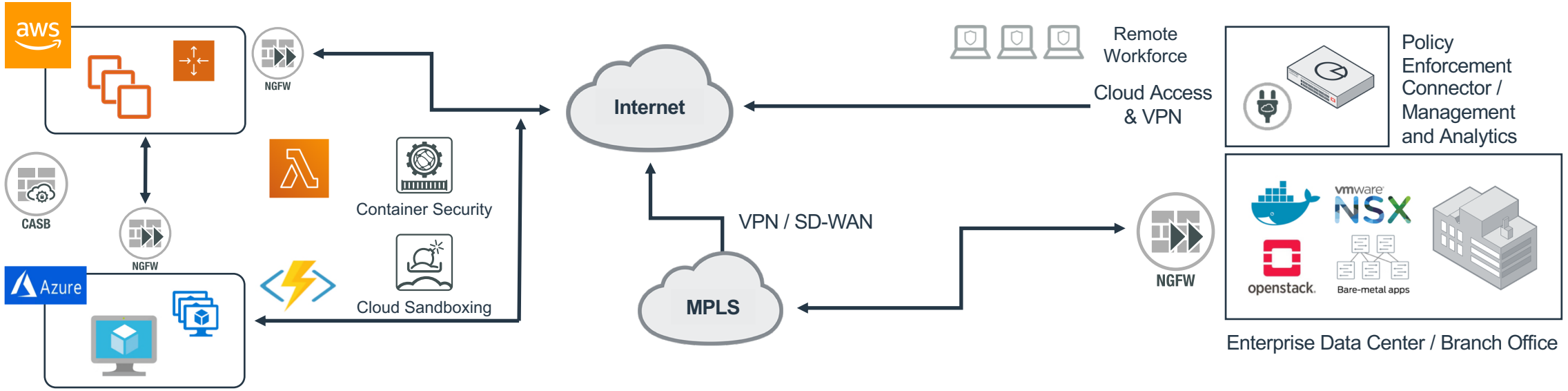
Multi-Cloud Security Reference Architecture

Ali Bidabadi

Cloud Solutions Architect

Global Products & Solutions

Multi-Cloud Security Reference Architecture



Zero Trust Deployment

- Block lateral threat propagation in East-West direction
- Comprehensive protection in North-South direction
- Advanced security (L7 Firewall, IPS, and ATP) for all traffic paths
- Security workflows that adapt to deployment changes
- Auto-provisioning of security services across all platforms

End-to-End Automation

AWS CFT

Azure ARM

Terraform

Python

Operational Simplicity

- Single Policy Set across all deployments
- Leverage metadata instead of traditional IP in security policies
- Automated workload and metadata discovery
- Centralized management & analytics across deployments
- Intuitive visibility
- Automated VPN provisioning for multi-cloud connectivity
- Quarantine infected workloads automatically

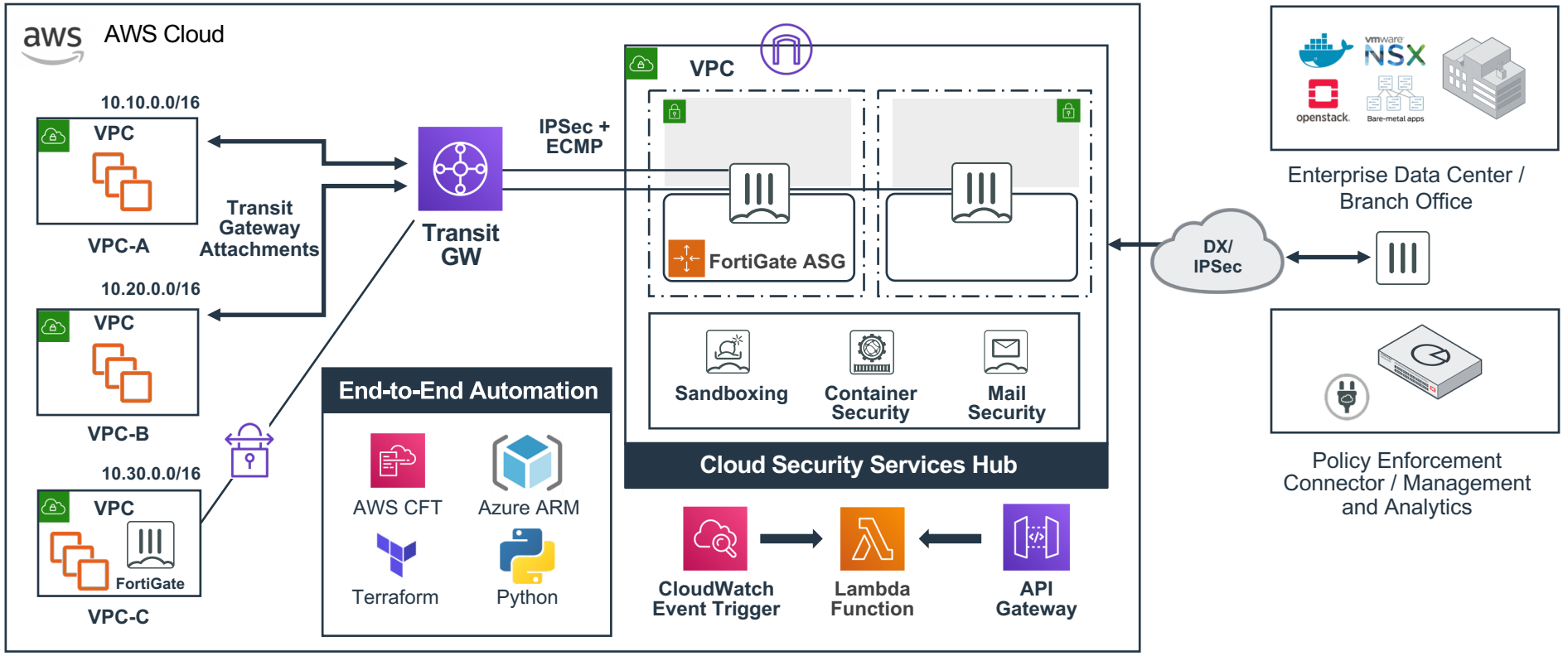
Cloud Security Components

- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Auto Scaling Security
- Denial of Service Protection

Fortinet Cloud Security Services Hub with Autoscaling and AWS Transit Gateway

Operational Simplicity

- Single Policy Set across all deployments
- Dynamically scalable security services
- Leverage metadata instead of traditional IP in security policies
- Automated workload and metadata discovery
- Centralized management & analytics across deployments
- Intuitive visibility
- Automated VPN provisioning for multi-cloud connectivity



