Univerzita Pardubice
Fakulta Ekonomicko-správní
Ústav systémového inženýrství a informatiky

Využití VPN v moderní síťové infrastruktuře

Jakub Bažant

Bakalářská práce
2020

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2019/2020

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Jakub Bažant**
Osobní číslo:	**E16935**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Téma práce:	**Využití VPN v moderní síťové infrastruktuře**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je přinést ucelený pohled na současné technologie realizace VPN a jejich využití v moderní síťové infrastruktuře.

Osnova:
1. Prostudování současných technologií realizace VPN.
2. Stanovení klíčových atributů pro hodnocení využití ve vybraných situacích.
3. Vyhodnocení a závěrečné shrnutí.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. 2. aktualiz. vyd. Praha : Computer Press, 2003. ISBN: 80-7226-849-X.

OLIFER, Natalia, OLIFER, Victor. Computer networks: principles, technologies and protocols for network design. Chichester : John Wiley, 2006. ISBN: 0-470-86982-8.

PUŽMANOVÁ, Rita. TCP/IP v kostce. České Budějovice : Kopp, 2004. ISBN 80-7232-236-2.

SOSINSKY, Barrie A. Mistrovství – počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Brno : Computer Press, 2010. ISBN: 978-80-251-3363-7.

Vedoucí bakalářské práce: **RNDr. Ing. Oldřich Horák, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **2. září 2019**
Termín odevzdání bakalářské práce: **30. dubna 2020**

L.S.

doc. Ing. Romana Provazníková, Ph.D.
děkanka

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 2. září 2019

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval/a samostatně. Veškeré literární prameny a informace, které jsem v práci využil/a, jsou uvedeny v seznamu použité literatury.

Byl/a jsem seznámen/a s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 10. 8. 2020 Jakub Bažant

PODĚKOVÁNÍ:
Děkuji svému vedoucímu práce panu RNDr. Ing. Oldřichu Horákovi, Ph.D., za metodickou pomoc, kterou mi poskytl při zpracování a za podnětné připomínky k formě a obsahu této bakalářské práce.

ANOTACE

Cílem této bakalářské práce je přiblížit současné technologie Virtuálních privátních sítí, stanovení modelových situací pro jejich použití a na základě zvolených atributů, vyhodnocení v jednotlivých situacích. Do rozhodování byly zařazeny technologie od OpenVPN, SoftEther a WireGuard.

KLÍČOVÁ SLOVA

OpenVPN, rozhodování, SoftEther, Virtuální privátní sítě, VPN, WireGuard

TITLE

Usage of VPN in modern networks

ANNOTATION

The goal of this bachelor thesis is to bring current technologies of Virtual private networks to wider audience, establishing model situations for their selection and after selecting key attributes determine their best use in theoretical situations. OpenVPN, SoftEther and WireGuard were considered in this decision-making.

KEYWORDS

OpenVPN, decision-making, SoftEther, Virtual private networks, VPN, WireGuard

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

3DES Triple Data Encryption Standard

AES Advanced Encryption Standard

AHP Analytic Hierarchy Process

ATM Asynchronous Transfer Mode

DDNS Dynamic Domain Name System

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

ESP Encapsulating Security Payload

GRE Generic Routing Encapsulation

IP Internet Protocol

IPsec Internet Protocol Security

L2TP Layer 2 Tunneling Protocol

LAN Local Area Network

NAS Network Attached Storage

NAT Network Address Translation

PKI Public Key Infrastructure

PPP Point-to-Point Protocol

PPTP Point-to-Point Tunneling Protocol

RDP Remote Desktop Protocol

SSL Secure Sockets Layer

SSTP Secure Socket Tunneling Protocol

TCP Transmission Control Protocol

TLS Transport Layer Security

UDP User Datagram Protocol

VNC Virtual Network Computing

VPN Virtual Private Network

VPNC Virtual Private Network Consorcium

VPS Virtual Private Server

WAN Wide Area Network

Úvod

V dnešním moderním světě je potřeba, aby spolu lidé a organizace komunikovali i na obrovské vzdálenosti. Zároveň je důležité, aby tato komunikace byla zabezpečená. Zabezpečené připojení lze efektivně vytvořit v lokálních sítích, ale efektivita klesá, pokud je spojení potřeba rozšířit do sítě WAN (např. internet). Před VPN se takovéto spojení muselo řešit soukromou vysokokapacitní linkou, což bylo velice nákladné řešení. VPN nám pomohly tento problém jednoduše vyřešit.

Jak prozrazuje samotný název, jedná se o virtualizované propojení sítí. VPN pouze vytváří dojem, že se jedná o soukromou linku dané organizace, ve skutečnosti se tvoří na linkách veřejných síťových poskytovatelů. To umožnuje minimalizovat náklady na zřízení linky, její provoz, zabezpečení a další výhody.

Účelem této práce je prostudování současných technologií VPN, stanovení modelových situací, které reflektují současné trendy, řešení těchto situací pomocí VPN, stanovení možných kritérií pro zhodnocení a vyhodnocení na jejich základě.

1 ÚVOD DO VPN

Virtuální privátní sítě neboli VPN (Virtual Private Networks), jsou základním prvkem zabezpečených datových spojů a bezpečné komunikace mezi sítěmi.

Definice VPN dle konsorcia VPNC:

„Virtual Private Network (VPN) je privátní datová síť, která využívá veřejné telekomunikační infrastruktury a zajišťuje soukromí pomocí tunelovacích protokolů a bezpečnostních procedur.“ [5]

Další možná definice:

„Neveřejná páteřní síť využívající veřejnou (sdílenou) komunikační infrastrukturu, kterou může být Internet, veřejná síť na bázi protokolu IP, veřejná síť ATM nebo Frame Relay.“ [3]

VPN spojení může být vytvořeno na základě příslušného softwaru, hardwaru nebo kombinací obojího. Takto vzniklé virtuální okruhy umožnují propojit jednotlivé uživatele nebo lokality uzavřeným spojením. Jednotlivé spojení mezi sítěmi je nutno autentizovat a autorizovat.

Pro vytvoření VPN sítě se využívá celá řada protokolů. Některé protokoly zabezpečují data tím, že je kryptograficky zašifrují, jiné se pak starají o zapouzdření dat, které je pro VPN nezbytné. Tyto protokoly doplňují ještě další, které se starají o přenos dat VPN linkou. Hlavní výhodou privátních sítí je jejich izolace od veřejné sítě, ať již virtuální, nebo fyzická. [2][3][4]

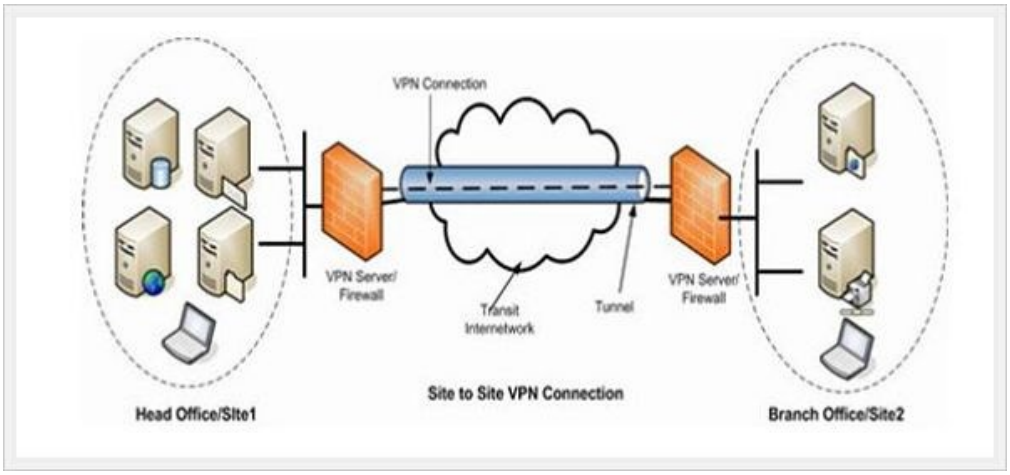
VPN lze chápat jako jednu síť, ve které jsou zdánlivě všichni uživatelé připojeni lokálně a všechny prostředky, které jsou jinak dostupné pouze na lokální úrovni, jsou sdíleny.

Většina VPN je založena na virtualizaci druhé nebo třetí vrstvy. V případě druhé vrstvy dochází k virtualizaci switche, na vrstvě třetí naopak přepínače.[2]

1.1 Typy sítí VPN

Site to Site

Site to Site je spojení mezi dvěma vzdálenými sítěmi LAN skrze WAN, nebo propojení dvou intranetů v rámci organizace nebo mezi různými organizacemi. Tento typ VPN může být snadnou kořistí útočníků, z důvodu statické adresace. Je tedy potřeba klást maximální požadavky na autentizaci.[3][4]

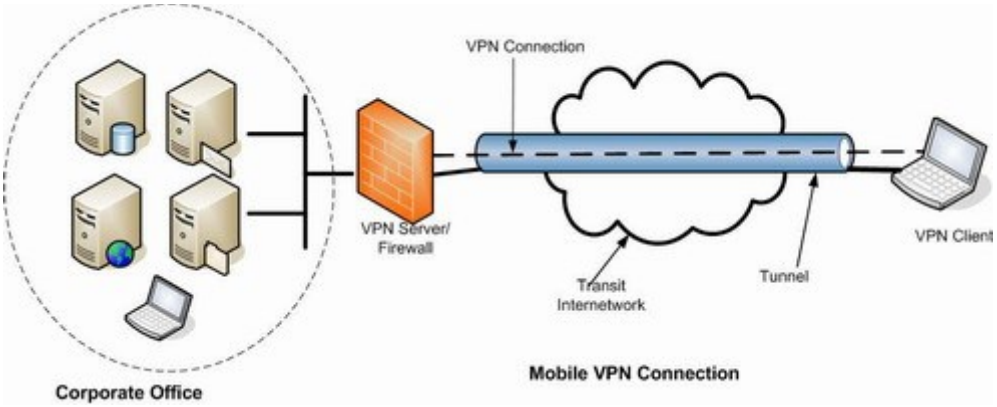


Obrázek 1: Site to Site

Zdroj: [6]

Remote access

Neboli také Client to Site. Přechodná spojení mezi klientem a serverem, nebo sítí, pro přístup uživatele do intranetu nebo v kombinaci s připojením na vzdálenou plochu skrze WAN. Brána VPN v tomto případě musí vykonávat funkci DHCP a DNS. Zde je potřeba klást nároky na autentizaci uživatelů, kteří se můžou připojit prakticky odkudkoliv.[3][4]



Obrázek 2: Client to Site

Zdroj: [6]

1.2 Adresace ve VPN

Brány VPN mohou ukončovat velké množství tunelů od vzdálených stanic. Z toho vyplývá, že je potřeba řešit i přidělování adres těmto zařízením. Existuje několik možností, jak toto přidělování zajistit. Většina bran podporuje více možných metod přidělování adres.

- **Statické přidělování adres** – brána VPN nebo autentizační server rezervuje pro každého klienta statickou IP adresu

- **Dynamické přidělování adres –** pro přidělování adres slouží DHCP server, který přiřazuje adresy z množiny adres, podobně jako při připojení v lokální síti.
- **Klientsky definované adresy –** klient si může zadat adresu sám

Adresy mohou náležet buďto do lokální podsítě, či je možné vytvořit virtuální podsíť jen pro účely VPN, vše závisí na velikosti adresového prostoru, který má podniková síť k dispozici.

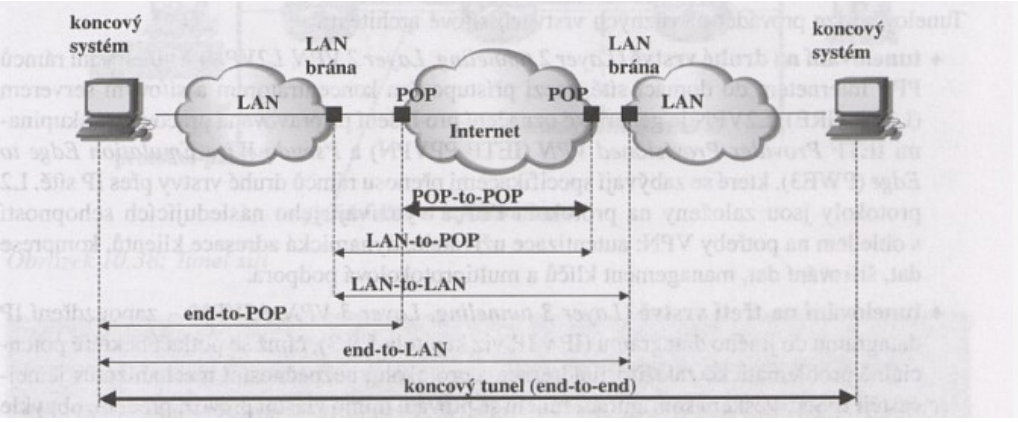
Při adresaci je možné použít i kombinaci způsobů přidělování adres, je však potřeba při nastavování myslet na možnou kolizi. Například uživatel vs. správce: uživateli je adresa přiřazena automaticky, správce bude mít přiřazenou statickou adresu, která bude vyhovovat přístupovým seznamům, které omezují přístup ke kritickým zdrojům a datům. [3]

2 TECHNOLOGIE VYUŽÍVANÉ PRO VPN

2.1 Tunelování

Tunelování se v počítačových sítích nazývá proces zapouzdření, směrování a následné odpouzdření. Tunel je logickou trasou, jeví se však jako Point-to-Point spojení v síti. Veškerá zařízení uvnitř tunelu jsou zdrojovému i cílovému systému skrytá.

VPN se realizuje pomocí tunelů přes veřejnou síť. VPN může být realizováno mnoha způsoby, nejčastěji však přes koncový tunel (end-to-end). V rámci tohoto tunelu může být ještě vnořen další tunel pro zvýšení bezpečnosti, například mezi přístupovými body do internetu (POP-to-POP) viz. Obrázek 3: Typy tunelů



Obrázek 3: Typy tunelů

Zdroj: [3]

Koncové body zajišťují autentizaci, řízení přístupu a dojednávání dalších bezpečnostních služeb.

