pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

METHODS AND ALGORITHMS FOR BUILDING SECURE VIRTUAL PRIVATE NETWORKS

Muratov Murat Xamroyevich[1], Odinayev Jonibek Khoshim ugli[2]
[1]Master's student, 2nd year, "University of Management and Future Technologies," Tashkent, 100208, Uzbekistan
[2]Master's student, 2nd year, "University of Management and Future Technologies," Tashkent, 100208, Uzbekistan
Corresponding author: murat.muratov_2026@list.ru; Tel.: +99890-017-73-17

Abstract: This article analyzes the fundamental concepts of Virtual Private Network (VPN) technology, its construction methods, and algorithms ensuring security. VPN technology is used to provide encrypted and protected connections over the Internet. The article discusses various VPN protocols such as PPTP, L2TP, OpenVPN, and WireGuard, as well as encryption algorithms including AES, Blowfish, and ChaCha20. The security and efficiency aspects of VPN technologies are analyzed, and modern solutions are recommended.

Keywords: VPN, encryption, security, algorithms, OpenVPN, WireGuard, authentication.

Introduction

Secure Virtual Private Networks (VPNs) are a tool that provides an introduction to VPN technology, its operating principles, advantages, and the security measures it offers. This section discusses the overall purpose of VPN technology and how it helps protect a user's online activity. Secure Virtual Private Networks (VPNs) are an essential tool for modern Internet security. Data transmitted over the Internet is often at risk, especially when using public Wi-Fi networks. A VPN is a technology that helps users protect their Internet connections, anonymize online activities, and ensure online security.

The operation of a VPN primarily involves creating a secure, encrypted tunnel between the user's device and the VPN server. Data transmitted through this tunnel is encrypted so that it cannot be read externally. Thus, when a user connects to the Internet via a VPN, their real IP address is hidden, and online activity remains confidential.

VPN technology also allows users to bypass geographical restrictions, censorship, or blocked websites. For example, some content may only be available in specific regions; with a VPN, a user can connect to a server in another region and access content available there.

This technology is also used by companies to provide secure remote network access for their employees. A VPN is primarily a tool necessary for protecting a user's network activity and enhancing security, playing a crucial role in encryption, anonymity, and secure communication.

Main Part

VPN technology allows users to ensure confidential and secure connections over a public Internet network. It consists of the following main components:

- **Tunnel creation:** Establishing an encrypted channel to securely exchange data over the network.
- **Encryption algorithms:** Technologies used to protect information.
- **Authorization and authentication:** Verifying and granting access to VPN users.

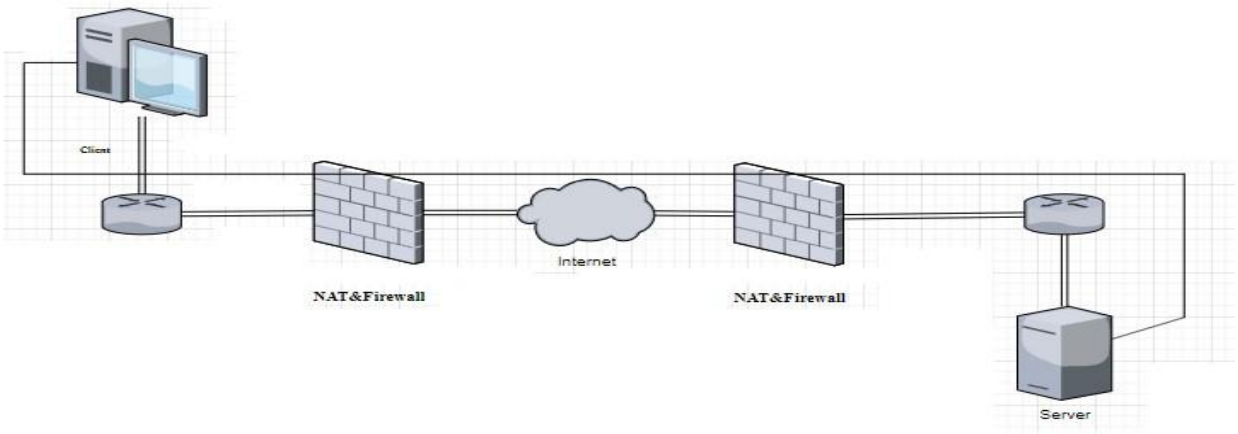
A VPN creates a local network among multiple computers. These computers may either be part of the same local network or located far apart via the Internet. They can also connect through specialized multimedia channels, such as wireless communication, satellite links, or switched networks.

