Полное руководство по работе с IPTABLES, Подробная энциклопедия с практическими примерами

1. Основные компоненты и принцип работы

Таблицы:

- **filter** (по умолчанию):
  - INPUT - управление входящими соединениями
  - OUTPUT - контроль исходящего трафика
  - FORWARD - обработка транзитных пакетов
- **nat**:
  - PREROUTING - преобразование перед маршрутизацией
  - POSTROUTING - преобразование после маршрутизации
- **mangle** - для специальной модификации пакетов

2. Базовые операции с IPTABLES

```
# Просмотр правил с нумерацией строк
iptables -L -n --line-numbers -v

# Очистка всех правил (осторожно!)
iptables -F && iptables -X
```

```
# Сохранение текущей конфигурации
iptables-save > /etc/iptables.conf

# Восстановление правил
iptables-restore < /etc/iptables.conf
```

3. Практические примеры использования

3.1. Базовая защита сервера

```
# Разрешаем локальный интерфейс
iptables -A INPUT -i lo -j ACCEPT

# Разрешаем установленные соединения
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# Открываем SSH только с доверенных IP
iptables -A INPUT -p tcp -s 192.168.1.100 --dport 22 -j ACCEPT

# Защита от SYN-флуда
iptables -A INPUT -p tcp --syn -m limit --limit 1/s -j ACCEPT
```

3.2. Настройка NAT и проброса портов

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

# Маскировка внутренней сети
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

# Проброс порта 80 на внутренний сервер
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 192.168.1.10:80
```

```
iptables -A FORWARD -p tcp -d 192.168.1.10 --dport 80 -j ACCEPT
```

4. Блокировка по географическому признаку

4.1. Установка и настройка ipset

```
apt install ipset  # Для Debian/Ubuntu
yum install ipset  # Для CentOS/RHEL

# Создаем набор для хранения IP-адресов
ipset create blocked_countries hash:net

# Добавляем правило блокировки
iptables -I INPUT -m set --match-set blocked_countries src -j DROP
```

4.2. Загрузка IP-диапазонов стран

```
# Создаем скрипт /usr/local/bin/update_countries.sh:
#!/bin/bash
COUNTRIES="cn ru"  # Коды стран для блокировки
TMP_SET=temp_countries

ipset create $TMP_SET hash:net

for country in $COUNTRIES; do
  wget -O $country.zone http://www.ipdeny.com/ipblocks/data/countries/$country.zone
  for ip in $(cat $country.zone); do ipset add $TMP_SET $ip; done
  rm -f $country.zone
done

ipset swap $TMP_SET blocked_countries
ipset destroy $TMP_SET
```

```
# Делаем исполняемым и запускаем
chmod +x /usr/local/bin/update_countries.sh
/usr/local/bin/update_countries.sh
```

4.3. Автоматическое обновление

```
# Добавляем в cron еженедельное обновление
echo "0 3 * * 1 /usr/local/bin/update_countries.sh" >> /etc/crontab
```

5. Мониторинг и отладка

```
# Просмотр статистики по правилам
iptables -L -n -v

# Логирование блокируемых пакетов
iptables -A INPUT -j LOG --log-prefix "BLOCKED: " --log-level 4

# Просмотр логов в реальном времени
tail -f /var/log/syslog | grep BLOCKED
```

> **Важные рекомендации**:
>
> 1. Всегда тестируйте правила на тестовом сервере
> 2. Имейте альтернативный доступ на случай ошибок
> 3. Регулярно обновляйте списки IP-адресов
> 4. Для сложных конфигураций используйте скрипты

Revision #1
Created 2026-11-19 13:04:30 UTC by Admin
Updated 2026-11-19 13:04:52 UTC by Admin