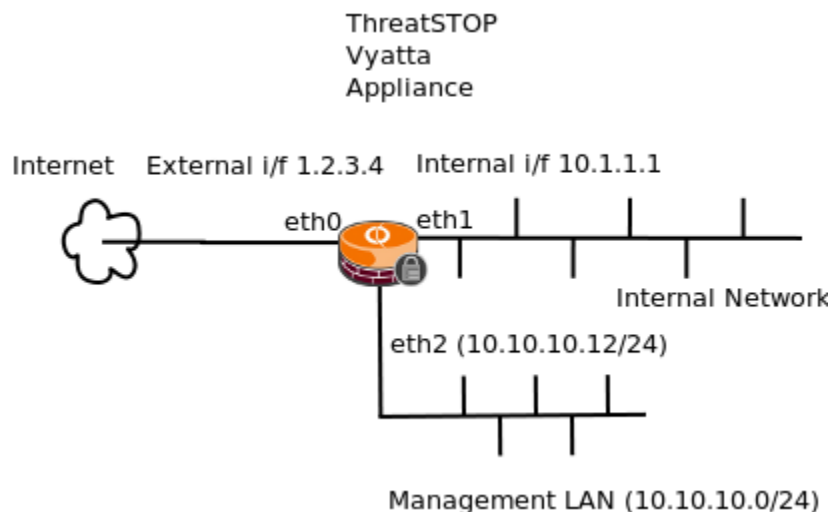


Vyatta Configuration Choices

ThreatSTOP can be run on a Vyatta appliance in either router or transparent bridge mode. Generally router mode is used when the Vyatta device is a router/firewall between your network and the Internet whereas bridge mode is used when the Vyatta device is being used in conjunction with an existing firewall/router. In bridge mode it is important to decide whether to place the Vyatta outside the firewall or inside as explained in the relevant section below

Our scripts assume there to be two or three interfaces active as illustrated in the diagrams below. Please contact ThreatSTOP Support if your desired configuration is radically different.

Router Mode

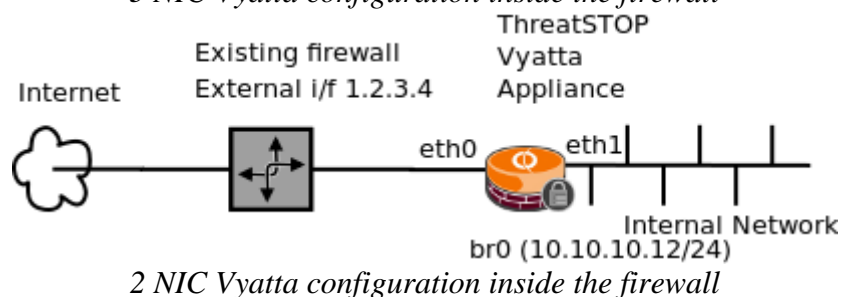
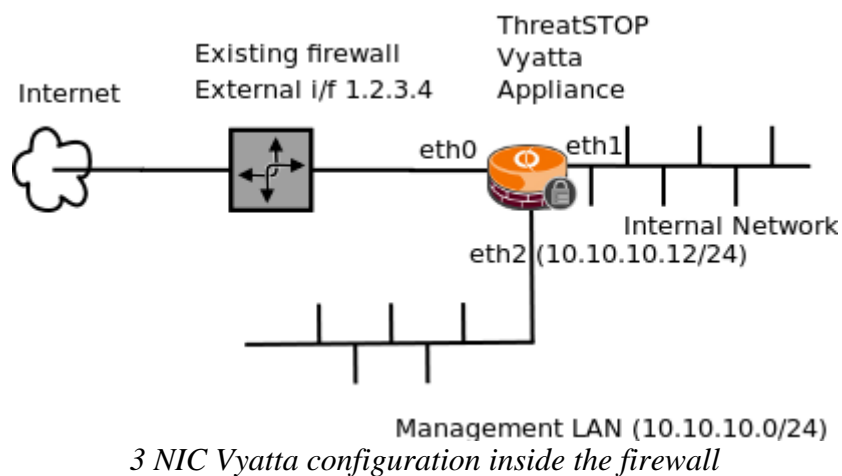
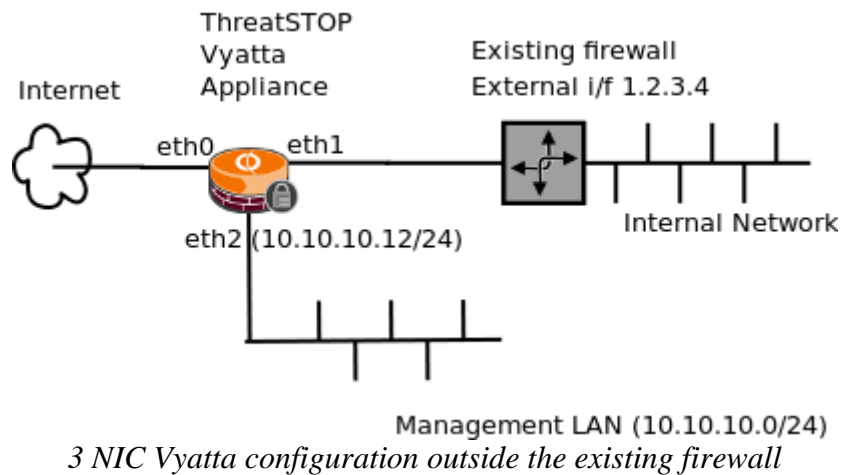


Sample Router Mode Configuration

In routed mode the Vyatta device acts as the gateway firewall/router between the Internet and your organization's internal networks as shown in the illustration above. In the ThreatSTOP scripts it is assumed to have a single external ethernet port connected to the Internet and some number of other ethernet ports on the internal network. If you have more than one external interface you will need to add the firewall rules created to the additional external interfaces manually. Our guides assume the presence of a management subnet in addition to other internal networks but this is merely a recommendation not a requirement.

Bridge Mode

The device may be set up using either two or three NICs and may be positioned either inside or outside the existing network firewall/router as shown in the three diagrams below.



Note that without some additional firewall rules to block external SSH access it is not recommended to deploy the 2 NIC configuration outside the firewall. Furthermore, it is in fact preferable for tracking down bots on your network to install the Vyatta box behind the firewall/router if it is doing NAT.

If, however, your firewall has multiple internal interfaces e.g. one for the intranet and another for DMZ servers etc. then you should place the Vyatta box outside the firewall. In this case you will have trouble identifying the IP addresses of any bots since they will be NATted by the firewall. The main advantage of having the Vyatta device outside the firewall is that it reduces the load on the firewall from inbound attacks since the Vyatta will stop traffic from the addresses known to ThreatSTOP which are probing your network and servers.