Tunelování lze zajistit různými transportními protokoly. Některé sady protokolů mají za úkol zapouzdření zašifrovaných paketů, další pak transport dat v síti, která nese tunel. Třetí protokol se může používat v záhlaví šifrovacího protokolu a obsahuje adresní informace paketu. Spojení tunelovacích protokolů (GRE, PPTP, L2TP) s šifrovacím protokolem IPsec se nazývá IPsec transport.

Rozdělené tunelování

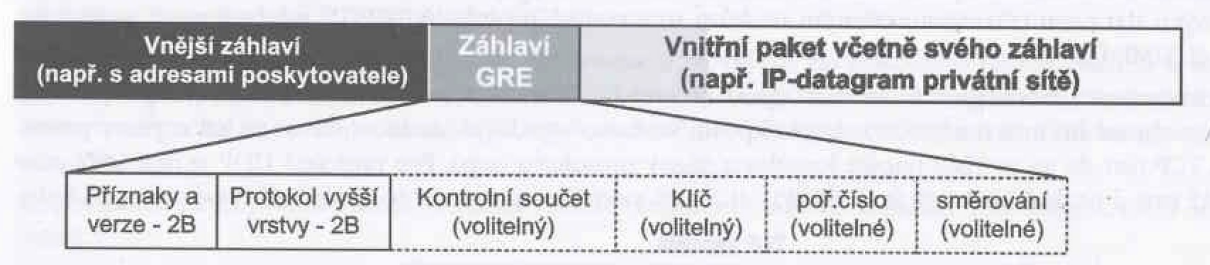
Některé VPN umožnují rozdělené tunelování, tzv. split tunneling. To dovoluje zároveň komunikovat jak přes VPN, tak přes internet. Pokud rozdělené tunelování není umožněno, veškerý uživatelský provoz probíhá přes VPN tunely.

Rozdělené tunelování znemožňuje přístup z internetu do VPN tunelu, takže potencionální útočník z internetu nemá možnost se do zabezpečeného spojení mezi privátními sítěmi dostat. [3]

2.2 Používané protokoly

Protokol GRE

Protokol GRE (Generic Encapsulation Protocol), jak již samotný název napovídá, se používá k zapouzdření paketů přenášených uvnitř VPN tunelu. Směrovač na straně odesílatele obalí pasažérský paket hlavičkou GRE, kde vznikne nový paket, který projde skrze tunel. Na straně příjemce směrovač přečte hlavičku GRE a posílá pasažérský paket k cíli.



Obrázek 4: Zapouzdření GRE

Zdroj: [1]

Jedná se o čistě směrovací protokol, který se ovšem nestará o samotné šifrování. Jsou v něm obsaženy také funkce vícesměrového (multicast) i všesměrového (multicast) vysílání.[1][3][4]

IP sec

IP sec je sada protokolů, které mohou sloužit k tunelování, šifrování i autentizaci. Pro správné fungování IP sec je zapotřebí, aby všechny zařízení na cestě paketu uměli s protokolem pracovat. Jinak by mohlo docházet ke ztrátě paketů, nicméně v současné době je podpora v zařízeních již standardem.

Nejprve IP sec vyžaduje od obou stran budoucího spojení vzájemnou autentizaci a následně šifruje veškerou komunikaci takto vzniklého spojení na základě domluveného algoritmu.

U IP sec můžeme mluvit o dvou režimech. Prvním, a tím jednodušším, je transportní režim, druhým je režim tunelovací. Transportní režim pouze rozšíří IP-datagram o bezpečnostní záhlaví, které specifikuje, jak je datová část zabezpečena. Pro vytvoření tunelu v tomto režimu je zapotřebí doplnit IPsec ještě o nosný protokol. Naproti tomu tunelovací režim vezme celý původní IP-datagram, zabezpečí ho a obalí datagramem novým. V tomto případě poskytuje protokol i zapouzdření a tím vytváří plnohodnotný tunel. [1][4]

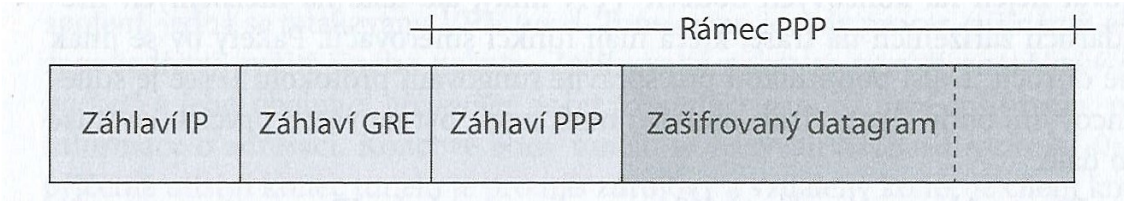
PPP

PPP (Point-to-Point Protocol) je protokol, který nad rozsáhlou sítí vytváří dvoubodové spojení, které podporuje multiprotokolové prostředí (podporuje více různých síťových protokolů na jednom spoji) a tudíž se hodí pro použití v prostředí, kde jsou zařízení různých výrobců. Umožnuje autentizaci, šifrování a kompresi přenášených dat. Protokol PPP dále využívají tunelovací protokoly PPTP a L2TP. [3]

PPTP

PPTP (Point-to-Point Tunneling Protocol) je protokol z dílny Microsoftu, díky němuž je možné vytvářet tunely a vzdáleně tak přenášet PPP data mezi uživateli VPN bránou, nebo VPN koncentrátorem. PPTP umožňuje využít šifrování o síle až 128 bitů, nicméně i přes to je možné tento protokol v dnešní době snadno prolomit.

V rámci PPTP je možné autentizovat pouze uživatele, nikoliv vzdálené počítače, což představuje omezení jeho využití. K zašifrování dat je využíváno heslo uživatele, tedy síla šifry je přímo úměrná kvalitě hesla uživatele. Při procesu zapouzdření je zašifrovaný datagram obalen záhlavím PPP, a navíc také záhlavím protokolů IP a GRE, jak je vidět na Obrázek 5: Paket PPTP



Obrázek 5: Paket PPTP

Zdroj: 48[4]

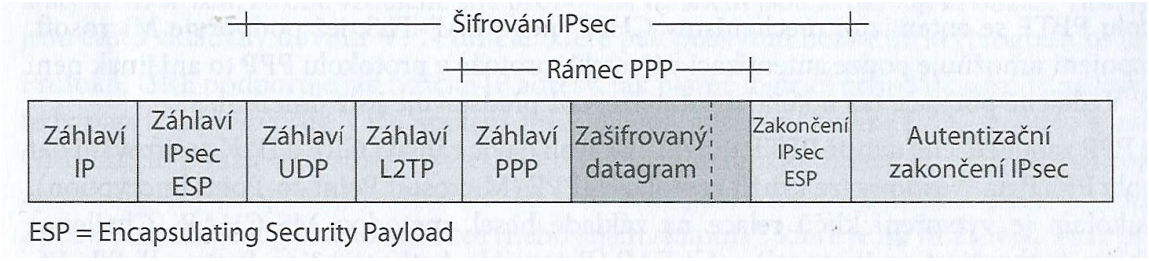
Navzdory všem jeho pozitivním vlastnostem, protokol PPTP není nadále doporučeno používat, z důvodu jeho jednoduchého prolomení. [4][7]

L2TP

L2TP (Layer 2 Tunneling Protocol) jako nástupce staršího protokolu L2F od společnosti Cisco, umožnuje propojení serverů NAS, VPN bran a koncentrátorů. Protokol pro sjednání podmínek tunelu používá spojení UDP. Protože L2TP neposkytuje žádné šifrování dat, používá se typicky ve spojení se sadou protokolů IPsec, takovéto spojení se nazývá L2TP/IPsec.

Využívá se především pro vzdálené připojení uživatelů do podnikové sítě. Při tomto spojení je většinou uživateli přidělena IP adresa z lokální sítě.

Paket L2TP/IPsec je tvořen tak, že k pasažérskému paketu je připojeno záhlaví L2TP a UDP zleva a zakončen IPsec zprava. Poté IPsec celý takto vytvořený nosný paket zašifruje a přidá k němu záhlaví IPsec ESP a autentizační zakončení IPsec. Pro poslání do VPN tunelu je zapotřebí ještě připojit záhlaví IP. Celý paket viz.: Obrázek 6: Zapouzdřený paket L2TP



Obrázek 6: Zapouzdřený paket L2TP

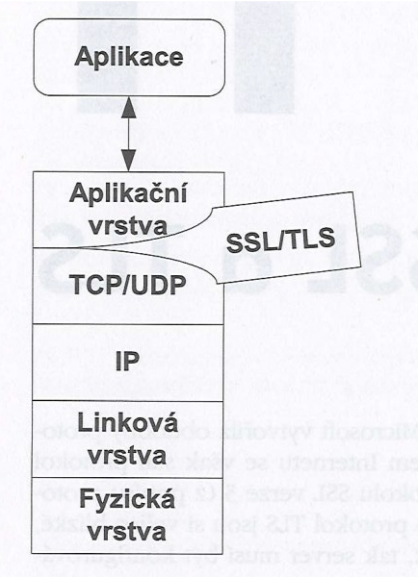
Zdroj: [4]

Moderní síťové prvky a operační systémy, kompatibilní s VPN, podporují i L2TP/IPsec. I proto je nastavení snadné, podobně jako u PPTP, díky čemuž je považován za jeho nástupce. Protože využívá UDP port, je potřeba si dát pozor na blokování tohoto portu firewally. V takovémto případě je potřeba nastavit port forwarding. [3][4][7]

SSL/TLS

SSL (Secure Socket Layer) je protokol založený firmou Netscape. Protokol zakládá bezpečná spojení v rámci transportní vrstvy pro vzdálený přístup. Pokud se spojení nepodaří navázat, žádná data se nepřenesou. Úroveň jeho zabezpečení však není dostačující pro dnešní standardy. Proto byl SSL v3 rozšířen a nahrazen standardem TLS, který je definován normou IETF RFC 5246, a je na rozdíl od SSL otevřeným řešením.

TLS (Transport Layer Security) je soubor kryptografických protokolů typu klient-server, který šifruje i autentizuje data odesílaná aplikací ze serveru. Protokol data předaná aplikační vrstvou nijak nezkoumá, pouze je zabezpečí a předá transportní vrstvě. V rámci TLS komunikace vždy dochází k autentizaci serveru, klient v nejjednodušší podobě být autentizován nemusí. Pro autentizaci klienta je potřeba zavést infrastrukturu veřejných klíčů PKI. TLS se dá uplatnit pro jakýkoliv TCP/IP provoz. Hlavní výhodou protokolů SSL/TLS je jejich implementace ve webových prohlížečích, který může být využit jako klientský software, a s tím spojená podpora na různých klientských platformách.[1][3][4][6]



Obrázek 7: TLS vloženo mezi transportní a aplikační vrstvu

Zdroj: [1]

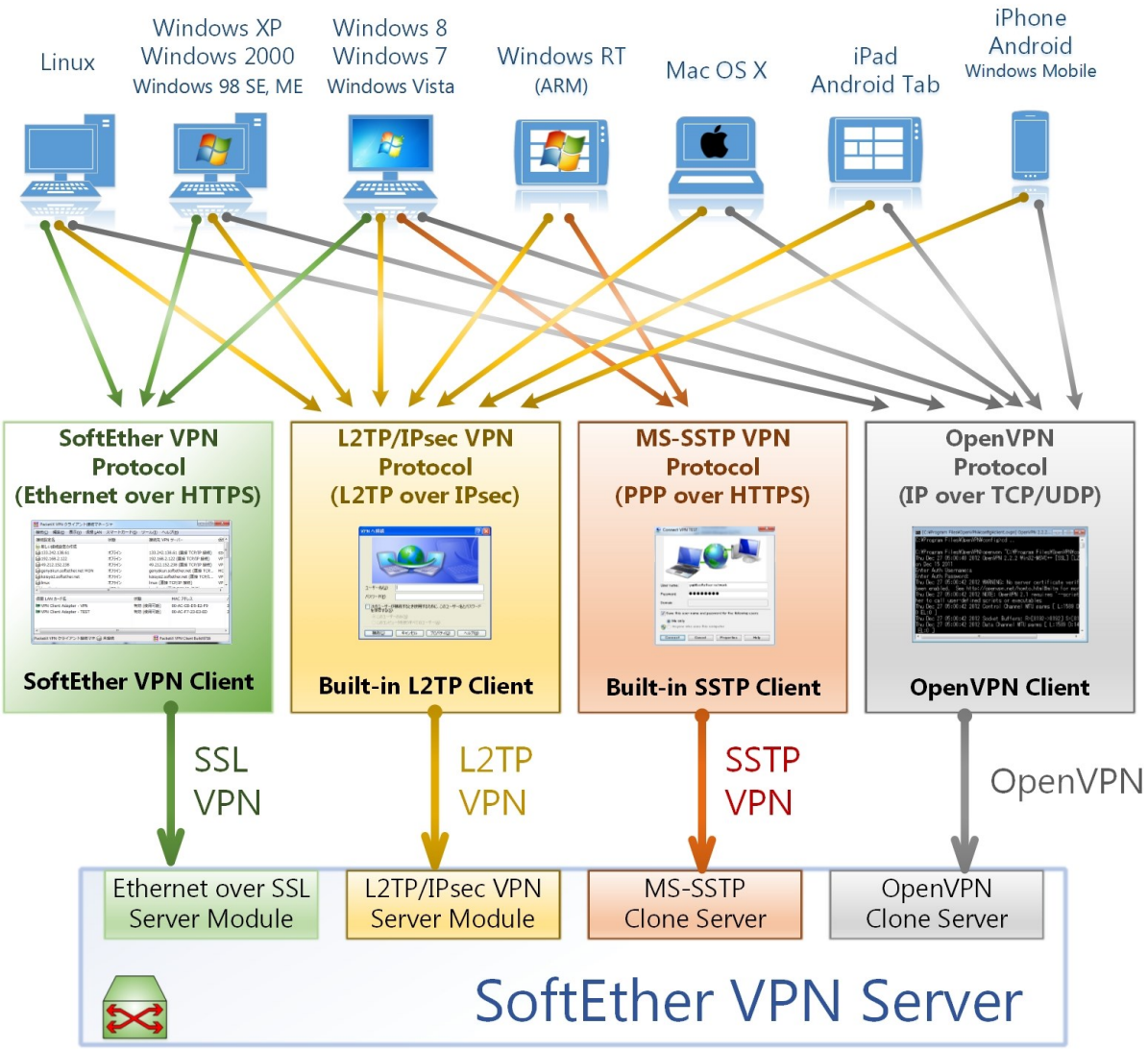
SSTP

SSTP (Secure Socket Tunneling Protocol) je protokol vyvíjený firmou Microsoft. SSTP mechanismus pro zapouzdřování a tunelování vychází ze spojení technologií PPP a TLSv3. Díky využití technologie TLS je SSTP schopný procházet firewally, které mají standartně zakázány protokoly vzdáleného přístupu (jako například GRE nebo L2TP/IPsec). Nevýhodou protokolu je fakt, že způsob, jakým byl navržen, podporuje pouze připojení typu remote access, takže site-to-site připojení v tomto případě není možné.

