DEPLOYMENT GUIDE

Alkira and Fortinet Integration Guide
# Table of Content

- **Introduction** .................................................. 3
- **Solution Overview** .......................................... 3
- **Topology** ......................................................... 4
- **Prerequisites** .................................................... 5
- **Configurations** ................................................. 5
- **Quick Start Configurations** ................................. 6
- **Configurations Details** ...................................... 9
Introduction

This guide covers the deployment of Fortinet FortiGate Firewall from Alkira's Marketplace. It provides the steps required to integrate FortiGate on the Alkira portal. The guide presumes the reader has basic understanding of Alkira CSX and the Fortinet products.

Solution Overview

The Fortinet FortiGate Next-Generation Firewall integration from Alkira's Marketplace provides seamless security service insertion for any network connected to the Alkira Cloud Exchange Points (CXPs). This enables our customers to gain full visibility and control for traffic from: customer premises networks to the cloud; traffic between virtual networks in the same cloud provider; and multi-cloud traffic between different cloud providers. Alkira allows customers to avoid the complexity of deploying and maintaining their own FortiGate instances in native-cloud environments.

With this integration, customers can leverage the FortiGate in the Alkira CXP as a service and extend their enterprise security postures to the cloud. Customers can simply assign cloud networks to groups, and then configure and apply Alkira's intent-based policies to traffic flows between the groups and intelligently steer them to FortiGate services. A high-level representation of the service is shown in the diagram below.

![Figure 1: Fortinet FortiGate and Alkira solution overview](image)
**Topology**

The high-level topology is depicted in Figure 2 where groups of FortiGates are deployed in regional Alkira CXP’s to provide security policy enforcement for application traffic between any set of endpoints connected to the Alkira global cloud backbone.

![Figure 2: On-premises FortiManager and FortiGate in Alkira CXP](image)

Typically, in customer environments, FortiGates are managed by the customer’s existing FortiManager system, which can be either on-premises or in the cloud. Figure 2 shows the FortiManager on-premises in the data center connected to Alkira CXP. FortiGate in Alkira can also have connectivity to a FortiManager on a public network via Internet Connector from Alkira CXP.

![Figure 3: FortiManager on public network and FortiGate in Alkira CXP](image)

Customers consume the FortiGate firewalls as a service and leverage Alkira’s intent-based policies to selectively forward data traffic to the FortiGate firewall services for inspection of east-west, north-south, and internet-bound traffic.
Prerequisites

Below are the prerequisites for deploying FortiGate on Alkira CXP:

- Before the deployment, identify how FortiGate will be managed. A FortiGate can be managed by a standalone FortiManager or from the FortiGate instance portal.
- Customers using BYOL must have a license file downloaded from FortiCloud.
- To get Fortinet support on PAYG on-demand licensing devices, customers are required to open a support case with Fortinet Customer Support.
- Customer has the access to Cloud Services Exchange (CSX) portal.
- Customer has identified the flows for the firewall and understands the process of onboarding on-prem and cloud connectors on CXP.
- Customer understands their HA and redundancy requirements.
- FortiGate version must be the same or lower than FortiManager's version running in the customer's environment. This deployment guide uses Fortinet version 6.4.7 on both the FortiGate instance and FortiManager.

Configurations

This section provides steps on how to deploy FortiGate in the CSX portal and configure the FortiManager to manage the firewall instances. The Quick Start Configurations section is for users that are familiar with the Alkira portal. For detailed configuration, please refer to the next section: Configuration Details.

The FortiGate integration has mainly three stages of configurations.

1. Deploy FortiGate in CXP portal.
2. Configure Alkira policy in CXP to redirect traffic to FortiGate.
3. Configure firewall policies on FortiGate/FortiManager.

These configuration stages apply to any use case that requires traffic to be redirected to the firewall in Alkira CXP. Customers may require a firewall for traffic from on-prem to cloud or internet, or from cloud to cloud or to internet. With the flexibility of choosing groups, segments and connectors as a source and/or destination in both Alkira policies and on firewall zone to groups mapping, any use case can be implemented following the same three stages of the configurations.
Quick Start Configurations

This section provides a quick summary of the configurations to deploy FortiGate in Alkira CXP.

Deploy FortiGate in CXP

Alkira automates the deployment of FortiGate with minimal configurations from the portal.