The VPN is provided with additional protection to make the virtual network private. Network traffic passing through a VPN is usually referred to as internal tunnel traffic, while other network traffic remains outside the tunnel.

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

Figure 1.1 illustrates how network traffic traditionally passes through network segments and the Internet. In this case, the traffic is relatively open for inspection and analysis; however, secured protocols such as HTTPS and SSH are less vulnerable to attackers.

1.1-picture

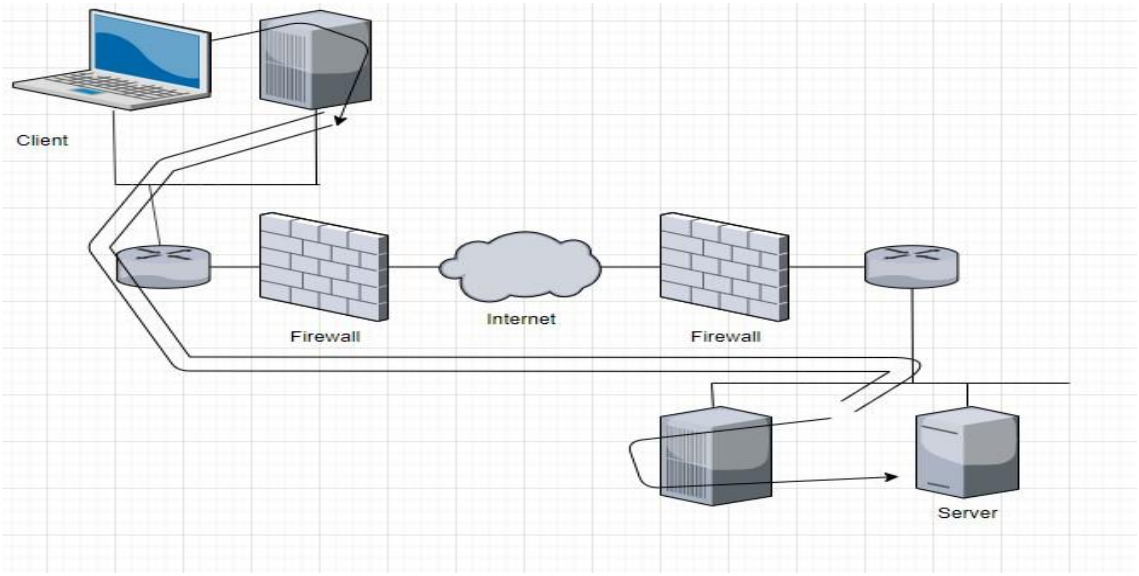


Here, attackers could still see through which type of connection a particular computer is connected to which server. However, when a VPN is used, the traffic inside the tunnel is no longer identifiable. Traffic within a VPN can be arbitrary, meaning that it is hidden regardless of whether it is transmitted over a local or global network.

Even if the VPN is routed over the Internet (as shown in Figure 1.1), devices along the network path can only see VPN traffic; these devices cannot determine what is happening inside the private tunnel or what data is being transmitted. While secured protocols such as HTTPS and SSH remain protected within a VPN from other VPN users, there is still traffic outside the tunnel that is not additionally visible.

A VPN not only encrypts traffic inside the tunnel but also conceals and protects separate data streams from individuals outside the tunnel.

