



FireNet Operations

ACE Team

Aviatrix Transit Firewall Network (FireNet)



Scale out, multi-AZ FW deployments, bootstrapping



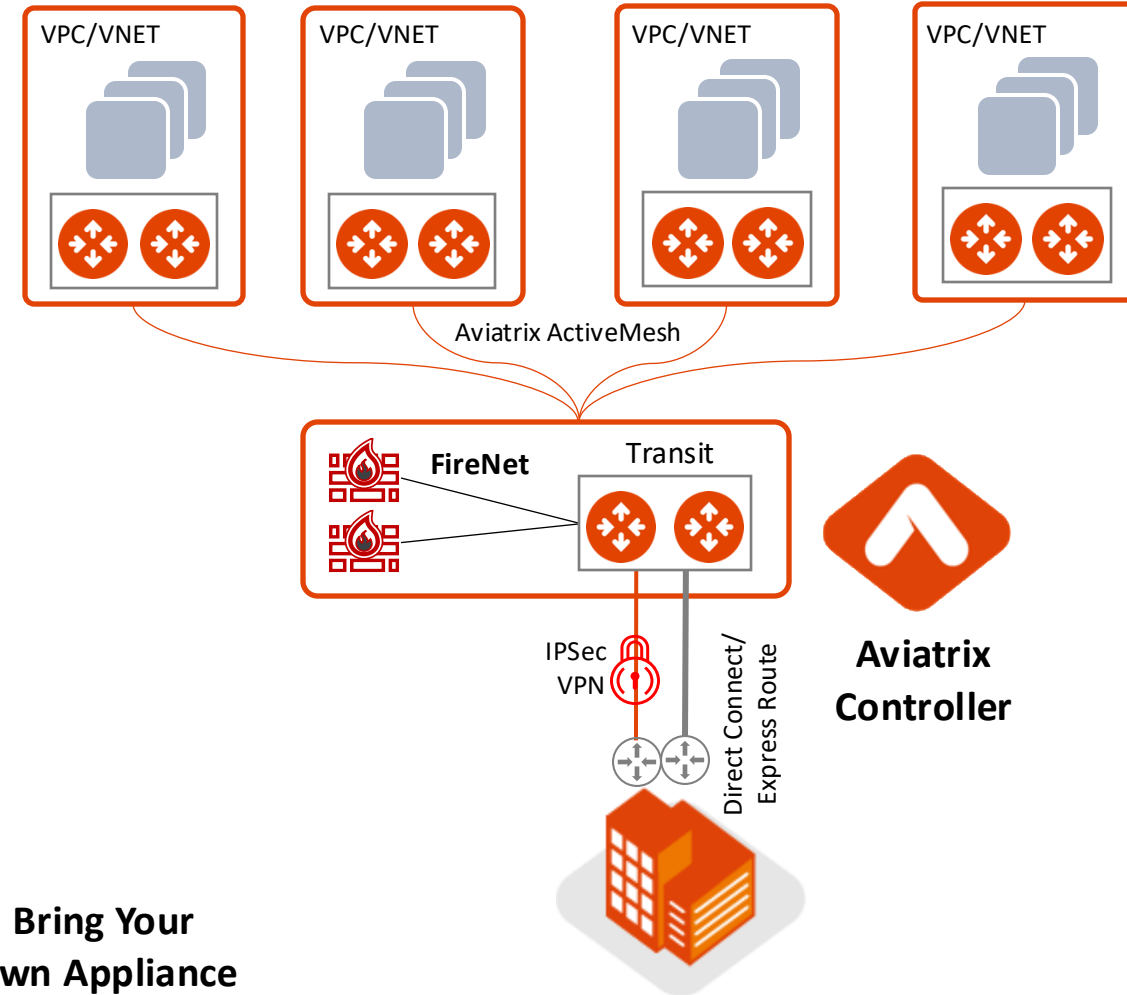
Automated route management, segmentation, and security policies