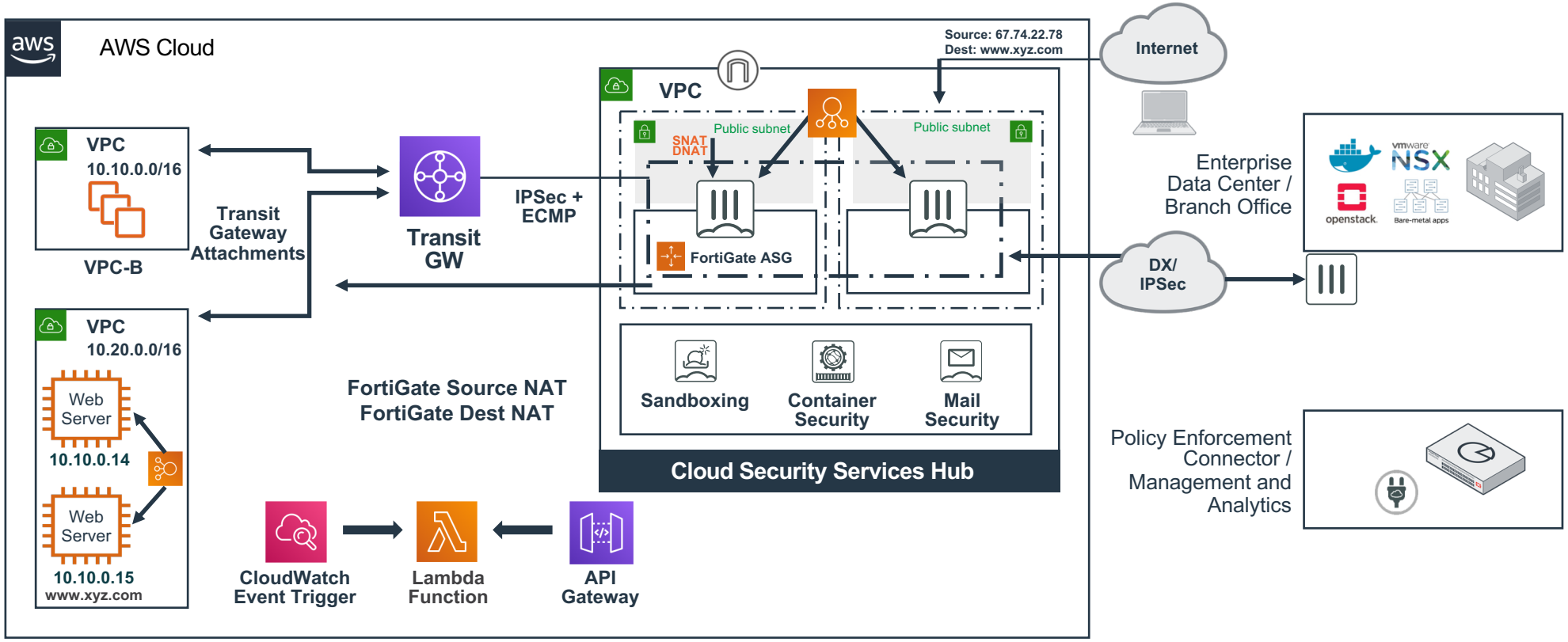
Cloud Security Components

- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Container Security
- Denial of Service Protection

Inbound Application Traffic with Firewall Resiliency

Operational Simplicity

- Single Policy Set across all deployments
- Dynamically scalable security services
- Leverage metadata instead of traditional IP in security policies
- Automated workload and metadata discovery
- Centralized management & analytics across deployments
- Intuitive visibility
- Automated VPN provisioning for multi-cloud connectivity



Cloud Security Components

- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Container Security
- Denial of Service Protection

East – West Traffic Inspection with Fortinet

Cloud Security Services Hub and AWS Transit Gateway

Zero Trust Deployment

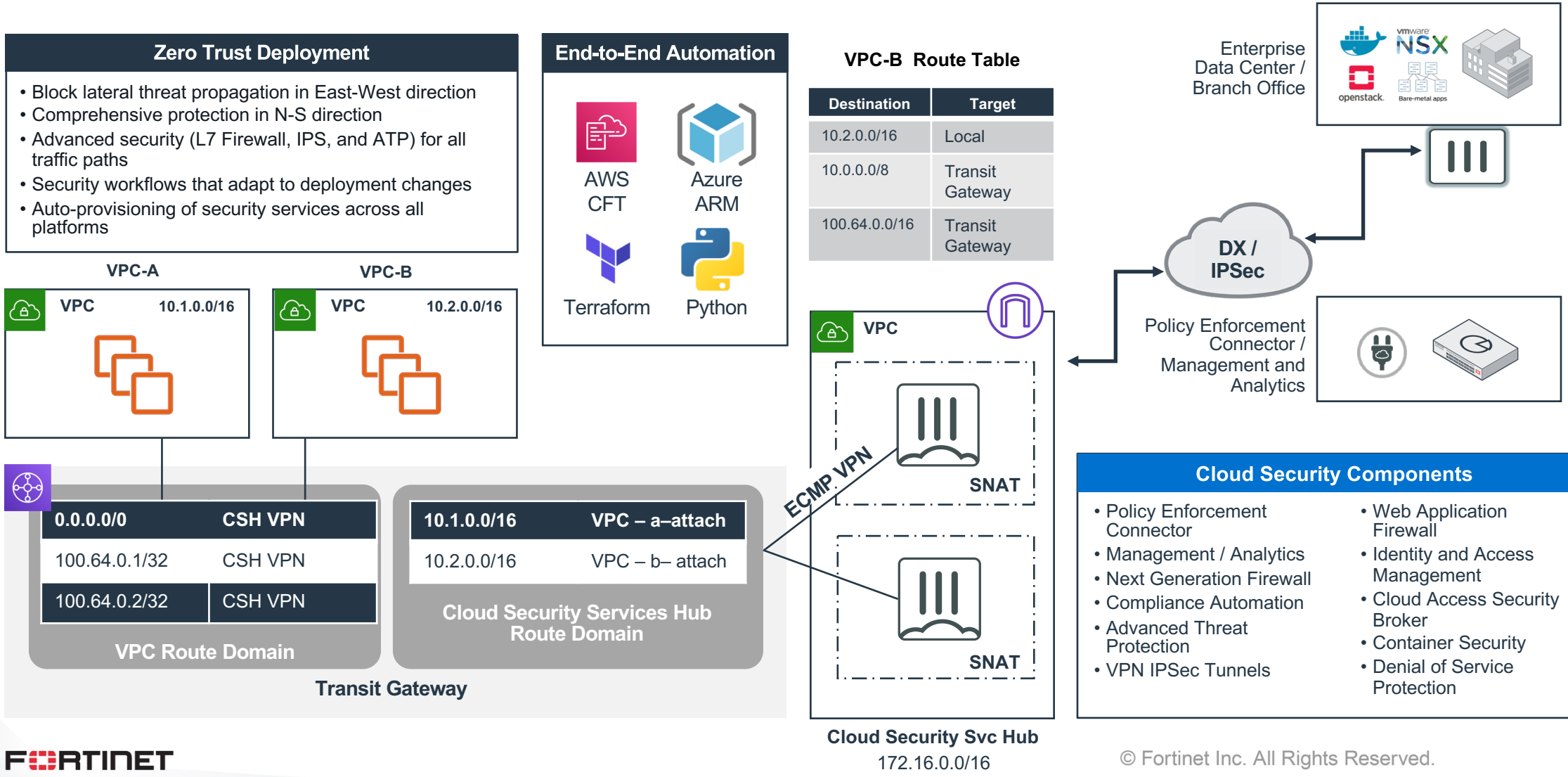
- Block lateral threat propagation in East-West direction
- Comprehensive protection in N-S direction
- Advanced security (L7 Firewall, IPS, and ATP) for all traffic paths
- Security workflows that adapt to deployment changes
- Auto-provisioning of security services across all platforms

End-to-End Automation

AWS CFT | Azure ARM | Terraform | Python

VPC-B Route Table

Destination	Target
10.2.0.0/16	Local
10.0.0.0/8	Transit Gateway
100.64.0.0/16	Transit Gateway

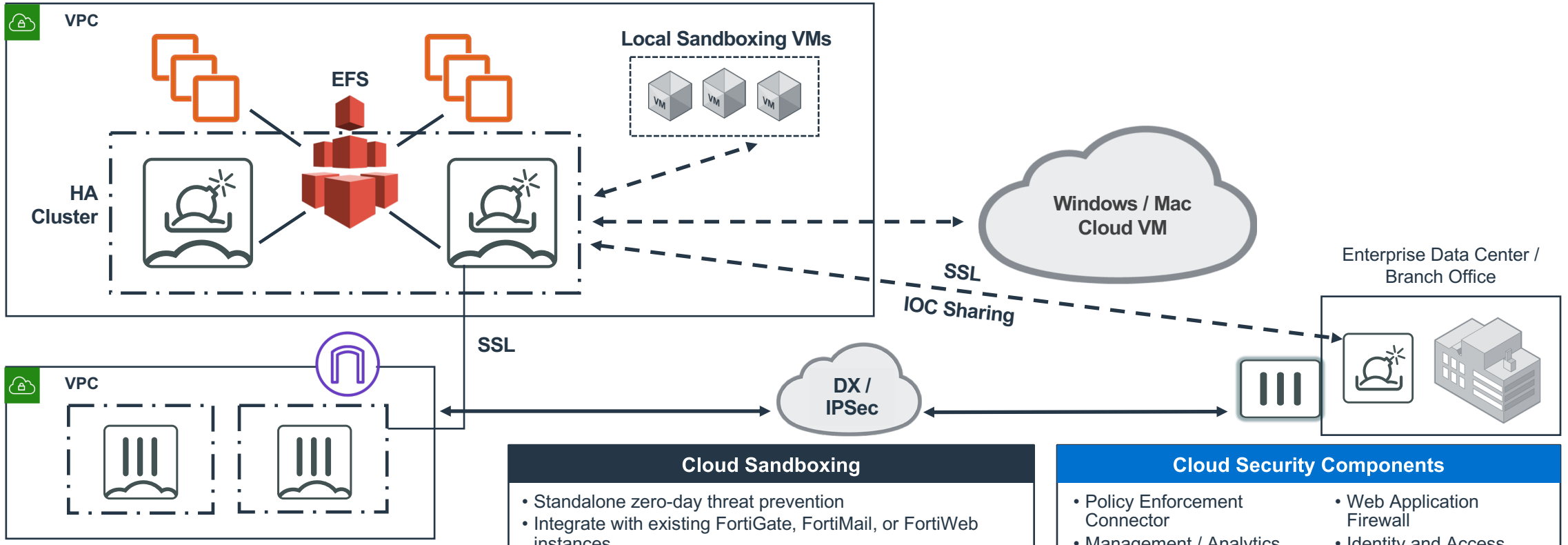


Cloud Security Components

- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Container Security
- Denial of Service Protection

