Latin American Journal of Education
www.lajoe.org

OPENVPN TEXNOLOGIYASI HAQIDA UMUMIY MA'LUMOT

https://doi.org/10.5281/zenodo.19005499

Habibjonova Guldofarid Murodjon qizi
Muxammad al – Xorazmiy nomidagi TATU "Kiberxavfsizlik va kriminalistika" kafedrasi stajyor o'qituvchisi
O'razaliyeva Rayxona Qaxramon qizi
Toshpo'lotov Maqsud Abduvali o'g'li
O'ktamov Doston Rustam o'g'li
Muxammad al – Xorazmiy nomidagi TATU talabalari

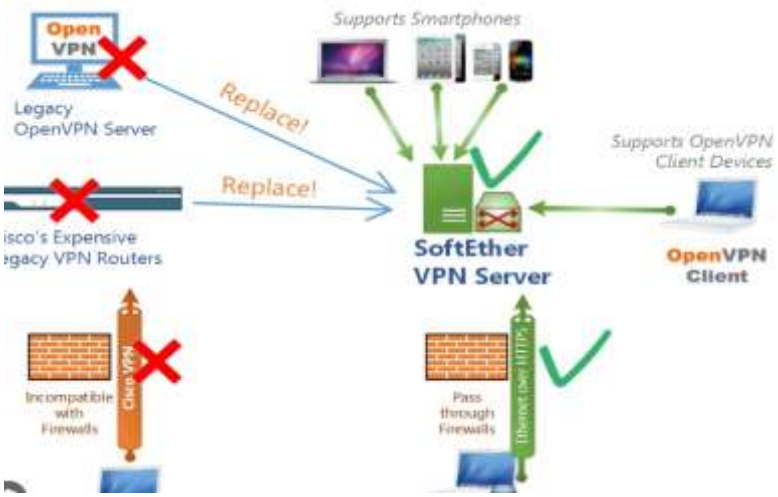
Annotatsiya: *Ushbu maqolada OpenVPN texnologiyasining ishlash prinsipi, arxitekturasi va xavfsizlik mexanizmlari tahlil qilinadi. OpenVPN virtual xususiy tarmoq texnologiyasi bo'lib, foydalanuvchilarga internet orqali xavfsiz va shifrlangan aloqa kanalini yaratish imkonini beradi. Maqolada OpenVPN tizimining server–mijoz arxitekturasi, uning asosiy komponentlari, autentifikatsiya jarayoni hamda shifrlash algoritmlarining ishlash tamoyillari ko'rib chiqiladi. Shuningdek, Windows muhitida OpenVPN dasturini o'rnatish va konfiguratsiya qilish bosqichlari yoritilgan.*

Kalit so'zlar: *OpenVPN, VPN texnologiyasi, kiberxavfsizlik, shifrlash algoritmlari, SSL/TLS protokoli, autentifikatsiya, virtual tunnel, tarmoq xavfsizligi, server–mijoz arxitekturasi, AES shifrlash.*

OpenVPN — bu Virtual Private Network (VPN) texnologiyalarining eng mashhur va xavfsiz turlaridan biri bo'lib, ochiq manba (open-source) tamoyili asosida ishlab chiqilgan. Ushbu tizim SSL/TLS (Secure Socket Layer / Transport Layer Security) protokollari asosida ishlaydi va ma'lumotlarni shifrlangan kanal orqali uzatishni ta'minlaydi.

OpenVPN foydalanuvchiga shifrlangan tarmoq aloqasini yaratish imkonini beradi. U platformalararo texnologiya bo'lib, Windows, Linux, macOS, Android, iOS tizimlarida ishlaydi.

Latin American Journal of Education
www.lajoe.org



1.1-rasm. OpenVPN — bu Virtual Private Network (VPN) texnologiyasi

OpenVPN dasturining asosiy afzalliklari:

OpenVPN arxitekturasi

OpenVPN tizimi server–mijoz (client–server) modelida ishlaydi. Bu modelda server markaziy uzel bo‘lib, barcha mijozlar (clientlar) unga ulanadi. Tizimning arxitekturasi quyidagi asosiy komponentlardan iborat (2.2-rasm):

1. OpenVPN Server — shifrlangan kanalni boshqaradi, foydalanuvchilarni autentifikatsiya qiladi va tarmoq ma’lumotlarini marshrutlaydi.

