УТВЕРЖДЕН
ПФНА.501540.001 31-ЛУ

ШЛЮЗ БЕЗОПАСНОСТИ

WAF Dallas Lock

(версия изделия 1.15.24)

Описание применения

ПФНА.501540.001 31

Аннотация

Данный документ выполнен в соответствии с ГОСТ 19.502-78 и распространяется на изделие «Шлюз безопасности web application firewall (WAF) «Dallas Lock» ПФНА.501540.001 (далее по тексту – изделие, шлюз безопасности WAF Dallas Lock, WAF DL).

В настоящем документе содержатся общие сведения о назначении изделия и программного обеспечения изделия (далее по тексту — ПО изделия), условиях применения, описание задачи, перечень входных и выходных данных.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

WAF	Web Application Firewall
SIEM	Security information and event management
DMZ	(Demilitarized Zone) демилитаризованная зона
LAN	(Local area network) локальная вычислительная сеть
WAN	(Wide Area Network) глобальная компьютерная сеть
ЕЦУ	Единый центр управления «Dallas Lock»
ИБ	информационная безопасность
МЭ	межсетевой экран
НСД	несанкционированный доступ
ОО	объект оценки
ПО	программное обеспечение
СОВ	средство обнаружения вторжений
ФБО	функциональная возможность безопасности ОО

1 НАЗНАЧЕНИЕ

Изделие предназначено для защиты уровня логических границ сети, защиты веб-сервера и реализации системы обнаружения вторжений при работе в многопользовательских автоматизированных системах, информационных системах персональных данных, автоматизированных системах управления производственными и технологическими процессами, государственных информационных системах, при защите значимых объектов критической информационной инфраструктуры. Изделие выполняет функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков и может использоваться в целях обеспечения защиты (некриптографическими методами) информации ограниченного доступа, а также функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях кражи, уничтожения, искажения и блокирования доступа к ней.

WAF Dallas Lock нацелено на защиту веб-серверов, расположенных в демилитаризованной зоне (DMZ), и сетевой инфраструктуры (LAN) от угроз, исходящих из глобальной сети Интернет (WAN) (рисунок 1).

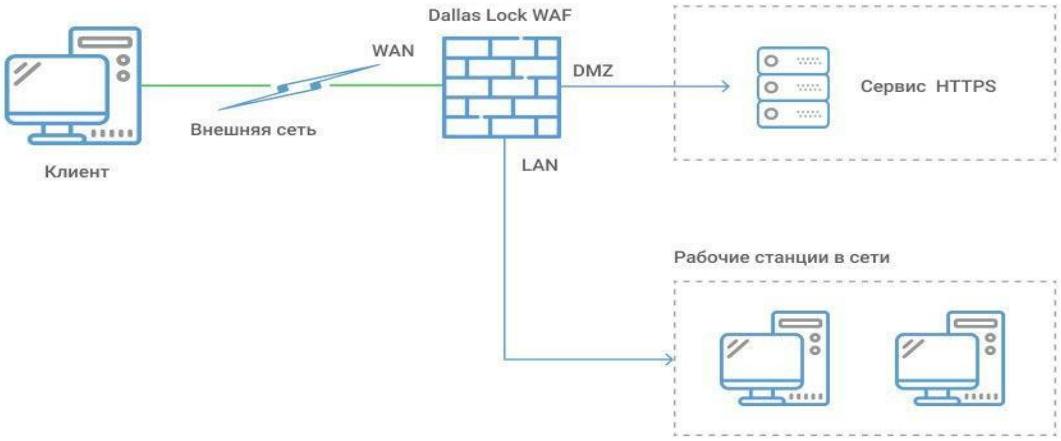

Рисунок 1. Типовая схема использования «WAF Dallas Lock»

2 УСЛОВИЯ ПРИМЕНЕНИЯ

Изделие устанавливается на серверные платформы, работающие на базе процессорной архитектуры семейства x86_64, с характеристиками:

- объем оперативной памяти должен составлять не менее 8 ГБ, предпочтительно 16 ГБ;
- количество ядер процессора должно быть не менее 4 с частотой 2 ГГц;
- объем памяти накопителя должен составлять не менее 32 ГБ, предпочтительно 1 ТБ;
- количество сетевых карт должно быть не менее трех (LAN, WAN, DMZ);
- должно обеспечиваться наличие режима совместимости (MBR) в BIOS.

