**TEZE ZA BSC**

* **UVOD:**

[**https://www.cert.rs/files/shares/VPN%20za%20mala%20i%20srednja%20preduzeca.pdf**](https://www.cert.rs/files/shares/VPN%20za%20mala%20i%20srednja%20preduzeca.pdf)

[**https://rti.etf.bg.ac.rs/rti/ir4roi/Prezentacije/02%20-%20VPN,%20MPLS,%20IPsec.pdf**](https://rti.etf.bg.ac.rs/rti/ir4roi/Prezentacije/02%20-%20VPN,%20MPLS,%20IPsec.pdf)

* **Vpn tehnologije:**

There are three types of VPN:

* remote access
* intranet-based site-to-site
* extranet-based site-to-site.[[10]](https://en.wikipedia.org/wiki/Virtual_private_network#cite_note-:1-10)

While individual users most frequently interact with remote access VPNs, businesses make use of site-to-site VPNs more often.[[10]](https://en.wikipedia.org/wiki/Virtual_private_network#cite_note-:1-10)

VPNs can be characterized as *host-to-network* or *remote access* by connecting a single computer to a network or as *site-to-site* for connecting two networks. In a corporate setting, remote-access VPNs allow employees to access the company's [intranet](https://en.wikipedia.org/wiki/Intranet) from outside the office. Site-to-site VPNs allow collaborators in geographically disparate offices to share the same virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar intermediate network, such as two [IPv6](https://en.wikipedia.org/wiki/IPv6) networks connected over an [IPv4](https://en.wikipedia.org/wiki/IPv4) network.[[11]](https://en.wikipedia.org/wiki/Virtual_private_network#cite_note-11)

VPN systems may be classified by:

* the tunneling protocol used to [tunnel](https://en.wikipedia.org/wiki/IP_tunnel) the traffic
* the tunnel's termination point location, e.g., on the customer [edge](https://en.wikipedia.org/wiki/Edge_device) or network-provider edge
* the type of topology of connections, such as site-to-site or network-to-network
* the levels of security provided
* the [OSI layer](https://en.wikipedia.org/wiki/OSI_model) they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
* the number of simultaneous connections
* **Kriterijumi odabira:**

[**https://en.wikipedia.org/wiki/Comparison\_of\_virtual\_private\_network\_services**](https://en.wikipedia.org/wiki/Comparison_of_virtual_private_network_services)

* **Sigurnosni mehanizmi:**

(Uvod **wiki**) A wide variety of (typically commercial) entities provide "VPNs" for all kinds of purposes, but depending on the provider and the application, they often do not create a true "private network" with anything meaningful on the local network. Nonetheless the term is increasingly prevalent. The general public has come to mainly use the term **VPN service** or just **VPN** specifically for a commercially marketed product or service that uses a VPN protocol to tunnel the user's internet traffic so an IP address of the service provider's server appears to the public to be the IP address of the user. Depending on the features properly implemented, the user's traffic, location and/or real IP may be hidden from the public, thereby providing the desired internet access features offered, such as [Internet censorship](https://en.wikipedia.org/wiki/Internet_censorship) circumvention, IP-address masking (not to be confused with anonymity), and [geo-unblocking](https://en.wikipedia.org/wiki/Geo-blocking). They tunnel the user's internet traffic securely only between the public internet and the user's device and there is typically no way for a user's devices connected to the same "VPN" to see each other. These VPNs can be based on typical VPN protocols or more camouflaged VPN implementations like [SoftEther VPN](https://en.wikipedia.org/wiki/SoftEther_VPN" \o "SoftEther VPN), but proxy protocols like [Shadowsocks](https://en.wikipedia.org/wiki/Shadowsocks" \o "Shadowsocks) are used as well.[[52]](https://en.wikipedia.org/wiki/Virtual_private_network#cite_note-52) These VPNs are usually marketed as privacy protection services.

On the client side, a common VPN setup is by design not a conventional VPN, but does typically use the operating system's VPN interfaces to capture a user's data to send through. This include virtual network adapters on computer OSes and specialized "VPN" interfaces on mobile operating systems. A less common alternative is to provide a [SOCKS](https://en.wikipedia.org/wiki/SOCKS) proxy interface.

