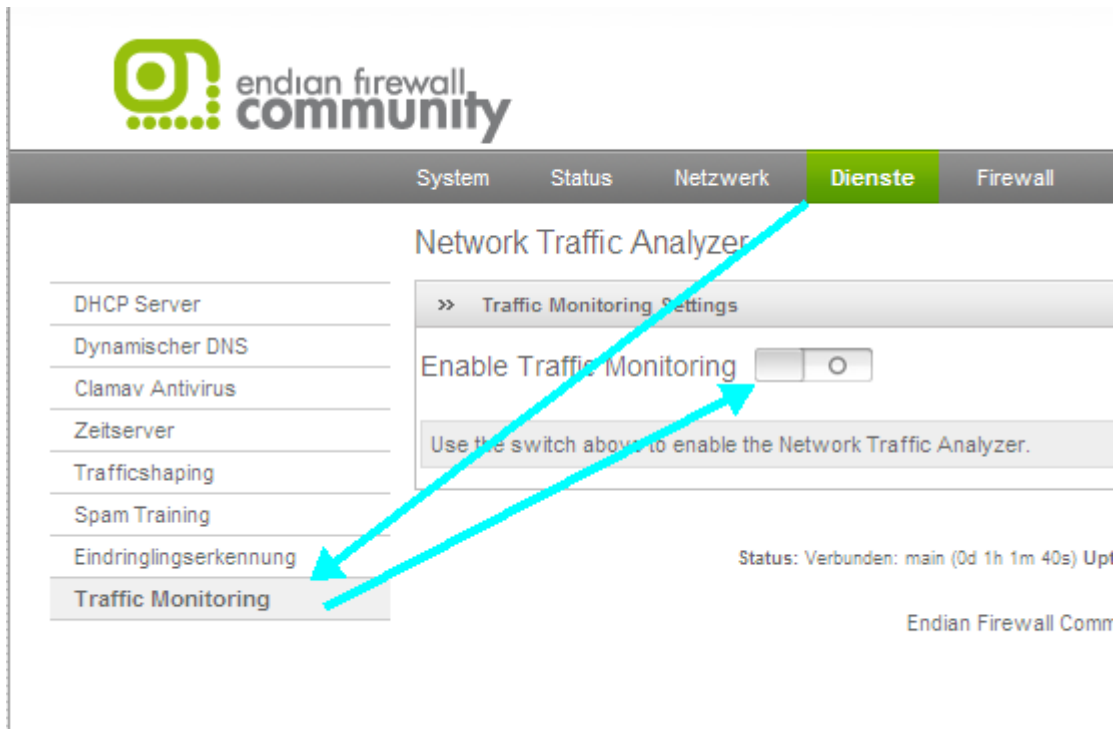


EFW Traffic Monitor Überwachung anderer Netzwerke Endian Community Firewall (EFW) testet on ver. 2.2RC2



Dieses Dokument erklärt wie man den Traffic Monitor einrichtet so das auch das Blaue oder Orange Netzwerk im Monitor auftaucht und man die Ansicht auf die Netze umschalten kann.

1. Melden Sie sich per Web Browser an Ihrer EFW an z.B. <https://184.10.10.1:10443>



Klicken Sie dort wie im Bild auf Dienste → Traffic Monitoring → Enable Traffic Monitoring
Der Dienst NTOP wird gestartet.

Zum Öffnen klicken Sie auf den im GUI stehenden Link

The Traffic Analyzer module is **active**: access to the [administration interface](#)

2. Über diese URL greifen sie auf den Traffic Monitor zu.

About **Summary** All Protocols IP Utils Plugins Admin

- Traffic
- Hosts
- Network Load**
- Network Flows



Global Traffic Statistics

| Network Interface(s) | Name | Device | Type | Speed | Sampling Rate | MTU | Header | Address | IPv6 Addresses |
|----------------------|---------------------------------|--------|----------|-------|---------------|------|--------|--------------|----------------|
| | br0 | br0 | Ethernet | | 0 | 1514 | 14 | 192.168.99.2 | |
| Local Domain Name | localdomain | | | | | | | | |
| Sampling Since | Wed Dec 10 11:38:02 2008 [4:36] | | | | | | | | |
| Active End Nodes | 20 | | | | | | | | |

Traffic Report for 'br0' [switch]

| | | |
|-------------------------|--------|--------|
| Dropped (libpcap) | 0.0% | 0 |
| Dropped (ntop) | 0.0% | 0 |
| Total Received (ntop) | 22,581 | |
| Total Packets Processed | 22,581 | |
| Unicast | 99.4% | 22,437 |
| Broadcast | 0.6% | 144 |
| Multicast | 0.0% | 0 |

The pie chart shows that 99.4% of the traffic is unicast, 0.6% is broadcast, and 0.0% is multicast. The broadcast slice is labeled 'Broadcast (1%)'.