1.2-



picture

Figure 1.2 shows the strengths of VPN technologies as well as one of the major threats.

VPN tunnels pass through routers and firewalls from both sides. Therefore, if special measures

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

are not taken to monitor VPN traffic, all network traffic passing through the VPN tunnel bypasses the usual network security.

Most VPN solutions use certain types of encryption and authentication. VPN encryption makes it impossible for third parties monitoring the network traffic to decode and analyze it, thereby protecting confidential information.

Authentication consists of two main components:

- **User and system authentication** – this is the process of verifying the system and user connecting to the authorized server. Such authentication is usually implemented using certificates or a username and password combination. Additionally, specific rules may be agreed upon, such as rules for certain routes, firewall policies, or other scripts and utilities. These are typically unique for each VPN connection, but if OpenVPN is used, they can be customized.
- **Additional protection of traffic flow** – each transmitted packet is verified using a signing method. Before encrypting VPN packets, each system checks that their signatures are correct. Authenticating encrypted packets allows the system to avoid encrypting packets that do not comply with authentication rules, saving processing time.

This type of authentication prevents potential Denial of Service (DoS) attacks and also mitigates Man-in-the-Middle (MITM) attacks, provided the signing keys are stored securely.

2.1 VPN Types

There are many VPN products on the market, offered both commercially and as open-source solutions. All VPN products can be categorized into the following four types:

- VPNs based on the PPTP protocol
- VPNs based on the IPSec protocol
- SSL-based VPNs
- OpenVPN

OpenVPN is also considered an SSL-based VPN because it uses an SSL- or TLS-like protocol to establish a secure connection. However, OpenVPN is distinguished from other SSL-based VPN solutions, so it is classified as a separate category.

2.1.1 PPTP

One of the VPN protocols is the Point-to-Point Tunneling Protocol (PPTP), developed by Microsoft and Ascend in 1999. The PPTP protocol is officially registered as RFC 263, and the PPTP client has been included in the Windows operating system since 1995 and is now available on most operating systems.

Currently, PPTP is considered an insecure protocol because the reliability of the secured connection depends directly on the security mechanisms it uses. For example, if a weak password is used during authentication, the VPN connection becomes unprotected. Most PPTP configurations use the MSCHAPv2 protocol, which provides password encryption.

To enhance PPTP security, X.509 certificates are used. These certificates protect the PPTP connection, but not all PPTP client software supports the EAP-TLS protocol, which is necessary for using X.509 certificates.

PPTP uses two channels:

- **Control channel** – used for connection setup.
- **Data channel** – used for data transmission.

The control channel is established via a TCP port, while the data channel uses the General Routing Encapsulation (GRE) protocol, which is an IP-based protocol.

PPTP client software is available on almost all operating systems, including Windows, Linux, Unix, iOS, and Android.

2.1.2 IPSec

IPSec (Internet Protocol Security) is officially recognized by IEEE/IETF as a standard for IP security. It is registered as RFC 2411 and included in the IPv6 standard. IPSec operates at the second and third layers of the OSI model. It incorporates the concept of a Security Policy,

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

making it highly flexible and powerful, although configuration and troubleshooting can be more complex.

The security policy allows an administrator to encrypt traffic between two network nodes based on the following parameters:

- Source IP address and destination IP address
- Source and destination TCP or UDP ports

IPSec can be configured to secure VPN connections using pre-shared keys or certificates. It supports mechanisms such as X.509 certificates, one-time passwords (OTP), and username/password authentication protocols.

IPSec operates in two modes:

- **Tunnel mode**
- **Transport mode**

Transport mode is often used in conjunction with L2TP (Layer 2 Tunneling Protocol), as L2TP provides user authentication. IPSec client software is integrated into operating systems and usually works with L2TP. However, it is also possible to configure connections using IPSec alone. On Microsoft Windows, IPSec VPN connections typically operate with L2TP, but this setting can be modified or disabled.

