**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Петербургский государственный университет путей сообщения**

**Императора Александра I»**

**(ФГБОУ ВО ПГУПС)**

Факультет «Автоматизация и интеллектуальные технологии»

Кафедра «Информатика и информационная безопасность»

Лабораторная работа № 2

по дисциплине

«Подтверждение соответствия, сертификация, анализ безопасности программного обеспечения»

на тему: «Разработка программы и методики испытаний межсетевого экрана по требованиям безопасности информации»

|  |  |  |
| --- | --- | --- |
| **Выполнил**  **обучающийся**  Курс 5  Группа КИБ-012 | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | Г.Е. Груздев |
|  |  |  |
| **Проверил** | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись, дата | С.В. Корниенко |

Санкт-Петербург

|  |  |
| --- | --- |
| **УТВЕРЖДЕНО** | **СОГЛАСОВАНО** |
| Генеральный директор  АО «НПО «Эшелон»  (подпись) И.И. Иванов  12.12.2024 | Глава отдела разработки  ОАО «Компания»  (подпись) П.П. Петров  12.12.2024 |

ОАО «Лаборатория ППШ»

Межсетевой экран «PfSense»

ЛИСТ УТВЕРЖДЕНИЯ

Программа и методика испытаний

643.1037804000563.001001.00001-01 51 01-ЛУ

Листов 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | |  | **СОГЛАСОВАНО:** | |  | Генеральный директор  ОАО «Лаборатория ППШ»  (подпись) Попов А.А  12.12.2024 | |  |

Санкт-Петербург

2024

УТВЕРЖДЕНО

643.1037804000563.001001.00001-01 51 01-ЛУ

ОАО «Лаборатория ППШ»

Межсетевой экран «PfSense»

ПРОГРАММА И МЕТОДИКА ИСПЫТАНИЙ

643.1037804000563.001001.00001-01 51 01

Листов 12

Санкт-Петербург

2024

**Оглавление**

[1. Объект испытаний 1](#_Toc152698950)

[2. Цель испытаний 2](#_Toc152698951)

[3. Требования к программе 3](#_Toc152698952)

[4. Требования к программной документации 4](#_Toc152698953)

[5. Состав и порядок испытаний 5](#_Toc152698954)

[6. Методы испытаний 7](#_Toc152698955)

[Лист регистрации изменений 12](#_Toc152698956)

1. Объект испытаний

Наименование испытуемой программы: 643.1037804000563.001001.00001 межсетевой экран PfSense .

Программный комплекс межсетевого экрана (далее ПК МЭ) PfSense предназначен для контроля информационных потоков и защиты локальной сети от внешних угроз с использованием сетевого фильтра. Фильтрация осуществляется на основе множества характеристик сетевых протоколов. Программа проводит алгоритмическую обработку и анализ данных в соответствии с заданными настройками, принимая индивидуальные решения для каждого сетевого пакета. Все операции с пакетами фиксируются в системном журнале, расположенном в **/var/log/filter.log**.

**Область применения испытуемой программы:**

Программный комплекс PfSense используется для обеспечения информационной безопасности в корпоративных и частных локальных сетях. Основное назначение — защита от несанкционированного доступа, сетевых атак и вредоносных действий в реальном времени. PfSense может быть эффективно применён в организациях с различными требованиями к уровню безопасности сетей, включая малый и средний бизнес, государственные учреждения и крупные корпоративные сети.

ПК МЭ PfSense включает собственную операционную систему на базе FreeBSD 14, и не требует предустановки какого-либо программного обеспечения.

Обозначение испытуемой программы: 643.1037804000563. 001001.00001

1. Цель испытаний

Целью сертификационных испытаний является определение соответствия программного изделия требованиям для межсетевого экрана (МЭ) по 4 классу защищенности, изложенным в руководящем документе ФСТЭК «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 25 июля 1997 года.

