УДК 004.056.53:004.7

Давыдов Виталий Владимирович

независимый исследователь

Козырев Владислав Сергеевич

независимый исследователь

МЕТОДИКА ОБЕСПЕЧЕНИЯ УСТОЙЧИВОСТИ ЗАЩИЩЕННЫХ ТУННЕЛЕЙ К АТАКАМ И ОШИБКАМ PATH MTU DISCOVERY

Аннотация. Исследуется устойчивость защищенных IP-туннелей при ошибках и преднамеренном искажении Path MTU Discovery. Показано, что классический PMTUD создает конфликт требований: фильтрация ICMP Packet Too Big приводит к «черной дыре» для крупных пакетов, а немедленное доверие неаутентифицированному сообщению позволяет неоправданно уменьшить рабочий MTU туннеля. Дополнительная проблема возникает при изменении накладных расходов инкапсуляции: внешний PMTU может оставаться прежним, тогда как допустимый размер внутреннего пакета уменьшается. Предложена двухконтурная методика, в которой ICMP используется только как сигнал для проверки, изменение рабочего размера подтверждается защищенной пробой, а состояние связывается с узлом туннеля, внешним путем и эпохой инкапсуляции. Сформулированы инвариант безопасной отправки и конечный автомат восстановления. В сценарном вычислительном эксперименте выполнено 400 000 трасс для пяти отказов и четырех политик. В авторской условной модели предложенная политика обеспечила 98,702% доставленных полезных данных, снизила долю трасс с black-hole-состоянием до 0,798% и долю ложного снижения MTU при поддельном PTB до 0,130%. Медианное время восстановления составило 154,927 мс. Результаты предназначены для сравнения архитектур при заданных предположениях и не являются статистикой реальных сетей.

Ключевые слова: защищенный туннель, VPN, Path MTU Discovery, PMTUD, DPLPMTUD, ICMP Packet Too Big, black hole, IPsec, WireGuard, фрагментация, MSS.

A METHOD FOR PROTECTED-TUNNEL RESILIENCE TO PATH MTU DISCOVERY ATTACKS AND FAILURES

Abstract. The paper studies protected IP-tunnel resilience when Path MTU Discovery fails or is deliberately manipulated. Classical PMTUD creates conflicting requirements: filtering ICMP Packet Too Big messages can black-hole large packets, while immediately trusting an unauthenticated message can force an unjustified reduction of the tunnel working MTU. A separate failure appears when encapsulation overhead changes: the outer PMTU can remain constant while the maximum safe inner packet becomes smaller. The proposed two-loop method treats ICMP only as a trigger, commits a working-size change after an authenticated probe, and keys state by tunnel peer, outer path, and encapsulation epoch. A safe-send invariant and a recovery state machine are defined. A reproducible scenario experiment evaluates 400,000 traces across five failures and four policies. Under the stated authorial assumptions, the proposed policy delivered 98.702% of useful data, reduced black-hole traces to 0.798%, and limited false MTU reductions under forged PTB messages to 0.130%. Median recovery time was 154.927 ms. The results compare architectures under explicit assumptions and must not be interpreted as measurements of operational incident frequency.

Keywords: protected tunnel, VPN, Path MTU Discovery, PMTUD, DPLPMTUD, ICMP Packet Too Big, black hole, IPsec, WireGuard, fragmentation, MSS.

Введение

Защищенный туннель добавляет к внутреннему IP-пакету внешний IP- и транспортный заголовки, служебные поля протокола и имитозащиту. Поэтому пакет, допустимый на внутреннем интерфейсе, после инкапсуляции может превысить MTU внешнего пути. Для WireGuard транспортное сообщение содержит тип, зарезервированное поле, идентификатор получателя, счетчик и AEAD-тег; вместе с UDP и внешним IP это дает различный объем накладных

данных для IPv4 и IPv6 [15]. В IPsec точная величина зависит от режима, алгоритма и дополнительных заголовков, а RFC 4301 прямо требует учитывать ESP/AH, синхронизационные данные и внешний IP-заголовок при обновлении PMTU ассоциации безопасности [11].

Классический PMTUD для IPv4 опирается на установленный DF и ICMP Destination Unreachable, Code 4 [6], а IPv6 использует ICMPv6 Packet Too Big [7]. Если такой сигнал не доходит до отправителя, малые запросы продолжают работать, а передача крупных блоков зависает. Этот диагностически сложный эффект получил название PMTUD black hole [12]. Полный запрет ICMP, таким образом, не является безопасной эксплуатационной политикой.

