3.3

Thursday, September 21, 2023 4:03 PM

Extranet - give access to auth users for priv resources

NAT hides IP addresses, not proxy

Application firewall

- app layer (layer 7)
- stateful multilayer inspection
- deep packet inspection

usually installed as app
can also be on UTM

VIP virtual IP

each server node has own
for load balancing

each server

IP but for load balancing

it advertises VIP

Clients go to IP or FQDN

and are routed accordingly

Gateway Load Balancing Protocol GLBP

load balance w/ VIP

CISCO

Common address redundancy protocol

similar to GLBP

agentless = mobile

non persistent/dissolvable may not

work for mobile

firewall does not scan for malware

Switches that support QoS use 802.1p header to prioritize frames

Out-of-band management - remote management of system

ex: console connection to router

Switch loop causes net connections to drop; packet can't make loop to next switch

also causes broadcast storms

dummy client switches deployed = no advanced config like:

- MAC filter
- port security

basic and let traffic flow freely

broadcast storms - when bridged net contains loop and broadcast traffic amplified by other switches

DHCP snooping - inspect traffic on access ports to ensure host isnt spoofing MAC addr

Bridge protocol data unit BPDU prevents BPDUs from comm network topology info on access ports

collector - combines multiple sensors to collect internet traffic for processing in IDS

reverse proxy can publish specific apps

Reverse proxy can publish specific apps from corp net to internet by listening for specific client requests

HTML5 VPN - uses web browsers to access/manage desktop w/ little lag

Clientless remote desktop gateway

L2TP requires VPN agent

web server farm

- persistent sessions will help for particular services but when using multiple wont help
- scheduling only good for Active/Active

- VIP ensures smooth trans to secondary load balancer

East-west traffic - network and platform configs that support Cloud and other internet services where most traffic is between servers in data center

Zero trust - continuous auth and conditional access to mitigate privilege escalation and account compromise

DMZ is North/south - to and from data centers

aggregation switch - connect multiple subnets to reduce # of active ports

subnets connected to switch, not router

correlation engine part of SIEM that captures and examines logged events to alert admins

VPN concentrator encorporates encrypt and auth to create VPN