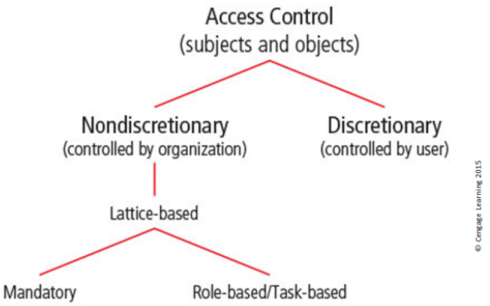
6-1 Access Control

- **Access Control** is the method by which systems determine whether and how to admit a user into a trusted area of the organization.
    - Information systems, Restricted areas (computer rooms) and physical location
    - Access control is achieved through a combination of policies, programs and technologies
    - Focussed on the permissions or privileges that a subject(user or system) has on an object(resource), including if/when and from where a subject may access an object and especially how the subject may use that object.
- **Discretionary Access Controls (DACs)**
    - Provide the ability to share resources in a peer-to-peer configuration that allows users to control and possibly provide access to information or resources at their disposal.
    - Users can allow general, unrestricted access or they can allow specific people or groups of people to access these resources.
- **Non-Discretionary Access Controls (NDACs)**
    - Managed by a central authority in the organization.
    - **Lattice-based access control(LBAC)**
        - Users are assigned a matric of authorizations for particular areas of access.
        - Authorization may vary between levels depending on the classification of authorizations that users possess for each group of information or resources
        - **Access Control Lists (ACLs) and Capabilities** tables specify the level of access each subject has to each object.
        - **Role-based Access Controls (RBACs)** and **Task-based Access Controls (TBACs)**
            - Tied to a person's duties and responsibilities
        - **Mandatory Access Controls (MACs)** form a lattice-based, non-discretionary access controls that use data classification schemes.
            - They give users and data owners limited control over access to information resources.
            - In a data classification scheme, each collection of information is rated and all users are rated to specify the level of information required.
        - **Attribute-based access controls (ABACs)**
            - Subject Attributes
                - Attributes of a subject such as name, date of birth, home address, training record and job function that combines to form a unique identity
                - ABACs uses one of these attributes to regulate access to a particular set of data.
                - Newer approach.
- Access Control Mechanisms
    - **Identification**
        - I am a user of the system
        - Uses a unique ID only tied to that entity that labels them to be known by the system
    - **Authentication**
        - I can prove Im a user of the system



        - The process of validating an unauthenticated entity's purported identity.
            - Something you know
                - password, pin, passphrase…
            - Something you have
                - Dumb card, smart card, U2F Yubikey
                - Synchronous tokens
                    - Synchronized with a server
                    - Uses a time-based database to generate a number that must be entered during the login phase
                - Asynchronous tokens
                    - Uses a challenge/response system
            - Something you are
                - Uses individual characteristics like fingerprints, palm prints, hand topography, retina and iris scans.
    - **Authorization**
        - Here's what I can do with the system
        - Matches an authenticated entity to a list of information assets and corresponding access levels (Access Control List or Matrix)
    - **Accountability**
        - You can track and monitor my use of the system
        - Ensures that all actions on a system can be attributed to an authenticated identity.
            - Accomplished by a series of system logs, database journals and the auditing of these records.
- Biometric Access Control
    - Relies on recognition
    - Fingerprints, palm print, iris scan, facial recognition, retina scan
    - Crossover Error Rate (CER)
        - The point at which false rejects and false accept rates intersect
- **Access Control Architecture Models**
    - **TCSEC's Trusted Computing Base**
        - Trusted Computer System Evaluation Criteria (older DoD standard)
        - Reference Monitor
            - The piece of the system that manages access controls.
            - Sys-ads must be able to audit or review the reference
        - Covert Channels
            - Can be used to exfiltrate sensitive data without being detected.
            - Storage Channels
                - Used in steganography and in embedding of data in TCP or IP header fields.
            - Timing Channels
                - Used in a system that places a long pause between packets to signify a 1 and a short pause between packets to signify a 0.
        - Part of the Rainbow Series