Противоположная стратегия также проблемна. ICMP-сообщение не защищается ключами туннеля, а его цитируемой части может не хватить для надежной привязки к исходному зашифрованному пакету. RFC 5927 анализирует атаки ICMP на TCP, включая принудительное изменение PMTU [13]. Cisco документировала отказ в обслуживании туннелей посредством сформированных сообщений «fragmentation needed» и ввела минимальную границу принимаемого PMTU для ряда реализаций [17]. Русскоязычная практическая работа воспроизводит снижение MTU IPsec-туннеля под действием поддельного ICMP [5]. Следовательно, задача состоит не в выборе между «разрешить ICMP» и «запретить ICMP», а в разделении сигнала и доказательства.

Цель работы — разработать методику, сохраняющую доступность туннеля при потере PTB и не позволяющую одному неподтвержденному PTB непосредственно изменять рабочий размер пакета. Для этого решаются четыре задачи: формализуется связь внешнего PMTU и внутреннего MPS; строится модель угроз и отказов; предлагается двухконтурный автомат подтверждения; четыре политики сравниваются в воспроизводимом вычислительном эксперименте. Научная новизна заключается не в замене DPLPMTUD, стандартизованного RFC 8899, а в его композиции с состоянием защищенного туннеля: ключ состояния включает узел, внешний путь и эпоху накладных

расходов, а подтвержденная внешняя оценка преобразуется в ограничение внутреннего пакета и TCP MSS.

Нормативная и научная основа

ГОСТ Р ИСО/МЭК 27033-1-2011 связывает сетевую безопасность с защитой передаваемой информации, услуг, устройств и конечных пользователей на основе оценки рисков [1]. ГОСТ Р ИСО/МЭК 27033-2-2021 требует документировать архитектуру и реализацию мер сетевой безопасности [2]. Для PMTUD это означает необходимость фиксировать источник MTU-состояния, срок его жизни и реакцию при недостоверном сигнале.

ГОСТ Р ИСО/МЭК 27033-4-2021 рассматривает шлюзы безопасности, их политику, мониторинг и проверку [3]. ГОСТ Р ИСО/МЭК 27002-2021 задает риск-ориентированный выбор мер, включая журналирование и управление сетевой безопасностью [4]. Стандарты не определяют алгоритм PMTU, но поддерживают проверяемость решения и отказоустойчивость, которые в рассматриваемой архитектуре реализуются журналом переходов и подтверждаемыми пробами.

RFC 1191 и RFC 8201 определяют классический PMTUD для IPv4 и IPv6 [6, 7]. RFC 2923 показывает, что потеря требуемого ICMP приводит к black hole, при котором небольшие пакеты проходят, а крупные многократно теряются [12]. Для UDP RFC 8085 рекомендует ограничивать размер дейтаграмм и использовать информацию PMTU либо механизм обнаружения пути [14]. В современных дейтаграммных протоколах это развитие получило форму DPLPMTUD.

RFC 8899 требует проверять PTB до использования, запрещает непосредственно устанавливать PLPMTU по сообщенному значению и предусматривает подтверждающие пробы, black-hole detection и повторный поиск увеличившегося размера [8]. RFC 9869 переносит подтверждаемую пробу на UDP Options: проба должна вызывать положительное подтверждение доставки конкретного размера [20]. Предложенная методика сохраняет эти принципы, но размещает автомат на границе защищенного туннеля и добавляет

преобразование внешнего PLPMTU во внутренний MPS с учетом текущей инкапсуляции.

Проблемы туннелей систематизированы в RFC 4459: возможны фрагментация внешнего пакета, сигнал источнику, резерв MTU в опорной сети или фрагментация внутреннего IPv4-пакета; универсального решения нет, особенно при вложенных туннелях [10]. RFC 8900 рассматривает IP-фрагментацию как хрупкий механизм из-за потерь фрагментов, сложности фильтрации и ресурсов сборки [9]. Поэтому фрагментация в работе не используется как нормальный режим, а остается явно контролируемым аварийным решением.

Операционные документы также показывают неоднородность реализаций. Cisco описывает различия GRE, IPsec и их комбинаций, а также MSS clamping, который помогает TCP, но не решает задачу для UDP [16]. Linux предоставляет режимы ip_no_pmtu_disc, нижнюю границу min_pmtu и время жизни кэша, то есть политика обработки PMTU является настраиваемой и влияет на все потоки к назначению [18]. Новая работа Feng и соавторов показывает, что совместное PMTU-состояние при разделяемом IP может становиться побочным каналом и нарушать изоляцию TCP-соединений [19]. Это дополнительно обосновывает привязку состояния не только к адресу назначения.

