Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Metody bezpečného připojení k podnikovým datovým zdrojům

Bakalářská práce

Autor: Jan Sakač
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Pavel Blažek Ph.D.

Hradec Králové Duben 2022

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 29.4.2022 Jan Sakač

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Pavlovi Blažkovi Ph.D. za metodické vedení práce, podnětné rady a čas, který mi věnoval.

Anotace

Bakalářská práce je zaměřena na vzdálený a zabezpečený přístup k podnikovým datovým zdrojům. Komunikace v datových sítích je postavena na přenosových protokolech, které v dnešní době již neposkytují dostatečnou ochranu před kompromitací přenášených dat, proto je nutné implementovat zabezpečení na vyšších vrstvách. Běžná činnost uživatele v prostředí internetu je široce rozptýlena mezi soukromou činnost, ale zahrnuje také podniková data. Kategorie zaměstnanců firem klade na konektivitu jiné nároky. Potřebují zabezpečený přístup k firemním datům a službám. Podobně je tomu v případě poboček a pracovišť s centrální konektivitou, kdy je pro ně nezbytné spojení se sítí mateřské firmy. K tomuto účelu jsou zřizovány VPN spoje, k nimž se váží různé prvky zabezpečení.

Klíčová slova

bezpečnost, vzdálený přístup, virtuální privátní síť, RADIUS, L2TP, IPsec

Annotation

Title: Methods of secure connection to corporate data sources

The bachelor thesis is focused on remote and secure access to corporate data sources. Communication in data networks is based on transmission protocols, which today do not provide sufficient protection against the compromise of transmitted data, so it is necessary to implement security at higher layers. The user's normal activity in the Internet environment is widely dispersed among private activity but also over corporate data. The category of company employees' places different demands on connectivity. They need secure access to corporate data and services. The same is true in the case of branches and workplaces with central connectivity, where a connection to the parent company's network is necessary for them. For this purpose, VPN connections are established, to which various security elements are attached.

Keywords

Security, remote access, virtual private network, RADIUS, L2TP, IPsec

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Postupně se rozvíjející možnosti a dostupné technologie způsobily masivní rozvoj internetu, který začal sloužit nejenom pro výzkumné účely, ale také pro usnadnění komunikace, pro osobní účely a pro využití v podnicích. Firmy svým rozvojem přesáhly jednu budovu a rozšířily se do mnoha míst nebo obchodů po celé zemi a celém světě. Aby firmy fungovaly efektivně, musejí se v různých lokalitách spolehnout na rychlý, bezpečný a spolehlivý přístup k podnikovým datům.

Před několika lety bylo nejběžnějším způsobem propojení počítačů mezi více kancelářemi a budovami pomocí pronajaté linky. Pronajaté linky, jako je ISDN (Integrated Services Digital Network, s přenosovou rychlostí 128 Kbps), jsou privátní síťová připojení, která jsou realizována skrze veřejné telekomunikační sítě, která může telekomunikační společnost pronajmout svým zákazníkům. Pronajaté okruhy poskytují společnosti způsob, jak rozšířit svou privátní síť mimo její bezprostřední geografickou oblast. Přestože jsou pronajaté okruhy spolehlivé a bezpečné, pronájmy linek jsou drahé a náklady rostou se zvětšující se vzdáleností mezi kancelářemi.

Hlavním impulsem rozvoje propojování vzdálených sítí byl mohutný rozvoj internetu. Dokud byly firemní pobočky propojeny pevnými linkami nebo frame-relay spoji, zpravidla státního Telecomu (tzv. plně privátní sítě), podniky necítily zvláštní potřebu chránit svá data. Situace se ale výrazně změnila, když vznikla možnost a nabídka levného propojení poboček nebo připojení uživatele ke vzdálenému zařízení přes internet. Podniky se rozšiřovaly, zvyšoval se počet různých oddělení a také počet budov, které bylo potřeba propojit do podnikové sítě, ve které se pohybovalo čím dál větší množství dat. [1]

Internet se postupně stával dostupnější než kdykoli předtím a poskytovatelé internetových služeb (ISP) dále vyvíjeli rychlejší a spolehlivější služby za nižší náklady než pronajaté linky. Technologie pro datové přenosy se neustále vyvíjejí a

postupně nahrazují nebo spolupracují se sítěmi pro přenos hlasu. Společně nyní tvoří univerzální datovou síť, která poskytuje všechny dostupné služby. Aby toho většina podniků využila, nahradila pronajaté okruhy novými technologiemi, které využívají připojení k internetu bez obětování výkonu a zabezpečení.

Jednou z prvních možností pro dosažení těchto cílů je VPN (virtuální privátní síť). VPN je soukromá síť, která využívá veřejnou síť ke spojení vzdálených webů nebo uživatelů. VPN využívá virtuální připojení vedená přes internet z privátní sítě podniku nebo služby VPN třetí strany ke vzdálenému webu nebo uživateli. VPN vzdálené připojení zajišťuje bezpečnost pomocí šifrování dat, které prochází skrze veřejnou síť. [2]

Z počátku se VPN používaly téměř výhradně v podnikání. Klíčovým momentem v historii technologie VPN však bylo náhlé narušení bezpečnosti, ke kterému došlo na počátku 21. století. Díky tomu si každodenní uživatelé internetu uvědomili skutečná rizika online práce a začali hledat bezpečnější způsoby vzdáleného připojení. Dnes se síť VPN používá k zabezpečení internetového připojení, prevenci malwaru a hackerů, zajištění digitálního soukromí, odemknutí geograficky omezeného obsahu a skrytí fyzické polohy uživatelů. Síť VPN, jejíž použití je snadnější a je cenově dostupnější než pronajaté linky, je základním nástrojem pro udržení bezpečí online. [3]

Dnešní podniky vlastní rozsáhlé IT prostředí a stále rozšiřují oblasti svého působení. Podniková data se šíří do nejvzdálenějších oblastí obchodního působení napříč budovami podniků a cloudovými platformami v různých formátech.

Masivní objem dat, nehledě na jejich různorodost a variabilnost, téměř znemožňuje jejich efektivní lokalizaci, řádnou klasifikaci podle úrovně jejich citlivosti a implementaci strategie ochrany informací pomocí konvenčních prostředků a metod. V potaz se také musí brát nárůst nařízení o ochraně osobních údajů, jako je GDPR, CCPA a HIPAA (a mnoha dalších), a požadavky na robustní přístup k minimalizaci rizika porušení těchto zákonů a na zabezpečení klíčových informací.

Mnoho organizací přehodnocuje své přístupy k zachování soukromí a bezpečnosti citlivých údajů.

Podniky se spoléhaly na vlastní strukturu zabezpečení na svých serverech, kde nástroje pro ochranu informací poskytoval dodavatel. Dnešní podniky však stále více přecházejí na cloudovou obchodní strategii a vynakládají více zdrojů na soukromá a veřejné cloudová řešení než v minulosti.

Data v moderním IT ekosystému jsou různorodá a jsou rozprostřena napříč různými platformami a operačními systémy, v různých aplikacích cloudových úložišť a prostředí, jak ve strukturovaných, tak i v nestrukturovaných formátech. Ukládání citlivých dat v tak široké škále operačních systémů, cloudových prostředí a objektů, vede ke zhoršování zjišťování, klasifikaci a aplikaci vhodných omezení použití – zejména u zastaralých manuálních procesů nebo řešení zprostředkované externím dodavatelem, která pokrývají pouze malou část uložených dat. [4]

Digitální transformace hluboce mění veškeré aspekty fungování dnešních podniků. Masivní objem dat, které podniky vytvářejí, s nimiž manipulují a ukládají je, roste a zvyšuje potřebu správy dat. Kromě množství dat jsou výpočetní prostředí složitější než v dřívějších dobách a běžně zahrnují veřejný cloud, podniková datová centra a řadu okrajových zařízení, od senzorů internetu věcí (IoT), po roboty a vzdálené servery. Tato složitost vytváří rozšířenou plochu útoku, jejíž sledování a zabezpečení je náročnější. [5]

Internet věcí se stává čím dál dostupnější a rozšířenější, nejenom pro domácí zařízení, která jsou používaná pro zlepšení každodenního života, ale také pro podniky, které nalézají jejich využití pro zlepšení a zjednodušení provozu (vnitřní (interní) části firmy).

