Palo Alto Networks: Securing Applications in AWS Single VPC via June 2020 Deployment Guide

Contents

About

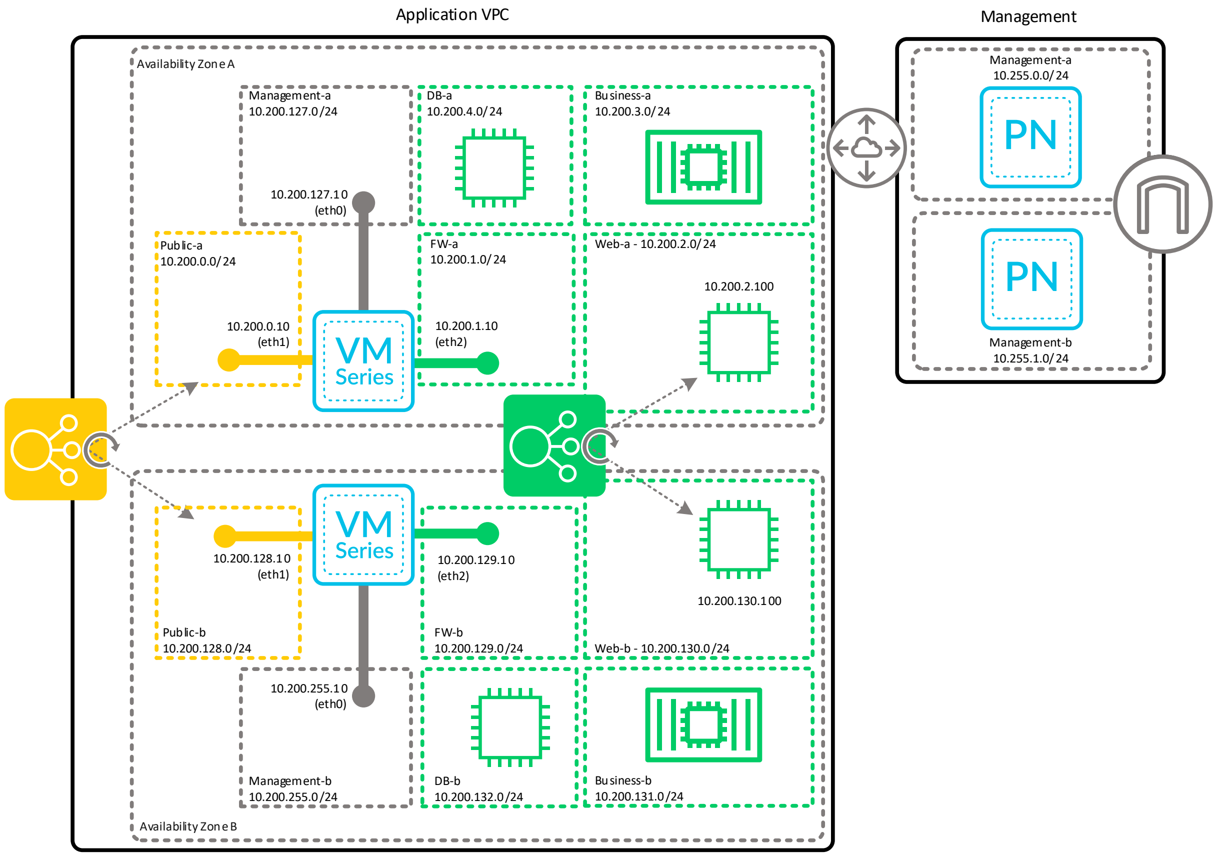
This document explains how to deploy the environment shown in the document *aws-single-vpc-model-deployment-guide.pdf* for the June 2020 deployment guide, Securing Applications in AWS Single VPC using VM-Series appliances and Panorama in AWS. This document can be found in the *docs* folder.

A single standalone VPC might be appropriate for small AWS deployments that:

- Provide the initial move to the cloud for an organization.
- Require a starting deployment that they can build on for a multi-VPC design.
- POC

Topology

The below topology displays the VPC and subnets to be deployed. It also shows the preexisting Panorama instance which will be needed in the same account and region for the purposes of the deployment and is only a requirement and pre-requisite for this template. This topology is deployed in a single account.



