КОНЦЕПТ
научно-методический электронный журнал

Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Концепт. – 2015. – № 02 (февраль). – ART 15039. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15039.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

ART 15039 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

Обзор средств фильтрации трафика в корпоративной сети

Аннотация. *В статье рассмотрены технологии фильтрации сетевого трафика в корпоративной среде, методы шейпинга пользовательского трафика.*
Ключевые слова: *информационная безопасность, экономическая безопасность, компьютерные сети, фильтрация сетевого трафика, корпоративная сеть, прокси-сервер, DansGuardian, Squid, Ideco ICS, DPI, CISCO, iptables, ClearOS.*
Раздел: *(04) экономика.*

С появлением сети Интернет произошло множество изменений в жизни людей. Эти изменения коснулись и фирм. Большинство сотрудников современных компаний используют интернет-подключение не по его прямому назначению. Пользователи «забивают» канал, используя торренты, просматривая видео в Интернете, скачивая файлы или играя в онлайн-игры.

Оптимизация использования сетевых ресурсов находится в списке обязанностей системного администратора. Можно выделить несколько основных проблем, с которым сталкивается администратор корпоративной сети:

- чрезмерная нагрузка на сеть, вызванная неконтролируемым скачиванием сотрудниками больших файлов из глобальной сети;
- нерациональное использование ресурсов сети и рабочего времени в результате деятельности любителей онлайн-игр с видео- и голосовыми чатами;
- снижение уровня безопасности сети предприятия – именно внутренние ресурсы и данные компании часто становятся объектом угроз и рисков при отсутствии полноценного контроля за посещением сотрудниками сайтов той или иной тематики.

Потенциальными зонами риска распространения вредоносного ПО и причинами фишинговых атак, причинами утечки информации, кражи паролей и других шпионских ухищрений были и остаются порносайты, а также социальные сети, развлекательные порталы и иные сайты, где ежедневно инфицируются тысячи новых страниц и появляются новые модификации хорошо известных угроз [1].

Немаловажной является проблема заполнения пропускной способности канала сети Интернет.

Для обеспечения безопасности и целостности информации, перекрытия каналов возможной утечки информации и повышения производительности сети необходимо управлять потоком трафика, входящего в локальную сеть. Для фильтрации доступа в Интернет важно анализировать сетевой трафик, который генерируется пользователями. Решением в борьбе с таким неконтролируемым трафиком в любой организации становится фильтрация интернет-запросов. Осуществляя контроль доступа к различным ресурсам при помощи настройки фильтров, можно легко решить вопросы использования канала доступа в Интернет и значительно уменьшить риск за-

КОНЦЕПТ
научно-методический электронный журнал
Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Концепт. – 2015. – № 02 (февраль). – ART 15039. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15039.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.
ART 15039 УДК 331.482:004.738

ражения внутренних ресурсов сети предприятия, но при это необходимо определить, как правильно и наиболее эффективно применить данные фильтры.

Обзор технологий фильтрации сетевого трафика

Фильтрация сетевого трафика обычно осуществляется на трех уровнях модели OSI [2]:

- сетевом (IP);
- транспортном (TCP, UDP);
- прикладном (FTP, TELNET, HTTP, SMTP и т. д.).

Фильтрация трафика − основная функция систем межсетевых экранов (или брандмауэров), которая позволяет сетевому администратору распределить пользователям как доступ из внешней сети к службам компьютеров, находящимся внутри сети предприятия, или к защищенному сегменту сети, так и доступ пользователей из внутренней сети к соответствующим ресурсам внешней сети [3].

Фильтрация трафика осуществляется несколькими способами:

- прокси-серверы;
- брандмауэры;
- фильтрация DPI (Deep Packet Inspection).

Рассмотрим подробнее каждую технологию.

Прокси-сервер – это кроссплатформенное программное обеспечение, которое служит для организации централизованного доступа к сайтам в Интернете по заранее определенным правилам. Эти правила могут ограничивать доступ на сайты для разных пользователей локальной сети. Обратим внимание на бесплатный прокси-сервер Squid и платное комплексное программное решение Ideco ICS.

Squid

Прокси-сервер Squid – это полнофункциональный кэширующий прокси-сервер, который предоставляет сервисы кэширования и прокси для HTTP, FTP и других популярных сетевых протоколов. Squid может осуществлять кэширование и проксирование SSL-запросов и кэширование результатов DNS-поиска, а также выполнять прозрачное кэширование. Данный прокси-сервер также поддерживает широкий набор кэширующих протоколов:

- ICP – кэширующий интернет-протокол;
- HTCP – гипертекстовый кэширующий протокол;
- CARP – протокол кэширования маршрутизации;
- WCCP – кэширующий протокол перенаправления контента.

