Cybersecurity devices and technologies

Security appliances

Can be **standalone devices like a router os software tools that are run on a network device**  
 they have 6 categories:

ROUTERS  
 - also provide **basic traffic filtering capabilities, define which computers from a   
 given network segment can communicate with which network segment**

FIREWALLS  
 - **look deeper into the network traffic itself and identify malicious behavior   
 that has to be blocked**. It can apply sophisticated security policies that apply to   
 the network traffic

INSTRUSION PREVENTION SYSTEMS  
 - ***IPS*** systems **use a set of traffic signatures that match and block malicious   
 traffic and attacks**

VIRTUAL PRIVATE NETWORKS  
 - **VPN** let remote employees use a **secure encrypted tunnel** from their mobile   
 computer and security connect back to the organizations network

ANTIMALWARE OR ANTIVIRUS  
 - these systems use signatures or behavioral analysis of applications to identify   
 and block malicious code from being executed

OTHER SECURITY DEVICES  
 - those can be web and email security appliances, decryption devices, client   
 access control servers and security management systems

Firewalls

Is **designed to control or filter which communications are allowed in and which are allowed   
 out of a device or network**

It 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 and all the host devices  
 (network-based firewall)  
 types:  
 network layer firewall  
 - this **filters communications based on source and destination IP**

transport layer firewall  
 - filters communications **based on source and destination data ports, as well as   
 connection state**

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 (NAT) firewall  
 - **hides or masquerades the private addressee of network hosts**

host-based firewall  
 - **filters ports and system service calls on a single computer operating system**

**port scanning**

in networking, each application running on a device is assigned an identifier called a port number. this is used both ends of the transmittion 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

TRY ZENMAP

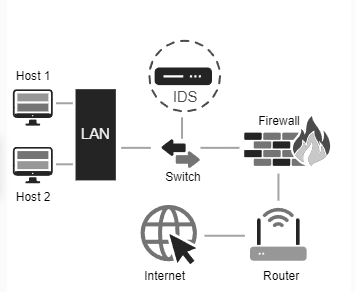
Intrusion detection and prevention systems

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

IDS

- it can either be a dedicated network device or one of several tools in a server, firewall or even a   
 host computer OS

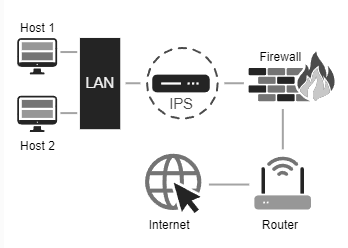
**It scans data** against a database of rules or attacks signatures, **looking for malicious traffic**  
 **When it does the IDS will log the detection and create an alert for a network administrator** it wont take action, its job is to detect, log and report



IPS

- **can block or deny traffic based on a positive rule or signature match**

- it can perform real-time traffic and port analysis, logging, content searching and matching, as   
 well as detect probes, attacks and execute port scans



Real-time detection

**Detecting attacks in real time requires** actively scanning for attacks using **firewall and IDS/IPS network devices**. Next gen client/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 detections

DDoS is one of the biggest attack threats requiring real-time detection and response  
 for many organizations, regulary occurring DDoS attacks cripple internet servers and network   
 availability its difficult to defend against them because they appear as legitimate traffic

Protecting against malware

One way of defending against zero-day attacks and advanced persistent threats (APTs) is to use   
 an enterprice-level advanced malware detection solution, like   
 (cisco advanced malware protection threat grid)

Security best practices

Many national and professional organizations have published lists of security best practices

Some of the most useful guidelines are found in organizational repositories such as the national institute of standards and technology, computer security resource center

Perform a risk assessment  
 **knowing and understanding the value of what you are protecting will help to justify   
 security expenditures**

Create a security policy  
 **create a policy that clearly outlines the organizations rules, job roles, and   
 responsibilities and expectations for employees**

Physical security measures  
 **restrict access to networking closets and server locations, as well as fire suppression**

Human resources 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 and updates  
 **regularly update server, client and network device OS 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 net gen routers, firewalls and other security appliances**

Implement a comprehensive endpoint security solution  
 **use enterprise level antimalware and antivirus software**

Educate users  
 **provide training to employees in security procedures** one of the most widely known and respected organizations for cybersecurity training is   
 the SANS

Encrypt data  
 **encrypt all sensitive organizational data, including email**