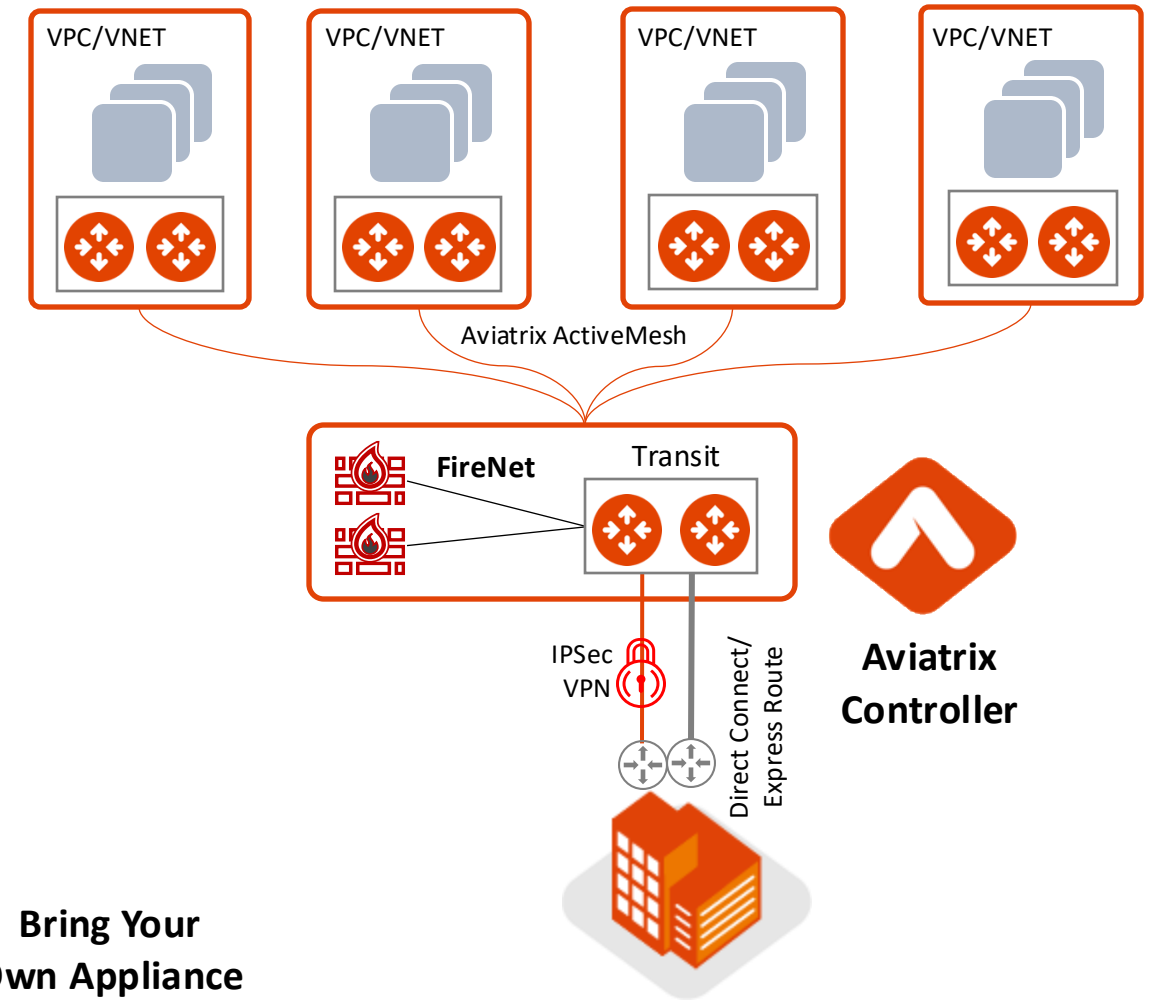
FireNet Operations

ACE Team

Aviatrix Transit Firewall Network (FireNet)

- Scale out, multi-AZ FW deployments, bootstrapping
- Automated route management, segmentation, and security policies
- Deep visibility and operational capabilities
- Repeatable across regions and clouds



