



# FireNet Operations

ACE Solutions Architecture Team

# Aviatrix Transit Firewall Network (FireNet)



Scale out, multi-AZ FW deployments, bootstrapping



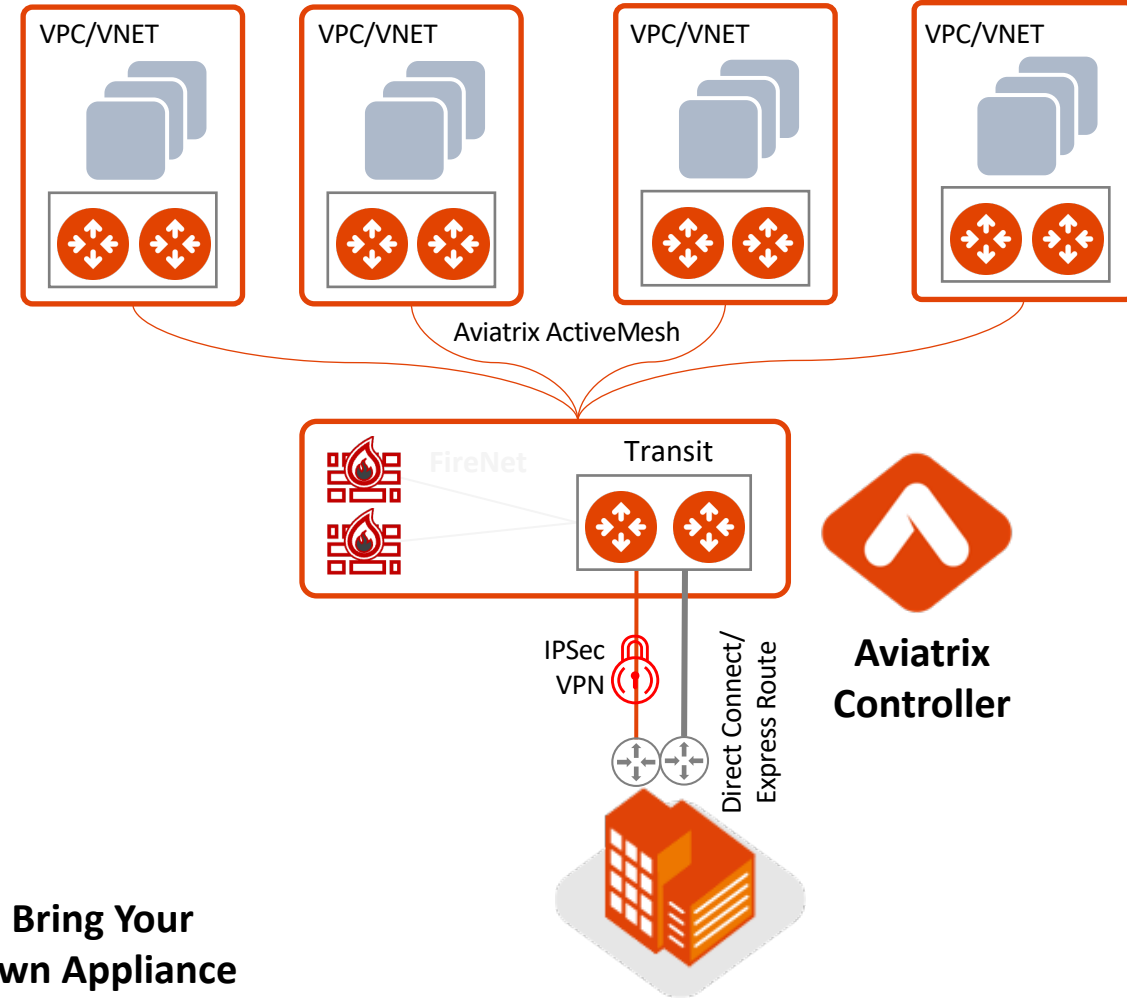
Automated route management, segmentation, and security policies



