CompTIa 4

**""""you can **dig **o query dns servers to verify that the dns server is reachable and verify that a dns server can resolve hostnames to ip addressess.. these tools can verify that a dns server has a host record that maps a hostname to an ip adress for a web server.. just like ns lookup.. dig verifies dns functionality.

nslookup -querytype=mx gegapremium.com
(((identify mail servers for gegarpremium)))
the lowest preferentce number(10) identifies the primary server..

```
└─$ nslookup -querytype=mx google.com
Server: 75.75.75.75
Address: 75.75.75.75#53

Non-authoritative answer:
google.com mail exchanger = 10 smtp.google.com.

Authoritative answers can be found from:
smtp.google.com internet address = 142.250.9.27
smtp.google.com internet address = 142.250.9.26
smtp.google.com internet address = 173.194.219.27
smtp.google.com internet address = 173.194.219.26
smtp.google.com internet address = 64.233.185.26
smtp.google.com has AAAA address 2607:f8b0:4002:c11::1a
smtp.google.com has AAAA address 2607:f8b0:4002:c11::1b
smtp.google.com has AAAA address 2607:f8b0:4002:c03::1b
smtp.google.com has AAAA address 2607:f8b0:4002:c03::1a
```

nslookup and dig are 2 command line tools use to test DNS Microsoft systems include nslookup and linux systems include dig. they can be query specific records such as mail servers when a sustem as multiple mail servers the lowest number preference identifies the primary mail server

.subscription use

quality of service.. refers to the technologies running on a network that measure and control different traffic types..

unicast

one to one traffic..
broadcast one to all traffic.

sWITCH can learn which computers are attached to each of its physical ports. it then uses this knowledge to create internal switch commands. when two computers talk to each other.

security benefit of switch. """ a pentester can install a protocol analyzer can stop data to a specific port. switch reduces the risk of an attacker capturing data. increases iefficien of network.

Posr security limits the computers that can connect to physical ports on a switch.

**port security includes disabling unused ports and limiting the number of mac adress per port a more advance implementation is to restict each physical port to only a single specific mac adresses. **

**A physical port used by a network device, such as a switch or a router, is entirely different from the logical ports discussed previously .. you plug in a cable into a physicla port.. a locigal port is a number embedded packet and identifies services and portocols.
this is like minute and minute.
study hashcat, md5sum network +

The secretary of defense directed members of different services to securetthe building. rg**

**MC FILTERING IS ANOTHER EAMPLE OF PORT SECURITY IN A SIMPLE IMPLEMENTATION THE SWITCH REMEMBTERS THE FIRST ONE OR TWO MAC ADDRESSES THAT CONNECTG TO A PORT.

broadcast storem and loop prevention.. ******
this floods the netrowk with traffic and can effectively disable a switch it also degrades the performance.

this is trivial for many netwokrk admins most current switches hace spanning tree protocol... stp pr newer Rapid stp installed and enabled.
**broadcast storm and loop prevention such as stp or rstp is a necessary to protect against switching and loop problems. such as those caused when two ports of a switch are connected together.
**

Bridge protocol data unit guard
stp uses bpdug messages in a network to detect loops when the loops are detected stp sthuts down or blocks traffic from switch ports sending redundant traffic switches exchange bpdu messages with each other using their non edge ports.
MAC BRIDGING?

ACL'S are rules implemented on a router, and on firewalls to identify what traffic is allowed and what traffic is denied. Rules within an ACL provide rule based management for the router and control inbound and outbound traffic. router acls provide basic packet filetering. they filter packets based on ipa ddresses ports, and some protocols such as icmp or ipsec. based on the protocol identifieers.

IP addresses and networks. you can add a rule in the ACL block.
you can fileter fraffic based on logical ports. for example if you want to block https traffic you ca create a

rule to block traffic outgoing traffic or both.

you can fileter traffic based on logical ports.

