Možnosti bezpečného VPN přístupu

Bc. Matúš Gavenda

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Matúš Gavenda**
Osobní číslo:	**A18340**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Forma studia:	**Prezenční**
Téma práce:	**Možnosti bezpečného VPN přístupu**
Téma práce anglicky:	**Secure VPN Access Options**

Zásady pro vypracování

1. Analyzujte stávající VPN protokoly a jejich zranitelnosti.
2. Specifikujte požadavky na VPN cluster.
3. Navrhněte VPN cluster postavený na technologii SoftEther.
4. Implementujte cluster v testovací infrastruktuře.
5. Otestujte VPN cluster, funkční a bezpečnostní testy. Stanovte limity dle zvoleného HW.

Forma zpracování diplomové práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. CRIST, F Eric; Jan Just KEIJSER. Mastering OpenVPN. Birmingham: PacktPublishing, 2015. ISBN 1-78355-314-6
2. Lewis, Mark. Comparing, Designing. And Deploying VPNs. místo neznámé : AdobePress, 2006.
3. TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. Praha: Grada,2009,384 s. Profesionál. ISBN 978,80-247-2098-2.
4. University of Tsukuba Japan. SoftEther VPN Project [online]. [cit. 2019-04-09].Dostupné z: https://www.softether.org/
5. Scott, Charlie, Wolfe, Paul a Erwin, Mike. Virtual Private Networks, Second Edition. místo neznámé : O'Reilly, 1999. 1-56592-529-7.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
Děkan
L.S.

Ing. Miroslav Matýsek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

Matúš Gavenda, v.r.
podpis studenta

ABSTRAKT

Hlavným cieľom diplomovej práce je oboznámenie čitateľa s možnosťami bezpečného VPN prístupu. Riešenie práce zahŕňa oboznámenie sa s možnosťami vytvorenia VPN clusteru v programe Softether, návrhu vlastného clusteru, jeho nastavenie a následné testovanie a určenie hardvérových limitov jednotlivých členov clusteru.

Úlohou teoretickej časti práce je zoznámenie čitateľa s problematikou VPN a s najčastejšie využívanými protokolmi, ktoré sú využívané pri týchto sieťach. Taktiež je v tejto časti definovanie požiadaviek na VPN cluster.

Praktická časť je zameraná na návrh vlastného VPN clusteru v programe Softether, testovanie jeho funkčnosti a nastavenie zabezpečenia. Tiež sú v tejto časti popísané záťažové testy pomocou ktorých bola táto sieť testovaná a vymedzenie hardvérových limitov pre navrhovaný cluster. Testovanie je doplnené syntaxou využívanou pri tvorení tejto práce.

Kľúčové slová: VPN, cluster, VMware, bezpečnosť, testovanie, softvér, nástroj

ABSTRACT

The main aim of this diploma thesis is to acquaint the reader with the possibilities of secure VPN access. The solution includes getting acquainted with the possibilities of creating a VPN cluster in the program called Softether, designing own cluster, its setup and subsequent testing and determining the hardware limits of individual cluster members.

The task of the theoretical part of this thesis is to acquaint the reader with the problems of VPN and the most used protocols that are used in these networks. There is also a definition of VPN cluster requirements in this part of diploma thesis.

The practical part is focused on the design of own VPN cluster in the Softether program, testing its functionality and security settings. This part also describes the stress tests with which this network was tested and hardware limits for the proposed cluster. Testing is supplemented by the syntax used in creating this thesis.

Keywords: VPN, cluster, VMware, security, testing, software, tool

Ďakujem Ing. Davidovi Malaníkovi, Ph.D., vedúcemu diplomovej práce, za jeho čas, cenné nápad a konštruktívnu kritiku. Taktiež ďakujem aj mojej rodine a kamarátom, za podporu počas celej doby môjho štúdia.

Prehlasujem, že odovzdaná verzia diplomové práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

Diplomová práca sa zaoberá návrhom, zostrojením a otestovaním bezpečnej súkromnej virtuálnej siete (VPN), presnejšie siete založenej na technológii clusteru. Hlavnou úlohou takto zostrojenej siete je zabezpečiť jej funkčnosť a zistiť hardvérové limity tejto siete. Celá diplomová práca je rozdelená na teoretickú a praktickú časť.

Teoretická časť sa skladá z troch kapitol, kde v prvej kapitole je obsiahnutý základný úvod do problematiky VPN. Presnejšie ide o vysvetlenie, čo to vlastne VPN je, jej rozdelenie, požiadavky na bezpečnosť a iné požiadavky závislé na využití siete. Následne sú čitateľovi predstavené najčastejšie používané VPN protokoly pri ktorých je vysvetlený ich princíp fungovania, výhody a nevýhody ich využitia a poukázanie na priame chyby v zabezpečení týchto protokolov pomocou CVE kódov. Ako posledné sú definované požiadavky na VPN cluster. Čitateľovi je vysvetlené k čomu slúžia radiče, členské servery, akým štýlom cluster vyrovnáva zaťaženie na sieti a akým štýlom reaguje na chyby.

V praktickej časti práce ide o samotný návrh clusteru v programe Softether, ktorý bol v tejto práci využitý pre vytvorenie. Návrh obsahuje aj syntax príkazov využitých pri zostrojovaní a následnom nastavovaní takto vytvoreného clusteru. Pri návrhu clusteru je taktiež ukázané základné zabezpečenie nastavením jednotlivých užívateľských skupín a taktiež nastavením access listov. Záver práce je venovaný záťažovým testom clusteru. Pre monitorovanie zaťaženia bol využitý nástroj Cockpit. Testovanie prebiehalo pomocou dvoch nástrojov slúžiacich pre zistenie hardvérových limitov siete.

Ku každému z testov je pripojená syntax príkazu ktorý bol využitý a celé testovanie je doplnené grafmi pre prehľadnejšie zobrazenie zaťaženia. V prílohe je taktiež pripojený výpis z testovania k bližšiemu doplneniu týchto grafov.

Práca ako celok slúži pre poukázanie na to, že k vytvoreniu VPN možno využiť, namiesto súčasne používaných riešení, aj takúto možnosť.

I. TEORETICKÁ ČASŤ

1 VIRTUAL PRIVATE NETWORK

Virtual Private Network (ďalej len VPN) je technológia, ktorá umožňuje zriadenie služieb súkromnej siete pre užívateľa alebo organizáciu pomocou verejnej, prípadne zdieľanej infraštruktúry. Medzi takúto infraštruktúru patrí napríklad Internet, ale aj chrbticová sieť (backbone) od poskytovateľa internetových služieb. Táto sieť je známa ako chrbtica VPN a slúži ako komunikačný bod pre viac sietí VPN, prípadne pre prevádzku bez VPN.

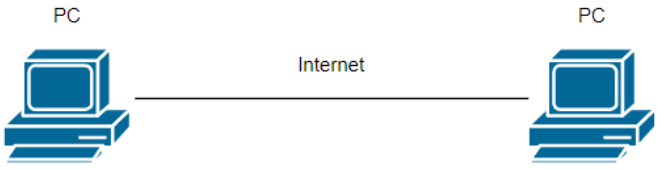
Obecne sa pri VPN jedná o systém medzi sebou prepojených zariadení vytvárajúcich zabezpečenú súkromnú sieť. Do tejto siete môžu byť pripojené aj zariadenia, ktoré sa nachádzajú na iných geografických lokáciách. Všetky dáta, ktoré sú posielané v tejto sieti, sa prenášajú cez takzvaný šifrovaný tunel, ktorý je vytvorený medzi týmito zariadeniami. Takýmto spôsobom dochádza k navýšeniu bezpečnosti pri prenášaní dát po takto vytvorenej sieti. V praxi sa môžeme stretnúť s takto nastavenou VPN napríklad vo firme s viacerými pobočkami pre ich prepojenie na centrálnu sieť firmy.

S navýšením bezpečnosti prichádza aj ďalšia výhoda využívania VPN a tou je aj ochrana súkromia. Pomocou VPN dokážeme skryť vyhľadávanie a históriu vyhľadávania na Internete. Je to umožnené tým, že je naša webová aktivita spojená s IP adresou VPN a nie adresou získanou od poskytovateľa internetového pripojenia.

1.1 Typy VPN

VPN sa môže deliť na 3 základné typy:

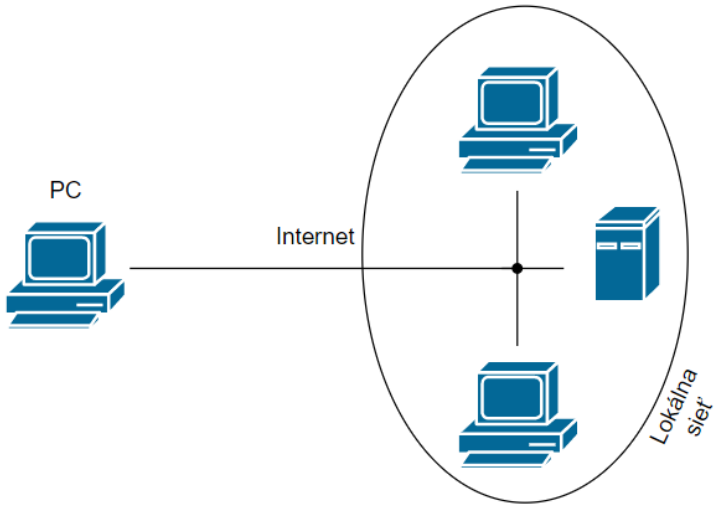
- Spojenie typu **point-to-point**. V súčasnosti predstavuje asi najpoužívanejší typ spojenia pri VPN. Jedná sa o trvalé priame komunikačné spojenie medzi dvoma stranami. V závislosti od typu môže byť toto spojenie použité pre rôzne aplikácie. Často sú týmto spôsobom vzájomne prepojené počítačové centrá alebo firemné pobočky so svojim ústredím. [1]



Obrázok 1 Spojenie typu point-to-point

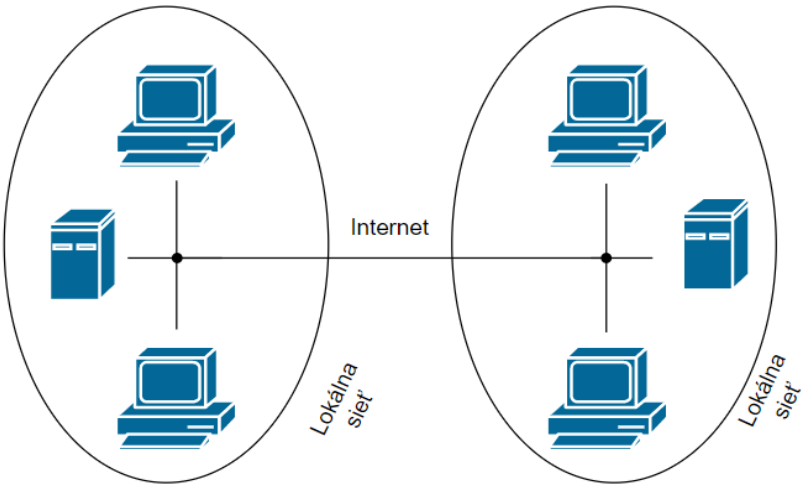
- Spojenie typu **point-to-site**. Toto spojenie umožňuje vytvoriť bezpečné pripojenie k VPN pomocou užívateľského zariadenia, napríklad počítača. Užívateľské

zariadenie toto pripojenie vytvorí a začne komunikáciu so sieťou ku ktorej pristupuje. Príkladom tohto spojenia môže byť pripojenie zamestnanca do firemnej siete zo vzdialeného miesta (iného mesta, apod.). Tento zamestnanec teda môže pristupovať ku všetkým dátam zo siete tak, akoby bol priamo vo firme. [2]



Obrázok 2 Spojenie typu point-to-site

- Spojenie typu **site-to-site**. Ako už vypovedá z názvu, ide o spojenie medzi dvoma alebo viacerými sieťami, napríklad medzi hlavnou podnikovou sieťou a sieťou pobočiek v rôznych častiach sveta, ktoré potrebujú neustály prístup a používanie podnikovej siete. Vďaka tomuto spojeniu môže spoločnosť bezpečne prepojiť svoju podnikovú sieť so vzdialenými kanceláriami. Pri komunikácií a zdieľaní zdrojov sa toto spojenie chová ako jedna veľká sieť. [3]



Obrázok 3 Spojenie typu site-to-site

1.2 Bezpečnosť VPN

VPN v dnešnej dobe plní hlavne úlohu zabezpečenej komunikácie medzi používateľmi. Kľúčovou požiadavkou na kvalitnú VPN je teda bezpečnosť tejto siete. V nasledujúcich odrážkach sú uvedené základné bezpečnostné požiadavky:

- **Autorizácia** – Bezpečnostný mechanizmus pre určovanie úrovní prístupu alebo privilégií užívateľov/klientov. Súvisí s udeľovaním alebo odmietaním prístupu k sieťovým prostriedkom. Umožňuje užívateľovi prístup k rôznym zdrojom nachádzajúcich sa na sieti, na základe jeho totožnosti a nastavených práv. [4] [5]
- **Autentifikácia** – Proces využívaný pre preukázanie toho, či daný používateľ alebo entita je skutočne tou, za ktorú sa vydáva. Všeobecne sa v rámci VPN využívajú 2 typy metód overovania. Buď *pomocou zdieľaných kľúčov* alebo *pomocou digitálneho podpisu*. V prípade zdieľaných kľúčov sú medzi zariadeniami, ktoré chcú medzi sebou nastaviť VPN, nakonfigurované a zdieľané rovnaké kľúče. Nevýhodou takéhoto typu overovania je nízka škálovateľnosť. To znamená, že nie sú využiteľné vo väčších a rozsiahlejších sieťach, pretože tým narastá bezpečnostné riziko. [6]
- **Dôveryhodnosť** – Jej cieľom je zabezpečiť a zabrániť únikom súkromných dát. K zaisteniu bezpečného prenosu dát je využívané šifrovanie, pomocou ktorého sú dáta spracované do ťažko čitateľnej podoby využitím šifrovacieho algoritmu a kľúča. Možnosť úniku jednotlivých dát závisí od kvality zvoleného algoritmu, prípadne dĺžkou použitého kľúča, ktorým boli dáta šifrované. [7]
- **Integrita** – Požiadavka na to, aby prenášané dáta dorazili do svojho cieľa v takej podobe, v akej boli poslané. K narušeniu integrity môže dochádzať napríklad v prípade poškodenia týchto dát útočníkom, prípadne chybným spojením pri odosielaní. Správnosť poslaných dát je najčastejšie zaisťovaná pomocou hashovacích funkcií, ale môžu byť využité aj rôzne opravné kódy. [8] [9]

1.3 Ďalšie požiadavky na VPN

Na ďalšie požiadavky a vlastnosti v rámci VPN sietí sa zameriavame hlavne kvôli konkrétnemu využitiu danej siete. Môže to byť napríklad:

- **Rýchlosť** – Požiadavka na to, aby mala sieť požadovanú prenosovú rýchlosť, malé oneskorenie.

- **Ľahká rozšíriteľnosť** – Požiadavka na rýchle a lacné rozšírenie siete.
- **Spoľahlivosť** – Požiadavka na to, aby sieť pracovala bez možných výpadkov a porúch.

Existuje však aj množstvo ďalších požiadaviek na ktoré sa užívateľ zameria podľa svojich vlastných preferencií a spôsobu využitia danej siete.

2 VPN PROTOKOLY

VPN protokol je súbor pravidiel alebo pokynov, ktoré určia, ako sa budú naše údaje a dáta posielať medzi počítačom alebo iným zariadením a serverom VPN. Tieto protokoly majú jedinečné špecifikácie, ktoré na základe okolností ponúkajú užívateľom VPN rôzne výhody. Niektoré z týchto protokolov sa môžu špecializovať na súkromie, iné kladú dôraz na rýchlosť posielania dát a podobne. Siete VPN využívajú rôzne protokoly v závislosti na použitom zariadení podľa toho, na čo chceme toto zariadenie využívať a ako ho chceme využívať. Ako príklad môžeme uviesť VPN pri sledovaní streamovaných filmov, kde zvolíme sieť s menším počtom bezpečnostných opatrení ale vyššou rýchlosťou pre plynulé sledovanie. [10] [11]

V nasledujúcej kapitole som sa zameral na najznámejšie používané VPN protokoly IPsec, PPTP, L2TP, SSL, OpenVPN, WireGuard. Na ich základný princíp fungovania, výhody a nevýhody využitia a známe zraniteľnosti.

