Threater - VMware Configuration

13 October 2023

Virtual Deployments

At Threater, we pride ourselves on providing our customers with a cost-effective means to make threat intelligence truly actionable, by blocking malicious traffic in real-time with no measurable impact on network performance. The majority of our customers deploy our Threater Enforce software on dedicated on-premise hardware, but for customers that are interested in protecting their virtual infrastructure, we also support virtual deployments using VMware. (And yes, we also support native protection for AWS, Azure, and GCP workloads, too.)

VMware Configuration Steps

The configuration steps outlined below can be used to properly configure a VMware image running the Threater Enforce software stack, suitable for protecting your VMware infrastructure.

1. Download the ISO file through the link that you received by email.
2. Deploy the ISO image in Vmware.
    a. Threater Enforce software requires the following resources.
        i. minimum of 2 CPU cores
        ii. minimum of 4 GB RAM
        iii. 200 GB Hard drive
        iv. Three network interfaces (admin, inside, and outside)
        v. Guest OS should be Ubuntu Linux (64-bit)
3. Network Information
    a. Network adapter 1 is the admin interface, adapter 2 is inside, and adapter 3 is outside.
    b. Network Adapter Type should be set to VMXNET 3.
    c. The admin interface will need to be connected in order to manage the device.
    d. The inside and outside interfaces can be disconnected until it is ready to be put inline.
    e. When you are ready to put it in line, Network adapter 2 (inside) is typically connected to a vSwitch that includes the firewall's outside interface. Network Adapter 3 (outside) is connected to a vSwitch that includes the internet router's interface. **IMPORTANT: these two vSwitches or port groups <u>must</u> have <u>Promiscuous Mode</u> and <u>Forged Transmits</u> enabled to allow the**

Threater Enforce software to protect traffic flowing between the two networks. The system will not function properly without those settings in place.

Installing Threater Enforce software

Once you have prepared your virtual appliance, please see our documentation on our support site for installing Threater Enforce using an ISO image.

Configuring Threater Enforce

Once you have installed the software, you will need to re-address the IP on your virtual appliance and configure Edge. Please see our documentation on our support site for configuring the Threater Enforce software.

Need assistance?

Please reach out to our Customer Success team for assistance.