Support Policy

This solution is released under an as-is, best effort, support policy. These scripts should be seen as community supported and Palo Alto Networks will contribute our expertise as and when possible. We do not provide technical support or help in using or troubleshooting the components of the project through our normal support options such as Palo Alto Networks support teams, or ASC (Authorized Support Centers) partners and backline support options. The underlying product used (the VM-Series firewall) by the scripts or templates are still supported, but the support is only for the product functionality and not for help in deploying or using the template or script itself.

Prerequisites

The following are the prerequisites to successfully launch the templates:

1. AWS account
2. Clone or download the files and folders to your local machine
3. Deploy Panorama in the same AWS account using the deployment guide, *Panorama on AWS - Deployment Guide - Jun20.*pdf, which can be found in the *docs* folder.
4. Generate a Panorama VM-Auth Key via the following document, https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/generate-the-vm-auth-key-on-panorama.html.
5. If one does not already exist, generate an api key for your primary panorama instance per https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/get-your-api-key.html.
6. Ensure AWS credentials are setup for terraform to use. Here are to guides that may assist with this:
    a. https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-credentials.html
    b. https://www.terraform.io/docs/providers/aws/index.html
7. BYOL licensing is used and requires two authcode(s) or an authcode that has at least two vm-series associated with it. The authcode(s) must be registered with the support portal. The following link provides instructions on how to do this https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/license-the-vm-series-firewall/register-the-vm-series-firewall.html.
8. In addition to the Panorama AWS Elastic IP, an additional 4 Elastic IP (EIP) will be required. By default, AWS generally only allots 5 initial Elastic IP addresses. You can log a support case for additional EIP. In total you will need at least 5 or if Panorama is in HA, 6.

Panorama Connection Methods

VM-Series connection to Panorama uses bootstrap method which is described at https://docs.paloaltonetworks.com/vm-series/9-1/vm-series-deployment/bootstrap-the-vm-series-firewall/vm-series-firewall-bootstrap-workflow.html. The bootstrap package does not use the bootstrap.xml file and all configuration information is pushed by Panorama once registered during the bootstrap process into the appropriate device group and template stack.

Panorama Configuration

This document is does not cover the deployment and initial configuration of Panorama. This guide

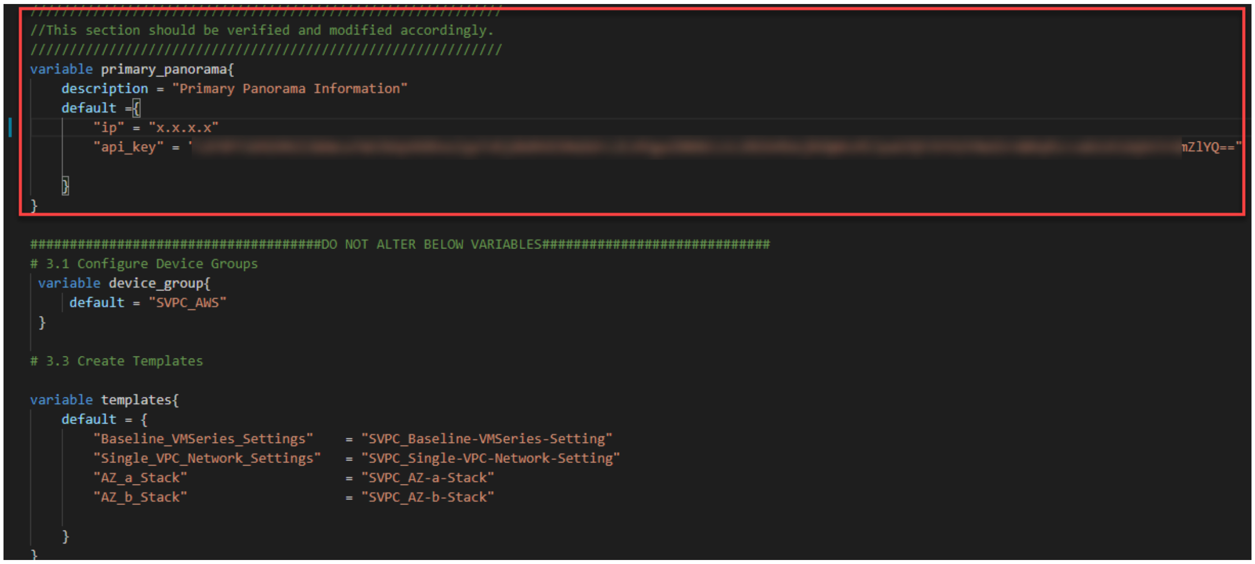
assumes that has been done and that the panorama instance(s) are accessible by the VM-Series during the bootstrap process. Use the deployment guide, *Panorama on AWS - Deployment Guide - Jun20.*pdf, which can be found in the *docs* folder.

