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
- 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

Cloud Security Components

<table>
<thead>
<tr>
<th>AWS CFT</th>
<th>Azure ARM</th>
<th>Terraform</th>
<th>Python</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPLS</td>
<td>Internet</td>
<td>Remote Workforce</td>
<td>Cloud Access &amp; VPN</td>
</tr>
</tbody>
</table>

Policy Enforcement Connector / Management and Analytics

Enterprise Data Center / Branch Office

© 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

---

**End-to-End Automation**
- AWS CFT
- Azure ARM
- Terraform
- Python
- CloudWatch
- Lambda Function
- API Gateway

---

**Transit Gateway Attachments**
- VPC-A: 10.10.0.0/16
- VPC-B: 10.20.0.0/16
- VPC-C: 10.30.0.0/16

---

**Cloud Security Services Hub**
- FortiGate ASG
- Sandboxing
- Container Security
- Mail Security

---

**AWS Cloud**
- Fortinet Cloud Security Services Hub with Autoscaling and AWS Transit Gateway
- FortiGate 10.30.0.0/16
- VPC - C
- 10.10.0.0/16
- VPC - B
- 10.20.0.0/16
- VPC - A
- 10.30.0.0/16

---

**Enterprise Data Center / Branch Office**
- DX/IPSec

---

**Policy Enforcement Connector / Management and Analytics**
- AWS Cloud
- Enterprise Data Center / Branch Office
- Policy Enforcement Connector / Management and Analytics
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

AWS Cloud

VPC 10.10.0.0/16
VPC-B

Transit Gateway Attachments

Transit GW

 IPSec + ECMP

FortiGate ASG

Sandboxing
Container Security
Mail Security

Source: 67.44.22.78
Dest: www.xyz.com

Cloud Security Services Hub

Public subnet

CloudWatch Event Trigger

Lambda Function

API Gateway

FortiGate Source NAT
FortiGate Dest NAT

Web Server 10.10.0.14

10.10.0.0/16

Web Server 10.10.0.15

www.xyz.com

Policy Enforcement Connector / Management and Analytics

Enterprise Data Center / Branch Office

DX/IPSec

Source: 67.42.42.14

Dest: www.xyz.com

Inbound Application Traffic with Firewall Resiliency

© 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-B Route Table

<table>
<thead>
<tr>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.2.0.0/16</td>
<td>Local</td>
</tr>
<tr>
<td>10.0.0.0/8</td>
<td>Transit Gateway</td>
</tr>
<tr>
<td>100.64.0.0/16</td>
<td>Transit Gateway</td>
</tr>
</tbody>
</table>

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

© Fortinet Inc. All Rights Reserved.
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

© Fortinet Inc. All Rights Reserved.
Micro-segmentation with Azure

User Defined Route (UDR) and FortiGate NGFW

**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

**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

---

**Table**

<table>
<thead>
<tr>
<th>Direction</th>
<th>Priority</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>2000</td>
<td>Internet</td>
<td>Web Subnet</td>
<td>Allow</td>
</tr>
<tr>
<td>Inbound</td>
<td>4000</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>Outbound</td>
<td>2000</td>
<td>Web Subnet</td>
<td>App Subnet</td>
<td>Allow</td>
</tr>
<tr>
<td>Outbound</td>
<td>4000</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

**Express Route/IPSec**

Enterprise Data Center / Branch Office

---

**Diagram**

- Web Tier 10.0.3.0/24
- App Tier 10.0.4.0/24
- DB Tier 10.0.5.0/24
- Private subnet 10.0.2.0/24
- Next Hop 10.0.1.4
- Public subnet 10.0.1.0/24
- Web UDR
- FortiGate 10.0.2.4
- Public Interface
- Private Interface
- Web subnet 10.0.2.4
- App subnet 10.0.2.4
- DB subnet 10.0.2.4
- Internet 10.0.2.4

**Rules**

- Inbound (Web Subnet): 2000
  - Source: Internet
  - Destination: Web Subnet
  - Action: Allow
- Inbound (Any): 4000
  - Source: Any
  - Destination: Any
  - Action: Deny
- Outbound (Web Subnet): 2000
  - Source: Web Subnet
  - Destination: App Subnet
  - Action: Allow
- Outbound (Any): 4000
  - Source: Any
  - Destination: Any
  - Action: Deny
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

![Diagram showing the interaction between FortiGate NGFW, Azure VMSS, and load balancer.]

- Apply SNAT at each FGT for both inbound and outbound
- Standard SKU Internal Load Balancer (HA Port)
- Public subnet 10.0.1.0/24
- Private subnet 10.0.2.0/24
- Protected subnet 10.0.3.0/24
- Destination | Next hop
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Private subnet</td>
<td>10.0.2.7</td>
</tr>
<tr>
<td>Internet (0.0.0.0/0)</td>
<td>10.0.2.7</td>
</tr>
</tbody>
</table>

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

VPC 10.0.0.0/16

Public Subnet (Data) 10.0.0.0/24

Public Subnet (Management) 10.0.0.0/24

Private Subnet (Data) 10.0.1.0/24

Private Subnet (Heartbeat) 10.0.2.0/24

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>

Secondary IP: 10.0.0.9 (EIP1)
Secondary IP: 10.0.1.9
Secondary IP: none (EIP2)
Secondary IP: none (EIP3)