Прокси-сервер Squid масштабируется для сетей от уровня регионального офиса до корпораций при обеспечении расширяемого разделяемого механизма контроля доступа и отслеживания критических параметров через протокол SNMP.

В Squid существует гибкая схема фильтрации внешних ссылок. С её помощью, например, можно закрыть доступ к определённым сайтам и ресурсам на них, избавиться от навязчивой рекламы (banners), ссылок непристойного содержания и т. п. Содержимое фильтруется с помощью настроек ACL и http_access deny, примеры которых приведены в squid.conf. Следует обратить внимание на то, что при задании фильтруемого URL или доменного имени сервера можно использовать регулярные выражения, таким образом в одной строке определяя фильтр для целого класса адресов или доменных имён.

DansGuardian (надстройка для Squid)

Безусловно, фильтрация по URL- и IP-адресам, которую осуществляет Squid, очень быстрая и простая, но существенно ограниченная. При минимуме изобрета-

КОНЦЕПТ
научно-методический электронный журнал
Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Концепт. – 2015. – № 02 (февраль). – ART 15039. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15039.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.
ART 15039 УДК 331.482:004.738

тельности ее можно обойти, и многие веб-сайты (особенно сомнительного содержания) постоянно изменяют свои параметры.

Ответом на все это является программа DansGuardian. Как и Squid, DansGuardian может блокировать IP-адреса, URL или целые домены, числящиеся в черном списке. Но подлинная причина, по которой его следует использовать, – та, что в первую очередь это фильтр содержимого (контента). DG действительно способен просканировать входящую веб-страницу и заблокировать ее, если ее текст нарушает некоторые определенные пользователем критерии.

DansGuardian не скачивает веб-страницы напрямую: он создан для работы поверх прокси-сервера, например Squid. При этом остаются доступными все преимущества повышения скорости, присущие прокси-серверам.

DansGuardian может определять неприемлемые страницы несколькими способами. Простейший из них, который DG разделяет с более традиционными веб-фильтрами, – это занесение в черные списки IP-адресов, определенных URL или целых доменов. Чтобы определить эти параметры с предельной гибкостью, можно использовать регулярные выражения.

Но главная особенность DansGuardian в распознавании слов или фраз, которые вы хотели бы заблокировать внутри текста веб-страницы. Многие слова и фразы, которые по общепринятым нормам следует блокировать, внесены в настройки по умолчанию. Также предусмотрена возможность разделения пользователей на группы, каждая со своими настройками фильтрации.

Как и веб-фильтры, DansGuardian может блокировать или ограничивать скачивание файлов, а также загрузку файлов на сервер через веб-формы. Типы MIME, расширения файлов или их размер – все это можно использовать как критерии блокировки. Есть и способы определения вирусов в допустимых вложениях.

Iptables – утилита для модификации правил, по которым встроенный брандмауэр Linux обрабатывает пакеты. В Linux брандмауэр является модулем ядра, называемым netfilter, и представляет собой набор хуков (hooks) для работы с сетевым стеком. Всю работу по фильтрации трафика выполняет ядро системы. Iptables не создает новых процессов в системе. Включение или выключение iptables – это всего лишь отправка сигнала в ядро. Большая скорость фильтрации достигается за счёт анализа только заголовков пакетов.

К основным возможностям iptables можно отнести:

- перенаправление пакетов по определенным параметрам;
- фильтрацию трафика на основе адресов отправителя и получателя пакетов, номеров портов;
- организацию доступа в сеть (SNAT);
- проброс портов из глобальной сети в локальную (DNAT);
- ограничение числа подключений;
- установление квот трафика;
- выполнение правил по расписанию.

Ideco ICS

Ключевой задачей, которую решает Ideco ICS, является управление трафиком – от маршрутизации до шифрования и балансировки нагрузки. Будучи установленным на границе корпоративной и глобальной сетей, шлюз позволяет контролировать и при необходимости ограничивать доступ сотрудников к онлайновым ресурсам и веб-контенту определенного содержания. Предусмотрены и средства ограничения скорости и объема передаваемых пользователями данных. Лимиты могут быть вы-

Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Концепт. – 2015. – № 02 (февраль). – ART 15039. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15039.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.

ART 15039 УДК 331.482:004.738

ставлены как для отдельных сотрудников компании, так и по отделам и предприятию в целом. Модуль формирования отчетов для директора и IT-менеджера помогает оперативно оценивать степень целевого использования сетевых ресурсов офисными сотрудниками.

