УДК 004.056

ФУНКЦИИ ФИЛЬТРАЦИИ И ШИФРОВАНИЯ DNS-СООБЩЕНИЙ НА МЕЖСЕТЕВОМ ЭКРАНЕ CHUWALL

Д.М. Мартинкевич[1], К.О. Янислaвский[1], Е.С. Белоусова[2]
[1]*Учреждение образования «Национальный детский технопарк», г. Минск, Республика Беларусь*
[2]*Учреждение образования «Белорусский государственный университет информатики и радиоэлектороники», г. Минск, Республика Беларусь*

Аннотация. В работе представлено описание реализации функций фильтрации DNS-сообщений и их шифрования для обеспечения информационной безопасности. На основе сервиса BIND9, метода DNS-Sinkholing и списков фильтрации доменов реализована функция проверки DNS-сообщений на межсетевом экране для обнаружения и блокировки кибератак CHUWALL. Для шифрования DNS-сообщений был настроен сервис dnscrypt_proxy, который поддерживает протокол DNS-over-HTTPS. В статье представлены результаты тестирования реализованных функций на межсетевом экране CHUWALL.
Ключевые слова: Межсетевой экран; CHUWALL; DNS; DNS-Sinkholing; BIND9; HaGeZi; TLD-сервер; dnscrypt_proxy; DNS-over-HTTPS (DoH); Яндекс DNS.

FILTERING AND ENCRYPTION FUNCTIONS OF DNS-MESSAGES ON THE CHUWALL FIREWALL

D.M. Martsinkevich[1], K.A. Yanislauski[1], E.S. Belousova[2]
[1]*Educational Institution "National Children's Technopark", Minsk, Republic of Belarus*
[2]*Educational Institution "Belarusian State University of Informatics and Radioeletronics", Minsk, Republic of Belarus*

Abstract. This article describes the implementation of DNS message filtering and encryption functions to ensure information security. Based on the BIND9 service, the DNS-Sinkholing method and domain filtering lists, a function of checking DNS messages has been implemented on the firewall to detect and block the cyber attacks CHUWALL. To encrypt DNS messages, dnscrypt_proxy has been set up, which supports the DNS-over-HTTPS protocol. The article presents the results of testing implemented functions on the CHUWALL firewall.
Keywords: Firewall; CHUWALL; DNS; DNS-Sinkholing; BIND9; HaGeZi; TLD-server; dnscrypt_proxy; DNS-over-HTTPS (DoH); Yandex DNS.

Введение

Протокол DNS по своей архитектуре не предоставляет механизмов обеспечения безопасности. Следовательно, возможны кибератаки типа отравления кэша, DoS, DNS-спуфинг и фишинг [1]. Для обеспечения конфиденциальности и целостности информации существует протокол DNS-over-HTTPS, с помощью которого DNS-трафик инкапсулируется в протокол HTTPS. Целью данной работы является реализация функций фильтрации и шифрования DNS-сообщений путем использования списка фишинговых сайтов, создания корпоративного списка фильтрации и шифрования по протоколу DNS-over-HTTPS (DoH).

Основная часть

В ходе разработки межсетевого экрана для обнаружения и блокировки кибератак CHUWALL [2], работающего на операционной системе Linux Ubuntu Server, реализована функция фильтрации и шифрования DNS-сообщений. Произведено исследование популярных сервисов (Unbound, dnsmasq, BIND9) с открытым исходным кодом для ОС Linux. По результатам сравнения был выбран сервис BIND9 по причине легковесности и эффективности (по сравнению с Unbound), поддержки файлов зон для фильтрации запросов (по сравнению с dnsmasq).

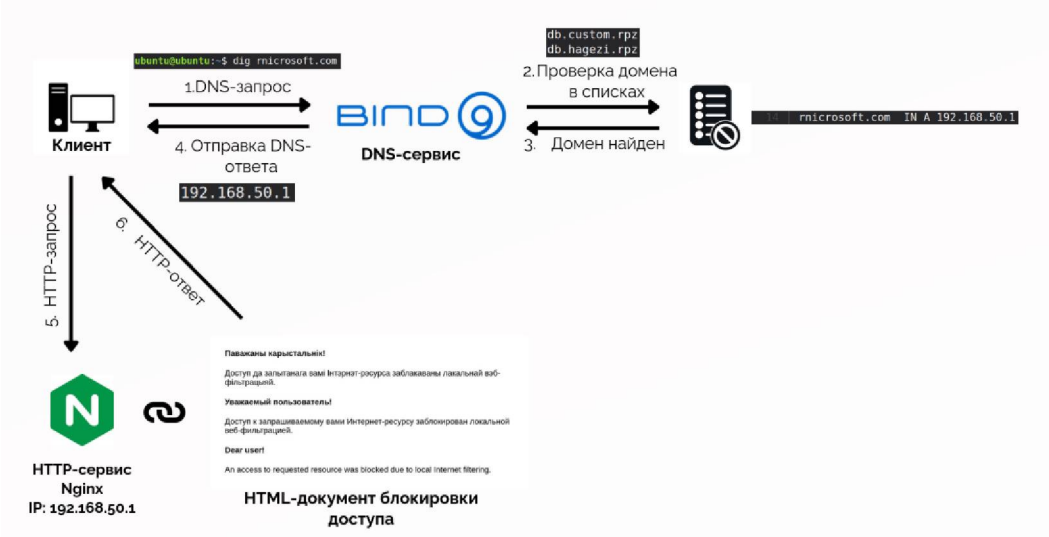
Для фильтрации запросов использован метод DNS-Sinkholing, предназначенный для перенаправления DNS-запросов на заданный сервер. В разрабатываемом межсетевом экране эта функция необходима для предотвращения доступа пользователя к нелегитимным доменам. Список HaGeZi (db.hagezi.rpz) использовался для блокировки фишинговых и рекламных доменов. Также использовался корпоративный список (db.custom.rpz), в который реализована возможность добавления доменов с помощью bash-скрипта.