Advanced Threat Protection—Fortinet

Fortinet Sandboxing in Public Cloud



Cloud Sandboxing

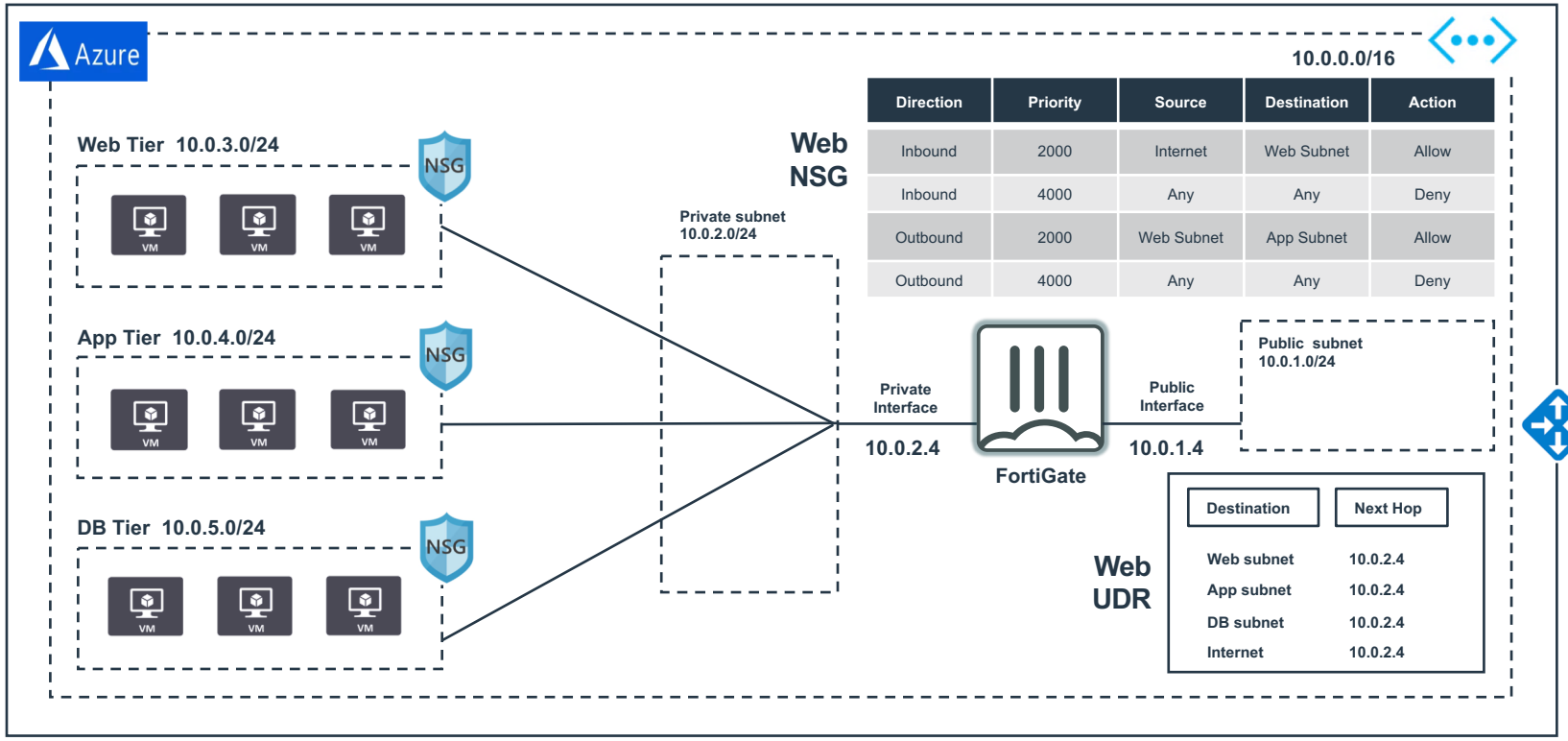
- Standalone zero-day threat prevention
- Integrate with existing FortiGate, FortiMail, or FortiWeb instances
- Support up to 8 local Windows VMs and up to 200 Cloud Windows/Mac VMs
- Synchronize with on-premises FortiSandbox to share Indicators of Compromise (IOC) intelligence
- Perform malware analysis in the Elastic File System (EFS) backup solution

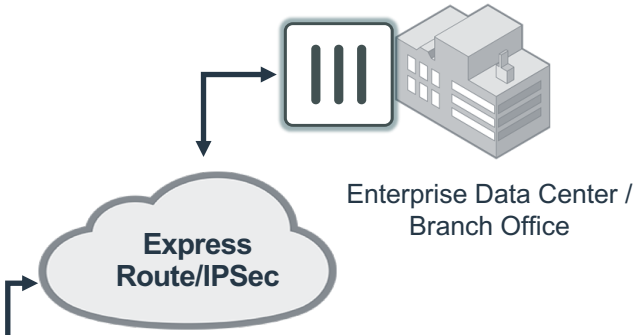
Cloud Security Components

- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Container Security
- Denial of Service Protection

Micro-segmentation with Azure

User Defined Route (UDR) and FortiGate NGFW





Cloud Security Components

- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Container Security
- Denial of Service Protection

End-to-End Automation

Python | Terraform | Azure ARM | Azure Function

Zero Trust Deployment

- Block lateral threat propagation in East-West direction
- Comprehensive protection in N-S direction
- Advanced security (L7 Firewall, IPS, and ATP) for all traffic paths
- Security workflows that adapt to deployment changes
- Auto-provisioning of security services across all platforms

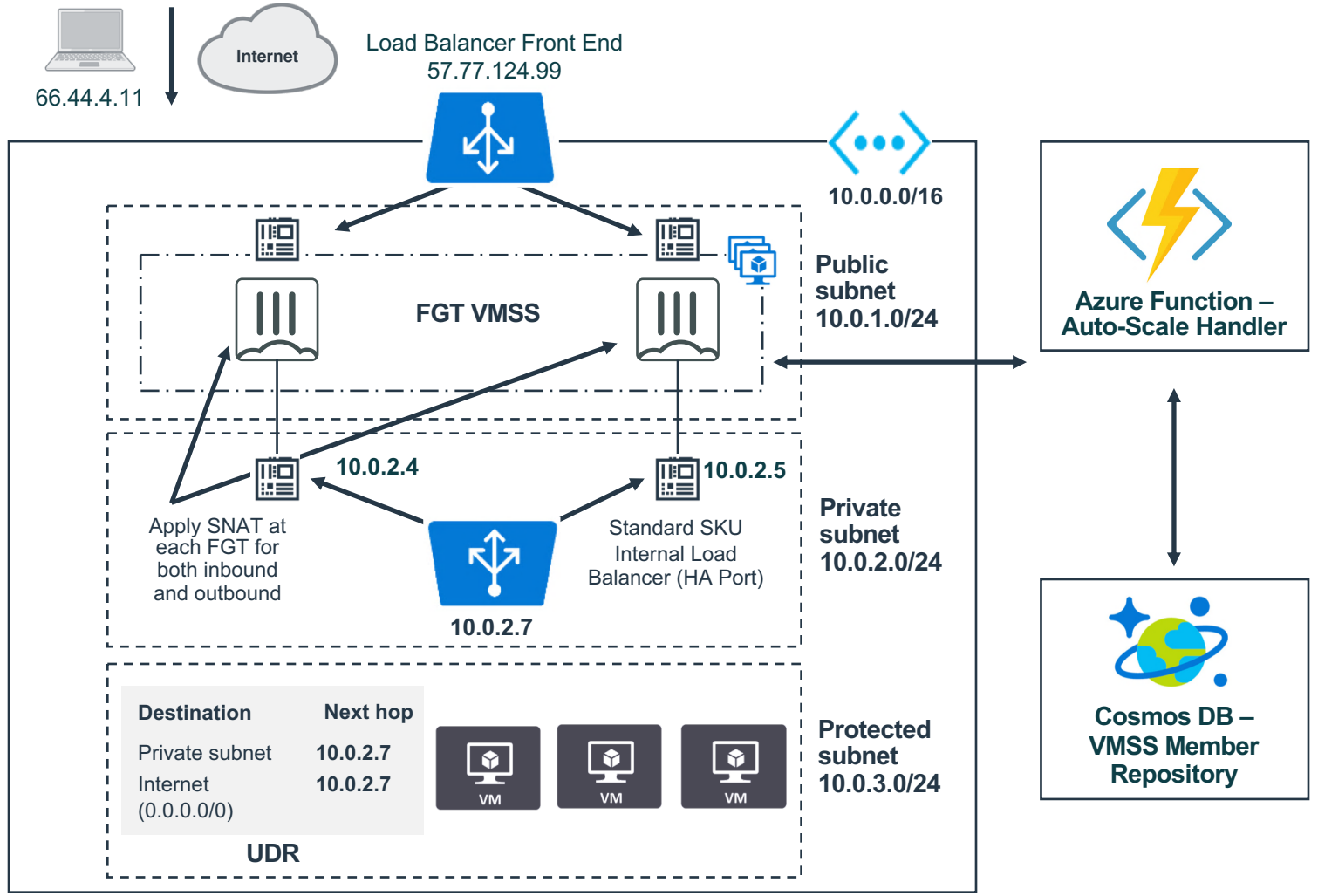
Elastic Load Balancing Sandwich with FortiGate NGFW and Azure Virtual Machine Scale Set (VMSS)

