Working in the Cloud

with ClearMedia Academy

ClearMedia WG FireboxV deployment

**Disclaimer**:

By using the ClearMedia vCloud Director templates, you can greatly reduce the amount of time needed to deploy new VMs. These templates have been configured with the best practices in mind, to assure optimal stability and performance. Although use of the template is not compulsory, it is recommended!

This guide assumes you are building a new vApp based on Template version 1.10 and deploying the template from the “Catalog” tab with a single server setup. This document covers connecting the new vApp to the internet via a basic Watchguard FireboxV virtual firewall appliance.

In-Depth explanation and step-by-step procedures

* We assume that you have started with the “How-To - VMware Template 1.10” Document.
* Request a Watchguard FireboxV feature key for your setup. Mention the customer name or contract. You can only request this for an active contract (activated quote). If the quote is not activated yet, do this first.
* Also request a public IP for the NAT IP you will find later on.
* Go to your vApp.
* Shutdown the vApp by pressing the red stop button under the tab vApp Diagram. Adding/deleting/changing networks requires that the vApp be in a shutdown state.
* Add VM’s by clicking on the 3 dots next to the vApp, and clicking on “Add” and then “Add VM…”

Afbeelding met tekst, binnen, schermafbeelding

Automatisch gegenereerde beschrijving

* A new Wizard appears. Click on “Add Virtual Machine”
* In the wizard, choose “From Template”, give the new VM a name, select the **FireboxV** template