3 INSTALACE JEDNOTLIVÝCH ŘEŠENÍ

3.1 SoftEther VPN

SoftEther je softwarové VPN řešení od studenta Daiyuu Nobori z Japonské Univerzity Tsukuba. Je to aplikace s otevřeným zdrojovým kódem a je zdarma k použití pro nekomerční i komerční využití. SoftEther je multiprotokolové řešení, je schopný pracovat s protokoly SSL, L2TP/IPsec a díky funkci klonu MS serveru a OpenVPN serveru i s protokoly SSTP a OpenVPN. Díky tomu je možné se k serveru připojit takřka z jakékoliv platformy. Shrnutí jednotlivých protokolů a jejich podpory v platformách viz. Obrázek 8 - možnosti SoftEther VPN

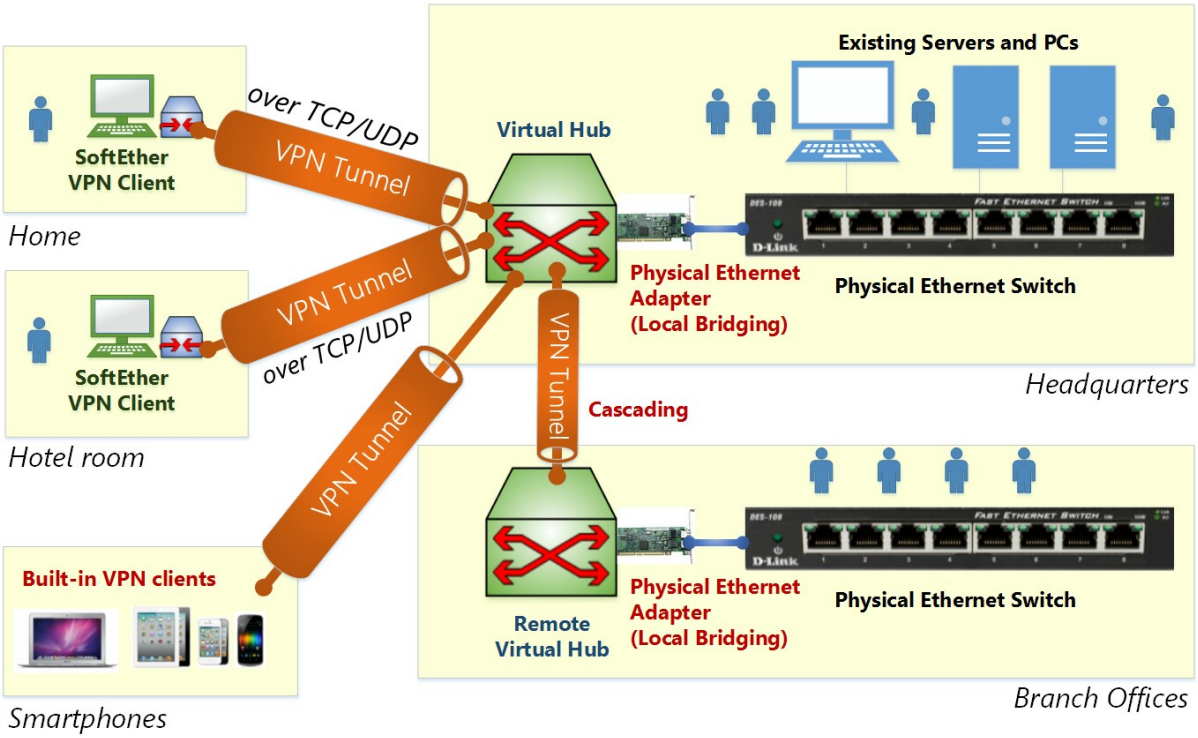


Obrázek 8: Možnosti SoftEther VPN

Zdroj:[9]

Architektura SoftEther VPN je založená na virtualizaci síťových prvků. Díky tomu je možná podpora vytváření obou typů VPN spojení a to site-to-site i remote access. Na straně klienta SoftEther vytváří jednu nebo více virtuálních síťových karet. Na straně serveru se vytváří jeden nebo více virtuálních hubů, neboli virtuální switch, který přijímá požadavky na připojení od klientů a zajišťuje tak VPN spojení. Virtuální hub navíc má FDB (forwarding database), který optimalizuje přenos Ethernet framů.

Založením spojení vzniká VPN tunel mezi VPN klientem a serverem. Spojení je realizováno přes TCP/IP a je šifrováno pomocí SSL/TLS. Díky tomu je možné založit připojení takřka kdekoliv, protože HTTPS port většinou není blokován firewally poskytovatele. Pro site-to-site VPN spojení využívá SoftEther software Cascade Connections mezi dvěma virtuálními huby.[9]



Obrázek 9: Virtualizace SoftEther

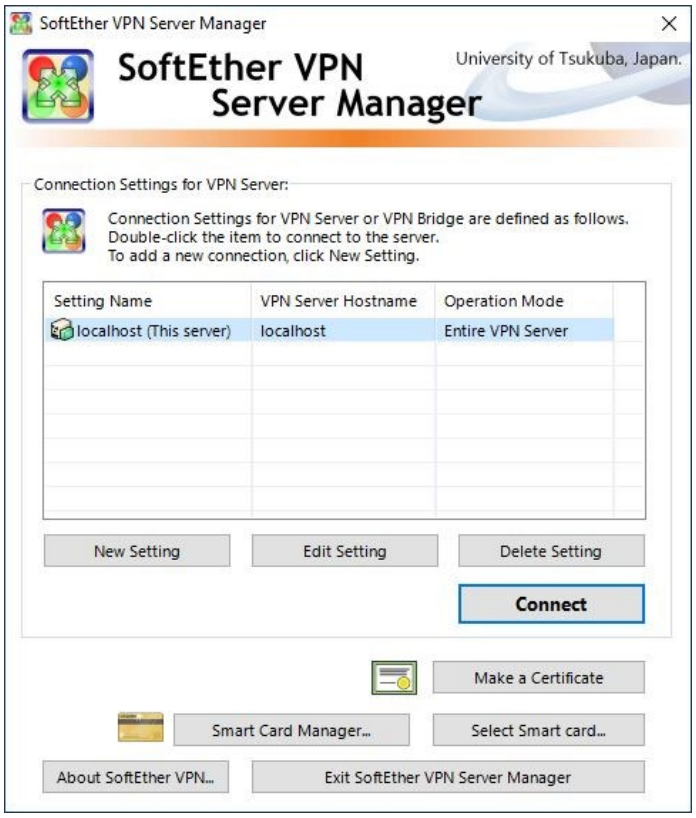
Zdroj: [9]

3.1.1 Postup instalace serveru

Na počítači, který bude v budoucnu sloužit jako VPN server, byly ze stránek SoftEther.org staženy potřebné instalační soubory. Pro stažení souborů je potřeba vyplnit formulář, ve kterém byly vyplněny údaje o operačním systému a typu instalačního souboru.

Dále byl otevřen stažený instalátor. V prvním kroku instalace je pouze informativní text o SoftEther a jeho možnostech na jednotlivých platformách, bylo to tedy potvrzeno tlačítkem

další. V následujícím kroku byly vybrány komponenty, které mají být nainstalovány. Pro instalaci serveru je to první možnost „SoftEther VPN Sever“. V dalším kroku byl potvrzen souhlas s licencí. Pokud je instalováno jinam, než je nastaveno jako výchozí, v dalším kroku je zapotřebí zvolit jiné umístění v počítači. Po potvrzení se již spustila samotná instalace. Pokud byla instalace úspěšná, v posledním kroku stačí pouze stisknout tlačítko „Dokončit“. Checkbox, který byl zatržený s informací, o spuštění VPN Server Manager byl ponechán, aby se hned po dokončení spustil panel, kde bylo pokračováno v nastavení serveru.

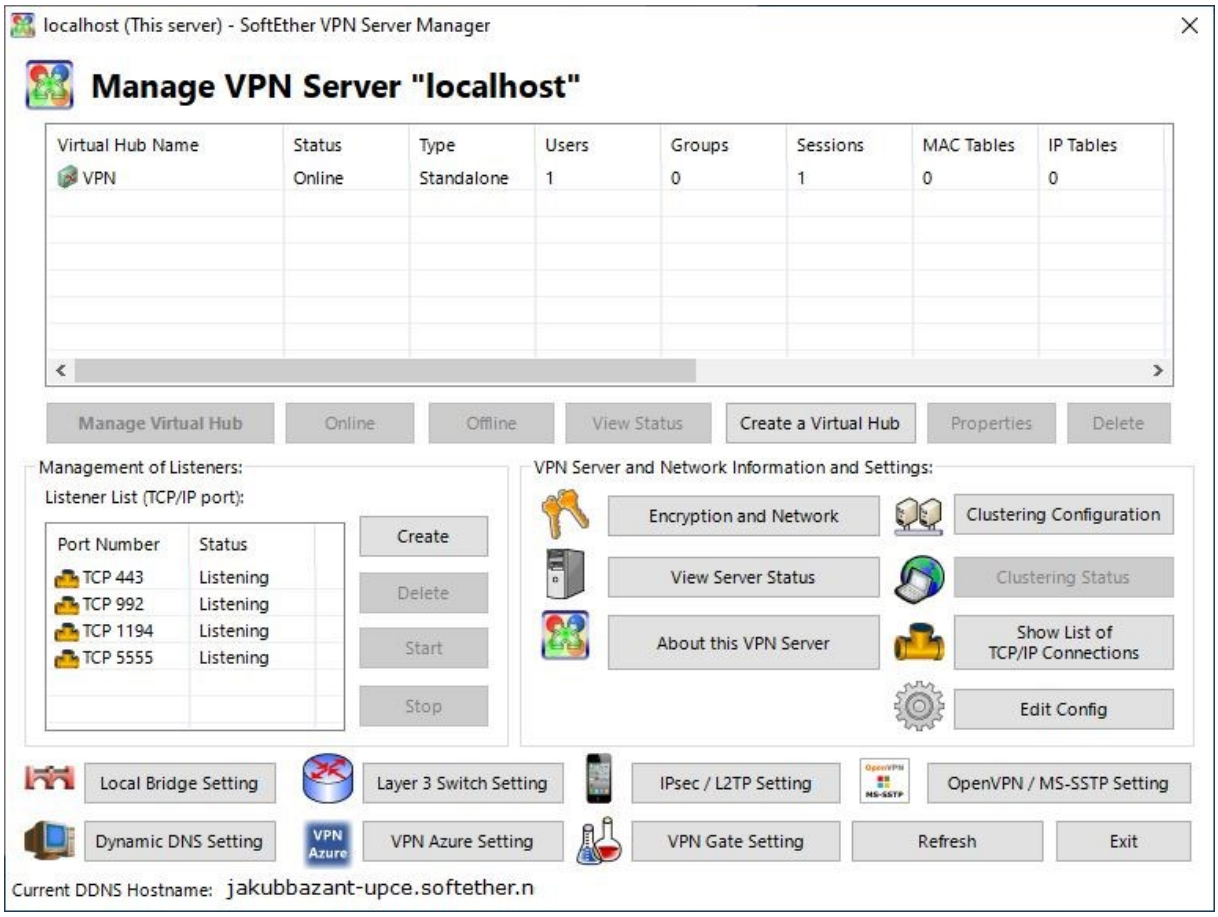


Obrázek 10: VPN Server Manager

Zdroj: instalace aplikace

V Server Manageru již je připravený localhost server. Stačí stisknout tlačítko „Connect“ pro začátek konfigurace serveru. V prvním kroku je zapotřebí nastavit heslo pro administraci serveru. Heslo bylo zvoleno dostatečně silné, takové, které je unikátní, je kombinací velkých a malých písmen, číslic a znaků, a není obsaženo v žádném slovníku. Dále byl zvolen typ VPN serveru. V tomto kroku je možné zvolit více typů najednou, tedy Remote Acess i Site-to-Site. V následujícím kroku byl pojmenován Virtual Hub a dále bylo pokračováno nastavením DDNS. DDNS je velice užitečný nástroj, který má SoftEther v sobě zabudovaný. Díky němu je možné vytvořit VPN server i bez veřejné IP adresy, stačí si vytvořit jedinečnou doménu třetího řádu, jehož vytvoření SoftEther pod svojí doménou softether.net nabízí zdarma. Po vytvoření jedinečné domény stačí stisknout tlačítko „Set to Above Hostname“ pro přiřazení domény

tomuto serveru. V levé části okna můžeme vidět aktuálně nastavenou doménu pro tento server a IP adresu, pod kterou server vystupuje na internetu. V dalších krocích je možné spustit funkce serveru jako je L2TP server klon a VPN Azure Cloud. Dále je potřeba vytvořit alespoň jednoho uživatele a vybrat fyzickou síťovou kartu, přes kterou je počítač připojen k internetu, pro přemostění. Po propojení karet a zavření okna bude už VPN server aktivní pro příchozí spojení. Zobrazí se VPN Server Manager, ze kterého je možné server spravovat a přidávat funkce, které v instalátoru nebyly přidány nebo spravovat uživatele a jejich přihlašování. Nachází se zde i nastavení klonovacích serverů OpenVPN a MS-SSTP.