paloalto NETWORKS

FORTINET

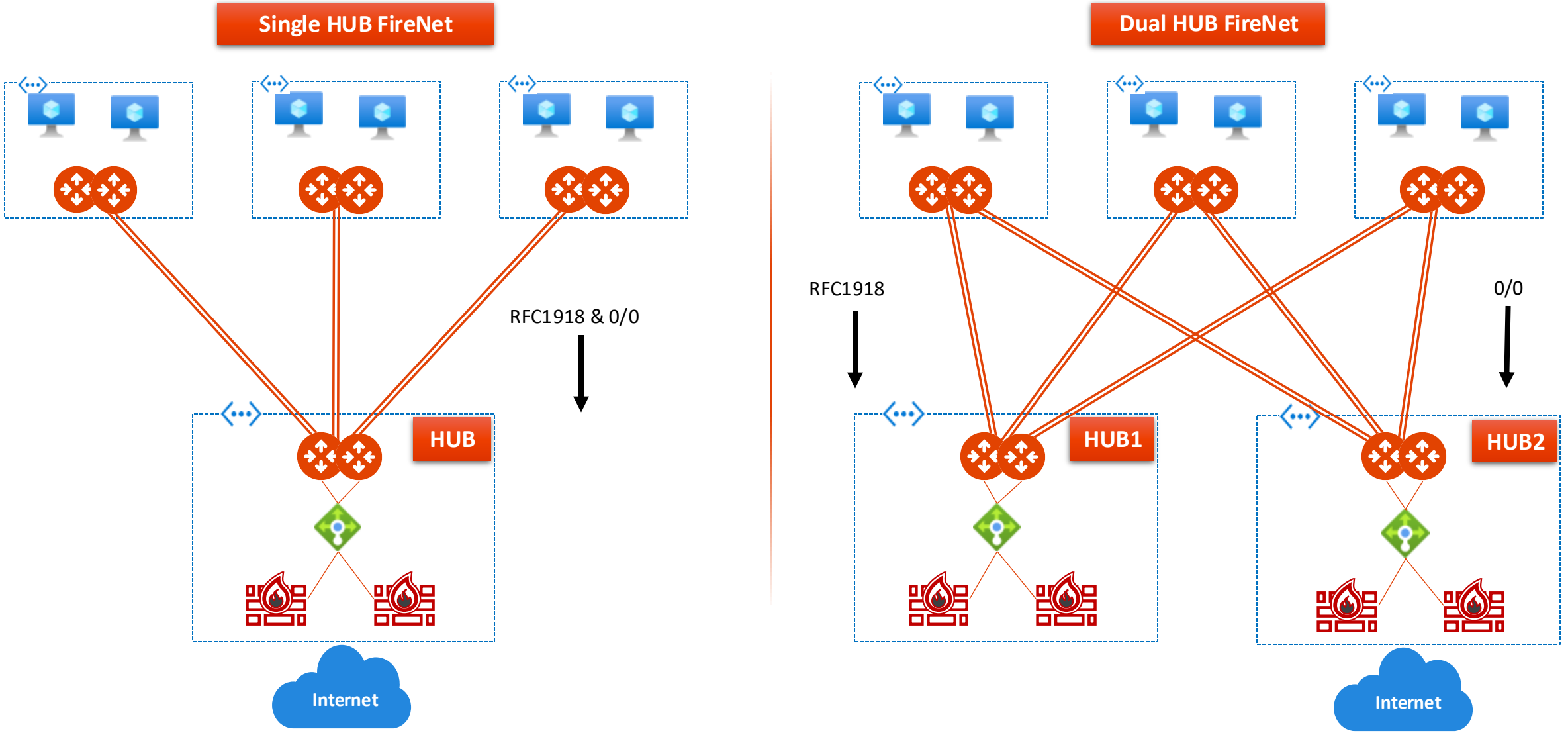
Check Point SOFTWARE TECHNOLOGIES LTD

f5

Bring Your Own Appliance

FireNet Architecture Options (Azure Example)

Each firewall set can scale independently based on need

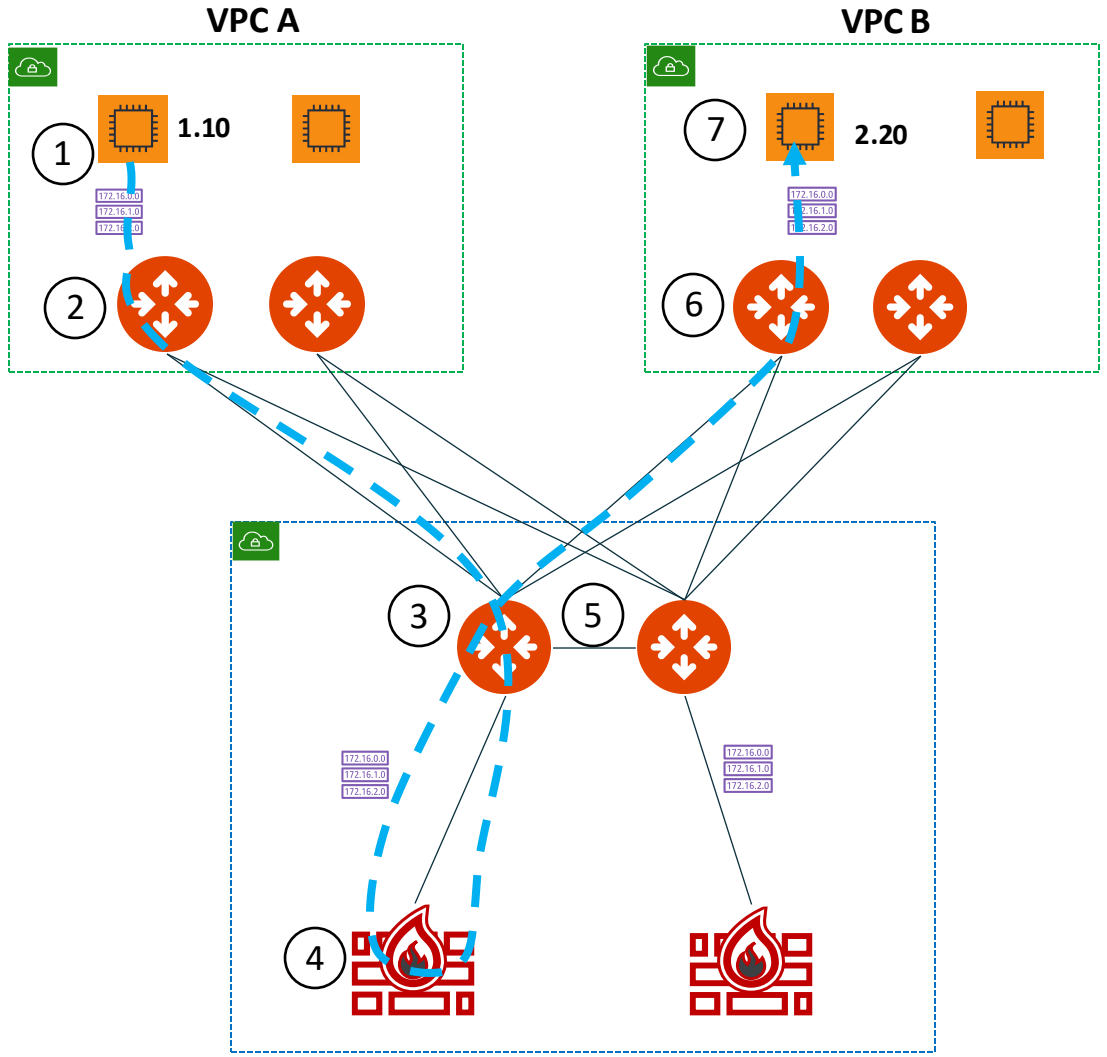


FireNet Packet Walk – AWS Example

A Host 1.10 communicating with 2.20 with VPC A inspected via FireNet

1. The local route table for 1.10 has RFC1918 routes pointed to its local gateway.
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways.
3. The Aviatrix Transit Gateway receiving the flow will check inspection policy to determine if either source or destination requires FireNet. If a match, traffic is redirected to the firewall in the same AZ.
4. The Firewall selected will process the packet and send the traffic back to its defined Transit Gateway.
5. The Aviatrix Transit Gateway will receive the processed packet and forward (ECMP) with 5-tuple hash towards the destination spoke.
6. The destination spoke gateway will receive the traffic and route the traffic out its local interface to the VPC route table. Note that this GW may not be in the same AZ as the destination instance.
7. The destination will receive the original traffic and see this as native VPC communication flow.

