УДК 004.771

Д.Р. Симашёв*, Ж.Р. Умарова, П.А. Кожабекова
магистрант, ЮКУ им. М.Ауэзова, Шымкент, Казахстан
PhD, доцент, ЮКУ им. М.Ауэзова, Шымкент, Казахстан
доцент, ЮКУ им. М.Ауэзова, Шымкент, Казахстан
***Автор для корреспонденции: ranyabro@gmail.com**

ОБЗОР ТЕХНОЛОГИЙ КОНТРОЛЯ И ЗАЩИТЫ ТРАФИКА В ОРГАНИЗАЦИЯХ

Аннотация

Современные компании имеют большое количество устройств с доступом в Интернет, которые используют пакеты данных для передачи информации. Каждый из этих пакетов несет информацию, которая может потенциально быть перехвачена и использована в плохих целях. Для этого можно использовать средства для контроля трафика. В статье описаны основные типы таких средств, методика их использования и рассмотрены плюсы и минусы каждой из таких систем. Также, описаны методы обслуживания таких систем, настройки и в общем смысла использования на предприятиях. Предложены различные методы использования систем для различных контролирующих органов организации, таких как анализ посещенных доменов, анализ эффективности работы с помощью систем контроля трафика, защита информации от кражи, контроль доступных к посещению доменов, управление сетью в целом. С помощью систем контроля трафика сама сеть становится защищеннее и более открытой к исследованию, получает возможность блокировки нежелательного контента, а также дает возможность оптимизации скорости и экономии затрат на оборудование по оптимизации сети.

Ключевые слова: Сеть, сервер, трафик, сетевой пакет, анализ трафика, перехват трафика.

Введение

В современных организациях имеется большое количество компьютеров, серверов и систем, подключенных к сети Интернет. Любое устройство, использующее сети, посылает пакеты данных по определенным адресам, после чего происходит их маршрутизация и возврат к отправителю ответа. В самой сети Интернет существуют протокола, такие как HTTPS и SSH, которые позволяют передавать зашифрованную информацию между двумя устройствами, однако в большинстве случаев, шифруется не вся информация, а лишь часть, которая считается уязвимой, например, пароли, логины или токены авторизации [1]. Для таких случаев, можно использовать системы шифрования по всей сети, такие как туннелирование и виртуальные частные сети, однако, в большинстве случаев это трудозатратно и замедляет скорость работы сети, а сам трафик не так легко перехватить за пределами сети самой компании, поэтому можно обезопасить саму сеть компании, не потеряв при этом в эффективности. Для некоторых сетей также будет достаточно просто сканировать трафик, проходящий в сети. Для обоих методов существуют свои решения, подходящие для каждого отдельного сценария [2].

Теоретическая часть

Необходимость в использовании систем контроля трафика может диктоваться различными потребностями организаций. Для организаций, можно определить два основных способа контроля трафика: с использованием прокси-сервера и без него. В первом случае, прокси-сервер устанавливается прямо в сеть, и все пакеты проходят через него. В этом же случае, возможности получить пакеты без него нет [3].