Obrázek 11: VPN Server Manager

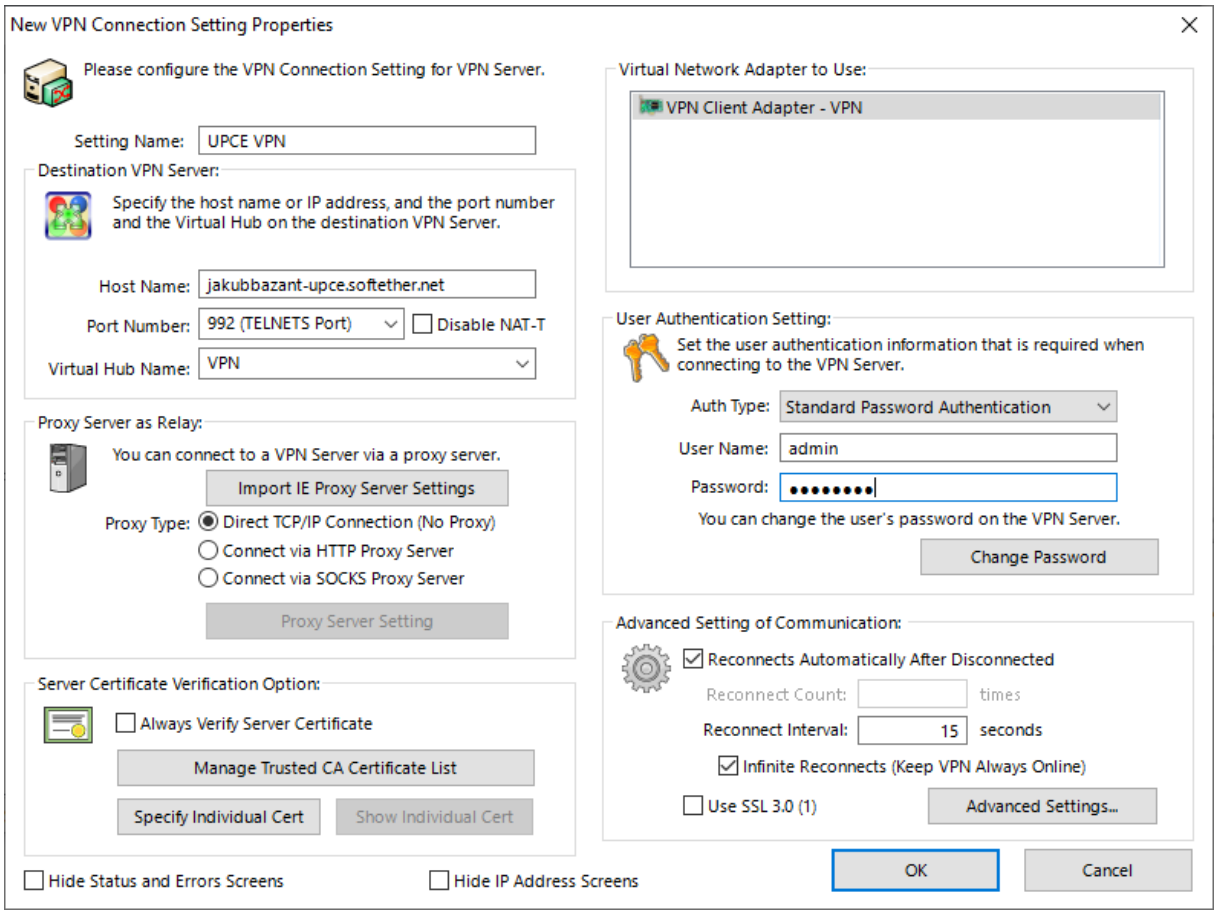
Zdroj: instalace aplikace

Pro správné fungování serveru je zapotřebí zajistit průchodnost paketů skrze router a firewall operačního systému. Na routeru, který je bránou do sítě, je zapotřebí nastavit port mapping (port forwarding), který bude zajišťovat předávání paketů na zvoleném portu, pro komunikaci mezi klientem a serverem, přímo na server. Je také zapotřebí nastavit firewall operačního systému, aby měl otevřený port pro příchozí komunikaci na daném portu. Pokud i tak komunikace nefunguje, může být na serveru daný port obsazen jinou aplikací.

3.1.2 Postup instalace klienta

Při stažení instalačních souborů pro klienta bylo postupováno obdobně jako na serveru, pouze ve formuláři bylo vybráno „SoftEther VPN Client“. Samotný instalátor je obdobný jako při instalaci serveru, rozdílný je VPN Client Manager, který je po úspěšném dokončení nainstalován.

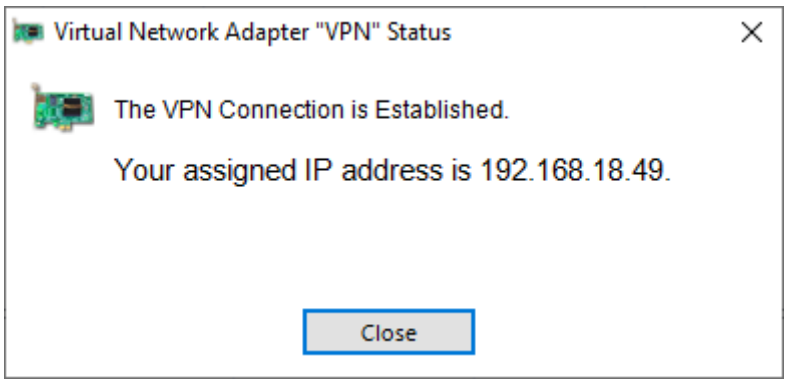
Po otevření VPN Client Manageru kliknutím na tlačítko „Add VPN Connection“ byl vytvořen zástupce pro spojení se serverem. Před samotným nastavením připojení k serveru jsme byli vyzváni k založení virtuální síťové karty. V průvodci je možné adaptér pojmenovat, dále bylo zapotřebí počkat, než průvodce vytvořil virtuální síťový adaptér. Po jeho vytvoření stačilo znovu kliknout na „Add VPN Connection“ a nastavit údaje pro připojení na VPN podle údajů serveru.



Obrázek 12: Nastavení VPN Client

Zdroj: instalace aplikace

Po vyplnění všech potřebných údajů bylo potvrzeno tlačítkem „OK“. Poté již bylo možné se z VPN Client Manageru připojit na server. Pokud bylo vše nastaveno správně, naváže se spojení a klient dostane adresu z podsítě serveru. Viz. Obrázek 13 Navázání spojení



Obrázek 13: Navázání spojení

Zdroj: instalace aplikace

3.2 OpenVPN

OpenVPN je jedním z nejznámějších softwarových open source VPN řešení. OpenVPN vychází z technologie SSL/TLS a knihovny OpenSSL. Díky jeho jednoduché a uživatelsky přívětivé konfiguraci tvoří konkurenci VPN založené na IPsec, při zachování stejné úrovně zabezpečení a funkčnosti.

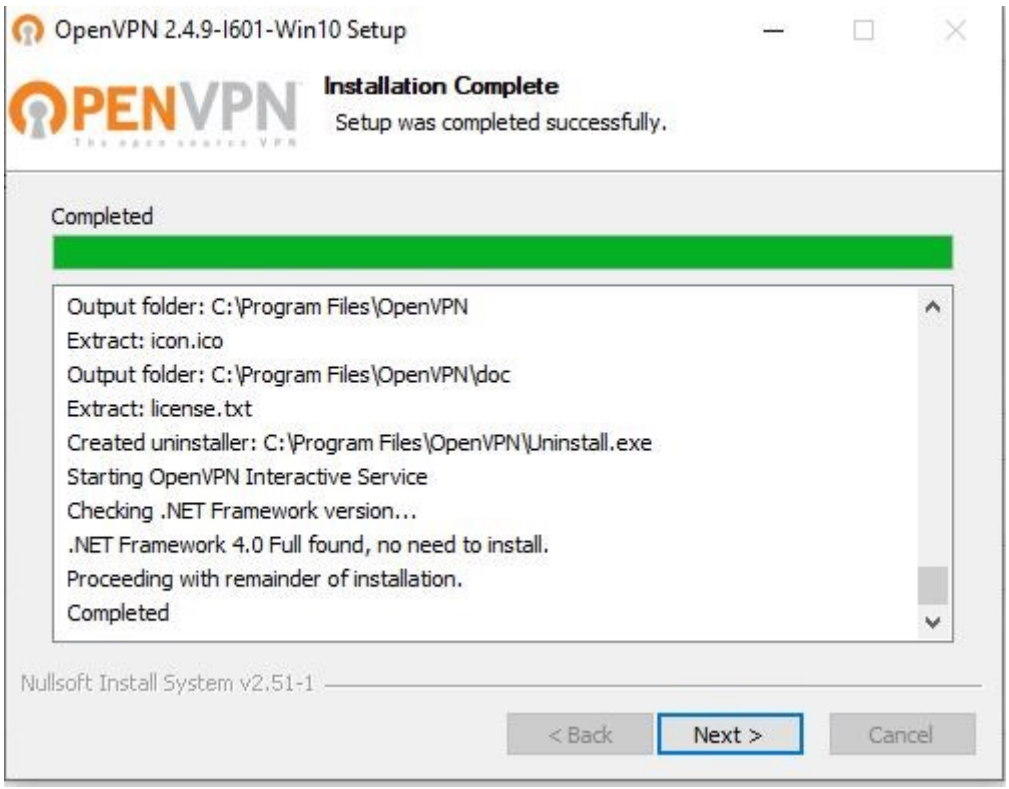
Open VPN nejlépe pracuje na UDP portu, ale je možné ho nakonfigurovat pro TCP nebo pro kterýkoliv jiný port. Díky OpenSSL knihovně podporuje celou řadu kryptografických algoritmů, jako 3DES, AES, Blowfish a jiné.

Díky jeho konfiguraci je možné ho použít pro implementaci řešení vzdáleného přístupu (remote access), propojení dvou sítí (Site-to-Site) a mnohé další. Pro autentizaci spojení s OpenVPN lze použít velké množství nejrůznějších metod, jako dvoufaktorové ověření, smart card, certifikáty apod. Instalační soubory jsou vydávané pro platformy Linux i Windows. [4][7][8]

Postup instalace OpenVPN

Ze stránek OpenVPN byl stažen instalační soubor pro verzi operačního systému, která byla na serveru nainstalována. Pozor, z důvodu rozdílného ověřování ovladačů v operačních systémech je rozdílná verze instalátoru pro Windows 7,8 a Windows 10. OpenVPN má pro klienta i pro server stejný instalátor, rozdíl je pouze v konfiguračních souborech, které rozlišují mezi klientem a serverem, které nahrajete do příslušné konfigurační složky.

První okno instalátoru je pouze informativní, stačí tedy pokračovat. V následujícím bylo potvrzeno licenční ustanovení a pokračováno dalším. Zde bylo potřeba zaškrtnout možnost „EasyRSA 2 Certifikate Management Script“, která není ve výchozím nastavení zaškrtnuta. Bylo pokračováno tlačítkem další, které již spustilo instalaci potřebných souborů pro OpenVPN server. Po úspěšné instalaci byl průvodce ukončen tlačítkem „Finish“.



Obrázek 14: Instralátor OpenVPN

Zdroj: instalace aplikace

Dále byly přepsány konfigurační sobory. Protože je OpenVPN původně vyvinut pro Linux, úprava konfiguračních souborů probíhá převážně v textových souborech, ke kterým se přistupuje pomocí příkazové řádky. Bylo tedy zapotřebí pokračovat otevřením příkazové řádky ve Windows a spustit jí jako správce. Pro přechod do složky OpenVPN byl užit příkaz:

```
cd "C:\Program Files\OpenVPN\easy-rsa"
```

Dále byl inicializován konfigurátor příkazem:

```
init-config
```

Během instalace je zapotřebí inicializovat konfiguraci pouze jednou.

Dále byl otevřen soubor vars.bat v textovém editoru:

```
notepad vars.bat
```

V tomto souboru bylo zapotřebí přepsat následující hodnoty tak, aby odpovídaly hodnotám organizace:

```
set KEY_COUNTRY=US
set KEY_PROVINCE=CA
set KEY_CITY=SanFrancisco
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@host.domain
```

Byla vyplněna země, provincie (v ČR se dá chápat jako kraj), město, organizace, email. Soubor byl uložen a dále byly provedeny příkazy:

```
Vars
clean-all
```

V dalším kroku následovalo sestavení Certifikátů a klíčů:

```
build-ca
```

V průběhu sestavování bylo zapotřebí vyplnění následujících informací, pokud vyhovují výchozí hodnoty uvedené v závorkách, stačí ponechat prázdné a potvrdit enterem:

```
Country Name (2 letter code) [CZ]:
State or Province Name (full name) [PardubickyKraj]:
Locality Name (eg, city) [Pardubice]:
Organization Name (eg, company) [JakubBazant]:
Organizational Unit Name (eg, section) []:JakubBazant-BP
Common Name (eg, your name or your server's hostname) []:JakubBazant-UPCE
Email Address [st49611@student.upce.cz]:
```

Nyní bylo možné iniciovat sestavení certifikátu serveru:

```
build-key-server server
```

Po vyzvání, bylo potvrzeno podepsání certifikátu klávesou „y“ a enter.

