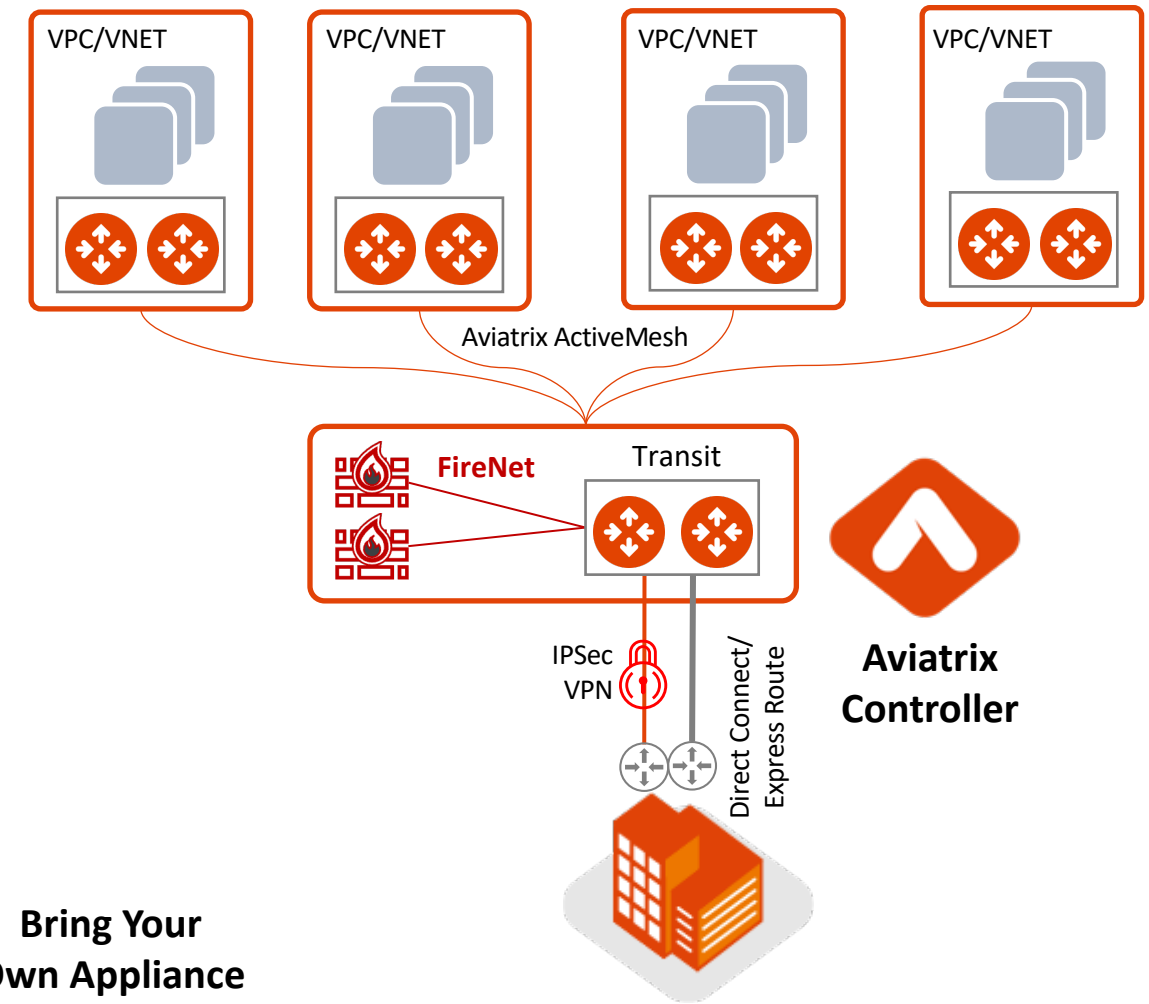
aviatrix

FireNet Operations

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