Модель угроз и семантический разрыв

Рассматривается двунаправленный защищенный туннель с между узлами u и v. Нарушитель вне пути способен отправлять поддельные ICMP PTB на внешний адрес u и угадывать общедоступные признаки потока, но не может сформировать корректное защищенное подтверждение от v. Нарушитель на пути может блокировать PTB, выборочно отбрасывать крупные пакеты либо сформировать правдоподобное сообщение с цитатой наблюдаемого пакета. Также учитываются неумышленные причины: фильтрация ICMP, асимметричная маршрутизация, ECMP с разными MTU и изменение набора заголовков при NAT-T или вложенной инкапсуляции. Компрометация конечного узла и криптографических ключей не рассматривается.

На рисунке 1 показаны два противоположных отказа. В корректном пути слишком большой внешний пакет вызывает PTB, после чего отправитель выбирает меньший размер. При фильтрации PTB прежний размер сохраняется и полезные пакеты теряются. При подделке PTB немедленное принятие значения создает устойчиво малый MPS даже при фактическом внешнем PMTU 1500 байт. Наличие шифрования полезной нагрузки не устраняет этот разрыв, поскольку решение меняется по внешнему, неаутентифицированному сигналу.

Рисунок 1. Два противоположных отказа классического PMTUD в защищенном туннеле

Пять сценариев эксперимента приведены в таблице 1. В S1 и S2 внешний PMTU уменьшается соответственно до 1360 и 1320 байт при 60 байтах накладных расходов. S3 сохраняет внешний PMTU 1500, но передает поддельное значение 576–900. S4 моделирует чередование путей 1500 и 1280, поэтому устойчивый внутренний предел равен 1220. В S5 внешний PMTU остается 1500, но накладные расходы возрастают с 60 до 96 байт, уменьшая внутренний предел с 1440 до 1404.

Таблица 1. Сценарии отказов и атак

S	Событие	O, байт	Обратная связь	M*, байт	Основной риск
1	PMTU 1500 -> 1360	60	PTB доставлен	1300	штатное снижение

S	Событие	O, байт	Обратная связь	M*, байт	Основной риск
2	PMTU 1500 -> 1320	60	PTB блокирован	1260	PMTUD black hole
3	PMTU = 1500	60	поддельный PTB 576-900	1440	ложное снижение
4	ECMP 1500 / 1280	60	непостоянный сигнал	1220	осцилляция размера
5	O: 60 -> 96	96	внешняя PMTU прежняя	1404	устаревший overhead

Примечание: параметры сценариев заданы автором для сравнения политик и не являются частотами реальных инцидентов.

Формальная модель безопасного размера

Пусть P(p,t) — фактический PMTU внешнего пути p, а O(c,e) — накладные расходы туннеля c в эпохе инкапсуляции e. Максимальный внутренний пакет, не требующий внешней фрагментации, равен:

$$M^*(c,p,t) = P(p,t) - O(c,e(t)).$$

Рабочее ограничение W(k,t) хранится по ключу k, который не сводится к адресу назначения:

$$k = \mathrm{Hash}(\mathrm{peer} \,\|\, \mathrm{outer\_path} \,\|\, \mathrm{route\_id} \,\|\, \mathrm{encapsulation\_epoch}).$$

Сообщение PTB с заявленным MTU m и цитатой q считается допустимым входом автомата, если цитата сопоставлена с недавно отправленным внешним пакетом, m находится между эксплуатационным минимумом и размером этого пакета, а возраст записи не превышает Δq:

$$\mathrm{ValidPTB}(m,q,t) = \mathrm{Match}(q,\mathrm{recent\_outer}) \wedge M_{floor} \le m < |q| \wedge t - t_q \le \Delta q.$$

Даже истинность ValidPTB не означает немедленного изменения W. Она переводит автомат в состояние CONFIRM_DOWN и задает размер пробы. Уменьшение фиксируется после защищенного подтверждения пробы меньшего

размера либо после устойчивого обнаружения black hole и подтверждения базового размера. Для внутреннего пакета x действует инвариант:

$$\mathrm{SafeSend}(c,k,x,t) = \mathrm{Auth}(c) \wedge x \le W(k,t) \wedge W(k,t) + O(c,e(t)) \le \hat{P}(k,t).$$

Здесь $\hat{P}$ — подтвержденная оценка внешнего пути. Если меняется только e, старая внешняя оценка может быть повторно использована, но внутреннее ограничение пересчитывается как $\min(W, \hat{P} - O_{new})$. Такое событие не должно ожидать ICMP: источник изменения находится на самом узле туннеля.

