КОНЦЕПТ
научно-методический электронный журнал
Чемодуров А. С., Карпутина А. Ю. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети // Концепт. – 2015. – № 01 (январь). – ART 15020. – 0,3 п. л. – URL: http://e-koncept.ru/2015/15020.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.
ART 15020 УДК 331.482:004.738

Чемодуров Александр Сергеевич,
студент ФГБОУ ВПО «Брянский государственный университет им. академика И. Г. Петровского», г. Брянск
ru.133mhz@gmail.com

Карпутина Анастасия Юрьевна,
студентка ФГБОУ ВПО «Брянский государственный университет им. академика И. Г. Петровского», г. Брянск
sachiko1195@gmail.com

Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети

Аннотация. *В статье рассмотрены реализация технологии фильтрации сетевого трафика в корпоративной среде с помощью nDPI и применение правил iptables для защиты сервера.*
Ключевые слова*: информационная безопасность, экономическая безопасность, компьютерные сети, фильтрация сетевого трафика, linux, администрирование серверов.*
Раздел: *(04) экономика.*

Корпоративная сеть часто испытывает трудности с пропускной способностью внешнего канала, а также безопасностью локальной сети предприятия в целом. Необходимо следить за безопасностью и нагрузкой сети. Для организации безопасности, а также фильтрации трафика следует использовать множество средств защиты. Основным средством защиты все же стоит считать брандмауэр, например, в Debian используется iptables, а также фильтрацию контент-фильтром нежелательных ресурсов.

На сервере, который выполняет функцию сетевого шлюза, установлена операционная система Debian Linux 7.8 с прокси-сервером Squid.

Цель работы – заблокировать трафик peer-to-peer. Peer-to-peer соединения используют проброс портов на наличие открытых и производят передачу данных. Даже при открытии основных портов велика вероятность попадания на эти порты торрент-соединений. Рассмотрим программную реализацию анализа и блокировки пакетов.

Для блокировки пакета в среде операционной системы Debian Linux используются правила межсетевого экрана netfilter, точнее, его надстройка – iptables, которая представлена в виде консольной утилиты. Каждое правило – это строка, содержащая в себе критерии, определяющие, подпадает ли пакет под заданное правило, и действие, которое необходимо выполнить в случае выполнения критерия. В общем виде правила записываются примерно так:

```
iptables [-t table] command [match] [target/jump]
```

Если в правило не включается спецификатор [-t table], то по умолчанию предполагается использование таблицы filter, которая служит для фильтрации трафика, то есть разрешения и запрещения пакетов и соединений.

В таблице filter содержатся цепочки:

INPUT – обрабатывает трафик, который поступает непосредственно хосту.

FORWARD – отвечает за возможность фильтрации транзитного трафика.

OUTPUT – возможность фильтрации трафика, исходящего от хоста.

Действия, являющиеся допустимыми в таблице filter:

ACCEPT – пропуск пакета. Пакет покидает текущую базовую цепочку и следует дальше по потоковой диаграмме.

КОНЦЕПТ
научно-методический электронный журнал
ART 15020 УДК 331.482:004.738
Чемодуров А. С., Карпутина А. Ю. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети // Концепт. – 2015. – № 01 (январь). – ART 15020. – 0,3 п. л. – URL: http://e-koncept.ru/2015/15020.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

REJECT – блокировка пакета и сообщение его источнику об отказе. По умолчанию об отказе сообщается отправкой ответного ICMP-пакета “icmp-port-unreachable”. Однако это действие поддерживает опцию --reject-with, которая позволяет указывать формулировку сообщения об отказе (возможные значения: icmp-net-unreachable, icmp-host-unreachable, icmp-proto-unreachable, icmp-net-prohibited, icmp-host-prohibited). Для протокола TCP возможна поддержка отказа в форме отправки RST-пакета (--reject-with tcp-reset).

DROP – блокировка пакета без сообщения источнику об отказе. Является наиболее предпочтительной при фильтрации трафика на интерфейсах, которые подключены к Интернету (из-за понижения информативности сканирования портов хоста злоумышленниками) [Iptables – Викиучебник: [сайт]. http://ru.wikibooks.org/wiki/Iptables].

Если же предполагается использование другой таблицы, то это требуется указать явно. Спецификатор таблицы также может быть указан в любом месте строки правила, но при этом стандартом считается указание таблицы в начале правила.

Далее сразу за именем таблицы должна находиться команда. Если спецификатора таблицы нет, то команда всегда должна стоять первой. Команда определяет действие iptables, например: вставка правила, добавление правила в конец цепочки или удаление этого правила и т. д.

