



FireNet Operations

ACE Team





Aviatrix Transit Firewall Network (FireNet)



Scale out, multi-AZ FW deployments, bootstrapping



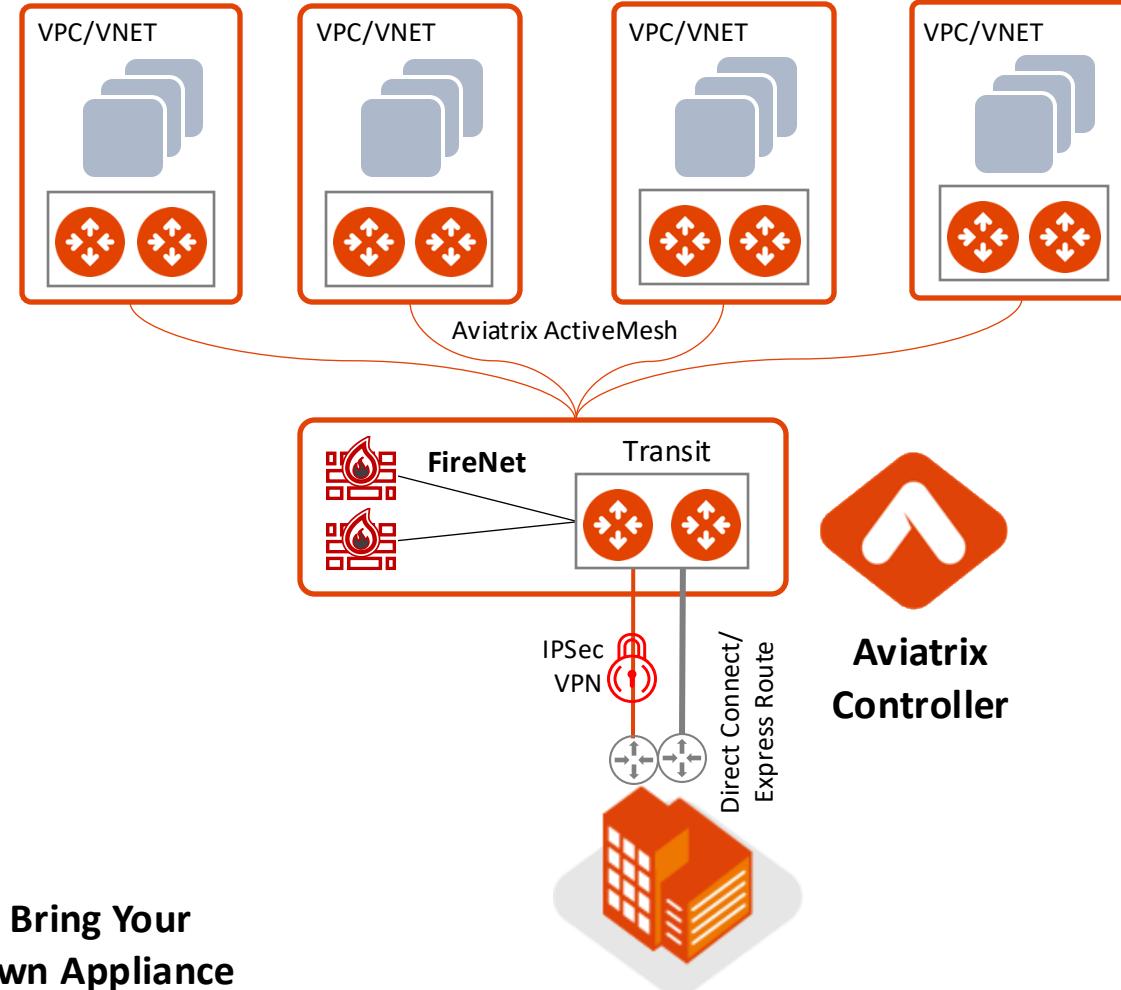
Automated route management, segmentation, and security policies



