

How-to Setup Internal routing on ESX/ESXi Host using Vyatta VC5 virtual appliance

Tom Halligan

Purpose:

If you need to setup an isolated network with VMs that still need access to a production network or the internet, you need to use a VM that is capable of routing traffic. Any number of possible solutions will work for this, a LINUX based firewall package like IPCOP or Smoothwall, a Unix VM with routing configured or even a Windows VM with ICS or ISA server installed.

To my mind the best solution out there at this time is Vyatta (<http://www.vyatta.org/>). Vyatta is an Open source package which is attempting to compete with Cisco in the routing product space. Regardless of how that may turn out, Vyatta is an excellent product which can be run on ESX(i), VMware Workstation or VMware Server and used for routing internal virtual machine traffic to external networks.

What I will cover here is how to setup Vyatta to act as a network bridge between a internal only vswitch and a vswitch with an uplink to the production network.

In this procedure I will use the Vyatta virtual appliance. You could build your own VM by downloading the ISO file from Vyatta's website but all things being equal the Virtual appliance can be brought up quicker when you have all the pieces in place.

Prerequisites:

Your ESX(i) host needs to be configured with at least two vswitches with Virtual machine port groups. One of these vswitches will uplink to your production network and the other will be internal with no uplink.

Procedure:

I. Download the Vyatta Virtual appliance and unzip it to folder on your local system.

<http://www.vyatta.com/downloads/vc5.0.2/vyatta-virtual-appliance-vc5.0.2.zip>

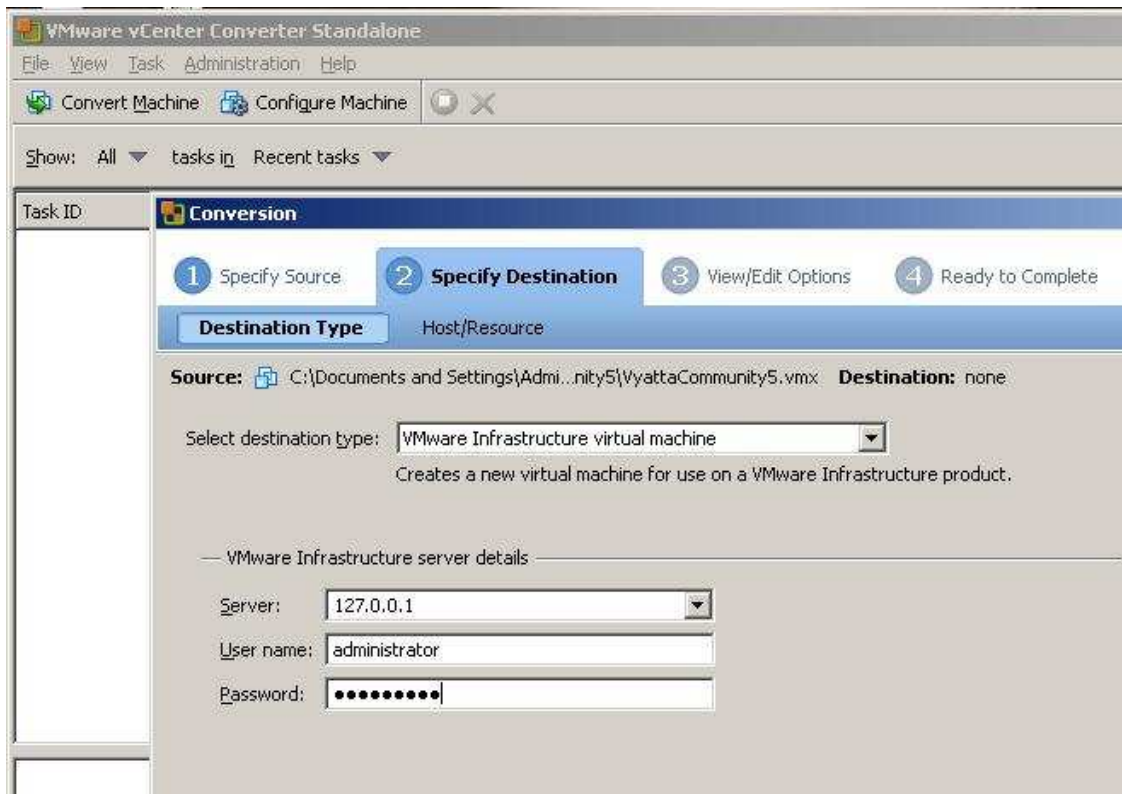
II. Import the appliance in with VMware converter

(<http://www.vmware.com/go/getconverter>).