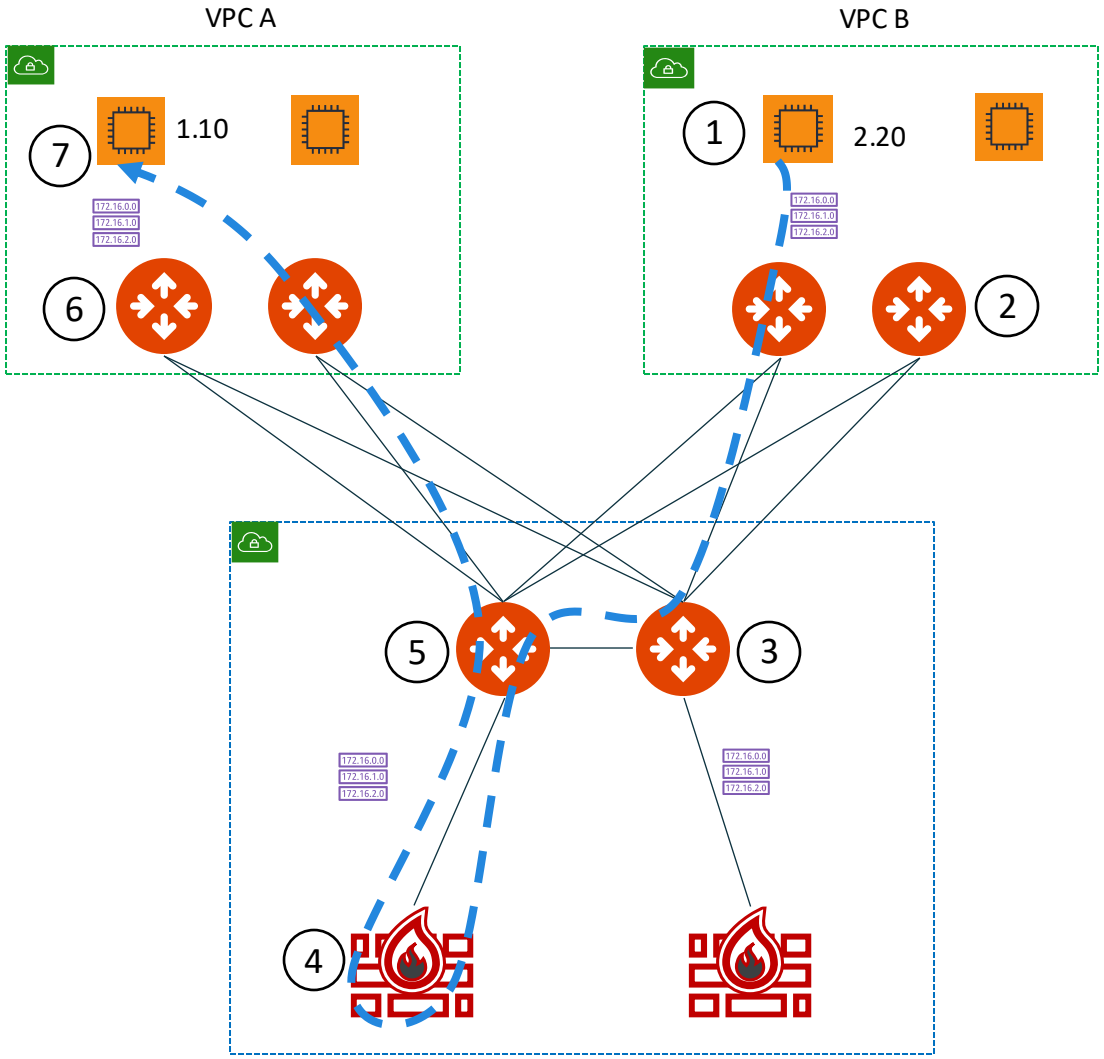
Aviatrix Transit tracks the health of Firewall



