



Data Center Automation with the VM-Series

Tech Note

PAN-OS 5.0

Contents

Overview 3

Process 3

Creating the Gold Standard 3

 Initial Deployment 3

 Licensing and Upgrading 4

 Initial Configuration 4

 Create the Pool 4

Automated Deployment 8

 Step 1: Convert to Virtual Machine 9

 Step 2: Assign Unique IP Address..... 9

 Step 3: Move the VM-Series to the New ESXi Host..... 10

 Step 4: Push Panorama Template 11

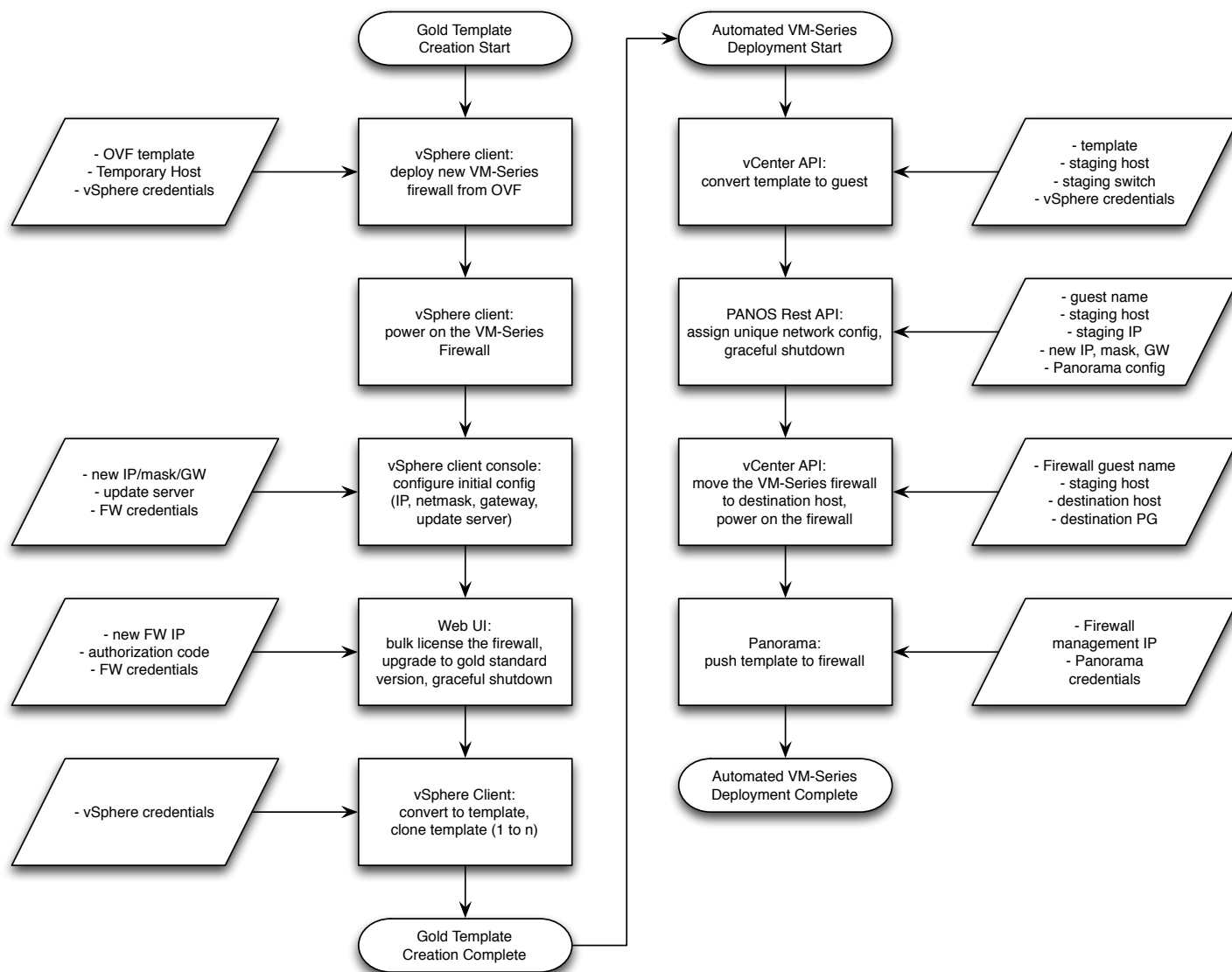
Summary 11

Overview

In a dynamic virtual data center, moves, adds, and changes happen rapidly. If the firewall could only be deployed manually, this would add an unacceptable bottleneck to data center processes. This TechNote explains how to automate the process of deploying a new VM-Series virtual firewall including a method of creating an initial “gold standard” firewall.

