Virtualization Features

PAN-OS® New Features Guide

Version 7.1
Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About this Guide

This guide describes how to use the new features introduced in PAN-OS 7.1. For additional information, refer to the following resources:

- For information on the additional capabilities and for instructions on configuring the features on the firewall, refer to https://docs.paloaltonetworks.com or search the documentation.
- For access to the knowledge base and community forums, refer to https://live.paloaltonetworks.com.
- For contacting support, for information on support programs, to manage your account or devices, or to open a support case, refer to https://www.paloaltonetworks.com/services/solution-assurance.
- For the most current PAN-OS and Panorama 7.1 release notes, go to https://docs.paloaltonetworks.com/pan-os/7-1/pan-os-release-notes.

To provide feedback on the documentation, please write to us at: documentation@paloaltonetworks.com.
Virtualization Features

The following are new virtualization features for the firewall and Panorama:

- Support for ELB on the VM-Series Firewalls in AWS
- Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall
- VM-Series for Microsoft Hyper-V
- Support for VMware Tools on Panorama and VM-Series on ESXi
- Support for Device Group Hierarchy in the VM-Series NSX edition firewall
- VM-Series Firewall in Microsoft Azure
- Support for Bootstrapping VM-Series Firewalls
Support for ELB on the VM-Series Firewalls in AWS

Elastic Load Balancing (ELB) is an Amazon web service that helps you improve the availability and scalability of your applications by routing traffic across multiple Elastic Compute Cloud (EC2) instances. ELB detects unhealthy EC2 instances and reroutes traffic to healthy instances until the unhealthy instances are restored. ELB can send traffic only to the primary interface of the next-hop, load-balanced EC2 instance. Therefore, to use ELB with a VM-Series firewall in AWS, the firewall must be able to use the primary interface (eth0) for dataplane traffic instead of management traffic.

- **VM-Series Firewall and Amazon ELB**
- **Use the AWS Management Console to Swap the Management Interface**
- **Configure ELB Health Checks**

**VM-Series Firewall and Amazon ELB**

Beginning with PAN-OS 7.1, you can configure the firewall to receive dataplane traffic on the primary interface in scenarios where the VM-Series firewall is behind the Amazon ELB. Before PAN-OS 7.1, the VM-Series firewall could not integrate with ELB because ELB could forward traffic only to the primary (eth0) elastic network interface (ENI) of an EC2 instance. You now have the ability to enable the primary interface on the VM-Series firewall to function as a dataplane interface, instead of functioning as the management interface, so that ELB can forward traffic to the firewall.

You cannot configure the firewall to send and receive dataplane traffic on eth0 when the firewall is in front of ELB. The VM-Series firewall must be placed behind the Amazon ELB to leverage this capability.

[If you want to deploy a load balancer sandwich topology, you must use the CFT, see Auto Scale VM-Series Firewalls with the Amazon ELB.]

To learn about specific scenarios and about how to use management interface mapping changes for use with Amazon ELB, see [VM-Series Firewall in AWS](#).

**Use the AWS Management Console to Swap the Management Interface**

Use these instructions when you are launching the firewall to perform a swap so that Elastic Network Interface (ENI) eth0 maps to ethernet1/1 and ENI eth1 maps to the MGT interface on the firewall.

### Management Interface Swap on the VM-Series Firewall Using the AWS Management Console

<table>
<thead>
<tr>
<th>Step 1</th>
<th>On the EC2 Dashboard, click <strong>Launch Instance</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the VM-Series Amazon Machine Image (AMI). To get the AMI, see <strong>Obtain the AMI</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose the <strong>EC2 instance type</strong> for allocating the resources required for the firewall and click <strong>Next</strong>. See <strong>EC2 instance types</strong> for a list of supported types.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the Amazon Virtual Private Cloud (VPC) and the subnet to which the VM-Series management interface will attach.</td>
</tr>
</tbody>
</table>
Virtualization Features

Management Interface Swap on the VM-Series Firewall Using the AWS Management Console (Continued)

Step 5 Select Launch as an EBS-optimized instance to leverage Amazon Elastic Block Store (EBS) benefits.

Step 6 Expand the Network Interfaces section and click Add Device to add another network interface. Swapping interfaces requires a minimum of two ENIs (eth0 and eth1). Make sure that your VPC has more than one subnet so that you can add additional ENIs at launch.

