УДК 004.94+004.056.5

Корякин Владислав Юрьевич, студент, РГУ нефти и газа (НИУ) имени И.М. Губкина, г.Москва

Тищенко Эльдар Валерьевич, студент, РГУ нефти и газа (НИУ) имени И.М. Губкина, г.Москва

ДЕТЕРМИНИРОВАННЫЕ ПОЛИТИКИ CISCO ASA ПРОТИВ DOS-АТАК НА WEBVPN

Аннотация

В работе рассматривается защита веб-сервера VPN (WebVPN) программного обеспечения Cisco Secure Firewall ASA от атак типа «отказ в обслуживании» (DoS), эксплуатирующих уязвимость неэффективного управления памятью (CVE-2026-20039). Предложена и проверена в лабораторном стенде комбинированная схема защиты, объединяющая политики ограничения соединений (connection limits) и поведенческую детекцию угроз (threat-detection) с автоматической блокировкой источника (shun), а также независимый контур мониторинга на базе IDS Suricata. Сформулирована гипотеза исследования, приведены количественные метрики срабатывания защиты, оценены время реакции, доля ошибочно отброшенных легитимных запросов (false positive) и влияние защитных политик на производительность сервиса. Обсуждается вариабельность результатов и направления дальнейшей экспериментальной проверки.

Annotation

This paper examines the protection of a web-based VPN server (WebVPN) of Cisco Secure Firewall ASA software from denial-of-service (DoS) attacks that exploit memory management inefficiency vulnerability (CVE-2026-20039). A combined protection scheme has been proposed and tested in a laboratory testbed, combining

connection limit policies and behavioral threat detection with automatic source blocking (shun), as well as an independent monitoring circuit based on Suricata IDS. The research hypothesis is formulated, quantitative metrics of protection triggering are provided, reaction time is evaluated, the proportion of falsely dropped legitimate requests (false positives) and the impact of protective policies on service performance are assessed. The variability of results and directions for further experimental verification are discussed.

Ключевые слова: Cisco ASA, WebVPN, DoS-атака, threat-detection, connection limits, Suricata, обнаружение вторжений, информационная безопасность.

Keywords: Cisco ASA, WebVPN, DoS attack, threat-detection, connection limits, Suricata, intrusion detection, information security

1. Введение

Удаленный доступ к корпоративным ресурсам через шлюзы SSL VPN остается одним из наиболее критичных и одновременно наиболее атакуемых сервисов периметра. Веб-сервер VPN в составе Cisco Secure Firewall Adaptive Security Appliance (ASA) и Cisco Secure Firewall Threat Defense (FTD) неоднократно становился объектом уязвимостей класса «отказ в обслуживании». Так, в опубликованном Cisco отчете безопасности от марта 2026 года описана уязвимость CVE-2026-20039: неаутентифицированный удаленный злоумышленник может вызвать перезагрузку устройства и состояние DoS, отправляя большое количество специально сформированных HTTP-запросов; причиной является неэффективное управление памятью веб-сервера VPN [1]. Аналогичные по природе дефекты управления памятью SSL VPN фиксировались Cisco и ранее [2], [3], что подтверждает системный характер проблемы для данного класса сервисов.

Существующие подходы к противодействию DoS-атакам на веб-сервисы условно делятся на три группы. Первая группа опирается на интеллектуальный анализ трафика и методы машинного обучения [7], [8], [9]; такие методы обладают высокой чувствительностью, но требуют репрезентативных обучающих выборок и подвержены переобучению при переносе в эксплуатируемую сеть. Вторая группа рассматривает обнаружение и нейтрализацию медленных маломощных атак прикладного уровня (Slowloris, Slow Read) на уровне выделенных систем предотвращения вторжений [5], [6], где блокировка строится на анализе аномалий сетевого трафика. Третья группа – общие архитектурные рекомендации по устойчивости к DoS и минимизации поверхности атаки, закрепленные в отраслевых документах [4], [10]. Настоящая работа занимает промежуточную нишу: вместо обучаемых моделей или внешних IPS она исследует встроенные детерминированные механизмы самого межсетевого экрана (политики ограничения соединений и поведенческую детекцию threat-detection), дополняя их независимым контуром мониторинга. Такой ракурс – количественная характеристика штатных средств ASA в применении к конкретной уязвимости WebVPN – в известных автору публикациях системно не представлен.

