



HOWTO: Set up a Vyatta device with ThreatSTOP in router mode

Overview

This document explains how to set up a minimal Vyatta device in a routed configuration and then how to apply ThreatSTOP to it. It is strongly recommended that you read the relevant Vyatta manuals (e.g. “Quick Start”, “Basic Configuration”, “Installing and Upgrading”, “Firewalls” and “LAN Interfaces”) in addition to this HOWTO guide.

Contents

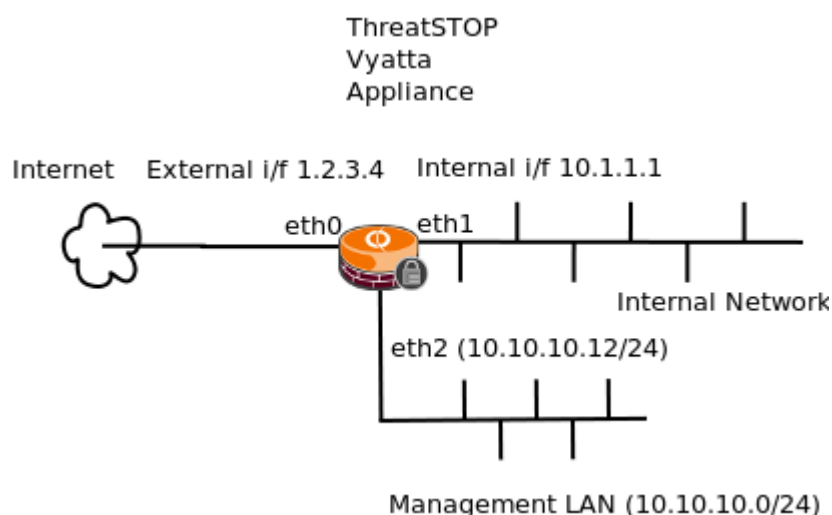
Overview	1
Contents	1
Requirements	2
ThreatSTOP Account	2
Sign up at ThreatSTOP	2
Add Device	3
Installation of Vyatta OS onto Hard Disk	4
Setup	5
Console commands	6
SSH from management console	6

Requirements

For a physical install, a Vyatta Appliance or a PC with two or three NICs and a Vyatta CD (for testing either one of the subscription editions or Vyatta Core is acceptable – for longer term support a subscription version is required). Vyatta recommend 1 GB of memory, however for testing purposes this is plenty and 512 or even less can be used, unless you are planning on using the device with many features enabled. A 4gb hard disk is likewise more than enough for testing and evaluation as Vyatta only requires about 1-2gb.

For a virtual install either a VM image or a blank VM and the ISO of the Vyatta CD is required. The same memory and disk requirements as for the physical install apply. If you are not using a Vyatta image then you must enable PAE support on the CPU otherwise Vyatta will not boot.

The device may be set up using either two or three NICs. In the diagram below a 3 NIC setup is shown with a separate management LAN (10.10.10.0/24) as well as the internal and external network interfaces.



3 NIC Vyatta configuration in router mode

This document briefly explains how to set up NAT so that devices on the 10.x.x.x networks can access the internet via the Vyatta and to firewall the external interface so that no access is allowed to the Vyatta's SSH console from outside. This is a very basic setup and most live deployments are more complex, including the configuration of VPNs access to internal web/mail servers from outside and so on.

In addition to the machine (or VM) that will be running Vyatta, a management platform is required. This machine should have an SSH client installed (linux/mac OS machines have this by default for windows you should install a client such as PuTTY - <http://www.putty.org/> - or Mindterm - <http://www.appgate.com/index/products/mindterm/>), access to the Internet and a web browser.

ThreatSTOP Account

Before you setup the Vyatta box you should sign yourself up with ThreatSTOP if you have not already done so and add the Vyatta device to your account.

Sign up at ThreatSTOP

Start the Trial Today

15 day Trial

Community

From the ThreatSTOP website (www.threatstop.com) look down on the left hand side for the “sign up” button. Select 15 day Trial and click sign up.

