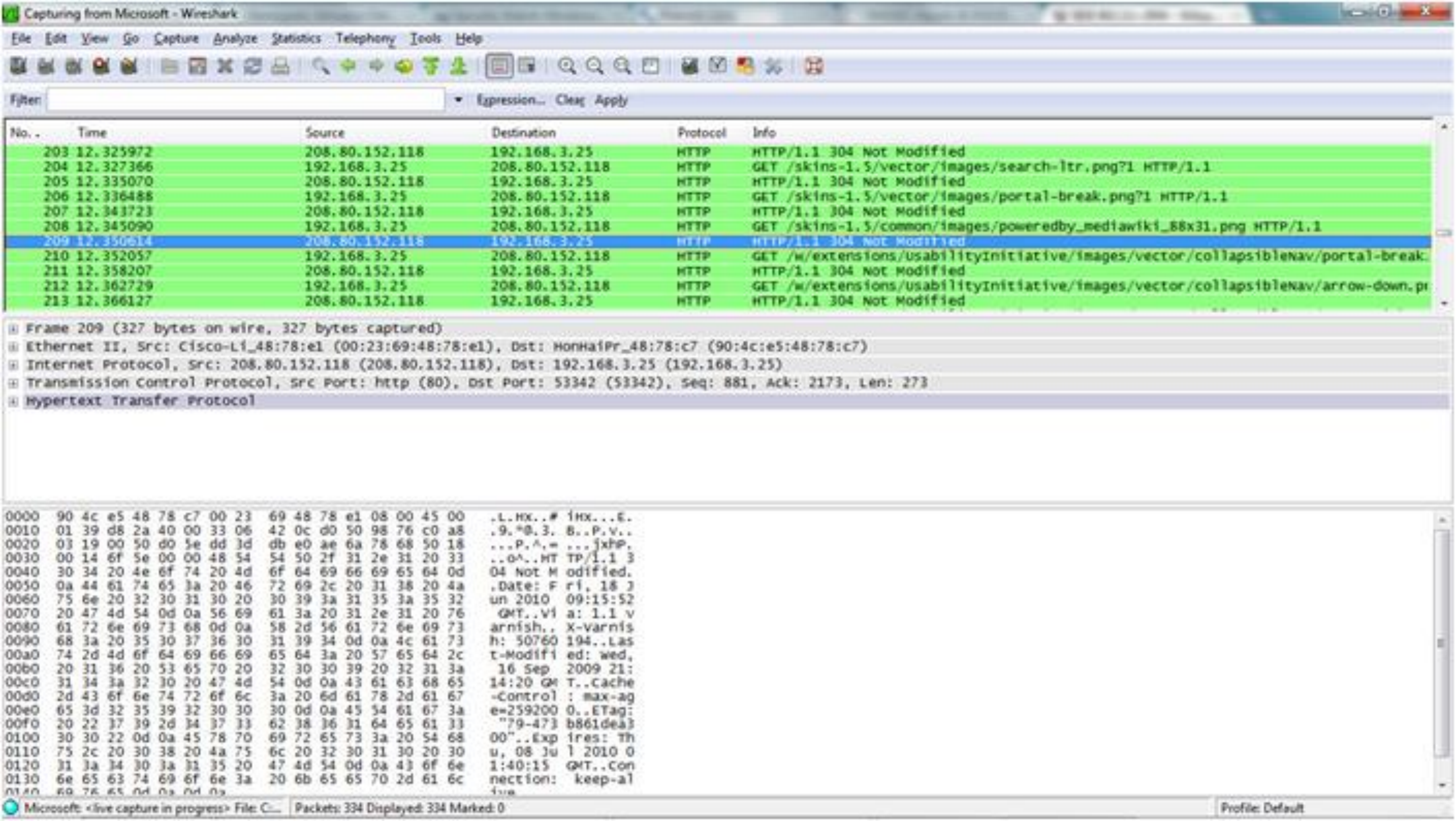
Spoofing

- The word spoof can be defined as a hoax. Protocol spoofing is the misuse of a network protocol to perpetrate a hoax on a host or a network device.
- Some common forms of protocol spoofing include:
  - ARP Spoofing
  - DNS Spoofing
  - IP Address Spoofing

Network Sniffing

- Network sniffing is a type of network analysis that is a very useful tool for network administrators responsible for maintaining networks and identifying network issues.
- It involves connecting a device to the network with the appropriate software to allow access to the details of the packets traversing the network.

