УДК 004.422.8.056.5

А.С. Шабуров, Р.Б. Рашевский

Пермский национальный исследовательский политехнический университет, Пермь, Россия

РЕАЛИЗАЦИЯ ОТКАЗОУСТОЙЧИВОГО РАСПРЕДЕЛЕННОГО МЕЖСЕТЕВОГО ЭКРАНА

Рассматривается возможность реализации отказоустойчивого распределенного межсетевого экрана на основе программы PacketFilter и операционной системы FreeBSD

Ключевые слова: межсетевой экран, отказоустойчивость, резервирование, сетевая атака

A.S. Shaburov, R.B. Rashevskiy

Perm National Research Polytechnic University, Perm, Russian Federation

IMPLEMENTATION OF FAULT-TOLERANT DISTRIBUTED FIREWALL

The article deals with implementation of fault-tolerant distributed firewall , based on PacketFilter and FreeBSD operating system

Keywords: firewall, high-availability, redundancy, fault tolerance, network attack

На сегодняшний день межсетевой экран (МСЭ) является основным компонентом любой информационной инфраструктуры, обязательным с точки зрения выполнения требований по защите информации для различных информационных систем [1]. МСЭ, установленные на границе сети, позволяют защитить информационную систему от несанкционированного доступа и сетевых атак, помимо этого современные МСЭ позволяют выполнять трансляцию и определяют приоритетность обработки сетевого трафика.

Очевидно, что для обеспечения отказоустойчивости в информационной инфраструктуре все основные компоненты (в том числе и МСЭ) должны быть, как минимум, дублированы, а в лучшем случае многократно резервированы [2]. При этом даже дублирование или резервирование функций МСЭ не исключает уязвимостей, связанных

с простоем в случае переключения с основного узла на резервный из-за возникновения отказов или сбоев. Для минимизации времени простоя целесообразно использовать схему резервирования Active-Active, при которой и основной, и резервные компоненты МСЭ находятся во включенном состоянии.

Более того, организация защищенного межсетевого взаимодействия требует обеспечения синхронизации сетевых потоков между основным и резервными МСЭ для исключения возможных потерь сетевого трафика во время переключения с основного МСЭ на резервный [3].

Основными современными требованиями к МСЭ с точки зрения их функционального предназначения являются следующие:

1) обеспечение отказоустойчивости за счет дублирования и резервирования информации;

2) дублирование/резервирование по схеме Active-Active;

3) синхронизация сетевых потоков между основным и резервными МСЭ.

Предлагается рассмотреть возможность реализации отказоустойчивого распределенного межсетевого экрана, удовлетворяющего перечисленным выше требованиям, на основе специализированного программного продукта PacketFilter и операционной системы FreeBSD.

Для обеспечения отказоустойчивости рассмотрена схема дублирования МСЭ, т.е. предполагается использовать два межсетевых экрана – один основной, второй дублирующий. При этом возникает проблема совместного использования одного сетевого адреса (IP-адреса) несколькими устройствами.

Для решения данной проблемы был использован протокол CARP (Common Address Redundancy Protocol – протокол резервирования общего сетевого адреса), который позволяет использовать один IP-адрес сразу несколькими устройствами в рамках одного сегмента сети.

Для обеспечения синхронизации сетевых потоков между основным и дублирующим МСЭ был использован протокол PFsync, реализованный в программном межсетевом экране PacketFilter [4].

Общая схема реализации отказоустойчивого распределенного МСЭ, а также взаимосвязь всех компонентов приведены на рис. 1.

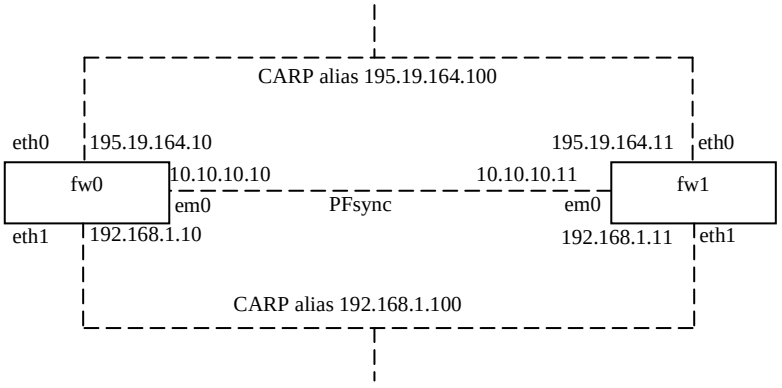

Рис. 1. Общая схема реализации отказоустойчивого распределенного межсетевого экрана

К основным компонентам, реализующим отказоустойчивый распределенный МСЭ, относятся:

– fw0 – основной МСЭ;

– fw1 – резервный МСЭ;

– em0 – интерфейс для синхронизации сетевых потоков между МСЭ по протоколу PFsync;

– eth0 – внешний сетевой интерфейс на МСЭ;

– eth1 – внутренний сетевой интерфейс на МСЭ;

– CARP alias – общий сетевой адрес для МСЭ.