В соответствии с алгоритмом фильтрации DNS-сообщений (рисунок), если клиент запрашивает нелегитимный домен rnicrosoft.com у локального DNS-сервера BIND9, то проверяется его наличие домена в списках. При обнаружении сервер возвращает вместо реального IP-адреса локальный IP 192.168.50.1, на котором запущен сервис Nginx, возвращающий страницу блокировки доступа при запросе. Подключение клиента к запрашиваемому домену не происходит.

Для легитимных доменов важным остается шифрование DNS-сообщений, ведь такой же сценарий подмены IP-адреса может осуществить нарушитель. Произведено исследование модификаций протокола DNS, а именно DNS-over-HTTPS, DNS-over-TLS, DNSCrypt, DNSSEC. По результатам сравнения был выбран протокол

DNS-over-HTTPS (DoH), так как он работает на порте TCP 443, в отличие от протокола DNS-over-TLS (DoT), работающего на порте TCP 853, что делает его легким для блокировки.

В качестве легковесного DNS-прокси, поддерживающего DoH был выбран сервис dnscrypt_proxy. Для использования TLD-сервера было проведено сравнительный анализ наиболее популярных DNS-провайдеров (Google DNS, Яндекс DNS, Белтелеком). В результате было решено использовать Яндекс DNS по причине нахождения серверов на территории Союзного государства и наличия большого количества кириллических доменов.



Алгоритм фильтрации DNS-сообщений для нелегитимного домена
DNS-messages filtration algorithm for illegitimate domain

Произведена проверка работы протокола DNS-over-HTTPS, при которой в дампе трафика не должны быть обнаружены сетевые пакеты с содержанием протокола DNS на седьмом уровне модели OSI. Соответственно должны быть обращения к IP-адресу TLD-сервера Яндекс DNS Safe по протоколу TLS на порт 443.

Заключение

Таким образом, было установлено, что реализация DNS-сервера на основе BIND9 и метода DNS-Sinkholing с использованием списка HaGeZi и корпоративного списка позволяет обеспечить фильтрацию DNS-сообщений, тем самым предотвратив коммуникацию пользователя с потенциально вредоносным доменом. Также установлено, что для шифрования DNS-сообщений лучше всего подходит протокол DNS-over-HTTPS (DoH), используемый сервисом dnscrypt_proxy для обращения к TLD-серверу. Полученные результаты позволяют рекомендовать межсетевой экран CHUWALL для блокировки попыток

обращения к вредоносным доменам, что может повысить уровень информационной безопасности различных организаций.

Список использованных источников

1. Борботько Ф.Т. (2023) Атаки с использованием DNS протокола и противодействие им. *Технические средства защиты информации*. 22–23.

2. Белоусова Е.С., Мальцев В.Л., Мартинкевич Д.М., Янислaвский К.О. (2026) Маршрутизатор с функциями анализа сетевого трафика. *Будущее через исследования*. 52–57.

References

1. Borbotko F.T. (2023) Attacks using the DNS protocol and counteracting it. *Technical means of information protection*. 22-23.

2. Belousova E.S., Maltsev V.L., Martsinkevich D.M., Yanislauski K.O. (2026) Router with network traffic analysis functions. *The future through research*. 52-57.

Сведения об авторах

Мартинкевич Д.М., учащийся, учреждение образования «Национальный детский Технопарк», srilankainform@gmail.com.

Янислaвский К.О., учащийся, учреждение образования «Национальный детский Технопарк», kirill.uspech@gmail.com.

Белоусова Е.С. канд. техн. наук, доц., доцент кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», belousova@bsuir.by.

Information about the authors

Martsinkevich D., Student, Educational Institution "National Children's Technopark", srilankainform@gmail.com.

Yanislauski K., Student, Educational Institution "National Children's Technopark", kirill.uspech@gmail.com.

Belousova E., PhD, Associate Professor, Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", belousova@bsuir.by.