CSE 3

Implementing Secure Network Designs

- **Network Appliances:** A number of network appliances are involved in provisioning a network architecture:
  - **Switches**—forward frames between nodes in a cabled network. Switches work at layer 2 of the OSI model and make forwarding decisions based on the hardware or Media Access Control (MAC) address of attached nodes.

- **Wireless access points**—provide a bridge between a cabled network and wireless clients, or stations. Access points work at layer 2 of the OSI model.

- **MCQ:** Swicthes make forwarding decisions based on the _____of attached nodes.
  - Logical Address
  - Hardware or Media Access Control (MAC) address
  - Port Address
  - IP address

- **MCQ:** Access points work at which layer of the OSI model?
  - Physical Layer
  - Data Link Layer
  - Network Layer
  - Application Layer

- **Routers**—forward packets around an internetwork, making forwarding decisions based on IP addresses. Routers work at layer 3 of the OSI model. Routers can apply logical IP subnet addresses to segments within a network.

- **MCQ:** Routers forward packets around an internetwork, making forwarding decisions based on_____.
  - Port addresses
  - IP addresses
  - MAC Addresses
  - Domain addresses

- Firewalls—apply an access control list (ACL) to filter traffic passing in or out of a network segment. Firewalls can work at layer 3 of the OSI model or higher.

- Load balancers—distribute traffic between network segments or servers to optimize performance. Load balancers can work at layer 4 of the OSI model or higher.

- Domain Name System (DNS) servers—host name records and perform name resolution to allow applications and users to address hosts and services using fully qualified domain names (FQDNs) rather than IP addresses. DNS works at layer 7 of the OSI model.

Routing and Switching Protocols

- **Address Resolution Protocol (ARP)**
  - The Address Resolution Protocol (ARP) maps a network interface's hardware (MAC) address to an IP address. Normally a device that needs to send a packet to an IP address but does not know the receiving device's MAC address broadcasts an ARP Request packet, and the device with the matching IP responds with an ARP Reply.

- **Internet Protocol (IP)**
- IP provides the addressing mechanism for logical networks and subnets. A 32-bit IPv4 address is written in dotted decimal notation, with either a network prefix or subnet mask to divide the address into network ID and host ID portions.

- **Routing Protocols**

- **RIP**
- **IGRP**
- **EIGRP**
- **OSPF**

Network Topology and Zones

- **Intranet (private network)**

- **Demilitarized Zones**
- If communication is required between hosts on either side of a DMZ, a host within the DMZ acts as a proxy.

Other Secure Network Design Considerations

- Network design must also be considered for data centers and the cloud. A datacenter is a facility dedicated to hosting servers, rather than a mix of server and client workstation machines.

- Traffic that goes to and from a data center is referred to as **north-south**. This traffic represents clients outside the data center making requests and receiving responses.

- most traffic is actually between servers within the data center. This is referred to as **east-west traffic.**

Loop Prevention

- Layer 2 loops are prevented by the **Spanning Tree Protocol (STP)**.

- **Broadcast Storm Prevention:** STP is principally designed to prevent **broadcast storms**.

Physical Port Security and MAC Filtering

- Configuring **MAC filtering** on a switch means defining which MAC addresses are allowed to connect to a particular port.

- Another option is to configure **Dynamic Host Configuration Protocol (DHCP) snooping**.
  - DHCP is the protocol that allows a server to assign IP address information to a client when it connects to the network.
  - DHCP snooping inspects this traffic arriving on access ports to ensure that a host is not trying to spoof its MAC address.
  - It can also be used to prevent rogue (or spurious) DHCP servers from operating on the network.
  - With DHCP snooping, only DHCP messages from ports configured as trusted are allowed.

Wireless Network Installation Considerations

- Wireless network installation considerations refer to the factors that ensure good availability of authorized Wi-Fi access points.
- The **access points** forward traffic to and from the wired switched network.
- Each WAP is identified by its MAC address, also referred to as its basic service set identifier (BSSID).

- Wireless networks can operate in either the 2.4 GHz or 5 GHz radio band.
- Each radio band is divided into a number of channels, and each WAP must be configured to use a specific channel.
- For performance reasons, the channels chosen should be as widely spaced as possible to reduce different types of interference:
  - Co-channel interference (CCI)—when two WAPs in close proximity use the same channel, they compete for bandwidth within that channel, as signals collide and have to be re-transmitted.

- Adjacent channel interference (ACI)—channels have only 5 MHz spacing, but Wi-Fi requires 20 MHz of channel space. When the channels selected for WAPs are not cleanly spaced, the interference pattern creates significant numbers of errors and loss of bandwidth.

- A **site survey** is used to measure signal strength and channel usage throughout the area to cover.

- Heat Map – it shows where a signal is strong (red) or weak (green/blue), and which channel is being used and how they overlap.
  - This data is then used to optimize the design, by adjusting transmit power to reduce a WAP's range, changing the channel on a WAP, adding a new WAP, or physically moving a WAP to a new location.

Wi-Fi Authentication Methods

- In order to secure a network, you need to be able to confirm that only valid users are connecting to it.
- Wi-Fi authentication comes in three types: **personal, open, and enterprise.**

- Within the personal category, there are two methods: pre-shared key authentication (PSK) and simultaneous authentication of equals (SAE).

Open Authentication and Captive Portals

- Selecting open authentication means that the client is not required to authenticate. This mode would be used on a public WAP (or "hotspot"). In WPA2, this also means that data sent over the link is unencrypted. Open authentication may be combined with a secondary authentication mechanism managed via a browser.

- When the client associates with the open hotspot and launches the browser, the client is redirected to a **captive portal** or splash page.

- **EAP-TLS** is one of the strongest types of authentication and is very widely supported.
  - An encrypted Transport Layer Security (TLS) tunnel is established between the supplicant and authentication server using public key certificates on the authentication server and supplicant.
  - As both supplicant and server are configured with certificates, this provides mutual authentication.
  - The supplicant will typically provide a certificate using a smart card or a certificate could be installed on the client device, possibly in a Trusted Platform Module (TPM).

