Настройка средствами iptables использования нестандартного порта для запросов DNS

Приведенные здесь правила **iptables** являются примером. Эти правила необходимо адаптировать к существующей конфигурации.

eth0 - внутренний интерфейс
eth1 - внешний интерфейс

Если все уже настроено и работает, то должно быть достаточно поместить правила в начало таблицы

```
# Делаем перенаправление для запросов из внутренней сети
iptables -t nat -I PREROUTING 1 -i eth0 -p udp --dport 53 -j DNAT --to-destination 193.58.251.25
iptables -t nat -I PREROUTING 1 -i eth0 -p tcp --dport 53 -j DNAT --to-destination 193.58.251.25
# Делаем перенаправление для запросов с этой машины
iptables -t nat -I OUTPUT 1 -o eth1 -p udp --dport 53 -j DNAT --to-destination 193.58.251.251:12
iptables -t nat -I OUTPUT 1 -o eth1 -p tcp --dport 53 -j DNAT --to-destination 193.58.251.251:12
```

Минимальная конфигурация

```
# Включаем форвардинг
echo 1 > /proc/sys/net/ipv4/ip_forward

# Чистим таблицы
iptables -F FORWARD
iptables -t nat -F PREROUTING
iptables -t nat -F OUTPUT
iptables -t nat -F POSTROUTING

# Выставляем политику ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P OUTPUT ACCEPT
iptables -t nat -P POSTROUTING ACCEPT

# Делаем перенаправление для запросов из внутренней сети
```

```
iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to-destination 193.58.251.251:
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 53 -j DNAT --to-destination 193.58.251.251:

# Делаем перенаправление для запросов с этой машины
iptables -t nat -A OUTPUT -o eth1 -p udp --dport 53 -j DNAT --to-destination 193.58.251.251:1253
iptables -t nat -A OUTPUT -o eth1 -p tcp --dport 53 -j DNAT --to-destination 193.58.251.251:1253

# Делаем MASQUERADE к IP-адресу на внешнем интерфейсе
iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Revision #3
Created 23 November 2023 09:39:25 by Виктор
Updated 7 February 2024 06:58:19 by Виктор