



Международный журнал информационных технологий и энергоэффективности

Сайт журнала:

<http://www.openaccessscience.ru/index.php/ijcse/>



УДК 004.9

СРАВНЕНИЕ РАЗЛИЧНЫХ ХАРАКТЕРИСТИК ОТЕЧЕСТВЕННЫХ ФАЙРВОЛОВ

¹Шаханова М.В., Четверик М.А., Шаханова В.С.

ФГБОУ ВО «ФГБОУ ВО «МОРСКОЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ АДМИРАЛА Г.И. НЕВЕЛЬСКОГО», Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, 50а), e-mail: ¹marinavl2007@yandex.ru

В статье проведен анализ и сравнение фаерволов от различных российских компаний. Рассмотрены технические характеристики, производительность устройств, максимальное количество поддерживаемых подключений и наличие необходимых сертификатов. В результате сравнительного анализа были определены лучший и худший варианты среди фаерволов, подходящих для использования в российских организациях.

Ключевые слова: Фаервол, Министерство обороны РФ, технические характеристики, производительность, пользователи, сертификаты, сравнение.

COMPARISON OF VARIOUS CHARACTERISTICS OF DOMESTIC FIREWALLS

¹Shakhanova M. V., Chetverik M.A., Shakhanova V.S.

MARITIME STATE UNIVERSITY NAMED AFTER G.I. NEVELSKOY, Vladivostok, Russia (690003, Vladivostok, Verkhneportovaya str., 50a), e-mail: ¹marinavl2007@yandex.ru

The article analyzes and compares firewalls from various Russian companies. The technical characteristics, device performance, the maximum number of supported connections and the availability of necessary certificates are considered. As a result of a comparative analysis, the best and worst options among firewalls suitable for use in Russian organizations were determined.

Keywords: Firewall, Ministry of Defense of the Russian Federation, technical specifications, performance, users, certificates, comparison.

Фаерволы, как программные, так и аппаратно-программные комплексы, контролируют сетевые пакеты, используя правила для их блокировки или разрешения. Они важны для защиты сетевых ресурсов, предотвращают нежелательный трафик и несанкционированные подключения через методы фильтрации и аутентификации. С уходом иностранных компаний, российские производители фаерволов усиливают свои позиции на рынке. При выборе фаерволов, особенно для критически важных секторов, важно учитывать сертификаты безопасности.

Данная статья представляет детальный анализ российских фаерволов, ориентированных на средний бизнес и корпорации. Обзор охватывает разнообразие моделей, включая программные и аппаратные решения, с акцентом на ключевые параметры, такие как

максимальное количество подключений, производительность и технические характеристики. Особое внимание уделено сертификации безопасности. Статья предоставляет всестороннюю информацию, полезную для выбора эффективных сетевых решений защиты информации [1].

Фаервол Diamond

В сфере компьютерной безопасности, российская компания ООО «ТСС» выделяется как производитель надежных решений, включая флагманский продукт — фаервол Diamond. Этот продукт обеспечивает эффективное шифрование данных в высокоскоростных каналах и функции межсетевой защиты, включая обнаружение вторжений, что важно для современных организаций с большими объемами данных. Получение сертификации от государственных структур подтверждает соответствие продукции строгим стандартам безопасности, делая ее подходящей для критически важных систем [2].

Фаервол DIONIS DPS

Фаервол DIONIS DPS, разработанный компанией Фактор-ТС, является важным элементом в ряду российских фаерволов и сертифицирован для соответствия высоким стандартам безопасности. Он предназначен для работы с персональными данными в корпоративной и государственной сферах. Особенностью DIONIS DPS является интегрированная система IDS/IPS на базе Snort, сертифицированная для обнаружения и предотвращения вторжений. Система работает в двух режимах - обнаружения и предотвращения атак, с возможностью создания пользовательских правил для анализа и фиксации сетевого трафика. Управление и мониторинг системы осуществляются через портал Dionis-SMP [3].

Фаервол «Континент».

