COMPTIA SECURITY+
STUDY GUIDE

Exam Code SYO-401
# TABLE OF CONTENTS

## I. Network Security: An Introduction

## II. Security Network Devices and Technologies: Functions and Purposes

1.1 All-in-One Security Appliances
1.2 Anti-SPAM and Email Hygiene
1.3 Content Inspection
1.4 Firewall
  1.4.1 Application Filtering Firewall
  1.4.2 Dual-Homed and Multi-Homed Firewalls
  1.4.3 Next Generation Firewall
  1.4.4 Packet Filtering Firewall
  1.4.5 Stateful Firewall
  1.4.6 Web Application Firewalls
1.5 Internet Content Filters
1.6 Load Balancer
1.7 Malware Inspection
1.8 Network Intrusion Detection Systems (NIDS)
1.9 Network Intrusion Prevention System (NIPS)
1.10 Network Protocol Analyzers (aka Packet Sniffers)
1.11 Proxies
1.12 Reverse Proxies
1.13 Routers
1.14 Screened Subnet
1.15 Switches
1.16 Uniform Resource Locator (URL) Filtering
1.17 Virtual Private Network Concentrators (VPN)
1.18 Web Security Gateways
III. Network Administration Principles: Application and Implementation
   1.1 802.1x
   1.2 Access Control Lists (ACL)
   1.3 Firewall Rules
   1.4 Flood Guard
   1.5 Implicit Deny
   1.6 Loop Protection
   1.7 Network Bridging
   1.8 Port Security
   1.9 Rule-Based Security Management
   1.10 Secure Router Configuration
   1.11 Security Event Managers (SEM)
   1.12 VLAN Management

IV. Design Elements and Compounds: Identification and Distinction
   1.1 Cloud computing
   1.2 Demilitarized Zone (DMZ)
   1.3 Network Access Control (NAC)
   1.4 Network Address Translation (NAT)
   1.5 Remote Access
   1.6 Remote Access Servers
   1.7 Subnetting
   1.8 Telephony
   1.9 Virtualization
   1.10 Virtual Local Area Network (VLAN)
V. Common Protocols: Implementation and Usage

1.1 Commonly Used Default Network Ports
1.2 Domain Name System (DNS)
1.3 File Transfer Protocol Secure (FTPS)
1.4 Hypertext Transfer Protocol Secure (HTTPS)
1.5 Internet Control Message Protocol (ICMP)
1.6 Internet Protocol Security (IPSec)
1.7 IPSec Key Management Functions
1.8 IPv4 and IPv6
1.9 Secure Copy (SCP)
1.10 Secure FTP
1.11 Secure Shell (SSH)
1.12 Secure Socket Layer (SSL)
1.13 Simple Network Management Protocol (SNMP)
1.14 Transmission Control Protocol / Internet Protocol (TCP/IP)
1.15 Transport Layer Security (TLS)

VI. Key Terms Review List

VII. Additional Resources
A secure network is essential to any organization’s business operations. An unsecured network is an open invitation to all kinds of cyber attacks, much like leaving the front door unlocked at night.

Each network is unique. Architecturally, a network is defined by physical dimensions such as equipment and connections, while logically it is defined by the applications, industries and services it provides. This means that network infrastructures are complex in structure, making the establishment of appropriate security controls a demanding process. However, this is not an excuse to compromise business performance for security. It is the job of network security professionals is to provide seamless integration of security controls to the business process with minimal impact.

This can be a challenging task. A network consists of interconnected devices, connections, protocols, and interfaces each with its individual set of concerns. Network security professionals must recognize, address and communicate these when applying security and network protection solutions against data loss and theft, trespasses and outages.
1.1 **All-in-one Security Appliances** – these appliances license different modules of the most popular and critical security controls that organizations commonly use separately at the Internet gateway. These are then combined to offer an attractive all-in-one security solution, preferably at a lower cost.

All-in-one security appliances feature security solutions such as:

- IPS
- IDS
- Web filtering
- Email filtering
- Malware scanning
- VPN support
- Combined firewalls
- Others

1.2 **Anti-SPAM and Email Hygiene** – are part of data loss prevention mechanism that organizations implement for regulations compliance and best practices
application. Messaging systems also offer secure email programs to reroute and encrypt messages according to predefined conditions.

Anti-SPAM and email hygiene measures seek to protect against threats such as:

- SPAM
- Scams
- Phishing attacks
- Malicious code attachments
- Other unsolicited email messages

Email filtering solutions come in both hardware and software versions. These ensure delivery of legitimate emails and denial of unsolicited ones. Email filtering strategies include:

- Black listing (Blockage)
- White listing (Approval)
- Heuristic analysis
- Scanning of malware
- Content filters
- Bayesian analysis
- Scoring of reputations
- Addressing of harvesting prevention
- DNS reverse lookup (Sender ID, SPF)
- Cloud leverage to identify zero hour/zero day spam attacks

Email filtering solutions are best placed nearest the sources of messages that need to be filtered. Ex. Internet-based email should be filtered at the gateway.

Note: The unsolicited email problem now extends to other technological divides such as phone-based text message and VoIP systems spamming.