1. Требования к программе

Для межсетевого экрана должны быть реализованы следующие функциональные возможности:

* межсетевое экранирование — пакетная фильтрация сетевого трафика до 4-го уровня модели OSI включительно;

**- IP-фильтрация:** фильтрация на основе IP-адресов, сетевых масок, источников и получателей.

**- TCP/UDP-портовая фильтрация:** контроль доступа к определенным портам на основе TCP и UDP.

**- ICMP:** управление доступом к ICMP-пакетам для ограничения работы сетевых утилит вроде ping.

**- IPv4/IPv6:** поддержка обоих версий IP протокола для совместимости с различными сетями.

* контроль приложений — определение используемых приложений независимо от используемого сетевого порта;

**- DPI (Deep Packet Inspection):** глубокий анализ пакетов для идентификации приложений вне зависимости от порта.

**- Протоколы уровня приложения:** такие как HTTP, HTTPS, DNS, FTP, SMTP, POP3 и другие, для более точной фильтрации на основе типов приложений и служб.

**- Application Layer Gateways (ALG):** позволяет межсетевому экрану "понимать" специфичные для приложений протоколы, такие как SIP или FTP, что упрощает их контроль.

* контентная фильтрация — анализ посещаемых пользователем интернет-страниц (URL) с целью предотвращения доступа к запрещенным или вредоносным ресурсам;

- **URL-фильтрация:** контроль доступа к веб-ресурсам с использованием баз данных запрещённых сайтов (URL Blacklist).

**- HTTP/HTTPS фильтрация:** анализ заголовков и содержимого запросов в HTTP и HTTPS для предотвращения доступа к нежелательным сайтам.

**- SNI (Server Name Indication) фильтрация:** позволяет блокировать сайты на основе имени сервера, даже если соединение зашифровано

* анализ сетевого трафика на предмет вторжений — сигнатурный анализ сетевого трафика с целью обнаружения активности вредоносов или попыток эксплуатации уязвимостей программного обеспечения;

**- IDS/IPS системы:** использует сигнатурный и аномальный анализ для выявления угроз, таких как Snort или Suricata.

**- Сигнатуры и базы данных угроз:** база данных известных сигнатур атак, таких как SQL-инъекции, DDoS, brute force, и других типов атак.

**- Протоколы уровня приложения и транспортного уровня:** контроль специфических протоколов (HTTP, FTP, DNS) для обнаружения и предотвращения попыток эксплуатации уязвимостей.

* аутентификация пользователей — аутентификация пользователей при сетевом доступе в интернет;

**- LDAP (Lightweight Directory Access Protocol):** для интеграции с корпоративными базами пользователей.

**- Kerberos:** безопасный протокол аутентификации, часто используемый в корпоративных сетях.

**- SAML/OAuth/OpenID Connect:** для реализации единого входа (SSO) и аутентификации пользователей.

* антивирусная проверка передаваемых файлов — сигнатурный анализ передаваемых файлов на предмет вредоносных программ;

**- HTTP/HTTPS/FTP сканирование:** проверка загружаемых файлов при помощи прокси и DPI для обнаружения вредоносного кода.

**- Сигнатурные антивирусные движки:** использование известных сигнатур вирусов для анализа содержимого файлов (например, ClamAV, Kaspersky).

**- ICAP (Internet Content Adaptation Protocol):** протокол, который позволяет интеграцию межсетевого экрана с антивирусными системами для сканирования контент

* встроенный почтовый сервер — сконфигурированный и настроенный корпоративный почтовый сервер;

**- SMTP (Simple Mail Transfer Protocol):** для отправки электронной почты.

**- POP3/IMAP:** для получения и управления электронной почтой.

**- SPF, DKIM, DMARC:** для защиты от спама и фальсификации исходных адресов.

**- Антивирусная и антиспам проверка:** фильтрация писем на наличие спама и вредоносных вложений.

* встроенный VPN-сервер — обеспечение возможности подключения удаленных пользователей к корпоративной сети.

**- IPSec (Internet Protocol Security):** защищенный протокол для туннелирования данных между удалёнными узлами.

**- SSL/TLS VPN (Secure Sockets Layer/Transport Layer Security):** шифрование для защиты данных на уровне транспортного слоя.