Internet věcí (IoT) se vyvíjí velmi rychle a ukazuje první náznaky chytrého prostředí pro budoucnost. Spolu s jejich oblibou se ale šíří obavy o bezpečnost IoT zařízení, zejména kvůli nedostatku standardních bezpečnostních kontrol, omezenými zdroji

pro vývoj zabezpečení, nebo absencí standardních síťových protokolů jiných bezpečnostních mechanismů. Nízká míra bezpečnosti udává, že IoT zařízení nejsou vhodná pro dynamické prostředí internetu. Současná prostředí IoT zařízení využívají převážně cloudové přístupy, kde se mohou data přeposílat v neomezeném množství, což vede k dalším rizikům pro bezpečnost a soukromí.

V IoT existuje ohromné množství připojených zařízení. Tato zařízení shromažďují a přenášejí velké objemy dat mezi zařízeními, ze zařízení do podnikových sítí a příležitostně ze zařízení k lidem. Vzhledem k jejich počtu existuje velké riziko krádeže identity a dat, manipulace se zařízením, falšování dat, manipulace se serverem či sítí a jejich následný dopad na podnikové aplikace. Zabezpečení internetu věcí má mnoho aspektů – zabezpečení zabudované v zařízení, zabezpečení přenosu dat a ukládání dat v systémech a jejich aplikacích.

Pro internet věcí se postupně přidávají standardní bezpečnostní protokoly, jako jsou virtuální privátní sítě, pro určitá prostředí internetu věcí, současně implementované modely mají několik variant a jsou prakticky neškálovatelné pro jakékoli dynamicky škálovatelné nasazení IoT. [6]

Před rokem 2020 se objevovaly benefity ve formě práce na dálku, ale teprve během pandemie COVID-19 byly podniky nuceny urychleně přijmout hybridní nebo vzdálenou pracovní politiku, aby udržely podniky v chodu a zároveň chránily své zaměstnance. Během tohoto období IT pracovníci nasazovali do provozů podnikové aplikace a zařízení do cloudů a zároveň umožňovali vzdálený přístup do podnikové sítě skrze nespravovaná zařízení a neschválené sítě. IT pracovníci museli rovněž poskytnout ochranu pro tento náhlý přechod a úspěšně zvládnout nárůst bezpečnostních problémů.

Zajištění bezpečnosti a nepřerušované připojení pro vzdálený přístup k podnikové datové síti, se stalo důležitější než kdy dříve. Kromě ochrany majetku společnosti a soukromí zaměstnanců, musejí společnosti zvládat nové bezpečnostní hrozby.

Stále více zaměstnanců používá svá osobní zařízení pro pracovní účely. Většina domácích zařízení ale nemá zavedenu takovou úroveň zabezpečení jako podniková zařízení, což z těchto zařízení činí snadný cíl pro narušení bezpečnosti. Narušitelé využívají měnícího se pracovního prostředí a nedostatečné povědomí zaměstnanců o bezpečnosti. Mnoho řadových zaměstnanců se během pandemie COVID-19 stalo terčem útoků. Mezi útoky patří hlavně nárůst phishingových e-mailů nebo podvodů typu clickbait.

Ochranou před útoky se může stát celá řada bezpečnostních opatření. Mezi nejzásadnější body patří vynucování zásad vzdáleného zabezpečení, zabezpečení koncových bodů, zajištění aktuálního softwaru, vynucení přístupových kódů a hesel na všech zařízeních, a další pokročilé metody, jako například skenování zranitelnosti a DMZ v síti, uzavření nepoužívaných portů a vytvoření samostatných brán firewallu. [7]

2 Cíl práce

Cílem bakalářské práce je nastudovat a popsat možnosti připojení vzdálených klientů ke službám ve firemní síti a také propojení poboček s mateřskými sítěmi, které se mohou nacházet v různých geografických lokacích. Na základě získaných poznatků navrhnout a realizovat VPN spoj s využitím běžně provozovaných technologií. Následně zhodnotit klady a zápory realizace a určit vhodnost pro cílovou skupinu dle množství obsluhovaných klientů.

3 Úvod do problematiky geograficky rozdělených sítí

Ve věku globální integrace, síťové konektivity a širokých partnerských spoluprací je práce zaměstnanců stále častěji vykonávána v geograficky rozptýlených lokalitách. Distribuované týmy a pobočky podniků sdílejí odpovědnost za produkt, službu nebo funkci, kvůli které se musejí seskupovat do různých, mnohdy virtuálních pracovních skupin a spolupracovat na společném úkolu. [7]

3.1 Klasifikace počítačových sítí

Počítačová síť je skupina počítačů, či periferií, které jsou mezi sebou propojeny k zajištění vzájemné komunikace libovolného uživatele s programem na libovolném počítači. To vše při maximálně vysoké spolehlivosti komunikace. [8] Počítačové sítě lze klasifikovat a kategorizovat na základě určitých kritérií.

Dělení počítačových sítí podle rozlehlosti

PAN (Personal Area Network) – PAN je osobní síť tvořená zařízeními komunikujícími na krátké vzdálenosti, obvykle několik málo metrů a je převážně využíván pro osobní účely [8]. Mezi PAN sítě patří například Bluetooth, IrDA (Infrared Data Association), nebo USB. [10]

LAN (Local Area Network) – LAN je lokální síť v rozlehlosti desítek až stovek metrů, obvykle v rámci jedné budovy. Propojuje koncová zařízení do jedné sítě. Mezi LAN sítě patří Wifi a Ethernet.

MAN (Metropolitan Area Network) – Jedná se o metropolitní síť o velikosti několika bloků budov, až celé město. Slouží zejména k propojení různých LAN sítí do společné sítě a často se jedná o přístupové sítě do internetu.

WAN (Wide Area Network) – WAN je velmi rozlehlá síť, která pokrývá rozsáhlé geografické území, jako je region, stát, či kontinent. Slouží zejména k vzájemnému propojení menších sítí (jako různé LAN a MAN sítě). [9]

Dělení sítí podle vlastnictví

Privátní síť – Privátní (interní či vnitřní) síť znamená soukromý, proprietární síťový zdroj přístupný pouze zaměstnancům, případně jednotlivým dodavatelům (tj. dočasným zaměstnancům) konkrétní korporace nebo podobnému obchodnímu subjektu. Interní síť nezahrnuje části internetu, ani žádnou jinou síťovou komunitu otevřenou veřejnosti, jako jsou skupiny, sdružení a podobné organizace, založené na členství nebo předplatném. Počítače a zdroje v soukromé síti jsou chráněné a přístupné pouze ověřeným uživatelům. [11]

Veřejná datová síť (Public Data Network) – je druh veřejné telekomunikační sítě pro přenos dat. Běžnými provozovateli veřejných sítí jsou propojovací organizace, mezi které současně patří i provoz telekomunikačních sítí (například veřejné datové sítě), určený pro přenos dat. Data mohou přenášet hlas, obraz, aj.

Provozovateli veřejných datových sítí se mohou stát jakékoliv subjekty, které vyhoví podmínkám pro získání licence na poskytování veřejných služeb přenosu dat. V České republice se o správu veřejných služeb pro přenos dat stará Český telekomunikační úřad. [12]

Virtuální privátní síť (VPN) – Zajišťuje privátní a zabezpečené spojení, které prochází přes nezabezpečenou datovou infrastrukturu. VPN vytváří tunel, tj. komunikační síť mezi dvěma body, ať už mezi koncovými nebo propojovacími body, zapouzdřením (encapsulation) původních dat. [9]

VPN sítě se dělí na dvě skupiny. První skupinou jsou VPN pro vzdálený přístup (anglicky Remote Access VPN), které umožňují uživatelům se připojit se k jiné síti přes soukromý šifrovaný tunel. Druhou skupinou jsou tzv. Site-to-Site VPN. Ty jsou používané především v podnikových prostředích, ve kterých mají podniky budovy na více místech. Site-to-Site vytváří uzavřenou interní síť, přes kterou se lze připojovat k jednotlivým pracovištím. Site-to-Site má také označení intranet. [13]

3.1.1 Definice firemních datových zdrojů

Dostupnost datových zdrojů je klíčem k fungování podniku. Jejich dostupnost může zařizovat firemní server ve vlastním datovém centru, který firma spravuje, nebo externě na cloudovém úložišti, kde využívá infrastrukturu třetí strany.

Data uložená na fyzických serverech v podnicích volí společnosti, které mají prostředky na jejich správu a zabezpečení. Bezpečnost a soukromí dat je zvláště důležité v případech, kdy servery obsahují kritická data firmy, jako firemní know-how, osobní údaje zaměstnanců, výzkum a vývoj nebo obchod. [14]

Cloudová řešení mohou využívat firmy z různých oblastí, od výrobní společnosti až po firemní sektor. Jejich hlavní výhodou je dostupnost. Nezáleží na místě, kde je možné se přihlásit do cloudu a veškerá data mají firmy neustále k dispozici. Typy cloudových služeb je možné rozlišit do následujícího modelu, kde se každý z nich zabývá jiným poskytnutím služby. [15]

IaaS – Model „Infrastructure as a Service“ (infrastruktura jako služba) označuje službu, která prostřednictvím webu poskytuje základní hardwarové a softwarové prostředky pro veškeré výpočetní prostředky, prostředky úložiště a síťové prostředky za uhrazování průběžných plateb.