Deep visibility and operational capabilities



Repeatable across regions and clouds



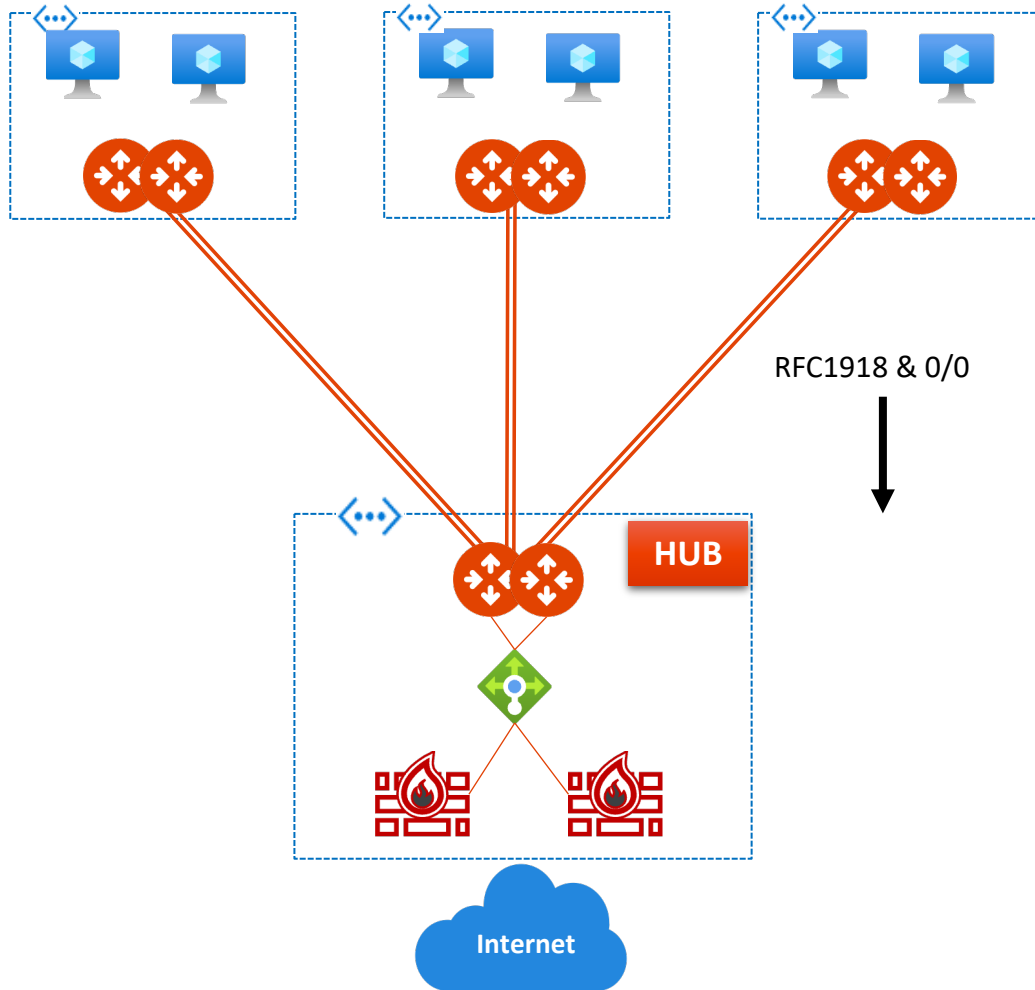
Bring Your Own Appliance



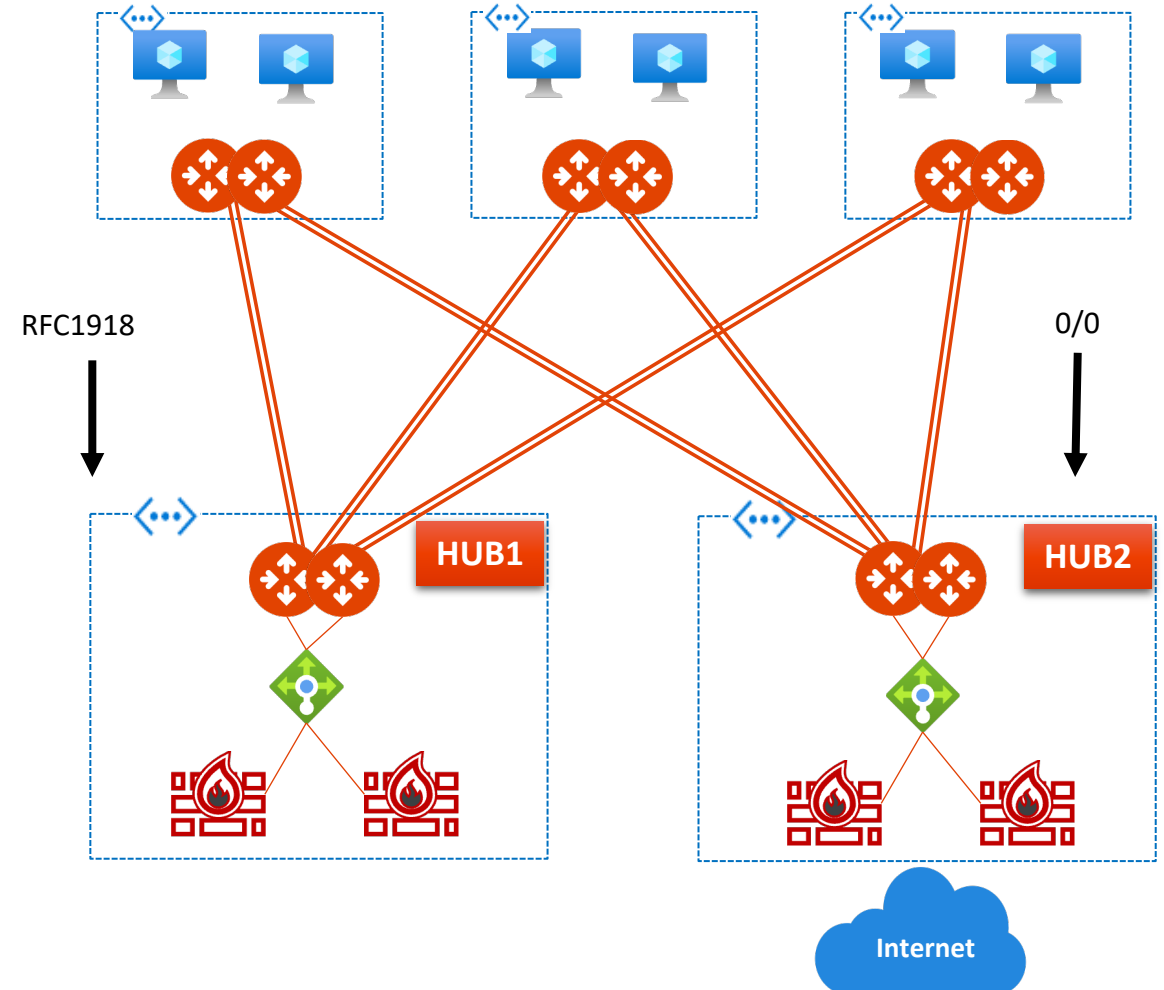
# FireNet Architecture Options (Azure Example)

