

Юрий Дмитришин <yuriy.dmitrishin@gmail.com>

**Использование PF для
фильтрации входящего и
исходящего трафика хостов ДМЗ**

OpenKyiv, 2009

Часто предполагают, что разрешение всего исходящего трафика, в отличие от входящего, не связано с риском, поэтому большинство сетевых администраторов не фильтруют исходящий сетевой трафик как рабочих станций, так и серверов. Далее рассматриваются проблемы, которые возникают при отсутствии фильтрации и показаны методы их устранения на примере использования межсетевого экрана OpenBSD PF. Предполагается, что локальная сеть защищена брандмауэром, а хосты, на которых запущены необходимые сетевые сервисы, расположены в демилитаризованной зоне.

Построение сети с использованием ДМЗ

ДМЗ (демитаризованная зона) – особый сегмент сети, находящийся между внешней сетью и экранированной локальной сетью (ЭЛС) и обеспечивающий дополнительный уровень информационной безопасности.

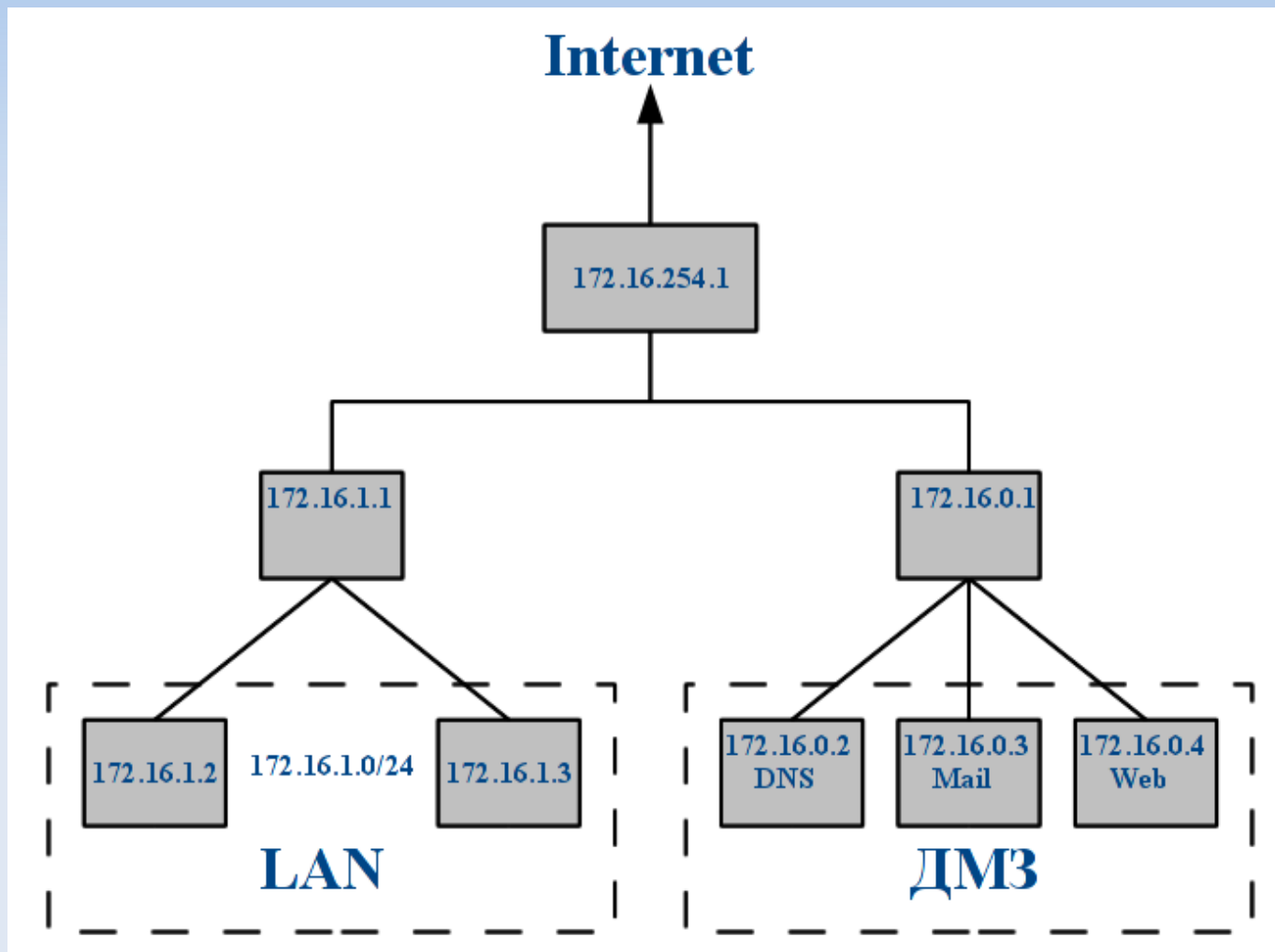
При таком дизайне прямая маршрутизация пакетов между хостами локальной и внешней сетей невозможна, поскольку все соединения между ЭЛС и внешней сетью проводятся через хосты, расположенные в ДМЗ.

