DOI: 10.55648/1998-6920-2023-17-1-107-116 УДК123.456.789

Анализ подходов к фильтрации трафика и эффективность применения черных и белых списков

М. А. Медведев, И. Л. Рева

Новосибирский государственный технический университет (НГТУ)

Аннотация: Одним из самых распространённых методов автоматизированного определения типа контента во входящем трафике и его ограничения является система черных и белых списков. Черные и белые списки представляют собой набор «надежных» или «ненадежных» правил классификации данных внутри пакетов информации, по которым фильтруется нежелательный контент. Объектом исследования является имеющийся трафик, который будет разделен на две группы в виде «True-трафика» и «False-трафика». По составленным черным и белым спискам определяется количество срабатываний каждой единицы трафика, по этим данным дана оценка такому подходу к анализу. На созданной испытательной площадке для исследования задач контент-фильтрации выявили, что при соответствии списку блокируемых сигнатур количество верных блокировок имеет высокие положительные показатели, а количество ложных срабатываний приближено к нулю, при VPN-соединении и запуске прокси-сервера можно обойти контент-фильтрацию, при переносе ресурса на другой URL-блокировка не происходит.

Ключевые слова: контент-фильтр, черные списки, белые списки, трафик, фишинг, MITM, IP-адрес, VPN, IP-пакет, TCP-пакет, URL-адрес

Для цитирования: Медведев М. А., Рева И. Л. Анализ подходов к фильтрации трафика и эффективность применения черных и белых списков // Вестник СибГУТИ. 2023. Т. 17, № 1. С. 107–116. https://doi.org/10.55648/1998-6920-2023-17-1-107-116.

Статья поступила в редакцию 30.01.2023;
переработанный вариант – 20.02.2023;
принята к публикации 09.03.2023.

1. Введение

Система черных и белых списков является одним из самых перспективных и распространенных методов автоматизированного определения типа контента во входящем трафике. Черные и белые списки – это набор правил классификаций «надежных» или «ненадежных» данных внутри пакетов информации, по которым фильтруется нежелательный контент. В силу прогресса нежелательного контента черные и белые списки необходимо постоянно пополнять, изменять и/или удалять. Контент-фильтр определяется как программа, которая блокирует доступ к веб-сайтам с содержимым, запрещённым для просмотра. Контент-фильтрация позволяет выполнить требования действующих законов и легко защитить пользователей от нежелательной информации, такой как экстремистские сайты и ресурсы из списка Минюста РФ.

Условно контентные фильтры можно разделить на два типа: продукты, которые устанавливаются на самих защищаемых устройствах (хостовые), и продукты, которые работают в качестве сетевого шлюза и фильтруют трафик, проходящий через них.

Продукты первого типа используются преимущественно на домашних и личных устройствах. Второй тип продуктов используется в интернет-шлюзах с функциями контентной фильтрации. Они помогают снизить риски, связанные с просмотром содержимого сети Интернет, фильтруя опасный или нежелательный контент, зловредные файлы, социальные медиа и другие веб-угрозы, а также позволяют осуществлять мониторинг веб-серфинга пользователей и оптимизировать потребление канала связи.

В данной статье авторы проводят исследование задач контент-фильтрации на базе испытательной площадки, используя черные и белые списки. В статье рассматривается, как формируются списки, какие существуют способы фильтрации трафика, в том числе приводятся примеры существующих возможных и основных угроз, предотвращаемых контент-фильтрами. Авторы вывели математическую модель на основе двух методов блокировок, где в результате выделили два метода: блокировка по DNS-записи и блокировка по URL-запросу. Также описывается эксперимент для подхода с использованием черных и белых списков для организации работы контент-фильтров.

2. Формирование списков

Стандарт, который описывает технические аспекты блокировки и фильтрации интернет-услуг, называется RFC7754 [1]. В этом документе рассматривается несколько технических подходов к блокировке и фильтрации Интернета с точки зрения их соответствия общей архитектуре Интернета.

Фильтрация организуется двумя способами:

– работа по «чёрному» списку: РАЗРЕШИТЬ всё, кроме;

– работа по «белому» списку: ЗАПРЕТИТЬ всё, кроме.

