Technology Partner Program Integration Guide

Author: Alkira

Revision History	
05-26-2020	New Integration Guide for Alkira Cloud Services Exchange (CSX) with Palo Alto Networks VM-Series.

Partner Information	
Company Name	Alkira, Inc.
Website	https://www.alkira.com
Partner Product	Alkira Cloud Services Exchange™
Partner Contact	Robin James, Product Manager, robin@alkira.com
Support Contact	support@alkira.com
Product Description	Alkira Cloud Services Exchange is an as-a-service multi-cloud network that offers a simple, secure, and scalable solution to connect users, branches, and data centers to a cloud or multiple clouds.

Table 1: Integration Details by Product

Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested	Alkira Versions Tested
VM-Series	Validated	VM-300, VM-700 PAN-OS 9.0.5-XFR	May 2020 (CSX is delivered as-a-service and hence does not have a software version)
Panorama	Validated	PAN-OS 9.1.2 Run same OS as VM-Series or higher	May 2020 (CSX is delivered as-a-service and hence does not have a software version)

Use Cases for Integration with the Palo Alto Networks VM-Series

Leveraging Alkira Cloud Services Exchange (CSX) organizations can now enforce their business security policies in the cloud with Palo Alto Networks VM-Series Virtual Next-Generation Firewalls. VM-Series firewalls would secure communication in the following use cases:

- On-premises to cloud
- Cloud to cloud
- Cloud to internet
- Cloud DMZ
- On-premises to internet

Integration Benefits

The ability to insert Next-Generation Firewalls for network traffic to and across clouds is imperative for successful cloud adoption. Integration of the Palo Alto Networks VM-Series firewall on the Alkira Cloud Services Exchange provides customers the following benefits:

- The capability to point and click Palo Alto Networks VM-Series firewalls (VM-300 and VM-700) into a global on-demand multi-cloud network.
- The capability to easily map various cloud and on-premises workloads to security zones on the firewall.
- The ability to inspect and apply policies on the VM-Series for traffic on the Alkira CSX.
    - On-premises to cloud
    - Cloud to cloud
    - Cloud to internet
    - Cloud DMZ
    - On-premises to internet
- Symmetric traffic steering and simplification of the deployment for the customer.
- Instantiation of VM-Series firewalls with correct instance sizing and capacity.
- Ease of auto-scaling the firewall deployment based on real-time capacity demand. This is done with a simple setting on the Alkira CSX Portal (graphical user interface).
- The ability to connect the VM-Series firewall to on-premises Palo Alto Networks Panorama™ network security management through an overlay network. This helps customers have a consistent enterprise security policy and operating model across a multi-cloud environment.

Integration Diagram

Alkira Cloud Services Exchange consists of globally distributed virtual infrastructure of Alkira Cloud Exchange Points™ (CXP). The CXPs are virtual multi-cloud points of presence with full routing stack and network services capabilities. The VM-Series firewall is deployed as a network service in the CXP.

