How to use the VoipNow 5 built-in firewall

Applies to VoipNow 5.X.X!

Starting with VoipNow 5.X.X, a built-in firewall is delivered at installation. It provides a quick and easy way to restrict access to your server using the iptables tool.

Step-by-step guide

Once VoipNow is installed, a firewall script is delivered. The script will automatically detect the roles running on your node and apply only the corresponding access rules. The script also contains a built-in safety feature to ensure you don't lose access to your server.

Usage

```
# /usr/local/voipnow/admin/bin/voipnow_firewall
Usage: /usr/local/voipnow/admin/sbin/voipnow_firewall -o (apply|remove) [options]
                -h                              help
                -o|--operation=apply/remove     apply/remove set/unset firewall rules
                -d|--distributed                distributed
                -t|--testmode=true/false        true/false apply/remove firewal rules and a 3 minutes safety
net.
                -f|--force=true/false           true/false overwrites existing firewall when set to true
```

Usage example

This is how you run firewall with a SafetyNet.

```
# /usr/local/voipnow/admin/sbin/voipnow_firewall  -o apply -t true
Testmode enabled. If everything is working ok, please apply the firewall with /usr/local/voipnow/admin/sbin
/voipnow_firewall --operation=apply --testmode=false
Your previous firewall has been saved in /tmp/iptables.20463
```

SafetyNet will clean the firewall in 3 minutes if no action is taken.

To make the changes permanent, you need to run the following command.

```
# /usr/local/voipnow/admin/sbin/voipnow_firewall --operation=apply --testmode=false
```

This is how you disable the firewall.

```
# /usr/local/voipnow/admin/sbin/voipnow_firewall -o remove
Firewall rules have been disabled
```

How to set up the firewall trusted network

VoipNow's built-in firewall has a Trusted Network feature that will allow full access only to the networks set as trusted. This feature is efficient if you have local private networks that you use for storage, management, and/or monitoring.

To set a network as trusted, please follow the steps below. In our example, we'll allow access to 172.16.100.0/24.

1. Edit /etc/voipnow/local.conf and uncomment the TRUSTED_NET variable, replacing its value with your local network IP and netmask.

   ```
   # Access from these networks is always allowed (e.g. TRUSTED_NET 10.10.34.12/32 10.10.33.1/24)
   # TRUSTED_NET NETWORK/MASK
   ```

   To look like this:

```
# Access from these networks is always allowed (e.g. TRUSTED_NET 10.10.34.12/32 10.10.33.1/24)
TRUSTED_NET 172.16.100.0/24
```

2. Then execute the following script.

```
# /usr/local/voipnow/admin/sbin/voipnow_firewall -o apply -t false
```

How to set up the firewall on VoipNow Distributed Infrastructure

Voipnow firewall also works on VoipNow Distributed Infrastructure, but requires reapplying firewall rules on each node every time you add new VoipNow Nodes.

After changing the infrastructure in the web interface from single node to distributed, you need to reapply the firewall on IC using the following command:

```
# /usr/local/voipnow/admin/bin/voipnow_firewall -o apply -d -t false
```

After successfully running this command, you need to clean SafetyNet and apply the firewall with the following command.

```
# /usr/local/voipnow/admin/bin/voipnow_firewall -o apply -d -t false -f true
```

Make sure to review the firewall and block access to MySQL, Elasticsearch, HubRing from external clients. Access to databases must be permitted only from Voipnow nodes.

Every time you add a new node, you must run the following command on all the other nodes.

```
# /usr/local/voipnow/admin/bin/voipnow_firewall -o apply -d -t false -f true
```

Custom firewall rules

VoipNow firewall allows you to add custom firewall rules. You can add them to `/etc/voipnow/firewall.conf`

Once the firewall rules are created, the script will be executed like any shell script. However, this will happen before the DROP rules are added at the end of INPUT chain.

If you want to open some custom ports, take the following example - we opened port 8000 in `/etc/voipnow/firewall.conf`

```
# iptables -A INPUT -p tcp --dport 8000 -j ACCEPT
```

Related articles

- How to use the VoipNow built-in firewall
- How to use the VoipNow 5 built-in firewall
- How to use VoipNow 3 behind a firewall