- In the Network section, click + in the Services column of CXP and select Add Fortinet Firewall.
- Specify Name to the firewall and select the firewall version.
- Provide FortiManager IP address if FortiGate is managed remotely.
- Select BYOL or PAYG license type and if autoscale is required then set minimum and maximum number of firewalls.
- Provide the password for admin user.
Choose the segments:

- Select the segment for data traffic and provide Alkira Groups to Firewall Zone mappings.
- Select the segment on which FortiManager is reachable.

Finally choose the size, billing tag and tunnel protocol.

That's it, click Save Firewall Service and hit Provision.

**Configure Alkira Policy**

By default, traffic between the Alkira connectors is permitted for direct communication. Configure Alkira policy to redirect traffic to FortiGate.

To configure Alkira policy to redirect the traffic to FortiGate, configure rule(s), rule list, and the traffic policy by following steps below:

**Policy**

- Under All Policies, click + to add new traffic policy.
- Name the policy and choose whether the policy should be in disable/enable state after provisioning completes.
- It is recommended to write a detailed description of the policy.
- Select the segment in which FortiGate is deployed.
- Choose From resource for Source and To resource for Destination of the flow.
- Select + to add new rule list.
Rule List
- Name the new rule list.
- It is recommended to write detailed description of the rule list.
- Click + to add rule(s) in the rule list.
- Either select existing rule(s) or click + to create new rule(s).

Rule
- Name the rule and select Allow to permit the traffic.
- Add from and to IP addresses and port information if redirection to FortiGate is required for only specific prefixes and/or ports.
- Under WITH section, open drop-down menu of Service Type and choose Fortinet FW Service.

Save Rule, Rule List, Policy, and then Provision
- Save changes for rules.
- Select the configured rule for the rule list and click ADD SELECTED.
- Save rule list.
- Select rule list in the policy and click Save Policy.

In the last step, go to Network and provision the changes to implement the new policy.

FortiManager Configurations
The newly deployed FortiGate uses the FortiManager IP address to register itself with FortiManager. Customers can configure and push the firewall policies to FortiGate from FortiManager. Note that Alkira does not access the customer's FortiManager directly during any part of the automated configuration process.
Configurations Details

This section provides the details of the configurations to deploy FortiGate in Alkira CXP.

Deploy FortiGate in CXP

Alkira automates the deployment of FortiGate with minimal configurations from the portal.

- In the Network section, click + in the Services column of CXP and select Add Fortinet Firewall.

Specify name of the firewall, which can be maximum 12 characters long. Customers typically use their companies’ naming convention to name firewalls.

- Select the available version for FortiGate from the drop down menu. Note that Alkira does not provide code version recommendations to customers for any services integrated in Alkira. Customers must reach out to the sales representative of third-party vendors for such information. Also note that FortiManager can only manage FortiGates that run equivalent or lower versions.
- Provide IPv4 address of FortiManager, if FortiGate is managed remotely. Alkira configures the customer-provided IP address of FortiManager in the Security Fabric connector settings of FortiGate during the bring-up process.

There are two things that must be considered for successful connectivity between FortiGate on CXP and FortiManager. First is to choose the correct management segment (configured in next steps) in which the management IP of FortiGate can reach FortiManager. This segment must also be one of the target segment selections. Secondly, identifying the path to reach FortiManager is configured for the flow from routing and security list/rules perspective. If the FortiManager is on the customer's premises for example, in the data center, validating that flow from FortiGate in CXP on port 541 is permitted to the FortiManager IP address from FortiGates. If FortiManager is in a public cloud with the public IP address, there must be an internet connector deployed in the segment that is identified as a management segment. The internet connector, by function, source NATs the egress traffic from Alkira to the internet. In case there is a security list before the public FortiManager, the NATed IP addresses of the internet connector should be added in the security lists by the customer to permit connectivity from FortiGate to FortiManager.

Next, select Autoscale options and License Type. At maximum, four instances can be configured for autoscaling. Alkira triggers autoscaling when the CPU usage of the instance is more than 80% for more than 10 minutes. The scale down of instances is if the CPU usage goes below 60% for more than 10 minutes. If redundancy is required, the customer should deploy two FortiGate instances for the same segments. Multiple instances in the same CXP are always active-active so customers must make sure to have the same configurations applied to all instances from FortiManager.

Alkira provides the option for both BYOL or PAYG license types.
Customers using BYOL must have a license file downloaded from FortiCloud along with the serial number. If autoscale is configured, Alkira requires the customer to provide the license files for the number of instances configured in the Maximum field of Autoscale. For PAYG license type, no license files are required. For PAYG pricing contact an Alkira sales representative.

