Security Technology: Firewalls and VPNs

* Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization that is information system, restricted areas such as computer rooms, and the entire physical location.
* Mandatory access controls use data classification schemes; they give users and data owner’s limited control over access to information resources.
* Lattice based access control users are assigned a matrix of authorizations for particular areas of access.
  + The column of attributes is referred to access control list
  + The row: capabilities table.
* Nondiscretionary controls are a strictly enforced version of MACs that are managed by a central authority in the organization and can be based on an individual’s role or set or tasks.
* Discretionary access controls are implemented at the discretion or option of the data user. The ability to share resources in a peer-to-peer config allows users to control and provide access to info or resources at their disposal.
* In general all access control approaches rely on:
  + Identification
  + Authentication
  + Authorization
  + Accountability
* Identification is a mechanism whereby an unverified entity (supplicant) seeks access to a resource proposes a label by which they are known in the system.
* Authentication is the process of validating a supplicant’s purported identity. Three widely used factors are:
  + Something a supplicant knows
    - Password, pass phrase
  + Something a supplicant has
    - Dumb cards such as user ID
    - Smart card that has a computer chip
    - Token, a card or key fob with a computer chip and a LCD that shows a computer-generated number used to support remote login authentication.
  + Something a supplicant is
    - Fingerprints, palm prints, retain scan
* Authorization is the matching of an authenticated entity to a list of information assets and corresponding access levels.
  + Authorization for each authenticated user
  + Authorization for members of a group
  + Authorization across multiple systems
* Accountability
  + Ensures that all actions authorized or unauthorized can be attributed to an authenticated identity.
* Firewalls are an information security program similar to a building’s firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network and the inside world known as the trusted network.
* Firewalls can be categorized by processing mode, development era or structure.
* Firewall processing modes
  + Firewalls fall into five processing-mode categories: packet filtering, application gateways, circuit gateways, MAC layer and hybrid.
  + Packet filtering examines the header information of data packets that come into the network. They examine every incoming packet header and can selectively filter packets based on header information such as destination address, source address, packet type, and other key information. Restrictions implemented are based on a combination of: IP source and destination address, direction, protocol, and TCP.
  + Dynamic packet-filtering firewalls allow only a particular packet with a particular source, destination and port address to enter.
  + Stateful inspection firewalls keep track of each network connection between internal and external systems using a state table that tracks the state and context of each packet by recording which station sent what packet and when. Disadvantage is that its additional processing and can leave vulnerable to DoS.
  + Application gateway is frequently installed on a dedicated computer, separate from the filtering route, but is commonly used in conjunction with a filtering router. This is also known as a proxy server. The proxy server is placed in an unsecured area of the network or in the DMZ so that it, rather than the Web server, is exposed to higher levels of risk from the less trusted networks. Disadvantage is it’s hard to reconfigure to protect against attacks on other protocols.
  + Circuit gateways operate at the transport layer. Like filtering firewalls, circuit gateway firewalls do not usually look at traffic lowing between one network and another, but they do prevent direction connections between one network and another. They accomplish this by creating tunnels connecting specific processes or systems on each side of the firewall and then allowing only authorized traffic in these tunnels.
  + MAC Layer firewalls are designed to operate at the media access control sub layer of the data link later. This enables these firewalls to consider the specific host computer’s identity as represented by its MAC or network interface card address in its filtering decisions.
* Firewall generations
  + 1st – static packet filtering firewalls.
  + 2nd – application level firewalls or proxy servers
  + 3rd – stateful inspection firewalls
  + 4th – dynamic packet-filtering firewalls
  + 5th – kernel proxy, a specialized form that works under Windows NT executive, which is the kernel of Windows NT. This type of firewall evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack.
* Firewalls categorized by structure.
  + Most commercial-grade firewalls are dedicated appliances. Stand-alone units running on fully customized computer platforms that provide both the physical network connection and firmware programming to perform their function.
  + A commercial-grade firewall system consists of application software that is configured for the firewall application and run on a general-purpose computer.
  + Small Office/Home Office (SOHO) connects the user’s LAN to the Internetworking device such as a cable modem or DSL router. Serves as a stateful firewall to enable inside-to-outside access.
  + Residential-grade firewall software installed on the users system directly. These applications claim to detect and prevent intrusion into the user’s system without affecting usability. Very limited configuration, increasingly difficult to use in everyday situations.
* Firewall Architectures
  + All firewall devices can be configured in a number of network connection architectures.
  + Configuration that works best depends on three factors: objectives of the network, organization’s ability to develop and implement the architectures and the budget available for the function.
  + Packet filtering routers can be configured to reject packets that the organization does not want to allow into the network.
  + Screened host firewalls combine the packet-filtering router with a separate, dedicated firewall such as a proxy server. The separate host is referred to as a bastion host. Sacrificial host is what it is known as because it is the only defense.
  + Dual-Homed host firewalls bastion host contains two NICs (network interface cards) rather than one, as in the bastion host configuration. With two NICs, all traffic must physically go through the firewall to move between the internal and external networks.
  + The dominant architecture used today is the screened subnet firewall. Provides a DMZ which can be a dedicated port on the firewall device linking a single bastion host or it can be connected to a screened subnet. A common arrangement finds the subnet firewall consisting of two or more internal bastion hosts behind a packet-filtering router, with each host protecting the trusted network. There are many variants of the screened subnet architecture. The screened subnet is an entire network segment that protects the DMZ systems and info from outside threats and it protects the internal networks by limiting how external connections can gain access to them.
  + SOCKS servers is to place the filtering requirements on the individual workstation rather than on a single point of defense. This frees the entry router form filtering responsibilities but it requires that each workstation be managed as a firewall detection and protection device.
* Selecting the right firewall:
  + - Which type offers balance between protection and cost?
    - What features are in the base price?
    - How easy is it to set up?
    - Can it adapt to growth?
* Configuring and managing firewalls – once the firewall architecture and technology have been selected, the organization must provide for the initial configuration and ongoing management of the firewalls.
* Best practices for firewalls
  + All traffic from the trusted network is allowed out.
  + The firewall device is never directly accessible from the public network for configuration or management purposes.
  + SMTP data is allowed o enter through the firewall, but is routed to a well-configured SMTP gateway to filter and route messaging traffic securely.
  + All Internet Control Message Protocol (ICMP) data should be denied.
  + Telnet access to all internal severs from the public networks should be blocked.
  + When Web services are offered outside the firewall, HTTP traffic should be blocked from internal networks through the use of some form of proxy access or DMZ architecture.
  + All data that is not verifiably authentic should be denied.
* Content filters are software filters that allows administrators to restrict access to content from within a network. Primary purpose to restrict access to external materials.
* War dialer is an automatic phone-dialing program that dials every number in configured range and checks to see if a person, answering machine or modem pick sup. If the modem answers, the war dialer program makes a note of the number and then moves on the next target number.
* RADIUS (Remote Authentication Dial-In User Service) system centralizes the management of user authentication by packing the responsibility for authenticating each user in the central RADIUS server.
* TACACS (Terminal Access Controller Access Control System) remote access authorization system that is based on a client/server configuration. Contains a centralized database and validates the user’s credentials.
* Diameter protocol defines the minimum requirements for a system that provides authentication, authorization and accounting services that can go beyond these basics and add commands.
* Kerbeos keeps a database cntaing the private keys of clients and servers.
* SESAME first authenticated to an authentication server and receives a token. Token is presented to privileged attribute server as proof of identity to gain a privilege.