Deployment Guide - Palo Alto Networks VM-Series Firewall

EDM09-141 - Version 2

Website

www.endace.com

Disclaimer

This document is provided on an "AS IS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND" basis, including (without limitation) any warranties or conditions as to accuracy, non-infringement, merchantability or fitness or a particular purpose. The documentation is subject to change without notice.

In no event shall Endace Technology Limited be liable for damages, losses (direct or indirect) or costs incurred as a result of the use of this documentation or any inaccuracies or errors contained in the documentation, and use of the documentation is at your own risk.

This document, or any part thereof, may not be copied, modified or distributed without the express written authorization of Endace Technology Limited and may be used only in connection with Endace Technology Limited products and services.

endace

Contents

Introduction 1

Platform Requirements 1
Security Considerations 1
Related Documents 1

Deploying a Single VM-Series Firewall 2

Overview 2
Transferring Image Files to the Host EndaceProbe 3
Host Network Bridge 3
  Configuring Network Bridging 3
Installing the Virtual Machine 4
Allocating CPU to the Virtual Machine 5
Configuring vDAGs 5
Sending Data to the Virtual Machine 6
Saving the Host Configuration 6
Powering on the Virtual Machine 6
Determining the Virtual Machine's IP Address (DHCP Only) 6
Deployment Complete 6

Deploying on High Capacity VM-Series Firewalls 7

Determine the Required Virtual Machine Size and Resources 8
  Platform Limitations 8
  Application Dock Sizes 8
Installing the Virtual Machine 9
Allocating CPU to the Virtual Machine 9
Assign and Configure Additional vDAGs 11
  Configuring vDAGs 11
Sending Data to the Virtual Machine - Multiple vDAGs 12
Distributing Data to Multiple vDAGs 12
Powering on the Virtual Machine 12
Saving the Host Configuration 12
Determining the Virtual Machine's IP Address 13
Deployment Complete 13

Additional Information 14

Controlling Virtual Machines 14
  Starting and Stopping Virtual Machines 14
  Set Virtual Machine Power State 14
  Removing a Virtual Machine 15
  Monitoring a Virtual Machine 16

Version History 17

Introduction

This document describes how to deploy and configure a Palo Alto Networks VM-Series Firewall for KVM in an Application Dock on the EndaceProbe. Every packet recorded by the EndaceProbe can be streamed to VM-Series Firewalls in real-time.

And, by hosting VM-Series Firewall in an Application Dock, security teams can extend their reach without truck rolls, leveraging the same hardware deployments for security monitoring and network recording.

Important:
The procedures described this guide can only be used on Host EndaceProbe running OSm software 6.4.x or greater.

Platform Requirements

The Palo Alto Networks VM-Series Firewall can be deployed as a virtual machine on any EndaceProbe platforms that supports a Single Application Dock instance. It cannot be deployed on an EndaceCMS.

Security Considerations

The Palo Alto Networks VM-Series Firewall comes with a default user and a default password. As these have documented, well known, passwords they should be changed. In the process of changing this, it is important to ensure that the deployed virtual machine follows your organization's security/hardening policies.

The Palo Alto Networks VM-Series Firewall has the following default accounts:

User name	admin
Password	admin

Related Documents

The following documents are referenced in this document. They provide additional information about how to configure EndaceProbe hosts.

- *EDM09-108 EndaceProbe User Guide - 112/124/404/4000/4100/9000/9200 Platforms*
- *EDM09-10 EndaceProbe User Guide - 3000/7000 Platforms*
- *EDM09-21 CLI Command Reference*

Deploying a Single VM-Series Firewall

Overview

This section details how to deploy and configure a Palo Alto Networks VM-Series Firewall in a virtual machine on an EndaceProbe.
This deployment:

- Installs a Palo Alto Networks VM-Series Firewall for KVM,
- uses a *VM-50 PAN-OS* license,
- is installed in a *Single* sized Application Dock,
- uses a single vDAG.