Для оценки используются четыре показателя. A — доля доставленных полезных байтов; B — доля трасс, где A отдельной трассы меньше авторского порога 0,95; D — доля трасс S3, завершившихся более чем на 128 байт ниже фактического M*; C — относительное число внешних дейтаграмм на доставленный полезный объем с учетом повторной передачи:

$$A(\pi) = \Sigma\ \mathrm{delivered\_bytes} / \Sigma\ \mathrm{offered\_bytes}.$$

$$B(\pi) = N(Ai < 0.95) / N.$$

$$D(\pi) = N(W_{final} < M^* - 128 \mid S3) / N(S3).$$

$$C(\pi) = (\mathrm{Payload}_{ideal} / \mathrm{Payload}_{\pi}) / A(\pi).$$

Порог 128 байт не является требованием стандарта; он выбран для отделения небольшого технологического запаса от существенного ухудшения. Все метрики интерпретируются только в рамках заданной модели.

Предлагаемая методика и архитектура

Сравниваются четыре политики. P0 немедленно принимает сопоставленный PTB и зависит от его доставки. P1 всегда использует внутренний MPS 1180 байт; это нижняя эксплуатационная точка выбранного стенда, а не универсальная рекомендация. P2 дополняет P0 минимальной границей 1200 байт. P3 реализует предложенную композицию: проверяет цитату, использует PTB только как подсказку, подтверждает размер защищенной пробой, обнаруживает потерю крупных пакетов без ICMP и пересчитывает MPS по событию изменения overhead.

Таблица 2. Сравниваемые политики PMTU

P	Реакция на PTB	Подтверждение	Ключ состояния	Следствие
0	PTB сразу изменяет W	нет	назначение / кэш PMTU	быстро при истинном PTB; уязвимо к блокировке и подделке
1	динамика игнорируется	MPS = 1180	глобальная константа	доступно в модели; постоянная пакетная цена
2	PTB изменяет W с floor	floor = 1200	назначение + минимум	ограничивает снижение; не устраняет black hole
3	PTB создает кандидата	защищенная проба	peer + путь + route + epoch	предложенный подтверждаемый инвариант

Архитектура P3 показана на рисунке 2. Внешний наблюдатель получает ICMP, но не имеет права записать рабочий MTU. Он передает нормализованный кандидат автомату. Генератор проб формирует защищенную дейтаграмму заданного внешнего размера с идентификатором, включенным в аутентифицированную полезную нагрузку. Ответ узла v подтверждает достижение конкретного размера. Хранилище разделяет состояния разных узлов, маршрутов и эпох инкапсуляции. Внутренний кондиционер применяет W к IP-пакетам и, как дополнительную меру для TCP, ограничивает MSS; для UDP и иных протоколов используется MPS, а не только MSS.

