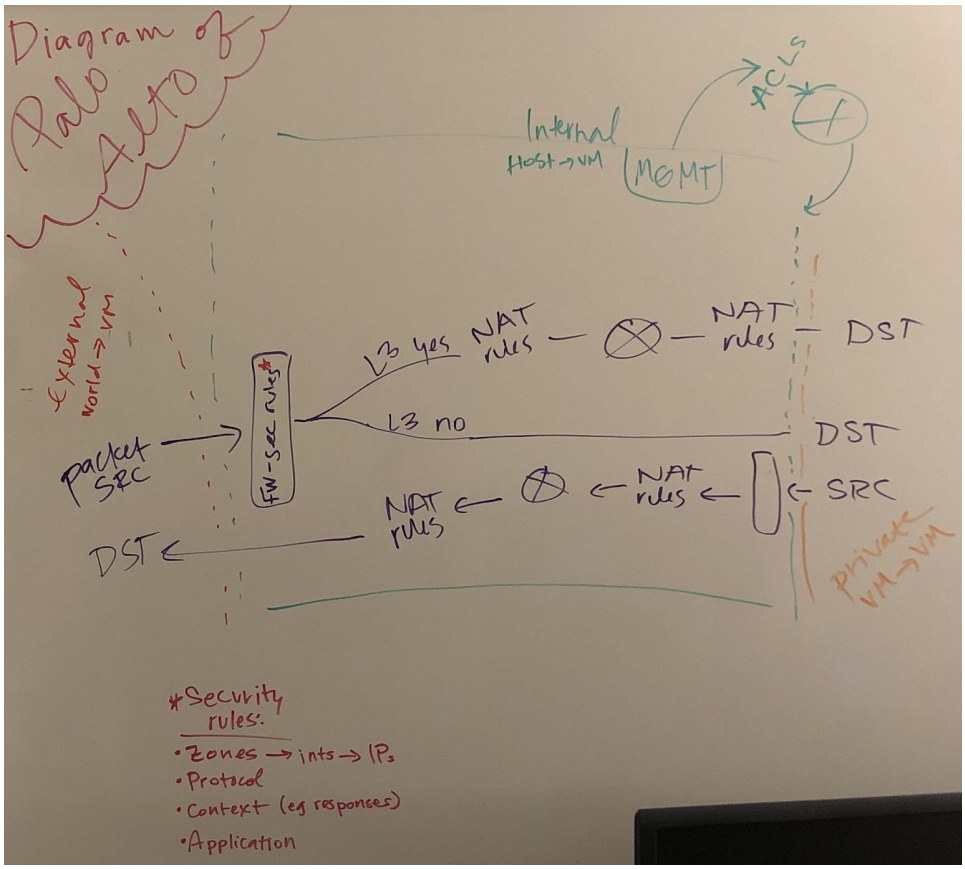
Palo Alto Firewalls

***************More specific rules must precede the more general ones (rules are evaluated top to bottom)***************
Configure mode prompt: #, normal mode prompt: >

DON'T FORGET TO COMMIT

1. Find management IP: `show interface management`
   ****Web GUI is only accessible via HTTPS****
   No web gui: knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cli0CAC
   a. Set static management IP address:
      `configure, set deviceconfig system type static, set deviceconfig system ip-address <ip address> netmask <netmask> default-gateway <default gateway> dns-setting servers primary <DNS ip address>`
      i. Set static IP: Device -> Setup -> Interface -> Management
      ii. Set DNS server: Device -> Setup -> Services
      iii. Go to the new IP you set to manage the firewall
2. Change passwords:
   a. Admin: Device -> Admins -> Click on username, change password
      i. `configure, set mgt-config users admin password`
      ii. Other admins: `show admins, delete mgt-config users <admin>`
   b. Local Users: Device -> Local User Database
      i. `show user user-ids all`
      ii. `configure, set mgt-config users <name> password`
   c. Adding a new user:
      ```
      configure
      set mgt-config users <name> password
      set mgt-config users <name> permissions role-based <role profile>
      ```
3. Check for user certificates: see guide
4. Check for SSH keys: see guide
5. ACL for accessing management interface: Device -> Setup -> Interfaces -> Management
   `configure, set deviceconfig system permitted-ip <ipaddress/netmask>`
6. Go through Network tab to get a better understanding of what's going on
   `show config running`
7. Check security rules: Policies -> Security
   a. Disable rules allowing unneeded services
   b. These rules are applied top to bottom
   c. Remember that these rules are evaluated after DoS Protection Policies
   d. Overall vision for applying security policies:
      i. Create a grouping (could be an object/zone/whatever…)
      ii. Create security profiles (can group security profiles into a security profile group)
      iii. Apply policies using security profiles/security profile groups
8. Check NAT rules: Policies -> NAT
9. Check port forwarding rules: Policies -> Policy Based Forwarding
10. Check service definitions (someone may've bound a bad port to a service): Objects -> Services
11. Prevent defined attacks: Objects -> Enable Security Profiles

Basic Life of A Packet in Palo Alto:



Zone Types:

TAP: Monitor traffic. Use with SPAN and RSPAN.
Virtual Wire: “transparent firewall”
Layer 2: Switch between 2+ networks
Layer 3: Route between 2+ networks. Interfaces need to be assigned an IP address for this to work.