The next page (<https://www.threatstop.com/index.php?page=index&action=trial>) is a standard sign up page requesting contact details and so on, as well as setting up your account password. Please make a note of the password as it will not be sent to you and ensure that the email address you use is valid. Once signed up an email will be sent with an activation link and instructions. The account must be activated for you to be able to log in.

Add Device

Ideally this section will be done from the management station that you will be later using to SSH to the Vyatta. Open a web browser and log in at <https://threatstop.com> using your registered email address and password. Once you have logged into the account you should click on “Manage Devices”, then on “Add Device” and start to fill in the device details

Enter a nickname to give the device so it is easy for you to recognize. The nickname is limited to 10 characters. The IP address must be the public or outside IP address of the device. Our DNS servers will not answer queries coming from a different address than the one you enter.

If your firewall or model is not listed, please use the “Other” option and fill in the the text box with some detail about which firewall you are using.

(Please note all fields marked with * are required)

#	Nickname *	Manufacturer *	Model *	IP Address *
2 of 10	<input type="text" value="vrouter"/>	<input type="text" value="Vyatta"/>	<input type="text" value="Router"/>	<input type="text" value="121"/> <input type="text" value="11"/> <input type="text" value="11"/> <input type="text" value="11"/>
Location of Device	<input type="text" value="United States"/>			Postal Code <input type="text" value="12345"/>

Configure ThreatSTOP Protection For This Device

ThreatSTOP Block Lists

Select the lists that you want associated with this device.

BASIC The core ThreatSTOP service. The IP addresses on the BASIC <i>active threat list</i> are the worst current sources of attacks, spam, and malware, and the currently active Botnet Command and Control servers. Connections from these addresses will be blocked, and if a system inside your network attempts to connect out to these addresses, it is most likely infected with malware and needs to be cleaned.
<input checked="" type="checkbox"/>
ADVANCED For firewalls with larger capacity, this <i>active threat list</i> includes a deeper look into the currently active sources of malware, network attacks, fast-flux botnets, crime hosting networks, phishing and browser hijacking sites, and the current Cymru Bogon List. If your firewall has sufficient capacity, you should include this list.
<input checked="" type="checkbox"/>

You should add the device as Manufacturer “Vyatta”, model “Router” and enter the IP address that it will be seen as on the internet (in this example document the address used is 1.2.3.4 but you must use the actual address of your device).

You should also select which block lists you wish to use. A good choice for a firewall with end users behind it would be “Basic”, “Advanced” and “Botnets” however you should feel free to ask ThreatSTOP tech support for advice. Since you can change your selection at any time without needing to change anything on the firewall there is no harm in making an initial choice now and then later modifying it.

Having entered the device details and chosen your blocklists, click on “save” to add the device and display the information on how to configure it. If you are using the management station keep this page open while you set up the Vyatta.

Note: if you have an account with “expert mode” enabled and you are strongly recommended to check with ThreatSTOP before enabling it and choosing feeds as some (the “parasites” feed in particular) are known to block access to sites that some people feel should not be blocked.

Installation of Vyatta OS onto Hard Disk

Note: Users of the Vyatta VM image or with a Vyatta Hardware Appliance should skip this section

Insert the CD into the drive (add the ISO if virtual) and boot/reboot the device. You should see a Vyatta logo and the option to press F1 for help or Enter to boot.



Press Enter.

```
Mounting Vyatta Config...done.  
Starting Vyatta router: migrate rl-system firewall configure.  
Welcome to Vyatta - vyatta tty1  
vyatta login: _
```

After a short while booting up you will see a login prompt. Login as user ‘vyatta’ password ‘vyatta’ (both lowercase and no “s”).