Modify Deployment Files

Use a IDE such as VSCode or file editor such as Notepad++ to modify the following files:

\setup_panorama\variables.tf

The items which need to be modified are in a section at the top as shown below:



```
//////////////////////////////////////////////////////////////
//This section should be verified and modified accordingly.
//////////////////////////////////////////////////////////////
variable primary_panorama{
    description = "Primary Panorama Information"
    default ={
        "ip" = "x.x.x.x"
        "api_key" = '[redacted]"

    }
}

######################################DO NOT ALTER BELOW VARIABLES#############################
# 3.1 Configure Device Groups
 variable device_group{
     default = "SVPC_AWS"
 }

# 3.3 Create Templates

variable templates{
    default = {
        "Baseline_VMSeries_Settings"    = "SVPC_Baseline-VMSeries-Setting"
        "Single_VPC_Network_Settings"   = "SVPC_Single-VPC-Network-Setting"
        "AZ_a_Stack"                    = "SVPC_AZ-a-Stack"
        "AZ_b_Stack"                    = "SVPC_AZ-b-Stack"

    }
}
```

\setup_aws\variables.tf

The items which need to be modified are in a section at the top.

\setup_aws\ init-cfg_a.txt and init-cfg_b.txt

In the two init-cfg files you will need to change the following key pair with the generated vm-auth key generated above:

- vm-auth-key=XXXXXXXXXXXX

Environment Information

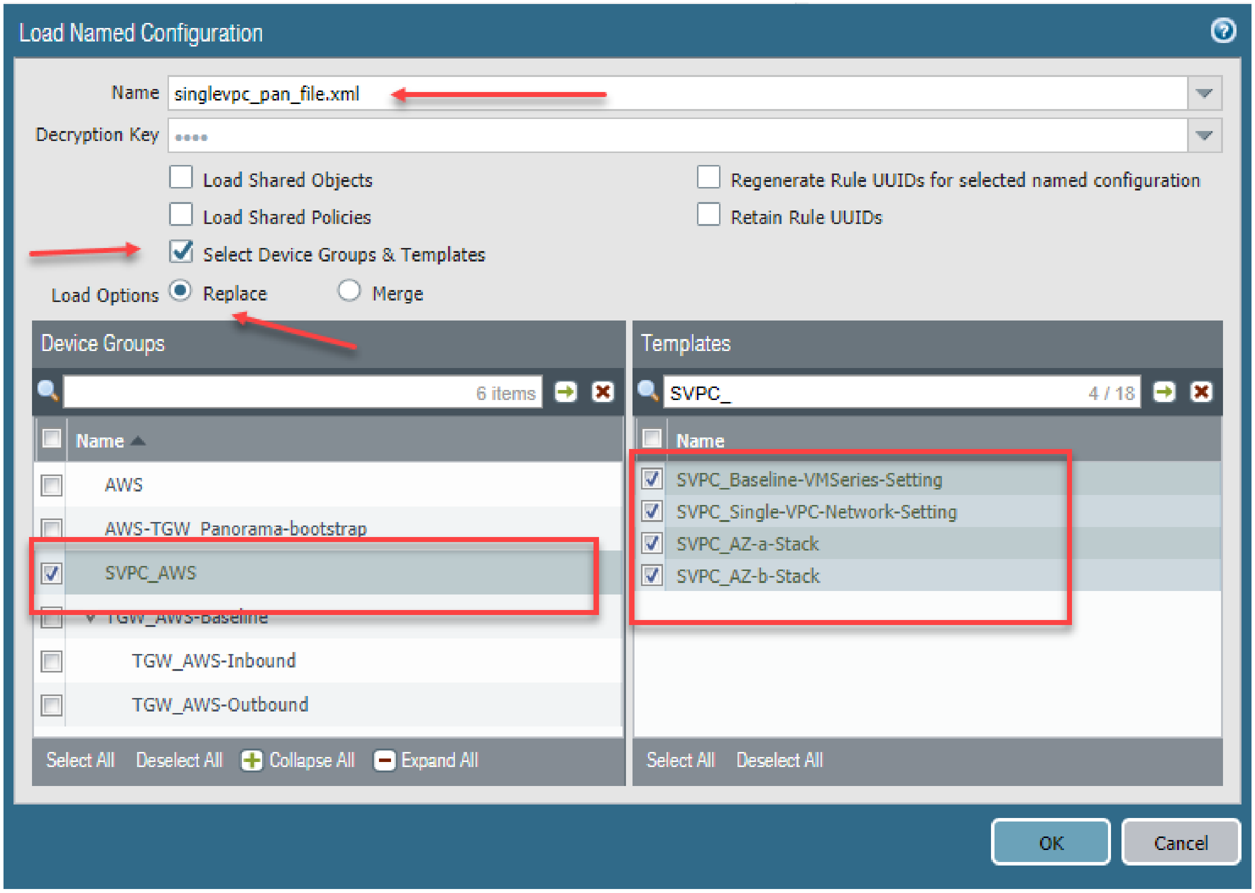
This guide used the following versions:

- Panorama: 9.1.2

- VM-Series: 9.1.3

Deploying the setup_panorama Template

1. Under the context of the setup_panorama folder, on the command line:
    a. Run *terraform init*
    b. Optionally, before you run apply you may want to run *terraform plan*
    c. Run *terraform apply --auto-approve*
2. In the Panorama UI, select Commit ->Commit to Panorama
3. Navigate to Panorama -> Setup -> Operations.
4. Select “Import named Panorama configuration snapshot”
5. Select the file *singlevpc_pan_file.cfg* from the \setup_panorama\panorama_configuration_file folder and then select *OK* to import the configuration.
6. Next, select “Load named Panorama configuration snapshot”.
7. In the resulting dialog
    a. Select the file *singlevpc_pan_file.cfg*
    b. Check the box for “Select Device Groups & Templates”
    c. For Load Options, select “Replace”
    d. Under Device Groups, select SVPC_AWS
    e. Under Templates, select
        i. SVPC_Baseline-VMSeries-Setting
        ii. SVPC-Single-VPC-Network-Setting
        iii. SVPC_AZ_a_Stack
        iv. SVPC_AZ_b_Stack
8. The resulting dialog will look like the below:



Load Named Configuration

Name: singlevpc_pan_file.xml

Decryption Key: ••••

☐ Load Shared Objects

☐ Load Shared Policies

☑ Select Device Groups & Templates

☐ Regenerate Rule UUIDs for selected named configuration

☐ Retain Rule UUIDs

Load Options: ● Replace ○ Merge

Device Groups (6 items)

	Name
☐	AWS
☐	AWS-TGW_Panorama-bootstrap
☑	SVPC_AWS
☐	TGW_AWS-Baseline
☐	TGW_AWS-Inbound
☐	TGW_AWS-Outbound

Templates (SVPC_ 4 / 18)

	Name
☑	SVPC_Baseline-VMSeries-Setting
☑	SVPC_Single-VPC-Network-Setting
☑	SVPC_AZ-a-Stack
☑	SVPC_AZ-b-Stack