Для работы с графическим интерфейсом пользователя на рабочее место должен быть установлен один из следующих браузеров:

- Google Chrome 113 и выше;
- Mozilla Firefox 113 и выше;
- Yandex 14 и выше;
- Microsoft Edge 104 выше.

Изделие может использоваться в виртуальной среде. В качестве средств виртуализации поддерживаются:

- VMware;
- Hyper-V;
- VirtualBox.

Требования к сетевым интерфейсам аппаратной платформы:

- количество портов подключения RJ45 должно быть не менее 2 со скоростью передачи данных не менее 1 Гб/с;
- количество портов подключения SFP+ должно быть не менее 2 со скоростью передачи данных не менее 10 Гб/с.

Изделие соответствует требованиям методических документов (требования безопасности информации ФСТЭК России):

- «Требования к системам обнаружения вторжений» (документ утвержден приказом ФСТЭК России № 638 от 6 декабря 2011 г.) — по 4 классу защиты;
- «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ;
- «Требования к межсетевым экранам» (документ утвержден приказом ФСТЭК России № 9 от 9 февраля 2016 г.) — по 4 классу защиты;
- «Профиль защиты межсетевых экранов типа «Б» четвертого класса защиты» ИТ.МЭ.Б4.ПЗ.
- «Профиль защиты межсетевых экранов типа «Г» четвертого класса защиты» ИТ.МЭ.Г4.ПЗ.
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утвержден приказом ФСТЭК России № 76 от 2 июня 2020 г.) — по 4 уровню доверия.

При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (ПФНА.501540.001 ФО), изделие может быть использовано в:

- защищенных автоматизированных системах до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- защищенных государственных информационных системах до 1 класса защищенности включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»);
- защищенных информационных системах персональных данных до 1 уровня защищенности персональных данных включительно (Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»);
- защищенных автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных

объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);

- защищенных значимых объектах критической информационной инфраструктуры до 1 категории значимости включительно (Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

3 ОПИСАНИЕ ЗАДАЧИ

Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» ПФНА.501540.001 ТУ.

Изделие включает в себя следующие функциональные модули:

- WAF, представляющий собой межсетевой экран уровня веб-сервера;
- UTM, представляющий собой межсетевой экран уровня логических границ сети и систему обнаружения вторжений уровня сети (СОВ).

Функциональный модуль WAF (ИТ.МЭ.Г4.ПЗ)

1. В изделии реализована поддержка различных версий протокола передачи гипертекста, различных кодировок текста и cookies.
2. В изделии реализована функциональная возможность оповещения уполномоченных лиц о событиях безопасности, связанных с обнаружением неразрешенных информационных потоков по протоколу передачи гипертекста, а также при обнаружении критичных событий безопасности, по электронной почте и предупреждением через графический интерфейс управления.
3. В изделии реализована поддержка различных версий протокола передачи гипертекста, различных кодировок текста и cookies, подвергшихся фрагментированию и/или сжатию путем реализации анализа сжатых данных по алгоритму Deflate.
4. В изделии реализовано обеспечение конфиденциальности данных пользователя при их передаче по внешнему каналу между изделием и другим доверенным продуктом ИТ путем реализации проприетарного протокола.
5. В изделии реализована функциональная возможность блокировки неразрешенного информационного потока по протоколу передачи гипертекста путем применения правил межсетевого экрана.
6. В изделии реализована виртуализация внешнего представления приложений веб-сервера на уровне трансляции сетевых портов, трансляции унифицированных идентификаторов ресурсов и виртуализации уровня сетевого адреса (порта), а также трансляции уровня URL.
7. В изделии реализован доверенный маршрут к пользователю защищаемых ресурсов, который логически отличим от других маршрутов связи и обеспечивает идентификацию его конечных сторон, а также защиту передаваемых данных от модификации или раскрытия, или других типов нарушения целостности или конфиденциальности путем применения протокола SSL.
8. В изделии реализовано ведение журналов изменений в системе, инцидентов, авторизации WAF.
9. ФБО способны к осуществлению выбора совокупности событий, подвергающихся аудиту, из совокупности событий, в отношении которых возможно осуществление аудита, базируясь на следующих атрибутах: идентификатор объекта, идентификатор пользователя, идентификатор субъекта, тип события.
10. ФБО изделия обеспечивают распространение фильтрации на все операции перемещения через МЭ информации к веб-серверу и от веб-сервера.
11. ФБО изделия осуществляют фильтрацию, основанную на типах атрибутов безопасности для субъектов и типов информации, находящихся под управлением политики.
12. ФБО изделия явно разрешают информационный поток, основываясь на устанавливаемом администратором ОО наборе правил фильтрации.
13. ФБО изделия явно запрещают информационный поток, основываясь на устанавливаемом администратором ОО наборе правил фильтрации или в случае обнаружения запроса пользователя к сайту и (или) иному веб-приложению на ввод данных, содержащих мобильный код.
14. ФБО изделия разрешают информационный поток между управляемым субъектом и управляемой информацией посредством управляемой операции, если выполняются следующие правила: значения атрибутов индикации наличия признаков нарушения безопасности в информации сетевого трафика указывают на отсутствие нарушений.
15. ФБО изделия осуществляют дополнительные правила политики управления информационными потоками.
16. ФБО изделия поддерживают контроль и анализ сообщений, отправляемых веб-браузером веб-серверу и содержащих текстовый контент и нетекстовый контент: изображения, видеоинформацию.
17. ФБО изделия для осуществления фильтрации предоставляют возможность модифицировать, удалять, создавать атрибуты безопасности только администраторам МЭ.
18. ФБО изделия для осуществления фильтрации предоставляют возможность модифицировать, удалять атрибуты безопасности для информации по протоколу передачи гипертекста