Cloud Security Components

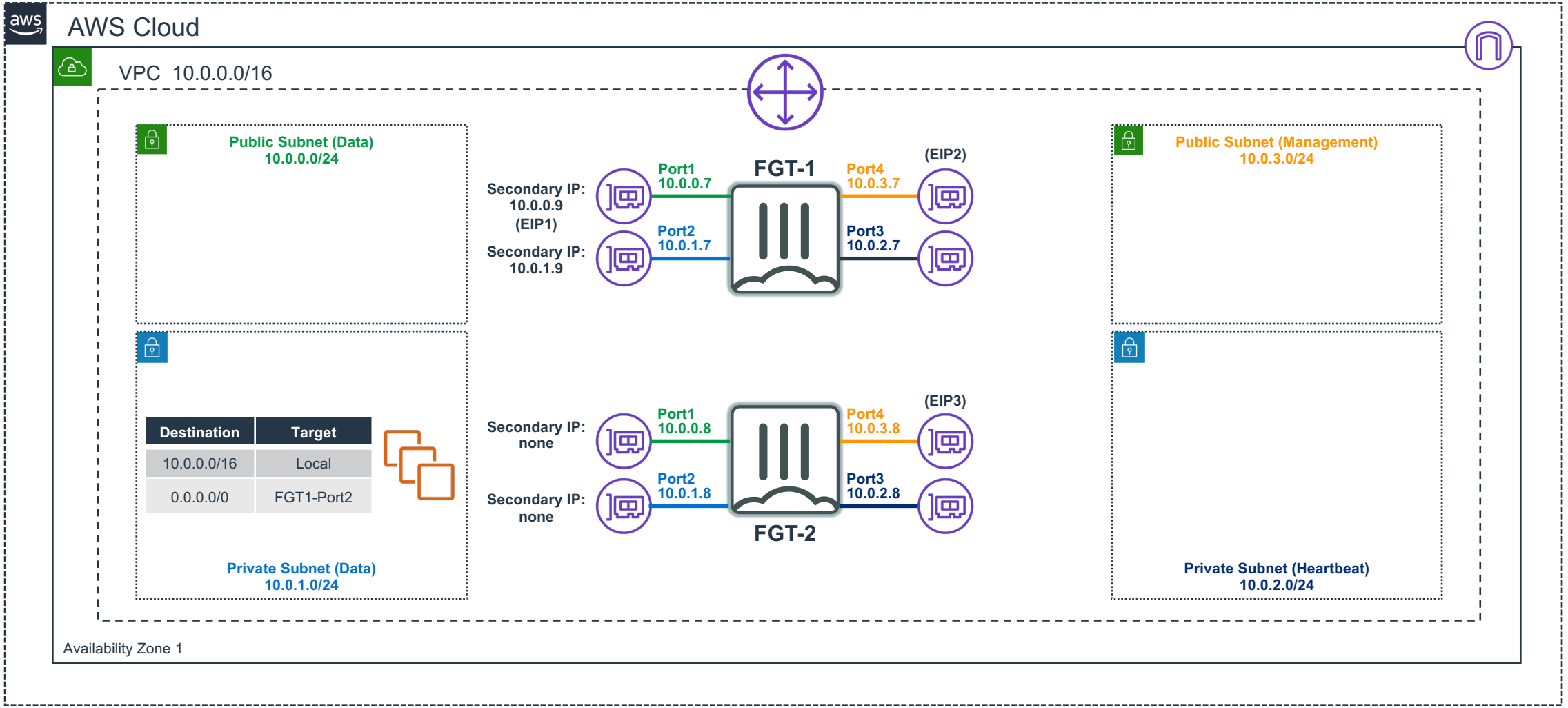
- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels
- Web Application Firewall
- Identity and Access Management
- Cloud Access Security Broker
- Container Security
- Denial of Service Protection

Auto Scaling Security

- Scale up and down capacity based on changing traffic volume
- Integrated with Azure VMSS and Azure Load Balancer
- Take advantage of Azure Internal Standard SKU Load Balancer to load balance outbound traffic
- Enable HA port to allow all protocols/ports
- FortiGate NGFW integrated with Azure Security Center
- Automatically failover when NGFW instances become unhealthy