Раздел match задает критерии проверки, определяющие подпадание пакета под действие этого правила. Здесь могут быть указаны различные критерии: IP-адрес источника пакета или сети, IP-адрес места назначения, порт, протокол, сетевой интерфейс и т. д.

Спецификатор target указывает на то, какое действие необходимо выполнить в случае выполнения критериев в правиле. Здесь можно заставить ядро передать пакет в другую цепочку правил, заблокировать пакет и забыть про него, выдать на источник сообщение об ошибке и прочее.

Ниже приведены некоторые основные правила для интернет-шлюза.

Включение политики по умолчанию – трафик на шлюз запретить, исходящий со шлюза – разрешить, транзит – запретить:

```
# iptables -P INPUT DROP
# iptables -P OUTPUT ACCEPT
# iptables -P FORWARD DROP
```

Разрешить трафик локальной петли:

```
# iptables -A INPUT -i lo -j ACCEPT
# iptables -A OUTPUT -o lo -j ACCEPT
```

Далее необходимо разрешить DNS-, http-, HTTPS-протоколы для доступа:

```
# iptables -A INPUT -i eth0 -p tcp --sport 53 -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A INPUT -i eth0 -p udp --sport 53 -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A OUTPUT -o eth0 -p udp --dport 53 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Чемодуров А. С., Карпутина А. Ю. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети // Концепт. – 2015. – № 01 (январь). – ART 15020. – 0,3 п. л. – URL: http://e-koncept.ru/2015/15020.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

```
# iptables -A OUTPUT -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 80 -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -A OUTPUT -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
# iptables -A INPUT -p tcp --sport 443 -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Далее необходимо настраивать NAT для каждого интерфейса или внутренней сети, например:

```
# iptables -t nat -A POSTROUTING -s 10.0.0.0/8 -o eth0 -j MASQUERADE
```

Следующим шагом будет применение технологии DPI.

Ранее существовали надстройки для межсетевого экрана, такие как L7-filter и ipp2p. Они позволяли фильтровать определенный трафик, анализируя информацию, в том числе и на прикладном уровне OSI. Эти механизмы легли в основу проекта OpenDPI, распространяемого по лицензии LGPLv3 и построенного на коде коммерческого продукта PACE компании “Ipoque”. OpenDPI являлся модулем для iptables и мог фильтровать большое количество различных типов пакетов. Проект прекратил свое существование в 2011 г., но появилась компания ntop, которая стала использовать исходники OpenDPI как основу для своих продуктов. Этот проект называется nDPI. Разработчики, которые на основе исходников nDPI создали модуль для iptables, таким образом восстановили проект OpenDPI.

В операционной системе Debian Linux установлено ядро linux-kernel-3.2, которое не поддерживается nDPI. Для установки nDPI необходимо пересобрать ядро операционной системы.

Все действия выполняются от имени суперпользователя.

```
$ sudo su
```

Для начала устанавливаем пакеты для сборки ядра fakeroot, kernel-package, libncurses5-dev:

```
# aptitude install fakeroot kernel-package libncurses5-dev
```

Переходим в директорию /usr/src/:

```
# cd /usr/src
```

Скачиваем с kernel.org ядро 3.17.1, распаковываем:

```
# wget https://www.kernel.org/pub/linux/kernel/v3.x/linux-3.17.3.tar.xz
# tar xf linux-3.17.3.tar.xz
```

Создаем символьную ссылку на скачанные исходные коды ядра:

```
# if [ -d linux ]; then rm linux; fi; ln -s linux-3.17.3 linux
```

КОНЦЕПТ
научно-методический электронный журнал
ART 15020 УДК 331.482:004.738
Чемодуров А. С., Карпутина А. Ю. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети // Концепт. – 2015. – № 01 (январь). – ART 15020. – 0,3 п. л. – URL: http://e-koncept.ru/2015/15020.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

Копируем настройки старого ядра:

```
# cp /boot/config-3.2.0-4-amd64 .config
```

Скачиваем nDPI и распаковываем его:

```
# wget http://devel.aanet.ru/ndpi/nDPI-1.5.1.r8636_v3.tar.gz
# tar xf nDPI-1.5.1.r8636_v3.tar.gz
```

Переходим в каталог со скачанным ядром:

```
# cd linux
```

Конфигурируем ядро и включаем поддержку NAT в netfilter и NF_CONNTRACK_LABELS:

```
# make menuconfig
> Networking support
-> Networking options
-> Network packet filtering framework (Netfilter)
-> IP: Netfilter Configuration
->> IPv4 NAT [M] (включаем)
->> IP tables support (required for filtering/masq/NAT) [M] (включаем)
->> iptables NAT support [M] //(включаем)

> Networking support
-> Networking options
-> Network packet filtering framework (Netfilter)
-> Core Netfilter Configuration
-> *** Xtables matches ***
-> "connlabel" match support [M] //(включаем)
```

