**РАЗРАБОТКА МОДУЛЯ ALTERATOR ДЛЯ НАСТРОЙКИ WIREGUARD.**

**ОПЕРАЦИОННА СИСТЕМА АЛЬТ – ALT Linux.**

Горшков М.А., Скворцов Д.О.

РГУ нефти и газа им. И. М. Губкина, г. Москва, Российская Федерация

*Рассмотрена актуальная разработка модуля ALTERATOR для настройки WireGuard на базе операционной системы Альт Linux. В данной статье подробно описан пошаговый процесс разработки модуля alterator для настройки WireGuard.*

*Ключевые слова: Linux, ALT-Linux, ALTERATOR, WireGuard, VPN, информационная безопасность, администрирование, локальная сеть.*

С нынешнем уходом большинства операционных систем и программных обеспечений из РФ, мы сталкиваемся с необходимостью создания собственных решений для надежного обеспечения конфиденциальности данных. Отечественная операционная система ALT от компании Базальт СПО, зарекомендовала себя как один из наиболее перспективных проектов, в которой интеграция модуля настройки WireGuard значительно увеличит ее функциональность, а также безопасность [1]. WireGuard – программное обеспечение, а также коммутационный протокол, который реализует зашифрованные виртуальные частные сети [2]. Разработка модуля web-интерфейса к серверу, поможет обеспечить надежную безопасность, а именно просмотр активных сессий, управление доступом и предотвращение несанкционированного проникновения.

В ходе разработки данного веб-интерфейса для WireGuard, есть несколько основных этапов, из которых состоит вся работа:

1. Разработка серверной части
2. Разработка интерфейса
3. Соединение интерфейса и серверной части
4. Тестирование

Перед тем как перейти к использованию веб-модуля интерфейса WireGuard, необходимо пройти авторизацию в личный кабинет, где необходимо указать:

* логин администратора (admin);
* пароль администратора (admin).



***Рис 1. Вход в личный аккаунт веб-интерфейса***

После того как прошла успешная авторизация, открывается несколько вкладок, которые необходимо заполнить для успешного использования данного проекта.

Вкладки, которые находятся в личном кабинете:

* Клиенты WireGuard
* Сервер WireGuard
* Общие настройки

В каждой из этих вкладок, производится определенная настройка сервера Wireguad.

После перехода во вкладку «Клиенты WireGuard» будут отображаться полные настройки всех зарегистрированных пользователей. В данном поле можно создать/удалить пользователя. Просмотреть все его данные, а также реализовать распределение трафика между всеми клиентами.

В личной карточке каждого пользователя хранится следующая информация (Рис. 2):

* Имя
* Почта
* Время запуска
* Время последнего подключения
* Состояние DNS-сервера
* IP Allocation



***Рис 2. Клиенты Wireguard***

Также необходимо провести настройку сервера WireGuard. В данной вкладке необходимо заполнить следующие поля (Рис. 3):

* Адреса интерфейса сервера – необходимы для принятия сигналов от клиентов - Порт прослушивания – это порт, по которому Wireguard будет прослушивать [3].

Так же при необходимости можно добавить несколько скриптов, которые будут выполняться согласно своему названию, то есть скрипт PostUp – это скрипт, который необходимо выполнить после запуска сервера, PreDown – скрипт, который выполняется перед выключением сервера и скрипт PostDown – он выполняется после выключения.

В данной вкладке также располагается пара ключей (Приватный ключ, Публичный ключ) – главное предназначение этих ключей, является подключение к серверу.



***Рис 3. Сервер Wireguard***



***Рис. 4 Общие настройки***

В данной вкладке «Общие настройки» необходимо заполнить следующие поля для удачного подключение (Рис. 4):

* Публичный IP-адрес сервера Wireguard, к которому будет подключаться клиент, также при нажатии на кнопку «Продолжить» можно автоматически определить публичный адрес сервера
* Также необходимо будет указать DNS-сервера, которые будут установлены в конфигурации клиента
* MTU – устанавливается в конфигурации сервера и клиента (по умолчанию 1450). Также размер MTU можно изменить, если используется одно из следующих соединений: PPPoE, 3G, спутниковая сеть [4].
* Постоянно поддерживающий сигнал. По умолчанию, пиры WireGuard остаются без действия если не нужно общаться, поэтому пиры, находяшиеся за NAT и/или браномауэром, могут быть недоступны для других пиров до тех пор, пока они не выйдут на связь с другими пиртами. Добавление Persistent Keepa Live может гарантировать, что соединение остается открытым.
* Добавьте совпадающую fwmark для всех пакетов, выходящих из туннеля WireGuard с не-умолчательным маршрутом. Значение по умолчанию: 0xca6c
* Значение для настройки Table в конфигурационном файле wg. Значение по умолчанию: auto.
* Путь к конфигурационному файлу сервера Wireguard. Необходимо убедиться, что родительский каталог существует и имеет разрешения на запись.

