УДК 004.056.53

СИСТЕМА ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ FORTIGATE

М.К. До[1], В.К. Фунг[2]

[1] Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

[2]Университет ИТМО, Санкт-Петербург, Россия

Аннотация. В статье представлены результаты исследования функциональности Intrusion Prevention System (IPS) межсетевого экрана FortiGate. Описаны методы выявления угроз и предотвращения их проникновения в сеть. Составлена методика конфигурации IPS-систем и тестирования ее работы.
Ключевые слова: IPS, FortiGate, FortiNet, FortiGuard, NGFW, сигнатура, аномалия, угроза.

FORTIGATE INTRUSION PREVENTION SYSTEM

M.K. Do[1], V.Q. Phung[2]

[1]Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

[2]ITMO University, Saint Petersburg, Russia

Abstract. The article presents the results of the study of the definition of Intrusion Prevention System (IPS) FortiGate firewall. The method of identifying threats and preventing their penetration into the network is shown. The configuration method of IPS systems and its operation testing is compiled.
Keywords: IPS, FortiGate, FortiNet, FortiGuard, NGFW, signature, anomaly, threat.

Введение

В современном мире, где информационные технологии играют ключевую роль в функционировании бизнеса и общества, защита данных и сетевой инфраструктуры становится одной из главных задач. Кибератаки на компьютерные системы становятся все более изощренными, что требует от организаций применения эффективных мер безопасности. Одним из таких решений является система предотвращения вторжений (Intrusion Prevention System, IPS), которая активно используется для защиты сетевых ресурсов. FortiGate – это межсетевой экран для обеспечения безопасности, предоставляемый компанией Fortinet. Он сочетает в себе функции межсетевого экрана, антивируса, системы предотвращения вторжений и др. FortiGate позволяет не только обнаруживать и блокировать угрозы в реальном времени, но и анализировать трафик, предоставляя администратору возможность оперативно реагировать на инциденты.

Основная часть

Система предотвращения вторжений (IPS) обнаруживает сетевые кибератаки и предотвращает угрозы, которые могут нанести ущерб сети, включая защищенные устройства. IPS может быть в виде отдельного устройства или части набора функций межсетевого экрана нового поколения (NGFW), такого как FortiGate [1]. IPS использует сигнатуры, декодеры протоколов, эвристику (или поведенческий мониторинг), аналитику угроз (например, FortiGuard Labs) и расширенное обнаружение угроз для предотвращения эксплуатации известных и неизвестных угроз нулевого дня. FortiGate IPS также выполняет глубокую проверку пакетов для сканирования зашифрованных полезных нагрузок для обнаружения и предотвращения угроз со стороны нарушителей.

Решение FortiNet объединяет ведущую в отрасли аналитику угроз от FortiGuard Labs с FortiGate NGFW для выявления новейших угроз и предотвращения их проникновения в сеть. Сигнатуры IPS являются одним из таких методов предоставления актуальной защиты. FortiGuard Labs использует искусственный интеллект (AI) и машинное обучение (ML) для анализа миллиардов событий каждый день. Исследовательская группа FortiGuard Labs также активно проводит исследования угроз для обнаружения новых уязвимостей и их эксплуатации и создает сигнатуры для выявления таких угроз. Сигнатуры IPS ежедневно обновляются на межсетевых экранах FortiGate.

Датчик FortiGate IPS представляет собой набор сигнатур и фильтров IPS, которые определяют область сканирования движка IPS при применении датчика IPS. Датчик IPS может иметь несколько наборов сигнатур и/или фильтров. Набор сигнатур IPS состоит из выбранных вручную сигнатур, в то время как набор фильтров IPS состоит из фильтров на основе атрибутов сигнатуры, таких как цель, серьезность, протокол, ОС и приложение. Каждая сигнатура имеет предопределенные атрибуты и действия (блокировать, разрешать, карантин и др.). Также можно создавать пользовательские сигнатуры IPS для применения к датчику IPS.

IPS-систем предоставляют следующие возможности:

– обнаружение вторжения или сетевой атаки и их предотвращение;

– выявление возможных кибератак и уязвимостей;

– документирование существующих угроз;

– обеспечение контроля качества безопасности администрирования;

– получение актуальной информации о кибератаках;

– определение расположение источника кибератаки по отношению к локальной сети (внешние или внутренние).

В результате конфигурации IPS-систем на межсетевом экране FortiGate была составлена следующая методика:

1. Подключение к веб-интерфейсу межсетевого экрана FortiGate.
2. Создание датчика IPS.
3. Конфигурация набора сигнатур и фильтров IPS.
4. Активация датчика IPS в политике безопастности межсетевого экрана.