PEAP, EAP-TTLS, and EAP-FAST

- In **Protected Extensible Authentication Protocol (PEAP)**, as with EAP-TLS, an encrypted tunnel is established between the supplicant and authentication server, but PEAP only requires a server-side public key certificate.

- **EAP-Tunneled TLS (EAP-TTLS)** is similar to PEAP. It uses a server-side certificate to establish a protected tunnel through which the user's authentication credentials can be transmitted to the authentication server.

- **EAP with Flexible Authentication via Secure Tunneling (EAP-FAST)** is similar to PEAP, but instead of using a certificate to set up the tunnel, it uses a Protected Access Credential (PAC), which is generated for each user from the authentication server's master key.

- A rogue access point is one that has been installed on the network without authorization, whether with malicious intent or not. It is vital to periodically survey the site to detect rogue WAPs.

- A rogue WAP masquerading as a legitimate one is called an evil twin. An **evil twin** might just have a similar name (SSID) to the legitimate one, or the attacker might use some DoS technique to overcome the legitimate WAP.

- A Wi-Fi **jamming** attack can be performed by setting up a WAP with a stronger signal. Wi-Fi jamming devices are also widely available, though they are often illegal to use and sometimes to sell.

Load Balancing

- A **load balancer** distributes client requests across available server nodes in a farm or pool.

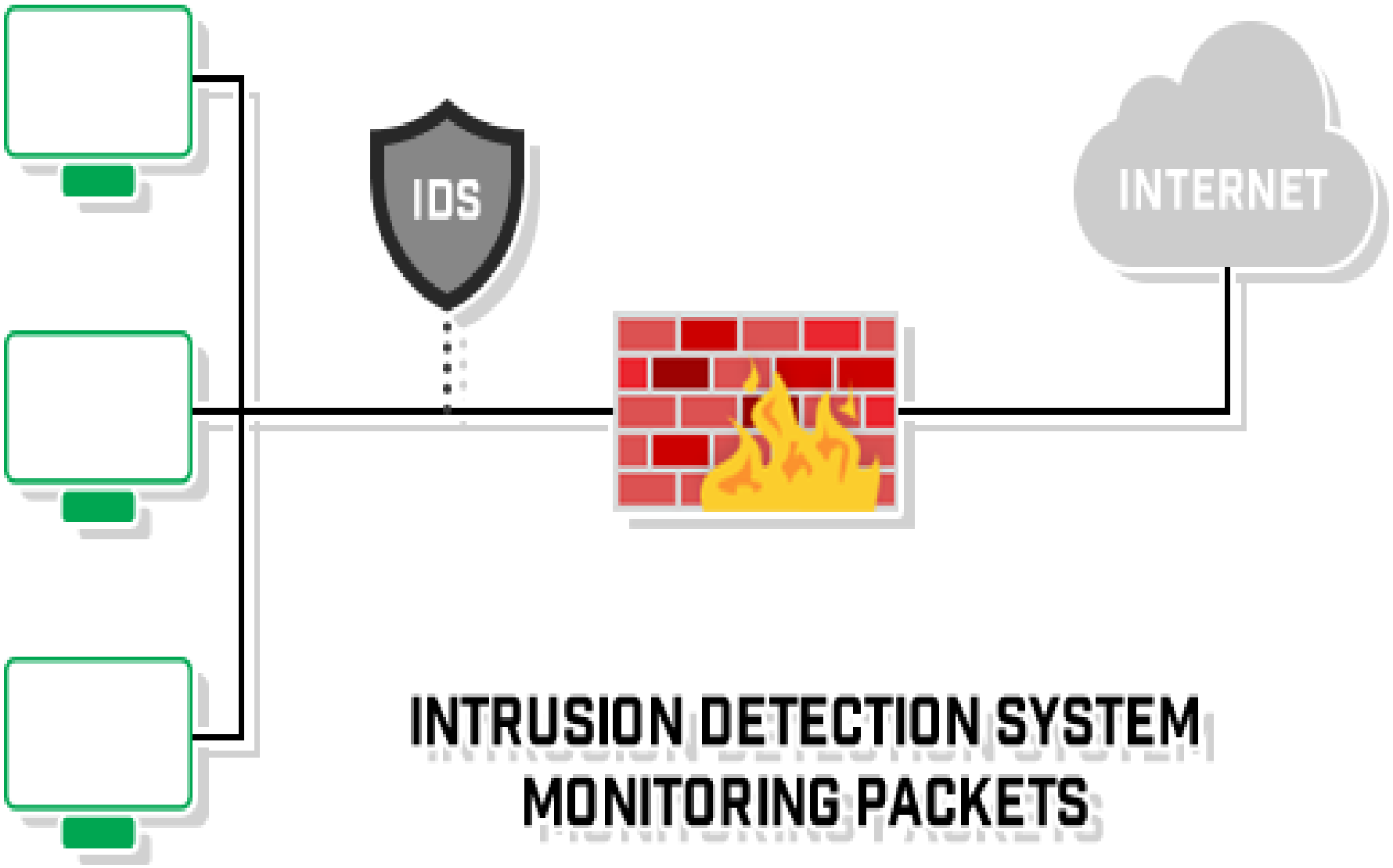
- There are two main types of load balancers:
  - Layer 4 load balancer—basic load balancers make forwarding decisions on IP address and TCP/UDP port values, working at the transport layer of the OSI model.
  - Layer 7 load balancer (content switch)—as web applications have become more complex, modern load balancers need to be able to make forwarding decisions based on application-level data, such as a request for a particular URL or data types like video or audio streaming. This requires more complex logic, but the processing power of modern appliances is sufficient to deal with this.

- **Clustering:** Where load balancing distributes traffic between independent processing nodes, **clustering** allows multiple redundant processing nodes that share data with one another to accept connections. This provides redundancy.