Deep visibility and operational capabilities



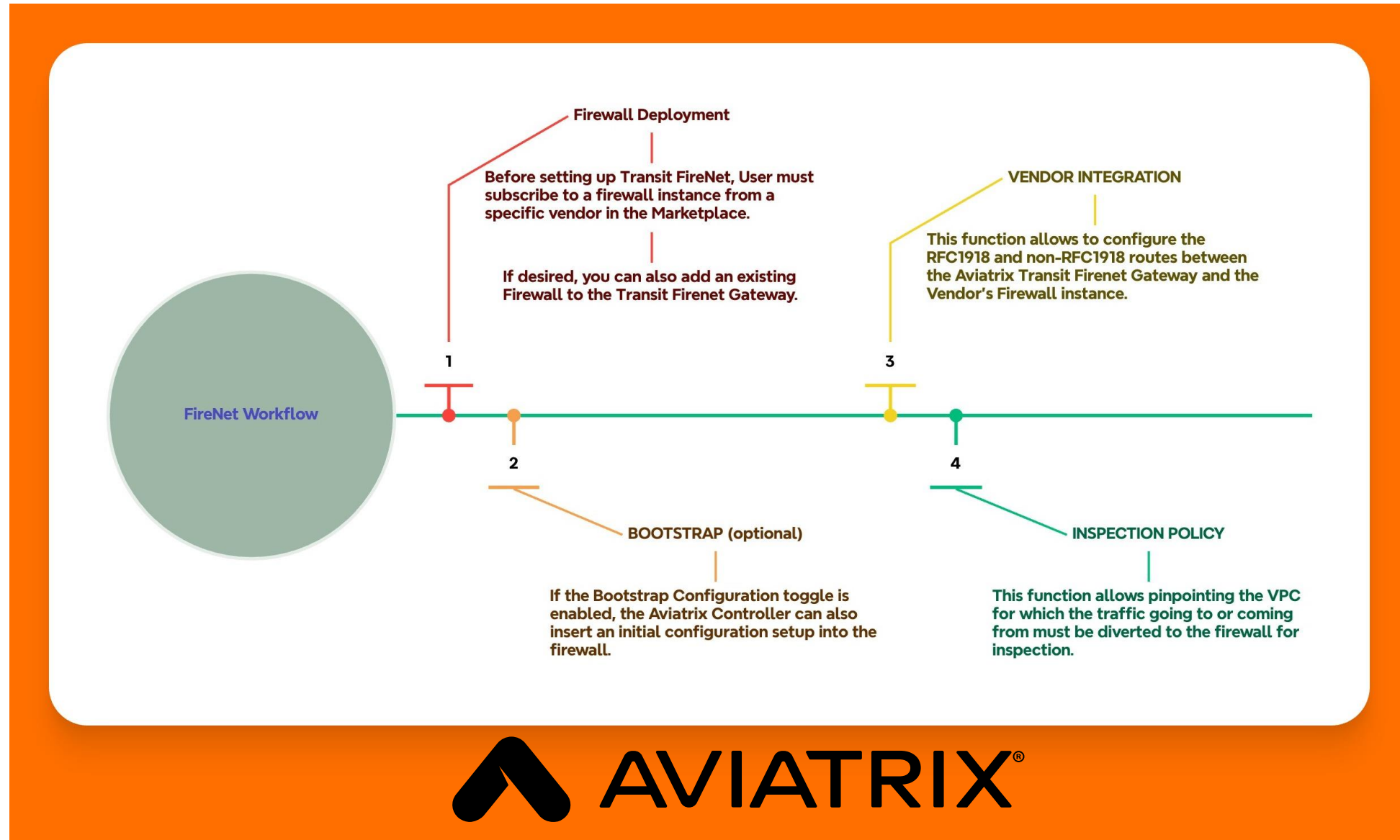