EIP1: 10.0.0.9
EIP2: 10.0.0.8
EIP3: 10.0.0.7

Port 1 10.0.0.7
Port 2 10.0.1.7
Port 3 10.0.2.7
Port 4 10.0.3.7

Port 1 10.0.0.8
Port 2 10.0.1.8
Port 3 10.0.2.8
Port 4 10.0.3.8

Destination | Target
-------------|--------|
0.0.0.0/0    | Local  |
0.0.0.0/0    | FGT1-Port2 |

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

Failover Process

AWS Cloud

<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>FGT2-Port2</td>
</tr>
</tbody>
</table>

Public Subnet (Data) 10.0.0.0/24

Secondary IP: none

Port1 10.0.0.7
Port2 10.0.1.7
Port3 10.0.2.7
Port4 10.0.3.7

Secondary IP: 10.0.0.9 (EIP1)
Secondary IP: 10.0.1.9
Secondary IP: 10.0.0.9 (EIP1)
Secondary IP: 10.0.1.9

Private Subnet (Data) 10.0.1.0/24

Public Subnet (Management) 10.0.3.0/24

Public Subnet (Heartbeat) 10.0.2.0/24

Availability Zone 1

© Fortinet Inc. All Rights Reserved.
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

Private Subnet 10.0.1.0/24
- lambda ENI

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

CloudWatch Event Trigger ➔ Lambda Function ➔ API Gateway

Region

VPC

AZ1 ➔ FGT-1 ➔ ENI1(port1) ➔ Public Subnet 10.0.0.0/24 ➔ ENI1(port2) ➔ Private Subnet 10.0.1.0/24 ➔ lambda ENI ➔ AZ2

AZ1 ➔ FGT-2 ➔ ENI1(port1) ➔ Public Subnet 10.0.2.0/24 ➔ ENI1(port2) ➔ Private Subnet 10.0.3.0/24 ➔ lambda ENI ➔ AZ2

<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>0.0.0.0/16</td>
<td>FGT1-ENI1</td>
</tr>
</tbody>
</table>

<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>0.0.0.0/16</td>
<td>FGT1-ENI1</td>
</tr>
</tbody>
</table>
A-P FortiGate HA
Failover Process

Region

VPC

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: none
- Lambda ENI
- Primary IP: 10.0.1.7

Private Subnet 10.0.1.0/24
- Destination 10.0.0.0/16 Local
- Destination 0.0.0.0/16 FGT2-ENI1

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: 52.57.21.122

Private Subnet 10.0.3.0/24
- Destination 10.0.0.0/16 Local
- Destination 0.0.0.0/16 FGT2-ENI1

CloudWatch Event Trigger
Lambda Function
API Gateway

Lambda ENI

AZ1

AZ2

FGT-1

ha:status: passive

FGT-2

ha:status: active

Primary IP: 10.0.3.7

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

Public Subnet
10.0.0.0/24

Primary IP: 10.0.0.21

Primary IP: 10.0.1.21

Private Subnet
10.0.1.0/24

Destination | Target
---|---
10.0.0.0/16 | Local
0.0.0.0/16 | FGT1-ENI1

Lambda ENI

ENI1|port1

ENI1|port2

Lambda ENI

Public Subnet
10.0.2.0/24

Primary IP: 10.0.2.21

Primary IP: 10.0.3.21

Private Subnet
10.0.3.0/24

Destination | Target
---|---
10.0.0.0/16 | Local
0.0.0.0/16 | FGT2-ENI1

Lambda ENI

ENI1|port1

ENI1|port2

Lambda ENI

CloudWatch Event Trigger

Lambda Function

API Gateway
A-A FortiGate HA

Failover Process
FortiGate with AWS Auto Scaling Group

AWS Cloud

Region

VPC

Public Subnet 10.0.0.0/24

FortiGate Gateway

Protected web servers

Private Subnet 10.0.1.0/24

FortiGate

Protected web servers

Internal

Protected web servers

Public Subnet 10.0.0.0/24

FortiGate Gateway

Private Subnet 10.0.3.0/24

FortiGate Gateway

Network Load Balancer

Auto Scaling Group

Amazon API Gateway

AWS Lambda

Amazon Dynamo DB

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

**AWS Cloud**

**VPC**

**Availability Zone 1**
- Public Subnet 10.0.0.0/24
  - Port 1: 10.0.0.7
  - Port 2: 10.0.1.7
- Private Subnet 10.0.1.0/24
- Web Server 10.0.1.12

**Availability Zone 2**
- Public Subnet 10.0.2.0/24
  - Port 1: 10.0.2.7
  - Port 2: 10.0.3.7
- Private Subnet 10.0.3.0/24
- Web Server 10.0.3.12

**Private Subnet 10.0.1.0/24**
- Target: FGT-1-ENI-1

**Private Subnet 10.0.3.0/24**
- Target: FGT-2-ENI-1

**Route Table Private Subnet – 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>FGT-1-ENI-1</td>
</tr>
</tbody>
</table>

**Route Table Private Subnet – Availability Zone 2**

<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>FGT-2-ENI-1</td>
</tr>
</tbody>
</table>
Transit VPC
Fortinet Transit VPC Architecture

Key: transitvpc: spoke
Value: true
Fortinet Transit Gateway Architecture