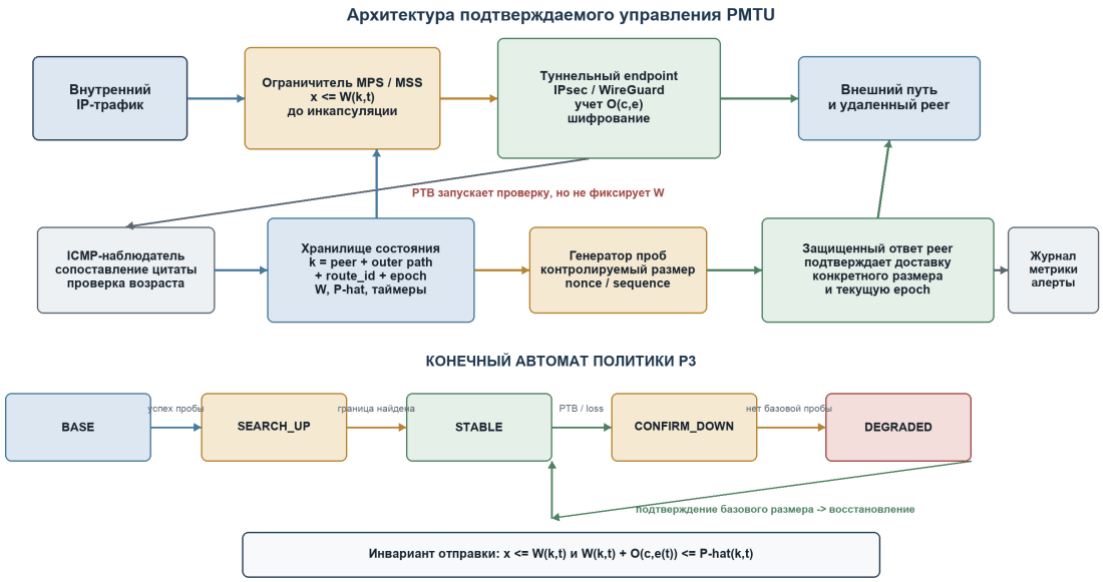

Рисунок 2. Архитектура подтверждаемого управления PMTU и автомат P3

Автомат содержит состояния BASE, SEARCH_UP, STABLE, CONFIRM_DOWN, DEGRADED и RECOVER. После установления защищенного канала BASE проверяет гарантированный размер. SEARCH_UP увеличивает пробу ступенями и после серии подтверждений фиксирует STABLE. PTB или серия потерь пакетов, превышающих текущую базу, переводит систему в CONFIRM_DOWN. Неподтвержденный PTB журналируется и не изменяет W. При неуспехе большой пробы, но успехе меньшей выбирается подтвержденная нижняя точка. DEGRADED ограничивает данные базовым размером, а RECOVER периодически проверяет увеличение с гистерезисом, чтобы не колебаться на ECMP-пути.

Обработка должна быть ограничена по частоте, поскольку разбор цитируемых заголовков сам может стать нагрузочной атакой; RFC 8899 допускает потерю PTB, так как DPLPMTUD не зависит от их обязательной доставки [8]. Для on-path-нарушителя одной проверки цитаты недостаточно: наблюдатель способен сформировать правдоподобное сообщение. Защита достигается тем, что заявленное значение только выбирает размер следующей пробы, а не становится рабочим состоянием.

Методика вычислительного эксперимента

Эксперимент реализован на Python 3.12.13 и NumPy 2.3.5 с фиксированным seed 20260819. Для каждой пары из пяти сценариев и четырех политик сгенерировано 20 000 трасс длительностью 10 с, всего 400 000. Событие изменения пути наступает нормально около 1500 мс со стандартным отклонением 180 мс и ограничением 700–2300 мс. RTT распределен логнормально с медианой 48 мс и параметром формы 0,42. Фоновая потеря задана как 0,018·Beta(1,2; 4,8). Безопасный MPS варьируется нормально вокруг значения сценария со стандартным отклонением 10 байт.

В S1 вероятность доставки классического PTB принята равной 0,94. В S2 PTB полностью блокируется; поздний fallback срабатывает с вероятностью 0,18 для P0 и 0,24 для P2. В S4 вероятность сходимости P0, P2 и P3 к устойчивой точке задана 0,79, 0,83 и 0,985. В S5 локальное распознавание изменившегося overhead для P0 и P2 срабатывает с вероятностью 0,44 и 0,58, тогда как P3 получает событие смены эпохи. Для P3 вероятность ложного подтверждения снижения в S3 принята равной 0,0015. Это авторские условные параметры для сравнения архитектур, а не измеренные частоты отказов или атак.

Трасса учитывает интервал до события, время восстановления, долю полезных данных, размер устойчивого пакета и повторную обработку при потерях. В S4 крупные пакеты затрагиваются на низком ECMP-пути с долей 0,25. Для долей B и D рассчитан 95%-й интервал Уилсона. Отдельно выполнено 60 пакетов по 20 000 локальных решений на Apple Silicon. Микротест включает только операции над уже разобранным состоянием и исключает сеть, криптографию, системные вызовы, журнал и поэтому задает нижнюю границу вычислительной цены, а не производительность VPN-шлюза.

Результаты и обсуждение

Агрегированные результаты приведены в таблице 3. P0 доставила 78,405% полезных данных; 37,245% трасс перешли порог black hole. Основной вклад дали S2 с блокированным PTB и S5, где внешняя оценка не учитывала новую инкапсуляцию. В S3 P0 приняла все поддельные значения, а медианный

внутренний MPS составил 677 байт. Минимальная граница P2 не устранила зависимость от доставки PTB: B снизилась только до 33,530%.

Таблица 3. Агрегированные результаты вычислительного эксперимента

P	A, %	B, % [95% ДИ]	D (S3), % [95% ДИ]	C	R50, мс	R95, мс	t50, нс
0	78,405	37,245 [36,946-37,545]	100,000 [99,981-100,000]	1,893	407,680	8713,607	46,077
1	99,641	0,000 [0,000-0,0038]	100,000 [99,981-100,000]	1,131	0,000*	0,000*	38,952
2	81,091	33,530 [33,238-33,823]	100,000 [99,981-100,000]	1,607	279,405	8693,915	77,590
3	98,702	0,798 [0,745-0,855]	0,130 [0,089-0,190]	1,020	154,927	445,414	77,026

*Примечание: A - доставленные полезные данные; B - трассы с A_i < 0,95; D - ложное снижение более чем на 128 байт в S3; C - относительная пакетная цена; R - время восстановления; t50 - медиана локального микротеста. * Статическая P1 начинает с MPS 1180 и не выполняет поиск вверх. 95% ДИ рассчитаны методом Уилсона.*

P1 обеспечила A = 99,641% и отсутствие black-hole-трасс в заданном диапазоне, поскольку 1180 байт помещались во все сценарные пути. Однако C = 1,131 означает на 13,1% больше внешних дейтаграмм на доставленный полезный объем относительно адаптивного идеала. D = 100% для P1 не означает успешную атаку: статическая политика изначально находится более чем на 128 байт ниже M* в S3. Этот результат показывает цену неадаптивного запаса.