Jedoch wird nur 1 Netzwerkkarte Überwacht.
Um dieses Abzuändern gehen Sie wie folgt vor.

Melden Sie sich an Ihrer EFW per WinSCP an.

Wie das funktioniert ist ebenfalls als Howto nach der Anmeldung im Forum unter www.efw-forum.de bei Downloads zu finden.

3. Bearbeiten Sie die Datei ntop die unter /etc/rc.d/init.d/ zu finden ist mit dem Editor der in WinSCP intrigiert ist.

```

#!/bin/bash
#
# ntop
#
# Source function library.
. /etc/init.d/functions

RETVAL=0

# See how we were called.

prog="ntop"
progdir="/usr/bin"
pidfile="/var/ntop/ntop.pid"
option="--user ntop --daemon --db-file-path /var/ntop --interface br0 --trace-level 3 --https-server 30

```

Tragen Sie hinter br0 welches Ihr grünes Netz darstellt Ihre von Ihnen gewünschte Netzwerke ein.

TIPP: Welche Karte welches Netz bedeutet erfahren Sie in Ihrer EFW Admin Oberfläche.

System **Status** Netzwerk Dienste Firewall Proxy VPN

Netzwerk Statusinformationen

[Schnittstellen](#) | [NIC status](#) | [Routingtabelleneinträge](#) | [ARP Tabelleneinträge](#)

- System-Status
- Netzwerkstatus**
- Systemdiagramm
- Netzwerkdiagramme
- Proxydiagramme
- Verbindungen
- OpenVPN Verbindungen
- SMTP Mailstatistik
- Mail Queue

```

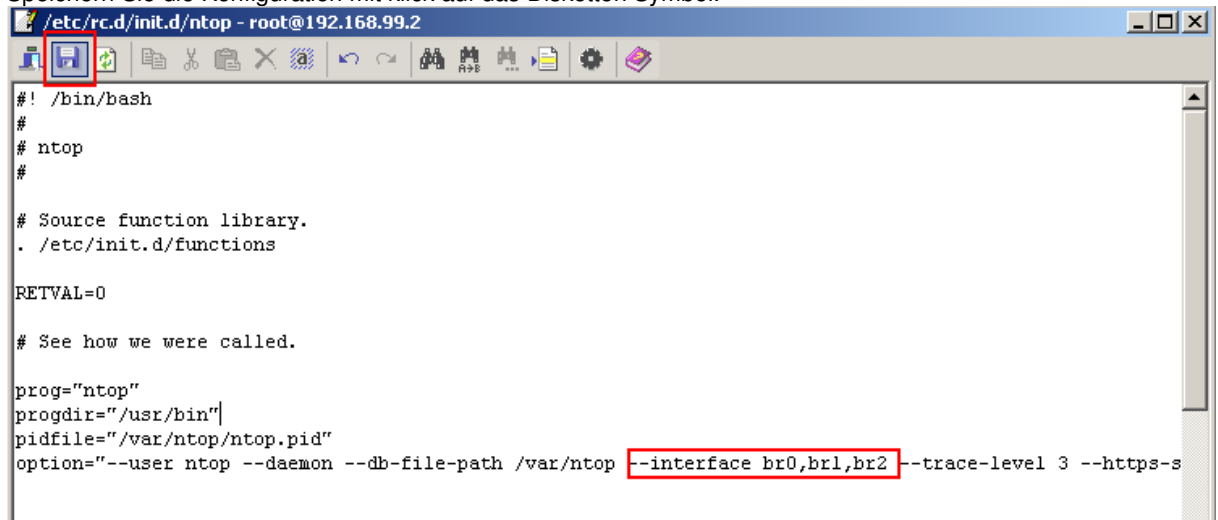
>> Schnittstellen
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   inet 127.0.0.1/8 scope host lo
   inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc
   link/ether 00:0c:29:1d:42:80 brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc
   link/ether 00:0c:29:1d:42:8a brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,PROMISC,UP,LOWER_UP> mtu 1500 qdisc
   link/ether 00:0c:29:1d:42:94 brd ff:ff:ff:ff:ff:ff
5: eth3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_f
   link/ether 00:0c:29:1d:42:9e brd ff:ff:ff:ff:ff:ff
   inet 1.1.1.1/24 brd 1.1.1.255 scope global eth3
   inet6 fe80::20c:29ff:fe1d:429e/64 scope link
       valid_lft forever preferred_lft forever
7: br0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
   link/ether 00:0c:29:1d:42:80 brd ff:ff:ff:ff:ff:ff
   inet 192.168.99.2/24 brd 192.168.99.255 scope global br0
8: br1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
   link/ether 00:0c:29:1d:42:8a brd ff:ff:ff:ff:ff:ff
   inet 10.10.10.1/24 brd 10.10.10.255 scope global br1
9: br2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue
   link/ether 00:0c:29:1d:42:94 brd ff:ff:ff:ff:ff:ff
   inet 11.11.11.1/24 brd 11.11.11.255 scope global br2

```

Es kann später auch noch bei DSL Verbindungen auch die ppp0 Schnittstelle hinzugefügt werden.