Белые списки блокируют весь контент, кроме явно разрешенного. Черные списки разрешают доступ ко всему контенту, кроме явно запрещенного. Пользовательские черные списки запрещают доступ, а белые списки разрешают доступ к веб-сайтам [2]. Ведение черного списка требует его постоянного обновления. Нужно обновлять вручную записи и убирать записи при удалении нежелательного контента [3]. При использовании белого списка нужно следить за актуальностью разрешенных ресурсов и добавлять новые. Часто обновление белого списка не успевает за потребностями пользователей сети в новых ресурсах. При помощи белого и черного списков можно указать ресурсы, на которые отправляются требования, и какие ресурсы влияют на показатели и состояние тестов программы. Белые и черные списки доступны только для тестов веб-страниц и тестов со сценариями [4]. При определении разрешенных или заблокированных положений черный список всегда переопределяет белый. В Табл. 1 описан режим фильтрации и блокировки для всех сценариев, которые содержат белый и черный списки.

Таблица 1. Режим фильтрации и блокировки для белого и черного списков

Черный список	Белый список	Режим	Код
Пустой	Пустой	Разрешить доступ	Правила фильтрации не заданы
Пустой	URL не соответствует записи в списке	Блокировать доступ	URL нет в белом списке
Пустой	URL соответствует записи в списке	Разрешить доступ	URL есть в белом списке. В черном списке нет записей, блокирующих доступ.

URL не соответствует записи в списке	Пустой	Разрешить доступ	URL нет в черном списке. Нет никаких записей белого списка, которые бы запрещали доступ к URL, отсутствующим в белом списке.
URL соответствует записи в списке	Пустой	Блокировать доступ	URL есть в черном списке
URL не соответствует записи в списке	URL не соответствует записи в списке	Блокировать доступ	URL нет в белом списке
URL не соответствует записи в списке	URL соответствует записи в списке	Разрешить доступ	URL есть в белом списке. URL нет в черном списке
URL соответствует записи в списке	URL не соответствует записи в списке	Блокировать доступ	URL нет в белом списке. URL есть в черном списке
URL соответствует записи в списке	URL соответствует записи в списке	Блокировать доступ	URL есть в черном списке. Запись в черном списке переопределяет запись в белом списке.

3. Способы фильтрации трафика

Система фильтрации трафика обычно работает на основе так называемых наборов правил – наборов записей (URL-адресов, IP-адресов, TCP-портов и т.п.), которые необходимо блокировать («чёрный список») или которые необходимо разрешать, блокируя все остальные («белый список») [5]. При поступлении очередного пакета из внешней сети система фильтрации перехватывает этот пакет, проверяет его метаданные и содержимое на совпадение с одной из записей набора правил, и при обнаружении совпадения либо пропускает пакет в локальную сеть, либо отбрасывает его – локальная сеть даже не узнает о существовании такого пакета. При этом для того, чтобы пользователь мог понимать, что трафик был заблокирован, система фильтрации может передать в локальную сеть, например, веб-страницу с информацией о причине блокировки (если был заблокирован запрашиваемый веб-сайт) [6].

3.1. Угрозы, предотвращаемые контент-фильтрами

Фишинг – подмена веб-приложений для получения от пользователя его персональных данных или корпоративной информации. Атаки «фишеров» становятся все более продуманными, применяются методы социальной инженерии. Фишинговые сайты, как правило, живут недолго (в среднем 5 дней) [7, 8].

Современные браузеры используют несколько типов защиты от фишинга [9]:

– *черные списки*: при открытии каждого нового соединения адрес открываемого ресурса передается на серверы с черными списками, где происходит проверка открываемого адреса на наличие в черном списке. Если адрес присутствует в черном списке, браузер отображает соответствующее сообщение об ошибке.

– *белые списки*: открываемые адреса из белых списков считаются доверенными, остальные адреса затем проверяются с помощью черного списка.

И черные, и белые списки содержат огромное количество записей, что создает дополнительные проблемы, связанные в первую очередь с производительностью компьютеров пользователей. Действительно, нельзя просто так взять и загрузить на компьютер пользователя черный список целиком. Во-первых, он содержит огромное количество записей, и его скачивание сильно нагрузит интернет-канал пользователя. Во-вторых, списки регулярно обновляются – поддерживать актуальность списков на удаленных компьютерах крайне сложно.

В-третьих, даже при наличии актуального черного списка на пользовательском компьютере поиск в нем адреса займет недопустимо большое время.