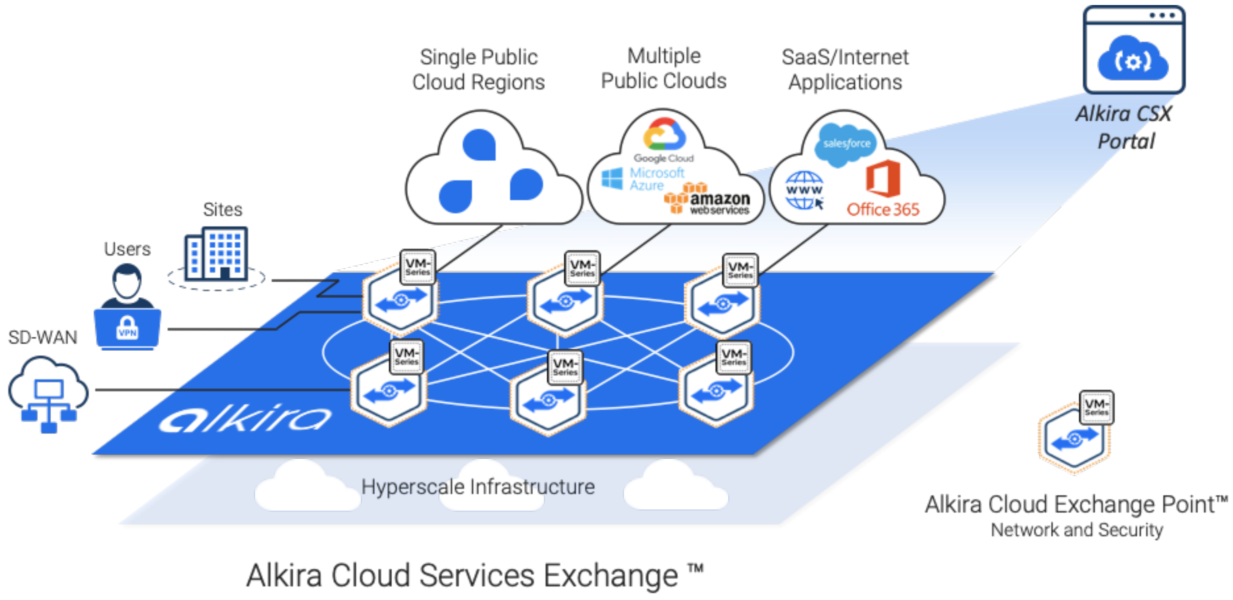
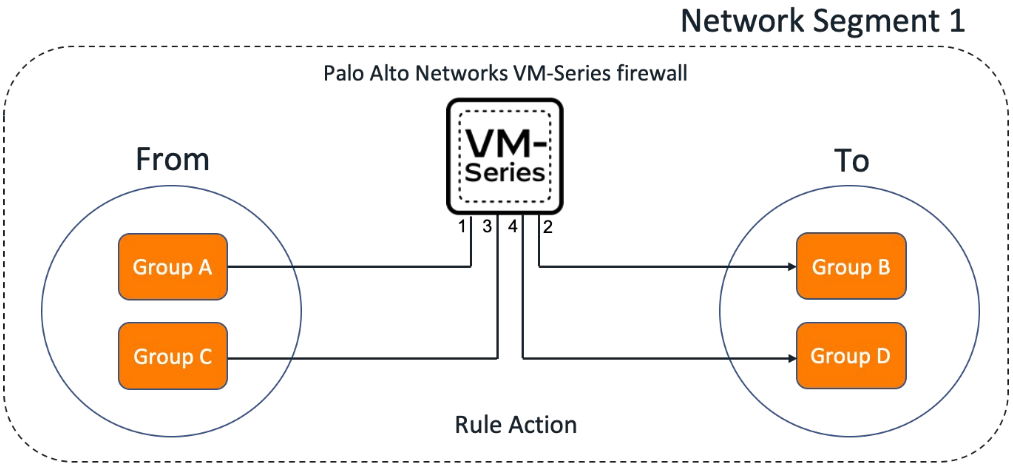


Figure 1: Cloud Services Exchange and VM-Series firewalls

Organizations create Alkira policies and rules in order to forward the application traffic of interest to the globally provisioned Palo Alto Networks firewalls. Policies identify the communication from/to parties and the particular network segment they belong to (different segments can have different policies). Communicating parties can be different cloud instances, sites communicating to the cloud, sites communicating to the internet and so on. Rules identify the traffic of interest to be subject to firewall inspection. Traffic of interest can be identified based on 6-tuple matching (including DSCP) or based on an application recognition engine.



Rule1: Send traffic from Group A (Zone1) to Group B (Zone2) to the Firewall for inspection

Rule2: Send traffic from Group C (Zone3) to Group D (Zone4) to the Firewall for inspection

Figure 2: VM-Series Firewall Integration with Alkira CSX

Before You Begin

- License
  - Customers can deploy the VM-series on Alkira CSX using their own enterprise license (ELA). This is considered the BYOL mode on Alkira CSX. To do this customer needs to obtain Auth Codes corresponding to the VM-Series model (VM-300 or VM-700) they choose to deploy. Customer also need to obtain the Licensing API key from their Palo Alto Networks Support Portal.
- Panorama
  - Managing the VM-Series on Alkira CSX through the existing enterprise Panorama is optional but recommended. It is mandatory if deploying more than one VM-Series on the CSX.
  - Customer needs to obtain Auth Key, Device Group name, Panorama IP address, and Template Stack name to connect the VM-Series to their existing enterprise Panorama.
  - The Panorama version should be higher than the VM-series version to be deployed.