2.1 Internet Security Protocol (IPsec)

Zabezpečenie IPSec je štandardný súbor protokolov IETF medzi dvoma komunikačnými bodmi v sieti. IPsec zaisťuje autentifikáciu, integritu a dôveryhodnosť údajov. Definuje tiež šifrované, dešifrované ale aj autentifikované pakety. IPsec taktiež obsahuje aj protokoly potrebné na bezpečnú výmenu kľúčov a ich manažment. [12] [11]

Použitím IPsec protokolu, je možné vykonávať nasledujúce činnosti:

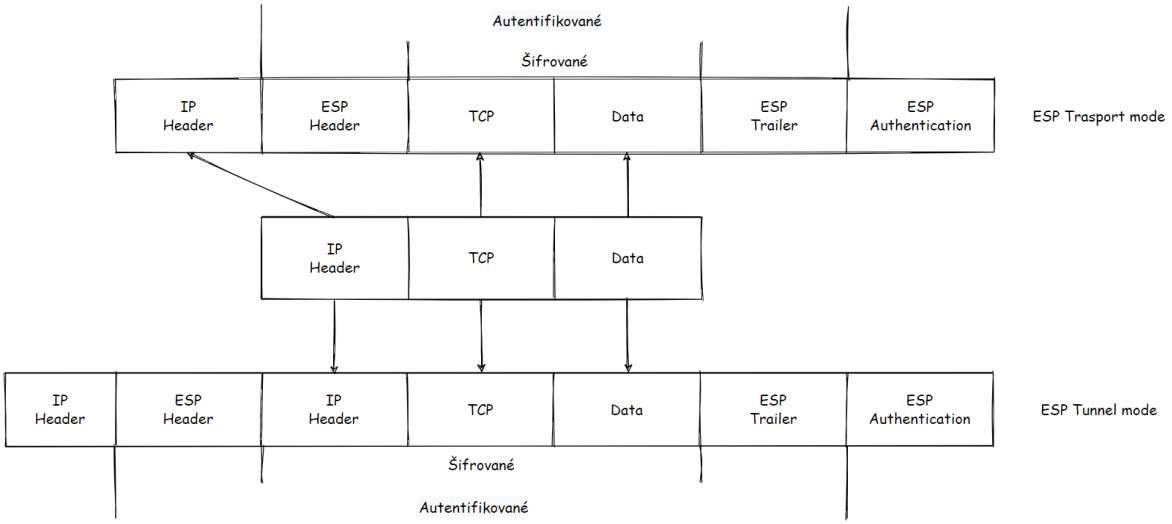
- šifrovanie dát aplikačnej vrstvy,
- zaistenie bezpečnosti smerovačov ktoré posielajú dáta cez verejný internet,
- poskytnutie autentifikácie bez šifrovania,
- ochranu sieťových dát nastavením obvodov používajúcich IPsec tunel, v ktorom sú všetky dáta, posielané medzi dvoma koncovými bodmi, zašifrované.

2.1.1 Encapsulating Security Payload (ESP)

Jedná sa o jeden z protokolov slúžiacich na zabezpečenie šifrovania a integrity dátových paketov. ESP sa vkladá za štandardnú hlavičku IP. Pretože je obsiahnutý za hlavičkou IP je ľahké ju smerovať pomocou bežných IP zariadení. Vďaka tomuto je protokol aj spätne

kompatibilný so smerovačmi IP a dokonca aj so zariadeniami, ktoré neboli pôvodne navrhnuté pre prácu s protokolom IPsec.

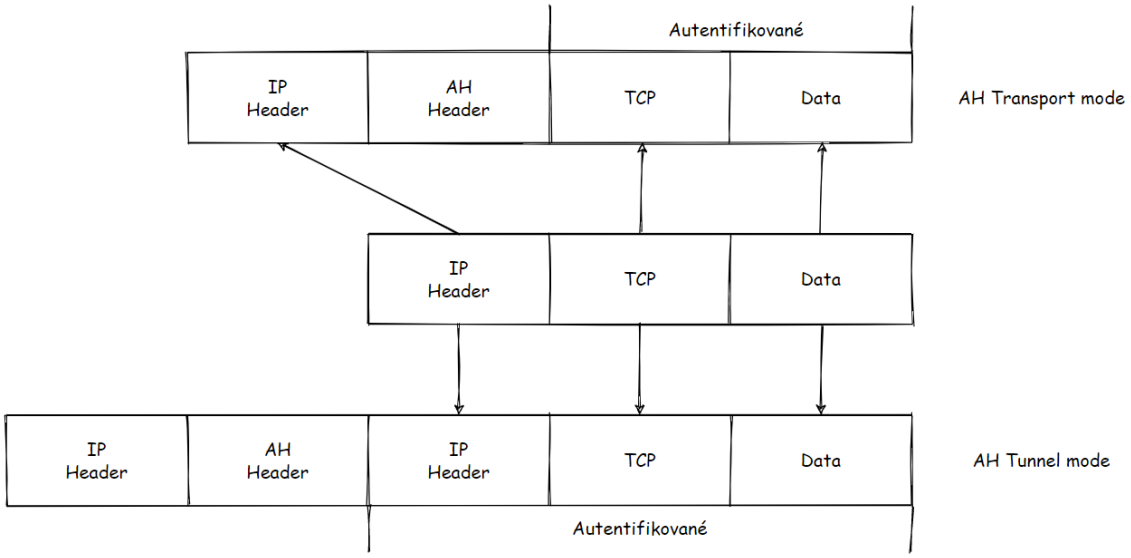
ESP pracuje na sieťovej vrstve s paketmi a skladá sa so šiestich častí, z ktorých dve slúžia na autentifikáciu (Security Parameter Index, Sequence Number), zatiaľ čo zvyšné štyri sú počas prenosu šifrované (Payload Data, Padding, Pad Length, Next Header). Podporuje aj veľké množstvo šifrovacích algoritmov a záleží len na používateľovi pre ktorý z nich sa rozhodne. Štandardne je pre šifrovanie dát využitý DES, ktorý ale nie je v dnešnej dobe považovaný za bezpečný. Z tohto dôvodu je využívaná jeho vylepšený variant 3DES. Môžu byť však použité aj ďalšie, ako napr. AES, Blowfish. [12] [13] [14]



Obrázok 4 IPsec ESP transportný a tunelový mód [15]

2.1.2 Authentication Header (AH)

V tomto protokole je zaisťovaná integrita dát a autenticita užívateľa. IP hlavička a dáta sú hashované pomocou jednosmerného hash kódu. Z tohto hash kódu je následne zostavená nová AH hlavička, ktorá je pripojená k paketu. Tento nový paket sa prenáša cez smerovač, kde smerovač použije hash na hlavičku a dáta. Je potrebné, aby obe tieto hodnoty hash boli rovnaké, inak dochádza k porušeniu integrity dát. [12] [13] [14]



Obrázok 5 IPsec AH transportný a tunelový mód [16]

2.1.3 Režimy šifrovania

Pre protokol IPSec sú k dispozícii dva režimy šifrovania. Oba tieto režimy majú svoje vlastné využitie a mali by sa používať opatrne v závislosti od jednotlivého riešenia.

- **Tunelový mód** – Použitý v prípade prepojenia celej siete. Šifrované dáta sú potom posielané iba medzi bránami jednotlivých sietí. Technicky tunelový mód funguje tak, že sa zoberie celý IP paket. Následne je tento paket zašifrovaný, zabalený do ESP a je k nemu priložená nová IP hlavička. Táto IP hlavička obsahuje adresy brán pripojených sietí. Z čoho vyplýva, že sa tunelový mód chová ako klasická VPN.
- **Transportný mód** – V prípade tunelového módu je časť ESP paketu, ktorá obsahuje šifrovanú transportnú hlavičku a dáta, chránená kontrolným súčtom. Je tým zamedzená prípadná zmena týchto dát. IP hlavička však nie je vôbec chránená. Na podobnom princípe funguje aj protokol AH. Rozdiel spočíva v tom, že v transportnom móde je, na rozdiel od módu tunelového, kontrolným súčtom chránená aj časť IP hlavičky.

  Tento variant je využívaný medzi koncovými zariadeniami a nevyžaduje pomoc routerov nachádzajúcich sa v ceste. Jeho hlavnou výhodou je, že sú všetky dáta chránené počas celej svojej púte od odosielateľa k cieľu. [13] [17] [11]

2.1.4 ISAKMP/IKE

K tomu, aby sme dokázali zapuzdriť alebo rozbaliť paket využívajúci ESP alebo AH, je potrebné poznať algoritmus, tajný kľúč a niektoré ďalšie údaje. Všetky tieto potrebné informácie sú uložené v Security Association (SA). S pomocou definovaných IPSec protokolov ponúka SA ochranu údajov pre jednosmerný prenos dát. Všeobecne ale platí, že tunel IPSec má dva jednosmerné SA, ktoré poskytujú bezpečný, plne duplexný kanál pre prenos dát. Všetky asociácie sú uložené v jednej centrálnej databáze Security Association Database. Tieto množiny SA uložené v databáze obsahujú:

- zdrojovú alebo cieľovú IP adresu, prípadne rozsah týchto adries,
- výber IPSec protokolu (AH alebo ESP),
- šifrovací algoritmus a tajný kľúč,
- security parameter index– jednoznačný ukazovateľ na SA zapísaný ako 32 bitové číslo v hlavičke IP paketu.

Podľa zvolenej implementácie môžu niektoré množiny obsahovať:

- **Životnosť SA** – Môže sa vytvárať buď manuálne alebo dynamicky, kde pri manuálnom vytvorení nemá určený čas životnosti, zatiaľ čo pri dynamickom vytvorení SA je určená doba platnosti.
- **Režim šifrovania** – Informácia o tom, či je použitý tunelový alebo transportný mód.

Všetky tieto parametre je možné nastaviť manuálne, avšak výmena šifrovacích algoritmov a kľúčov sa stáva problematickou, pretože tieto dáta musia byť zdieľané medzi jednotlivými zariadeniami v sieti. Z toho dôvodu je využitý protokol Internet Key Exchange. Tento protokol zaisťuje výmenu týchto dát tak, že vytvára bezpečný komunikačný kanál medzi zariadeniami, ktoré si dohodnú s akým šifrovacím a hashovacím algoritmom budú pracovať, zvolia si autentizačnú metódu a prípadne ďalšie potrebné informácie.

IKE protokol pracuje v dvoch fázach, kde sa v prvej fáze stanoví tzv. ISAKMP SA ktorého cieľom je dohodnúť všetky parametre prenosu. Po dohodnutí a použití všetkých parametrov prechádza do fáze číslo dva. V tejto fáze, pomocou dohodnutých parametrov, zavedie ďalšie bezpečnostné parametre a tiež IPSec SA, ktorý je potrebný pre bezpečný prenos dát.

Internet Security Association and Key Management Protocol je protokol, slúžiaci na definovanie mechanizmu zavedenia protokolu pre výmenu kľúča a jednotlivých vlastností zabezpečenia. V súčasnosti podporuje iba jeden protokol a to je IKE. [12] [13] [14]

2.1.5 Zraniteľnosť

V nasledujúcej podkapitole sú v tabuľke ukázané známe zraniteľnosti protokolu IPsec podľa webovej stránky CVE s ich základným popisom.

CVE-2020-5938	Na BIG-IP 13.1.0-13.1.3.4, 12.1.0-12.1.5.2 a 11.6.1-11.6.5.2, pri vyjednávaní IPsec tunelov s nakonfigurovanými a overenými užívateľmi, môže tento užívateľ vyjednať rozdielnu dĺžku kľúča než umožňuje BIG-IP konfigurácia.
CVE-2020-3220	Zraniteľnosť v hardvérovom krypto ovládači Cisco IOS XE softvéru pre Cisco 4300 sériu integrovaných servisných routerov, ktoré povoľujú neoverenému útočníkovi odpojiť IPsec VPN relácie od postihnutého zariadenia.
CVE-2020-3190	Zraniteľnosť v IPsec paketovom procesore softvéru Cisco IOS XR, ktorá môže neoprávnenému útočníkovi umožniť postihnutému zariadeniu DoS útok na relácie protokolu IPsec

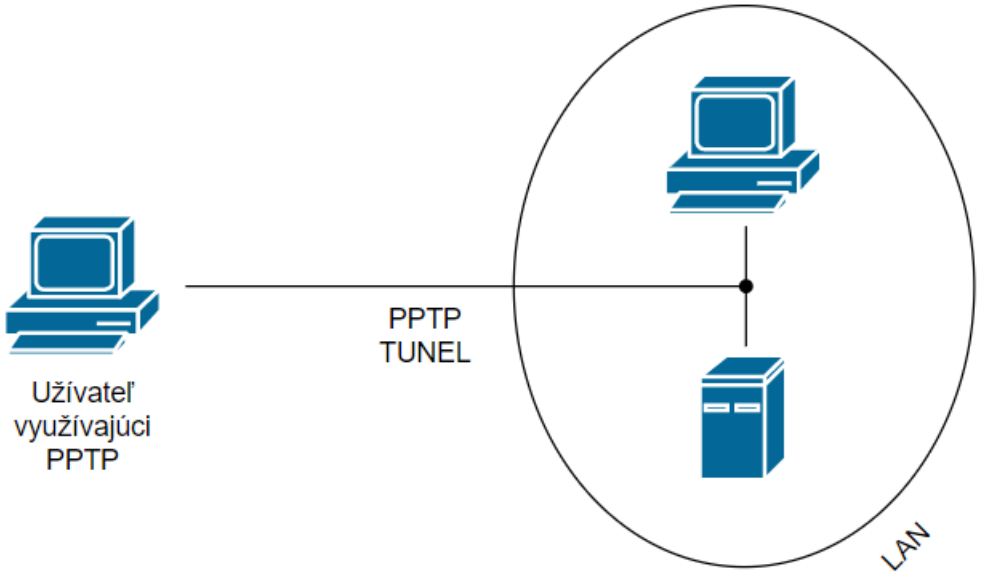
Tabuľka 1 CVE kódy pre IPsec [18]

2.2 PPTP – Point-To-Point Tunneling Protocol

PPTP je v dnešnej dobe zastaraná metóda implementácie VPN. K svojej činnosti využíva protokol Point-to-Point. Tento protokol slúži na nadviazanie komunikácie medzi dvoma bodmi. PPTP nad touto komunikáciou vytvára tunely, ktoré sú nastavované užívateľom.

2.2.1 PPTP Tunel

K vytvoreniu PPTP tunelu dochádza v dvoch krokoch. V prvom kroku sa užívateľ spojí k prístupovému serveru pomocou Point-to-Point protokolu. Následne je ale hneď toto spojenie ukončené. V druhom kroku je spustený PPTP klient a nad TCP portom 1723 sa vytvorí riadiace spojenie s požadovaným serverom PPTP, ku ktorému má užívateľ prístupové práva. Tento tunel je teda vytvorený PPTP serverom bez toho, aby sa komunikácie zúčastnil aj prístupový server. [19] [20] [11]



Obrázok 6 PPTP Tunel [21]

2.2.2 Výhody a nevýhody

PPTP bol v minulosti veľmi rozšírený vďaka spoločnosti Microsoft, ktorá ho často propagovala v produktoch či dokonca aj ako súčasť ich operačného systému. Práve preto boli tieto siete realizované u firiem s požiadavkou na jednoduchý prístup do podnikovej siete bez zložitej inštalácie. Táto vlastnosť je aj najväčšou výhodou a dôvodom, prečo boli tak obľúbené.

Nevýhodou PPTP protokolu je to, že nie je presne definovaný spôsob, ktorým má prebiehať overovanie a šifrovanie dát. Je teda možné, že pri komunikácií medzi dvoma zariadeniami od rôznych výrobcov, bude každé zariadenie overovať a šifrovať dáta svojim vlastným spôsobom a tým medzi nimi neprebehne komunikácia. [19] [20] [11]

2.2.3 Zraniteľnosť

V nasledujúcej podkapitole sú v tabuľke ukázané známe zraniteľnosti protokolu PPTP podľa webovej stránky CVE s ich základným popisom.