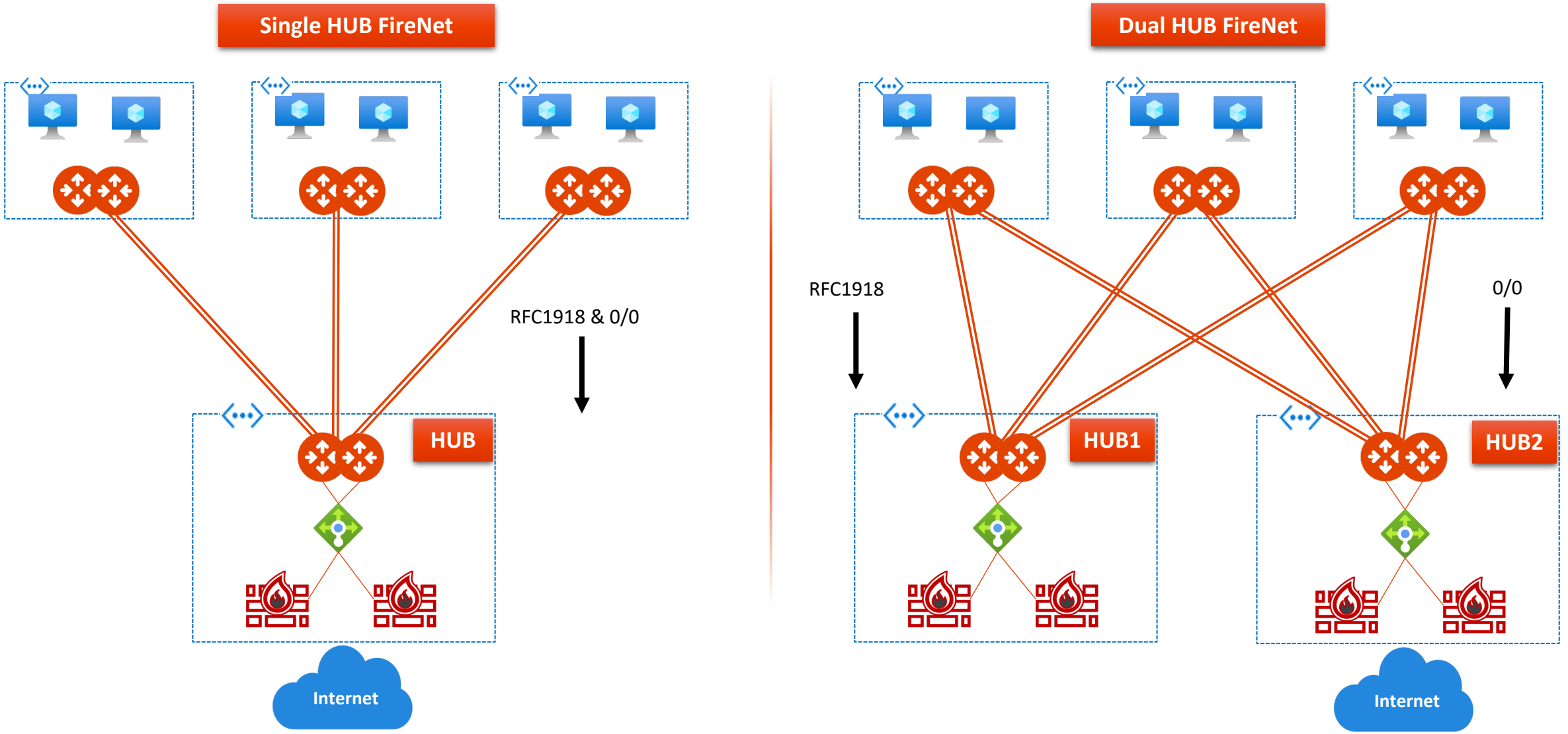
f5

Bring Your Own Appliance

aviatrix

FireNet Architecture Options (Azure Example)