Other things to do:

- Block people from logging into web mgmt...even if they can see it’s there

- Check for API key:

https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-panorama-api/pan-os-xml-api-request-types/pan-os-xml-api-request-types-and-actions.html

- Watch for data exfiltration:
  - Objects -> Data Patterns
  - Objects -> Data Filtering

VPN Setup:

https://docs.paloaltonetworks.com/globalprotect/7-1/globalprotect-admin/globalprotect-quick-configs/remote-access-vpn-certificate-profile
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClFoCAK

Basic hardening guides:

https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClIaCAK
https://www.cisecurity.org/benchmark/palo_alto_networks/ -> register with a spam email for free

Overall Layout:

ACC: (Application Command Center)

Network Activity
Threat Activity
Blocked Activity
Tunnel Activity
**sort of like an ELK. Analyze intel within network

Monitor:

Logs
Packet Capture
App Scope (Change Monitor, ACC, Traffic Map)
Session Browser
Botnet
Reports
**more of the raw data available than in ACC

Policies:

Security: usual ufw type rules
NAT: NAT rules
QoS: set quality of service (bandwidth, limits on http, etc) rules
Policy Based Forwarding: port forwarding, usually used with NAT. Has precedence over routing table.
Decryption: Decrypt traffic that uses encryption
Tunnel inspection: inspect traffic that is unencrypted...could be session stuff, lets you check traffic that didn't have tunnel shutdown immediately
Application override: define application, allow/deny through for specific IPs/zones/whatever
Authentication: "you have to use duo auth, etc"
DoS Protection: deny specific IPs. Evaluated before security policies.
Identify the egress interface for applications that you want to receive QoS treatment. Add a QoS policy rule. Add a QoS profile rule. Enable QoS on a physical interface. Commit.

Objects:

- Addresses
- Address Groups
- Regions
- Applications
- Application Groups
- Application Filters
- Services
- Service Groups
- Tags
- GlobalProtect
  - HIP Objects
  - HIP Profiles
- External Dynamic Lists
- Custom Objects
  - Data Patterns
  - Spyware
  - Vulnerability
  - URL Category
- Security Profiles
  - Antivirus
  - Anti-Spyware
  - Vul Protection
  - URL Filtering
  - File Blocking
  - WildFire Analysis
  - Data Filtering
  - DoS Protection
    - https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-admin/threat-prevention/dos-protection-against-flooding-of-new-sessions/configure-dos-protection-against-flooding-of-new-sessions
- Security Profile Groups
- Log Forwarding
- Authentication
- Decryption - Decryption Profile
- Schedules

Network:

- Interfaces
- Zones (contains interfaces which contain IPs)
- VLANs
- Virtual Wires
- Virtual Routers
- IPSec Tunnels
- DHCP

- DNS Proxy
- Global Protect
- QoS
- LLDP
- Network Profiles
    - GlobalProtect IPSec Crypto
    - IKE Gateways
    - IPSec Crypto
    - IKE Crypto
    - Monitor
    - Interface Mgmt
    - Zone Protection
    - QoS Profile
    - LLDP Profile
    - BFD Profile

Device:

- Setup
    - Management
    - Operations
        - Revert, Save, Load, Export, Import
        - Reboot, Shutdown
    - Services
    - Interfaces
    - Telemetry
    - Content-ID
    - Wildfire
    - Session
    - HSM
- High Availability
    - General
    - Link and Path Monitoring
- Config Audit
- Password Profiles
- Admins
- Admin Roles
- Auth Profile
- Authentication Sequence
- User ID
    - User Mapping
    - Connection Security
    - User-ID Agents
    - Terminal Services Agents
    - Group Mapping Settings
    - Captive Portal Settings
- VM Info Sources
- Cert Mgmt

- Certificates
- Certificate Profile
- OCSP Responder
- SSL/TLS Service Profile
- SCEP
- SSL Decryption Exclusion

Response Pages
Log Settings
Server Profiles

- SNMP Trap
- Syslog
- Email
- HTTP
- Netflow
- RADIUS
- TACACS+
- LDAP
- Kerberos
- SAML Identity Provider
- MultiFactor Authentication

Local User Database

- Users
- User Groups

Scheduled Log Export
Software
GP Client
Dynamic Updates
Licenses
Support
Master Key and Diagnostics