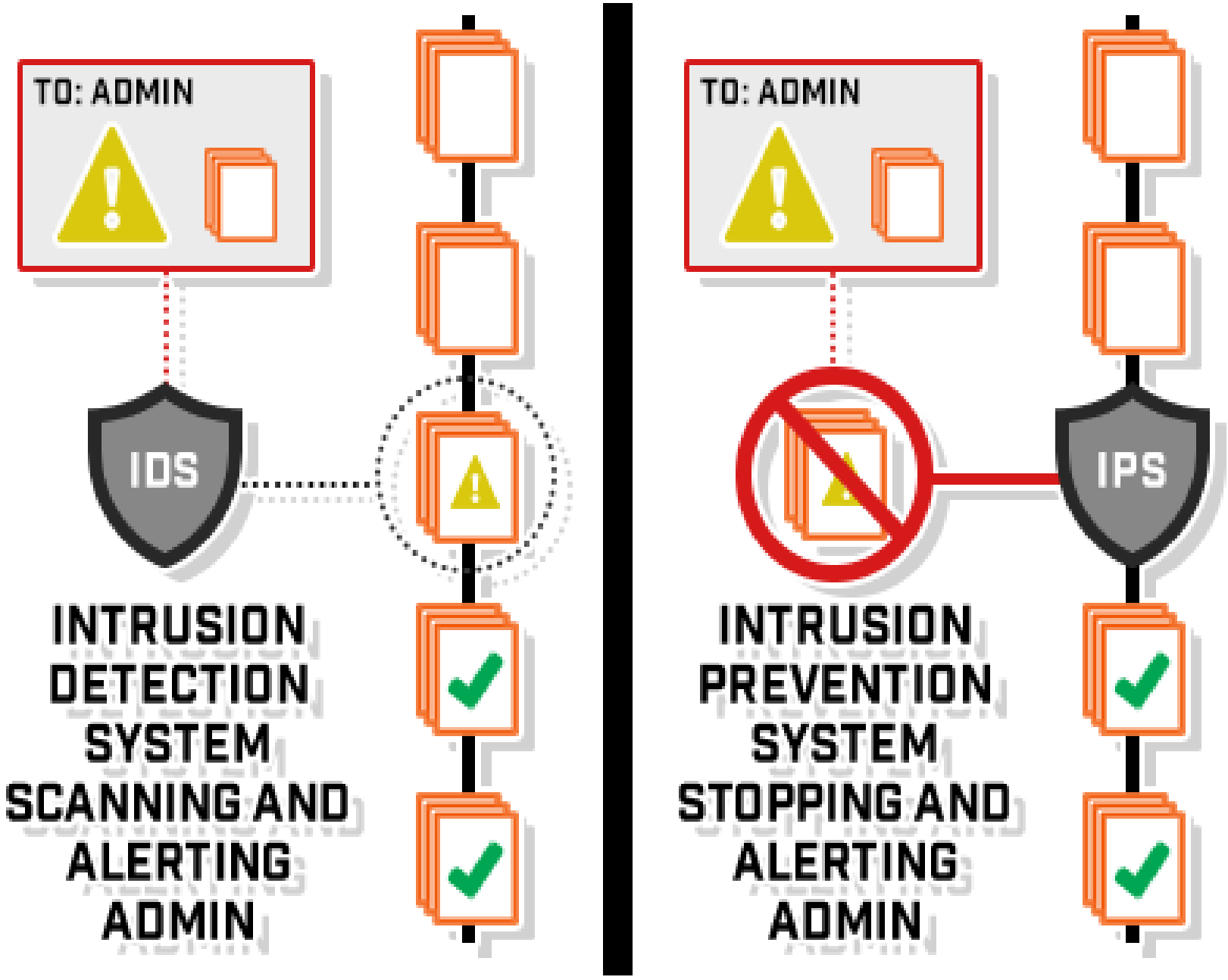
- **Virtual IP:** For example, you might want to provision two load balancer appliances so that if one fails, the other can still handle client connections. Unlike load balancing with a single appliance, the public IP used to access the service is shared between the two instances in the cluster. This is referred to as a virtual IP or shared or floating address.

- Intrusion Detection

- Intrusion detection is a **strategy** that any organization must consider.
- Intrusion detection can be defined as **the ability to monitor and react to computer misuse**.
- Many hardware and software products on the market today provide various levels of intrusion detection.


IDS
INTERNET
INTRUSION DETECTION SYSTEM
MONITORING PACKETS

- An **intrusion detection system (IDS)** is a device or software application that monitors a network for malicious activity or policy violations.
- Any malicious activity or violation is typically reported or collected centrally using a security information and event management system.
- Some IDS's are capable of responding to detected intrusion upon discovery.
- These are classified as intrusion prevention systems (IPS).


TO: ADMIN
IDS
INTRUSION DETECTION SYSTEM SCANNING AND ALERTING ADMIN
TO: ADMIN
IPS
INTRUSION PREVENTION SYSTEM STOPPING AND ALERTING ADMIN

There are two main categories of these systems: **passive and active**.

- *A passive system, like an IDS, will only monitor, log, and provide alerts to activity, while an active system will automatically take action based on software design.*
- In an active system, like an IPS, innocent traffic can be seen as malicious and, therefore, will be blocked from the network.

IDS Detection Types

- There is a wide array of IDS, ranging from antivirus software to tiered monitoring systems that follow the traffic of an entire network. The most common classifications are:
- **Network intrusion detection systems (NIDS):** A system that analyzes incoming network traffic.
- **Host-based intrusion detection systems (HIDS):** A system that monitors important operating system files.

- There is also subset of IDS types.

- The most common variants are based on *signature detection* and *anomaly detection.*

- **Signature-based:** Signature-based *IDS detects possible threats by looking for specific patterns*, such as byte sequences in network traffic, or known malicious instruction sequences used by malware.
- This terminology originates from antivirus software, which refers to these detected patterns as signatures.
- Although signature-based IDS can easily detect known attacks, it is impossible to detect new attacks, for which no pattern is available.

- **Anomaly-based:** a newer technology designed to detect and adapt to unknown attacks, primarily due to the explosion of malware.
- This detection method uses machine learning to create a defined model of trustworthy activity, and then compare new behavior against this trust model.
- While this approach enables the detection of previously unknown attacks, previously unknown legitimate activity can accidentally be classified as malicious.

- **Hybrid Detection:** A hybrid IDS uses both signature-based and anomaly-based detection.
- This enables it to **detect more potential attacks** with a lower error rate.