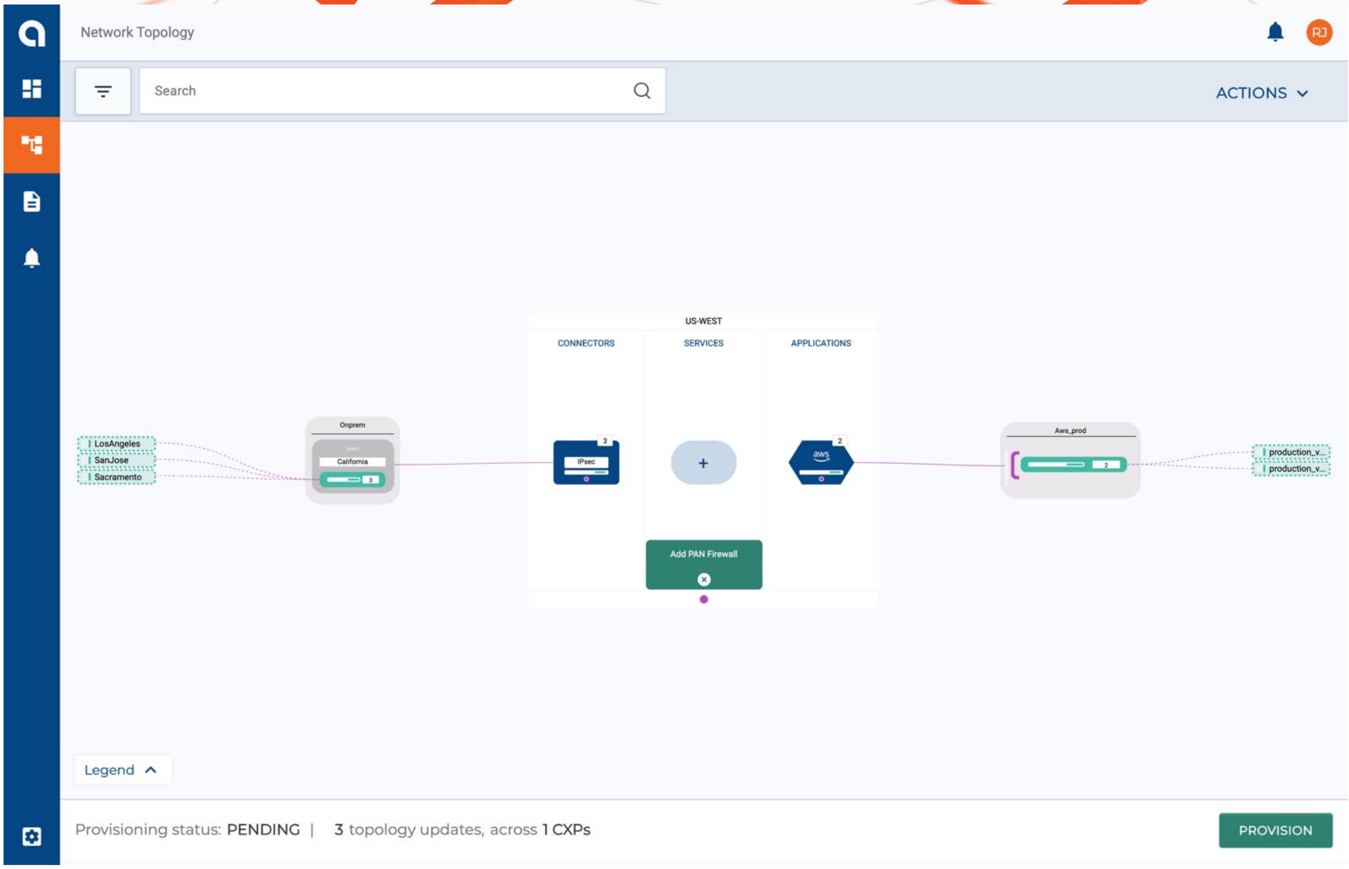
Palo Alto Networks Configuration

Palo Alto Networks VM-Series firewalls are easily instantiated on the Alkira CSX using a few steps on the Alkira CSX graphical user interface (see next section). Once deployed, the customer can manage the VM-Series using the enterprise Panorama. Alternatively, the customer can access the VM-Series directly using the management IP displayed on the Alkira CSX GUI. The customer is only required to define the business security policies for inter-zone and intra-zone traffic. For guidelines on how to create security policies on PAN-OS®, please refer to the Admin Guide: https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-admin/policy/security-policy/create-a-security-policy-rule.html.

