



آموزش نتورک پلاس

Security Technologies

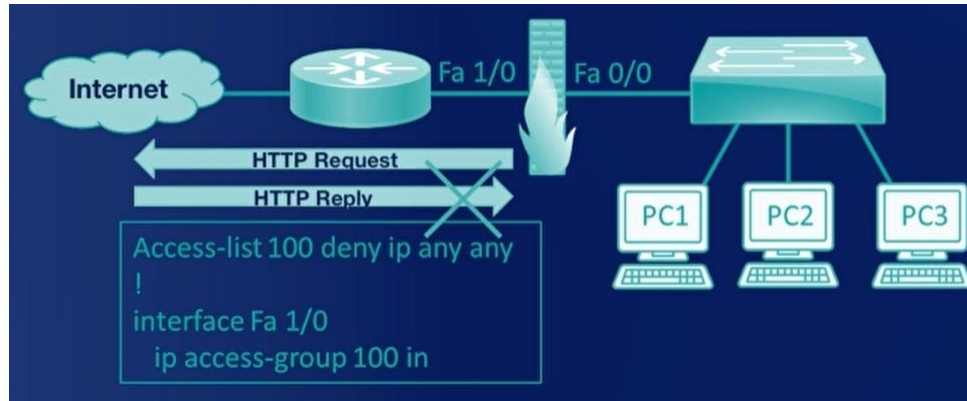
Firewall

- » Software or Hardware
- » Virtual or Physical
- » Host-based or Network-based
- » NAT and PAT



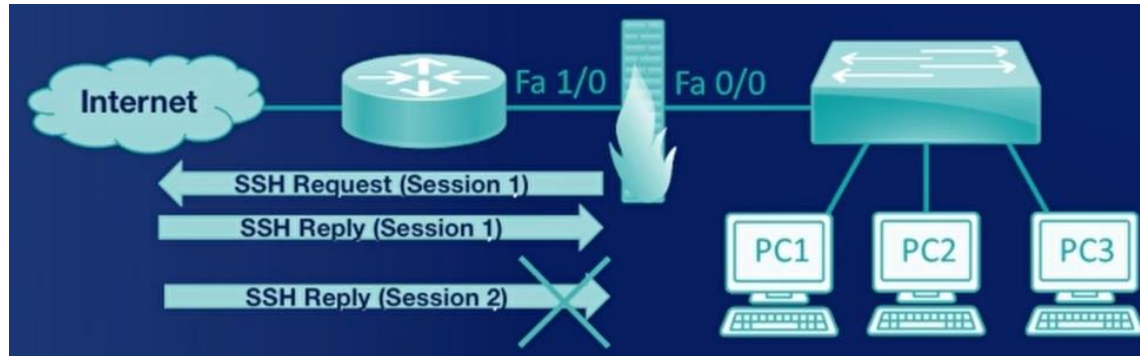
Packet-Filtering Firewall

- » Permits or denies traffic based on packet header



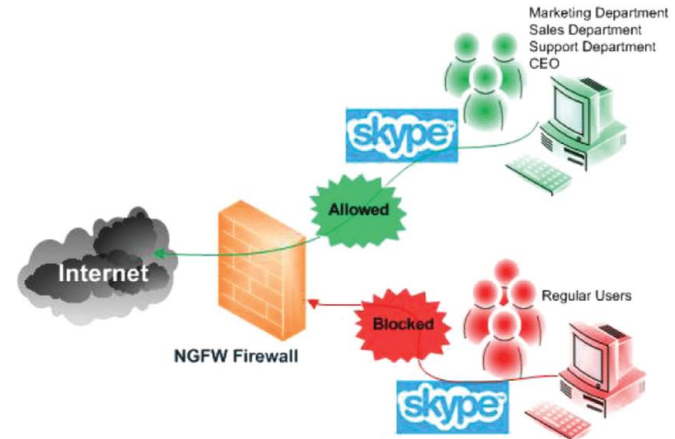
Stateful Firewall

- » Inspects traffic as part of a session and recognizes where the traffic originated.



NextGen Firewall (NGFW)

Third-generation firewall that conducts deep packet inspection and packet filtering.



Access Control List (ACL)

Set of rules applied to device (Switch, Router, Firewall) interfaces that permit or deny certain traffic.

