

DOI: <https://doi.org/10.60797/IRJ.2024.146.99>

РАЗРАБОТКА И ТЕСТИРОВАНИЕ ДЕМОНСТРАЦИОННОЙ СРЕДЫ ДЛЯ ОТЕЧЕСТВЕННЫХ СЕТЕВЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Научная статья

Махфуд Б.А.¹, Мангушева А.Р.^{2,*}, Кремлева Э.Ш.³, Лаптева М.Г.⁴

³ORCID : 0000-0003-0858-0575;

¹Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань, Российская Федерация

^{2,4}Казанский национальный исследовательский технологический университет, Казань, Российская Федерация

³Казанский национальный исследовательский технический университет им. А. Н. Туполева – КАИ, Казань, Российская Федерация

* Корреспондирующий автор (alinamr[at]mail.ru)

Аннотация

В данной работе рассматривается проблема импортозамещения в сфере сетевых средств защиты информации в России, обусловленная уходом зарубежных производителей с отечественного рынка и увеличением количества кибератак. Внедрение отечественных средств защиты информации, соответствующих требованиям российских стандартов безопасности, позволит снизить риски, связанные с использованием зарубежного ПО и оборудования, и повысить уровень информационной безопасности в стране. Цель работы заключается в создании демонстрационной среды информационной инфраструктуры с применением отечественного межсетевых экранов нового поколения. Для её достижения решаются следующие задачи: выявить функциональные требования к сетевым средствам защиты информации, провести проектирование демонстрационной среды и осуществить её тестирование с развернутым отечественным межсетевым экраном. Основное внимание уделяется созданию демонстрационной тестовой среды для оценки функциональности и безопасности отечественного межсетевых экранов нового поколения. Проведенные тестирования различных модулей, таких как антивирус и система обнаружения и предотвращения вторжений (СОВ), а также нагрузочные тестирования с использованием ПО Iperf и Cisco TRex показали, что производительность межсетевых экранов UserGate не зависит линейно от количества включенных модулей и количества правил, продемонстрировали его способность эффективно блокировать вредоносные активности и защищать корпоративные сети. Прделанная работа вносит значительный вклад в процесс импортозамещения в сфере сетевой защиты информации и демонстрирует потенциал российских продуктов для надежной защиты корпоративных сетей от различных угроз и атак.

Ключевые слова: импортозамещение, информационная безопасность, межсетевых экран, система обнаружения и предотвращения вторжений, антивирус, нагрузочное тестирование, защита информации, отечественные средства защиты, UserGate, кибератаки, VPN, HTTPS-инспекция.

DEVELOPMENT AND TESTING OF A DEMONSTRATION ENVIRONMENT FOR DOMESTIC NETWORK INFORMATION PROTECTION TOOLS

Research article

Makhfud B.A.¹, Mangusheva A.R.^{2,*}, Kremleva E.S.³, Lapteva M.G.⁴

³ORCID : 0000-0003-0858-0575;

¹Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan, Russian Federation

^{2,4}Kazan National Research Technological University, Kazan, Russian Federation

³Kazan National Research Technical University named after A. N. Tupolev – KAI, Kazan, Russian Federation

* Corresponding author (alinamr[at]mail.ru)

Abstract

This work examines the problem of import substitution in the field of network information protection equipment in Russia due to the withdrawal of foreign manufacturers from the domestic market and the increasing number of cyberattacks. The implementation of domestic information protection means that meet the requirements of Russian security standards will reduce the risks associated with the use of foreign software and equipment and increase the level of information security in the country. The aim of the work is to create a demonstration environment of information infrastructure with the use of domestic firewall of new generation. To achieve it, the following tasks are solved: to identify functional requirements for network means of information protection, to design a demonstration environment and to test it with a deployed domestic firewall. The main focus is on creating a demonstration test environment to evaluate the functionality and security of a new generation domestic firewall. Testing of various modules, such as antivirus and intrusion detection and prevention system (IDS), as well as load testing using Iperf and Cisco TRex software showed that UserGate firewall performance does not depend linearly on the number of enabled modules and the number of rules, and demonstrated its ability to effectively block malicious activity and protect corporate networks. The performed work makes a significant contribution to the process of import substitution in the field of network information protection and demonstrates the potential of Russian products for reliable protection of corporate networks from various threats and attacks.

Keywords: import substitution, information security, firewall, intrusion detection and prevention system, antivirus, load testing, information protection, domestic protection means, UserGate, cyberattacks, VPN, HTTPS inspection.

Введение

Актуальность темы импортозамещения в сфере сетевых средств защиты информации обусловлена существенными изменениями на российском рынке информационной безопасности (ИБ). Уход зарубежных производителей с отечественного рынка ИБ привел к полной или частичной блокировке их решений в сетевых инфраструктурах конечных потребителей, создавая необходимость в развитии и применении отечественных альтернатив. Таким образом, возникает потребность в анализе имеющихся сетевых средств защиты информации, произведенных в Российской Федерации, и оценке их эффективности и применимости в различных сетевых инфраструктурах.

Для оценки эффективности отечественных решений в области сетевых средств защиты информации [1], [2] требуется разработать демонстрационную тестовую среду. Разработка среды позволит не только протестировать функциональность и безопасность российских продуктов, но и продемонстрировать их потенциал специалистам информационной безопасности и другим заинтересованным сторонам, способствуя укреплению доверия к отечественным средствам защиты информации и содействуя развитию национальной отрасли информационной безопасности.

При выборе отечественного решения в области защиты информации необходимо провести всесторонний анализ требований, которые обычно предъявляются к зарубежным средствам и технологиям. Этот анализ должен стать неотъемлемой частью процесса выбора отечественных средств защиты информации (СЗИ). Кроме того, при определении и выборе отечественного СЗИ необходимо проанализировать его универсальность для различных корпоративных сетей и его совместимость с другими информационными системами, наиболее часто встречающимися в сетевых инфраструктурах предприятий.

Цель данной работы заключается в создании демонстрационной среды информационной инфраструктуры с применением отечественного межсетевых экранов нового поколения. Для достижения этой цели поставлены задачи:

1. Выявить функциональные требования, предъявляемые к сетевым средствам защиты информации.
2. Провести проектирование демонстрационной среды информационной инфраструктуры.
3. Провести тестирование демонстрационной среды с развернутым отечественным межсетевым экраном.

Анализ актуальности импортозамещения на отечественном рынке информационной безопасности показывает, что уход зарубежных производителей с российского рынка ИБ и рост атак со стороны зарубежных злоумышленников привели к практически одномоментному открытию большого количества уязвимостей в сетевой инфраструктуре предприятий. Это увеличивает шансы получения несанкционированного доступа к информационным системам и информации, обрабатываемой в них.

Согласно данным компании «Positive Technologies», в 2023 году продолжилась тенденция наращивания количества и разнообразия кибератак на российские компании [3]. За первое полугодие 2023 года количество инцидентов выросло на 17% относительно того же периода 2022 года. Выросла доля целевых атак, они составили 78% от общего количества [4]. Для организаций самыми распространенными последствиями успешных кибератак стали утечки конфиденциальной информации (67%) и нарушение основной деятельности (44%) [5].

На начало 2022 года преобладающую долю рынка сетевой информационной безопасности занимали межсетевые экраны иностранного производства. Однако дальнейшие события привели к существенным сложностям для организаций, использующих эти продукты:

- Блокировка работы функционала своих продуктов на территории РФ.
- Ограничение доступа к базам знаний и технической поддержке.
- Блокировка продаж лицензий на существующее оборудование.

Все это оказало влияние на развитие процесса импортозамещения в сфере ИБ на отечественном рынке. Кроме того, законодательные меры, такие как Указ Президента Российской Федерации №166 от 30.03.2022 г., устанавливающий запрет на применение иностранных ПО и оборудования на стратегических информационных системах с января 2025 года.

