Set Virtual Server Firewall Rules

With OnApp you can set firewall rules for the network interfaces of virtual servers. There are two types of firewall rule:

- *ACCEPT* – defines the packets that will be accepted by the firewall
- *DROP* – define the packets that will be rejected by the firewall

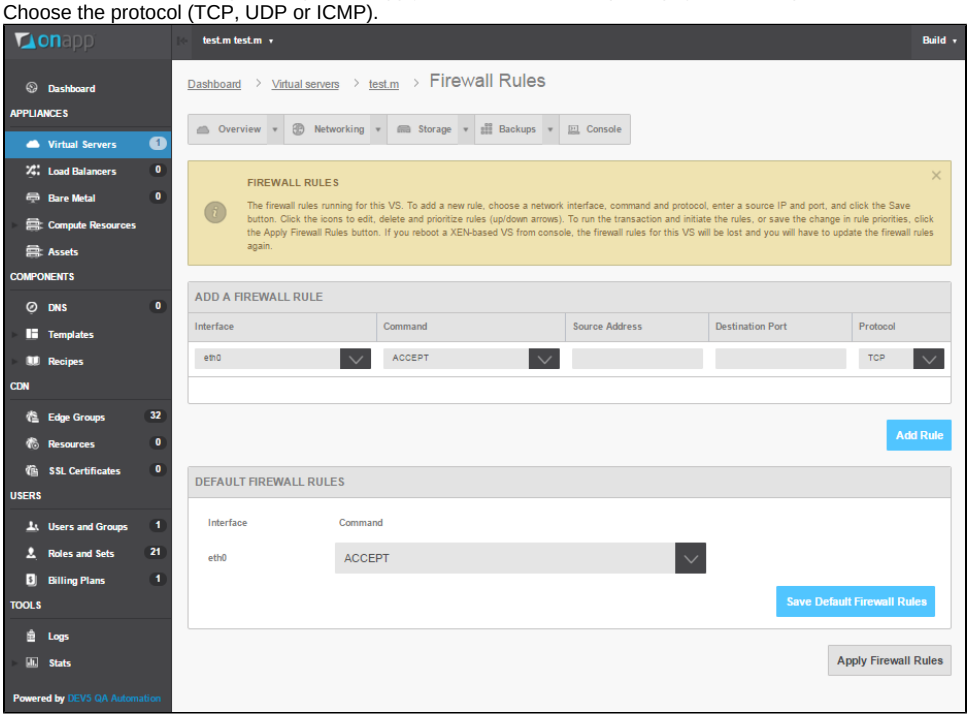
Ensure that the following permissions are enabled before setting firewall rules for your virtual server:

- Create own firewall rules
- Destroy own firewall rules
- Read own firewall rules
- Update own firewall rules
- Update own virtual server
- Read own virtual server

You can not apply firewall rules to virtual servers which are parts of a blueprint.

To configure a firewall rule:

1. Go to your Control Panel's **Virtual Servers** menu.
2. Click the label of the VS for which you want to configure a firewall rule.
3. Click the **Networking** tab, then click **Firewall.**
4. On the page that appears, set the following:
    a. Choose the network interface.
    b. Specify if the rule defines requests that should be accepted or dropped.
    c. Set the IP address for which this rule is active.
        - Leave the empty field to apply this rule to all IPs
        - Enter hyphen-separated IPs to apply the rule to an IP range (e.g. 192.168.1.1-192.168.1.10)
        - Enter the IPs with slash to apply the rule to CIDR (e.g. 192.168.1.1/24)
    d. Set the port for which this rule will is effective.
        - Leave the empty field to apply the rule to all ports
        - Enter colon-separated ports to apply the rule to a port range (e.g. 1024:1028)
        - Enter comma-separated ports to apply the rule to the list of ports (e.g. 80,443,21)
    e. Choose the protocol (TCP, UDP or ICMP).



5. Save the rule by clicking the **Add Rule** button. The rule will be saved in the UI, but the transaction won't be started until you click the Apply Firewall Rules button.
6. To start the transaction which runs firewall rules for a VS, click **Apply firewall rules** button.
7. Use **Up** and **Down** arrow buttons in the left column to change firewall rule position.
8. To edit or delete a firewall rule click the appropriate icon in the last column.

Example:

The Int1 ACCEPT 122.158.111.21 22 TCP firewall rule means that the Int1 network interface will accept all requests and packets addressed from 122.158.111.21 using the TCP protocol on port 22.
The Int2 DROP 122.158.111.21 22 UDP firewall rule means that the Int2 network interface will reject all requests and packets from 122.158.111.21 using the UDP protocol on port 22.

If you reboot a Xen-based VS from the console, the firewall rules for this VS will be lost, and you will need to update the firewall rules again.