Process

At a high level, the process for automating VM-Series deployments requires 1) the creation of a gold standard firewall template and 2) an inventory of cloned gold standard firewalls. Once the gold standard is manually created and the inventory is created, the firewalls can be automatically deployed from the inventory. The entire process is introduced below.



Creating the Gold Standard

Initial Deployment

The first step is to deploy an initial instance of a VM-Series firewall from the downloaded OVF. This process is covered in the admin guide and the VM-Series Deployment Tech Note and won't be repeated here.

Licensing and Upgrading

After the first VM-Series instance has been deployed and the initial configuration has been committed, the VM-Series firewall will need to be licensed. The steps to license are:

1. Get the capacity Auth-Code.
2. Ensure the Device->setup->services->update server = updates.paloaltonetworks.com
3. Device->licenses->Activate feature using auth code-> enter the auth-code
4. Once the device reboots and has a serial number then apply the Support auth-code using step 3
5. Once this is done then going to device->software->check now will show the list of latest software updates

The next step is to upgrade the VM-Series to the PAN-OS version you will be standardizing on for your data center. All future automated VM-Series deployments will use this initial firewall as a template and will therefore have this version of software running.

When a new software version is adopted in the future for your data center, you will need to upgrade the templates to ensure all future automated deployments are compliant with the new standard.

Initial Configuration

At this point, the VM-Series instance should be given all configuration details that will be common to all future automated data center deployments. Examples of items to consider include:

- Administrator accounts
- Panorama/log server(s)
- DNS, NTP, update servers
- Common security policy including
 - any data center standardized zones
 - any data center wide whitelisted or blacklisted applications
- Common addresses and address groups

In some cases, it might be beneficial to include a configuration element even if it will need to be modified later. It might take less scripting and less time to modify a configuration you create manually now rather than create it completely from scratch later.

As with the software version chosen above, the template configurations will need to be updated and maintained as data center standards and policies evolve over time.

Create the Pool

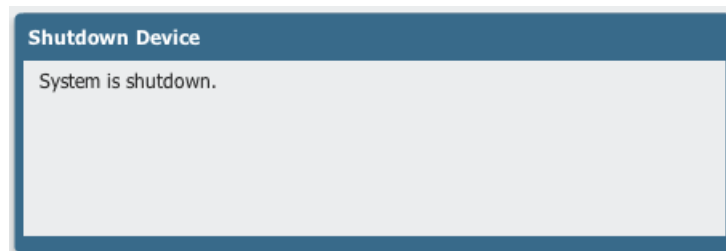
The initial VM-Series instance is now the gold standard for the data center. Its configuration should be backed up and changes should be frozen. The next step is to convert the gold standard to a vCenter Server template. This type of template can be stored on a vSphere datastore. Ideally, you should choose a datastore that is shared by the hosts that will eventually run the new VM-Series deployments. If the gold standard is stored on a datastore that is not shared by the target hosts, each automated deployment will require a copy of the virtual machine from one datastore to another greatly increasing the time to deploy (from seconds to several minutes depending on bandwidth, storage contention, etc.)

To convert the gold standard to a template you will need to first shutdown the firewall. This can be done in the CLI or Web UI as shown.