Deep visibility and operational capabilities



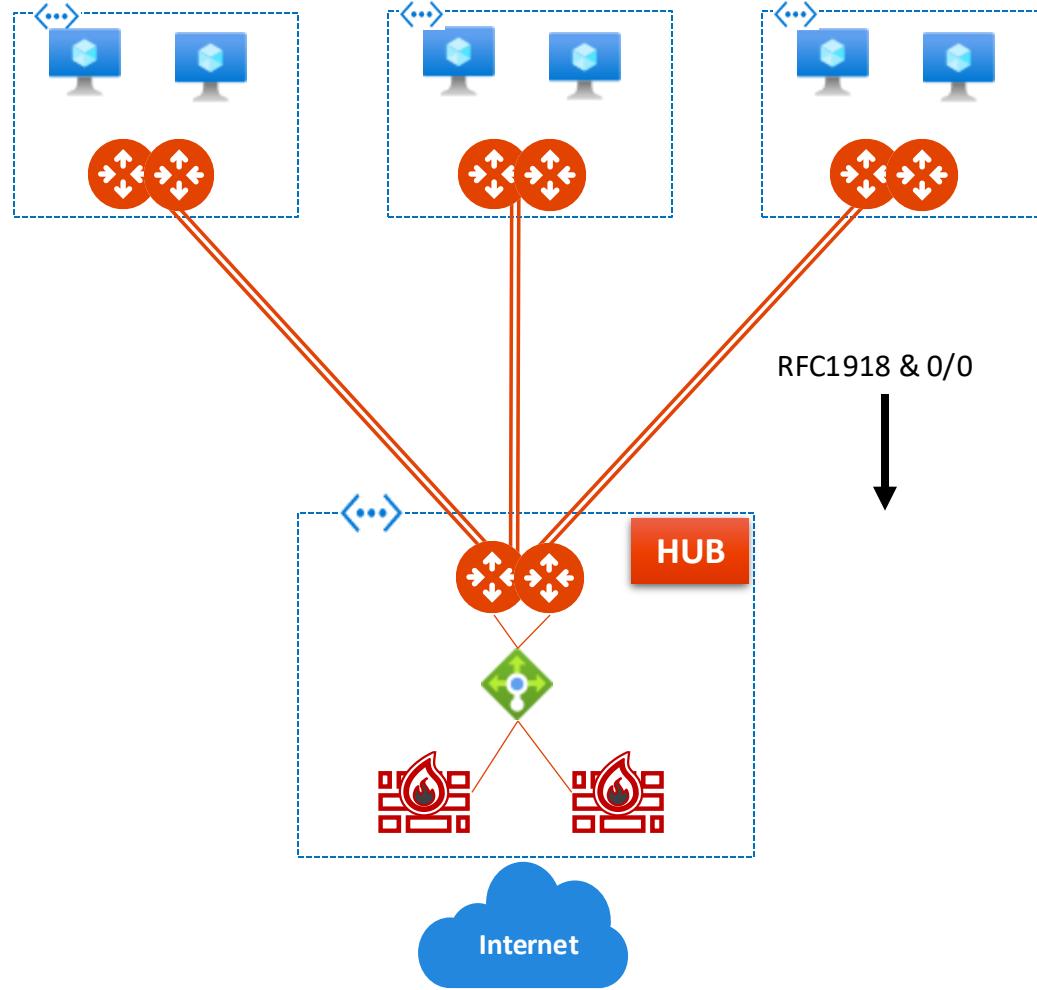
Repeatable across regions and clouds



FireNet Architecture Options (Azure Example)

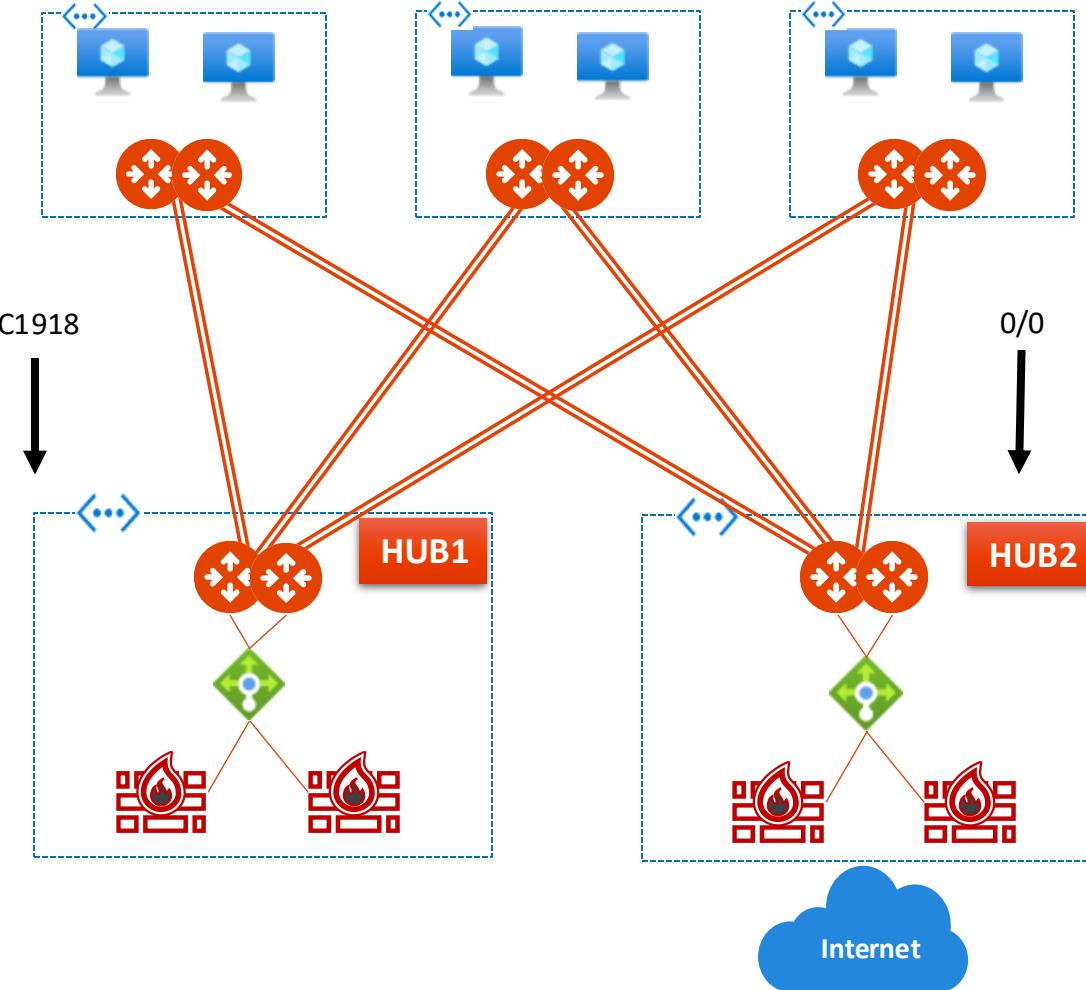
Each firewall set can scale independently based on need