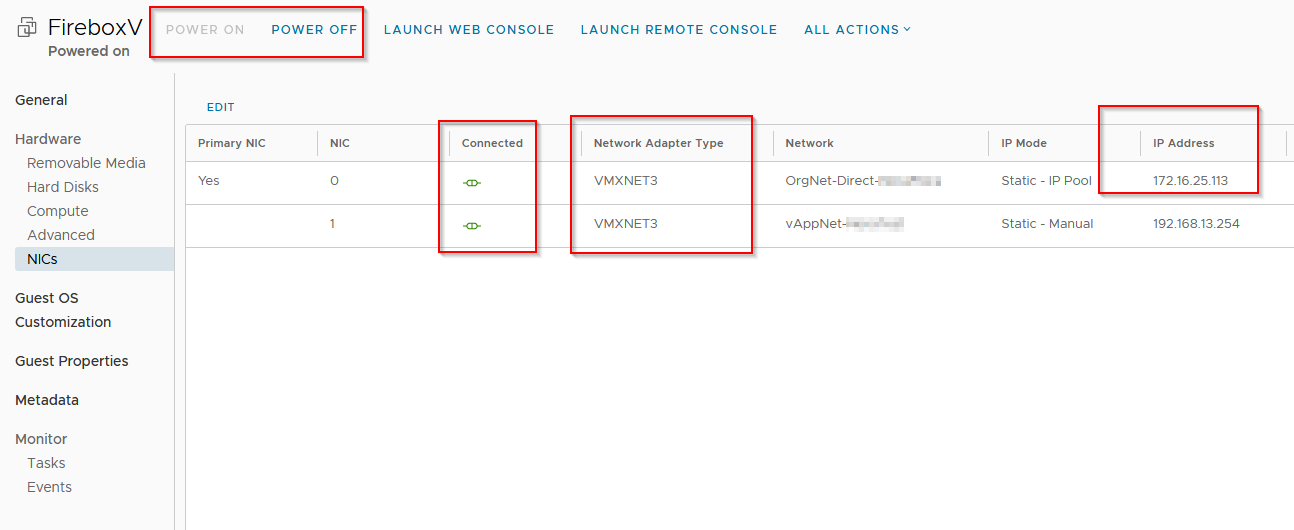
Afbeelding met tekst

Automatisch gegenereerde beschrijving

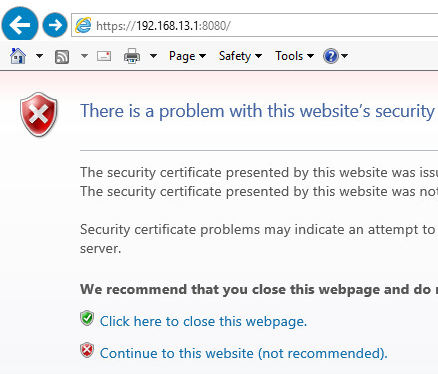
Afbeelding met tekst

Automatisch gegenereerde beschrijving

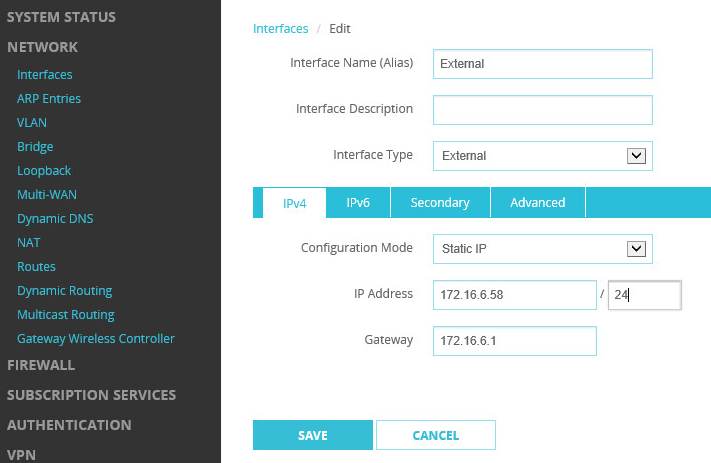
* + At the network adapters verify you are using a “VMXNET 3” adapter with Windows VM and the “Connected” icon is green.
* Start the FireboxV and at least one VM by right clicking on it and pressing “Power On”
* While waiting, find the NAT IP for your vApp under the Virtual Machines tab, at NIC 0 of the FireboxV device and note it down. You will need it later on for your request to ClearMedia.



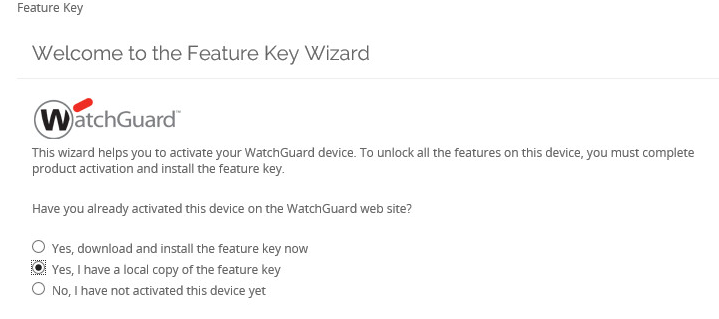
* Open the Windows console using the “How-To VM Console” document, login on the server and open a browser.
* Open the WatchGuard admin Web interface via <https://192.168.13.1:8080>
* Ignore any security warnings about the Self Signed SSL certificate.



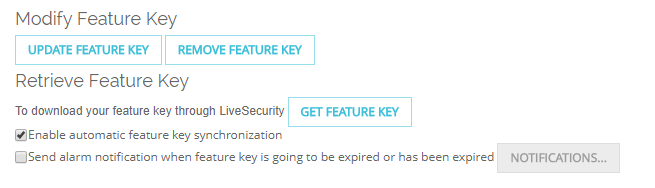
* Login with credentials “admin” and password “readwrite”.
* Open the tab “Network” and subtab “Interfaces”, click on the External interface and choose “Edit”.
* On the IPv4 tab, change the “Configuration Mode” to Static IP and enter IP address and Gateway



* For the External IP address you must use the same IP that you have found on the NIC0 interface of the WatchGuard FireboxV. For Gateway address, use the 172.16.x.x address.
* For extra public IP’s, you can add extra NAT IP’s under the “Secondary” tab. However, **NEVER** use a NAT IP out of the “Static Pool”. **Always** use NAT IP’s outside of the “Static Pool” for secondary IP’s. You noted this pool down during the step on de administration tab.
* Do not forget to click on the “**Save**” button.
* On the top, click on the banner that says “Add a feature key”.
* In the wizard, click on “Yes, I have a local copy of the feature key”



* Paste the entire feature key in the input box that you received from ClearMedia Support.
* Verify alarm notification is turned **OFF** and that Automatic feature key sync is turned **ON.**



* **Communicate the NAT IP for the vApp (172.16.x.x) to ClearMedia support so we can link it to a public WAN IP. Otherwise incoming internet traffic will not be possible.**
* Open the server again and Sync the iNSTALL folder with the ClearMedia GitHub site by right clicking on C:\iNSTALL\SyncGit.ps1 and clicking “Run with Powershell”.
* Use the ClearMedia provided BG Info script, under C:\iNSTALL\BGInfo\PresetAndBgInfo – Shortcut to verify that the correct public IP is used.
* Remember: WebUI access from external is disabled by default. You must configure the firewall rule first, to allow remote access to the Watchguard Web Mgmt Interface.
* You should also reboot the Windows Server behind the Watchguard so it can activate the Windows license correctly.
* **Finished!**