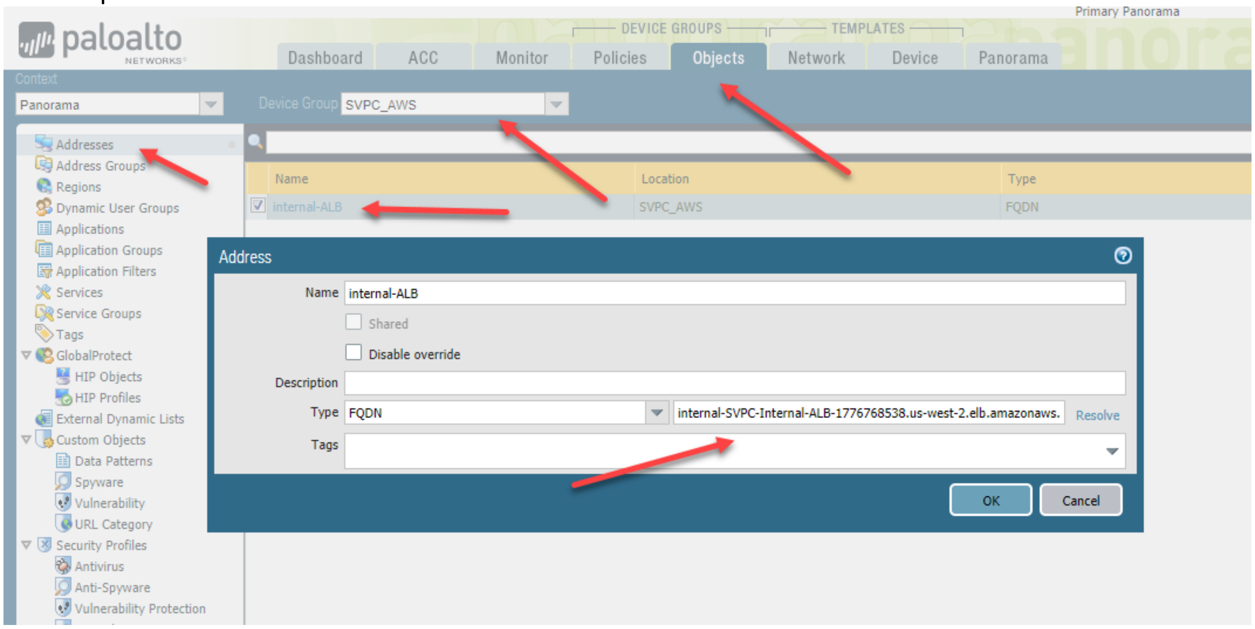
9. Click OK to close the dialog. Ensure the Load job has completed by viewing the Tasks Manager. You can select the tasks manager by clicking on the bottom right icon which says “Tasks”.
10. Once the load job has completed, select Commit->Commit to Panorama.

Deploying the setup_aws Template

1. On the command line under the context of the setup_aws directory:
   a. Run *terraform init*
   b. Before you run apply you may want to run *terraform plan -var="create_webservers=0"*
   c. Run *terraform apply -var="create_webservers=0" --auto-approve*
      i. Ensure there are no errors, it is common to not have enough Elastic IP addresses for the region. In that case, you will need to open a support case with AWS to get additional Elastic IP. Same may happen with VPCs. If you get an error about an **Elastic Network Interface not being allocated correctly or not in a correct state** you can attempt to immediately run the template again. If bothvm-series firewalls do not successfully register with Panorama, then you may need to restart this step.
2. The firewalls take quite a while to come up and register with Panorama once the terraform template has completed (20-30 minutes). Validate the firewalls have come up by navigating on

Panorama to Panorama->Managed Devices->Summary. The two new firewalls should come up under the correct template stacks SVPC_AZa-Stack and SVPC_AZ-b-Stack and the device group SVPC_AWS.

3. Once all the firewalls are registered with Panorama complete the following:
   - From the guide complete 4.2 Refresh the VM-Series Firewall's License to Enable Cortex Data Lake
   - Update the internal load balancer as picture below in the address object from the output of the terraform template which (5.2 Configure the NAT Policy) and commit and push on Panorama