Особенность рассматриваемого вектора в том, что трафик к WebVPN передается по HTTPS, поэтому отбросить запрос по содержимому (например, по наличию большого числа HTML-сущностей   в теле) на сетевом уровне невозможно, так как полезная нагрузка зашифрована. Это смещает акцент защиты с фильтрации по сигнатуре содержимого на поведенческие и количественные признаки: интенсивность подключений, число полуоткрытых соединений, скорость с одного источника. Подобный подход согласуется с выводами обзорных работ по распознаванию компьютерных атак, где поведенческие методы выделяются как предпочтительные для поиска аномалий

[4], а также с практикой защиты от медленных маломощных атак прикладного уровня [5], [6].

Настоящая работа решает прикладную задачу: показать, что штатными средствами Cisco ASA (без дополнительного оборудования и до установки патча) можно существенно снизить эффективность DoS-атаки на WebVPN и обеспечить ее обнаружение. В отличие от ряда исследований, делающих акцент на обнаружении атак методами машинного обучения [7], [8], [9], здесь рассматривается комбинация детерминированных политик устройства и независимого сетевого мониторинга, что важно для эксплуатируемых сетей, где может преобладать переобучение моделей.

Объект исследования – процесс защиты и мониторинга WebVPN-сервиса Cisco ASA в условиях DoS-атаки, эксплуатирующей уязвимость неэффективного управления памятью CVE-2026-20039.

Предмет исследования – детерминированные штатные механизмы Cisco ASA (политики ограничения соединений и поведенческая детекция threat-detection с автоматической блокировкой shun) и независимый контур обнаружения на базе IDS Suricata, а также их количественные характеристики при противодействии указанной атаке.

Цель работы – экспериментально установить, в какой мере штатные детерминированные средства Cisco ASA (без дополнительного оборудования и до установки исправления производителя) снижают эффективность DoS-атаки на WebVPN и обеспечивают ее обнаружение, и дать этим средствам количественную оценку.

Для достижения цели поставлены следующие задачи: построить лабораторный стенд, воспроизводящий топологию доступа к WebVPN-сервису; настроить два уровня детерминированной защиты (ограничение соединений и threat-detection с shun) и независимый контур мониторинга на Suricata; смоделировать нарастающую по интенсивности DoS-нагрузку и зафиксировать

пороговое поведение защитных механизмов; оценить время реакции, долю ошибочно отброшенных легитимных запросов и влияние политик на устойчивость сервиса; сформулировать рекомендации по эшелонированной (многоуровневой) защите сервиса.

Научная новизна работы состоит в следующем. Во-первых, получена количественная характеристика порогового поведения механизма threat-detection: автоматическая блокировка источника наступает при одновременном достижении Trigger=5 в 10-минутном окне и Trigger≥1 в часовом окне, что соответствует накоплению около 1500 событий; этот воспроизводимый параметр отсутствует в эксплуатационной документации Cisco. Во-вторых, дана оценка доли ложных отказов в привязке к политике per-client-max: около 33–50 % отказов для агрессивного клиента при близкой к нулю доле для обычного пользователя – практически значимая характеристика, не приводимая в официальных руководствах. В-третьих, проверка выполнена с использованием отечественного программного обеспечения: контур наблюдения и сбора журналов стенда построен на ОС «Альт», что придает результатам дополнительную ценность в контексте импортозамещения.

2. Гипотеза исследования и критерии оценки

Гипотеза исследования. Комбинация политик ограничения соединений (connection limits на уровне per-client) и поведенческой детекции угроз (threat-detection с автоматической блокировкой shun) обеспечивает блокировку источника DoS-атаки на WebVPN-сервис Cisco ASA при интенсивности паразитного трафика, не доводя устройство до перезагрузки, при этом независимый контур мониторинга (IDS Suricata) фиксирует факт атаки в режиме реального времени.