Новизна и оригинальность работы заключаются в разработке и тестировании отечественного решения, способного заменить зарубежные аналоги, обеспечивая высокий уровень защиты корпоративных сетей. В отличие от существующих зарубежных решений, отечественные межсетевые экраны адаптированы к российским стандартам безопасности и законодательным требованиям, что делает их предпочтительными для использования в отечественных корпоративных сетях.

Таким образом, данный проект направлен на разработку и внедрение отечественного решения в сфере сетевой защиты информации, что является важным шагом для обеспечения информационной безопасности российских предприятий и организаций.

Функциональные требования к межсетевым экранам нового поколения

Для обеспечения надежной защиты корпоративных сетей от различных угроз и атак необходимо тщательно определить ключевые функции, которыми должны обладать межсетевые экраны нового поколения. Это особенно актуально в условиях импортозамещения, когда отечественные производители стремятся предложить продукты, конкурентоспособные с международными аналогами. Анализ функциональных требований, выявленных в опросе специалистов по информационной безопасности предприятий, позволяет выделить следующие ключевые характеристики, необходимые для выбора решения для демонстрационной среды:

1) Поддержка централизованного управления: централизованное управление позволяет администраторам эффективно контролировать и настраивать межсетевые экраны из одного центрального интерфейса. Это упрощает

управление большими сетевыми инфраструктурами, снижает затраты на администрирование и минимизирует риск ошибок при настройке безопасности.

2) Наличие функционала системы обнаружения и предотвращения вторжений (IDPS): система обнаружения и предотвращения вторжений является критически важной для своевременного выявления и нейтрализации угроз. Она анализирует сетевой трафик в реальном времени, используя сигнатуры и эвристические методы для обнаружения аномалий и вредоносной активности.

3) Встроенный потоковый антивирус: наличие встроенного антивируса позволяет межсетевому экрану проверять входящий и исходящий трафик на наличие вредоносного программного обеспечения. Это обеспечивает дополнительный уровень защиты от вирусов, червей и других типов вредоносного ПО, проникающего через сеть.

4) Возможность организации защищенного удаленного доступа (VPN): защищенный удаленный доступ с использованием VPN-клиента необходим для обеспечения безопасного подключения удаленных пользователей к корпоративной сети. Это особенно важно в условиях увеличения числа удаленных сотрудников и необходимости обеспечения безопасности при доступе к корпоративным ресурсам.

5) Механизмы обеспечения отказоустойчивости, резервирования и кластеризации: поддержка отказоустойчивости и резервирования критически важна для обеспечения непрерывной работы сетевой инфраструктуры. Кластеризация межсетевых экранов позволяет распределить нагрузку и обеспечить автоматическое переключение на резервный узел в случае сбоя основного.

6) Поддержка не менее 1000 приложений: широкая поддержка приложений позволяет межсетевому экрану эффективно управлять и контролировать трафик различных приложений, обеспечивая их безопасность и производительность.

7) Возможность URL-фильтрации: URL-фильтрация предоставляет возможность блокировать доступ к нежелательным или вредоносным веб-сайтам, что способствует защите пользователей и корпоративной сети от фишинга и других интернет-угроз.

8) Блокировка доступа к вредоносным сайтам: эта функция позволяет автоматически блокировать доступ к сайтам, содержащим вредоносное ПО или участвующим в фишинговых атаках, защищая пользователей и данные от киберугроз.

9) Поддержка протоколов динамической маршрутизации: динамическая маршрутизация позволяет межсетевому экрану автоматически адаптироваться к изменениям в сетевой топологии, обеспечивая оптимальный маршрут для трафика и повышая общую производительность сети.

10) Поддержка HTTPS-инспекции: инспекция HTTPS-трафика необходима для проверки зашифрованных данных, что позволяет обнаруживать и блокировать угрозы, скрытые в зашифрованных соединениях.

11) Режим пакетной фильтрации с контролем сессий: пакетная фильтрация с контролем сессий позволяет более детально анализировать сетевой трафик, обеспечивая высокий уровень безопасности и предотвращая несанкционированный доступ.

12) Наличие сертификата ФСТЭК не ниже 6 уровня доверия: сертификат ФСТЭК подтверждает соответствие межсетевому экрану установленным стандартам безопасности и надежности, что является обязательным требованием для использования в государственных и корпоративных сетях.

13) Интеграция с контроллерами домена: интеграция с контроллерами домена позволяет межсетевому экрану эффективно управлять доступом пользователей и контролировать сетевой трафик на основе учетных записей и групп, определенных в домене.

14) Включение отдельных сигнатур в режим обнаружения или предотвращения: гибкость в управлении сигнатурами позволяет адаптировать систему обнаружения и предотвращения вторжений под специфические требования безопасности организации, повышая эффективность защиты.

Эти функциональные требования являются основой для разработки и выбора межсетевых экранов нового поколения, обеспечивая надежную защиту корпоративных сетей от различных угроз и атак.

Проектирование демонстрационной среды

Ниже представлена информация о физическом и логическом подключении демонстрационной среды. Данная информация является основой для дальнейшей настройки компонентов стенда.

Компоненты демонстрационного стенда подключаются к сетевому оборудованию согласно таблице 1.

Таблица 1 - Параметры подключения оборудования

DOI: <https://doi.org/10.60797/IRJ.2024.146.99.1>

Оборудование	Порт	Сетевое оборудование	Порт
Основной шлюз ПАК UserGate E1000	port8	Внутренний коммутатор Cisco Extreme №1	XGi0/0/25
	port9	Внутренний коммутатор Cisco Extreme №1	XGi0/0/26
	port10	Внешний коммутатор Cisco Extreme №2	XGi0/0/25
	port11	Внешний коммутатор	XGi0/0/26

Оборудование	Порт	Сетевое оборудование	Порт
		Cisco Extreme №2	
	port6	Резервный шлюз ПАК UserGate E1000	port6
	port7	Резервный шлюз ПАК UserGate E1000	port7
Резервный шлюз ПАК UserGate E1000	port8	Внутренний коммутатор Cisco Extreme №1	XGi0/0/27
	port9	Внутренний коммутатор Cisco Extreme №1	XGi0/0/28
	port10	Внешний коммутатор Cisco Extreme №2	XGi0/0/27
	port11	Внешний коммутатор Cisco Extreme №2	XGi0/0/28
	port6	Основной шлюз ПАК UserGate E1000	port6
	port7	Основной шлюз ПАК UserGate E1000	port7

Структурная схема подключения оборудования представлена ниже на рисунке 1.

