PAN Academy Module 1

CCDC Scored Services

HTTP/HTTPS: Request for web page will be made. Once the req is made, result will be stored and compared.

* Matching needed for awarded points

SMTP: Email sent and received through valid email via SMTP. Simulate an employee using their email.

* Each successful test of email functionality will be awarded points
* Must always be able to support either unauthenticated sessions or sessions using AUTH LOGIN (base64).

POP3: Simulated user connection will be made where the user logs in using valid userid and password and checks for mail

* Must accept logins as described in the critical service description

SSH: SSH session will be initiated to simulate a vendor account logging in to check error logs

* Each successful login and log check will be awarded points.

SQL: A SQL request will be made to the database server. The result will be stored and compared against an expected result.

* Each successfully served SQL request will be awarded points

DNS: DNS lookups will be performed against the DNS server.

* Each successfully served request will be awarded points.

FTP: Connections are made to the FTP server (anonymous or valid user, depends on description) to check for presence and availability of specific files.

Hardware Firewall

MGT port: retrieve licenses and signature from updates, used to access WebUI and SSH commandline

IP: 192.168.1.1

Lock down everything: Console port is better because you have to physically there.

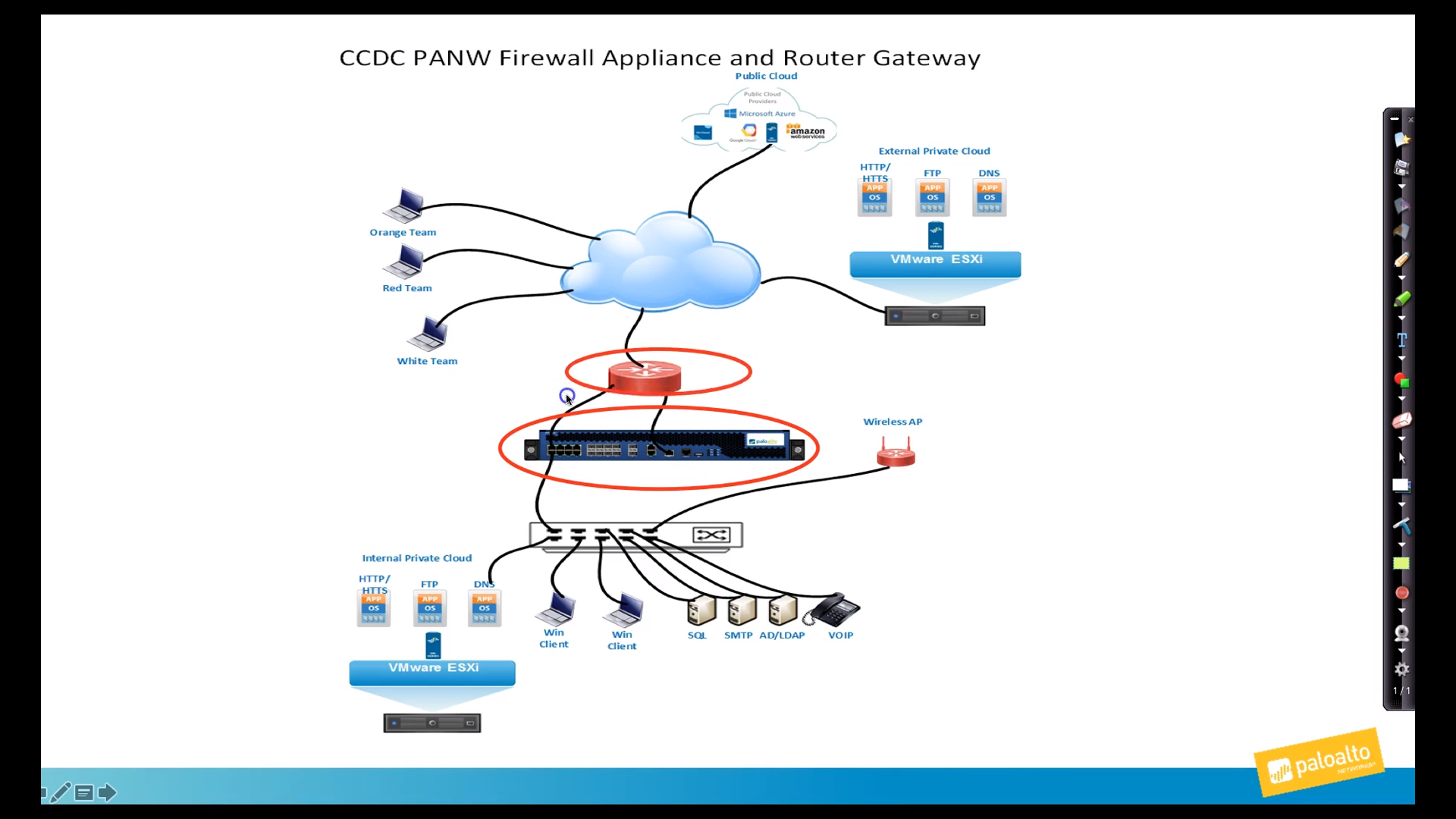
MGT Port doesn’t have tpo be used for updates.