IPSec uses two channels:

- **Control channel** – used to establish the connection and operates via UDP.
- **Data channel** – uses the Encapsulating Security Payload (ESP) protocol, which is an IP-based protocol.

The integrity of IPSec packets is ensured through HMAC (Hashed Message Authentication Code), the same method used by OpenVPN.

One of the main drawbacks of IPSec is that different vendors have implemented additional extensions, which can make interoperability between solutions from different vendors difficult. IPSec software is included not only in operating systems but also in firewalls, routers, and firmware.

2.1.3 SSL-Based VPN

An SSL-based VPN is a VPN technology based on SSL and TLS protocols. SSL-based VPNs are often referred to as clientless VPNs or Web VPNs, although some providers offer dedicated client software, such as Cisco AnyConnect and Microsoft SSTP.

SSL-based VPNs use the same network protocol as HTTPS (just like secure websites), while OpenVPN uses a special format to encrypt and sign data traffic. This is the main reason why OpenVPN is classified as a separate VPN category.

There is no strictly defined standard for SSL-based VPNs, but in most cases, SSL and TLS protocols are used to establish and secure the connection.

Connections are commonly secured using:

- Certificates
- One-time passwords (OTP)
- Username and password authentication

SSL-based VPNs closely resemble the technologies used for secure websites (HTTPS) and often use the same protocol and port (TCP port 443).

Although SSL-based VPNs are often called web- or client-based VPNs, some providers enhance VPN connections using browser plugins or ActiveX controls. However, this approach may not be compatible with certain browsers or operating systems, which can create limitations for some users.

2.1.4 OpenVPN

OpenVPN is an SSL-based VPN because it uses SSL and TLS protocols to establish a secure connection. However, OpenVPN combines HMAC (Hashed Message Authentication Code) and hash algorithms to ensure packet integrity.

OpenVPN supports:

pISSN:2349-5707 Volume:12,Issue 11,November-2025 eISSN:2349-5715

- Pre-shared keys
- Authentication via certificates

These features are often not available in other SSL-based VPN technologies.

Additionally, OpenVPN uses TUN or TAP devices as virtual network adapters. This adapter serves as an interface between the OpenVPN client software and the operating system.

Any operating system that supports TUN or TAP devices can work with OpenVPN. Currently, these systems include:

- Linux, FreeBSD, OpenBSD, NetBSD, Solaris, AIX, Windows, macOS, iOS, and Android

On all these platforms, the OpenVPN client software must be installed, which differentiates it from Web-VPN or clientless VPN technologies that run through a browser.

The OpenVPN protocol is not defined in an RFC standard; however, being open-source software, it is considered an open and transparent protocol.

Because OpenVPN is open-source:

- The security level is high since the code is continuously reviewed by multiple individuals.
- The likelihood of hidden “backdoors” is very low.

OpenVPN uses two channels:

- **Control channel** – encrypted and protected using SSL/TLS protocols
- **Data channel** – protected using a specialized encryption protocol

However, all network traffic passes through a single UDP or TCP connection. The standard protocol and port for OpenVPN are UDP, port 1194.

Conclusion

Creating secure Virtual Private Networks is of significant importance for modern information security. Through VPN technologies and their algorithms, encrypted and secure communication can be ensured. The choice of protocol and algorithms may vary depending on the requirements, but modern technologies such as OpenVPN and WireGuard provide high security and efficiency.

References:

1. Stallings, W. (2017). Cryptography and Network Security: Principles and Practice. Pearson.
2. Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography Engineering: Design Principles and Practical Applications. Wiley.
3. Kurose, J. F., & Ross, K. W. (2021). Computer Networking: A Top-Down Approach. Pearson.
4. RFC 5246 - The Transport Layer Security (TLS) Protocol.
5. RFC 8410 - Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure.
6. OpenVPN Documentation - https://openvpn.net
7. WireGuard Documentation - https://www.wireguard.com