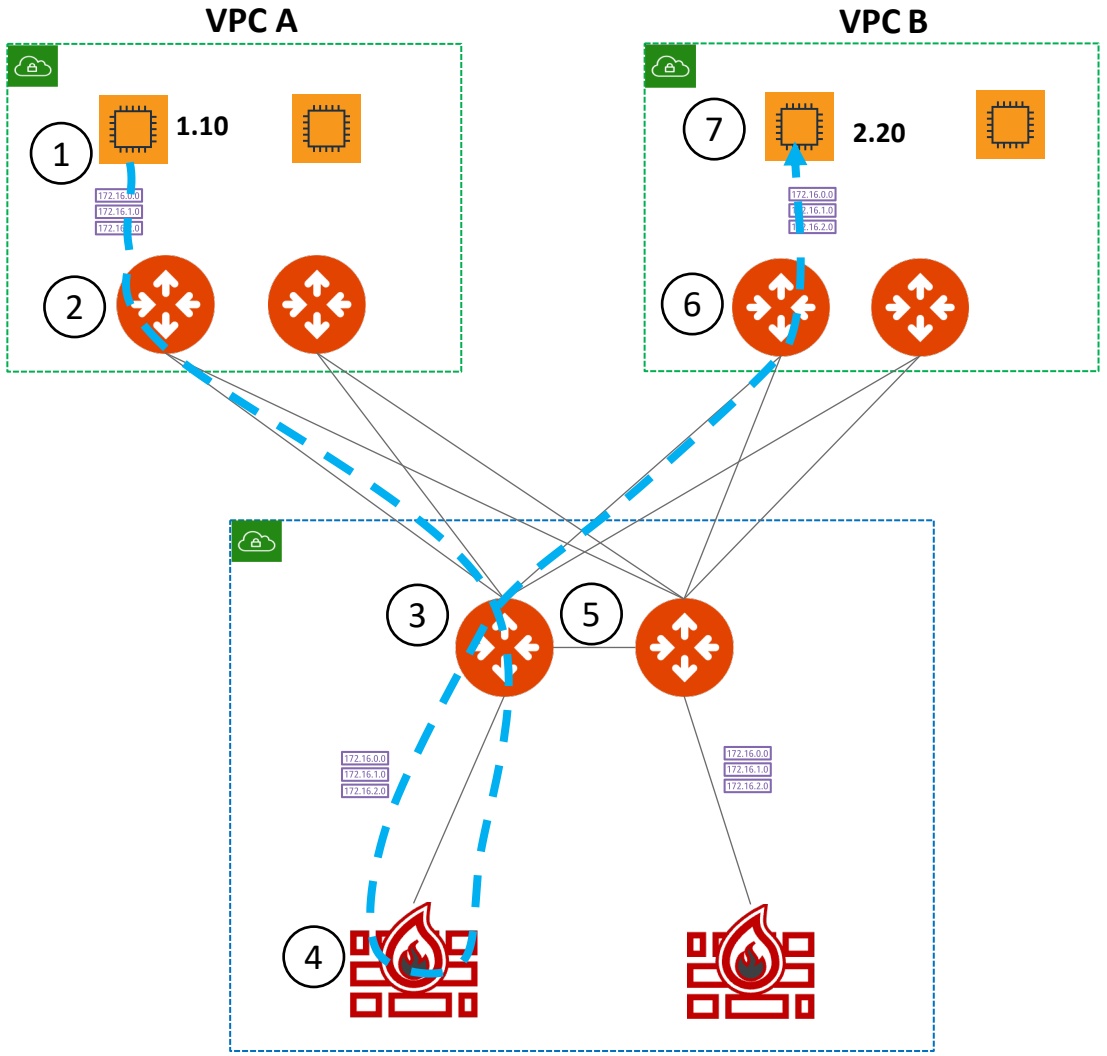
Each firewall set can scale independently based on need



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.