Note that to get Fortinet support on PAYG on-demand licensed devices, customer is required to open a support case with Fortinet Customer Support and provide the following information:

- The serial number of your FortiGate-VM instance
- The email ID of your Fortinet account. If you don’t have a Fortinet account, you can create one at Customer Service & Support.
- Provide the password for admin user. This password overrides the default password of the admin user during provisioning. To log in to FortiGate using HTTPS or SSH, the host must be able to reach the management IP address of FortiGate in the management segment.

Choose the target segments and zones to group associations. The same FortiGate instance in CXP can be used in multiple Alkira segments. Each segment connects to a separate FortiGate VRF maintaining end-to-end segmentation. Select a Segment from the drop down menu.

Firewall zones to Alkira groups mapping is optional and it is the customer’s decision whether to design their zone-based policies on the firewall. If zones are not configured for provisioning, then all traffic redirected to the firewall is part of the default zone on the firewall. To create zone-based policies on the firewall, customers can map the Alkira groups with zones on the FortiGate.

- Under the segment, click + Add a new Zone. Up to eight zones to group mappings can be configured.
The number in parenthesis (#) next to the zone name shows the number of groups associated with the zone. Click the zone and associate the Alkira group with the zone. The firewall zone to Alkira group is one-to-many mapping. Customers can map multiple groups to a single zone per the security requirements.

![Add a new Zone](image)

The number in parenthesis now shows (1).

Another zone with the name Internet is added in the configuration. Customers can configure inter-zone and intra-zone policies on the firewall and Alkira maintains the symmetry of the flows from source and destinations.

Note that additional target segment(s) can be added to the FortiGate after the provisioning by following the same configuration steps.

- Select the management segment for the FortiGate management interface. The FortiGate management IP must be in a segment that has reachability to FortiManager. Note that it is a requirement to have Management Segment as one of the target segments.

![Management Segment](image)

Note that for each zone and the management interface, Alkira creates two IPsec tunnels and BGP sessions over it. In the FortiGate Instance Overview section later in the document, the interface mapping to segments and zones is explained in detail.

- Finally, choose the Service Size, Billing Tag, and Tunnel Protocol for the FortiGate instance.
The supported service sizes depend on the size of the CXP.

<table>
<thead>
<tr>
<th>FortiGate Size</th>
<th>Bandwidth</th>
<th>vCPU</th>
<th>CXP</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>100 Mbps</td>
<td>2</td>
<td>Small, medium, large, 2 and 5 large</td>
</tr>
<tr>
<td>M</td>
<td>500 Mbps</td>
<td>2</td>
<td>Medium, large, 2 and 5 large</td>
</tr>
<tr>
<td>L</td>
<td>1 Gbps</td>
<td>4</td>
<td>Large, 2 and 5 large</td>
</tr>
<tr>
<td>2L</td>
<td>2 Gbps</td>
<td>8</td>
<td>2 large, 5 large</td>
</tr>
<tr>
<td>5L</td>
<td>5 Gbps</td>
<td>16</td>
<td>5 large</td>
</tr>
</tbody>
</table>

To gain higher throughput, customers can deploy up to four FortiGates in a CXP where each instance can support up to 2 gigabit throughput. However, Alkira’s infrastructure is horizontally scalable. If more than four firewalls are required per CXP, customers can contact the Alkira support team. There can be a maximum of four segments mapped to the firewall. Also, when designing and planning zones, across all services in the CXP, up to 36 zones can be configured. Note that the performance numbers of FortiGate features are dependent on the type of Fortinet license used by the customer.

Customers can also configure one or more Billing Tags.

- Choose the Tunnel Protocol for connectivity from each segment to its mapped VRF in the FortiGate instance. By default, Alkira uses IPSEC as a Tunnel Protocol for both data tunnels and management-interface tunnels.
- Click Save Firewall Service and plan to provision the pending changes.

**Configure Alkira Policy**

To redirect the traffic to FortiGate in CXP, configure Alkira traffic policy. Traffic policy consists of the rule(s) and rule-list. Alkira provides a simple workflow to configure policy, rule-list, and rule(s).

- In the Network Topology section, go to Actions and Add New Policy.
- Since we require a change to the behavior of the network traffic, choose Traffic Policy.