CVE-2018-13366	Zraniteľnosť pri sprístupňovaní informácií vo Fortinet FortiOS 6.0.1, 5.6.7 a nižšie, umožňujúce útočníkovi odhaliť sériové číslo FortiGate pomocou názvu hostiteľa definovaného v paketoch kontrolujúcich pripojenie protokolu PPTP
CVE-2017-15637	Zariadenia TP-LINK WVR, WAR a ER umožňujú vzdialeným overeným správcom vykonávať ľubovoľné príkazy

	prostredníctvom vkladania príkazov do premennej *pptphellointerval* v súbore *pptp_server.lua*.
CVE-2016-6398	Server PPPT v systéme Cisco IOS 15.5 (3) nesprávne inicializuje vyrovnávanie pamäte paketov, čo umožňuje útočníkom získať citlivé informácie zo staršej sieťovej komunikácie čítaním paketových údajov.

Tabuľka 2 CVE kódy pre PPTP [18]

2.3 Layer 2 Tunneling Protocol (L2TP)

Ide o novší typ protokolu, ktorý vznikol skombinovaním staršieho štandardu L2F od spoločnosti CISCO a tiež štandardu PPTP od spoločnosti Microsoft popísaného vyššie. Existuje aj verzia tohto protokolu využívajúca aj protokol IPSec pre zaistenie dôveryhodnosti dát, nazývajúca sa L2TP/IPSec

2.3.1 Princíp fungovania

Protokol funguje s dvoma základnými prvkami: *prístupový koncentrátor* (L2TP Access Concentrator) a *sieťový server* (L2TP Network Server). V prístupovom koncentrátore, je fyzicky ukončený vytáčaný hovor. Sieťový server slúži pre zakončenie a prípadnú autentizáciu dátového toku.

Princíp vytvorenia tunelu pre pripojenie užívateľa do siete pri L2TP funguje nasledovne:

- Point-to-Point spojenie k poskytovateľovi pripojenia je zahájené užívateľom.
- Spojenie je následne prijaté prístupovým koncentrátorom.
- Užívateľ sa spolu so sieťovým serverom dohodne na parametroch LCP protokolu.
- V čase dohadovania parametrov taktiež prebehne overenie užívateľa pomocou prístupového koncentrátoru.
- Akonáhle je užívateľ overený, je presmerovaný na koncový bod, teda na sieťový server. V opačnom prípade je mu prístup na server zamietnutý.
- Následne prichádza k vytvoreniu tunelu medzi oboma koncami (medzi LAC a LSN).
- Po úspešnom vytvorení tunelu je vytvorená komunikačná relácia L2TP. Pomocou tejto relácie je užívateľ schopný pristupovať do podnikovej siete. [20]

2.3.2 Výhody a nevýhody

Hlavnou výhodou L2TP protokolu je vysoká miera zabezpečenia, ktorá neobsahuje zásadné bezpečnostné riziká. Protokol využíva 256 bitové šifrovanie jeho kľúčov. Toto šifrovanie však samotný protokol nezabezpečuje, preto je k nemu používaný zvyčajne aj IPSec štandard. Medzi ďalšie výhody patrí: vysoká kompatibilita, ľahká inštalácia, stabilita a prevencia proti možným útokom MITM (Man-In-The-Middle).

Nevýhodou tohto protokolu je menšia rýchlosť, čo je spôsobené práve vysokou mierou zabezpečenia. Zvyčajne sa pre zvýšenie rýchlosti využíva pripojenie OpenVPN. Ďalšími nevýhodami sú využívanie zdieľaných kľúčov pri prenose dát, podpora limitovaného počtu portov (ľahko zablokovateľné firewallom) a náchylnosť na odpočúvanie siete pomocou zachytených zdieľaných kľúčov. [20]

2.3.3 Zraniteľnosť

V nasledujúcej podkapitole sú v tabuľke ukázané známe zraniteľnosti protokolu L2TP podľa webovej stránky CVE s ich základným popisom.

CVE-2020-7465	L2TP implementácia s názvom MP2 pred verziou 5.9 umožňuje útočníkovi, ktorý môže poslať špeciálne vytvorený riadiaci paket L2TP s kódom AVP Q.931, vykonanie ľubovoľného kódu alebo DoS (poškodenie pamäte).
CVE-2017-8338	Zraniteľnosť v programe MikroTik 6.38.5 umožňujúca neoverenému útočníkovi vyčerpanie CPU záplavou paketov UDP na port 500 (je využívaný pre L2TP cez IPsec), čo má za následok odpojenie všetkých zariadení od smerovača a odstránenie protokolov.
CVE-2015-6267	Cisco IOS XE pred verziou 2.2.3 za zariadeniach ASR 1000 umožňuje DoS prostredníctvom vytvoreného paketu L2TP.

Tabuľka 3 CVE kódy pre L2TP [18]

2.4 Secure Socket Layer (SSL)

Protokol SSL definuje spôsoby šifrovania medzi stranami, ktoré spolu komunikujú a ich overovania. Často sa uvádza označenie SSL/TLS a to z dôvodu, že protokol SSL je vo svojej verzii 3.0 minimálne rozdielny so svojím nasledovníkom - protokolom TLS.

Pre zaistenie zvýšenej bezpečnosti protokol SSL využíva symetrické a asymetrické šifrovanie. Pred naviazaním komunikácie si obe strany overia svoju totožnosť pomocou asymetrickej šifry. Po tomto úspešnom overení pokračujú v komunikácií za pomoci rýchleho symetrického šifrovania. Integrita dát v takto realizovanej komunikácií býva zaisťovaná hashovacími funkciami. [22] [11]

2.4.1 Výhody a nevýhody

Sieť VPN využívajúca protokol SSL poskytuje rôzne výhody. K vytvoreniu bezpečnej SSL VPN siete nie je potrebný žiaden prídavný softvér a zdĺhavé nastavovanie. Tento protokol je v dnešnej dobe obsiahnutý v každom internetovom prehliadači, takže k vytvoreniu tejto siete postačuje mať aktualizovaný internetový prehliadač. V tomto prípade je ale nutné pri vstupovaní do zabezpečenej siete poučovať užívateľov o používaní nezabezpečených zariadení, ktoré môžu byť potencionálnym bezpečnostným rizikom pre takúto sieť. Existujú však aj také SSL VPN ktoré umožňujú nastavenie parametrov, bez ktorých neumožnia prístup zariadeniam, pokiaľ tieto parametre nespĺňajú. Rovnako tak tento protokol umožňuje segmentovaný prístup, čo v praxi znamená, že užívatelia nemajú prístup ku všetkým zdrojom nachádzajúcim sa v sieti ku ktorej pristupujú, ale iba k časti ku ktorej požadujú prístup.

Nevýhodou použitia SSL protokolu môže byť to, že jeho použitie cez webové prehliadače má za následok iba obmedzené služby, ako napríklad prenos emailov, súbor, ... Pre využívanie viacerých služieb je nutná inštalácia ďalších klientov. V tomto prípade to ale znamená, že sieť stráca schopnosť ľahkej rozšíriteľnosti medzi ďalších užívateľov. [22] [11]

2.4.2 Zraniteľnosť

V nasledujúcej podkapitole sú v tabuľke ukázané známe zraniteľnosti protokolu SSL podľa webovej stránky CVE s ich základným popisom.

CVE-2021-28196	Špecifická funkcia ASUS BMC’s na webovej stránke neoveruje dĺžku reťazca zadanú užívateľmi, čo spôsobuje pretečenie vyrovnávacej pamäte.
CVE-2021-27189	Aplikácii CIRA Canadian Shield pred verziou 4.0.13 pre iOS chýba overenie certifikátu SSL.

CVE-2020-4340	IBM Security Secret Server pred 10.9 mohol útočníkovi umožniť obísť zabezpečenie SSL z dôvodu nesprávneho overenia certifikátu.

Tabuľka 4 CVE kódy pre SSL [18]

2.5 OpenVPN

OpenVPN je systém VPN implementujúci techniky pre vytvorenie bezpečných spojení typu Point-to-Point alebo Site-to-Site, a je vlastne protokolom VPN ale aj softvérom, ktorý je toto spojenie schopný vytvoriť. Mimo to, že je v dnešnej dobe najpopulárnejším protokolom, je to jediný open-source VPN protokol s vlastnou open-source aplikáciou.

Aplikácia OpenVPN je kompatibilná s veľkým množstvom operačných systémov (Linux, Windows, macOS, Android a mnoho ďalších). Je potrebné mať však na pamäti to, že aj keď zvládne toto množstvo, nie je kompatibilný s klientami VPN používajúcimi protokoly L2TP/IPsec alebo PPTP VPN. [11]

2.5.1 Princíp fungovania

Pre posielanie dát cez internet používa OpenVPN protokoly UDP alebo TCP. TCP a UDP sú protokoly pracujúce na transportnej vrstve, bežiace nad IP. Protokol TCP je najbežnejšie používanou možnosťou, pretože je spoľahlivý s možnosťou opravy chýb. Je taktiež známy ako stavový protokol. Pri každom odoslaní paketu pomocou protokolu TCP, odosielateľ čaká na potvrdenie o uvoľnení linky pre ďalší paket. Takéto posielanie má však zásadný dopad na rýchlosť spojenia. Zvyčajne sa to premieta na vyššej odozve, aj keď záleží aj od umiestnenia užívateľa a servera.

Druhým protokolom, ktorý môže OpenVN tiež používať, je protokol UDP. V tomto prípade je komunikácia medzi zariadením a serverom oveľa rýchlejšia. Dáta sa posielajú bez čakania na potvrdenie a nie sú opätovne preposielané ak nie sú prijaté. Preto sa tento protokol nazýva aj bezstavový. Vďaka menšiemu zaťaženiu pri prenose sa zrýchľuje odozva. Práve kvôli tomu sa tento protokol zvykne používať pre aplikácie, ktoré sú citlivejšie na zmenu odozvy, napríklad streamovanie videa alebo hranie online hier. [23] [11]

2.5.2 Bezpečnosť

V súčasnej dobe je OpenVPN považovaný za jeden z najbežnejšie a najčastejšie používaných protokolov. Za svoju bezpečnosť vďačí 256-bitovému šifrovaniu a používaným šifrovacím algoritmom (AEs, Camellia, 3DES, CAST-128 alebo Blowfish).

Touto kombináciou dosahuje vysokú mieru zabezpečenia a eliminuje možnosť dešifrovať prenášané dáta. Navyše, na základe auditu vykonaného v roku 2017, bolo dokázané, že OpenVPN obsahoval iba niekoľko menších chýb, ktoré však boli následne opravené. [23] [24] [11]

2.5.3 Výhody a nevýhody

Niektoré z výhod OpenVPN už boli spomenuté vyššie a to, napríklad, vysoká kompatibilita, zabezpečenie a taktiež to, že sa jedná o open-source VPN protokol. Ďalšou z výhod je, že podporuje takzvanú Perfect Forward Secrecy - veľmi bezpečnú metódu šifrovania, ktorá pomáha v boji proti mnohým online hrozbám. Taktiež nie je zachytávaný firewallmi a hĺbkovou paketovou kontrolou, takže VPN komunikácia pôsobí dojmom bežnej HTTPS komunikácie.

Nevýhodou OpenVPN je potreba prídavného softvéru. Takže aj keď je kompatibilný s obrovským množstvom operačných systémov, tie ho štandardne neobsahujú vo svojej programovej sade. Ďalšou z nevýhod je zložitý a rozsiahly užívateľský manuál a s tým spojené zložité nastavovanie. [24] [11]

2.5.4 Zraniteľnosť

V nasledujúcej podkapitole sú v tabuľke ukázané známe zraniteľnosti protokolu OpenVNP podľa webovej stránky CVE s ich základným popisom.

CVE-2020-9442	OpenVPN Connect 3.1.0.361 v systéme Windows má nezabezpečené povolenia pre %PROGRAMDATA%\ OpenVPN\ Connect\ drivers\ tap\ amd64\ win10, umožňujúce lokálnym užívateľom získať oprávnenie kopírovaním škodlivého súboru *drvstore.dll.*
CVE-2020-8953	OpenVPN Access Server 2.8.x pred verziou 2.8.1 umožňuje obísť overenie LDAP.
CVE-2020-15074	OpenVPN Access Server starší ako 2.8.4 generuje nové overovacie tokeny používateľov namiesto opätovného použitia rovnakých tokenov, čo umožňuje obchádzať platnosť časovej značky tokenu.

Tabuľka 5 CVE kódy pre OpenVPN [18]

2.6 WireGuard

WireGuard je nový protokol VPN, ktorý začal ako experiment a postupne sa vyvinul v alternatívu k OpenVPN a IPSec. Bol oficiálne verejne vydaný 30. marca 2020 a zahrnutý do verzie Linux jadra 5.6. Jeho cieľom je poskytnúť univerzálnu VPN technológiu, ktorá je bezpečnejšia, jednoduchšia a rýchlejšia, s jednoduchým nasadením do prevádzky od serverov vyššej kategórie až po zariadenia nižšej triedy (napr. Raspberry Pi). Aj keď bol WireGuard pôvodne vyvinutý pre systém Linux, je v súčasnosti schopný poskytovať VPN pre Windows, macOS, Android a iOS. [25]

2.6.1 Princíp fungovania

WireGuard protokol má niekoľko zaujímavých princípov fungovania. Bol navrhnutý takým spôsobom, aby bol čo najviac skrytý. Aplikácia WireGuard neodosiela žiadne pakety, ktoré obsahujú údaje o užívateľoch, čo obmedzuje dostupné informácie pre potencionálnych útočníkov. Šifrovanie WireGuard je založené na smerovaní Cryptokey a funguje tak, že sa verejné kľúče spájajú so zoznamom IP adries tunela VPN, ktoré sú akceptované pre využívanie VPN tunelu. Ku každému sieťovému rozhraniu je navyše priradený jedinečný súkromný kľuč a zoznam užívateľov. Každý užívateľ VPN tak môže posielať pakety na sieťové rozhranie so zdrojovou adresou IP zodpovedajúcou jeho zoznamu povolených adries IP. Ak chce sieťové rozhranie preniesť paket na užívateľa, pozrie sa na cieľovú adresu IP dátového paketu a porovná ju so zoznamom povolených adries každého užívateľa, aby určil kam ho poslať. [26] [25]

2.6.2 Výhody a nevýhody

WireGuard ponúka množstvo dôležitých výhod popísaných nižšie.

- Aplikácia používa najnovšie a najrobustnejšie šifrovacie algoritmy, napr. ChaCha20, SipHash24, a ďalšie.
- Jeho základný zdrojový kód v súčasnosti obsahuje iba asi 4000 riadkov na rozdiel od iných riešení, ktoré sa zvyčajne skladajú z 400 000 až 600 000 riadkov. Avšak, aj keď je veľkosť zdrojového kódu obrovskou výhodou, prináša aj určite obmedzenia uvedené v nevýhodách.
- VPN často trpí obmedzeniami rýchlosti z rôznych dôvodov. WireGuard bol navrhnutý tak, aby ponúkal významné vylepšenia rýchlosti VPN. Pretože bol

navrhnutý primárne pre Linux, využíva kombináciu vysokorýchlostných kryptografických základov, čo má za následok bezpečné prenášanie dát pri vysokých rýchlostiach. Je výhodný pre robustné servery ale aj pre malé zariadenia ako napríklad smartfóny.

- WireGuard pre identifikáciu a šifrovanie používa verejné kľúče na rozdiel od OpenVPN, ktorý používa certifikáty.

Aj keď WireGuard obsahuje množstvo výhod, v súčasnosti má aj niekoľko nevýhod, ktorými sú:

- WireGuard je stále vo vývoji, aj keď je dobré poznamenať, že aj keď ešte nie je dokončený a neprešiel žiadnymi bezpečnostnými auditmi, existuje niekoľko sietí VPN, ktoré už ponúkajú alebo sa chystajú zaradiť do svojej ponuky podporu WireGuard.
- Aj keď WireGuard ponúka výhody z hľadiska bezpečnosti a výkonu, jeho dizajn stále vyvoláva určité otázky týkajúce sa ochrany súkromia. Viacerí poskytovatelia VPN vyjadrili obavy z použitia systému WireGuard bez prídavných protokolov a z toho, aký vplyv to môže mať na súkromie užívateľov. [26]

2.6.3 Zraniteľnosť

V nasledujúcej podkapitole sú v tabuľke ukázané známe zraniteľnosti protokolu WireGuard podľa webovej stránky CVE s ich základným popisom.

CVE-2020-9429	Vo Wireshark 3.2.0 až 3.2.1 mohol zlyhať disektor WireGuard. Disektor bol adresovaný v epan/dissectors/packet-wireguard.c, a problém vyriešený nastavením určitej dátovej štruktúry na hodnotu NULL.

Tabuľka 6 CVE kódy pre WireGuard [18]

Čo sa týka ďalších zraniteľností tohoto protokolu, zatiaľ nie sú známe, keďže protokol WireGuard je nový.