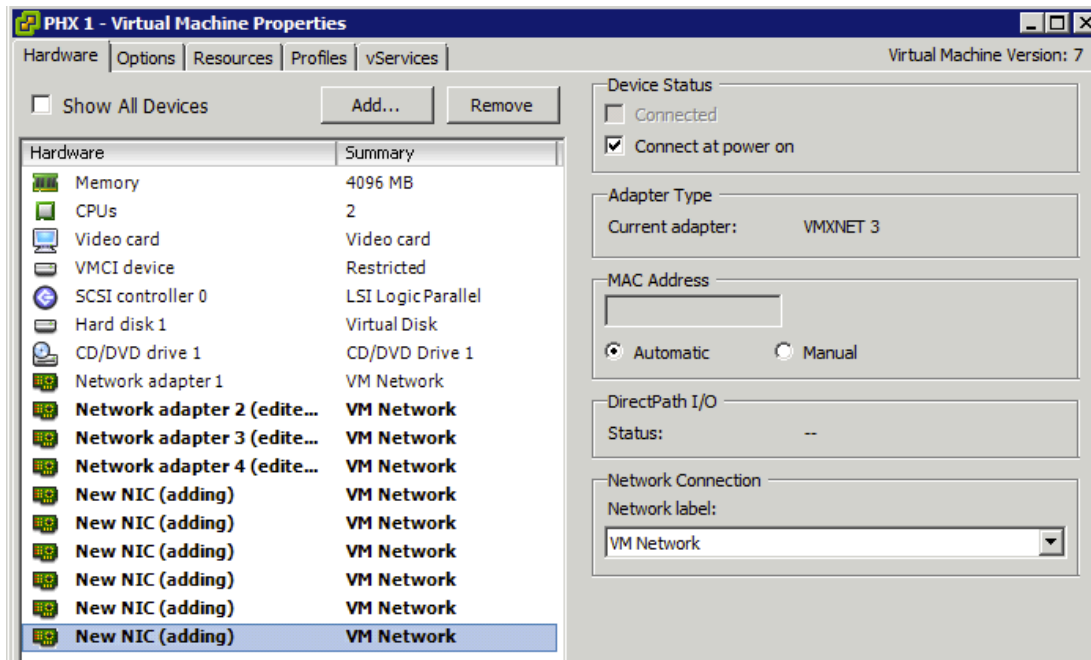
```
warby@PHX> request shutdown system
Warning: executing this command will leave the system in a shutdown state. Power must
be removed and reapplied for the system to restart. Do you want to continue? (y or n)

Broadcast message from root (pts/0) (Tue Jun 12 10:03:42 2012):

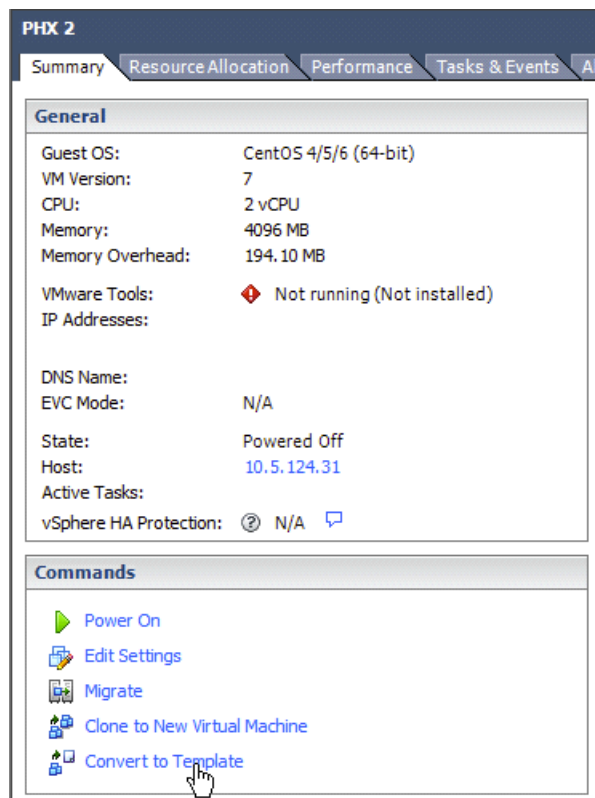
The system is going down for system halt NOW!
```






Depending on your data center and VM-Series deployment design, it might be helpful to maximize the VMNICs in vSphere at this point. Each time a new VMNIC is added to a VM-Series virtual machine, the firewall must be rebooted before the VMNIC can be used. By adding the maximum number of VMNICs (currently VMware limits this to ten total), you can eliminate the need of one or more future reboots. It may help to tie the yet unused interfaces to a virtual port group that is always available for this purpose. The downside to this strategy is the pre-allocation of virtual switch ports that may never be needed but this is a small penalty for most vSphere deployments. Make sure to choose VMXNET3 each time:

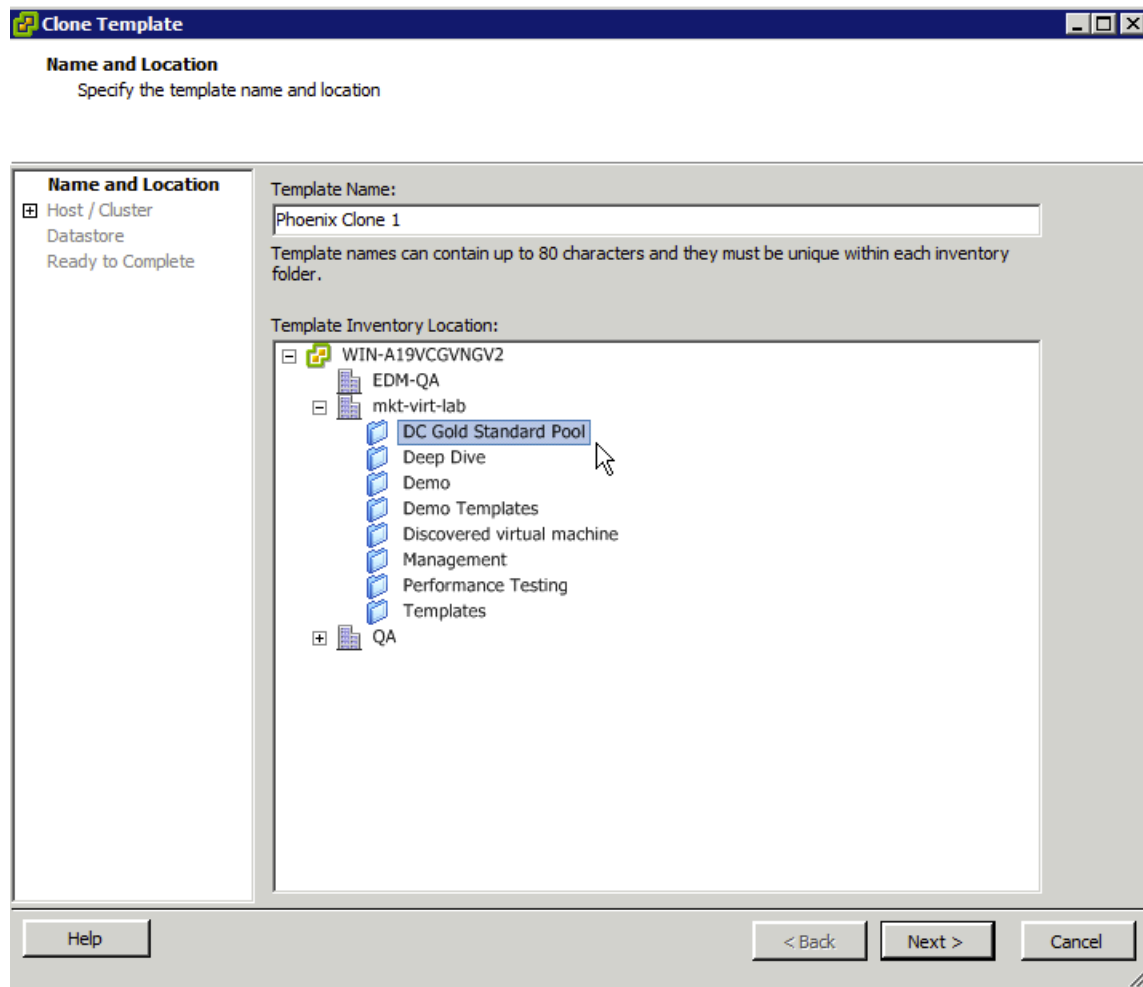


Next, use the vSphere Client to connect to vCenter Server and convert the firewall to a template:



Recent Tasks		
Name	Target	Status
 Mark virtual machine as template	 PHX 2	 Completed

Next, you will need to clone the template to populate the gold standard pool:



Select the host on the next screen (used to verify the required networks are available.)

Next, select the datastore where the template will be stored. Again, ideally this will be a datastore shared by the future target hosts.

Clone Template

Choose a Datastore for the Template
Where do you want to store the template files?

[Name and Location](#)
[Host / Cluster](#)
Datastore
Ready to Complete

Select a virtual disk format:
Same format as source

Select a destination storage for the template files:
VM Storage Profile: [Warning Icon]

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provision
vDisk1	Non-SSD	599.75 GB	352.58 GB	260.43 GB	VMFS3	Supported
vDisk2	Non-SSD	604.75 GB	383.72 GB	235.99 GB	VMFS3	Supported

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provision
------	------------	----------	-------------	------	------	----------------

Advanced >>

Compatibility:
Validation succeeded

Help < Back Next > Cancel

Review the settings and select **Finish**.

Repeat the cloning process until your template pool is full. The size of the pool will depend on several factors including where your shared datastores are located, the frequency the firewall will be deployed, the size of your data center, your license type for the VM-Series, etc.