Repeatable across regions and clouds



Bring Your Own Appliance



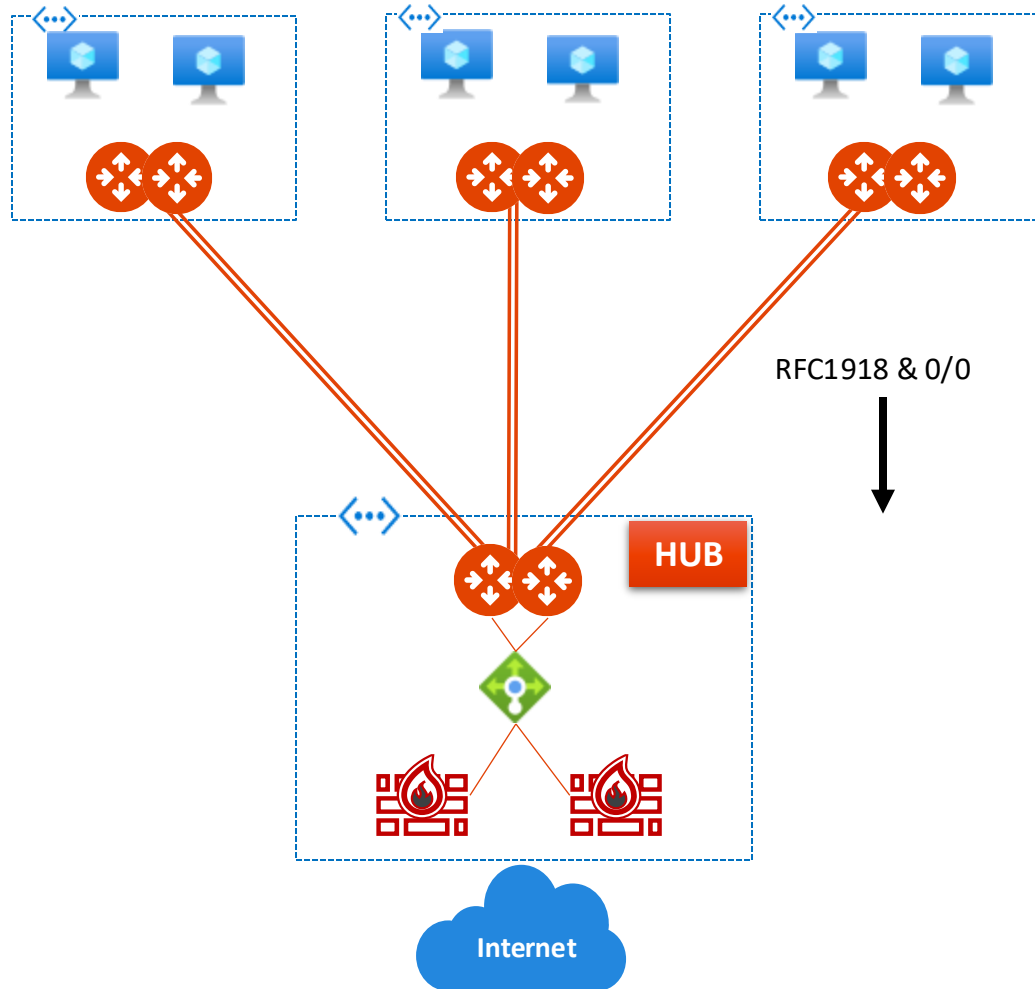