To deploy and configure a virtual machine with another PAN-OS license, a larger virtual machine will be required. For details, see Deploying on High Capacity VM-Series Firewalls (page 7).

The following is an overview of the steps required to deploy a VM-Series Firewall on an EndaceProbe:

1. Transfer the image file to the host EndaceProbe.
   See Transferring Image Files to the Host EndaceProbe (page 2).
2. Check / Configure a host network bridge.
   See Host Network Bridge (page 3).
3. Install the VM-Series Firewall.
   See Installing the Virtual Machine (page 4).
4. Allocate CPU to the virtual machine.
   See Allocating CPU to the Virtual Machine (page 5).
5. Configure the vDAGs.
   See Configuring vDAGs (page 5)
6. Send captured data to the Palo Alto Networks virtual machine.
   See Sending Captured Data to the Virtual Machine (page 5)
7. Save the host EndaceProbe configuration.
   See Saving the Host Configuration (page 6)
8. Power on the Palo Alto Networks VM-Series Firewall virtual machine.
   See Powering on the Virtual Machine (page 6)
9. Determine the IP Address.
   See Determining the Virtual Machine's IP Address (page 6)

Congratulations - the deployment is complete!

Additional Useful Information

- Controlling Virtual Machines (page 14)
- Set Virtual Machine Power State (page 14)
- Deploying on High Capacity VM-Series Firewalls (page 7)

Transferring Image Files to the Host EndaceProbe

The file can be transferred to the EndaceProbe using the EndaceProbe CLI using FTP, SFTP, TFTP, SCP, HTTP or HTTPS, or it can be pushed to the EndaceProbe using a SCP client.

To **pull** the image file onto the EndaceProbe:

1. Copy the image file to a suitable location on the file server.

   The file server must:

   - Be accessible to either EndaceProbe.
   - Support TLS 1.2.
   - Provide a connection using any or all of FTP, SFTP, TFTP, SCP, HTTP or HTTPS.
2. Using the host EndaceProbe CLI, transfer the image to the host EndaceProbe by running either:

   ```
   virt volume fetch url http://<host probe name>:<port>/<path>/<file name>
   ```

   or

   ```
   virt volume fetch url scp://<user name>[:password]@<host probe name>/<path>/<file name>
   ```

Alternatively, use

- SCP from a remote system to **push** the image file onto the EndaceProbe:

  ```
  scp <file name> <user name>@<host probe name>:/endace/vm/pools/default
  ```

Host Network Bridge

A network bridge on the host EndaceProbe enables all locally installed virtual machines to be visible on the management network.

EndaceProbe hosts that have been upgraded from an earlier version of OSm may not have a configured network bridge as the previous network interface configuration is retained and remains functional.

If a virtual machine is not installed, absence of the network bridge does not affect the operation of the EndaceProbe hosts themselves.

To check if a bridge is configured on the EndaceProbe host, run the following in *enable* mode:

```
show bridges
```

Configuring Network Bridging

To create a network bridge on the Host EndaceProbe, complete the following steps:

1. Log into the host EndaceProbe CLI - *configure terminal* mode.
2. Type in the following command:

   ```
   bridge br0 migrate-from <eth port>
   ```

   where `<eth port>` is the Ethernet port you want to bind to the Bridge - typically **eth0**.

   For further details on this command, refer to the *Network Bridging* section in *EDM09-21 CLI Command Reference*.

Once the bridge migration is complete, the Setup > Interface page displays the new configuration. **br0** replaces **eth0** as the default network interface.

The network bridge binds **br0** to **eth0** and means **br0** has the same HW addr (MAC address) as **eth0**.

Installing the Virtual Machine

The following details how to deploy and configure a virtual machine with a *VM-50 PAN-OS* license in a *Single* sized virtual machine.