	Name	Location	Type
☑	internal-ALB	SVPC_AWS	FQDN

Name: internal-ALB

☐ Shared

☐ Disable override

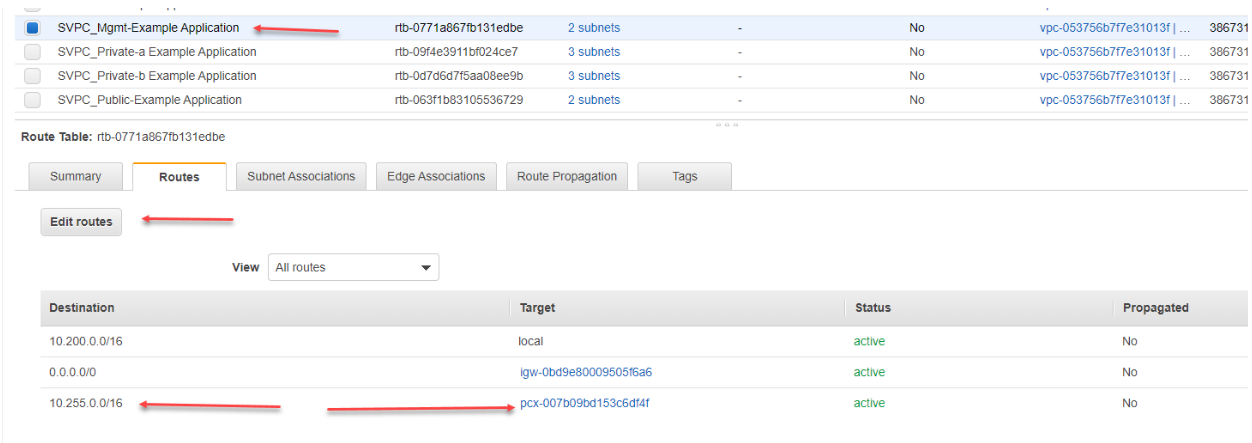
Description:

Type: FQDN internal-SVPC-Internal-ALB-1776768538.us-west-2.elb.amazonaws.

Tags:

4. Now that the vm-series firewalls are setup and configured with Panorama, run the template a second time but change the *create_webservers* variable to create the webservers and attach them to the internal ALB. Run the following command: *terraform apply -var="create_webservers=1" --auto-approve*

***There appears to be a **bug** in the Terraform provider where running this a second time removes the route for the firewalls to get to panorama. You will know this since the firewalls will show as disconnected after initially showing as connect to Panorama. If this is the case you can either run the template again with create_webservers=1 or you will need to manually add the route. The route table is SVPC_Mgmt-Example Application and ensure you select as the target *peering connection* as shown below:



■	SVPC_Mgmt-Example Application	rtb-0771a867fb131edbe	2 subnets	-	No	vpc-053756b7f7e31013f | ...	386731
□	SVPC_Private-a Example Application	rtb-09f4e3911bf024ce7	3 subnets	-	No	vpc-053756b7f7e31013f | ...	386731
□	SVPC_Private-b Example Application	rtb-0d7d6d7f5aa08ee9b	3 subnets	-	No	vpc-053756b7f7e31013f | ...	386731
□	SVPC_Public-Example Application	rtb-063f1b83105536729	2 subnets	-	No	vpc-053756b7f7e31013f | ...	386731

Route Table: rtb-0771a867fb131edbe

View: All routes

Destination	Target	Status	Propagated
10.200.0.0/16	local	active	No
0.0.0.0/0	igw-0bd9e80009505f6a6	active	No
10.255.0.0/16	pcx-007b09bd153c6df4f	active	No

Verifying Deployment

Login for two vm-series firewalls is: svpc_admin / svpc_PaloAlto!

Once the webservers are up and configured you can quickly determine outgoing traffic but looking at the Monitors->Logs-Traffic and you should see outgoing traffic from the webservers to ntp and yum. You can validate incoming traffic by using the output from the template run, specifically the The Inbound Pubic Application Load Balancer FQDN can be put as the address in a browser and should resolve to one of the two web servers. Refresh several times and you will see the hostname in the response change.

Cleanup

To destroy the environment:

1. Run the command, *terraform destroy* in the context of setup_aws folder. This will destroy the AWS environment.
2. Run the command terraform destroy in the context of setup_panorama folder.
3. In Panorama, navigate to Panorama->Managed Devices->Summary and delete the two vm-series firewalls which were already destroyed. They should now be under, *No Device Group Assigned.*
4. Commit the changes to Panorama via Commit->Commit to Panorama

Once completed, all resources in both AWS and Panorama should be removed.