- » Src/Des MAC
- » Src/Des IP
- » Src/Des Port
- » VLAN

Access Control List (ACL)

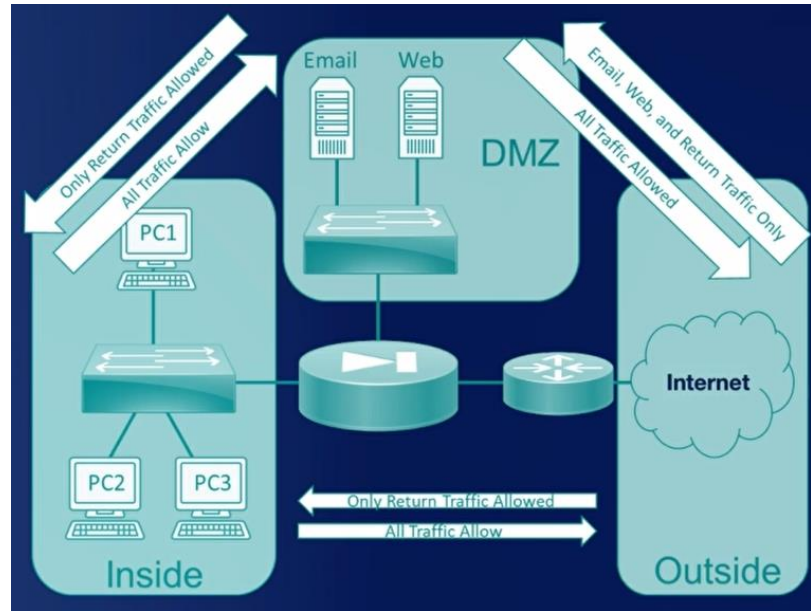
Explicit and implicit denies

Guest list

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____
11. _____
12. _____

Firewall Zone

- » Inside
- » Outside
- » DMZ



Unified Threat Management (UTM) Device

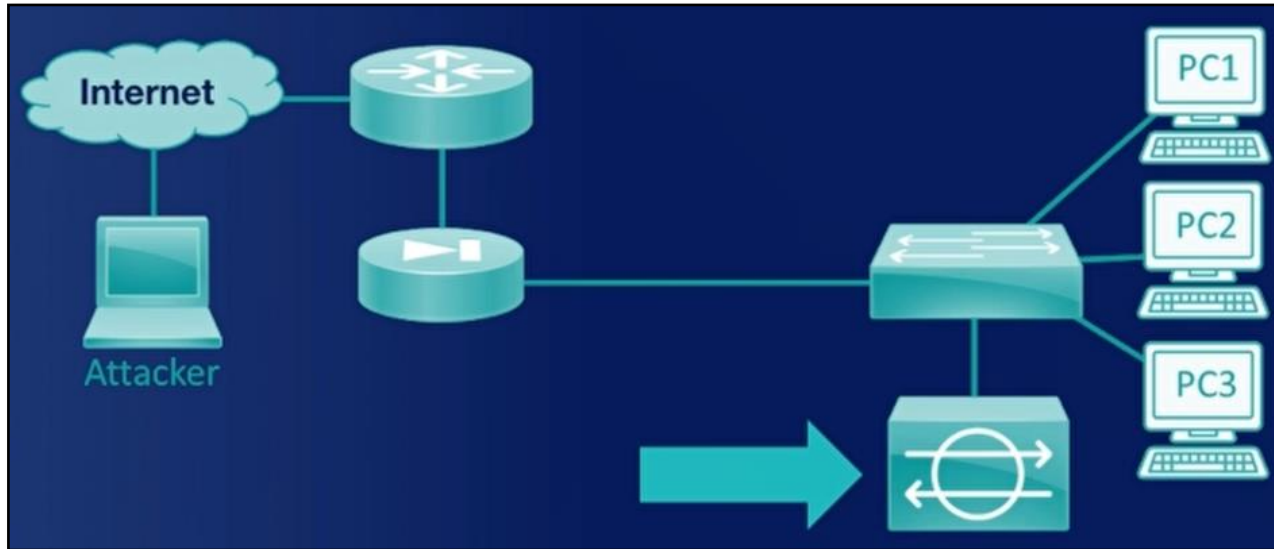
- » Combines firewall, router, IDP, IPS, Anti-malware, and other features into a single device.