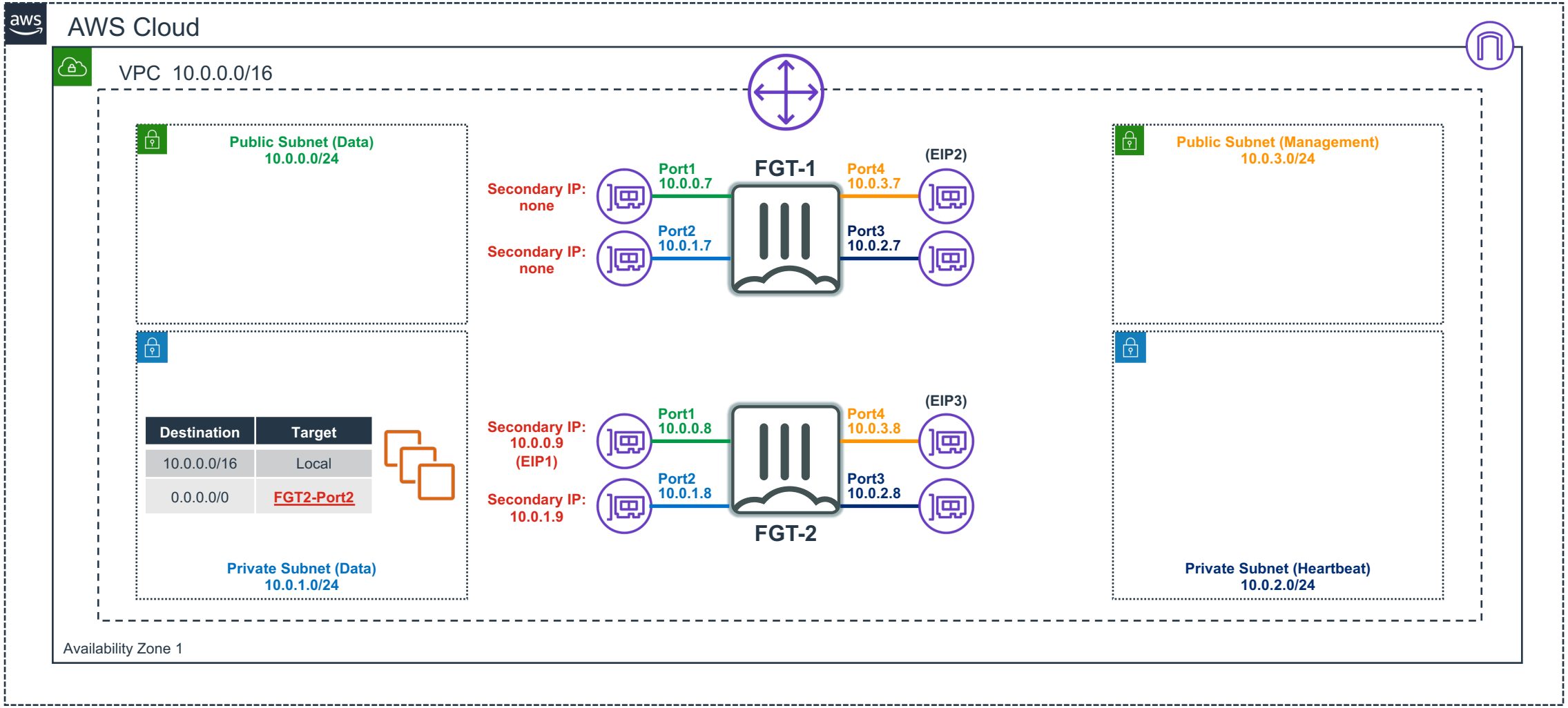


Native Active–Passive HA

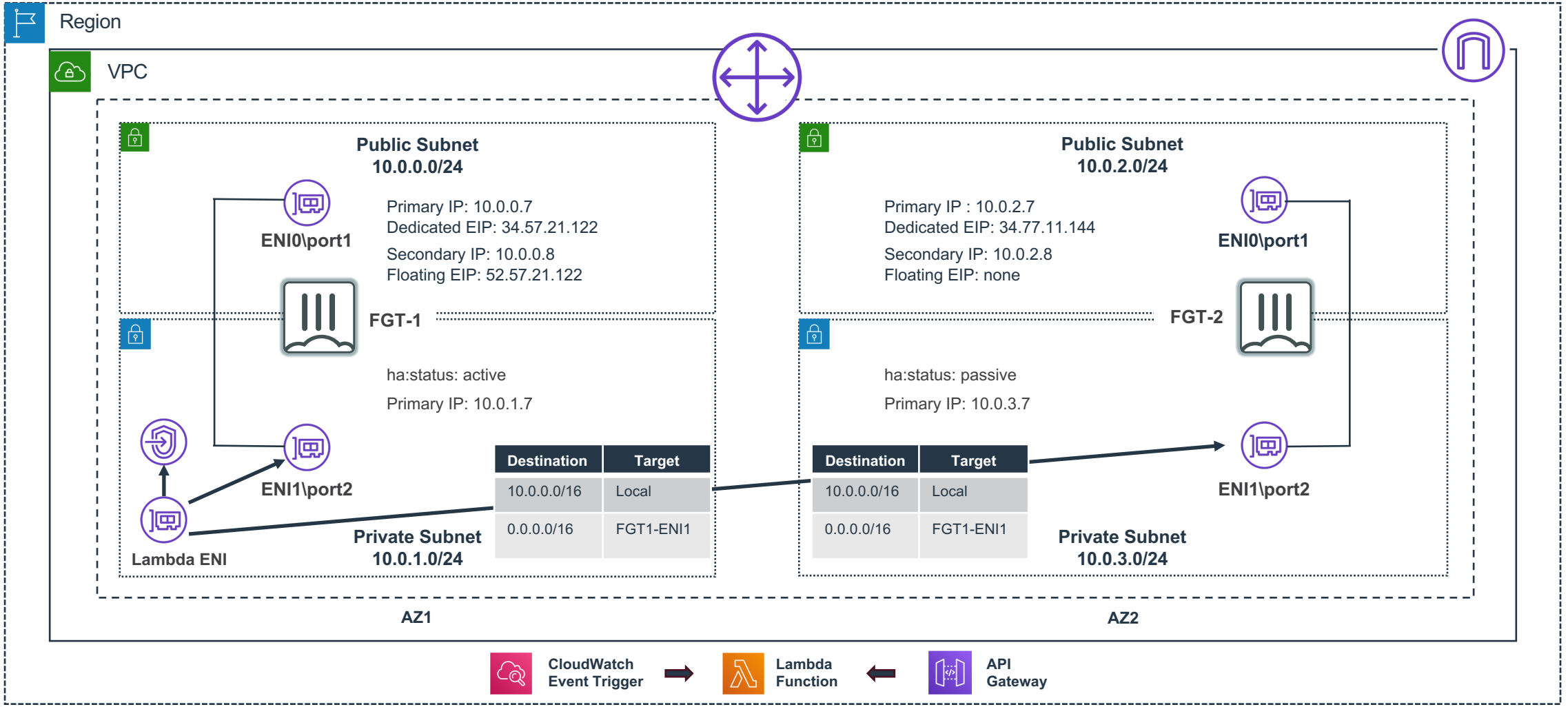


Native Active–Passive HA

Failover Process

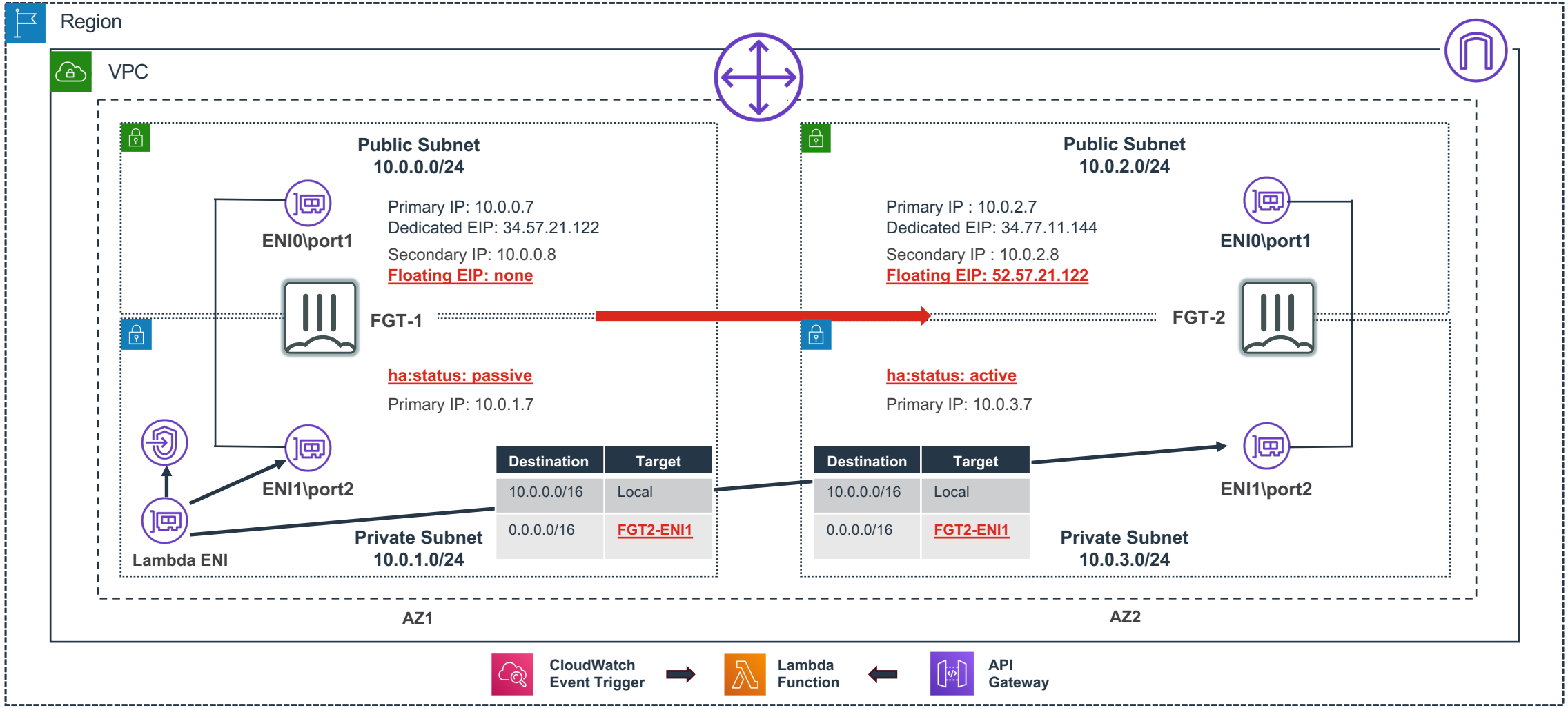


A-P FortiGate HA

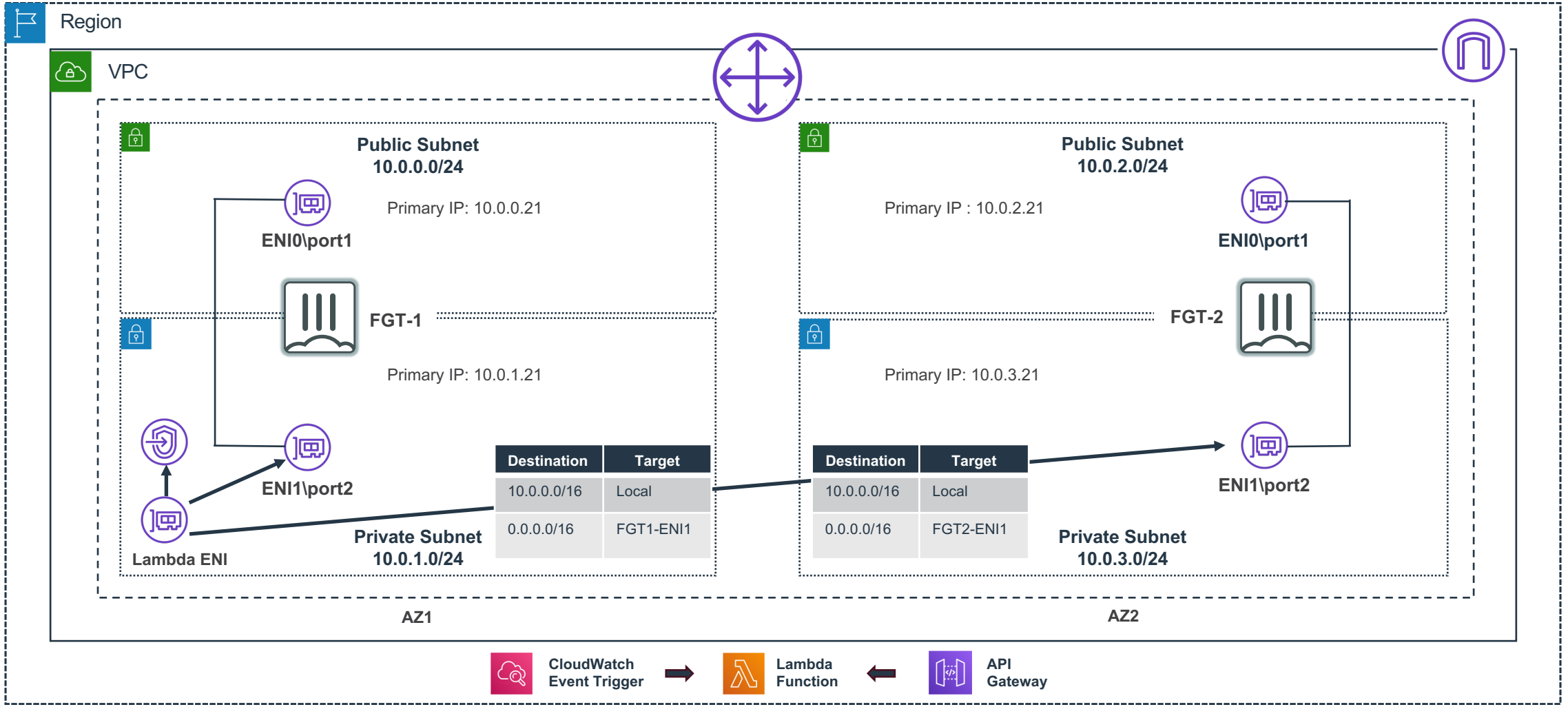