    - Replaced in 2005 with **The Common Criteria**
- **ITSEC**
    - Information Technology System Evaluation Criteria
    - An international set of criteria for evaluating computer systems similar to TCSEC
    - Targets of Evaluation are compared to detailed security function specifications, resulting in an assessment of systems functionality and comprehensive penetration testing.
    - Replaced by **the Common Criteria**
- **The Common Criteria**
    - *The Common Criteria for Information Technology Security Evaluation.*
    - ISO/IEC 15408 standard for computer security certification.
    - CC and CEM are the technical bases for CCRA, an international agreement which ensures that products can be evaluated to determine their particular security properties
    - CC Terminology
        - **Target of Evaluation (ToE)**
        - **Protection Profile (PP)**
        - **Security Target (ST)**
        - **Security Functional Requirements (SFRs)**
        - **Evaluation Assurance Levels**
            - **EAL1**
                - Functionally Tested: Confidence in operation against non serious threats
            - **EAL2**
                - Structurally Tested: More confidence required but comparable with good business practices
            - **EAL3**
                - Methodically Tested and Checked: Moderate level of security assurance
            - **EAL4**
                - Methodically Designed, Tested and Reviewed: Rigorous level of security assurance but still economically feasible without specialized development
            - **EAL5**
                - Semi Formally Designed and Tested: Certification requires specialized development above standard commercial products
            - **EAL6**
                - Semi Formally Verified Design and Tested: Specially designed security ToE
            - **EAL7**
                - Formally Verified Design and Tested: Developed for extremely high-risk situations or for high-value systems.
- **Bell-LaPadula Confidentiality Model**
    - State Machine Reference Model
        - A model of an automated system that is able to manipulate its state or status over time

        - The intent of any state machine model is to devise a conceptual approach in which the system being modeled can always be in a known secure condition (provably secure)
    - BLP ensures the confidentiality of the modeled system by using MACs, data classification, and security clearances.
    - Only allows access to those with clearance equal to and above the classification
    - **Access Modes**
        - **Simple Security** (the read property)
            - Prohibits a subject of lower clearance from reading an object of higher clearance but allows a subject with a higher clearance level to read an object at a lower level.
        - **The Star(*) Property** (the write property)
            - Prohibits a high-level subject from sending messages to a lower-level object.
            - BLP uses access permission matrices and a security lattice for access control
- **Biba Integrity Model**
    - Similar to BLP
    - Simple Integrity (read) property
        - Permits a subject to have read access to an object only if the subject's security level is lower than or equal to the level of the object
    - Integrity * Property (Write)
        - Permits a subject to have write access to an object only if the subject's security level is equal to or higher than that of the object.
    - Biba model ensures that no information from a subject can be passed on to an object in a higher security level
- **Clark-Wilson Integrity Model**
    - Uses change control (not integrity levels)
        - No changes by unauthorized subjects
        - No unauthorized changes by unauthorized subjects
        - The maintenance of internal and external consistency.
            - Internal consistency means that the system does what it is expected to do every time, without exception
            - External consistency means that the data in the system is consistent with similar data in the outside world.
    - The intent is to provide an environment where security can be proven through the use of separated activities, each of which is provably secure
    - Controls
        - Subject authentication and identification
        - Access to objects by means of well-formed transactions
        - Execution by subjects on a restricted set of programs
    - Elements
        - Constrained data item (CDI): Data item with protected integrity
        - Unconstrained data item: Data not controlled by Clark-Wilson; non validated input or any output
        - Integrity Verification Procedure (IVP): a Procedure that scans data and confirms its integrity.
        - Transformation Procedure (TP): a Procedure that only allows changes to a constrained data item.

