УДК 004.052.2

Соколов Андрей Юрьевич

РГУ Нефти и Газа (Национальный исследовательский университет) им. И.М. Губкина

Москва

НАГРУЗОЧНОЕ ТЕСТИРОВАНИЕ WINDOWS FIREWALL

Аннотация: данная статья рассматривает нагрузочное тестирование штатного МЭ Windows Firewall на базе Windows Server 2025. Цель эксперимента: исследовать производительность Windows Firewall и архитектуры Windows Filtering Platform в условиях лабораторного нагрузочного тестирования.

Практическая часть включает эксперимент по имитации сетевой активности множества устройств с помощью параллельных сессий нагрузочного ПО iperf3, запущенных на физических клиентах. Опытным путем анализируются возможности архитектуры Windows Filtering Platform по обработке массивов правил фильтрации, оценивается нагрузка на пропускную способность канала и ресурсы центрального процессора.

Результаты исследования призваны показать, в каких случаях встроенные средства Windows могут стать технически оправданной заменой специализированным проприетарным или open-source решениям.

Ключевые слова: Windows Firewall, Windows Server 2025, сетевая безопасность, импортозамещение ПО, нагрузочное тестирование, iperf3, Windows Filtering Platform (WFP), оптимизация инфраструктуры, шлюз по умолчанию.

Введение

Вопросы производительности встроенных механизмов сетевой защиты операционных систем представляют значительный интерес как с практической, так и с исследовательской точки зрения. Архитектура Windows Filtering Platform (WFP), лежащая в основе Windows Firewall, декларирует высокую эффективность за счет обработки трафика на уровне ядра ОС. Однако количественные данные о том, как изменение параметров фильтрации (количество правил, интенсивность потока) влияет на пропускную способность и потребление ресурсов процессора, в открытой литературе представлены недостаточно, особенно для актуальной версии Windows Server 2025.

Цель данной работы — в лабораторных условиях провести нагрузочное тестирование Windows Firewall для изучения характеристик производительности платформы WFP. В рамках эксперимента решаются следующие задачи:

- Определить зависимость пропускной способности и загрузки ЦП от количества активных правил фильтрации;
- Оценить влияние многопоточного трафика на стабильность работы межсетевого экрана;
- Выявить потенциальные «узкие места» в виртуализированной среде, имитирующей изолированный сегмент сети.

Важно подчеркнуть, что исследование носит экспериментальный характер и ограничено условиями конкретного виртуального стенда. Полученные результаты позволяют сделать выводы об эффективности алгоритмов WFP, но

не являются прямым руководством для проектирования промышленных инфраструктур без учета их специфики.

Описание экспериментального стенда

Эксперимент реализован в виртуальной среде на базе гипервизора VMware Workstation. Для проведения нагрузочного тестирования была реализована изолированная сетевая инфраструктура, состоящая из трех ключевых узлов. Сетевая топология приведена на Рисунке 1.