IDS Usage in Networks

- When **placed** at a strategic point or points within a network to monitor traffic to and from all devices on the network, an IDS will perform an ***analysis of passing traffic***, and match the traffic that is passed on the subnets to the library of known attacks.
- Once an attack is identified, or abnormal behavior is **sensed**, the alert can be sent to the administrator.

IDS vs Firewalls

- Intrusion Detection Systems and firewalls are both cybersecurity solutions that can be **deployed to protect** an endpoint or network.

- However, they differ significantly in their purposes.

- An IDS is a ***passive*** monitoring device that detects potential threats and generates **alerts**, enabling security operations center (SOC) analysts or incident responders to investigate and respond to the potential incident.
- An IDS provides no actual protection to the endpoint or network.

- A firewall, on the other hand, is designed to act as a **protective system**.
- It performs analysis of the metadata of network packets and allows or blocks traffic based upon predefined rules.
- Firewall analyzes the ***source of the traffic***, ***destination address***, ***destination port***, ***source address***, and ***protocol type*** to determine whether to allow or block the traffic coming in.
- This creates a boundary over which certain types of traffic or protocols cannot pass.

- Since a firewall is an active protective device, it is more like an Intrusion Prevention System (IPS) than an IDS.
- An IPS is like an IDS but actively blocks identified threats instead of simply raising an alert.

- This complements the functionality of a firewall, and many next-generation firewalls (NGFWs) have integrated IDS/IPS functionality.
- This enables them to both enforce the predefined filtering rules (firewalls) and detect and respond to more sophisticated cyber threats (IDS/IPS).

The Top Intrusion Detection Systems are:

- 1) SolarWinds Security Event Manager
- 2) Bro
- 3) OSSEC
- 4) Snort
- 5) Suricata
- 6) Security Onion
- 7) Open WIPS-NG
- 8) Sagan
- 9) McAfee Network Security Platform
- 10) Palo Alto Networks

- Network Security Tools and Devices

Network Security Tools

- **Network Security Monitoring Tools**

1. Argus
2. P0f
3. Nagios
4. Splunk
5. OSSEC

- **Encryption Tools**

1. Tor
2. KeePass
3. TrueCrypt

- **Web Vulnerability Scanning Tools**

1. Burp Suite
2. Nikto
3. Paros Proxy
4. NMap
5. Nessus Professional
6. Nexpose

- **Penetration Testing tools**

1. Metasploit
2. Kali Linux

- **Packet Sniffers and Password Auditing Tools**

1. John the Ripper
2. Tcpdump
3. Wireshark

- **Network Defense Wireless Tools**

1. Aircrack
2. Netstumbler
3. KisMAC

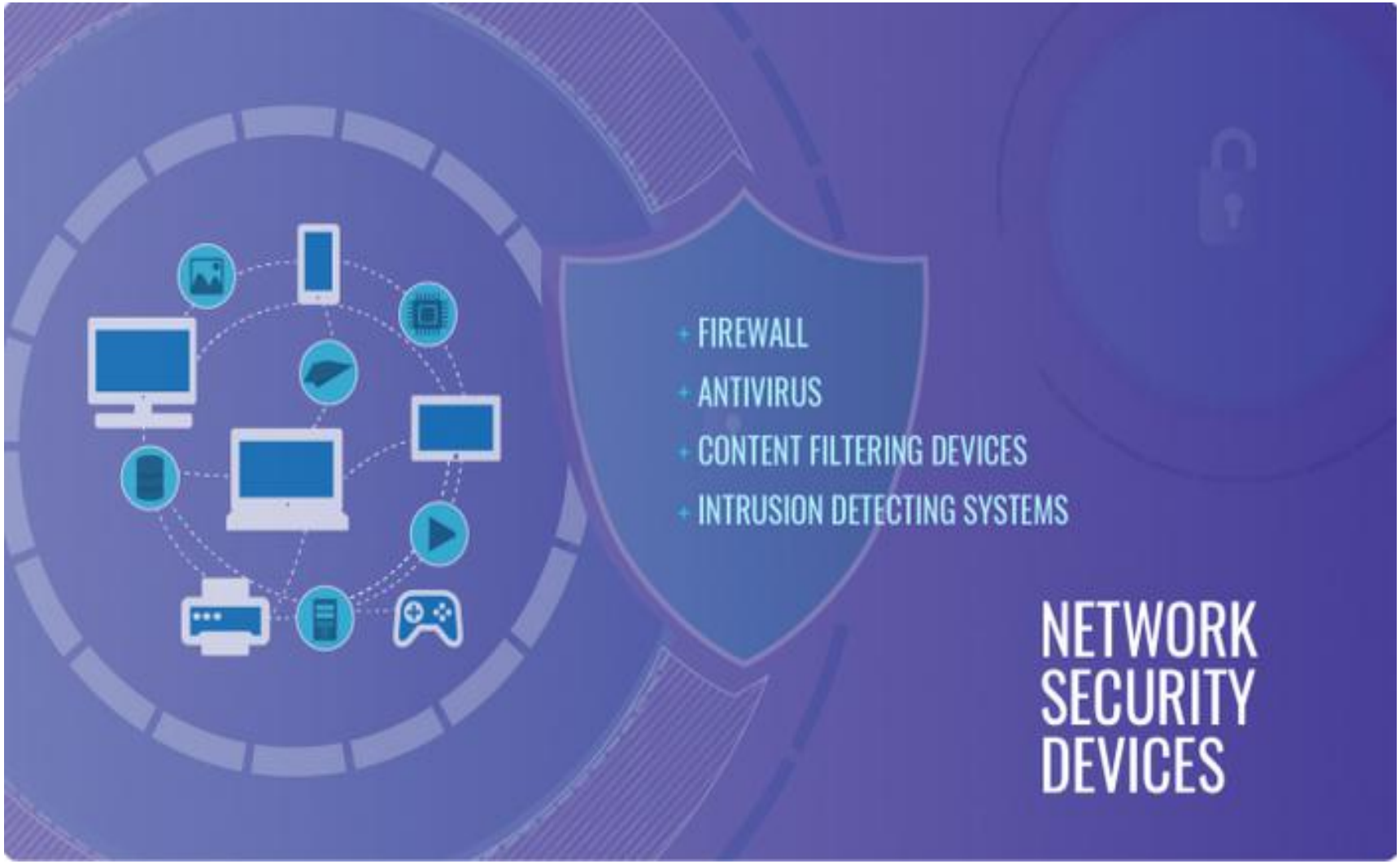
- **Network Intrusion & Detection tools**

1. Snort
2. Forcepoint
3. GFI LanGuard
4. Acunetix

- Good network security describes everything that potentially could impact your company's systems and everything that helps keep those threats away.
- Network security tools **focus on** *hardware, software, even policies, and procedures* to encourage everyone in an organization to practice smart approaches to keeping data safe.
- Network security also can include keeping up with global threats and making sure systems stay safe from everyone from individual hackers to larger organized breach attempts.