2 ways of Hardware Firewall

VM Firewall web UI + commands are the same.

Deployment scenario both as firewall and gateway. Because support OSPF BGP,

Deploted alongside with a gateway router.



MgtInt

* 2 primary functions
  + Connects to the update server (by default, can change)
    - Licensing
    - Signatures, vuln
    - URL/Web categories (If there is bad domains -> block and catergorize bad domains)
  + Configuration
    - Web-UI
    - SSH-CLI (can do everything)
    - Can close down MGT port for config and config everything through console via cmd.
      * Web UI provides graphic view of firewall log
      * MIND YOUR LOGS
    - MgtInt has an open port = target for Red Team
      * Lock down through console port
        + Change password
        + Make sure no other users using it
        + Only allow certain IP Address to access the Web UI

Services

* In Public Cloud, External Private Cloud, Internal Private Cloud, Bare metal machines
* Have Virtual Firewall for Clouds and Physical for bare metal
* Source of Threats:
  + Red Team (Ext – Int) (North-South traffic)
    - => Build a wall (lul) i.e Firewall
  + Not the case for only NS traffic.
  + East – West traffic (Client -> Services)
  + => Trust zones/networks
  + => NO TRUST ZONES => Zero trust.
    - Don’t trust anything in DMZ, Internal, traffic between, etc.
    - Have all the traffic goes through the firewall
  + How to filter traffic:
    - Security policies
    - Default policies
      * Block everything and only allow what you want
      * Match packet to rules
      * If not match -> default (block)
    - At least inspect and block traffic
      * Configure network so that everything between zones goes through firewall.
      * Connect each of machines to the port (not enough)
      * Trunking (VLAN trunks)
      * May not have control over the switch
        + Require a lot of practice
        + Can practice on Virtual
      * Separate port groups connecting to firewall appliance
      * => Separate zones and zero trust

Part 2

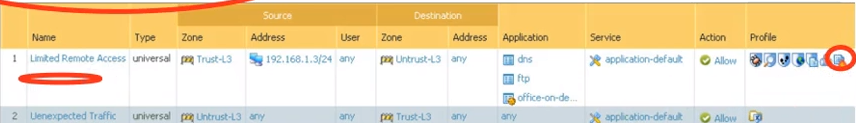
* Same configuration, WEB UI and command for virtual or physical
* MGT port
  + By default has to be internet facing port to download signatures and license firewall appliance
  + By default where you access webUI
  + WebUI quicker than CLI
  + WebUI better view of log
  + Secure Mgt Int if face IntConnected ports
  + Change default behavior from MGT to Data ports
  + So data port downloading signatures
  + Add signatures from client computer that connects to update server and upload to firewall appliance
  + Quicker and easier if Mgt connects internet facing port
* Cyber Attack Lifecycle
* Disrupt any lifecycles
  + Reconnaissance
    - Scanning
    - Firewall can defend against scanning
      * Config zone protection profile
      * Assign it to external zone
      * Configure the firewall so if receive so many scans from IP then block it
        + Careful, if block legit IP as red team can camouflage
      * Can consume resources if continuously blocking
      * Easier to allow scanning and monitor
  + Weaponization
    - FW can’t do anything
  + Delivery (Firewall can disrupt)
    - FW can be instrumental
    - May enter the room and malware already in the client
    - Not have time to configure
    - Block the delivery known attacks
  + Exploitation
    - Through browsers, pdf, word or phishing
    - Can’t do much
  + Installation
    - Can’t do much either
    - Remove log info
    - Reg key
    - Persistence
  + Command and Control
    - FW can protect
    - Malware will try to connect to command center to get commands
    - Configure FW to block traffic that exfiltrating data (data filtration, security profile)
  + Act on Objective
    - FW can protect
    - Same as above

