2 options for creating new FW:

1. Manually configure FW after TF creation – connect with ssh and manually run commands.
2. Create configurations in panorama for automatic bootstrapping.

\* This guide will show steps for option 2.

The newly created FWs will need an internet connection. We have 2 options:

1. We need to create Cloud NAT in order for the firewall to be able to connect to the internet, but ONLY at the start, while it is still being configured in order for it to allow access to Palo’s license, version, and overall configuration. After we end the creation process, we MUST REMOVE the Cloud NAT, (we dont want direct internet connection to our FWs more than we have to).
2. We can configure the VPN connection to Panorama in AWS to route all traffic to AWS and from them to the internet. In this scenario we don’t need to open internet connection in GCP.

\* This guide will show steps for option 1

STEPS FOR CREATION IN Panorama

\*Read reference document 2 pages 26-41

STEPS FOR CREATION IN GCP

1. Create a Cloud NAT for first connection from fw to internet in management VPC to receive license from palo cloud
2. Create **route** with dest 0.0.0.0/0 to default internet GW in management VPC – this will route to cloud nat
3. Create FW rule to allow ports 3978, 28443 from management VPC to panorama
4. Manually create windows machine in management VPC for SSH and https connection to FWs
5. Create FW rules to allow ping, ssh, and https between win machine and FWs (within management VPC)
6. Create VM for FW with an image of Palo-Alto (example image name: vmseries-flex-byol-1114h7 – this image is for version 11.1.4-h7)
7. Add the following metadata to the VM:
   1. vm-auth-key=
      1. Generate from panorama server -> Command:“request bootstrap vm-auth-key generate lifetime <?>”
      2. Replace <?> With amount of time, for example 24 would generate an auth key valid for 24 hours
      3. A vm auth key is used to create a ssl session between the fw and panorama
   2. dgname=
      1. Receive from Panorama device group name.
   3. tplname=
      1. Receive from Panorama template name
   4. hostname=
      1. Use a meaningful name, will be used to identify FW in Panorama.
   5. authcodes=
      1. Generate from license pool in palo support portal and use newly generated auth code.
   6. panorama-server=
      1. Take Panorama server private IP address
   7. dns-primary= 169.254.169.254
   8. block-project-ssh-keys=true
   9. serialport-enable=true
   10. mgmt-interface-swap=enable
   11. dhcp-accept-server-hostname=yes
   12. dhcp-accept-server-domain=yes
8. Create ssh keys for connecting to FWs

\* Reference document 2 pages 42-52

STEPS FOR VALIDATING CREATION

Check FW creation worked:

* See we can connect to FW with SSH keys from win machine -> ssh to FW
  + Troubleshoot -
    - Wrong ssh keys
    - No routing
    - No FW rule allowing connection
    - Check win and FWs are in same VPC
* See if FWs have serial numbers from inside the FW (to check internet connection) -> “show system info | match serial”
  + Troubleshoot -
    - No access to internet – try “ping host 8.8.8.8”. If doesn’t work missing routing or FW rule
    - Wrong authcodes in metadata
* Check bootstrap status from FW -> “show system bootstrap status”
  + Troubleshoot -
    - Wrong dgname in metadata
    - Wrong tplname in metadata
    - Wrong panorama-server ip in metadata
    - No routing to panorama
    - VPN not working
    - No FW rule allowing connection
* See if FW have bootstrapped to panorama from FW -> “show panorama-status"
  + Troubleshoot -
    - Wrong dgname in metadata
    - Wrong tplname in metadata
    - Wrong panorama-server ip in metadata
    - No routing to panorama
    - VPN not working
    - No FW rule allowing connection
* See if the new FWs show up in panorama -> “device” -> “summary”, make sure they are connected and synced
  + Troubleshoot -
    - If all steps passed except this one wait 15 minutes to finish bootstrap
    - Try pushing to devices (FWs) if they’re connected but not synced
    - \*\*Specific error\*\* – if an error occurs from av profile (OOXML):
      1. In FW -> device > dynamic updates
      2. check now
      3. Download and install content and apps
      4. Download and install wildfire
      5. Commit and push on panorama

**OR**

1. In Panorama > panorama > device deployment > dynamic updates
2. Repeat above steps 2-5 through panorama UI instead of FW
   * + If still doesn’t work, look at previous troubleshooting steps and validate correct steps taken

* Make sure the FWs have all the current configurations from panorama -> https from win to FW, check security + NAT policies, objects, and anything else that comes to mind.
  + Troubleshoot -
    - Make sure push from panorama completes without error
    - Make sure of matching FWs in device group
* Make sure there’s proper communication, both between VPCs and egress.
  + Troubleshoot -
    - Check the LB configured in the hub (both frontend and backend)
    - Make sure of proper FW rules in relevant hubs and spokes
    - Make sure of proper routing in relevant hubs and spokes

Common commands for start of debugging/FW usage:

* To reset password:
  + ssh to FW
  + configure
  + set mgt-config users admin password
* To search for serial number:
  + ssh to FW
  + show system info | match serial
* To show system bootstrap status
  + ssh to FW
  + show system bootstrap status

**Notes while using palo’s guide to configure new FWs to panorama:**

* When configuring Interfaces, IPv4 -> configure with DHCP client and check setting for “Automatically create default route pointing to default gateway provided by server”
* We are deploying the common-firewall option!
* Create Zone in panorama for each NIC on VM in GCP
* Create routing for all the zones and VPCs via the section of the virtual router -> static routing in Panorama
* Create NAT policy rule for the health checks of the load balancer to work properly.

Creation of the Profiles:

* Objects -> security policies-> antivirus, just leave as default, copied from an existing profile
* Anti-spyware profile, just create the severities we would like to do, for simple-critical we setup reset-both action
* Inline cloud analysis tab in the anti-spyware profile, disable the checkbox about the cloud analysis
* Vulnerability protection profile, add category: protocol anomaly, rule name: anomaly, action: drop
* Medium-high-critical, action: drop, setup severity for medium-high-critical
* Low-info: setup for low and info severity levels
* URL filtering, create a profile and set all actions of all rules to alert, and the action of severe rules like drugs gambling etc. To block.
* File blocking, copy and existing profile, set it to block all risky file types
* Wildfire analysis, copy an existing profile and leave it on default
* Create a security profile group for “outbound-group,” set all the profiles we just created to this group, just like in Prisma-Access, and inbound group with all the same as outbound just without the URL filtering profile, we do not need it in the inbound

References:

1. https://github.com/PaloAltoNetworks/terraform-google-swfw-modules/blob/v2.0.9/modules/vmseries/README.md

1. <https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/guides/gcp-shared-vcp-deployment-guide>