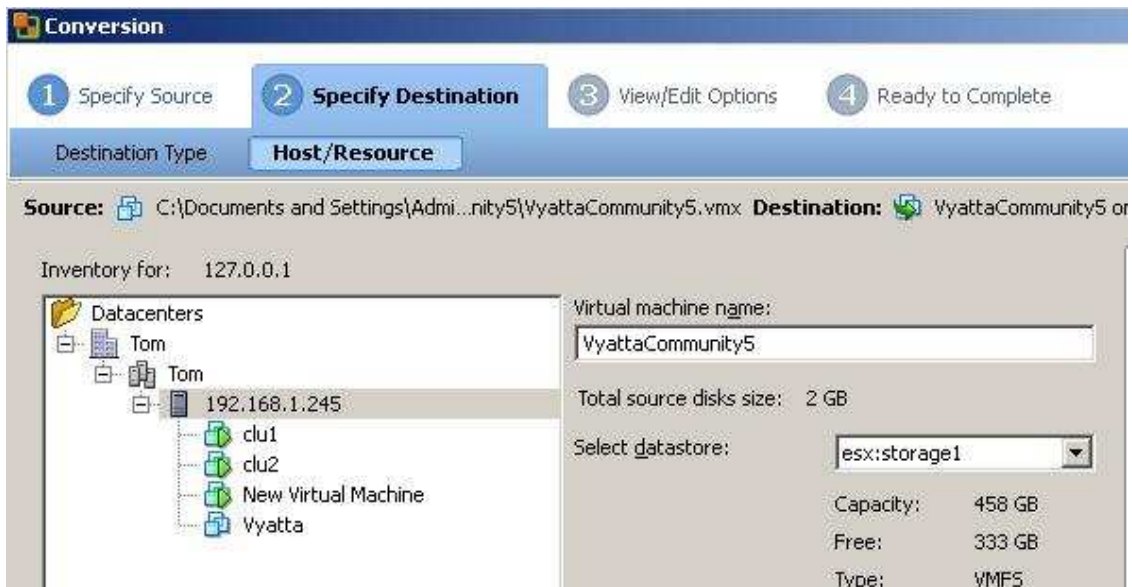
1. Open converter and select **“VMware Workstation or other virtual machine”** and browse to where you extracted the files and select **“VyattaCommunity5.vmx”** file. Click **“Next”**



2. Select you destination as **“VMware Infrastructure virtual machine”** and input your server address and credentials to authenticate to your ESX host or Vcenter server. Click **“Next”**



