**Firewalls**

FIREWALL TYPES

* Control or filter incoming or outgoing communications on a network or device
* Common firewall types
  + **Network Layer Firewall** – source and destination IP addresses
  + **Transport Layer Firewall** – source and destination data ports, connection states
  + **Application Layer Firewall** – application, program or service
  + **Context Aware Application Firewall** – user, device, role, application type, and threat profile
  + **Proxy Server** –web content requests
  + **Reverse Proxy Server** – protect, hide, offload, and distribute access to web servers
  + **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts
  + **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system

PORT SCANNING

* Process of probing a computer, server or other network host for open ports
* Port numbers are assigned to each running application on a device.
* Reconnaissance tool to identify running OS and services
  + Nmap – A port scanning tool
* Common responses:
  + **Open or Accepted** - a service is listening on the port.
  + **Closed, Denied, or Not Listening** – connections will be denied to the port.
  + **Filtered, Dropped, or Blocked** – no reply from the host.

APPLIANCES

Security appliances fall into these general categories:

* **Routers** - can have many firewall capabilities: traffic filtering, IPS, encryption, and VPN.
* **Firewalls** – may also have router capability, advanced network management and analytics.
* **IPS** - dedicated to intrusion prevention.
* **VPN** - designed for secure encrypted tunneling.
* **Malware/Antivirus** - Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.
* **Other Security Devices** – includes web and email security appliances, decryption devices, client access control servers, and security management systems.

DETECTING ATTACKS IN REAL TIME

1. Zero-day attack
   1. A hacker exploits a flaw in a piece of software before the creator can fix it.
2. **Real Time Scanning from Edge to Endpoint**
   1. Actively scanning for attacks using firewall and IDS/IPS network device
   2. detection with connections to online global threat centers
   3. detect network anomalies using context-based analysis and behavior detection
3. **DDoS Attacks and Real Time Response**
   1. DDoS, one of the biggest attack threats, can cripple Internet servers and network availability.
   2. DDoS originates from hundreds, or thousands of zombie hosts, and the attacks appear as legitimate traffic.

SECURITY BEST PRACTICES

* **Perform Risk Assessment** – Knowing the value of what you are protecting will help in justifying security expenditures.
* **Create a Security Policy** – Create a policy that clearly outlines company rules, job duties, and expectations.
* **Physical Security Measures** – Restrict access to networking closets, server locations, as well as fire suppression.
* **Human Resource Security Measures** – Employees should be properly researched with background checks.
* **Perform and Test Backups** – Perform regular backups and test data recovery from backups.
* **Maintain Security Patches and Updates** – Regularly update server, client, and network device operating systems and programs.
* **Employ Access Controls** – Configure user roles and privilege levels as well as strong user authentication.
* **Regularly Test Incident Response** – Employ an incident response team and test emergency response scenarios.
* **Implement a Network Monitoring, Analytics and Management Tool** - Choose a security monitoring solution that integrates with other technologies.
* **Implement Network Security Devices** – Use next generation routers, firewalls, and other security appliances.
* **Implement a Comprehensive Endpoint Security Solution** – Use enterprise level antimalware and antivirus software.
* **Educate Users** – Educate users and employees in secure procedures.
* **Encrypt data** – Encrypt all sensitive company data including email.

**Behavior Approach to Cybersecurity**

1. Botnet
   1. A group of bots connect through the Internet
   2. Controlled by malicious individuals or groups
2. Bot
   1. Typically infected by visiting a website, opening an email attachment, or opening an infected media file

Kill Chain is the stages of an information systems attack.

**1. Reconnaissance** – Gathers information

**2. Weaponization** - Creates targeted exploit and malicious payload

**3. Delivery** - Sends the exploit and malicious payload to the target

**4. Exploitation** – Executes the exploit

**5. Installation** - Installs malware and backdoors

**6. Command and Control** - Remote control from a command-and-control channel   
or server.

**7. Action** – Performs malicious actions or additional attacks on other devices

BEHAVIOR BASED SECURITY

* Honeypots
  + Lures the attacker by appealing to the attackers’ predictable behavior
  + Captures, logs and analyze the attackers’ behavior
  + Administrator can gain more knowledge and build better defense
* Cisco’s Cyber Threat Defense Solution Architecture
  + Uses behavior-based detection and indicators
  + Provide greater visibility, context and control

NETFLOW

* Gather information about data flowing through a network
* Important components in behavior-based detection and analysis
* Establish baseline behaviors

**Cisco’s Approach to Cybersecurity**

* Computer Security Incident Response Team
  + help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents
  + provides proactive threat assessment, mitigation planning, incident trend analysis, and security architecture review
* Security Playbook
  + Collection of repeatable queries against security event data sources that lead to incident detection and response
  + What does it need to accomplish?
    - Detect malware infected machines.
    - Detect suspicious network activity.
    - Detect irregular authentication attempts.
    - Describe and understand inbound and outbound traffic.
    - Provide summary information including trends,   
      statistics, and counts.
    - Provide usable and quick access to statistics and metrics.
    - Correlate events across all relevant data sources.
* Tools for Incident Prevention and Detection
  + SIEM – Security Information and Event Management
    - Software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network
  + DLP – Data Loss Prevention
    - Stops sensitive data from being stolen or escaped from the network
    - Designs to monitor and protect data in three different states
  + Cisco Identity Services Engine (Cisco ISE) and TrustSec
    - Uses role-based access control policies
* IDS and IPS
  + IDS – Intrusion Detection System
    - Usually placed offline
    - Does not prevent attacks
    - Detect, log, and report
  + IPS – Intrusion Prevention System
    - Ability to block or deny traffic based on a positive rule or signature match
  + IDS/IPS system
    - Snort
    - Sourcefire (Cisco)