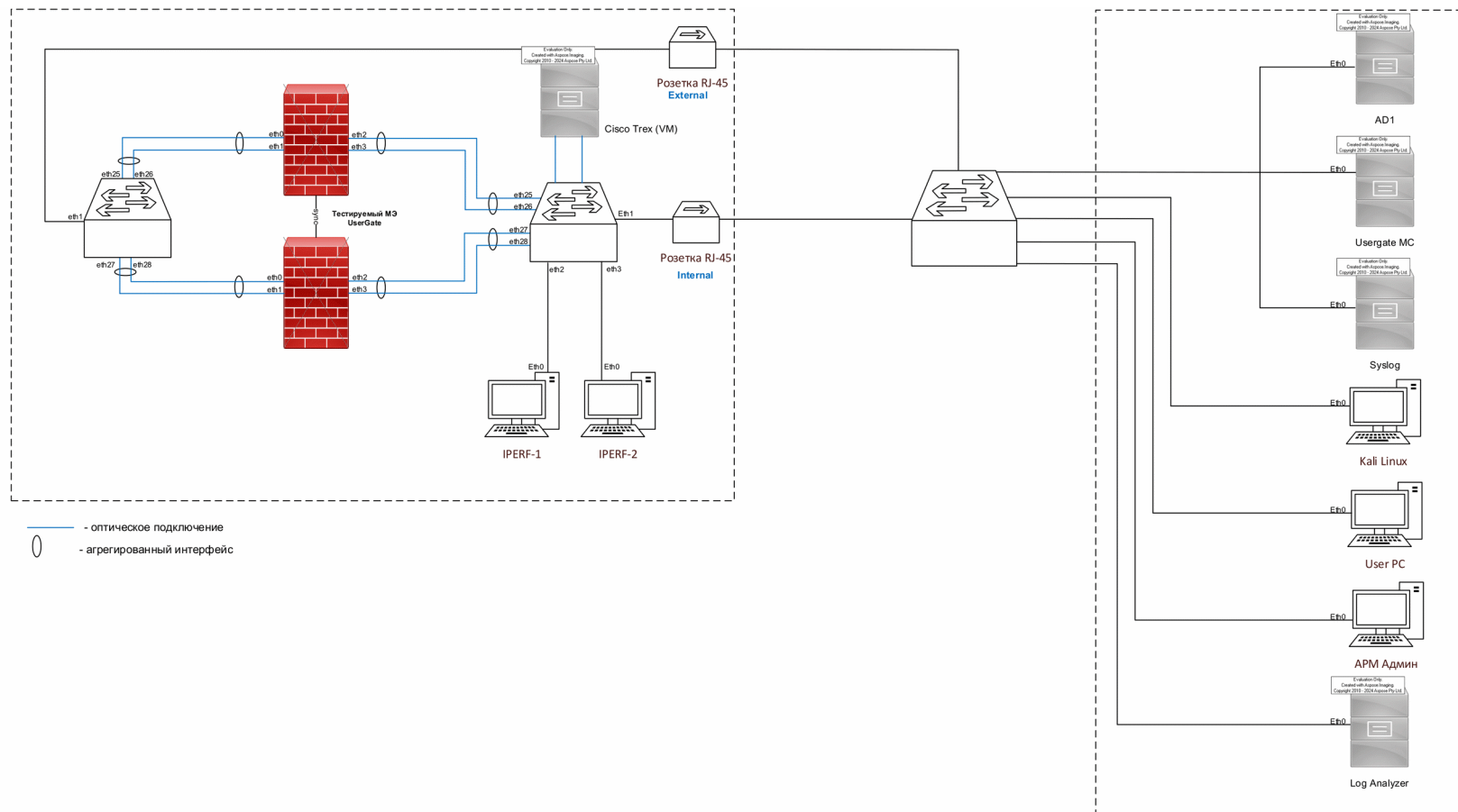


Рисунок 1 - Структурная схема
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.2>

Сегменты, выделяемые на компонентах демонстрационной среды приведены в таблице 2.

Таблица 2 - Сегменты, выделяемые на компонентах среды

DOI: <https://doi.org/10.60797/IRJ.2024.146.99.3>

Наименование сегмента	IP-адрес/маска	Номер Vlan
Сегмент Интернет	10.210.120.24/29	-
Сегмент тестовой нагрузки №1	192.168.10.0/29	10
Сегмент тестовой нагрузки №2	192.168.20.0/29	20
Сегмент синхронизации	192.168.255.252/30	-
Сегмент транзитный с внутренней сеть.	10.210.120.16/29	-
Сегмент пользовательский	192.168.11.0/24	11
Сегмент серверный	192.168.110.0/24	110
Сегмент нагрузочный	192.168.111.0/24	111
Внешний сегмент VPN (пользователи)	172.16.1.0/24	-

Настройка статической маршрутизации шлюзов кластеров МЭ и кластера криптографической защиты каналов связи выполняется в соответствии с таблицей 3.

Таблица 3 - Настройки статической маршрутизации кластера МЭ

DOI: <https://doi.org/10.60797/IRJ.2024.146.99.4>

Сеть назначения	Маска подсети	Шлюз
0.0.0.0	0.0.0.0	10.210.120.30
192.168.11.0	255.255.255.0	10.210.120.22
192.168.110.0	255.255.255.0	10.210.120.22
192.168.111.0	255.255.255.0	10.210.120.22

Логическая схема подключения оборудования стенда приведена на рисунке 2.

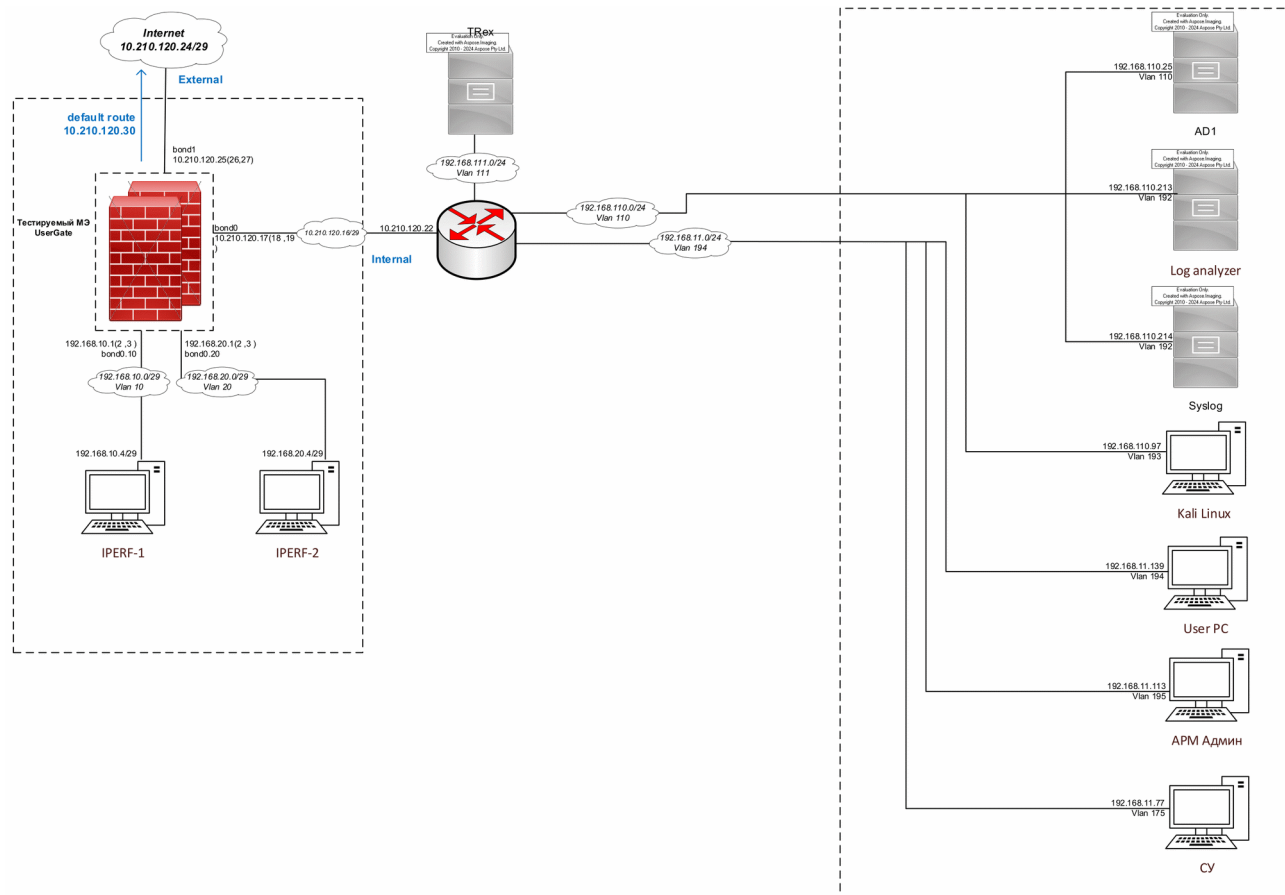


Рисунок 2 - Логическая схема
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.5>

Данные о физическом и логическом подключении демонстрационной среды являются результатом проектирования этой среды. Эта информация представляет собой основу для начальной конфигурации компонентов системы и позволяет обеспечить их взаимосвязь и работоспособность. Важно понимать, что эти данные не только описывают, как компоненты связаны друг с другом, но и определяют шаги по настройке и эксплуатации системы.