Important:
To deploy and configure a higher capacity Palo Alto Networks VM-Series Firewall a Double or Quad sized Application Dock is required. This changes the deployment steps. To deploy a higher capacity VM-Series Firewall, go to *Deploying on High Capacity VM-Series Firewalls (page 7)* *and complete the deployment using the listed steps.*

To install the virtual machine on an EndaceProbe, complete the following steps:

1. Log into the host EndaceProbe CLI - *configure terminal* mode.
2. Install the virtual machine , run:

   ```
   virt vm <virtual machine name> quick-deploy size single copy-from <file name>
   ```

   Where:

<virtual machine name>	The name of the virtual machine you are creating.
<file name>	The name of the image file to install in the virtual machine. Tip: Start typing the file name and press tab to complete the name.

   This installation can take 15 to 30 minutes to complete. The time taken depends on the image file and the available resources on the host EndaceProbe. During the installation, the virtual drive is created then the image file is installed.
3. Verify the virtual machine is now listed as a virtual machine.

   ```
   show virt vm <virtual machine name>
   ```

Allocating CPU to the Virtual Machine

On the Host EndaceProbe, multiple CPUs are allocated to specific virtual machines by pinning vCPUs to that virtual machine. This ensures CPUs are solely available for use by a specific virtual machine.

Note:

- *These steps must be completed before the virtual machine is started.*
- *The affinity settings on your EndaceProbe must be as defined in the* EDM07-19 Endace Performance and Application Dock Resource Guidelines.

1. On the host EndaceProbe, pin the CPUs to the virtual machine using the following CLI commands. The CPU must be pinned in pairs and in order.

   ```
   virt vm <virtual machine name> vcpus vcpu <vcpu number> pin <cpu number>
   ```

   The following CPU pinning commands **apply only** to 4000 and 9000 platforms where this is the **first virtual machine** installed. For CPU pinning details for other platforms, contact Endace Support.

   ```
   virt vm <virtual machine name> vcpus vcpu 0 pin 2
   virt vm <virtual machine name> vcpus vcpu 1 pin 22
   virt vm <virtual machine name> vcpus vcpu 2 pin 3
   virt vm <virtual machine name> vcpus vcpu 3 pin 23
   ```

Additional Single Application Dock Instances- 4000 and 9000 EndaceProbe Platforms

If there are previously installed virtual machines on the EndaceProbe, the CPU pinning requirements are as follows. In there is an existing Double-sized Application Dock, use the third Single Application Dock CPU pinning below. For further details, contact Endace Support.

First Single Application Dock		Second Single Application Dock		Third Single Application Dock		Fourth Single Application Dock	
vCPU Number	CPU Number	vCPU Number	CPU Number	vCPU Number	CPU Number	vCPU Number	CPU Number
0	2	0	4	0	6	0	8
1	22	1	24	1	26	1	28
2	3	2	5	2	7	2	9
3	23	3	25	3	27	3	29

Configuring vDAGs

vDAGs are virtual interfaces the virtual machine uses for receiving data from the monitored network.
The host EndaceProbe captures the data and passes it to the virtual machine via one or more configured vDAG.

Each vDAG must be configured to the correct NIC mode for the PAN-OS.

If additional vDAGs are required, see Assign and Configure Additional vDAGs (page 11).

1. Identify the vDAG assigned to this virtual machine.

   ```
   show virt vdag
   ```

2. For each vDAG assigned to the Palo Alto Networks virtual machine set the NIC mode to **virtio** using the follow two CLI commands.

   ```
   virt vdag <vdag number> nic-mode enable
   virt vdag <vdag number> nic model virtio
   ```

Sending Data to the Virtual Machine

The traffic captured by the EndaceProbe needs to be sent to the Palo Alto Networks VM-Series Firewall so it can be processed. This requires the creation of a Data Pipe on the host EndaceProbe. For details on creating a Data Pipe, refer to the *Data Pipe* chapter in your *EndaceProbe User Guide*.

1. Using the GUI, create and start a Data Pipe with the:
   - input as the DAG module and port receiving traffic, and
   - output as the vDAG configured to feed the virtual machine.