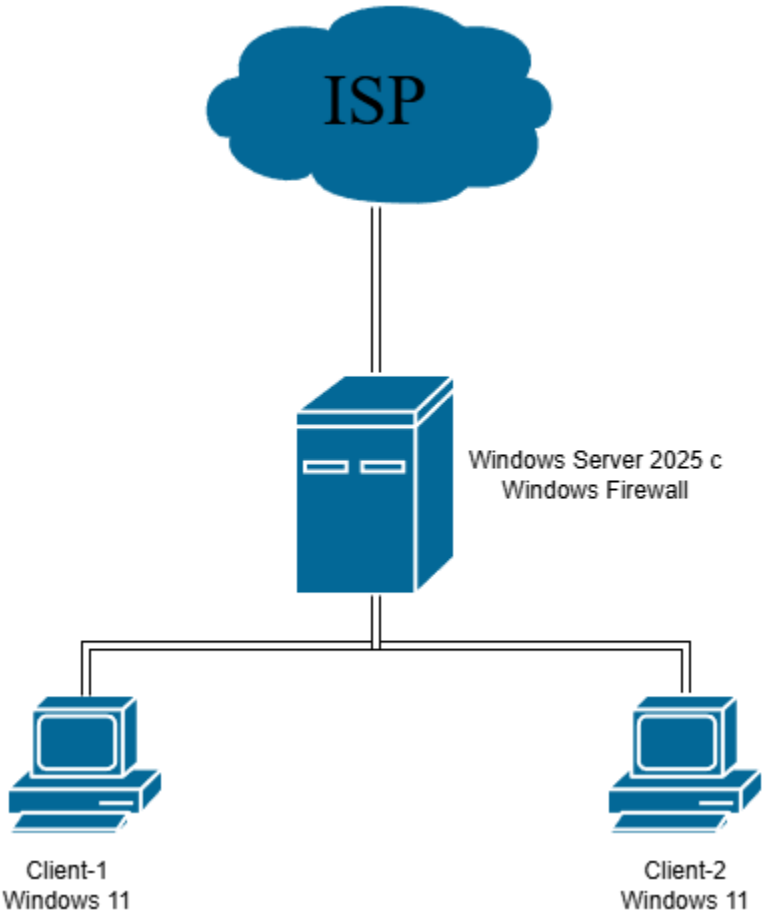

Рисунок 1. Топология экспериментального стенда

Параметры хост-системы:

- Процессор Intel Core i5-11400F;
- 32 GB DDR4 оперативной памяти;

Параметры виртуальных машин:

- vCPU – 2 ядра с поддержкой аппаратной виртуализации VT-x;
- RAM: 4 GB;
- Сетевые интерфейсы в режиме неограниченной пропускной способности виртуального коммутатора;
- Для Windows Server используется два виртуальных сетевых адаптера: NAT и внутренняя сеть. Для клиентов – только внутренняя сеть.

Используемый инструментарий

Для автоматизации и проведения нагрузочного тестирования используется следующий инструментарий:

- **iperf3** будет использован для измерения максимальной пропускной способности сети. С данным инструментом будут созданы параллельные TCP-сессии для создания огромного потока пакетов, проходящих через Windows Firewall;
- **Windows PowerShell** используется для автоматического создания правил для Windows Firewall, для внесения корректив в работу МЭ;
- **PerfMon** – сбор метрик процессора (% Processor Time) и сетевых интерфейсов (DPC Queued/sec) для получения результатов нагрузочного тестирования.

Методика тестирования

Главная задача методики – обеспечить повторяемость эксперимента и чистоту полученных данных. Для оценки влияния Windows Firewall на систему будут считываться три ключевых показателя:

- Пропускная способность – количество данных, переданных на прикладном уровне, Гбит/с;
- Нагрузка на процессор (% Processor Time). Так как фильтрация

происходит на уровне ядра, основная нагрузка ложится на процессор, потому необходимо отслеживать общую загрузку для выявления момента, когда CPU становится «узким местом».

- Стабильность потока, которая заключается в количестве повторных передач пакетов. Данная метрика позволяет увидеть, начинает ли брандмауэр отбрасывать легитимные пакеты из-за нехватки ресурсов для их обработки.

Самый первый сбор метрик – «нулевой замер» для получения эталонных параметров, с которыми можно будет сравнивать, данные параметры показывают то, сколько ресурсов потребляет работа самой ВМ. В рамках данного пункта на Windows Server 2025 отключаются все правила фильтрации и сама служба МЭ.

Для отсутствия погрешностей необходимо ввести следующую процедуру сбора данных, которая будет соблюдаться при выполнении эксперимента:

- Перед каждым замером трафик прогоняется на протяжении 10 секунд;
- Каждый тест исполняется трижды, после чего вычисляется среднее значение;
- PerfMon запускается в фоновом режиме с интервалом снятия данных 1 раз в секунду.

Сценарии тестирования

Нагрузочное тестирование разделено на четыре ключевых сценария, каждый из которых имитирует различную степень нагрузки на межсетевой экран.

Стандартная команда для тестирования для сценариев: iperf3 -c 192.168.1.1 -t 40 -P 10, где P – параллельные потоки, t – время тестирования.

