

Презентация к докладу

Виртуальные частные сети

Ким М. А.

2 октября 2023

Российский университет дружбы народов, Москва, Россия

Вводная часть

- Ограниченность зарубежных ресурсов на территории РФ.
- Блокировки некоторых VPN-протоколов на территории РФ.

- VPS на базе Linux Ubuntu 20.4
- Клиенты на базе Windows 10, Linux Mint Cinnamon 21.1, Android, IOS.
- Протоколы, предоставляющие VPN-соединение, а также туннельные прокси.

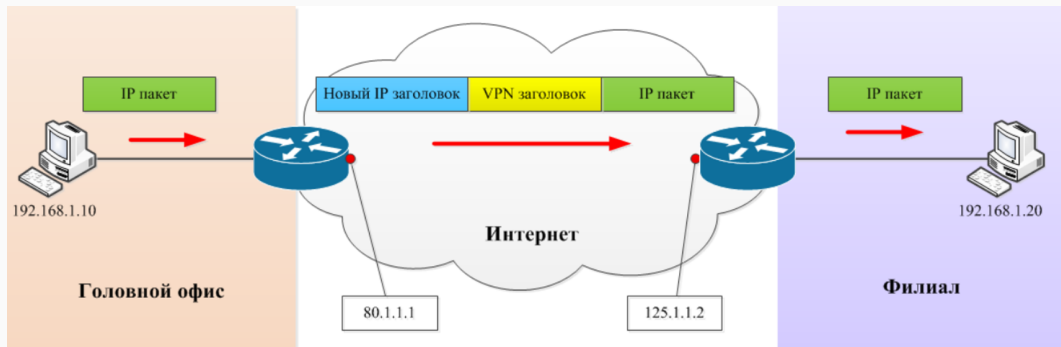
- Определить основные используемые протоколы, предоставляющие VPN-соединение, или эмулирующие его.
- Сравнить их быстродействие и защищенность.

Процесс выполнения работы

Теоретическое введение

VPN (Virtual Private Network) — виртуальная частная сеть — широко распространённая технология, позволяющая организовывать виртуальные сети поверх существующих реальных сетей. Построение VPN-а означает создание туннелей. Под туннелем подразумевается канал между двумя устройствами, по которому передаётся данные.

Принцип работы VPN



Вот как выглядит инкапсулируемый пакет:

Адрес отправителя 80.1.1.1	Адрес получателя 125.1.1.2	VPN заголовок	Адрес отправителя 192.168.1.10	Адрес получателя 192.168.1.20	Данные
-------------------------------	-------------------------------	---------------	-----------------------------------	----------------------------------	--------

Рис. 1: Пересылка пакета при установленном VPN-соединении

Deep Packet Inspection (DPI) — глубокая проверка пакетов — технология проверки сетевых пакетов по их содержимому с целью регулирования и фильтрации трафика, а также накопления статистических данных. В отличие от брандмауэров, Deep Packet Inspection анализирует не только заголовки пакетов, но и полезную нагрузку, начиная со второго уровня модели OSI.

Рассмотрение протоколов

1. Сравнительно небольшая скорость работы.
2. Возможность выбора между TCP и UDP протоколами для передачи трафика.
3. Слабая устойчивость к блокировкам со стороны DPI.

1. Сравнительно небольшая скорость работы (однако быстрее, нежели OpenVPN).
2. Слабая устойчивость к блокировкам со стороны DPI.

1. Высокая скорость работы по сравнению со всеми существующими VPN-протоколами.
2. Работа посредством UDP-протокола.
3. Отсутствие устойчивости к блокировкам со стороны DPI.

WireGuard. Состав приветственного пакета.

The screenshot shows the Wireshark interface with the following details:

- Packet List:** Shows the handshake sequence from 1 to 13. The first three packets are WireGuard, and the rest are TCP/HTTP.
- Packet Details:** For the selected packet (Frame 7), it shows:
 - Ethernet II, Src: 42:01:0a:00:00:01, Dst: 42:01:0a:00:00:0e
 - Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.1
 - User Datagram Protocol, Src Port: 40248, Dst Port: 51820
 - WireGuard Protocol, Type: Transport Data (4), Reserved: 000000, Receiver: 0x8e5bee31, Counter: 3, Encrypted Packet [Stream index: 0]
 - Internet Protocol Version 4, Src: 10.0.2.2, Dst: 10.0.2.1
 - Transmission Control Protocol, Src Port: 47676, Dst Port: 80, Seq: 1, Ack: 1, Len: 72
 - Hypertext Transfer Protocol
- Packet Bytes:** Shows the raw packet data in hexadecimal and ASCII.

Annotations in red:

- A red box highlights the "User Datagram Protocol" and "WireGuard Protocol" sections.
- Red arrows point to the "udp" and "wireguard" labels.
- A red arrow points to the "encrypted" label.
- Red arrows point to the "ip", "tcp", and "http" labels.

Рис. 2: Состав handshake-пакета WireGuard

1. Относительно низкая скорость работы.
2. Эмуляция VPN-туннеля посредством прокси с обфускацией.
3. Уязвимость к replay-атакам и атаками методом active probing.
4. Устарел и более не поддерживается.

1. Все еще относительно низкая скорость работы.
2. Эмуляция VPN-туннеля посредством прокси с обфускацией.
3. Отсутствие уязвимости к replay-атакам и атаками методом active probing.
4. Крайне сложное детектирование протокола методом удара по радиусу.

V2Ray/V2Fly/XRay — фреймворки, работающие с протоколами:

1. VMess — устарел, не используется. Для сокращения размера реферата рассматривать его не вижу смысла.
2. VLESS — протокол, активно использующийся в текущий момент времени. Поддерживает следующие аддоны:
 - XTLS — отсутствие ненужного двойного шифрования.
 - XTLS-Reality — определение “свой/чужой” здесь происходит еще на этапе TLS-хендшейка в момент чтения ClientHello.

Результаты

- Рассмотрены основные VPN-протоколы.
- Проведено их сравнение.

Среди всех рассмотренных протоколов для использования я выбрал только два. WireGuard как самый легковесный и быстрый VPN-протокол, при этом не защищенный от блокировок со стороны поставителя интернет-услуг. Его использование обусловлено скоростью работы и инертностью провайдеров. При блокировке соединения по средствам WireGuard мною используется фреймворк XRay с протоколом VLESS и аддоном XTLS-Reality. Он обеспечивает стабильную, однако более медленную, работу даже в странах с “жесткими” блокировками: в Китае и Туркменистане.