Saving the Host Configuration

Once the virtual machine is correctly configured, the details must be saved on the Host EndaceProbe. This ensures the configuration persists after a reboot of the host EndaceProbe.

1. On the host EndaceProbe, save the running configuration.
   ```
   configuration write
   ```

Note:
*This can also be done on the GUI by clicking the **Save** option on the top right corner below the menu bar.*

Powering on the Virtual Machine

To power on the virtual machine, complete the following steps:

1. Power on the virtual machine:
   ```
   virt vm <virtual machine name> power on
   ```

Determining the Virtual Machine's IP Address (DHCP Only)

To determine the assigned IP address for the virtual machine, complete the following steps:

1. In the Host EndaceProbe CLI, use the text console to connect to the virtual machine:
   ```
   virt vm <virtual machine name> console connect text
   ```
   Where `<virtual machine name>` is the name you previously assigned.
   A command line opens and reports the following:
   ```
   Connected to console /dev/pts/1
   Escape character is: 'Ctrl ^'
   ```
2. Press **Enter**.
   The virtual machine completes its start-up process and displays information on the screen.
   One the virtual machine has booted, the IP address of the virtual machine displays.
3. Exit the text console and return to the host EndaceProbe CLI:
   ```
   Ctrl ^
   ```

1. In a separate session, login in to the virtual machine using its IP address, default user and password.
   See Security Considerations (page 1).
2. Review the network configuration as per the PAN-OS instructions.
   For further details refer to the Palo Alto Networks PAN-OS technical documentation.

Deployment Complete

Congratulations you have completed the deployment and configuration of the Palo Alto Networks VM-Series Firewall. You can now log and use the VM-Series Firewall.

Deploying on High Capacity VM-Series Firewalls

To deploy and configure a higher capacity Palo Alto Networks VM-Series Firewall a Double or Quad sized Application Dock is required.

This adds extra installation steps - these extra steps are included below and are identified with "*".

This deployment:

- installs a Palo Alto Networks VM-Series Firewall for KVM
- uses a *VM-100 PAN-OS* or greater license
- is installed in a *Double* or *Quad* sized Application Dock
- uses multiple vDAG.

The following is an overview of the steps required to deploy a Palo Alto Networks VM-Series Firewall on an EndaceProbe:

1. Transfer the image file to the host EndaceProbe.
   See *previous* step - Transferring Image Files to the Host EndaceProbe (page 2).
2. * Determine the required PAN-OS license and required Application Dock installation size.
   Extra step - See Determine the Required Virtual Machine Size and Resources (page 8).
3. Install the Palo Alto Networks VM-Series Firewall.
   See Installing the Virtual Machine (page 8).
4. Allocate CPU to the virtual machine.
   See Allocating CPU to the Virtual Machine (page 9).
5. * Assigning and configure additional vDAGs virtual machine.
   Extra step - See Assign and Configure Additional vDAGs (page 11).
6. * Distribute the data to the multiple vDAGs.
   Extra step - See Distributing Data to Multiple vDAG (page 12).
7. * Send data to the virtual machine via multiple vDAGs
   Extra step - See Sending Data to the Virtual Machine - Multiple vDAGs (page 12).
8. Save the host EndaceProbe configuration.
   See Saving the Host Configuration (page 12).
9. Power on the Palo Alto Networks VM-Series Firewall virtual machine.
   See Powering on the Virtual Machine (page 12).
10. Determine the IP Address.
    See Determining the Virtual Machine's IP Address (page 13).

Congratulations - the deployment is complete!

Additional Useful Information

- Controlling Virtual Machines (page 14)
- Set Virtual Machine Power State (page 14)
- Deploying on High Capacity VM-Series Firewalls (page 7)

Determine the Required Virtual Machine Size and Resources

The amount of data to be processed by the virtual machine determines what PAN-OS license is required. The license then determines the required Dock size. The amount of data to be processed also determines the number of streams of data (vDAGs) required into the virtual machine.