3 VPN CLUSTER

Clustering je vo všeobecnosti metóda spracovania dát. Umožňuje spracovania veľkého množstva dát pomocou viacerých zariadení, pretože jednému zariadeniu by toto spracovanie trvalo príliš dlho. Tento spôsob spracovania dát sa koncovému užívateľovi javí ako jedno zariadenie a nie je si vedomý skutočnosti, že ide o koordinované spracovanie viacerými zariadeniami na pozadí.

Pri konfigurácií clusteru s viacerými VPN server zariadeniami je jedno zariadenie spustené v režime cluster controller a zvyšné zariadenia pracujú ako členské servery clusteru. VPN server štandardne po inštalácií pracuje v samostatnom režime a žiadne iné clustery nie sú nakonfigurované.

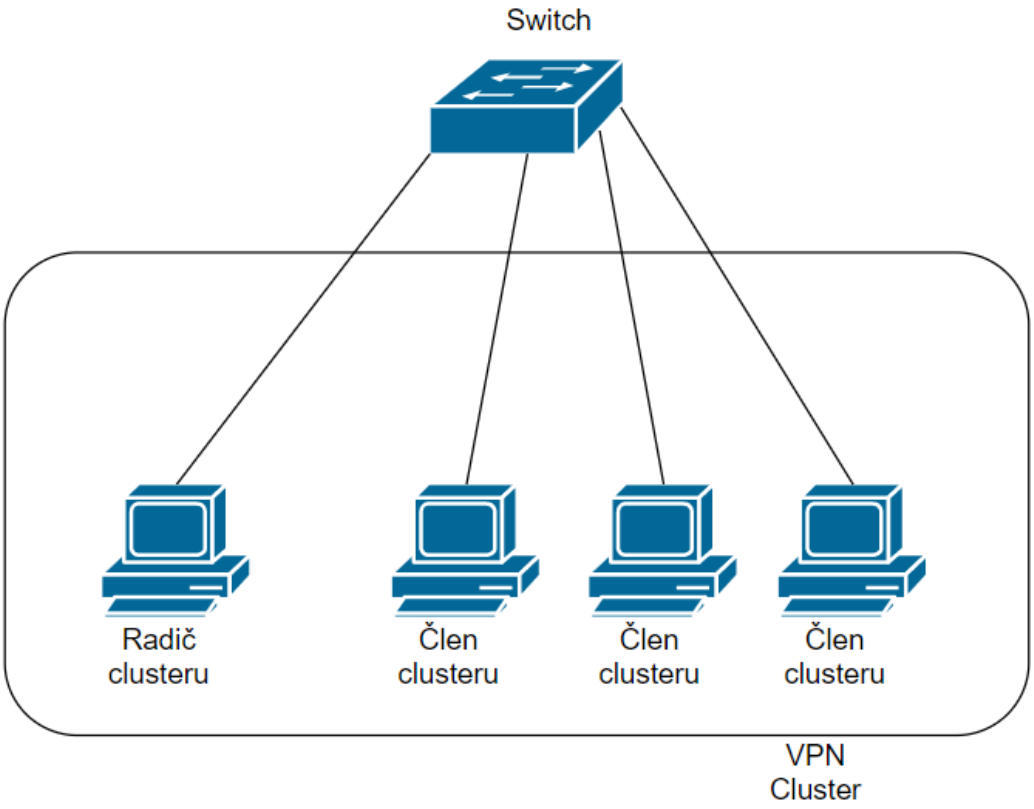
Clustering umožňuje:

- V prostrediach, kde je potrebné spracovávať veľké množstvo pripojení VPN, umožňuje clustering ich integrované spracovanie na viacerých serveroch VPN prostredníctvom zdieľania záťaže, kde by jedno zariadenie pokúšajúce sa o rovnakú úlohu nebolo schopné toto vykonať, alebo by toto veľké množstvo pripojení malo vážny dopad na výkon zariadenia.
- V prípade, že jeden člen tohto clusteru pozastaví svoju činnosť, napríklad z dôvodu hardvérového problému alebo aktualizácie softvéru, prevezme kontrolu nad spracovaním iný člen clusteru. Preto, aj keď dlhodobá prevádzka jednotlivých serverov môže viesť k poruche, ako celok môžu tieto servery pracovať takmer bez prerušenia.
- Pri prevádzke virtuálneho hubu v rámci clusteru je možné voliť ako prevádzkový režim statický alebo dynamický hub, v závislosti od požiadavky.
- Správca serveru a správcovia virtuálnych hubov sa môžu pripojiť iba k radiču clusteru a vykonávať správu jednotlivých členov serveru bez toho, aby si boli vedomí jeden druhého.

Pri pripojovaní jednotlivých serverov VPN je odporúčané ich pripájať k sieti s minimálnym oneskorením a vysokou priepustnosťou. Spravidla sa každý server pripája ku clusteru na rovnakom mieste. V tomto prípade je pravdepodobne najžiadanejšie, aby boli všetky členské servery jedného clusteru priamo pripojené k radiču clusteru v rovnakom segmente bez cestovania cez smerovač. Je však možné nastaviť na úkor výkonu radič clusteru a členské

servery na samostatných miestach prostredníctvom smerovača. V oboch týchto prípadoch je však nutné, aby radič clusteru bol na mieste, ktoré umožňuje komunikáciu TCP/IP od všetkých ostatných členov. [27] [28]

Nasledujúce podkapitoly čerpajú hlavne z oficiálnej dokumentácie softvéru Softether a to aj z dôvodu, že praktická časť diplomovej práce je zameraná hlavne na vytvorenie clusteru a následné testovanie v tomto softvéri.



Obrázok 7 Pripojenie radiču clusteru a členských serverov

3.1 Radič clusteru

Radič clusteru je zariadenie tvoriace jadro celého clusteru. Takto nastavené zariadenie slúži aj ako vstupná brána do clusteru. Užívateľ, ktorý sa pokúša o prístup do clusteru, zadáva pri pokuse o pripojenie práve IP adresu alebo názov zariadenia slúžiaceho ako radič clusteru.

Keď radič clusteru príjme požiadavku na pripojenie od zariadenia pripojujúceho sa k VPN, vykoná overenie užívateľa rovnakým spôsobom ako bežné pripojenie VPN. Po úspešnom overení sa radič clusteru automaticky rozhodne, ktorý členský server má vykonať spracovanie a zrealizuje zdieľanie zaťaženia presmerovaním na tento členský server. Samostatný server VPN, ktorý je radičom clusteru, je taktiež cieľom zdieľania záťaže. Algoritmus zdieľania záťaže porovnáva zaťaženie každého VPN serveru a automaticky

určuje cieľ priradenia novo pripojenej relácie VPN. V súčasnosti používa celé čísla, ktoré sa v zozname členov clasteru označujú ako body. Predvolením položky (Function Standard Ratio in Cluster) pre radič a členské servery je možné manuálne upravovať parametre zdieľania zaťaženia.

Server VPN pracuje v predvolenom prevádzkovom režime ako samostatný server. Zmena tohto režimu na radič clusteru umožňuje server VPN bežať v režime radiča clusteru. Toto a všetky ďalšie nastavenia súvisiace s clusteringom môže vykonávať iba správca celého VPN serveru. [28] [29]

3.2 Členské servery clusteru

Pojem členské servery clusteru označuje akékoľvek zariadenia, ktoré sú súčasťou clusteru ale zároveň sa nejedná o radič. Servery pripojené k radiču clusteru sú kontrolované týmto radičom a zdieľajú nastavenia v rámci celého clusteru.

Pri pridávaní nového člena k existujúcemu radiču je vyžadovaný názov hostiteľa alebo IP adresa radiča, číslo portu a heslo pre správu.

V súčasnosti sú potrebné nasledujúce položky:

- **Názov radiča alebo IP adresa** – Určujú názov alebo IP adresu zariadenia radiča clusteru.
- **Číslo portu radiča** – Určuje port TCP/IP cieľového radiča clusteru.
- **Heslo pre správu** – Určuje heslo pre správu cieľového radiča. Účasť každého člena v clusteri je povolená alebo zakázaná v závislosti od toho, či sa hash hodnota vloženého hesla pre správu zhoduje s nastaveným heslom. Pri zmene tohto hesla je tiež potrebné zmeniť heslo na všetkých členských serveroch clusteru. Toto heslo nie je spojené s heslom pre správu samotného VPN servera.
- **Verejná IP adresa** – Táto adresa je používaná ako adresa pre presmerovanie v prípade, že je členský server clusteru vybraný radičom ako cieľ zdieľania. Ak nie je zadaná žiadna IP adresa, automaticky sa použije IP adresa sieťového rozhrania, ktoré je použité pre pripojenie clusteru k radiču. Ak chceme použiť inú verejnú IP adresu než je adresa sieťového rozhrania, je nutné ju nastaviť.

- **Zoznam verejných portov** – Číslo verejného portu člena clusteru. Spravidla je určený zoznam portov, ktorý zverejní členský server clusteru. Musí byť určené viac ako jedno číslo verejného portu.

Servery VPN bežiace v režime člena clusteru sú nepretržite pripojené k radiču špeciálnym pripojením TCP/IP, ktoré sa nazýva „clusterové pripojenie“. Členský server sa pokúsi čo najdlhšie udržiavať spojenie medzi riadiacim clusterom a samotným radičom. Ak je toto pripojenie neúspešné, uskutočňujú sa opakované pokusy v intervaloch niekoľkých sekúnd do doby, kým sa spojenie nepodarí. [28] [30]

3.3 Vyrovnávanie zaťaženia

Radič VPN clusteru, ktorý prijíma pripojenie zo zdroja VPN, vykoná overenie tohto pripojenia a potom vyberie člena clusteru, ktorému priradí danú reláciu. V tomto prípade sa používajú nasledujúce algoritmy:

- **Virtuálny hub je navrhnutý pre VPN destináciu staticky** – Radič clusteru presmeruje pripojenie k serveru VPN s najvyššou bodovou hodnotou medzi všetkými momentálne dostupnými.
- **Virtuálny hub je navrhnutý pre VPN destináciu dynamicky** – Ak je relácia VPN pripojená ku clusteru a ešte neexistuje na žiadnom zo serverov v clusteri, je presmerovaná na server VPN s najvyššou bodovou hodnotou. Keď je relácia VPN pripojená a už existuje na jednom zo serverov, pripojenie je presmerované práve na tento server. [28] [31] [32]

3.4 Vyrovnávanie zaťaženia pomocou štandardného pomeru výkonu

Ako už bolo spomenuté v podkapitole vyššie, keď radič clusteru vyberie server s najnižším zaťažením spomedzi všetkých VPN serverov v clusteri, reálne vyberá server VPN s najvyššou bodovou hodnotou. Takto vyberané body sú približne určované nasledujúcim vzorcom:

$$body = \left(4096 - počet\ súbežných\ vpn\ relácií * \frac{100}{váha}\right) * 100000/4096$$

Vyššie uvedený vzťah umožňuje definovať štandardný pomer výkonu každého servera VPN nastaveným parametru váhy pre každý server. Na každom serveri VPN je možné voľne meniť parameter váhy. Predvolené nastavenie parametra váhy je 100.

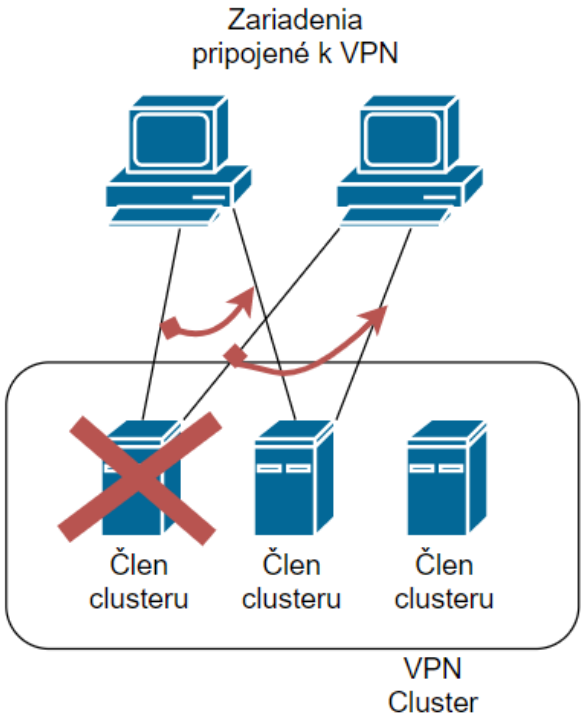
Hodnota štandardného pomeru výkonu sa nastavuje proti hodnote 100. Napríklad keď majú dva príslušné servery hodnoty 100 a 200, znamená to, že druhý server je schopný spracovať dvojnásobné množstvo relácií VPN ako prvý server. Radič clusteru VPN určuje, koľko relácií je schopný celý VPN server spracovať prevažne na základe takto nastavenej hodnoty a podľa toho rozdeľuje zaťaženie. [28] [33]

3.4.1 Nastavenie pre zamedzenie spracovania dát VPN radiča clusteru

Pri spracovaní veľkého množstva dát predstavuje toto množstvo výrazné veľké zaťaženie celého serveru. Je možné znížiť toto zaťaženie samotného radiča clusteru tak, že radič prevezme iba úlohu presmerovania všetkých relácií VPN každému členovi clusteru. To bráni radiču clusteru vo vyberaní samého seba pri rozhodovaní, ktorému serveru VPN priradí novú reláciu. [28]

3.5 Odolnosť voči chybám

Keď členský server clusteru náhle ukončí pripojenie z dôvodu hardvérovej alebo softvérovej poruchy, alebo ak nastane situácia v ktorej musí dočasne ukončiť svoju činnosť z dôvodu aktualizácie, tento server stratí spojenie s radičom clusteru, takže ho radič automaticky považuje za odpojený a vylúči ho z vyrovnávania záťaže. Okrem toho všetky relácie, ktoré boli pripojené k serveru ktorý prestal fungovať, automaticky preberajú ďalšie členské servery clusteru. Toto spracovanie sa vykonáva automaticky bez akejkoľvek špeciálnej manipulácie s klientskym zariadením VPN zdroja. Preto, aj keď sa časť viacerých zariadení servera VPN, používaná poskytovateľom služieb alebo spoločnosťou, ukončí z dôvodu poruchy alebo sa kvôli údržbe musí vypnúť, tento mechanizmus umožní celej sieti pokračovať v činnosti bez zastavenia, pokiaľ zostanú pripojené iné zariadenia v clustery. [32] [33]



Obrázok 8 Odolnosť voči chybám

3.6 Statické virtuálne huby

Virtuálne huby, ktoré nevyužívajú clustering, nie sú nijako zvlášť klasifikované, ale v prostredí clusteringu sú klasifikované do dvoch typov: statické a dynamické virtuálne huby. Zatiaľ čo pri vytváraní je potrebné určiť typ virtuálneho hubu, je možné ho neskôr zmeniť.

Statický virtuálny hub sa používa pre pohodlné vytvorenie virtuálneho centra pre VPN so vzdialeným prístupom. Vytvorenie statického virtuálneho hubu v clusteri vygeneruje inštanciu (entitu) hubu vo všetkých smeroch VPN v clusteri, ktorý bude naďalej pracovať na všetkých serveroch VPN pokiaľ bude cluster v prevádzke.

Keď je zdrojový softvér VPN (zvyčajne klient VPN koncového užívateľa), ktorý si želá vytvoriť pripojenie so vzdialeným prístupom, pripojený k radiču clusteru, radič využije vyššie uvedené algoritmy na výber jedného zo serverov VPN a presmeruje pripojenie na statický virtuálny hub. [28]

3.7 Dynamické virtuálne huby

Dynamický virtuálny hub je typ hubu vhodný pre poskytovanie služieb servera VPN, ako je napríklad vytváranie veľkého počtu virtuálnych hubov v clusteri a umožnenie voľnej

komunikácie používateľom pripojeným k rovnakému virtuálnemu hubu. Dynamické huby sú vhodné napríklad ako spôsob, ktorým môžu systémové oddelenia veľkých spoločností vytvárať virtuálne huby pre každé svoje oddelenie, alebo pomocou ktorého poskytovatelia internetových služieb vytvárajú virtuálne huby ako službu pre svojich užívateľov. Tieto oddelenia a užívatelia majú na správu hubu oprávnenie.