Ideco ICS обеспечивает защиту локальной сети от внешних угроз и утечек конфиденциальной информации. Встроенный в шлюз модуль Data Leak Prevention (DLP) сканирует исходящий трафик и блокирует передачу защищенных документов через электронную почту и веб-протоколы, распознавая конфиденциальные данные при помощи технологии цифровых отпечатков.

Выделим основные возможности продукта:

- организация совместного доступа в Интернет – прокси-сервер и NAT с возможностью управления доступом в Интернет и учетом трафика;
- защита ресурсов внутренней сети – firewall, блокировка IP-адресов, узлов и протоколов, блокировка некоторых сетевых атак, антивирус (ClamAV, DrWeb, Антивирус Касперского), контентная фильтрация по 14 категориям (с базой русских сайтов) и антиспам (три уровня: предварительный, DSPAM и Dr. Web Antispam);
- управление трафиком – балансировка нагрузки, оптимизация трафика (перенаправление разного типа трафика на оптимальные каналы), приоритезация трафика – QoS, portmaper.

Перехваченные файлы, которые попадают в категорию «для служебного пользования», имеют возможность сохранения на сервере для их дальнейшего просмотра администратором или сотрудником службы безопасности.

Данный продукт является платным.

ClearOS. Предлагаемый ClearFoundation дистрибутив ориентирован на применение в небольших распределенных сетях, где он может играть роль шлюза или сервера. В названии подчеркнута доступность, и теперь все, что было в платном варианте, можно получить совершенно свободно и бесплатно. Как шлюз ClearOS обеспечивает:

- антивирусную, антиспам, антифишинг, контентную фильтрацию;
- пакетный фильтр и фильтр протоколов/приложений;
- управление пропускной способностью;
- веб-прокси с контролем доступа.

Среди особенностей дистрибутива выделяются полностью открытая архитектура, исключающая зависимость от одного проприетарного вендора, низкая стоимость обслуживания, возможность наращивания компонентов и расширенная поддержка.

Система DPI (Deep Packet Inspection) осуществляет глубокий анализ всех проходящих через неё пакетов. Под термином «глубокий» подразумевается анализ пакета на верхних уровнях модели OSI, а не только по стандартным номерам сетевых портов. Помимо изучения пакетов по стандартным образцам, которые позволяют однозначно определить принадлежность пакета к определённому приложению, например по форматам заголовков, номерам портов и т. д., система DPI осуществляет и так называемый поведенческий анализ трафика, позволяющий распознавать приложения, которые не используют уже известные заголовки и структуры данных для обмена данными. Наиболее ярким примером может служить протокол BitTorrent. Для идентификации таких приложений необходимо осуществлять анализ последовательности пакетов, обладающих одинаковыми признаками (*Source_IP: port – Destination_IP:port*, размер пакета, частота открытия новых сессий в единицу времени) по моделям поведения, которые соответствуют этим приложениям. Эта функция может реализовываться программным решением и оборудованием, но сколько про-

Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Концепт. – 2015. – № 02 (февраль). – ART 15039. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15039.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.
ART 15039 УДК 331.482:004.738

изводителей такого аппаратного обеспечения – столько и интерпретаций поведенческих моделей соответствующих протоколов, а следовательно, точность определения также будет различаться. Наиболее крупными производителями и их продуктами на рынке аппаратных DPI являются “Allot Communications”, “Procera Networks”, “Cisco”, “Sandvine”. Набирают популярность интегрированные в маршрутизаторы решения DPI. Так поступают многие – “Cisco”, “Juniper”, “Ericsson”. Такие решения, как правило, являются компромиссными и весь спектр сервисов, доступных аппаратным решениям, предоставить не могут. Но этого вполне достаточно для решения большинства задач [4].

Условия блокирования пакета:

- любой порт TCP;
- любой флаг;
- по фактическому наличию в пакете (в любом порядке) строк:

GET /*.html

Host: any.host.ru

- совпадение IP-источника с указанным в списке для запрета.

