Data-plane attacks and Mitigation Techniques:

1. **CAM Table OverFlow Attack (DoS attack)(macof –i eth0):** Port-Security

2. **DHCP Starvation Attack (DoS attack):** Port-Security and Rate-limiting requests.

3. **DHCP Spoofing/Rogue DHCP Attack (Mitm attack):** DHCP Snooping

4. **VLAN Hopping attack (negotiate trunk using DTP)(yersinia -G):** set all the ports not connected to switches to no-negotiate and access ports, as by default they are set to negotiate i.e. 'dynamic-auto'.

Also don't use vlan1 as native vlan.

5. **Rogue Switch Attack (Switch Mitm i.e. becomes the root bridge):** portfast and BPDU Guard (turned ON globally if the port is an access port)(shuts the port down).

BPDU Filter (Doesn't allow BPDUs, but doesn't shut the port down).

Root Guard (tell the switch that certain ports can't be root ports i.e. if you are connected to legitimate switches).

6. **Arp Spoofing/ARP Poisoning attack (Gratuitous ARP) (Mitm attack):** DAI (Dynamic Arp Inspection)

Classification of Firewalls:

Static packet-filtering (layer3)
Circuit-level (layer4)
Application layer (layers3,4,5,7)
Dynamic packet-filtering (stateful firewall) (layers 3,4,5)
Transparent firewalls (layer2)

STATELESS

Stateless firewalls watch network traffic, and restrict or block packets based on source and destination addresses or other static values. They are not 'aware' of traffic patterns or data flows. A stateless firewall uses simple rule-sets that do not account for the possibility that a packet might be received by the firewall 'pretending' to be something you asked for.

STATEFUL

Stateful firewalls can watch traffic streams from end to end. They are are aware of communication paths and can implement various IP Security (IPsec) functions such as tunnels and encryption. In technical terms, this means that stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, synchronization acknowledge or established), it can tell if the MTU has changed, whether packets have fragmented etc.

Password recovery ASA:

1. Press Ctrl+Break while router is powering up for router to go into ROMmon.
2. rommon 0>confreg 0x41 (default is 0x01) and rommon 1>boot
3. no to the initial setup script
4. R1#copy start run
5. ASA(config)#enable secret cisco
6. sh run aaa

no aaa authentication enable console LOCAL
no aaa authentication serial console LOCAL
no aaa authentication ssh console LOCAL
no aaa authentication command LOCAL
sh version
6. ASA(config)#config-register 0x01
7. ASA#copy run start
8. ASA#reload

Removing the existing Config:
ASA#write erase
ASA#reload
Factory default:
ASA(config)#config factory-default

Base Configuration:
Interface config:
ASA(config)#interface vlan 1
ASA(config-if)#nameif inside !(default security is 100)
ASA(config-if)#ip address 192.168.1.1 255.255.255.0
ASA(config)#interface Ethernet 0/0
ASA(config-if)#switchport access vlan 1
ASA(config-if)#speed 1000
ASA(config-if)#duplex full
ASA(config-if)#no shut

ASA(config)#interface vlan 2
ASA(config-if)#nameif outside !(default security is 0)
ASA(config-if)#ip address dhcp setroute
ASA(config)#interface Ethernet 0/1
ASA(config-if)#switchport access vlan 2
ASA(config-if)#no shut

ASA(config)#interface vlan3
ASA(config-if)#nameif dmz
ASA(config-if)#security-level 50

ASA(config)# nat (inside,outside) dynamic interface
ASA(config)#route outside 0 0 12.3.4.6

ASA(config)#object network obj_any
ASA(config-network-object)#subnet 0.0.0.0 0.0.0.0

Telnet:
ASA(config)#telnet 192.168.0 255.255.255.0 inside !(will accept connections from)
ASA(config)#passwd cisco
ASA(config)#telnet timeout 4 !(default is 5 mins)

SSH (Secure Shell):

ASA(config)#crypto key generate rsa modules 1024
ASA(config)#ssh 192.168.0 255.255.255.0 inside
ASA(config)#username user123 password password123
ASA(config)#aaa authentication ssh console LOCAL
ASA(config)#ssh timeout 4
ASA(config)# wr mem

ASDM (ASA Security Device Manager):

ASA(config)#http 192.168.130.0 255.255.255.0 inside
ASA(config)#http server enable

ACLs:

(same as IOS but it uses subnet mask instead of a wildcard mask)

Network Object Groups:

ASA(config)#object-group network Accounting
ASA(config-network-object-group)#network-object host 10.1.0.1
ASA(config-network-object-group)#network-object 10.2.0.0 255.255.0.0
ASA(config)#access-list demo2 permit tcp object-group Accounting any eq www
ASA(config)#access-list demo2 permit tcp object-group Accounting any eq 443

Applying an ACL:

ASA(config)#access-group demo2 in interface outside

NAT:

PAT:

ASA(config)#object-group network net-192.168.1
ASA(config-network-object-group)#subnet 192.168.1.0 255.255.255.0
ASA(config-network-object-group)#nat (inside,outside) dynamic interface

Static NAT:

ASA(config)#object-group network www-host
ASA(config-network-object-group)#host 192.168.1.2
ASA(config-network-object-group)#nat (inside,outside) static interface service tcp www www
ASA(config-network-object-group)#access-list outside_access_in permit tcp any host 192.168.1.2 eq www
ASA(config)#access-group outside_access_in in interface outside

IPSec Site to Site VPN:

ESP(Encapsulating Security Payload)
AH(Authentication Header)

HAGLE:

Hashing: MD5(Message Digest)(128bit),SHA-1(Secure Hashing Algorithm)(160bit)
Authentication: PSK,RSA Signatures
Group: DH(Diffie Hellman)(group2 1024bit)
Lifetime:
Encryption: DES(Data Encryption Standard)(56bit),3DES(168bit),AES(Advanced Encryption Standard)(128,192,256bit)

CLI Config:

Create an ACL:

ASA(config)#crypto isakmp enable outside
ASA(config)#object network net-local
ASA(config-network-object)#subnet 192.168.101.0 255.255.255.0
ASA(config-network-object)#object network net-remote
ASA(config-network-object)#subnet 192.168.102.0 255.255.255.0
ASA(config)#access-list outside_1_cryptomap permit ip object net-local object net-remote

Create and configure the tunnel group:

ASA(config)#tunnel-group 192.168.0.12 type ipsec-l2l
ASA(config)#tunnel-group 192.168.0.12 ipsec-attributes
ASA(config-tunnel-ipsec)#pre-shared-key password123
ASA(config-tunnel-ipsec)#isakmp keepalive threshold 10 retry 2

Configure Phase1:

ASA(config)#crypto isakmp policy 10 authentication pre-share
ASA(config)#crypto isakmp policy 10 encrypt aes
ASA(config)#crypto isakmp policy 10 hash sha
ASA(config)#crypto isakmp policy 10 group 2
ASA(config)#crypto isakmp policy 10 lifetime 86400

Configure Phase2:

ASA(config)#crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
ASA(config)#crypto map outside_map 1 match address outside_1_cryptomap
ASA(config)#crypto map outside_map 1 set pfs graoup2
ASA(config)#crypto map outside_map 1 set peer 192.168.0.12
ASA(config)#crypto map outside_map 1 set transform-set ESP-AES-SHA
ASA(config)#crypto map outside_map interface outside

Configure Nat:

ASA(config)#nat (inside,outside) 1 source static net-local net-local destination static net-remote net-remote
ASA(config)#route outside 0 0 192.168.0.12
sh run crypto
sh run object
sh run access-list
sh run tunnel-group
sh run nat
sh run route