Ak bol v clusteri vytvorený dynamický virtuálny hub ale nie je k nemu pripojená žiadna inštancia (entita), neexistuje na žiadnom zo serverov vo VPN clusteri. Keď prvá relácia označí, že virtuálny hub vytvorí VPN pripojenie, radič vyberie VPN server, ktorý by mal spustiť inštanciu virtuálneho hubu prvý krát. Následne vytvorí hub inštanciu pre VPN server a presmeruje reláciu VPN na tento server. Pri druhej a nasledujúcich reláciách sa k tomuto hubu automaticky presmerujú na VPN server, na ktorom je spustená inštancia hubu. V tom prípade, bez ohľadu na počet serverov v clusteri, sú tieto relácie pripojené k rovnakému hubu na rovnakom VPN serveri. Ak nie je k virtuálnemu hubu pripojená žiadna relácia, jeho inštancia sa automaticky zastaví a uvoľní sa vyhradené miesto v procesore a pamäti. [28]

3.8 Pripojenie k ľubovoľným serverom pomocou statických virtuálnych hubov

Ako bolo spomenuté v predchádzajúcich kapitolách, pripojenie VPN k statickému hubu sa vykonáva automaticky, takže nie je možné zistiť ku ktorému serveru VPN sa pripojí až do nadviazania spojenia.

Môže sa však stať, že budeme musieť pripojiť statický hub k ľubovoľnému serveru v clustery. V takomto prípade, pri vytváraní nastavania pripojenia v klientovi VPN, označíme adresu servera VPN a názov virtuálneho hubu ku ktorému sa potrebujeme priamo pripojiť, namiesto označenia radiča clusteru ako cieľového servera VPN pripojenia. Okrem toho je potrebné určiť aj administrátorské heslo. Táto výnimka umožňuje vytvoriť pripojenie priamo k statickému hubu bez použitia smerovača ku ktorému je pripojený radič clusteru. [28]

3.9 Hromadná správa clusteru

Po vytvorení clusteru musia správca celého VPN servera a správcovia virtuálneho hubu vytvoriť iba administratívne pripojenie k radiču, aby mohli hromadne spravovať stav a VPN relácie všetkých hubov pracujúcich v clusteri. Táto správa sa vykonáva pomocou nástroja Server Manager alebo obslužného programu *vpncmd* rovnakým spôsobom ako keď sa nepoužíva funkcia clustering.

Jednoduchým pripojením k radiču clusteru môžu správcovia VPN serverov spravovať všetky huby v clusteri. Každý správca však môže spravovať iba hub na ktorý má oprávnenie.

Existujú aj situácie, pri ktorých je potrebné, aby správcovia VPN serverov nadviazali priame administračné spojenie k iným členom clusteru než je radič. Ide o nasledujúce situácie:

- Pri odpojení členského serveru od clusteru a jeho nastavení do operačného režimu samostatného serveru.
- Pri potvrdení, ktoré inštancie (entity) skutočne pracujú na členských serveroch clusteru.
- Pri úprave položiek člena clusteru, získavania obsahu konfiguračného súboru alebo požiadavky na stav serveru.

Správcovia virtuálneho hubu môžu vykonávať iba administračné pripojenie k radiču clusteru a nie k členským serverom. Nastavenie lokálneho mosta a prepínača virtuálnej 3. vrstvy sa vykonávajú pre každý VPN server. Pre tieto nastavenia je však potrebné plné oprávnenie. [28]

3.10 Funkcie ktoré nie sú k dispozícii súčasne s clusteringom

Pri povolení funkcie clusteringu nie je možné súčasne využívať nasledujúce funkcie:

- Kaskádové pripojenie,
- Virtuálny NAT.

Funkcie miestneho premostenia a prepínača virtuálnej 3. vrstvy je možné používať normálne. Lokálne premostenie však môže fungovať iba medzi VPN serverom na ktorom tieto inštancie (entity) skutočne existujú. V prípade hubov so statickou inštanciou zvyčajne existuje na všetkých VPN serveroch. V prípade dynamických hubov však môže byť v clusteri iba jeden VPN server na ktorom môže existovať inštancia. Takže funkcie lokálneho premostenia nie sú zvyčajne k dispozícii. [28]

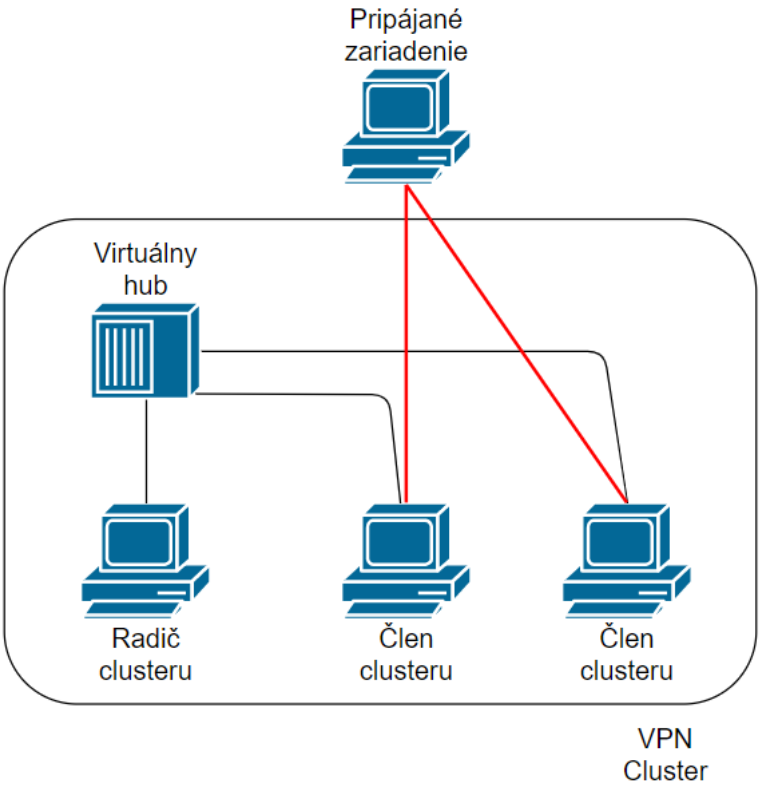
II. PRAKTICKÁ ČASŤ

4 NÁVRH VPN CLUSTERU

V tejto časti diplomovej práce sa zaoberám návrhom VPN clusteru použitím technológie SoftEther. Celý návrh je následne implementovaný a testovaný pomocou programu VMware Workstation Pro vo verzii 16.1.1.. Program je využívaný preto, že celý návrh VPN clusteru je vytvorený v operačnom systéme CentOS 8, ktorý je zvolený ako najideálnejšie riešenie pre následné testovanie na reálnej testovacej infraštruktúre. V priloženej prílohe môžeme vidieť bližšie hardvérové špecifikácie jednotlivých zariadení. Tieto nastavenia sú rovnaké pri každom jednom zariadení a to z dôvodu limitovaných hardvérových prostriedkov pri vytváraní návrhu.

4.1 Popis návrhu

Návrh mnou vytvoreného VPN clusteru môžeme vidieť na *obrázku 9*. Ide o základný návrh skladajúci sa z jedného zariadenia nastaveného ako radič clusteru. Na tomto radiči je vytvorený virtuálny hub, ku ktorému sú pripojené ďalšie zariadenia nastavené ako členy clusteru. Tieto členy si budú rozdeľovať prácu v závislosti na počte pripojených zariadení. V našom prípade postačí mať pripojené „len“ dva tieto členy. Pre väčšie zaťaženie siete a pri väčšom počte pripojených zariadení nie je problém pridať do siete nové členy.



Obrázok 9 Návrh VPN clusteru

4.2 Nastavenie radiča clusteru

Nastavenie zariadenia ako radiča clusteru prebiehalo nasledovne: na vybrané zariadenie bol nainštalovaný program *SoftEther VPN Server* z webovej stránky www.softether.org. Po úspešnom nainštalovaní tohto programu nasleduje nastavenie zariadenia ako VPN radiču celej siete.

V prvom kroku je potrebné spustiť server.

```
[root@192 vpnserver]# ./vpnserver start
The SoftEther VPN Server service has been started.

Let's get started by accessing to the following URL from your PC:

https://192.168.160.128:5555/
  or
https://192.168.160.128/

Note: IP address may vary. Specify your server's IP address.
A TLS certificate warning will appear because the server uses self signed certificate by defau
lt. That is natural. Continue with ignoring the TLS warning.
```

Obrázok 10 Spustenie serveru

Nasleduje príkaz pre spustenie konfigurácie nášho VPN.

```
[root@192 vpnserver]# ./vpncmd
vpncmd command - SoftEther VPN Command Line Management Utility
SoftEther VPN Command Line Management Utility (vpncmd command)
Version 4.34 Build 9745   (English)
Compiled 2020/04/05 23:39:56 by buildsan at crosswin
Copyright (c) SoftEther VPN Project. All Rights Reserved.

By using vpncmd program, the following can be achieved.

1. Management of VPN Server or VPN Bridge
2. Management of VPN Client
3. Use of VPN Tools (certificate creation and Network Traffic Speed Test Tool)

Select 1, 2 or 3: 
```

Obrázok 11 Výber konfigurácie serveru

Po spustení tohto príkazu sa nám objavia možnosti konfigurácie daného zariadenia. V tomto prípade zvolíme možnosť číslo 1 a tou je konfigurácia VPN serveru alebo VPN bridge-u. Následne sa nám objavia možnosti, ukázané nižšie, v ktorých si môžeme nastaviť nami zvolenú IP adresu a názov hubu. V tomto prípade necháme tieto možnosti prázdne a tým sa nám server nastaví ako *localhost* s predvolenými hodnotami nastavenia.

```
Specify the host name or IP address of the computer that the destination VPN Server or VPN Bri
dge is operating on.
By specifying according to the format 'host name:port number', you can also specify the port n
umber.
(When the port number is unspecified, 443 is used.)
If nothing is input and the Enter key is pressed, the connection will be made to the port numb
er 8888 of localhost (this computer).
Hostname of IP Address of Destination:

If connecting to the server by Virtual Hub Admin Mode, please input the Virtual Hub name.
If connecting by server admin mode, please press Enter without inputting anything.
Specify Virtual Hub Name:
Connection has been established with VPN Server "localhost" (port 443).

You have administrator privileges for the entire VPN Server.
```

Obrázok 12 Zadanie údajov pre server

Nasleduje nastavenie hesla, ktoré je potrebné pre administrátorský prístup a následné nastavovanie. Po zadaní hesla a získaní prístupu do zaradenia je potrebné toto zariadenie nastaviť ako radič clusteru nasledovne:

```
VPN Server>ClusterSettingController
ClusterSettingController command - Set VPN Server Type as Cluster Controller
The command completed successfully.
```

Obrázok 13 Nastavenie serveru ako radič clusteru

Po úspešnom nastavení je potrebné vytvoriť virtuálny hub, ku ktorému sa budú pripájať ostatní členovia VPN clusteru majúci za úlohu spracovávať dáta pripojených užívateľov.

```
VPN Server>HubCreate Hub
HubCreate command - Create New Virtual Hub
Please enter the password. To cancel press the Ctrl+D key.
```

Obrázok 14 Vytvorenie virtuálneho hubu

Akonáhle je virtuálny hub vytvorený je ešte potrebné vytvoriť užívateľov. Pre každé zariadenie pripájané sa ku clusteru je nutné vytvoriť jedného užívateľa. Pri vytváraní je potrebné nastaviť názov užívateľa. Na výber sú však aj ďalšie nastavenia, ako napríklad celý názov, názov skupiny do ktorej bude daný užívateľ patriť a popis tohto užívateľa. Tieto možnosti sú však nepovinné.

```
VPN Server/Hub>UserCreate
UserCreate command - Create User
User Name: Member 1

Assigned Group Name:

User Full Name:

User Description:

The command completed successfully.
```

Obrázok 15 Vytvorenie užívateľa

Úspešné vytvorenie užívateľov si môžeme skontrolovať jednoduchým príkazom ukázaným nižšie.

```
VPN Server/Hub>userlist
UserList command - Get List of Users
Item             |Value
-----------------+-----------------------
User Name        |Member 1
Full Name        |
Group Name       |-
Description      |
Auth Method      |Password Authentication
Num Logins       |0
Last Login       |(None)
Expiration Date  |No Expiration
Transfer Bytes   |0
Transfer Packets |0
The command completed successfully.
```

Obrázok 16 Kontrola vytvorených užívateľov

4.3 Nastavenie člena clusteru

Nastavenie zariadenia ako člena clusteru prebieha podobne ako nastavenie zariadenia na radič clusteru. Je potrebné stiahnuť a nainštalovať program *SoftEther VPN Server*. Rozdiel nastáva až po nastavenie administrátorského hesla a získanie prístupu do zariadenia. Akonáhle získame prístup, je potrebné toto zariadenia nastaviť ako členský server clusteru.

```
VPN Server>ClusterSettingMember
ClusterSettingMember command - Set VPN Server Type as Cluster Member
Destination Controller Host Name and Port Number:
```

Obrázok 17 Nastavenie serveru ako člena clusteru

Po zadaní príkazu nás program vyzve k zadaniu IP adresy radiča a čísla portu na ktorý sa dané zariadenie bude pripájať. Po zadaní týchto parametrov je zariadenie úspešne pripojené k radiču clusteru a môže začať komunikovať s užívateľmi.

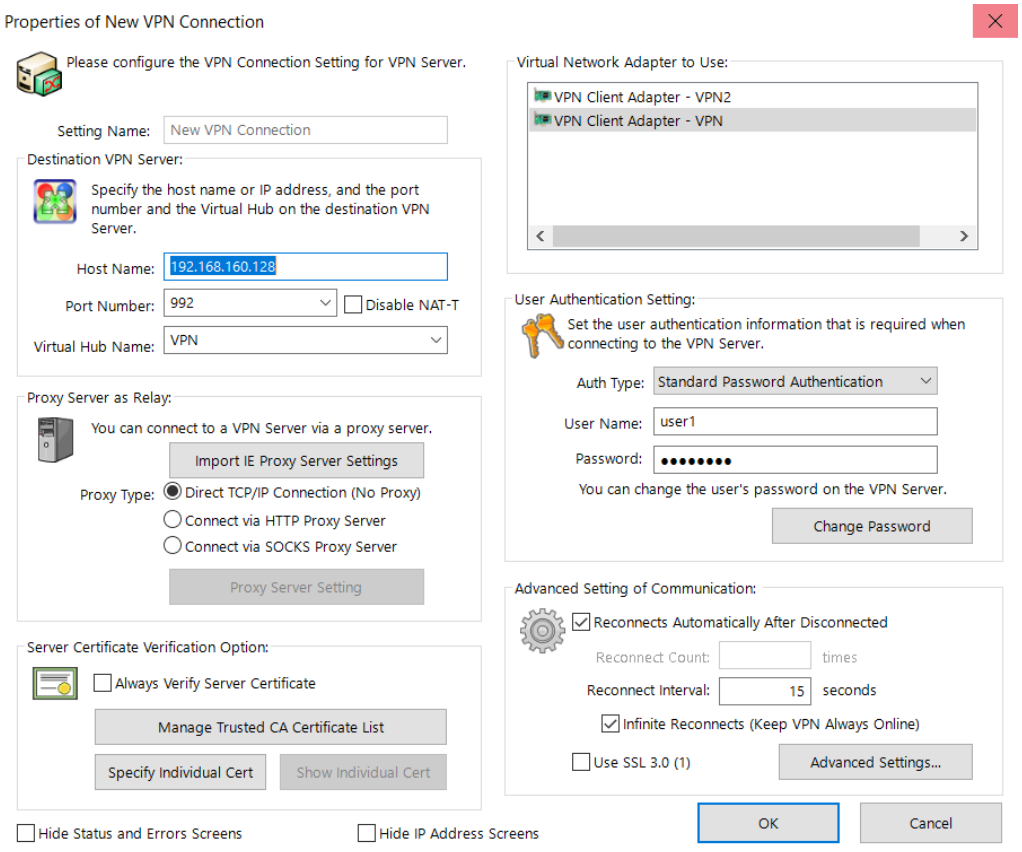
Pre zistenie, či sú členské servery clusteru pripojené k radiču, slúži nasledujúci príkaz, ktorý musí byť zadaný na serveri predstavujúci radič. Tento príkaz vypíše IP adresy a ďalšie informácie každého pripojeného člena.

```
ClusterMemberList command - Get List of Cluster Members
        ID|Type      |Connection Started at    |Host Name            | Point|Number of Sessions|Numb
er of TCP Connections|Number of Operating Hubs|Using Client Connection Licenses|Using Bridge Connect
ion Licenses
----------+----------+-------------------------+---------------------+------+------------------+----
---------------------+-----------------------+--------------------------------+--------------------
------------
 684152376|Controller|2021-04-23 (Fri) 08:32:28|localhost.localdomain|100000|                 0|
                  14|                        0|                               0|
            0
 649529603|Member    |2021-04-23 (Fri) 08:36:41|192.168.160.130      |100000|                 0|
                  12|                        0|                               0|
            0
4252315599|Member    |2021-04-23 (Fri) 08:36:43|192.168.160.129      |100000|                 0|
                  12|                        0|                               0|
            0
The command completed successfully.
```

Obrázok 18 Vypísanie pripojených členov clusteru

4.4 Nastavenie zariadenia pripájaného ku clusteru

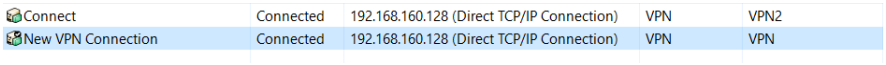
Pre pripojenie zariadenia k vytvorenému clusteru popísanému vyššie, bol využitý program *SofEther VPN Client Manager.* Program simuluje sieťové adaptéry jednotlivých užívateľov pripájajúcich sa k VPN sieti. Pre testovanie komunikácie medzi užívateľom a sieťou je tento program plne dostačujúci.