Построение сети с использованием ДМЗ

При идеальном варианте используется 3 брандмауэра:

- 1) для контроля внутренней сети;
- 2) для контроля внешней сети;
- 3) для контроля ДМЗ.

Построение сети с использованием ДМЗ



Фильтровать исходящий трафик необходимо для предотвращения:

- 1) утечки конфиденциальной информации;
- 2) защиты от вирусов;
- 3) защиты от атак типа spoofing (ARP-, MAC-, TCP-, IP-, ICMP-);
- 4) защиты от атаки TCP-hijacking.

Методы фильтрации:

- 1) фильтрация по MAC-адресам;
- 2) фильтрация по IP-адресам и портам;
- 3) использование правил anti-spoof;
- 4) контроль за прохождением пакетов с SYN и ACK при установке флага SYN и включение модуляции;
- 5) запрет передачи определенных данных во внешнюю сеть.

Какие МСЭ используются в BSD-системах?

1. **PF** – МСЭ, разрабатываемый в рамках проекта OpenBSD.
2. **IPF** – не зависящий от ОС фильтр и преобразователь сетевых адресов, автором которого является Darren Reed.
3. **IPFW** – МСЭ, включенный в состав FreeBSD.

Почему PF?

У PF, в отличии от IPFW и IPF, есть:

- 1) простой синтаксис конфигурационного файла;
- 2) удобные элементы конфигурации: списки, таблицы, якоря;
- 3) возможность нормализации трафика (scrub);
- 4) возможность проксирования рукопожатия (synproxy);
- 5) возможность авторизации на шлюзе для обеспечения дополнительных возможностей;
- 6) наличие *pfsync* для использование совместно с CARP.

Конфигурационный файл РФ МСЭ ДМЗ

#####

Макросы

#####

Внутренний интерфейс

int = "fxp0"

Внешний интерфейс

ext = "fxp1"

DNS-сервер

DNS = "172.16.0.2"

Порты DNS-сервера

DNS_ports = "{ 53 }"

Mail-сервер

Mail = "172.16.0.3"

Порты Mail-сервера

Mail_ports = "{ 25, 143, 993 }"

Web-сервер

Web = "172.16.0.4"

Порты Web-сервера

Web_ports = "{ 80, 443 }"

Межсетевой экран, контролирующий доступ в интернет

Internet = "172.16.254.1"

Локальная сеть

LAN = "172.16.1.1"

Немаршрутизируемые адреса

NoRouteIPs = "{ 127.0.0.0/8, 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8 }"

Конфигурационный файл PF МСЭ ДМЗ

```
#####  
# Таблицы #  
#####
```

```
# Таблица содержит IP-адреса, которые подбирали пароли к ssh  
table <Bruteforce> persist
```

```
#####  
# Опции #  
#####
```

```
# Разрешенные типы ICMP-сообщений  
icmp_types="{ echoreq, unreachable }"
```

```
# Тип оптимизации  
set optimization normal
```

```
# Политика блокировки  
set block-policy drop
```

```
# Установка приоритетов  
set require-order yes
```

```
# Пропуск фильтрации на интерфейсе обратной петли  
set skip on lo0
```

```
# Протоколирование  
set loginterface $ext
```

Конфигурационный файл PF МСЭ ДМЗ

#####

Нормализация

#####

**# Нормализация всего входящего трафика
scrub in all**

#####

Трансляция

#####

**# Разрешить трансляцию для всех портов
nat on \$ext from \$int:network to any -> (\$ext)**

**# Перенаправление портов DNS-сервера
rdr on \$ext proto tcp from { \$LAN, \$Internet } to me port \$DNS_ports -> \$DNS
rdr on \$ext proto tcp from \$LAN to me port 22002 -> \$DNS port 22**

