ETVEP Deployment Guide

Rev A

8/13/12

Table of Contents

Introduction

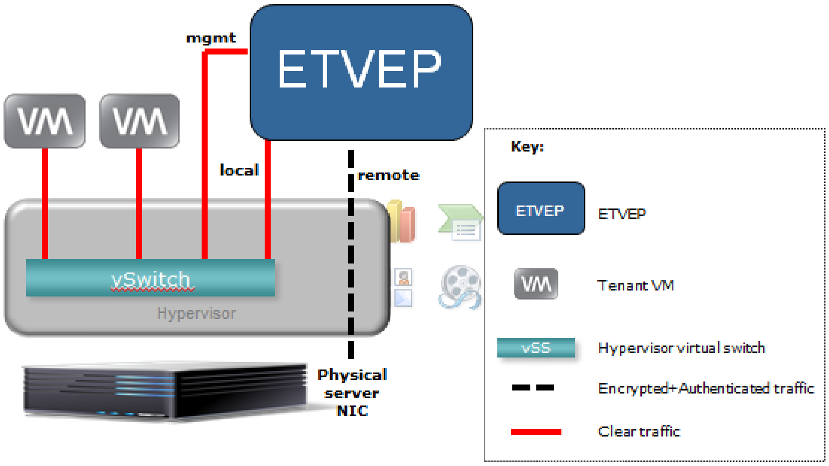
The ETVEP is a virtual appliance for VMWare ESX/ESXi environments that enables sensitive workloads to execute and communicate securely in untrusted networks. The ETVEP provides data confidentiality and integrity for sensitive data in motion in shared environments and prevents one tenant from monitoring the network traffic or attacking the virtual servers of another tenant. Furthermore, the ETVEP allows the data owner or a trusted third party to control the encryption keys without the need to share the encryption keys to the infrastructure provider.

ETVEP Virtual Connectivity

The ETVEP uses proven Black Box EncrypTight group encryption technology to provide scalable network encryption without tunnels. The ETVEP protects one or more virtual servers by enforcing the encryption and isolation policies specified in Black Box EncrypTight Manager (the centralized key and policy management system for EncrypTight appliances). EncrypTight Manager is designed for automated policy provisioning and integration with cloud operating environments.

The ETVEP is a bump in the virtual wire that connects between tenant VMs and the rest of the network using virtual network switches that are built into the hypervisor. This allows the ETVEP to protect VMs without adding software to the VMs and without requiring custom hypervisor changes.

The diagram below illustrates how the ETVEP is typically connected to the rest of the network. The ETVEP has three network interfaces: Local, Remote, and Management. The Local interface of the ETVEP connects to the trusted network on which the protected VMs reside using a Virtual Standard Switch (vSS) to switch all of the traffic to and from the protected VMs through the ETVEP. This allows the ETVEP to apply encryption and authentication policies to the traffic. The ETVEP's Remote interface connects to the shared (untrusted) network. The ETVEP remote interface can be connected directly to the physical server's network interface card (NIC), or it can be connected to a different vSS or even a Virtual Distributed Switch (vDS). The ETVEP's Management interface is used to manage the ETVEP and it can be bridged to the trusted network or connected to a separate out-of-band management network.



AES encryption using software algorithms

The introduction of instructions added to the Intel processors is believed to be a key development that will improve performance on a pure software platform.

Intel's AES instructions are a new set of processor instructions that will be introduced in Intel processors. These instructions enable fast and secure data encryption and decryption, using the Advanced Encryption Standard (AES) which is defined by FIPS Publication number 197. Since AES is the dominant block cipher, and it is deployed in various protocols, the new instructions will be valuable for a wide range of applications.

The architecture consists of six instructions that offer full hardware support for AES. Four instructions support the AES encryption and decryption, and the other two instructions support the AES key expansion. Together, they offer a significant increase in performance compared to pure software implementations.

The AES instructions have the flexibility to support all three standard AES key lengths, all standard modes of operation, and even some nonstandard or future variants.

Beyond improving performance, the AES instructions provide important security benefits. Since the instructions run in data-independent time and do not use lookup tables, they help in eliminating the major timing and cache-based attacks that threaten table-based software implementations of AES. In addition, these instructions make AES simple to implement, with reduced code size. This helps reducing the risk of inadvertent introduction of security flaws, such as difficult-to detect side channel leaks.

Performance

- Edit the "rc.local" file to turn off IGMP
  1. First you need root access.
  2. Log in as root.
  3. From the shell enter:

     ```
     echo 'echo 0 > /sys/devices/virtual/net/br*/bridge/multicast_snooping'
     > /etc/init.d/rc.local chmod a+x /etc/init.d/rc.local
     ```

  NOTE: You need to do this after every time you upgrade. The "rc.local" file does not get copied on upgrades.

- Tuning ESX performance is necessary to get the most from your ETVEP. Without tuning, the default ESX network settings may result in poor performance. These settings have been found in our testing to help. Making changes to these settings can result in substantial performance improvements. Since each environment is unique these settings may not improve performance for your specific application.
- Please be sure to record any changes and do testing in your environment to make sure that these will work for your application. You may need to reverse out these changes if they do not work for your application.

VMXNET3

- Make sure that you are using the VMXNET3 driver for the ETVEP and all guest machines. This driver is optimized for high network speeds and is the only driver that is able to saturate a gig link with clear traffic.

Enable VMDQ

- If using an Intel NIC make sure that Netqueue is enabled. This will take advantage of VMDq support on the Intel NIC. VMDq is optional and disabled by default.
- **NOTE**: Modifications to VMDq settings require a reboot of the ESX host.
- Please see vmware knowledgebase article 1026094 for full instructions on how to enable VMDQ for the igb driver (Intel 82576 and 82580 ethernet chip families).
- For the ixgbe driver (Intel 82599 10G chipset) see VMWare KB article 1004278
- **TODO**: References to Intel NIC notes

Enable LRO for ESX

- Enable LRO on the hypervisor by connecting to the Vsphere console. Go to Configuration -> Software -> Advanced. Change the setting for Net.VmklnxLROEnabled from 0 to 1. You may also want to change Net.VmklnxLROMaxAggr to be larger than 6. A value of 12 may work well. A reboot is required for changes to this setting to take effect.

Increase the size of the RX Ring for the ESX NIC

- From the CLI of the ESX host you can increase the size of the RX buffer on the NIC. To do this you will need to use thtool. Example: ethtool –G vmnic0 rx 1024.
- This can be an important setting to change if you see lots of dropped packets at the hypervisor level or physical NIC level.
- Changes to this setting can impact packet latency. Increasing the size of the buffer can increase latency at the gain of fewer dropped packets.

Use VMDirectPath I/O

- This will dedicate a physical NIC port to the ETVEP. This would make the most sense for the Remote port of a ETVEP.
- Please see VMWare KB Article 1010789 for full details on how to configure VMDirectPath