- Effective network security defines all that may influence any organization's networks and all that helps prevent those attacks.
- Network security tools are designed to enable all organizations to take smart approaches in policies and processes to safeguard data, networks, and systems.

Network Security Devices



- **Application Security:** HTTP Security, Electronic Mail, Firewalls

- Application security is the process of developing, adding, and testing security features within applications to **prevent security vulnerabilities** against threats such as unauthorized access and modification.

Types of application security features

- Different types of application security features include *authentication, authorization, encryption, logging, and application security testing*.

- **Authentication**: When software developers build procedures into an application **to ensure** that only authorized users gain access to it.
- Authentication procedures ensure that a user is who they say they are.
- This can be accomplished by requiring the user to provide a user name and password when logging in to an application.
- Multi-factor authentication requires more than one form of authentication—the factors might include something you know (a password), something you have (a mobile device), and something you are (a thumb print or facial recognition).

- **Authorization**: After a user has been authenticated, the user may be authorized **to access** and use the application.
- The system can validate that a user has **permission** to access the application by comparing the user's identity with a list of authorized users.
- Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.

- **Encryption**: After a user has been authenticated and is using the application, other security measures can **protect sensitive data** from being seen or even used by a cybercriminal.
- In cloud-based applications, where traffic containing sensitive data travels between the end user and the cloud, that traffic can be **encrypted** to keep the data safe.

- **Logging**: If there is a security breach in an application, **logging can help identify** who got access to the data and how.
- Application log files provide a time-stamped record of which aspects of the application were accessed and by whom.

- **Application security testing**: A necessary process to ensure that all of these security controls **work properly**.

- Application security in the **cloud** poses some extra challenges. Because cloud environments provide *shared resources*, special care must be taken to ensure that users only have access to the data they are authorized to view in their cloud-based applications.

- Mobile devices also transmit and receive information across the Internet, as opposed to a private network, making them vulnerable to attack. Enterprises can **use virtual private networks (VPNs)** to add a layer of mobile application security for employees who log in to applications remotely.

- Web application security applies to **web applications**—apps or services that users access through a browser interface over the Internet. Because web applications live on remote servers, not locally on user machines, information must be transmitted to and from the user over the Internet.

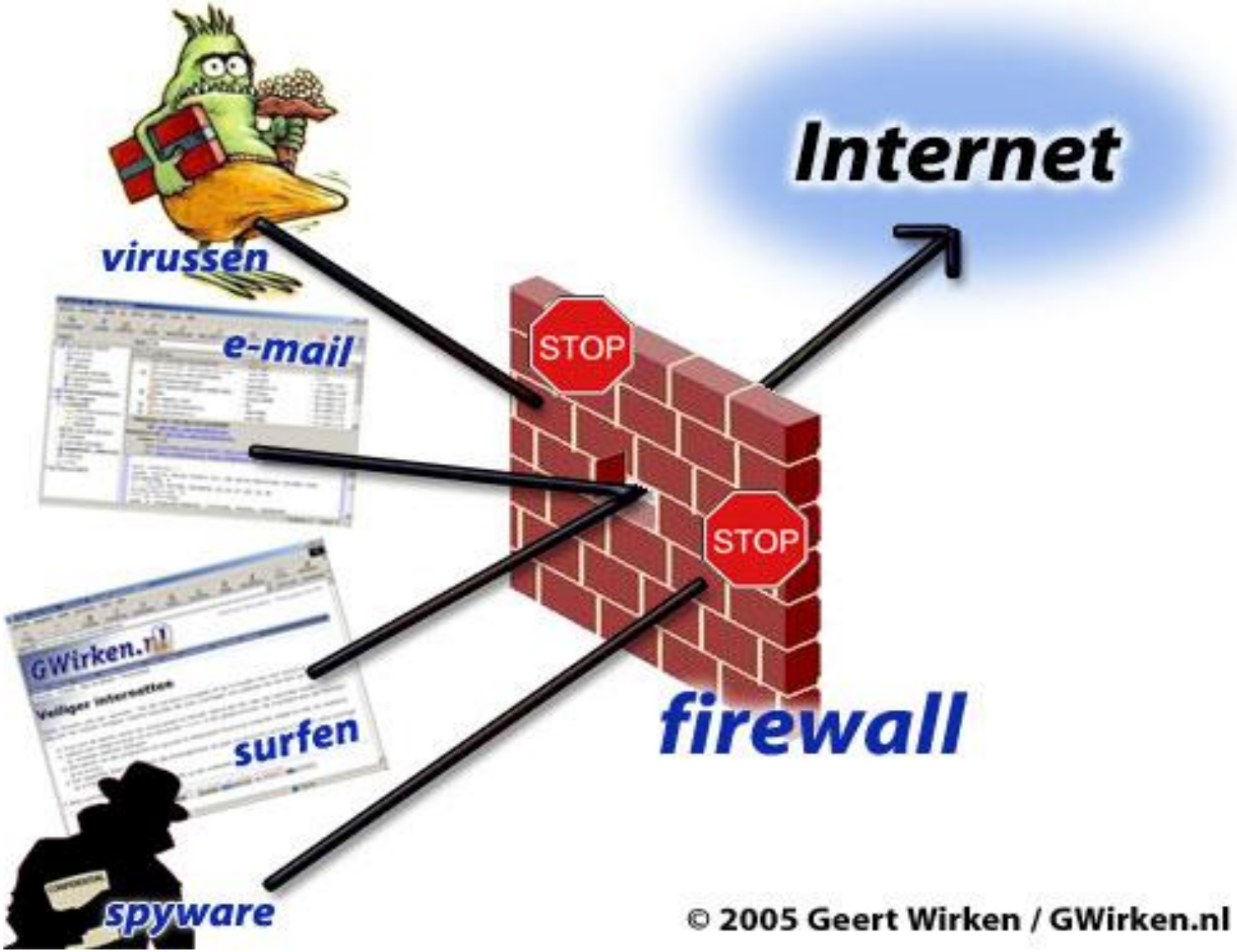
- Application security **controls** are techniques to enhance the security of an application at the coding level, making it less vulnerable to threats.