FireNet Deployment



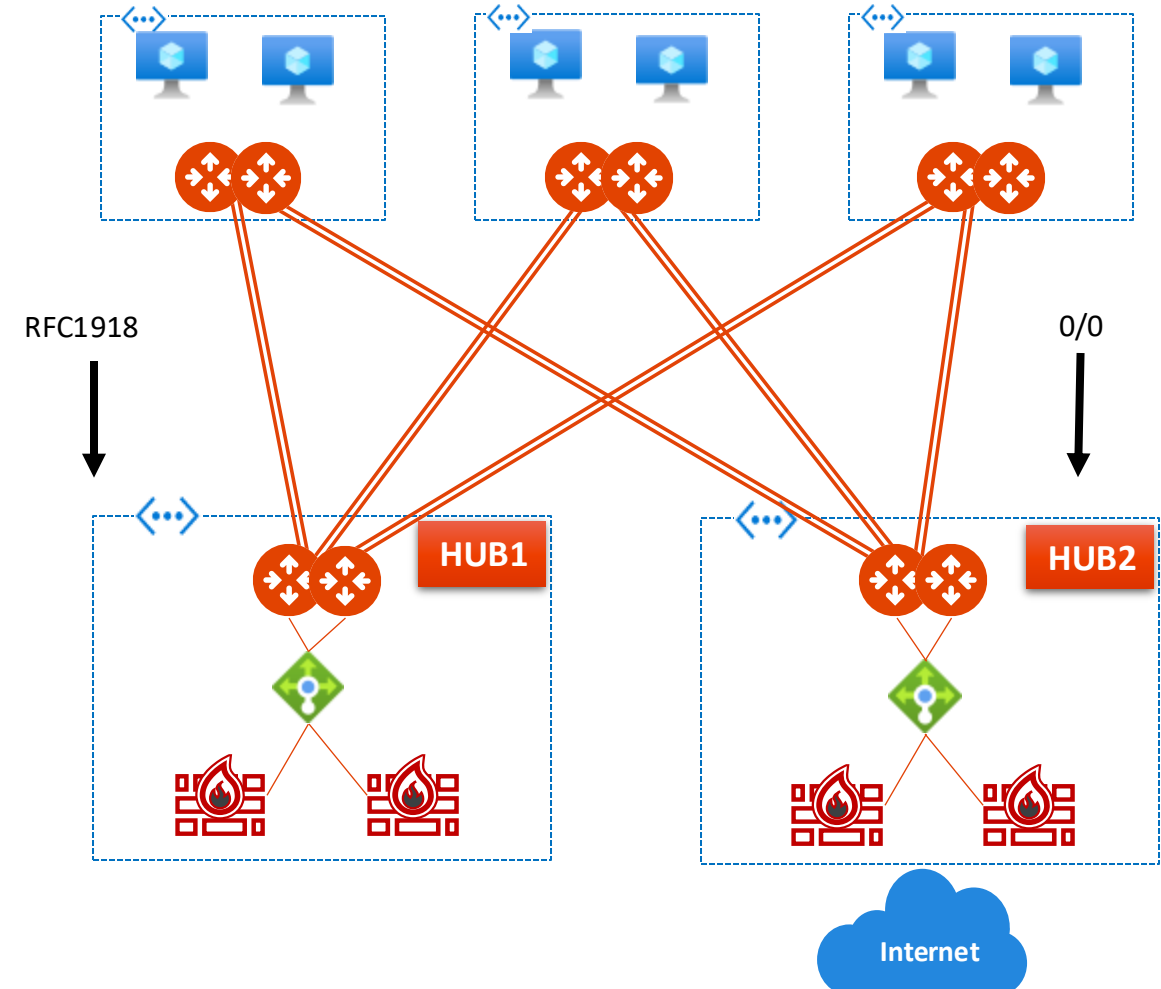
FireNet Architecture Options (Azure Example)