Obrázok 19 SoftEther client manager

Pre pripojenie je potrebné v programe nastaviť názov, ktorý sa zobrazuje priamo v programe, IP adresu radiča, číslo portu a názov virtuálneho hubu clusteru ku ktorému sa chceme pripojiť. Rovnako tak potrebujeme vytvoriť a vybrať virtuálny adaptér. A ako poslednú vec pre prístup do VPN siete je potrebné zadať názov a heslo užívateľa, ktorý už je vytvorený na radiči. Bez týchto dvoch údajov nie je možné pristupovať do siete.

Po správnom zadaní všetkých údajov môžeme vidieť v programe úspešné pripojenie k VPN.

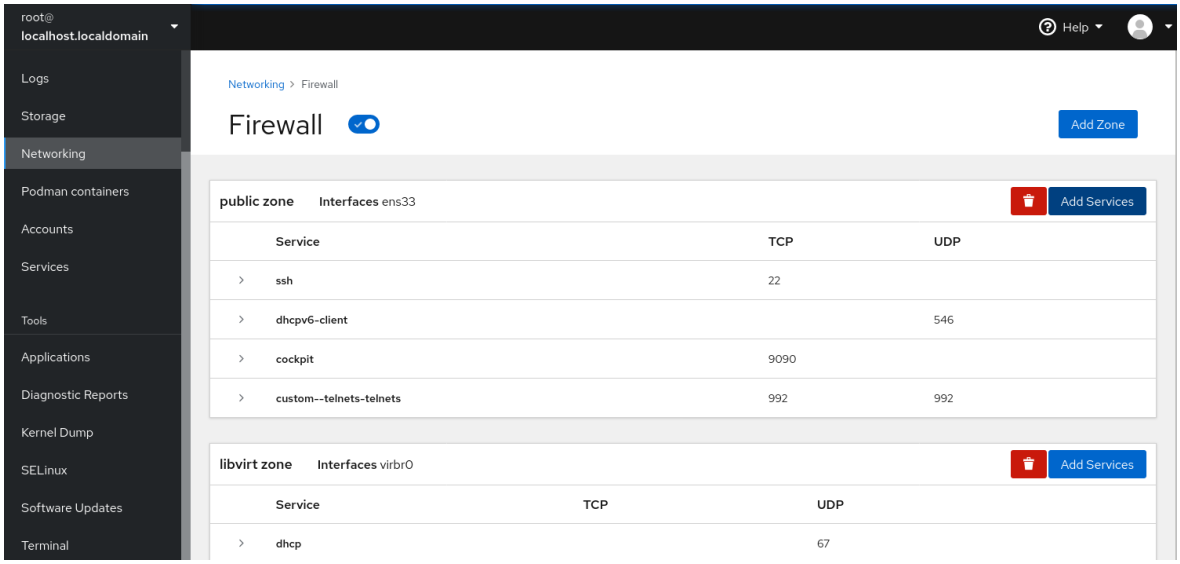


Obrázok 20 Pripojené zariadenia

4.5 Možné problémy pri nastavovaní

Pri zostavovaní VPN clusteru sa môžeme stretnúť s problémom pri pripojení jednotlivých členov s radičom. Je to spôsobené firewallom jednotlivých zariadení, ktorý filtruje komunikáciu na používanom sieťovom porte. Preto odporúčam nastaviť v systéme na každom zariadení výnimku vo firewalle pre používaný port.

V našom prípade som pre nastavenie výnimky v operačnom systéme CentOS využil program *Cockpit.* Tento program je priamo nainštalovaný v operačnom systéme, avšak je potrebné ho aktivovať. Po aktivovaní tohto programu ho spustiť priamo v internetovom prehliadači zariadenia. Do kolónky pre zadanie webovej adresy vložiť *IP adresa zariadenia:9090.* Následne sme vyzvaní pre prihlásenie ako administrátor. Po prihlásení sa získame prístup k balíku nástrojov slúžiacich pre jednoduchšiu správu systému aj iným spôsobom ako pomocou príkazového riadku. Jedným z týchto nástrojov je aj správa a nastavenie firewallu systému. V tomto nástroji je možné povoliť alebo zakázať komunikáciu cez špecifické sieťové porty viz. obrázok nižšie.



Obrázok 21 Cockpit nástroj pre správu firewallu

4.6 Nastavenie zabezpečenia clusteru

Pri nastavení zabezpečenia VPN clusteru som zvolil dva postupy. V prvom prípade sa jedná o *nastavenie na úrovni užívateľských skupín*, v prípade druhom ide o *nastavenie access listov pre celý cluster*. V nasledujúcich podkapitolách je popísané mnou zvolené nastavenie týchto dvoch možností.

4.6.1 Nastavenie skupiny užívateľov

Pri nastavovaní nasledujúcich zabezpečení odporúčam nainštalovať do svojho zariadenia nástroj *Server Manager od SoftEtheru*. Tento nástroj zjednoduší prácu s pridávaním, odstránením a správou jednotlivých užívateľov, ktorí vstupujú do clusteru. Rovnako tak je zjednodušená aj správa užívateľských skupín, do ktorých je možno jednotlivých užívateľov priradiť. Takýmto spôsobom som v mojom testovacom VPN clusteri priradil jednotlivých vytvorených užívateľov do dvoch skupín, viz. *Obrázok 22*.

User Name	Full Name	Group Name	Description	Auth Method	Num Logins	Last Login
privilegovany1		Priv_uzivatel		Individual Certific...	0	2021-05-03
user1	user1	Uzivatelia		Password Authen...	0	2021-05-03
user2		Uzivatelia		Password Authen...	0	2021-05-03

Obrázok 22 Uživateľské skupiny

Prvá vytvorená skupina slúži pre prístup užívateľov s vyššími prístupovými právami vo VPN clusteri. Tento užívateľ môže napríklad komunikovať v rámci siete s ostatnými užívateľmi, má menej nastavení filtrácie jednotlivých paketov a taktiež povolený monitorovací mód, pomocou ktorého dokáže tento užívateľ sledovať všetky pakety prechádzajúce virtuálnym

hubom. Taktiež je pre tohto užívateľa nastavená overovacia metóda pomocou individuálneho certifikátu, takže nie je potrebné zadávanie hesla

V druhej vytvorenej skupine slúžiacej pre bežných užívateľov pripojených do clusteru je ako overovacia metóda zvolené užívateľské meno a heslo. Rovnako je pre túto skupinu obmedzená väčšina nastavení, vrátane komunikácie medzi sebou, prípadne monitorovania prevádzky na sieti.

4.6.2 Access Listy clusteru

Rovnako ako v prvom prípade, aj tu bol využitý nástroj *Server Manager*. Pomocou tohto nástroja je zjednodušené nastavovanie jednotlivých access listov. Keďže užívatelia pristupujúci k VPN clusteru používajú pre svoje prihlásenie meno a heslo, toto nastavenie nemusí byť vždy najbezpečnejšie. Preto sú nastavené nasledujúce povolenia, viz. *Obrázok 23.*

ID	Action	Status	Prior...	Contents
1	Discard	Enable	100	(ipv4) DstIPv4=192.168.30.128/28, SrcUser=Uzivatelia
2	Discard	Enable	100	(ipv4) DstIPv4=192.168.30.144/28, SrcUser=Uzivatelia
3	Discard	Enable	100	(ipv4) DstIPv4=192.168.160.128/32, SrcUser=Uzivatelia
4	Pass	Enable	200	(ether) SrcUser=Uzivatelia

Obrázok 23 Access listy

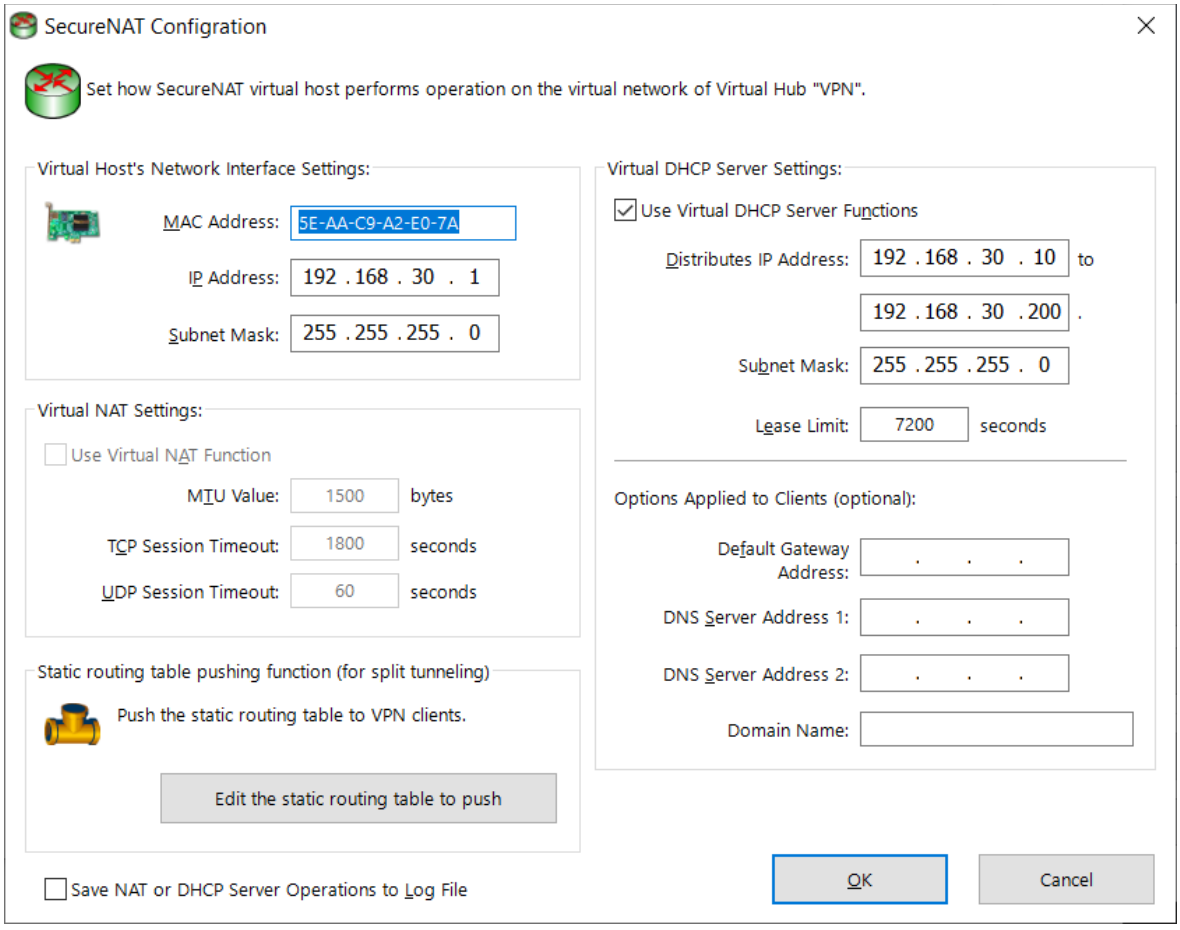
V jednotlivých listoch sú nastavené povolenia na komunikáciu pre skupinu užívateľov pomocou rozsahu IP adries, ku ktorým užívateľ z tejto skupiny môže pristupovať. Jedná sa o zablokovanie prístupu ku dvom podsieťam slúžiacim pre administráciu a jednému zariadeniu, ktoré v clustery vykonáva úlohu radiča. Rovnako tak, keďže cluster využíva protokol DHCP, je v listoch obsiahnuté aj povolenie využívať tento protokol. Posledný access list povoľuje všetky ostatné IP adresy ku ktorým môžu užívatelia pristupovať. Takto rozdelené access listy na skupiny užívateľov uľahčujú ich správu. V rozsiahlejších sieťach tak nie je problém doplniť access listy o ďalšie skupiny, prípadne upravovať skupiny už vytvorené.

V prípade zvýšenia bezpečnosti vo VPN clusteri je tiež dobré udržiavať si tabuľku IP adries priradených jednotlivým užívateľom. V takom prípade je odporúčané spolu s access listom na MAC adresu užívateľa, vytvoriť access list aj na IP adresu tohto užívateľa. Nevýhodou takéhoto nastavenia je veľký počet IP a MAC adries pri rozsiahlejšej virtuálnej sieti.

4.6.3 VirtualNAT a Virtual DHCP

Je to jedna z možností, ktorú môžeme nastaviť pri zostavovaní VPN clusteru. Ide o značné zvýšenie bezpečnosti pripojovaniu k sieti. Presnejšie teda využitím virtuálneho DHCP, kde je možnosť distribúcie IP adries jednotlivým zariadeniam pomocou serveru. Táto technológia však nefunguje samostatne a je zahrnutá v programe *Softether*. Obe tieto technológie pracujú pod takzvaným SecureNAT a iba s jeho povolením je možne spomenuté technológie využívať.

Hlavnou výhodou využitia DHCP je nastavenie určitého rozsahu IP adries, ktoré budú prideľované jednotlivým užívateľom automaticky. Táto možnosť spolu s nastavením access listov, ktoré sú ukázané v predchádzajúcej podkapitole, obmedzuje pripojenie ostatných zariadení, ktoré svojou IP adresou nespadajú do nastaveného rozsahu a nedovoľuje im pripojiť sa k sieti. Všetky ostatné, manuálne zadané IP adresy jednotlivých zariadení, by nemali byť pri tejto spustenej možnosti schopné pripojiť sa do siete ani po správnom zadaní užívateľského mena a hesla.



Obrázok 24 Nastavenie virtuálneho DHCP

5 TESTOVANIE VPN CLUSTERU

V predošlej kapitole bol predstavený návrh VPN clusteru vytvorený v programe VMware spoločne so základným nastavením slúžiacim pre zabezpečenie celého clusteru. Toto nastavenie prebiehalo dvoma spôsobmi, či už sa jednalo o jednotlivých užívateľov pristupujúcich do clusteru alebo access listov obmedzujúcich prístup do celej siete.

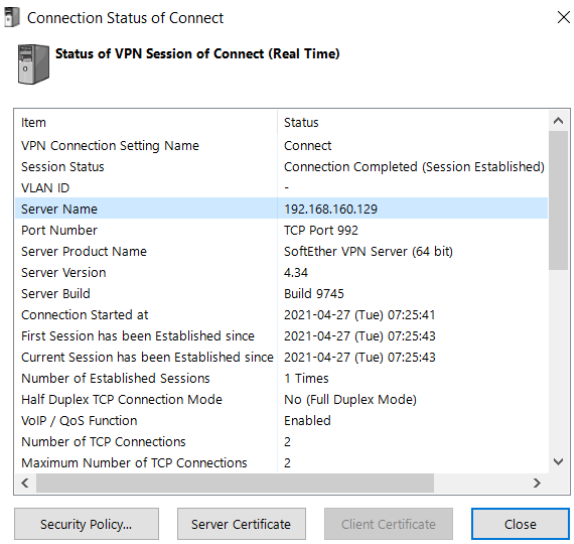
V tejto kapitole diplomovej práce je poukázané na testovanie navrhnutého clusteru. Konkrétnejšie ide o testy zamerané na odolnosť voči poruchám, zabezpečenia clusteru aj v prípade zmeny IP adresy užívateľa a záťažový test.

