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
- 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

Operational Simplicity
- Auto Scaling Security
- Denial of Service Protection
- 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

Cloud Security Components

© Fortinet Inc. All Rights Reserved.
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 Services Hub**

- VPC 10.10.0.0/16
- VPC 10.20.0.0/16
- Internet
- Enterprise Data Center / Branch Office
- DX/ IPSec
- 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

**Source:** 67.74.22.78
Dest: www.xyz.com

© Fortinet Inc. All Rights Reserved.
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-A
- VPC 10.1.0.0/16
- VPC Route Domain
- 0.0.0.0/0 CSH VPN
- 100.64.0.1/32 CSH VPN
- 100.64.0.2/32 CSH VPN

VPC-B
- VPC 10.2.0.0/16
- VPC Route Domain
- 10.1.0.0/16 VPC – a-attach
- 10.2.0.0/16 VPC – b-attach

VPC-B Route Table
- Destination: 10.2.0.0/16 Target: Local
- Destination: 10.0.0.0/8 Target: Transit Gateway
- Destination: 100.64.0.0/16 Target: Transit Gateway

Cloud Security Components
- Policy Enforcement Connector
- Management / Analytics
- Next Generation Firewall
- Compliance Automation
- Advanced Threat Protection
- VPN IPSec Tunnels

Enterprise Data Center / Branch Office
DX / IPSec
Policy Enforcement Connector / Management and Analytics

© Fortinet Inc. All Rights Reserved.
Advanced Threat Protection—Fortinet

Fortinet Sandboxing in Public Cloud

- 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 Sandboxing

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

- 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

Cloud Security Components
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

Apply SNAT at each FGT for both inbound and outbound

UDR

Destination Next hop
Private subnet 10.0.2.7
Internet (0.0.0.0/0) 10.0.2.7

Load Balancer Front End
57.77.124.99

Public subnet 10.0.1.0/24
Private subnet 10.0.2.0/24
Protected subnet 10.0.3.0/24

Azure Function – Auto Scale Handler

Cosmos DB – VMSS Member Repository

© Fortinet Inc. All Rights Reserved.
Native Active–Passive HA

AWS Cloud

VPC 10.0.0.0/16

Public Subnet (Data) 10.0.0.0/24

Private Subnet (Data) 10.0.1.0/24

Availability Zone 1

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>FGT1-Port2</td>
</tr>
</tbody>
</table>

Public Subnet (Management) 10.0.3.0/24

Private Subnet (Heartbeat) 10.0.2.0/24

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
</tbody>
</table>

Secondary IP:
- Port1: 10.0.0.7 (EIP1)
- Port2: 10.0.1.7
- Port3: 10.0.2.7
- Port4: 10.0.3.7 (EIP2)

Secondary IP:
- Port1: 10.0.0.8
- Port2: 10.0.1.8
- Port3: 10.0.2.8 (EIP3)

Secondary IP:
- FGT1-Port2

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>none</td>
<td>FGT1-Port2</td>
</tr>
</tbody>
</table>
Native Active–Passive HA

Failover Process
A-P FortiGate HA

Public Subnet 10.0.0.0/24
- Primary IP: 10.0.0.7
- Dedicated EIP: 34.57.21.122
- Secondary IP: 10.0.0.8
- Floating EIP: 52.57.21.122
  - ha:status: active
  - Primary IP: 10.0.1.7

Private Subnet 10.0.1.0/24
- Destination: 10.0.0.0/16
  - Target: Local
- Destination: 10.0.0.0/16
  - Target: 0.0.0.0/16

Public Subnet 10.0.2.0/24
- Primary IP: 10.0.2.7
- Dedicated EIP: 34.77.11.144
- Secondary IP: 10.0.2.8
- Floating EIP: none
  - ha:status: passive
  - Primary IP: 10.0.3.7

Private Subnet 10.0.3.0/24
- Destination: 10.0.0.0/16
  - Target: Local
- Destination: 10.0.0.0/16
  - Target: 0.0.0.0/16

AZ1
- ENI0/port1
- ENI1/port2
- Lambda ENI

AZ2
- ENI0/port1
- ENI1/port2
A-P FortiGate HA

Failover Process

- **FGT-1**
  - Primary IP: 10.0.0.7
  - Dedicated EIP: 34.57.21.122
  - Secondary IP: 10.0.0.8
  - Floating EIP: none
  - ha:status: passive
  - Primary IP: 10.0.1.7

- **FGT-2**
  - Primary IP: 10.0.2.7
  - Dedicated EIP: 34.77.11.144
  - Secondary IP: 10.0.2.8
  - Floating EIP: 52.57.21.122
  - ha:status: active
  - Primary IP: 10.0.3.7