For more information on vDAGs, see Assigning vDAGs to the Virtual Machine (page 11).

PAN-OS License	Dock Size
VM-50	Single
VM-100 / VM-200	Single or Double
VM-300	Double
VM-500	Quad

*Refer to Palo Alto Networks product selection for complete performance metrics.

Note:
The Nominal Performance metrics are published by Palo Alto Networks (refer to the Palo Alto Networks website for further details). The details are reprinted here for convenience - they do not represent a performance guarantee by Endace.

Platform Limitations

Each model of Host EndaceProbe has different amounts of RAM and CPU cores. These differences affect the way virtual machines can be deployed. Considerations must be given to the following when planning how many virtual machines are installed:

- The maximum number of capturing RotationFiles on an appliance.
- The number of allowed interactive concurrent users.
- The number of instances of virtual machine deployed on a host.

For further information, refer to the applicable version of host *OSm Release Notes*.

CPU Affinity

Host EndaceProbe have specific CPU cores allocated to virtual machines. These differ depending on the Host EndaceProbe model. To learn how CPU cores are allocated, refer to the *OSm Release Notes*.

Sizing Recommendations

Each EndaceProbe platform has recommendations for the size of virtual machine and the number of input vDAGs. See the following table for details.

Dock Size	Maximum Number of vDAGs
Single	3
Double	6
Quad	8

Application Dock Sizes

To simplify deployment of virtual machine, there are three Application Dock sizes. These sizes enables virtual machines to be quickly and easily created with pre-defined resources.

- The *Application Dock size* determines the amount of RAM and number of CPU.
- The *image file* determines the size of the created volume size.

Quick-deploy option	RAM (GB)	Number of CPU cores
Single	12	2
Double	24	4
Quad	48	8

Installing the Virtual Machine

To install a higher capacity virtual machine on an EndaceProbe, complete the following steps:

1. Log into the host EndaceProbe CLI - *configure terminal* mode.
2. Install the virtual machine , run:

```
virt vm <virtual machine name> quick-deploy size <size> copy-from <file name>
```

Where:

<size>	The selected Application Dock size. The options are • Single • Double • Quad

Allocating CPU to the Virtual Machine

On the Host EndaceProbe, multiple CPUs are allocated to specific virtual machines by pinning vCPUs to that virtual machine. This ensures CPUs are solely available for use by a specific virtual machine.

Note:

- *These steps must be completed before the virtual machine is started.*
- *The affinity settings on your EndaceProbe must be as defined in the* EDM07-19 Endace Performance and Application Dock Resource Guidelines.

1. On the host EndaceProbe, pin the CPUs to the virtual machine using the following CLI commands. The CPU must be pinned in pairs and in order.

```
virt vm <virtual machine name> vcpus vcpu <vcpu number> pin <cpu number>
```

The following CPU pinning commands **apply only** to 4000 and 9000 platforms where this is the **first virtual machine** installed. For CPU pinning details for other platforms, contact Endace Support.

```
virt vm <virtual machine name> vcpus vcpu 0 pin 2
virt vm <virtual machine name> vcpus vcpu 1 pin 22
virt vm <virtual machine name> vcpus vcpu 2 pin 3
virt vm <virtual machine name> vcpus vcpu 3 pin 23
```

To pin eight CPUs to a *Double* dock:

Four from above plus

```
virt vm <virtual machine name> vcpus vcpu 4 pin 4
virt vm <virtual machine name> vcpus vcpu 5 pin 24
virt vm <virtual machine name> vcpus vcpu 6 pin 5
virt vm <virtual machine name> vcpus vcpu 7 pin 25
```

To pin 16 CPUs to a *Quad* dock:

Eight CPU from above plus

```
virt vm <virtual machine name> vcpus vcpu 8 pin 6
virt vm <virtual machine name> vcpus vcpu 9 pin 26
virt vm <virtual machine name> vcpus vcpu 10 pin 7
virt vm <virtual machine name> vcpus vcpu 11 pin 27
virt vm <virtual machine name> vcpus vcpu 12 pin 8
virt vm <virtual machine name> vcpus vcpu 13 pin 28
virt vm <virtual machine name> vcpus vcpu 14 pin 9
virt vm <virtual machine name> vcpus vcpu 15 pin 29
```

Additional Single Application Dock Instances- 4000 and 9000 EndaceProbe Platforms

If there are previously installed virtual machines on the EndaceProbe, the CPU pinning requirements are as follows. In there is an existing Double-sized Application Dock, use the third Single Application Dock CPU pinning below. For further details, contact Endace Support.

First Single Application Dock		Second Single Application Dock		Third Single Application Dock		Fourth Single Application Dock	
vCPU Number	CPU Number	vCPU Number	CPU Number	vCPU Number	CPU Number	vCPU Number	CPU Number
0	2	0	4	0	6	0	8
1	22	1	24	1	26	1	28
2	3	2	5	2	7	2	9
3	23	3	25	3	27	3	29

Two Double Application Docks - 4000 and 9000 EndaceProbe Platforms

The CPU pinning requirements when *Double* Application Docks are installed on an EndaceProbe, are as follows:

First Double Application Dock		Second Double Application Dock	
vCPU Number	CPU Number	vCPU Number	CPU Number
0	2	0	6
1	22	1	26
2	3	2	7
3	23	3	27
4	4	4	8
5	24	5	28
6	5	6	9
7	25	7	29

Assign and Configure Additional vDAGs

vDAGs provide a means of passing monitored data from the host EndaceProbe into the virtual machine. Within the virtual machine, each vDAG provides a stream of data into the processing application.

Higher capacity virtual machine require additional vDAGs.

By default, a single vDAG is assigned to each installed virtual machine. Additional vDAGs need to be attached to higher capacity virtual machines - as described below.

The number of existing virtual machines on the host EndaceProbe has an impact on the number of vDAGs available for allocation. You will need to determine if the required number of vDAGs are available to be allocated.

For details on how many vDAGs are required, see Determine the Required Virtual Machine Size and Resources (page 8).

To assign additional vDAGs to a virtual machine, complete the following steps:

1. Log into the host EndaceProbe CLI - *configure terminal* mode.
2. Review the instances of vDAG available for assignment:
   ```
   show virt vdag
   ```
   For example, on 4000 and 9000 platforms the CLI lists the following:
   ```
   vDAGs assigned to VMs:
     16  <virtual machine name> (extension header stripped)   (nic-mode disabled)

   Unassigned vDAGs: 17  18  19   20   21   22   23   24   25   26   27   28   29   30   31
   ```
3. Identify the numbers of the unassigned vDAG you want to assign to the virtual machine. Select the next available numbers.
4. Ensure the virtual machine is powered off, run:
   ```
   show virt vm <virtual machine name>
   ```
5. For **each vDAG** allocated to the virtual machine run the following:
   ```
   virt vm <virtual machine name> vdag <vdag number>
   ```

Configuring vDAGs

vDAGs are virtual interfaces the virtual machine uses for receiving data from the monitored network. The host EndaceProbe captures the data and passes it to the virtual machine via one or more configured vDAG.

Each vDAG must be configured to the correct NIC mode for the PAN-OS.

If additional vDAGs are required, see Assign and Configure Additional vDAGs (page 11).

1. Identify the vDAG assigned to this virtual machine.
   ```
   show virt vdag
   ```
2. For each vDAG assigned to the Palo Alto Networks virtual machine set the NIC mode to **virtio** using the follow two CLI commands.
   ```
   virt vdag <vdag number> nic-mode enable
   virt vdag <vdag number> nic model virtio
   ```

To remove a vDAG assignment:

```
no virt vm <virtual machine name> vdag <vdag number>
```

Sending Data to the Virtual Machine - Multiple vDAGs

For details see Sending Data to the Virtual Machine - Multiple vDAGs (page 5).