Для проверки гипотезы введены количественные критерии успеха/неуспеха защитного механизма:

1) число событий threat-detection, накопленных за интервал наблюдения (10-минутное и часовое окно), и значение текущей интенсивности (eps);
2) значение счетчиков срабатывания триггеров (Trigger) в 10-минутном и часовом окнах;
3) факт и момент активации автоматической блокировки источника (shun), который является основным бинарным критерием успеха;
4) доля легитимных запросов, ошибочно отброшенных при действующих политиках (false positive rate);
5) оценка влияния защитных политик на производительность и устойчивость WebVPN-сервиса (отсутствие перезагрузки, изменение времени отклика).

Атака считается успешно нейтрализованной, если источник переводится в состояние shun до того, как накопленная нагрузка приведет к исчерпанию ресурсов устройства; защита считается неуспешной, если устройство перезагружается либо если доля ошибочно отброшенных легитимных запросов превышает приемлемый порог при отсутствии реальной атаки.

3. Описание экспериментального стенда

Стенд построен на физическом коммутаторе Cisco Catalyst 3750 и межсетевом экране Cisco ASA 5506 с включенным сервисом WebVPN (AnyConnect). Сегмент «снаружи» (VLAN 10, сеть 10.0.0.0/24) объединяет интерфейс ASA с развернутым WebVPN (10.0.0.27), машину злоумышленника (VM1) и машину мониторинга/сбора статистики (VM2). Маршрутизация направлена на интерфейс ASA, поэтому трафик к WebVPN обрабатывается на control-plane как нетранзитный. Логическая топология стенда приведена на рисунке 1.

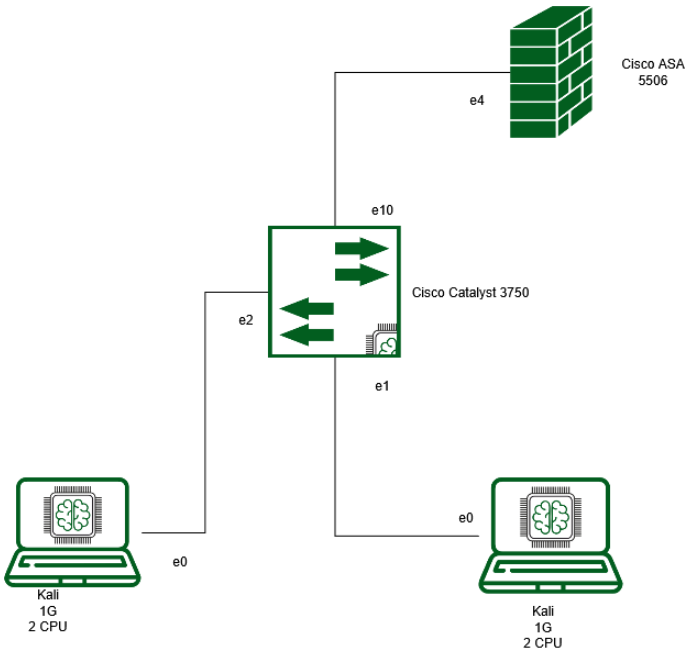

Рисунок 1 – L1 топология экспериментального стенда

Перечень аппаратного и программного обеспечения стенда с указанием версий приведен в таблице 1.

Таблица 1 – Версии оборудования и программного обеспечения стенда.

Компонент	**Модель**	**Роль в стенде**
Межсетевой экран	Cisco ASA 5506	WebVPN, политики защиты, threat-detection
Коммутатор	Cisco Catalyst 3750	Коммутация сегмента VLAN 10
ВМ злоумышленника (VM1)	Kali Linux (1 ГБ ОЗУ, 2 vCPU)	Генерация атакующего трафика
ВМ мониторинга (VM2)	Kali Linux (1 ГБ ОЗУ, 2 vCPU)	Мониторинг и сбор статистики (Suricata)

Компонент	Модель	Роль в стенде
IDS	Suricata 8.0.4	Независимый контур обнаружения

На ASA последовательно настроены два уровня защиты. Первый включает политики ограничения соединений, применяемые к HTTPS-трафику, адресованному интерфейсу WebVPN:

- conn-max 100: не более 100 одновременных соединений к WebVPN суммарно;
- embryonic-conn-max 50: не более 50 полуоткрытых (SYN без ACK) соединений;
- per-client-max 5: не более 5 соединений с одного клиента (ключевой параметр против DoS с одного IP);
- per-client-embryonic-max 3: не более 3 полуоткрытых соединений с одного клиента;
- timeout embryonic 0:00:10: полуоткрытые соединения сбрасываются через 10 секунд.