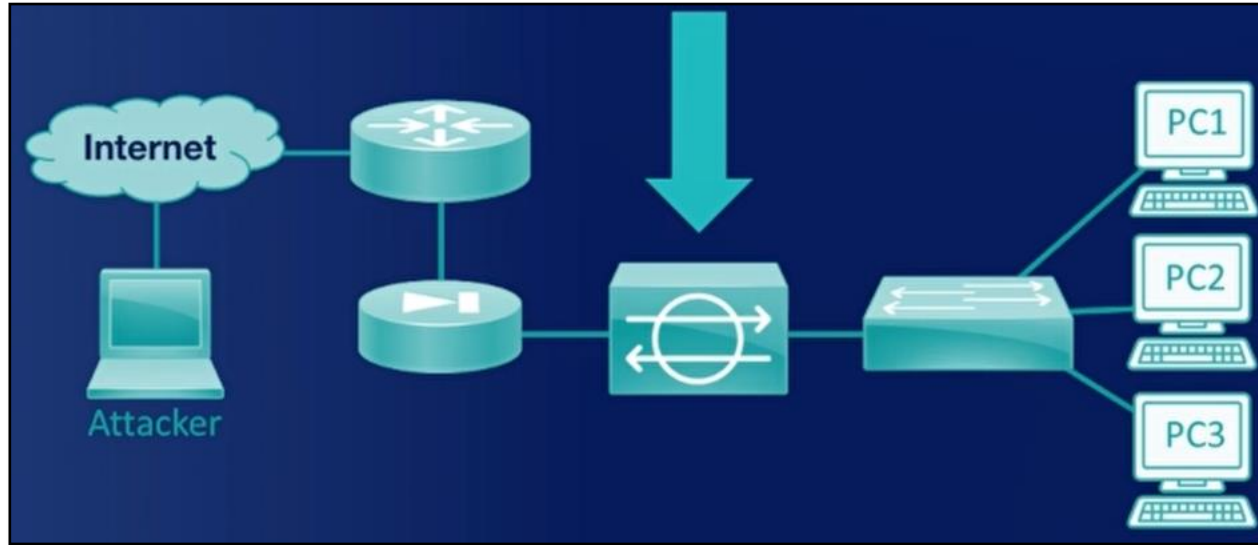
Hands-on with Firewalls

- » Windows
- » Modem Router

Intrusion Detection System (IDS)



Intrusion Prevention System (IPS)



Detection Methods

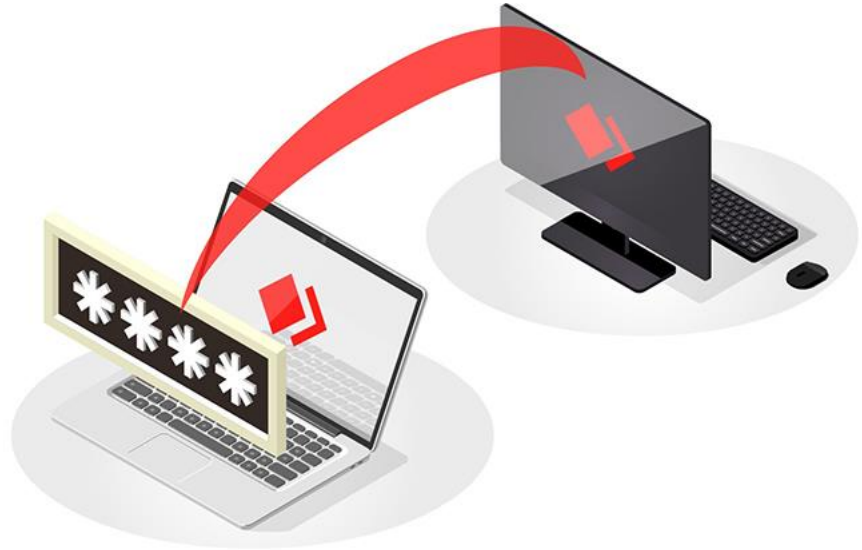
- » Signature-based
- » Policy-based
- » Anomaly-based

IDS and IPS

- » Host-based
- » Network-based

Remote Access

- » Telnet
- » SSH
- » RDP
- » RDG
- » VNC
- » VPN
- » VDI



Telnet (Teletype Network)

- » TCP port 23
- » Sends text-based commands to remote devices and is a very old networking protocol.