Также, помимо фишинга, широко распространена концепция MITM. Термин обозначает тип кибератаки, при которой злоумышленники перехватывают разговор или передачу данных путем подслушивания либо притворяясь легальным участником [10]. Целью MITM-атаки является получение конфиденциальных данных, таких как данные банковского счета, номера банковских карт или учетные данные для входа, которые могут быть использованы для совершения дальнейших преступлений – кражи личных данных или незаконных переводов средств [11]. Успешная MITM-атака включает в себя две конкретные фазы: перехват и дешифрация.

Современные браузеры решают проблемы полноты, актуальности и оперативности, используя два подхода [12]:

1. Белые списки, объем которых крайне мал, хранятся на пользовательском компьютере в виде фрагментов хэшей адресов сайтов, что позволяет экономить место на жестком диске и очень быстро искать совпадения адресов. Поддерживать актуальность белых списков так же просто из-за их сравнительно малого объема.

2. Черные списки, имеющие большой объем, хранятся на специализированных облачных серверах, специально предназначенных для быстрой однотипной обработки информации в большом массиве данных. Такие системы называются репутационными.

3.2. Фильтрация трафика по IP-адресам

IP-адресация четвертой и шестой версий имеет иерархическую структуру, т.е. адрес узла записывается блоками чисел, которые администратор каждой конкретной сети может использовать для группировки узлов по логическим или физическим критериям [13].

Для фильтрации трафика по IP-адресу система фильтрации в первую очередь получает пакет и читает данные из заголовка IP-пакета. В этом заголовке всегда указаны в незашифрованном виде IP-адрес источника (Source address) и IP-адрес назначения (Destination address), которые всегда указывают на изначальный источник пакета (за исключением случаев, когда используется VPN или другое туннелирование – в этом случае фильтрация трафика стандартными средствами невозможна, и единственный способ ограничить доступ к хостам в этом случае – ограничивать доступ к самим VPN-серверам) [14].

Соединение VPN – это так называемый «туннель» между компьютером пользователя и компьютером-сервером. Каждый узел шифрует данные до их попадания в «туннель». При подключении к VPN система идентифицирует сеть и начинает аутентификацию [15].

Далее сервер авторизует, то есть предоставляет право на выполнение определенных действий: чтение почты, интернет-серфинг и т.д. После установления соединения весь трафик передается между ПК и сервером в зашифрованном виде. ПК имеет IP-адрес, предоставленный интернет-провайдером. Этот IP блокирует доступ к некоторым сайтам. VPN-сервер меняет IP на свой. Уже с VPN-сервера все данные передаются к внешним ресурсам, которые запрашивает пользователь.VPN открывает доступ к заблокированным ресурсам, и по итогу многие готовы мириться с более низкой скоростью интернета и возможными логами программ. Хотя VPN использует довольно надежные алгоритмы шифрования, включение VPN-клиента на ПК не гарантирует 100 % сохранности конфиденциальной информации, поэтому следует внимательно отнестись к выбору VPN-провайдера [16].

3.3. Фильтрация трафика по TCP-портам

Принцип фильтрации по TCP-портам похож на фильтрацию по IP-адресам с той разницей, что для определения трафика используются TCP-порты – идентификаторы приложений, реализованные на транспортном уровне сетевой модели. Соответственно, для этого система фильтрации трафика должна также считать порт назначения (Destination port) из заголовка

TCP-пакета, вложенного в IP-пакет. TCP-пакеты также передаются по сети в незашифрованном виде, что обеспечивает надёжность такого способа фильтрации [17].

3.4. Фильтрация трафика по URL-адресам

Для реализации этого компонента необходимо, чтобы устройство, на котором размещён фильтр трафика, имело доступ к DNS-серверу – серверу преобразования доменных имён в IP-адреса, либо было установлено непосредственно на DNS-сервере. Это связано с тем, что пакеты в сети Интернет идентифицируются только по IP-адресам, а URL-адреса имеют однозначные преобразования в такие адреса и созданы только для удобства пользователя [9].

Соответственно, при получении пакета сетевой фильтр должен определить доменное имя по IP-адресу источника пакета. После получения доменного имени система может продолжать свою работу, сравнивая полученный домен со списком правил.