1.3 **Content Inspection** – this type of filter evaluates displayed web page content for irrelevant, sensitive, and objectionable data to a business’ operations. Content inspection is commonly used as data loss prevention control as well as to deny access to specific content.

1.4 **Firewalls** – Most commonly the first line of defense against Internet-based attacks, firewalls are an integral component of network security strategies. Firewalls
are a software package or appliance that segregates public and private networks in a logical manner. It supervises transmitted traffic between the two in both **ingress** (network inbound) and **egress** (network outbound) directions. Firewalls use network rule sets and traffic filtering mechanisms to recognize traffic that should be allowed or denied access to a network. It can also be used to extend protection to internal sub-networks under the main network scope.

Previously, firewalls were developed according to their functions, platform support and placement and positioning within a network. Modern firewalls today are capable of network traffic deep packet analysis through a combination of application filtering and use of intrusion prevention technology into a single unit. These are often used not only on network perimeters but also on internal networks, workstations, and servers in response to menacing progress observed in threats.

**1.4.1 Application Filtering Firewall** – application filtering assess port usage, service requests (DNS, FTP, web, etc.), and input/output commands. Second generation firewalls filtered network traffic content by operating through 1-7 layers of the OSI model. Application filtering firewalls are an integral part of Next Generation firewalls and are used to stop peer-to-peer network traffic.

**Note:** Application filtering firewalls are used in a process called **baselining**. This means that application firewalls are applied in a proxy or reverse proxy configuration where they require pre-defined rule sets to ‘learn’ what is regarded as ‘normal’ application ‘behavior’.

**1.4.2 Dual-Homed and Multi-Homed Firewalls** - As their names suggest, dual-homed and multi-homed firewalls differ in the number of network interfaces they use. Dual-home firewalls use separate interfaces for the external and internal networks while multi-homed firewalls contain multiple interfaces for both connections. Multiple interfaces are typically used to define demilitarized zone (DMZ) segments. These allow Internet facing services (such as email, serves, and DNS) to function without exposing an internal network to risk.
1.4.3 Next Generation Firewall (NGF) – This latest generation of firewalls seek to merge several of the most widely-used network perimeter security controls into one powerful system. This practice often results in the coupling of application filters with an intrusion prevention system (IPS). Some providers include URL content inspection as well as identification of malware. Vendor’s offerings in this area are often varied.

Note: Many security analysts and providers use the term Next Generation Firewalls due to its popularity.

1.4.4 Packet Filtering Firewalls—packet filtering determines access by checking packet data against information established in pre-defined network rule sets. These were used by first generation firewalls as security controls in network traffic monitoring. Packet filtering firewalls function at the first three layers of the OSI model: Physical, Data-Link and Network.

Rule sets or access control lists (ACL) are generally configured to evaluate packets through analysis of packet headers for source and destination addresses, ports (TCP/UDP), protocols or a combination of these. Based on these assessments, packet filtering firewalls will make a decision whether to allow or deny packets access.

Packet filtering firewalls are scalable, useful for restricting traffic flow and usually perform well. However, they are also vulnerable to attacks, particularly those that exploit potential loopholes in applications. Packet filtering firewalls are also incapable of recognizing packets that bear falsified or spoofed network addresses.

Note: Routers also use packet filtering technology.

1.4.5 Stateful Firewall – Considered as third generation firewalls, stateful firewalls limit traffic flow between hosts by using stateful packet inspection. These operate at the OSI model’s one through four layers.

Stateful firewalls record communication sessions by keeping a state table which is checked for existing connections when packets are received. Once it is confirmed that the packet data doesn’t have any relative connections to the state table, the
packet will be checked against the firewall’s access control list to see if a new connection should be permitted.

1.4.6 Web Application Firewalls – fulfill a special function in web-based application protection, particularly those accessed by Internet users. Web filtering firewalls are used for supervising web traffic directed at a web server. Web application firewalls scan for:

- Cross-site scripting
- SQL injection attacks
- Vandalism
- Other malicious codes

Aside from scanning for threats, web application firewalls also validate user input, sanitize output and learn how an application should operate. Organizations that process Internet-based credit card transactions and need to comply with PCI standards use web application firewalls or submit a vulnerability assessment of web application environment. The Open Web Application Security Project (OWASP) is the authority that certifies whether web application firewalls meet or go beyond requirements.

Note: Web application firewalls differ from network firewalls because they fulfill a specific role and provide countermeasures that network firewalls don’t.

1.5 Internet Content Filters – because no restrictions exist regarding the content posted on the Internet, individuals and organizations alike set their own policies to manage content delivery using Internet content filters. These filters restrict different types of information by scanning for questionable or malicious:

- Keywords
- Hostnames
- URLs
- Malware

Web security gateways, all-in-one security appliances and host-based solutions address risks linked with accessing Internet hosted content.

1.6 Load Balancer – load balancers disperse a huge load across multiple systems, devices and networks to avoid overload on a single unit. It comes in both hardware
and software forms, with different options for services. Another kind of load balancing is known as **round robin DNS**, which does not need dedicated hardware or software. Round robin DNS instead designates multiple IP addresses to one specified fully qualified domain name (FQDN).