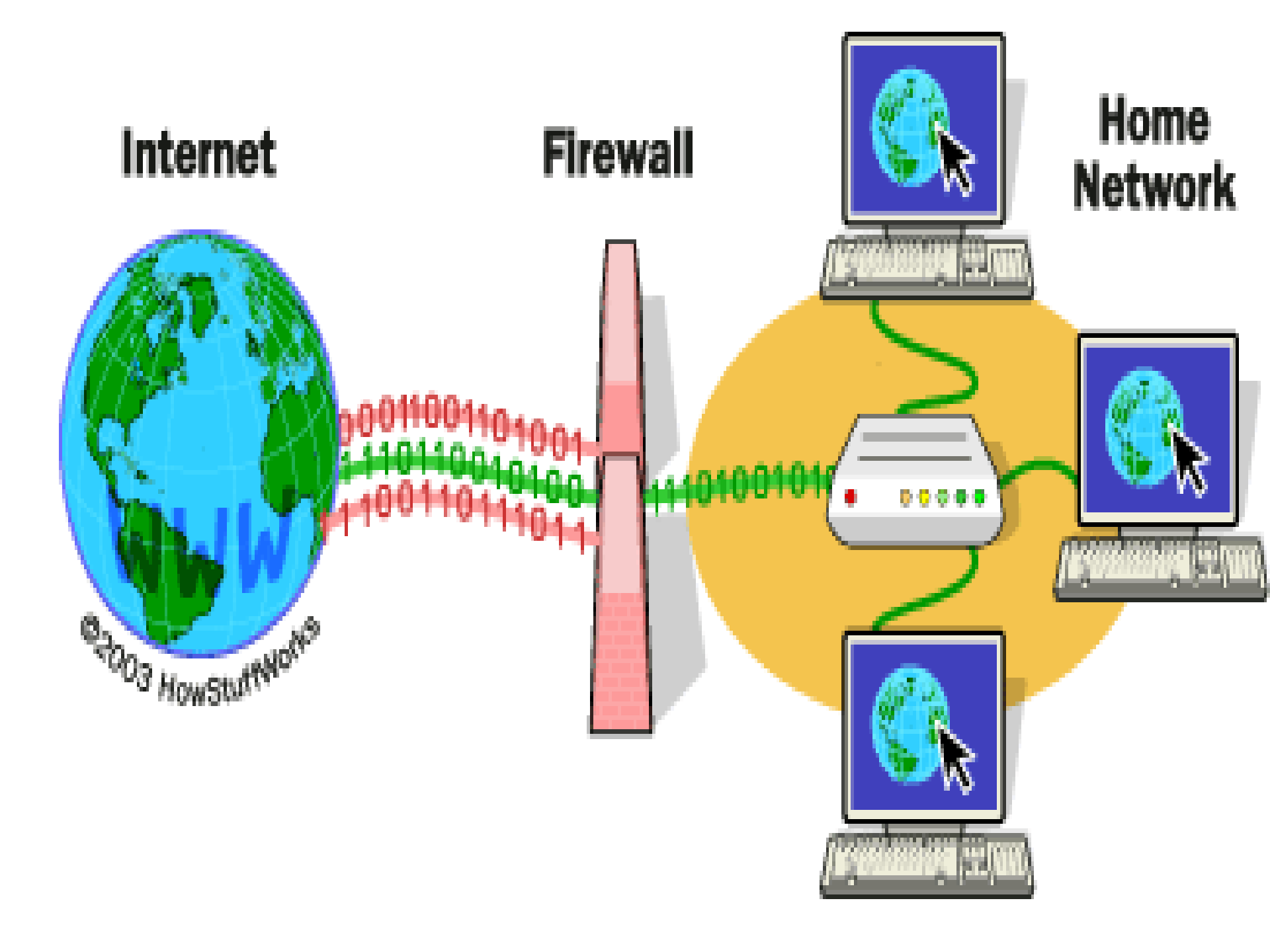
- **Email security** is ***a term for describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise***.
- Email is often used to spread malware, spam and phishing attacks.

Firewall

- A **FIREWALL** is simply a program or hardware device that *filters* the information coming through the Internet connection into your private network or computer system.

- If an incoming packet of information is *flagged* by the filters, it is not allowed through.


Internet
virussen
e-mail
STOP
STOP
GWirken.nl
surfen
firewall
spyware
© 2005 Geert Wirken / GWirken.nl


Internet
Firewall
Home Network
WWW
©2003 HowStuffWorks

- Firewalls use one or more of three **methods** to control traffic flowing in and out of the network:

- ***1. Packet filtering -*** Packets (small chunks of data) are analyzed against a set of **filters**. Packets that make it through the filters are sent to the requesting system and all others are discarded.

- ***2. Proxy service*** - Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.

- ***3. Stateful inspection*** - A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information.

- Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics.
- If the comparison yields a reasonable match, the information is **allowed** through.
- Otherwise it is **discarded**.

Firewall Configuration / Rules

- Firewalls are ***customizable***.

- This means that you can add or remove filters based on several conditions.

Some of these are:

- **i) IP addresses** - Each machine on the Internet is assigned a unique address called an IP address. IP addresses are 32-bit numbers, normally expressed as four "octets" in a "dotted decimal number." A typical IP address looks like this: 216.27.61.137.