Single HUB FireNet



RFC1918 & 0/0

Dual HUB FireNet

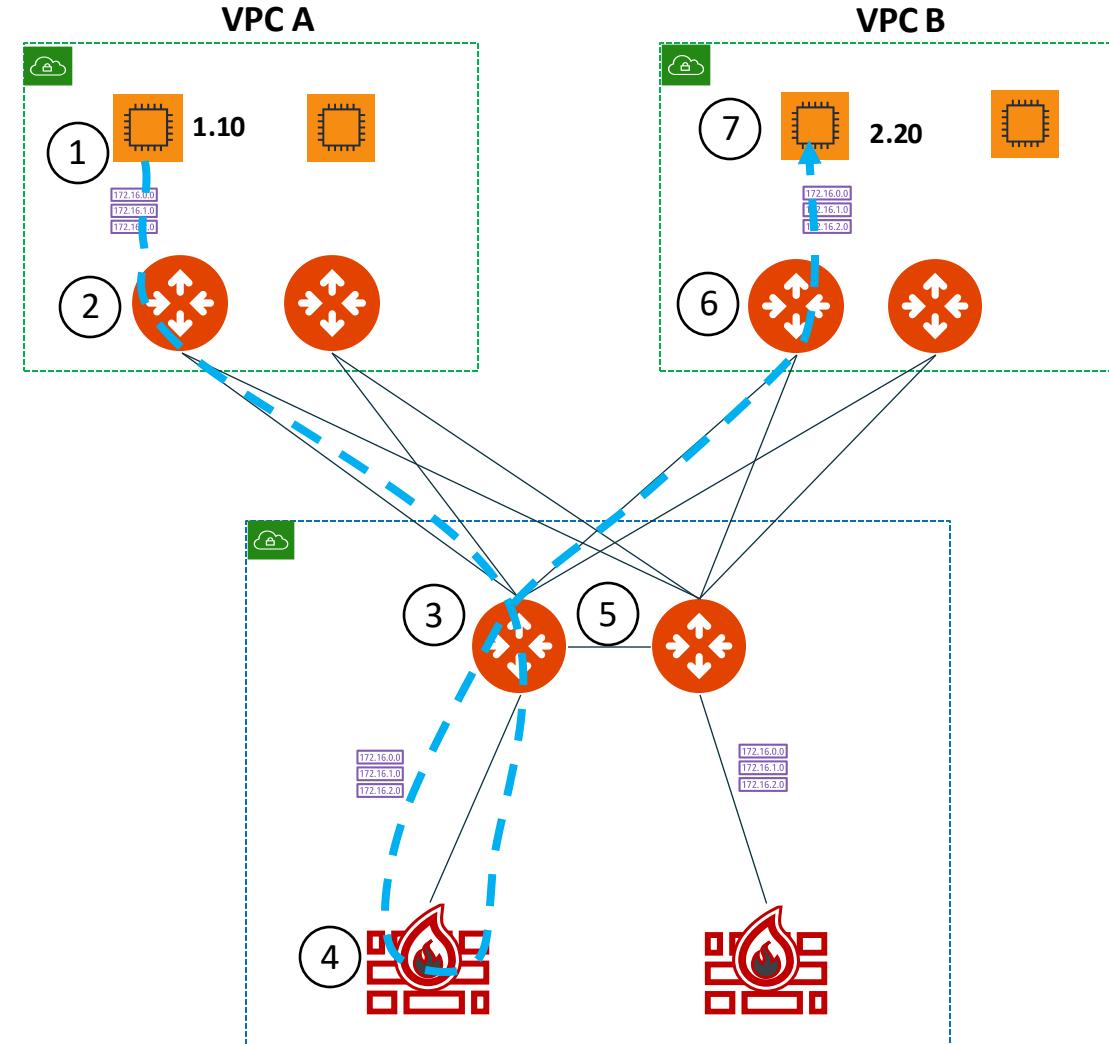


FireNet Packet Walk – AWS Example

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.

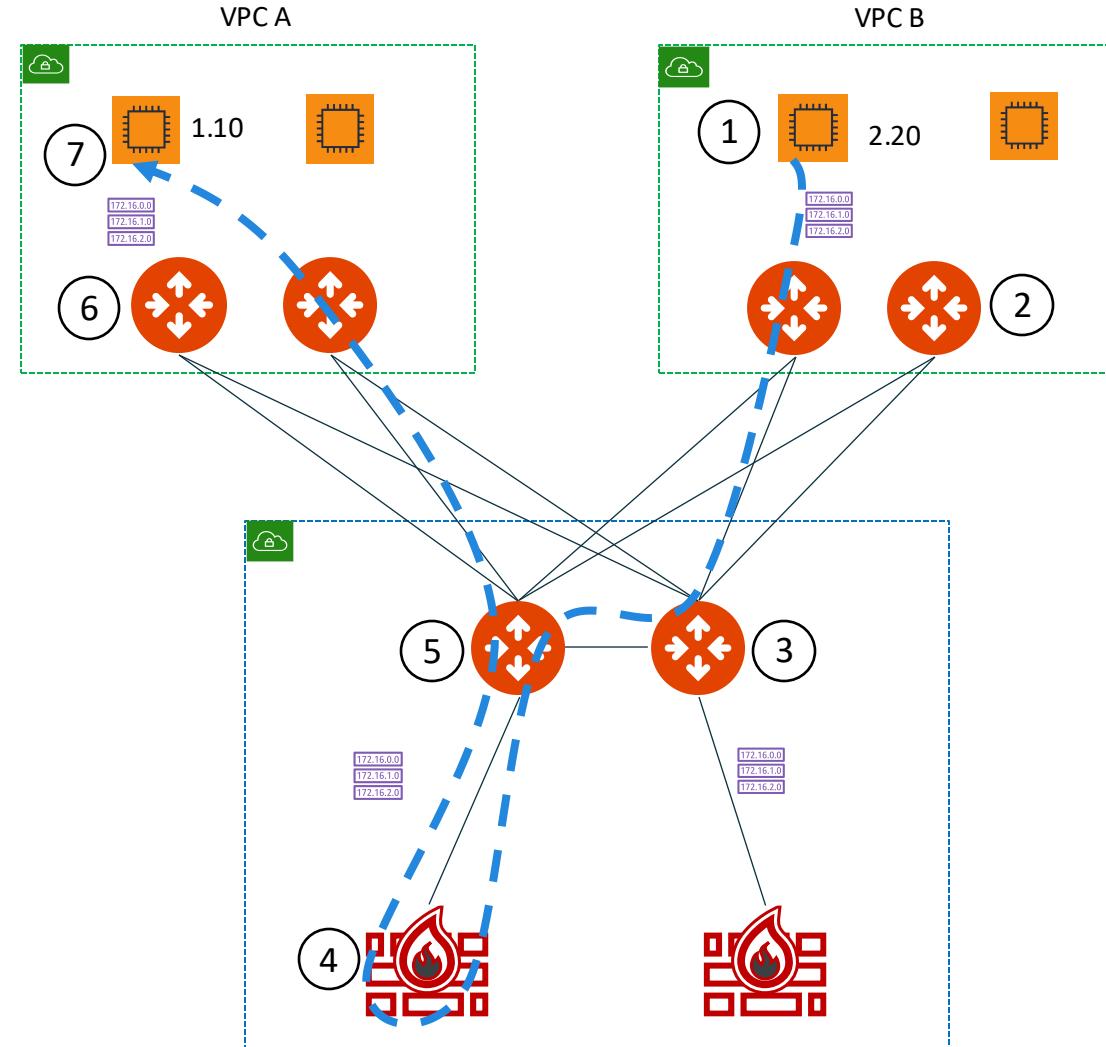
Aviatrix Transit tracks the health of Firewall