Load balancers are often required in business continuity plans to act as a compensating control in event of a load balancer resource attack or outage resulting in failure. This way, services can maintain availability and function. In addition, load balancers provide:

- Redundancy in event of system failure
- Control against **DoS** attacks against resources connected to the load balancer

---

**Note:** Load balancing solutions can be improved with clustering or application of redundancy measures.

---

1.7 **Malware Inspection** - also known as **malware scanning engines**, these filter web content and files being downloaded/uploaded to the Internet for malicious software. Pairing malware inspection at the Internet gateway with host-based malware scanning systems is a strongly recommended security measure.

1.8 **Network Intrusion Detection Systems (NIDS)** – Some network attack sequences leave patterns that turn into scanning engine ‘signatures’. NIDS determine suspicious network activity by comparing these signatures against observed traffic to detect potential attacks in the future. NIDS determines:

- Denial of Service attacks (DoS)
- Invalid connection requests
- Malware behavior
- Port scans
- Others

Once these are identified, NIDS sends alerts to administrators for investigation.

1.9 **Network Intrusion Prevention System (NIPS)** – almost identical to NIDS in terms of duties but serves in a more active role. Where NIDS alerts administrators, NIPS takes action immediately without need for human interaction. NIPS enacts
predefined action upon confirmation of certain attacks. Immediate measures may include connection termination, activating firewall blocks, etc.

1.10 Network Protocol Analyzers (aka Packet Sniffers) – protocol analyzers configure a computer’s network interface to a more permissive state, also known as promiscuous mode configuration. This allows network stack processing of packets intended for other units which are usually filtered by NIC. Network protocol analyzers acts as a viewfinder into network traffic protocol and patterns. By doing so, administrators are able to observe private conservations, transactions of sensitive nature, and other activities between workstations for troubleshooting or investigatory reasons. It follows that use of packet sniffers and network protocol analyzers offer opportunities for abuse like eavesdropping, espionage, and interception of critical protocol transactions.

1.11 Proxies – proxies assess connection requests according to administrative rule sets and may judiciously filter traffic that corresponds to criteria. A proxy acts as a mediator between client and server, concealing internal machines behind anonymity and improving network performance by caching resources which are commonly requested.

Note: Proxy placement may either be centralized at a gateway server or positioned at individual workstations.

1.12 Reverse Proxy – these process requests originating from external sources and forwards them to dedicated systems for handling. This is the reason why reverse proxies are often deployed on an Internet facing segment serving web pages or Internet-based apps. Using reverse proxies adds a layer of protection by keeping internal networks hidden and then acting as their representative to outside requests.

1.13 Routers – are defined as packet-switching devices capable of enhanced traffic handling. Routers communicate in OSI layer 3 protocol packets. Multi-protocol routers act as a translator between different network protocols. Routers also forward packets according to source and destination IP addresses, and may offer forms of basic security through use of ACLs.

Sometimes used together with firewalls in cases of Internet-facing connections, some routers are also designed with firewall capabilities. Routers perform network address translation (NAT) to hide system addresses behind the router. This is to guard against systems that establish connections using the router’s external interface. In
these cases the router replies to the connections with unique addresses. Traffic is forwarded to their proper destinations using router tables.

Routers are not meant to replace firewalls, which are designed and dedicated to security. Therefore strict guidelines should be enforced when a router is added to a network to address exposure issues. Unlike internal network routers or physically connected routers, wireless routers/wireless access points/Internet facing routers are more exposed.

| Note: Switches join local network segments while routers set up connectivity between networks (public, private, or separate). |

1.14 **Screened Subnet** – screened subnets are defined by a configuration where external traffic passes through a router first before going through a firewall. Traffic must pass through an additional firewall if it is destined for hosts within an internal network.

| Note: DMZ can be configured as screened subnets. |

1.15 **Switches** – switches restrict network traffic by exclusively delivering traffic to the switch a host is connected to. To accomplish this, switches keep a table which map device MAC addresses to switchport numbers.

Switches function at OSI protocol layers one to three devices that connect network segments and individual computers. They come in a variety of sizes and shape from compact four-port Ethernet units to 48-port Gigabit units.

Network switches are able to establish **virtual LANs** (VLANs) for improved corporate network administration and security. VLAN is the logical grouping of systems based on security, resource, or business reasons rather than physical location. Modern multilayer switches are capable of:

- Inspecting packets
- Ranking traffic priority
- Performing as Routers
- Serving as Load Balancers
- Adding Quality of Service (QoS) to network traffic
However, switches are susceptible to several kinds of attacks such as:

- Denial of Service (DoS)
- ARP spoofing
- MAC spoofing / flooding

To properly guard against such threats, switches and VLANs alike need to be configured correctly.

Note: Hubs broadcast traffic on all ports while switches deliver exclusively.

1.16 **Uniform Resource Locator (URL) Filtering** – URL filters check hyperlinks and URL for specific commands, keywords, and malicious code. This type of filtering is usually utilized by web and email scanning engines. URL filters use reputation services and usually access the suspicious content in a sandboxed environment to check if resource request is questionable in nature. For tiny URLs, a plug-in is necessary for URL filtering.

Note: Use of tiny or short URLs is a technique often used by cyber attackers.