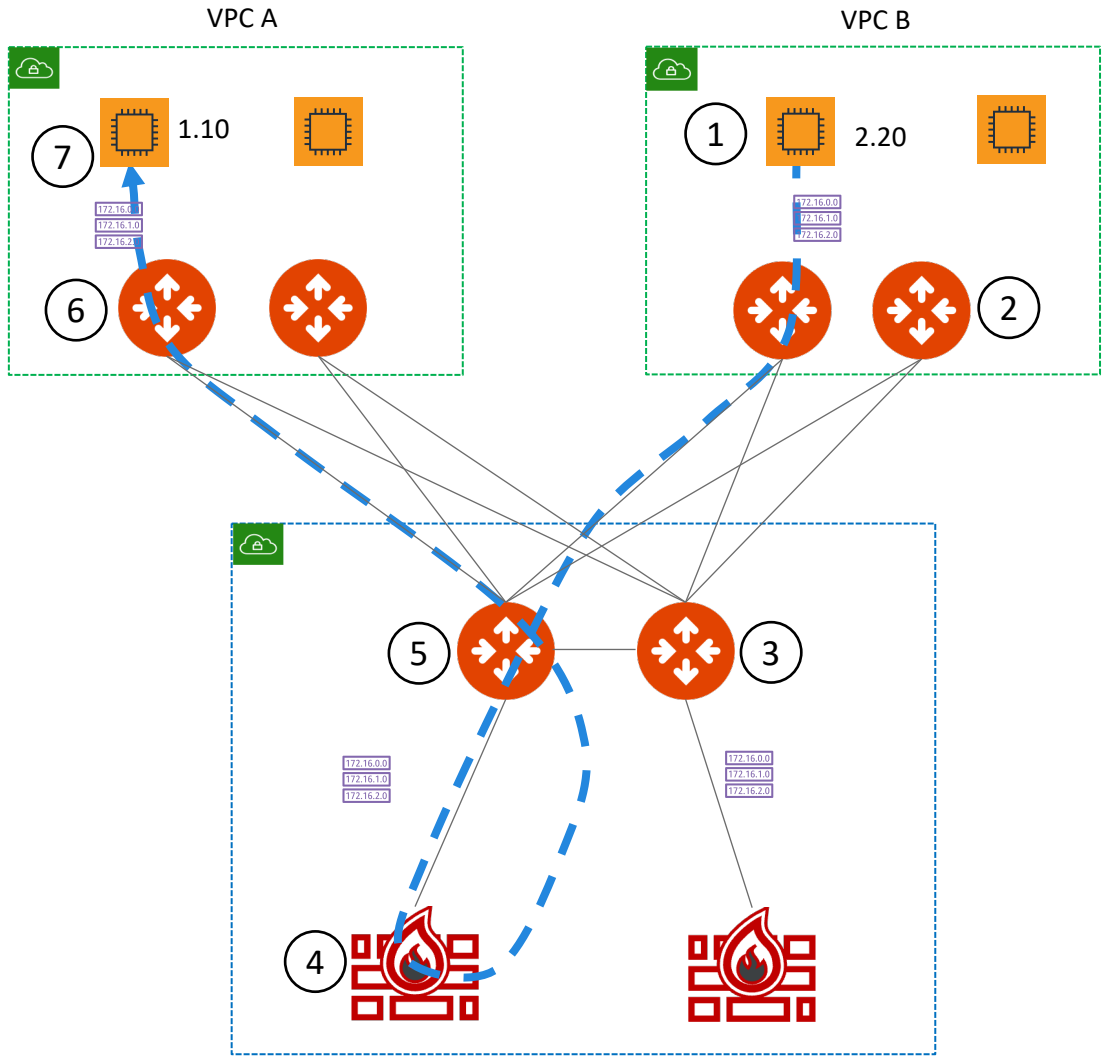


Aviatrix Transit tracks the health of Firewall

FireNet Packet Walk – AWS Example

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

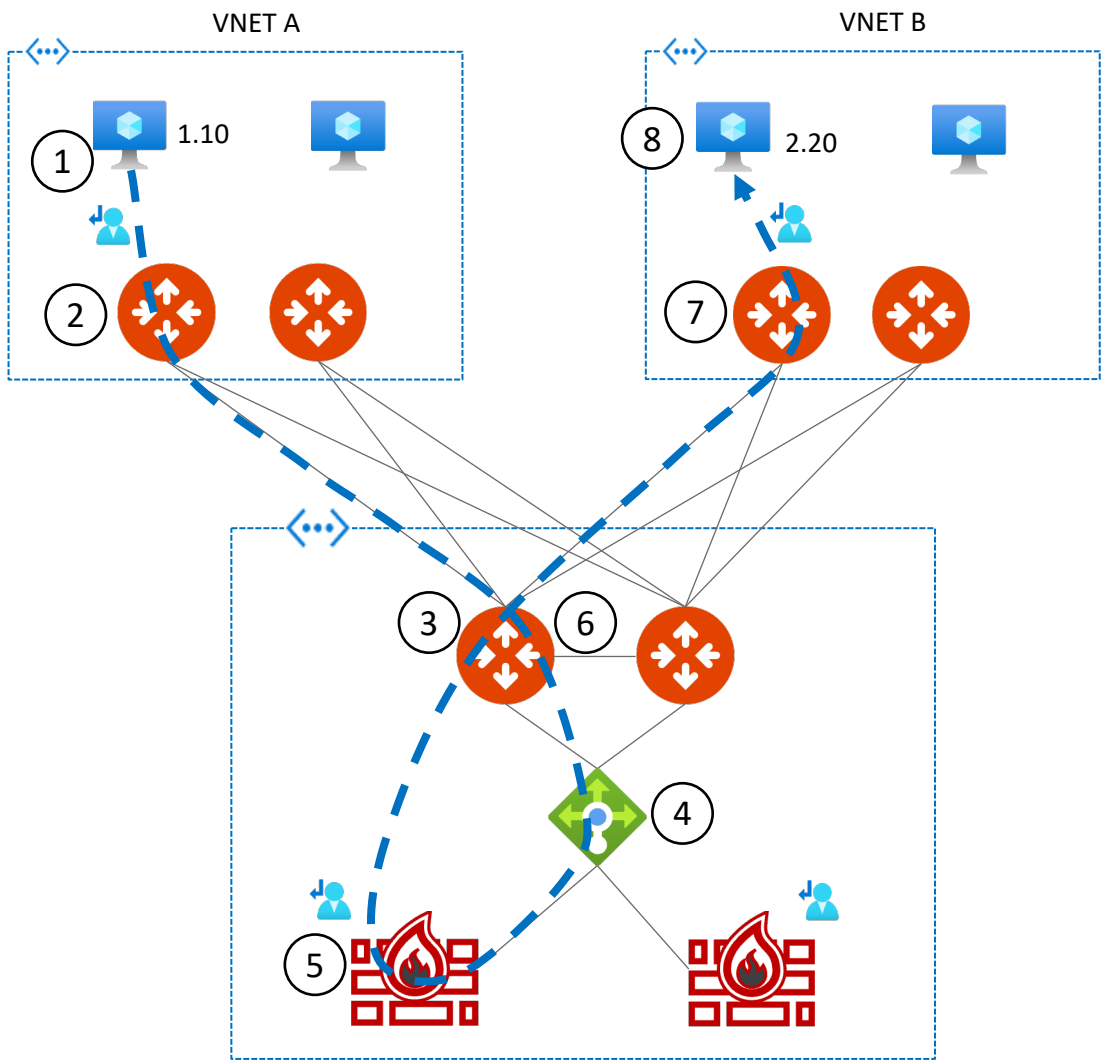
1. The local route table for 2.20 has RFC1918 routes pointed to its local spoke gateway for return traffic.
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways.
3. The Aviatrix Transit Gateway receiving the traffic will pass the traffic to the 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 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.