Анализ продукции компании «Код безопасности», действующей на российском рынке информационной безопасности, выделяет ключевые аспекты в сегменте аппаратных фаерволов. Компания предлагает две серии устройств: «Континент 3» и «Континент 4», охватывающие широкий спектр производительности от базовых до высокопроизводительных моделей. «Континент 3» целевая аудитория – крупные центры обработки данных, где важны высокая производительность и надежность. «Континент 4» выделяется устройствами с виртуальным исполнением, идеально подходящими для виртуализированных сред. Эти модели способствуют сокращению затрат на аппаратное обеспечение, при этом обеспечивая высокий уровень защиты. Основной фокус анализа – оценка наиболее производительных моделей обеих серий для определения их эффективности в обеспечении безопасности информационных систем и сетей [4].

Фаервол «Рубикон»

Компания «Эшелон» представила программно-аппаратные комплексы «Рубикон», нацеленные на защиту сетевых периметров организаций и соответствие требованиям регулирующих органов. Комплексы «Рубикон» сочетают программное и аппаратное обеспечение для комплексной безопасности информации. Они включают функции фаервола, системы маршрутизации и обнаружения вторжений для блокировки нежелательного трафика и предотвращения угроз [5].

Линейка «Рубикон» предлагает разные модели для специфических целей:

Основная модель «Рубикон» предназначена для военных систем и обработки государственной тайны, гарантирует высший уровень защиты.

«Рубикон А» адаптирован для государственных информационных систем, в том числе для обработки государственной тайны.

«Рубикон К» фокусируется на защите систем с конфиденциальной информацией и персональными данными, обеспечивает их конфиденциальность и целостность, идеально подходит для организаций, стремящихся к защите информации.

Файрвол UserGate

Компания UserGate, специализирующаяся в сфере информационной безопасности, предлагает решения для широкого круга клиентов, включая средний бизнес, крупные корпорации и государственные учреждения. Она акцентирует внимание на аппаратных файрволах для корпоративных сетей, предназначенных для средних и крупных предприятий. Эти файрволы характеризуются расширенной функциональностью, поддерживая концепцию SOAR и включая системы IDS/IPS, а также возможности для анализа инцидентов безопасности и фильтрации интернет-контента [6].

Ключевые особенности продуктов UserGate включают удаленное администрирование, высокую надежность и поддержку кластеризации. Файрволы обеспечивают множество функций, таких как обратный прокси, контроль доступа к интернету и приложениям и др.

Файрвол Idesco

В заключительной части анализа рассматриваются аппаратные файрволы от компании Idesco, с акцентом на их соответствие нормативным требованиям информационной безопасности.

Устройства Idesco для малого бизнеса, обслуживающие до 100 подключений, предлагают функции установления трафиковых ограничений, защиты периметра сети, сегментации сети и поддержки множественных интернет-провайдеров, идеально подходит для организаций, нуждающихся в безопасности и настраиваемости сети.

Исследование включает тестирование российских файрволов на производительность и эффективность в условиях различного количества подключений и объемов трафика, в частности, на сети ЕМІХ, что важно для обоснованного выбора средств обеспечения безопасности. Общее тестирование российских файрволов, согласно количеству подключений и трафика ЕМІХ представлено в табл. 1.

Таблица 1 – Общее тестирование российских файрволов, согласно количеству подключений и трафика ЕМІХ

Наименование	Максимальное количество подключений	Свидетельство ФСТЭК	Разрешение ФСБ	Разрешение Министерства Обороны	Скорость обработки трафика, Гбит/с	Скорость контроля приложений, Гбит/с	Скорость предотвращения атак через ЕМІХ, Гбит/с
DIONIS DPS 3000	200	Есть	Есть	-	До 9,4 Гигабит/сек	-	До 2,7 Гигабит/сек