1. Create a Data Pipe with:
   - the input (sink) as the DAG module -
     In the example below DAG module 1 port A.
   - the output (source) as the previously configured load balancing output.

   For example, in the CLI:

   ```
   erfstream pipe <pipe_name> source dag dagmod.1.a sink hlb <name>
   ```

   The Data Pipe can also be created on the GUI.

Distributing Data to Multiple vDAGs

When multiple vDAGs are assigned to a virtual machine, each vDAG can pass a proportion of the captured to the traffic to the virtual machine. This is configured on the EndaceProbe as a HLB (Hash Loading Balancing) output. This assigns a percentage of the received traffic to each vDAG.

1. Configure a *HLB output* and define what percentage of received traffic is to be sent to each vDAG.

   The VM-Series Firewall is used in passive mode. This means the monitored traffic can be load-balanced across the allocated vDAGs.

   For example, a virtual machine with six vDAGs requires the following:

   ```
   erfstream hlb <name> algorithm 5
   sink vdag <vdag num>.<virtual machine name>.1 range 0-16
   sink vdag <vdag num>.<virtual machine name>.2 range 16-33
   sink vdag <vdag num>.<virtual machine name>.3 range 33-49
   sink vdag <vdag num>.<virtual machine name>.4 range 49-66
   sink vdag <vdag num>.<virtual machine name>.5 range 66-82
   sink vdag <vdag num>.<virtual machine name>.6 range 82-100
   ```

   For example, a virtual machine with four vDAGs requires the following:

   ```
   erfstream hlb hlb1 algorithm 5
   sink vdag <vdag num>.<virtual machine name>.1 range 0-25
   sink vdag <vdag num>.<virtual machine name>.2 range 25-50
   sink vdag <vdag num>.<virtual machine name>.3 range 50-75
   sink vdag <vdag num>.<virtual machine name>.4 range 75-100
   ```

   Note:
   When copy and pasting the above configuration in the EndaceProbe CLI remember to remove the line breaks - it must be a continuous string.

   The selected HLB algorithm is `Source IP XOR dest IP`

Powering on the Virtual Machine

For details see Powering on the Virtual Machine (page 6).

To power on the virtual machine, complete the following steps:

1. Power on the virtual machine:

   ```
   virt vm <virtual machine name> power on
   ```

Saving the Host Configuration

For details see Saving the Host Configuration (page 6).

Once the virtual machine is correctly configured, the details must be saved on the Host EndaceProbe.
This ensures the configuration persists after a reboot of the host EndaceProbe.

1. On the host EndaceProbe, save the running configuration.

   ```
   configuration write
   ```

Note:
*This can also be done on the GUI by clicking the **Save** option on the top right corner below the menu bar.*

Determining the Virtual Machine's IP Address

To determine the assigned IP address for the virtual machine, complete the following steps:

1. In the Host EndaceProbe CLI, use the text console to connect to the virtual machine:
   ```
   virt vm <virtual machine name> console connect text
   ```
   Where `<virtual machine name>` is the name you previously assigned.
   A command line opens and reports the following:
   ```
   Connected to console /dev/pts/1
   Escape character is: 'Ctrl ^'
   ```
2. Press **Enter**.
   The virtual machine completes its start-up process and displays information on the screen.
   One the virtual machine has booted, the IP address of the virtual machine displays.
3. Exit the text console and return to the host EndaceProbe CLI:
   ```
   Ctrl ^
   ```

1. In a separate session, login in to the virtual machine using its IP address, default user and password.
   See Security Considerations (page 1).
2. Review the network configuration as per the PAN-OS instructions.
   For further details refer to the Palo Alto Networks PAN-OS technical documentation.

Deployment Complete

Congratulations you have completed the deployment and configuration of the Palo Alto Networks VM-Series Firewall. You can now log and use the VM-Series Firewall.