2. OpenVPN Client — serverga ulanib, shifrlangan tunel orqali ma’lumot uzatadi.

3. CA (Certificate Authority) — sertifikat va kalitlarni yaratish hamda ularni boshqarish uchun ishlatiladi.

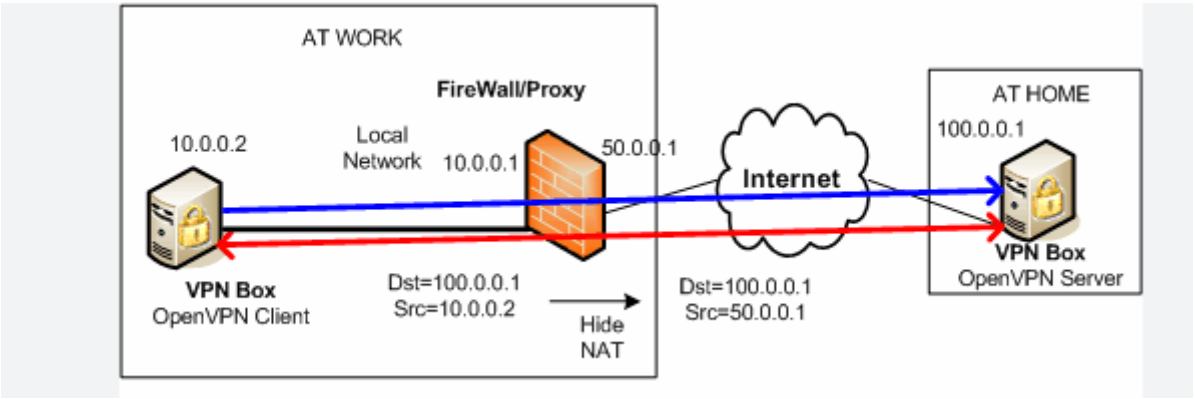
4. Konfiguratsiya fayllari (.ovpn) — server va mijoz uchun alohida sozlamalarni o‘z ichiga oladi.

5. Tarmoq interfeysi (TAP/TUN) — virtual adapter bo‘lib, VPN tunnel orqali ma’lumot almashishni ta’minlaydi.

Latin American Journal of Education
www.lajoe.org

```
[Client] ⇄ [OpenVPN Tunnel] ⇄ [Server] ⇄ [Internet / LAN]
```

1.2-rasm. Tizimning umumiy ishlash diagrammasi



1.3-rasm. OpenVPN arxitekturasi.

OpenVPN ishlash mexanizmi

OpenVPN quyidagi bosqichlarda ishlaydi:

1. Autntifikatsiya (tasdiqlash):Mijoz va server bir-birini sertifikatlar yordamida tekshiradi.

Bu jarayon SSL/TLS protokoli orqali amalga oshiriladi.

2. Tunnel yaratish: Autentifikatsiya muvaffaqiyatli o‘tgach, tizim shifrlangan virtual tunnel (TUN/TAP interfeysi) hosil qiladi.

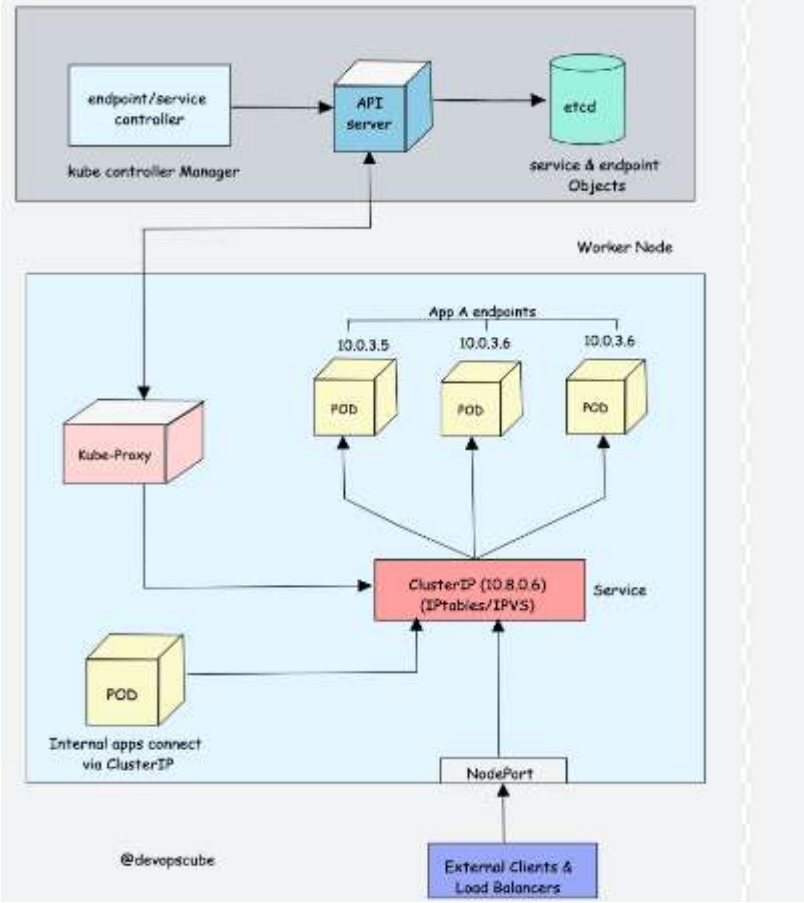
3. Shifrlangan aloqa: Ma’lumotlar AES yoki ChaCha20 algoritmlari yordamida shifrlanadi va faqat VPN tunnel orqali uzatiladi.