Осуществление взаимодействия на основе протокола CARP обоих МСЭ (основного и резервного) предполагает использование одного IP-адреса, при этом собственные IP-адреса каждого из МСЭ (интерфейсы eth0 и eth1) применяются для передачи широковещательных пакетов между МСЭ по протоколу CARP.

Для поддержки протокола CARP со стороны операционной системы FreeBSD необходимо обеспечить загрузку модуля ядра. Порядок загрузки ядра, модулей и их дальнейшей инициализации в ОС FreeBSD определяет конфигурационный файл /boot/loader.conf (см. ниже).

```
#### FreeBSD 10 /boot/loader.conf
 ##

 # load the PF CARP module
 carp_load="YES"
```

Помимо загрузки модуля ядра для поддержки протокола CARP также необходимо инициализировать параметры ядра операционной

системы FreeBSD, отвечающие за сетевое взаимодействие. При этом необходимо, чтобы инициализация параметров происходила автоматически при каждом запуске системы. Для этого необходимо прописать необходимые параметры в конфигурационном файле /etc/sysctl.conf:

```
#### FreeBSD 10 /etc/sysctl.conf
 ##

 net.inet.ip.forwarding=1      # (default 0)
 net.inet.ip.fastforwarding=1  # (default 0)
 net.inet6.ip6.forwarding=1    # (default 0)

 net.inet.carp.preempt=1  # (default 0)
```

Параметры конфигурационного файла net.inet.ip.forwarding, net.inet.ip.fastforwarding и net.inet6.ip6.forwarding разрешают пересылку пакетов между различными интерфейсами каждого из МСЭ по протоколам IPv4 и IPv6.

Параметр net.inet.carp.preempt обеспечивает работу механизма переключения с основного МСЭ на резервный в случае возникновения неполадок.

Необходимо отметить, что конфигурационные файлы /boot/loader.conf и /etc/sysctl.conf являются идентичными для основного и резервного межсетевых экранов. Однако помимо общих настроек обоих МСЭ необходимо внести индивидуальные настройки для каждого из межсетевых экранов.

Индивидуальные настройки распространяются на такие параметры, как сетевое имя, IP-адрес и т.д. Для выполнения индивидуальных настроек каждого из МСЭ необходимо внести параметры в файл /etc/rc.conf:

```
#### FreeBSD 10 /etc/rc.conf

hostname="fw0"

## PF firewall
pf_enable="YES"
pf_rules="/etc/pf.conf"
pflog_enable="YES"
pflog_logfile="/var/log/pflog"
## ipv4 - native addresses
 ifconfig_eth0="inet 195.19.164.10/24"
 defaultrouter="195.19.164.1"
 ifconfig_eth1="inet 192.168.1.10/24"
## CARP aliases - EXTERNAL
```

```
      ifconfig_eth0_alias0="vhid 7 pass 12af7a alias
195.19.164.100/32"
     ## CARP aliases - INTERNAL
      ifconfig_eth1_alias0="vhid 17 pass 5bf2d9 alias
192.168.1.100/32"
     ## pfsync
      ifconfig_em0="10.10.10.10/24"
      pfsync_enable="YES"
      pfsync_syncdev="em0"
```

Для выполнения индивидуальных настроек каждого из МСЭ необходимо внести параметры в файл /etc/rc.conf:

```
     #### FreeBSD 10 /etc/rc.conf

     hostname="fw1"

     ## PF firewall
     pf_enable="YES"
     pf_rules="/etc/pf.conf"
     pflog_enable="YES"
     pflog_logfile="/var/log/pflog"
     ## ipv4 - native addresses
      ifconfig_eth0="inet 195.19.164.11/24"
      defaultrouter="195.19.164.1"
      ifconfig_eth1="inet 192.168.1.11/24"
     ## CARP aliases - EXTERNAL
      ifconfig_eth0_alias0="vhid 7 pass 12af7a alias
195.19.164.100/32"
     ## CARP aliases - INTERNAL
      ifconfig_eth1_alias0="vhid 17 pass 5bf2d9 alias
192.168.1.100/32"
     ## pfsync
      ifconfig_em0="10.10.10.11/24"
      pfsync_enable="YES"
      pfsync_syncdev="em0"
```