Второй уровень – поведенческая детекция threat-detection: базовая детекция аномалий (basic-threat), сбор статистики, правила dos-drop (за окна 600 и 3600 с) и scanning-threat с автоматической блокировкой источника. Такой двухконтурный принцип «фильтрация плюс поведенческий анализ» соответствует архитектуре современных средств сетевой защиты, включая межсетевые экраны нового поколения [10] и системы предотвращения вторжений [11].

Контур мониторинга реализован на VM2 средствами IDS Suricata 8.0.4 (отдельным правилом, фиксирующим обращения к WebVPN). Suricata выбрана как открытая высокопроизводительная платформа анализа трафика в реальном времени, эффективность которой подтверждена в ряде исследований [12], [13].

Инструменты генерации нагрузки на стороне злоумышленника приведены в таблице 1.

Таблица 2 – Инструменты генерации тестовой нагрузки.

Инструмент	Версия	Назначение
curl	8.19.0	Одиночные/крафтовые запросы к WebVPN
Apache-utils (ab)	2.3	Массовая генерация HTTP-запросов
slowhttptest	1.9.0	Медленные атаки прикладного уровня (slow headers/body/read)

4. Методика проведения эксперимента

В эксперименте проверяется срабатывание защитных политик и автоматической блокировки при нарастающей интенсивности атаки. Тремя инструментами (curl, ab, slowhttptest) генерируется «шумный» трафик к WebVPN; нагрузка наращивается волнами, на каждой фиксируются показатели threat-detection. На VM2 средствами Suricata выполняется независимый мониторинг обращений к WebVPN. Также проверяется ограничение доступа к сервису списком доступа.

5. Результаты и их обсуждение

5.1. Срабатывание защитных политик (фактические количественные данные)

Динамика срабатывания threat-detection по мере наращивания нагрузки приведена в таблице 3, которая отражает накопленное число событий сканирования за 10-минутное окно, текущую интенсивность, значения триггеров в 10-минутном и часовом окнах и факт блокировки источника.

Таблица 3 – Динамика метрик threat-detection по волнам атаки.

Волна	**События 10 мин**	**eps**	**Trigger 10 мин**	**Trigger 1 час**	**Shun**
1-я	133	0	1	0	-
2-я	229	11	1	0	-
3-я	327	11	1	0	-
4-я	824	20	3	0	-
5-я	1187	13	4	1	-
6-я	**1523**	16	**5**	1	**10.0.0.1**

Из таблицы 3 следуют три наблюдения. Во-первых, на малой нагрузке (волны 1-3, до ~330 событий за 10 минут, eps ≤ 11) фиксируется лишь одиночное срабатывание триггера, автоматическая блокировка не применяется. Во-вторых, при росте интенсивности до 20 eps (волна 4) число срабатываний триггера в 10-минутном окне увеличивается до 3, но shun по-прежнему не активируется. В-третьих, автоматическая блокировка источника 10.0.0.1 происходит при одновременном достижении Trigger=5 в 10-минутном окне и Trigger≥1 в часовом окне, что соответствует накоплению около 1500 событий. Таким образом, поведение защиты не бинарно «сработало/не сработало», а описывается количественной зависимостью момента блокировки от накопленной нагрузки и интенсивности.

Этот результат прямо подтверждает гипотезу: при интенсивности порядка единиц–десятков eps комбинация политик и threat-detection доводит источник до автоматической блокировки, не вызывая перезагрузки устройства.

5.1.1. Подтверждающие материалы эксперимента

Фактические данные таблицы 3 получены из вывода команд мониторинга на ASA. На рисунке 2 показан вывод show threat-detection rate в момент роста

нагрузки: по строке Scanning видно нарастание счетчика Trigger и накопленного числа событий (Total events), что соответствует переходу от волны к волне.