Partner Product Configuration

With Alkira, your multi-cloud network and VM-Series firewall security are offered as a service, on-demand, when you need it. You do not need to perform tedious network and routing configuration tasks. Your entire global multi-cloud network with Palo Alto Networks firewalls is modeled through the intuitive Alkira Cloud Services Exchange graphical user interface in point-and-click fashion.

a. Select the Alkira Cloud Exchange Point (CXP) where you want to provision the VM-Series firewall. In a geographically distributed deployment, VM-Series firewall instances should be provisioned in multiple Alkira Cloud Exchange Points to enforce security policy closest to the source.



Provisioning status: PENDING | 3 topology updates, across 1 CXPs

Figure 3: Alkira CSX Network Topology Page

b. Select the Bring-Your-Own-License (BYOL) licensing option for the VM-Series firewall deployment. Please also provide the firewall license key.

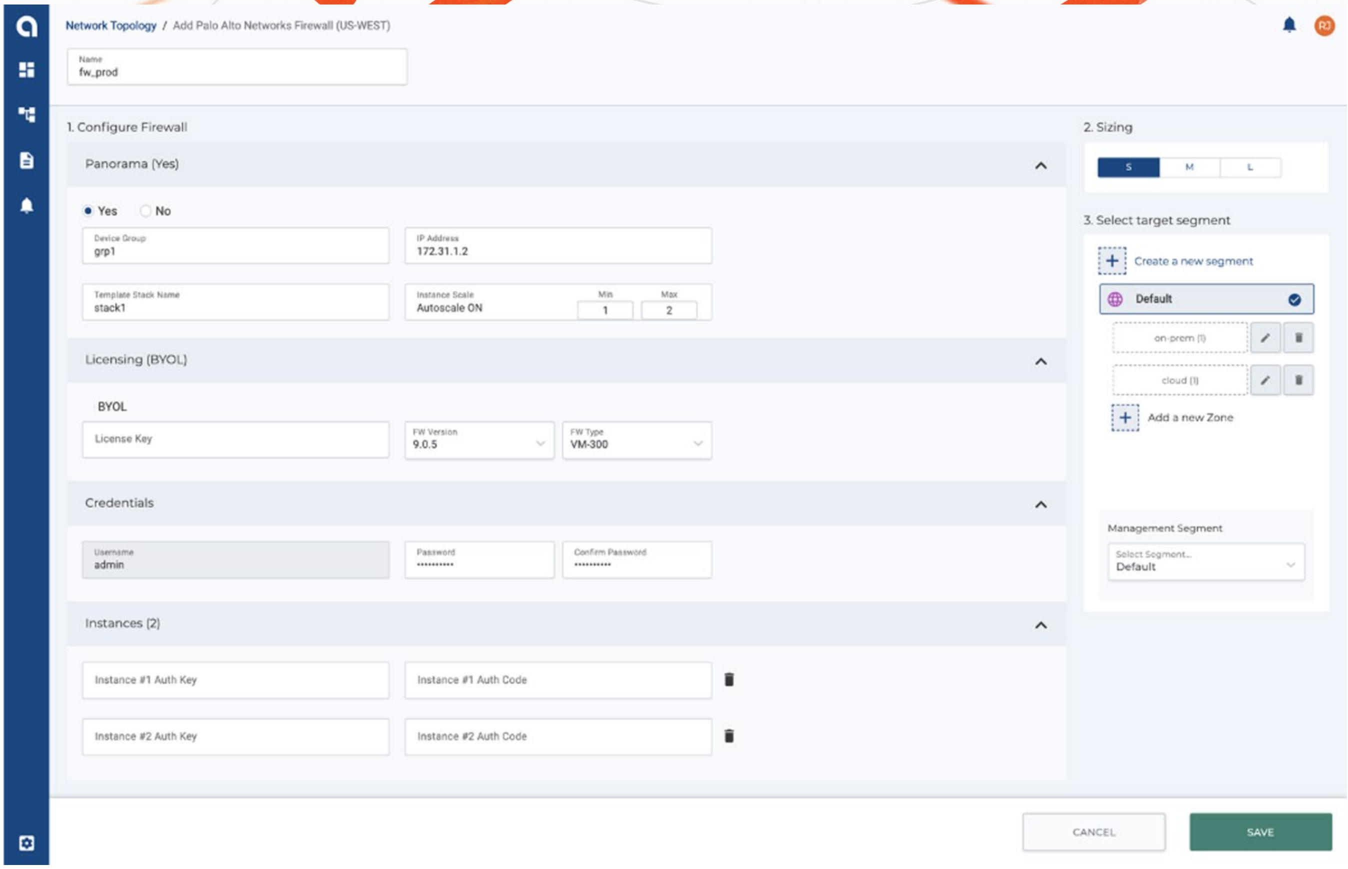
c. Choose whether you want to use Panorama with your VM-Series firewall deployment. If yes, provide the details of your Panorama deployment, such as server IP address, the device group the Firewall belongs to, and the Firewall instance authentication key.