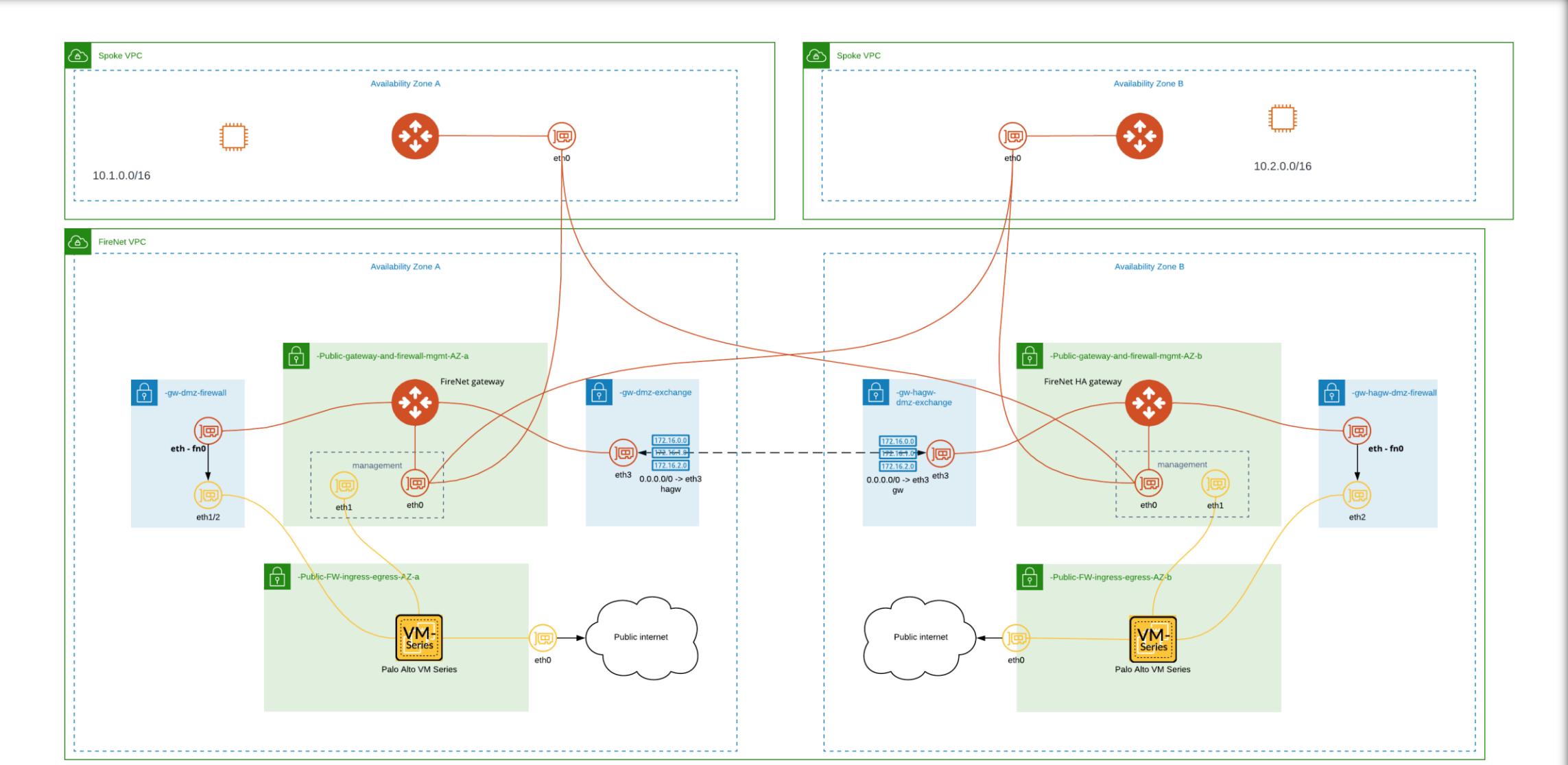
FireNet Packet Walk – AWS Example

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

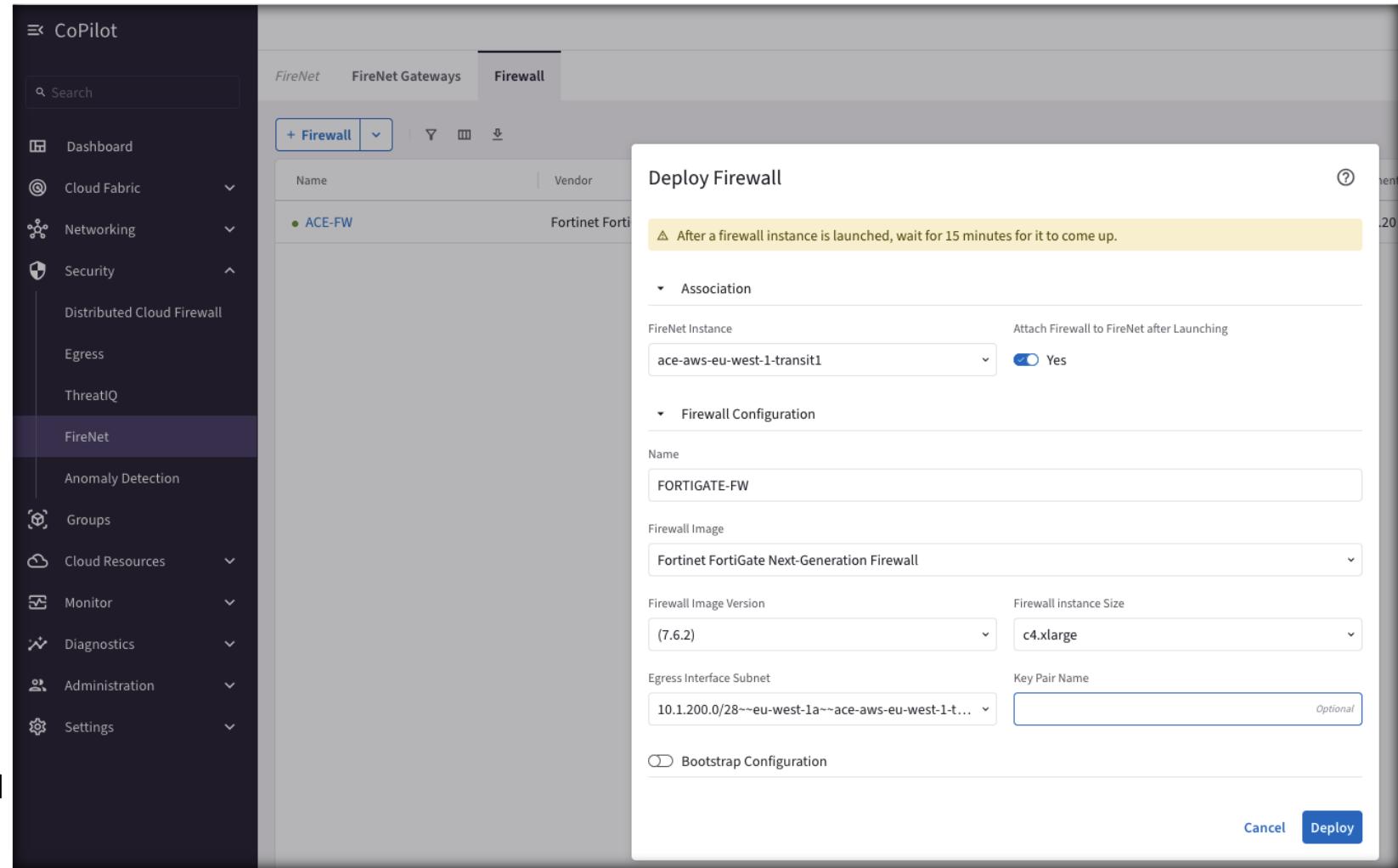




Tools for Operating your FireNet

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.



The screenshot shows the Aviatrix CoPilot interface. On the left is a dark sidebar with various navigation options: Dashboard, Cloud Fabric, Networking, Security, Distributed Cloud Firewall, Egress, ThreatIQ, FireNet (which is selected), Anomaly Detection, Groups, Cloud Resources, Monitor, Diagnostics, Administration, and Settings. The main area has tabs for FireNet, FireNet Gateways, and Firewall, with the Firewall tab selected. Below the tabs is a table with one row labeled 'ACE-FW' under the 'Name' column and 'Fortinet Forti' under the 'Vendor' column. A large modal window titled 'Deploy Firewall' is open. It contains fields