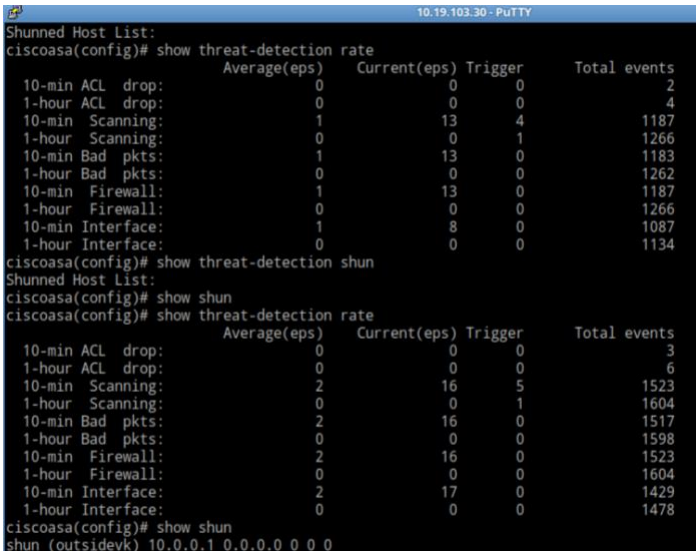

Рисунок 2 – Вывод show threat-detection rate: рост счетчиков Scanning

Идентификация источника атаки подтверждается выводом show threat-detection scanning-threat (рисунок 3): в списке атакующих хостов фигурирует адрес 10.0.0.1 (интерфейс outsidevk), который затем переводится в состояние shun.

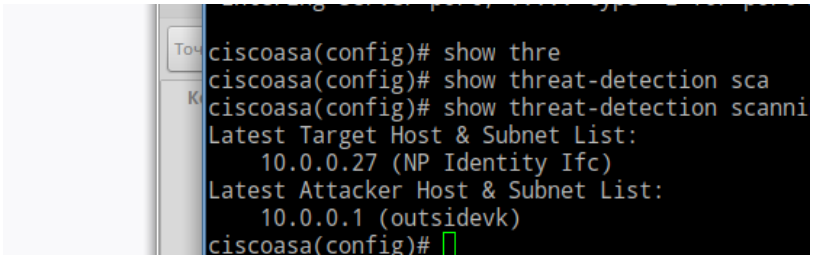

Рисунок 3 – Идентификация источника атаки: 10.0.0.1 (outsidevk)

Результат срабатывания защиты со стороны атакующего показан на рисунке 4: после блокировки утилита slowhttptest фиксирует статус «service available: NO» и завершает работу с ошибкой установления соединения (Cannot establish connection). Это прямое подтверждение того, что источник лишен доступа к WebVPN.

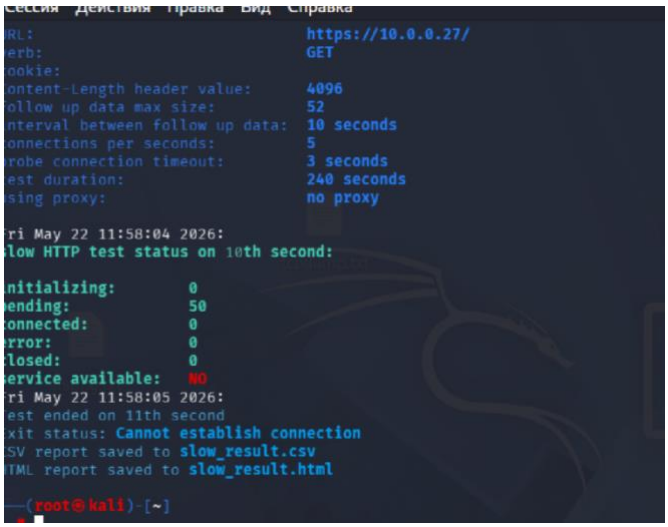

Рисунок 4 – Реакция slowhttptest после блокировки: сервис недоступен для источника

Независимый контур мониторинга на Suricata (эксперимент 1.2) фиксирует обращения к WebVPN в реальном времени. На рисунке 5 в журнале Suricata видны срабатывания пользовательского правила с пометкой CVE 2026-20039 для соединений к 10.0.0.27:443, что подтверждает как факт атаки, так и корректность сопоставления ее с рассматриваемой уязвимостью [1], [12].

