FortiGate CLI Commands Documentation (8 Steps)

1. A1-HA (High Availability)

Device: HQ-Firewall2

Description: Configures HQ-Firewall2 as the secondary unit (priority 100) in the Active-Active (

```
config system ha
    set group-name "HQ"
    set mode a-a
    set hbdev "port3" 0
    set session-pickup enable
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
        edit 1
            set interface "port6"
            set dst 192.168.1.0 255.255.255.0
            set gateway 192.168.1.1
        next
    end
    set override disable
    set priority 100
    set monitor "port4" "port5"
end
```

2. LAG/LACP (Link Aggregation)

Device: HQ-Firewall2

Description: Creates a Link Aggregation Group named AggreLAN by bundling physical interfaces por

```
config system interface
    edit "AggreLAN"
        set vdom "root"
        set type aggregate
        set member "port1" "port2"
        set device-identification enable
        set lldp-transmission enable
        set role lan
    next
end
```

3. VLAN 10, 20 GW (HQ Perimeter FG)

Device: HQ-Firewall2

Description: Defines VLAN sub-interfaces on the AggreLAN interface to serve as the default gatew

```
config system interface
    edit "VLAN10"
```

```
        set vdom "root"
        set ip 10.1.1.1 255.255.255.0
        set allowaccess ping https
        set role lan
        set interface "AggreLAN"
        set vlanid 10
    next
    edit "VLAN20"
        set vdom "root"
        set ip 10.1.2.1 255.255.255.0
        set allowaccess ping https
        set role lan
        set interface "AggreLAN"
        set vlanid 20
    next
end
```

4. VLAN 30, 40 GW (DC Perimeter FG)

Device: DC-FG

Description: Defines VLAN sub-interfaces on the internal port (port1) to serve as the default ga

```
config system interface
    edit "VLAN30"
        set vdom "root"
        set ip 10.1.3.1 255.255.255.0
        set allowaccess ping
        set role dmz
        set interface "port1"
        set vlanid 30
    next
    edit "VLAN40"
        set vdom "root"
        set ip 10.1.4.1 255.255.255.0
        set allowaccess ping
        set role dmz
        set interface "port1"
        set vlanid 40
    next
end
```

5. The Two Groups Can Speak with Each Other (Inter-VLAN/Inter-Segment Communication)

Device: HQ-Firewall2 & DC-FG

```
DC-FG (Intra-Zone Communication):
config firewall policy
    edit 4
        set name "ToInternet"
        set srcintf "LAN"
        set dstintf "LAN"
        set action accept
        set srcaddr "Vlan30Network" "Vlan40Network"
        set dstaddr "Vlan30Network" "Vlan40Network"
        set schedule "always"
        set service "ALL"
    next
end

HQ-Firewall2 (LAN-to-DC Transit Communication Policies):
config firewall policy
    edit 1
        set name "LANToV40"
        set srcintf "LAN"
        set dstintf "TransitV40"
        set action accept
        set srcaddr "Vlan10Netowrk" "VLAN20 address"
        set dstaddr "Vlan40Network"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
    edit 2
        set name "LANTV30"
        set srcintf "LAN"
        set dstintf "TransitV30"
        set action accept
        set srcaddr "Vlan10Netowrk" "VLAN20 address"
        set dstaddr "Vlan30Network"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

6. All VLANs Access Internet (NAT Policies)

```
HQ-Firewall2:
config firewall policy
    edit 5
        set name "LANtoInternet"
        set srcintf "LAN"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "Vlan10Netowrk" "Vlan20Network"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

DC-FG:
config firewall policy
    edit 4
        set name "ToInternet"
        set srcintf "LAN"
        set dstintf "port2"
        set action accept
        set srcaddr "Vlan30Network" "Vlan40Network"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end

FG-DE:
config firewall policy
    edit 1
        set name "ToInternet"
        set srcintf "port4"
        set dstintf "virtual-wan-link"
        set action accept
        set srcaddr "all"
        set dstaddr "all"
        set schedule "always"
        set service "ALL"
        set nat enable
    next
end
```

7. SD-WAN Configuration

```
Device: HQ-Firewall2 & FG-DE

HQ-Firewall2 SD-WAN Zone & Service Rule:
config system sdwan
    set status enable
    config zone
        edit "virtual-wan-link"
        next
        edit "VPN-EG"
        next
    end
    config service
        edit 1
            set name "VPN"
            set dst "remote"
            set src "local"
            set priority-members 4 3
        next
    end
end
```

8. IPsec over SD-WAN Configuration

```
Device: HQ-Firewall2 & FG-DE

HQ-Firewall2:
```

```
config vpn ipsec phase1-interface
    edit "VPN-To-DE-Wan1"
        set interface "port4"
        set ike-version 2
        set local-gw 192.168.1.50
        set remote-gw 192.168.1.100
        set psksecret ENC XXXXXXXXXXXXXXXXXXX
        set proposal des-sha512
        set mode-cfg enable
    next
    edit "VPN-To-DE-Wan2"
        set interface "port5"
        set ike-version 2
        set local-gw 192.168.75.3
        set remote-gw 192.168.75.11
        set psksecret ENC XXXXXXXXXXXXXXXXXXX
        set proposal des-sha512
    next
end

config vpn ipsec phase2-interface
    edit "VPN-To-DE-Wan1"
        set phase1name "VPN-To-DE-Wan1"
        set proposal des-sha512
        set auto-negotiate enable
    next
    edit "VPN-To-DE-Wan2"
        set phase1name "VPN-To-DE-Wan2"
        set proposal des-sha512
        set auto-negotiate enable
    next
end

config system sdwan
    config members
        edit 3
            set interface "VPN-To-DE-Wan1"
            set zone "VPN-EG"
        next
        edit 4
            set interface "VPN-To-DE-Wan2"
            set zone "VPN-EG"
        next
    end
end

FG-DE:
config vpn ipsec phase1-interface
    edit "VPN-To-EG"
        set interface "port1"
        set ike-version 2
        set local-gw 192.168.1.100
        set remote-gw 192.168.1.50
        set psksecret ENC XXXXXXXXXXXXXXXXXXX
        set proposal des-sha512
    next
    edit "VPNtoEG-wan2"
```

```
        set interface "port5"
        set ike-version 2
        set local-gw 192.168.75.11
        set remote-gw 192.168.75.3
        set psksecret ENC XXXXXXXXXXXXXXXXXXX
        set proposal des-sha512
    next
end

config vpn ipsec phase2-interface
    edit "VPN-To-EG"
        set phase1name "VPN-To-EG"
        set proposal des-sha512
        set auto-negotiate enable
    next
    edit "VPNtoEG-wan2"
        set phase1name "VPNtoEG-wan2"
        set proposal des-sha512
        set auto-negotiate enable
    next
end
```