If you launch the firewall with only one ENI, the interface swap command will cause the firewall to boot into maintenance mode.

Step 7 Expand the Advanced Details section and set User data to mgmt-interface-swap=enable As text to perform the interface swap during launch.

Step 8 Accept the default Storage settings.

Step 9 Add one or more tags to create your own metadata to identify the VM-Series firewall. For example, add a Name tag with a Value that helps you remember that the ENI interfaces have been swapped on this VM-Series firewall.

Step 10 Select an existing Security Group or create a new one. This security group is for restricting access to the management interface of the firewall. At a minimum, consider enabling HTTPS and SSH access for the management interface (eth1).

Step 11 If prompted, select an appropriate SSD option for your setup.

Step 12 Select Review and Launch to ensure your selections are accurate and then click Launch. Select an existing key pair or create a new one and acknowledge the key disclaimer.

Step 13 Download and save the private key to a safe location; the file extension is .pem.

You cannot regenerate this key if lost.
Management Interface Swap on the VM-Series Firewall Using the AWS Management Console (Continued)

Step 14 View the progress of the installation on the EC2 Dashboard. It can take five minutes or longer to launch the VM-Series firewall. When the process is complete, the VM-Series firewall will display on the Instances page of the EC2 Dashboard.

Step 15 Assign an EIP to eth1 and then use the EIP address to open an SSH session to the CLI of the VM-Series firewall and configure the administrative password.

Step 16 Verify that the interfaces have been swapped. Use the following command to verify:

```
debg show vm-series interfaces all
```

<table>
<thead>
<tr>
<th>Phoenix_interface</th>
<th>Base-OS_port</th>
<th>Base-OS_MAC</th>
<th>PCI-ID</th>
<th>Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgt(interface-swap)</td>
<td>eth0</td>
<td>0e:53:96:91:ef:29</td>
<td>0000:00:04.0</td>
<td>ixgbevf</td>
</tr>
<tr>
<td>Ethernet1/1</td>
<td>eth1</td>
<td>0e:4d:84:5f:7f:4d</td>
<td>0000:00:03.0</td>
<td>ixgbevf</td>
</tr>
</tbody>
</table>

If you want to swap the management interface on a VM-Series firewall that you have already deployed, use the VM-Series Firewall CLI.

Configure ELB Health Checks

ELB periodically checks the health of the EC2 instance using pings or by sending requests to test the availability of the firewall. On the Amazon EC2 console, configure the health check to use port 80 or 443 of the web server behind the firewall. This allows you to compute the health using the total path of the HTTP request and includes routing on the firewall, NAT, and availability of the web server itself. For instructions on configuring health checks, refer to the AWS documentation.
Virtualization Features

Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall

Beginning with PAN-OS 7.1, the VM-Series NSX edition firewall includes support for multi-tenancy, which means that you can use the VM-Series firewall to secure traffic from multiple tenants (or sub-tenants) hosted in the vSphere environment. The VM-Series NSX edition firewall allows you to create up to 32 service definitions, each with a unique device group and template. The device group allows you to create and manage policy rules for a tenant (or sub-tenant) and the template allows you to define one or more zones so that you can isolate traffic for each tenant or sub-tenant. Each tenant (or sub-tenant) is mapped to a specific zone on Panorama, and the zone becomes available as a service profile on the NSX Manager; the NSX security administrator can select the appropriate service profile to logically isolate traffic and redirect it to the VM-Series firewall.

In previous releases, the VM-Series NSX edition firewalls were all assigned to one service definition with a single template (with one default zone and, hence, a single service profile for redirecting traffic) and a single device group (one set of security policies). With the support for multiple service definitions in PAN-OS 7.1, whether you have a shared compute infrastructure and need shared security policies, or you have a dedicated compute infrastructure and need dedicated security policies, or you have shared compute infrastructure and need dedicated security policies (multiple instances of the VM-Series firewall per host in an ESXi cluster), you can configure the firewall for your needs.

For details on multi-tenant deployment options, see What is Multi-Tenant Support on the VM-Series NSX Edition Firewall?