- For example, if a certain IP address outside the company is reading too many files from a server, the firewall can block all traffic to or from that IP address.

- **ii) Domain names**

  You can only allow certain specific domain names to access your systems/servers or allow access to only some specified types of domain names or domain name extension like .edu or .mil.

- **iii) Protocols**

  A firewall can decide which of the systems can allow or have access to common protocols like IP, SMTP, FTP, UDP, ICMP, Telnet or SNMP.

- **iv) Ports** - Any server machine makes its services available to the Internet using numbered ports, one for each service that is available on the server.

- *For example*, if a server machine is running a Web (HTTP) server and an FTP server, the Web server would typically be available on port 80, and the FTP server would be available on port 21.
- A company might block port 21 access on all machines but one inside the company.

- **v) Keywords**

  Firewalls also can filter through the data flow for a match of the keywords or phrases to block out offensive or unwanted data from flowing in.

Types of Firewall

- ***Software firewalls***

  New generation Operating systems come with built in firewalls or you can buy a firewall software for the computer that accesses the internet or acts as the gateway to your home network.

- ***Hardware firewalls***

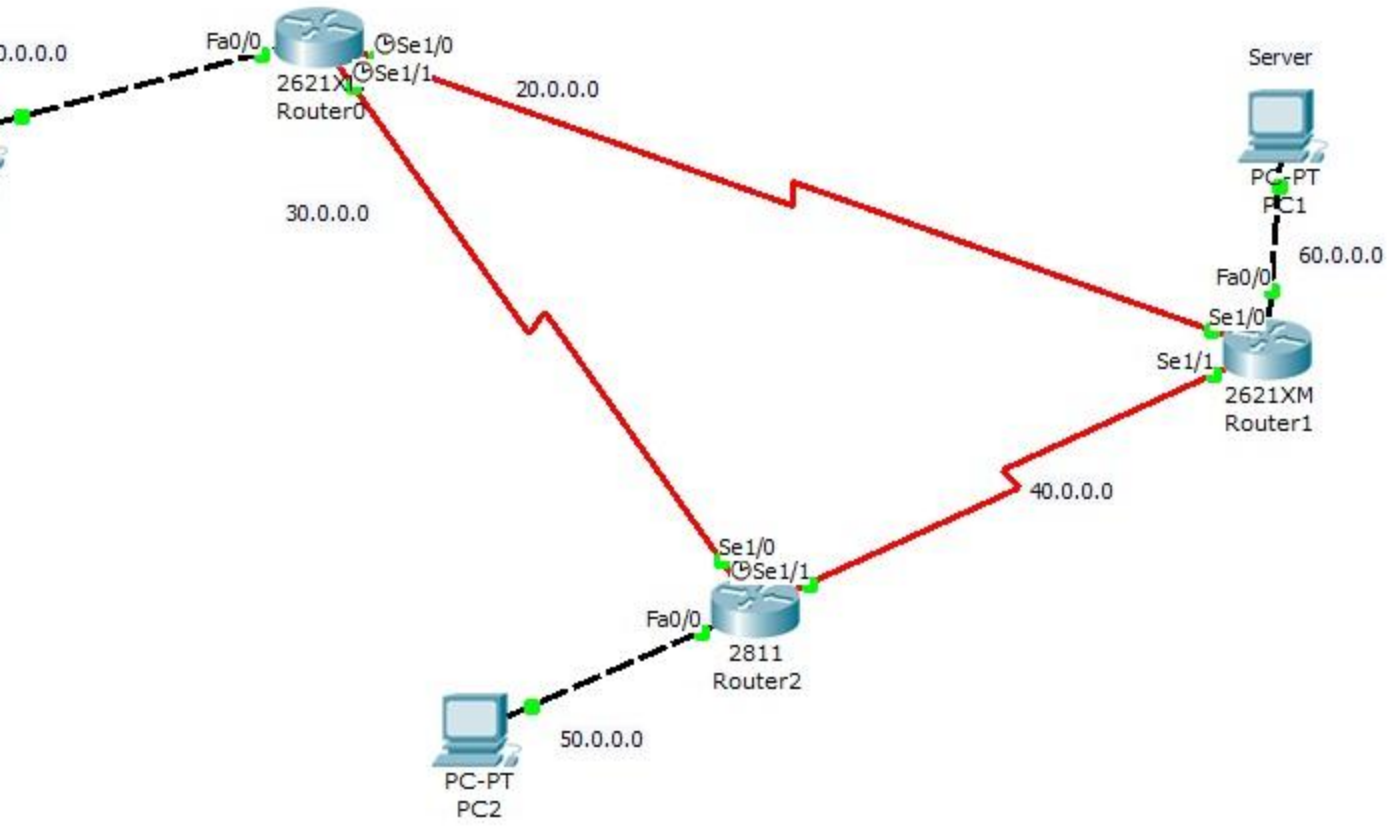
  Hardware firewalls are usually routers with a built in Ethernet card and hub.

- Your computer or computers on your network connect to this router & access the web.

hi\Cisco Packet Tracer 5.3.2\saves\Firewall.pkt

Extensions Help

New Cluster Move Object Set



Standard Access-List near to destination

```
Router>enable
Router#config t
Router(config)#access-list 1 permit 10.0.0.0 0.255
Router(config)#interface fa0/0
Router(config-if)#ip access-group 1 out
```

Devices Fast Forward Time

2620XM 2621XM 2811 Generic Generic

Scenario 0

New Delete

Toggle PDU List Window

Fire	Last Status	Source	Destination	Type	Colo
	Successful	PC0	PC1	ICMP	
	Failed	PC2	PC1	ICMP	

- An **inbound** firewall protects the network against **incoming traffic** from the Internet or other network segments, namely disallowed connections, malware and denial-of-service attacks.
- An **outbound** firewall protects against **outgoing** traffic originating inside an enterprise network.

If the Windows Firewall is turned off then it will have no effect, and the Inbound and Outbound rules will mean nothing.

