Network Security Devices, Design, and Technology

> A degree of security can be achieved with standard security features, and proper hardware orientation, but improper configuration can introduce vulnerabilities

OSI Model:

- 7 layers (like dip)
- each has different networking tasks
- each cooperates with adjacent layers

Devices

- bridges
  - 1-to-1 connection between two networks (operates at layer 2, ethernet)
  - most OSs allow a software bridge - i.e. to share a network connection, but can introduce vulnerabilities
- switches
  - layer 3 switches (smart switch)
  - can learn which device is connected at each port (ARP), inspects MAC address of frames to store in MAC table
  - forwards frames intended for a specific device rather than broadcast (like a hub)
  - proper configuration includes loop prevention and flood guards (port security)
  - port security limits the number of MAC addresses linked to a port
- routers
  - forward packets across different networks (layer 3)
  - can filter traffic with access control lists
  - can blacklist networks
- load balancers
  - distributes work over multiple devices
  - reduces chance of overload, and increases bandwidth of service
  - software or hardware based
  - layer 4 (network & transport layers) or layer 7 (application layer - HTTP)
  - different scheduling mechanisms - round-robin, affinity, other
- proxies
  - forward proxy - relays requests on behalf of the user
  - application / multipurpose proxy - specific protocols
  - reverse proxy - routes requests coming in to correct internal server (load balancing?)

  - transparent proxy - does not require any user configuration - manipulates packages & headers
  - advantages:
    - increases speed
    - reduces tech costs
    - improved management
    - stronger security

Hardware

Provide greater security than standard devices

Firewalls

- software or hardware based
- inspect packets and accept or deny entry
- hardware firewalls are harder to configure and are more expensive
- software firewalls only protect that device, host-based firewall
- stateless packet filtering - individual packets are approved by rules
- stateful packet filtering - keeps a record of state per connection, makes decisions based on connection & decisions
- “allow”, “drop”, “reject”
- rule-based firewalls have a decision graph, but are static in nature
- application-aware firewalls operate at a higher level
  - predefined application signatures, header inspection, payload analysis
  - web application firewalls inspect HTTP

Virtual Private Network (VPN)

- all transmitted data between host and VPN is encrypted
- remote-access VPN - user-to-LAN
- site-to-site - between hosts on the WWW
- always-on VPN - allow the user to always stay connected
- endpoint may be software on a computer (OpenVPN) or a VPN concentrator
  - dedicated hardware that aggregates hundreds or thousands of VPN connections
- full tunnel (all traffic is routed) vs. split tunnel (only some traffic)

Mail Gateway

- SMTP (sending), POP/POP3 (downloads inbox), IMAP (mail remains on server)
- monitors for and rejects unwanted mail
  - inbound can be searched for malware, spam, and phishing

    - outbound can be searched for sensitive data

Network Intrusion Detection and Prevention

Intrusion Detection System (IDS)

- Inline IDS acts like a bridge to your network
    - can block attacks, but can block service
- Passive IDS connects to a port on your switch, and gets a copy of the traffic
    - can't block attacks, but can at most cause false alarms
- can be configured in-band (via network protocols in its own network), or out-of-band via remote access
- Host Intrusion Detection System (HIDS)
    - monitors system calls and file system access
    - recognizes unauthorized registry modification
    - watches for shifty I/O
    - can't watch network traffic, only local traffic
    - all log data is local
    - resource intensive
- Network Intrusion Detection System (NIDS)
    - installed on firewalls & routers
    - can sound alarm & log events
- Application-aware IDS
    - uses contextual knowledge in real time
    - it can know OS versions & which applications are running, and what vulnerabilities are present

Monitoring

- anomaly-based compared to some baseline
- signature-based compared to well-known attacks
- behavior-based by watching abnormal actions of processes and programs - alerts user
- heuristic monitoring via experience-based techniques

Intrusion Prevention System

- Monitors traffic to immediately block attacks
- similar to NIDS, NIPS is inline to the firewall
- application-aware IPS

Security and Information Event Management (SIEM)

- Real-time monitoring and aggregation for reports
- Can be a separate device, software, or a 3rd party

- Aggregation, correlation, automated alerts and triggers, time sync, event duplication, logs

Hardware Security Module

- For storing crypto keys

SSL Decrypter

SSL/TLS Accelerator

- Card installed into web server

Media Gateway

Unified Threat Management (UTM)

- Antispam, antiphishing, antispyware, encryption, intrusion protection, web filtering

Internet Content Filter

- Restricts based on keywords

Web Security Gateway

- Application-level content examination

Network Architecture

> Network design can make a system more robust, by utilizing security zones and network segregation

- One zone may be permitted to users, while sensitive access is not permitted, partly because it's on a different network
  - common examples: demilitarized zones, NAT (network address translation)
- DMZ is "outside" the secure network - untrusted users can access DMZ
- NAT masks IP addresses of private users

Terms:

- *Intranet* - a private network internal to an organization
- *Extranet* - a private network 3rd parties can operate on
- *Guest Network* - a public network

Types of Network Segregation

- Physical Network Segregation - isolates network physically with an air Gap - No connection between private and other network
- Network Hierarchy - core switches at the top, workgroup switches at the bottom
- Virtual LAN - logical grouping, but potentially sparse hosts
  - special tagging for switches operating with VLANs

Methods for securing a network

Network Access Control

- prevents suboptimally secure hosts from connecting to main network - may quarantine them
- host agent health checks - either permanent or dissolvable
- can be embedded in Microsoft Windows Active Directory domain controller
- if AD scans the device, it's "agentless"
- quarantine is based on health certificates generated by a health registry authority

Data Loss Prevention

> **content inspection** - security analysis of the transaction within its approved context

- common uses include monitoring emails, and blocking flash drives from copying files
- operates by content inspection
- looks at:
  - security level of content
  - who's requesting it
  - where it's stored
  - when it was requested
  - where it is going
- three types of DLP sensors:
  - DLP network sensors
  - DLP storage sensors
  - DLP agent sensors
- policy violations are reported by DLP agent to DLP server
  - can block data
  - redirect request to authoritative individual to examine request
  - quarantine the data until later
  - alert a supervisor