Network Sniffing



```
No. -   Time        Source            Destination       Protocol  Info
    203 12.325972   208.80.152.118    192.168.3.25      HTTP      HTTP/1.1 304 Not Modified
    204 12.327366   192.168.3.25      208.80.152.118    HTTP      GET /skins-1.5/vector/images/search-ltr.png?1 HTTP/1.1
    205 12.335070   208.80.152.118    192.168.3.25      HTTP      HTTP/1.1 304 Not Modified
    206 12.336488   192.168.3.25      208.80.152.118    HTTP      GET /skins-1.5/vector/images/portal-break.png?1 HTTP/1.1
    207 12.343723   208.80.152.118    192.168.3.25      HTTP      HTTP/1.1 304 Not Modified
    208 12.345090   192.168.3.25      208.80.152.118    HTTP      GET /skins-1.5/common/images/poweredby_mediawiki_88x31.png HTTP/1.1
    209 12.350614   208.80.152.118    192.168.3.25      HTTP      HTTP/1.1 304 Not Modified
    210 12.352057   192.168.3.25      208.80.152.118    HTTP      GET /w/extensions/UsabilityInitiative/images/vector/collapsibleNav/portal-break.
    211 12.358207   208.80.152.118    192.168.3.25      HTTP      HTTP/1.1 304 Not Modified
    212 12.362729   192.168.3.25      208.80.152.118    HTTP      GET /w/extensions/UsabilityInitiative/images/vector/collapsibleNav/arrow-down.pr
    213 12.366127   208.80.152.118    192.168.3.25      HTTP      HTTP/1.1 304 Not Modified
```

```
⊞ Frame 209 (327 bytes on wire, 327 bytes captured)
⊞ Ethernet II, Src: Cisco-Li_48:78:e1 (00:23:69:48:78:e1), Dst: HonHaiPr_48:78:c7 (90:4c:e5:48:78:c7)
⊞ Internet Protocol, Src: 208.80.152.118 (208.80.152.118), Dst: 192.168.3.25 (192.168.3.25)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 53342 (53342), Seq: 881, Ack: 2173, Len: 273
⊞ Hypertext Transfer Protocol
```

```
0000  90 4c e5 48 78 c7 00 23  69 48 78 e1 08 00 45 00   .L.HX..# iHX...E.
0010  01 39 d8 2a 40 00 33 06  42 0c d0 50 98 76 c0 a8   .9.*@.3. B..P.v..
0020  03 19 00 50 d0 5e dd 3d  db e0 ae 6a 78 68 50 18   ...P.^.= ...jxhP.
0030  00 14 6f 5e 00 00 48 54  54 50 2f 31 2e 31 20 33   ..o^..HT TP/1.1 3
0040  30 34 20 4e 6f 74 20 4d  6f 64 69 66 69 65 64 0d   04 Not M odified.
0050  0a 44 61 74 65 3a 20 46  72 69 2c 20 31 38 20 4a   .Date: F ri, 18 J
0060  75 6e 20 32 30 31 30 20  30 39 3a 31 35 3a 35 32   un 2010  09:15:52
0070  20 47 4d 54 0d 0a 56 69  61 3a 20 31 2e 31 20 76    GMT..Vi a: 1.1 v
0080  61 72 6e 69 73 68 0d 0a  58 2d 56 61 72 6e 69 73   arnish.. X-Varnis
0090  68 3a 20 35 30 37 36 30  31 39 34 0d 0a 4c 61 73   h: 50760 194..Las
00a0  74 2d 4d 6f 64 69 66 69  65 64 3a 20 57 65 64 2c   t-Modifi ed: Wed,
00b0  20 31 36 20 53 65 70 20  32 30 30 39 20 32 31 3a    16 Sep  2009 21:
00c0  31 34 3a 32 30 20 47 4d  54 0d 0a 43 61 63 68 65   14:20 GM T..Cache
00d0  2d 43 6f 6e 74 72 6f 6c  3a 20 6d 61 78 2d 61 67   -Control : max-ag
00e0  65 3d 32 35 39 32 30 30  30 0d 0a 45 54 61 67 3a   e=259200 0..ETag:
00f0  20 22 37 39 2d 34 37 33  62 38 36 31 64 65 61 33    "79-473 b861dea3
0100  30 30 22 0d 0a 45 78 70  69 72 65 73 3a 20 54 68   00"..Exp ires: Th
0110  75 2c 20 30 38 20 4a 75  6c 20 32 30 31 30 20 30   u, 08 Ju l 2010 0
0120  31 3a 34 30 3a 31 35 20  47 4d 54 0d 0a 43 6f 6e   1:40:15  GMT..Con
0130  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0140  69 76 65 0d 0a 0d 0a                               ive....
```

