# Deploying a WhiteHat Security Satellite in Your Infrastructure

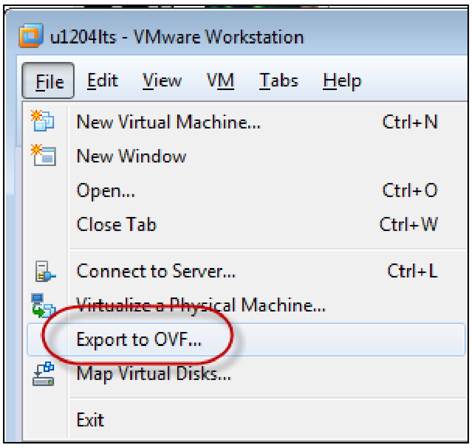
**Jason Rahm, 2013-15-05**

DevCentral uses WhiteHat Security's Sentinel service in our application development lifecycle as well as for production compliance. Beyond the direct benefits of improving our SDLC practices and reducing our window of exposure, F5 Networks and WhiteHat Security offer an integrated solution utilizing their tools and BIG-IP Application Security Manager with context-aware, adaptive, and instant virtual patching. Read here for more information on the solution overview.

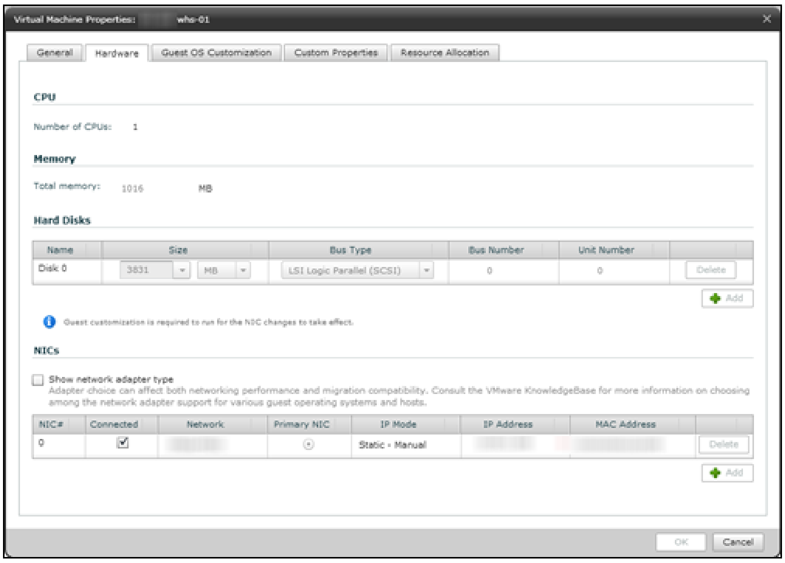
We recently eliminated public access to our pre-production test ground, so we had to come up with an alternative scanning solution for this environment. Thankfully, in addition to their internet-facing services, WhiteHat offers a satellite scanner in an appliance or virtual machine package that you can deploy behind your public infrastructure. These satellite scanners can perform the same duties as the scanners that hit your publicly available sites without exposing your pre-production development efforts to unnecessary risk. This article will demonstrate the steps required to get a WhiteHat Sentinel Satellite deployed, scanning, and communicating with the mother ship.

## Deploying the Satellite Virtual Machine

The download for the VM is in OVA format, but the Bluelock virtual datacenters we're deployed in require an OVF template for upload. You can use VMware's ovftool for this, or if you have Workstation, you can just open the OVA in your Workstation app and then select that VM and export to OVF.


u1204lts - VMware Workstation
File
Edit
View
VM
Tabs
Help
New Virtual Machine... Ctrl+N
New Window
Open... Ctrl+O
Close Tab Ctrl+W
Connect to Server... Ctrl+L
Virtualize a Physical Machine...
Export to OVF...
Map Virtual Disks...
Exit

Now that the VM is in the proper form for my environment, I can upload ~~"To the Cloud!" (sorry, couldn't resist)~~ to the virtual datacenter and build the VM. The OVF template should take care of your cpu, memory, and disk allocations, but if the cpu and memory are blank, you can just set to 1 cpu and 1G of RAM as shown in the hardware properties below.



Virtual Machine Properties: [redacted] whs-01

General | Hardware | Guest OS Customization | Custom Properties | Resource Allocation

**CPU**

Number of CPUs: 1

**Memory**

Total memory: 1016 MB

**Hard Disks**

| Name | Size | | Bus Type | Bus Number | Unit Number | |
|---|---|---|---|---|---|---|
| Disk 0 | 3831 | MB | LSI Logic Parallel (SCSI) | 0 | 0 | Delete |

Add

Guest customization is required to run for the NIC changes to take effect.

**NICs**

☐ Show network adapter type
Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapter support for various guest operating systems and hosts.

| NIC# | Connected | Network | Primary NIC | IP Mode | IP Address | MAC Address | |
|---|---|---|---|---|---|---|---|
| 0 | ☑ | [redacted] | ● | Static - Manual | [redacted] | [redacted] | Delete |

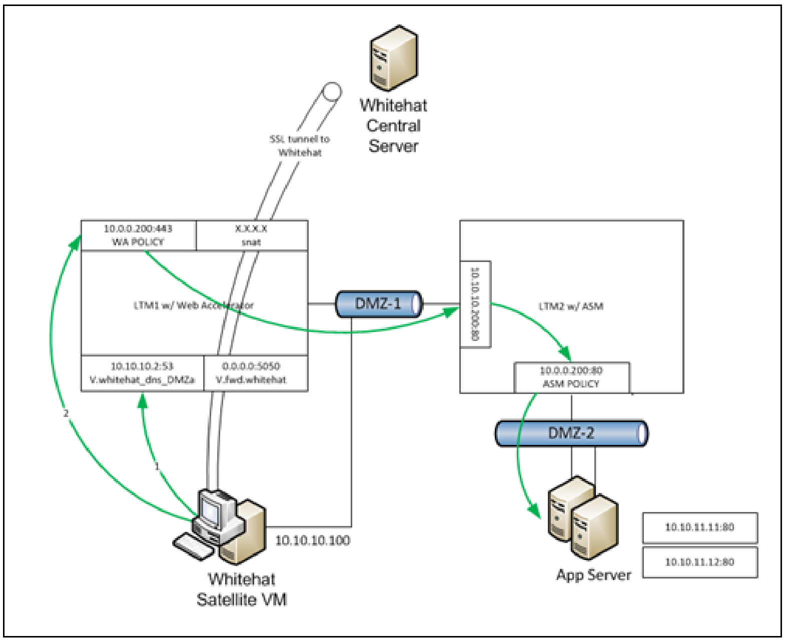
Add

OK Cancel

I attached the NIC to DMZ-1 and then powered the VM on. At boot, the only thing you have access to in the console is a configuration menu for the IP address, the mask, the gateway, and a DNS server. The first three were trivial, but the DNS requirement presented a challenge in our environment.

## Configuring the Infrastructure

I wrote a blog last week about the DNS challenge presented with this solution, so I won't rehash that here, but you can see in the drawing below that step 1 for the scanner is to do a DNS lookup of the host. A virtual server has an iRule attached to provide a single response to queries from the Sentinel satellite, and then the rest of the app infrastructure is already in place for scanning.



The only part left to handle is the communication between the satellite and WhiteHat. The support/operations teams within WhiteHat need to be able to control and report from the satellite, so I configured a virtual server that forwards on the required tcp port 5050 and snat the source to our external IP addresses. Immediately after activating that configuration the satellite synced up with WhiteHat's server and we were good to go.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com