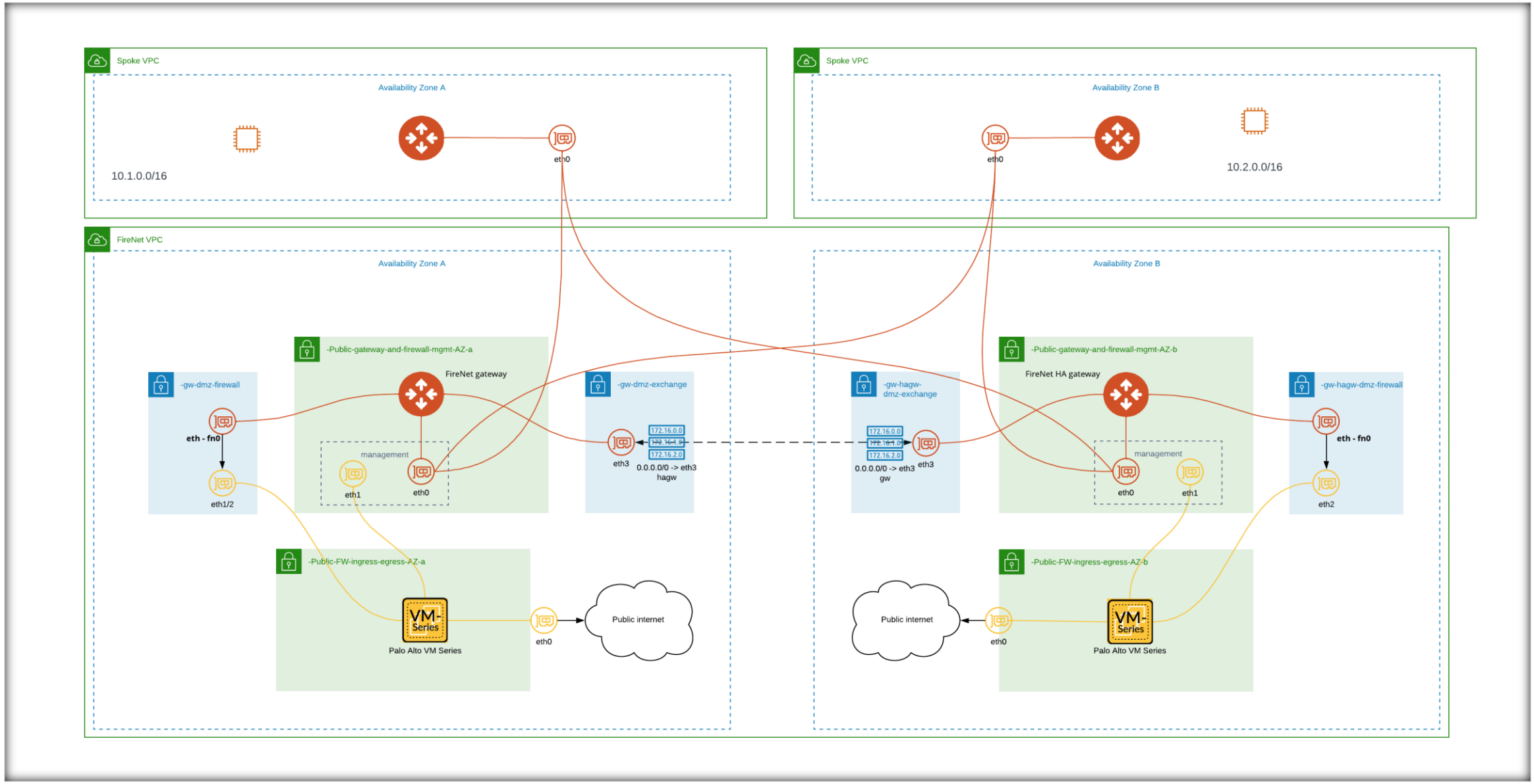
FireNet Packet Walk – AWS Example

Return Flow: 1.10 communicating with 2.20 with VPC A inspected via FireNet

1. The local route table for 2.20 has RFC1918 routes pointed to its local spoke gateway for return traffic.
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways.
3. The Aviatrix Transit Gateway receiving the traffic will pass the traffic to the the same FW which handled the initial flow to maintain symmetry.
4. The stateful Firewall will process the return traffic and route the traffic back to its designated gateway.
5. The Aviatrix gateway will ECMP traffic with 5-tuple hash to one of the destination spoke gateways.
6. The destination spoke gateway will route this traffic out its local interface to the native VPC route table.
7. The original source will receive the return traffic and see this as native VPC communication flow.



FireNet – Under the hood

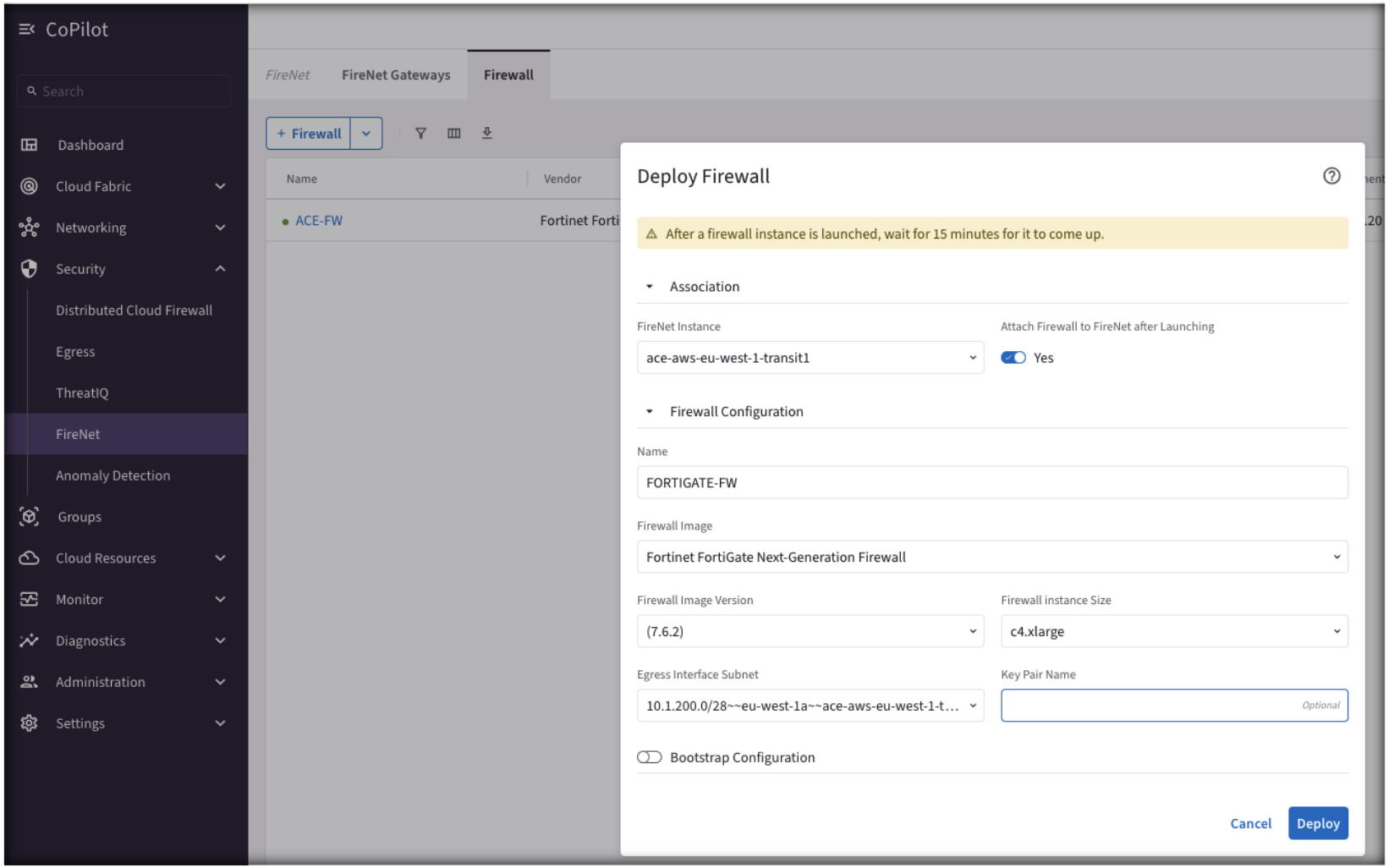


Tools for Operating your FireNet

Firewall Deployment Workflow

- **PATH**: Security > FireNet > Firewall
  1. Select the Transit FireNet GW
  2. Select the Firewall Image (requirement: *Subscribe to the firewall instance from the Marketplace*)
  3. Firewall Image Version
  4. Firewall Instance Size
  5. Egress Interface Subnet
  6. Management Interface Subnet (Palo Alto/AWS only)
  7. Bootstrap Configuration (*optional*)

- **Supported Firewall Vendors**: Palo Alto VM-Series, Check Point CloudGuard, Fortinet FortiGate, BYOA
  - **Panorama** is also supported as a firewall manager for Palo Alto VM-Series.



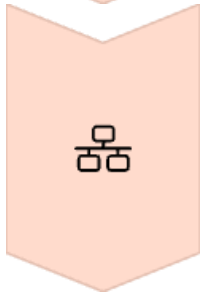
FireNet Workflow

Firewall Deployment

Subscribe to a vendor firewall from Marketplace or add your existing firewall to Transit FireNet Gateway.

