

Best Practice - Performance Tuning on VMware Hypervisors

<https://campus.barracuda.com/doc/46209503/>

VMware offers several virtualization technologies to improve the performance of virtual networks and hosts. You can increase the throughput of your virtual Barracuda NextGen Firewall F-Series by improving the virtual machine's performance and optimizing the virtual and physical network infrastructure surrounding your Barracuda NextGen Firewall F-Series Vx.

You can tune the following settings:

Manual MAC Addresses

Use manually assigned MAC addresses for your virtual network adapters. The license of the Barracuda NextGen Firewall F-Series Vx is bound to the MAC address of the first network interface. If you do not reconfigure the virtual network adapter to use a manually assigned MAC address before the first start, the VMware hypervisor automatically assigns a MAC address. These automatically generated MAC addresses can change when you move your configuration file to another directory on the same host or move the VM to another host machine, rendering your license invalid. The MAC address can also change if you edit or remove the following options from the VM's vmx configuration file (where n is the network interface number):

```
ethernet[n].generatedAddress  
ethernet[n].addressType  
ethernet[n].generatedAddressOffset  
uuid.location  
uuid.bios  
ethernet[n].present
```

VMware reserves a range of MAC addresses for automatic assignment. The hypervisor refuses to start any VM using a network adapter with a manual MAC out of the reserved range. If an automatic MAC address has already been assigned and you have not licensed the Barracuda NextGen Firewall F-Series Vx yet, remove the NIC from the VM's configuration and add a new Ethernet adapter. Make sure that you use the same virtual network adapter (e1000, VMXNET2, or VMXNET3).

Virtual Network Adapters

The Barracuda NextGen Firewall F-Series Vx supports three virtual network adapters:

- **e1000** – The old, emulated network adapter used for the Barracuda NextGen Firewall F-Series Vx version 5.2.X.
- **VMXNET2 (Enhanced)** – The standard, paravirtualized network adapter for Barracuda NextGen Firewall F-Series Vx OVA images, version 5.4.1 to 5.4.2. VLANs are not supported by this driver.
- **VMXNET3** – The recommended and top-performing paravirtualized network adapter for the Barracuda NextGen Firewall F-Series Vx machines using version 5.4.1 or above. OVAs for version 5.4.3 or later use vmxnet3 as the default network adapter.

Changing the Network Adapter to VMXNET 3

By default, the older OVA packages up to version 5.4.2 use the the VMXNET2 network adapter, which does not support VLANs. VLANs are only supported by the e1000 or VMXNET3 network adapters. If you are deploying a new Barracuda NextGen Firewall F-Series or NextGen Control Center, VMXNET3 is used as the default.

To select a non-default virtual network adapter for your Barracuda NextGen Firewall F-Series Vx or Barracuda NextGen Control Center Vx, use Barracuda F-Series Install for deployment. For instructions, see [How to Deploy a NextGen F-Series Vx using Barracuda F-Series Install on a VMware Hypervisor](#).

You cannot change the network adapter type for existing virtual network interfaces. You must delete the old network interfaces and create new Ethernet adapters using the new network driver. Do not delete the network interface that the management IP address and license is on. If the MAC address of the network interface changes, your license is invalidated. If the virtual hardware changes, the Barracuda NextGen Firewall F-Series will not be able to bring up the network interface.

Virtual Network Adapters and DirectPath I/O

The performance of the virtual networking infrastructure is generally dependent on CPU resource availability. You can significantly improve network performance by increasing the available CPU resources.

If CPU resources are not the limiting factor, network performance can benefit by using VMware's DirectPath I/O. DirectPath I/O uses the Intel VT-d and AMD-Vi CPU extensions to grant the guest operating system direct access to the host's hardware components. If you use DirectPath I/O, networking performance generally benefits by increasing the available RAM, rather than CPU resources. The following virtualization features are not available when using DirectPath I/O: physical NIC sharing, memory overcommit, vMotion, and Network I/O Control.

TCP Offload Engine (TOE)

TCP offload engines cannot be used with routing devices such as the Barracuda NextGen Firewall F-Series.

Channel Bonding (Interface Bundles, Etherchannel)

Channel bonding is useful for scenarios in which networking hardware is the limiting factor. Generally, all connections that interact between the VMware hypervisor and the physical network can benefit by channel bonding. This includes the connection from the vswitch to the physical network.

Do not use channel bonding with virtualized network interfaces because this increases the management overhead by the hypervisor and decreases the overall network performance.

Disk I/O

You can increase the performance of your virtual disk by:

- Using eager zeroed thick provisioning when creating the virtual disk. If you are already using thin provisioned disks, you can convert them to thick provisioning on the VMware host.
- Increasing the timeout for the disks in the Barracuda NextGen Firewall F-Series Vx to at least 180 sec.

If you have changed your MAC address and invalidated your license, [contact Barracuda Networks Technical Support](#).

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.