Сценарий 1. Данный сценарий был описан ранее в методике тестирования. В рамках первого сценария необходимо определить эталонных показатели для фиксации максимальной пропускной способности виртуальной сети в условиях отсутствия фильтрации. В рамках конфигурации необходимо остановить службу Windows Defender Firewall.

Сценарий 2. Имитация стандартной конфигурации системы, из «коробки» (например, разрешены только системные службы вроде RDP и ICMP). Данный сценарий позволяет оценить влияние подсистемы WFP в сетевом стеке, но в минимальном виде.

Сценарий 3. Масштабирование базы правил. Это основная часть тестирования, с помощью PowerShell в таблицу Inbound Rules последовательно вносятся группы блокирующих правил (от 500 штук). Будут намеренно использоваться блокирующие правила для случайных диапазонов IP, потому что в архитектуре WFP каждый пакет проверяется до первого соответствия, следовательно, огромный список лишних запретов заставляет систему прогонять каждый пакет через всю цепочку фильтров, создавая максимальную нагрузку.

Сценарий 4. Предельная нагрузка, stress testing. Генерация 5000 правил при многопоточном трафике. Цель данного сценария в нахождении точки отказа, когда время обработки пакета в ядре начнет приводить к росту задержек и потере пакетов.

Сценарий 5. Продолжение стресс теста. Дополнительно к 5000 правилам будут добавлены еще 30 параллельных потоков, утилита iperf3 будет запущена с двух клиентских машин.

Продемонстрируем сбор данных по сценарию 1 для определения эталонных показателей. На Рисунке 1 показан сбор данных с клиента (передача данных и пропускная способность), на Рисунке 2 в утилите Perfmon

показана нагрузка на процессор сервера при передаче данных.