Once you are logged in enter the command

```
vyatta@vyatta:~$ install-system
```

and follow the instructions. Note: If you follow the defaults (recommended) you will totally reformat the hard disk. If you wish to not destroy all data then you should not select auto from the partition choice but rather either have the partitions set up in advance (Skip) or choose Parted.

```

each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyatta@vyatta:~$ install-system
Welcome to the Vyatta install program. This script
will walk you through the process of installing the
Vyatta image to a local hard drive.

Would you like to continue? (Yes/No) [Yes]: y
Probing drives: OK
Looking for pre-existing RAID groups...none found.
The Vyatta image will require a minimum 1000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted? If
you have already setup your partitions, you may skip this step.

Partition (Auto/Union/Parted/Skip) [Auto]: a

I found the following drives on your system:
sda      8590MB

Install the image on? [sda]:

This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: y_

```

Near the end of the process you will be asked for a password for the Vyatta account – unless you are very sure of your test network this password should probably not be ‘vyatta’. Once the install has finished you can eject the CD and reset the machine.

The machine will now boot Vyatta from the hard disk. When presented with the login prompt you should log in as ‘vyatta’ using the password you defined during the install process.

Setup

VM Image users: boot the VM and then when you get to a login prompt login as user ‘vyatta’ password ‘vyatta’ (both lowercase and no “s”).

Hardware Appliance users: Follow the basic instructions that came with your appliance to unpack, connect, and attach a management station to your Appliance. When you get to a login prompt login as user ‘vyatta’ password ‘vyatta’ (both lowercase and no “s”).

Setup is divided in to two sections, the first is done from the console of the Vyatta device and the second done while SSHing in. It is possible to do all of the work from the console but the use of SSH allows you to paste lines from this document directly which is generally quicker and less likely to lead to errors.

Note: When entering commands on the Vyatta console (or SSH terminal) you can press the TAB key at any time to auto complete a word so – for example – the command

```
set interfaces ethernet eth1 address 1.2.3.4/24
```

may be entered

```
set int<TAB> et<TAB> eth1 ad<TAB> 1.2.3.4/24
```

If there are multiple possibilities these will be listed.

Also pressing the up arrow gives access to the history of prior commands that may be edited and/or reapplied.

Console commands

Having logged in to the console you will need to set up the Ethernet interfaces, enable SSH and set the default nameserver and gateway. As noted above, you may optionally set up other services and options either from the console or via SSH. Likewise you can set the gateway and nameserver via SSH if the management station is on the same IP subnet as the Vyatta.

To configure anything on the Vyatta device it is necessary to enter configuration mode by typing "configure" at the console:

```
vyatta@vyatta:~$ configure
[edit]
vyatta@vyatta#
```

First enable ssh:

```
vyatta@vyatta# set service ssh
[edit]
vyatta@vyatta#
```

Then if you have three NICs you should set up the ip address of the management interface on eth2:

```
vyatta@vyatta# set interfaces ethernet eth2 address 10.10.10.12/24
[edit]
vyatta@vyatta#
```

If you have two NICs you should set up the ip address of the internal interface (eth1):

```
vyatta@vyatta# set interfaces ethernet eth1 address 10.1.1.1/24
[edit]
vyatta@vyatta#
```

Now set up the external IP address, default gateway and name server (the default gateway is the next hop external route, the name server may be internal or external so long as it can resolve external names such as www.threatstop.com).

```
vyatta@vyatta:~$ configure
[edit]
vyatta@vyatta# set system gateway-address 1.2.3.1
[edit]
vyatta@vyatta# set system name-server 10.10.10.5
[edit]
vyatta@vyatta#
```

Finally commit your changes, save and exit.

```
vyatta@vyatta# commit
Restarting OpenBSD Secure Shell server: sshd.
[edit]
vyatta@vyatta# save
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
Done
[edit]
vyatta@vyatta# exit
exit
vyatta@vyatta:~$
```

At this point the Vyatta device is correctly set up for basic SSH access.

