УДК 004

Рулёв С.А.
РГУ нефти и газа (НИУ) имени И.М. Губкина
(г. Москва, Россия)

Календарев Е.М.
РГУ нефти и газа (НИУ) имени И.М. Губкина
(г. Москва, Россия)

ФУНКЦИОНАЛЬНОЕ СРАВНЕНИЕ МЭ НА ОС АЛЬТ

***Аннотация**: Данная статья посвящена функциональному сравнению межсетевых экранов (firewall) на операционной системе Alt Linux, рассматривая инструменты firewalld и UFW. Цель исследования – анализ архитектуры и практическая оценка возможностей указанных инструментов в тестовой среде на базе Alt Workstation 10. Методология включает теоретический обзор принципов работы межсетевых экранов, анализ доступной документации и проведение экспериментов с использованием виртуальных машин для моделирования сценариев фильтрации трафика. В практической части представлены результаты тестирования firewalld и UFW, включая настройку правил, мониторинг логов и оценку эффективности блокировки нежелательного трафика. Материал ориентирован на специалистов по информационной безопасности и системных администраторов, работающих с Linux-системами, и может служить основой для дальнейших разработок в области сетевой защиты на платформе Alt Linux.*

***Ключевые слова**: Alt Linux, межсетевой экран, firewall, firewalld, UFW, ufw, сетевой трафик, Linux.*

Rulev S.A.
National University of Oil and Gas «Gubkin university»
(Moscow, Russia)

Kalendarev E.M.
National University of Oil and Gas «Gubkin university»
(Moscow, Russia)

Functional comparison of firewalls on Alt OS

Abstract*: This article is devoted to the functional comparison of firewalls on the Alt Linux operating system, with an emphasis on firewalld and UFW tools. The purpose of the study is to analyze the architecture and practical assessment of the capabilities of these tools in a test environment based on Alt Workstation 10. The methodology includes a theoretical overview of how firewalls work, an analysis of available documentation, and conducting experiments using virtual machines to simulate traffic filtering scenarios. The practical part presents the results of testing firewalld and UFW, including setting up rules, monitoring logs, and evaluating the effectiveness of blocking unwanted traffic. The material is aimed at information security specialists and system administrators working with Linux systems, and can serve as a basis for further developments in the field of network protection on the Alt Linux platform.*

Keywords*: Alt Linux, firewall, firewall, firewalld, UFW, ufw, network traffic, Linux.*

Введение

Операционные системы на базе Linux, такие как российская платформа Alt Linux, широко используются в государственных учреждениях, образовательных организациях и коммерческих структурах благодаря своей открытости, надежности. Одним из важнейших элементов защиты сетевого трафика в таких системах являются межсетевые экраны (firewall), которые обеспечивают фильтрацию входящих и исходящих данных на основе заданных правил. Alt Linux, как дистрибутив, ориентированный на безопасность и импортозамещение, поддерживает несколько инструментов для управления межсетевыми экранами, такие как firewalld и UFW, каждый из которых обладает уникальными характеристиками и областями применения. Актуальность данного исследования обусловлена ростом киберугроз, таких как DDoS-атаки, несанкционированный доступ и утечка данных. Целью работы является всесторонний анализ архитектуры межсетевых экранов на Alt Linux и сравнение их эффективности в тестовой среде. Для достижения этой цели поставлены следующие задачи:

- Изучить принципы работы firewalld и UFW;
- Провести экспериментальное тестирование firewalld и UFW в виртуальной среде, оценить их преимущества и недостатки, а затем сформулировать рекомендации по выбору межсетевой экран

Результаты исследования могут служить практическим руководством для специалистов по информационной безопасности и системных администраторов, работающих с Alt Linux, а также заложить основу для дальнейших разработок в области сетевой защиты.

Анализ источников

В процессе подготовки исследования были проанализированы материалы, посвящённые архитектуре, функциональности и практическому использованию межсетевых экранов в операционных системах семейства Linux.

Официальная документация ALT Linux Team [1][2] содержит подробное описание компонентов системы безопасности, инструментов управления сетевыми интерфейсами и механизмов фильтрации трафика.

Документация по firewalld [3][4][5] представляет собой источник, описывающий архитектуру данного инструмента управления межсетевых экранов. В ней подробно описана концепция зон безопасности, механизм динамического изменения правил без перезапуска службы, а также принципы интеграции с графической утилитой firewall-config.

Источники, посвящённые UFW [6][7][8], описывают подход к настройке межсетевых экранов, направленный на повышение удобства администратора. Материалы сообщества Ubuntu и публикации DigitalOcean акцентируют внимание на командных шаблонах, базовых сценариях блокировки и разрешения трафика, а также на практических примерах интеграции UFW в пользовательские и серверные конфигурации.

Источник [9] описывает методики тестирования систем безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта, что важно во время формирования стандартов безопасности сетевого трафика в Linux-средах при выборе эталонного инструмента защиты.

