Paloalto

High Availability

Version 10.0.0

Paloalto
HA Development

Definition:
→ HA stands for high availability which acts between two identical firewall that are placed in network which provides redundancy in case of a single point of failure on enterprise and data center network.
   ◊ *Paloalto stated that up to 16 firewalls can place in a group.*

HA Modes
- Active/Passive – one firewall actively manages the traffic while second firewall take a passively role, as soon as a path, link systems or network failed on first firewall then second firewall takes an active role to manage the all-same traffic and, in this mode both firewall sync to each other and share same configuration setting.

   ◊ *Active/passive supported in the v-wire, layer-2 and layer-3*

- Active/Active – If two firewall placed in the network then both pair will be in active state and processing the traffic work synchronously to handle session setup and session ownership. And each firewall maintains session tables and routing tables and sync each other.

   ◊ *Active/Active supported v-wire and Layer-3*

      - In this mode DHCP client doesn't support only active firewall can act as DHCP relay.
      - An active/active configuration does not load-balance traffic. Although you can load-share by sending traffic to the peer, no load balancing occurs. Ways to load share sessions to both firewalls include using ECMP, multiple ISPs, and load balancers.

Development:

Step 1:   we have two paloalto FW and make sure below parameter must match to each other.
- App version
- Threat version
- Antivirus version
- PAN-OS version
- GlobalProtect version
- Model version (VM or BareMetal)
- Type of interface
- Set of licenses

Topo

ET

e0/0

e0/2 ▶ INT-SW1

Du

e0/0

e0/2 ▶ INT-SW2

eth1/2

eth1/2

eth1/3
eth1/4
eth1/5

eth1/3
eth1/4
eth1/5

Data-Link 172.31.16.0/24 -Primary -eth1/3
Data-Link 172.31.17.0/24 -Backup -eth1/4

Control-Link 172.31.16.0/24 -Primary -eth1/5
Control-Link 172.31.17.0/24 -Backup -eth1/6

▶ Main_et

eth1/6

eth1/6

▶ DR_du

eth1/1

eth1/1

mgmt

Mgmt

e1/0

▶ SW

e0/0

e0/3

mgmt

Lan-subnet -10.10.1.0/24

e0/2

e0/1

▶ LAN-SW

e0/3

Gateway-10.10.1.100 on both FW

e0

▶ Win-lan

ᴇrif