1.17 **Virtual Private Network (VPN) Concentrators** – offer remote users a secure way for Internet-based connection into an organization’s internal network. VPN concentrators are used where a network requires support for massive incoming VPN connections.

VPN concentrators are offered by vendors in various feature set model by model. These can be used to establish connections between remote offices and organizations. VPN concentrators come in both IPSec and SSL configuration (few providers offer support for both). Superior VPN concentrators are able to encrypt entire sessions and wipe them out once they are concluded. Other VPN concentrators integrate firewall technologies to permit or deny access according to health checks of connecting systems like security patches and antivirus programs. VPN concentrators may offer remediation options for discovered issues as well.
1.18 Web security gateways – are used to filter inbound and outbound web traffic, suspicious codes, malicious content, and usage of application to guard against Internet-based attacks.

In cases of outdated web browsers and neglected security updates, web security gateways serve as an essential feature in defense-in-depth strategy residing at an organization’s Internet Gateway. Web security gateways are generally available as appliances which offer several modules and licensing options.

Note: Application firewalls are frequently deployed in reverse proxy configurations.

Using a web security gateway offers the following benefits:

- Filtering of web traffic (malicious content and code)
- Detect and take action on applications
- Avert information leakage
- Impose email security controls

In addition, web security gateways protect networks against drive-by downloads and Internet based zero-day or zero-hour threats. These are downloads or program installations that take place on a user’s system without their approval.
1.1 **802.1x** – 802.1x originated from the discovery of vulnerabilities in Wired Equivalency Privacy (WEP). Since then, the Institute of Electrical and Electronics Engineers (IEEE) port authentication standard 802.1x has been established to control network access and deny rogue system infiltration.

802.1x is commonly used with:

- RADIUS systems
- TACACS+
- Network Access Control (NAC)
- Network Access Protection (NAP)
- Others

802.1x wraps Extensible Authentication Protocol (EAP) in Ethernet frames before sending it over both wired and wireless network. The EAP method offers a variety of authentication procedures such as token IDs, passwords and digital certificates once network connections are made.
However, 802.1x doesn’t use the Point-to-Point Tunneling protocol that EAP traditionally requires. In fact, 802.1x is fully capable of creating encrypted tunnels where credentials can pass between devices and the authentication server.

Devices requesting connection to the network, also known as supplicants, are first sent to an authenticator to be fitted with credentials (e.g., user ID/password set). The credentials are forwarded by the authenticator to the authentication server to be validated for access permission or denial.

1.2 Access Control Lists (ACL) – ACLs constitute basic security checklists that are used in assessing permitted access and actions. An access control list dictates which actions a user may execute when modifying, accessing or creating a specific object such as applications and services. These are defined by administrators as basic permission schemes to specify how a subject or group of subjects may interact with a protected data or resource.

ACLs are derived by leveraging information defined in:

- Rule-based (action) access models
- Role-based (job function) models
- Mandatory access (security labels)
- Discretionary access (group membership)

Several technologies from file permissions to firewalls are deployed to preserve ACL and avert illegal access to protected resources.

1.3 Firewall Rules – firewall rules should be set to ‘deny all’ unless purposely allowed. This can be configured by setting the last rule in the set to either deny-any or block. Firewalls rules in this context are specified to deny traffic that failed to meet pre-defined criteria in the rule set. By following the deny-all concept, firewall rules achieve the most secure design. It also presents an effective point of discussion in cases where business requirement validation necessitates a new rule or modification in the existing rule set.

1.4 Flood Guard – flood guards serve as preventive control against denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks. Flood guards are available either as standalone devices or as firewall components. It is capable of monitoring network traffic to identify DoS attacks in progress generated through packet flooding. Examples of DoS and DDoS attacks are:
- Ping flood
- MAC flood
- UDP flood
- ICMP flood
- SYN flood

These attacks seek to disrupt or take down network services by overwhelming the target network with requests. When a flood guard detects a DoS attack it drops the packets or applies filters rule sets on switches and routers.

1.5 Implicit Deny – the ‘implicit deny’ security stance treats everything not given specific and selective permission as suspicious. Network boundaries that follow an implicit deny concept only allows specific IP addresses and/or service ports while blocking all others. On the contrary, a network implicitly allows traffic when it operates on an open computing environment to which any connection may be established. The “implicit deny” concept generally applies to information security principles.

Note: An ‘explicit deny’ security stance blocks traffic from particular addresses and towards specific ports.

1.6 Loop Protection – Looping can be taken advantage of by attackers to initiate DoS attacks because of its repetitive nature. When transmissions loop, they needlessly consume bandwidth and disrupt network services. Loop protection consists of enabling STP (spanning tree protocol) on the network switches. The STP records available network paths and then enacts pre-defined decisions regarding active and standby routes. STP then closes down routes deemed vulnerable to looping. Bridges also support STP for loop protection.

1.7 Network Bridging – network bridging is purposefully used in some cases but introduces several risks if it occurs unintentionally. Some of these are:

- Operational problems
- Security risks
- Possible looping
- Degradation of network performance

One common way of network bridging is when a laptop simultaneously connects to both a wired and a wireless network, creating a passage for traffic to move from one network to the other.
Network bridging can be prevented using two methods:

1. **Network separation** – physically separates networks to avoid bridging.
2. **Ethernet port configuration** – configuring Ethernet ports to automatically disconnect once bridging is recognized on a host machine.