DIONIS DPS 7000	2000	Есть	Есть	-	До 90 Гигабит /сек	-	До 20 Гигабит/сек
Diamond VPN/FW 4101	200	Есть	Есть	Нет	До 1,8 Гигабит /сек	-	Присутствует, с постоянным обновлением баз
VPN/FW 7151	5000	Есть	Есть	Нет	До 35 Гигабит /сек	-	Присутствует, с постоянным обновлением баз
Континент 3.9 IPC-R50	100	Есть	Есть	Есть	До 1,2 Гигабит /сек	Отсутствует	До 0,025 Гигабит/сек
Континент 4 IPC-R1000	3000	Есть	Нет	Нет	До 40.2 Гигабит /сек	-	До 10 Гигабит/сек
Мини: Рубикон, Рубикон-А, Рубикон-К	100	Есть	-	Есть	До 2 Гигабит /сек	-	До 1,6 Гигабит/сек
Мультипортовый: Рубикон, Рубикон-А, Рубикон-К	5000	Есть	-	Есть	До 6 Гигабит /сек		До 2,5 Гигабит/сек
UserGate C100	100	Есть	-	-	До 2 Гбит/сек	До 1,9 Гбит/сек	До 0,3 Гбит/сек
UserGate F8000	10000	Есть	-	-	До 40 Гигабит /сек	До 40 Гигабит/сек	До 8 Гигабит/сек
Idec0 MX Cert	350	Есть	-	-	До 3 Гигабит /сек	До 0,7 Гигабит/сек	До 0,3 Гигабит/сек
Idec0 EX	5000	-	-	-	До 42 Гигабит /сек	До 8,0 Гигабит/сек	До 5 Гигабит/сек

Для оценки результатов тестирования фаерволов и выявления лучшего и худшего продукта, следует проанализировать предоставленные данные, основываясь на критериях производительности, максимального количества активных подключений, наличия сертификации и функциональных возможностей.

Лучший фаервол. Согласно данным, наилучшим фаерволом является UserGate F8000. Он поддерживает до 10000 подключений, что является самым высоким показателем среди представленных. Его производительность во всех параметрах, включая общий трафик ЕМІХ (40 Гигабит/сек), контентную фильтрацию (15 Гигабит/сек), контроль данных (40 Гигабит/сек) и предотвращение атак (8 Гигабит/сек) показывает выдающиеся результаты.

Худший фаервол. В качестве менее предпочтительного варианта можно выделить Континент 3.9 ІРС-R50. Этот фаервол поддерживает лишь 100 подключений, что является одним из самых низких показателей. Кроме того, его производительность в ключевых областях, таких как трафик ЕМІХ (1,2 Гигабит/сек) и предотвращение вторжений (0,025 Гигабит/сек), значительно ниже по сравнению с другими представленными моделями. Отсутствие данных по контентной фильтрации и контролю приложений также указывает на ограниченные функциональные возможности.

Следует отметить, что окончательный выбор наиболее и наименее предпочтительного фаервола зависит от конкретных потребностей и требований пользователя. Например, для небольших предприятий с ограниченным числом подключений и менее требовательными к производительности задачами, более простые и менее мощные устройства могут быть более предпочтительными.

Список литературы

1. Обзор и сравнение межсетевых экранов отечественных производителей. Режим доступа: <https://habr.com/ru/articles/726662/> (дата обращения: 28.11.2023)
2. Фаервол Diamond. Режим доступа: <https://master--tssru.netlify.app/products/diamond-vpn> (дата обращения: 28.11.2023)
3. Фаервол DIONIS DPS. Режим доступа: <https://dps.factor-ts.ru/> (дата обращения: 28.11.2023)
4. Фаервол «Континент». Режим доступа: https://www.securitycode.ru/products/apksh_kontinent/ (дата обращения: 28.11.2023)
5. Фаервол «Рубикон». Режим доступа: <https://npo-echelon.ru/production/65/11342> (дата обращения: 28.11.2023)
6. Фаервол UserGate Режим доступа: <https://usergate.axoft.ru/> (дата обращения: 28.11.2023)

References

1. Overview and comparison of firewalls of domestic manufacturers. Access mode: <https://habr.com/ru/articles/726662/> (accessed: 11/28/2023)
2. The Diamond firewall. Access mode: <https://master--tssru.netlify.app/products/diamond-vpn> (accessed: 11/28/2023)
3. Firewall DIONIS DPS. Access mode: <https://dps.factor-ts.ru/> (accessed: 11/28/2023)
4. Firewall "Continent". Access mode: https://www.securitycode.ru/products/apksh_kontinent/ (accessed: 11/28/2023)

5. The Rubicon firewall. Access mode: <https://npo-echelon.ru/production/65/11342> (date of application: 11/28/2023)
 6. UserGate Firewall Access mode: <https://usergate.axoft.ru/> (accessed: 11/28/2023)
-