   For centralized and consistent management of all global Palo Alto Networks firewalls deployed in the Alkira Cloud Services Exchange, it is recommended to use Panorama. The Alkira service does not deploy the Panorama server, but it does provide all the necessary connectivity from the VM-Series firewalls to the Panorama server deployed by your organization. Note: You must enable Panorama if you want to use the Firewall auto-scaling feature of the Alkira Cloud Services Exchange.

d. Provide firewall-specific details, such as the model of your VM-Series firewall(s), the desired PAN-OS® software version, and the username and password for the firewall administrative account.

e. All defined network segments are automatically extended to all provisioned Palo Alto Networks firewalls across the entire Alkira Cloud Services Exchange. This allows Palo Alto Networks firewalls to inspect application traffic in any of the segments. Map the various cloud or on-premises workloads to their corresponding zones on the Palo Alto Networks firewalls. Palo Alto Networks firewalls can also provide secure cross-segment communication, if desired.

f. Optionally, enable firewall auto-scaling. Firewall auto-scaling, as the name suggests, allows horizontal scaling in and out of VM-Series firewall instances deployed in the Alkira Cloud Exchange Point based on required capacity. You can set the minimum and maximum number of Palo Alto Networks firewall instances deployed with auto-scaling to make sure there is sufficient minimum firewall capacity always available for both typical use and a sufficient maximum firewall capacity for burst use. During off-peak hours, when firewall load subsides, the Alkira solution will automatically scale in the firewall capacity by bringing down unneeded firewall nodes, potentially all the way down to the minimum specified number.



Network Topology / Add Palo Alto Networks Firewall (US-WEST)

Name
fw_prod

1. Configure Firewall

Panorama (Yes)

● Yes ○ No

Device Group
grp1

IP Address
172.31.1.2

Template Stack Name
stack1

Instance Scale
Autoscale ON

Min
1

Max
2

Licensing (BYOL)

BYOL

License Key

FW Version
9.0.5

FW Type
VM-300

Credentials

Username
admin

Password
••••••••••

Confirm Password
••••••••••

Instances (2)

Instance #1 Auth Key

Instance #1 Auth Code

Instance #2 Auth Key

Instance #2 Auth Code

2. Sizing

S M L

3. Select target segment

Create a new segment

Default ✓

on-prem (1)

cloud (1)