VLANs can be specified in switches to establish firewall routers and logically isolated networks to prevent network bridging.

**1.8 Port Security** – port security can be divided into two categories based on the OSI model.

<table>
<thead>
<tr>
<th>Physical Port Security</th>
<th>Network Port Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can be unplugged</td>
<td>Unused ports are closed</td>
</tr>
<tr>
<td>Can be enabled with MAC address recognition</td>
<td>Monitored by firewalls</td>
</tr>
<tr>
<td>Covers physical objects such as Ethernet jacks and USB ports</td>
<td>Controls port usage with TCP and UDP protocols</td>
</tr>
<tr>
<td>Can be blocked on a local system using:</td>
<td>A significant number of most commonly used ports are frequently left open (0-1023 of 65,535 ports available)</td>
</tr>
<tr>
<td>- Physical plugs</td>
<td></td>
</tr>
<tr>
<td>- BIOS settings</td>
<td></td>
</tr>
<tr>
<td>- Device control settings</td>
<td></td>
</tr>
<tr>
<td>Device products generally allow for exclusive use of permitted devices</td>
<td></td>
</tr>
</tbody>
</table>

Network ports are usually scanned by attackers to identify available ports and the services allowed on them. Security professionals should ensure that only ports crucial to a business’ operations are left open, with strict rules sets to govern traffic. The amount of traffic should also match the port’s requirements.

**Note:** A technique called *port knocking* considers all ports closed until a connection request is made to a particular port. In the event of a connection request, firewall rules are immediately changed once the connecting system supplies an encrypted packet or sends the correct sequence on the connection string.

**1.9 Rule-Based Security Management** – this type of security management uses rule sets to define the scope of what kind of activities should be allowed on a network. If the requested activity fails to match the pre-defined rules for the network it is
implicitly denied. This entails that the last rule in the set should default to a deny action or decision.

Rule-based security management designs are supported by systems that utilize rule-driven controls or filters security policy monitoring and implementation on communications and other IT-related activities. Examples of systems that use a rule-based security model are:

- Firewalls
- IPS
- Proxies
- Email filters
- Web filters
- IDS

1.10 Secure Router Configuration – while existing designs of routers incorporate firewall technologies such as port-blocking, routers are not replacements for security devices and are susceptible to threats. Routers need to be securely configured before they are positioned on a network. Some of the steps taken to securely configure routers are:

- Supplying a unique name to a device
- Defining IP addresses as well as ranges
- Assign a password (encrypted if possible)
- Disable unneeded ports
- Backup the configuration
- Block ICMP redirect traffic

The last step mentioned above, blocking the ICMP redirect traffic, acts as a preventive security control against attacks such as ICMP floods and the ping of death that leverage ICMP protocol for malicious purposes.

Note: Setting up wireless routers and wireless access points for secure router configuration require additional steps.

1.11 Security Event Managers (SEM) – also known as Security Information event managers (SIEM), these are key components that store, analyze and mine data
from several logs on multiple systems across a network. SEMs records a local copy of received logs and are able to provide a forensically-sound archive in the event of original log loss. Additionally, SEMs are able to send alerts based on its identification of similar events in multiple logs. SEMs can also provide an interface for efficient scouring of log data.

1.12 VLAN Management – A VLAN management model necessitates configuring specific deny functions or removing creation of unjustifiable routes to deny access to network resources or other VLANs. Some switches come with an integrated VLAN management solution that enables administrators to view and control their VLAN environments.
1.1 Cloud computing – is an environment hosted by an Internet-based server/network of servers or a private network cloud. In cloud computing, all activities such as applications, data, and processing take place in the cloud environment.

Companies that rely on cloud computing and cloud-based resources should take effective means to implement stable and secure Internet connection. Multiple Internet connections, failover, and load-balancing should also be considered when using cloud services.

Cloud computing is a powerful tool that carries its own benefits and risks. Companies should weigh these carefully before using cloud computing for their operations.
While cloud computing reduces cost and need for additional resources, it carries significant security risks that companies need to be prepared for.

**1.2 Demilitarized Zone (DMZ)** – a DMZ is a portion of a network kept separate from the protected internal network for security purposes. The DMZ sets up a physically separate buffer zone meant for public-facing private company servers like web and FTP. DMZs provide a compromise between public services and private servers operation without full exposure to threats and high-risk environments.
1.3 Network Access Control (NAC) – a frequently used networking security solution, NAC seeks to validate existing functional security controls on a system requesting connection before it is allowed access to the network. NAC checks for and defines security controls such as:

- Firewalls
- Operating system
- Virus protection
- Service packs
- 802.1x
- Other network security enforcement procedures

NAC is useful for implementing system health requirements upon network access. Systems that are recognized to be unhealthy are either administratively denied access or redirected to an issue resolution site relevant to its security issues. For example, a system with outdated anti-malware protection may be forwarded to an Intranet Web site to mitigate its security issues. Once the security risk has been addressed, users are usually allowed to reconnect.