P3 обеспечила A = 98,702%, B = 0,798% [0,745–0,855%] и C = 1,020. В S3 ложное снижение произошло в 0,130% [0,089–0,190%] трасс из-за принятой в модели комбинации потерь подтверждающих проб. Медианное время перехода к безопасному состоянию для S1, S2, S4 и S5 составило 154,927 мс, 95-й процентиль — 445,414 мс. Статическая P1 начинает в безопасной точке и поэтому имеет нулевое время восстановления, но не выполняет поиск увеличения.

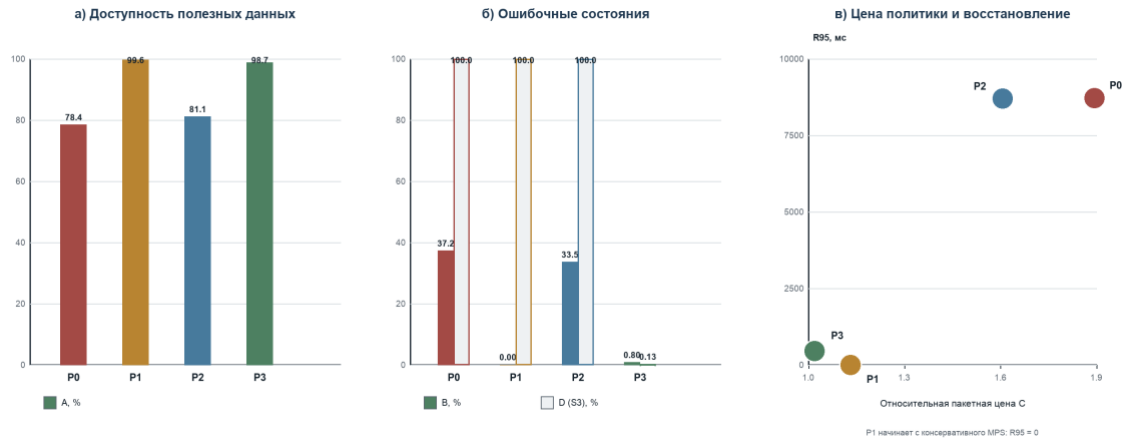

Рисунок 3. Доступность, ошибочные состояния и цена сравниваемых политик

Локальный микротест дал медианы 46,077; 38,952; 77,590 и 77,026 нс на решение P0–P3. Сходство P2 и P3 объясняется тем, что измерен уже разобранный набор целочисленных условий. В реальной системе цену P3 определят защищенные пробы, RTT, таблица состояния и журнал, а не десятки наносекунд локальной ветви. Поэтому результат используется лишь для проверки отсутствия алгоритмически тяжелой операции в пути решения.

Полученное преимущество P3 соответствует нормативной логике DPLPMTUD: PTB может ускорить поиск, но не должен напрямую устанавливать рабочий PLPMTU [8]. Отличие работы состоит в явном согласовании трех величин — внешнего подтвержденного PMTU, меняющегося overhead и внутреннего MPS — и в изоляции состояния по туннельному контексту. Это важно для современных схем с разделяемыми адресами, где общее PMTU-состояние способно нарушать изоляцию потоков [19].

Ограничения исследования

Первое ограничение — событийная, а не пакетная модель. Она не реализует IP-фрагменты, конкретный IPsec SA, WireGuard-код или очереди сетевой карты. Распределения RTT, потерь и вероятности сходимости заданы автором. Результаты показывают последствия выбранных правил, но не прогнозируют частоту атак. Для конкретного продукта необходим стенд с Linux network namespaces или аппаратными шлюзами, управляемым ICMP-фильтром и несколькими внешними MTU.

Второе ограничение — доверие конечным узлам туннеля. Защищенное подтверждение доказывает доставку пробы узлу v, но не гарантирует, что последующие пакеты пойдут по тому же ECMP-пути. Гистерезис уменьшает колебания, однако при per-packet balancing безопасной оценкой может оказаться минимум наблюдаемых путей. Привязка route_id требует сигнала от маршрутизатора или сетевого пространства имен и зависит от реализации.

