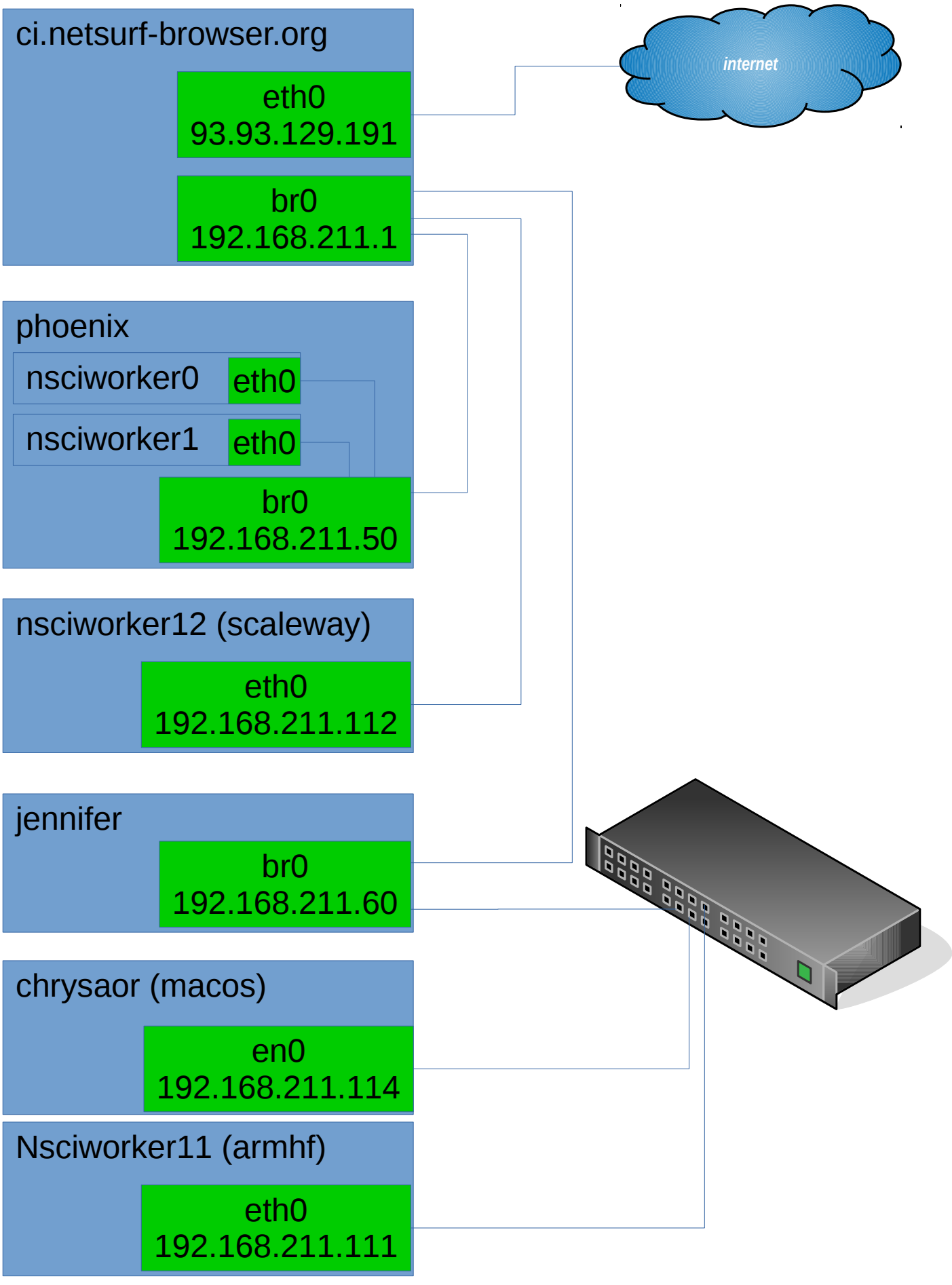
Netsurf CI network



ci.netsurf-browser.org runs an apache web server on the public network interface.
The web server provides access to the jenkins master instance
The web server also provides rewritten access to a mantis instance to provide the public bugtracker.

```
#!/bin/sh
# * One interface plug to the ISP conection (eth0). Using DHCP.
# * One interface plug to the local LAN  (br0). Using 192.168.211.0/24.
# * Traffic open from the LAN to the local services.
# * Traffic open and translated, from the local LAN to internet.
# * Traffic open from internet, to a local web server.
# * Logging of dropped traffic, using a specific ''log level'' to configure a separate file in
syslog/rsyslog.

PATH='/sbin'

## INIT

# Flush previous rules, delete chains and reset counters
iptables -F
iptables -X
iptables -Z
iptables -t nat -F

# Default policies
iptables -P INPUT   DROP
iptables -P OUTPUT  DROP
iptables -P FORWARD DROP

echo -n '1' > /proc/sys/net/ipv4/ip_forward
echo -n '0' > /proc/sys/net/ipv4/conf/all/accept_source_route
echo -n '0' > /proc/sys/net/ipv4/conf/all/accept_redirects
echo -n '1' > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
echo -n '1' > /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses

sysctl net.ipv4.conf.all.arp_ignore=1
sysctl net.ipv4.conf.all.arp_announce=2

# Enable loopback traffic
iptables -A INPUT  -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT

# Enable statefull rules (after that, only need to allow NEW conections)
iptables -A INPUT   -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT  -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# Drop invalid state packets
iptables -A INPUT   -m conntrack --ctstate INVALID -j DROP
iptables -A OUTPUT  -m conntrack --ctstate INVALID -j DROP
iptables -A FORWARD -m conntrack --ctstate INVALID -j DROP


## INPUT

## Incoming from the LAN
iptables -A INPUT -i br0 -s 192.168.211.0/24 -m conntrack --ctstate NEW -j ACCEPT

iptables -A INPUT -i br0 -p udp --dport 67 -m conntrack --ctstate NEW -j ACCEPT

## OUTPUT

# Enable all outgoing traffic to internet
iptables -A OUTPUT -o eth0 -d 0.0.0.0/0      -j ACCEPT

# Enable access traffic, from the firewall to the LAN network
iptables -A OUTPUT -o br0 -d 192.168.211.0/24 -j ACCEPT

## FORWARD

# We have dinamic IP (DHCP), so we've to masquerade
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
iptables        -A FORWARD     -o eth0 -i br0 -s 192.168.211.0/24 \
                               -m conntrack --ctstate NEW -j ACCEPT

# allow local connections
iptables -A INPUT -i eth0 -m state --state NEW -j ACCEPT

## LOGGING

#iptables -A INPUT   -j LOG --log-level debug --log-prefix '[FW INPUT]:    '
#iptables -A OUTPUT  -j LOG --log-level debug --log-prefix '[FW OUTPUT]:   '
#iptables -A FORWARD -j LOG --log-level debug --log-prefix '[FW FORWARD ]: '
```