4.1.1 Security Appliances

Network Devices or software that run a network.

Routers : While routers are primarily used to interconnect various network segments together, they usually also provide basic traffic filtering capabilities. This information can help you define which computers from a given network segment can communicate with which network segments.

Firewall : firewall look deep into the network traffic and identify malicious behavior that has to be blocked. Firewalls follow security policies applied to the traffic that is passing through them.

Intrusion Prevention System : IPS system use set of traffic signatures that match and block malicious traffics and attacks.

Virtual Private Networks : VPN system let remote employees use a secure encrypted tunnel from their computer and securely ssh to the organization network. VPN systems can also secure branch offices with the hq office network.

Antimalware | antivirus : these systems use signature or behavior analysis of apps to identify and block malicious code from being executed.

Other Security Devices : other security device include web and email security apps, decryption device, client access control servers and security management systems.

4.1.3 Firewalls

a firewall is designed to filter which communications are allowed in and which are blocked on a network. A firewall can be installed on a single computer with the purpose of protecting that one computer (host-based firewall) or it can be a standalone network device that protects an entire network of computers and all of the host devices on that network (network-based firewall).

As computer and network attacks have become more sophisticated, new types of firewalls have been developed, which serve different purposes.

Network layer firewall : filters communications based on source and destination ip.

Transport layer firewall : Filters communications based on source and destination data ports.

Application layer firewall : Filters communications based on an application, program or service.

Context aware layer firewall : Filters communications based on the user, device, role, application type and threat profile.

Proxy Server : Filters web content requests like URLs, domain names and media types.

Reverse Proxy Server : Placed in front of web servers, reverse proxy servers protect, hide, offload and distribute access to web servers.

Network Address Translation Firewall : This firewall hides or masquerades the private addresses of network hosts.

Host-Based Firewall : Filters ports and system service calls on a single computer operating system.

4.1.5 Port Scanning

In networking, each application running on a device is assigned an identifier called a port number. This port number is used on both ends of the transmission so that the right data is passed to the correct application. Port scanning is a process of probing a computer, server or other network host for open ports. It can be used maliciously as a reconnaissance tool to identify the operating system and services running on a computer or host, or it can be used harmlessly by a network administrator to verify network security policies on the network.

4.1.7 Intrusion Detection and Prevention System

Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are security measures deployed on a network to detect and prevent malicious activities.

IDS : An IDS can either be a dedicated network device or one of several tools in a server, firewall or even a host computer operating system, that scans data against a database of rules or attack signatures, looking for malicious traffic. If a match is detected, the IDS will log the detection and create an alert for a network administrator. It will not take action and therefore it will not prevent attacks from happening. The

job of the IDS is to detect, log and report. The scanning performed by the IDS slows down the network (known as latency). To prevent network delay, an IDS is usually placed offline, separate from regular network traffic. Data is copied or mirrored by a switch and then forwarded to the IDS for offline detection.

IPS : An IPS can block or deny traffic based on a positive rule or signature match. One of the most well-known IPS/IDS systems is Snort. The commercial version of Snort is Cisco's Sourcefire. Sourcefire can perform real-time traffic and port analysis, logging, content searching and matching, as well as detect probes, attacks and execute port scans. It also integrates with other third-party tools for reporting, performance and log analysis.

4.1.8 Real-Time Detection

Detecting attacks in real time requires actively scanning for attacks using firewall and IDS/IPS network devices. Next generation client and server malware detection with connections to online global threat centers must also be used. Today, active scanning devices and software must detect network anomalies using context-based analysis and behavior detection.

DDoS is one of the biggest attack threats requiring real-time detection and response. For many organizations, regularly occurring DDoS attacks cripple Internet servers and network availability. These attacks are extremely difficult to defend against because the attacks originate from hundreds, even thousands, of zombie hosts, and the attacks appear as legitimate traffic.

4.1.9 Protecting against malware

One way of defending against zero-day attacks and advanced persistent threats (APTs) is to use an enterprise-level advanced malware detection solution, like Cisco's Advanced Malware Protection (AMP) Threat Grid.

This is client/server software that can be deployed on host endpoints, as a standalone server or on other network security devices. It analyzes millions of files and correlates them against hundreds of millions of other analyzed malware artifacts for behaviors that reveal an APT. This approach provides a global view of malware attacks, campaigns and their distribution.

4.1.10 Security Best Practices

Perform a risk assessment : Knowing and understanding the value of what you are protecting will help to justify security expenditures.
Creating a Security Policy : Create a policy that clearly outlines the organization's rules, job roles, and responsibilities and expectations for employees.
Physical Security Measures : Restrict access to networking & server locations, as well as fire suppression.
Human Resource Security Measures : Background checks should be completed for all employees.
Perform and Test Backups : Back up information regularly and test data recovery from backups.
Maintain Security patches/updates : Regularly update server, client and network device operating systems and programs.
Employ access control : 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 network monitoring, analytics tools : Choose a security monitoring solution that integrates with other technologies.
Implement network security device : next gen routers, firewall and other security appliances.
Implement comprehensive endpoint security solutions : Use enterprise level antimalware and antivirus software.
Educate Users : Provide training to employees in security procedures.
Encrypt data : Encrypt all sensitive organizational data, including email.

4.2.1 Behavior Based Security

Behavior-based security is a form of threat detection that involves capturing and analyzing the flow of communication between a user on the local network and a local or remote destination. Any changes in normal patterns of behavior are regarded as anomalies, and may indicate an attack.

Honeypots : A honeypot is a behavior-based detection tool that lures the attacker in by appealing to their predicted pattern of malicious behavior. Once the attacker is inside the honeypot, the network administrator can capture, log and analyze their behavior so that they can build a better defense.