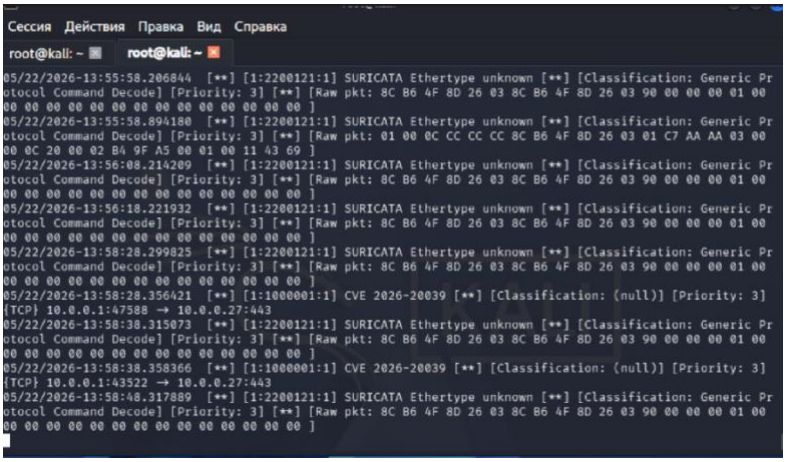

Рисунок 5 – Журнал Suricata: срабатывания правила на трафик к WebVPN

5.2. Время реакции механизмов защиты

Время реакции определяется как интервал от начала генерации паразитного трафика до момента активации shun. Прямого таймстемпа в исходном прогоне не фиксировалось, поэтому величина оценивается из параметров конфигурации и

наблюденной динамики (значение прогнозное). Блокировка наступает при Trigger=5 в 10-минутном окне; правило scanning-threat использует rate-interval 600 с со средним порогом 5 событий/с. При наблюденной устойчивой интенсивности 13-20 eps пороговое среднее достигается в пределах одного интервала усреднения. С учетом дискретности накопления счетчиков (шаг ~10 минут между волнами 4-6) расчетная оценка времени реакции в данном прогоне составляет порядка 10-20 минут от устойчивого превышения порога. Это согласуется с тем, что детекция на основе средних/пиковых скоростей за длинные окна сознательно консервативна и устойчива к кратковременным всплескам [4]. Для сценариев, требующих более быстрой реакции, время может быть снижено уменьшением rate-interval ценой роста доли ложных срабатываний (см. 5.3).

5.3. Доля ошибочно отброшенных легитимных запросов (false positive)

Ключевой источник ложных отказов в данной схеме – политика per-client-max 5, которая позволяет ограничить все соединения сверх пяти одновременных с одного IP. Этот эффект был зафиксирован экспериментально на этапе мониторинга: при генерации нагрузки утилитой ab с конкурентностью, превышающей лимит, отклонялся примерно каждый второй-третий запрос с тестового источника. Это дает наблюдаемую оценку доли отказов на уровне ~33–50 % для клиента, превышающего лимит одновременных соединений. Важно подчеркнуть природу этих отказов: они являются ожидаемым следствием политики и относятся к источнику, ведущему себя как агрессивный клиент; для обычного пользователя WebVPN лимит per-client-max 5 не достигается, и прогнозируемая доля ложных отказов близка к нулю.

5.4. Мониторинг средствами Suricata и ограничение доступа

В эксперименте мониторинга правило Suricata фиксировало обращения к WebVPN: при повторной генерации запросов в журнале появлялись соответствующие записи (см. рисунок 5), что подтверждает возможность независимого аудита событий и их последующей обработки. Применимость

Suricata для подобного контроля и ее точность обнаружения исследованы в [12], [13]. Наличие отдельного контура мониторинга важно, как «второе мнение» к встроенной детекции ASA и как источник данных для возможного перехода к интеллектуальному анализу трафика [7], [9].

Также доступ к WebVPN был ограничен списком разрешенных сетей. Такое решение снижает поверхность атаки, так как сервис становится недоступным для внешнего трафика, и является рекомендуемой мерой до установки исправления от производителя [1]. Подход согласуется с принципом минимизации доступной поверхности, описанным в обзорах по межсетевому экранированию [10], [15].