Методы исследования

Тип исследования: прикладной эксперимент с элементами сравнительного анализа, проведённый в изолированной виртуальной среде с целью оценки функциональных возможностей и практической эффективности межсетевых экранов firewalld и UFW на платформе Alt Workstation 10.

Характеристика выборки: в качестве объектов исследования выбраны два популярных инструмента управления межсетевыми экранами в Linux – firewalld и UFW. Эксперименты выполнялись на трёх виртуальных машинах Alt Workstation 10: атакующая машина и две целевые машины с установленными UFW и firewalld соответственно. На целевых машинах развёрнут тестовый веб-сервер Apache на порте 80 и активирован SSH-демон на порте 22 для проверки правил фильтрации и сценариев доступа

Методы сбора данных: информация собиралась путём практического тестирования и документирования результатов исполнения команд в контролируемой виртуальной сети. Выполнялись следующие процедуры: установка и активация соответствующих межсетевых экранов, конфигурирование правил и применение конфигураций, а также верификация поведения с атакующей машины с помощью утилит для сканирования портов nmap, проверки http-запросов curl, попыток подключения по SSH.

Методы управления межсетевыми экранами и анализ инструментов

Работа межсетевого экрана в Linux опирается на механизмы ядра – подсистему Netfilter и её реализации через iptables или nftables. В рамках исследования рассмотрены два таких инструмента – firewalld и UFW, их архитектурные принципы, основные методы конфигурирования и особенности практического применения.

Firewalld реализует модель зон безопасности, где каждой зоне соответствует набор сервисов, портов и политик, а сетевые интерфейсы привязываются к выбранной зоне. Основные особенности и методы управления:

- Поддержка зон и привязка интерфейсов, что позволяет применять разные политики для разных сетевых сегментов;
- Разделение временных изменений и постоянных измененияй конфигураций, что даёт возможность вносить срочные правки без перезапуска службы;
- Наличие расширенных правил с возможностью указать источник, действие, логирование, условия;
- Управление через cli и графический интерфейс;
- Интеграция с nftables или iptables в зависимости от конфигурации системы.

UFW является удобным и минималистичным интерфейсом для iptables или nftables. Он ориентирован на простоту и скорость настройки. Основные особенности и методы управления:

- Простой и понятный синтаксис команд;
- Поддержка rate-limit для защиты сервиса от перебора;
- Просмотр и управление правилами и возможность их удаления по номеру;
- Подходит для быстрого развёртывания базовой политики.

Результаты теоретического анализа

Таким образом, инструменты firewalld и UFW являются разными подходами к управлению сетевой безопасностью.

Firewalld основан на зонах безопасности и поддерживает динамическое изменение правил без перезапуска службы. Его архитектура обеспечивает гибкость и возможность тонкой настройки с использованием расширенных правил, что делает firewalld удобным в сложных сетевых конфигурациях, где требуется разграничение политик и управление несколькими интерфейсами.

UFW, напротив, ориентирован на простоту и скорость настройки. Он предоставляет простой синтаксис команд. Данный подход делает UFW оптимальным для небольших серверов и рабочих станций, где важны быстрота и надёжность базовой защиты.

Результаты практического исследования

Исследование включало тестирование двух инструментов управления межсетевыми экранами firewalld и UFW в контролируемой виртуальной среде. В качестве контрольной точки рассматривалась корректность применения правил, отсутствие ложных пропусков и соответствие поведения ожидаемой политике.

Таблица 1 – Сравнение инструментов

	UFW	firewalld

Разработчик	Canonical Ltd.	Red Hat / Fedora Project
Версия в Alt Workstation 10	0.35	0.9.11
Версия разработчика	0.36.2-9	2.1.0
Лицензия	GNU General Public License (GPL)	GNU General Public License (GPL)

В первом случае, при использовании firewalld, был установлен и активирован сервис на целевой машине 192.168.56.105. Интерфейс был назначен в зону public, выполнены стандартные операции: разрешение сервиса HTTP (firewall-cmd --zone=public --add-service=http --permanent), удаление сервиса SSH (firewall-cmd --zone=public --remove-service=ssh --permanent) и добавлена расширенная rich-rule для конкретного источника (--add-rich-rule='rule family="ipv4" source address="192.168.56.104" port port=80 protocol=tcp accept'). После firewall-cmd --reload проверка с атакующей машины (nmap -p 80,22 192.168.56.105, curl http://192.168.56.105, попытка ssh user@192.168.56.105) показала: порт 80 открыт и отвечает (страница Apache доступна), порт 22 закрыт (подключение отклонено). Время настройки составило примерно 5-7 минут.