Параметры конфигурационного файла обеспечивают решение следующих задач:

– hostname – задает сетевое имя системы;

– ifconfig_eth0, ifconfig_eth1 и ifconfig_em0 – задают тип сетевого подключения и IP-адрес;

– pf_enable – обеспечивает запуск программного МСЭ PacketFilter;

– pf_rules – определяет конфигурационный файл с правилами фильтрации МСЭ PacketFilter;

– pflog_enable и pflog_logfile обеспечивают ведение и хранение журнала работы МСЭ;

– pfsync_enable – инициализирует работу МСЭ по протоколу PFsync;

– pfsync_syncdev – определяет сетевой интерфейс по которому будут передаваться пакеты по протоколу PFsync;

– ifconfig_eth0_alias0 и ifconfig_eth1_alias0 – обеспечивают корректную совместную работу нескольких межсетевых экранов по протоколу CARP.

В качестве данных параметров задается строка, которая содержит дополнительные параметры. Параметр vhid (Virtual Host ID) – число от 1 до 255, идентичный на основном и резервном межсетевых экранах, служит для идентификации МСЭ, работающих по протоколу CARP. Параметр pass – пароль, состоящий не более чем из 30 символов, который используется при передаче пакетов по протоколу CARP от одного узла к другому.

На последнем этапе необходимо выполнить настройку программного межсетевого экрана PacketFilter для корректного взаимодействия PacketFilter, CARP и PFsync между собой. Настройка программного МСЭ PacketFilter выполняется с помощью конфигурационного файла /etc/pf.conf (см. ниже).

```
    ################ FreeBSD 10 pf.conf
##########################
    # Required order: options, normalization, queueing,
translation, filtering.
    # Note: translation rules are first match while filter
rules are last match.
    …
    ################ Filtering
###################################
    …
    # CARP firewall failover
     pass quick on em0   proto pfsync keep state (no-sync)
     pass quick on eth0  proto carp   keep state (no-sync)
     pass quick on eth1  proto carp   keep state (no-sync)
    …
```

С помощью правила pass quick on em0 proto pfsync keep state выполняется разрешение прохождения трафика по протоколу PFsync на сетевом интерфейсе с идентификатором em0. Аналогично действуют остальные два правила в программном межсетевом экране PacketFilter.

Таким образом, рассмотрение реализация отказоустойчивого распределенного межсетевого экрана, с использованием схемы их дуб-

лирования на основе программы PacketFilter и операционной системы FreeBSD, удовлетворяет требованиям по обеспечению отказоустойчивости, резервирования по схеме Active-Active и синхронизации сетевых потоков между основным и резервным МСЭ.

Библиографический список

1. О реализации требований по защите персональных данных в информационной системе пермского филиала ФГУП «РЧЦ ПФО» / О.Б. Екимов, А.С. Шабуров, И.П. Исаков, П.В. Мазунин, А.Н. Шляков // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2013. – № 8. – С.144 – 155.

2. Бирюков А.А. Информационная безопасность: защита и нападение. – М.: ДМК-Пресс, 2013.

3. Korff Y., Hope P., Potter B. Mastering FreeBSD and OpenBSD Security. – O'Reilly. – Newton, 2005.

4. Hansteen P.N. The book of PF, 3rd edition. – No Starch Press. – San Francisco, 2014.

References

1. Ekimov O.B., Shaburov A.S., Isakov I.P., Mazunin P.V., Shliakov A.N. O realizatsii trebovanii po zashchite personal'nykh dannykh v informatsionnoi sisteme permskogo filiala Federal'nogo gosudarstvennogo unitarnogo predpriiatiia «Radiochastotnyi tsentr Privolzhskogo federal'nogo okruga»[About implementation of requirements for protection of personal information in information system of the Perm branch Federal State Unitary Enterprise “Radio-frequency Center of the Volga Federal District”]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhniche-skogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia,* 2013, no. 8, pp. 144-155.

2. Biriukov A.A. Informatsionnaia bezopasnost': zashchita i napadenie [Information security: protection and attack]. Moscow: DMK-press, 2013.

3. Korff Y., Hope P., Potter B. Mastering FreeBSD and OpenBSD Security. Newton: O'Reilly, 2005.

4. Hansteen P.N. The book of PF, 3rd edition. San Francisco: No Starch Press, 2014.

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.ru).

Рашевский Роман Борисович (Пермь, Россия) – студент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: roman@rashevskiy.com).

About the authors

Shaburov Andrey Sergeevich, (Perm, Russia) Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

Rashevskiy Roman Borisovich (Perm, Russia) is student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail:roman@rashevskiy.com).

Получено 12.09.2014