Each firewall set can scale independently based on need

Single HUB FireNet



Dual HUB FireNet



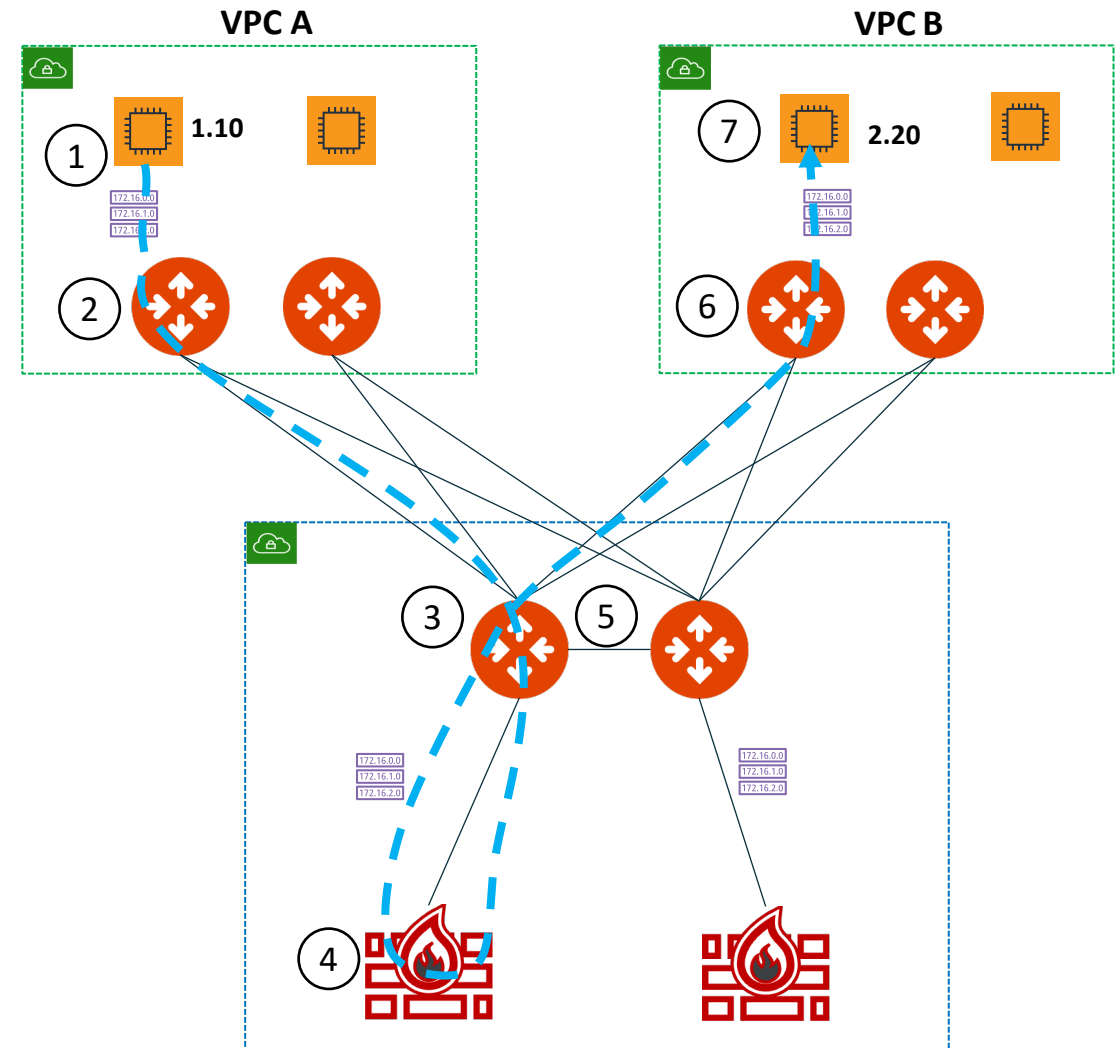
# FireNet Packet Walk – AWS Example



## 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.

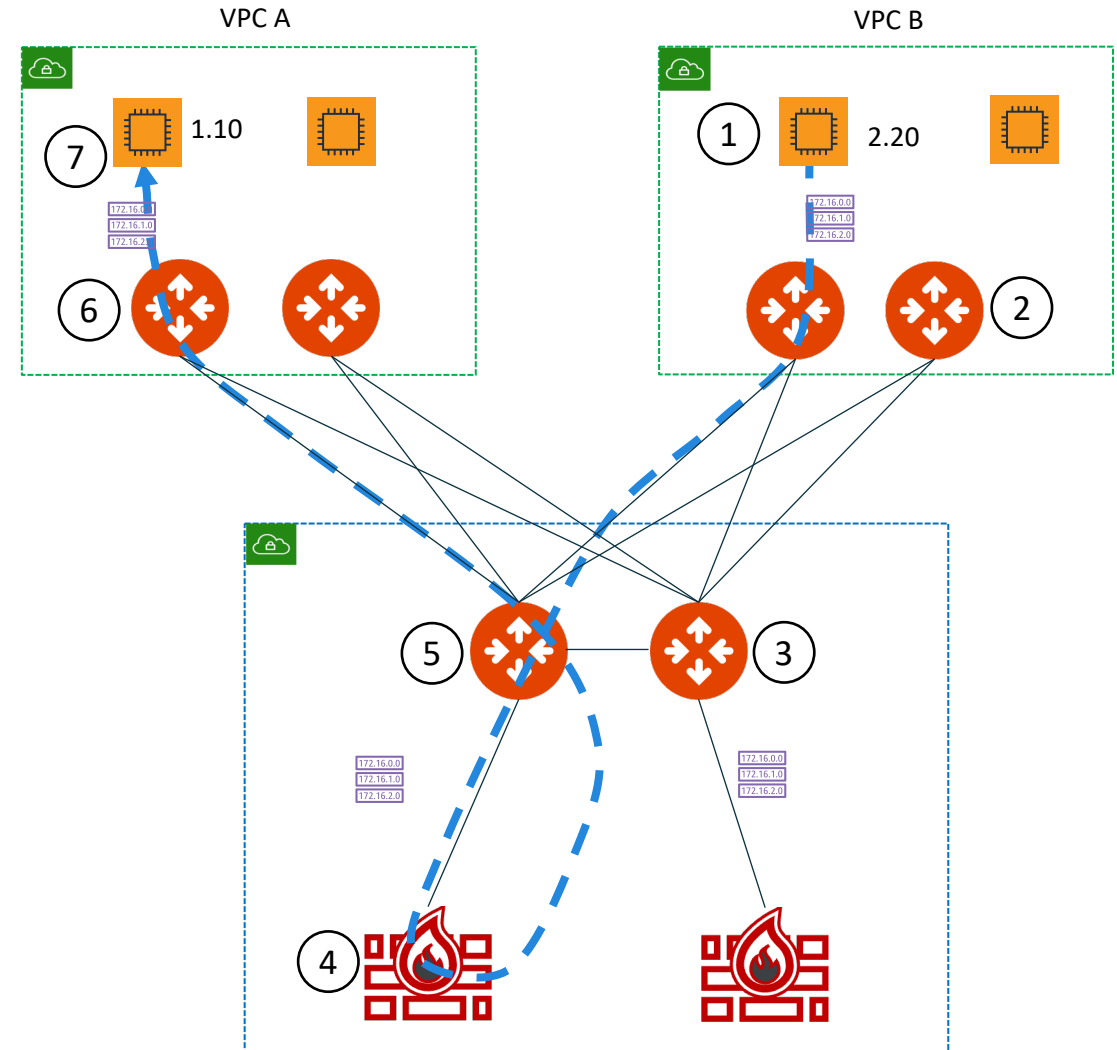
## Aviatrix Transit tracks the health of Firewall



