Примеры использования IPTables

Здесь приведены примеры использования IPTables.

Шлюз доступа в интернет

По умолчанию всё запрещено, действуют только разрешающие правила.

Технологии:

- Bacula
- Туннель IPIP
- OpenVPN
- Squid
- Zabbix

Интерфейсы:

- `LAN` - локальная сеть
- `WAN` - интернет
- `ITS` - сеть для терминальных серверов доступа в интернет

Структура файла:

- Переменные
- Инициализация
- Основные правила
- Трансляция
- Преобразование сетевых адресов (NAT)

Fix Me!

/etc/network/if-pre-up.d/iptables

```
#!/bin/sh -

#                                                                       Переменные
#=============================================================================
# Сетевые интерфейсы
LAN_IF=eth0
LAN=10.12.0.1
WAN_IF=eth2
WAN=192.168.0.2
WAN_White=БЕЛЫЙ_IP
ITS_IF=eth1
ITS=192.168.253.1

# Службы
DNS_WAN="8.8.8.8"
DNS_LAN_1="10.11.0.3,10.11.0.4,10.11.0.5,10.11.0.17,10.11.0.23"
DNS_LAN_2="10.12.0.1,10.12.0.5,10.12.0.10"
SSH_WAN="0.0.0.0/24"
SSH_LAN="10.12.0.6,10.12.0.201,10.11.0.10,10.11.0.12,10.11.0.15,10.11.0.16,10.11.0.114"
Bacula_SD=10.11.0.15
Bacula_FD=10.11.0.15
Zabbix_Server=10.12.0.201
SMTP_LAN_Clients="10.12.0.201"
SMTP_LAN_1="10.11.0.17,10.11.0.14,10.11.0.5"
SMTP_LAN_2="10.12.0.5,10.12.0.10"
```

```
# Приложения
Squid_LAN="10.12.0.5,10.12.0.6,10.12.0.7,10.12.0.8,10.12.0.10"
Squid_ITS="192.168.253.3"
SOCKS_LAN="10.12.0.201"
FTP_Clients="10.12.0.201,10.12.0.190,10.12.5.0/24"
HTTP_LAN="10.12.0.0/24,10.12.3.0/24,10.12.4.0/24,10.12.5.0/24,10.12.6.0/24"

OpenVPN_IF="tun1"

IPIP_IF="tun0"
IPIP_WAN_1=БЕЛЫЙ_IP_1
IPIP_LAN_1=10.12.254.10
IPIP_LAN_NET_1=10.11.0.0/24
IPIP_WAN_2=БЕЛЫЙ_IP_2
IPIP_LAN_2=10.12.254.9
IPIP_LAN_NET_2=10.12.0.0/24

Admin_LAN_1="10.11.0.10,10.11.0.12,10.11.0.16,10.11.0.114,10.11.0.4"
Admin_LAN_2="10.12.0.201"

WEBMAIL_LAN_1="10.11.0.3,10.11.0.14,10.11.0.5"
WEBMAIL_LAN_2="10.12.0.5,10.12.0.10"

LDAP_LAN_1="10.11.0.4,10.11.0.3,10.11.0.14,10.11.0.5"
LDAP_LAN_2="10.12.0.5,10.12.0.10"

#                                                                    Инициализация
=====================================================================
# Очистка таблиц
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X

# Применение политики по умолчанию
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
#=============================================================================

# Разрешаем LoopBack
iptables -A INPUT  -i "lo" -j ACCEPT
iptables -A OUTPUT -o "lo" -j ACCEPT
# Разрешаем исходящие соединения с шлюза и входяшие по установленным исходящим (Для всех)
#iptables -A INPUT  -m state --state ESTABLISHED,RELATED -j ACCEPT
#iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# Разрешаем исходящие соединения с шлюза и входяшие по установленным исходящим (WAN)
iptables -A INPUT -i $WAN_IF -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -o $WAN_IF -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
# Только для группы proxy
iptables -A OUTPUT -o $WAN_IF -m state --state NEW,ESTABLISHED,RELATED -m owner --gid-
owner proxy -j ACCEPT

#ICMP LAN
iptables -A INPUT -p icmp -d $LAN -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp -s $LAN -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

#ICMP WAN
iptables -A INPUT -p icmp -d $WAN -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp -s $WAN -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -p icmp -d $WAN_White -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A OUTPUT -p icmp -s $WAN_White -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT

# ICMP ITS
iptables -A INPUT -p icmp -d $ITS -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -A OUTPUT -p icmp -s $ITS -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

# ICMP IPIP
iptables -A INPUT -p icmp -d $IPIP_LAN_1 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A OUTPUT -p icmp -s $IPIP_LAN_1 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A INPUT -p icmp -d $IPIP_LAN_2 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A OUTPUT -p icmp -s $IPIP_LAN_2 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT

# DNS WAN servers
iptables -A INPUT -p udp -i $WAN_IF -s $DNS_WAN --sport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o $WAN_IF -d $DNS_WAN --dport 53 -j ACCEPT

# DNS LAN Servers
iptables -A INPUT -p udp -i $LAN_IF -s $DNS_LAN_2 --sport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o $LAN_IF -d $DNS_LAN_2 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF -s $DNS_LAN_2 --sport 53 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $DNS_LAN_2 --dport 53 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF -s $DNS_LAN_2 --dport 53 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $DNS_LAN_2 --sport 53 -j ACCEPT

# DNS LAN Clients
iptables -A INPUT -p udp -i $LAN_IF --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o $LAN_IF --sport 53 -j ACCEPT

# DNS ITS Clients
iptables -A INPUT -p udp -i $ITS_IF --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o $ITS_IF --sport 53 -j ACCEPT
# DNS OpenVPN
iptables -A INPUT -p udp -i $OpenVPN_IF --dport 53 -j ACCEPT
iptables -A OUTPUT -p udp -o $OpenVPN_IF --sport 53 -j ACCEPT

# DHCP
iptables -A INPUT -p udp -i $LAN_IF --sport 67 -j ACCEPT
iptables -A OUTPUT -p udp -o $LAN_IF --sport 67 -j ACCEPT

# NTP
iptables -A INPUT -p udp -i $LAN_IF --dport 123 -j ACCEPT
iptables -A OUTPUT -p udp -o $LAN_IF --sport 123 -j ACCEPT
iptables -A OUTPUT -p udp -o $WAN_IF --dport 123 -j ACCEPT

# HTTP
iptables -A INPUT -p tcp -i $LAN_IF -s $HTTP_LAN --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $HTTP_LAN --sport 80 -j ACCEPT

# HTTP WEBMAIL
iptables -A INPUT -p tcp -i $LAN_IF -s $Admin_LAN_1 --dport 8080 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $Admin_LAN_1 --sport 8080 -j ACCEPT

# APCUPSd
iptables -A INPUT -p tcp -i $LAN_IF -s $HTTP_LAN --dport 3551 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $HTTP_LAN --sport 3551 -j ACCEPT

# SSH LAN
```

```
iptables -A INPUT -p tcp -i $LAN_IF -s $SSH_LAN --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $SSH_LAN --sport 22 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF -s $SSH_LAN --sport 22 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $SSH_LAN --dport 22 -j ACCEPT

# SSH WAN
if [ $SSH_WAN ]; then
    iptables -A INPUT -p tcp -i $WAN_IF -s $SSH_WAN --dport 22 -j ACCEPT;
    iptables -A OUTPUT -p tcp -o $WAN_IF -d $SSH_WAN --sport 22 -j ACCEPT;
fi

# FTP LAN
iptables -A INPUT -p tcp -i $LAN_IF -s $FTP_Clients --dport 21 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $FTP_Clients --sport 21 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF -s $FTP_Clients --dport 65299:65534 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $FTP_Clients --sport 65299:65534 -j ACCEPT
# FTP WAN
iptables -A INPUT -p tcp -i $WAN_IF --dport 21 -j ACCEPT
iptables -A OUTPUT -p tcp -o $WAN_IF --sport 21 -j ACCEPT
iptables -A INPUT -p tcp -i $WAN_IF --dport 65299:65534 -j ACCEPT
iptables -A OUTPUT -p tcp -o $WAN_IF --sport 65299:65534 -j ACCEPT

# Squid LAN
iptables -A INPUT -p tcp -i $LAN_IF -s $Squid_LAN --dport 3128 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $Squid_LAN --sport 3128 -j ACCEPT

# Squid ITS
if [ $Squid_ITS ]; then