Microsoft: <live capture in progress> File: C...

Packets: 334 Displayed: 334 Marked: 0

Common Attack Methods

- Denial-of-Service/Distributed Denial of Service (DoS/DDoS) Attacks
- IP Spoofing to Bypass Network Security
- Man in the Middle Attacks
- Back Door Attack
- DNS Poisoning
- Replay Attack
- Weak Encryption Keys
- Social Engineering

Common Attack Methods

- Password Cracking
- Dictionary Attack
- Brute Force Attack
- Software Vulnerability Attack
- Buffer Overflow Attack
- Remote Code Execution Attack
- SQL Injection Attack
- Cross Site Scripting Attack

Wireless LAN (WLAN)

- A Wireless LAN (WLAN) allows users to connect to a network while allowing them to remain mobile.
- The most basic component of the wireless network is the SSID (Service Set IDentifier), which is defined in the IEEE 802.11 standard as a name for the WLAN.

Wired Equivalency Privacy (WEP)

- The very first security capability available to WLAN users was WEP (Wired Equivalency Privacy).
- WEP rapidly fell out of favor when a flaw with the encryption mechanism was found.
- The flaw in WEP makes it relatively easy for an attacker to crack the encryption and access the wireless network, so it is generally only used if no other solution is available (WEP is better than nothing) or the WLAN is being used with older devices, or devices like PDAs or handheld games that require the use of WEP.

WPA/WPA2

- WPA (Wi-Fi Protected Access) was designed as the interim successor to WEP.
  - WPA included a new security protocol, Temporal Key Integrity Protocol (TKIP)
- WPA2 (Wi-Fi Protected Access version 2) is the standards-based version of WPA, except WPA2 implements all of the IEEE 802.11i standards.

WLAN and MAC addresses

- You can use MAC addresses to control what systems are able to connect to a WLAN through the use of MAC filters.
- By turning MAC filtering on, you can limit network access to only permitted systems by entering the MAC address information into the MAC filters.
- The table of permitted MAC addresses is maintained by the wireless access points.

Summary

- A firewall is a system that is designed to protect a computer or a computer network from network-based attacks.
- Network Access Protection (NAP) allows administrators a more powerful way to control access to network resources.
- Virtual LANs (VLANs) were developed as an alternate solution to deploying multiple routers.

Summary

- Intrusion detection systems (IDS) is a solution designed to detect unauthorized user activities, attacks, and network compromises.
- An intrusion prevention system (IPS) is very similar to an IDS, except that in addition to detecting and alerting, an IPS can also take action to prevent to breach from occurring.
- Honeypots, honey nets and padded cells are complementary technologies to IDS/IPS deployments. A honeypot is a trap for hackers.

Summary

- A DMZ is a firewall configuration used to secure hosts on a network segment.
- In most DMZs, the hosts on the DMZ are connected behind a firewall which is connected to a public network like the Internet.
- Network Address Translation (NAT) is a technique used to modify the network address information of a host while traffic is traversing a router or firewall.