# 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.



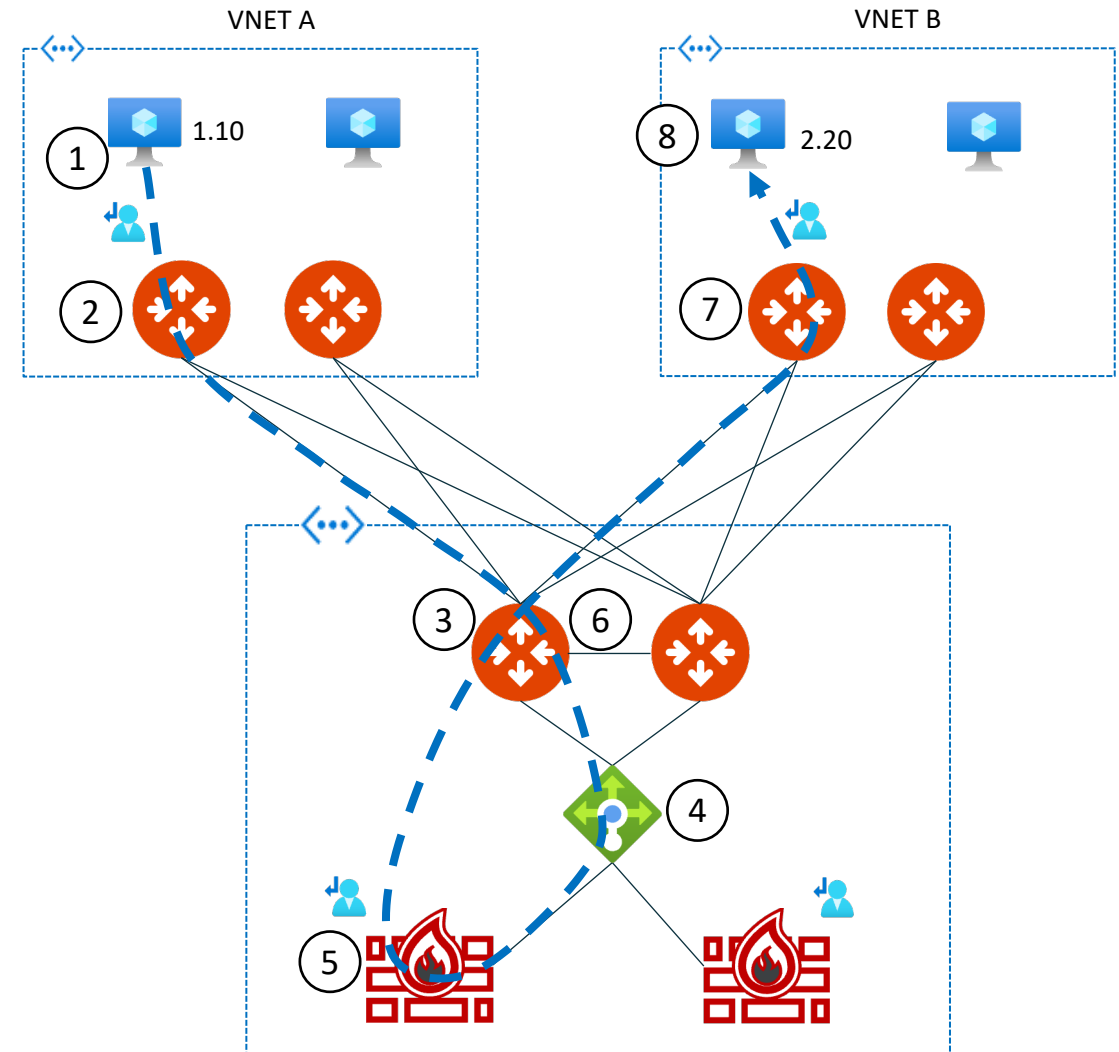
# FireNet Packet Walk – Azure Example

## A Host 1.10 communicating with 2.20 with VNET 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 the inspection policy to determine if either source or destination requires FireNet. If a match, traffic is redirected to Azure ILB.
4. The Azure ILB will perform a 5-tuple hash to send the traffic to one of the backend pool members.
5. The Firewall selected will process the packet and send the traffic back to its defined Transit Gateway.
6. The Aviatrix Transit Gateway will receive the processed packet and forward (ECMP) with 5-tuple hash towards the destination spoke.
7. The spoke gateway will receive the traffic and route the traffic out its local interface to the Azure VNET route table.
8. The destination will receive the original traffic and see this as native Azure communication flows.