Третье ограничение — минимальная точка. Значения 1180 и 1200 выбраны для конкретной модели с внешним минимумом 1280 и максимальным overhead 96. Их нельзя переносить как универсальную настройку. Для IPv6 RFC 8201 требует учитывать минимальный IPv6 MTU, но внутренний MPS туннеля дополнительно уменьшается на его заголовки [7]. Эксплуатационный Mfloor должен вычисляться из поддерживаемых семейств адресов, инкапсуляций и обязательных сообщений управления.

Четвертое ограничение — on-path-нарушитель. Он способен последовательно отбрасывать все пробы больше выбранного размера, и никакой PMTUD не отличит это от реального узкого канала. P3 предотвращает неподтвержденное изменение и сохраняет базовую связность, но не доказывает физическую причину ограничения. Для расследования требуются журнал маршрута, телеметрия соседних узлов и корреляция с изменениями конфигурации.

Практическое внедрение

Внедрение начинается с инвентаризации мест, где размер пакета меняется: внешний IP, UDP, ESP, GRE, VLAN, NAT-T, дополнительные метки и алгоритмически зависящее выравнивание. Для каждой комбинации вычисляется O и создается encapsulation_epoch. Изменение любого элемента увеличивает epoch и немедленно пересчитывает внутренний предел из последней подтвержденной внешней оценки.

ICMP PTB не следует блокировать полностью. Шлюз принимает его на ограниченный обработчик, проверяет адреса, протокол, цитату недавно отправленного пакета, заявленный диапазон и rate limit. Успех проверки создает событие PTB_CANDIDATE, но не запись рабочего MTU. Неподтвержденные и повторяющиеся сообщения журналируются с хэшем цитаты. Для защищенной пробы достаточно расширения управляющего протокола туннеля или специальной аутентифицированной дейтаграммы, размер которой контролирует отправитель.

Внутреннее ограничение применяется до инкапсуляции. TCP MSS clamping полезен как дополнительная защита для транзитного TCP, но не покрывает UDP и не должен быть единственным механизмом, что согласуется с эксплуатационным анализом туннелей [16]. Внешняя фрагментация по умолчанию запрещается; если она необходима для наследуемого протокола, режим оформляется отдельной политикой с лимитами сборки и мониторингом, поскольку фрагментация остается хрупкой [9].

Приемочные испытания должны включать пять сценариев таблицы 1, IPv4 и IPv6, изменение адреса внешнего узла, ротацию ключей без смены overhead, вложенный туннель, потерю отдельных фрагментов ICMP-цитаты и всплеск поддельных PTB. Положительный критерий требует не только сохранения ping: крупный UDP-обмен и TCP-передача должны восстановиться, рабочий MPS не должен изменяться от одного неподтвержденного сообщения, а новая эпоха инкапсуляции должна появиться в журнале до пропуска превышающих предел внутренних пакетов.

Заключение

Ошибки PMTUD образуют для защищенного туннеля двусторонний риск. Потеря PTB создает black hole, а немедленное доверие PTB позволяет занизить рабочий размер. Статический консервативный MPS обеспечивает доступность только в заранее известном диапазоне и увеличивает число обрабатываемых дейтаграмм. Дополнительный класс отказов связан не с внешним путем, а с изменением накладных расходов самого туннеля.

Предложенная методика отделяет прием сигнала от фиксации состояния. PTB проходит проверку и выбирает размер пробы; изменение подтверждается защищенным ответом, а рабочая запись связывается с узлом, путем и эпохой инкапсуляции. В авторском эксперименте P3 обеспечила 98,702% доставленных данных, снизила black-hole-трассы до 0,798%, ложные снижения S3 — до 0,130% и имела относительную пакетную цену 1,020. Практический вывод состоит в размещении автомата на туннельном endpoint, использовании внешнего DPLPMTUD совместно с внутренним MPS и отказе как от безусловного доверия ICMP, так и от полного запрета обратной связи.

Список литературы

1. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. М.: Стандартинформ, 2012. URL: https://protect.gost.ru/gost/details/775007f4-c66c-48e3-a0e9-8f0c3bad18b2 (дата обращения: 19.08.2026).

2. ГОСТ Р ИСО/МЭК 27033-2-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 2. Рекомендации по проектированию и реализации безопасности сетей. М.: Стандартинформ, 2021. URL: https://protect.gost.ru/gost/details/835bbe29-f2b4-4e51-8eb0-14df14a6b4e5 (дата обращения: 19.08.2026).