Users must consider that when the transmitted content is not encrypted *before* entering a VPN, that data is visible at the receiving endpoint (usually the public VPN provider's site) regardless of whether the VPN tunnel *wrapper* itself is encrypted for the inter-node transport. The *only* secure VPN is where the participants have oversight at *both* ends of the entire data path, or the content is encrypted before it enters the tunnel provider.

VPNs cannot make online connections completely anonymous, but they can usually increase privacy and security. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using [tunneling protocols](https://en.wikipedia.org/wiki/Tunneling_protocol) and [encryption](https://en.wikipedia.org/wiki/Encryption_software) techniques.

The VPN security model provides:

* [confidentiality](https://en.wikipedia.org/wiki/Information_security#Confidentiality) such that even if the network traffic is sniffed at the packet level, an attacker would see only [encrypted data](https://en.wikipedia.org/wiki/Encryption)
* sender [authentication](https://en.wikipedia.org/wiki/Authentication) to prevent unauthorized users from accessing the VPN
* message [integrity](https://en.wikipedia.org/wiki/Data_integrity) to detect any instances of tampering with transmitted messages.

Secure VPN protocols include the following:

* [Internet Protocol Security](https://en.wikipedia.org/wiki/Internet_Protocol_Security) ([IPsec](https://en.wikipedia.org/wiki/Internet_Protocol_Security" \o "Internet Protocol Security)) uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
* [Transport Layer Security](https://en.wikipedia.org/wiki/Transport_Layer_Security) ([SSL/TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security)) can tunnel an entire network's traffic or secure an individual connection. A number of vendors provide remote-access VPN capabilities through SSL. An SSL VPN can connect from locations where IPsec runs into trouble with [Network Address Translation](https://en.wikipedia.org/wiki/Network_Address_Translation) and firewall rules.
* [Datagram Transport Layer Security](https://en.wikipedia.org/wiki/Datagram_Transport_Layer_Security) ([DTLS](https://en.wikipedia.org/wiki/Datagram_Transport_Layer_Security)) – used in Cisco [AnyConnect](https://en.wikipedia.org/wiki/AnyConnect" \o "AnyConnect) VPN and in [OpenConnect](https://en.wikipedia.org/wiki/OpenConnect" \o "OpenConnect) VPN to solve the issues [SSL/TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) has with tunneling over [TCP](https://en.wikipedia.org/wiki/Transmission_Control_Protocol) (tunneling TCP over TCP can lead to big delays and connection aborts).
* [Microsoft Point-to-Point Encryption](https://en.wikipedia.org/wiki/Microsoft_Point-to-Point_Encryption) ([MPPE](https://en.wikipedia.org/wiki/Microsoft_Point-to-Point_Encryption)) works with the [Point-to-Point Tunneling Protocol](https://en.wikipedia.org/wiki/Point-to-Point_Tunneling_Protocol) and in several compatible implementations on other platforms.
* Microsoft [Secure Socket Tunneling Protocol](https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol) ([SSTP](https://en.wikipedia.org/wiki/Secure_Socket_Tunneling_Protocol)) tunnels [Point-to-Point Protocol](https://en.wikipedia.org/wiki/Point-to-Point_Protocol) (PPP) or Layer 2 Tunneling Protocol traffic through an [SSL/TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) channel
* Multi Path Virtual Private Network (MPVPN). Ragula Systems Development Company owns the registered [trademark](https://en.wikipedia.org/wiki/Trademark) "MPVPN".
* Secure Shell (SSH) VPN – [OpenSSH](https://en.wikipedia.org/wiki/OpenSSH" \o "OpenSSH) offers VPN tunneling (distinct from [port forwarding](https://en.wikipedia.org/wiki/Port_forwarding)) to secure remote connections to a network or to inter-network links. OpenSSH server provides a limited number of concurrent tunnels. The VPN feature itself does not support personal authentication.
* [WireGuard](https://en.wikipedia.org/wiki/WireGuard) is a protocol. In 2020, WireGuard support was added to both the Linux and Android kernels, opening it up to adoption by VPN providers. By default, WireGuard utilizes [Curve25519](https://en.wikipedia.org/wiki/Curve25519) for [key exchange](https://en.wikipedia.org/wiki/Key_exchange) and [ChaCha20](https://en.wikipedia.org/wiki/ChaCha20) for encryption, but also includes the ability to pre-share a symmetric key between the client and server. Almost all commercial VPNs adopted this protocol as the default one.

Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use [passwords](https://en.wikipedia.org/wiki/Passwords), [biometrics](https://en.wikipedia.org/wiki/Biometrics), [two-factor authentication](https://en.wikipedia.org/wiki/Two-factor_authentication) or other [cryptographic](https://en.wikipedia.org/wiki/Cryptographic) methods. Network-to-network tunnels often use passwords or [digital certificates](https://en.wikipedia.org/wiki/Digital_certificates). They permanently store the key to allow the tunnel to establish automatically, without intervention from the administrator

https://www.barracuda.com/resources/Barracuda\_SSLVPN\_WP\_VPN\_Technologies

* Ipsec:

IPsec, or IP security, is a standard for encrypting and/or authenticating IP packets at the network layer. IPsec has a set of cryptographic protocols for two purposes: securing network packets and exchanging encryption keys.

<http://www.esi.ftn.uns.ac.rs/images/predmet-orm2/2017/07.pdf>

[https://www.calyptix.com/research-2/ssl-vpn-and-ipsec-vpn-how-they-work/#:~:text=IPsec%20VPN%20is%20one%20of,than%20just%20a%20single%20device).&text=IPsec%20VPNs%20come%20in%20two%20types%3A%20tunnel%20mode%20and%20transport%20mode.](https://www.calyptix.com/research-2/ssl-vpn-and-ipsec-vpn-how-they-work/%23:~:text=IPsec%20VPN%20is%20one%20of,than%20just%20a%20single%20device).&text=IPsec%20VPNs%20come%20in%20two%20types%3A%20tunnel%20mode%20and%20transport%20mode.)

Deciding between IPsec and SSL/TLS for a given scenario can be complicated. One consideration is that SSL/TLS can work through a NAT-based firewall; IPsec cannot, but both protocols work through firewalls that do not translate addresses.

IPsec encrypts all IP traffic that flows between two computers. SSL/TLS is specific to an application. SSL/TLS uses expensive asymmetric encryption functions to establish a connection, and more efficient symmetric encryption functions to secure a running session.

* **Zaključak:**

VPN (virtualna privatna mreža) je postao nužnost u ovom dobu online praćenja, pogotovo ako želite zaštititi svoju privatnost i osigurati vaše podatke na računaru koji mogu biti izloženi putem raznih spywarea, malwarea itd.

VPN stvara privatni „tunel“, zatvorenu vezu koju ne može dekriptirati neka druga strana, kao što su vaš provajder (ISP) ili, uopšteno, neke web stranice. To znači da se podaci koje šaljete više ne mogu presresti i/ili ukrasti.

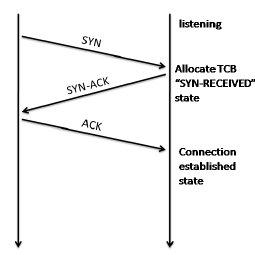
-ISO/OSI TCP

Komunikacionim protokolom se označava skup pravila i procedura koji kontroliše tok komunikacije između serijski spregnutih uređaja u okviru računarske mreže. Posredstvom komunikacionih protokola se obezbeđuje uspešna interakcija između udaljenih procesa [1].

OSI (eng. Open Systems Interconnection Basic Reference Model) model je model koji deli arhitekturu mreže u sedam logičkih nivoa (Tabela 3.1), daje spisak funkcija, servisa i protokola koji funkcionišu na svakom od nivoa. Jedan od najvećih razloga zašto je uveden referentni model je da se izvrši standardizacija samih protokola.

TCP (eng. Transfer Control Protocol) je jedan od glavnih protokola za razmjenu podataka na internetu. Nastao je u početnoj implementaciji mreže u kojoj je dopunio internet protokol (IP). S toga se cijeli paket obično naziva TCP/IP. TCP pripada četvrtom nivou OSI referentnog modela. Pruža pouzdanu i uređenu isporuku toka okteta (bajtova) između aplikacija koje se izvode na hostovima i komuniciraju putem IP mreže [2].

TCP je connection-oriented protokol, zahtjeva uspostavljanje veze između klijenta i servera prije slanja podataka. Veza se uspostvlja tako što klijent i server urade „rukovanje“, odnosno razmjene tri poruke sa podešenim odgovarajućim kontrolnim bitima (Slika 3.1.1).



*Slika 3.1.1 Uspostavljanje veze koristeći TCP protokol*