PaaS – Model „Platform as a Service“ (platforma jako služba) využívají nejčastěji vývojáři a provozovatelé softwaru. Služby tohoto modelu zprostředkovávají uživateli pracovní prostředí pro vývoj, tvorbu a testování webových aplikací.

SaaS – Model „Software as a Service“ (software jako služba) dává uživateli k dispozici softwarové aplikace, jejichž údržbu, správu a uchovávání dat řeší poskytovatel služby. Uživatel má k dispozici pouze klientské rozhraní aplikace dostupné přes internet. Jedná se model, který je nejčastěji poskytován pro koncové uživatele.

Cloudové služby mohou být privátní, veřejné, případně hybridní. Každé řešení se využívá v jiném prostředí, má své klady a zápory. Jednou z největších výhod je vyšší bezpečnost. Poskytovatelé cloudových služeb dokážou zajistit lepší a kvalitnější bezpečnost služeb. [16]

Interní počítačová síť

Interní počítačovou síť firmy se zde rozumí lokální počítačová síť (LAN), která ve firmě propojuje alespoň dvě zařízení a nejčastěji slouží k přenosu nebo sdílení dat (např. souborů, interních emailů) a dále ke komunikaci či sdílení připojení k internetu pouze v rámci firmy. [15]

Intranet

Intranet je druhem aplikace, či webové stránky, jejímž hlavním obsahem je usnadnit sdílení obsahu a služeb v rámci podniku. Intranet není dostupný veřejnosti, jeho přístup vyžaduje autentizaci uživatele v místní síti podniku. Případný přístup pro vzdálené uživatele je realizován skrze určitou službu, jako je VPN. Hlavním účelem intranetu je zefektivnit procesy uvnitř podniku, jako je efektivnější komunikace, zjednodušení a centralizace plánování, snazší sdílení dokumentů a podpora podnikové kultury. [17]

Extranet

Extranet je speciální webová stránka či rozšíření intranetu, která slouží ke komunikaci (on-line předávání souborů a informací) s oprávněnými dodavateli, prodejci, partnery, zákazníky a jinými subjekty, kteří jsou organizačně, obchodně nebo místně mimo centrálu firmy. Přístup do extranetu je možný až po autorizaci (přihlášení). [18]

Datové zdroje

Podnikové datové zdroje jsou v síti jedné organizace. Pro geograficky rozdělené firemní prostředí musí být datové zdroje dostupné mezi všemi objekty v rámci

organizace. Pro realizaci dostupnosti datových zdrojů v rámci jedné organizace se využívá tzn. virtuální privátní síť neboli VPN.

Datové zdroje jsou typicky data obrovského rozsahu. Tyto rozsáhlé datové zdroje se rozdělují do určitých druhů, aby bylo možné zajistit efektivní a bezpečný přístup, pro práci a manipulaci s daty [15]. Data procházející podnikovou sítí nejsou homogenní. Typicky jsou v různých formátech – strukturované, nestrukturované, polostrukturované, případně některé jejich kombinace. Ke složitosti dat přispívá i fakt, že každá kategorie dat vyžaduje své vlastní standardy, týkající se různých úrovní přístupu a zabezpečení pro zaměstnance a jiné systémy. [4]

3.1.2 Geografické blokování

Internetový protokol (IP) je hlavní protokol pro identifikaci uživatelů na internetu. Každý uživatel na internetu má jedinečnou IP adresu. Adresy se používají ke směrování IP paketů ze zdroje uživatele k cílovému zdroji, prostřednictvím různých uzlů. Každý paket je spojen se zdrojovou IP a cílovou IP.

Spojení IP adresy s geografickou polohou se však nebere na vědomí. Routery a switche, které směrují pakety do svého cíle, nedbají na geografické umístění zdroje nebo umístění paketu. Tyto informace však mohou najít účel v celé řadě bezpečnostních opatření nebo různých aplikací. IP adresy v paketech se používají pro směrování na místo určení. Hledání zdroje nebo cíle geografického místa packetu v reálném čase je z obecného důvodu nepraktické, protože se upřednostňuje rychlost přenosu paketů. [19]

Geografické blokování nebo také filtrování je úkon odepření nebo omezení přístupu k obsahu na základě geografické polohy daného uživatele, či zařízení, které se snaží přistoupit určitému obsahu. Geografické blokování funguje u všech typů obsahu na internetu, včetně webových stránek, článků, služeb a zvláště videí.

Jednotlivé organizace nebo vládní orgány mohou použít geografické filtry na celé státy, města, a dokonce i budovy, či jednotlivé kanceláře. Stupeň filtrace se může lišit na základě požadované služby.

Při využívání služby používané zařízení pošle zprostředkovatelskému serveru IP adresu pro určení místa, na které má požadovaná data odeslat. IP adresu zprostředkovává poskytovatel internetových služeb (ISP) a ta může s různou úrovní přesnosti identifikovat geografickou polohu zařízení. Funkce ze strany serveru se mohou dále rozhodnout, jestli dané IP adrese umožnit přístup k požadovanému obsahu, případně ji zamítnout.

Obecné důvody geografického blokování

Copyright a licencování – Nejčastějším důvodem je ochrana licencovaného obsahu nebo obsahu chráněného autorským právem. Poskytovatelé obsahu tedy ukládají geografická omezení, aby splnili licenční podmínky.

Segmentace trhu – Některé společnosti používají geografickou filtraci k rozdělení světa na různé segmenty trhu. Výsledkem tohoto rozdělení mohou být omezení přístupu, změna poskytovaného obsahu, nebo jiné ceny za služby, a to vše na základě polohy.

Omezení nelegálního obsahu – Vládní orgány mohou využívat geografické blokování k prosazování svých zákonů a omezovat tak obsah jako je např. hazard, nebo jiný nevhodný obsah. [20]

Geografické blokování je ale také dalším bezpečnostním prvkem pro podnikovou datovou síť. Filtrování IP adres a jejich redukce pouze na určité, se kterými podnik spolupracuje, je účinným způsobem, jak zabránit útokům na základě příchozí i odchozí IP adrese. Pokročilé firewally a poskytovatelé ISP nabízejí možnosti, jak sledovat příchozí IP adresy prostřednictvím informací o registraci DNS. [19]

Nabízí se také možnost nejenom zabraňovat útokům zvenčí, ale také chránit podniky před útoky po narušení bezpečnosti ze strany vzdáleného zaměstnance. Omezení vzdáleného přístupu pro zaměstnance na základě jejich bydliště, či jiné, předem domluvené lokalitě, se může stát dalším stupněm bezpečnosti v podnikové politice bezpečnosti.

3.2 Možnosti propojení sítí a připojení k nim

Na základě požadovaného typu připojení je možné určit způsob, jakým se sítě dají propojit. Správně vybraným druhem spojení sítí jde dosáhnout výrazně větší bezpečnosti, efektivity, či spolehlivosti. Důležitým prvkem pro výběr sítí je jednoznačně vymezit účel připojení na základě kterého bude vybrán typ spojení.

3.2.1 Architektura VPN sítí

Virtuální privátní sítě jsou primárně využívané pro přenos dat. Způsob jejich přenosu je definován architekturou VPN sítí na základě jejich charakteristik.

