Разработка информационно-аналитической системы контроля сетевого трафика сотрудников компании

Автор: Лиджигоряев В.А.

Аннотация.

В данной научной статье исследуется тема контроля сетевого трафика сотрудников компаний в контексте цифровизации общества и активного использования сети сотрудниками и использование автоматизированных средств для осуществления управления трафиком. С цифровой трансформацией общества компании сталкиваются с растущей потребностью в эффективном управлении сетевым трафиком, особенно в контексте повышенного использования сети сотрудниками. Цель работы заключается в изучении и оценки методов управления сетевой активностью внутри компаний для увеличения безопасности и производительности в этих организациях.

Работа проводит анализ неэффективных паттернов работы в организациях над проектами, в которых сетевое взаимодействие необходимо, также рассматриваются методы контроля трафика, которые могут повысить эффективность и снизить трудозатраты сотрудников и в то же время повысить безопасность рабочей среды организации и проводится анализ аналогичных систем контроля сетевого трафика. Результатом работы служат собранные требования к новой системе, которая закрывает рассмотренные неудобства сотрудников и имеет уникальные возможности по сравнению с аналогичными системами.

Abstract.

In this scientific article, the topic of controlling network traffic of company employees in the context of societal digitalization and active network usage by employees, as well as the use of automated tools for traffic management, is being explored. With the digital transformation of society, companies face an increasing need for effective network traffic management, especially considering the heightened usage of the network by employees. The aim of the article is to examine and assess methods of managing network activity within companies to enhance security and productivity in these organizations.

The paper analyzes inefficient work patterns within organizations on projects where network interaction is essential. It also discusses traffic control methods that can enhance efficiency, reduce employee workload, increase workplace safety, and conducts an analysis of similar network traffic control systems. The outcome of the study is the gathered requirements for a new system that addresses the identified inconveniences faced by employees and offers unique capabilities compared to similar systems.

Введение.

В настоящее время, в век цифровизации, практически все компании для своей работы используют компьютерные технологии. Сотрудники компаний пользуются различными программами, которые значительно облегчают их труд и повышают их эффективность. Зачастую организации разрешают своим работникам выходить в сеть Интернет, так как это может иметь прямое отношение к их работе. В случае удаленного формата работы это само собой разумеющееся, компания не может на это повлиять. На компьютерах сотрудников может находиться большое количество разрабатываемых проектов компании, которые могут иметь большое значение для нее.

Количество утечек корпоративных данных, а также конфиденциальных данных самих сотрудников не только не уменьшается, но и увеличивается, несмотря на использование всевозможных программных и аппаратных решений.

В то же время неограниченное использование сети сотрудниками компаний может снижать их продуктивность и эффективность, исходя из прямых побуждений этих сотрудников или неумышленного временного застоя в выполнении рабочих задач из-за невозможности шейпинга или приоритезации трафика, который как раз позволит сделать использование сети оптимальным конкретно под текущие задачи. Прямыми побуждениями сотрудников, которые могут замедлять работу, можно считать посещение Интернет-ресурсов, не связанных напрямую с работой, к примеру, социальных сетей, зачастую проверка почты, уведомлений мессенджеров может затянуться на часы, при этом трудозатраты на выполнение поставленных задач растет, что не есть хорошо для компании. Также сотрудники, работающие с большими объемами данных, их отправкой между отделами по сети или внешним членам рабочих процессов, к примеру, заказчикам, могут сталкиваться с проблемой ожидания отправки или скачивания больших файлов в случае, если их текущие и дальнейшие задачи тоже связаны с активным использованием сети.

Исследование, представленное в данной статье, фокусируется на анализе методов управления информационным трафиком с интегрированным подходом, включающим функции блокировок трафика, его ограничений по скорости или объему (шейпинг трафика).

Цель данного исследования заключается в оценке эффективности работы сотрудников, использующих неограниченный выход в сеть и повышении безопасности компании через анализ рабочих процессов, систем контроля и мер безопасности. Исследование направлено на выявление слабых сторон в организационной деятельности, идентификацию потенциальных рисков и нарушений безопасности, а также разработку рекомендаций по оптимизации трудовых процессов и повышению уровня защиты информации в компании-заказчике “52 lab”.

Для достижения этой цели ставятся следующие задачи:

1. Изучение рабочих процессов компании.
2. Анализ проблемных мест в этих процессах и выявление точек повышения эффективности и снижению временных затрат на выполнение рабочих процессов.
3. Выявление требований к разрабатываемой системе, выполняющей функции сетевого трафика на компьютерах сотрудников организации.

Первая часть работы посвящена рабочим процессам компании и проблемам в них. Далее мы рассмотрим возможности для решения этих проблем с помощью методов контроля сетевого трафика. В конечном итоге представляется набор требований к новой системе контроля трафика. Заключительная часть содержит выводы и перспективы дальнейших исследований.

Основная часть.