Merken Sie sich nun die br0,br1,br2 tragen Sie diese nun wie Oben unter Punkt 3 ein.
Wichtig ist das Sie die einzelnen Schnittstellen mit (,) Komma trennen

Speichern Sie die Konfiguration mit klick auf das Disketten Symbol.



```
#!/bin/bash
#
# ntop
#
# Source function library.
. /etc/init.d/functions

RETVAL=0

# See how we were called.

prog="ntop"
progdir="/usr/bin"
pidfile="/var/ntop/ntop.pid"
option="--user ntop --daemon --db-file-path /var/ntop --interface br0,br1,br2 --trace-level 3 --https-s
```

4. Jetzt müssen Sie noch den Dienst neustarten.

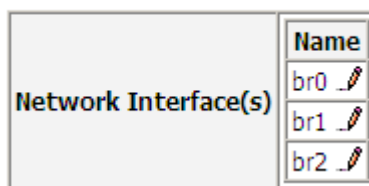
Entweder in der EFW Admin GUI mit klick auf  wird der Dienst beendet und mit einem erneuten klick auf  dieser wieder gestartet.

Alternativ können Sie auch via Console den Dienst mit

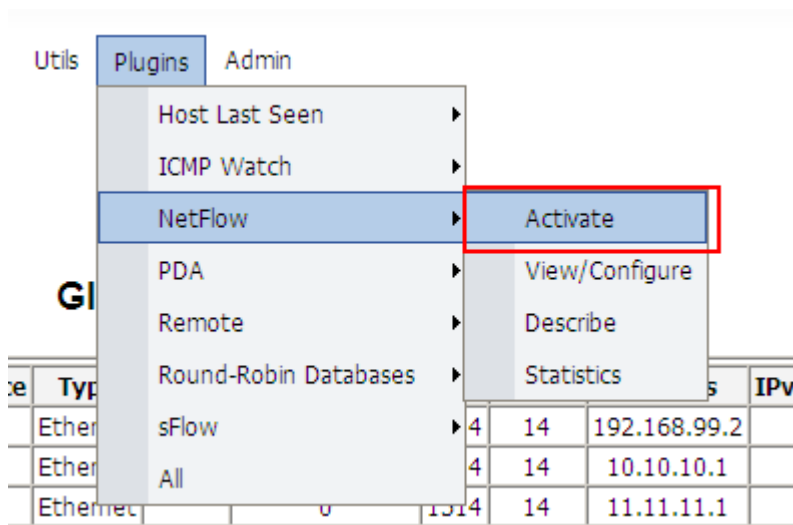
```
/etc/rc.d/init.d/ntop restart
```

Neustarten.

Wenn Sie nun die NTOP Oberfläche öffnen erscheinen Ihre gerade hinzugefügten Geräte.



5. Um jetzt noch die Interfaces umzuschalten klicken Sie auf



Und Aktivieren die das NetFlow Plugin mit klick auf „YES“

NetFlow

| View | Configure | Description | Version | Author | Active [click to toggle] |
|------|-----------|--|---------|--------|--------------------------|
| | NetFlow | This plugin is used to setup, activate and deactivate NetFlow support. ntop can both collect and receive NetFlow V1/V5/V7/V9 and IPFIX (draft) data. Received flow data is reported as a separate 'NIC' in the regular ntop reports. Remember to <i>switch</i> the reporting NIC. | 4.1 | L.Deri | No |

6. Jetzt können Sie die Infertaces umschalten.

Global Traffic Statistics

| Network Interface(s) | Name | Device | Type | Speed | Sampling Rate | MTU | Header | Address | IF |
|----------------------|------|--------|----------|-------|---------------|------|--------|--------------|----|
| | br0 | br0 | Ethernet | | 0 | 1514 | 14 | 192.168.99.2 | |
| | br1 | br1 | Ethernet | | 0 | 1514 | 14 | 10.10.10.1 | |
| | br2 | br2 | Ethernet | | 0 | 1514 | 14 | 11.11.11.1 | |

Local Domain Name:
 Sampling Since: Wed Dec 10 12:32
 Active End Nodes:

Traffic Report for 'br0' [switch]

7. Wählen Sie Ihr Interface aus und klicken Sie auf → „Switch NIC“

Available Network Interfaces:

- br0 [id=0]
- br1 [id=1]
- br2 [id=2]

Switch NIC

Reset