ROUTERS AND STATELESS FIREWALLS OR PACKET FILTERING FIREWALLS PERFORM BASIC FILTERING WITH AN ACCESS CONTROL LIST. acl IDENTIFY WHAT TRAFFIC IS ALLOWED AND WHAT TRAFFIC IS BLOCKED . AN acl CAN CONTROL TRAFFIC BASED ON NETWORKS SUBNETS iop ADDRESS PORTS AND SOME PROTOCOLS IMPLICIT DENY BLOCKS ALL ACCESS CONTROL LIST. ..
**host based firewall
A FIREWAL FILTER, INCOMING AND OUTGOING TRAFFIC FOR A SINGLE HOST R BETWEEN NETWORKS IN OTHER WORDS A FIREWALL CAN ENSURE ONLY SPECIFIC TYPES OF TRAFFIC ARE ALLOWED INTO A NETWORK.

software vs. hardware firewalls

Host based firewalls provide protection for individual hosts, such as servers or workstations. A host based firewall provides intrusion protection for the host. linux systems support xtables for firewall capabilitiies Network based firewalls are often dedicated servers and provide protetion for the network. '
**stateless firewall rules
**

use rules implemented in ACLs to identify allowed and blocked traffic. thisis similar to how a router uses rules within acls fire3walls use an implicity deny strategy to block traffic

FIREWALLS USE A DENY ANY ANY DENY ANY OR DROP ALL STATEMENT AT THE END OF THE ACL TO ENFORCE AN IMPLICIT DENY STRATEGY THE STATEMENT FORCES THE FIREWALL TO BLOCK ANY TRAFFIC THAT WASNT PREVIOUSLY ALLOWED IN TE ACL

'A WEB APPLICATION FIREWALL SPECIFICALL DESINED TO PROTECT A WEB APPLICATION. a web server and web server clients.

a STATEFUL FIREWALL**
inspects traffic and makes decisions based on traffic context or state. it keeps track of established sesisons inspects traffic based on its state within a session and it blocks traffic that isnt part of a established connection**

a stateless fireall blocks traffic using an acl and stateful firewall blocks traffic based on the state of the packet within the session web application firewalls provide strong protection for web servers they protect agains severel diff types of attacks focusing on web application attacks.

NGFW ----NEXT GENERATION FIREWALL. ;;;;; an advanced firewall that adds capabilities that arent availabie in first generation or second generation firewalls. the first generation of firewalls were packet filtering. using stateless, and could only allow or block traffic after evaluating individual packets.

a nfgw performs deep packet inspection adding applicationlevel inspection as a coref feature the ngfw is aware of common application protocols. such as ftp and http.

NETWORK DESIGNS.

iNTRANET=== AN INTERNAL NETWORK. pEOPLE USE THE INTRANET TO COMMUNICATE AND SHARE CONTENT WITH EACH OTHER WHILE ITS COMMON FOR AN INTRANET TO INCLUDE WEB SERVERS IT IS NOT A REQUIREMENT.

EXTRANET===== IS A PART OF A NETWORK THAT CAN BE ACCESSED BY AUTHORIZED ENTITIES FROM OUTSIDE OF PARTENERS CUSGOMERS VENDORS OR OTHERS.

SCREENED SUBNET
also known as a demiilitarized zone or DMZ a buffered zone between a private network and the internet. Attackers seek out servers on the internet so any server placed directly on the internet has the highes amount of risk.

A Screened subnet is a buffer zone between the internet and an internal network. It allows access to services while segmenting acces to the internal network. in other words, internet cliencts can access the services hosted on servers in the screened subnet but the screened subnet provides a layer of protection for the intranet(internal network)

Network Address Translation Gateway
... a protocol that translates puplic ip adry used form of NAT is network adress and port translation commonly called pORT address translation.

ess to private address back to public..
a network adress translation gateay hosts NAT and provides internal clients with private IP adresses a path to the internet. INSTEAD of using NAT gateway its also a possible to enable NAT on an internet facing firewall a commonl

PUBLIC IP ADDRESSES DONT NEED TO BE PURCHASED FOR ALL CLIENTS.

NAT HIDES INTERNAL COMPUTERS FROM THE INTERNET

STATIC NAT USES SINGLE PUBLIC IP ADRESS IN A ONE ON ONE MAPPPING. IT MAPS PRIVATE IP ADDRESS WITH A SINGLE PUBLIC IP ADDRESS.

DYNAMIC NAT USES MUILTPLE PUBLIC IP ADRESSES IN A ONE TO MANY MAPPING dYNAMICNAT DECIDES WHICH PUBLIC IP ADRESS TO USE BASED ON THE LOAD.