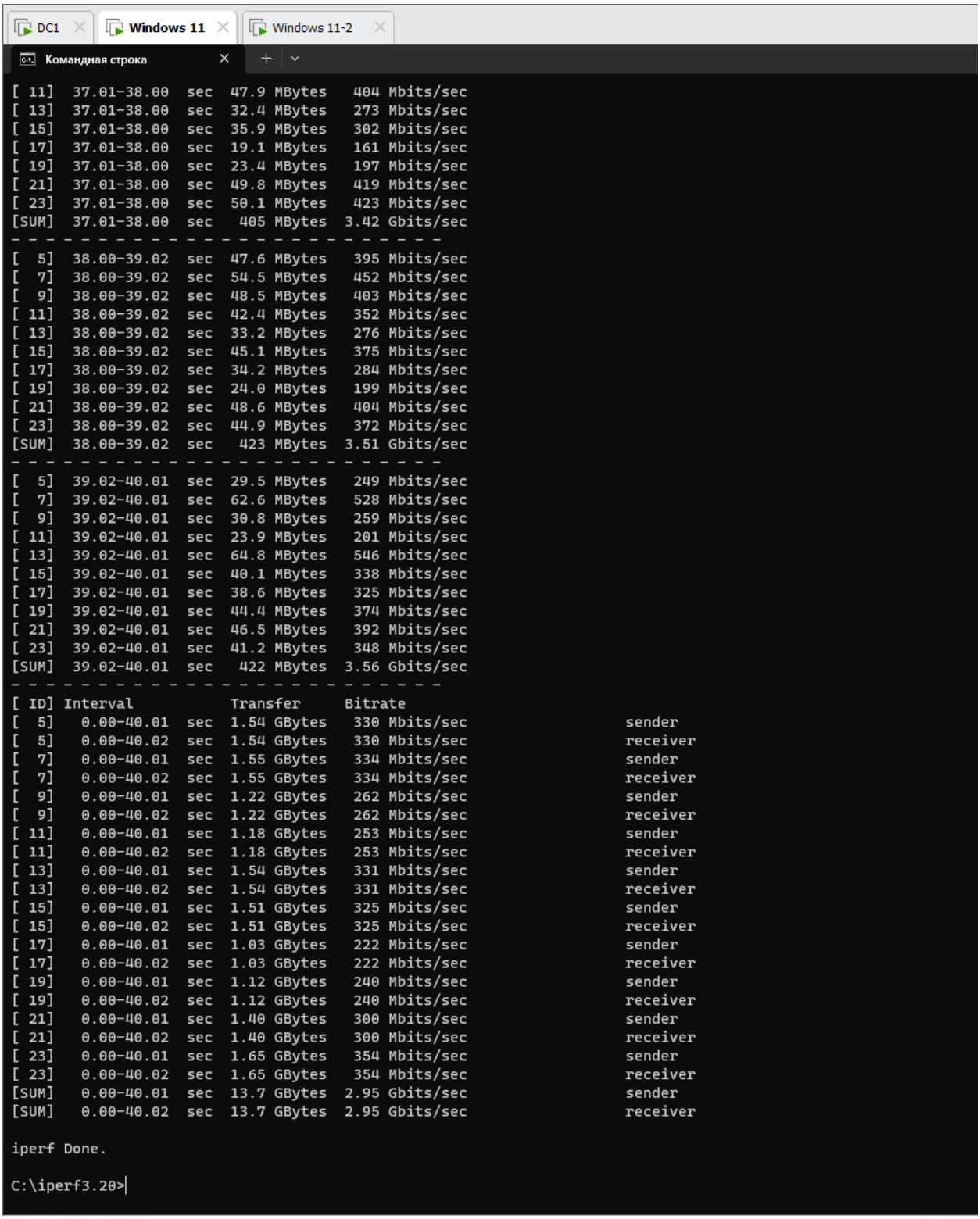

Рисунок 2. Отработка утилиты iperf3 с клиента

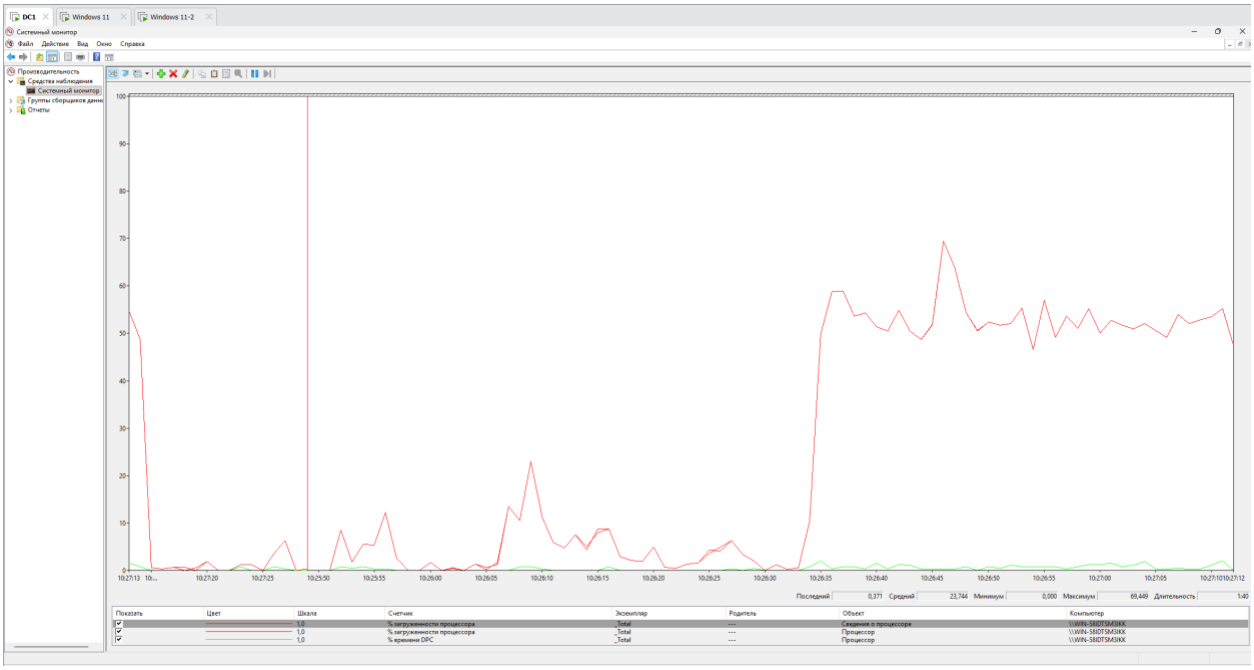

Рисунок 3. Сбор показателей работы Windows Firewall

Технические особенности проведения сценариев нагрузочного тестирования:

1. Запуск утилиты в режиме сервера на DC1 (с Windows Firewall) – iperf3.exe -s;

2. Генерация нагрузки на клиентах – iperf3.exe -c 192.168.1.1 -t 40 -P 10 (аргументы команды разбирались ранее);

3. Создание правил с Powershell, пример (рандомизируется ip-адрес и создается блокирующее правило):

$ip = "192.10.$((Get-Random -Minimum 1 -Maximum 255)).$((Get-Random -Minimum 1 -Maximum 255))"

New-NetFirewallRule -DisplayName "Block_LoadTest_$_" -Direction Inbound -Action Block -RemoteAddress $ip -Enabled True -Profile Any | Out-Null»

Анализ результатов и выводы

В данном разделе представлены данные, полученные в ходе выполнения

пяти сценариев испытаний. Результаты измерений пропускной способности, утилизации ресурсов процессора и других метрик сведены в Таблицу 3.

Таблица 3. Сравнение производительности Windows Firewall при различной нагрузке

Сценарий	**Количество правил**	**Пропускная способность (Гбит/с)**	**Нагрузка на процессор (%)**	**Стабильность передачи данных**
1	0 (Windows Firewall выключен)	2,95	56	Потерь нет
2	Стандартный набор правил	3,80	52	Потерь нет
3	Дополнительные 500 блокирующих правил	3,81	54	Потерь нет
4	Дополнительные 5000 блокирующих правил	4,07	56	Потерь нет
5	Дополнительные 5000 блокирующих правил, 40 параллельных потоков с двух клиентов	2,66	55	Деградация канала передачи пакетов, но сам Windows Firewall справляется с приходящими пакетами

Интерпретация полученных результатов с учетом лабораторного характера эксперимента позволяет сделать следующие выводы:

1. Неожиданный эффект отключения службы. Сравнение сценариев 1 и 2 показало, что полная остановка службы Windows Firewall привела к снижению пропускной способности с 3,80 до 2,95 Гбит/с. Данный феномен

противоречит классическим представлениям о накладных расходах фильтрации и требует отдельного изучения. Выдвинутая гипотеза о том, что отключение брандмауэра изменяет режим работы драйверов сетевого адаптера (возможно, переводя их в состояние с меньшей эффективностью обработки прерываний), согласуется с общими принципами взаимодействия драйверов и WFP, описанными в руководствах по настройке производительности [3]. Для подтверждения этой гипотезы необходима глубокая трассировка с использованием средств диагностики ядра (ETW), что выходит за рамки данной работы. В контексте нашего исследования важен сам факт: штатный механизм фильтрации в данной конфигурации не только не создает дополнительной нагрузки, но и демонстрирует более высокую производительность по сравнению с отключенным состоянием.

2. Независимость производительности от количества правил. В сценариях 3 и 4 увеличение числа блокирующих правил с 500 до 5000 практически не повлияло на пропускную способность (осталась на уровне ~4 Гбит/с) и загрузку ЦП (52–56%). Этот результат эмпирически подтверждает высокую эффективность структур данных, используемых в WFP для классификации пакетов. Отсутствие линейной зависимости времени обработки от размера таблицы правил свидетельствует о применении оптимизированных алгоритмов поиска (например, хэширования или сбалансированных деревьев), что соответствует архитектурным описаниям платформы. Стабильность загрузки ЦП при варьировании числа потоков от 10 до 40 (сценарии 2–4) дополнительно указывает на то, что процессор не являлся ограничивающим ресурсом в данных тестах.