Controlling Virtual Machines

Starting and Stopping Virtual Machines

You can start and stop virtual machines using either the CLI or GUI of the EndaceProbe.

Make sure you shut down the operating system *from within the virtual machine* prior to using the host to shut down the virtual machine.

CLI

Once the virtual machine system has shut down you can stop, start or restart the virtual machine as follows:

To stop a virtual machine, run:

```
virt vm <virtual machine name> power off
```

To start a virtual machine, run:

```
virt vm <virtual machine name> power on
```

To stop and immediately restart a virtual machine, run:

```
virt vm <virtual machine name> power cycle
```

Where `<virtual machine name>` is the name you previously assigned.

To learn more about starting and stopping a virtual machine, refer to the *Actions* section in the *Application Dock* chapter of *EDM09-21 CLI Command Reference*.

GUI

Refer to the *Dock* section of your *EndaceProbe User Guide*.

For details on how to shut down the operating system from within the virtual machine prior to using the host to shut down the virtual machine, refer to the Palo Alto Networks PAN-OS technical documentation.

Set Virtual Machine Power State

To set the power state for the virtual machine when the host is powered on, use the following CLI command:

```
virt vm <virtual machine name> boot auto-power [on|off|last]
```

Removing a Virtual Machine

To remove a virtual machine, follow these steps:

1. On the host EndaceProbe, stop and delete the Data Pipe that is sending data to the PAN-OS virtual machine.
2. Log into the host EndaceProbe CLI - *configure terminal* mode.
3. List details of virtual drives bound to virtual machine:

   ```
   show virt vm <virtual machine name> storage
   ```

   Where `<virtual machine name>` is the name previously assigned.

   The CLI lists details of virtual drives bound to `<virtual machine name>`.
4. Do the following:
   a. Take note of the names of the system source files.
   b. Take note of the name of the source pool in which the virtual disk resides. The source pool names will be 'default', indicating the system drive of the EndaceProbe.
5. Stop the virtual machine:

   ```
   virt vm <virtual machine name> power off
   ```
6. Remove the virtual machine:

   ```
   no virt vm <virtual machine name>
   ```
7. Remove the virtual machine's source file:

   ```
   no virt volume file <system volume name>
   ```

   Where `<system volume name>` is the name of the system source file you recorded at step 3.
8. Remove the virtual disk source file:

   ```
   no virt volume file <virtual disk source file name>
   ```

   Where `<virtual disk source file name>` is the name of the virtual disk source file previously identified.
9. Confirm that the virtual machine has been removed:

   ```
   show virt vm
   ```

   The virtual machine is no longer listed.
10. Confirm that the system source file for virtual machine has been removed:

    ```
    show virt volume
    ```

    The file is no longer listed.

Monitoring a Virtual Machine

You can monitor the state of a virtual machine with one of the following:

- The command line interface (CLI) of the Host EndaceProbe. See the *CLI* topic below.
- The graphical user interface (GUI) of the Host EndaceProbe.
  Refer to the *Dock* section of your *EndaceProbe User Guide*.

GUI

On the EndaceProbe GUI you can monitor the state of deployed virtual machine on the *Dock* tab.
For further details, refer to the *Dock* section of your *EndaceProbe User Guide*.

CLI

The following CLI commands allow you to monitor the state of a deployed virtual machine.
To run the following commands, you must be in *enable* or *configure terminal* modes.

General Information

To review this information for all instances of virtual machine:

```
show virt vm
```

To review an individual instance of virtual machine:

```
show virt vm <virtual machine name>
```

To review information about an instance of virtual machine in greater detail:

```
show virt vm <virtual machine name> detail
```

Storage Pools and Files

To review information about storage pools and the files they contain:

```
show virt volume
```

Virtual Networks

To review information about virtual networks (vnets) currently configured for the host computer:

```
show virt vnet
```

Version History

Version	Date	Reason
1	November 2017	First release
2	October 2018	Revised and updated for 6.4.x


endace