OpenVPN Bridges

Enable Packet forwarding for IPv4

- The machine running CoovaChilli will act as a router and thus needs to be configured as such.
- This means that the IP packets needs to be **forwarded** from one interface to the other.
- Edit the **/etc/sysctl.conf**.
- Find and uncomment **net.ipv4.ip_forward=1** line.

Building and Installing Coova Chilli

- The version of CoovaChilli is 1.6 as of this writing.
- We will download and build the .deb package from source.
- First ensure the required packages to build the .deb package are installed.

```
sudo apt-get install build-essential libssl-dev libjson-c-dev gengetopt
sudo apt install devscripts debhelper
```

- Download the release **1.6**'s .tar.gz file of the source here:
  https://github.com/coova/coova-chilli/releases
- Before we can build the package, we have to remove a dependency (hasrl) specified in the Debian control file.
- This dependency is not required and including it causes trouble when you want to install the package.

```
# If you downloaded with wget
tar -xzvf 1.6.tar.gz
# If you downloaded with the browser
tar -xzvf coova-chilli-1.6.tar.gz
cd coova-chilli-1.6/

vi debian/control
#Look for this part
#------
#Depends:
# ${shlibs:Depends},
# iptables,
# haserl,
# adduser,
#------
#------ CHANGE TO THIS (remove haserl as a dependency)
#------
#Depends:
# ${shlibs:Depends},
# iptables,
# adduser,
#-----

debuild -i -us -uc -b
cd ..
```

```
sudo dpkg --install coova-chilli_1.6_amd64.deb
```

- From the output of the dpkg command you will see that CoovaChilli is by default disabled. In the next section we will configure it to become a working entity.

```
Selecting previously unselected package coova-chilli.
(Reading database ... 125842 files and directories currently installed.)
Preparing to unpack coova-chilli_1.6_amd64.deb ...
Unpacking coova-chilli (1.6) ...
Setting up coova-chilli (1.6) ...
Chilli default off. Look at /etc/default/chilli
Processing triggers for libc-bin (2.31-0ubuntu9.2) ...
Processing triggers for systemd (245.4-4ubuntu3.6) ...
Processing triggers for man-db (2.9.1-1) ...
```

Configuring Coova Chilli

Enable CoovaChilli

- Edit the following file

```
sudo vi /etc/default/chilli
```

- Change it to look like this

```
START_CHILLI=1
CONFFILE="/etc/chilli.conf"
HS_USER="chilli"
```

- Save the file.

Create the main config file

- Create a file called **/etc/chilli/config** and use the following as reference:

/etc/chilli/config

```
HS_WANIF=eth0               # WAN Interface toward the Internet
HS_DNS1=4.4.4.4
HS_DNS2=8.8.8.8
HS_RADIUS=164.160.89.129
HS_RADIUS2=164.160.89.129
HS_RADSECRET=testing123     # Set to be your RADIUS shared secret
HS_UAMSECRET=greatsecret     # Set to be your UAM secret
HS_UAMALIASNAME=chilli
HS_UAMSERVER=$HS_UAMLISTEN
HS_UAMFORMAT=https://cloud.radiusdesk.com/cake4/rd_cake/dynamic-
details/chilli-browser-detect/
HS_UAMHOMEPAGE=http://\$HS_UAMLISTEN:\$HS_UAMPORT/www/coova.html
HS_MODE=hotspot
HS_TYPE=coovachilli
```

```
HS_WWWDIR=/etc/chilli/www
HS_WWWBIN=/etc/chilli/wwwsh
HS_PROVIDER=Coova
HS_PROVIDER_LINK=http://coova.github.io/
HS_LOC_NAME="My HotSpot"            # WISPr Location Name and used in
portal
HS_UAMUISSL=on
HS_SSLKEYFILE=/etc/chilli/key.pem
HS_SSLCERTFILE=/etc/chilli/cert.pem
HS_UAMALIASNAME=uam
HS_DNS_DOMAIN=mesh-manager.com
HS_UAMUIPORT=4990
```