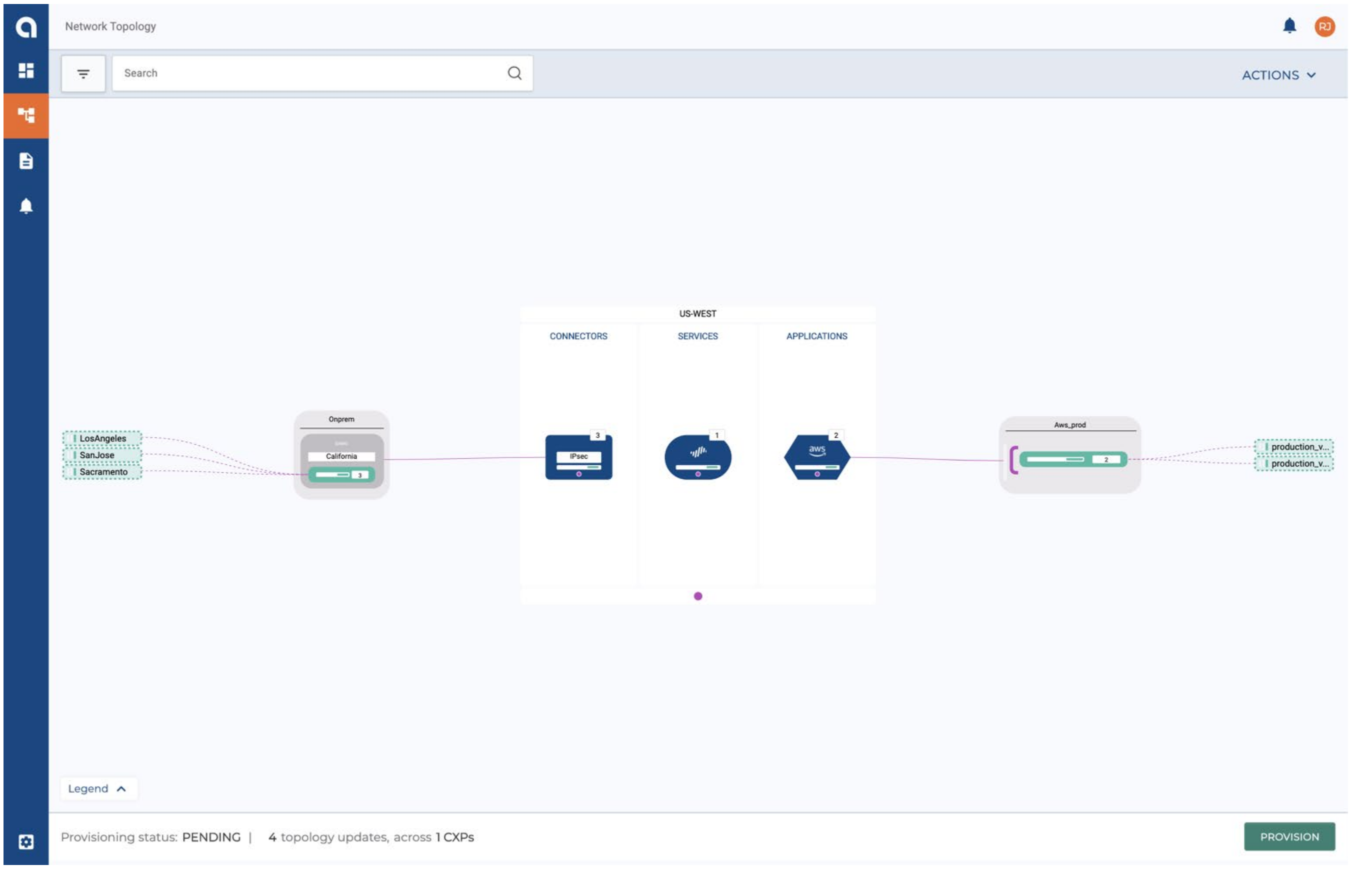
Add a new Zone

Management Segment

Select Segment...
Default

Figure 4: VM-Series Firewall Service Configuration Page

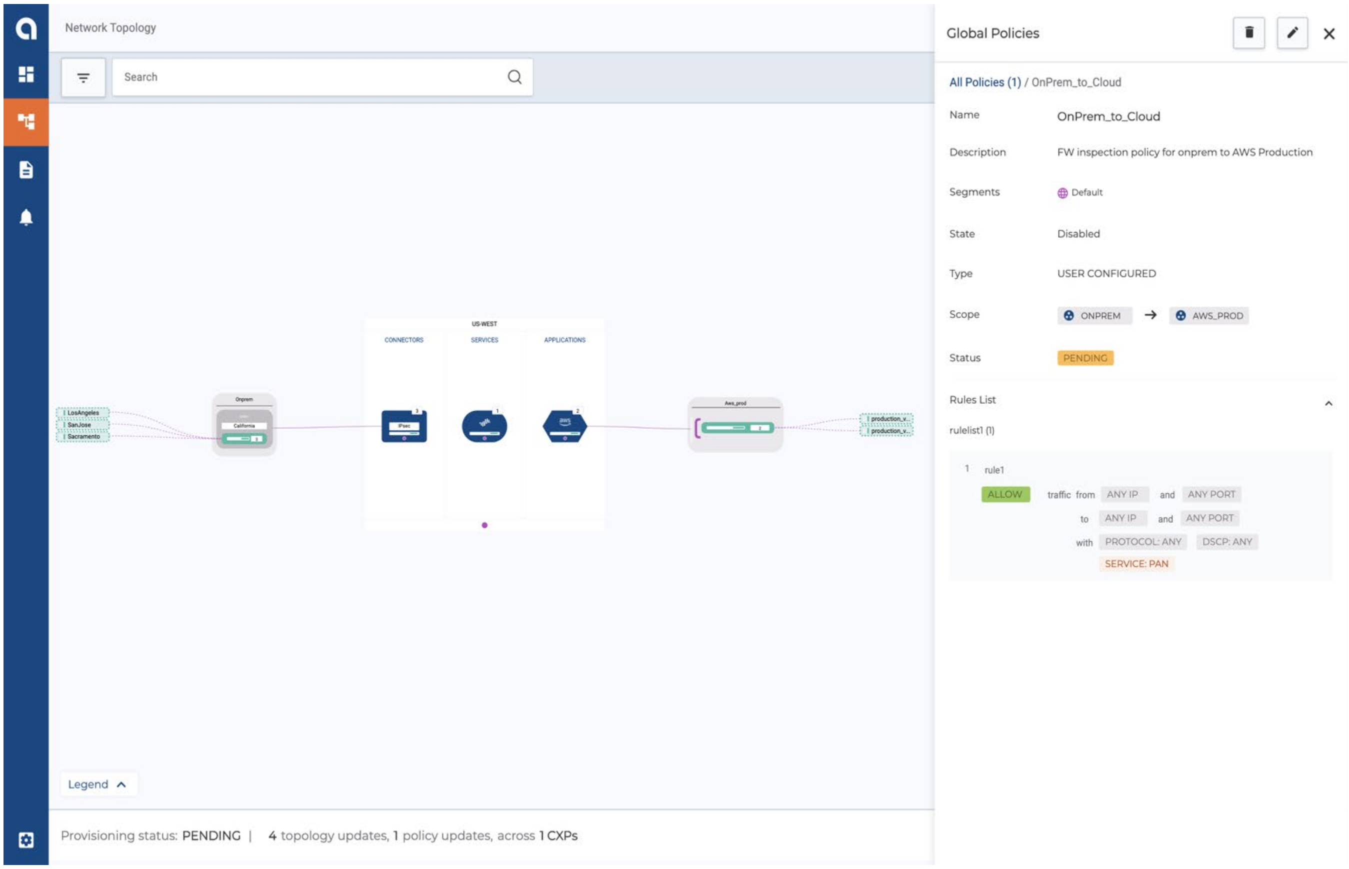
g. Save the VM-Series deployment configuration and click "Provision" to deploy the VM-Series firewall in the global multi-cloud network.



Provisioning status: PENDING | 4 topology updates, across 1 CXPs

Figure 5: Network Topology page with VM-Series Firewall

h. Create Alkira policies and rules in order to forward the application traffic of interest to the globally provisioned Palo Alto Networks firewalls. Policies identify the communication “from”/“to” parties and the particular network segment they belong to (different segments can have different policies). Communicating parties can be different cloud instances, sites communicating to the cloud, sites communicating to the internet, and so on. Rules identify the traffic of interest to be subjected to firewall inspection. Traffic of interest can be identified based on 6-tuple matching (including DSCP) or based on an application recognition engine.



Global Policies

All Policies (1) / OnPrem_to_Cloud

Name: OnPrem_to_Cloud

Description: FW inspection policy for onprem to AWS Production

Segments: Default

State: Disabled

Type: USER CONFIGURED

Scope: ONPREM → AWS_PROD

Status: PENDING

Rules List

rulelist1 (1)

1 rule1

ALLOW traffic from ANY IP and ANY PORT
to ANY IP and ANY PORT
with PROTOCOL: ANY DSCP: ANY
SERVICE: PAN