SSH from management console

Using your ssh tool connect to the Vyatta as user vyatta

```
MindTerm home: C:\Users\francis\Application Data\MindTerm\
SSH Server/Alias: 10.10.10.12
No settings file for 10.10.10.12 found.
(^C = cancel, ^D or empty = don't save)
Save as alias : 10.10.10.12
Current settings file: 'C:\Users\francis\Application Data\MindTerm\10.10.10.12.mtp'
```

Connected to server running SSH-2.0-OpenSSH_5.1p1 Debian-5

```
Server's hostkey (ssh-rsa) fingerprint:
openssh md5: 84:5a:9d:5c:0a:a8:14:9c:0b:fa:4b:8e:75:40:56:b2
bubblebabble: xipag-vomal-lebuk-zuvyb-nimyl-dipek-modid-sofol-vebus-segig-guxox
```

```
Host key not found in 'C:\Users\francis\Application
Data\MindTerm\hostkeys\key_22_10.10.10.12.pub'
```

```
10.10.10.12 login: vyatta
vyatta@10.10.10.12's password: *****
Linux vyatta 2.6.32-1-586-vyatta-virt #1 SMP Mon Aug 2 23:28:02 PDT 2010 i686
Welcome to Vyatta.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyatta@vyatta:~$
```

Now add NAT so that computers inside can access external resources and save.

```
vyatta@vyatta# set service nat rule 10 type masquerade
[edit]
vyatta@vyatta# set service nat rule 10 outbound-interface eth0
[edit]
vyatta@vyatta# set service nat rule 10 source address 10.10.10.0/24
[edit]
vyatta@vyatta# set service nat rule 11 type masquerade
[edit]
vyatta@vyatta# set service nat rule 11 source address 10.1.1.0/24
[edit]
vyatta@vyatta# set service nat rule 11 outbound-interface eth0
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta# save
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
Done
[edit]
vyatta@vyatta# exit
exit
vyatta@vyatta:~$
```

If you wish to you may configure the Vyatta further to add additional features. If you intend to add custom firewall rules it is strongly recommended that this be done after you have enabled ThreatSTOP on the device.

Verify that you can see the world and can ping both threatstop.com and the threatstop dns 64.87.26.147 (press Ctrl-C once you get a couple of responses)

```
vyatta@vyatta:~$ ping threatstop.com
PING threatstop.com (64.87.26.148) 56(84) bytes of data.
64 bytes from www.threatstop.com (64.87.26.148): icmp_seq=1 ttl=43 time=234 ms
64 bytes from www.threatstop.com (64.87.26.148): icmp_seq=2 ttl=43 time=232 ms
64 bytes from www.threatstop.com (64.87.26.148): icmp_seq=3 ttl=43 time=233 ms
64 bytes from www.threatstop.com (64.87.26.148): icmp_seq=4 ttl=47 time=233 ms
^C
--- threatstop.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3008ms
rtt min/avg/max/mdev = 232.764/233.798/234.675/0.680 ms
vyatta@vyatta:~$ ping 64.87.26.147
PING 64.87.26.147 (64.87.26.147) 56(84) bytes of data.
64 bytes from 64.87.26.147: icmp_seq=1 ttl=47 time=230 ms
64 bytes from 64.87.26.147: icmp_seq=2 ttl=43 time=242 ms
64 bytes from 64.87.26.147: icmp_seq=3 ttl=47 time=235 ms
^C
--- 64.87.26.147 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 230.852/236.388/242.377/4.715 ms
vyatta@vyatta:~$
```

Finally verify that the Vyatta device is in our database.

```
vyatta@vyatta# wget -qO - https://www.threatstop.com/cgi-bin/validip.pl
Your IP address: 1.2.3.4
Address is in the list of authorized hosts
```

If the address is NOT in the database then the response will be

```
vyatta@vyatta# wget -qO - https://www.threatstop.com/cgi-bin/validip.pl
Your IP address: 1.2.3.4
Address is not in the list of authorized hosts
Host list updated every 15 minutes and last updated at
Wed Oct 27 11:15:01 2010 GMT. It is now Wed Oct 27 11:22:16 2010
```

If the address reported is the one you entered for the device when you added it at <https://threatstop.com> then you should wait for about 15 minutes and then try again. If the address remains invalid then contact ThreatSTOP tech support to find out why.

If the address reported is not the address you entered for the device at the ThreatSTOP website then you should correct that entry and wait about half an hour before retrying.