<table>
<thead>
<tr>
<th>High-Level Workflow for Deploying the VM-Series NSX Edition Firewall for Multi-Tenancy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Register the VM-Series firewall as a service on the NSX Manager.</strong></td>
</tr>
<tr>
<td>To enable communication between the NSX Manager and Panorama and to deploy the firewall as a service on the NSX Manager, you must provide the IP address or hostname along with the credentials of the NSX Manager on the VMware service manager configuration on Panorama. The registration also allows the NSX Manager to update Panorama with dynamic changes to the software-defined data center (SDDC).</td>
</tr>
</tbody>
</table>

| **On the NSX Manager, use the NSX service composer to create security groups.** The NSX security group allows you to define which objects—DVS port-group, logical switch (VXLAN), or virtual machines—are included or excluded from the group. When you create a security group in NSX, the information is transmitted to Panorama. On Panorama, the security administrator can then use NSX security groups as match criteria or tags within dynamic address groups and then use dynamic address groups in security policy rules and push the rules to the VM-Series firewalls. |

| **On Panorama, create the building blocks for redirecting traffic to the VM-Series firewall for policy enforcement.** |
| • Create the **template(s) and device group(s).** On each template, create one or more zones (NSX service profile zone) for each tenant or sub-tenant from which you want to redirect traffic to the firewall. The firewall automatically creates a pair of virtual wire subinterfaces for each zone. |
| • Create dynamic address groups and use them in security policy rules. You can now use an NSX service profile zone name as the source and destination zone (must be the same zone) in a security policy rule. Using dynamic address groups in policy allows you to secure virtual machines as they are dynamically added or removed from your vSphere environment. |

| **Create the service definition(s) on Panorama.** |
| The service definition includes the template and device group to which a VM-Series firewall belongs. When the firewall connects to Panorama, it receives its configuration settings, including the zone(s) for each tenant or department that the firewall will secure and its policy settings from the device group specified in the service definition. |
Virtualization Features

High-Level Workflow for Deploying the VM-Series NSX Edition Firewall for Multi-Tenancy (Continued)

- On the NSX Manager, create security policies to granularly define which traffic flows to redirect to the VM-Series firewall for inspection and enforcement. NSX security policies allow you to assign security services, such as the VM-Series firewall for network introspection of traffic, for the objects that belong to NSX security groups. After you deploy the firewalls, the traffic redirection rules allow you to steer traffic to the appropriate Service Profile. The NSX Manager receives these Service Profile(s) from Panorama and each profile maps to the NSX service profile zone you created in the Panorama template. Make sure to select the correct service and profile when defining NSX security policies. To create policies, see Create Policies.
  Traffic allowed by the VM-Series firewall is then returned to the NSX virtual switch for delivery to the final destination (guest virtual machine or physical device).

- Deploy the VM-Series firewalls. For instructions, see Deploy the VM-Series Firewalls.
  On the NSX Manager, make sure to select the appropriately defined service to ensure that you properly secure the ESXi cluster.
VM-Series for Microsoft Hyper-V

The VM-Series firewall can now be deployed on Hyper-V Server 2012 R2 (standalone edition) and on Windows Server 2012 R2 (standard and datacenter editions) with the Hyper-V role that lets you create and manage virtual machines. You can deploy the firewall using the Hyper-V Manager (guided user interface) or Windows PowerShell (command line interface).

The VM-Series firewall on Hyper-V supports the following:

- Tap, virtual wire, Layer 2, and Layer 3 interface deployments. See Supported Deployments on Hyper-V.
- All capacity model licenses—VM-100, VM-200, VM-300, and VM-1000-HV.
- Active/active and active/passive high availability (HA) configurations.

The VM-Series firewall on Hyper-V is bundled with the Linux Integration Services package to improve integration between the host and the virtual machine. This bundle allows you to:

- Use the Hyper-V Manager to view the IP address assigned to the management interface on the firewall.
- Synchronize time and heartbeat between the host and the firewall to ensure that the firewall is operating properly.
- Gracefully shutdown the firewall from the Hyper-V Manager.
Support for VMware Tools on Panorama and VM-Series on ESXi

VMware Tools is now supported on the VM-Series firewall and Panorama virtual machine deployed on VMware ESXi. The tool is bundled with the software image and is automatically enabled when you launch the VM-Series firewall and the Panorama virtual machine. Because VMware Tools is bundled with the software image for the firewall and Panorama, any updates will be made available with a new OVF image; you cannot upgrade VMware Tools using the vCenter server.