**- L2TP (Layer 2 Tunneling Protocol) с IPSec:** для туннелирования на втором уровне с дополнительной защитой IPSec.

**- OpenVPN:** широко используемый VPN-протокол с поддержкой SSL/TLS для шифрования трафика.

1. Требования к программной документации

Состав программной документации должен включать в себя:

1. Руководство администратора МЭ:

* Межсетевой экран PfSense. Руководство администратора 643.1037804000563.001001.00001-01 91 01.

2. Тестовая документация:

* Межсетевой экран PfSense. Программа и методика испытаний по передаче в опытную эксплуатацию МЭ PfSense 643.1037804000563.001001.00001-01 51 02.
* Межсетевой экран PfSense. Протокол тестовых испытаний 643.1037804000563.001001.00001-01 92 02.

3. Конструкторская документация:

* Техническое задание на разработку СЗИ PfSense 643.1037804000563.001001.00001-01 90 01.

1. Состав и порядок испытаний

Место проведения испытаний: АО «Лаборатория ППШ»

(Российская Федерация, Санкт-Петербург, наб. реки Смоленки, 25Е, телефон 8 (812) 555-5555).

Период проведения испытаний: с 12.11.2024 по 13.12.2024.

**5.1 Технические и программные средства, используемые во время испытаний**

Для проведения испытаний необходимо собрать стенд (рис.1), имитирующий 2 сегмента сети (внешний и внутренний).

В состав внутреннего сегмента сети входят:

• 2 пользовательских узла (компьютер 1 и 2);

• Коммутатор (Switch);

• Узел администратора (компьютер 3) с установленным МЭ.

В состав внешнего сегмента сети входит:

• Компьютер 4;

• Маршрутизатор (Router).

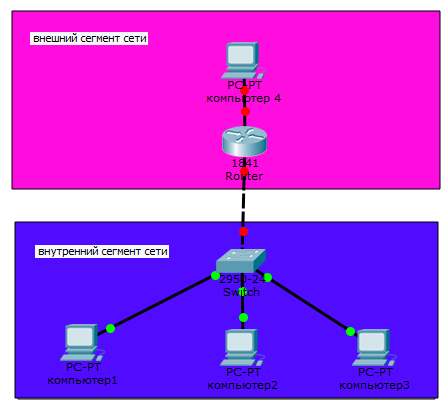


Рисунок 1 - Структурная схема стенда

Требования к техническим характеристикам рабочих станций:

СВТ должны удовлетворять следующим характеристикам:

- процессор - 64-битный amd64 (x86-64) совместимый CPU;

- оперативной памяти — 1 Гб или больше;

- жесткий диск - 8 Гб или больше, IDE/SATA/SCSI;

- сетевое оборудование - одна или более сетевые карты 10/100/1000 Base-T;

- для установки необходим привод CD-ROM (IDE/SATA/SCSI/USB).

Используемые технические средства:

Для компьютеров 1, 2, 4:

- процессор: AMD Ryzen 5 3500 OEM, 6 x 3.6 ГГц

- оперативная память: Kingston FURY Beast Black

- SATA накопитель: 240 ГБ 2.5" SATA накопитель ADATA SU650

- Сетевая карта TP-Link TG-3468

- Материнская плата MSI PRO H610M-E DDR4

Для компьютера 3 (сервера):

- процессор: Intel Xeon Silver 4214 OEM, 12 x 2.2 ГГц

- оперативная память: Kingston FURY Beast Black

- SATA накопитель: 960 ГБ 2.5" SATA накопитель Kingston A400

- Сетевая карта TP-Link TG-3468

- Материнская плата Supermicro X12DPL-i6 ATX LGA 4189

Маршрутизатор (Router):

- модель MikroTik hEX PoE

Коммутатор (Switch):

- модель MikroTik hEX S RB760iGS

**5.2 Программные средства, используемые во время испытаний**

Для проведения испытаний необходимо установить:

* На пользовательские узлы – систему Windows 10.
* На сервер – межсетевой экран;
* Для генерации пакетов – программу Scapy на внешний узел.
* Для анализа трафика – программу Wireshark на сервер.