for 'Association' (FireNet Instance: 'ace-aws-eu-west-1-transit1', Attached: 'Yes'), 'Firewall Configuration' (Name: 'FORTIGATE-FW', Firewall Image: 'Fortinet FortiGate Next-Generation Firewall'), 'Firewall Image Version' (selected: '(7.6.2)'), 'Firewall instance Size' (selected: 'c4.xlarge'), 'Egress Interface Subnet' (selected: '10.1.200.0/28~eu-west-1a~ace-aws-eu-west-1-t...'), 'Key Pair Name' (Optional), and 'Bootstrap Configuration' (checkbox). At the bottom right of the modal are 'Cancel' and 'Deploy' buttons.

FireNet Workflow



Firewall Deployment



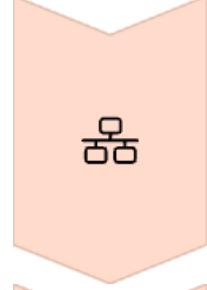
Subscribe to a vendor firewall from Marketplace or add your existing firewall to Transit FireNet Gateway.



Bootstrap Configuration (Optional)



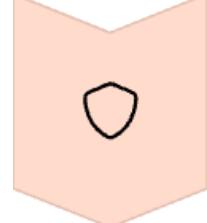
Enable Bootstrap Configuration toggle to let Aviatrix Controller insert initial setup into the firewall.