Remote Access VPN

Remote Access umožňuje jedinému zařízení navázat zabezpečené spojení mezi sítí připojovaného zařízení a vzdálené podnikové síti. VPN pro vzdálený přístup vytvoří šifrovaný tunel. [21]

Může se jednat o jakékoliv zařízení, které má instalované VPN klienta, který se připojí ke vzdálenému VPN serveru. Server pro připojení VPN služby vyžaduje autentizaci, buď využije vlastní proces ověření přihlašovacích údajů, nebo ověření zprostředkuje ověřovací server. Remote Access umožňuje hostitelskému počítači bezpečně přijímat a odesílat šifrovaná data skrze veřejný internet. [23]

Site-to-Site VPN

Architektura Site-to-Site zajišťuje spojení mezi dvěma nebo více sítěmi. Tuto architekturu využívají hlavně společnosti s větším počtem poboček v různých

geografických lokalitách, k využití internetového připojení pro nepřetržitý, snadný a bezpečný přístup k podnikovým datovým zdrojům v jejich vlastní síti, ať už jsou hostovány lokálně nebo v cloudu. Díky této architektuře mohou společnosti bezpečně propojit svá data skrze veřejný internet mezi své pobočky, komunikovat a sdílet zdroje jako jedna síť [24]. Primárním účelem Site-to-Site VPN je poskytovat bezpečný přístup k citlivým datům a síťovým zdrojům včetně interních zákaznických a prodejních systémů a místního úložiště souborů pro zaměstnance, kteří k nim přistupují z různých zařízení a potenciálně nebezpečných Wi-Fi připojení. [22]

Koncová zařízení musí být předem nakonfigurovaná s informacemi pro vytvoření zabezpečeného tunelu [24]. Sítě jsou připojené k internetu skrze routery, které při zjištění, že mají odeslat data do vzdálené sítě, data zašifrují, a to jak na začátku komunikace, tak i během relace. Šifrovaná data se odesílají skrze veřejný internet do vzdálené sítě, kde nastane dešifrovací proces a dešifrovaná data se následně odešlou do cílové destinace. [23]

Decentralizovaná VPN

Pomocí běžné VPN se vytvoří zabezpečené spojení mezi zařízením koncového uživatele a serverem poskytovatele VPN. Přidává další vrstvu ochrany internetového připojení a přináší určité výhody v oblasti soukromí a zabezpečení.
Decentralizovaná VPN (také známá jako dVPN nebo P2P VPN) se nejprve připojí k síťovému uzlu. Decentralizovaným síťovým uzlem může být jakékoliv zařízení, například server, počítač, notebook nebo smartphone.

Největší rozdíl mezi VPN sítěmi je konfigurace sítě. Při použití běžné VPN služby se klient připojí k serveru, který je vlastněn a konfigurován VPN službou, která se ve většině případů zavazuje chránit soukromí uživatelů a zamezit shromažďování osobních údajů. Uživatelé musí plně důvěřovat poskytovatelům VPN, že nezasahují do jejich soukromého provozu ani nezaznamenávají žádné osobní údaje. Je důležité uvést, že poskytovatelé VPN jsou komerční subjekty, které se mohou spoléhat na jiné komerční subjekty. Může nastat situace, kdy se i důvěryhodný poskytovatel

může nevědomky účastnit problému, jako je chybná konfigurace, sbírání osobních údajů, a dokonce i hackování. Každý z těchto problémů může ohrozit soukromí uživatelů a podniků. [25]

Decentralizované nebo distribuované VPN (dVPN) jsou druhem virtuálních privátních sítí, které mají za úkol vyřešit problémy s důvěrou a soukromí centralizovaných VPN služeb s využitím distribuované architektury. Decentralizované sítě využívají dynamického spojení distribuované sítě nezávisle provozovaných serverů. Větší počet zabezpečených serverů může umožnit, aby decentralizované sítě VPN fungovaly efektivněji a bezpečněji než centralizované sítě VPN. [26]

Mnoho počítačů spojuje svůj provoz s decentralizovanou VPN a komunikuje pomocí systému Peer-to-Peer (P2P), kde každý počítač může fungovat jako server. Většina dVPN funguje s pomocí technologie blockchain, která nabízí silné zabezpečení.
dVPN je založena na myšlence, že síťové uzly dVPN by měly mít schopnost určit jaký druh provozu budou přenášet, např. komprimované soubory nebo zpravodajské weby. Zároveň by měly přijímat takový provoz, o kterém mají poskytovatelé nulové znalosti, tj. aby neznali přesný obsah síťového provozu. Nakonec se snaží poskytovat takovou bezpečnost a funkce, které jsou známé z běžných VPN, a to s minimálním dopadem na uživatele. [25]

Split tunneling

Split tunneling je jedna z VPN funkcí, která umožňuje rozdělovat internetový provoz přes dva různé tunely, z nichž jeden je šifrovaný a provoz určité aplikace nebo URL adres směřuje skrze zabezpečený kanál, zatímco zbytek provozu je stále přenášen prostřednictvím otevřené sítě. Split tunneling umožňuje výběr dat, která mají zůstat zabezpečená.

Rozdělené sítě umožňují používat dvě připojení současně, z nichž jedno směřování bude používáno pouze pro citlivá data, která mají být šifrovaná, přičemž umožňuje využívat zbytek internetové kapacity pro jiné účely. Touto funkcí je možné zvýšit

rychlost internetového připojení, protože veškerý internetový provoz není nucen procházet přes VPN server. [27]

Zároveň také umožňuje přistupovat k více sítím současně, tudíž vzdálení pracovníci mohou být neustále připojeni k podnikové síti s bezpečnostními protokoly bez použití více zařízeními v danou chvíli a současně být připojeni k místní síti. Použití rozdělené sítě VPN navíc zmírňuje možné problémy, se kterými se můžou pracovníci setkat, například s nutností vyměnit sítě před použitím místní sítě. [28]

Typy Split tunneling

Split tunneling založený na URL – Umožňuje vybrat konkrétní URL adresy, které se budou šifrovat a přeposílat přes VPN server a zbytek provozu bude putovat přes internet. Některé adresy URL by měly být před veřejností zašifrovány, například přihlašovací formuláře nebo databáze, které by mohly být potenciálně odhaleny. Tento proces lze provést pomocí rozšíření prohlížeče VPN.

Split tunneling založený na aplikacích – Podobně jako u rozděleného tunelování založeného na URL se určí, které aplikace budou směrovány skrz VPN tunel. Tyto funkce je vhodné použít při používaní aplikací, které mají přístup k vysoce citlivým datům.

Inverzní Split tunneling – Inverzní Split tunneling přiřadí veškerou komunikaci přes šifrovaný tunel a umožňuje vybrat, které aplikace nebo URL adresy budou mít možnost procházet nezabezpečeným tunelem. Tato metoda je z hlediska bezpečnosti nejlepší možnou volbou. Tento proces je podobný Firewallu jako službě, kde se vytváří zásady brány firewall na základě uživatelsky definovaných rolí v místních sítích. [28]

3.3 Bezpečnostní aspekty připojení

Bezpečnost je stěžejní část vzdáleného připojení. Důraz na různé prvky v bezpečnosti a jejich správa a aktualizování jsou v dnešní digitální době nejdůležitější částí správy podniků. Jednotlivé prvky bezpečnosti jsou v globální sféře testovány útočníky, kteří se je snaží prolomit a získat přístup k citlivým údajům v podnicích. Vzhledem ke zvyšování důmyslnosti útočníků se také zvyšuje důraz na stále se vyvíjející bezpečnostní principy.

3.3.1 Typy VPN protokolů

Pro VPN služby existuje několik protokolů, které mají různé úrovně zabezpečení. Skládají se z přenosových protokolů a šifrovaných standardů, které poskytují efektivní a bezpečný přenos dat. Míra zabezpečení záleží na jednotlivých typech používaných protokolů.

PPTP protokol

Jeden z nejstarších VPN protokolů je **Point-to-Point Tunneling Protocol (PPTP)**, který byl vytvořen firmami Microsoft a Ascend v roce 1999 a stále se používá ve všech verzích systému Windows od Windows 95. PPTP je stále podporovaný většinou zařízení (Windows, Unix, Android a částečně i iOS), díky vysoké rychlosti přenášených dat, rozšířeností a jednoduchostí protokolu. Rychlost může dosahovat od 70 do 100 Mbps.

Z pohledu bezpečnosti je tento protokol považován za zásadně zastaralý a zranitelný, protože síla bezpečnosti přímo závisí na síle zvoleného ověřovacího mechanismu. Zranitelné (slabé) heslo tedy vede ke zvýšení rizika nezabezpečeného připojení k VPN. Většina PPTP používá MS-CHAPv2 protokol k šifrování hesel, ale dle [29] byl tento protokol před řadou let prolomen a nadále se nepovažuje za bezpečný.

Další možností zabezpečení PPTP protokolu je využití X.509 certifikace pro tento protokol, který se vyznačuje vyšší bezpečností, než má MS-CHAPv2, ale ne všichni klienti podporují EAP-TLS, který je nutný pro X.509 certifikaci. [30]

Fungování PPTP – PPTP pracuje na principu klient – server na 2 vrstvě modelu OSI (linková vrstva). PPTP pracuje na základě vytvoření Point-to-Point relace. Využívá 2 kanály: kontrolní kanál pro nastavení spojení a kanál pro přenos dat. Kontrolní kanál je realizován přes PCT port 1723 [10]. Přenosový kanál využívá Generic Routing Encapsulation (GRE) pro zapouzdření dat. GRE je protokol ze skupiny TCP/IP s IP protokolem 47, určený pro zapouzdření paketů jednoho protokolu do jiného protokolu. [31]

L2TP Protokol

L2TP protokol byl vyvinut ve spolupráci společností Cisco a Microsoft, pro poskytování fyzického a logického tunelování. Principem fungování L2TP protokolu je vytvoření virtuální cesty přes různá připojení a vytvoření efektu, kdy síť tvoří fyzický tunel mezi uzly sítě. L2TP je podobný Data Link Layer Protocol v referenčním OSI modelu, protože propojuje fyzická zařízení, jako by byla ve stejné místní síti. Rozdíl je však ve využívání autentizace.