**5.3 Порядок проведения испытаний**

1. Испытания управления доступом;

2. Испытания процесса регистрации;

3. Испытания процесса администрирования: идентификация и аутентификация;

4. Испытания процесса администрирования: регистрация;

5. Испытания процесса контроля за целостностью;

6. Испытания процедуры восстановления;

7. Испытания регламентного тестирования;

8. Проверка руководства администратора безопасности;

9. Проверка тестовой документации;

10. Проверка конструкторской документации;

1. Методы испытаний

**1) Управление доступом**

* ПК МЭ PfSense должен обеспечивать фильтрацию на сетевом уровне: решение по фильтрации может приниматься независимо для каждого сетевого пакета на основе, по крайней мере, сетевых адресов отправителя и получателя, или на основе других эквивалентных атрибутов.
* ПК МЭ PfSense должен обеспечивать фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.
* ПК МЭ PfSense должен обеспечивать фильтрацию с учетом входного и выходного сетевого интерфейса посредством проверки подлинности сетевых адресов.
* ПК МЭ PfSense должен обеспечивать фильтрацию с учетом любых значимых полей сетевых пакетов.

Для проверки фильтрации на сетевом уровне должна быть проведена проверка фильтрации основных протоколов этого уровня:

• IPv4/IPv6, Internet Protocol;

• IPsec, Internet Protocol Security.

Для проверки фильтрации пакетов служебных протоколов, необходимо проверить работу с пакетами протокола:

• ICMP, Internet Control Message Protocol.

Проверка проводится с помощью последовательной генерации пакетов, указанных выше протоколов и отправкой их с компьютера 4 с помощью утилиты Scapy во внутренний сегмент сети (компьютеры 1, 2, 3) при предварительной настройке запрета трафика с данного удаленного узла (пакеты не должны проходить в сеть) и при разрешении трафика с данного узла (пакеты должны свободно доходить до адресатов).

Результат испытания считается положительным, если при запрете трафика с данного узла пакеты фильтруются верно и отбрасываются, а при разрешении трафика с данного узла пакеты свободно доходят до адресатов.

**2) Регистрация**

ПК МЭ PfSense должен обеспечивать возможность регистрации и учета фильтруемых пакетов, при этом в параметры регистрации должны включаться адрес, время и результат фильтрации.

Проверка проводится с помощью просмотра результатов фильтрации пакетов из испытания прошлого пункта в «Журнале событий» во вкладке «Брандмауэр» и «Журнале пакетов». Для доступа к журналу событий необходимо предварительно включить режим аудита.

Результат испытания считать положительным, если в журнале событий МЭ и «Журнале пакетов» верно отображаются информация о всех фильтруемых пакетах.

**3) Администрирование: идентификация и аутентификация**

ПК МЭ PfSense должен обеспечивать идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ.

ПК МЭ PfSense должен обеспечивать возможность идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.

Результат испытания считать положительным, если при запуске программы требуется ввод учётных данных администратора (логина и пароля), а также при изменении настроек параметров программы система требует повторный ввод пароля администратора.

**4) Администрирование: регистрация**

ПК МЭ PfSense должен обеспечивать регистрацию входа (выхода) администратора ПК МЭ Ideco ICS 3, либо загрузки и инициализации системы и ее программного останова. Регистрация выхода не проводится в моменты аппаратурного отключения ПК МЭ PfSense;

В параметрах регистрации должны указываться:

* дата, время и код регистрируемого события;
* результат попытки осуществления регистрируемого события - успешная или неуспешная;
* идентификатор администратора ПК МЭ PfSense, предъявленный при попытке осуществления регистрируемого события.

ПК МЭ PfSense должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

Проверка проводится с помощью просмотра данных о запуске программы и статусе её компонентов в «Журнале событий» во вкладке «Внутренние события». Для доступа к журналу событий необходимо предварительно включить режим аудита.

Результат испытания считать положительным, если в журнале «Внутренние события» верно отображается информация о входах администратора в систему и запусках программы.

**5) Целостность**

ПК МЭ PfSense должен содержать средства контроля целостности своей программной и информационной части.

Проверка производится путем проверки наличия модуля контроля целостности в составе программы, путем изучения технической документации и проверки функциональности.

Результат испытания считать положительным, если программа содержит модуль контроля целостности.