Vendor Integration



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



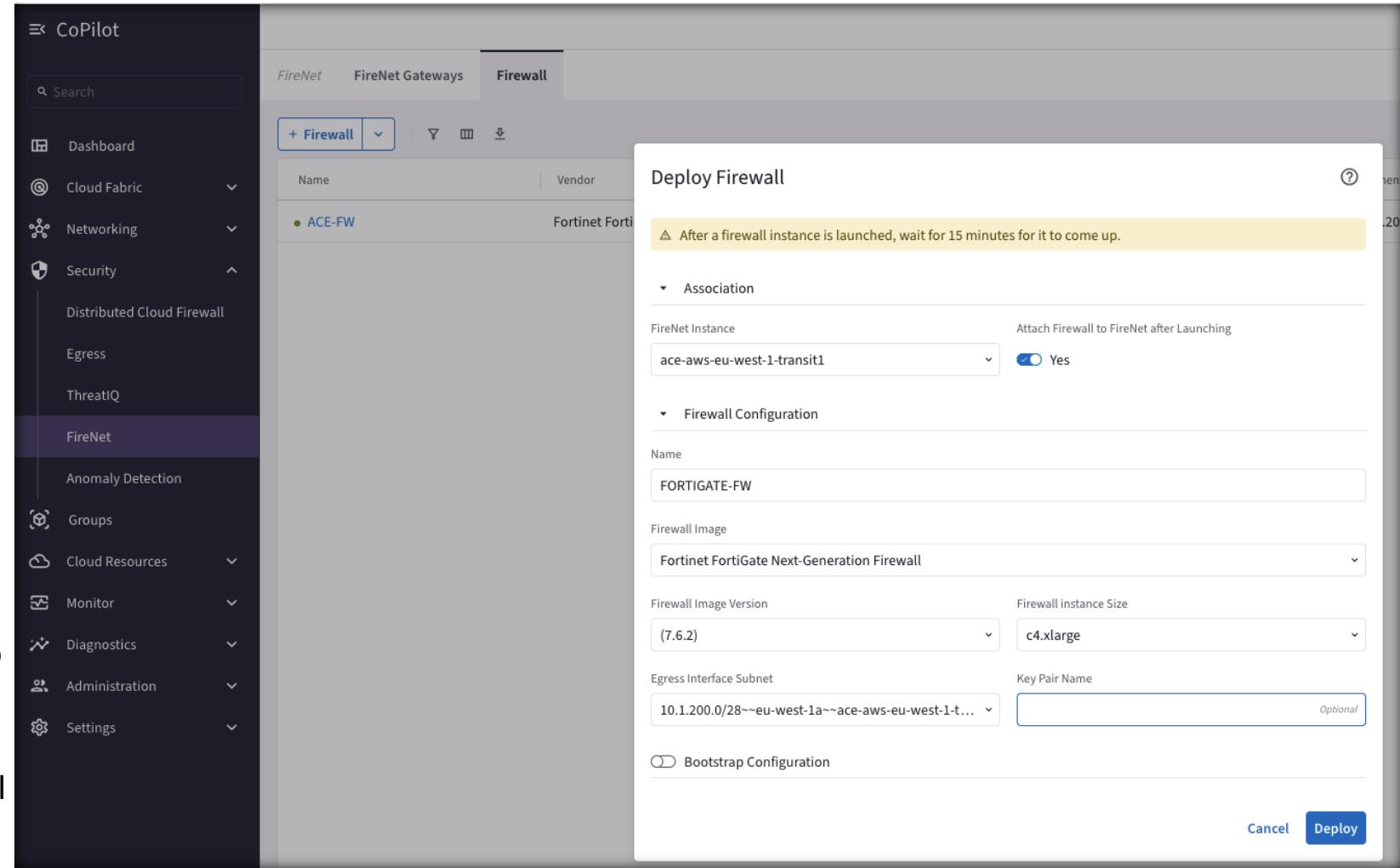
Inspection Policy



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.

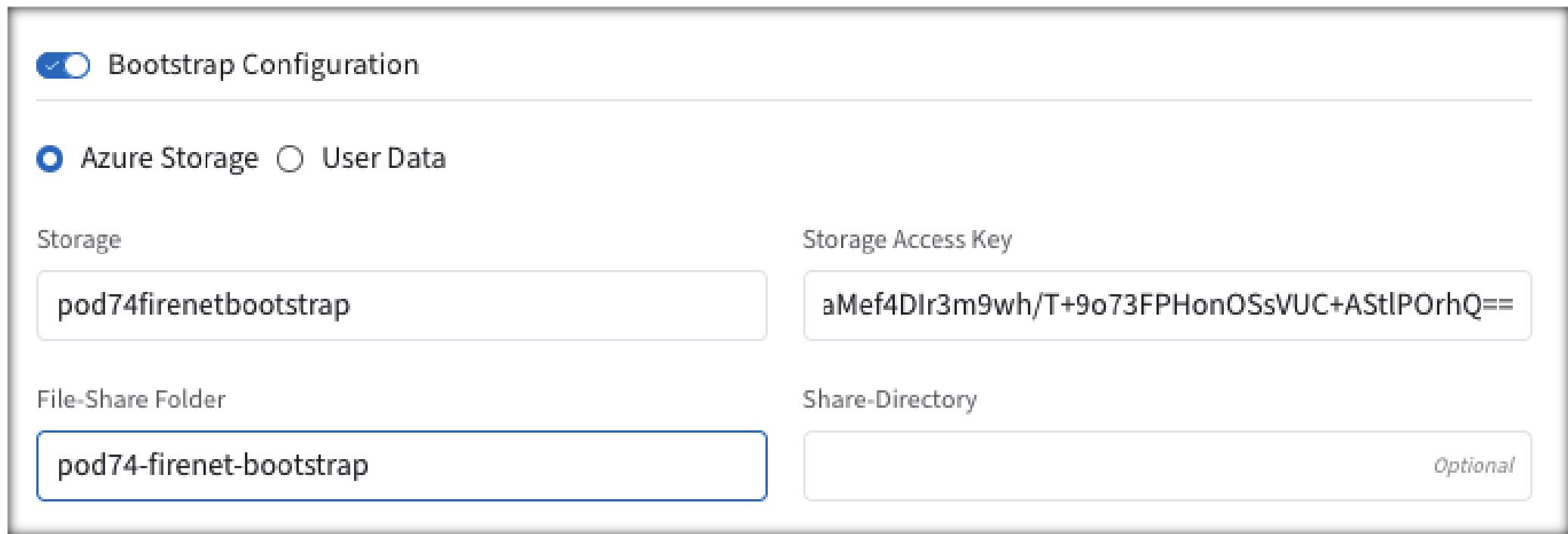


The screenshot shows the Aviatrix CoPilot interface for deploying a Firewall. The left sidebar has a dark theme with various navigation options like Dashboard, Cloud Fabric, Networking, Security, FireNet, Anomaly Detection, Groups, Cloud Resources, Monitor, Diagnostics, Administration, and Settings. The main area has tabs for FireNet, FireNet Gateways, and Firewall, with the Firewall tab selected. Below the tabs is a table with one row labeled 'ACE-FW' under the 'Name' column and 'Fortinet Forti' under the 'Vendor' column. A large modal window titled 'Deploy Firewall' is open on the right. It contains fields for 'Association' (FireNet Instance: 'ace-aws-eu-west-1-transit1', Attached: 'Yes'), 'Firewall Configuration' (Name: 'FORTIGATE-FW', Firewall Image: 'Fortinet FortiGate Next-Generation Firewall'), 'Firewall Image Version' (selected: '(7.6.2)'), 'Firewall instance Size' (selected: 'c4.xlarge'), 'Egress Interface Subnet' (selected: '10.1.200.0/28~eu-west-1a~ace-aws-eu-west-1-t...'), 'Key Pair Name' (Optional), and 'Bootstrap Configuration' (checkbox). At the bottom of the modal are 'Cancel' and 'Deploy' buttons.

Bootstrap (*optional*)

- **Bootstrap Configuration toggle**

- *Toggle Disabled (default)*: the FW is deployed with an empty configuration
- *Toggle Enabled*: the 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.)



The screenshot shows the Bootstrap Configuration settings for an Aviatrix Controller. The 'Bootstrap Configuration' toggle is enabled (checked). The 'Azure Storage' radio button is selected. The 'Storage' field contains 'pod74firenetbootstrap'. The 'Storage Access Key' field contains 'aMef4Dlr3m9wh/T+9o73FPhonOSsVUC+AStlPOrhQ=='. The 'File-Share Folder' field contains 'pod74-firenet-bootstrap'. The 'Share-Directory' field is empty and labeled 'Optional'.