Podobně jako pro server byly sestaveny certifikáty a klíče pro každého klienta, který se připojuje k serveru. To bylo učiněno příkazem:

```
build-key jakub-laptop
```

Kdy místo „jakub-laptop“ byl pro každého klienta použit jedinečný identifikátor. Stejný identifikátor byl také použit po výzvě o vepsání „Common Name“.

Po vytvoření pro každého klienta bylo iniciováno generování Deffie Hellman parametru, které je důležité pro šifrování.

```
build-dh
```

Dále byl vygenerován sdílený klíč:

```
"C:\Program Files\OpenVPN\bin\openvpn.exe" --genkey --secret "C:\Program
Files\OpenVPN\easy-rsa\keys\ta.key"
```

Nyní je na řadě samotná úprava konfiguračních souborů. Nejdříve byl upraven pro server. Jako první byl zapotřebí zkopírovat ukázkový konfigurační soubor příkazem:

```
copy "C:\Program Files\OpenVPN\sample-config\server.ovpn" "C:\Program
Files\OpenVPN\easy-rsa\keys\server.ovpn"
```

Následovala editace v poznámkovém bloku:

```
notepad "C:\Program Files\OpenVPN\easy-rsa\keys\server.ovpn"
```

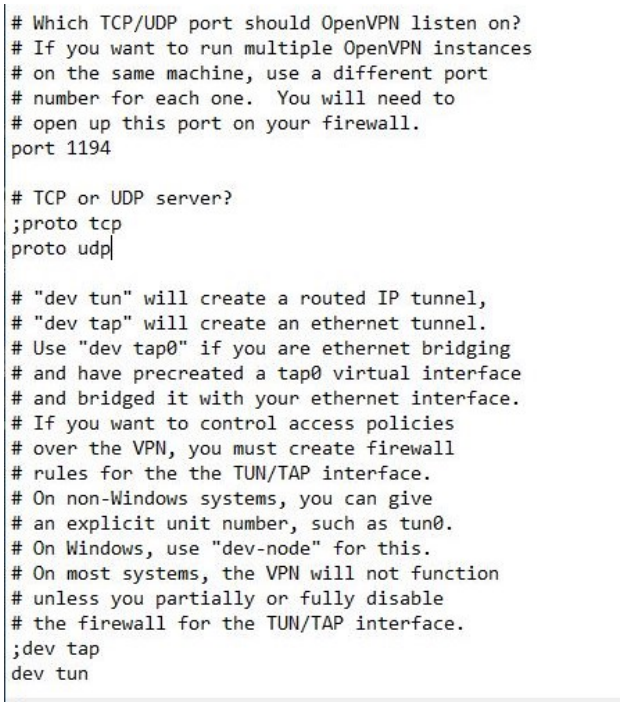
Kde bylo zapotřebí najít následující řádky:

```
ca ca.crt
cert server.crt
key server.key
dh dh2048.pem
```

a upravit je do této podoby:

```
ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\server.crt"
key "C:\\Program Files\\OpenVPN\\config\\server.key"
dh "C:\\Program Files\\OpenVPN\\config\\dh2048.pem"
```

Po editaci byl konfigurační soubor uložen a bylo možné poznámkový blok zavřít.



Obrázek 15: Náhled konfiguračního souboru server

Zdroj: instalace aplikace

Dále byl překopírován klientský ukázkový konfigurační soubor. Bylo zapotřebí změnit název souboru podle zvoleného „Common Name“, tedy soubor pro každého klienta bude mít jiný název.

```
copy "C:\Program Files\OpenVPN\sample-config\client.ovpn" "C:\Program
Files\OpenVPN\easy-rsa\keys\jakub-laptop.ovpn"
```

Po zkopírování byl použit příkaz pro otevření konfiguračního souboru:

```
notepad "C:\Program Files\OpenVPN\easy-rsa\keys\jakub-laptop.ovpn"
```

ve kterém byli vyhledány následující řádky:

```
ca ca.crt
cert client.crt
key client.key
```

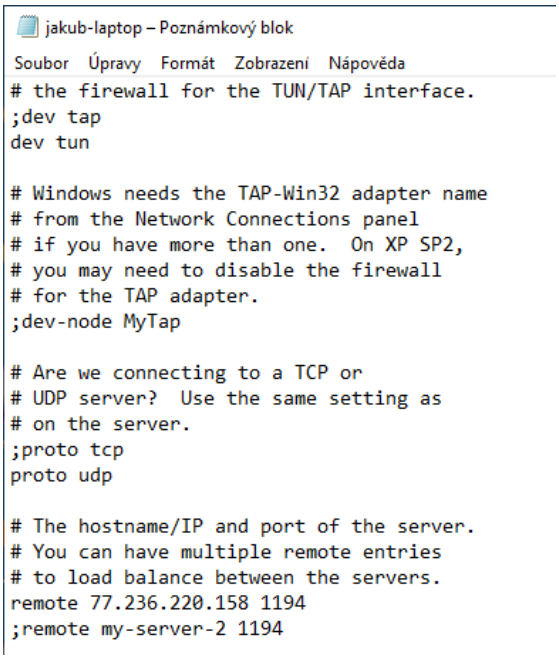
a nahrazeny textem s úplnou cestou k souborům. Bylo potřeba přepsat adresu pro „cert“ a „key“ pro každého klienta, podle zvoleného „Common Name“:

```
ca "C:\\Program Files\\OpenVPN\\config\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\config\\jakub-laptop.crt"
key "C:\\Program Files\\OpenVPN\\config\\jakub-laptop.key"
```

Dále byla změněna adresa pro přístup k serveru, přístup může být adresován buď IP adresou nebo doménovým jménem, pokud je potřeba, je také možné změnit číslo portu (výchozí 1194).

```
remote 77.236.220.158 1194
```

Soubor byl uložen. Tento postup byl zopakován pro každého klienta.



Obrázek 16: Náhled konfiguračního souboru klient

Zdroj: instalace aplikace

Nyní už je zapotřebí pouze konfigurační a soubory certifikátu překopírovat ze složky \easy-rsa\keys\ do složky \config\. To pro server bylo provedeno příkazem robocopy:

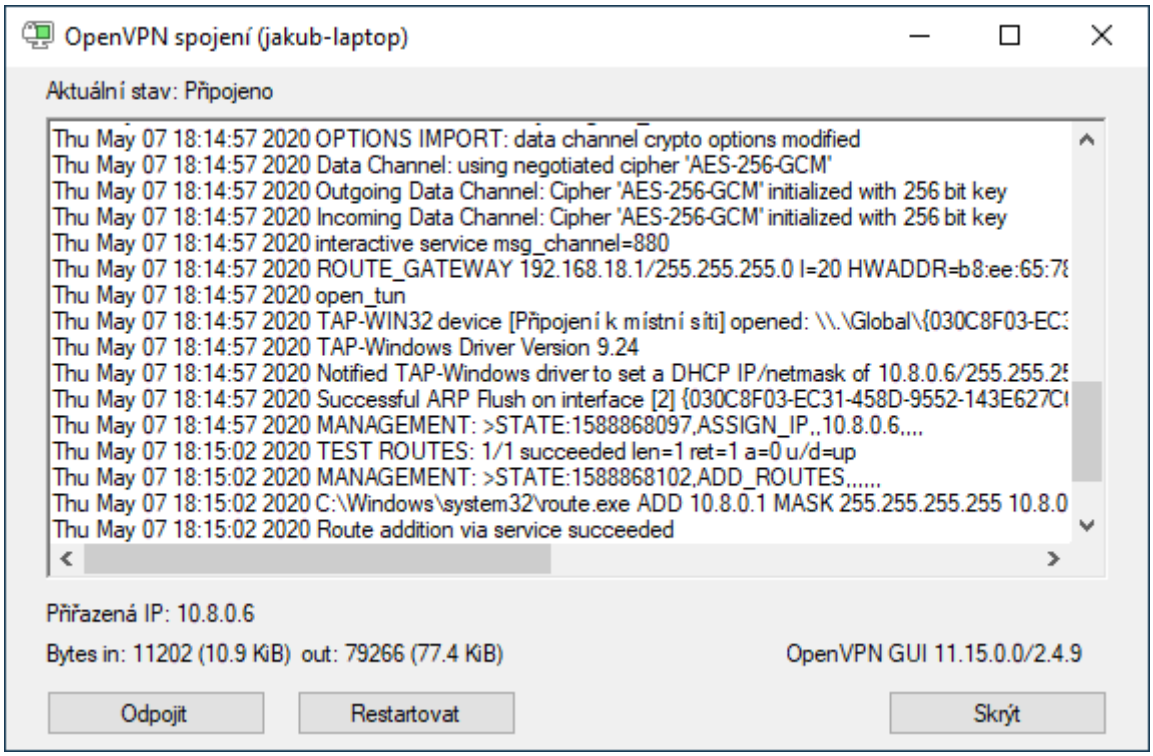
```
robocopy "C:\Program Files\OpenVPN\easy-rsa\keys\ " "C:\Program
Files\OpenVPN\config\ " ca.crt ta.key dh2048.pem server.crt server.key
server.ovpn
```

Pro každého klienta byly přeneseny soubory s jeho jménem, s pomocí Flash disku. Přeposlání e-mailem není v tomto případě bezpečné, proto je Flash disk preferován.

```
ca.crt
ta.key
jakub-laptop.crt
```

```
jakub-laptop.key
jakub-laptop.ovpn
```

Jako u předchozí instalace, bylo zapotřebí zajistit průchod paketů skrze router a firewall ve Windows. Na NAT zařízení, bylo nutné nastavit port mapping (port forwarding), který bude předávat pakety s hlavičkou portu, která je nastavena pro komunikaci, přímo na server. Dále byl nastaven Windows Firewall, aby měl otevřený port pro příchozí komunikaci na daném portu.



Obrázek 17: OpenVPN úspěšné spojení

Zdroj: instalace aplikace

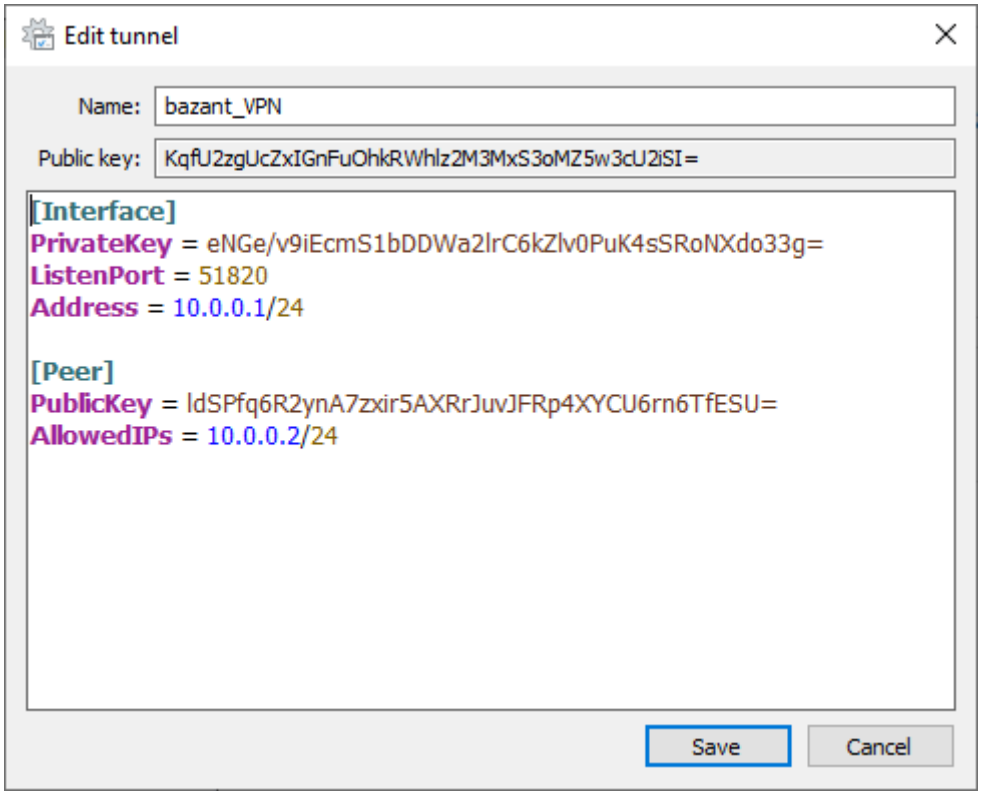
3.3 WireGuard

WireGuard je VPN nástroj, který byl představen v roce 2015. Původně byl vyvinut pro jádro Linuxu, dnes je již multiplatformní (Windows, macOS, BSD, iOS, Android). Jeho jádro je vydáváno pod licencí GLPv2 a projekty z něj vycházející jsou licencovány jako MIT, Apache 2.0, nebo GPL. Při vývoji WireGuard byl kladen důraz na jednoduchost kódu a vysokou přenosovou rychlost. Jak autor sám uvádí, protokol je stále ve fázi vývoje, takže je do budoucna možné jeho další zrychlování. Díky těmto přednostem se tento protokol začíná těšit velké oblibě, tuto technologii využívá například Mozilla VPN nebo některé servery NordVPN. Jako jedno ze známých omezení WireGuard je podpora pouze UDP spojení a není zde umožněno změnit způsob šifrování. Tyto známé omezení jsou z důvodu co nejvyšší výkonosti. [14][19][20][21]

Postup instalace WireGuard

Ze stránek https://www.wireguard.com/ bylo zapotřebí stáhnout instalační soubor. WireGuard má pouze jeden instalační soubor pro klienta i server, rozdíl je pouze v konfiguraci. Po úspěšném stažení stačilo soubor otevřít, instalace nevyžadovala žádnou další iniciativu a program byl automaticky nainstalován. Po otevření programu bylo potřeba vytvořit tunel rozkliknutím šipky u tlačítka: „Add Tunnel“ a pokračováním volbou „Add empty tunnel“. V nově otevřeném okně byl vygenerován privátní a veřejný klíč. Po vyplnění jména připojení bylo možné přejít k samotné konfiguraci. To je možné provést také v tomto okně, které zároveň slouží jako editor konfiguračních souborů.