3. ГОСТ Р ИСО/МЭК 27033-4-2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов

безопасности. М.: Стандартинформ, 2021. URL: https://protect.gost.ru/gost/details/7cca26f3-1131-479d-8062-d1c4fbb22359 (дата обращения: 19.08.2026).

4. ГОСТ Р ИСО/МЭК 27002-2021. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности. М.: Стандартинформ, 2021. URL: https://protect.gost.ru/gost/details/be00167c-6e26-4042-ac31-36be8a9d6b2e (дата обращения: 19.08.2026).

5. Бондаренко Я. IPsec & path MTU discovery: фича али баг? / пер. braonle // Хабр. 2023. URL: https://habr.com/ru/articles/778914/ (дата обращения: 19.08.2026).

6. Mogul J., Deering S. Path MTU Discovery. RFC 1191. IETF, 1990. DOI: 10.17487/RFC1191. URL: https://www.rfc-editor.org/rfc/rfc1191.html (дата обращения: 19.08.2026).

7. McCann J., Deering S., Mogul J., Hinden R. Path MTU Discovery for IP version 6. RFC 8201. IETF, 2017. DOI: 10.17487/RFC8201. URL: https://www.rfc-editor.org/rfc/rfc8201.html (дата обращения: 19.08.2026).

8. Fairhurst G., Jones T., Tüxen M., Rüngeler I., Völker T. Packetization Layer Path MTU Discovery for Datagram Transports. RFC 8899. IETF, 2020. DOI: 10.17487/RFC8899. URL: https://www.rfc-editor.org/rfc/rfc8899.html (дата обращения: 19.08.2026).

9. Bonica R., Baker F., Huston G., Hinden R., Troan O., Gont F. IP Fragmentation Considered Fragile. RFC 8900. IETF, 2020. URL: https://www.rfc-editor.org/rfc/rfc8900.html (дата обращения: 19.08.2026).

10. Savola P. MTU and Fragmentation Issues with In-the-Network Tunneling. RFC 4459. IETF, 2006. DOI: 10.17487/RFC4459. URL: https://www.rfc-editor.org/rfc/rfc4459.html (дата обращения: 19.08.2026).

11. Kent S., Seo K. Security Architecture for the Internet Protocol. RFC 4301. IETF, 2005. DOI: 10.17487/RFC4301. URL: https://www.rfc-editor.org/rfc/rfc4301.html (дата обращения: 19.08.2026).

12. Lahey K. TCP Problems with Path MTU Discovery. RFC 2923. IETF, 2000. DOI: 10.17487/RFC2923. URL: https://www.rfc-editor.org/rfc/rfc2923.html (дата обращения: 19.08.2026).
13. Gont F. ICMP Attacks against TCP. RFC 5927. IETF, 2010. DOI: 10.17487/RFC5927. URL: https://www.rfc-editor.org/rfc/rfc5927.html (дата обращения: 19.08.2026).
14. Eggert L., Fairhurst G., Shepherd G. UDP Usage Guidelines. RFC 8085. IETF, 2017. DOI: 10.17487/RFC8085. URL: https://www.rfc-editor.org/rfc/rfc8085.html (дата обращения: 19.08.2026).
15. Donenfeld J. A. WireGuard: Next Generation Kernel Network Tunnel. 2017. URL: https://www.wireguard.com/papers/wireguard.pdf (дата обращения: 19.08.2026).
16. Cisco Systems. Resolve IPv4 Fragmentation, MTU, MSS, and PMTUD Issues with GRE and IPsec. 2023. URL: https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html (дата обращения: 19.08.2026).
17. Cisco Systems. Crafted ICMP Messages Can Cause Denial of Service. Security Advisory cisco-sa-20050412-icmp. URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20050412-icmp (дата обращения: 19.08.2026).
18. Linux Kernel Documentation. IP Sysctl: ip_no_pmtu_disc, min_pmtu, mtu_expires. URL: https://www.kernel.org/doc/html/latest/networking/ip-sysctl.html (дата обращения: 19.08.2026).
19. Feng X., Li Z., Li Q., Wang Z., Sun K., Xu K. Off-Path TCP Exploits: PMTUD Breaks TCP Connection Isolation in IP Address Sharing Scenarios. arXiv:2509.11833, 2025. DOI: 10.48550/arXiv.2509.11833. URL: https://arxiv.org/abs/2509.11833 (дата обращения: 19.08.2026).
20. Fairhurst G., Jones T. Datagram Packetization Layer Path MTU Discovery (DPLPMTUD) for UDP Options. RFC 9869. IETF, 2025. DOI: 10.17487/RFC9869. URL: https://www.rfc-editor.org/rfc/rfc9869.html (дата обращения: 19.08.2026).