1.4 Network Address Translation (NAT) – NAT is a one-to-many or one-to-one mapping of public-to-private IP address spaces. Using NAT lessens the need for multiple public IP addresses through an ISP. This is accomplished by establishing an address pool mapping (defined by administrators) of the internal network and bundling the connections as a single source without unnecessary exposure of internal endpoints on the Internet. The repackaged connections are typically centralized at a router device or gateway service.

NAT enables a company to share a single public external connection among multiple internal computers.

The Internet Assigned Numbers Authority (IANA) reserves the routable IP addresses range below for private Intranet use according to the RFC 1918.

<table>
<thead>
<tr>
<th>IP Address Range</th>
<th>Number of Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0 – 10.255.255.255</td>
<td>16,777,216</td>
</tr>
<tr>
<td>172.16.0.0 – 172.31.255.255</td>
<td>1,048,576</td>
</tr>
<tr>
<td>192.168.0.0</td>
<td>65,536</td>
</tr>
</tbody>
</table>
1.5 **Remote Access** – offers convenient remote connection to networks. Remote access solutions can be applied in a variety of ways such as:

- Remote desktop or terminal services (Windows)
- Dial-up
- VPN
- Others

Remote access servers that allow access to internal network resources should be protected irrespective of the remote access solution used. It is recommended that publicly accessible RAS systems be audited and monitored for security purposes.

1.6 **Remote Access Servers** – these systems provide connection to a server for authentication and access grant to internal network resources. Connections usually are made through modem from the Internet.

RAS implement policies on connecting systems regulating requirements and operation of sessions within particular parameters. These include:

- Time boundaries
  - Availability
  - Session length
  - Timeouts
- Implementation of particular authentication mechanism
- Directing network traffic to travel along specified route

RAS servers are frequently positioned in DMZ, with firewall devices next in line along the route.

1.7 **Subnetting** – is the logical division of a network into classes of smaller networks, or subnets. Subnetting prevents Ethernet collisions and conflicts in address assignment.

A subnet is a compartmentalized collection of designated layer 3 IP addresses. These addresses are compatible with gateway devices, servers, network endpoints, and end-user units among other intermediary devices.
Subnets are classified into Class A, B and C segments according to their progressively smaller sizes. These can be individually protected by firewalls as well as given various access rights and network permissions based on their job functions.

1.8 Telephony – supplies long haul connections for communication purposes by transmitting and translating analog voice data into digital voice formats. The term telephony is synonymous with telecommunications and embraces the general use of communication devices such as:

- Wired/wireless phones
- Voicemail systems
- Digital computers

1.9 Virtualization – virtualization is available in both hardware and software. It is used to establish multiple virtual operating systems (guests) on a host (usually a single physical device). The logical systems residing inside a single physical system are usually independent of their host and run in their logically segment memory space.

Virtualization is useful for:

- Data center designing
- New technologies testing
- Business continuity procedures creation
- System consolidation

Both guest systems and the physical system should have security measures implemented such as firewalls and virus protection.


1.10 Virtual Local Area Network (VLAN) – VLAN is logically arranging a single physical switched network into segments of multiple logical networks. A single company may use multiple VLAN broadcast domains to quarantine cross-contaminations and manage departments. Each VLAN broadcast domain may be individually protected according to the needs of the network. LAN segments may be dispersed across a single campus or throughout various regions in the country.
1.1 Commonly Used Default Network Ports – Port usage is assigned by the Internet Assigned Numbers Authority (IANA) to applications and processes. These are divided into three ranges:

- Well known – 0-1023 range
- Registered – 1024-41951 range
- Private/dynamic – 41952-65535 range

Port usage is frequently checked when utilizing technology in environments. As a basic security measure, default ports should be changed and well-known ports communicate to questionable sources through a firewall.
List of default network ports:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Transfer (FTP)</td>
<td>21</td>
</tr>
<tr>
<td>Secure FTP / SSH FTP (SFTP)</td>
<td>22</td>
</tr>
<tr>
<td>FTP Secure (FTPS)</td>
<td>989 (data), 990 (command)</td>
</tr>
<tr>
<td>Trivial File Transfer Protocol (TFTP)</td>
<td>69</td>
</tr>
<tr>
<td>Telnet</td>
<td>23</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol (HTTP)</td>
<td>80</td>
</tr>
<tr>
<td>Hypertext Transfer Protocol Secure (HTTPS)</td>
<td>443</td>
</tr>
<tr>
<td>Secure Copy (SCP)</td>
<td>22</td>
</tr>
<tr>
<td>Secure Shell (SSH)</td>
<td>22</td>
</tr>
<tr>
<td>Simple Mail Transport Protocol (SMTP)</td>
<td>25</td>
</tr>
<tr>
<td>Simple Network Management Protocol (SNMP)</td>
<td>160, 161, 162</td>
</tr>
<tr>
<td>NetBIOS</td>
<td>137 (name service), 138 (datagram), 139 (session)</td>
</tr>
</tbody>
</table>

1.2 Domain Name System (DNS) – DNS is a key network component that preserves hosts records and resolves host names to IP addresses for system access through name or IP address. A company’s name servers need auditing and assessment to avoid security risks facing DNS such as:

- Exposure of organizational footprint including server roles/versions and network devices
- Domain reversal inconsistencies
- Zone transfer
- RFC non-compliance
- Outdated versions

1.3 File Transfer Protocol Secure (FTPS) – FTPS incorporates additional support to FTP for TLS and SSL so that connecting systems can securely transfer files. FTPS operates in two modes:
### Explicit Mode
- FTPS-aware customers negotiate with the FTP server to determine the proper encryption method to use
- In cases where clients lack FTPS, the FTPS server chooses one of these actions:
  a. Drop connection
  b. Allow connection but with limited functionality
  c. Allow connection with no restrictions

### Implicit Mode
- All clients must be FTPS-aware
- Upon connection, clients must establish encrypted session with FTPS server

---

Note: Secure FTP and SSH File Transfer Protocol are not the same as FTPS.

### 1.4 Hypertext Transfer Protocol Secure (HTTPS)
HTTPS is a standard TCP mechanism for content and message exchange between web servers and browsers. HTTPS is responsible for most of visually presentable content on the Internet. Use of HTTP offers unlimited flexibility and delivery of multimedia, file formats, and documents but is also susceptible to malicious activities and attacks.

HTTP is technically defined as an application layer OSI layer 7 transport method. It operates in plaintext which sends transmissions in unencrypted format. To guard against potential eavesdroppers, TLS and SSL are often used to secure HTTP especially when positioned between endpoints of secured conversations.

HTTPS connections operate below application layers for HTTP messages encryption before being transmitted. This is also applicable to incoming message decryption upon arrival. Web browsers generally integrate HTTPS for page request encryption and decryption across TCP port 443 instead of port 80 (usually used with HTTP).

Note: HTTPS is not the same as secure HTTP (S-HTTP, RFC 2660). The latter is an alternative though commonly used for web transaction encryption.

### 1.5 Internet Control Message Protocol (ICMP)
ICMP is part of the Internet Protocol (IP) suite and used in error message transmission (not data). ICMP is utilized by...
traceroute, pings and other similar tools. Routers can block ICMP traffic delivery to avoid network attacks such as ICMP flooding and ping of death.

1.6 Internet Protocol Security (IPSec) – IPSec is an OSI layer 3 network level cryptographic framework that provides authentication header (AH) and encapsulating security payload (ESP) services. Using AH and ESP together enables secure communication and data integrity through the following steps:

IPSec functions in two modes of operation:

<table>
<thead>
<tr>
<th>IPSec Operation Modes</th>
<th>Function</th>
<th>Application</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport Mode</td>
<td>Only encrypts packet payload (Note: Plaintext Telnet sessions can travel between workstation to router via IPSec)</td>
<td>Endpoints connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ex. Host-to-host Host-to-gateway</td>
</tr>
<tr>
<td>Tunnel Mode</td>
<td>Serves like a proxy to accommodate hidden hosts Encrypts entire packet including the header</td>
<td>Used between gateways in network topology</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ex. Secure connectivity between branch office-headquarters, house-workplace, etc.</td>
</tr>
</tbody>
</table>
1.7 IPSec Key Management Functions – The Internet security association and key management protocol (ISAKMP) establishes key management functionality for IPSec. Key functions include authentication, distribution and generation of cryptographic keys for secure communications. ISAKMP also integrates mechanisms for negotiation, establishment, modification, and deletion of security associations (SAs) including respective attributes. Through ISAKMP, cryptographic Internet Key Exchange (IKE) keys and SAs can be dispersed in a scalable and standard method. ISAKMP also provides procedures for:

- Peer authentication
- Creation, generation, and management of keys or SAs
- Neutralization of well-known network attacks

1.8 IPv4 and IPv6 – both IPv4 and IPv6 are essential computer networking protocols but differ from each other in several respects. $2^{128}$, or approximately $3.4 \times 10^{38}$ addresses, or more than $7.9 \times 10^{28}$ times as many as IPv4.

<table>
<thead>
<tr>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Most widely used protocol</td>
<td>Created to succeed IPv4</td>
</tr>
<tr>
<td>IPv4 addresses use 32-bit value</td>
<td>IPv6 addresses use 128-bit</td>
</tr>
<tr>
<td>(typically displayed in dotted decimal form ex. 192.153.5.3)</td>
<td>Comprised of an estimated $3.4 \times 10^{38}$ addresses (more than $7.9 \times 10^{28}$ times as many compared to IPv4)</td>
</tr>
<tr>
<td>Comprised of 2x32 or more than 4.2 billion unique addresses</td>
<td></td>
</tr>
<tr>
<td>Feared to running out of addresses</td>
<td></td>
</tr>
</tbody>
</table>

Network address translation (NAT) addressed IPv4 exhaustion concerns but IPv6 remains relevant.

Note: IPv6 requires IPSec support.
1.9 Secure Copy (SCP) – SCP is a protocol for transferring files through a SSH session using RCP commands on a Unix system. Unlike FTP, SCP retains file permissions and timestamps through inclusion with the transferred files themselves, thereby ensuring data confidentiality during transit.

Note: SCP sessions are not susceptible to packet sniffers.

1.10 Secure FTP – also known as SSH FTP (SFTP) and FTP Secure (FTPS). Both supply mechanisms for secure file transfer but vary in method.