- Name the policy and choose whether the policy should be in disable or enable state after provisioning completes. Customers typically keep the policies in disable state during the staging and provisioning and enable them during routine maintenance windows. Provisioned policies in disable state can be enabled with no or minimal impact to traffic.

- It is recommended to write a detailed description of the policy that identifies the purpose, flow and source/destinations of the policy.

- Select the segment in which FortiGate is deployed. Note that if multiple target segments are configured for FortiGate, then each segment requires a separate traffic policy to redirect the traffic to FortiGate.

- Choose From resource for Source and To resource for destination of the flow.

- Select + to add new rule list.
- Name the new rule list
- It is recommended to write a detailed description of the rule list to identify the purpose of the rule list.

- Click + to add rule(s) in the rule list.
- Either select existing rule(s) or click + to create new rule(s).

The last part of the policy is to create the rule. A rule can be configured for further granularity on the selection of the traffic based on 5-tuple.
- Name the rule and select ALLOW to permit the traffic. The Allow option is in effect only when the policy is in enable state.
- Add FROM and TO IP addresses and port information if redirection to FortiGate is required for only specific prefixes and/or ports.
- Open drop down menu of Service Type and choose Fortinet FW Service.

**Save Rule, Rule List, Policy, and then Provision**

- Save changes for rules.
- Select the configured rule for the rule list and click ADD SELECTED.
- Save rule list.
- Select Rule List in the policy and click Save Policy.

Once saved, verify the policy configurations and view the path of the policy from the action under Network Topology. Select All Policies and then click the eye icon of the new policy. This shows the exact traffic path for which the policy is applied.

In the last step, go to Network and provision the pending changes to implement the new policy.

**FortiGate Instance Overview**

The provisioning of FortiGate instances in CXP creates the required VRFs, tunnels, BGP sessions, and management interface.

In Network Topology, click on the Fortinet Firewall in the services section of the CXP. The Fortinet Firewall Service plane shows the provisioning status, health of the FortiGate instance, and tunnel status. Note that for each zone, Alkira creates two tunnels for redundancy.
The management IP address of the instance is automatically chosen from the IP block of the management segment. Use this IP address to log in the FortiGate instance from a host that is connected to the management segment.

After login, go to Network in the left panel and then Interfaces. This page provides details of the number of physical interfaces, VRFs, tunnels, and zones.

To understand information on this page, note that there are three zones. Management zone is the result of management segment and apps-zn and INET-zn are mappings under the target segment configuration in Alkira portal.
A loopback interface is used as a management interface. This loopback is enabled for PING, SSH, HTTPS, and is also configured to connect to FortiManager. Each of the zones from Alkira groups mapping creates two tunnels each. The figure below shows that the management zone, INET-zn, and apps-zn have two tunnel interfaces each.

Management and each of the target segments identified in the Alkira portal are mapped to separate VRFs. Thus the tunnel interfaces associated with the zones from the specific segments are in the VRFs on the FortiGate instance that are mapped to their respective segments.
The BGP section shows the BGP sessions that are established over the tunnels.

FortiGate Firewall Policies

Customers are responsible for creating and maintaining the firewall policies per their security requirements. Policies on the firewalls are created either directly from the FortiGate instance or from FortiManager and then pushed to the FortiGate instance. The figure below shows the basic existing policies on the FortiGate to permit zones to port communications.

- Click + Create New to configure a new policy and add incoming zone, outgoing zone, Source, Destination, Service, and ACCEPT.
Disable NAT option. NAT from FortiGate is not required because NAT is performed at the internet connector for egress traffic and Alkira CXP intelligently maintains the symmetry for the return traffic to FortiGate. Enable the policy as required to the migration timeline and click OK to save the policy. FortiGate Firewall Policy is now configured.

Manage from FortiManager

To manage FortiGate from FortiManager, discover the new FortiGate instance in FortiManager.

- From the main dashboard of FortiManager, go to Add Device and then Discover devices.
- Provide the IP address of the FortiGate instance from Alkira with user credential and click Next.

Click Next to onboard the discovered device.
Per the notification from FortiManager, to manage policies and objects of the device, they need to be imported into the FortiManager database.

- Click Import Now and all policies that were configured on FortiGate are shown. Modify policy package name as required and click Next.

Policies are successfully imported.
To create a new policy for the FortiGate instance, go to Policy & Objects and under Policy Packages, click + Create New for the Policy Package. For any further configuration guidelines for FortiGate and FortiManager, please refer to Fortinet Configuration Guides by Fortinet.