Для тестирования правильности работы IPS-систем на межсетевом экране FortiGate было осуществлено моделирование кибератаки, имитирующей несанкционированное удаленное подключение по протоколу RDP. Для этого был разработан макет корпоративной сети на платформе GNS3 [2-4]. В GNS3 была смоделирована локальная сеть, состоящая из FortiGate, FortiAnalyzer, FortiManager, ПК с операционной системой (ОС) Windows 7. Также в смоделированную сети добавлено устройство нарушителя с операционной системой Kali Linux (рисунок 1).

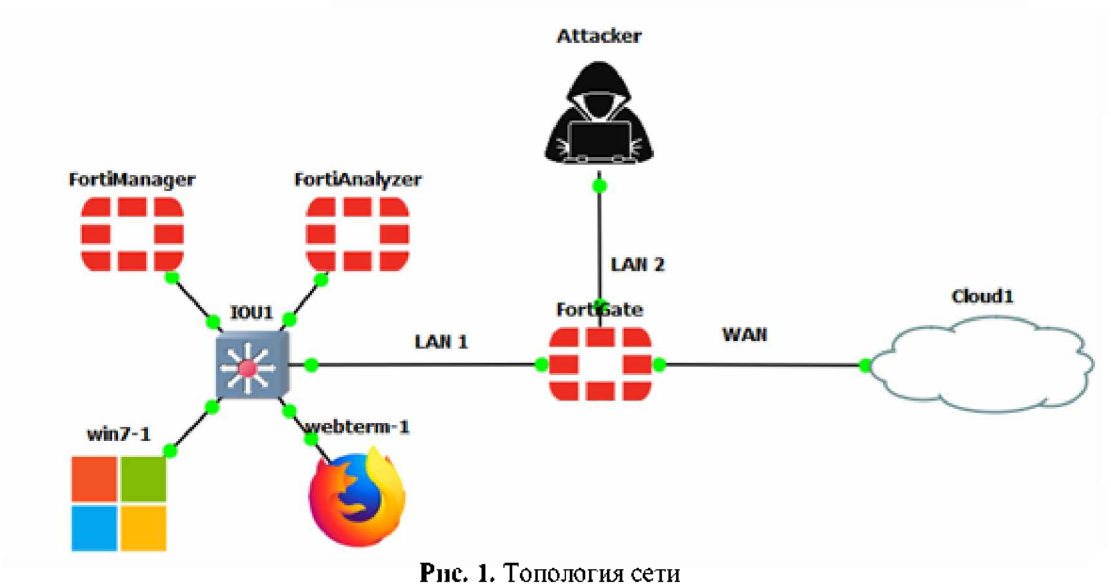
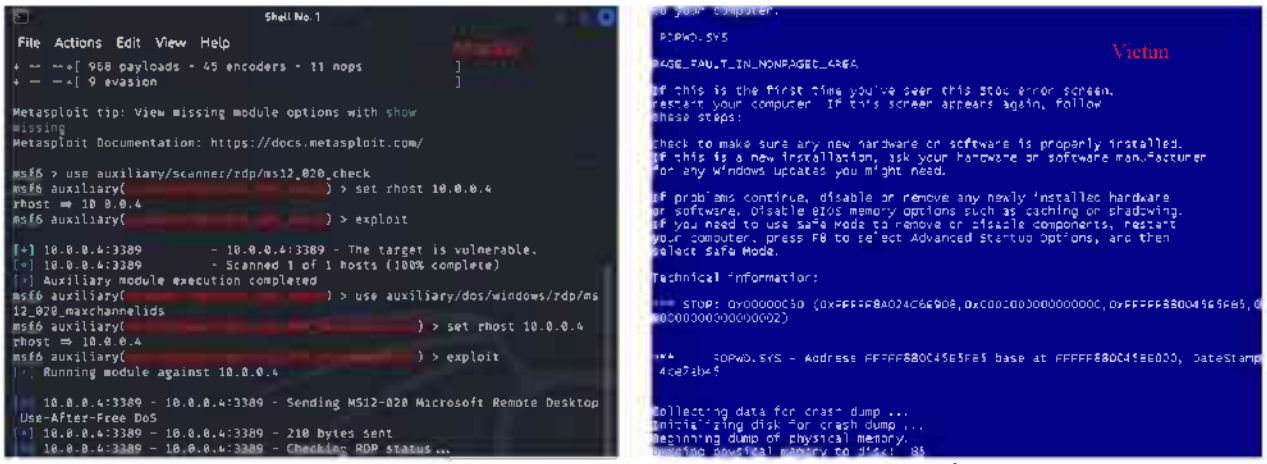