**NAT TRANSLATEDS PUBLIC IP ADDRESSES TO PRIVATE IP ADDRESSES AND PRIVATE IP

```
ADDRESSES BACK TO PUBLIC  A COMMON FORM OF NAT IS PORT ADDRESS TRANSLATION
DYNAMIC NAT USES MUILIPLE PUBLIC IP ADDRESS WHILE STATIC NAT USES SINGLE
PUBLIC IP ADDRESSES.****strong text***
```

PHYSICAL ISOLATION AND AIR GAPS.. ----------ENSURES THAT ONE NETWORK IS NOT CONNECTED TO ANOTHER NETWORK. CONSIDER supervisory control and data acquisition SCADA systems THese are typically industiral control systems within large facilityies such as power plants or water treatment. an AIR GAP privides physical isolation . with a gap of air between an isolated system and other systems*

*_an air gap isolates one network from another from ensuring there is physical space. literally a gap of air between all system and cables. **strong text**_

Logical seperation and segmentation**

routers/firewalls provide a basic level of seperation. *

Segmentation with a virtual local area network.

isolating traffic with VLAN

uses a switch to a group of several different computers into a virtual network. you can group the computers based on depts. job functions.

virtual local are networks seperate or segment traffic on physical networks and you can create multiple vlans with a single layer 3 switch a VLAN can logically group several different compters together or lgically seperate compters without regard to their physical locations vlans are also used to seperate traffic types such as voice traffic on one vlan and data traffic on a seperate vlan.

East-West traffic refers to traffic between servers. traffic between clients and servers is north to south.

A zero trust network is a network that doesnt trust any devices by default even if tt ws previously verified. ....

Network appliances are diedicated systems designed to fulfill a specific need. the intent of the word applance is to evoke a sense of simplicity
firewall, proxy.. ""ect.

Proxy servers;;;;;;;; to gorward requests for services such as http https from clients they can imporve performance by caching content and soem proxy servers can restic users access to inappropriate websites. administrators configure internal clients to us e proxy server for specific protocols.

caching content for performance. ....the proxy server increases the performance of the internet requests by caching each result received from the internet.

REVERSE PROXY ACCEPTS REQUESTST FROM THE INTERNET. TYPICALLY FOR A SINGLE WEB SERVER.-----iT APPEARS TO CLIENCTS AS A WEB SERVER BUT IS FORWARDING THE REQUESTS TO THE WEB SERVER AND SERVING THE PAGES RETURNED BY THE WEB SERVER.

**WHEN USED WITH A WEB FARM IT CAN SCT AS A LOAD BALANCER YOU WOULD PLACE A LOAD BALANCER IN THE SCREENED SUBNET TO ACCEPT THE REQUESTS THEN FORWARDS THE REQUESTS TO DIFFERENT SERVERS IN THE WEB FARM USING A LOAD BALANCING ALGORITHM.

A**PROXY SERVER FORWARS REQUESTS FOR SERVICES FROM A CLIENT IT PROVIDES CASHING TO IMPROVE PERFORMANCE AND REDUCE INTERNET BANDWITDTH SUAGE. TRANSPARENT PROXY SERVERS USE URL FILTERS TO RESTRICT ACCESS TO CERTAIN SITES.

UNIFIED THREAT MANAGEMENT.****** IS A SINGLE SOLUTION THAT COMBINES MULTIPLE SECURITY CONTROLS. tHE OVERALL GOAL OF UTMS TR PROVIDE BETTER SECURITY WHILE ALSO DIMPLIFYING MANAGEMENT REQUIREMENTS IN MNY CASES A UTM DEVICE WILL REDUCE THE WORKLOAD OF ADMINISTRATORS WITHOUT SACRIFICING SECURITY.

Url filtering. url filters within a utm security appliance perform the same job as a proxy server they block access

Malware inspection often comes into a network via spam or malicious webpages. the malware inspection component of a utm appliance screes incoming data for knwn malware and blocks it.

content inspection

Content inspection includes combination of different content filters it monitors incoming data streams and attempts to block any malicious content.

**A unified threat management appliance combines multiple security controls ina a single appliance. they can inspect data streams and often include URL filtering malwre ispectiona and content inspection components many utms include ddos mitigator to blockk ddos attacks. **

ddos mitigator attemtps to detect ddos attacks and block them this is similar to how intrusion prevention systems(ips)block attacks

It is common to put utm appliances at the border

**A Jump server is placed between different security zones and providessecure access from devices in one zone todevice in the other zone it can provide secure access in devices in a screenes subnet from an internal network. **

```
ssh -j maggie@jump maggie@ca1
```

**connecting a jump server using a passwordless ssh

Security implications of ipv6 on ipv4 networks.
Simple Network Management Protocol version 3 snmpv3 MONTIROS AND MANAGES NETWORK DEVICES such as routers or switches this includes using snmp3 to modify the devices configuration

**Administrators use SNMP3 to manage and monitor network devices and SNMP uses udp PORTS 161 and 162 SNMPV3 encrypts credentials before sending them over the network and is more secure than earlier versions. **