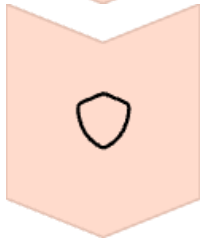
Bootstrap Configuration (Optional)

Enable Bootstrap Configuration toggle to let Aviatrix Controller insert initial setup into the firewall.



Vendor Integration

Configure RFC1918 and non-RFC1918 routes between Aviatrix transit FireNet Gateway and vendor's firewall.



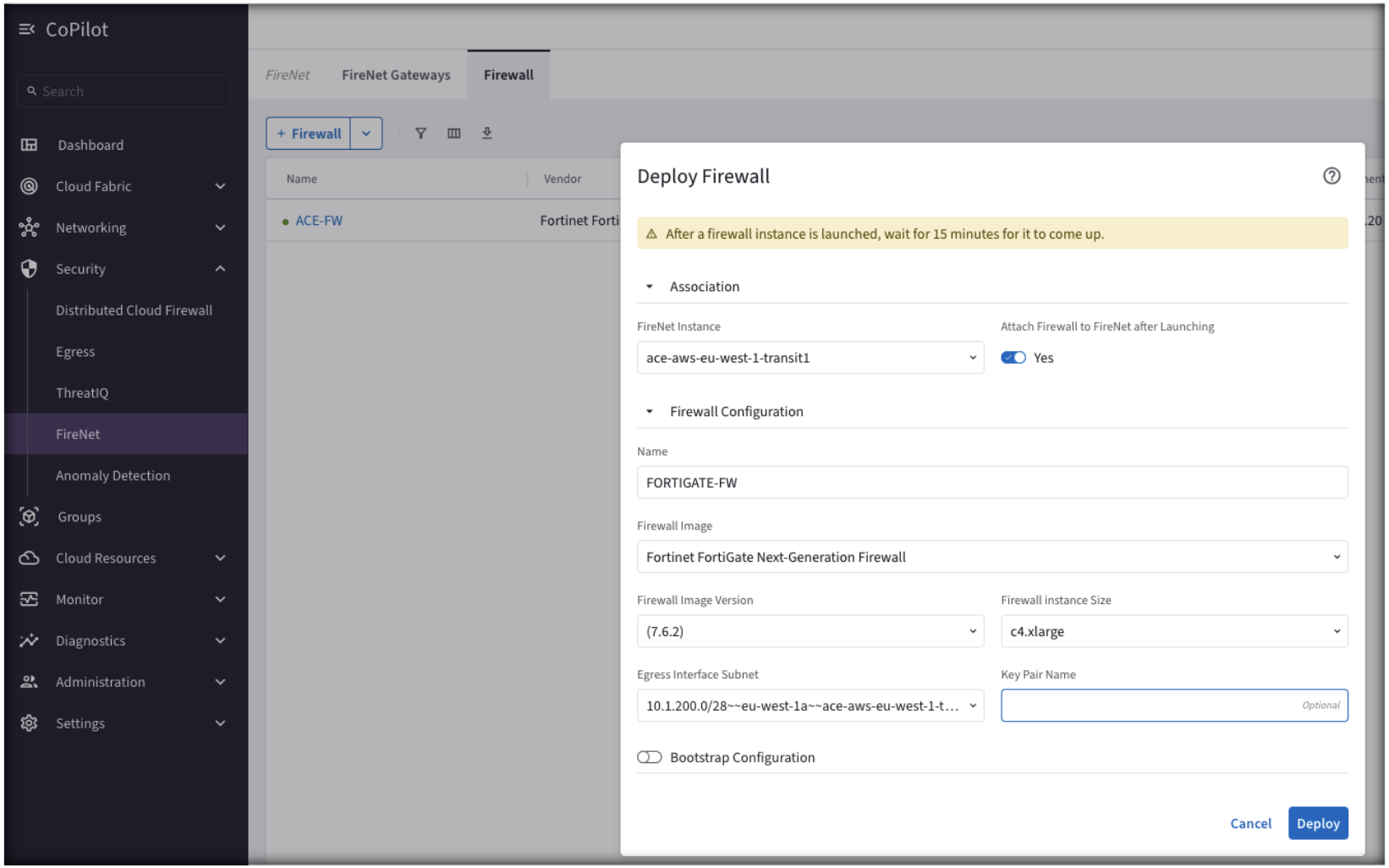
Inspection Policy

Identify specific VPCs where traffic must be diverted for firewall inspection.

Firewall Deployment

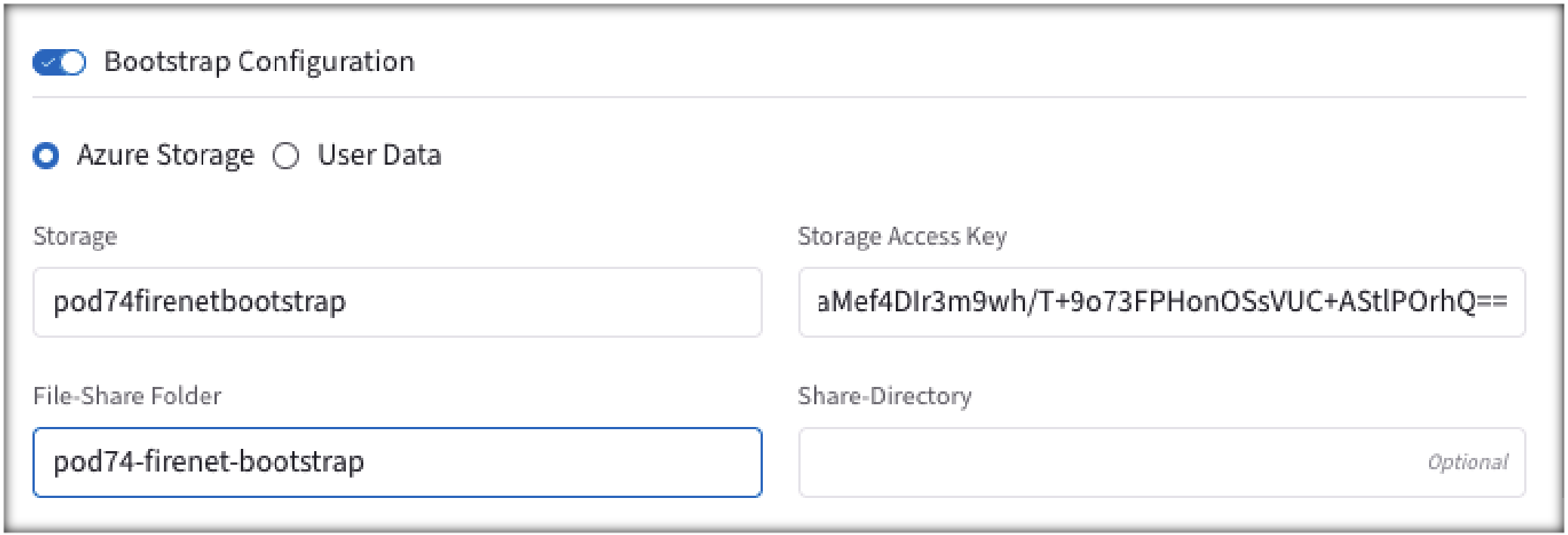
- **PATH**: Security > FireNet > Firewall
  1. Select the Transit FireNet GW
  2. Select the Firewall Image (requirement: *Subscribe to the firewall instance from the Marketplace*)
  3. Firewall Image Version
  4. Firewall Instance Size
  5. Egress Interface Subnet
  6. Management Interface Subnet (Palo Alto/AWS only)
  7. Bootstrap Configuration (*optional*)