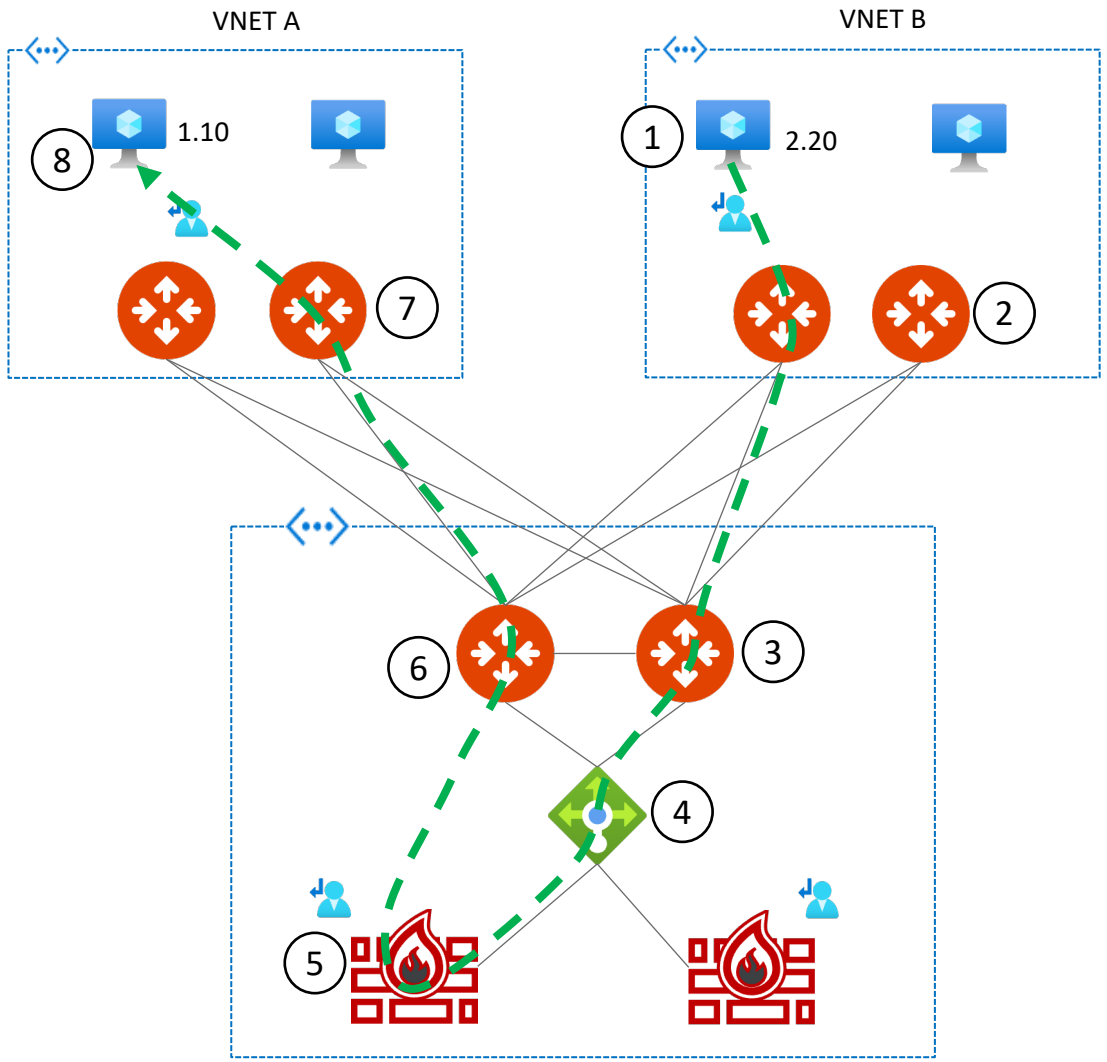


ILB tracks the health of Firewall
Health check is not configurable in Azure via Controller

FireNet Packet Walk – Azure Example

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

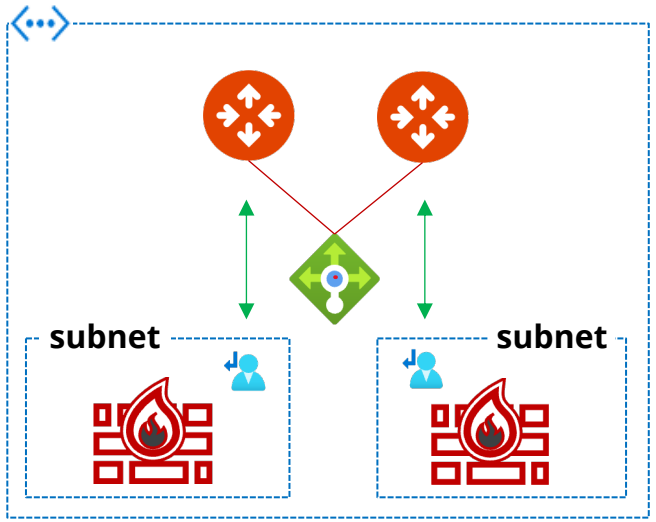
1. The local route table for 2.20 has RFC1918 routes pointed to its local spoke gateway for return traffic.
2. The local Aviatrix spoke gateway will ECMP traffic with 5-tuple hash to one of the Aviatrix Transit Gateways.
3. The Aviatrix Transit Gateway receiving the traffic will pass the traffic to the 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