Cisco's Cyber Threat Defense Solution Architecture : This security architecture uses behavior- based detection and indicators to provide greater visibility, context and control. The aim is to know who is carrying out the attack, what type of attack they are performing and where, when and how the attack is taking place. This security architecture uses many security technologies to achieve this goal.

4.2.2 NetFlow

NetFlow technology is used to gather information about data flowing through a network, including who and what devices are in the network, and when and how users and devices access the network.

NetFlow is an important component in behavior-based detection and analysis. Switches, routers and firewalls equipped with NetFlow can report information about data entering, leaving and traveling through the network.

This information is sent to NetFlow collectors that collect, store and analyze NetFlow data, which can be used to establish baseline behaviors on more than 90 attributes, such as source and destination IP address.

4.2.3 Penetration Testing

act of assessing a computer system, network or organization for security vulnerabilities. A pen test seeks to breach systems, people, processes and code to uncover vulnerabilities which could be exploited. This information is then used to improve the system's defenses to ensure that it is better able to withstand cyber attacks in the future.

Planning : pen tester gathers as much information as possible about a target system or network, its potential vulnerabilities and exploits to use against it. This involves conducting passive or active reconnaissance (footprinting) and vulnerability research.

Scanning : The pen tester carries out active reconnaissance to probe a target system or network and identify potential weaknesses which, if exploited, could give an attacker access. Active reconnaissance may include:

- port scanning to identify potential access points into a target system
- vulnerability scanning to identify potential exploitable vulnerabilities of a particular target
- establishing an active connection to a target (enumeration) to identify the user account, system account and admin account.

Gaining Access : The pen tester will attempt to gain access to a target system and sniff network traffic, using various methods to exploit the system including:

- launching an exploit with a payload onto the system
- breaching physical barriers to assets
- social engineering
- exploiting website vulnerabilities
- exploiting software and hardware vulnerabilities or misconfigurations
- breaching access controls security
- cracking weak encrypted Wi-Fi.

Maintaining Access : The pen tester will maintain access to the target to find out what data and systems are vulnerable to exploitation. It is important that they remain undetected, typically using backdoors,

Trojan horses, rootkits and other covert channels to hide their presence. When this infrastructure is in place, the pen tester will then proceed to gather the data that they consider valuable.

Reporting : The pen tester will provide feedback via a report that recommends updates to products, policies and training to improve an organization's security.

4.2.5 Impact Reduction

Communicating the issue : Internally, all employees should be informed and a clear call to action communicated. Externally, all clients should be informed through direct communication and official announcements.

Be Sincere and Accountable : Respond to the breach in an honest and genuine way, taking responsibility where the organization is at fault.

Provide Details : explain why the breach took place and what information was compromised.

Find the cause : Take steps to understand what caused and facilitated the breach. This may involve hiring forensics experts to research and find out the details.

Lesson learned : lessons learned from forensic investigations are applied to prevent similar breaches from happening in the future.

Check again : Attackers will often attempt to leave a backdoor to facilitate future breaches. To prevent this, make sure that no backdoors are installed and nothing else has been compromised.

Educate : Raise awareness, train and educate employees, how to prevent future breaches.

4.2.6 Risk Management

Risk management is the process of identifying and assessing risk in an effort to reduce the impact of threats and vulnerabilities. You cannot eliminate risk completely but you can determine acceptable levels by weighing up the impact of a threat with the cost of implementing controls to mitigate it. The cost of a control should never be more than the value of the asset you are protecting.

Frame the risk : identify threat that increase risk.

Assess the risk : determine severity of the threat.

Response to the risk : develop an action plan to reduce overall risk exposure. Detailing where risk can be eliminated, mitigated, transferred or accepted.

Monitoring the risk : Continuously review any risk reduced through elimination, mitigation or transfer actions. Not all risks can be eliminated, so you will need to closely monitor any threats that have been accepted.

4.3.1 Cisco's CSIRT

Computer Security Incident Response Team (CSIRT), review and respond to computer security incident reports. Cisco CSIRT goes a step further and provides proactive threat assessment, mitigation planning, incident trend analysis and security architecture review in an effort to prevent security incidents from happening. Cisco collaborates with the Forum of Incident Response and Security Teams (FIRST), the National Safety Information Exchange (NSIE), the Defense Security Information Exchange (DSIE) and the DNS Operations Analysis and Research Center (DNS-OARC) to ensure we stay up-to-date with new developments.

4.3.2 Security Playbook

A security playbook is a collection of repeatable queries or reports that outline a standardized process for incident detection and response. Ideally, a security playbook should:

- highlight how to identify and automate the response to common threats such as the detection of malware-infected machines, suspicious network activity or irregular authentication attempts.
- describe and clearly define inbound and outbound traffic.
- provide summary information including trends, statistics and counts.
- provide usable and quick access to key statistics and metrics.

correlate events across all relevant data sources.

4.3.3 Tools for Incident Detection and Prevention

there are a range of tools used to detect and prevent security incidents:

A Security Information and Event Management(SIEM) system collects and analyzes security alerts, logs and other real time and historical data from security devices on the network to facilitate early detection of cyber attacks.

A Data Loss Prevention(DLP) system is designed to stop sensitive data from being stolen from network. It monitors, protects data in three different states: in use, at rest and at use.

4.3.4 Cisco's ISE and TrustSEC

Cisco Identity Services Engine (ISE) and TrustSec enforce user access to network resources by creating role-based access control policies.

An IPS can block or deny traffic based on a positive rule or signature match.
An IDS scans data against a database of rules or attack signatures, looking for malicious traffic.
A DLP system is designed to stop sensitive data from being stolen from or escaping a network.
A SIEM system collects and analyzes security alerts, logs and other real-time and historical data from security devices on the network.