- **Supported Firewall Vendors**: Palo Alto VM-Series, Check Point CloudGuard, Fortinet FortiGate, BYOA
  - **Panorama** is also supported as a firewall manager for Palo Alto VM-Series.



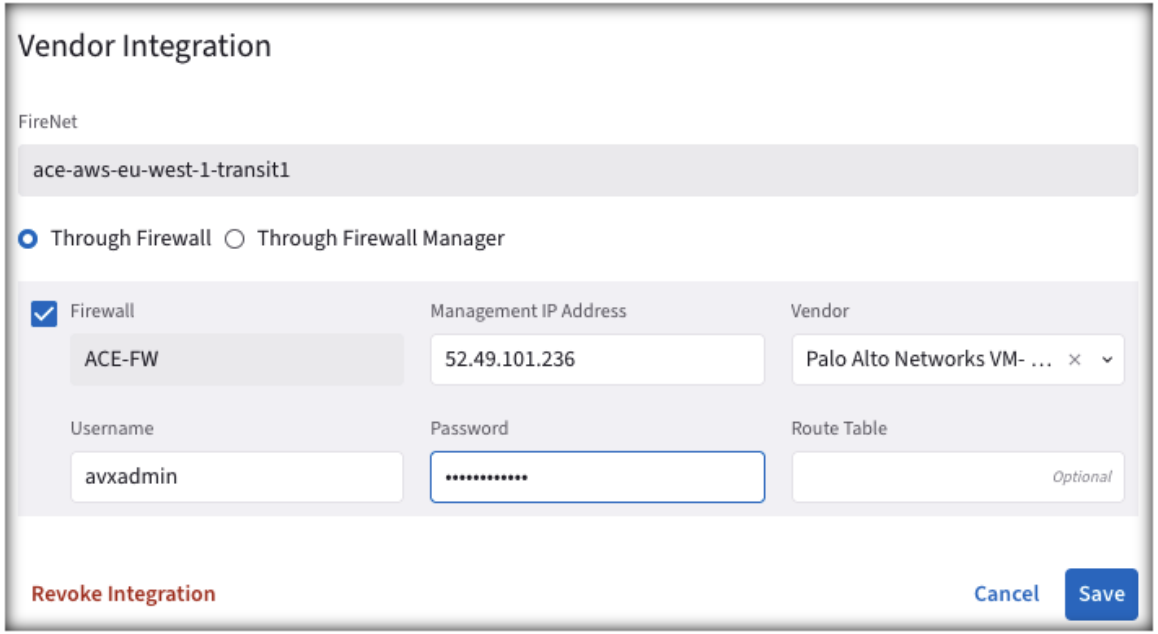
Bootstrap (*optional)*

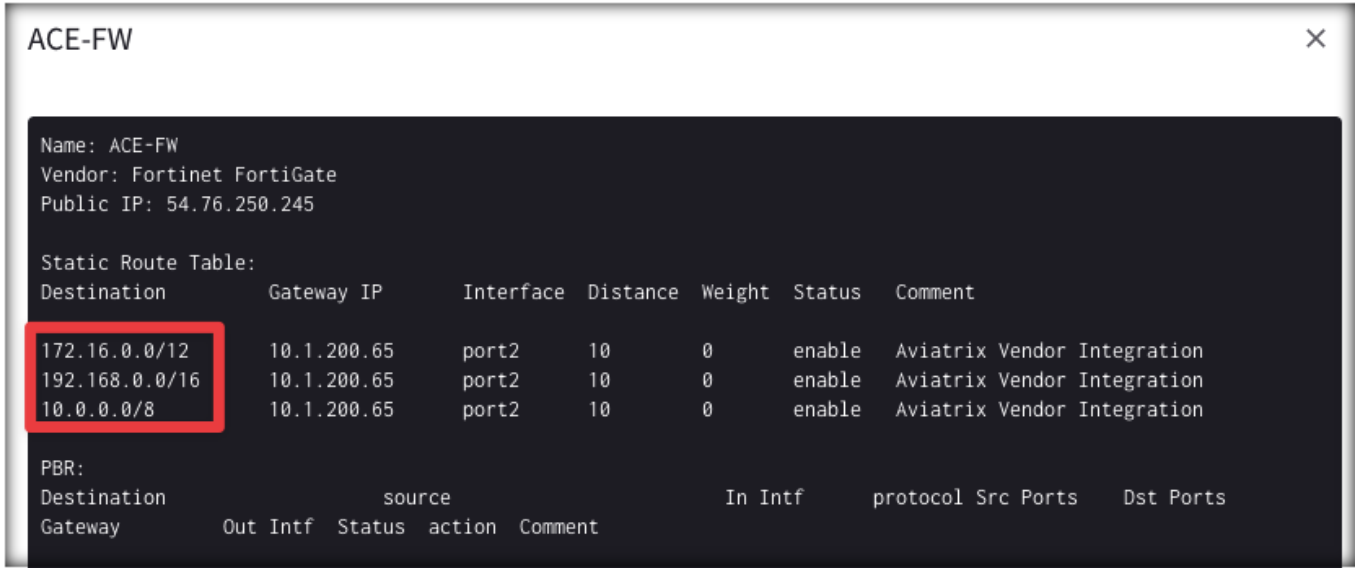
- **Botostrap Configuration toggle**
  - *Toggle Disabled* (default): the FW is deployed with an empty configuration
  - *Toggle Enabled: t*he FW is deployed with an initial configuration
    - You need to specify the Location where the AVX Controller will retrieve the initial configuration (e.g. Azure Storage, S3 Bucket, etc.)