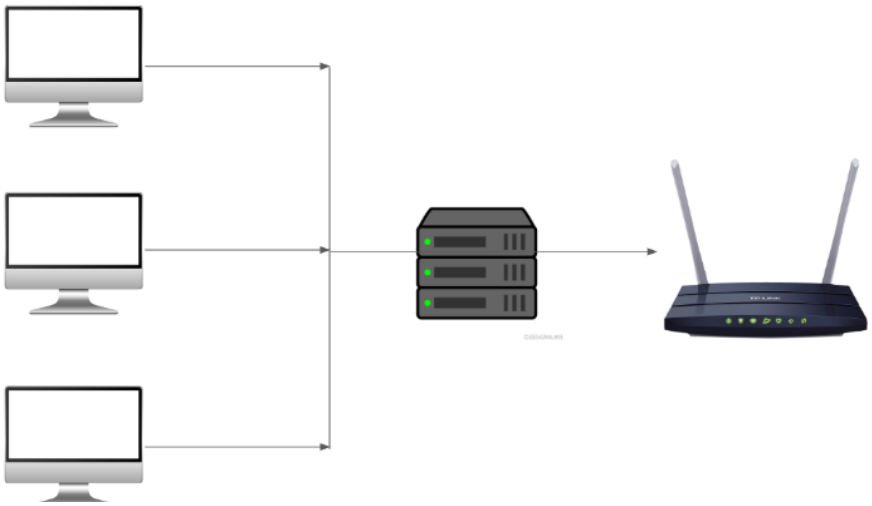

Рис. 1 - Схема сети с прокси-сервером

На рисунке 1 видно, как будет выглядеть схема сети, в который будет подключен прокси-сервер. Видно, что сервер является своеобразным мостом между роутером и устройствами. Такой подход имеет как плюсы, так и минусы. К плюсам можно отнести: однозначный контроль над сетью и манипулирование пакетами данных в ней. Причиной этому является расположение сервера в сети, весь трафик будет пропускаться через прокси, что означает, что каждый пакет может проходить анализ и логироваться. Также, так как весь трафик проходит через один сервер, этот сервер может полноценно управлять доступом в сеть как отдельных устройств, так и доступ этих устройств к определенным компонентам сети. Например, можно ограничить протокола, через которые ведется связь, до важных для рабочего процесса, тем самым повысив общую безопасность системы [4].

Во втором случае, сервер располагается в самой сети параллельно с рабочими устройствами.

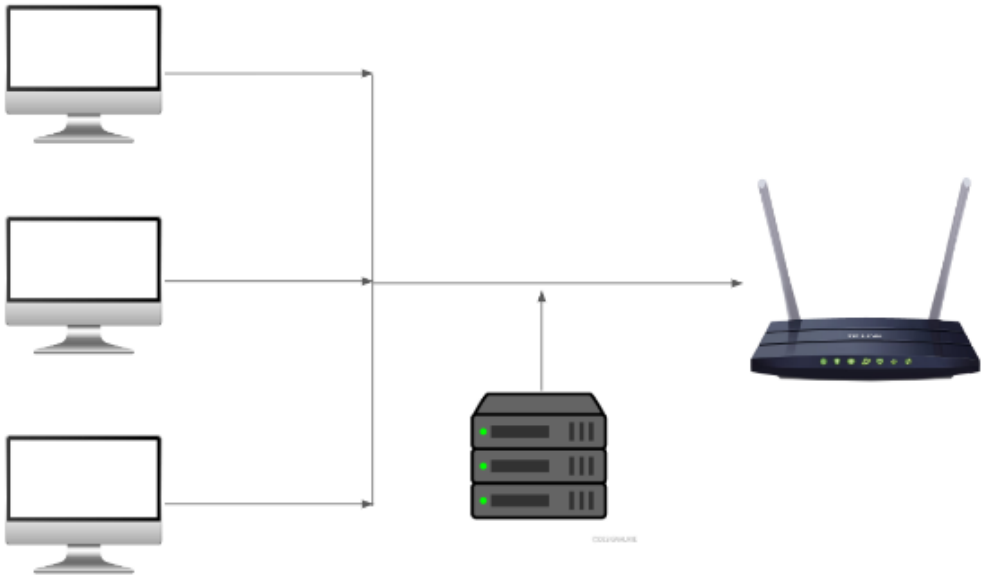

Рис. 2 - Схема сети без прокси-сервера

Если расположить устройства в сети таким образом, чтобы контроль сервер

располагался параллельно остальным устройствам, то можно получить систему, не зависящую от контроль сервера, и иметь возможность просматривать трафик сети, но контролирование трафика при этом становится проблематичным, так как для его реализации нужно будет перехватывать уже идущие пакеты с помощью MITM-атак. На практике, выбор схемы расположения сервера контроля трафика ложится на плечи разработчиков в зависимости от пожеланий заказчика [5].