A-P FortiGate HA

Failover Process

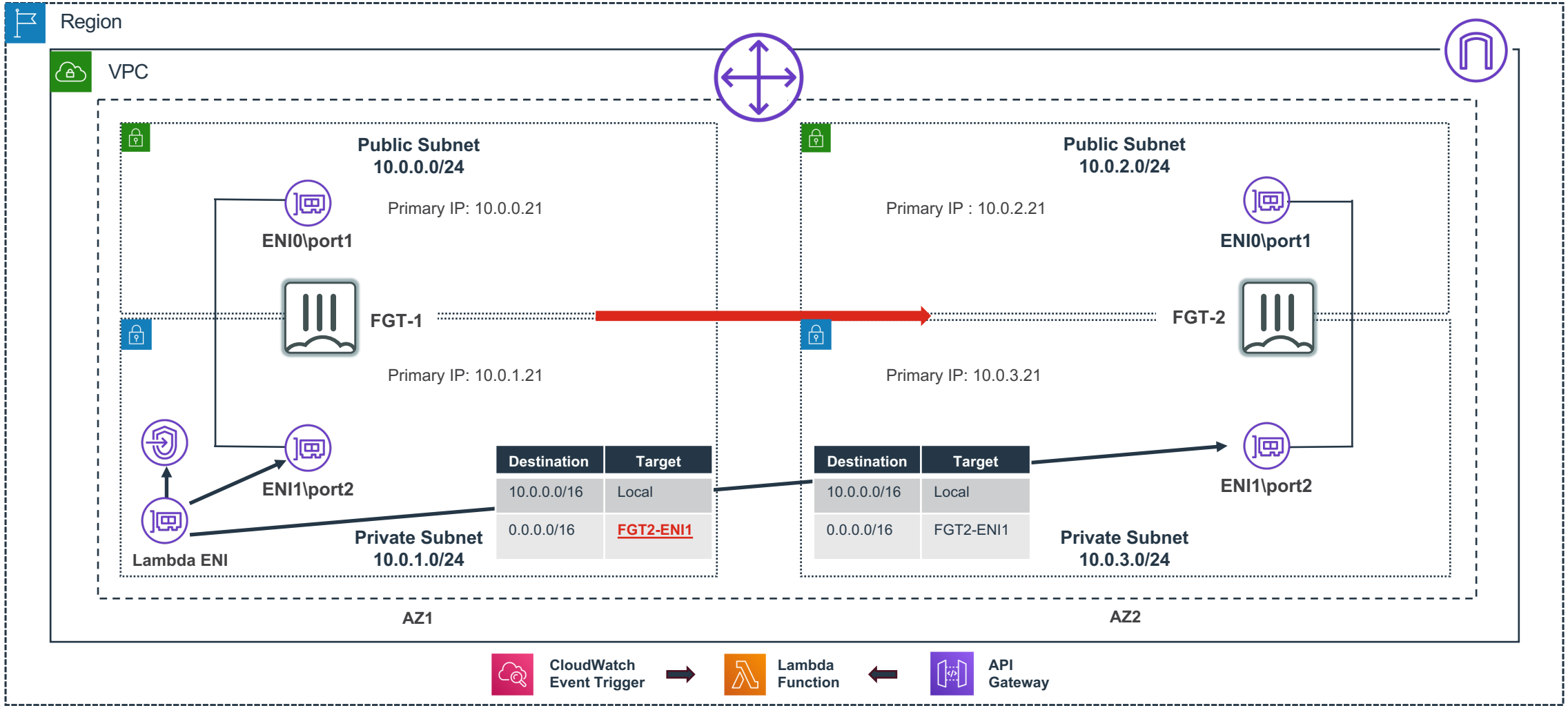


A-A FortiGate HA

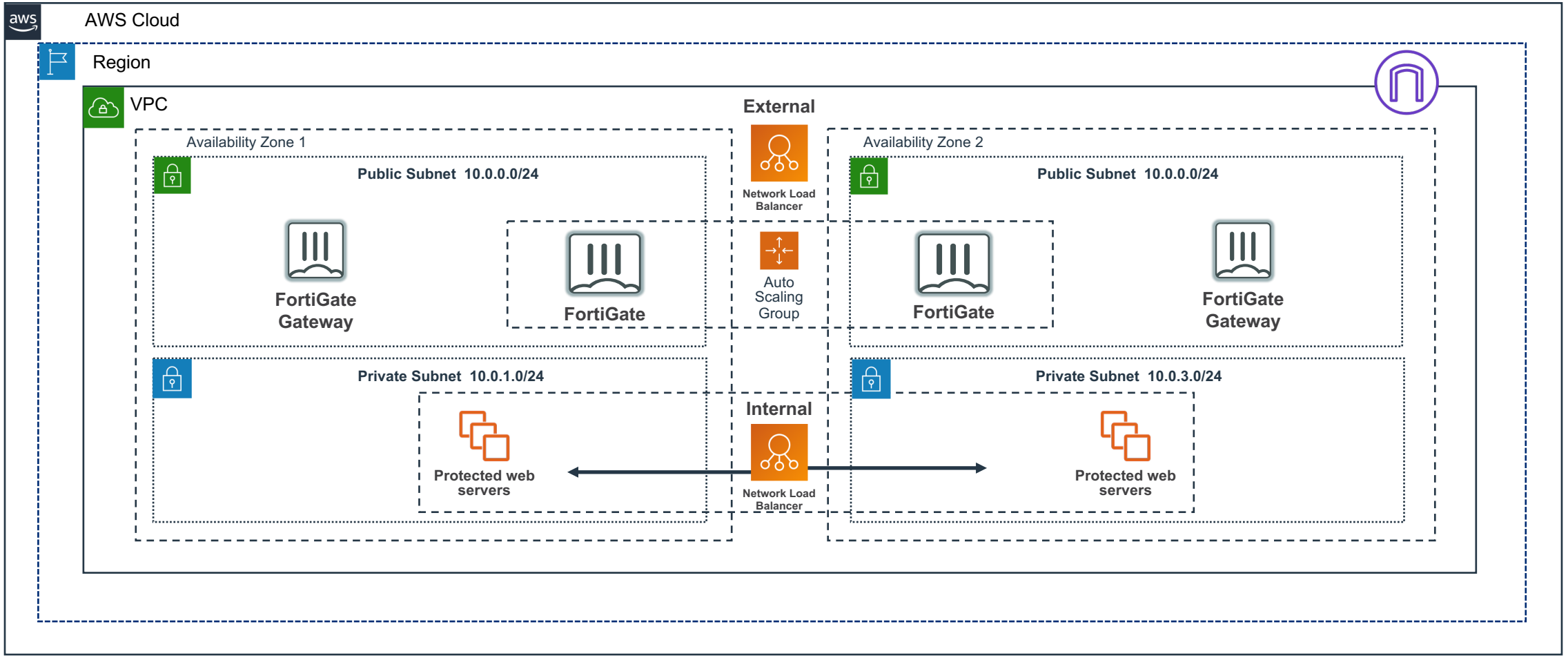


A-A FortiGate HA

Failover Process



FortiGate with AWS Auto Scaling Group