администраторам МЭ.

19. ФБО изделия предоставляют канал связи между собой и веб-сервером, который логически отличим от других каналов связи и обеспечивает уверенную идентификацию его конечных сторон, а также защиту данных канала от модификации или раскрытия.
20. ФБО изделия обеспечивают возможность отключения примененной блокировки информационных потоков.
21. ФБО изделия осуществляют блокирование всех информационных потоков, проходящих через МЭ, основанное на атрибутах, указывающих на нарушение функционирования МЭ.
22. ФБО изделия осуществляют проверку каждого пакета по таблице состояний для определения того, не противоречит ли состояние (статус, тип) пакета ожидаемому состоянию.
23. ФБО изделия обеспечивают конфиденциальность данных ФБО, в частности сетевого адреса МЭ, при передаче данных пользователя из МЭ путем не включения данных ФБО в состав передаваемой информации.
24. В изделии реализована возможность расширенной настройки для протоколов WebSockets, HTTP/2.0, TLS.
25. В изделии реализована защита от атак типа DoS/DDoS 7 уровня сетевой модели OSI.

Функциональный модуль UTM (ИТ.МЭ.Б4.ПЗ, ИТ.СОВ.С4.ПЗ.)

1. В изделии реализовано управление событиями безопасности, в том числе:
   - оповещение о событиях безопасности (НСД);
   - аудит и регистрация событий безопасности;
   - генерация событий безопасности (НСД);
   - возможность автоматического объединения событий аудита в событие НСД (события безопасности), предустановленные шаблоны НСД, возможность настройки событий НСД;
   - реализация возможности оповещения администратора при обнаружении критических событий безопасности (сбои, события НСД) через электронную почту и предупреждением через графический интерфейс управления.
2. В изделии реализован контроль доступа на просмотр журналов ИБ в виде возможности администратору МЭ или другому уполномоченному пользователю предоставления полной информации аудита через графический интерфейс.
3. В изделии реализована функциональная возможность предоставления администраторам СОВ модификации режима выполнения и изменения данных функциональных возможностей СОВ.
4. В изделии реализованы отдельные роли для ФБО СОВ.
5. В изделии реализована функциональная возможность тестирования и самотестирования СОВ.
6. В изделии реализован сбор, регистрация и анализ данных СОВ в части реализации обеспечения сбора данных о сетевом трафике, а также информации, связанной с трафиком — даты и времени события, типа события, идентификатора субъекта.
7. В изделии реализован эвристический анализ информационного потока путем применения действий как реакции на группу (последовательность) событий.
8. В изделии реализована функциональная возможность реакции СОВ при обнаружении вторжения (пропускание информационного потока, журналирование, блокирование информационного потока).
9. В изделии реализованы механизмы обнаружения вторжений на основе анализа служебной информации (проверки на нарушение целостности пакетов) протокола сетевого уровня (минимально), а также других уровней базовой эталонной модели взаимосвязи открытых систем.
10. В изделии реализован механизм удаленного администрирования СОВ (управление через веб-интерфейс по протоколу HTTPS).
11. В изделии реализовано автоматизированное обновление базы решающих правил путем получения новых сигнатур с сервера, расположенного в сети Интернет, вручную или с задаваемой периодичностью, только для администраторов.
12. В изделии реализован графический интерфейс администрирования СОВ.
13. В изделии реализована инспекция SSL/TLS на границе сети, анализ экспортируемого из сети и импортируемого в сеть трафика.
14. В изделии реализовано наличие сигнатур или наличие не сигнатурных механизмов защиты от перечисленных угроз из списка OWASP TOP 10.
15. ФБО изделия регистрируют в каждой записи аудита, по меньшей мере, следующую информацию:
    - чтение информации из записей аудита;
    - неуспешные попытки читать информацию из записей аудита;
    - все модификации режима выполнения функций, связанных со сбором данных о системе ИТ, их анализом и ответными реакциями;