### ILB tracks the health of Firewall

Health check is not configurable in Azure via Controller

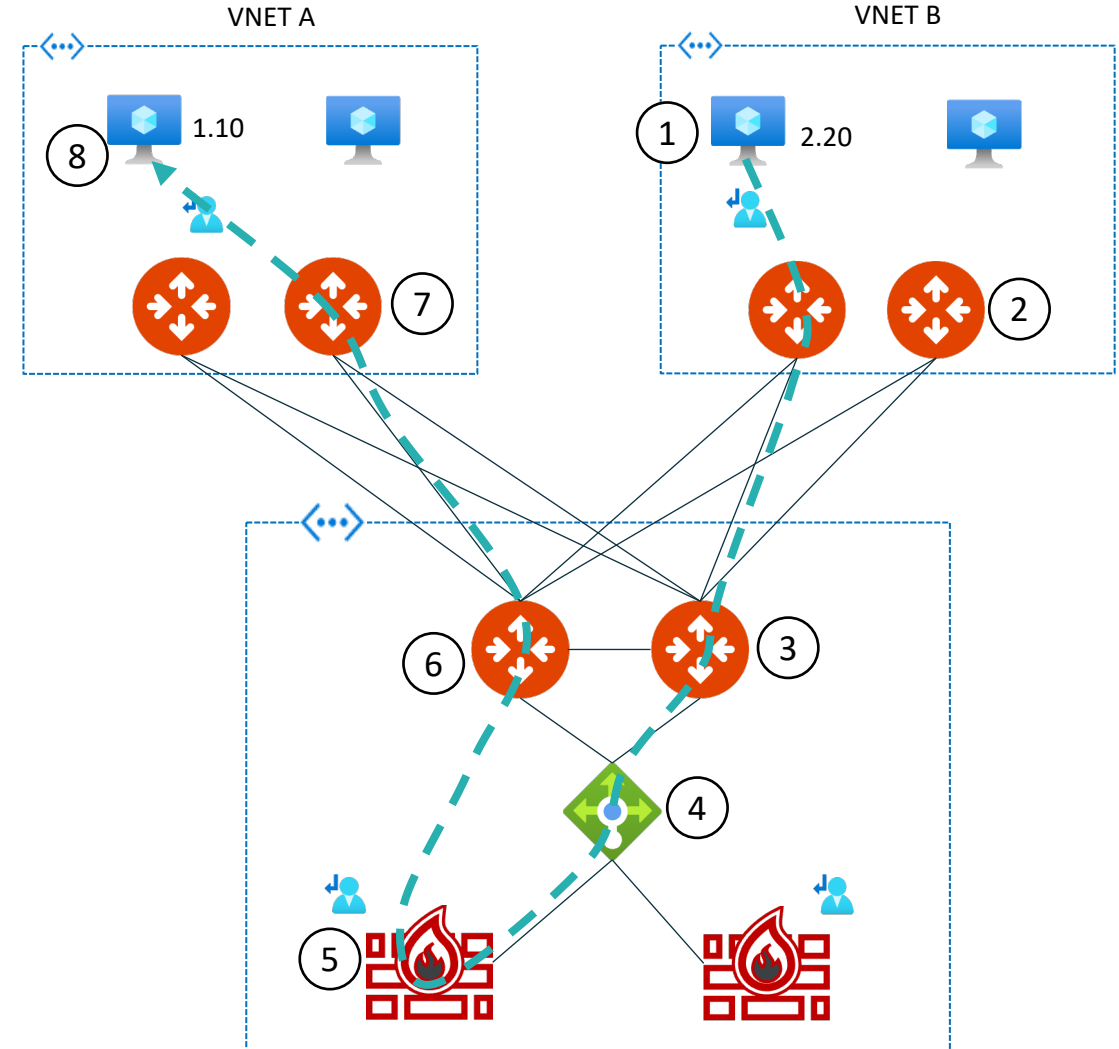


# FireNet Packet Walk – Azure Example



**Return Flow: 1.10 communicating with 2.20 with VNET A inspected via FireNet**

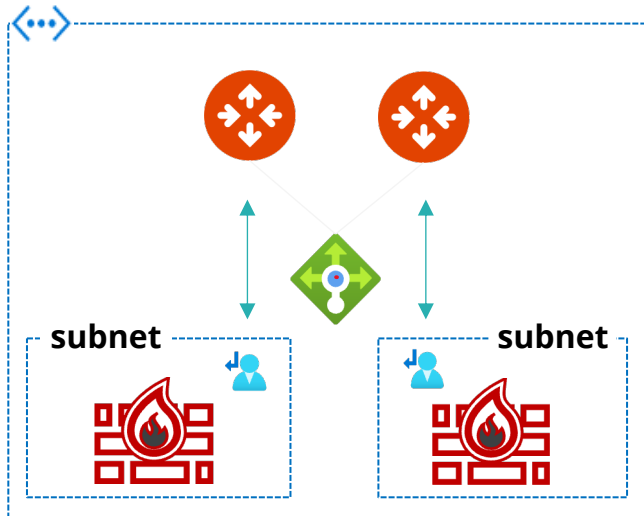
1. The local route table for 2.20 has RFC1918 routes pointed to its local spoke gateway for return traffic.
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways.
3. The Aviatrix Transit Gateway receiving the traffic will pass the traffic to the ILB. The gateway will PBR the traffic back to the ILB for FireNet.
4. The Azure load balancer will hash the traffic however, the reverse flow hash will match the initial flow to ensure symmetry.
5. The stateful Firewall will process the return traffic and route the traffic back to its designated gateway.
6. The Aviatrix gateway will ECMP traffic with 5-tuple hash to one of the destination spoke gateways.
7. The destination spoke gateway will route this traffic out its local interface to the native Azure route table
8. The original source will receive the return traffic and see this as native Azure communication flows



# FireNet in Azure – 3 States

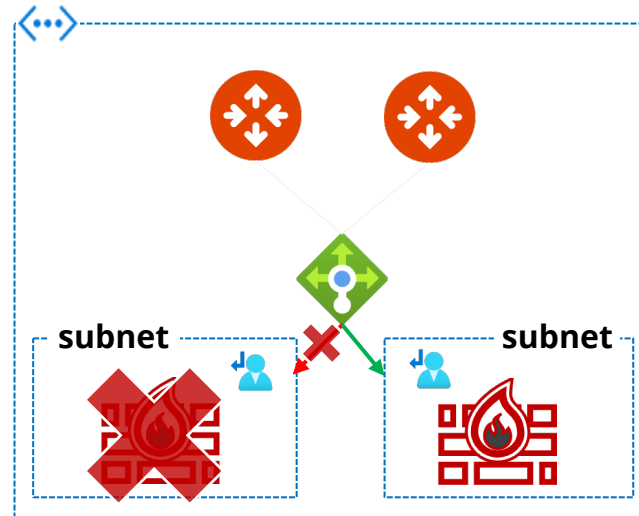
## Steady State

- Each Firewall is associated to an Aviatrix Transit GW
- Firewalls are part of the LB backend pool
- UDR in each Firewall subnet point to a single gateway