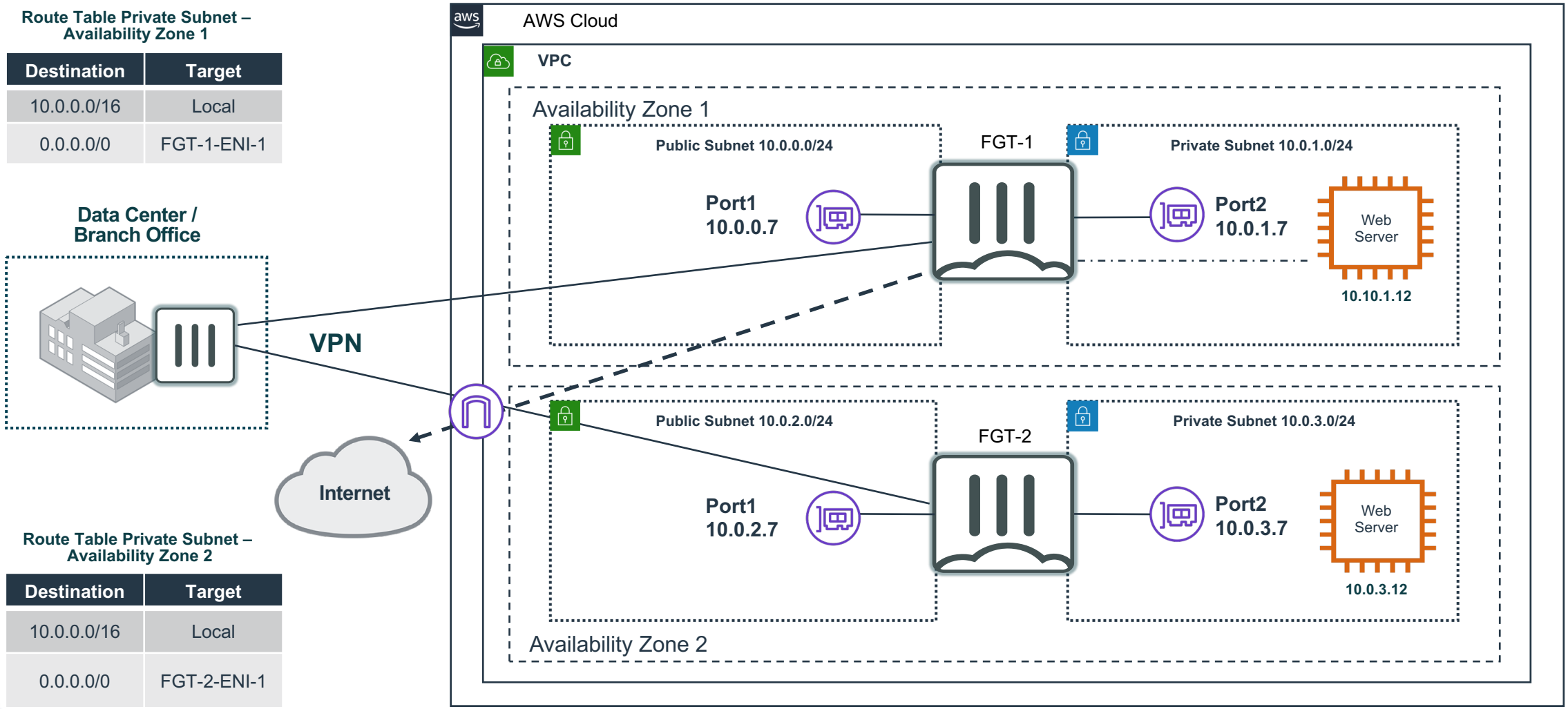
Resilient Outbound Connection to On-Premises Network

Route Table Private Subnet – Availability Zone 1

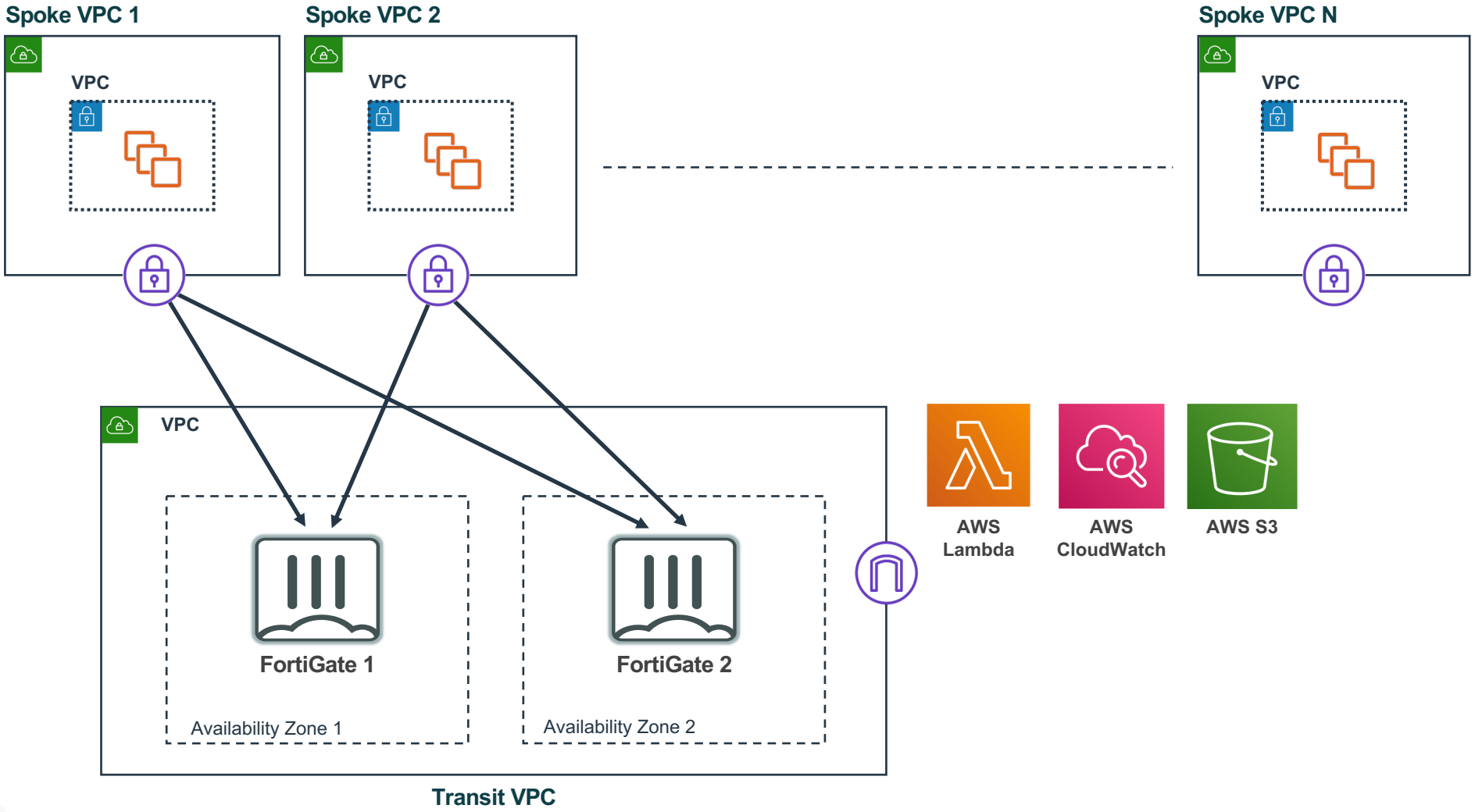
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	FGT-1-ENI-1