- **ENI0/port1**
- **ENI0/port2**
- **ENI1/port1**
- **ENI1/port2**

- **Public Subnet 10.0.0.0/24**
- **Private Subnet 10.0.1.0/24**
- **Public Subnet 10.0.2.0/24**
- **Private Subnet 10.0.3.0/24**

- **Destination**
  - 10.0.0.0/16
  - 0.0.0.0/16

- **Target**
  - Local

- **CloudWatch Event Trigger**
- **Lambda Function**
- **API Gateway**

© Fortinet Inc. All Rights Reserved.
A-A FortiGate HA

- Public Subnet 10.0.0.0/24
  - Primary IP: 10.0.0.21
  - ENI: port1
  - ENI: port2

- Private Subnet 10.0.1.0/24
  - Primary IP: 10.0.1.21
  - Lambda ENI

- Public Subnet 10.0.2.0/24
  - Primary IP: 10.0.2.21
  - ENI: port1

- Private Subnet 10.0.3.0/24
  - Primary IP: 10.0.3.21
  - ENI: port2

CloudWatch Event Trigger
Lambda Function
API Gateway

© Fortinet Inc. All Rights Reserved.
A-A FortiGate HA

Failover Process

Region

VPC

Public Subnet 10.0.0.0/24

Primary IP: 10.0.0.21

Private Subnet 10.0.1.0/24

Lambda ENI

ENI0/Port1

FGT-1

Primary IP: 10.0.1.21

ENI1/Port2

CloudWatch Event Trigger

Lambda Function

API Gateway

Destination | Target
-------------|-------------
10.0.0.0/16 | Local
0.0.0.0/16  | FGT2-EN1

Public Subnet 10.0.2.0/24

Primary IP: 10.0.2.21

Private Subnet 10.0.3.0/24

FGT2-EN1

ENI1/Port2

FGT-2

Primary IP: 10.0.3.21

Destination | Target
-------------|-------------
10.0.0.0/16 | Local
0.0.0.0/16  | FGT2-EN1

AZ1

AZ2

© Fortinet Inc. All Rights Reserved.
FortiGate with AWS Auto Scaling Group

AWS Cloud

Region

VPC

Availability Zone 1

Public Subnet 10.0.0.0/24

FortiGate Gateway

Private Subnet 10.0.1.0/24

Protected web servers

FortiGate Gateway

Internal

Protected web servers

Network Load Balancer

Auto Scaling Group

Availability Zone 2

Public Subnet 10.0.0.0/24

FortiGate

Private Subnet 10.0.3.0/24

Protected web servers

Network Load Balancer

FortiGate Gateway

External

FortiGate

© Fortinet Inc. All Rights Reserved.
Resilient Outbound Connection to On-Premises Network

<table>
<thead>
<tr>
<th>Route Table Private Subnet – Availability Zone 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Target</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>FGT-1-ENI-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Center / Branch Office</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Route Table Private Subnet – Availability Zone 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Target</td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>0.0.0.0/0</td>
<td>FGT-2-ENI-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AWS Cloud</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>VPC</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability Zone 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Subnet 10.0.0.0/24</td>
<td></td>
</tr>
<tr>
<td>FGT-1</td>
<td></td>
</tr>
<tr>
<td>Private Subnet 10.0.1.0/24</td>
<td></td>
</tr>
<tr>
<td>Port1 10.0.0.7</td>
<td></td>
</tr>
<tr>
<td>Port2 10.0.1.7</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability Zone 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Subnet 10.0.2.0/24</td>
<td></td>
</tr>
<tr>
<td>FGT-2</td>
<td></td>
</tr>
<tr>
<td>Private Subnet 10.0.3.0/24</td>
<td></td>
</tr>
<tr>
<td>Port1 10.0.2.7</td>
<td></td>
</tr>
<tr>
<td>Port2 10.0.3.7</td>
<td></td>
</tr>
</tbody>
</table>

© Fortinet Inc. All Rights Reserved.
Transit VPC

Spoke VPC 1
- VPC
- FortiGate 1 (Availability Zone 1)
- FortiGate 2 (Availability Zone 2)

Spoke VPC 2
- VPC
- FortiGate 1 (Availability Zone 1)
- FortiGate 2 (Availability Zone 2)

Spoke VPC N
- VPC

Transit VPC
- AWS Lambda
- AWS CloudWatch
- AWS S3

© Fortinet Inc. All Rights Reserved.
Fortinet Transit VPC Architecture

Key: transitvpc: spoke
Value: true