Hlavní výhodou L2TP je rychlost a efektivnost, kterou poskytuje zejména díky používání UDP komunikace. L2TP poskytuje bezpečný, spolehlivý, škálovatelný, rychlý a flexibilní tunel, s velmi dobrou autorizační politikou pro ověřování uživatelů ve službě VPN, nicméně L2TP neposkytuje šifrování ani ochranu provozu, kterým prochází. Zabezpečený přístup k sítím vzniká až se spojením s IPsec (IP Security) protokolem. Společně se označuje jako L2TP/IPsec protokol a je navržen tak, aby specifikoval zabezpečení mezi komunikačními kanály dvou zařízení, jako jsou počítače, brány, směrovače a firewally. Spojením s IPSec protokolem se ale přidává celková velikost IP packetu o IPSec šifrování.

Pro vzdálený přístup je L2TP vhodnější než jiné protokoly typu point-to-point. Zásluhou použití IPsec protokolu podporuje IP protokoly. Dále podporuje více

tunelů, je kompatibilní s překladem síťových adres (NAT). L2TP řídí provoz mechanismem řízení toku, který řeší přetížení a udržuje režii na minimu. [32]

IPSec protokol

IPsec je skupina protokolů, které se používají společně k nastavení šifrovaného připojení mezi zařízeními. Pomáhá zabezpečit data odesílaná přes veřejné sítě. IP Security (IPSec) je oficiální standart pro bezpečnost v protokolu IP, který zajišťuje IEEE/IETF. Je zaznamenán jako norma RFC2411. IPSec byl původně vytvořen pro IPv6, poté byl implementován i do IPv4. IPSec pracuje na druhé a třetí vrstvě ISO/OSI modelu. V základně IPSec zabezpečuje data už na síťové vrstvě. Zabezpečení na vyšších vrstvách ISO/OSI modelu vyžaduje podporu v IPSec. [30]

IPSec využívá kryptografické bezpečnostní služby pro ochranu komunikace prostřednictvím IP protokolu. Je velice flexibilní a silný, ale také velmi složitý ke konfiguraci a zjištění problémů. Bezpečnostní politika umožňuje šifrovat přenos na základě mnoha parametrů, jako jsou zdrojová a cílová IP adresa, nebo zdrojový a cílový TCP nebo UDP port.

IPSec může být konfigurován s použitím předem-sdílenými klíči nebo X.509 certifikací pro vytvoření bezpečného VPN připojení. [30]

IPSec má dva režimy provozu:

V transportním režimu je každý packet šifrován, ale hlavička IP packetu zůstává stejná. Zprostředkující směrovače vědí o místě určení packetu, pokud není použitý tunelovací režim. [33]

Tunelovací režim se používá mezi dvěma vyhrazenými směrovači, přičemž každý z nich funguje jako jeden konec virtuálního tunelu. V režimu tunelu se kromě packetu také šifruje záhlaví IP packetu, které obsahuje místo určení. Poté je zapouzdřen do nového paketu IP s novou hlavičkou IP. [33] [34]

IPSec využívá, podobně jako PPTP, dva kanály. Kontrolní kanál pro nastavení spojení a kanál pro přenos dat. Kontrolní kanál je realizován přes UPD protokol, na

portu 500 nebo 4500. Kanál pro přenos dat Encapsulating Security Payload (ESP) protokol, což je protokol, který poskytuje packetům šifrování, autentizaci a kontrolu integrity dat, ale hlavička zůstává nešifrovaná [35]. Integrita IPSec packetů je zajištěna pomocí Hash-based Message Authentication Code (HMAC), což je stejný způsob, jaký využívá OpenVPN. [30]

Protokol AH (Authentication Header) zajišťuje integritu dat v hlavičce packetu pomocí kontrolního součtu, jako třeba MD5. Dále zajišťuje autentizaci odesílatele a příjemce, a zabraňuje zpětnému odesílání. Hlavní účel AH spočívá v šifrování hlavičky v packetu. Zbytek packetu zůstává nezakódovaný. [36]

VPN umožňuje Sloučení AH a ESP. Sloučením těchto protokolů se získá celý chráněný IP datagram. [37]

Mezi největší nevýhody IPSec je, že do protokolu bylo přidáno mnoho rozšíření, díky kterému je obtížné připojit koncové body od různých prodejců. [30]

SSL Protokol

V současnosti nejvíce používaný protokol pro VPN jsou VPN založená na Secure Sockets Layer (SSL), který je založený na SSL/TLS (Transport Layer Security) protokolu. SSL protokol je přidaná vrstva mezi transportní a aplikační vrstvu OSI modelu, která poskytuje šifrovanou komunikaci a autentizaci mezi zařízeními v síti [17]. VPN založená na SSL protokolu využívají stejnou síť jako zabezpečená stránka HTTPS. Mají stejný protokol a kanál (TCP protokol a port 443). [38]

Ve většině případů je bezpečné připojení realizováno použitím X.509 certifikátu, který používá jednorázové heslo nebo přihlašovací jméno / heslo pro autorizované připojení.

VPN založená na SSL jsou často nazývaná VPN bez klienta nebo webové VPN. U SSL protokolů je také možné, že s přidáním pluginu pro prohlížeče, nebo přidáním

frameworku ActiveX, jak to dělají někteří výrobci, se protokol stane neschopným spolupracovat s nepodporovanými prohlížeči, či operačními systémy. [30]

SSL se nejčastěji využívá u internetových obchodů, které přijímají platební karty, nebo webové stránky s citlivými údaji. [39]

OpenVPN protokol

OpenVPN je open source software (volně dostupným zdrojovým kódem), který je tvořen spojením SSL/TLS protokolu pro navázání bezpečného spojení spolu s šifrováním HMAC a hashovacím algoritmem pro zajištění integrity u dodání packetů. Ověřování konfigurace spojení může být realizováno pomocí předem sdílených klíčů (pre-shared keys), nebo digitálních certifikátů, jako je certifikát X.509. Touto kombinací se liší od předchozích protokolů založených na SSL protokolech [30]. OpenVPN na rozdíl od jiných VPN protokolů používá virtuální síťový adaptér (TUN/TAP device), jako interface mezi uživatelským a operačním systémem. Obecně, na každém zařízení, které podporuje TUN/TAP, lze spustit OpenVPN. To zahrnuje Windows, Linux, Mac OS, iOS, Android, a další. Pro spuštění na podporovaných platformách je potřeba instalace klienta. [40]

Protokol OpenVPN není standardizován žádnou společností ani organizací, je veřejně dostupný open-source licencí. To z OpenVPN dělá velmi bezpečný protokol, díky neustálému dohledu lidí. Také vytváří prostor pro neustálou bezpečnost protokolu a snížení možnosti pro vytvoření zadních vrátek na obejití běžné autentizace.

OpenVPN, obdobně jako jiné VPN protokoly, používá kontrolní kanál a kanál pro přenos dat. Oba kanály jsou šifrovány a zvlášť zabezpečeny. Jedna z největších výhod OpenVPN jsou velké možnosti konfigurace a také nabídka zvolení rovnováhy mezi rychlostí a bezpečností. OpenVPN nabízí možnost využití jak TCP, tak UDP portů. TCP port je pro větší bezpečnost, zatímco UDP je rychlejší a nabízí třeba živé vysílání. Kontrolní kanál je zabezpečen pomocí SSL/TLS protokolu, a kanál pro

přenos dat je zabezpečen pomocí vlastního šifrovacího protokolu, který je buď předem definován, nebo nastaven uživatelem.

Ve výchozím nastavení se u OpenVPN používá UPD protokol s portem 1194. Ve dřívějších verzích se může vyskytovat port 5000. [30]

3.3.2 AAA protokol

AAA protokol znamená authentication, authorization and accounting protocol, česky autentizační, autorizační a účtovací protokol. AAA protokol byl vyvinut Internet Engineering Task Force (IETF) v roce 1998 pro potřeby autentizace, autorizace a účetnictví pro přístup k síti. Cílem bylo vytvořit protokol, který by podporoval různé druhy přístupů k síti, včetně Network Access Server (NAS), Mobile-IP a roamingu (ROAMOPS). Základním fungováním protokolu je zabránit neoprávněným uživatelům přístup k síti a kontrolovat, případně analyzovat oprávněné uživatele.