Тестирование демонстрационной среды

Для проверки интеграции работы МЭ UserGate с Active Directory [6], [7] требуется создать тестовое правило для проверяемого пользователя (Рис. 3).

#	Название	Действие	Зона исто...	Адрес исто...	Зона назн...	Адрес назн...	Пользоват...	Сервис	Приложен...	Время	Сценарий	Устройств...
Пре-правила												
1	Управление устройствами	Разреш...	Любая	Любая	Любая	Любая	Любой	Любой	Любой	Любой	---	Любая
2	Тестовое правило автор...	Разреш...	Любая	Любая	Любая	INTERN...	Тестов...	Любой	Любой	Любой	---	Любая
3	UserGate to UserGate	Разреш...	Любая	UserGate	Любая	UserGate	Любой	Любой	Любой	Любой	---	Любая

Рисунок 3 - Разрешающее правило
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.6>

Введем тестовую машину с IP адресом 192.168.11.139 в тестовый домен и проведем авторизации под пользователей Тестовый пользователь. Проведем проверку доступа в интернет. Доступ в интернет у тестового пользователя имеется, также проверяем, что пользователь определился в журналах событий UserGate [8], [9] (Рис. 4).

Узел:	fw-lab-01
Время:	16:39:06
Пользователь:	ti-lab.ru\testuser
Действие:	✔ Разрешить
Тип:	🌐 Межсетевой экран
Правило:	Тестовое правило авторизации
Приложение:	📄 SSL
Протокол прикладного уровня:	SSL
Протокол:	TCP
Зона источника:	🏠 Transit to LAN
Страна источника:	🔍 Неизвестно
IP источника:	192.168.11.139
Порт источника:	62775
Зона назначения:	🏠 Untrusted
Страна назначения:	🇺🇸 United States
IP назначения:	8.8.8.8
Порт назначения:	443
Байт отправлено/получено:	1206 / 52
Пакетов отправлено/получено:	4 / 1

Рисунок 4 - Журнал трафика разрешающий
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.7>

Изменим действие правила на «Запретить» и проверим доступ в интернет по данному правилу (Рис. 5).

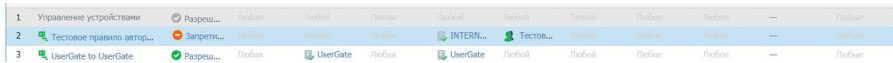


Рисунок 5 - Запрещающее правило
 DOI: <https://doi.org/10.60797/IRJ.2024.146.99.8>

При обращении к ресурсу 8.8.8.8 трафик не проходит, соединение блокируется правилом №1, о чем присутствует запись в журнале системных событий сервера Log Analyzer (Рис. 6).

Узел:	fw-lab-01
Время:	16:42:43
Пользователь:	ti-lab.ru\testuser
Действие:	Запретить
Тип:	Межсетевой экран
Правило:	Тестовое правило авторизации
Приложение:	SSL
Протокол прикладного уровня:	SSL
Протокол:	TCP
Зона источника:	Tranzit to LAN
Страна источника:	Неизвестно
IP источника:	192.168.11.139
Порт источника:	622315
Зона назначения:	Untrusted
Страна назначения:	United States
IP назначения:	8.8.8.8
Порт назначения:	443
Байт отправлено/получено:	176 / 21
Пакетов отправлено/получено:	4 / 1

Рисунок 6 - Журнал трафика запрещающий
 DOI: <https://doi.org/10.60797/IRJ.2024.146.99.9>

При проверке наличия данных событий в SIEM системе также был получен положительный результат. В системе сбора системных журналов успешно отображаются данные – это говорит о том, что система МЭ успешно отправляет syslog события в систему. Об этом также свидетельствует наличие пакетов syslog в файле, собранном командой tcpdump (Рис. 7).

1 0.000000	192.168.1.1	192.168.1.120	Syslog	453 USER.INFO
2 2.000551	192.168.1.1	192.168.1.120	Syslog	447 USER.INFO
3 2.000700	192.168.1.1	192.168.1.120	Syslog	448 USER.INFO
4 2.000836	192.168.1.1	192.168.1.120	Syslog	446 USER.INFO
5 48.004239	192.168.1.1	192.168.1.120	Syslog	448 USER.INFO
6 51.004473	192.168.1.1	192.168.1.120	Syslog	514 USER.INFO
7 61.018718	192.168.1.1	192.168.1.120	Syslog	494 USER.INFO
8 69.019491	192.168.1.1	192.168.1.120	Syslog	494 USER.INFO
9 75.020010	192.168.1.1	192.168.1.120	Syslog	449 USER.INFO
10 83.020835	192.168.1.1	192.168.1.120	Syslog	495 USER.INFO
11 94.021676	192.168.1.1	192.168.1.120	Syslog	494 USER.INFO
12 111.823548	192.168.1.1	192.168.1.120	Syslog	503 USER.INFO

Рисунок 7 - Файл tcpdump
 DOI: <https://doi.org/10.60797/IRJ.2024.146.99.10>

Для проверки модуля антивируса в системе UserGate были проведены работы по обращению к различным зловредным ресурсам из сети Интернет с тестовой рабочей машины. При обращении к зловредным ресурсам у тестового пользователя был оборван доступ в Интернет, а в журналах событий информационной безопасности отображаются соответствующие записи (Рис. 8, 9).

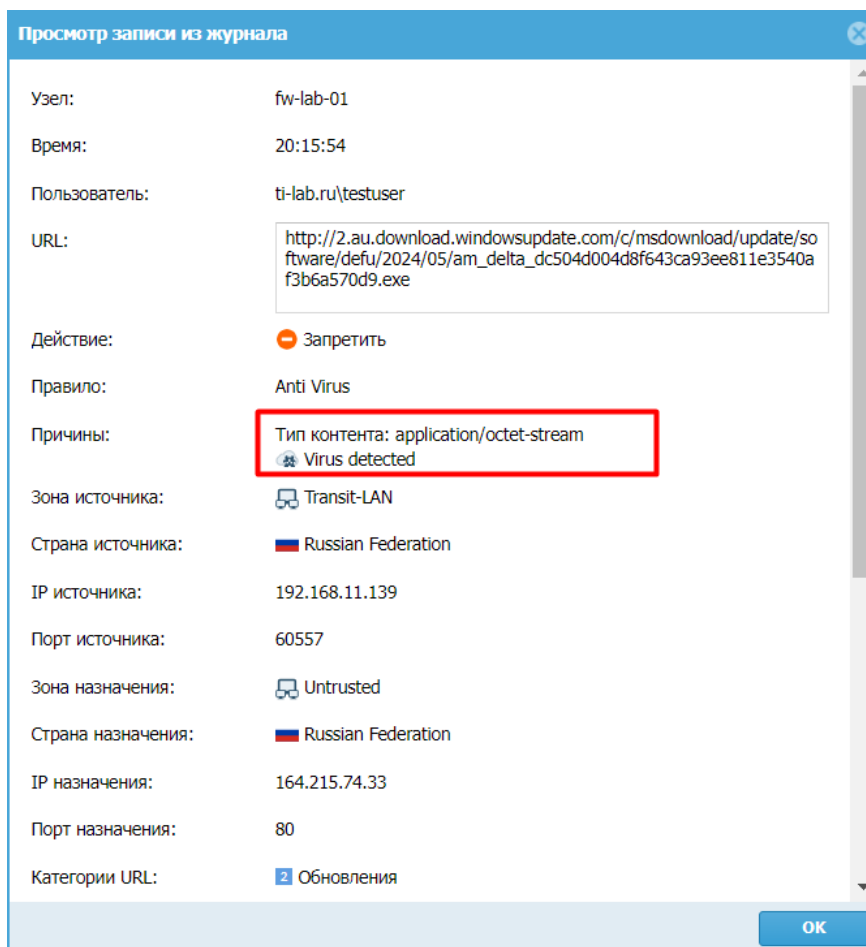


Рисунок 8 - Блокировка антивирусом
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.11>