Рис. 1. Топология сети
Fig. 1. Network topology

С устройства с ОС Kali-Linux проведена кибератака на устройство с ОС Windows7 с помощью набора инструментов Metasploit (рисунок 2, а). В результате на компьютере с ОС Windows7 при выходе пользователя из системы появляется синий экран, как показано на рисунке 2, б.



a *b*

Рис. 2. Несанкционированное удаленное подключение по протоколу RDP (*a*) и его результат (*b*)
Fig. 2. Unauthorized remote connection via RDP protocol (*a*) and its result (*b*)

Для предотвращения вторжений нарушителя необходимо актировать IPS на FortiGate с профилем высокой безопасности, который фильтрует все предопределенные сигнатуры с определенными действиями и следующими типами: критический, высокий, средний (рисунок 3). Для сигнатур с низким типом устанавливается действие по умолчанию. В результате процесс несанкционированного удаленного подключения будет заблокирован, и попытка проникновения будет внесена в отчет событий на FortiAnalyzer, как показано на рисунке 4.

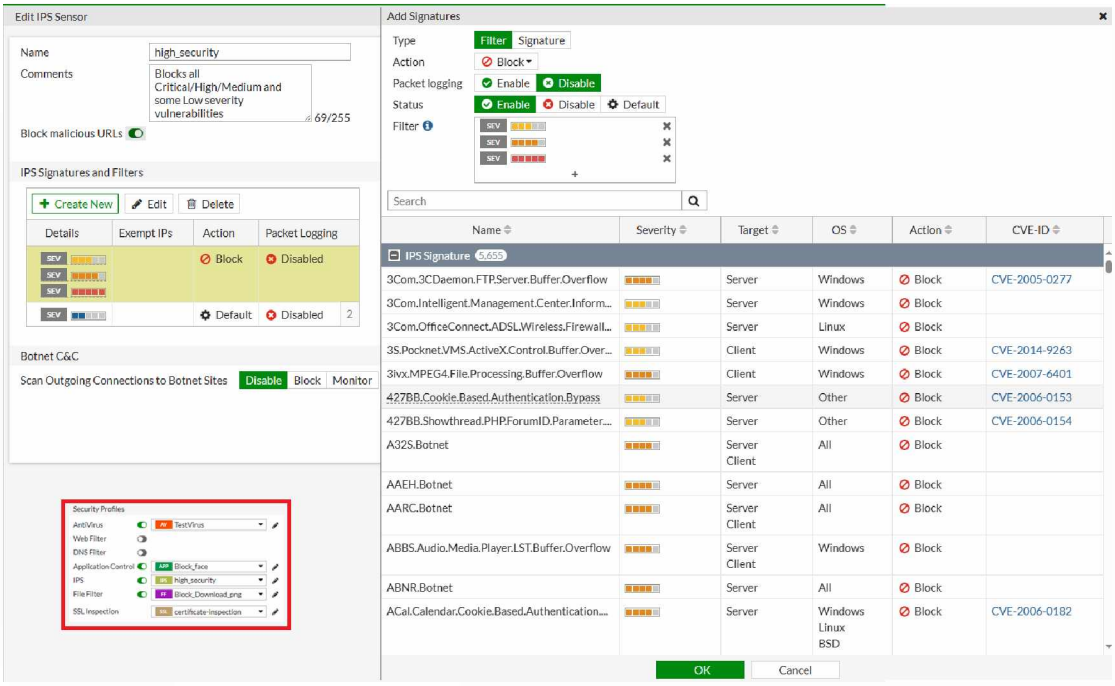


Рис. 3. Настройка IPS-систем с профилем высокой безопасности
Fig. 3. Configure IPS systems with a high security profile