Na straně serveru je definován pod „[Interface]“ privátní klíč, který již byl předdefinován. Dále „ListenPort“ na kterém server naslouchá a „Address“, což je adresa serveru. Také je zde definována část „[Peer]“, kde je uveden „PublicKey“, veřejný klíč zkopírován z tunelu klienta a „AllowedIPs“ kde je definována adresa, která bude tomuto připojení přidělena. Pro každého nového klienta je zapotřebí vytvořit novou sekci „[Peer]“ s jeho veřejným klíčem a přidělenou adresou, která nebude kolidovat s již použitými.

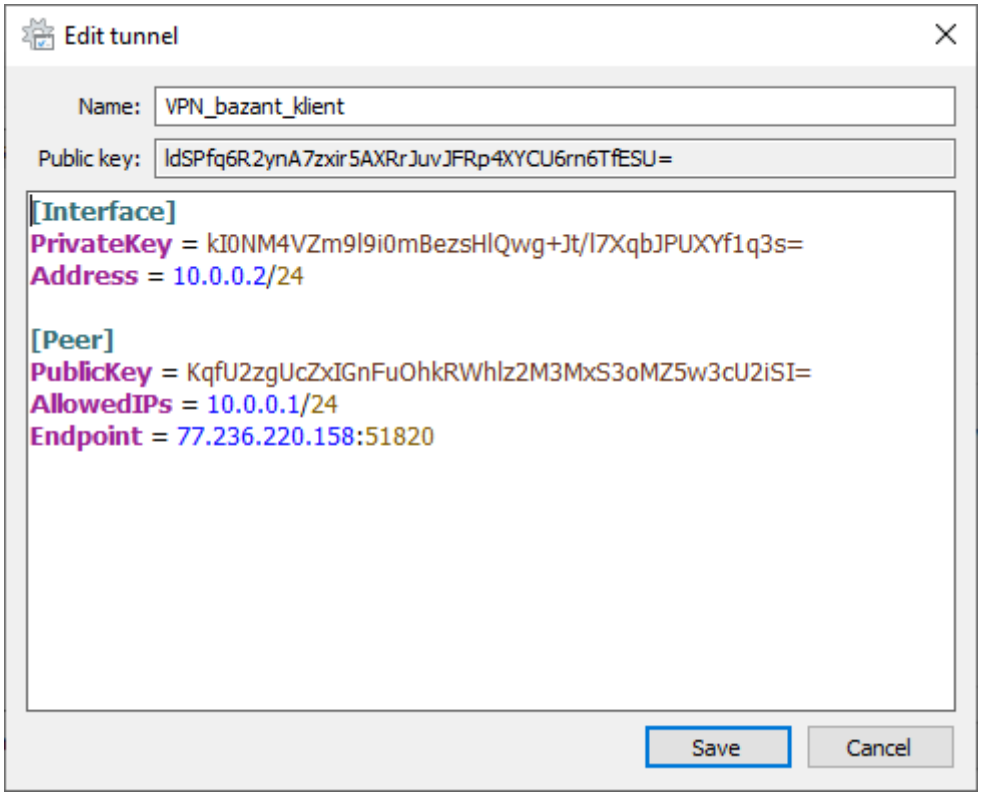


Obrázek 18: Konfigurační soubor WireGuard (server)

Zdroj: instalace aplikace

Na straně klienta bylo pod „[Interface]“ doplněno „Address“, což je IP adresa klienta. V sekci „[Peer]“ byl přidán „PublicKey“, kde byl překopírován veřejný klíč serveru, „AllowedIPs“

neboli privátní IP adresa serveru a „Endpoint“, ve kterém je uvedena veřejná adresa serveru a za dvojtečkou port, na kterém server naslouchá.



Obrázek 19: Konfigurační soubor WireGuard (klient)

Zdroj: instalace aplikace

Stejně jako v předchozích případech bylo potřeba přidat pravidla do port forwarding (mapping) na směrovači v síti serveru a výjimku pro otevření portu ve firewallu na serveru.

4 MODELOVÉ SITUACE

Tato kapitola bude věnována situacím, pro jejichž řešení se hojně využívá Virtuálních Privátních Sítí (VPN). Tyto případy nejlépe reflektují skutečnost, jak je využití VPN v současné moderní síťové infrastruktuře nepostradatelné. V některých firmách je dokonce zapotřebí řešit i více takovýchto situací současně.

Navržené modelové situace a kritéria pro hodnocení vznikly na základě rozhovorů se správci sítí z různých firem. I přesto, že jsou zobecněné, vychází z reálných potřeb moderních společností.

4.1 Připojení ke vzdálené ploše

První modelovou situací je připojení ke vzdálené ploše, pomocí které lze vyzdvihnout důležitost VPN a její významnou roli při zabezpečení v moderní síťové infrastruktuře. Pro připojení ke vzdálené ploše je standardem používat Remote Desktop Protocol (RDP), nebo Virtual Network Computing (VNC), kteří ve svém výchozím nastavení naslouchají na TCP portu 3389 pro RDP a na TCP portech, v rozmezí 5900 až 5906, pro VNC. Tyto protokoly jsou samostatně schopny při správném nastavení NATu, nebo při správné identifikaci počítače pro vzdálené připojení, například za pomocí DDNS, být použity i pro komunikaci přes veřejnou síť. Pro své časté využití jsou bohužel často napadány zvenčí a tím je ohrožena bezpečnost uživatelských i firemních dat. Jako řešení tohoto problému se na první pohled může zdát využití změny portu pro přístup, to však není vždy dostatečné řešení. Tou nejlepší možností v současné době je však využití kombinace VPN a některého z protokolů pro připojení ke vzdálené ploše. VPN protokoly zajišťují šifrované tunelové spojení mezi vzdáleným klientem připojeným přes veřejnou síť a VPN serverem v lokální síti. Po úspěšném navázání spojení klienta se serverem se klient virtuálně nachází v lokální síti LAN a má tedy možnost využití protokolů pro připojení ke vzdálené ploše, i když jsou nastaveny pouze pro lokální přístup. V takto navrženém spojení jsou všechny stanice, které jsou nastaveny pro vzdálené připojení, schovány za routerem a je možno k nim přistupovat buď na lokální úrovni nebo z veřejné sítě prostřednictvím bezpečného VPN spojení.[11]

Vzdálená správa serveru

V dnešní době jsou po celém světe rozmístěny milióny serverů, které dohromady se síťovými prvky vytvářejí největší síť, kterou známe, a tou je internet. K takovýmto serverům je nutné přistupovat zvláště opatrně, je potřeba u nich dbát na zvýšenou bezpečnost a nastavit je tak, aby byly přístupné pouze ty části, u kterých je to nezbytně nutné. Protože takovéto servery

často poskytují veřejnou službu, jsou tak jednoduše přístupné z vnější sítě. To může vést ke zvýšenému zájmu potencionálního útočníka k prolomení jejich zabezpečení.

Modelovou situací může být kancelář firmy, ve které je také server, na kterém jsou provozovány stránky firmy. K tomu je samozřejmě zapotřebí, aby webový server byl dostupný kterémukoliv klientovi na světě. Zároveň je však nutné k tomuto serveru přistupovat z veřejné sítě pro vzdálenou správu pomocí protokolu RDP. V takovém případě je nemyslitelné, aby se nastavilo přesměrování portu 3389 přímo na server a tím zajistilo vzdálené připojení. Vhodnější cestou je přistupovat ke správě serveru prostřednictvím VPN serveru. Při takto navrženém řešení bude z vnějšku viditelný pouze webový a VPN server, které jsou na případné útoky lépe připravené než samotný RDP nebo jiný protokol. Takto získáme skvělý nástroj pro zabezpečený a šifrovaný přístup k serveru a jeho správě odkudkoliv.

Terminálový server pro účetnictví

Dalším příkladem využití může být terminálový server pro účetnictví. Je hypotetická firma, kde nastala potřeba umožnit přístup více lidem současně k účetnímu programu. Možností řešení je hned několik, avšak některé z nich nejsou univerzálně použitelné nebo dostatečně bezpečné. Řešení přes terminálový server v kombinaci s VPN serverem je z nich nejefektivnější, nejbezpečnější a univerzálně použitelný.

Ať již na fyzickém, nebo virtuálním Privátním Serveru (VPS), máme nainstalovanou příslušnou verzi pro síťový provoz. Server nastavíme tak, aby jeho služby byly dostupné pouze z lokální sítě, a to včetně terminálových služeb. Dále na samotném serveru, nebo směrovači, nastavíme VPN pro přístup do LAN. Klient se nejdříve připojí pomocí klientského softwaru zvoleného VPN řešení do podsítě, kde se nachází terminálový server. Tímto postupem se připojený klient virtuálně dostane do stejné podsítě jako terminálový server a může se připojit ke vzdálené ploše.

Home office

Příkladem budiž firma zabývající se tvorbou webových stránek a e-shopů, která má kanceláře v centru města. Každý zaměstnanec disponuje vlastním stolním PC, na kterém má nainstalovaný potřebný software (např. grafické, programovací, projektové a jiné programy), které jsou potřebné k výkonu jejich zaměstnání a cena licencí bývá zpravidla velmi vysoká. Dále je ve firemní síti zřízeno datové úložiště (NAS), na které zaměstnanci ukládají dokončené a průběžné verze svých projektů.

Aby zaměstnanci firmy získali přístup ke svým firemním počítačům, je zapotřebí na každé stanici nastavit připojení ke vzdálené ploše. Dále zřídíme VPN server, s jehož pomocí

zaměstnanci vytvoří bezpečný tunel do podnikové sítě. Při takovéto implementaci by však museli být všechny pracovní stanice zapnuté, proto se nabízí možnost přidání Wake on LAN. V tomto případě stačí mít počítače v režimu spánku a pouze je vzdáleně probudit.

4.2 Propojení více sítí

Prostředí větších podniků někdy vyžaduje bezpečné propojení dvou a více fyzických podnikových sítí. V takové situaci se nám nabízí řešení pomocí Site-to-Site VPN, které nám umožní vytvořit tunel mezi těmito sítěmi. Při tomto propojení může být směrováno velké množství aktivity na síti do tunelu, proto je zapotřebí daleko více dbát na správnou optimalizaci VPN, aby nedocházelo k přerušení tohoto spojení. V otázce správného poměru mezi bezpečností, zvolenou metodou šifrování a výkonem, je dobré se obrátit na experta.

Propojení dvou poboček firmy

Mnoho firem, které mají více poboček, řeší otázku bezpečného propojení, často i stovky kilometrů od sebe vzdálených pracovišť. Pro řešení tohoto problému se nám nabízí využití právě Site-to-Site VPN skrze síť WAN, která nám zajistí dostupnost sdílených síťových prostředků v rámci většího množství poboček společnosti.

Propojení datových center

„Datové centrum lze definovat jako prostor pro uložení počítačových technologií a přidružených technologií jako jsou telekomunikační a centralizovaná úložiště, ať už fyzická nebo virtuální, pro skladování, řízení a šíření údajů a informací“ [10]

Ať již jsou datacentra hned vedle sebe, nebo několik desítek kilometrů daleko, je možnost Site-to-Site stejně vhodná i v případě propojení dvou či více serveroven. Toto propojení zřizujeme z důvodů společné analýzy nebo plného spojení pro potřeby sloučení výkonu.

4.3 Komerční VPN

Pod pojmem komerční VPN je v tomto případě myšlena služba, kterou si od některého z poskytovatelů může zákazník předplatit a tím získá přístup pro připojení k jeho serverům. Toto tzv. předplatné funguje na principu, kdy předplatitel má nainstalovaný klientský software, s jehož pomocí je jeho veškerá online aktivita směrována do tunelu k serveru poskytovateli služby, a díky tomu je jeho činnost na internetu skryta. Poskytovatel má zpravidla více, někdy i tisíce, serverů po celém světě a uživatel si může v aplikaci vybrat zemi, pod kterou bude vystupovat.

Takovéto VPN řešení už neslouží pouze ke skrytí ilegálních aktivit, ale má zajisté své využití i ve firemním prostředí. Zde si lze přiblížit několik případů konkrétního využití.

Prvním případem je zvýšení zabezpečení při konferenčním hovoru, kdy všichni jeho účastníci využívají komerční VPN, a díky tomu je jejich hovor dvojnásobně šifrován. V tomto případě je daleko složitější takový hovor nějakým způsobem odposlouchávat. Druhým využitím může být možnost obcházet geolokační pravidla dokumentu nebo webové stránky. Díky tomu, že aktivita uživatele je skryta pod serverem v jiné zemi, vystupuje na internetu jako by se v této zemi právě nacházel. Může si tedy vybrat do jaké země se připojí a tím se vyhne těmto pravidlům. Třetím, a posledním příkladem, bude možnost penetrace firewallu nebo restrikcí na webové stránky, které mohou být nastaveny státem, poskytovatelem připojení či na hotelové Wi-Fi. S tímto nástrojem jsme schopni tyto restrikce obejít.

5 VYHODNOCENÍ

Pro vyhodnocení optimálního VPN řešení v jednotlivých modelových situacích bylo zvoleno multikriteriální rozhodování za použití AHP, též známé jako Saatyho metoda, jejímž tvůrcem je Dr. L. H. Saaty.