**# Перенаправление портов Mail-сервера
rdr on \$ext proto tcp from { \$LAN, \$Internet } to me port \$Mail_ports -> \$Mail
rdr on \$ext proto tcp from \$LAN to me port 22003 -> \$Mail port 22**

**# Перенаправление портов Web-сервера
rdr on \$ext proto tcp from { \$LAN, \$Internet } to me port \$Web_ports -> \$Web
rdr on \$ext proto tcp from \$LAN to me port 22004 -> \$Web port 22**

Конфигурационный файл PF МСЭ ДМЗ

```
#####  
# Фильтрация #  
#####
```

```
# Блокировать весь входящий и исходящий трафик  
block all
```

```
# Использовать антиспуфинг на внутреннем и внешнем интерфейсах  
antispoof log quick for { $int, $ext } inet
```

```
# Блокировать адреса, не находящиеся в таблице маршрутизации  
block in quick from urpf-failed label uRPF
```

```
# Блокировать доступ из-вне из немаршрутизируемых адресов  
block in quick on $ext from $NoRouteIPs to any  
block out quick on $ext from any to $NoRouteIPs
```

```
# Разрешить весь трафик из локальной сети к брандмауэру и обратно  
pass in on $int from $int:network to any keep state  
pass out on $int from any to $int:network keep state
```

```
# Блокировать доступ ко внутреннему интерфейсу всем, кроме подсети 172.16.0.0/24  
block drop in log quick on $int from !$int:network to any
```

```
# Блокировать доступ ко внешнему интерфейсу всем, кроме МСЭ внутренней  
# и внешней сетей  
block drop in log quick on $ext from {! $LAN, ! $Internet} to any
```

```
# Блокировать доступ всем из таблицы "Bruteforce"  
block drop log quick from <Bruteforce>
```

Конфигурационный файл PF МСЭ ДМЗ

Доступ по ssh к МСЭ DMZ

```
pass in on $ext proto tcp from { $LAN, $Internet } to $ext port ssh queue ( qssh, qack ) \  
    synproxy state ( max-src-conn-rate 1/120, overload <Bruteforce> flush global )
```

Доступ по ssh к DNS-серверу

```
pass in on $ext proto tcp from { $LAN, $Internet } to $DNS port ssh queue ( qssh, qack ) \  
    synproxy state ( max-src-conn-rate 1/120, overload <Bruteforce> flush global )
```

Доступ по ssh к Mail-серверу

```
pass in on $ext proto tcp from { $LAN, $Internet } to $Mail port ssh queue ( qssh, qack ) \  
    synproxy state ( max-src-conn-rate 1/120, overload <Bruteforce> flush global )
```

Доступ по ssh к Web-серверу

```
pass in on $ext proto tcp from { $LAN, $Internet } to $Web port ssh queue ( qssh, qack ) \  
    synproxy state ( max-src-conn-rate 1/120, overload <Bruteforce> flush global )
```

Пропускать пакеты для DNS-сервера

```
pass in on $ext proto tcp from { $LAN, $Internet } to $DNS port $DNS_ports flags S/SA synproxy state
```

Пропускать пакеты для Mail-сервера

```
pass in on $ext proto tcp from { $LAN, $Internet } to $Mail port $Mail_ports flags S/SA synproxy state
```

Пропускать пакеты для Web-сервера

```
pass in on $ext proto tcp from { $LAN, $Internet } to $Web port $Web_ports flags S/SA synproxy state
```

Конфигурация других МСЭ

Для МСЭ "LAN" и "Internet" необходимо также выполнить фильтрацию трафика средствами PF для обеспечения максимальной безопасности. Политика пакетных фильтров при этом должна удовлетворять следующие критерии:

- 1) блокировать трафик со всех IP адресов;
- 2) разрешить прохождение трафика с адресов хостов ДМЗ и к ним, причем должно выполняться соответствие IP-адреса и порта для каждого хоста.

Выводы

Большой ошибкой является наличие правила типа "разрешать весь исходящий трафик". Правильная фильтрация исходящего трафика хостов ДМЗ предотвращает значительное число распространенных сетевых атак, уменьшает риск заражения сети компьютерными вирусами и помогает снизить вероятность утечки конфиденциальной информации. Межсетевой экран PF, разработанный в рамках проекта OpenBSD, обладает гибким синтакисом, большой функциональностью и удобством в настройке.