For example, if you have one large shared datastore you might need a pool of five or ten gold standard templates. On the other hand, if you have several ESXi clusters that have separate datastores, you might be better off with multiple gold standard template pools with only two or three templates each.

Each time a gold standard template is used, it is converted from a template to a virtual machine. This can happen in less than ten seconds (the boot time will take longer than the actual deployment.) After each deployment, your script will need to kick off a background cloning process to replenish the inventory. This process will take longer (several minutes) but is not in the critical path of the automated deployment process.

Automated Deployment

Now that the gold standard template pool is fully populated, the automated processes can take over. These processes should be part of an overall Data Center Orchestration strategy that coordinates the deployment, maintenance and removal of servers, firewalls and network infrastructure (physical and virtual.)

In the One-VM-Series-per-Host data center model, each ESXi host has one VM-Series deployment with enough layer two interfaces for each VLAN (or subnet or server.) In this model, the VM-Series is only deployed during the initial setup of a new ESXi host. The automated steps to deploy a new VM-Series are as follows:

Step 1: Convert to Virtual Machine

The first step is to convert a gold standard template into a running machine. This can be done with the vSphere API. In the following example, the Perl vSphere Software Development Kit (SDK) is used. The required command line options for the Perl script are:

- Hostname or IP
- Name of the template
- Universal resource locator (URL) of the vSphere API
- Credentials
- Target pool

The following example converts the template “PHX 2” to a new virtual machine using the `vmtemplate.pl` script provided with the vSphere Perl SDK:

```
/usr/lib/vmware-vcli/apps/vm/vmtemplate.pl --host <<hostname>> --vmname 'PHX 2' --url  
https://<<vcenter-ip>>:443/sdk/vimService --username administrator --password  
<<password>> --operation VM --pool <<pool-name>>
```

After the new VM-Series firewall has been deployed, it will need to be powered on again using the vSphere Perl SDK:

```
/usr/lib/vmware-vcli/apps/vm/vmcontrol.pl --url https://<<vcenter-  
ip>>:443/sdk/vimService --host <<hostname>> --username administrator --password  
<<password>> --vmname 'PHX 2' --operation poweron
```

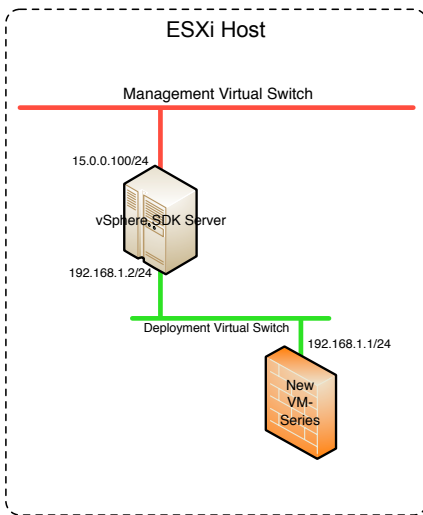
Once PAN-OS has finished loading, the new VM-Series firewall will be reachable only on its temporary IP address.

Step 2: Assign Unique IP Address

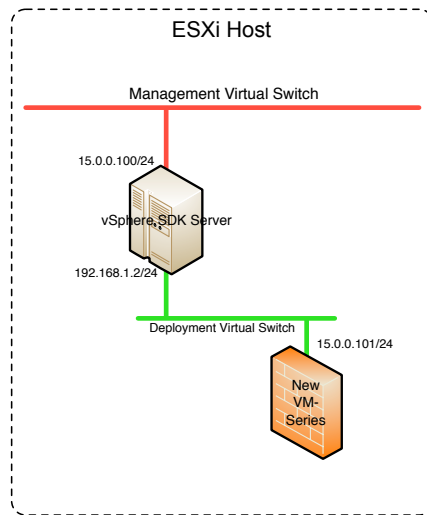
Because the firewall will always have the same initial IP address (192.168.1.1), it will need to be on a separate virtual switch with only access to the server running the vSphere SDK scripts. If the management interface is tied to a shared virtual switch, it could create a conflict (or simply be unreachable.)

Initially, the new VM-Series instance will have a non-unique IP address on a dead-end virtual switch. Next, the VM-Series firewall will be given a unique management interface IP address (and default gateway) using the PAN-OS XML API. Finally, the new VM-Series firewall can be safely moved to the shared management virtual switch using the vSphere SDK. These three steps are illustrated below.

