ВЕБ-ПРИЛОЖЕНИЕ ДЛЯ УПРАВЛЕНИЯ МЕЖСЕТЕВЫМ ЭКРАНОМ

Жихар А.Г., студент

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Медведев С.А. – канд. техн. наук, доцент

Современные организации сталкиваются с вызовами эффективного управления сетевой безопасностью в условиях постоянно растущих киберугроз и сложных IT-инфраструктур. Ручное администрирование межсетевых экранов и настройка правил безопасности часто занимает значительное время и требует глубоких знаний в области сетевой безопасности, что может привести к неэффективности в реагировании на инциденты и увеличению уязвимостей. Традиционные решения по управлению межсетевыми экранами не всегда обеспечивают такие возможности, как интеллектуальный анализ трафика, автоматическое обновление правил и интеграцию с другими системами защиты, что делает их недостаточно эффективными для современного бизнеса. Также наличие большого объема сетевого трафика и разнообразие используемых приложений усложняют процессы мониторинга и анализа событий безопасности. Сложные архитектуры сетей, включая облачные решения и удаленные рабочие места, требуют более гибких подходов к управлению безопасностью. Таким образом, традиционные методы не только замедляют процесс реакции на инциденты, но и увеличивают вероятность человеческой ошибки, что может привести к серьезным угрозам для целостности и конфиденциальности данных. Разработка специализированного веб-приложения для управления межсетевым экраном позволяет автоматизировать процессы настройки и мониторинга безопасности, оптимизировать использование ресурсов сети и значительно сократить время на реагирование на угрозы. Внедрение таких решений обеспечит возможность проведения анализа в реальном времени, выявления аномалий и проактивной защиты на основе поведенческих моделей трафика. Это, в свою очередь, повысит уровень защиты информации и позволит организациям сосредоточиться на стратегическом развитии, не отвлекаясь на рутинные задачи администрирования. Кроме того, упрощение интерфейса и автоматизация процессов делают систему доступной для пользователей с различным уровнем подготовки, что увеличивает общую безопасность всей инфраструктуры [1].

В процессе разработки было применено глубокое исследование предметной области, включая анализ существующих решений и требований пользователей различных категорий: сетевых администраторов, специалистов по безопасности и руководителей IT-отделов. На этапе проектирования разработана многослойная архитектура системы, которая обеспечивает четкое распределение обязанностей между компонентами: уровень представления, уровень бизнес-логики и уровень доступа к данным. Для реализации использованы современные технологии и инструменты: и Python и его фреймворк Tornado для построения серверной части и REST API, PostgreSQL для хранения информации о сетевых правилах и событиях, а также Nginx для управления серверными запросами [2]. Пользовательский интерфейс разработан с применением HTML5, CSS3, JavaScript для обеспечения адаптивности на различных устройствах. При проектировании интерфейса учтены принципы юзабилити и доступности для обеспечения комфортного взаимодействия пользователей с системой.

Разработанное программное средство обеспечивает эффективную автоматизацию процесса управления межсетевым экраном, повышает удобство мониторига сетевой безопасности и способствует лучшему контролю над сетевыми ресурсами. Применение современных веб-технологий и многослойной архитектуры гарантирует масштабируемость системы, возможность добавления новых функциональных модулей и интеграции с внешними сервисами безопасности. Система легко адаптируется к изменяющимся требованиям пользователей и росту объема данных о сети, что обеспечивает долгосрочное развитие платформы управления безопасностью. Внедрение данной системы позволит организациям сократить время на настройку и мониторинг межсетевых экранов, повысить уровень защиты информации и общую эффективность работы сети. Высокая рентабельность проекта подтверждает его целесообразность и коммерческий потенциал. Дальнейшее развитие системы может включать расширение функциональности путем добавления интеграции с инструментами анализа и отчетности, внедрения алгоритмов машинного обучения для улучшения автоматизации мониторинга угроз и разработки дополнительных средств аналитики для оценки состояния сетевой безопасности.

Список использованных источников:

1. Мартин, Р. Чистая архитектура. Искусство разработки программного обеспечения / Р. Мартин. – СПб : Питер, 2022. – 352 с.

2. Основы REST API для веб-приложений / Хэдс, Д. – O'Reilly Media, 2018. – 280 с.