Firewall BEST PRACTICES

1. Complete visibility of traffic
   1. Know applications for allow
      1. Custom Apps
      2. NS traffic or EW traffic
      3. Know what traffic to allow coming in and what traffic running in the system
      4. Allow applications that let scored services up and running
         1. In public cloud, private cloud, etc.
   2. SSL Decryption (Decryption Module)
      1. Have it buried malware if can’t decrypt
      2. Configure decryption policy on firewall to decrypt traffic
      3. Decrypt SSH + SSL traffic
      4. Important to detect malware
      5. 50-60% traffic in SSL
      6. May not decrypt all
         1. HIPPA
         2. Commerce
            1. => PCI Compliance
         3. If in EU then can’t decrypt anything
         4. If can’t decrypt then host intrusion detection system is important
            1. Memory forensics
         5. Any App that use Cert-pinning
            1. From inside to outside
            2. FW proxy cert
   3. User-ID (User-ID Module)
      1. Not enough IP Address, what user are doing
2. Reduce attack surface area
   1. Whitelist Applications
      1. App = anything that can be detected, monitored and blocked
      2. App-ID to detect app by signatures
      3. Sig downloaded by MgtInt
      4. Add in sec policy
   2. Creating Custom App-ID’s
   3. Dynamic address lists and groups
      1. Traditionally used to blocking traffic
         1. Not sure of blocking efficiency since red team can IP Address
      2. Any changes to lists can be updated auto in sec policy
   4. SSL Protocol Settings
      1. Decryption policy
         1. TLS version
         2. Block bad/expired certs
   5. Security Policies
      1. List of rules
         1. Rule order is important
         2. Deny or allow
         3. If no match then go down rules and then default
            1. Block everything if different zones
         4. Default policy in same zone = allow
         5. When set up default, only allow this traffic to a particular IP address
         6. Only server = aligning IP address
      2. Stateful
         1. Inbound sec policy is allowed then outbound is allowed
3. Protect against known attacks
   1. Assign security profiles to firewall security policies
      1. Anti-virus profile
      2. Vulnerability profile
      3. Anti-Spyware
      4. File blocking
      5. URL -> URL Filtering Module
      6. All in Content-ID Module
   2. Protect against DoS
      1. Zone protection profile -> zone external
      2. DoS profile and policies -> Servers
      3. Be very careful it might be too restrictive
   3. Sec Profile = additional rules
      1. Anti-Virus
         1. Get updates everyday
      2. Anti-Spyware
         1. Weekly
      3. Vulnerability
         1. Weekly
      4. URL Category
         1. Stored in cache memory
         2. If can’t connect to update server => cache expired
         3. If the url accessing isn’t in the cache, then consult update server. If can’t then return unknown
         4. Prevent DNS beacon attacks
            1. When Red team registers a domain
            2. Might take a while for firewall to catergorize
            3. Malware query to the registered DNS and tries to connect
            4. There might be a time period server not recognized

Prevent = unknown category = block

* + 1. All rely on signatures

1. Protect against unknown attacks
   1. WildFire Security Profile -> WildFire Module
      1. White Team might help Red Team (Phishing?)
      2. Make a copy to MgtInt, send to WildFire sandbox
         1. Send down to FW a report
         2. Generate a signature to block
            1. Within 5 mins
            2. Employ by make sure AV SP is using WildFire signature (must configure)
      3. The original is allowed through firewall and into the client.
         1. => Check WildFire Report to clean up Client
2. First steps:
   1. Secure MgtInt using Console port
      1. Hypervisor on VM
      2. Practice CLI
         1. Change password
         2. Permitted IP control list to restrict access
         3. Get rid of any unsafe services
            1. Telnet
            2. HTTP
            3. SNMP
         4. Should have services:
            1. HTTPS
            2. SSH
            3. Ping
         5. Admin Users created before entered => delete it if not needed using CLI
   2. Advice: It’s nice to be nice lmao