5.5. Дополнительные меры эшелонированной защиты

Полученные результаты показывают, что ни один из исследованных механизмов по отдельности не закрывает рассматриваемый класс угроз полностью. Поведенческая детекция threat-detection эффективно блокирует объемный (flood-подобный) паразитный трафик, но по своей природе срабатывает на превышение порогов интенсивности и потому не реагирует на эксплойт самой уязвимости CVE-2026-20039, который использует точечные низкоинтенсивные специально сформированные запросы. Политики ограничения соединений снижают давление на сервис со стороны одиночного агрессивного источника, но ценой ложных отказов для клиентов, превышающих лимит. Ограничение доступа списком разрешенных сетей радикально снижает поверхность атаки, но применимо только там, где круг легитимных источников заранее известен. Отсюда следует, что защита WebVPN-сервиса должна строиться по принципу эшелонирования (defense in depth), при котором перечисленные меры дополняют друг друга и компенсируют взаимные ограничения [4], [10].

Предлагаемая схема эшелонированной защиты включает следующие уровни. Первый уровень – сокращение поверхности атаки: ограничение доступа

к интерфейсу WebVPN списком разрешенных сетей и отключение неиспользуемых методов доступа, что соответствует принципу минимизации поверхности атаки, закрепленному в отраслевых рекомендациях по межсетевому экранированию [10] и в общих рекомендациях по устойчивости интернет-сервисов к отказу в обслуживании [4]. Второй уровень – детерминированные политики ограничения соединений на уровне per-client, сдерживающие одиночный источник и образующие нижнюю границу устойчивости сервиса даже при отсутствии срабатывания детекции. Третий уровень – поведенческая детекция threat-detection с автоматической блокировкой shun как активный механизм против объемных атак; его пороги (rate-interval, средний и пиковый порог событий) следует настраивать как компромисс между временем реакции и долей ложных срабатываний (см. 5.2, 5.3). Четвертый уровень – независимый контур мониторинга на IDS Suricata, обеспечивающий аудит событий и «второе мнение» к встроенной детекции, а также служащий источником данных для последующего интеллектуального анализа трафика [5], [6].

Отдельно следует подчеркнуть принципиальное ограничение всех сетевых мер применительно к данной уязвимости. Поскольку трафик к WebVPN передается по протоколу HTTPS, сигнатурная фильтрация по содержимому запроса (в том числе по характерному для эксплойта шаблону HTML-сущностей   в теле) на сетевом уровне неосуществима: полезная нагрузка зашифрована, и правила Suricata в данной работе выступают как поведенческий, а не сигнатурный детектор. Поэтому единственной полной мерой устранения уязвимости остается установка исправления производителя; рассмотренные детерминированные политики являются компенсирующими мерами на период до обновления [1]. В качестве перспективного направления развития сетевого обнаружения, не нарушающего конфиденциальность зашифрованного канала, целесообразно рассматривать пассивное снятие отпечатков TLS-клиента (JA3/JA4), позволяющее выделять аномальные клиентские реализации без

расшифровки трафика; экспериментальная проверка этого подхода выходит за рамки настоящей работы и составляет задачу дальнейших исследований.

6. Заключение

В работе сформулирована и экспериментально проверена гипотеза о том, что комбинация политик ограничения соединений и поведенческой детекции threat-detection с автоматической блокировкой обеспечивает нейтрализацию DoS-атаки на WebVPN-сервис Cisco ASA, эксплуатирующей уязвимость CVE-2026-20039, при интенсивности порядка единиц–десятков eps без перезагрузки устройства. Получены количественные метрики срабатывания защиты: блокировка источника наступает при Trigger=5 в 10-минутном окне и Trigger≥1 в часовом окне при накоплении около 1500 событий. Экспериментально зафиксирован эффект ложных отказов, обусловленный политикой per-client-max, и дана его оценка (≈33–50 % для клиента, превышающего лимит одновременных соединений, при близкой к нулю доле для обычного пользователя). Показана работоспособность независимого контура мониторинга на Suricata и эффективность ограничения доступа списком как компенсирующей меры. На основе анализа сильных и слабых сторон отдельных механизмов сформулированы рекомендации по эшелонированной (многоуровневой) защите WebVPN-сервиса, объединяющей сокращение поверхности атаки, детерминированные политики ограничения соединений, поведенческую детекцию с автоматической блокировкой и независимый контур мониторинга. Подчеркнуто, что в силу шифрования трафика по HTTPS сетевая сигнатурная фильтрация эксплойта неосуществима, а полное устранение уязвимости обеспечивается только установкой исправления производителя; перспективным направлением неинтрузивного сетевого обнаружения признано снятие отпечатков TLS-клиента (JA3/JA4).