- Make sure you include the **key.pem** and **cert.pem** in order for SSL to work correct.
- You can use these from the MESHdesk firmware
- https://github.com/RADIUSdesk/openwrt-meshdesk/tree/main/MESHdesk/files/MESHdesk/captive_portals
- Create the VLAN config directories

```
#Here you will need **ifconfig** to be installed
sudo su
cd /etc/chilli
./newmulti.sh br0.101
./newmulti.sh br0.102
  * Create the three VLAN configs
./newmulti.sh br0.103
```

- Create the three VLAN configs

/etc/chilli/br0.101/config

```
HS_LANIF=br0.101              # WAN Interface toward the Internet
HS_NETWORK=10.101.0.0        # HotSpot Network (must include
HS_UAMLISTEN)
HS_NETMASK=255.255.0.0   # HotSpot Network Netmask
HS_UAMLISTEN=10.101.0.1  # HotSpot IP Address (on subscriber network)
HS_UAMPORT=3990              # HotSpot UAM Port (on subscriber network)
HS_UAMUIPORT=4990            # HotSpot UAM "UI" Port (on subscriber
network, for embedded portal)

HS_DYNIP=10.101.1.1
HS_DYNIP_MASK=255.255.0.0
HS_STATIP=10.101.0.1
HS_STATIP_MASK=255.255.255.0
# HS_DNS_DOMAIN=

HS_NASID=rd-vlan101
HS_SSID=rd-vlan101-ssid
```

/etc/chilli/br0.102/config

```
HS_LANIF=br0.102              # WAN Interface toward the Internet
HS_NETWORK=10.102.0.0        # HotSpot Network (must include
HS_UAMLISTEN)
HS_NETMASK=255.255.0.0    # HotSpot Network Netmask
HS_UAMLISTEN=10.102.0.1  # HotSpot IP Address (on subscriber network)
HS_UAMPORT=3991               # HotSpot UAM Port (on subscriber network)
HS_UAMUIPORT=4991             # HotSpot UAM "UI" Port (on subscriber
network, for embedded portal)

HS_DYNIP=10.102.1.1
HS_DYNIP_MASK=255.255.0.0
HS_STATIP=10.102.0.1
HS_STATIP_MASK=255.255.255.0
# HS_DNS_DOMAIN=

HS_NASID=rd-vlan102
HS_SSID=rd-vlan102-ssid
```

/etc/chilli/br0.103/config

```
HS_LANIF=br0.103              # WAN Interface toward the Internet
HS_NETWORK=10.103.0.0        # HotSpot Network (must include
HS_UAMLISTEN)
HS_NETMASK=255.255.0.0    # HotSpot Network Netmask
HS_UAMLISTEN=10.103.0.1  # HotSpot IP Address (on subscriber network)
HS_UAMPORT=3992               # HotSpot UAM Port (on subscriber network)
HS_UAMUIPORT=4992             # HotSpot UAM "UI" Port (on subscriber
network, for embedded portal)

HS_DYNIP=10.103.1.1
HS_DYNIP_MASK=255.255.0.0
HS_STATIP=10.103.0.1
HS_STATIP_MASK=255.255.255.0
# HS_DNS_DOMAIN=

HS_NASID=rd-vlan103
HS_SSID=rd-vlan103-ssid
```

Add NAT Support

- By default CoovaChilli does not do NAT between the two interfaces. We have to add NAT support during start-up in order to have a working system.

> ⊗   Failing to do this step will leave you with a broken system.

- Edit the /etc/init.d/chilli file and add the following:

```
test ${HS_ADMINTERVAL:-0} -gt 0 && {
    (crontab -l 2>&- | grep -v $0
        echo "*/$HS_ADMINTERVAL * * * * $0 radconfig"
        ) | crontab - 2>&-
}

#NAT mod
iptables -F POSTROUTING -t nat
iptables -I POSTROUTING -t nat -o $HS_WANIF -j MASQUERADE
# ---HEADS-UP--
#NOTE The $HS_WANIF dit not populate for some unknown reason so I had to do
#iptables -I POSTROUTING -t nat -o eth0 -j MASQUERADE
#END NAT mod

ifconfig $HS_LANIF 0.0.0.0
```