Экспериментальная часть

Для реализации контроль сервера можно использовать методику перехвата пакетов, совмещенную со стандартными методами защиты сети. В случае прокси-сервера можно использовать Squid, популярный пакет для установки прокси-сервера, поддерживающий множество настроек [6]. Важным аспектом настройки будет установка автозапуска и логирования. Логирование в данном контексте - сбор информации о всех пакетах, проходящих через прокси-сервер, и так как прокси сервер пропускает через себя все пакеты, он собирает информацию о всех пакетах сети. Для настройки логирования можно изменить строку logformat в конфигурационном файле squid.conf [7]. Можно настроить практически все что угодно, начиная от времени получения пакета и заканчивая именами серверов и направлением пакета. Данный метод помогает настроить получение только важной для организации информации, опуская всю ненужную и конфиденциальную [8]. В дальнейшем, мы получаем сухие данные в виде таблиц логов, которые затем можно будет обрабатывать и получать полноценные данные. Для обработки можно использовать множество инструментов, визуализаторов, экспортеров данных. Например, ELK-Stack, который помогает собирать, обрабатывать и визуализировать данные, пригодится аналитикам и специалистам по сетевой безопасности [9].

Также, важнейшим аспектом контроля трафика является защита сети от вторжений и кражи данных. Для защиты сети от вторжений можно использовать системы Anti-DDoS защиты, под которую отлично подойдет, например, система Snort, система для предотвращения вторжений. Это мощное средство, которое устанавливается на прокси-машину и выполняет также функцию файрволла. Также, в случае наличия конфиденциальных данных, которые отправляются между пользователями, можно использовать полноценное TLS/SSL шифрование в локальной сети. Для установки сертификата SSL на прокси-сервер необходимо либо купить сертификат у доверенного поставщика сертификатов, в этом случае нужно будет установить его только на прокси-сервер, либо вручную регистрировать сертификаты на каждом устройстве, что с другой стороны, будет безопаснее, так как новое устройство не сможет получить доступ в сеть вообще, из-за недоверия к сертификату.

Заключение

В заключении, можно отметить основные тезисы при создании средства по контролю трафика. Необходимо определиться, какая система нужна, с прокси-сервером или без, какой уровень безопасности данных необходим в сети, вследствие чего искать возможность установки сертификата для шифрования всех данных, поступающих в сеть. Также, стоит задуматься, нужна ли защита от внешних угроз, таких как DDoS-атаки. В случае необходимости сбора информации, стоит определить, какую именно информацию хочется иметь в логах, как она должна обрабатываться, куда эти данные отправляются дальше, для дальнейшего анализа человеком или для системы защиты. Это крайне важный шаг для любой компании, выбор, который сильно повлияет на дальнейшее развитие компании.

Список литературы

1. Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. Network Traffic Anomaly Detection and Prevention. NYC: Springer, 2017. 263p.
2. Baiocchi A. Network Traffic Engineering. Hoboken: Wiley, 2020. 816p.
3. Мендкович Н.А. Анализ трафика некоммерческих сетей. М: ЛитРес, 2022, 127 с.

4. Беспалов Д.А., Костюк А.И. Администрирование баз данных и компьютерных сетей. РнД: Издательство Южного Федерального Университета, 2020, 125с.
5. Мерритт М., Поллино Д. Безопасность беспроводных сетей. М.: ЛитРес, 2022, 273с.
6. Марухленко А.Л., Марухленко Л.О., Ефремов Л.А. Технологии обеспечения безопасности информационных систем. М.: Директ-медиа, 2020, 205с.
7. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК-Пресс, 2010, 530с.
8. Топорков С. Компьютерные сети для продвинутых пользователей. М.: ДМК-Пресс, 2022, 192с.
9. Астанин И.К., Крыжко И.Б., Астахова И.Ф. Компьютерные науки. Деревья, операционные системы, сети. М.: ЛитРес, 2022, 88с.

References

1. Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. Network Traffic Anomaly Detection and Prevention. NYC: Springer, 2017. 263p.
2. Baiocchi A. Network Traffic Engineering. Hoboken: Wiley, 2020. 816p.
3. Mendkovich N.A. Analiz trafika nekommercheskih setej. M: LitRes, 2022, 127 s.
4. Bespalov D.A., Kostjuk A.I. Administrirovanie baz dannyh i komp'juternyh setej. RnD: Izdatel'stvo Juzhnogo Federal'nogo Universiteta, 2020, 125s.
5. Merritt M., Pollino D. Bezopasnost' besprovodnyh setej. M.: LitRes, 2022, 273s.
6. Maruhlenko A.L., Maruhlenko L.O., Efremov L.A. Tehnologii obespechenija bezopasnosti informacionnyh sistem. M.: Direkt-media, 2020, 205s.
7. Shan'gin V.F. Zashhita komp'juternoj informacii. Jeffektivnye metody i sredstva. M.: DMK-Press, 2010, 530s.
8. Toporkov S. Komp'juternye seti dlja prodvinutyh pol'zovatelej. M.: DMK-Press, 2022, 192s.
9. Astanin I.K., Kryzhko I.B., Astahova I.F. Komp'juternye nauki. Derev'ja, operacionnye sistemy, seti. M.: LitRes, 2022, 88s.