SSH (Secure Shell)

- » TCP port 22
- » Encrypts everything that is being sent and received between the client and the server.

RDP (Remote Desktop Protocol)

- » TCP port 3389
- » Provides graphical interface to connect to another computer over a network connection.

RDG (Remote Desktop Gateway)

- » Provides a secure connection using the SSL/TSL protocols to the server via RDP.

VPN (Virtual Private Network)

- » Establishes a secure connection between a client and a server over an untrusted public network like the Internet.

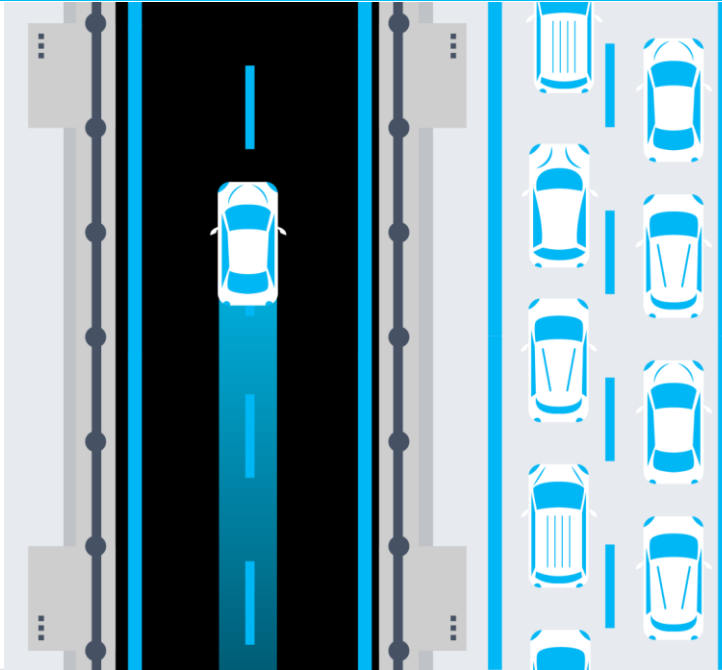
VNC (Virtual Network Computing)

- » Port 5900
- » Designed for thin client architectures and things like Virtual Desktop Infrastructure.

VDI (Virtual Desktop Infrastructure)

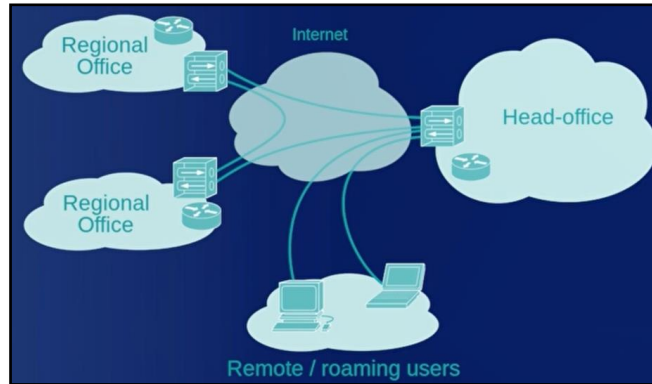
- » Hosts a desktop environment on a centralized server.

In-Band Management vs Out-Of-Band Management



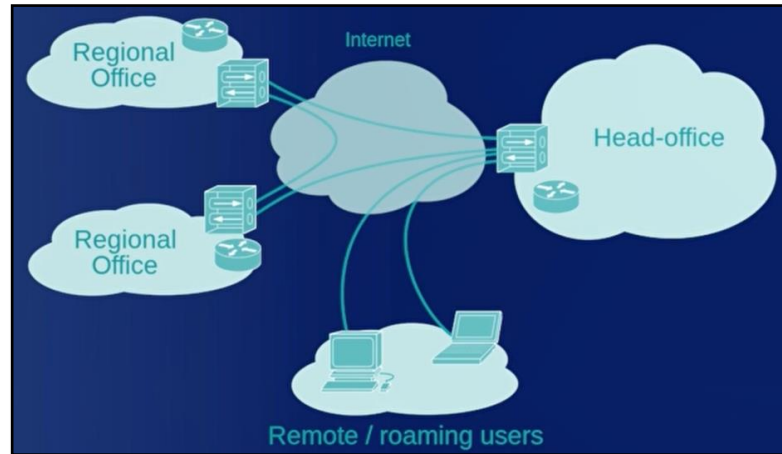
Virtual Private Network (VPN)

- » Extends a private network across a public network and enables sending and receiving data across shared or public networks.