Test it out

- Restart CoovaChilli for the latest changes to be effected.

```
#This is required
systemctl disable chilli
#Now issue the following
sudo systemctl stop chilli
sudo systemctl status chilli
sudo systemctl start chilli
```

- Confirm it started fine

```
sudo systemctl status chilli

.......
● chilli.service - LSB: Start CoovaChilli daemon at boot time
   Loaded: loaded (/etc/init.d/chilli; generated)
   Active: active (running) since Sat 2022-06-11 03:05:26 UTC; 2s ago
     Docs: man:systemd-sysv-generator(8)
  Process: 7619 ExecStart=/etc/init.d/chilli start (code=exited,
status=0/SUCCES
    Tasks: 1 (limit: 1108)
   CGroup: /system.slice/chilli.service
           └─7706 /usr/sbin/chilli -c /etc/chilli.conf

Dec 21 03:05:26 osboxes systemd[1]: Started LSB: Start CoovaChilli daemon at
boo
Dec 21 03:05:26 osboxes chilli[7706]: PID 7706 saving options to
/var/run/chilli
Dec 21 03:05:26 osboxes chilli[7706]: PID 7706 loading binary options file
/var/
Dec 21 03:05:26 osboxes chilli[7706]: Loading modules
```

```
Dec 21 03:05:26 osboxes chilli[7706]: CoovaChilli 1.4. Copyright 2002-2005
Mondr
Dec 21 03:05:26 osboxes chilli[7706]: TX queue length set to 100
Dec 21 03:05:26 osboxes coova-chilli[7713]: PID 7713 loading binary options
file
Dec 21 03:05:26 osboxes coova-chilli[7713]: Loading modules
Dec 21 03:05:26 osboxes coova-chilli[7713]: USER root(0/0), GROUP root(0/0)
CHIL
Dec 21 03:05:26 osboxes coova-chilli[7713]: Running /etc/chilli/up.sh (0/0)
.......
```

- Reboot the system and make sure CoovaChilli started up fine

Startup sequence

- We need to make sure that CoovaChilli starts at the right time.
- The right time will be:
  - First we configure the bridges.
  - Then we start up OpenVPN tunnels.
  - Then we start up CoovaChilli.
- Disable the normal startup sequence of CoovaChilli

```
systemctl disable chilli
```

- Edit the **/etc/rc.local** file and add the following below the startup of OpenVPN

```
#Add the startup of OpenVPN
systemctl start openvpn@server_vlan_101
systemctl start openvpn@server_vlan_102
systemctl start openvpn@server_vlan_103

#Add the startup of CoovaChilli
systemctl start chilli

exit 0
```

- Reboot the system and make sure everything is up and running after the reboot.

System Checks

- To confirm the bridges are up along with the OpenVPN tunnels

```
root@localhost:/home/system# brctl show
bridge name  bridge id          STP enabled    interfaces
br0.101      8000.002222ffffff    no           eth1.101
                                               tap0
br0.102      8000.002222ffffff    no           eth1.102
                                               tap1
br0.103      8000.002222ffffff    no           eth1.103
                                               tap2
```

- To check if CoovaChilli started up fine:

```
ifconfig

....
tun0: flags=81<UP,POINTOPOINT,RUNNING>  mtu 1500
        inet 10.101.0.1  netmask 255.255.0.0  destination 10.101.0.1
        inet6 fe80::70ad:961c:836d:ea9  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen
100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 592 (592.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun1: flags=81<UP,POINTOPOINT,RUNNING>  mtu 1500
        inet 10.1.0.1  netmask 255.255.255.0  destination 10.1.0.1
        inet6 fe80::dfa6:b905:30f9:8478  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen
100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 592 (592.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun2: flags=81<UP,POINTOPOINT,RUNNING>  mtu 1500
        inet 10.1.0.1  netmask 255.255.255.0  destination 10.1.0.1
        inet6 fe80::c5e:ff84:c088:a947  prefixlen 64  scopeid 0x20<link>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen
100  (UNSPEC)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 10  bytes 592 (592.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

....
```

From:
https://www.radiusdesk.com/wiki/ - **RADIUSdesk**

Permanent link:
https://www.radiusdesk.com/wiki/technical/openvpn-bridges-prep-coova

Last update: **2024/01/16 10:46**