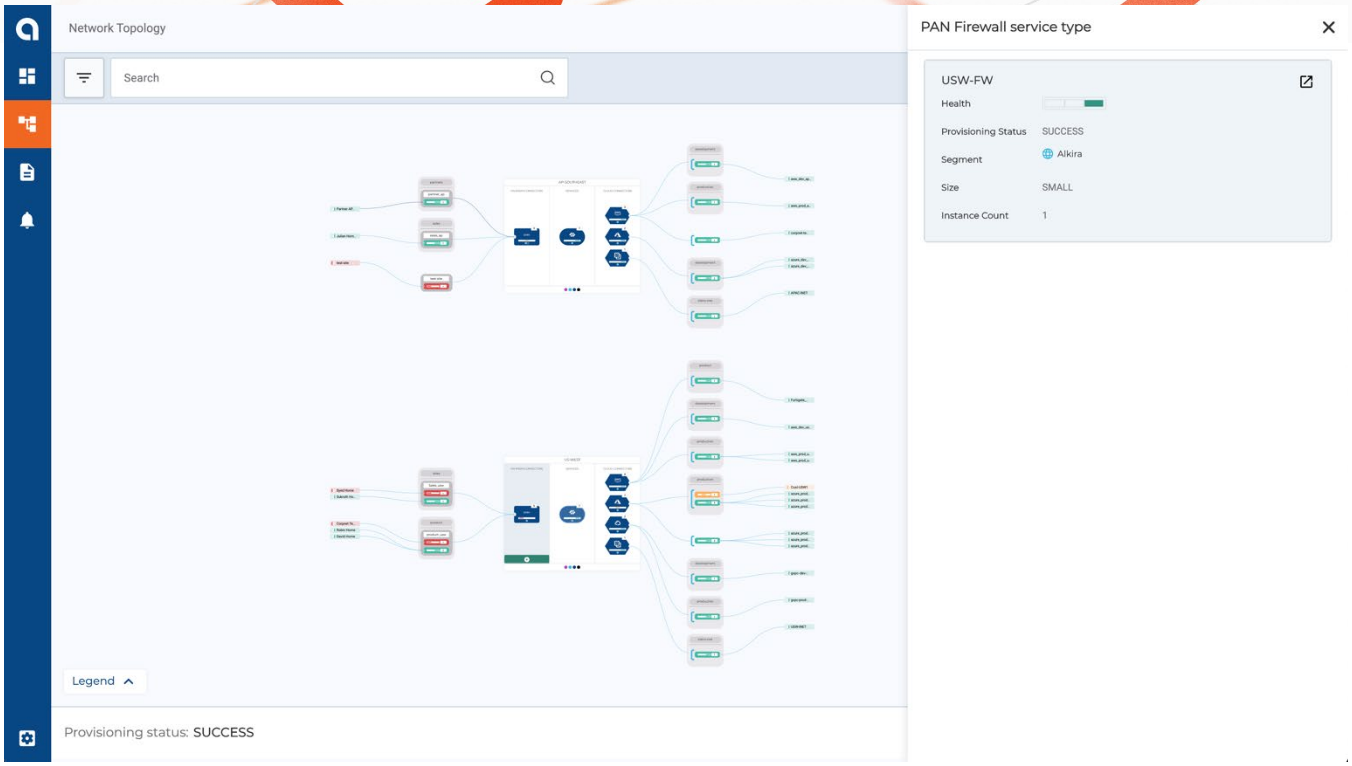
Provisioning status: PENDING | 4 topology updates, 1 policy updates, across 1 CXPs

Figure 6: Alkira Policy to steer traffic to VM-Series Firewall

i. You can then enforce your enterprise security policy on the VM-Series firewall by defining intra-zone security policies. This is done by pushing policies from the Panorama connected to the VM-Series or, alternatively, by directly logging in the VM-Series over the overlay network.

Troubleshooting

- Check the Alkira Topology page for the status on the network connectivity from Alkira CSX to VM-Series firewalls. This page will indicate the status of the IPSec & BGP connection to the VM-Series.
  - GREEN indicates the IPSec tunnel and BGP protocol is UP.
  - RED indicates the IPSec Tunnel and/or BGP protocol is DOWN. This happens if all the VM-Series firewalls are DOWN or connectivity to all of them is DOWN.
  - ORANGE indicates marginal connectivity. This happens in a HA scenario if one of the VM-Series firewalls is DOWN or connectivity to one of the firewalls is DOWN.
- Additional details for each VM-Series instance is shown on the Monitoring Dashboard.
  - Navigate to the Services Dashboard from the Main Dashboard. At this page the customer will be able monitor health of each VM-Series instance.
  - The Dashboard will show:
    - Throughput per VM-Series firewall
    - Total Sessions per VM-Series firewall
    - Throughput to each Zone on the VM-Series firewall
    - All of the above data can be seen for the last 2 hrs, 24 hrs, 1 week, 1 month, and 1 year



Provisioning status: SUCCESS

PAN Firewall service type

USW-FW

Health	
Provisioning Status	SUCCESS
Segment	Alkira
Size	SMALL
Instance Count	1

Figure 7: VM-Series Firewall Health Status

- **Contact information for support:** support@alkira.com
- **Member of TSANet**