AHP je technika rozhodování, která pomáhá vybrat optimální variantu na základě přednastavených kritérií a jejich vah. Tato metoda je vhodná při použití kvantitativních i kvalitativních dat. Metoda AHP byla vytvořena tak, aby reflektovala způsob, jakým lidé při rozhodování myslí, a i proto je tato metoda stále jednou z nejuznávanějších.[16]

Pro výpočet za pomocí této metody je zapotřebí zjistit:

- preferenční vztahy a stanovení vah pro každou dvojici kritérií
- postupné určení velikosti preference všech dvojic variant (z hlediska každého kritéria)[15]

tyto preferenční vztahy jsou hodnoceny podle následující tabulky:

Tabulka 1: Saatym doporučená bodová stupnice

Počet bodů	Popis
1	Jsou stejně závislá
3	První je slabě významnější než druhé
5	První je dosti významnější než druhé
7	První je prokazatelně významnější než druhé
9	První je absolutně významnější než druhé

Zdroj: upraveno podle [18]

5.1 Klíčové atributy pro hodnocení

Pro správné zvolení nejlepšího dostupného produktu, který lze následně implementovat do firemního systému, je zapotřebí si správně zvolit klíčové atributy pro multikriteriální rozhodování a jejich váhu. Váha jednotlivých kritérií samozřejmě závisí hlavně na konkrétní situaci, někdy je například důležitější výkon VPN a není tak podstatné, jak hodně vznikající VPN spojení zatěžují hardware. Níže jsou popsány některé atributy, které při rozhodování mohou hrát důležitou roli.

Výkon

Atributem výkon se v tomto smyslu myslí výkon VPN tunelu, tedy jakou má maximální propustnost/rychlost a odezvu. Rychlost značně souvisí se zvoleným VPN softwarem a jím používanými technologiemi. Odezva i rychlost může souviset s kvalitou linky, na které jsou oba body tunelu připojeny, vzdáleností od páteřní sítě a také fyzickou vzdáleností od sebe. Pokud se uživatel VPN tunelem připojí z Evropy na server pobočky firmy do Ameriky, bude s největší pravděpodobností odezva vyšší.

Tabulka 2: Rychlost alternativ

	Rychlost [Mbps]
OpenVPN	258
SoftEther	980
WireGuard	1011

Zdroj: vlastní zpracování podle dat z [9][14]

Tabulka 3: Matice porovnání vybraných alternativ, kritérium výkon

Výkon	*OpenVPN*	*SoftEther*	*WireGuard*
OpenVPN	1	1/7	1/7
SoftEther	7	1	1
WireGuard	7	1	1

Zdroj: vlastní zpracování

Jak je zřejmé z Tabulka 2: Rychlost alternativ, podle dostupných zdrojů, je SoftEther pouze zanedbatelně pomalejší než WireGuard. Na druhou stranu, co se týče rychlosti, OpenVPN nad svými konkurenty značně zaostává.

Bezpečnost

Bezpečností se rozumí možné způsoby autentizace uživatelů, úroveň šifrování přenášených dat a šifrovacího algoritmu, popřípadě možnost použití jiného, vhodnějšího, algoritmu. Při bezpečnosti hraje také roli kvalita kódu aplikace a včasné odstraňování zranitelných míst. Vysoká úroveň zabezpečení nicméně může mít i negativní vliv na stabilitu celé VPN, nevhodně zvolený šifrovací algoritmus nebo nadměrná úroveň šifrování může klást větší nároky na hardware i na rychlost VPN.

Tabulka 4: Srovnání šifrování alternativ

	Šifrování
OpenVPN	Blowfish, 3DES, AES
SoftEther	AES, RSA
WireGuard	ChaCha20Poly1305

Zdroj: vlastní zpracování podle dat z [8][9][14]

Tabulka 5: Matice porovnání vybraných alternativ, kritérium bezpečnost

Bezpečnost	*OpenVPN*	*SoftEther*	*WireGuard*
OpenVPN	1	3	6
SoftEther	1/3	1	3
WireGuard	1/6	1/3	1

Zdroj: vlastní zpracování

Hlavní výhoda SoftEther a OpenVPN je možnost zvolení používané šifry. OpenVPN má na výběr z více šifer než SoftEther, proto byl OpenVPN hodnocen nejlépe. OpenVPN je ve většině komerčních VPN použita jako výchozí a zároveň má velkou komunitu, která se podílí na vývoji, což znamená, že je často auditována a zkoumána na bezpečnostní chyby. Proto je OpenVPN mnohými zdroji považována za nejbezpečnější variantu. [7][17]

V blízké budoucnosti se dá očekávat, že WireGuard předčí v otázce bezpečnosti OpenVPN. Díky krátkému a čistému kódu je jednodušeji auditovatelný, zároveň je psán s ohledem na bezpečnost. V této práci byl však hodnocen nejhůře z důvodu krátkého působení a množství auditů. To se dá očekávat, že se s jeho vzrůstající popularitou, bude měnit. [19][21]

Autentizace

Způsob autentizace úzce souvisí s bezpečností celé firemní sítě. Autentizace je mechanismus, při kterém dochází k ověření uživatele nebo počítače a jejich příslušnost k určité skupině. V některých systémech nám může záležet na tom, aby VPN bylo možné co nejlépe přidat do již používané autentizace ve firmě.[4]

Tabulka 6: Způsoby autentizace alternativ

	Způsoby autentizace
OpenVPN	sdílený klíč, certifikáty X.509 + SmartCards
SoftEther	Anonymní, pomocí jména a hesla, RADIUS, NT Domain a Active Directory, certifikáty X.509 + SmartCards
WireGuard	Pouze sdílený klíč

Zdroj: vlastní zpracování podle dat z [8][9][14]

Tabulka 7: Matice porovnání vybraných alternativ, kritérium autentizace

Autentizace	*OpenVPN*	*SoftEther*	*WireGuard*
OpenVPN	1	1/3	4
SoftEther	3	1	6
WireGuard	1/4	1/6	1

Zdroj: vlastní zpracování

Nejvíce možností autentizace, jak je zřejmé z Tabulka 6: Způsoby autentizace alternativ, má řešení od SoftEther. V tomto programu je možné nakonfigurovat autentizaci pomocí SmartCards, propojení s Active Directory a mnohé další.

Podpora v zařízeních

Dalším důležitým aspektem při výběru může být podpora v zařízeních. Tím se rozumí jak na straně serveru, tak případného klienta. Tento údaj je jednoduché dohledat na stránkách softwarového nebo hardwarového vydavatele VPN. Je obvyklé, že čím je větší podpora, tím lepší, a to hlavně na straně klienta. V některých konkrétních řešeních může být naopak pozitivní podpora jen pro konkrétní platformu, například pouze pro platformu Microsoft Windows.

Tabulka 8: Přehled podpory v zařízeních alternativ

	Podpora Server	Podpora Klient
OpenVPN	Windows, Linux, OpenBSD, FreeBSD, NetBSD, Mac OS X, Solaris. Microtik router OS, Cisco IOS	Windows, Mac OS X, Linux, Android, iOS
SoftEther	Windows, Linux, FreeBSD, Mac OS X, Solaris	Windows, Linux, Mac OS X (beta), další dostupné díky build-in klonům
WireGuard	Windows, Linux, FreeBSD, Mac OS X, Android	Windows, Linux, FreeBSD, Mac OS X, Android

Zdroj: vlastní zpracování podle dat z [8][9][14]

Tabulka 9: Matice porovnání vybraných alternativ, kritérium podpora v zařízeních

Podpora v zařízeních	*OpenVPN*	*SoftEther*	*WireGuard*
OpenVPN	1	4	3
SoftEther	1/4	1	1/2
WireGuard	1/3	2	1

Zdroj: vlastní zpracování

Protože OpenVPN server je možné nainstalovat i na Mikrotik RouterOS a Cisco IOS, byl hodnocen jako řešení s nejlepší podporou. Jako řešení s nejmenší podporou bylo hodnoceno SoftEther, nicméně tento program v sobě obsahuje klony jiných VPN serverů, jako OpenVPN nebo podporu technologie SMTP a v případě spuštění klonu je podpora v zařízeních značně rozšířena.

Jednoduchost použití na straně klienta

V otázce nejlepšího řešení je třeba brát v potaz i uživatele, který s výslednou podobou návrhu může pracovat denně. Proto je důležité neopomenout kritérium jednoduchosti použití na straně klienta. V takovém případě je dobré oslovit samotné zaměstnance a vyhodnotit jejich zpětnou vazbu už při jednotlivých návrzích řešení. Nesmí se však opomenout, že hodnocení uživatelské přívětivosti může být silně individuální, a tedy, že se mohou názory v rámci pracovního kolektivu rozcházet.

Tabulka 10: Matice porovnání vybraných alternativ, kritérium jednoduchost použití

Jednoduchost použití	*OpenVPN*	*SoftEther*	*WireGuard*
OpenVPN	1	1/3	2
SoftEther	3	1	4
WireGuard	1/2	1/4	1

Zdroj: vlastní zpracování

Jednoduchost použití byla hodnocena subjektivně při instalaci jednotlivých VPN řešení, které jsou popsány v kapitole 3. Na základě této zkušenosti bylo nejlépe ohodnoceno řešení od SoftEther, které má velice přehledného a intuitivního klienta.

5.2 Stanovení vah kritérií

Protože v každé modelové situaci můžou mít jednotlivá kritéria různé váhy, byly stanoveny tři tabulky pro výsledné hodnocení v jednotlivých kategoriích modelových situací.

Remote Access

Tabulka 11: Matice porovnání vybraných kritérií, modelová situace Remote Access

Remote Access	Výkon	Bezpečnost	Autentizace	Podpora v zařízeních	Jednoduchost použití
Výkon	1	1/7	1/5	1/3	1/3
Bezpečnost	7	1	3	5	5
Autentizace	5	1/3	1	3	3
Podpora v zařízeních	3	1/5	1/3	1	1
Jednoduchost použití	3	1/5	1/3	1	1

Zdroj: vlastní zpracování

V rámci modelových situací Remote Access byla největší váha přidělena kritériu bezpečnosti. Jako další důležité kritérium byl vybrán způsob autentizace, který by měl co nejlépe pasovat do již používaných technologií a měl by být zvolen takový způsob autentizace, který bude možné technologicky zajistit i mimo firemní prostředí. Jako kritérium s nejmenší vahou byl zvolen

výkon. Výše zvolené modelové situace nevyžadují při provozu tak velké datové toky, proto i nejpomalejší z porovnávaných VPN bude mít dostatečnou rychlost při autentizaci.

Site to Site

Tabulka 12: Matice porovnání vybraných kritérií, modelová situace Site to Site

Site to Site	Výkon	Bezpečnost	Autentizace	Podpora v zařízeních	Jednoduchost použití
Výkon	1	1	8	8	9
Bezpečnost	1	1	8	8	9
Autentizace	1/8	1/8	1	1	3
Podpora v zařízeních	1/8	1/8	1	1	3
Jednoduchost použití	1/9	1/9	1/3	1/3	1

Zdroj: vlastní zpracování

Pro vyhodnocení v rámci Site to Site modelových situací byly nejvyšší váhou ohodnoceny kritéria bezpečnost a výkon. Protože přes takto vzniklý VPN tunel mohou putovat i velice citlivá a důležitá firemní data, je zapotřebí dbát na co největší bezpečnost, zároveň při prolomení bezpečnostních opatření by potencionální útočník mohl získat přístup do celé firemní sítě. Dále se předpokládá, že v takto propojených sítích bude zapotřebí vysoká rychlost vzniklého tunelu, z tohoto důvodu byla velká důležitost připsána i kritériu výkon.

Komerční VPN

Tabulka 13: Matice porovnání vybraných kritérií, modelová situace Komerční VPN

Komerční VPN	Výkon	Bezpečnost	Autentizace	Podpora v zařízeních	Jednoduchost použití
Výkon	1	1	5	2	2
Bezpečnost	1	1	5	2	2
Autentizace	1/5	1/5	1	1/2	1/2
Podpora v zařízeních	1/2	1/2	2	1	1
Jednoduchost použití	1/2	1/2	2	1	1

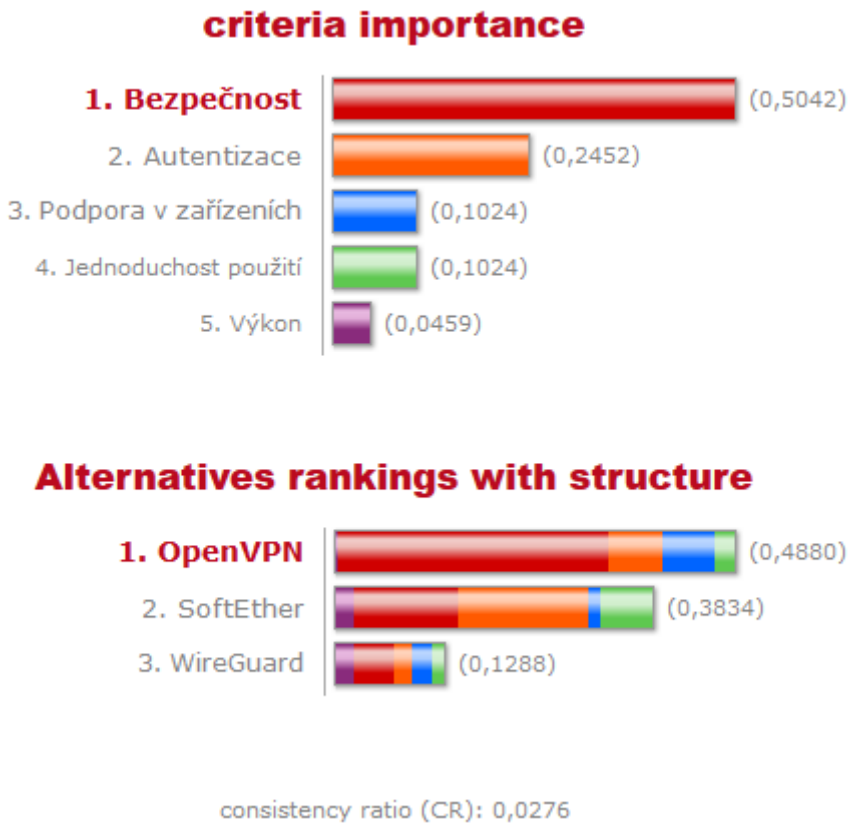
Zdroj: vlastní zpracování

Při výběru technologie serveru některého z poskytovatelů komerční VPN byl největší důraz kladen na výkon a bezpečnost, dále je důležité, aby byla zajištěna dostatečná podpora v zařízeních a také jednoduchost použití. Výkon se může hodit při zmiňovaných konferenčních hovorech. Z důvodu co nejvyššího komfortu by měla být také zajištěna dostatečná podpora v zařízeních a jednoduchost použití.