Toto testovanie je obmedzené tým, že bolo celé vytvárané a vykonané na pracovnom notebooku, teda vo virtuálnom prostredí. V prípade nasadenia clusteru do bežného prostredia, teda na reálne súčiastky, by bolo testovanie obsiahlejšie a s lepšími výsledkami.

5.1 Testovanie odolnosti voči chybám

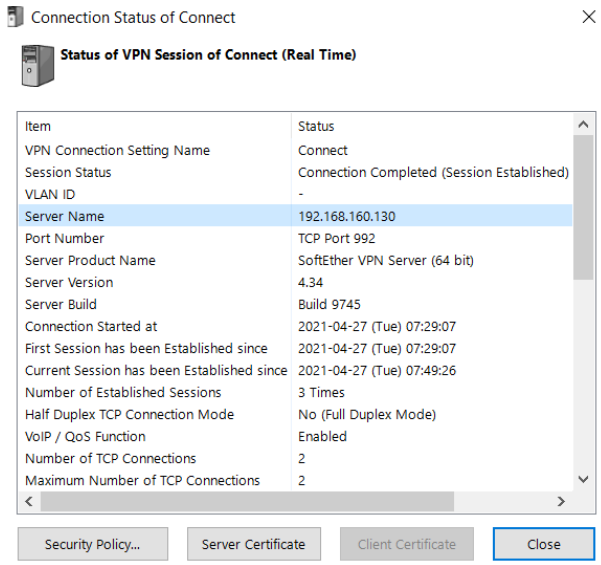
Ako bolo popísané v teoretickej časti (*kapitola 3),* jednou z hlavných výhod VPN clusteru je odolnosť voči chybám. Presnejšie, že pri poruche jedného z členov clusteru sú všetky zariadenia, pripojené k poruchovému členu, presmerované na funkčného člena clusteru bez zdĺhavého čakania.

V našom prípade testovanie prebiehalo spôsobom odpojenia jedného z členských serverov clusteru priamo v programe VMware. Na nasledujúcom obrázku môžeme vidieť pôvodné pripojenie užívateľa na členský server, resp. IP adresu zariadenia na ktoré je užívateľ pripojený.



Obrázok 25 Pripojenie zariadenia pred odpojením serveru

Po následnom vypnutí serveru s vyššie zobrazenou IP adresou sa nám zobrazí u jednotlivých užívateľov pop-up okno s hlásením, že bol stratený prístup k tomuto zariadeniu. Po kliknutý na možnosť opakovania pokusu o pripojenie sa následne zariadenia pripoja k fungujúcemu členu clusteru, viz. *Obrázok 26.*



Obrázok 26 Pripojenie zariadenia po odpojení serveru

V závislosti na tomto teste môžeme tvrdiť, že nastavený cluster pracuje správne a toto nastavenie by bolo funkčné aj pri nasadení do reálnej prevádzky. Taktiež môžeme pozorovať z obrázkov vyššie, že za správu prideľovania jednotlivých členov k serveru je zodpovedný radič, pretože všetky zariadenia pripájané do siete používajú ako destinačnú adresu práve adresu radiča.

5.2 Testovanie zabezpečenia clusteru

Jednotlivé spôsoby testovania zabezpečenia clusteru sú popísané v tejto podkapitole. Toto testovanie je obmedzené z toho dôvodu, že je celý VPN cluster vytvorený v programe VMware. Pri možnosti nasadenia siete na reálne zariadenia by bolo toto testovanie obsiahlejšie.

5.2.1 Zmena IP adresy užívateľa

Ako bolo spomenuté vyššie, skupina užívateľov má vytvorené svoje vlastné access listy zamedzujúce prístup do určitých podsietí a k užívateľovi. Tento access list umožňuje alebo zabraňuje pripojeniu užívateľa do siete, prípadne jeho komunikáciu s ostatnými zariadeniami.

Testovanie prebiehalo spôsobom vytvorenia nového užívateľa s inou MAC adresou než užívateľa, ktorý je nastavený pre prístup do siete. Bolo vzaté do úvahy to, že užívateľské meno a heslo je pre novo pristupujúceho užívateľa známe, rovnako tak aj IP adresa zariadenia. Po zadaní jednotlivých údajov bolo síce toto zariadenie pripojené do clusteru, ale nezískalo absolútne žiaden prístup ku komunikácií v sieti.

5.3 Záťažové test

V nasledujúcich riadkoch je popísaný spôsob testovania navrhnutého a zapojeného VPN clusteru. Testovanie prebiehalo pozorovaním prevádzky na servery slúžiacom ako radič celého clusteru. Na tomto radiči som pomocou nástroja Cockpit monitoroval celkové zaťaženie siete a to s použitím nasledujúcich nástrojov slúžiacich pre testovanie.

5.3.1 Nástroj iPerf

Pomocou nástroja iPerf bola zmeraná maximálna možná šírka pásma v navrhnutom VPN clusteri. Tento test slúžil na vyhodnotenie toho, či sieťová karta alebo rýchlosť pripojenia clusteru má v tomto prípade zásadný vplyv na rýchlosť komunikácie v celej našej sieti.

Nástroj bol nainštalovaný v dvoch zariadeniach. Jedno zo zariadení bol server pracujúci v našej sieti ako radič clusteru. Druhá inštalácia bola na zariadení mimo pripojenú sieť. Toto zariadenie vlastne simulovalo užívateľa pristupujúceho mimo našu sieť a v ďalšom testovaní slúžilo aj ako Apache server.

Na radiči po nainštalovaní *iPerf* je tento nástroj spustený pomocou príkazu *iperf3 -s*. Tento príkaz spôsobí, že sa na zariadení zapne server slúžiaci pre testovanie rýchlosti pripojenia s predvolene nastaveným portom, v tomto prípade port s číslom 5201. Následne je pomocou nástroja Cockpit, presnejšie v nastavení firewallu, tento port na radiči otvorený.

Na zariadení pristupujúcom mimo sieť je tento server spustený pomocou príkazu *iperf3 -c „ip_adresa“*. Po správnom spustení môžeme na oboch zariadeniach pozorovať výpis pri posielaní dát na sieti v určitom časovom intervale, predvolene nastavenom na 10 sekúnd.

```
Accepted connection from 192.168.160.131, port 53522
[  5] local 192.168.160.128 port 5201 connected to 192.168.160.131 port 53524
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-1.00   sec   383 MBytes  3.21 Gbits/sec
[  5]   1.00-2.00   sec   372 MBytes  3.12 Gbits/sec
[  5]   2.00-3.00   sec   433 MBytes  3.63 Gbits/sec
[  5]   3.00-4.00   sec   426 MBytes  3.57 Gbits/sec
[  5]   4.00-5.00   sec   424 MBytes  3.56 Gbits/sec
[  5]   5.00-6.00   sec   445 MBytes  3.73 Gbits/sec
[  5]   6.00-7.00   sec   422 MBytes  3.54 Gbits/sec
[  5]   7.00-8.00   sec   441 MBytes  3.70 Gbits/sec
[  5]   8.00-9.00   sec   426 MBytes  3.57 Gbits/sec
[  5]   9.00-10.00  sec   437 MBytes  3.67 Gbits/sec
[  5]  10.00-10.04  sec  17.2 MBytes  3.78 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-10.04  sec  4.13 GBytes  3.53 Gbits/sec                  receiver
```

Obrázok 27 Priepustnosť pri 10 sekundách

V našom prípade som v príkaze pre testovanie pridal argument *–t „číslo s“,* kde som v sekundách navolil čas testovania dostačujúci pre otestovanie priepustnosti. Nastavenie času bolo zvolené na 180 sekúnd.

```
[  5] 169.00-170.00 sec   258 MBytes  2.16 Gbits/sec
[  5] 170.00-171.00 sec   375 MBytes  3.14 Gbits/sec
[  5] 171.00-172.00 sec   389 MBytes  3.26 Gbits/sec
[  5] 172.00-173.00 sec   375 MBytes  3.15 Gbits/sec
[  5] 173.00-174.00 sec   385 MBytes  3.23 Gbits/sec
[  5] 174.00-175.00 sec   363 MBytes  3.05 Gbits/sec
[  5] 175.00-176.00 sec   352 MBytes  2.95 Gbits/sec
[  5] 176.00-177.00 sec   390 MBytes  3.27 Gbits/sec
[  5] 177.00-178.00 sec   387 MBytes  3.24 Gbits/sec
[  5] 178.00-179.00 sec   385 MBytes  3.23 Gbits/sec
[  5] 179.00-180.00 sec   308 MBytes  2.58 Gbits/sec
[  5] 180.00-180.05 sec  14.9 MBytes  2.56 Gbits/sec
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate
[  5]   0.00-180.05 sec  69.9 GBytes  3.34 Gbits/sec                  receiver
-----------------------------------------------------------
Server listening on 5201
-----------------------------------------------------------
```

Obrázok 28 Priepustnosť pri 180 sekundách

Z výsledkov testovania môžeme vidieť, že dátový tok medzi zariadeniami je rádovo v jednotkách Gigabit za sekundu. Môžeme preto tvrdiť, že rýchlosť pripojenia, respektíve rýchlosť sieťovej karty, nemá vplyv na spracovanie dát vo vytvorenom VPN clusteri.

5.3.2 Apache Benchmark

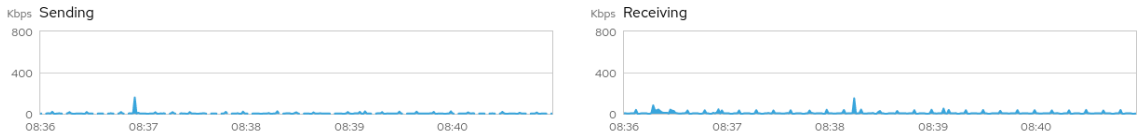
V prípade Apache Benchmarku nejde iba o testovanie sieťového zaťaženia, ale berú sa do úvahy aj komponenty v tomto zariadení. Pri tomto testovaní môžeme určiť, či rýchlosť procesoru alebo veľkosť operačnej pamäte ovplyvňujú rýchlosť posielania dát na sieti. V tomto prípade prebiehalo testovanie dvoma spôsobmi.

Prvým spôsobom bolo monitorovanie v prípade, že cluster pracuje iba v takom nastavení, v akom je ukázaný pri jeho návrhu tak, že sú pripojené dva členské servery clusteru a tri zariadenia pristupujúce mimo cluster. Z týchto zariadení sú dve nastavené ako obyčajný

užívateľ, zatiaľ čo tretie zariadenie pracuje ako privilegovaný užívateľ s povolenými niektorými právami.

Na *Obrázku 29* môžeme pozorovať bežné zaťaženie radiča clusteru pri mnou navrhovanom zapojení tohto clusteru. Môžeme vidieť, že priemerná rýchlosť prijímania a odosielania dát sa pohybuje rádovo v desiatkach kilobit za sekundu.

Na rovnakej úrovni rýchlostí sa pohybujú aj jednotlivé členy celého clusteru, keďže zaťaženie radiču je rovnomerne rozdeľované medzi tieto členy.



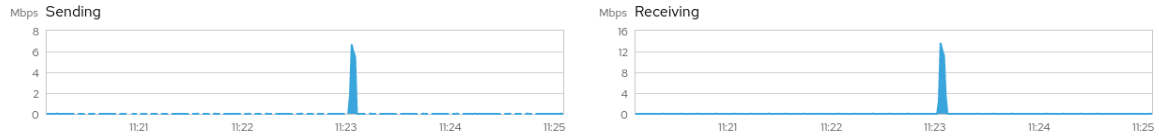
Obrázok 29 Zaťaženie siete navrhovaného clusteru

Druhý spôsob monitorovania je úzko spätý s prvým spôsobom. Monitorovanie rovnako prebieha pomocou nástroja Cockpit. Rozdiel nastáva s pripojenými zariadeniami, kde na radič clusteru je, okrem navrhovaných zariadení, pripojený aj Apache server. Pomocou nástroja benchmark sú z tohto serveru posielané požiadavky na radič a monitorovaná jeho záťaž. Tieto požiadavky sú nastavované priamo užívateľom a je možné nastavenie aj viacnásobného pripojenia v jeden moment. Syntax príkazu pre testovanie je: *ab -n „číslo“ -c „číslo“ protokol:///“ip_adresa:port/“,* kde argument *n* označuje počet požiadaviek a argument *c* počet pripájaných zariadení v jeden moment.

Na nasledujúcich obrázkoch môžeme pozorovať zvýšenie rýchlosti odosielania a prijímania dát na jednotlivých grafoch. Rýchlosť už je limitovaná hardvérovým zložením zariadenia, teda presnejšie rýchlosťou procesora alebo veľkosťou pamäte RAM.

V prvom prípade môžeme vidieť test pri nastavení benchmarku s 10 000 požiadavkami pri pokuse s pripojením 100 užívateľov v jeden moment. Ako ukazuje obrázok, vykonanie trvá rádovo pár jednotiek sekúnd. Podrobnejší výpis z benchmarku je ukázaný v prílohe. V tomto prípade príkaz pre test vypadal nasledovne:

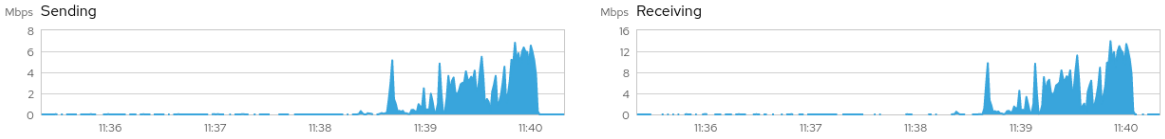
ab -n 10000 -c 100 https://192.168.160.128:992/



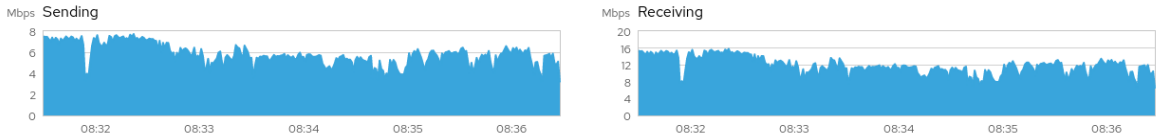
Obrázok 30 Mierne zaťažanie clusteru

V druhom benchmarku je užívateľom nastavených 100 000 požiadaviek pri 100 pripojeniach v jeden čas. Na tomto obrázku môžeme lepšie pozorovať obmedzenie hardvéru. Maximálna rýchlosť odosielania a prijímania dát je rovnaká ako pri predchádzajúcom pripojovaní. Zmenil sa akurát čas potrebný pre vykonanie tohto testu, kde z pár sekundového testu, ako to bolo v predchádzajúcom prípade, sa doba testu zvýšila na rádovo minúty. Príkaz pre test vypadal nasledovne:

ab -n 100000 -c 100 https://192.168.160.128:992/

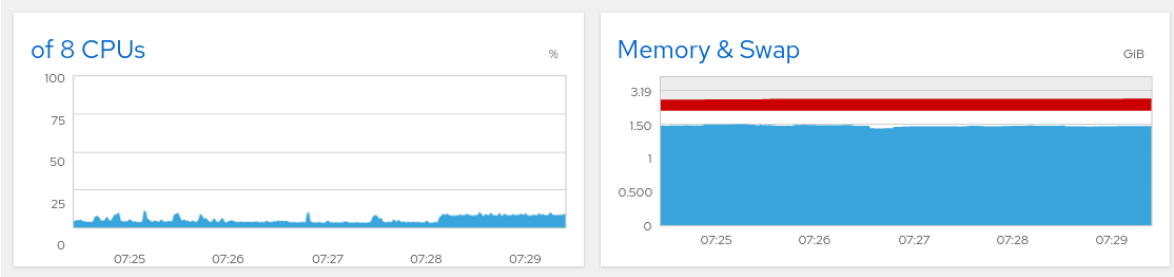


Obrázok 31 Väčšie zaťaženie clusteru



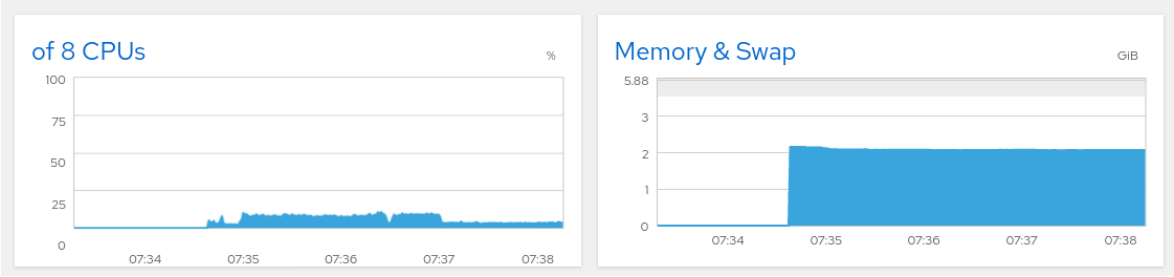
Obrázok 32 Maximálne zaťaženie

V tomto prípade môžeme tvrdiť, že hardvérovým obmedzením celého clusteru je veľkosť operačnej pamäte zariadenia, keďže jednotlivé zariadenia majú nastavenú pamäť na 2 GB. Pri dosiahnutí tohto limitu sa bude doba vykonávania jednotlivých požiadaviek predlžovať, čo môže mať za následok veľké oneskorenie siete. Ide však o limitáciu pri obrovskom počte pripojených zariadení. Pri menších, stredných a firmách so zariadeniami do 10 000 užívateľov je toto oneskorenie siete zanedbateľné.