Route Table Private Subnet – Availability Zone 2

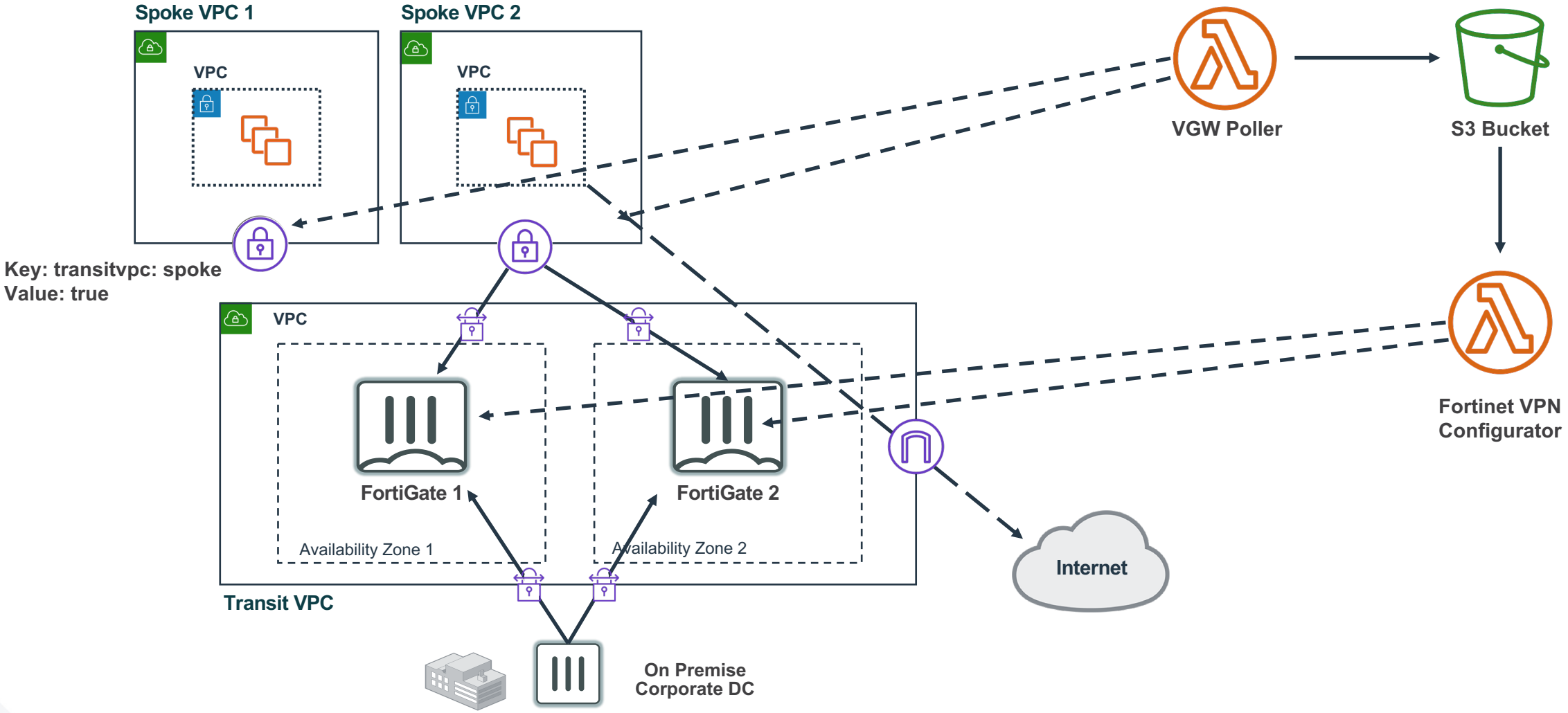
Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	FGT-2-ENI-1



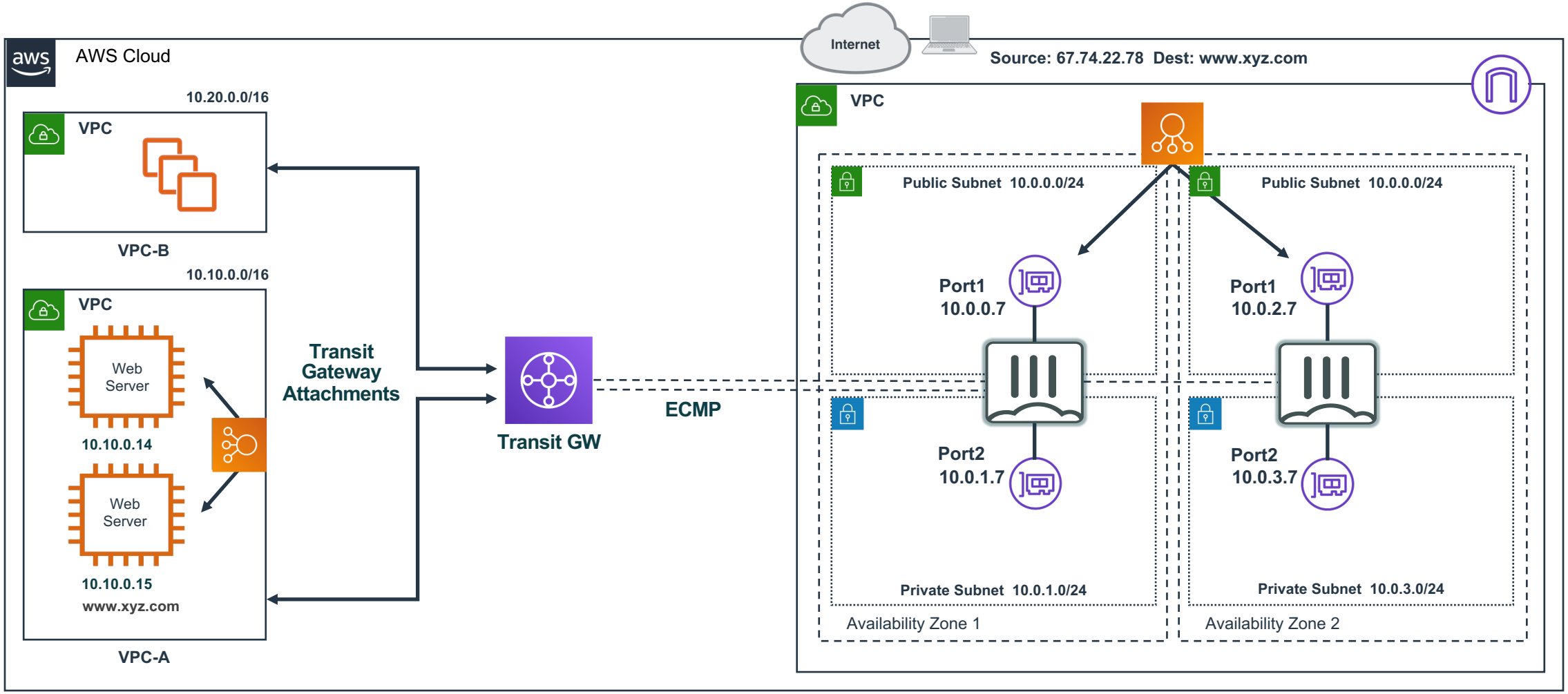
Transit VPC



Fortinet Transit VPC Architecture



Fortinet Transit Gateway Architecture




FORTINET