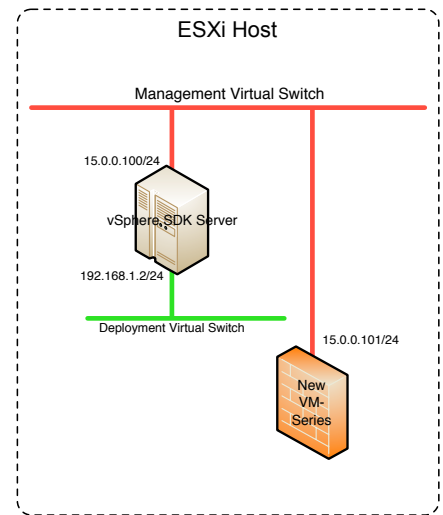
1: New VM-Series Non-Unique IP



2: New VM-Series Unique IP



3: New VM-Series Management Virtual Switch



To assign the unique IP address, the PAN-OS XML API is used. In the example below I used the PAN-Perl package:

```
/phoenix/PAN-perl-20120107/bin/panxapi -h 192.168.1.1 -K "<<API-key>>" -S
"<ip-address>15.0.0.101</ip-address>"
"/config/devices/entry[@name='localhost.localdomain']/deviceconfig/system"

/phoenix/PAN-perl-20120107/bin/panxapi -h 192.168.1.1 -K "<<API-key>>" -C
"<commit></commit>"
```

Finally, the management interface of the new VM-Series firewall needs to be moved to the management virtual switch. So we are back to the vSphere Perl SDK:

```
/usr/lib/vmware-vcli/apps/vm/updateVMPortgroup.pl --url https://<<vcenter-ip>>:443/sdk/vimService --
username administrator --password <<password>> --server <<vcenter-ip>> --vmname "PHX 2" --vnic 1 --
portgroup "Management Virtual Switch"
```

Step 3: Move the VM-Series to the New ESXi Host

In this step, the new VM-Series firewall is ready to be located on the new ESXi host. Because I used a datastore that is common to both the staging host and the destination host, no storage copying is required. I simply need to power down the firewall and do a migration to the new host and then power up. Because the VM-Series firewall cannot run VMWare Tools, hot migration (i.e. vMotion) is not an option here. But this is a new firewall that is not yet in production so vMotion is not a requirement.

First, I will shut down the firewall using the PAN-OS XML API:

```
/phoenix/PAN-perl-20120107/bin/panxapi -h 15.0.0.101 -K "<<API-key>>" -C
"<request><shutdown><system></system></shutdown></request>"
```

Next I migrated to the destination host using the vSphere Perl SDK:

```
/usr/lib/vmware-vcli/apps/vm/vmmigrate.pl --url https://<<vcenter-  
ip>>:443/sdk/vimService --username administrator --password <<password>>  
--sourcehost <<source>> --targethost <<destination>> --vmname "PHX 2"
```

Finally, I boot the VM-Series firewall one last time:

```
/usr/lib/vmware-vcli/apps/vm/vmcontrol.pl --url https://<<vcenter-  
ip>>:443/sdk/vimService --host <<newhost>> --username administrator --password  
<<password>> --vmname 'PHX 2' --operation poweron
```

Step 4: Push Panorama Template

At this point, the VM-Series firewall is up and running with a unique management IP address. How to proceed from here will vary widely depending on your requirements but a common approach might be to now use Panorama to push a template with common configuration elements. The gold standard VM-Series template should include configuration elements for Panorama. If that can't be included (perhaps because there is more than one possible Panorama to choose from) then the PAN-OS XML API can be used to configure the VM-Series firewall to use the correct Panorama server.

In addition, Panorama will need to have the serial number of the new VM-Series firewall. The serial number can be extracted from the VM-Series XML API and added to using the Panorama XML API. An alternative to Panorama would be to use the VM-Series XML API to push configuration elements as needed. This again will be heavily dependent on run time specifics and examples are not shown here.

Summary

Using a combination of the vSphere API and the PAN-OS API, most and possibly all VM-Series firewall operations can be fully integrated with data center orchestration. Operations like creating a new firewall, applying an initial configuration, applying common security policy and maintaining that policy can all be automated.

In a large, dynamic data center with a high rate of change, this automation not only improves response times for firewall changes but also reduces the chance of outages caused by firewall administrator errors.

Any data center orchestration strategy should include the VM-Series as part of the automated infrastructure and the VM-Series firewalls should be treated like any other part of the data center infrastructure.