Once the address is confirmed as being in the ThreatSTOP database, you are ready to set the device up with ThreatSTOP. If you did not do the initial device addition on the ThreatSTOP website from this computer (or you closed the browser) then you should log in to your ThreatSTOP account at <https://threatstop.com>, select “manage devices” and then click on “rules” for the device you added.

Look down the webpage until you see a section like:

Setup

Copy and paste the following line into the Vyatta ssh session

```
wget -O - http://testing.threatstop.com/downloads/ts-vyatta-0.99.tar.gz | tar
xzv ; sudo ts-vyatta/setup.pl --type r --blocklist vr-001-
netb.Threat16.threatstop.local
```

As the instructions say, it is a good idea to first save a copy of the current working configuration.

```
vyatta@vyatta:~$ configure
[edit]
vyatta@vyatta# save prethreatstop
Saving configuration to '/opt/vyatta/etc/config/prethreatstop'...
Done
[edit]
vyatta@vyatta# exit
exit
vyatta@vyatta:~$
```

Then copy the text from the website (it will be slightly different to both the one above and the one below) and paste it into your SSH terminal. You will then be asked a number of questions, for which you can accept the default answers if you have just followed this HOWTO but which you may wish to change if you have enabled more features on the device.

```
vyatta@vyatta:~$ wget -qO - https://www.threatstop.com/downloads/ts-vyatta.tar.gz | tar
xzv ; sudo ts-vyatta/setup.pl --type r --blocklist vrouter-001-
netb.demonstr.threatstop.local
ts-vyatta/
ts-vyatta/revert.sh
ts-vyatta/README
ts-vyatta/setup.pl
ts-vyatta/ipsetget.pl
ts-vyatta/ipsetapply.sh
ts-vyatta/dig
ts-vyatta/loguploadclient.pl
ThreatSTOP Vyatta setup script 1.0
```

If you have not specified setup options on the command line then you will be given the chance to specify them now. First time users running this by pasting in the command from the ThreatSTOP website should probably not change anything except the firewall names and start rule number if you have already created some firewall rules.

On subsequent runs probably the only things to change will be the block and allow list ids. For each option the default value is specified in [], just press the ENTER key to accept it.

Note for the paranoid. The proposed changes to the Vyatta config, the changes to /etc/rc.local, /etc/logrotate.d/messages and the new crontab are created in the installation directory. If you choose not to allow this script to apply the changes automatically then you can review them and then apply them manually.

Threatstop installation directory [/home/vyatta/ts-vyatta/]

Normally there is no reason to change the install directory so just press enter

Threatstop ipset prefix [TS]

Install type routed - external interface id [eth0]

Likewise there is generally no reason to not accept the defaults for the prefix. If eth0 is not the external interface (it is in this example) you should type in the correct interface id.

Firewall name for interface eth0 direction in: [TSrtinrule]

Insert ThreatSTOP rules beginning at number? [10]

Add default accept? (strongly recommended if you do not have other rules for this firewall name, not otherwise)[y]

Firewall name for interface eth0 direction local: [TSrtllocalrule]

Insert ThreatSTOP rules beginning at number? [10]

Add default accept? (strongly recommended if you do not have other rules for this firewall name, not otherwise)[y]

Firewall name for interface eth0 direction out: [TSrtoutrule]

Insert ThreatSTOP rules beginning at number? [10]

Add default accept? (strongly recommended if you do not have other rules for this firewall name, not otherwise)[y]

In a simple Vyatta configuration such as the one we have created above with no other firewall activity the default Firewall names and rule start locations should be accepted, as should the suggestion to add the default accept rule. This is common when the Vyatta is being set up from scratch as we recommend you add other firewall rules after the ThreatSTOP ones. However, if you did create firewall rules for the external interface then you will need to change the name appropriately and possibly insert the rules at a different number. ThreatSTOP needs 4 consecutive free numbers and it is generally better if the ThreatSTOP rules are applied first so if you have a rule 10 you should set the start number to 1 or 5.