- Inbound rules: These are to do with other things accessing your computer. If you are running a Web Server on your computer then you will have to tell the Firewall that outsiders are allowed to connect to it.
- Outbound rules: These are so that you can let some programs use the Internet, and Block others. You will want to let your Web Browser (Internet Explorer, Firefox, Safari, Chrome, Opera...) have access to the Internet, so you will tell Windows Firewall that it's allowed.

To create an inbound rule

- On the computer that is running the Microsoft Dynamics NAV Web Server components, on the **Start** menu, choose **Control Panel**, choose **System and Security**, and then choose **Windows Firewall**.
- In the navigation pane, choose **Advanced settings**.
- In the **Windows Firewall with Advanced Settings** window, in the navigation pane, choose **Inbound Rules**, and then in the Actions pane, choose **New Rule**.
- On the **Rule Type** page, choose **Port**, and then choose the **Next** button.
- On the **Protocol and Ports** page, choose **Specific local ports**, and then enter the port number. For example, enter 8080 for the default port of the Microsoft Dynamics NAV Web client.
- Choose the **Next** button.
- On the **Action** page, choose **Allow the connection**, and then choose the **Next** button.
- On the **Profile** page, choose the profiles, and then choose the **Next** button.
- On the **Name** page, type a name for the rule, and then choose the **Finish** button.

To create an outbound port rule

- 1. Open the Group Policy Management Console to Windows Firewall with Advanced Security.
- 2. In the navigation pane, click **Outbound Rules**.
- 3. Click **Action**, and then click **New rule**.
- 4. On the **Rule Type** page of the New Outbound Rule wizard, click **Custom**, and then click **Next**.

- 5. On the **Program** page, click **All programs**, and then click **Next**.
- 6. On the **Protocol and Ports** page, select the protocol type that you want to block. To restrict the rule to a specified port number, you must select either **TCP** or **UDP**. Because this is an outbound rule, you typically configure only the remote port number.
- If you select another protocol, then only packets whose protocol field in the IP header match this rule are blocked by Windows Firewall. Network traffic for protocols is allowed as long as other rules that match do not block it.
- To select a protocol by its number, select **Custom** from the list, and then type the number in the **Protocol number** box.
- When you have configured the protocols and ports, click **Next**.

- 7. On the **Scope** page, you can specify that the rule applies only to network traffic to or from the IP addresses entered on this page. Configure as appropriate for your design, and then click **Next**.
- 8. On the **Action** page, select **Block the connection**, and then click **Next**.
- 9. On the **Profile** page, select the network location types to which this rule applies, and then click **Next**.

- 10. On the **Name** page, type a name and description for your rule, and then click **Finish**.

- **System Security:** General System Security Threats, Hardware and Peripheral Devices, OS and Application Security, Virtualization, System-Based Security Applications, Understanding Linux Security, System Monitoring and Auditing.

General System Security Threats

Types of Threats

- Interception: an unauthorized subject has gained access to an object, such as stealing data, overhearing others communication, etc.
- Interruption: services or data become unavailable, unusable, destroyed, and so on, such as lost of file, denial of service, etc.
- Modification: unauthorized changing of data or tempering with services, such as alteration of data, modification of messages, etc.
- Fabrication: additional data or activities are generated that would normally no exist, such as adding a password to a system, replaying previously send messages, etc.


Spyware
Trolan
&Key Logger
Virus &
Worm
Browser
Helper Object
Adware
& Malware
Back Door
Malicious
Software
Dialer & Hijacker
Email-Worm/Virus

What is computer virus?

Computer virus refers to a program which damages computer systems and/or destroys or erases data files

Basic Computer Viruses

- **Spyware** is a **software** that aids in gathering information about a person or organization **without their knowledge** and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge

Trojan Horse is a type of Spyware

- Trojan Horses
  - appears as interesting program file but when installed it allows intruders to access and read your files

Worms

- Worm is a virus that **copies and multiplies** itself by using computer networks and security flaws
- A **worm** is also a destructive program that fills a computer system with self-replicating information, clogging(block) the system so that its operations are slowed down or stopped

- a **backdoor** refers to any method by which authorized and unauthorized users are able to get around normal security measures and gain high level user access (aka root access) on a computer system, network, or software application.
- Once they're in, cybercriminals can use a backdoor to steal personal and financial data, install additional malware, and hijack devices.

- **Browser Helper Object, BHO** is a helper object added to your Internet browser.
- For example, the Google Toolbar is considered a Browser Helper Object.
- This add-on enables users to perform Google searches through the toolbar and contains additional features that help improve a user's experience.
- Although most BHO's are helpful, some can also be malicious and hijack your browser to visit sites he or she may not want to visit, track your viewing habits, etc.
- These Browser Help Objects are often considered spyware or malware.

- ***Adware*** is unwanted software designed to throw advertisements up on your screen, most often within a web browser.

- **Malware** (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants.

Signs Your Computer is Infected (Detection)

- Functions slower than normal
- Responds slowly and freezes often
- Restarts itself often
- See uncommon error messages, distorted menus, and dialog boxes
- Notice applications fail to work correctly
- Fail to print correctly

Prevention

- Upload and use antivirus software
- Be aware of the e-mails and attachments you open
- Check for updates on antivirus software regularly
- Make sure antivirus software is installed correctly

Actions to prevent virus infection

Always update your anti-virus software at least weekly.

Back up your important files and ensure that they can be restored.

Change the computer's boot sequence to always start the PC from its hard drive

Actions to prevent virus infection

Don't share Drive C: without a password and without read-only restrictions.

Empty floppy drives of diskettes before turning on computers, especially laptops.

Actions to prevent virus infection

Forget opening unexpected e-mail attachments, even if they're from friends

Get trained on your computer's anti-virus software and use it.

Have multiple backups of important files. This lowers the chance that all are infected.

Actions to prevent virus infection

Install security updates for your operating system and programs as soon as possible.

- ***ADDITIONAL READING IS STRONGLY RECOMMENDED***

References

- https://www.barracuda.com/glossary/intrusion-detection-system
- https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/
- https://www.accessagility.com/blog/understanding-intrusion-detection-and-prevention-systems
- https://phoenixnap.com/blog/best-network-security-tools
- https://www.vmware.com/topics/glossary/content/application-security.html