    iptables -A INPUT -p tcp -i $ITS_IF -s $Squid_ITS --dport 3128 -j ACCEPT
    iptables -A OUTPUT -p tcp -o $ITS_IF -d $Squid_ITS --sport 3128 -j ACCEPT
fi
# SOCKS proxy LAN
if [ $SOCKS_LAN ]; then
    iptables -A INPUT -p tcp -i $LAN_IF -s $SOCKS_LAN --dport 1080 -j ACCEPT
    iptables -A OUTPUT -p tcp -o $LAN_IF -d $SOCKS_LAN --sport 1080 -j ACCEPT
fi

# OpenVPN
iptables -A INPUT -p udp -i $WAN_IF --dport 1194 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p udp -o $WAN_IF --sport 1194 -j ACCEPT;

# SMTP WAN Вход
iptables -A INPUT -p tcp -i $WAN_IF --dport 25 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp -o $WAN_IF --sport 25 -j ACCEPT;

# SMTP WAN Выход (разрешен выход на любые внешние серверы  SMTP)
iptables -A INPUT -p tcp -i $WAN_IF --sport 25 -m state --state NEW -j ACCEPT
iptables -A OUTPUT -p tcp -o $WAN_IF --dport 25 -j ACCEPT;

# SMTP LAN Серверы
iptables -A INPUT -p tcp -i $LAN_IF -s $SMTP_LAN_1 --sport 25 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $SMTP_LAN_1 --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF -s $SMTP_LAN_1 --dport 25 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $SMTP_LAN_1 --sport 25 -j ACCEPT

# SMTP LAN Клиенты
iptables -A INPUT -p tcp -i $LAN_IF -s $SMTP_LAN_Clients --dport 25 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $SMTP_LAN_Clients --sport 25 -j ACCEPT

# Bacula
iptables -A INPUT -p tcp -i $LAN_IF -s $Bacula_FD --dport 9102 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $Bacula_FD --sport 9102 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF -s $Bacula_SD --sport 9103 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $Bacula_SD --dport 9103 -j ACCEPT
```

```
# Zabbix Server
iptables -A INPUT -p tcp -i $LAN_IF -s $Zabbix_Server --sport 10050:10051 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF -s $Zabbix_Server --dport 10050:10051 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $Zabbix_Server --sport 10050:10051 -j ACCEPT
iptables -A OUTPUT -p tcp -o $LAN_IF -d $Zabbix_Server --dport 10050:10051 -j ACCEPT

# ------------------------- IPIP ---------------------------------
# IPIP WAN
iptables -A OUTPUT -s $IPIP_WAN_2 -d $IPIP_WAN_1 -j ACCEPT
# IPIP LAN
iptables -A INPUT -s $IPIP_LAN_1 -d $IPIP_LAN_2 -j ACCEPT
iptables -A OUTPUT -s $IPIP_LAN_2 -d $IPIP_LAN_1 -j ACCEPT
iptables -A INPUT -s $IPIP_LAN_2 -d $IPIP_LAN_1 -j ACCEPT
iptables -A OUTPUT -s $IPIP_LAN_1 -d $IPIP_LAN_2 -j ACCEPT

# IPIP ICMP
iptables -A INPUT -p icmp -d $IPIP_LAN_NET_1 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A OUTPUT -p icmp -s $IPIP_LAN_NET_2 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A INPUT -p icmp -d $IPIP_LAN_NET_1 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT
iptables -A OUTPUT -p icmp -s $IPIP_LAN_NET_2 -m state --state NEW,ESTABLISHED,RELATED -j
ACCEPT

# Трансляция ============================================================
# Разрешаем обратную трансляцию для установленных соединений (Для всех)
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
# IPIP
# Admin (2) -> Admin (1) RDP
iptables -A FORWARD -i $LAN_IF -s $Admin_LAN_2 -o $IPIP_IF -d $Admin_LAN_1 -p tcp --dport
3389 --syn -j ACCEPT
iptables -A FORWARD -i $LAN_IF -s $Admin_LAN_2 -o $IPIP_IF -d $Admin_LAN_1 -p tcp --dport
21 --syn -j ACCEPT
iptables -A FORWARD -i $LAN_IF -s $Admin_LAN_2 -o $IPIP_IF -d $Admin_LAN_1 -p tcp --dport
65299:65534 --syn -j ACCEPT

# Admin (1) -> Admin (2) RDP RAdmin FTP
iptables -A FORWARD -i $IPIP_IF -s $Admin_LAN_1 -o $LAN_IF -d $Admin_LAN_2 -p tcp --dport
3389 --syn -j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $Admin_LAN_1 -o $LAN_IF -d $Admin_LAN_2 -p tcp --dport