Threatstop block list: vrouter-001-netb.demonstr.threatstop.local

Threatstop allow list []

dig command location [/home/vyatta/ts-vyatta/dig]

Logfile to upload [/var/log/messages]

URL for submitting logs [https://threatstop.com/cgi-bin/logupload.pl]

Again there is generally no reason to modify these. The script then verifies that it can resolve your blocklist on our DNS and, assuming this is successful, offers to make the required changes.

```

Initial set up complete, testing
/home/vyatta/ts-vyatta/dig +tcp -t ptr @64.87.26.147 vrouter-001-
netb.demonstr.threatstop.local
Test successful
Creating routing rules to configure.route.sh
Creating local copy of logrotate.d/messages file
Creating crontab file
Creating local copy of rc.local file
Apply changes: /home/vyatta/ts-vyatta/configure.route.sh, /etc/logrotate.d/messages,
/etc/rc.local, crontab (Y/N)[Y]

```

Press 'Enter' to accept, or 'N Enter' to halt the script so that you can review the proposed changes.

```

Merging /home/vyatta/ts-vyatta/configure.route.sh

Removing and creating new crontab for root
# Update the ThreatSTOP lists. Every 2 hours, 48 minutes after the hour
# (00:48, 02:48, 04:48, etc.)
48 */2 * * * * /home/vyatta/ts-vyatta/ipsetget.pl
# Force a logrotate if the log is > 100k. Check every 53 minutes after the hour
53 * * * * * perl -e'exec q(/usr/sbin/logrotate -f
/etc/logrotate.d/messages) if (stat q(/var/log/messages))[7]>100000;'

Copying modified /etc/logrotate.d/messages
`/home/vyatta/ts-vyatta/logrotated.messages' -> `/etc/logrotate.d/messages'

Copying modified /etc/rc.local
`/home/vyatta/ts-vyatta/rc.local' -> `/etc/rc.local'

Get block list now? (Y/N) [Y]

```

Finally you are asked if you would like to actually download the blocklist and apply it. Unless you had problems above there is no reason why you should say no to this.

The script downloads and applies the blocklist – this can take a few seconds to complete, prints out the results and terminates with the message

```
Threatstop setup complete.
```

Congratulations

You have now set up ThreatSTOP on a Vyatta in router mode. You should now add a firewall rule to the external interface to block ssh access to the Vyatta itself:

```

vyatta@vyatta# set firewall name TSrtlocalrule rule 20 destination port 22
[edit]
vyatta@vyatta# set firewall name TSrtlocalrule rule 20 action drop
[edit]
vyatta@vyatta# set firewall name TSrtlocalrule rule 20 protocol tcp
[edit]
vyatta@vyatta# set firewall name TSrtlocalrule rule 20 log enable
[edit]
vyatta@vyatta# commit
[edit]
vyatta@vyatta#

```

[Note: If the commit doesn't work and reports an error you may have hit an intermittent Vyatta bug which can be resolved by rebooting. Exit discarding changes. Reenter configuration mode, save and then reboot.

```

vyatta@vyatta# exit discard
exit
vyatta@vyatta:~$ configure
[edit]
vyatta@vyatta# save
Saving configuration to '/opt/vyatta/etc/config/config.boot'...
Done
[edit]
vyatta@vyatta# exit
exit

```

```
vyatta@vyatta:~$ reboot  
Proceed with reboot? [confirm] Y
```

]

Once you have added the SSH rule and any other firewall rules you want and verified that the configuration works, you should probably save the configuration again as a named config and as the default.

```
vyatta@vyatta:~$ configure  
[edit]  
vyatta@vyatta# save threatstop  
Saving configuration to '/opt/vyatta/etc/config/threatstop'...  
Done  
[edit]  
vyatta@vyatta# save  
Saving configuration to '/opt/vyatta/etc/config/config.boot'...  
Done  
[edit]  
vyatta@vyatta# exit  
exit  
vyatta@vyatta:~$
```

In general, as noted above, due to a bug that makes Vyatta only accept a limited number of configuration changes before it doesn't take any more you should reboot after completing the installation.

```
vyatta@vyatta:~$ reboot
```