Each firewall set can scale independently based on need

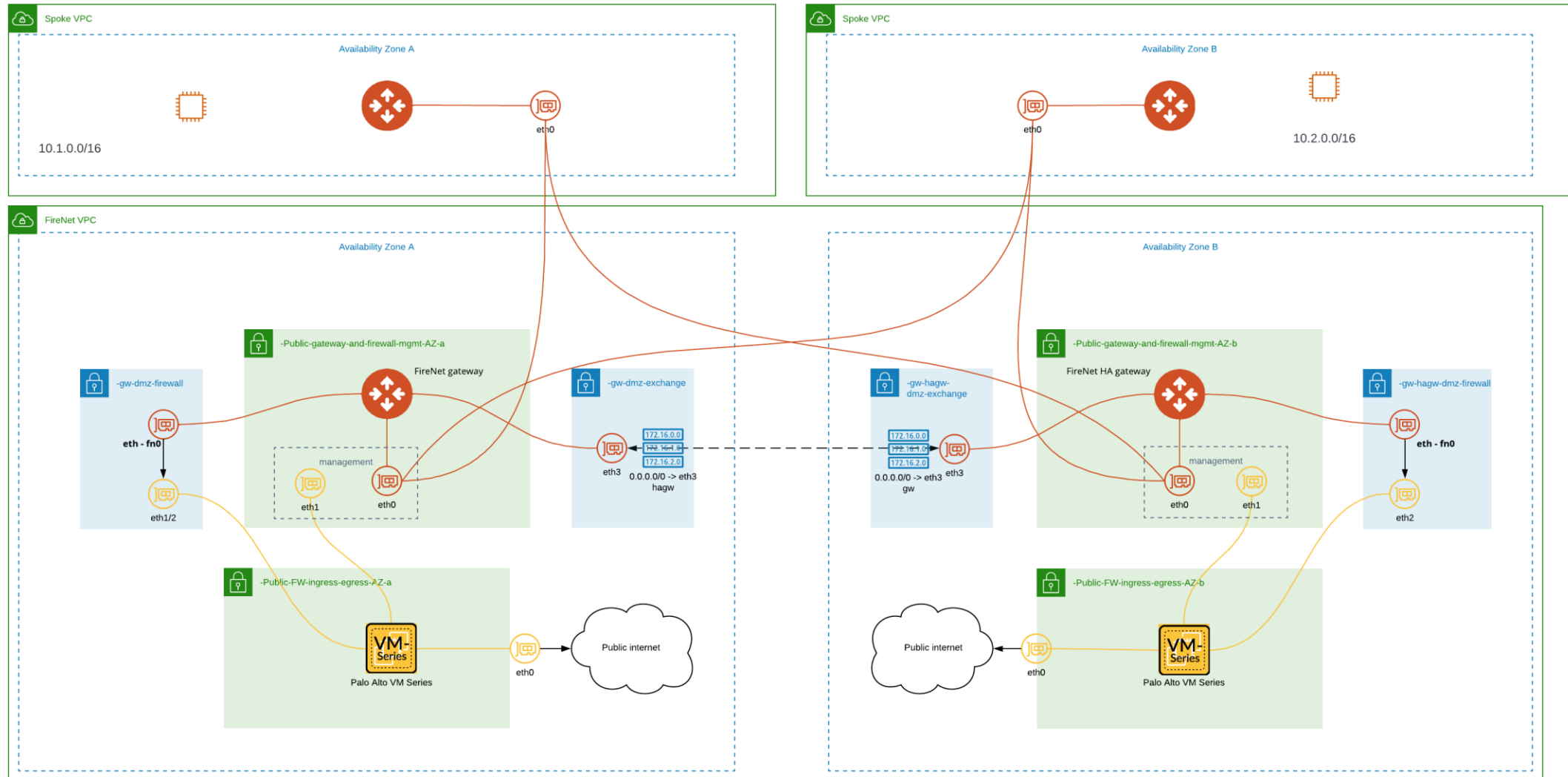
Single HUB FireNet



Dual HUB FireNet



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.

CoPilot

FireNet FireNet Gateways Firewall

+ Firewall

Name	Vendor
ACE-FW	Fortinet FortiGate

Deploy Firewall

⚠ After a firewall instance is launched, wait for 15 minutes for it to come up.

Association

FireNet Instance: ace-aws-eu-west-1-transit1 Attach Firewall to FireNet after Launching: ☒ Yes

Firewall Configuration

Name: FORTIGATE-FW

Firewall Image: Fortinet FortiGate Next-Generation Firewall

Firewall Image Version: (7.6.2) Firewall instance Size: c4.xlarge

Egress Interface Subnet: 10.1.200.0/28~~eu-west-1a~~ace-aws-eu-west-1-t... Key Pair Name: Optional

☐ Bootstrap Configuration

Cancel Deploy

Bootstrap (*optional*)

- **Botostrap 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.)

☒ Bootstrap Configuration

☒ Azure Storage ☐ User Data

Storage

pod74firenetbootstrap

Storage Access Key

aMef4Dlr3m9wh/T+9o73FPHonOSsVUC+AStlPOrhQ==

File-Share Folder

pod74-firenet-bootstrap

Share-Directory

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

☒ Firewall

ACE-FW

Management IP Address

52.49.101.236

Vendor

Palo Alto Networks VM- ... x v

Username

avxadmin

Password

Route Table

Optional

Revoke Integration

Cancel

Save

ACE-FW

Name: ACE-FW

Vendor: Fortinet FortiGate

Public IP: 54.76.250.245

Static Route Table:

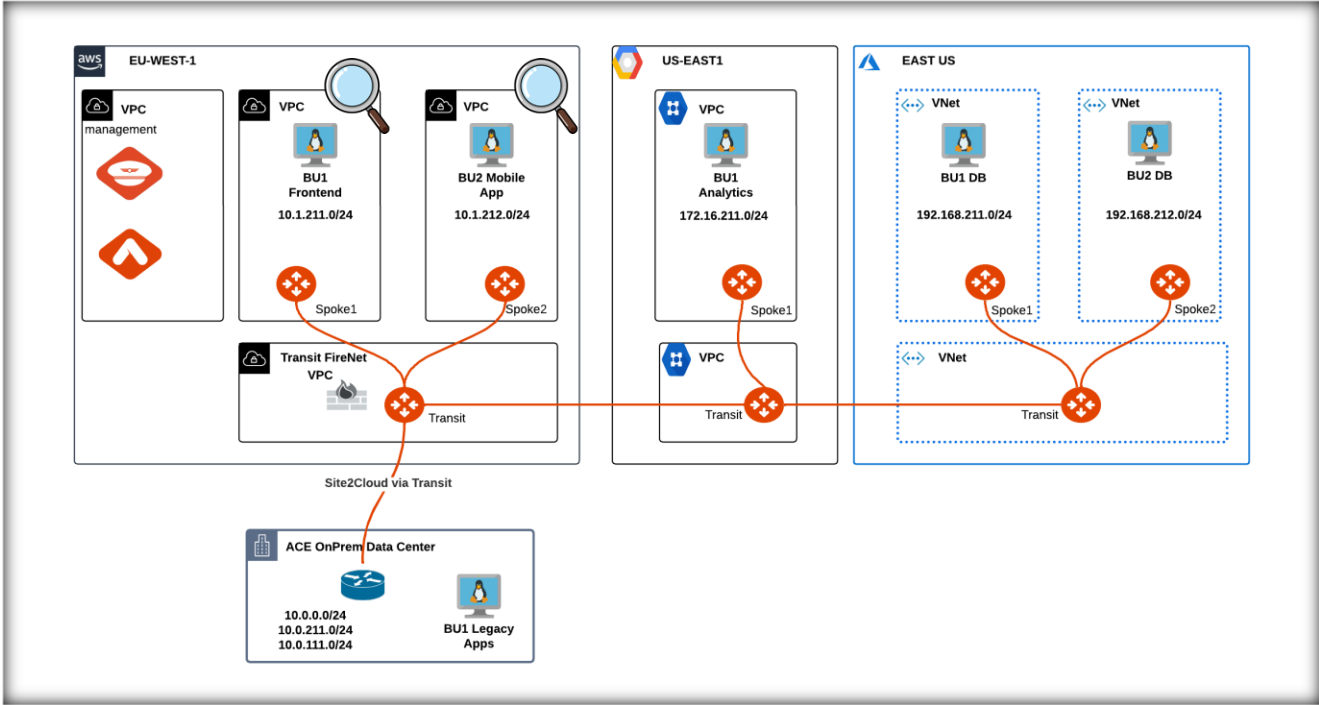
Destination	Gateway IP	Interface	Distance	Weight	Status	Comment
172.16.0.0/12	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration
192.168.0.0/16	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration
10.0.0.0/8	10.1.200.65	port2	10	0	enable	Aviatrix Vendor Integration

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.



FireNet

FireNet Gateways

Firewall

<

ace-aws-eu-west-1-transit1

✎

🗑

Firewall

Policy

VPC/VNet Route Tables

Vendor Integration

Settings

Actions

Azure Spoke Subnet Groups

🔍

📄

⬇

<input type="checkbox"/> Name	Type ↓	Inspection
<input type="checkbox"/> ace-aws-eu-west-1-spoke1	SPOKE	On
<input type="checkbox"/> ace-aws-eu-west-1-spoke2	SPOKE	On
<input type="checkbox"/> ACE-ONPREM-DC	SITE2CLOUD	Off
<input type="checkbox"/> ace-gcp-us-east1-transit1	PEERING	Off
<input type="checkbox"/> ace-azure-east-us-transit1	PEERING	Off

Information to Collect / Checklist

FireNet				
FireNet Gateways				
Firewall				
Name	Vendor	Vendor Integration	Association	Management UI
Up ACE-FW	Fortinet FortiGate	Fortinet FortiGate	ace-aws-eu-west-1-transit1	https://54.229.210.72

- 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

Vendor Integration

FireNet

ace-aws-eu-west-1-transit1

☒ Through Firewall ☐ Through Firewall Manager

☒ Firewall

ACE-FW

Management IP Address: 54.229.210.72

Vendor: Fortinet FortiGate

API Token:

Route Table: Optional

Revoke Integration

Cancel Save

Information to Collect - Checklist for the Support Team

- Aviatrix CoPilot version
- 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 / ?

Aviatrix CoPilot
 v4.3.1 | Appliance v3

Aviatrix Controller 184.72.224.60
 v7.1.2131

[Documentation](#)
[Support Portal](#)

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	

Exclude From East-West Inspection

Subnet(s)

172.16.1.3/32
 ×

FireNet				
FireNet Gateways				
Firewall				
<div>+ Firewall</div> <div> <div></div> <div></div> <div></div> </div>				
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