4. Marshrutlash:Tarmoq paketlari VPN interfeysi orqali o‘tadi, foydalanuvchining asl IP manzili yashiriladi.

5. Ulanishni nazorat qilish: Server har bir client uchun log yuritadi va trafikni nazorat qiladi.

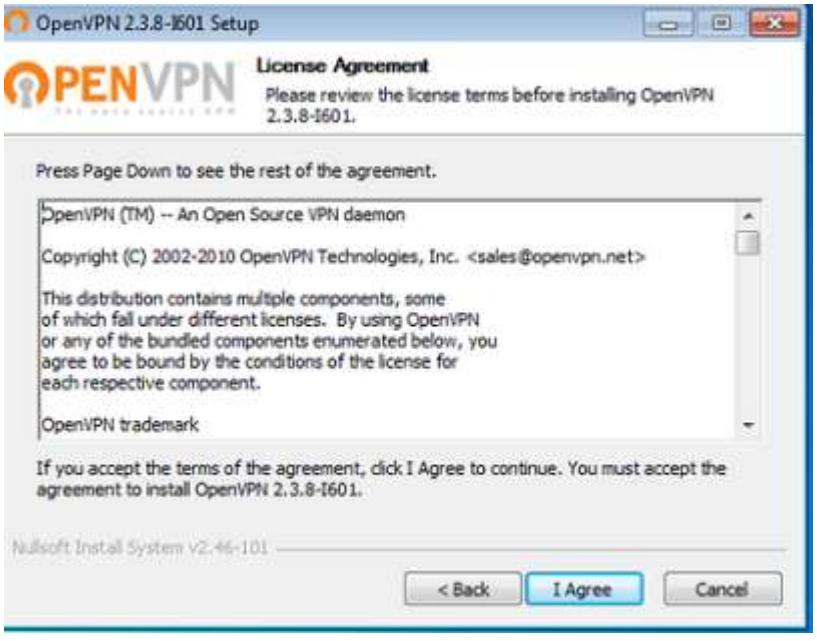
Bu jarayon foydalanuvchi uchun ko‘rinmaydi — barcha tarmoq almashinuvi fon rejimida sodir bo‘ladi.

Latin American Journal of Education
www.lajoe.org



1.4-rasm. OpenVPN ishlash mexanizmi

OpenVPN konfiguratsiyasi (Windows muhiti uchun)



1.5-rasm. OpenVPN konfiguratsiyasi (Windows muhiti uchun)

Windows tizimida OpenVPN quyidagi bosqichlarda sozlanadi:

Latin American Journal of Education
www.lajoe.org

1. OpenVPN dasturini o‘rnatish: Dastur rasmiy saytdan (https://openvpn.net) yuklab olinadi va Windows tizimiga o‘rnatiladi.

2. Sertifikatlar va kalitlarni yaratish: EasyRSA yordamida quyidagilar yaratiladi:

- Root CA sertifikati
- Server sertifikati
- Client sertifikati
- Difgurfie-Hellman kaliti (DH)

```
port 1194
proto udp
dev tun
ca ca.crt
cert server.crt
key server.key
dh dh.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120
cipher AES-256-CBC
persist-key
persist-tun
status openvpn-status.log
log-append /var/log/openvpn.log
verb 3
```

1.6-rasm. Server konfiatsiyasi (server.ovpn):

```
bash

client
dev tun
proto udp
remote your_server_ip 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client.crt
key client.key
cipher AES-256-CBC
verb 3
```