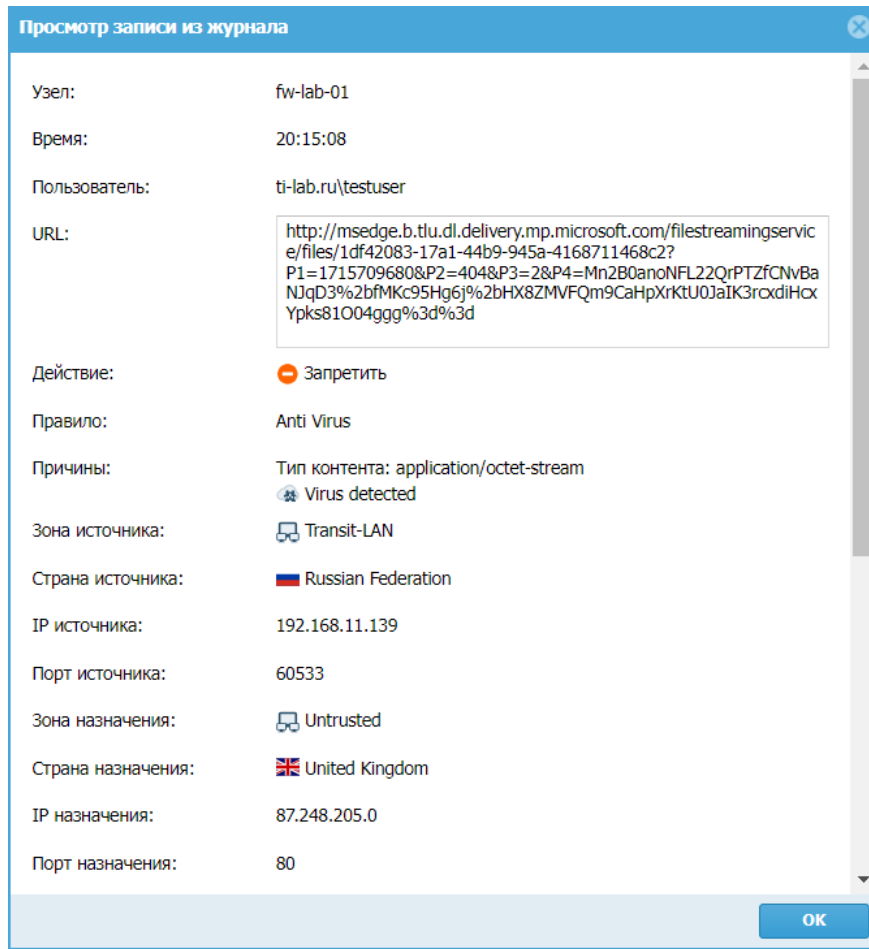


Рисунок 9 - Блокировка антивирусом
 DOI: <https://doi.org/10.60797/IRJ.2024.146.99.12>

Для проверки работоспособности модуля COB запустим множественные сканирования через ОС Kali Linux командой nmap -sS -O 192.168.11.139. В результате многие порты были не обнаружены системой nmap, так как МЭ обрывал новые соединения, когда обнаружил сработки сигнатуры сканирования, о чем присутствует запись в журнале COB (Рис. 10).

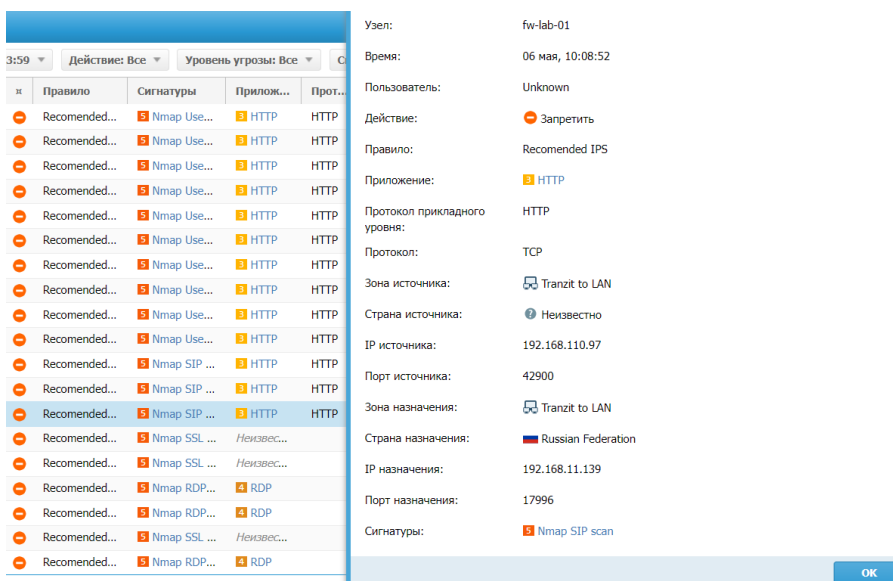


Рисунок 10 - Журналы COB
 DOI: <https://doi.org/10.60797/IRJ.2024.146.99.13>

Далее проводится проверка определения троянской программы, которая запускает реверсивное управление командной строки на атакуемом устройстве.

На время тестов отключим работу модуля COB и запустим выполнение зловредного троянского кода командой `msfpayload windows/meterpreter/reverse_tcp LHOST=<192.168.110.97> X > Desktop/Backdoor.exe`.

После создания файла с внедренным эксплойтом необходимо перенести файл на атакуемую машину и запустить его. Файл на созданной машине запустился без ошибок, эксплойт установлен успешно (Рис. 11).

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost .213
lhost => .213
msf exploit(handler) > exploit -j -z
[*] Exploit running as background job.