Компания ООО “52 lab” – студия креативного агентства и продакшена, которая занимается реализацией медиапроектов для федеральных каналов, рекламных кампаний и других различных медиакомпаний от идеи до полной реализации – съемка, монтаж и постпродакшен. Это могут быть как телепередачи, рекламные ролики, так и целые документальные фильмы или сериалы, выход которых заранее объявляется в оговоренную дату. Видеофайлы, с которыми в основном работают сотрудники студии, могут достигать десятков и сотни гигабайт, они являются основным ресурсом рабочих проектов компании. Нередко бывает, что проекты должны выполняться в узких временных рамках, дедлайн может сдвигаться, в таком случае скорость передачи таких больших объемов данных для их оценки, замечаний, очень важна. Не менее важным моментом является и то, что сотрудники компании – творческие люди, которые работают удаленно и работа которых связана с креативностью, часто источником их вдохновения для проектной деятельности становятся различные ресурсы в соцсетях, видеохостингах, мессенджерах и других Интернет-площадках. Однако, как показал анализ внутри организации, сотрудники часто используют такие ресурсы сверх меры, вызывая простои в выполнении проектов. При этом контролировать работу удаленных сотрудников звонками или сообщениями в мессенджерах менеджеры не могут по нескольким причинам – во-первых, это может отвлекать самих сотрудников от своей работы, а во-вторых, это не совсем современный подход к удаленному менеджменту.

Данные проблемные моменты можно решить при помощи применения методов шейпинга, ограничения и блокировки сетевого трафика:

Выставление приоритетов приложений, использование шейпинга трафика при сжатых сроках и близких дедлайнах, когда скорость как никогда важна, позволит выделять

больше сетевых ресурсов для приложения, которое выполняет отправку медиаконтента (например, браузер через почту), что позволяет повысить эффективность сотрудников и снизить простои.

Метод блокировок сетевого трафика может использоваться всеми компаниями для тотального контроля и уверенности в том, что сотрудники тратят время только на рабочие задачи, а также для защиты корпоративных данных и интеллектуальной собственности посредством запрета на посещение потенциально вредоносных ресурсов в Интернете, которые могут стать причиной несанкционированного доступа к ней.

Представленные методы контроля трафика требуют личной настройки всех правил каждым сотрудником или администратором. Это может занимать много времени, если машин много, и может быть критично если необходимо применить эти сетевые правила быстро (к примеру, скоро трансляция медиаконтента в эфир телеканала), в таком случае централизованное управление всеми машинами позволит в одном месте и быстро все сделать.

Проектирование интегрированной системы.

С учетом выявленных методов контроля трафика и анализа существующих решений на рынке систем для управления сетевым трафиком, проектируется и разрабатывается информационная система управления сетевым трафиком, требования к ее разработке представлены ниже:

1. Система должна позволять применять различного рода сетевые правила, которые проецируются на рассмотренные ранее методы контроля трафика (блокировки, ограничения по максимальной скорости и объему, приоритезация).
2. Система должна представлять широкий спектр критериев или фильтров, которые должны служить маркерами для контролируемого трафика и последующего применения правил к нему.
3. Система должна предоставлять возможность импортирования и экспортирования сетевых правил не только с помощью файлов конфигураций, но и с помощью сохранения на сервере.
4. Система должна предоставлять удаленного задания сетевых правил на компьютере сотрудника.

На основе результатов исследования предлагаются следующие практические рекомендации:

1. Внедрение разработанной системы в организации, где обеспечение безопасности и эффективного управления сетевой активностью является критическим.

2. Регулярное обновление и модернизация системы в соответствии с новыми требованиями пользователей системы.

3. Проведение обучения и поддержки пользователей для эффективного использования всех функциональных возможностей системы.

Заключение.

Основываясь на проведенном исследовании, разработанная система представляет собой значимый шаг в области управления корпоративным информационным трафиком, обеспечивая не только высокий уровень безопасности, но и создание точек для решения проблем эффективного решения рабочих задач. Практическое внедрение данной системы может эффективно поддерживать современные потребности в области информационной безопасности и управления сетевым трафиком.

Литература

1. Олифер В. Г., Олифер Н. А. 0-54 Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. — СПб.: Питер, 2010 — 944 е.: ил
2. Родичев Ю. А. Р60 Нормативная база и стандарты в области информационной безопасности. Учебное пособие. — СПб.: Питер, 2017. — 256 с.: ил. — (Серия «Учебник для вузов»).
3. Сергеев А. Н. Основы локальных компьютерных сетей: Учебное пособие. – СПб.: Издательство «Лань», 2016. – 184 с.: ил. - (Учебники для вузов. Специальная литература).
4. Джеймс Куроуз, Кит Росс. Компьютерные сети : Нисходящий подход. – 6-е изд. – Москва : Издательство «Э», 2016. – 912 с. – (Мировой компьютерный бестселлер).
5. Джереми Сиэрс, Майкл Шмидт, Джеймс Уиндзор. "TCP/IP Протоколы сетевого стека". — СПб.: Питер, 2019. — 880 с.