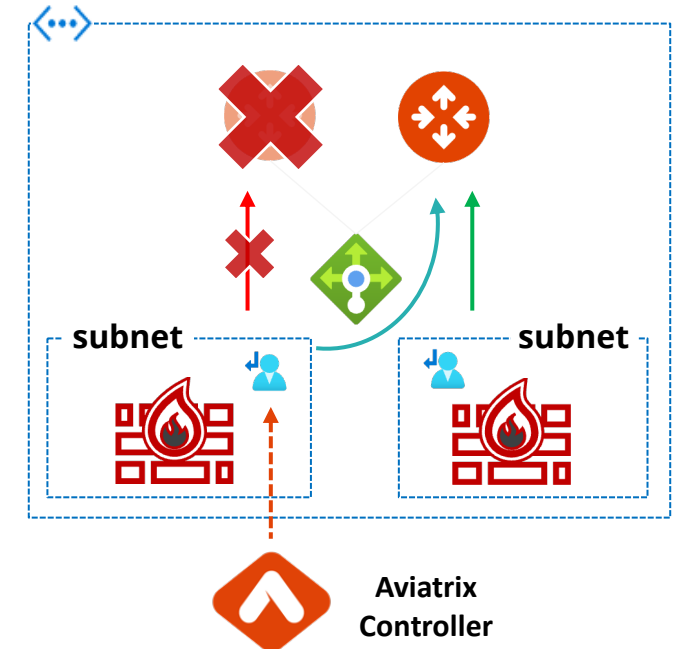
## Firewall Failure State

- Each Firewall is associated to an Aviatrix Transit GW
- Firewalls are part of the LB backend pool
- If Firewall fails, LB will remove the firewall from the backend pool



## Gateway Failure State

- Each Firewall is associated to an Aviatrix Transit GW
- UDR in each Firewall subnet point to a single gateway
- If Gateway fails, an API call is made to update the UDR to point to the other healthy gateway