[*] Started reverse handler on .213:4444
[*] Starting the payload handler...
msf exploit(handler) > [*] Sending stage (769536 bytes) to .214
[*] Meterpreter session 1 opened .213:4444 -> .214:49220 at 2021-05-10 17:37:50 +0400
sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 2400 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
(c) 00000000 0000000000 (Microsoft Corp.), 2009. 000 000000000.
```

Рисунок 11 - Установка эксплойта в тестируемой машине
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.14>

Подключение к удаленному узлу, используя shell означает, что политики COB пропустила данный эксплойт, это означает, что эксплойт работает корректно.

Переведем модуль COB в активное состояние и повторим данный вид атаки, убедимся, что команда shell не дает никаких результатов, а в журналах событий модуля COB присутствуют соответствующие записи (Рис. 12).

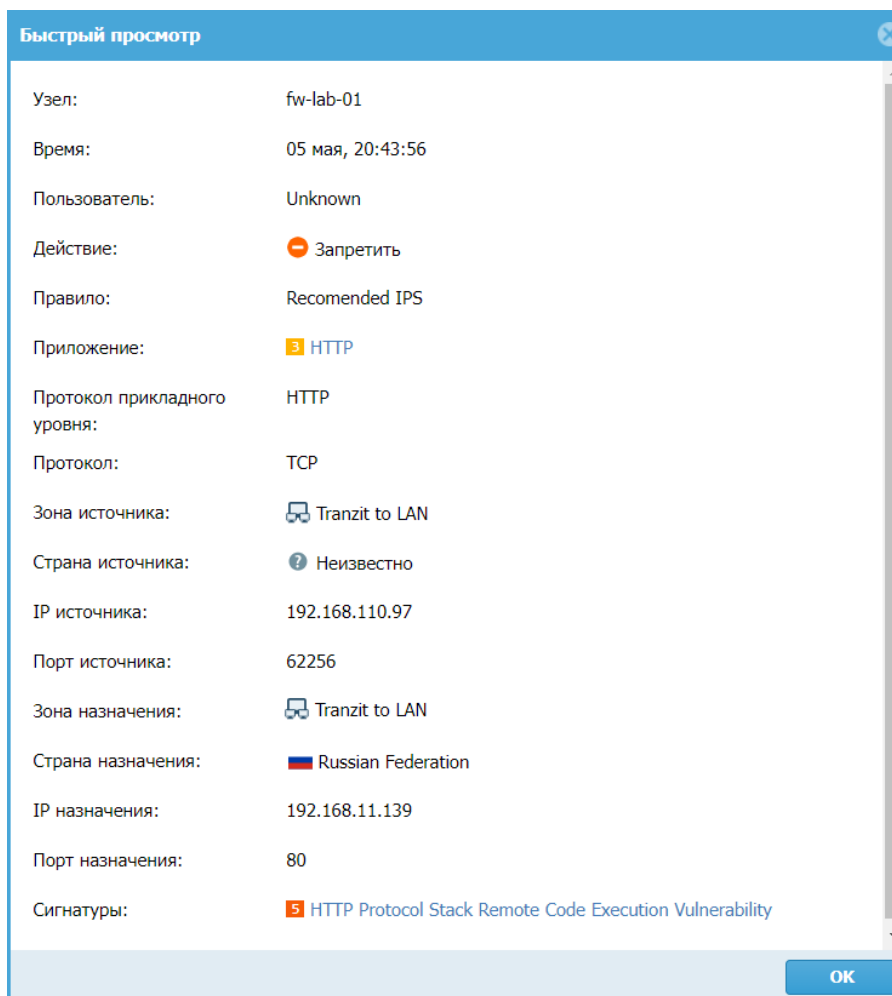


Рисунок 12 - Блокировка троянской активности
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.15>

Для нагрузочного тестирования будут использованы два варианта тестов:

- через ПО Iperf;
- через ПО Cisco TRex.

Рассмотрим первый вариант тестирования. Для реализации данного тестирования запустим ПО Iperf на обоих АРМах из сегментов сети 192.168.10.0/24 и 192.168.20.0/24. Один АРМ будет выступать в роли инициатора трафика, другой в качестве приемника трафика. Для получения максимально правдивых результатов команда для запуска ПО будет одинаковой для различных вариантов тестирования – iperf3.exe -c 192.168.10.4.

Параметры проведенного тестирования и его результаты представлены в таблице 3.

Таблица 4 - Результаты нагрузочного тестирования iperf

DOI: <https://doi.org/10.60797/IRJ.2024.146.99.16>

№ п/п	Включенные модули	Результат при 1 правиле МЭ, Гбит/с	Результат при 300 правилах МЭ, Гбит/с
1.	МЭ	1	1
2.	МЭ + АВ	1	1
3.	МЭ + СОВ	1	1
4.	МЭ+АВ+СОВ	1	0,98

По результатам нагрузочного тестирования видно, что ПО Iperf [10], [11] не может выдать количество трафика более 1 Гбит в секунду, в связи с этим результаты тестирования получаются не достоверными.

Приступим к тестированию 2 варианта реализации нагрузочных тестов. Для нагрузочных тестов был использован следующая конфигурация для генерации трафика:

- максимальные HTTPS = 800 000 активных сессий;
- генерация UDP трафика без сессий максимальная пропускная способность в 15 Гбит/с;
- EMIX трафик 10 GB/s и 786444 сессии.

По результатам данного варианта нагрузочного тестирования удалось получить следующие результаты (Табл. 4)

По результатам второго нагрузочного тестирования результаты при использовании разных модулей МЭ и разного количества правил практически идентичные. Это говорит о том, что производительность МЭ UserGate линейно не зависит от количества включенных модулей и количества правил МЭ.

Для получения более точных результатов тестирования требуется развернуть физический сервер с сетевой картой 40 Гбит/с для сервера нагрузочного тестирования. В рамках данной работы провести такого рода тесты не представляется возможным.

Таблица 5 - Результаты нагрузочного тестирования Cisco TRex

DOI: <https://doi.org/10.60797/IRJ.2024.146.99.17>

№ п/п	Включенные модули	Тип трафика	Результат при 1 правиле МЭ, Гбит/с	Результат при 300 правилах МЭ, Гбит/с
1.	МЭ	HTTPS	20	20
2.	МЭ	UDP	15	15
3.	МЭ	EMIX	10	10
4.	МЭ + АВ	HTTPS	20	19
5.	МЭ + АВ	UDP	15	13,5
6.	МЭ + АВ	EMIX	10	10
7.	МЭ+АВ+СОВ	HTTPS	20	19,8
8.	МЭ+АВ+СОВ	UDP	15	15
9.	МЭ+АВ+СОВ	EMIX	10	8,8

Для осуществления подключения и проверки работоспособности решения требуется настроить клиентскую машину под ОС Windows. Будут использованы встроенные в ОС средства установки VPN соединения. В окне установки VPN соединения требуется указать публичный IP адрес, к которому будут осуществляться подключения, а также метод подключения – для тестовой среды используется метод L2TP over IPsec (Рис. 13).

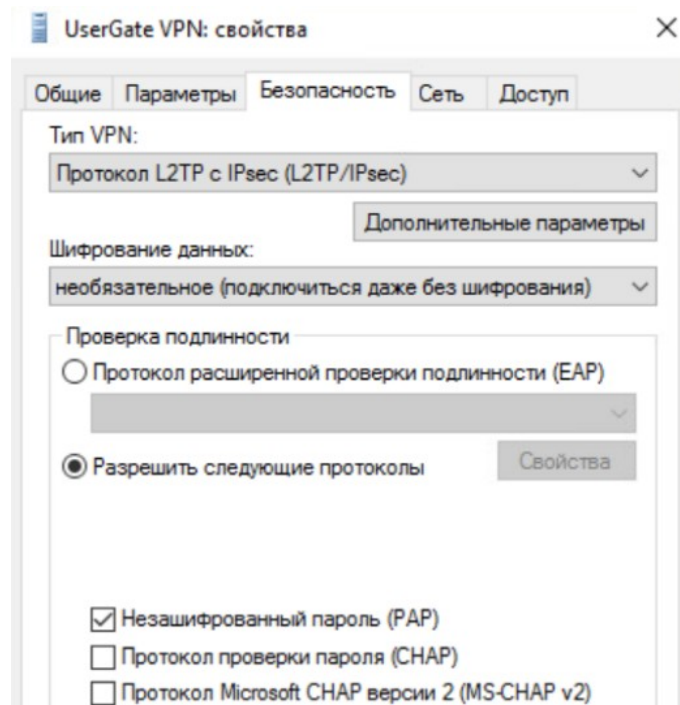


Рисунок 13 - Настройка VPN
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.18>

После успешного ввода логина пароля пользователь был подключен к инфраструктуре среды и имеет доступ к информационным ресурсам стенда. Также в журналах системных событий присутствует соответствующая запись об успешной установке подключения к VPN (Рис. 14).

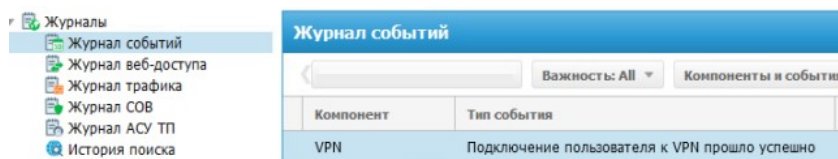


Рисунок 14 - Событие подключения к VPN
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.19>

Подключение через протокол Site-to-Site осуществляется аналогичным образом, что и для Remote Site, только подключение осуществляется уже не с конечным клиентом, а маршрутизирующим оборудованием. В нашем случае маршрутизатор Mikrotik, который расположен на удаленной площадке. Для инициализации удаленного подключения требуется назначить настройки первой и второй фазы VPN, данные фазы должны содержать идентичные алгоритмы, что и на UserGate. По результатам был создан профиль на оборудовании Mikrotik [12], который представлен ниже (Рис. 15, 16).

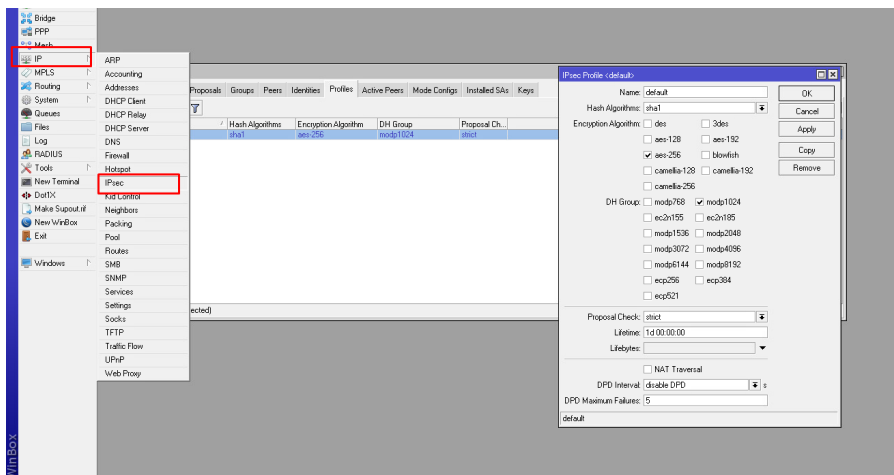


Рисунок 15 - Первая фаза Site-to-site
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.20>

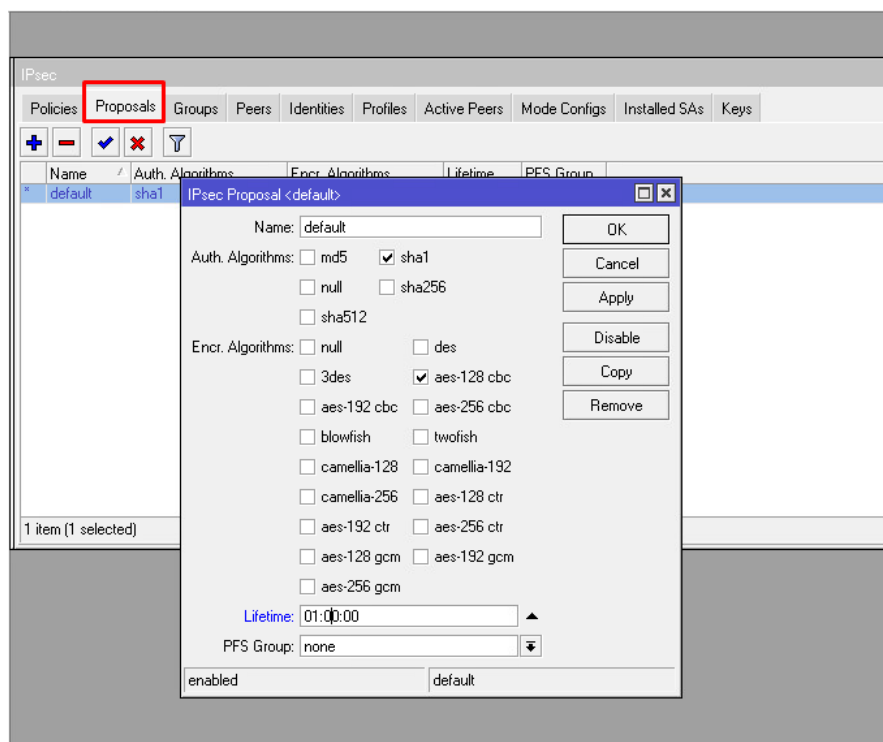