<input checked="" type="checkbox"/> Bootstrap Configuration	
<input checked="" type="radio"/> Azure Storage <input type="radio"/> User Data	
Storage	Storage Access Key
pod74firenetbootstrap	aMef4Dlr3m9wh/T+9o73FPhonOSsVUC+AStlPOrhQ==
File-Share Folder	Share-Directory
pod74-firenet-bootstrap	Optional

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

Vendor Integration

FireNet

ace-aws-eu-west-1-transit1

Through Firewall Through Firewall Manager

<input checked="" type="checkbox"/> Firewall	Management IP Address	Vendor
ACE-FW	52.49.101.236	Palo Alto Networks VM- ... ×
Username	Password	Route Table
avxadmin	*****	Optional

[Revoke Integration](#) [Cancel](#) [Save](#)

ACE-FW

Name: ACE-FW
Vendor: Fortinet FortiGate
Public IP: 54.76.250.245

Static Route Table:

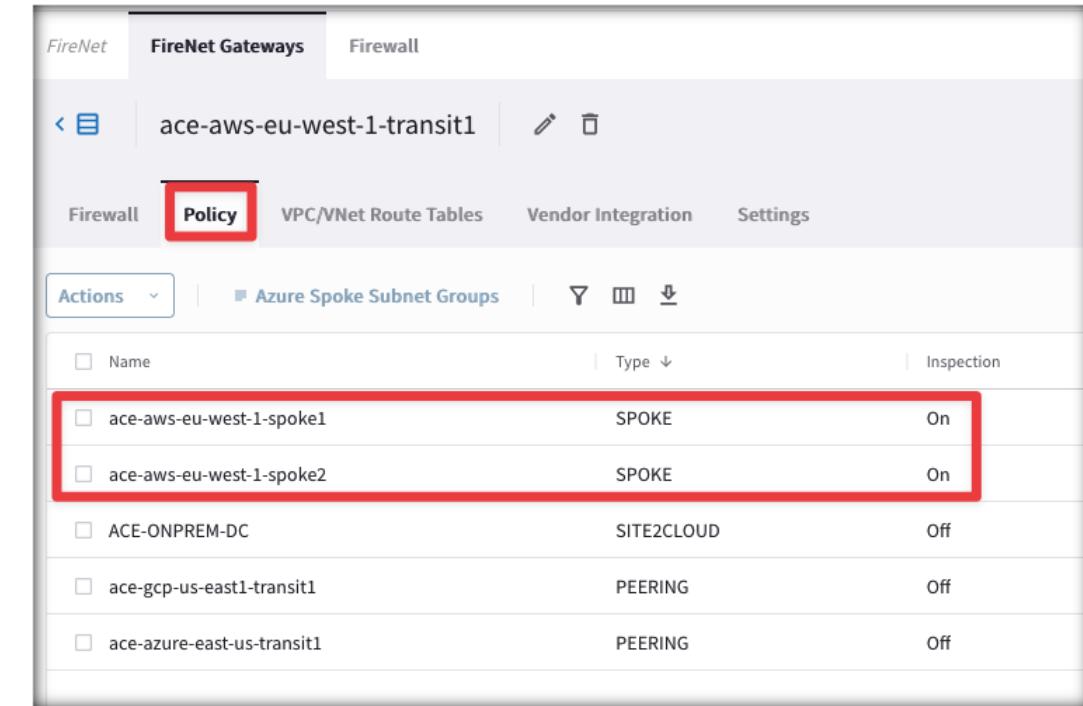
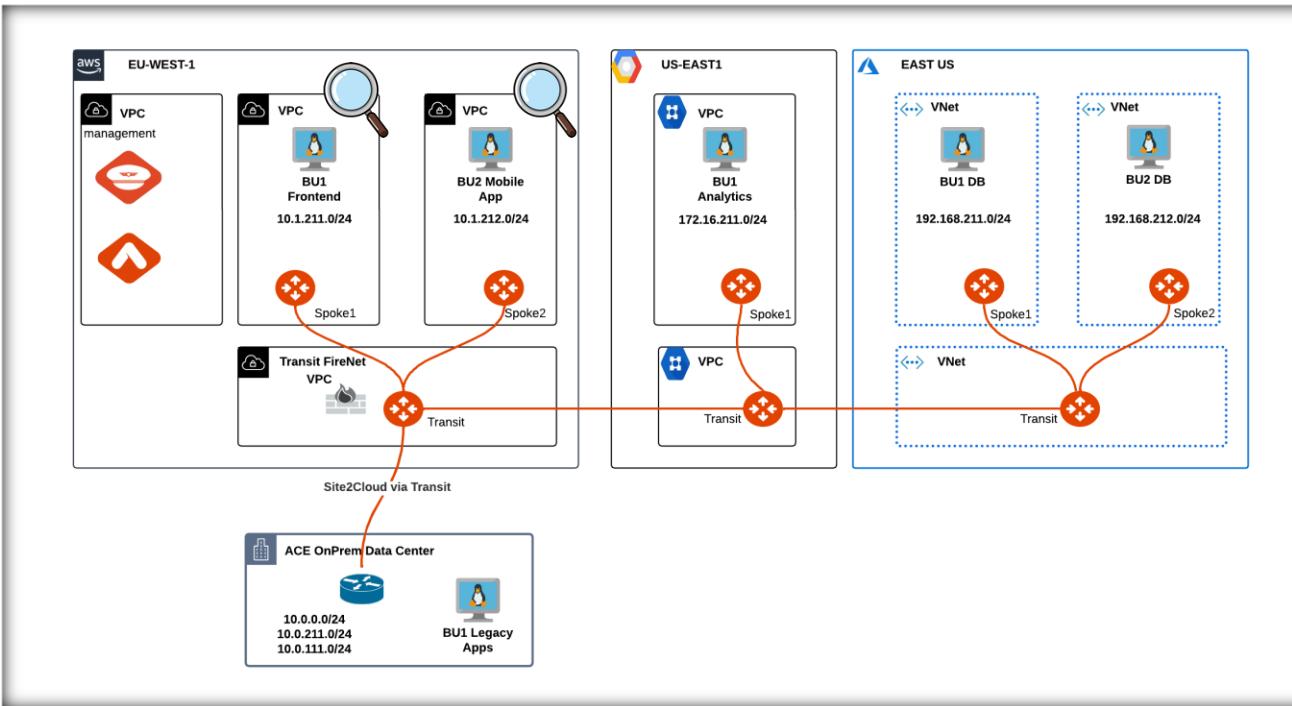
Destination	Gateway IP	Interface	Distance	Weight	Status	Comment
172.16.0.0/12	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration
192.168.0.0/16	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration
10.0.0.0/8	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration

PBR:

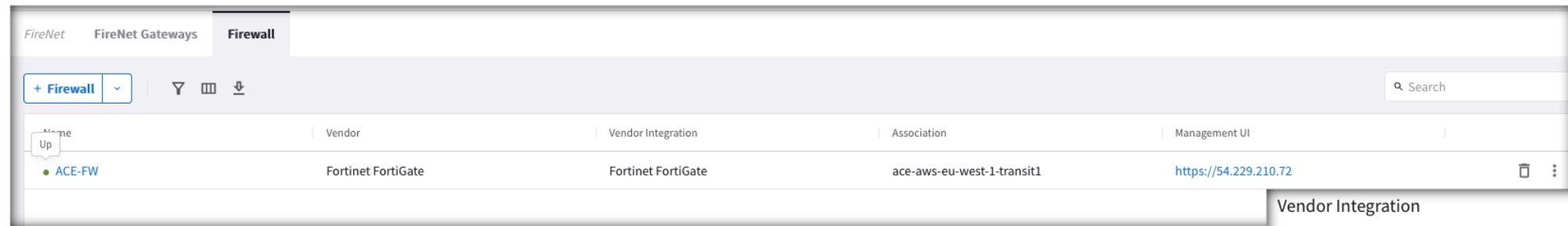
Destination	source	In Intf	protocol	Src Ports	Dst Ports
Gateway	Out Intf	Status	action	Comment	

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.*

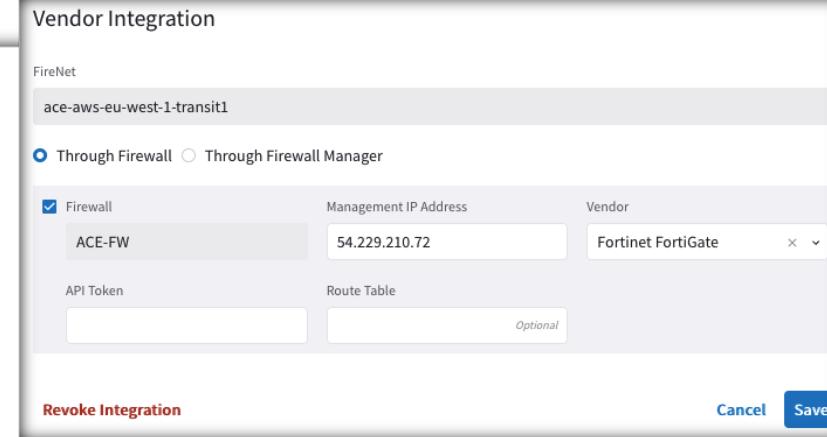


Information to Collect / Checklist



The screenshot shows the Aviatrix Cloud Fabric interface under the 'Firewall' tab. It displays a list of firewalls, with one entry for 'ACE-FW' (Fortinet FortiGate) selected. The details shown include the vendor as 'Fortinet FortiGate', the association as 'ace-aws-eu-west-1-transit1', and the management UI URL as 'https://54.229.210.72'. A search bar and various navigation icons are also visible.

- 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



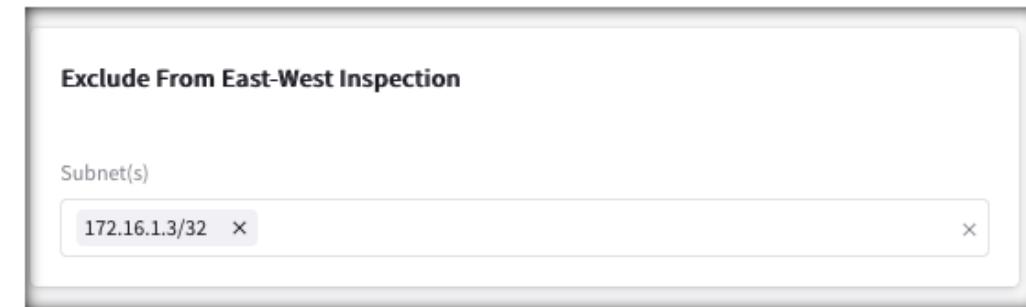
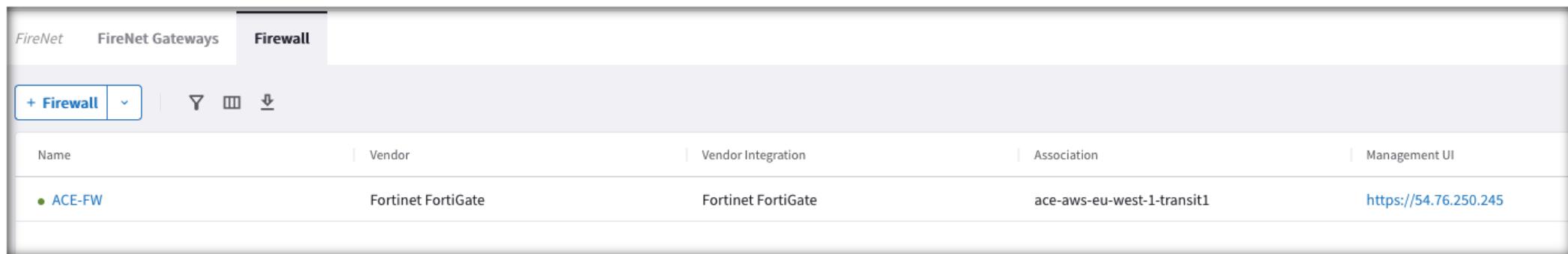
The screenshot shows the 'Vendor Integration' configuration dialog. It is set up for a 'Firewall' named 'ACE-FW' (Management IP Address: 54.229.210.72, Vendor: Fortinet FortiGate). The 'Through Firewall' option is selected. There is a 'Revoke Integration' button at the bottom left and 'Cancel' and 'Save' buttons at the bottom right.

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 / ?



Static Route Table:						
Destination	Gateway IP	Interface	Distance	Weight	Status	Comment
172.16.0.0/12	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration
192.168.0.0/16	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration
10.0.0.0/8	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration

Name	Vendor	Vendor Integration	Association	Management UI
ACE-FW	Fortinet FortiGate	Fortinet FortiGate	ace-aws-eu-west-1-transit1	https://54.76.250.245



Next:

Lab 3 FireNet - Interface
Lab 4 FireNet - Routes