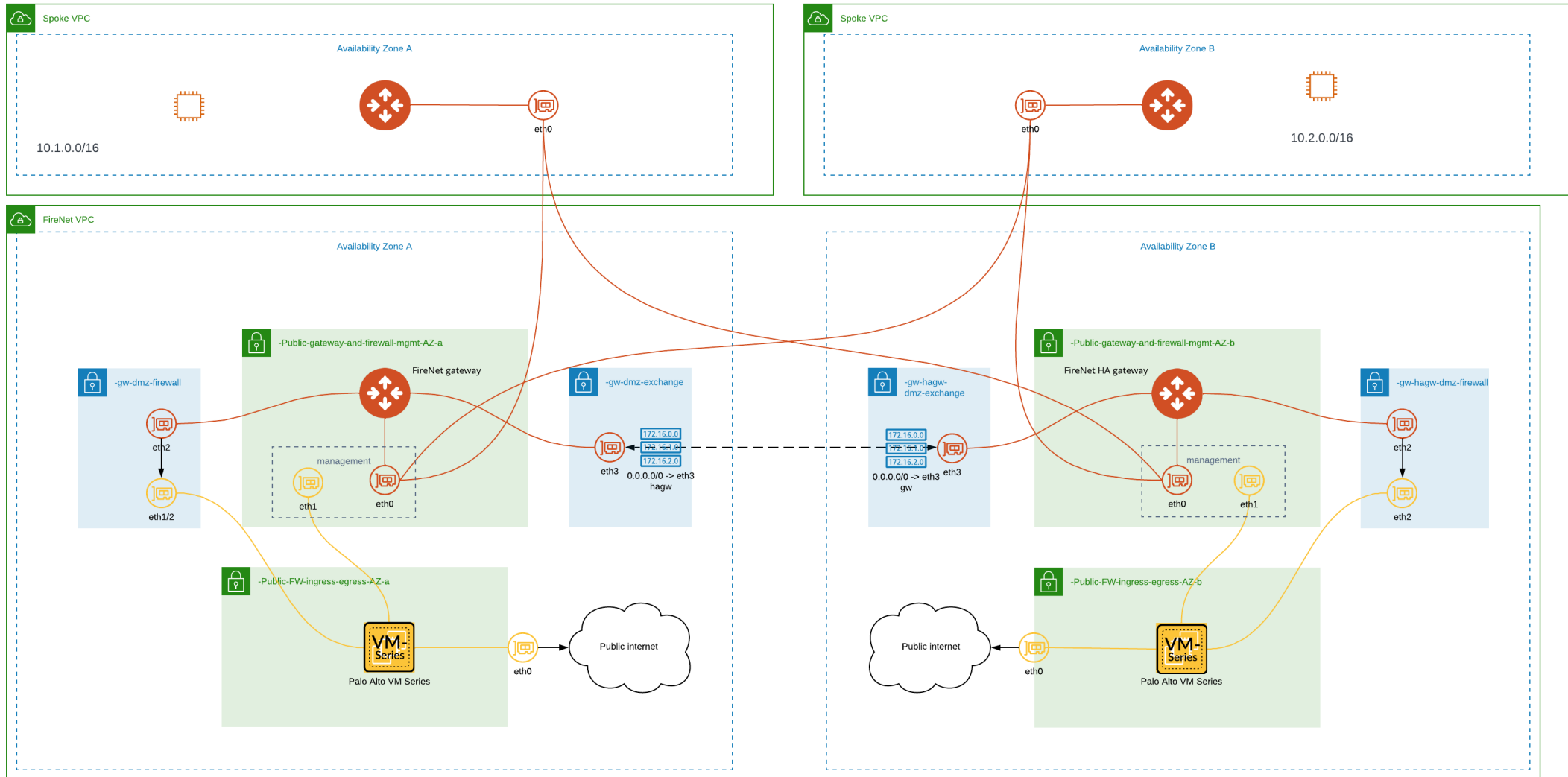






# Tools for Operating your FireNet

# FireNet – Under the hood



# Firewall Deployment Workflow

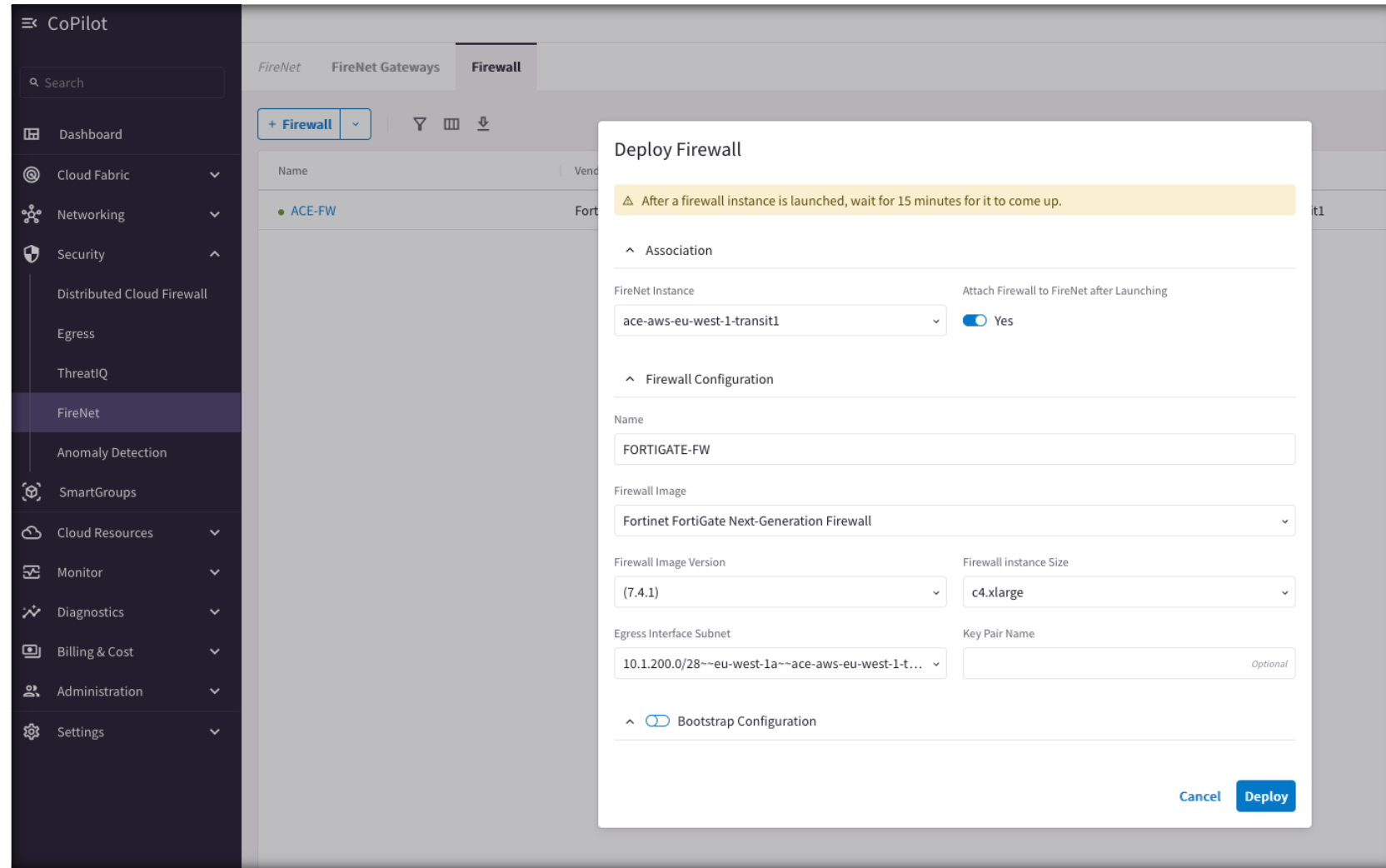


- **PATH:** Security > FireNet > Firewall

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*)