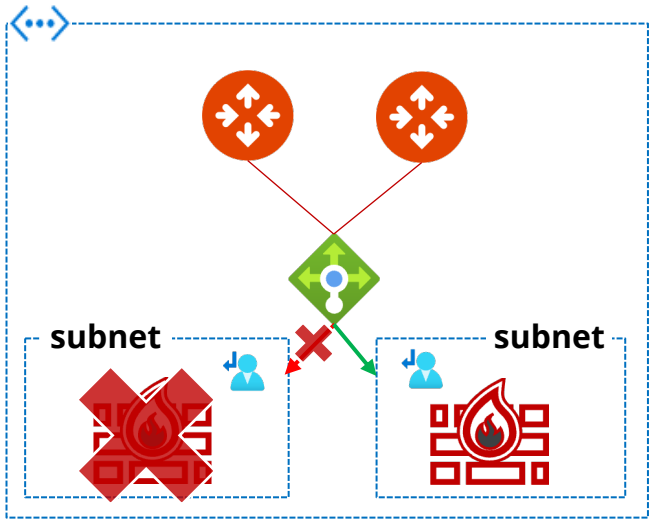
Steady State

- 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



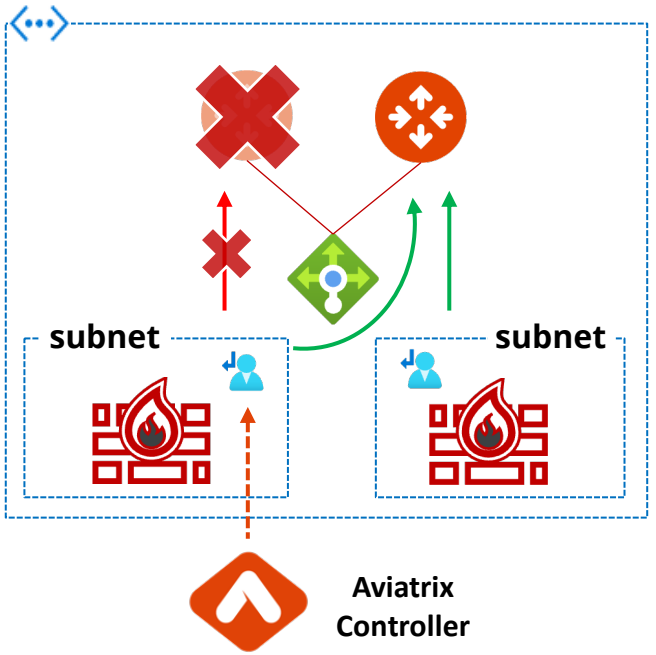
Firewall Failure State

- 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



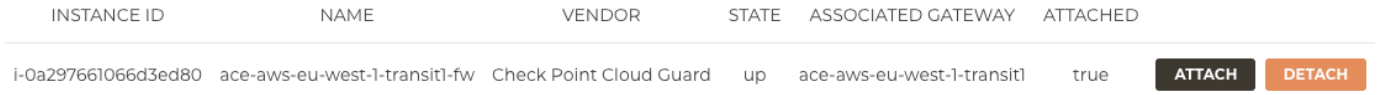
Gateway Failure State

- 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

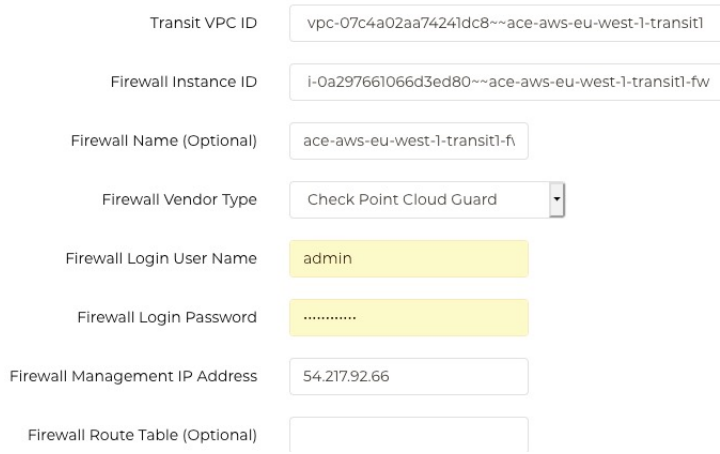


Tools for Operating your FireNet

Information to Collect / Checklist [2]



- 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 MULTI-CLOUD TRANSIT > List > Details



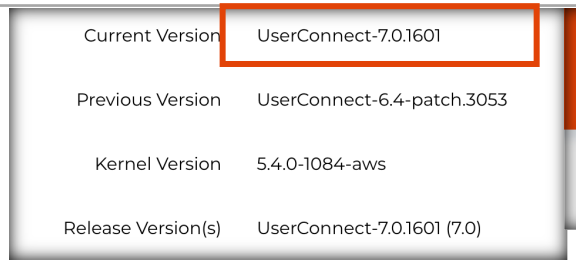
How does Controller Integrate with Firewall vendor?*

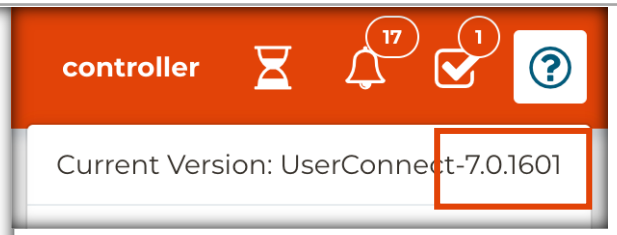
- Day 0 – You can deploy a Palo Alto, Check Point, or Fortinet firewall directly from the Controller
- Day 1 – Vendor integration allows automatic route updates in firewall routing tables by the Aviatrix Controller
- Verify routes on Firewall from:
  Controller > FIREWALL NETWORK > Vendor Integration