Vendor Integration

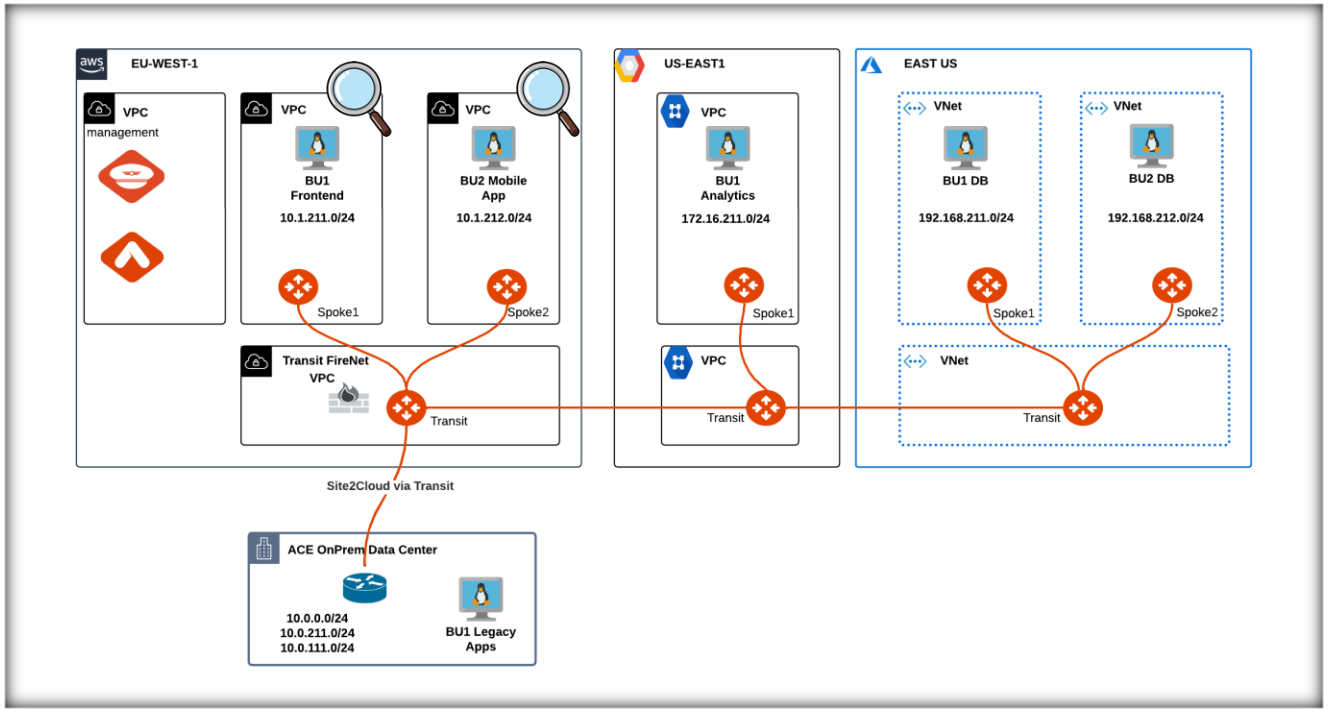
- The Vendor Integration function allows the Controller to log into a firewall or firewall manager and change the route table on the firewall to program the routing for FireNet, or to change routing if a gateway in FireNet fails.
- Vendor Integration allows to configure the **RFC 1918 routes** and **non-RFC 1918 routes** on the Vendor's firewall instance