Cisco Service Control Engine (SCE) представляет собой сетевой элемент, специально предназначенный для использования в сетях операторского класса, в которых требуются высокопроизводительные функции классификации и управления IP-трафиком приложений на уровне отдельного абонента (подписчика), с контролем состояния приложений и сессий. Иными словами, Cisco SCE – это устройство DPI анализа трафика. SCE позволяет классифицировать трафик клиента вплоть до 7-го уровня сетевой модели OSI и на основании классификации трафика применять к нему какие-либо действия, будь то ограничение скорости, фильтрация трафика, перенаправление запроса на другой сервер и обнаружение аномальной активности в сети (спам рассылки, DDOS-атаки). Особенностью интеграции SCE в сетевую инфраструктуру является то, что она устанавливается в разрыв сети, например между маршрутизатором широкополосного удалённого доступа и пограничным маршрутизатором на выходе из сети. Такая схема интеграции позволяет пропустить через SCE весь трафик на выходе из сети оператора, получается узкое место для отказа. Весь комплекс Cisco Service Control Engine – это не только железное решение, это еще и целый комплекс программ, устанавливаемых для полнофункциональной работы всей системы. В этот комплекс входит Subscriber Manager (SM), Collection Manager (CM) и SCA BB Console, последняя как раз и служит для настройки всего этого хозяйства. Серверы с SM и CM должны устанавливаться на физически или логически разные серверы, работать на одном сервере они не будут. Сама SCE может работать и без этого софта, но тогда у нас не будет возможности собирать статистику, чтобы рисовать отчеты в виде графиков, и не будет некоторой гибкости в управлении подписчиками, что в масштабах большого оператора играет очень важную роль.

В данной статье были рассмотрены основные принципы и технологии фильтрации сетевого трафика, такие как прокси-сервер Squid, контент-фильтр DansGuardian, встроенный брандмауэр Linux iptables, технология анализа сетевого пакета DPI, комплексное решение Ideco ICS и аппаратное средство Cisco Service Control Engine. Стоит отметить, что Ideco ICS обладает очень богатым функционалом, но при этом имеет высокую стоимость, зависящую от количества подключений, т. е. компьютерного парка организации. Cisco Service Control Engine также имеет высокую стоимость, но при этом она не зависит от количества подключений. В качестве бесплатной альтернативы на интернет-шлюзе хорошим аналогом будет считаться установка

КОНЦЕПТ
научно-методический электронный журнал
Чемодуров А. С., Карпутина А. Ю. Обзор средств фильтрации трафика в корпоративной сети // Концепт. – 2015. – № 02 (февраль). – ART 15039. – 0,4 п. л. – URL: http://e-koncept.ru/2015/15039.htm. – Гос. рег. Эл № ФС 77-49965. – ISSN 2304-120X.
ART 15039 УДК 331.482:004.738

и администрирование ClearOS. Если же есть готовый корпоративный сервер с предустановленной UNIX-like операционной системой, то решением может являться вариант с настройкой и администрированием связки прокси-сервера Squid с контент-фильтром DansGuardian для создания качественной веб-фильтрации. Для глубокого анализа стоит применять технологию DPI, которая позволяет блокировать соединения известных протоколов (bittorrent, steam и прочие), а также поможет установить правильный подбор правил iptables.

Любые устройства и решения по отдельности будут являться не очень функциональными и, по сути, не очень эффективными. Конечно, любые из них можно настроить на сервере, но для этого потребуется определенное время и знания.

Ссылки на источники

1. Фильтрация трафика как первый шаг к безопасности сети: [сайт]. – URL: http://www.osp.ru/win2000/2009/08/10556459/
2. Краткий обзор технологии DPI – Deep Packet Inspection: [сайт]. – URL: http://habrahabr.ru/post/111054
3. Многоуровневая фильтрация сетевого трафика: [сайт]. – URL: http://best-practice.su/sistemy-obnaruzheniya-vtorzhenij/132-mnogourovnevaya-filtraciya-setevogo-trafika
4. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов. 4-е изд. – СПб.: Питер, 2010. – 113 с.

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

ISSN 2304-120X 02
9 772304 120159

Overview filter traffic on the corporate network

Abstract. The article deals with network traffic filtering technology in a corporate environment, methods of user traffic shaping.

Key words: information security, economic security, computer networks, network traffic filtering, corporate network, proxy server, DansGuardian, Squid, Ideco ICS, DPI, CISCO, iptables, ClearOS.

References

1. *Fil'tracija trafika kak pervyj shag k bezopasnosti seti: [saj*t]. Available at: http://www.osp.ru/win2000/2009/08/10556459/ (in Russian).
2. *Kratkij obzor tehnologii DPI – Deep Packet Inspection: [sajt].* Available at: http://habrahabr.ru/post/111054 (in Russian).
3. *Mnogourovnevaja fil'tracija setevogo trafika: [sajt].* Available at: http://best-practice.su/sistemy-obnaruzheniya-vtorzhenij/132-mnogourovnevaya-filtraciya-setevogo-trafika (in Russian).
4. Olifer, V. G. & Olifer, N. A. (2010) *Komp'juternye seti. Principy, tehnologii, protokoly: ucheb. dlja vuzov*. 4-e izd., Piter, St. Peterburg, 113 p. (in Russian).

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