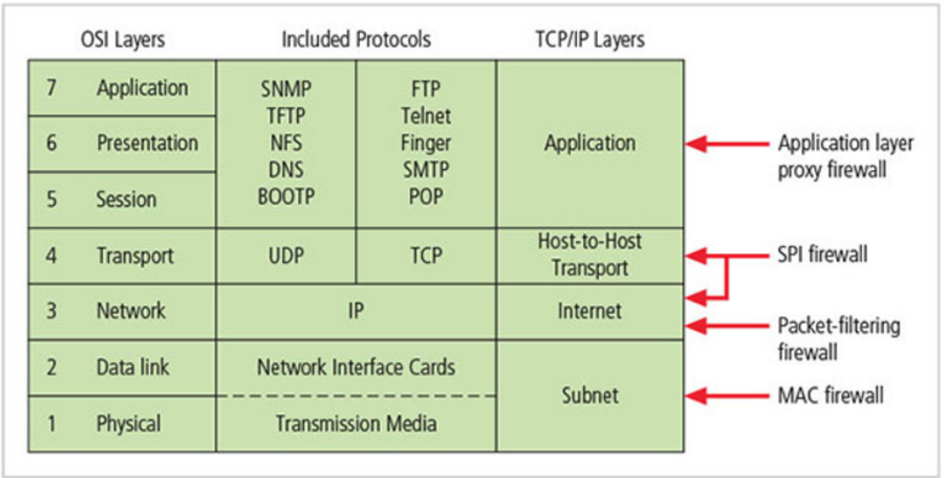
        - All subjects and objects are labeled with TPs.
            - TPs operate as the intermediate layer between subjects and objects.
            - Each data item has a set of access operations that can be performed on it.
            - Each subject is assigned a set of access operations that it can perform.
    - **Graham-Denning Access Control Model**
        - Has three parts:
            - Set of subjects
                - Subjects are made with a process and a domain
                    - The domain is the set of constraints that control how subjects may access objects.
            - Set of objects
            - Set of rights
                - Governes how subjects may manipulate the passive objects
        - 8 Primitive Protection rights
            - Create Object
            - Create Subject
            - Delete Object
            - Delete Subject
            - Read Access Right
            - Grant Access Right
            - Delete access right
            - Transfer access right.
    - **Harrison-Ruzzo-Ullman Model**
        - Defines a method to allow changes to access rights and the addition and removal of subjects and objects
            - BLP does not allow
            - Systems change and their protective states need to change.
        - Built on an Access Control Matrix
            - Create Subject/Create object
            - Enter right X into
            - Delete right X from
            - Destroy subject/destroy object
    - **Brewer-Nash Model (Chinese Wall)**
        - Designed to prevent a conflict of interest between two parties.
        - Requires users to select one of two conflicting sets of data, after which they cannot access the conflicting data.

6-2 Firewalls

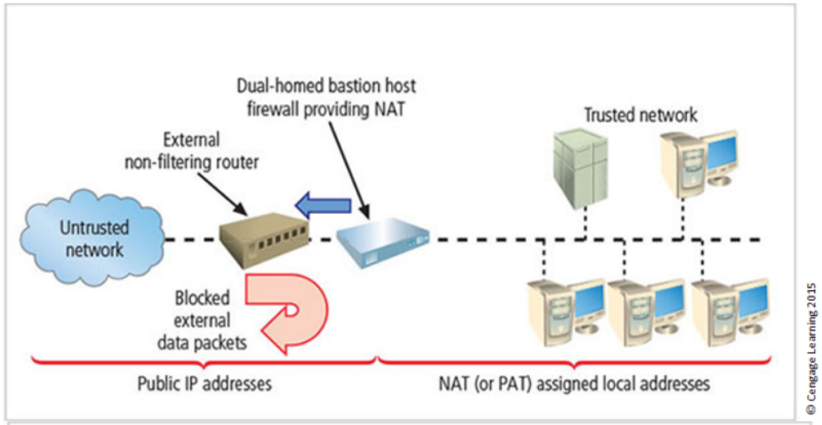
- Prevents specific types of information from moving between two different levels of networks.
- **Firewall Processing Modes**
    - **Packet-Filtering**
        - Examines the header information of data packets that come into a network