**6) Восстановление**

ПК МЭ PfSense должен предусматривать процедуру восстановления после сбоев и отказов оборудования, обеспечивая тем самым восстановление своих свойств.

Проверка проводится аварийным завершением работы системы с последующим её перезапуском.

Результат испытания считать положительным, если МЭ предусматривает процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.

**7) Тестирование**

ПК МЭ PfSense должен обеспечивать возможность регламентного тестирования:

* реализации правил фильтрации;
* процесса идентификации и аутентификации администратора ПК МЭ PfSense;
* процесса регистрации действий администратора ПК МЭ PfSense;
* процесса контроля за целостностью программной и информационной части ПК МЭ PfSense;
* процедуры восстановления;
* процесса регистрации.

Результат испытания считать положительным, если были получены успешные результаты испытаний вышеперечисленных пунктов.

**8) Руководство администратора безопасности**

Производится визуальный контроль документа.

Состав руководства администратора безопасности:

* Руководство по эксплуатации СЗИ PfSense 643.1037804000563.001001.00001-01 91 01.

Документ должен содержать:

* описание контролируемых функций ПК МЭ PfSense;
* руководство по настройке и конфигурированию ПК МЭ PfSense;
* описание старта ПК МЭ PfSense и процедур проверки правильности старта;
* руководство по процедуре восстановления.

Результат испытания считать положительным, если руководство администратора МЭ содержит вышеперечисленные пункты.

**9) Тестовая документация**

Производится визуальный контроль документов.

Состав тестовой документации:

* Межсетевой экран PfSense. Программа и методика испытаний по передаче в опытную эксплуатацию МЭ PfSense 643.1037804000563.001001.00001-01 51 02.
* Межсетевой экран PfSense. Протокол тестовых испытаний 643.1037804000563.001001.00001-01 92 02.

Результат испытания считать положительным, если тестовая документация содержит описание тестов и испытаний, которым подвергался ПК МЭ PfSense, и их результаты.

**10) Конструкторская (проектная) документация**

Производится визуальный контроль документа.

Состав конструкторской документации:

* Техническое задание на разработку СЗИ PfSense (PfSense) 643.1037804000563.001001.00001-01 90 01.

Документация должна содержать:

* общую схему ПК МЭ PfSense;
* общее описание принципов работы ПК МЭ PfSense;
* описание правил фильтрации;
* описание средств и процесса идентификации и аутентификации;
* описание средств и процесса регистрации;
* описание средств и процесса контроля за целостностью программной и информационной части ПК МЭ PfSense;
* описание процедуры восстановления свойств ПК МЭ PfSense.

Результат испытания считать положительным, если конструкторская документация содержит вышеперечисленные пункты.

**7 ИНТЕГРАЛЬНАЯ ОЦЕНКА ИСПЫТАНИЙ**

После проведения испытаний, требуется составить протокол об их проведении с указанием полученных результатов:

|  |  |
| --- | --- |
| Испытание | Результат испытания |
| Управление доступом |  |
| Реализация процесса регистрации |  |
| Реализация процесса администрирования: идентификация и аутентификация |  |
| Реализация процесса администрирования: регистрация |  |
| Реализация процесса контроля за целостностью |  |
| Реализация процедуры восстановления |  |
| Тестирование |  |
| Руководство администратора безопасности |  |
| Тестовая документация |  |
| Конструкторская документация |  |
| Итого |  |

Если по итогам проведенных испытаний все десять проверок имеют положительный результат, то исследуемый межсетевой экран соответствует требованиям руководящего документа «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации» – по 4 классу защищенности информации от несанкционированного доступа.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Заместитель начальника  АО «Лаборатория ППШ» | | | | |  | | | | Волков С.В. | | |
|  | Лист регистрации изменений | | | | | | | | | | |
|  | Номер листов (страниц) | | | | | Всего листов (страниц) | № докум | Входящий номер сопроводит. документа и дата | | Подпись | Дата |
|  | Изм | изменен | заменен | новых | аннулир |
|  | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | 9 | 10 |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |
|  |  |  |  |  |  |  |  |  | |  |  |