3. Выявление ограничений виртуальной среды. В сценарии 5, при увеличении нагрузки до 40 параллельных потоков с двух клиентов, суммарная пропускная способность упала до 2,66 Гбит/с, однако загрузка ЦП сервера

осталась на уровне ~55%. Такое поведение с высокой вероятностью свидетельствует о том, что «узким местом» стал не сам Windows Firewall, а компоненты виртуализации — производительность виртуального коммутатора (vSwitch) гипервизора VMware Workstation. Таким образом, в рамках лабораторного стенда достичь «точки перегиба» производительности самого межсетевого экрана не удалось; его потенциальные возможности оказались выше пропускной способности виртуальной сетевой подсистемы.

4. Интерпретация количественных значений. Полученные абсолютные цифры пропускной способности (до 4 Гбит/с) характеризуют производительность конкретного виртуального стенда и не могут быть непосредственно перенесены на физические серверы с высокоскоростными интерфейсами (1/10/40 GbE). Однако качественные закономерности — отсутствие деградации при росте числа правил, низкие накладные расходы фильтрации — обусловлены архитектурой WFP и, предположительно, сохранятся и на физическом оборудовании, что требует дальнейшей проверки.

Заключение

В результате выполнения лабораторного нагрузочного тестирования Windows Firewall на базе Windows Server 2025 в среде VMware Workstation были получены следующие основные результаты:

Экспериментально подтверждена высокая эффективность платформы Windows Filtering Platform: пропускная способность и загрузка процессора практически не зависят от количества активных правил фильтрации в диапазоне до 5000 записей.

Выявлен неочевидный эффект: отключение службы брандмауэра привело к снижению производительности, что требует дальнейшего изучения и, вероятно, связано с изменением режима работы сетевых драйверов. Этот

факт подчеркивает сложность и нелинейность взаимодействия компонентов сетевой подсистемы Windows.

Продемонстрировано, что в условиях использованного виртуального стенда ограничивающим фактором производительности стала не система фильтрации, а возможности гипервизора. «Точка перегиба» для самого Windows Firewall достигнута не была, что говорит о его значительном запасе производительности даже в виртуализированной среде.

Следует отметить, что задачи оценки отказоустойчивости (моделирование сбоев службы, потери связности) и поиска абсолютных пределов производительности не входили в рамки данного эксперимента и требуют отдельного исследования на физическом оборудовании с использованием специализированных методик (например, RFC 2544, RFC 3511).

Таким образом, проведенное исследование вносит вклад в понимание реальной производительности встроенного межсетевого экрана Windows Server 2025. Полученные данные могут служить основой для дальнейших экспериментов на физических серверах, а также для выработки рекомендаций по настройке политик фильтрации без опасения за деградацию пропускной способности. В контексте лабораторной работы цель, поставленная во введении, достигнута: архитектурные особенности WFP изучены и количественно оценены в контролируемых условиях.

Список литературы и источников

1. Microsoft Learn. Windows Filtering Platform Architecture Overview [Электронный ресурс]. – URL: https://learn.microsoft.com/en-us/windows/win32/fwp/windows-filtering-platform-architecture-overview (дата обращения: 15.02.2026).

2. Microsoft Learn. What's new in Windows Server 2025 [Электронный ресурс]. – URL: https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-windows-server-2025 (дата обращения: 15.02.2026).
3. Microsoft Learn. Performance Tuning Guidelines for Windows Server 2025 [Электронный ресурс]. – URL: https://learn.microsoft.com/en-us/windows-server/administration/performance-tuning/ (дата обращения: 15.02.2026). (Примечание: ссылка обобщенная, так как точный раздел по сетевым адаптерам теперь интегрирован в общее руководство)
4. Microsoft Learn. Windows Defender Firewall with Advanced Security [Электронный ресурс]. – URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/ (дата обращения: 15.02.2026).
5. Yosifovich P., Ionescu A., Solomon D. A., et al. Windows Internals, Part 1 & 2. – 7th Edition. – Microsoft Press, 2021. – 800 с.
6. Уймин А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: Практикум. – СПб.: Лань, 2024. – 116 с.
7. Microsoft Corporation. Windows Server 2025 Networking Performance Tuning [Электронный ресурс]. – 2025. – URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/network-subsystem/net-sub-performance-tuning-nics (дата обращения: 15.02.2026).