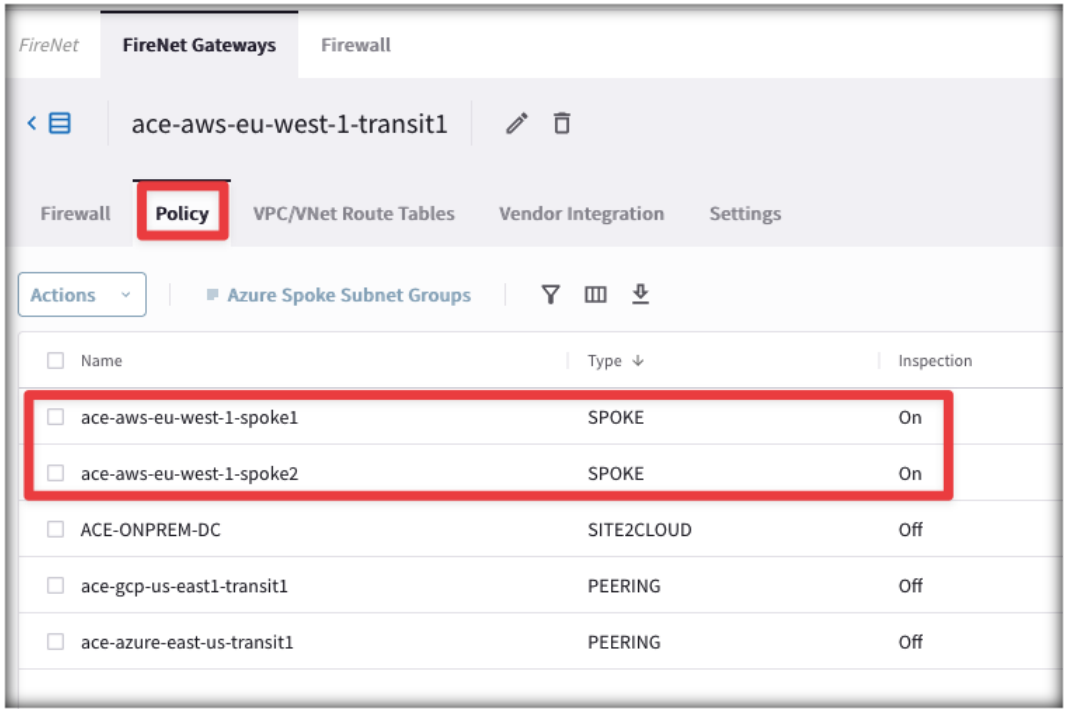




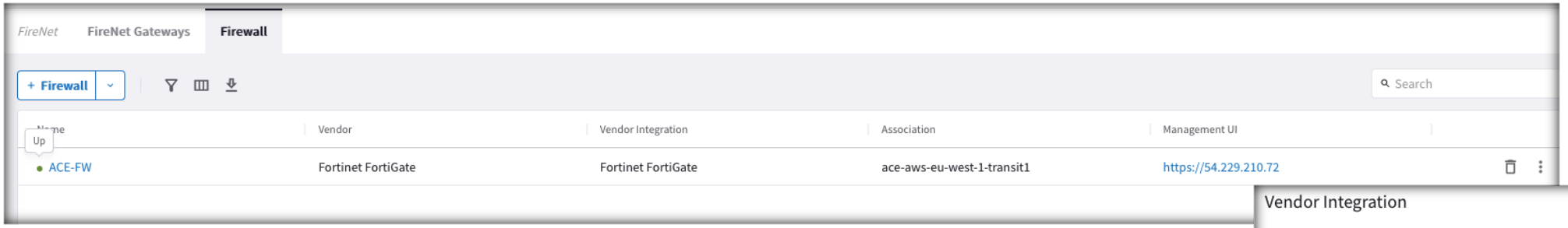
Inspection Policy

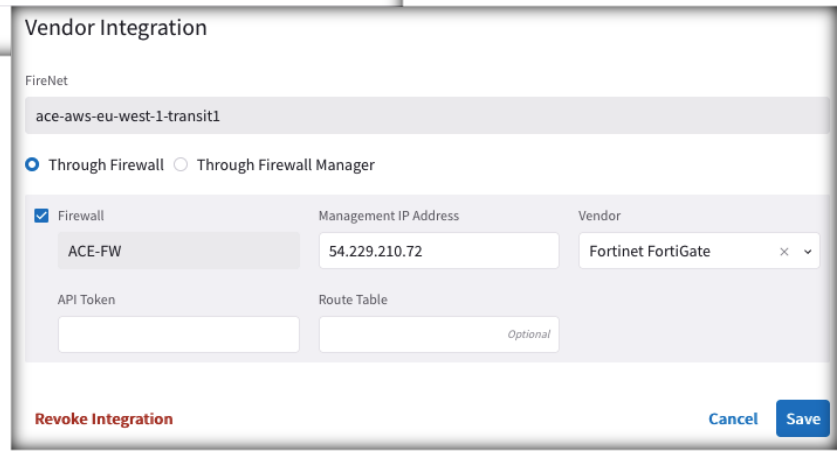
- On the FireNet **Policy** tab you can add or remove the **inspection policy** for the selected VPC/Vnet/VCN. When an inspection policy is added the traffic related to the Transit FireNet's attachment (Spoke/Edge gateway, peered Transit, Site2Cloud connection) is inspected by the firewall within the selected Transit FireNet.
- *By default*, FireNet inspects ingress and east-west traffic only.





Information to Collect / Checklist

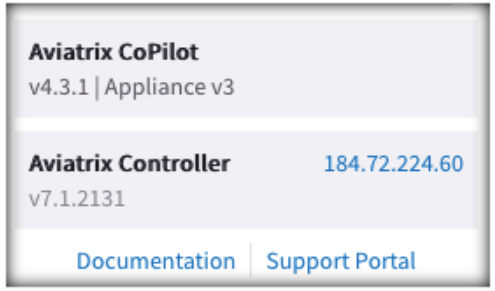


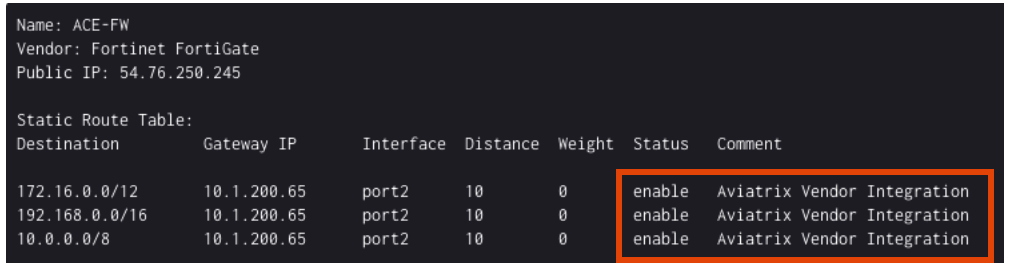


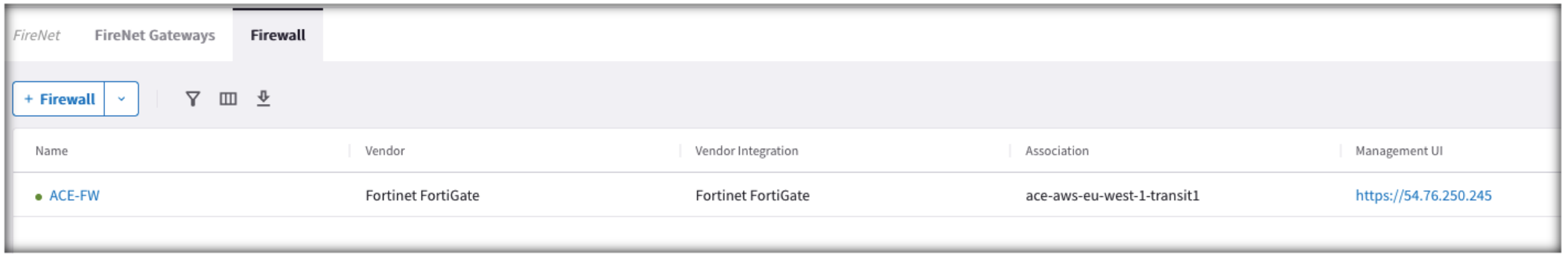
- Make sure Aviatrix sees the FW as “healthy”
  - For Ingress: Check if any native LB deployed in front of the FWs is also configured correctly
- Vendor Integration: make sure the controller can reach the FW
  - Nothing preventing the communication, NACLs, NSGs, SLs, etc.
- Make sure there are no “uncommitted” pending changes on the FW
- Make sure your Network Domain/Spoke is configured for inspection
- Make sure Connected Transit is enabled (if necessary)
- Make sure your Spoke is attached to Transit
- Verify Spoke and Transit GW routes in Cloud Fabric > Gateways

Information to Collect - Checklist for the Support Team

- Aviatrix Controller version
- Firewall Vendor
- Transit FireNet: Inspection Policy
  - Is the Spoke VPC/VNet supposed to be Inspected at all?
- E/W Traffic inspection enabled?
- Egress Traffic inspection enabled?
- Ingress Traffic enabled and working?
- Exclude list created for CIDR/IP from being inspected by FireNet?
- Is there any automation running every day / hour / ?







Next:

Lab 3 FireNet - Interface
Lab 4 FireNet - Routes