Settings

Configuration

1. Run *Network configuration* in Menu **System**. Make sure you assign the correct red interface which is passed to the vm from the physical Server.
2. *Edit hosts* in Menu **Network**. Add all hosts with static IPs here.
3. *DHCP server* in Menu **Services**. Make sure all interfaces are off, and refer to DHCP Server - dnsmasq
4. Setup *Dynamic DNS* in Menu **Services**.
5. Click *Time server* and edit time zone.
6. Enable *Intrusion prevention* in Menu **Services**.
7. Setup *Port forwarding / NAT* in Menu **Firewall**. Add all ports you need to forward traffic to the respective machine, including HTTP(80) and HTTPS(443) to the web server. Make sure receiving machines such as NAS are configured correctly to access the internet.
8. Disable the Outgoing firewall in *Outgoing traffic*.

SSH Server

You need to enable the SSH Server to be able to login remotely without password.

1. run ssh-keygen on your host
2. copy the id_rsa.pub file to a USB stick, then attach the stick to the box, or use SCP file transfer
3. copy the host's id_rsa.pub file to /root/.ssh/authorized_keys
4. in the box' web interface, set Allow public key based authentication only in *SSH access* in Menu **System**

Phishtank

You might want to disable phishtank to avoid false positives, for example on www.google.com

1. Modify the script which downloads the malware definitions from phishtank, add the following before the script code:

   ```
   vim /usr/local/bin/getblackholedns
   import sys
   sys.exit(0)
   ```

   The script normally gets invoked once a day through an entry in /etc/anacron.daily. Removing that entry does not help, as it is reestablished after a reboot.

2. Delete the malware definitions file, or modify the file to avoid the false positives:

   ```
   rm /var/signatures/dnsmasq/phishtank.csv
   ```

3. Remove the conf file for dnsmasq. This file will be overwritten at next reboot, but because of

the missing phishtank.csv it will be empty:

```
rm /var/signatures/dnsmasq/blackholedns.conf
```

Firewall (iptables)

Check whether the firewall is set and hit on a specific port with:

```
iptables -t nat -L -v -n
```

Links

- Administrative Guide
- Port Forwarding Tester

From:
https://wiki.condrau.com/ - **Bernard's Wiki**

Permanent link:
https://wiki.condrau.com/efw:settings?rev=1596730486

Last update: **2020/08/06 23:14**