Mezi klíčové vlastnosti AAA protokolu jsou vysoká míra bezpečnosti (díky distribuovanému modelu klient/server), ověřené transakce, flexibilní autentizační mechanismy a rozšiřitelné protokoly. Distribuovaný model odděluje ověřování od přenosu dat. Pomocí toho umožňuje ukládat informace o ověřování uživatelů do jediné centralizované databáze. [41]

Informace o uživateli se předávají na AAA server, který vrací odpověď, podle které jednají. Servery přijímají požadavky na připojení uživatele do sítě, ověřují uživatele a vracejí klientské stanici odpověď s potřebnými konfiguračními informacemi k poskytování služeb. Vrácené informace mohou zahrnovat parametry přenosu, protokolu, nebo dodatečné požadavky na autentizaci. Sdílení mezi klientem a uživatelem jsou ověřována a citlivé informace jsou šifrovány pomocí sdíleného tajného klíče. [42]

Autentizace je krok k ověření uživatele pomocí autorizované autority. Autentizačním krokem se potvrzuje, že uživatel, přistupující do sítě je platným uživatelem poskytovaných služeb. Autentizace může být rozdělena do třech typů:

- autentizace důkazem znalostí – uživatel prokáže svou identitu znalostí, např. správným heslem nebo PIN kódem
- autentizace důkazem vlastnictví – uživatel se prokáže pomocí vlastněného předmětu, jako je čipová karta nebo UBS disk
- autentizace důkazem vlastností – uživatel prokáže identitu pomocí své vlastnosti, např. sken oční sítnice nebo otisk prstu

Autorizace znamená přidělení přístupových práv ověřovanému uživateli, který splnil podmínky autentizace. Určuje, co mohou a nemohou uživatelé po své autentizaci dělat [43]. Autorizace může znamenat omezení, které omezuje uživatele. Omezení se můžou týkat například přihlášení pouze v dané hodině nebo přihlášení pouze z určitého místa.

Účtování znamená sběr provozních informací o autorizovaném uživateli, jako například data o přeneseném množství dat, času připojení a odpojení k síti a údaje o přístupovém bodu, přes který byl uživatel přihlášen do sítě. Sledované údaje mohou být využity pro optimalizaci, správu, nebo bezpečností analýzu sítě. [43]

RADIUS

Protokol RADIUS (Remote Authentication Dial In User Service) je protokol, který poskytuje služby centralizované autentizace, autorizace, účtování a správy IP uživatelům vzdáleného přístupu na dané síti mezi přístupovým serverem (RADIUS klient) a autorizačním RADIUS serverem. Model klient/server byl vytvořen jako open-source s možností rozšiřitelnosti pro snadné přizpůsobení protokolu pro práci s produkty třetích stran.

RADIUS server reaguje na požadavky uživatelů tím, že ověří uživatele a poté vrací konfigurační informace serveru, který pak může autentizovaným uživatelům poskytnout předem definované služby.

V případě, kdy se RADIUS server stává nedosažitelným, může systém směrovat požadavky na alternativní server. Tak je možné fungovat s jedním přihlašovacím ID v rámci celého podniku, nikoli jediné firemní budovy, a nerozhoduje se o jaký přístupový bod se jedná. [45]

Základní implementace RADIUS serveru má dva konfigurační soubory. Konfigurační soubor klienta obsahuje klientovu adresu a sdílený tajný klíč, který používá k ověření transakcí. Uživatelský soubor obsahuje uživatelskou identifikaci a autentizační informace (například ID uživatele a heslo) a také parametry připojení a autorizace. [41] [42]

Packet RADIUS využívá protokol UDP s portem 1812. Parametry jsou předávány mezi klientem a serverem bez řízení přenosu. Spojení mezi RADIUS klientem a serverem je šifrováno sdíleným tajemstvím pomocí hashovacího algoritmu MD5, který posílá všechna uživatelská hesla přes síť v šifrované podobě. Zamezuje se tím zjištění hesla na síti pomocí odposlouchávání sítě, ale další parametry (uživatelské jméno, autorizace a účetnictví) posílá v prosté textové podobě [46]. Formát protokolu umožňuje zpracovávat velké objemy požadavků, ale také nezaručuje příjem dat ani jejich úplnost, zvláště při velkých datových zátěžích u opakovaných přenosů nebo u nedosažitelných uzlů. [42]

TACACS+

TACACS+ je rozšířeným systémem TACACS (Terminal Access Controller Access-Control System), který oproti TACACS podporuje všechny části architektury AAA. TACACS byl původně vyvinutý jako protokol pro komunikaci s autentizačním serverem. Měl omezenou funkčnost a používal přenos UDP. Pozdější verze, označována jako XTACACS (Extended TACACS) obsahovala rozšiřující funkce a byla zpětně kompatibilní s původním TACACS.

TACACS+ byl vyvinut společností Cisco pro jejich architekturu AAA, ale jejich verze TACACS+ nemá mnoho společného s původní verzí a nejsou zpětně kompatibilní. Největším vylepšením je oddělení autentizace, autorizace a účetnictví a přidání šifrování do všech přenosů z AAA serveru. Komunikace probíhá přes TCP na portu 49. TACACS+ musí mít implementované řízení přenosu. Může tak detekovat chyby přenosu, jako ztráty packetů, časový limit a další. Cisco vylepšilo rozšiřitelnost protokolu, které poskytuje více typů autentizačních požadavků a povolení libovolné délky posílaných dat.

TACACS+ servery používají jeden konfigurační soubor k nastavování možností serveru, definování uživatelů, řízení akcí autentizace a autorizace, a nastavování atribut/hodnota (AV – attribute/value). Dále obsahuje údaje o nastavení provozních parametrů služby, sdílení tajného klíče a názvu účetního souboru. Poslední části v konfiguračním souboru jsou řady definic uživatelů a skupin, které se používají k řízení definovaných akcí a autorizace. Definice uživatelů a skupin jsou ve formátu atribut/hodnota, například „user = novakpa“.

Klient, který zahájí TCP relaci, předá na server skupinu AV párů, který obsahuje standartní formát záhlaví a následuje pole dat s proměnlivou délkou. Záhlaví obsahuje:

- Hlavní verze
- Vedlejší verze
- Typ (autentizace, autorizace nebo účetnictví)
- Číslo sekvence
- Příznaky
- ID relace
- Délka

TACACS+ zajišťuje bezpečné šifrování, zatímco protokol TCP zajišťuje spolehlivé doručení. Nevýhodou je zvyšující se počet komunikací, které mohou mít vliv na výkon služby během velkého zatížení. [41]

3.3.3 Bezpečnost připojení

Kvalita hesla

Zabezpečení pomocí hesel je jedním ze základních zabezpečení systému a jejich kvalita rozhoduje o bezpečnosti těchto systémů. Samotná kvalita hesla závisí na času, potřebném k prolomení hesla. Čím delší čas si prolomení hesla vyžádá, tím se považuje za bezpečnější. Bezpečné heslo by se mělo skládat z minimálně 12 znaků složených z malých a velkých písmen, číslic a speciálních znaků. Jedním ze způsobů měření kvalit hesel je entropie hesla. Entropie je měřítkem nepředvídatelnosti hesla, které je založeno na použité znakové sadě (malá a velká písmena, číslice a speciální symboly) a jeho délce. Entropie hesla předvídá obtížnost prolomení hesla pomocí hádání, útoků hrubou silou (Brute-force attack) nebo slovníkovým útokem [48]. Měří se v bitech a pro jeho výpočet existuje vzorec:

$$E = \log2(R) * L$$

kde E je entropie, R je počet dostupných znakových sad a L je délka hesla. Znakové sady se dělí na malá písmena (26 znaků), velká písmena (26 znaků), číslice (10 znaků), speciální znaky (32 znaků), písmena s háčky (16 znaků) a písmena s dlouhými hlásky (8 znaků). [47]

Tabulka 1 – Přehled síly hesel, Zdroje: Prolomení https://www.passwordmonster.com/ , Entropie - http://rumkin.com/tools/password/passchk.php

Heslo	Prolomení	Entropie	Síla hesla
Adam&Eva	2.74 minut	35.3 bits	Slabé
Adam&Eva@4Ever	2 měsíce	64.3 bits	Silné
Adamek&Evička@4Ever	123 milionů let	115.2 bits	Velmi silné

Správa účtů v podniku

Správa podnikových účtů musí podléhat mnoha zabezpečením, aby se minimalizovala možnost prolomení podnikové ochrany. Jedním ze základních opatření je zavedení centrální správy uživatelských účtů a jejich oprávnění. Nastavení jednotné bezpečnostní politiky je nedílnou součástí kyberbezpečnosti.