- все модификации данных СОВ, данных аудита и всех прочих данных ОО;
- модификация группы пользователей — исполнителей роли;
- изменения внутреннего представления времени;
- выполнение и результаты самотестирования компонентов СОВ.

16. ФБО изделия способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

17. ФБО изделия предоставляют возможность изменения значений по умолчанию, модификации, удаления, очистки настроек и журналов ИТ только уполномоченным администраторам безопасности.

18. ФБО изделия предпринимают следующие действия при достижении или превышении данными ФБО установленных выше ограничений: блокировка сущности субъекта, инициировавшего превышение ограничений.

19. ФБО изделия имеют механизмы локального администрирования СОВ.

20. ФБО изделия осуществляют фильтрацию, основанную на следующих типах атрибутов безопасности субъектов: отправитель, получатель — сетевой адрес; ОО — интерфейс ОО.

21. ФБО изделия разрешают информационный поток между управляемым субъектом и управляемой информацией посредством управляемой операции.

22. ФБО изделия осуществляют блокирование всех информационных потоков, проходящих через МЭ, основанное на атрибутах, указывающих на нарушение функционирования МЭ.

23. ФБО изделия осуществляют посредничество в передаче, фильтрацию, передачу информационных потоков с переназначением сетевых адресов отправителя и получателя при экспорте информации сетевого трафика за пределы МЭ.

24. ФБО изделия предоставляют возможность изменения значений по умолчанию, запроса, модификации, удаления, очистки, списка данных ФБО только уполномоченным идентифицированным ролям.

25. ФБО изделия предоставляют возможность определять режим выполнения, отключать, подключать, модифицировать режим выполнения функций ОО только уполномоченным идентифицированным ролям.

26. В изделии реализована функциональная возможность интеграции со сторонними сервисами для автоматической блокировки запросов к защищаемому ресурсу.

Общие подсистемы изделия

1. В изделии реализован аудит и регистрация событий безопасности модуля СОВ, а также управление событиями безопасности, в том числе:

- оповещение о событиях безопасности (НСД);
- аудит и регистрация событий безопасности;
- генерация событий безопасности (НСД);
- возможность автоматического объединения событий аудита в событие НСД (события безопасности);
- предустановленные шаблоны НСД;
- возможность настройки событий НСД.

2. В изделии реализован контроль доступа к журналам СОВ.

3. В изделии реализовано управление журналами МЭ в части настройки визуального отображения журналов регистрации событий, а также поиска, фильтрации и сортировки.

4. В изделии реализован импорт собственных архивных журналов аудита.

5. В изделии реализована возможность поиска, сортировки и фильтрации событий в журналах аудита.

6. В изделии реализована фильтрация сетевого трафика NAT.

7. В изделии идентификация и аутентификация пользователей проводится до момента получения возможности реализовывать какие-либо действия с МЭ.

8. В изделии реализованы роли безопасности (уполномоченные идентифицированные роли) и ассоциации ролей безопасности.