Рисунок 16 - Вторая фаза Site-to-site
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.21>

Следующим этапом выполняется указание публичного IP адреса шлюза, к которому будет осуществлено подключение и строится соединение VPN. По результату установки VPN соединения маршрутизатор Mikrotik и МЭ UserGate обмениваются маршрутами, которые участвуют в VPN, тем самым разрешая строить соединение между двумя ЛВС. Соединения VPN проходят также через политику МЭ, что позволяет руководить соединением и доступами к конечным ресурсам.

Заключение

Импортозамещение в сфере сетевых средств защиты информации является актуальной задачей, обусловленной значительными изменениями на российском рынке информационной безопасности. Уход зарубежных производителей и увеличение количества кибератак привели к необходимости разработки и внедрения отечественных решений, способных обеспечить надежную защиту информационных систем российских организаций.

В ходе работы была создана демонстрационная тестовая среда, которая позволила оценить функциональность и безопасность отечественного межсетевого экрана нового поколения. Были проведены тестирования различных модулей, таких как антивирус и система обнаружения и предотвращения вторжений, а также нагрузочные тестирования с использованием ПО Iperf и Cisco TRex [13], [14]. Результаты тестов показали, что производительность межсетевого экрана UserGate нелинейно зависит от количества включенных модулей и количества правил, а также

продемонстрировали его способность эффективно блокировать вредоносные активности и защищать корпоративные сети.

Внедрение отечественных средств защиты информации, соответствующих требованиям российских стандартов безопасности, позволит снизить риски, связанные с использованием зарубежного ПО и оборудования, и повысить уровень информационной безопасности в стране. Дальнейшее развитие и совершенствование отечественных решений в этой области будет способствовать укреплению национальной информационной безопасности и независимости.

Таким образом, данная работа внесла значительный вклад в процесс импортозамещения в сфере сетевой защиты информации и показала потенциал российских продуктов для обеспечения надежной и эффективной защиты корпоративных сетей от различных угроз и атак.

Конфликт интересов

Не указан.

Рецензия

Белашова Е.С., Казанский национальный исследовательский технический университет им. А.Н. Туполева – КАИ, Казань Российская Федерация
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.22>

Conflict of Interest

None declared.

Review

Belashova E.S., Kazan National Research Technical University named after A.N. Tupolev – KAI, Kazan Russian Federation
DOI: <https://doi.org/10.60797/IRJ.2024.146.99.22>

Список литературы / References

1. Утеев Г. Разработка децентрализованной системы идентификации личности по биометрическим данным с помощью технологии блокчейн и компьютерного зрения / Г. Утеев, Р.Ф. Гибадуллин // Международный научно-исследовательский журнал. — 2024. — № 4(142). — DOI: 10.23670/IRJ.2024.142.6.
2. Гибадуллин Р.Ф. Построение сети на основе технологии GPON / Р.Ф. Гибадуллин, А.П. Никитин, М.Ю. Перухин // Вестник Технологического университета. — 2017. — Т. 20. — № 5. — С. 104-108.
3. Lapshina I.V. Modern cybersecurity from the perspective of cognitive modeling / I.V. Lapshina, A.V. Kravets // Engineering Journal of Don. — 2023. — № 1(97). — P. 80-95.
4. Косякова В.В. Кибербезопасность в современном мире / В.В. Косякова, А.М. Наумова // Труды Братского государственного университета. Серия: Экономика и управление. — 2023. — Т. 1. — С. 123-126.
5. Ковалев О.Г. Кибербезопасность современной России: теоретические и организационно-правовые аспекты / О.Г. Ковалев, Н.В. Семенова // Столыпинский вестник. — 2021. — Т. 3. — № 1. — С. 13.
6. Толганбаев Т.К. Доменные службы active directory и ядро сервера / Т.К. Толганбаев // Вестник магистратуры. — 2014. — № 6-1(33). — С. 27-29.
7. Муратов И.И. Служба каталогов Active Directory Domain Services / И.И. Муратов, А.А. Перфильев // Наука и образование в жизни современного общества: сборник научных трудов по материалам Междунар. научно-практической конференции. — Тамбов: Юком, 2012. — Т. 1. — С. 100-101.
8. Максимов И. UserGate – безопасный прокси-сервер / И. Максимов // Системный администратор. — 2007. — № 5(54). — С. 17.
9. Шпак С. UserGate Proxy&Firewall Сертифицированный защитник сетей / С. Шпак // Системный администратор. — 2011. — № 3(100). — С. 110-112.
10. Свидетельство о государственной регистрации программы для ЭВМ № 2019663127. «Модуль настройки службы измерения пропускной способности сети по протоколу IPerf» («Модуль настройки IPerf»): № 2019662165: заявл. 07.10.2019; опубл. 10.10.2019; заявитель Общество с ограниченной ответственностью «Фактор-ТС».
11. Зайцев С.В. Интерфейсы управления инструментами измерения производительности на примере генератора трафика iPerf / С.В. Зайцев // Вестник научных конференций. — 2016. — № 6-2(10). — С. 39-41.
12. Tiara Komala Sutra M. Implementasi Load Balancing Dan Failover to Device Mikrotik Router Menggunakan Metode Equal Cost Multi Path (ECMP) / M. Tiara Komala Sutra, R. Ruuhwan, R. Rizal // Informatics and Digital Expert (INDEX). — 2023. — Vol. 4. — № 2. — P. 81-86. — DOI: 10.36423/index.v4i2.1189.