Сохраняем конфигурацию ядра и выходим:

```
[Save] [Exit]
```

Приступаем к сборке (ревизия ядра (здесь это 01ndpi10012015) должна начинаться с цифры).

```
# make-kpkg clean
# fakeroot make-kpkg --initrd --revision=01ndpi10012015 kernel_image
Собираем всё в deb-пакеты
# fakeroot make-kpkg --initrd --revision=01ndpi10012015 kernel_headers
# fakeroot make-kpkg --initrd --revision=01ndpi10012015 kernel_manual
# fakeroot make-kpkg --initrd --revision=01ndpi10012015 kernel_doc
# fakeroot make-kpkg --initrd --revision=01ndpi10012015 kernel_source
```

Чемодуров А. С., Карпутина А. Ю. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети // Концепт. – 2015. – № 01 (январь). – ART 15020. – 0,3 п. л. – URL: http://e-koncept.ru/2015/15020.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

Теперь устанавливаем пакеты:

```
# cd /usr/src
# dpkg -i linux-doc-3.17.3_01ndpi10012015_all.deb
# dpkg -i linux-headers-3.17.3_01ndpi10012015_amd64.deb
# dpkg -i linux-image-3.17.3_01ndpi10012015_amd64.deb
# dpkg -i linux-manual-3.17.3_01ndpi10012015_all.deb
# dpkg -i linux-source-3.17.3_01ndpi10012015_all.deb
```

Перезагружаем машину:

```
# reboot
```

Переходим в директорию /usr/src/nDPI-1.5.1.r8636_v3/ndpi-netfilter и компилируем iptables-extension и модуль ядра:

```
# cd /usr/src/nDPI-1.5.1.r8636_v3/ndpi-netfilter
# make
# make install
```

Если make install не сработал, то можно воспользоваться утилитой checkinstall и изменить ревизию netfilter на 01 и установить deb-пакет:

```
# make modules_install
```

Теперь можно применять правила с использованием nDPI – необходимо выбрать нужный протокол и создать на его основе правило в iptables:

```
# iptables -A FORWARD -m ndpi --bittorrent -j DROP
# iptables -A FORWARD -m ndpi --steam -j DROP
# iptables -A FORWARD -m ndpi --gnutella -j DROP
# iptables -A FORWARD -m ndpi --edonkey -j DROP
# iptables -A FORWARD -m ndpi --battlefield -j DROP
# iptables -A FORWARD -m ndpi --quake -j DROP
# iptables -A FORWARD -m ndpi --halflife2 -j DROP
# iptables -A FORWARD -m ndpi --worldofwarcraft -j DROP
# iptables -A FORWARD -m ndpi --warcraft3 -j DROP
# iptables -A FORWARD -m ndpi --world_of_kung_fu -j DROP
```

В данной статье были рассмотрены основные принципы защиты сервера с помощью брандмауэра iptables, а также технология DPI и ее реализация на сетевом шлюзе под управлением операционной системы Debian. Был сделан вывод о том, что использование технологии DPI позволяет администратору значительно снизить нагрузку на интернет-канал, обеспечив комфортную работу всем пользователям организации.

На практике была произведена пересборка ядра операционной системы Debian Linux с целью использования пакета nDPI. Пакет nDPI является свободно распространяемым программным обеспечением, следовательно, не требуется значительных финансовых затрат на его настройку и дальнейшее использование, что является одним из его основных преимуществ перед платными решениями сторонних производителей решений для фильтрации сетевого трафика.

КОНЦЕПТ
научно-методический электронный журнал

Чемодуров А. С., Карпутина А. Ю. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети // Концепт. – 2015. – № 01 (январь). – ART 15020. – 0,3 п. л. – URL: http://e-koncept.ru/2015/15020.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

ISSN 2304-120X

ART 15020 **УДК 331.482:004.738**

Alexander Chemodurov,
Student, Bryansk State University named after Academician Ivan Georgiyevich Petrovsky, Bryansk
ru.133mhz@gmail.com
Anastasia Karputina,
Student, Bryansk State University named after Academician Ivan Georgiyevich Petrovsky, Bryansk
sachiko1195@gmail.com

Internet gateway protection and filtering network traffic corporate network

Abstract. The article describes the implementation of network traffic filtering technology in a corporate environment with using nDPI and iptables rules to protect the server.

Key words: information security, economic security, computer networks, network traffic filtering, linux, server administration.

Рекомендовано к публикации:
Горевым П. М., кандидатом педагогических наук, главным редактором журнала «Концепт»;
Утёмовым В. В., кандидатом педагогических наук