Однако принцип работы URL-фильтрации в целом намного сложнее предыдущих. Это связано с тем, что IP-адреса не всегда соответствуют реальным доменным именам и наоборот. Существуют так называемые виртуальные серверы, которые при запросе веб-сайта перенаправляют пользователя на другой сервер с другим доменным именем. Обычно это делается для балансировки нагрузки, но усложняет работу фильтра трафика. В качестве примера можно привести информацию, полученную с помощью утилиты nslookup:

```
C:\>nslookupgoogle.com
Server: router.asus.com
Address: 192.168.1.1
Name: google.com
Addresses: 2a00:1450:4010:c0f::64
2a00:1450:4010:c0f::8b
2a00:1450:4010:c0f::8a
2a00:1450:4010:c0f::65
108.177.14.139
108.177.14.113
108.177.14.101
108.177.14.100
108.177.14.102
108.177.14.138
C:\>nslookup 108.177.14.138
Server: router.asus.com
Address: 192.168.1.1
Name: It-in-f138.1e100.net
Addresses: 108.177.14.138
```

Как видно из примера, имеет место множественное соответствие IP-адресов и доменных имён, доменному имени google.com соответствует сразу несколько IP-адресов. При этом при попытке определить доменное имя одного из этих адресов оно оказывается совершенно другим – в реальности серверы поисковой системы Google находятся на серверах *.1e100.net. Исходя из этого, можно сделать вывод, что система фильтрации трафика по URL-адресам должна, как минимум, создавать и поддерживать актуальную таблицу связей IP-адресов и доменов, поскольку даже статические домены могут менять своё расположение. При получении пакета система должна проверять URL на соответствие не только напрямую у списка правил, но и по другим доменам, связанным с этим IP-адресом или URL.

4. Математическая модель

На данный момент существует две группы подходов к фильтрации контента – статические и динамические. И. Э. Стрекалов, А. А. Новиков и Д. В. Лопатин [10] в качестве основной идеи статических подходов называют блокирование нежелательных веб-ресурсов на основе постоянно пополняемых баз данных черных и белых списков. Они указывают, что в настоящее время в системах контентной фильтрации применяются методы ограничения доступа к веб-ресурсу по имени DNS или конкретному IP-адресу, по ключевым словам, внутри веб-контента и по типу файла. Чтобы блокировать доступ к определенному веб-узлу или группе узлов, необходимо задать множество URL-ресурсов или IP-адресов, содержащих нежелательный контент. А. А. Бабенко, Ю. С. Бахрачева и А. Р. Алеева [11] выделили три вида фильтрации интернет-трафика:

– пакетная фильтрация;
– фильтрация по протоколам прикладного уровня;
– фильтрация по контенту.

Базируясь на этих исследованиях, мы выделяем два метода: блокировка по DNS-записи и блокировка по URL-запросу.

Обозначим через U множество URL-адресов, $U = \{u_1, \ldots, u_n\}$. Отдельный URL-адрес u_i можно представить в виде $u_i = (d_i, p_i)$, где d_i – доменное имя в URL-адресе, p_i – путь запроса в URL-адресе. Из доменных имен (DNS-записей) формируется множество $D = \{d_1, \ldots, d_m\}$, $m \le n$. В этих множествах мы выделяем подмножества запрещенных URL-адресов $U^{\mathrm{D}} = \{u_1^{\mathrm{D}}, \ldots, u_k^{\mathrm{D}}\}$, $k \le n$, и подмножество запрещенных DNS-имен $D^{\mathrm{D}} = \{d_1^{\mathrm{D}}, \ldots, d_t^{\mathrm{D}}\}$, $t \le m$.

Критерий блокировки по URL-адресам $\mathrm{Den}_{\mathrm{URL}}$ состоит в определении принадлежности адреса подмножеству U^{D}:

$$\mathrm{Den}_{\mathrm{URL}} = \begin{cases} 1, & u_i \in U^{\mathrm{D}} \\ 0, & u_i \notin U^{\mathrm{D}} \end{cases},$$

причем блокирование осуществляется только тогда, когда критерий принимает значение 1.

Аналогично критерий блокировки по DNS-именам состоит в определении принадлежности доменного имени подмножеству D^{D}:

$$\mathrm{Den}_{\mathrm{DNS}} = \begin{cases} 1, & d_i \in D^{\mathrm{D}} \\ 0, & d_i \notin D^{\mathrm{D}} \end{cases},$$

блокировка осуществляется при значении критерия 1.

5. Анализ и эксперимент

В рамках решения поставленных выше задач была организована испытательная площадка с общей топологией сети, представленной на рис. 1.