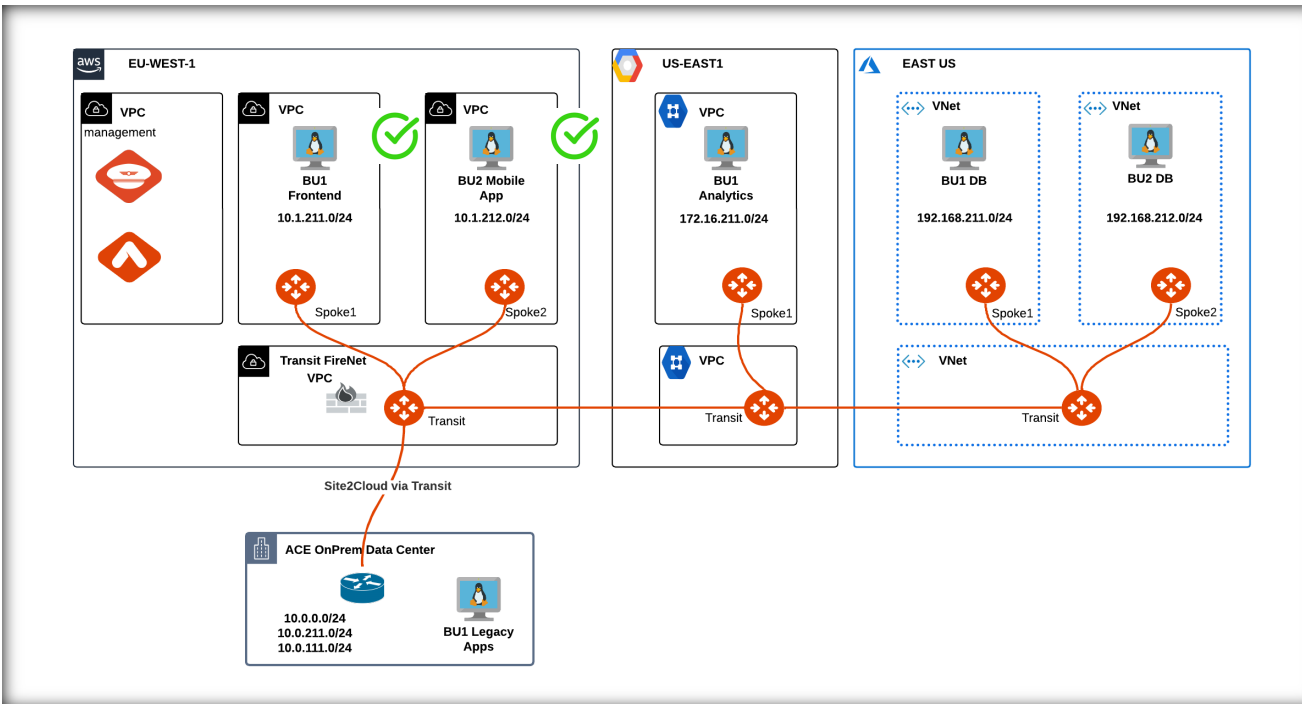
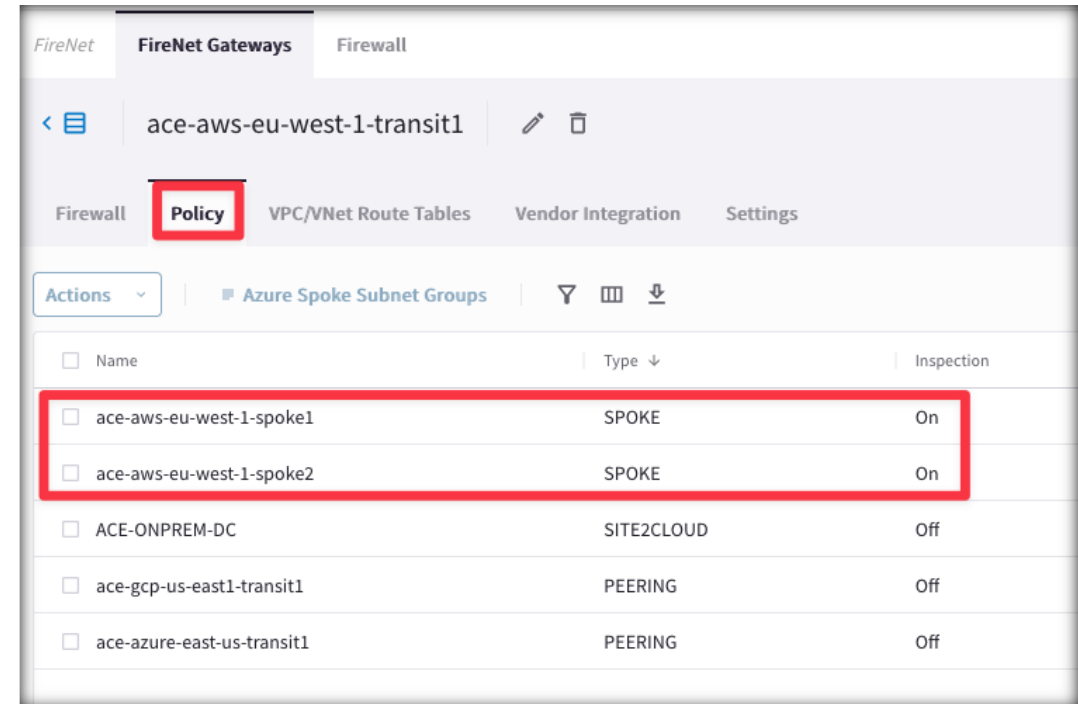
- **Supported Firewall Vendors:** Palo Alto VM-Series, Check Point CloudGuard, Fortinet FortiGate, BYOA

- **Panorama** is also supported as a firewall manager for Palo Alto VM-Series.



# Inspection Policy

- On the FireNet Policy tab you can add or remove **inspection policies** for the selected FireNet. 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.

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

# 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

aws-syd-transit-firenet-2

☒ Through Firewall
 ☐ Through Firewall Manager

☒ Firewall

aws-syd-fw-2

Management IP Address

3.105.242.193

Vendor

Fortinet FortiGate

API Token

Route Table

Optional

☒ Firewall

aws-syd-fw-2-1

Management IP Address

54.79.150.86

Vendor

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	

# Information to Collect / Checklist

FireNet				
FireNet Gateways				
Firewall				
<div>+ Firewall</div> <div> <div>Up</div> <div>ACE-FW</div> </div>				
Name	Vendor	Vendor Integration	Association	Management UI
ACE-FW	Fortinet FortiGate	Fortinet FortiGate	ace-aws-eu-west-1-transit1	<a href="https://54.229.210.72">https://54.229.210.72</a>

- 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

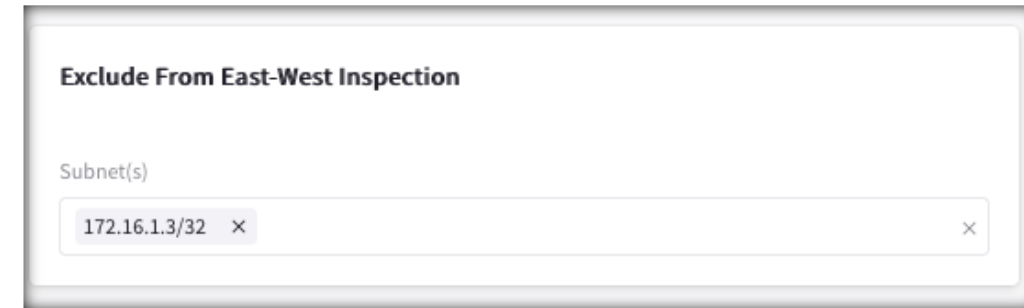
- Aviatrix Controller version
- Firewall Vendor
- Transit FireNet: Inspection Policy
  - Is the Spoke VPC/VNet supposed to be Inspected at all?
- E/W Traffic inspection enabled?
- Egress Traffic inspection enabled?
- Ingress Traffic enabled and working?
- Exclude list created for CIDR/IP from being inspected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



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



FireNet				
FireNet Gateways				
Firewall				
+ Firewall				
Name	Vendor	Vendor Integration	Association	Management UI
ACE-FW	Fortinet FortiGate	Fortinet FortiGate	ace-aws-eu-west-1-transit1	<a href="https://54.76.250.245">https://54.76.250.245</a>



Next:

Lab 3 FireNet - Interface

Lab 4 FireNet - Routes