Virtual Private Network (VPN)

- » Site to site
- » Client to site
- » Clientless (SSL,TLS,DTLS)
- » Full tunnel vs Split tunnel

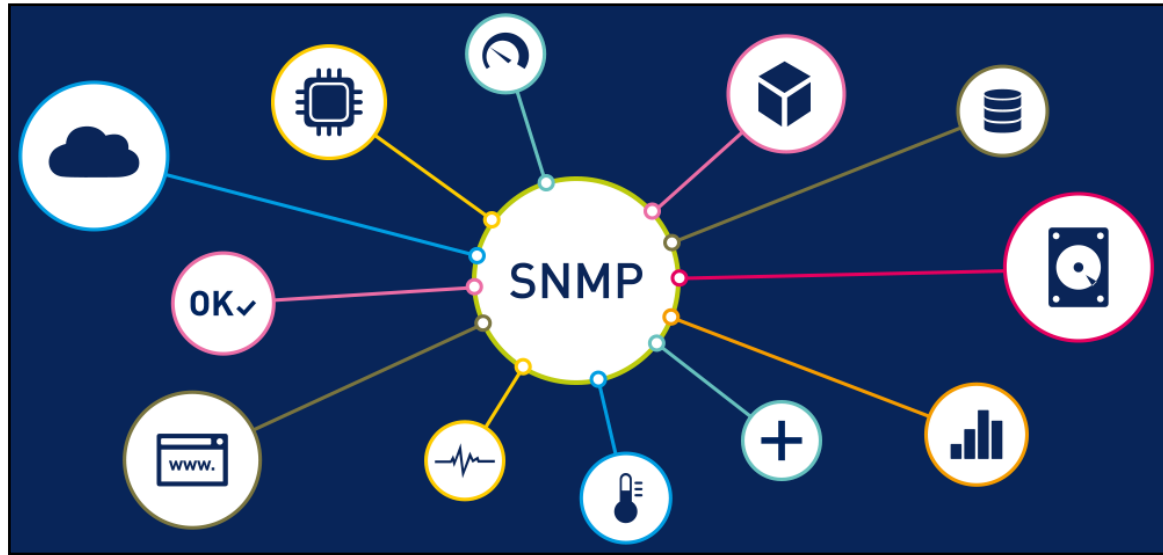


IP Security

- » Provides authentication and encryption of packets to create a secure encrypted communication path between two computers.

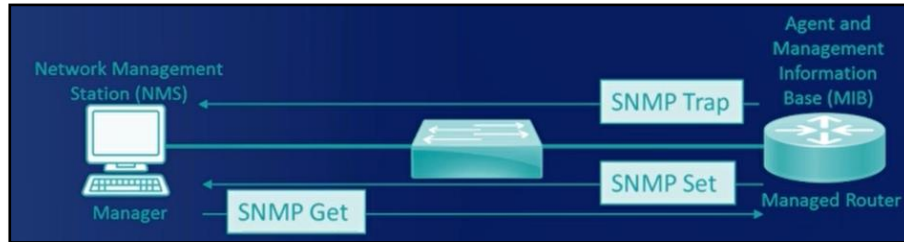
Protection	Method
Confidentiality	Using data encryption
Integrity	Ensuring data is not modified in transit
Authentication	Verifying parties are who they claim to be
Anti-Replay	Checking sequence numbers on all packets prior to transmission

Simple Network Management Protocol (SNMP)



Simple Network Management Protocol (SNMP)

» SNMP v1, v2, v3



System Logging Protocol (Syslog)

- » Sends system log or event messages to a central server, called a syslog server.

Level	Condition	Indication
0	Emergency	The system has become unstable
1	Alert	A condition should be corrected immediately
2	Critical	A failure in the system's primary application requires immediate attention
3	Error	Something is preventing proper system function
4	Warning	An error will occur if action is not taken soon
5	Notice	The events are unusual
6	Information	Normal operational message that requires no action
7	Debugging	Useful information for developers

Security Information and Event Management (SIEM)

- » Provides real-time or near-real-time analysis of security alerts generated by network hardware and applications.



عباس ولی زاده

مدرس دوره های شبکه و امنیت