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: определить целесообразность использования Windows Firewall в качестве основного узла контроля трафика для инфраструктуры, оценить отказоустойчивость.

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.

Abstract: This article discusses the load testing of the native Windows

Firewall based on Windows Server 2025. The experiment aims to determine the feasibility of using Windows Firewall as the primary traffic control node for an infrastructure and to evaluate its fault tolerance.

The practical section involves an experiment simulating the network activity of many devices using parallel sessions of the iperf3 load testing software running on physical clients. The study empirically analyzes the capabilities of the Windows Filtering Platform architecture regarding the processing of filtering rule sets, while assessing the impact on channel throughput and CPU resource utilization.

The research results intend to demonstrate scenarios where built-in Windows tools can serve as a technically justified alternative to specialized proprietary or open-source solutions.

Keywords: Windows Firewall, Windows Server 2025, network security, software import substitution, load testing, iperf3, Windows Filtering Platform (WFP), infrastructure optimization, default gateway.

Введение

В рамках обеспечения информационной безопасности инфраструктуры системные администраторы сталкиваются с следующим выбором: использовать дорогостоящие проприетарные межсетевые экраны или сложные в настройке open-source решения. Для малых и средних инфраструктур, которые уже построены на стеке Microsoft, проприетарные продукты либо неоправданно дороги, либо избыточны по функционалу.

В связи с этим актуальным вопросом является эффективность штатных инструментов безопасности, интегрированных напрямую в ОС. Ключевым компонентом защиты в Windows Server 2025 остается Windows Firewall, архитектура – Windows Filtering Platform, которая позволяет осуществлять фильтрацию трафика непосредственно на уровне ядра ОС, что минимизирует

накладные расходы.

Основными недостатками использования Windows Firewall в роли пограничного шлюза могут быть рост задержек и падение пропускной способности по мере усложнения правил фильтрации и увеличения инфраструктуры.

Потому цель данной исследовательской работы – проверить Windows Firewall в условиях, приближенных к промышленной эксплуатации с имитацией реальной инфраструктуры. В рамках результатов должны быть получены пределы производительности и «точки перегиба», при которых происходит критическое снижение эффективности обработки трафика

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.

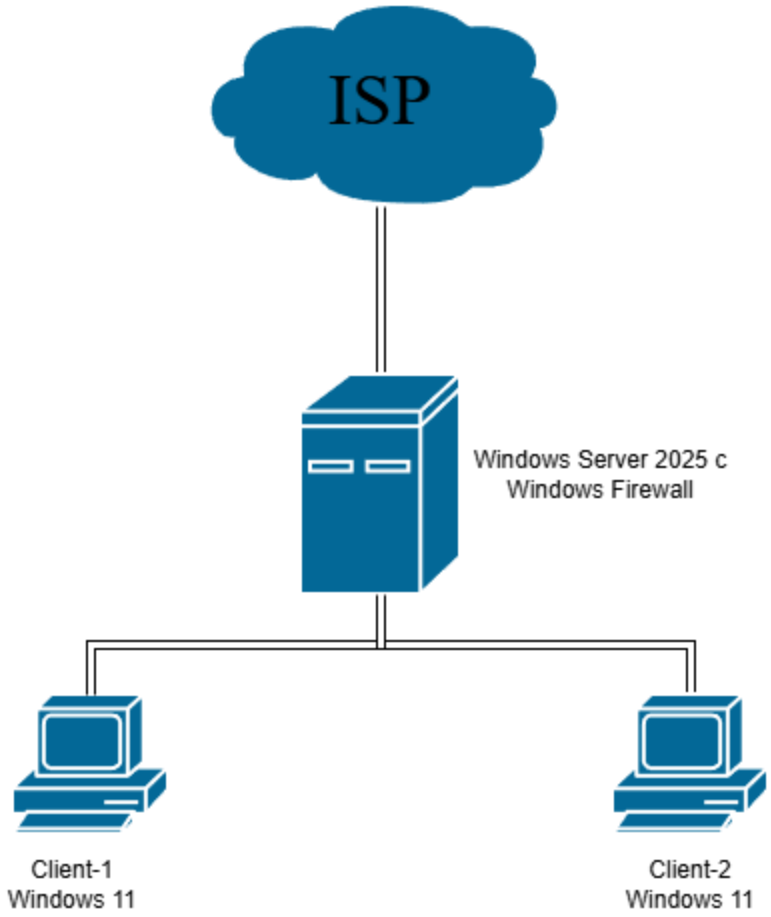

Рисунок 1. Топология экспериментального стенда

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.