FTPS – uses SSL or TLS for traffic flow encryption

SFTP – uses SSH to tunnel an FTP session to a SFTP server

SFTP clients must transact with a SFTP client or run a command line. SFTP servers will not work with standard FTP clients and vice versa.

1.11 Secure Shell (SSH) – SSH was traditionally designed to secure remote administrative login and shell. SSH establishes secure activities between networked devices such as logins, channels, and transfers. SSH prevents malicious third party attacks such as eavesdropping, connection tampering, and interception.

Because Telnet, FTP and NFS are vulnerable to attacks due to transmission of details in cleartext (ex. login credentials), SSH supplies the need for cryptography to ensure network privacy. SSH2 uses public key cryptography as well as traditional username/password logins for authentication.

Note: SSH uses port 22 for operation.

1.12 Secure Socket Layer (SSL) – SSL is an OSI layer 4 transport layer encryption protocol used for securing end-to-end tunnels that HTTP and application traffic use to pass through. SSL sessions are ‘stateful’ because connection states are kept from initiation to connection teardown.

Note: TLS rendered SSL, SSLv2, SSLv3 versions obsolete.
1.13 Simple Network Management Protocol (SNMP) – SNMP collects network events and statistics from network-attached devices using SNMP agents. SNMP can configure devices (up to a certain degree); provide relevant information to network performance and alert administrations regarding issues. SNMP agents monitor services such as WINS and DHCP. Activated agents also monitor devices such as hubs, printers, servers and routers.

SNMP is available in 3 versions with their respective functions and abilities.

- **SNMP Versions 1 and 2** – transmits in clear text, sets default community strings to read/write.
- **SNMP Version 3** – provides additional confidentiality and integrity by incorporating packet encryption to transmitted data.

Note: SNMP should be disabled on devices that do not require it. Default community strings preferably should be changed once SNMP is installed.

1.13 Transmission Control Protocol / Internet Protocol (TCP/IP) – TCP/IP are networking components considered part of TCP/IP protocol suites.

1.14

<table>
<thead>
<tr>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>- Commonly used by Internet applications, email, file transfers, etc.</td>
</tr>
<tr>
<td>- Supplies a stable data stream between programs from different systems</td>
</tr>
<tr>
<td>- Able to request package resending if they fail to arrive or corrupt ones are received</td>
</tr>
</tbody>
</table>
### IP

- Addresses hosts and route packets from source to destination over networks
- Host-assigned IP addresses can be subnetted into multiple networks which IP protocol can route over
- Works with TCP to establish data integrity

**Note:** TCP and IP are melded into one term (TCP/IP) because they are frequently used together.

---

**1.15 Transport Layer Security** – TLS is preceded by the SSLv3 protocol, which it phased out. TLS follows the same Internet Engineering Task Force (IETF) standards track RFC 5246 originally based on early SSL specification. TLS is not backward-compatible with its predecessor SSL but creates cryptographically-secure endpoint (ex. host-to-host) connectivity that can guard against attacks like tampering, message forgery, and eavesdropping. Both parties of a conversation can be mutually authenticated using TLS thanks to its bidirectional authentication mode.
<table>
<thead>
<tr>
<th>Phases</th>
<th>Protocol Layers</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Algorithm support through negotiating with peers</td>
<td>1. TLS Record protocol – encapsulates information for secure exchange and operates at the lowest level</td>
</tr>
<tr>
<td>2. Key exchange and authentication of endpoints</td>
<td>2. TLS Handshake protocol – uses a complex protocol exchange involving parameter and properties definition to establish secure client-server connectivity</td>
</tr>
<tr>
<td>3. Authentication of messages and symmetric cipher encryption</td>
<td></td>
</tr>
</tbody>
</table>
VI. KEY TERMS REVIEW LIST

- Asymmetric Encryption
- Authentication
- Authentication Factors /Two factor
- Backdoors
- Block Ciphers
- Botnet
- Certificate Authority
- Certificate Revocation List
- Chain of Custody
- CIA
- Ciphers
- Cryptography
- Denial of Service (DOS)
- Device Encryption
- Digital Certificates
- Discretionary Access Control
- Distributed Denial of Service (DDOS)
- DNS Poisoning
- Evil Twin
- Flood Guards
- Honeypot
- Hot Site/ Cold Site / Warm Site
- Job Rotation
- Kerberos
- Key Escrow
- Least Privilege
- Logic Bombs
- Looping/SPT
- Mandatory Access Control
- Mandatory Vacations
- Mantrap
- Mutual Authentication
- NAC - Network Access Control
- NAT - Network Address Translation
- Non-Repudiation
- Phishing
- PKI
- Positive pressurization
- RAID and Types
- Registration Authority
- Remote Wipe /Sanitation
- Rogue Access Points
- Role based Access Control
- RootKits
- Rule based Access Control
- Separation of Duties
- Skimming
- Smart Card
- Social Engineering
- SPAM
- SPIM
- Stream
- Symmetric Encryption
- Trojans
- UPS
- Virus
- Vishing
- VOIP/SIP and RTP
- War Dialing
- War driving/War Chalking
- Whaling
- White Box/Black Box