Данную настройку необходимо произвести, как показана на рисунке 4.

**Описание фрагмента кода:**

В данном фрагменте кода реализовано два обработчика API (SuggestIPAllocation и ApplyServerConfig).

Функция SuggestIPAllocation отвечает за получение списка предложенных IP-адресов для клиента. В начале она запрашивает конфигурацию сервера из базы данных. Если возникает ошибка, в лог записывается сообщение, и клиенту возвращается ответ с кодом 400 [5].

Затем функция использует утилиту GetAllocatedIPs, чтобы получить список выделенных IP-адресов. В случае ошибки логируется сообщение и возвращается ответ с кодом 500 [6].

Далее обрабатывается параметр sr из запроса, чтобы определить список CIDR для поиска доступных IP-адресов. Если CIDR не указан, используются адреса интерфейса сервера. Затем функция идет по каждому CIDR в searchCIDRList и пытается найти доступные IP-адреса через утилиту GetAvailableIP. Если доступный IP найден, он добавляется в множество ipSet, чтобы избежать дубликатов. Ошибки при поиске также фиксируются в логах. В конце, если доступные IP-адреса были найдены, они добавляются в срез suggestedIPs и возвращаются клиенту с кодом 200 [7]. Если IP-адреса не найдены, возвращается ответ с кодом 500 и сообщением об ошибке.

Функция ApplyServerConfig отвечает за применение конфигурации сервера и перезапуск сервера Wireguard. Обработчик сначала получает конфигурацию сервера, список клиентов и пользователей, а также глобальные настройки из базы. При любой ошибке происходит логирование и возврат ответа с кодом 500. Затем функция записывает конфигурационный файл сервера Wireguard с помощью утилиты WriteWireGuardServerConfig. Если возникает ошибка, она логируется и возвращается клиенту. После успешной записи конфигурации вызывается UpdateHashes, чтобы обновить хеши в базе данных. Если на этом шаге происходит ошибка, она также логируется. В конце при успешном завершении всех операций клиент получает ответ с кодом 200 и сообщением о том, что конфигурация сервера успешно применена.

Данный код реализован для управления IP-адресами и конфигурацией сервера WireGuard, предоставляя доступные IP-адреса для новых клиентов, а также возможность вносить изменения в конфигурации сервера.



***Рис 5. Фрагмент кода 1***



***Рис 6. Фрагмент кода 2***

**ЛИТЕРАТУРА**

1. Операционные системы «АЛЬТ». - URL: https://alt-linux.ru/ (дата обращения 29.10.2024)
2. «WireGuard – прекрасный VPN будущего». – URL: https://habr.com/ru/articles/432686 (дата обращения 01.11.2024)
3. Уймин, А. Г. Демонстрационный экзамен базового уровня. Сетевое и системное администрирование: Практикум. Учебное пособие для вузов / А. Г. Уймин. – Санкт-Петербург: Издательство "Лань", 2024. – 116 с. – (Высшее образование). – ISBN 978-5-507-48647-2. – EDN BZJRIQ.
4. PPPoE. – URL: https://ru.wikipedia.org/wiki/PPPoE (дата обращения 11.11.2024)
5. Ошибка 400: что такое и как исправить. – URL: https://help.reg.ru/support/hosting/sayt-ne-rabotayet/oshibka-400-chto-takoye-i-kak-ispravit#0
6. Ошибка 500 на сайте: что такое и как исправить. - URL: https://help.reg.ru/support/hosting/sayt-ne-rabotayet/oshibka-500-na-sayte-chto-takoye-i-kak-ispravit#0
7. 200 – это хорошо или это плохо? – URL: https://habr.com/ru/articles/440382/