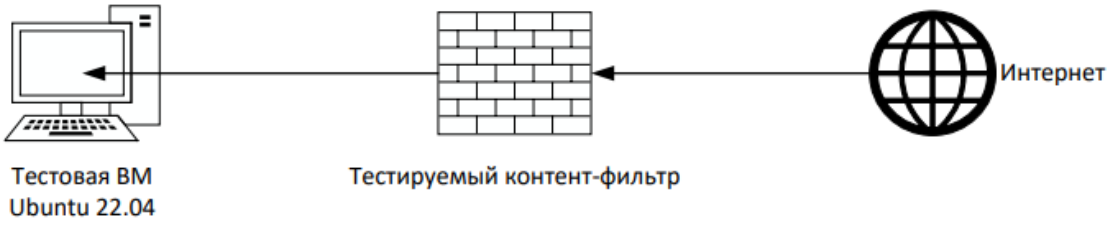

Рис. 1. Схема тестовой сети

При тестировании контент-фильтров UTM, DLP и разработанного ПО на основе математической модели, изложенной в четвертой главе, мы получили высокий положительный результат фильтрации трафика. Но во время проведения эксперимента выявили три проблемы, связанные с использованием черных и белых списков.

Первая проблема заключается в том, что значительно увеличиваются время и трудозатраты на поддержание и обновление вручную черных и белых списков.

Вторая проблема выявилась при использовании VPN и прокси-сервера, так как с помощью них злоумышленники обходят все ограничения, сформированные с помощью черных и белых списков.

Третья проблема оказалась в невозможности охватить полностью контент, так как черные и белые списки могут оказаться неполными, а именно: новые сайты появляются ежедневно, что приводит к невозможности учесть всевозможные категории и типы контента. Точность контент-фильтрации прямо пропорционально зависит от полноты списка, то есть в рамках организации контент-фильтрации необходимо предусмотреть различные варианты «слов» – если какой-то из вариантов не будет указан, то «злоумышленник» обойдет систему контент-фильтра.

Из вышесказанного вытекает потребность в разработке автоматизированных систем по расширению черных и белых списков.

В аналитическом модуле черный и белый списки применяются согласно описанной выше математической модели к проходящему через узел сети трафику, в результате чего определяется количество срабатываний на тот или иной трафик. Данная процедура в различных научных исследованиях чаще всего осуществляется методом перебора, при котором трафик блокируется, если в черном списке имеются похожие факторы для блокировки, и пропускается, если таковых не имеется. Та же самая процедура повторяется и для белого списка в случае пропускания трафика. При наличии обоих списков и невозможности отнести трафик к разрешенному или запрещенному в журнал заносится статус трафика «не определен».

Структурировав результаты блокировки, мы собрали информацию в следующем формате: ресурс, допуск/недопуск, отметка времени, причина.

Мы разместили контент-фильтр на участке сети, использовав предоставленные черные-белые списки и на основе этого выгрузили данные в .csv формате в количестве 2000+ ресурсов и применили к трафику объемом более 10 млн обращений. На основе полученных результатов мы делаем следующий вывод, что подход использования черных и белых списков пригоден для организации работы контент-фильтров, но при динамическом изменении интернет-ресурсов злоумышленниками система черных и белых списков требует быстрого реагирования и дополнения новыми элементами, что, в свою очередь, может быть трудоемко из-за ручного внесения данных о блокировках и ручного подхода к формированию черных и белых списков соответственно.

6. Заключение

Была создана испытательная площадка для исследования задач контент-фильтрации, где на участке сети был размещен контент-фильтр с использованием предоставленные черных и белых списков. Далее выгрузили данные в *csv*-формате в количестве 2000+ ресурсов и применили к трафику размером более 10 млн обращений. Были получены следующие результаты:

1. При полном соответствии со списком блокируемых сигнатур количество верных блокировок имеют высокие положительные показатели, а количество ложных срабатываний приближено к нулю.
2. При изменении «слова» с добавлением внутри «слова» пунктуации, кириллицы и т.д. черные и белые списки пропускали данный контент и не относили его к нежелательному, соответственно, его не блокировали, хотя данный контент относится к нежелательной информации, требующей блокировки.
3. При запуске контент-фильтра при VPN-соединении и при запуске прокси-сервера контент-фильтрация обходилась.
4. При переносе ресурса на другой URL блокировки также не происходило.