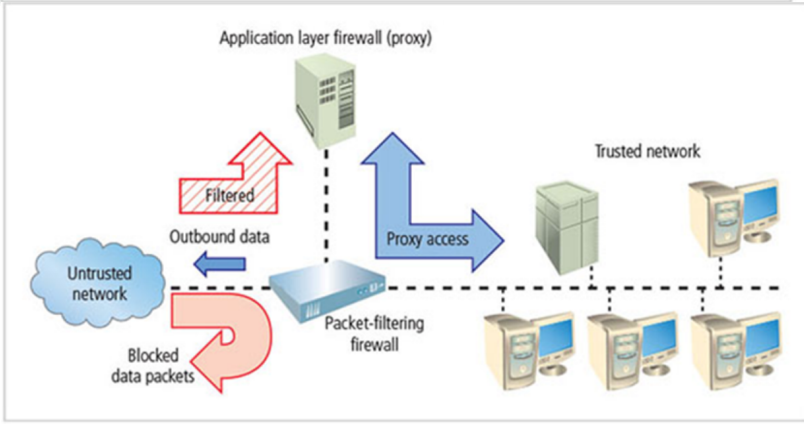
- Typically functions at the IP layer and determines to drop or forward a packet
- Restrictions available
  - IP source and IP destination
  - Direction (inbound or outbound)
  - Protocol
  - TCP or UDP source and destination port requests
- Static
  - Determine that packet filtering rules be developed and installed with the firewall
- Dynamic
  - Can react to an emergent event and update or create rules to deal with that event
- Stateful (SPI)
  - Uses a state table
    - Tracks the state and context of each packet in the conversation by recording which station sent what packet and when.

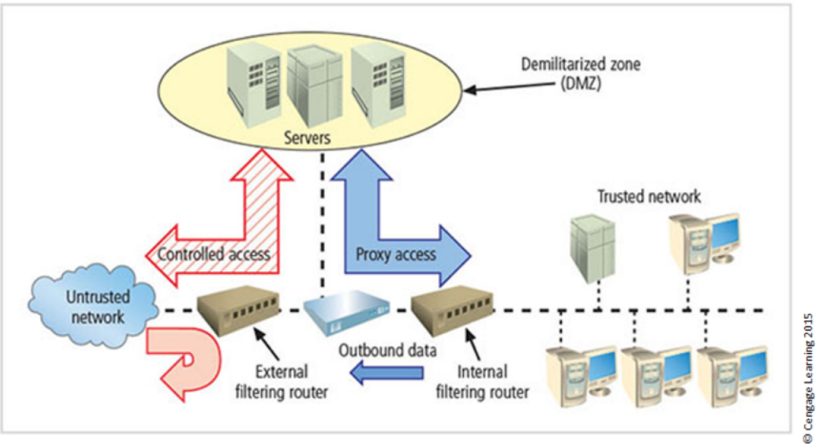
- **Application Layer Proxy**
  - Also called a proxy server or reverse proxy
  - Can be placed in a DMZ to serve web page to users
  - Cannot be easily configured to protect against attacks and only has a few uses
    - FTP, Telnet, HTTP, SMTP, SNMP...
- **Media Access Control layer**
  - Make filtering decisions based on the specific host computer's identity as represented by its MAC address
  - Operates at Datalink Layer
- **Hybrid**
  - Combine the elements of other types of firewalls.
    - A layer of packet filtering, application layer proxy, and media access control
  - May consist of two separate firewall devices
    - Connected and work in tandem
  - Unified Threat Management (UTM)
    - Categorized by their ability to perform:
      - SPI firewall,
      - Network intrusion detection and prevention,
      - content filter,
      - Spam filter,
      - Malware scanner and filter.
    - Primary source of failure if it goes down
  - Next Generation Firewall (NGFW)



