* 7 domains to protect.
  + User Domain
    - actual users (Employees, consultants, contractors or other third party users)
  + Workstation Domain
    - End-user’s desktop devices such as desktop computer, laptop, VoIP telephone or other end-point devices
  + LAN Domain
    - Physical and logical local area network (LAN) technologies (e.g. 1000 Mbps switched Ethernet, 802.11-family of wireless LAN technologies)
  + LAN to WAN Domain
    - organization’s internetworking and interconnectivity point between LAN and the WAN network infrastructure
  + Remote Access Domain
    - authorized and authenticated remote access procedures for users to remotely access the organization’s IT infrastructure, systems and data
  + WAN Domain
    - Organizations with remote locations require WAN to interconnect them
  + Systems/Application Domain
    - hardware, operating system software, database software, client/server applications, and data that is typically housed in the organization’s data center and/or computer rooms
* VLAN reduces network traffic and provide a degree of security
  + Similar to subnetting
  + VLANs can be isolated so that sensitive data is transmitted only to members of the VLAN
* Network security component:
  + Network Anti-virus and anti-spyware
  + Intrusion detection systems (IDS), Intrusion prevention systems (IPS)
    - identify fast-spreading threats, such as zero-day or zero-hour attacks
  + Virtual Private Networks (VPNs)
    - provide secure remote access
  + Firewall
    - block unauthorized access to your network
    - monitors and control incoming and outgoing traffic base on predetermined security rules.
    - establishes a barrier between a trusted, secure internal network and untrusted outside network, such as the Internet
* Common interface types:
  + Tap
    - no changes to the existing network design
    - cannot block traffic or filter based on URL
    - mostly use to scan/monitor network activity only
  + Layer 2
    - Provide switch feature
    - Each group of interfaces must be assigned to a VLAN
  + Virtual Wire
    - Binds TWO firewall interfaces together through Virtual Wire object
    - Typically used when no switching or routing is needed
    - No configuration change needed
  + Layer 3
    - Enables routing between multiple interfaces (like a router):
      * Requires a virtual router
    - Requires network configuration to accommodate new IP addresses
* Security zone
  + A logical grouping based on a particular type of traffic on your network
  + Traffic within the same zone is allowed by default.
  + Traffic between different zones is denied by default.
  + Separate zones must be created for each type of interface
  + each interface must be assigned to a zone before it can process traffic
  + Security policies can be defined only between zones of the same interface
* Rule
  + Security policies is applied in the first come first service order
    - If the traffic matches the rule, no further rules below the list are evaluated (**Rule Shadowing)**
  + implicit rules
    - Traffic within a single zone (intra-zone) is allowed.
    - Traffic between two zones (inter-zone) is denied.
    - Implicit rules do not generate traffic log entries
* Filtering
  + Ingress filtering
    - When an internal LAN address appears as a source address in a packet on its way into a network from outside – this is a spoofed address
  + Egress filtering
    - If a packet with a source address from the outside such as an Internet address is received by a firewall from an interface inside the private LAN – then this is a spoofed address
  + Stateless packet filtering
    - The information about the passing packets is not remembered by the firewall
    - The allow/deny decisions are taken on packet by packet basis
    - Do not relate to the previous allowed/denied packets.
  + Stateful packet filtering
    - The firewall remembers the information about the previously passed packets
    - These can be termed as smart firewalls.
  + Advantage:
    - lower cost
    - lower resource usage
    - best suited for smaller networks.
  + Disadvantage:
    - Work only on the Network Layer
    - Do not support complex rule based models
    - Vulnerable to Spoofing in some cases
* Circuit Level Gateways
  + Work at the session layer
  + Monitor TCP handshaking between packets to determine whether a requested session is legitimate
  + Advantage:
    - Comparatively inexpensive
  + Disadvantage:
    - Do not filter Individual packets
    - After Establishing a Connection, an Attacker may take advantage of this.
* Application-level gateways
  + Work at the Application layer
  + Would work only for the protocols which are configured
* Stateful multilayer inspection firewalls
  + Work at the application , session, network layer
  + Allow direct connection between client and host, alleviating the problem caused by the lack of transparency of application level gateways
* Next Generation Firewall
  + Standard capabilities of the first-generation firewall:
    - Packet filtering, stateful protocol inspection, network-address translation (NAT), VPN connectivity, etc.
  + Truly integrated intrusion prevention:
    - Support for both vulnerability-facing and threat-facing signatures and suggesting rules (or taking action) based on IPS activity.
    - Allow both the functions collaborating together via the NGFW
  + Full stack visibility and application identification:
    - ability to enforce policy at the application layer independently from port and protocol.
  + Extra-firewall intelligence:
    - ability to take information from external sources and make improved decisions.
      * creating blacklists or whitelists and being able
      * to map traffic to users and groups using active directory.
  + Adaptability to the modern threat landscape:
    - support upgrade paths for integration of new information feeds and new techniques to address future threats.
  + In-line support with minimum performance degradation or disruption to network operations.
* NAT
  + A technique to hide the internal address from the external network.
  + Allow one or a small set of public IP addresses to be used by many hosts behind the router/firewall.
* Evasive application
  + applications that change port as needed
  + can bypass a traditional stateful inspection firewall
  + use tactics such as port hopping, non-standard ports, SSL encryption and emulation to evade the firewall
* App-ID component
  + Protocol decoder
    - Detect protocol in protocol within a session
    - Provide context for application signature
  + Application signature
    - Detect layer 7 signature with a session
  + Protocol decryption
    - SSL & SSH decryption
    - App-ID that use HTTPS must have a decryption policy for it to work
  + Heuristic
    - Look for patterns of communication when no signature exists