Черные и белые списки эффективно фильтруют трафик, но существует три проблемы, из-за которых можно обойти блокировку трафика и иметь доступ ко всему контенту. Чтобы этого избежать авторы предлагают разработать автоматизацию систем по расширению черных и белых списков.

Литература

1. Technical Considerations for Internet Service Blocking and Filtering – RFC 7754.
2. *Бухарин В. В., Закалкин П. В., Карайчев С. Ю., Бречко А. А.* Метод защиты сервера услуг от DDOS атак за счет использования списков IP-адресов // Вопросы оборонной техники. Серия 16: технические средства противодействия терроризму. 2019. №11–12. С. 29–35.
3. *Гречишников Е. В., Добрышин М. М.* Оценка эффективности деструктивных программных воздействий на сети связи // Системы управления, связи и безопасности. 2015. № 2. С. 135–146.
4. *Ажмухамедов И. М., Запорожец К. В.* Усовершенствованный метод фильтрации нежелательного трафика // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2014. №1. С. 98–104.
5. *Нгуен М. Т.* Тестирование методов машинного обучения в задаче классификации http запросов с применение технологии TF-IDF // Вестник Волжского государственного университета. Серия: Системный анализ и информационные технологии. 2019. № 4. С. 119–131.
6. *Болдырихин Н. В., Бельчикова Д. А., Закут М.* Анализ современных технологий межсетевого экранирования // Сборник статей международной научной конференции «Высокие технологии и инновации в науке», Санкт-Петербург, 2020. С. 129–134.
7. *Карайчев С. Ю., Бухарин В. В., Пикалов Е. Д.* Способ защиты от деструктивных программных воздействий в мультисервисных сетях связи // Вопросы кибербезопасности. 2016. № 3. С. 18–25.
8. *Коцыняк М. А., Лаута О. С., Нечепуренко А. П.* Модель системы воздействия на информационно-телекоммуникационную систему специального назначения в условиях информационного противоборства // Вопросы оборонной техники. 2019. В. 3. С. 40–44.
9. *Литвинов Г. А.* Скрытые каналы передачи информации на основе DNS-запросов // Материалы региональной молодежной научно-практической конференции «Нанотехнологии. Информация. Радиотехника (НИР-22)», Омск, 21 апреля 2022 г. С. 81–85.

10. *Стрекалов И. Э., Новиков А .А., Лопатин Д. В.* Методы динамической фильтрации веб-контента // Вестник российских университетов. Математика. 2014. № 1. С. 1–2.
11. *Бабенко А. А., Бахрачева Ю. С., Алеева А. Р.* Система фильтрации нежелательных приложений интернет-ресурсов // НБИ-технологии. 2020. № 4. С. 6–11.

Медведев Михаил Александрович
ассистент кафедры защиты информации НГТУ (630073, Новосибирск, пр-т К. Маркса, 20), тел. +7 383 346 08 53, e-mail: m.medvedev@corp.nstu.ru, ORCID: 0000-0001-7674-9964.

Рева Иван Леонидович
к.т.н., доцент кафедры защиты информации НГТУ (630073, Новосибирск, пр-т К. Маркса, 20), тел. +7 383 346 08 53, e-mail: reva@corp.nstu.ru, ORCID: 0000-0001-7241-4438.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Analysis of Traffic Filtering Approaches and the Effectiveness of Blacklisting and Whitelisting

Mikhail A. Medvedev, Ivan L. Reva

Novosibirsk State Technical University (NSTU)

Abstract: One of the most common methods for automatically determining the type of content in incoming traffic and limiting it is the system of black and white lists. Blacklists and whitelists are a set of “trusted” or “untrustworthy” rules for classifying data within information packets by which unwanted content is filtered. The object of the research is the existing traffic that will be divided into two groups in the form of "True-traffic" and "False-traffic". According to the compiled black and white lists, the number of hits of each traffic unit is determined and according to these data, an assessment of this approach to analysis is given. In accordance with the list of blocked signatures, the number of true blockings has high positive indicators and the number of false positives is close to zero with a VPN connection and starting a proxy server you can bypass content filtering, with transferring the resource to another URL blocking doesn’t occur, that was revealed on the cyberpolygon created to study the tasks of content filtering.

Keywords: content filter, blacklists, whitelists, traffic, phishing, MITM, IP address, VPN, IP packet, TCP packet, URL.