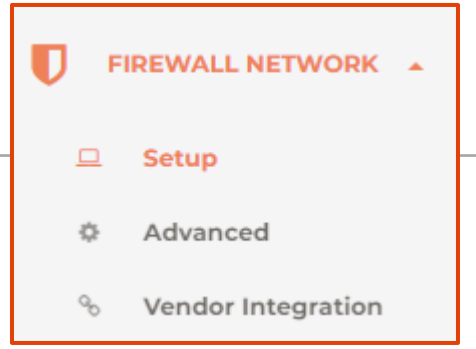
Clouds	PAN	Check Point	Fortinet
AWS	Required for RFC 1918 and non-RFC 1918	Required for non-RFC 1918	Required for non-RFC 1918
Azure	Required for RFC 1918 and non-RFC 1918	Required for non-RFC 1918	Required for RFC 1918 and non-RFC 1918
GCP	Required for RFC 1918 and non-RFC 1918	Required for non-RFC 1918	Required for RFC 1918 and non-RFC 1918

*Consult the latest Aviatrix docs to verify the behavior in your release.
The behaviors described above comes from version 6.7.
Consult the docs for proper configuration of your Firewall, including opening ports for health checks.

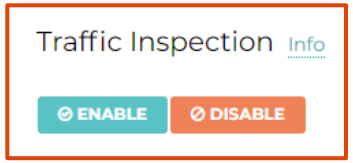
Information to Collect - Checklist for the Support Team

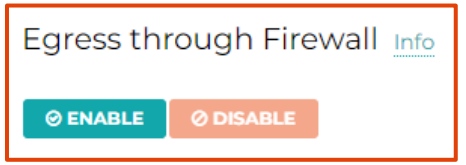


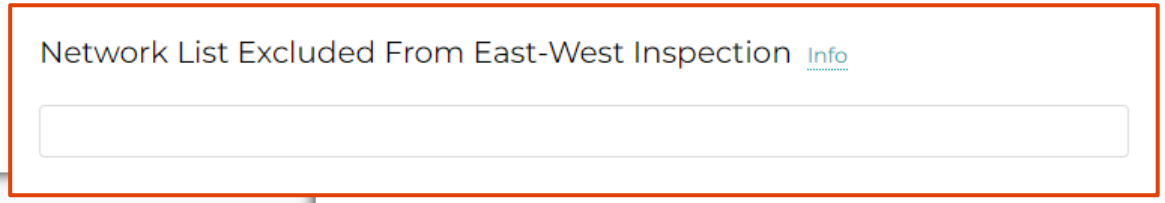


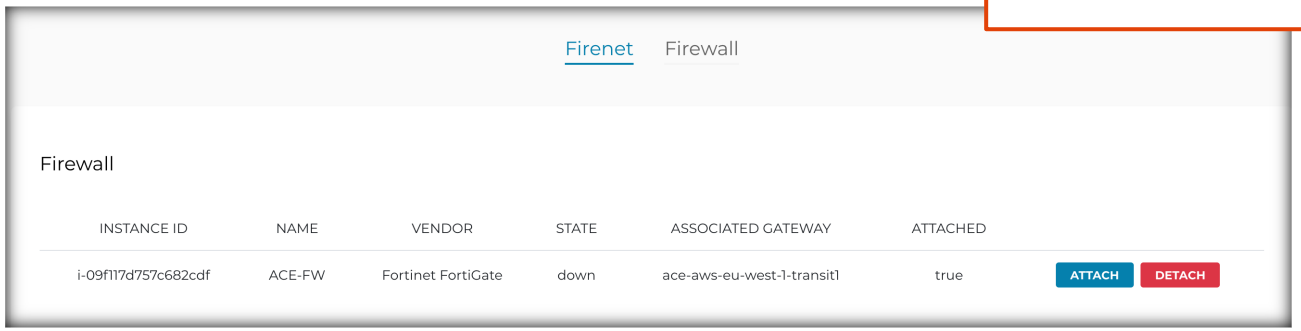


- Aviatrix Controller version
- Firewall Vendor
- Transit FireNet: Inspection Policy
  - Is the Spoke VPC/VNet supposed to be Inspected at all?
- E/W Traffic inspection enabled?
- Egress Traffic inspection enabled?
- Ingress Traffic enabled and working?
- Exclude list created for CIDR/IP from being inspected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









aviatrix

Next:

Lab 3 FireNet - Interface
Lab 4 FireNet - Routes