Obrázok 33 Limity vyťaženia CPU a RAM

Pre overenie, že obmedzenie rýchlosti prenosu má za následok veľkosť operačnej pamäte, je pri radiči v programe *VMware* zvýšená veľkosť operačnej pamäte pre systém na 4 GB. Z obrázku môžeme vidieť, že hodnota sa drží stále na 2 GB operačnej pamäte. Je to preto, že celý cluster pracuje tak rýchlo, ako rýchly je jeho najpomalší člen, čo v tomto prípade sú oba členské servery. Rovnako tak môžeme vidieť, že rýchlosť procesoru je dostačujúca, pretože za celý čas testovania vyťaženie neprekročilo ani 25 %.



Obrázok 34 Limity vyťaženia CPU a RAM pri zvýšení RAM

ZÁVER

Výsledkom diplomovej práce bolo poukázanie na možnosti vytvorenia VPN aj iným spôsobom, než je v súčasnosti pri väčšine sietí štandardné. Presnejšie teda formou clusteru v programe Softether.

V teoretickej časti práce sú popísané základné informácie o VPN - čo to VPN je, k čomu sa používa, jej základné rozdelenie na typy VPN v závislosti od prístupu a základné, či už bezpečnostné alebo iné požiadavky, v závislosti od celkového využitia tejto siete. V nasledujúcej kapitole je práca zameraná na najpoužívanejšie protokoly využité pri zabezpečení VPN. Pri jednotlivých protokoloch je vysvetlený princíp fungovania, výhody a nevýhody využitia takéhoto protokolu a jeho základný popis. Taktiež je pri každom protokole poukázané na jeho priame chyby v zabezpečení formou vybraných CVE kódov. V závere teoretickej časti sú špecifikované požiadavky na VPN cluster. Je tu vysvetlené k čomu slúži radič clusteru, jednotliví členovia, akým spôsobom cluster reaguje pri poruchách a akým štýlom vyrovnáva celkové zaťaženie siete. Taktiež sú doplnené informácie o statických a dynamických huboch a hromadnej správe clusteru.

V praktickej časti je následne navrhnutý vlastný VPN cluster. Tento návrh je implementovaný v testovacej infraštruktúre. V tomto prípade implementácia clusteru prebiehala pomocou programu VMware, teda vo virtuálnom prostredí. Implementácia takto vytvoreného clusteru je podrobnejšie popísaná v prvej kapitole praktickej časti. Celá implementácia je doplnená o obrázky a syntax jednotlivých príkazov slúžiacich pre vytvorenie a následné nastavenie siete. Rovnako tak je v tejto časti poukázané na základné zabezpečenie clusteru, či už formou nastavenia jednotlivých skupín pre užívateľské účty, tak aj formou access listov povoľujúcich prístup do siete špecifickým užívateľom.

Výsledkom práce je následné otestovanie vytvoreného clusteru, ako z pohľadu funkčnosti, tak základného zabezpečenia clusteru a záťažových testov. Tieto testy taktiež slúžia pre vymedzenie hardvérových limitov clusteru, na ktoré je poukázané v závere práce. Celé testovanie je taktiež doplnené syntaxou a grafmi.

ZOZNAM POUŽITÝCH ZDROJOV

[1] NFON. *P2P.* [Online] [Dátum: 21. 3 2021.] https://www.nfon.com/en/service/knowledge-base/knowledge-base-detail/p2p#:~:text=A%20point%2Dto%2Dpoint%20connection,up%20or%20disconnected%20following%20communication..

[2] Microsoft. *About Point-to-Site VPN.* [Online] 2. 9. 2020. [Dátum: 3. 2. 2021.] https://docs.microsoft.com/en-us/azure/vpn-gateway/point-to-site-about#:~:text=A%20Point%2Dto%2DSite%20(,it%20from%20the%20client%20computer..

[3] paloaltonetworks. *What Is a Site-to-Site VPN?* [Online] [Dátum: 3. 2. 2021.] https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn.

[4] The Economic Times. *Definition of 'Authorization'.* [Online] [Dátum: 31. 3 2021.] https://economictimes.indiatimes.com/definition/authorization.

[5] wikipedia. *Authorization.* [Online] [Dátum: 31. 3 2021.] https://en.wikipedia.org/wiki/Authorization.

[6] Internet-Computer-Security. *VPN Authentication - IPsec VPN Tutorial Guide.* [Online] [Dátum: 3. 2. 2021.] http://www.internet-computer-security.com/VPN-Guide/Authentication.html.

[7] webcubatortechnologies. *What Is The Meaning Of Credible Data?* [Online] 17. 7 2020. [Dátum: 31. 3 2021.] https://webcubatortechnologies.medium.com/what-is-the-meaning-of-credible-data-554ae3cee1e6.

[8] techopedia. *Integrity.* [Online] [Dátum: 31. 3 2021.] https://www.techopedia.com/definition/10284/integrity#:~:text=Integrity%2C%20in%20the%20context%20of,safeguarded%20from%20unauthorized%20user%20modification..

[9] microsoft. *Ensuring Data Integrity with Hash Codes.* [Online] 14. 7 2020. [Dátum: 31. 3 2021.] https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes#:~:text=A%20hash%20value%20is%20a,length%20that%20uniquely%20identifies%20data.&text=Hash%20values%20are%20also%20useful,whether%20the%20data%20was%20altered.

[10] Calvello, Mara. learn. *VPN Protocols: Are You Using the Right One?* [Online] 28. 4 2020. [Dátum: 6. 4 2021.] https://learn.g2.com/vpn-protocols.

[11] Crist, Eric F a Keijser, Jan Just. *Mastering OpenVPN.* Birmingham : PackPublishing, 2015. ISBN 1-78355-314-6.

[12] geeksforgeeks. *IP security (IPSec).* [Online] 4. 2 2020. [Dátum: 1. 4 2021.] https://www.geeksforgeeks.org/ip-security-ipsec/.

[13] rapid7. *Basics of IPsec.* [Online] 13. 2 2017. [Dátum: 1. 4 2021.] https://blog.rapid7.com/2017/02/13/basics-of-ipsec/.

[14] security-portal. *Jak funguje IPSEC ?* [Online] 7. 12 2005. [Dátum: 1. 4 2021.] https://www.security-portal.cz/clanky/jak-funguje-ipsec.

[15] wikimedia. *IPsec.* [Online] [Dátum: 1. 4 2021.] https://upload.wikimedia.org/wikipedia/commons/6/64/Ipsec-esp-tunnel-and-transport.svg.

[16] wikimedia. *IPsec.* [Online] [Dátum: 1. 4 2021.] https://upload.wikimedia.org/wikipedia/commons/a/a8/Ipsec-ah.svg.

[17] zive. *Jak na zabezpečení komunikace přes IPsec.* [Online] 9. 2 2012. [Dátum: 1. 4 2021.] https://connect.zive.cz/clanky/jak-na-zabezpeceni-komunikace-pres-ipsec/sc-320-a-162291/default.aspx.

[18] cve. *Common Vulnerabilities and Exposures.* [Online] [Dátum: 6. 4 2021.] https://cve.mitre.org/index.html.

[19] networkencyclopedia. *Point-to-Point Tunneling Protocol (PPTP).* [Online] [Dátum: 1. 4 2021.] https://networkencyclopedia.com/point-to-point-tunneling-protocol-pptp/.

[20] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí.* Brno : CP Books, 2005. ISBN 8025104176.

[21] networkencyclopedia. *Point-to-Point Tunneling Protocol (PPTP).* [Online] [Dátum: 6. 4 2021.] https://networkencyclopedia.com/wp-content/uploads/2019/09/point-to-point-tunneling-protocol-pptp.gif.

[22] Team, SSL Support. ssl. *What is SSL?* [Online] 2. 10 2019. [Dátum: 6. 4 2021.] https://www.ssl.com/faqs/faq-what-is-ssl/.

[23] openvpn. *OpenVPN (OSS).* [Online] [Dátum: 1. 4 2021.] https://community.openvpn.net/openvpn/wiki/OverviewOfOpenvpn.

[24] vladtalks. *What is the OpenVPN protocol, and what are its 5 hype advantages?* [Online] 23. 2 2021. [Dátum: 1. 4 2021.] https://vladtalks.tech/vpn/what-is-openvpn-protocol.

[25] vladtalks. *What is WireGuard and why it may be your new VPN friend.* [Online] 3. 3 2021. [Dátum: 1. 4 2021.] https://vladtalks.tech/vpn/what-is-wireguard.

[26] wireguard. *WireGuard: Next Generation Kernel Network Tunnel.* [Online] 1. 6 2020. [Dátum: 1. 4 2021.] https://www.wireguard.com/papers/wireguard.pdf.

[27] paloaltonetworks. *Create a VPN Cluster.* [Online] [Dátum: 7. 4 2021.] https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/configure-sd-wan/create-a-vpn-cluster.html.

[28] softether. *3.9 Clustering.* [Online] [Dátum: 7. 4 2021.] https://www.softether.org/4-docs/1-manual/3._SoftEther_VPN_Server_Manual/3.9_Clustering.

[29] sciencedirect. *Cluster Controller.* [Online] [Dátum: 7. 4 2021.] https://www.sciencedirect.com/topics/computer-science/cluster-controller.

[30] mik. *Cluster Membership Concepts https://docstore.mik.ua/manuals/hp-ux/en/B3936-90078/ch01s01.html.* [Online] [Dátum: 7. 4 2021.] https://docstore.mik.ua/manuals/hp-ux/en/B3936-90078/ch01s01.html#:~:text=A%20cluster%20is%20a%20networked%20collection%20of%20nodes.&text=As%20nodes%20enter%20and%20leave,halt%2C%20reboot%2C%20or%20crash..

[31] citrix. *What is load balancing?* [Online] [Dátum: 7. 4 2021.] https://www.citrix.com/solutions/app-delivery-and-security/load-balancing/what-is-load-balancing.html#:~:text=Load%20balancing%20is%20defined%20as,server%20capable%20of%20fulfilling%20them..

[32] imperva. *Fault Tolerance.* [Online] [Dátum: 7. 4 2021.] https://www.imperva.com/learn/availability/fault-tolerance/.

[33] Lamb, Joseph M. *Windows 2000 Clustering and Load Balancing Handbook.* 1st edition. mesto neznáme : Pearson, 2001. s. 432. ISBN 978-0130651990.

[34] Lewis, Mark. *Comparing, Designing And Deploying VPNSs.* místo neznámé : AdobePress, 2006.

[35] Trulove, James. *Sítě LAN: hardware, instalace a zapojení.* Praha : Grada, 2009. s. 384. ISBN 978,80-247-2098-2.

[36] Scott, Charlie, Wolfe, Paul a Erwin, Mike. *Virtual Private Networks.* Second Edition. místo neznámé : O'Reilly, 1999. 1-56592-529-7.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

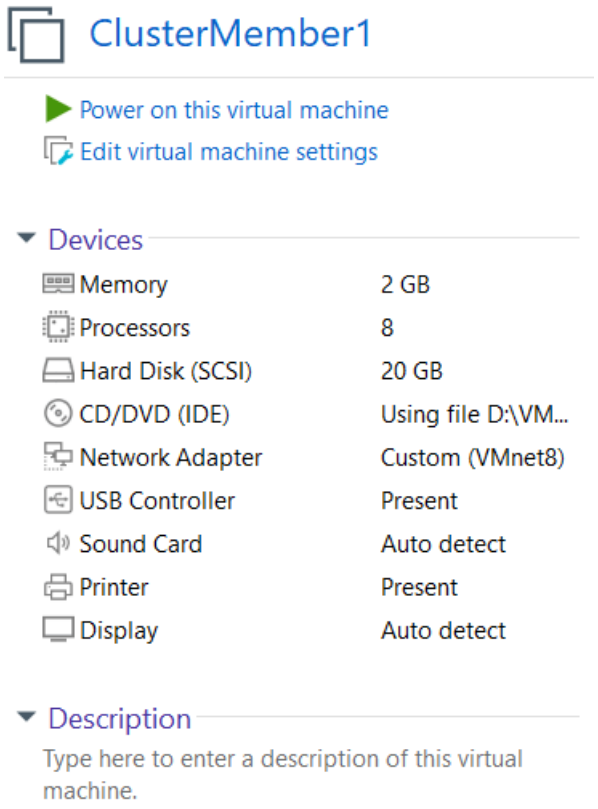
VPN	**V**irtual **P**rivate **N**etwork
P2S	**P**oint-to-**S**ite
IP	**I**nternet **P**rotocol
IPsec	**I**nternet **P**rotocol **Sec**urity
IETF	**I**nternet **E**ngineering **T**ask **F**orce
ESP	**E**ncapsulating **S**ecurity **P**ayload
AH	**A**uthentication **H**eader
SA	**S**ecurity **A**ssociation
SAD	**S**ecurity **A**ssociation **D**atabase
SPA	**S**ecurity **P**arameter **I**ndex
IKE	**I**nternet **K**ey **E**xchange
ISAKMP	**I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol
PPTP	**P**oint-to-**P**oint **T**unneling **P**rotocol
TCP	**T**ransmission **C**ontrol **P**rotocol
L2TP	**L**ayer 2 **T**unneling **P**rotocol
L2F	**L**ayer 2 **F**orwarding Protocol
LCP	**L**ine **C**ontrol **P**rotocol
LAC	**L**2TP **A**ccess **C**oncentrator
LNS	**L**2TP **N**etwork **S**erver
MITM	**M**an-**I**n-**T**he-**M**iddle
SSL	**S**ecure **S**ocket **L**ayer
TLS	**T**ransport **L**ayer **S**ecurity
UDP	**U**ser **D**atagram **P**rotocol
DoS	**D**enial **o**f **S**ervice
TCP/IP	**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: HARDVÉROVÁ ŠPECIFIKÁCIA ZARIADENIA



PRÍLOHA P II: VÝPIS APACHE BENCHMARKU PRI HODNOTE 10 000 A 100 000

```
Concurrency Level:      100
Time taken for tests:   2.968 seconds
Complete requests:      10000
Failed requests:        0
Total transferred:      33936 bytes
HTML transferred:       31984 bytes
Requests per second:    3368.95 [#/sec] (mean)
Time per request:       29.683 [ms] (mean)
Time per request:       0.297 [ms] (mean, across all concurrent requests)
Transfer rate:          11.16 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    0   0.0      0       0
Processing:     7   25   4.2     23      50
Waiting:        0    0   0.0      0       0
Total:          7   25   4.2     23      50

Percentage of the requests served within a certain time (ms)
  50%     23
  66%     25
  75%     26
  80%     27
  90%     30
  95%     33
  98%     37
  99%     39
 100%     50 (longest request)
```

```
Concurrency Level:      100
Time taken for tests:   28.879 seconds
Complete requests:      100000
Failed requests:        27164
   (Connect: 0, Receive: 0, Length: 27164, Exceptions: 0)
Total transferred:      33936 bytes
HTML transferred:       31984 bytes
Requests per second:    3462.70 [#/sec] (mean)
Time per request:       28.879 [ms] (mean)
Time per request:       0.289 [ms] (mean, across all concurrent requests)
Transfer rate:          1.15 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:        0    0   1.1      0      92
Processing:     8   29 269.2     25   21394
Waiting:        0    2   9.8      0      50
Total:          8   29 270.3     25   21398

Percentage of the requests served within a certain time (ms)
  50%     25
  66%     26
  75%     27
  80%     28
  90%     29
  95%     30
  98%     32
  99%     34
 100%  21398 (longest request)
```