Литература

1. Cisco Secure Firewall ASA and Secure Firewall Threat Defense Software VPN Web Server Denial of Service Vulnerability (CVE-2026-20039): Cisco Security Advisory cisco-sa-asaftd-vpn-dos-SpOFF2Re. – Cisco Systems, March 2026 [Электронный ресурс]. – URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-SpOFF2Re.
2. Cisco ASA and FTD Software SSL VPN Memory Management Denial of Service Vulnerability: Cisco Security Advisory cisco-sa-asaftd-webvpn-dos-hOnB9pH4. – Cisco Systems, October 2024 [Электронный ресурс]. // Cisco Security Advisory. – URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-dos-hOnB9pH4.
3. Cisco ASA and FTD Software Remote Access VPN Web Server Denial of Service Vulnerability: Cisco Security Advisory cisco-sa-asaftd-vpnwebs-dos-hjBhmBsX. – Cisco Systems, August 2025 [Электронный ресурс]. – URL: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpnwebs-dos-hjBhmBsX.
4. Добкач Л. Я. Анализ методов распознавания компьютерных атак // Вопросы кибербезопасности. – 2020. – С. 67–75. – DOI: 10.21681/1994-1404-2020-1-67-75.
5. Hirakawa T., Ogura K., Bista B. B., Takata T. A Defense Method against Distributed Slow HTTP DoS Attack [Электронный ресурс]. // 2016 19th International Conference on Network-Based Information Systems (NBiS).
6. Tripathi N., Hubballi N., Singh Y. How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection [Электронный ресурс]. // 2016 11th International Conference on Availability, Reliability and Security (ARES).

7. Куликова О. В., Корнилова А. В., Буровских Д. В. Обнаружение веб-атак с использованием машинного обучения // Молодой ученый. – 2023. – № 20. – С. 10–13.
8. Исследование обнаружения DDoS-атак с использованием машинного обучения // Молодой исследователь Дона. – 2022. – № 6.
9. Крыгин Н. Д. DDoS-атаки и защиты от них // Столыпинский вестник. – 2022. – № 4.
10. Косинская А. Р., Демкин Д. А. Межсетевые экраны нового поколения (NGFW): обзор, технологии, представители // Вестник науки. – 2024. – Т. 1, № 7. – С. 516–521.
11. Waleed A., Jamali A. F., Masood A. Which Open-Source IDS? Snort, Suricata or Zeek // Computer Networks. – 2022. – Т. 109116. – DOI: 10.1016/j.comnet.2022.109116.
12. Бондяков А.С. Основные режимы работы системы предотвращения вторжений (IDS/IPS Suricata) для вычислительного кластера // Современные информационные технологии и ИТ-образование. – 2017. – № 3. – С. 31–37.
13. Саматов М.А. АНАЛИЗ ЭФФЕКТИВНОСТИ IDS/IPS-СИСТЕМ НА БАЗЕ SURICATA В ОБЕСПЕЧЕНИИ СЕТЕВОЙ КИБЕРБЕЗОПАСНОСТИ // Вестник науки. – 2024. – № 12. – С. 1352–1363.
14. Muraleedharan N., Janet B. Behaviour Analysis of HTTP Based Slow Denial of Service Attack [Электронный ресурс]. // 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).
15. Scarfone K., Hoffman P. Guidelines on Firewalls and Firewall Policy: NIST Special Publication 800-41, Revision 1. – Gaithersburg, MD: National Institute of Standards and Technology, 2009. – DOI: 10.6028/NIST.SP.800-41r1.
16. Крибель А.М., Перов Р.А., Лаута О.С., Сычужников В.Б. МЕТОДИКА ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК С ПОМОЩЬЮ ФРАКТАЛЬНОГО АНАЛИЗА И МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ //

Известия Тульского государственного университета. Технические науки. – 2022. – № 5. – С. 166–178.