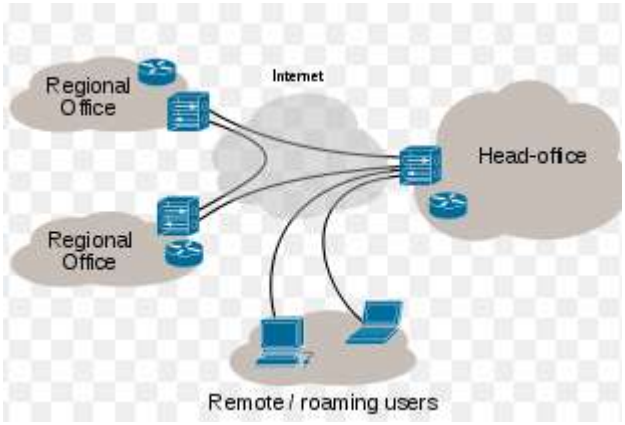
1.7-rasm. Mijoz konfiguratsiyasi (client.ovpn):

1. Tizimni ishga tushirish:
   - Server: openvpn --config server.ovpn
   - Client: openvpn --config client.ovpn

2. Aloqa testini o‘tkazish: ping buyrug‘i orqali VPN tunnel orqali aloqaning mavjudligi sinovdan o‘tkaziladi.

Latin American Journal of Education
www.lajoe.org

2.5. OpenVPN’da xavfsizlikni ta’minlash mexanizmlari



1.8-rasm. OpenVPN’da xavfsizlikni ta’minlash mexanizmlari

OpenVPN yuqori darajadagi xavfsizlikni quyidagi texnologiyalar orqali ta’minlaydi:

1. Shifrlash algoritmlari: AES-256, RSA-4096, Blowfish, ChaCha20-Poly1305.
2. Autentifikatsiya: foydalanuvchi sertifikatlari va parollar orqali amalga oshiriladi.
3. HMAC (Hash-based Message Authentication Code): uzatilgan paketlarning butunligini tekshiradi.
4. TLS-auth: MITM (Man-in-the-Middle) hujumlarini oldini oladi.
5. Re-keying: har bir sessiyada kalitlar avtomatik yangilanadi.

Ushbu mexanizmlar OpenVPN’ni ko‘plab tijorat VPN yechimlariga nisbatan xavfsizroq qiladi.

OpenVPN arxitekturasining ustunliklari

OpenVPN boshqa VPN protokollariga (PPTP, L2TP, IPSec) nisbatan quyidagi afzalliklarga ega:

– Platformalararo ishlash: turli operatsion tizimlarda ishlaydi.
– Moslashuvchan sozlama: port, protokol, shifrlash turini foydalanuvchi belgilashi mumkin.
– Ochiq manba kodi: har kim tomonidan xavfsizlik tahlili o‘tkazilishi mumkin.
– Kuchli kriptografiya: AES256, RSA va TLS asosidagi himoya.
– Firewall orqali o‘tish: 443-port (HTTPS) orqali o‘tib, tarmoq cheklovlarini chetlab o‘tadi.

XULOSA

Xulosa qilib aytganda, OpenVPN texnologiyasi zamonaviy tarmoq xavfsizligini ta’minlashda muhim o‘rin tutadi. Ushbu tizim SSL/TLS protokollari asosida ishlagan holda foydalanuvchilar o‘rtasida shifrlangan virtual tunnel hosil qiladi. Natijada ma’lumotlarning maxfiyligi, yaxlitligi va xavfsizligi ta’minlanadi. OpenVPN’ning ochiq manba kodi, kuchli kriptografik algoritmlardan foydalanishi hamda turli operatsion tizimlarda ishlash imkoniyati uni keng qo‘llaniladigan VPN texnologiyalaridan biriga aylantirgan. Shuningdek, tizimning moslashuvchan

Latin American Journal of Education
www.lajoe.org

konfiguratsiya imkoniyatlari uni korporativ tarmoqlar, masofaviy ulanishlar hamda axborot xavfsizligi sohasida samarali qo‘llash imkonini beradi. Shu sababli OpenVPN zamonaviy kiberxavfsizlik infratuzilmasining muhim elementlaridan biri hisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

1. OpenVPN Inc. OpenVPN Documentation. https://openvpn.net
2. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education, 2017.
3. Kurose J., Ross K. Computer Networking: A Top-Down Approach. Pearson, 2021.
4. Tanenbaum A., Wetherall D. Computer Networks. Pearson, 2019.
5. Rescorla E. SSL and TLS: Designing and Building Secure Systems. Addison-Wesley, 2018.
6. RFC 5246. The Transport Layer Security (TLS) Protocol. IETF.