3. Select your ESX/(i) host and Datastore. Also chose a name for you routing VM. Click “Next”

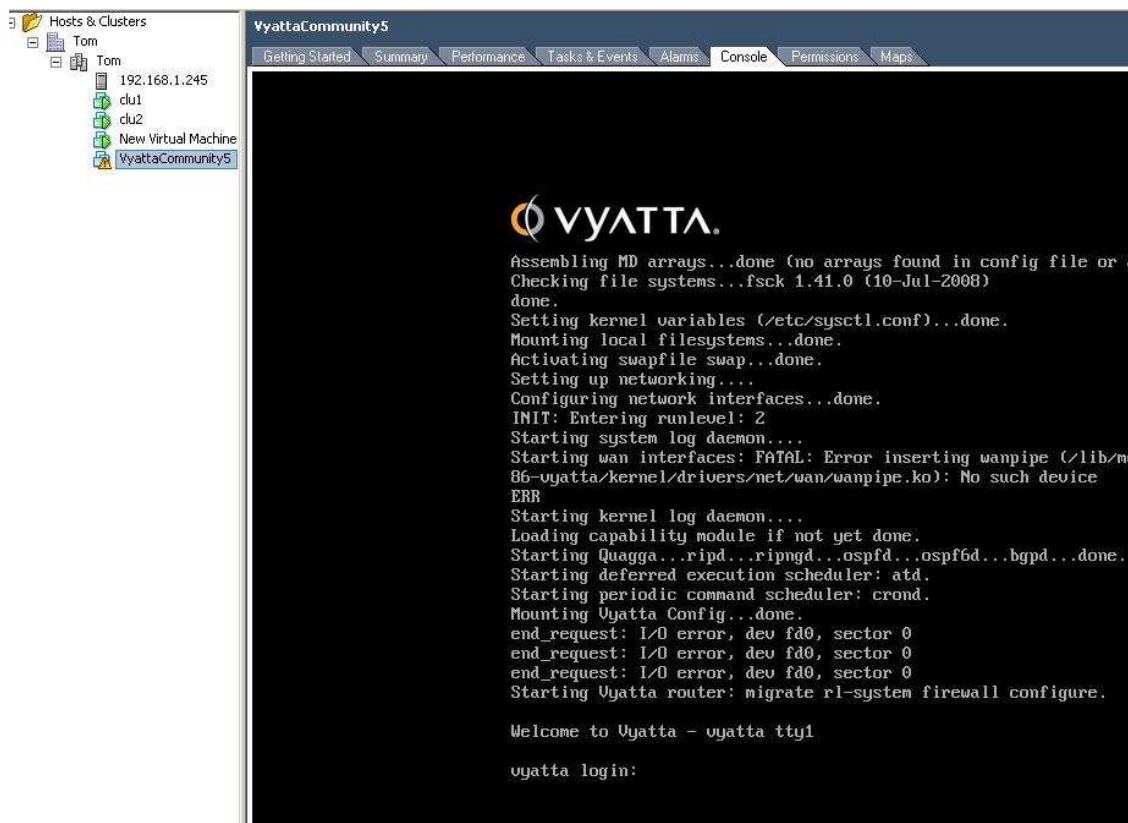


4. Click “Next” at the “View and Edit Options” screen

5. Click “**Finish**” at the “**Summary**” page. The VM will take 5 or so minutes to import (Depending on network speed between your location and the host or VC server).

6. Once the VM has been imported edit the VM settings and configure the first VNIC to attach to the vswitch that uplinks to your production network (This will be **eth0** on the appliance). The second VNIC should be attached to your "Internal" vswitch where your isolated VMs will reside. There is a third interface which you can leave unconfigured or simply remove from the VM.

7. Now power on your VM and watch boot up from console window.



III. Now we want to setup the eth0 interface and enable remote ssh¹ access.

By doing this we will be able to connect to the VM via putty and copy and paste the rest of the configuration entries (I hate typing). This will speed up the setup. Logon to the Vyatta VMs console from VIC client and use the following credentials

User: **vyatta** Password: **vyatta**

At the command prompt type **configure** this will place you in configuration mode. Then type the following commands

set interfaces ethernet eth0 address xxx.xxx.xxx.xxx/24 (Where xxx.xxx.xxx.xxx is an IP address from your routable production network that you have assigned for use by the VM. Also I have used CIDR /24 assuming a class C production network, your value may vary)

set service ssh

*commit*²

Now you should be able to use putty or another SSH client to connect to the VM from your production network using the IP you have just assigned to eth0 on the VM.

IV. Now we configure the "internal" interface, setup NAT and (optionally) configure External default gateway on Vyatta router.

Setup the internal interface

set interfaces ethernet eth1 address xxx.xxx.xxx.xxx/24

Setup NAT for the internal network

set service nat rule 1 source address xxx.xxx.xxx.0/24 (xxx.xxx.xxx.0/24 is the network your internal VMs reside on)

set service nat rule 1 outbound-interface eth0

set service nat rule 1 type masquerade

commit

Now set your VMs on the internal vswitch to use the IP assigned to **eth1** as their default gateway and those VMs will have access to the production network.

To allow those VMs access to the internet (Which you may not want to do) you have to configure the Vyatta VM to use the default gateway of you production network, to do so issue the following commands.

set protocols static route 0.0.0.0/0 next-hop xxx.xxx.xxx.xxx (Where xxx.xxx.xxx.xxx is gateway of external network)

commit

V. Test and save configuration

Once setup is complete you should be able to ping systems on your production network and the internet. You should now save the changes so that they will be retained on the VM between reboots. To do so in configure mode type **save**

```
vyatta@vyatta# save
```

You should see the following indicating that the configuration has been saved

```
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
```

```
Done
```

Security Note:

1. You should change passwords from defaults on VM for users **root** and **vyatta** once you have it up and running. You may also wish to disable ssh access and only enable it when needed.

¹ Vyatta VC5 had a web based GUI. I prefer the command line interface but if you want give it a try

² Like Cisco IOS the configuration is not saved until such time as you have committed your changes and saved you config. At any time in this process if you just want to start from scratch just reboot the VM before saving the config (last step). Bearing in mind you will have to assign an IP address eht0 and enable ssh again to access the VM from ssh client