        - May only be a difference in scope
        - UTM does a good job at a lot of things, NGFW does a good job at a handful of things.
- Firewall Architectures
    - **Single Bastion Hosts**
        - A single firewall that provides protection behind the organizations router.
        - Can be implemented as a packet filtering firewall
        - Sometimes referred as a **Sacrificial Host**
            - Stands alone on the network perimeter.
        - NAT
            - A method of mapping valid, external IP addresses to special ranges of non-routable internal private IP addresses.
            - PAT (Port Forwarding)
                - NAT performs a one-to-one mapping
                - PAT performs a one-to-many mapping
    - **Screened Host Architecture**
        - Combines the packet-filtering router with a separate, dedicated firewall, which retrieves information on behalf of other system users and often caches copies. (proxy server, website)
        - Allows router to prescreen packets to minimize the traffic/load on internal proxy
        - Requires an external attack to compromise two separate systems before the attack can access internal data
    - **Screened Subnet Architecture (with DMZ)**
        - Dominant architecture used today
        - Consists of two or more internal firewalls behind packet-filtering router, with each protecting a trusted network
            - Connections from outside network are routed through external filtering router
            - Connections from outside network are routed into and out of routing firewall to separate the network segment known as DMZ (DMZ creates extranets)
            - Connections into trusted internal network are allowed only from DMZ bastion host servers.
        - Performs two functions
            - Protects DMZ systems and information from outside threats.
            - Protects the internal networks by limiting how external connections can gain access to internal systems







- **Configuring Firewall**
  - Rule set 1:
    - Responses to internal requests are allowed
  - Rule Set 2:
    - The firewall device is never accessible directly from the public network
  - Rule Set 3
    - All traffic from the trusted network is allowed out
  - Rule Set 4
    - Rule set for SMTP traffic
  - Rule Set 5:
    - All ICMP data should be denied
  - Rule Set 6:
    - Telnet (terminal emulation) access should be blocked to all internal servers from the public networks.
  - Rule Set 7
    - When Web services are offered outside the firewall, HTTP and HTTPS traffic should be blocked from the internal networks via the use of some form of proxy access or DMZ
    - Direct all HTTP requests to the proxy server and configure the firewall/router only to allow the proxy server to access the internal Web server.
      - This requires the DNS entries be configured as if the proxy server were the Web server
  - Rule Set 8
    - The clean up rule
      - Deny any traffic not allowed by policy by default.
- Content filter
  - Like if you wanted to block content you don't want through like porn or Fox News...

Port Number	Protocol
7	Echo
20	File Transfer [Default Data] (FTP)
21	File Transfer [Control] (FTP)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name System (DNS)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol version 3 (POP3)
161	Simple Network Management Protocol (SNMP)

External Filtering Firewall Inbound Interface Rule Set

Rule #	Source address	Source port	Destination address	Destination port	Action
1	10.10.10.0	Any	Any	Any	Deny
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny

4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	Any	Any	10.10.10.0	>1023	Allow
7	Any	Any	10.10.10.6	25	Allow
8	Any	Any	10.10.10.0	7	Deny
9	Any	Any	10.10.10.0	23	Deny
10	Any	Any	10.10.10.4	80	Allow
11	Any	Any	Any	Any	

External Filtering Firewall Outbound Interface Rule Set

Rule #	Source address	Source port	Destination address	Destination port	Action
1	10.10.10.12	Any	10.10.10.0	Any	Allow
2	Any	Any	10.10.10.1	Any	Deny
3	Any	Any	10.10.10.2	Any	Deny
4	10.10.10.1	Any	Any	Any	Deny
5	10.10.10.2	Any	Any	Any	Deny
6	10.10.10.0	Any	Any	Any	Allow

7	Any	Any	Any	Any	Deny

Internal Filtering Firewall Inbound Interface Rule Set

Rule #	Source address	Source port	Destination address	Destination port	Action
1	Any	Any	10.10.10.3	Any	Deny
2	Any	Any	10.10.10.7	Any	Deny
3	10.10.10.3	Any	Any	Any	Deny
4	10.10.10.7	Any	Any	Any	Deny
5	Any	Any	10.10.10.0	>1023	Allow
7	10.10.10.5	Any	10.10.10.8	Any	Allow
8	Any	Any	Any	Any	Deny