4899 --syn -j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $Admin_LAN_1 -o $LAN_IF -d $Admin_LAN_2 -p tcp --dport
21 --syn -j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $Admin_LAN_1 -o $LAN_IF -d $Admin_LAN_2 -p tcp --dport
65299:65534 --syn -j ACCEPT

# IPIP SMTP LAN
iptables -A FORWARD -i $IPIP_IF -s $IPIP_LAN_NET_1 -o $LAN_IF -d $SMTP_LAN_2 -p tcp --
dport 25 --syn -j ACCEPT
iptables -A FORWARD -i $LAN_IF -s $IPIP_LAN_NET_2 -o $IPIP_IF -d $SMTP_LAN_1 -p tcp --
dport 25 --syn -j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $IPIP_LAN_1 -o $LAN_IF -d $SMTP_LAN_2 -p tcp --dport
25 --syn -j ACCEPT

# IPIP SMTP Gate
iptables -A INPUT -p tcp -i $IPIP_IF -s $SMTP_LAN_2 --sport 25 -j ACCEPT
iptables -A OUTPUT -p tcp -o $IPIP_IF -d $SMTP_LAN_2 --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -i $IPIP_IF -s $SMTP_LAN_2 --dport 25 -j ACCEPT
iptables -A OUTPUT -p tcp -o $IPIP_IF -d $SMTP_LAN_2 --sport 25 -j ACCEPT

# IPIP DNS 1 -> 2
iptables -A FORWARD -i $IPIP_IF -s $DNS_LAN_1 -o $LAN_IF -d $DNS_LAN_2 -p udp --dport 53
```

```
-j ACCEPT
iptables -A FORWARD -i $LAN_IF -s $DNS_LAN_2 -o $IPIP_IF -d $DNS_LAN_1 -p udp --dport 53
-j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $DNS_LAN_1 -o $LAN_IF -d $DNS_LAN_2 -p tcp --dport 53
-j ACCEPT
iptables -A FORWARD -i $LAN_IF -s $DNS_LAN_2 -o $IPIP_IF -d $DNS_LAN_1 -p tcp --dport 53
-j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $IPIP_LAN_1 -o $LAN_IF -d $DNS_LAN_2 -p udp --dport 53
-j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $IPIP_LAN_1 -o $LAN_IF -d $DNS_LAN_2 -p tcp --dport 53
-j ACCEPT

# IPIP DNS 2 -> 1
iptables -A INPUT  -s $DNS_LAN_2 -d $DNS_LAN_1 -p udp --dport 53 -j ACCEPT
iptables -A OUTPUT -s $DNS_LAN_1 -d $DNS_LAN_2 -p udp --sport 53 -j ACCEPT
iptables -A INPUT  -d $DNS_LAN_1 -s $DNS_LAN_2 -p tcp --dport 53 -j ACCEPT
iptables -A OUTPUT -s $DNS_LAN_1 -d $DNS_LAN_2 -p tcp --sport 53 -j ACCEPT

# IPIP HTTP WEBMAIL
iptables -A FORWARD -i $LAN_IF -s $IPIP_LAN_NET_2 -o $IPIP_IF -d $WEBMAIL_LAN_1 -p tcp --
dport 80 --syn -j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $IPIP_LAN_NET_1 -o $LAN_IF -d $WEBMAIL_LAN_2 -p tcp --
dport 80 --syn -j ACCEPT

# IPIP LDAP
iptables -A FORWARD -i $LAN_IF -s $IPIP_LAN_NET_2 -o $IPIP_IF -d $LDAP_LAN_1 -p tcp --
dport 389 --syn -j ACCEPT
iptables -A FORWARD -i $IPIP_IF -s $IPIP_LAN_NET_1 -o $LAN_IF -d $LDAP_LAN_2 -p tcp --
dport 389 --syn -j ACCEPT

# OpenVPN 01
iptables -A FORWARD -i $OpenVPN_IF -s 192.168.168.22 -o $LAN_IF -d 10.12.0.201 -p tcp --
dport 4899 --syn -j ACCEPT
iptables -A FORWARD -i $OpenVPN_IF -s 192.168.168.22 -o $LAN_IF -d 10.12.0.201 -p tcp --
dport 3389 --syn -j ACCEPT
iptables -A FORWARD -i $OpenVPN_IF -s 192.168.168.22 -o $LAN_IF -d 10.12.0.190 -p tcp --
dport 3389 --syn -j ACCEPT
# OpenVPN 02
iptables -A FORWARD -i $OpenVPN_IF -s 192.168.168.26 -o $LAN_IF -d 10.12.0.190 -p tcp --
dport 3389 --syn -j ACCEPT

# Преобразование сетевых адресов (NAT) -------------------------------------
# SNAT
iptables -A POSTROUTING -t nat -o $WAN_IF -j SNAT --to $WAN_White
#==============================================================================
```

Запрещающие правила

По умолчанию всё разрешено, действуют только запрещающие правила.

/etc/network/if-pre-up.d/iptables

```
#!/bin/sh -

iptables -F

LAN_IF="eth0"
SMTP_LAN="10.12.0.2,10.12.0.10"

# SMTP
```

```
iptables -A INPUT -p tcp -i $LAN_IF -s $SMTP_LAN --dport 25 -j ACCEPT
iptables -A INPUT -p tcp -i $LAN_IF --dport 25 -j REJECT

exit
```

http://sysadminmosaic.ru/examples/iptables

2020-08-25 09:21