VMware Tools gives you the following capabilities for managing the VM-Series firewall and Panorama from the VMware infrastructure:

- Displays the IP address of the management interface and the PAN-OS version running on the firewall or Panorama.
- Provides resource utilization metrics on the hard disk, memory, and CPU. You can use these metrics to enable alarms or actions on the vCenter server.
- Graceful shutdown and restart of the firewall and Panorama using the power off function in vCenter.
- Enables a heartbeat mechanism between the vCenter server and the firewall or Panorama to verify whether it is functioning or rebooting. If the firewall goes into maintenance mode, heartbeats are disabled so that the vCenter server does not shut down the firewall. Disabling heartbeats allows the firewall to stay operational in maintenance mode when it cannot send heartbeats to the vCenter server.

The current version of the implementation uses Open VMware Tools version 9.4.6.
Virtualization Features

Support for Device Group Hierarchy in the VM-Series NSX edition firewall

When deploying the VM-Series NSX edition firewall, you can now use a template stack and a device group hierarchy in the VMware Service Manager configuration on Panorama. Both template stacks and device group hierarchy (introduced in PAN-OS 7.0) allow you to organize devices based on some common criteria in order to minimize redundant configuration.

- A template stack allows you to push all the necessary settings to the set of firewalls assigned to a stack without the redundancy of adding every setting to every template.
- A device group hierarchy allows you to nest device groups in a tree hierarchy of up to four levels, with lower-level groups inheriting the settings (policy rules and objects) from higher-level groups.

To create context awareness between the virtual and security environments for Dynamic Address Groups referenced in policy, you can also select one or more device groups in a hierarchy for notification when virtual machines are provisioned or removed from the network. The firewalls use this update to determine the most current list of members that constitute Dynamic Address Groups referenced in policy.

For configuration details, see Create Template(s) and Device Group(s) on Panorama. For additional new features on the VM-Series NSX edition firewall, see Support for Multi-Tenancy and Multiple Sets of Policy Rules on the VM-Series NSX Edition Firewall.
VM-Series Firewall in Microsoft Azure

Microsoft Azure allows you to deploy a virtual network in the cloud so that you can deploy a private cloud solution or you can extend the on-premises IT infrastructure to create a hybrid or cross-premises solution. The VM-Series firewall in Azure must be deployed in a virtual network (VNet) using the Azure Resource Manager (ARM) deployment mode only; the classic mode (Service Management-based deployments) is not supported. The VM-Series firewall in Azure must be of the Standard tier and any of the following types—A4, D3, D3_v2, D4 and D4_v2—that meet the minimum system requirements. Because the Azure VNet is a Layer 3 network, the VM-Series firewall in Azure supports only Layer 3 interfaces. The VM-Series firewall in Azure supports the Bring Your Own License (BYOL) model and the usage-based licensing (PAYG) model.

The VM-Series firewall (PAN-OS 7.1.1) is available on Azure Government, and the Azure Government Marketplace offers the BYOL option only. To deploy the VM-Series firewall on Azure Government, you will follow the same steps for BYOL deployments that are outlined in the documentation.

You can deploy a VM-Series firewall in Azure to function as a VNet gateway that secures traffic destined to the servers in the VNet, as a VPN termination point to securely extend your physical data center to the Azure private cloud into Azure, or to set up an IPSec tunnel for traffic between two Azure VNets. You can also deploy the VM-Series firewall to function as a GlobalProtect gateway and portal to safely enable your mobile users with consistent security policy when they are not on the corporate network.

To deploy the VM-Series firewall, Palo Alto Networks provides an solution template in the Azure Marketplace and a customizable ARM template in the Palo Alto Networks GitHub repository. The ARM template includes two JSON files (a Template File and a Parameters File) to help you deploy the firewall. For more information, see the VM-Series Deployment Guide.

The VM-Series firewall in Azure does not support native VM Monitoring capabilities for virtual machines that are hosted in Azure. VM-Series high availability configuration is not supported either; use the integration with Azure Gateway and Load balancer to address availability requirements for web facing applications.
Virtualization Features

Support for Bootstrapping VM-Series Firewalls

See Bootstrapping Firewalls for Rapid Deployment.