Internal Filtering Firewall Outbound Interface Rule Set

Rule #	Source address	Source port	Destination address	Destination port	Action
1	Any	Any	10.10.10.3	Any	Deny
2	Any	Any	192.168.2.1	Any	Deny
3	10.10.10.3	Any	Any	Any	Deny

4	192.168.2.1	Any	Any	Any	Deny
5	Any	Any	192.168.2.0	>1023	Allow
6	192.168.2.0	Any	Any	Any	Allow
7	Any	Any	Any	Any	Deny

6-3 Protecting Remote Connections

- **Remote Access**
  - **Dial-up Based**
    - Systems that authenticate user credentials for those trying to access an organization's network via dial-up
    - **RADIUS (Remote Authentication Dial-In User Service)**
      - Remote worker dials NAS and submits username and password
      - NAS passes username and password to a central RADIUS server
      - RADIUS server approves or rejects request and provides access authorization
      - NAS provides access to authorized remote worker
    - **Diameter**
      - A derivative of RADIUS
    - **TACAS (Terminal Access Controller Access Control System)**
      - Validates user's credentials at centralized server (like RADIUS)
      - Based on client/server configuration.
  - **Kerberos**
    - Uses symmetric key encryption to validate an individual user to various network resources.
    - Keeps a database containing the private keys of clients and servers.
    - Generates temporary session keys.
    - 3 interacting services
      - Authentication Server (AS)
      - Key Distribution Center (KDC)
      - Kerberos Ticket-Granting Service (TGS)
    - Based on the following principles

        - The KDC knows the secret keys of all clients and servers on the network
        - The KDC initially exchanges information with the client and server by using these secret keys.
        - Kerberos authenticates a client to a requested service on a server through TGS and by issuing tem session keys for communications between the client and KDC, the server and KDC, and the client and server
        - Communications then take place between the client and server using these temporary session keys.
    - **SESAME (Secure European System for Applications in a Multivendor Environment)**
        - User is authenticated to an authentication server and receives a token
        - The token is then presented to a privilege attribute server instead of a ticket-granting service as proof identity to gain a Privilege Attribute Certificate (PAC)
            - Similar to kerberos ticket but PAC conforms to ECMA and ISO/ITU-T
        - Ability to delegate responsibility for allowing access.
        - More auditing features.
        - More scalable encryption systems
- **VPN**
    - A means of private network communications on a public network
    - **Encapsulation** of incoming and outgoing data in which the native protocol of the client is embedded within the frames of a protocol that can be routed over the public network and be usable by the server network environment
    - **Encryption** of incoming and outgoing data to keep the data contents private while in transit over the public network, but usable by the client and server computers on both ends of the network.
    - **Authentication** for the remote computer and maybe the remote user as well.
    - Transport Mode:
        - The data within an IP packet is encrypted but the header information is not.
        - Eavesdroppers can still identify the destination system
    - Tunnel Mode
        - Establishes two perimeter tunnel servers to encrypt all traffic that will traverse an unsecured network.
        - The entire packet is encrypted and added as the data portion of a packet addressed from one tunneling service to another.
        - Receiving server decrypts the packet and sends it to the final address

Ch.6 Review Questions:

1. What is the typical relationship among the untrusted network, the firewall, and the trusted network?
    a. The firewall usually separates the two networks at the firewall, which filters what comes in from the untrusted network.
2. What is the relationship between a TCP packet and UDP packet? Will any specific transaction usually involve both types of packets?
    a. A TCP connection is connection-oriented while a UDP packet is connectionless. Typically these two are not used together in a single transaction.
3. How is an application layer proxy firewall different from a packet-filtering firewall?
    a. A packet filtering firewall only filters traffic based on IP packets, while an application firewall takes into consideration the state of the application and what it is doing.
4. How is static filtering different from dynamic filtering of packets? Which is perceived to offer improved security?
    a. Static filtering is set manually by the administrator/tech and does not change. Dynamic filtering is meant to change based on preset rules to handle different types of events. Dynamic is perceived to work better towards improving security.
5. What is stateful inspection? How is state information maintained during a network connection or transaction?
    a. SPI keeps track of the state of a packet over-time by storing data in a state-table (who sent the packet, when, etc)
6. Explain the conceptual approach that should guide the creation of firewall rule sets.
    a. All traffic is blocked by default, only allowing what you need
7. What special function does a cache server perform? Why is this useful for larger organizations?
    a. A cache server allows you to store content in memory from services/pages that you access often, such as a webpageDescribe how the various types of firewalls interact with network traffic at various levels of the OSI model.
8. What is a hybrid firewall?
    a. A hybrid firewall combines elements from the other firewalls: packet-filtering, proxy-server, etc. May also have more than one firewall device at different locations on the network that communicate with each other.
9. Describe Unified Threat Management. Why might it be a better approach than single-point solutions that perform the same functions? How does UTM differ from Next Generation Firewalls?
    a. UTM describes a firewall categorized by its ability to perform the work of multiple firewall devices: SPI, NIDPS, content filters, spam filter, malware filter etc.
    b. The throughput is the main difference between the two besides marketing/labeling being the biggest difference.
10. What is a Next Generation Firewall (NextGen or NGFW)?
    a. A hybrid firewall that combines the functionality of other types of firewalls with other security functions. A security appliance that delivers UTM management capabilities in a single device.
11. What is the primary value of a firewall?
    a. To deny/filter traffic between untrusted and trusted networks.

12. What is Port Address Translation (PAT) and how does it work?
    a. A variation of NAT. PAT takes routable external IP addresses and maps them to internal IP addresses. PAT has a one to many mapping where NAT has a one-to-one mapping. PAT assigns a unique port number to each external IP address and maps the address+port combination to the internal IP address.
13. How do screened host architectures for firewalls differ from screened subnet firewall architectures? Which offers more security for the information assets that remain on the trusted network?
    a. Screened Host uses a dedicated firewall and NAT to protect the internal network while Screened Subnet architecture creates a DMZ which is more secure
14. What is a sacrificial host? What is a bastion host?
    a. A sacrificial host is the sole defender and stands alone on the network perimeter. The two terms are synonymous with each other. A bastion host receives screened network traffic
15. What is a DMZ? Is this really an appropriate name for the technology, considering the function this type of subnet performs?
    a. A DMZ, also called a Demilitarized Zone, is a middle-ground area in your network that is public facing giving access to people from the public internet. A DMZ essentially gives trusted access to an untrusted network and is usually done by using a set of firewall rules. The name is appropriate for the function of this subnet operation. You can think of physical DMZ like the border between North and South Korea. You would only put services that need to be there to serve your clients like a web server and you would not keep important services here such as access to your company database of users and passwords. This helps maximize the value you give to your users/clients and minimizes the risk of giving access to your sensitive features needed to run your organization.
16. What questions must be addressed when selecting a firewall for a specific organization?
    a. 1. Which type of firewall technology offers the right balance between protection and cost for the needs of the organization?
    b. 2. What features are included in the base price? What features are available at extra cost? Are all cost factors known?
    c. 3. How easy is it to set up and configure the firewall? Does the organization have staff on hand that are trained to configure the firewall, or would the hiring of additional employees (or contractors or managed service providers) be required?
    d. 4. Can the firewall adapt to the growing network in the target organization?
17. What is RADIUS? What advantage does it have over TACACS?
    a. RADIUS-RemoteAuthentication-Dial-in-User-Service. RADIUS checks/authenticates anyone trying to access the network via dial-up.
    b. TACACS was developed by Cisco and pretty much only works with their devices. This is changing however, but the vendor-agnostic nature of RADIUS is a good reason to choose it.
18. What is a content filter? Where is it placed in the network to gain the best result for the organization?
    a. A software program or hardware/software appliance that allows administrators to restrict content that comes into or leaves a network.
19. What is a VPN? Why is it becoming more widely used?

a. A VPN is a Virtual Private Network that allows you to have a secure private network across/on an open network. People need to work remotely as a demand/opportunity brought on by the internet. This means we need secure communications on the untrusted network.