Výhodou centrální správy účtů jsou i možnosti nastavení parametrů hesel a kontroly uživatelských účtů a jejich oprávnění.

Správu účtů, oprávnění a zabezpečení mají na starosti administrátoři. Administrátoři jsou zodpovědní za bezpečný a plynulý chod podnikové IT infrastruktury, kterou spravují. Pro správu systému se využívají administrátorské účty, které se vyznačují plným přístupem k systému a možnosti nastavování bezpečnostních politik. Kvůli plnému přístupu k podnikovým systémům administrátorské účty podléhají vyššímu zabezpečení, mezi které patří jiné požadavky na složitost a délku hesla, oddělení administrátorského učtu od účtu pro běžnou práci a případné vynucení vícefaktorové autentizace. [51]

Vícefaktorové ověřování

Ověřování založené pouze na jednom faktoru (např.: uživatelské jméno a heslo) je nespolehlivé, neboť se může stát cílem útoků hrubou silou a jeho prolomení se stává pouze otázkou času. Použití vícefaktorového ověřování znamená větší bezpečnost.

Vícefaktorové ověřování (anglicky Multi-Factor authentication (MFA)) je zabezpečený proces autentizace, který vyžaduje více než jednu autentizační metodu vybranou z na sobě nezávislých faktorů. Mezi hlavní faktory MFA patří: ověření znalostí, ověření vlastnictvím a ověření vlastností. [49]

Mezi ověření znalostí patří:

- Bezpečnostní otázka
- Heslo
- PIN

Mezi ověření vlastnictvím patří:

- Jednorázový kód, dostupný přes mobilní aplikaci nebo email
- Přístupové zařízení, jako přístupová karta, USB zařízení, nebo bezpečnostní klíč
- Softwarový token nebo certifikát

Mezi ověření vlastností patří:

- Otisk prstu, sken oční duhovky, rozpoznání obličeje nebo hlasu
- Analýza chování

Další způsoby ověřování byli začleněny do MFA s využitím strojového učení a umělou inteligencí. Využití těchto technologií zahrnuje:

Ověření na základě polohy – ověřování na základě polohy zjišťuje IP adresu a případně i geografickou polohu přihlašujícího se uživatele. Tyto informace jsou použity pro zablokování přístupu uživatele, který se snaží o připojení mimo firemní prostory, nebo jiná povolená místa.

Adaptivní autentizace nebo autorizace na základě rizika – adaptivní autentizace analyzuje faktory na základě souvislosti a chování při přihlašování. Zodpovídá otázky spojené s úrovní rizika. Například:

- Odkud uživatel přistupuje k informacím?
- Kdy se pokouší dostat k informacím, během normální pracovní doby nebo mimo pracovní dobu?
- Jaké zařízení používá? Je stejné jako obvykle?
- Je připojen skrze soukromou nebo veřejnou datovou síť?

Na základě těchto otázek vyhodnotí adaptivní autentizace úroveň rizika a určí, zda se uživatel může připojit do sítě, nebo vydá příkaz k dalšímu ověření bezpečnostním faktorem.

MFA kombinuje dva či více typů ověřování pro lepší a bezpečnější způsob ověřování uživatelů a zavádí se v případech, kdy je potřeba zajistit ověření identity pro uživatele s přístupem k citlivým údajům. Přihlašovací údaje uživatele musí pocházet alespoň ze dvou, či více různých kategorií nebo faktorů. Dvoufaktorová autentizace nebo 2FA je podmnožinou MFA, kde jsou požadovány pouze dva faktory, ale MFA může použít libovolný počet faktorů. Nejběžnějším příkladem se stal bankovní

automat. Pro přístup k účtu musí uživatel vložit kreditní kartu (faktor vlastnictví) a poté musí vložit PIN (faktor znalosti). [50]

3.3.4 Bezpečnostní model Zero Trust

Zero Trust (Bezpečnostní model nulové důvěry) znamená, že síť ověřuje každou žádost o přístup k podnikovým zdrojům a umístí ji do virtuální zabezpečené oblasti, ve které mají uživatelé či zařízení přístup pouze ke zdrojům, které skutečně potřebují. Bezpečnostní model Zero Trust představuje přístup zaměřený hlavně na data a identity. Odstraněním ověřeného uživatele ve výchozím stavu nedůvěřuje uživatelům zvenčí ani zevnitř sítě a je vyžadováno ověření od každého uživatele, který se snaží získat přístup ke zdrojům v síti. Před udělením přístupu musí být veškeré údaje vždy ověřené. Se Zero Trust zavádí bezpečnostní tým zásady pro ověření každého pokusu o připojení, a pro inteligentní omezení přístupu. Přístup nulové důvěry zajišťuje, že centralizovaný datový trezor je vždy chráněn, a to i v případě ohrožení od vzdáleného uživatele. [52]

Zero Trust (ZT) se od VPN odlišuje hlavně tím, že odstraňuje koncept ověřeného uživatele. Standardní zabezpečení sítě důvěřuje ověřenému uživateli, tudíž ve vnitřní síti nedochází k dalším kontrolám. Tento způsob může vést ke zranitelnosti v oblasti bezpečnosti, zvláště pokud podniky nemají data uložena pouze na jednom místě, ale disponují rozlehlou sítí, jejíž kontrola bezpečnosti může být komplikovaná [52]. Data uložená v dnešním digitálním, cloudovém, distribuovaném a mobilním pracovním prostředí, mohou být neustále v ohrožení. Zero Trust kombinuje zabezpečení na hardwarové i softwarové úrovni spolu s využitím propracovaných nástrojů pro sběr dat a jejich následnou analýzou. [54]
Použití Zero Trust může zajistit:

- Zabránění šíření hrozeb mezi zařízeními či aplikací pomocí segmentace sítě (lateral movement)
- Ochranu před krádeží identity (context-aware security)
- Chránit zařízení před hrozbami a v případě ohrožení je izolovat

- Klasifikovat a šifrovat všechna podniková data
- Detekovat a zmírňovat hrozby a bezpečnostní rizika
- Využívaní nástrojů pro automatizaci bezpečnostních úkolů a reakcí na incidenty

Hlavní principy nulové důvěry

Mikrosegmentace – Mikrosegmentace je v praxi rozdělování sítě do malých zón, tak aby byl zachován samostatný přístup pro jednotlivé části sítě. Jmenovitě, myšlenkou je rozdělit a ovládat sítě budováním mikroobvodů kolem cenných aktiv. Osoba nebo program s přístupem do jedné z těchto zón nebude mít přístup k žádné z ostatních zón bez samostatného oprávnění. Například síť se soubory žijícími v jediném datovém centru, které využívá mikrosegmentaci, může obsahovat desítky samostatných zabezpečených zón.

Explicitní ověřování – Princip Zero Trust předpokládá, že v síti i mimo ni jsou útočníci, takže všem uživatelům a zařízením automaticky nedůvěřuje. Identita a oprávnění uživatele i zařízení jsou periodicky ověřovány a jejich připojení se po uplynulé době skončí, což nutí uživatele a zařízení k neustálému opakování ověřování. Ověřování a autorizace se provádí na základě dostupných datových bodů, které zahrnují uživatelskou identitu, geografickou polohu, zabezpečení a stav zařízení nebo různé anomálie v chování uživatelů.

Nejmenší výsada – Přístup uživatelů je omezený nejnižšími oprávněními. Uživatelům se poskytne pouze takový přístup, který potřebují. Tento způsob maximalizuje ochranu dat. Implementace nejmenší výsady vyžaduje pečlivou správu uživatelských oprávnění.

Ochrana Zařízení – Cíle útočníků jsou různé a rozmanité, překračují sítě a pracovní stanice a stále více zahrnují mobilní zařízení (z nichž většina je v osobním vlastnictví), zařízení s podporou internetu věcí (IoT) a operačních technologií (OT). IoT a OT jsou zařízení, která jsou zvláště zranitelná. Obvykle jsou připojena k

podnikovým sítím a běží na nespravovaném systému bez dostatečných přídavných zabezpečení.

Ochrana dat – Síťová struktura podniků je složitá a může obsahovat bezpečnostní rizika. Ochrana dat je náročná, protože jsou neustále sdílena mezi pracovními stanicemi, mobilními zařízeními, aplikačními servery, databázemi, aplikacemi SaaS a napříč podnikovými a veřejnými sítěmi. Přístup k zabezpečení dat s nulovou důvěrou je nutností a vyžaduje kombinaci šifrování dat, klasifikace a ochrany všech dat, která jsou buď uložená na serverech, při jejich přenosu nebo při používání.