Д.Р. Симашев*, Ж.Р. Умарова, П.А. Қожабекова
магистрант, М.Әуезов атындағы ОҚУ, Шымкент, Қазақстан
PhD, доцент, М.Әуезов атындағы ОҚУ, Шымкент, Қазақстан
доцент, М.Әуезов атындағы ОҚУ, Шымкент, Қазақстан
***Корреспондент авторы:** ranyabro@gmail.com

ҰЙЫМДАРДАҒЫ ЖОЛ ҚЫЗМЕТІН БАҚЫЛАУ ЖӘНЕ ҚОРҒАУ ТЕХНОЛОГИЯЛАРЫН ҚАРАУ

Түйін

Қазіргі заманғы компанияларда ақпаратты беру үшін деректер пакеттерін пайдаланатын көптеген Интернетке қол жетімді құрылғылар бар. Бұл пакеттердің әрқайсысы ықтимал ұсталатын және жаман мақсатта пайдаланылуы мүмкін ақпаратты алып жүреді. Ол үшін трафикті бақылау құралдарын пайдалануға болады. Мақалада мұндай құралдардың негізгі түрлері, оларды қолдану әдістемесі сипатталған және осындай жүйелердің әрқайсысының оң және теріс жақтары қарастырылған. Сондай-ақ, мұндай жүйелерге қызмет көрсету әдістері, параметрлері және жалпы мағынада кәсіпорындарда пайдалану сипатталған. Ұйымның әртүрлі бақылаушы органдары үшін жүйелерді пайдаланудың әртүрлі әдістері ұсынылған, мысалы, кірілген домендерді талдау, трафикті бақылау жүйелері арқылы жұмыс тиімділігін талдау, ақпаратты ұрлықтан қорғау, кіруге болатын домендерді бақылау, жалпы желіні басқару. Трафикті басқару жүйелерінің көмегімен желінің өзі қауіпсіз және зерттеуге ашық болады, қажетсіз мазмұнды бұғаттау мүмкіндігін алады, сонымен қатар желіні оңтайландыру үшін жылдамдықты оңтайландыруға және жабдық шығындарын үнемдеуге мүмкіндік береді.

Кілттік сөздер: желі, сервер, трафик, желілік пакет, трафикті талдау, трафикті ұстау.

D.R. Simashev*, Zh.R. Umarova, P.A. Kozhabekova
master student, M.Auezov SKU, Shymkent, Kazakhstan
PhD, Associate Professor, M.Auezov SKU, Shymkent, Kazakhstan
Associate Professor, M.Auezov SKU, Shymkent, Kazakhstan
***Corresponding author's email:** ranyabro@gmail.com

REVIEW OF TRAFFIC CONTROL AND PROTECTION TECHNOLOGIES IN ORGANIZATIONS

Abstract

Modern companies have a large number of devices with Internet access that use data packets to transmit information. Each of these packets carries information that can potentially be intercepted and used for bad purposes. To do this, you can use traffic control tools. The article describes the main types of such tools, the methodology of their use and discusses the pros and cons of each of these systems. Also, the methods of maintenance of such systems, settings and the general meaning of use in enterprises are described. Various methods of using systems for various regulatory bodies of the organization are proposed, such as analysis of visited domains, analysis of performance using traffic control systems, protection of information from theft, control of accessible domains, network management in general. With the help of traffic control systems, the network itself becomes more secure and more open to research, gets the opportunity to block unwanted content, and also makes it possible to optimize speed and save equipment costs for network optimization.

Keywords: network, server, traffic, network packet, traffic analysis, traffic interception.