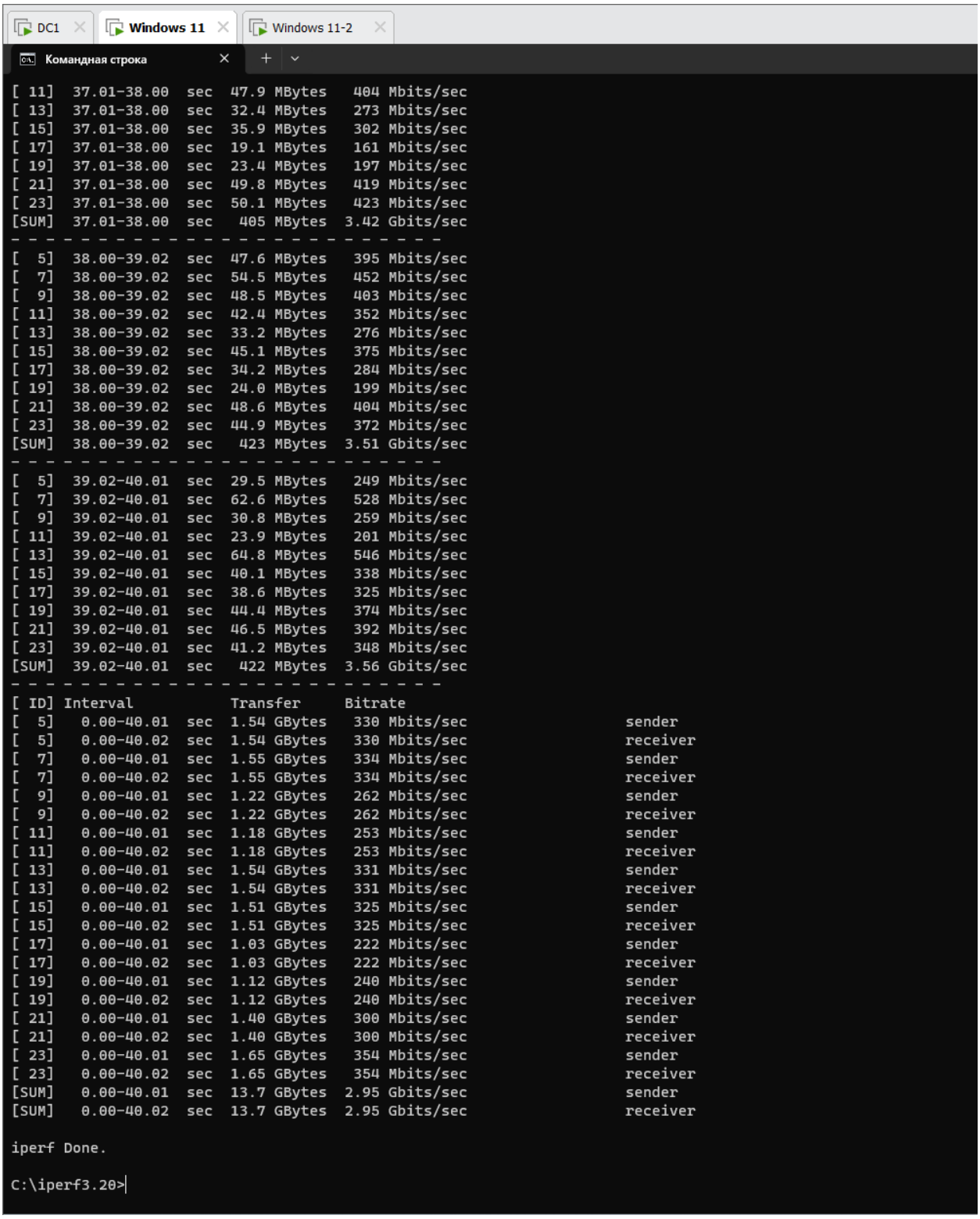

Рисунок 2. Отработка утилиты iperf3 с клиента

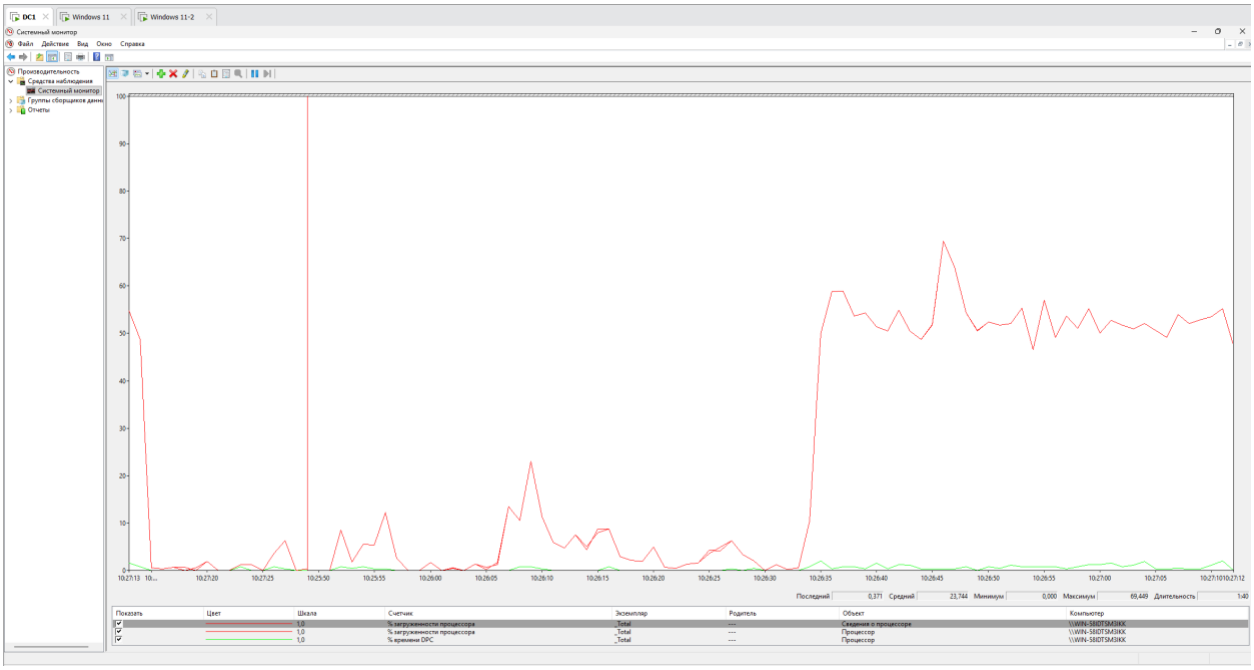

Рисунок 3. Сбор показателей работы Windows Firewall

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

Анализ полученных данных позволяет сделать следующие **выводы**:

1. Сравнение сценариев 1 и 2 выявило следующий результат: полное отключение службы Windows Firewall привело к снижению пропускной способности с 3,80 до 2,95 Гбит/с. Данное снижение показывает связь драйверов сетевого адаптера с подсистемой Windows Filtering Platform. При отключении службы обработка трафика перешла в менее эффективный режим:

2. Как показано в сценариях 3 и 4 увеличение количества блокирующих правил с 500 до 5000 не привело к деградации производительности. Пропускная способность сохранилась на уровне ~4 Гбит/с, а нагрузка на ЦП осталась в диапазоне 52–55%. Это говорит о том, что в Windows Firewall используются продвинутые механизмы поиска соответствий, где время поиска не зависит линейно от количества записей;

3. При увеличении нагрузки (два клиента, 40 потоков) суммарная скорость упала до 2,66 Гбит/с, однако загрузка процессора сервера не выросла. Windows Firewall не стал ограничивающим местом, не справилась система виртуальной коммутации гипервизора в связи с возросшим количеством пакетов.

Заключение

В результате работы была исследована производительность межсетевого экрана Windows Firewall на базе Windows Server 2025. Результаты показали, что МЭ справляется с нагрузкой при огромном количестве трафика и при множестве блокирующих правил.

Следовательно, для малых и средних предприятий использование Windows Firewall в роли МЭ является оправданным решением, не требующим ограничений в создании сложных политик безопасности ради увеличения производительности.

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 Network Adapters [Электронный ресурс]. URL: https://learn.microsoft.com/en-us/windows-server/networking/technologies/network-subsystem/net-sub-performance-tuning-nics (дата обращения: 15.02.2026).

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. Microsoft Learn. Best practices for configuring Windows Defender Firewall [Электронный ресурс]. URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/best-practices-configuring (дата обращения: 15.02.2026).

6. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург: Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2.

7. Yosifovich P., Ionescu A., Solomon D. A., et al. Windows Internals, Part 2. 7th Edition. Microsoft Press, 2021.

8. Davies J. Windows Server 2022 Administration Fundamentals. — Birmingham: Packt Publishing, 2022.