9. В изделии реализованы значения по умолчанию для атрибутов безопасности (как возможность присвоения атрибутам безопасности объектов значений по умолчанию, так и сброс настроек).

10. В изделии реализовано ведение и отображение таблицы состояния, а также обеспечение присвоения информации состояния соединения только допустимых значений.

11. В изделии реализованы прокси-агенты для каждого типа трафика в части реализации возможности поддержки списка типов сетевого трафика для осуществления посредничества в передаче, предусматривающего разделение трафика по типам в виде сигнатур по портам и типам трафика.

12. В изделии реализован аварийный режим МЭ в виде возможности перехода изделия в режим аварийной поддержки, который предоставляет возможность возврата МЭ к штатному режиму функционирования.

13. В изделии реализована возможность получения надежных меток времени от внешних доверенных источников при проведении аудита.

14. В изделии реализована возможность тестирования (самотестирования) функциональных требований безопасности, а также контроль целостности исполняемого кода изделия, в виде проведения процедуры контроля целостности.

15. В изделии реализовано обеспечение работоспособности отдельных функциональных возможностей и сохранения полной работоспособности после наступления сбоя, в виде перезагрузки и проведения процедуры контроля целостности.

16. В изделии реализована возможность согласованно интерпретировать управляющие команды, атрибуты сетевого трафика и иные данные, получаемые от взаимодействующих с МЭ средств защиты информации, а также поддержка правил интерпретации данных, получаемых от взаимодействующих с МЭ средств защиты информации, в частности, с Единым Центром Управления (ЕЦУ) «Dallas Lock».

17. В изделии реализовано качество обслуживания (QoS) в виде реализации приоритезации и фильтрации информационных потоков на основе установленных приоритетов и значений заданной функции.

18. В изделии реализовано управление через командную строку.

19. В изделии реализованы шаблоны настроек безопасности для узлов и популярного ПО. Реализована возможность быстро настроить набор сигнатур для защищаемых узлов при использовании профилирования сигнатур. Сигнатуры могут использовать как встроенное профилирование по типам сигнатур, так и дополнительное категорирование, которое активирует актуальный набор сигнатур блоком настроек (активацией шаблонов) для защищаемых узлов.

20. В изделии реализованы построения отчетов по результатам срабатывания сигнатур на конкретном узле с иконографикой, и возможность просмотра этих отчетов.

21. В изделии реализована идентификация пользователя в сценариях, с отслеживанием стандартного поведения пользователя на сайте, и возможность детектирования аномального поведения на сайте (simple UBA).

22. В изделии реализована возможность централизованного управления в составе домена безопасности в качестве клиента ЕЦУ. Централизованное управление обеспечивается в части:

- регистрации в домене безопасности ЕЦУ и синхронизации;
- отображения состояния и информации о клиенте в консоли управления ЕЦУ;
- оперативного управления;
- получения информации о событиях безопасности;
- передачи журналов с клиента в ЕЦУ;
- формирования заданий для клиента через консоль управления ЕЦУ;
- настройки инцидентов безопасности.
- В изделии реализована функциональная возможность кластеризации WAF Dallas Lock для обеспечения:
- отказоустойчивости;
- миграции конфигураций между несколькими экземплярами WAF Dallas Lock.

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входные данные

Входными данными являются:

- файлы конфигураций модулей WAF DL, используемые при установке;
- логин и пароль, уникальные для каждого администратора;
- шаблоны правил обработки трафика;
- идентификационные данные пользователей защищаемых ресурсов;
- идентификационные данные защищаемых ресурсов;
- сетевой трафик уровня приложения (для СОВ, WAF);
- сетевой трафик сетевого и транспортного уровня (для МЭ, СОВ);
- установленные соединения (для МЭ, СОВ);
- события, регистрируемые в журналах аудита.

Выходные данные

Выходными данными являются:

- сообщения WAF DL на действия пользователей в сети и на защищаемых ресурсах;
- журналы событий, создаваемые WAF DL в процессе работы;
- значения контрольных сумм объектов, на которых установлен контроль целостности, и исполняемых файлов;
- резервные копии программных компонентов WAF DL;
- файлы конфигураций модулей WAF DL;
- отчеты по результатам автоматического тестирования функционала;
- сообщения WAF DL в случае сигнализации при попытках несанкционированного доступа.