For citation: Medvedev M. A., Reva I. L. Analysis of traffic filtering approaches and the effectiveness of blacklisting and whitelisting (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 1. pp. 107-116. https://doi.org/10.55648/1998-6920-2023-17-1-107-116.

The article was submitted: 30.01.2023;
revised version: 20.02.2023;

accepted for publication 09.03.2023.

References

1. Technical Considerations for Internet Service Blocking and Filtering - RFC 7754.
2. Bukharin V. V., Zakalkin P. V., Karaichev S. Yu., Brechko A. A. Metod zashchity servera uslug ot DDOS atak za schet ispolzovaniya spiskov IP-adresov [Method of protecting the service server from DDOS attacks by using lists of ip-addresses]. *Voprosy oboronnoi tekhniki. Seriya 16: tekhnicheskie sredstva protivodeistviya terrorizmu*, 2019, no. 11-12, pp. 29-35.
3. Grechishnikov E. V., Dobryshin M. M. Otsenka effektivnosti destruktivnykh programmnykh vozdeistvii na seti svyazi [Evaluation of the effectiveness of destructive program impacts on communication networks]. *Sistemy upravleniya, svyazi i bezopasnosti*, 2015, no. 2, pp. 135-146.
4. Azhmukhamedov I. M., Zaporozhets K. V. Usovershenstvovannyi metod filtratsii nezhelatelnogo trafika [Advanced method for filtering unwanted traffic]. *Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika*, 2014, no. 1, pp. 98-104.
5. Nguen M. T. Testirovanie metodov mashinnogo obucheniya v zadache klassifikatsii http zaprosov s primenenie tekhnologii TF-IDF [Testing machine learning methods in the task of classifying http requests using TF-IDF technology]. *Vestnik Volzhskogo gosudarstvennogo universiteta. Seriya: Sistemnyi analiz i informatsionnye tekhnologii*, 2019, no. 4, pp. 119-131.
6. Boldyrikhin N. V., Belchikova D. A., Zakut M. Analiz sovremennykh tekhnologii mezhsetevogo ekranirovaniya [Analysis of modern firewall technologies]. 2020, pp. 129-134.
7. Karaichev S. Yu., Bukharin V. V., Pikalov E. D. Sposob zashchity ot destruktivnykh programmnykh vozdeistvii v multiservisnykh setyakh svyazi [A method of protection against destructive program influences in multiservice communication networks]. *Voprosy kiberbezopasnosti*, 2016, no. 3, pp. 18-25.
8. Kotsynyak M. A., Lauta O. S., Nechepurenko A. P. Model sistemy vozdeistviya na informatsionno-telekommunikatsionnuyu sistemu spetsialnogo naznacheniya v usloviyakh informatsionnogo protivoborstva [Model of the system of influence on the information and telecommunication system of special purpose in the conditions of information confrontation]. *Voprosy oboronnoi tekhniki*, 2019. iss. 2, pp. 40-44.
9. Litvinov G. A. Skrytye kanaly peredachi informatsii na osnove DNS-zaprosov [Hidden channels of information transfer based on DNS queries]. *Materialy regional'noi molodezhnoi nauchno-prakticheskoi konferentsii «Nanotekhnologii. Informatsiya. Radiotekhnika (NIR-22)»*, 2022, pp. 81-85.
10. Strekalov I. E., Novikov A. A., Lopatin D. V. Metody dinamicheskoi filtratsii veb-kontenta [Web Content Dynamic Filtering Techniques]. *Vestnik rossiiskikh universitetov. Matematika*, 2014, no. 1, pp.1-2.
11. Babenko A. A., Bakhracheva Yu. S., Aleeva A. R. Sistema filtratsii nezhelatelnykh prilozhenii internet-resursov [System for filtering unwanted applications of Internet resources]. *NBI-technologies*, 2020, no. 4, pp. 6-11.

Mikhail A. Medvedev

Assistant of the Department of Information Security, NSTU (630073, Novosibirsk, K. Marks Ave., 20), tel. +7 383 346 08 53, e-mail: m.medvedev@corp.nstu.ru, ORCID: 0000-0001-7674-9964.

Ivan L. Reva

PhD (Engineering), Associate Professor of the Department of Information Security, NSTU (630073, Novosibirsk, K. Marks Ave., 20), tel. +7 383 346 08 53, e-mail: reva@corp.nstu.ru, ORCID: 0000-0001-7241-4438.