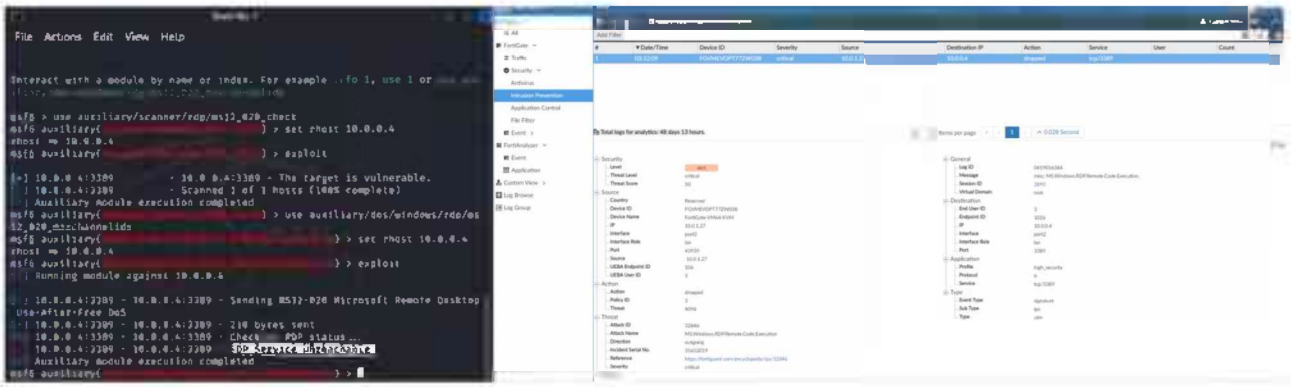


Рис. 4. Успешно блокировка несанкционированного удаленного подключения
Fig. 4. Successfully blocked unauthorized remote connection

Заключение

Таким образом, посредством реализации разработанной методики настройки IPS-систем и тестирования ее работы было установлено, что FortiGate использует сигнатуры, декодеры протоколов, эвристику, аналитику угроз и расширенное обнаружение угроз для предотвращения эксплуатации различных угроз. Благодаря такому раннему обнаружению угроз аномалии кибератак пакеты блокируются еще до проверки другими политиками (антивирус, веб-фильтр и др.). Также необходимо отметить, что составными элементами IPS-систем являются сенсоры IPS, которые проверяют сетевой трафик, поступающий на интерфейс, на наличие аномальных параметров, указывающих на кибератаку.

Список использованных источников

1. Руководства администратора FortiGate/FortiOS 6.4.12 // Fortinet [Электронный ресурс] – 2025. – Режим доступа: https://docs.fortinet.com/document/forti-gate/6.4.12/administration-guide/565562/intrusion-prevention. – Дата доступа: 06.02.2025.

2. До, М.К. Обоснование выбора эмулятора GNS3 для изучения принципов построения локальных сетей с межсетевым экранированием / М.К. До, Е.С. Белоусова // 59-я научная конференция аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 17–21 апреля 2023 г., БГУИР, Минск, Беларусь: сборник материалов. – Мн. – 2023. – С. 41-43.

3. Богатырев В.А. Структурная надежность многопутевой маршрутной сети с реконфигурациями при переключении маршрутов / Богатырев В.А., Ле А., Абрамова Е.А. // Международная российская конференция по автоматике (RusAutoCon), 2022, стр. 414-418.

4. Богатырев В.А. Надежность реконфигурируемой сети с переключением сегментов / Богатырев В.А., Ле А., Абрамова Е.А. // Волновая электроника и инфокоммуникационные системы: материалы XXVI международной научной конференции (Санкт-Петербург, 29 мая-2 июня 2023г.) – 2023. – Т. 1. – С. 26-31.

References

1. Admin Guides FortiGate/FortiOS 6.4.12 // Fortinet [Electronic resource] – 2025. – Access mode: https://docs.fortinet.com/document/fortigate/6.4.12/administration-guide/565562/intrusion-prevention. – Date of access: 06.02.2025.

2. Do, M.K. Justification for the Choice of the GNS3 Emulator for Studying the Principles of Building Local Area Networks with Firewalling / M.K. Do, E.S. Belousova // 59th Scientific Conference of Postgraduate, Master's and Undergraduate Students of the Educational Institution "Belarusian State University of Informatics and Radioelectronics", April 17-21, 2023, BSUIR, Minsk, Belarus: Collection of Materials. – Mn. – 2023. – P. 41-43.

3. Bogatyrev V.A. Structural reliability of a multipath routing network with reconfigurations when switching routes / Bogatyrev V.A., Le A., Abramova E.A // 2022 International Russian Automation Conference (RusAutoCon), 2022, pp. 414-418.

4. Bogatyrev V.A. Reliability of a reconfigurable network with segment switching / Bogatyrev V.A., Le A., Abramova E.A. // Wave electronics and infocommunication systems: materials of the XXVI international scientific conference (St. Petersburg, May 29 - June 2, 2023) –2023. – V. 1. – P. 26-31.

Сведения об авторах

До М.К., магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», domanhkiemnd@gmail.com.
Фунг В.К., аспирант, университет ИТМО, phungvanquy97@gmail.com

Information about the authors

Do M.K., Master's student of the Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", domanhkiemnd@gmail.com.
Phung V.Q., Post-Graduate Student, ITMO University, phungvanquy97@gmail.com.