Во втором случае, при использовании UFW, на целевой машине 192.168.56.102 был установлен и включён UFW; добавлены правила ufw allow 80/tcp, ufw deny 22/tcp и ufw limit 22/tcp для защиты от перебора. После ufw reload проверка с атакующей машины (nmap -p 80,22 192.168.56.102, curl http://192.168.56.102, попытка ssh user@192.168.56.102) показала: порт 80 открыт и отвечает, порт 22 закрыт. Время настройки составило примерно 3-5 минут.

Результаты тестирования сведены в таблицу 2.

Таблица 2 – Результаты практического исследования

Показатель	UFW	firewalld
Базовая политика	Allow outgoing / deny incoming	Public зона, deny по умолчанию
Разрешение http	ufw allow 80/tcp	firewall-cmd --zone=public --add-service=http
Блокирование ssh	ufw deny 22/tcp	firewall-cmd --zone=public --remove-service=ssh
Кол-во запросов	50 000	50 000
Параллельных запросов одновременно	1000	1000
Обработано запросов в секунду	2371	1033
Время обработки	48.379 с	21.085 с
Среднее время ответа	421.69 мс	967.59 мс
Максимальное время запроса	14414 мс	48531 мс
Средняя загрузка	1.59 – 0.46 – 0.24	4.57 – 10.79 – 6.15
Загрузка памяти	663 МБ / 1.9 ГБ	988 МБ / 1.9 ГБ
Загрузка процессора (1 / 2 ядро)	100% / 35.6%	80.2% / 55.4%
Средняя нагрузка httpd процессов	1.4-2.8%	2.0-3.2%
Количество httpd процессов	10-16	17-20

Ошибки в ходе тестирования	Отсутствуют	Отсутствуют

Как можно заметить, firewalld лучше справляется с параллельной нагрузкой. Им было обработано 2371 запросов в секунду, в то время как UFW обработал 1033 запросов в секунду. Firewalld сократил общее время теста почти вдвое. При этом максимальная задержка у firewalld оказалась ниже 14.4 с, 48.5 с оказалась у UFW. Это говорит о том, что firewalld более стабилен под нагрузкой.

Повышенная производительность firewalld достигается за счёт большего расхода ресурсов. Использование памяти выше примерно на 325 МБ, а системная нагрузка и число запущенных httpd процессов превышают показатели UFW.

Заключение

Проведённое исследование было направлено на функциональное сравнение инструментов управления межсетевыми экранами firewalld и UFW в операционной системе Alt Workstation 10. В ходе работы были изучены архитектурные особенности, функциональные возможности и практическая эффективность данных инструментов при фильтрации сетевого трафика.

Результаты эксперимента показали, что оба решения успешно выполняют свои функции по контролю входящих и исходящих соединений. Firewalld продемонстрировал высокую гибкость и расширенные возможности управления за счёт гибко настраиваемой структуры зон и использования расширенных правил. Данная особенность делает его более предпочтительным для сложных инфраструктур и корпоративных систем. UFW показал простоту конфигурации и скорость настройки. При развертывании на рабочих станциях и серверах с типовыми политиками безопасности это является удобством.

Результаты исследования подтверждают, что использование правильно настроенного межсетевого экрана остаётся одним из ключевых элементов обеспечения информационной безопасности в Linux-средах. Полученные выводы могут быть использованы при выборе инструментов для построения

систем сетевой защиты и при обучении специалистов по администрированию Alt Workstation 10.

Список литературы

1. ALT Linux Team. Официальная документация / [Электронный ресурс]. — URL: https://docs.altlinux.org (дата обращения: 10.10.2025).
2. Документация по ОС Альт – ALT Linux / [Электронный ресурс]. — URL: https://www.basealt.ru/documentation (дата обращения: 10.10.2025).
3. Firewalld. Официальный сайт / [Электронный ресурс]. — URL: https://firewalld.org (дата обращения: 12.10.2025).
4. Firewalld. Документация / [Электронный ресурс]. — URL: https://firewalld.org/documentation/ (дата обращения: 12.10.2025).
5. Using and configuring firewalld // Red Hat Enterprise Linux Documentation / [Электронный ресурс]. — URL: https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/configuring_firewalls_and_packet_filters/using-and-configuring-firewalld_firewall-packet-filters (дата обращения: 12.10.2025).
6. UFW — Community Help Wiki / [Электронный ресурс]. — URL: https://help.ubuntu.com/community/UFW (дата обращения: 19.10.2025).
7. Wiki Ubuntu: Uncomplicated Firewall / [Электронный ресурс]. — URL: https://wiki.ubuntu.com/UncomplicatedFirewall (дата обращения: 19.10.2025).
8. DigitalOcean. UFW Essentials: Common Firewall Rules and Commands / [Электронный ресурс]. — URL: https://www.digitalocean.com/community/tutorials/ufw-essentials-common-firewall-rules-and-commands (дата обращения: 19.10.2025).
9. Уймин, А. Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2024. – № 5(610). – С. 59-65. – EDN VSLWIA (дата обращения: 19.10.2025).