5.3 Vyhodnocení v jednotlivých modelových situacích

Vyhodnocení bylo realizováno v softwaru dostupném z http://123ahp.com/, který má integrován algoritmus pro výpočet pomocí Saatyho metody. Tento program na základě zadání párových preferencí doporučí nejoptimálnější řešení a vygeneruje také přehledné grafy, které zobrazují jednotlivé vlivy na konečný výsledek. Tento software také počítá CR. Jde o parametr konzistenčního poměru (Consistency Ratio), který hovoří o smysluplně sestavené Saatyho matici. Všeobecně je uplatňován požadavek CR <0.1. [16]

Vyhodnocení AHP v modelových situacích Remote Access

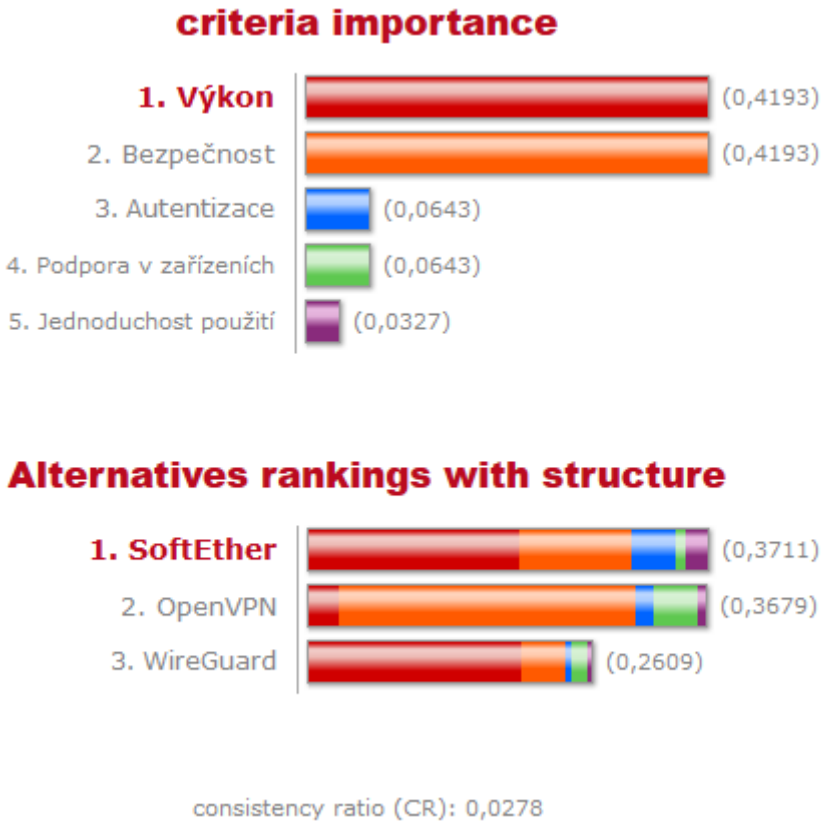


Obrázek 20: Graf s výsledky AHP v rámci Remote Access

Zdroj: vlastní zpracování v [16]

Jako nejlepší variantu pro VPN typu Remote Access bylo programem doporučeno řešení od OpenVPN. Na tomto rozhodnutí mělo největší váhu kritérium bezpečnosti, ve které si OpenVPN z porovnávaných variant vede nejlépe.

Vyhodnocení AHP v modelových situacích Site to Site

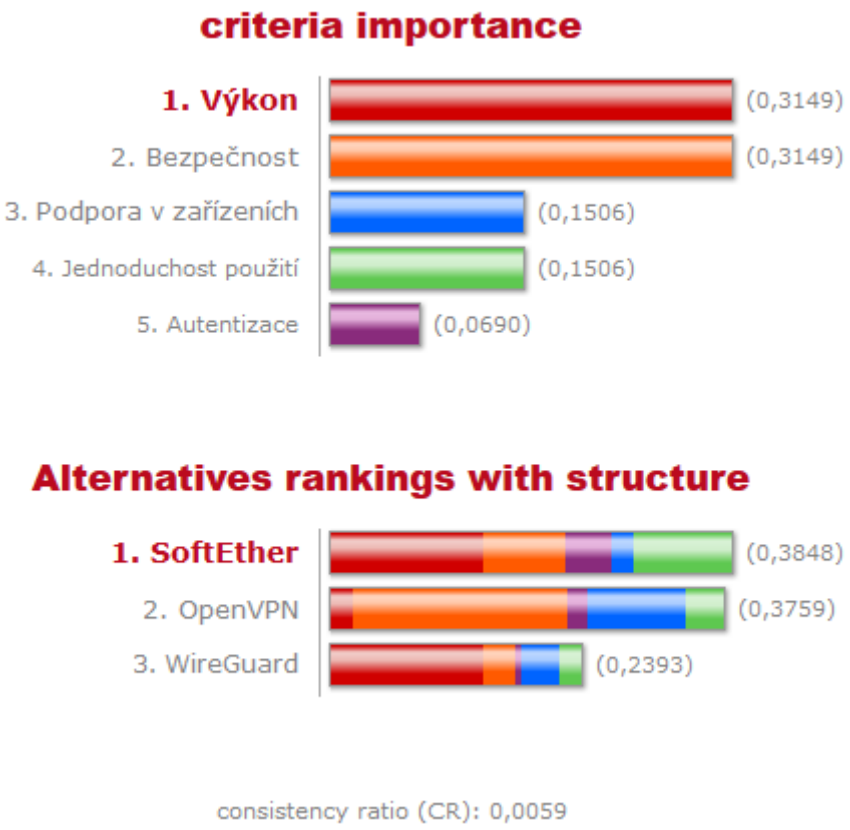


Obrázek 21: Graf s výsledky AHP v rámci Site to Site

Zdroj: vlastní zpracování v [16]

V rámci ohodnocení variant pro modelové situace kategorie Site to Site se jeví jako nejlepší řešení od SoftEther. Nicméně tento model neukazuje jasného favorita. V takovémto rozhodování by zajisté hrály klíčovou roli reálné požadavky. Pokud bychom uvažovali situaci, ve které nebude zapotřebí takový výkon vzniklého tunelu mezi sítěmi, můžeme upřednostnit řešení od OpenVPN z důvodu jeho vyšší bezpečnosti.

Vyhodnocení AHP v modelových situacích Komerční VPN



Obrázek 22: Graf s výsledky AHP v rámci Komerční VPN

Zdroj: vlastní zpracování v [16]

Mnozí poskytovatelé služeb VPN připojení pro skrytí aktivit na internetu nabízejí možnost výběru technologie zajišťující připojení k jejich serverům. Tyto výsledky hodnotí používané technologie pro připojení v rámci poskytované služby. Z výsledků je zřejmé, že nejlepší variantou je řešení od SoftEther, především díky vysokému výkonu oproti OpenVPN. Pokud uživatel není schopen využít tento výkon, je poté lepší zvolit variantu s vyšší bezpečností, například OpenVPN.

ZÁVĚR

Cílem této bakalářské práce je přinést ucelený obraz o technologiích VPN a jejich využití v moderní síťové infrastruktuře. Toho bylo dosaženo doporučením vhodné aplikace pro použití ve stanovených modelových situacích. Tyto modelové situace byly zvoleny na základě rozhovorů s odborníky z jednotlivých firem, kde technologie VPN využívají. Protože v každé modelové situaci je kladen důraz na různá kritéria, jsou alternativy hodnoceny pro každou situaci zvlášť.

Doporučení bylo stanoveno na základě multikriteriálního rozhodování, při kterém byla použita Saatyho metoda. Do komparace byly zařazeny řešení SoftEther, OpenVPN a WireGuard. Tyto programy byly autorem práce vybrány tak, aby byly zdarma i pro komerční použití, měli otevřený zdrojový kód, byly kompatibilní s platformou Windows i Linux a reflektovaly současné trendy v moderní síťové infrastruktuře. Jednotlivé alternativy byly hodnoceny v rámci kritérií výkon, bezpečnost, autentizace, podpora v zařízeních a jednoduchost použití.

Pomocí metody AHP, na základě ohodnocení párových preferencí a vah kritérií, bylo jako nejlepší alternativa v modelové situaci „Vzdálený přístup“, vyhodnocena OpenVPN. V této modelové situaci byl kladen největší význam kritériu bezpečnost, proto řešení od OpenVPN tak významně převýšilo nad ostatními. V případě „Propojení více sítí“ a „Komerční VPN“ řešení od SoftEther. V těchto modelových situacích nicméně není výsledek až tak zřejmý a výsledné doporučení by případně záleželo na očekáváních firmy. Pokud by byla dostačující rychlost do 100 Mbps, bylo by doporučeno spíše OpenVPN, které se dá považovat za bezpečnější, bohužel však nedosahuje vyšších rychlostí.

Je také vhodné zmínit řešení od WireGuard. I přes velký důraz na zabezpečení, toto řešení bylo hodnoceno jako nejhorší z hlediska bezpečnosti. Pravděpodobně je to kvůli krátkému působení na trhu, z čehož pramení dosavadní nedůvěra. V následujících letech se však dá předpokládat, že popularita tohoto řešení poroste, hlavně s přibývajícím množstvím nezávislých bezpečnostních analýz.

POUŽITÁ LITERATURA

[1] DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. 2., aktualit. vyd. Praha: Computer Press, 2003. ISBN 80-7226-849-X.

[2] OLIFER, Natalia a Victor OLIFER. Computer networks: principles, technologies and protocols for network design. Chichester: John Wiley, c2006. ISBN 0-470-86982-8

[3] PUŽMANOVÁ, Rita. TCP/IP v kostce. České Budějovice: Kopp, 2004. ISBN 80-7232-236-2

[4] SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Přeložil Josef POJSL, přeložil Pavel VAIDA. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7

[5] VPN Technologies: Definitions and Requirements. *Virtual Private Network Consortium -- VPNC* [online]. 2008 [cit. 2020-04-12]. Dostupné z: http://www.vpnc.org/vpn-technologies.html

[6] Secure Remote Access (SSL VPN). *Technology, Life and other sutff that come along* [online]. 2006 [cit. 2020-04-12]. Dostupné z: http://nirlog.com/2006/01/23/secure-remote-access-ssl-vpn/

[7] Srovnání VPN Protokolů: PPTP vs. L2TP vs. OpenVPN vs. SSTP vs. IKEv2 [online]. In: . [cit. 2020-04-17]. Dostupné z: https://cs.vpnmentor.com/blog/srovnani-vpn-protokolu-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/

[8] *OpenVPN project Wiki / Tracker* [online]. In: . [cit. 2020-04-20]. Dostupné z: https://community.openvpn.net/openvpn/wiki

[9] *SoftEther VPN* [online]. [cit. 2020-04-20]. Dostupné z: https://www.softether.org/

[10] *Datová centra* [online]. In:. [cit. 2020-06-16]. Dostupné z: https://www.unismini.cz/cs/datova-centra

[11] *Varování: probíhá útok na RDP protokol pro vzdálený přístup k počítači* [online]. In: . [cit. 2020-07-02]. Dostupné z: [11] https://www.idnes.cz/technet/internet/kyberutoky-kyberutok-na-rdp-protokol-vzdaleny-pristup-cr-cesko-bitdefender-brute-force-utok-kyberbez.A200702_122503_sw_internet_nyv?

[12] *40 Years of Microprocessor Trend Data* [online]. In: . [cit. 2020-07-02]. Dostupné z: https://www.karlrupp.net/2015/06/40-years-of-microprocessor-trend-data/

[13] NOBORI, Daiyuu. *Design and Implementationof SoftEther VPN* [online]. In: . 16.1.2013, s. 53 [cit. 2020-07-07]. Dostupné z: https://www.softether.org/@api/deki/files/399/=SoftEtherVPN.pdf

[14] *WireGuard: fast, modern, secure VPN tunnel* [online]. [cit. 2020-07-07]. Dostupné z: https://www.wireguard.com

[15] FOTR, Jiří a Lenka ŠVECOVÁ. *Manažerské rozhodování: postupy, metody a nástroje*. 2., přeprac. vyd. Praha: Ekopress, 2010. ISBN 978-80-86929-59-0.

[16] *123AHP: my choice, my decision* [online]. [cit. 2020-07-08]. Dostupné z: http://123ahp.com/Default.aspx

[17] *What Is OpenVPN & Is It Safe Enough To Use In 2020?* [online]. [cit. 2020-07-13]. Dostupné z: https://www.vpnmentor.com/blog/what-is-openvpn-is-it-safe-enough-to-use/

[18] KŘUPKA, Jiří, Miloslava KAŠPAROVÁ a Renáta MÁCHOVÁ. *Rozhodovací procesy* [online]. Pardubice: Univerzita Pardubice, 2012 [cit. 2020-07-18]. ISBN 978-80-7395-478-9. Dostupné z: https://docplayer.cz/1157600-Jiri-krupka-miloslava-kasparova-renata-machova.html

[19] *WireGuard: moderní a snadno použitelná VPN v linuxovém jádře* [online]. [cit. 2020-07-26]. Dostupné z: https://www.root.cz/clanky/wireguard-moderni-a-snadno-pouzitelna-vpn-v-linuxovem-jadre/

[20] *Mozilla VPN* [online]. [cit. 2020-07-26]. Dostupné z: https://vpn.mozilla.org/

[21] *NordVPN: You're Getting a Speed Boost, Thanks to WireGuard Implementation* [online]. [cit. 2020-07-26]. Dostupné z: *https://www.pcmag.com/news/nordvpn-youre-getting-a-speed-boost-thanks-to-wireguard-implementation*