13. Крипаков А.В. Использование приложения Snappi-trex для генерации трафика с помощью Cisco trex / А.В. Крипаков // Современные проблемы лингвистики и методики преподавания русского языка в ВУЗе и школе. — 2022. — № 37. — С. 1447-1452.
14. Райхлин В.А. Конструктивное моделирование систем информатики / В.А. Райхлин, И.С. Вершинин, Р.Ш. Минязев [и др.] — Казань: Фэн, 2016. — 312 с.

Список литературы на английском языке / References in English

1. Uteev G. Razrabotka decentralizovannoj sistemy identifikacii lichnosti po biometricheskim dannym s pomoshh'ju tehnologii blokchejn i komp'yuternogo zrenija [Development of decentralized system of personal identification by biometric data using blockchain technology and computer vision] / G. Uteev, R.F. Gibadullin // Mezhdunarodnyj nauchno-issledovatel'skij zhurnal [International Research Journal]. — 2024. — № 4(142). — DOI: 10.23670/IRJ.2024.142.6. [in Russian]
2. Gibadullin R.F. Postroenie seti na osnove tehnologii GPON [Network construction on the basis of GPON technology] / R.F. Gibadullin, A.P. Nikitin, M.Ju. Peruhin // Vestnik Tehnologicheskogo universiteta [Bulletin of Technological University]. — 2017. — Vol. 20. — № 5. — P. 104-108. [in Russian]

3. Lapshina I.V. Modern cybersecurity from the perspective of cognitive modeling / I.V. Lapshina, A.V. Kravets // *Engineering Journal of Don*. — 2023. — № 1(97). — P. 80-95.
4. Kosjakova V.V. Kiberbezopasnost' v sovremennom mire [Cyber security in the modern world] / V.V. Kosjakova, A.M. Naumova // *Trudy Bratskogo gosudarstvennogo universiteta. Serija: Jekonomika i upravlenie* [Proceedings of Bratsk State University. Series: Economics and Management]. — 2023. — Vol. 1. — P. 123-126. [in Russian]
5. Kovalev O.G. Kiberbezopasnost' sovremennoj Rossii: teoreticheskie i organizacionno-pravovye aspekty [Cybersecurity of modern Russia: theoretical and organizational-legal aspects] / O.G. Kovalev, N.V. Semenova // *Stolypinskij vestnik* [Stolypin's Bulletin]. — 2021. — Vol. 3. — № 1. — P. 13. [in Russian]
6. Tolganbaev T.K. Domennye sluzhby active directory i jadro servera [Active directory domain services and server core] / T.K. Tolganbaev // *Vestnik magistratury* [Bulletin of Magistracy]. — 2014. — № 6-1(33). — P. 27-29. [in Russian]
7. Muratov I.I. Sluzhba katalogov Active Directory Domain Services [Active Directory Domain Services] / I.I. Muratov, A.A. Perfil'ev // *Nauka i obrazovanie v zhizni sovremennogo obshhestva: sbornik nauchnyh trudov po materialam Mezhdunar. nauchno-prakticheskoy konferencii* [Science and education in the life of modern society: a collection of scientific papers on the materials of the International Scientific and Practical Conference]. — Tambov: Jukom, 2012. — Vol. 1. — P. 100-101. [in Russian]
8. Maksimov I. UserGate – bezopasnyj proksi-server [UserGate – a secure proxy server] / I. Maksimov // *Sistemnyj administrator* [System Administrator]. — 2007. — № 5(54). — P. 17. [in Russian]
9. Shpak S. UserGate Proxy&Firewall Sertificirovannyj zashhitnik setej [UserGate Proxy&Firewall Certified network defender] / S. Shpak // *Sistemnyj administrator* [System Administrator]. — 2011. — № 3(100). — P. 110-112. [in Russian]
10. Svidetel'stvo o gosudarstvennoj registracii programmy dlja JeVM № 2019663127. «Modul' nastrojki sluzhby izmerenija propusknnoj sposobnosti seti po protokolu IPERF» («Modul' nastrojki IPERF») [Certificate of State Registration of Computer Programme No. 2019663127. "IPERF protocol network throughput measurement service configuration module" ("IPERF configuration module"): no. 2019662165; № 2019662165: appl. 07.10.2019; publ. 10.10.2019; applicant Limited Liability Company "Factor-TS" [in Russian]
11. Zajcev S.V. Interfejsy upravlenija instrumentami izmerenija proizvoditel'nosti na primere generatora trafika iPerf [Management interfaces of performance measurement tools on the example of iPerf traffic generator] / S.V. Zajcev // *Vestnik nauchnyh konferencij* [Bulletin of Scientific Conferences]. — 2016. — № 6-2(10). — P. 39-41. [in Russian]
12. Tiara Komala Sutra M. Implementasi Load Balancing Dan Failover to Device Mikrotik Router Menggunakan Metode Equal Cost Multi Path (ECMP) / M. Tiara Komala Sutra, R. Ruuhwan, R. Rizal // *Informatics and Digital Expert (INDEX)*. — 2023. — Vol. 4. — № 2. — P. 81-86. — DOI: 10.36423/index.v4i2.1189.
13. Kripakov A.V. Ispol'zovanie prilozhenija Snappi-trex dlja generacii trafika s pomoshh'ju Cisco trex [Use of Snappi-trex application for traffic generation with Cisco trex] / A.V. Kripakov // *Sovremennye problemy lingvistiki i metodiki prepodavanija russkogo jazyka v VUZe i shkole* [Modern problems of linguistics and methods of teaching Russian language at university and school]. — 2022. — № 37. — P. 1447-1452. [in Russian]
14. Rajhlin V.A. Konstruktivnoe modelirovanie sistem informatiki [Constructive modelling of computer science systems] / V.A. Rajhlin, I.S. Vershinin, R.Sh. Minjazev [et al.] — Kazan: Fjen, 2016. — 312 p. [in Russian]