Zabezpečení pracovní zátěže rozšířenou viditelností a zásady – Zabezpečení pracovní zátěže, aplikací a programů, které jsou zranitelné, kvůli dynamickému prostření v interní sítí, či v cloudu, je klíčové pro bezpečnost provozu v síti. Důležité je mít úplný přehled o provozu, pro posouzení stavu zabezpečení, odhalení nesprávné konfigurace a bezpečnostních mezer a prosazovat přizpůsobené zásady. Toho lze ale docílit neustálým monitorováním, protokolováním a analyzováním všech aktivit v síti. Tímto způsobem mohou být rychle detekovány hrozby a zmírněny ztráty. [53]

Zero Trust Network Access

Zero Trust Network Access (ZTNA) je kategorie technologií, které organizacím umožňují implementaci modelu Zero Trust. Umožňují vzdálený přístup k aplikacím a službám na základě definovaných zásad řízení přístupu. ZTNA skrývá většinu infrastruktury a služeb a nastavuje individuální šifrované spojení mezi zařízeními a zdroji, které potřebují, a připojená zařízení si neuvědomují žádné jiné zdroje než ty, ke který jsou připojeny. [55]

ZTNA typicky fungují na aplikační vrstvě ISO/OSI síťového modelu. Pro připojení k síti skrze VPN službu je nutná instalace softwaru na všechny koncové body. V ZTNA může být stejná konfigurace, ale není ji nutné používat vždy. Častější případ pro využití ZTNA, spíše než připojení do podnikové datové sítě, je připojení do cloudu, které umožňuje navázat spojení bez dopadu na výkon interní sítě. ZTNA nastavuje

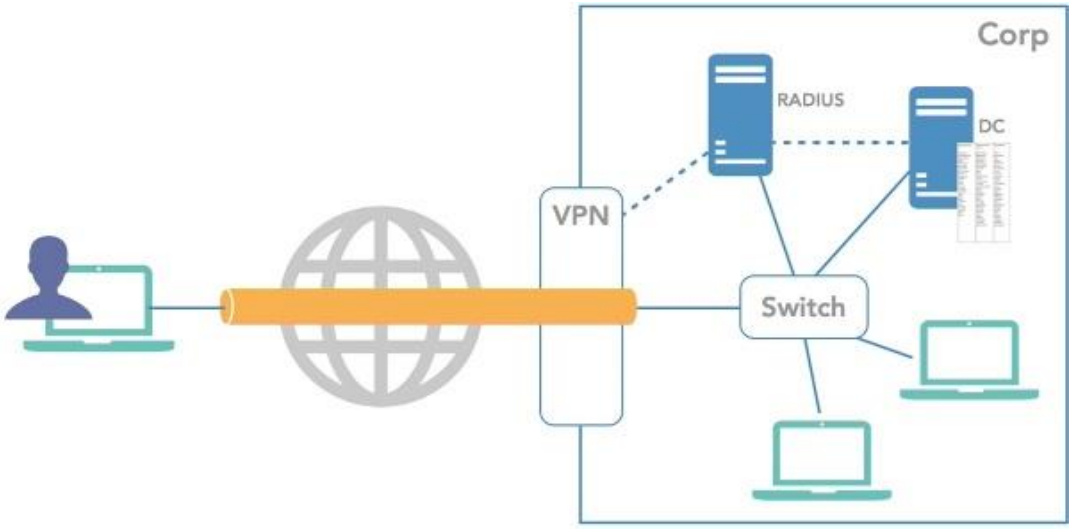
individuální šifrovaná spojení mezi zařízením uživatele a danou aplikací nebo serverem pouze ke konkrétním datům. [56]

3.4 Návrh implementace připojení

3.4.1 Vytvoření VPN přístupového bodu do vnitřní sítě

Cílem implementační části je vytvořit modelovou situaci pro komunikaci mezi zařízeními mimo vnitřní síť prostřednictvím služby VPN. Komunikace skrze internet je běžná záležitost. Pro připojení z veřejného internetu do vnitřní sítě se kvůli bezpečnosti musí uvažovat o přidání bezpečnostního prvku. Prostřednictvím VPN se zařízení připojující do vnitřní sítě připojí skrze internet šifrovaným tunelem, který zajistí bezpečnost pro posílaná data. Připojení do vnitřní sítě bude probíhat skrze ověření NAS (Network Access Server – server pro přístup k sítí), který tvoří RADIUS server, a je členem podnikové domény.

Z logického pohledu se jedná o model:



Obrázek 1 Návrh řešené situace, zdroj: https://www.linkedin.com/learning/windows-server-2016-remote-access-solutions/installing-and-configuring-radius

3.4.2 Použitá zařízení

Mikrotik RB493G

Mikrotik RB493G je síťový prvek od společnosti Mikrotik, který bude realizovat spojení mezi zařízením připojeným k internetu a vnitřní sítí, ke které se bude připojovat. Zařízení RB493G má devět gigabitových ethernetových portů, tři miniPCI sloty a dva přepínací čipy, a ethernetové porty lze propojit dohromady ve dvou skupinách přepínačů pro přenosovou rychlost.

RB493G má také port USB 2.0 a slot pro kartu microSD pro přidání další paměti nebo 3G USB modem pro záložní konektivitu.

Operační systém tvoří RouterOS ve verzi 6.28 od společnosti Mikrotik, který je vybaven vysoce výkonným procesor Atheros AR7161 a k dispozici má 256 MB vestavěnou paměť RAM. RouterOS umožňuje ze zařízení RB493G vytvořit, podle potřeb, výkonný router, switch nebo bridge. [1]

Windows Server 2016 Standart Edition

Windows Server 2016 je serverový operační systém vytvořený společností Microsoft pro realizaci služeb klientům v modelu klient – server. Jednou z nabízených služeb je autentizace a autorizace přístupu, která v případě nasazení se službou Active Directory (AD) znamená možnost využití SSO (Single Sing-On), tedy možnost AAA v rámci vzdáleného přístupu. Služba NPS (Network Policy Server) umožňuje konfiguraci vzdáleného ověřování pomocí protokolu RADIUS vytvořením ověřovacího serveru.

[1] Dokumentace Mikrotik Router RB493G https://mikrotik.com/product/RB493G#fndtn-specifications.

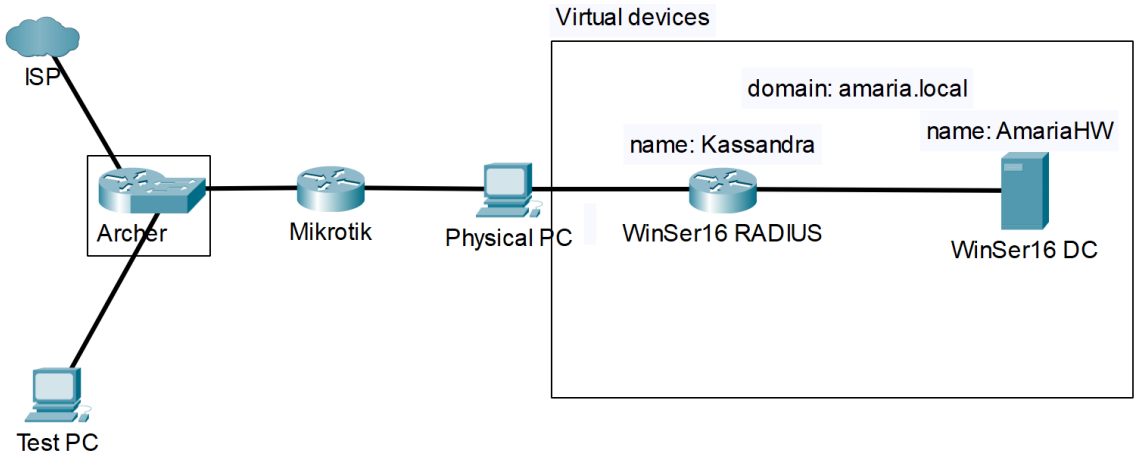
4 Návrh a realizace vzdáleného připojení

Cílem práce je vytvořit bezpečné VPN spojení mezí podnikovou (interní) sítí a zařízením mimo tuto síť. Pro tuto část práce se předpokládá, s využitím vnitřní sítě, do které se připojí Mikrotik, zařízení sloužící jako router s funkcí RADIUS klienta, který bude ověřovat přístupové údaje na RADIUS serveru. RADIUS server představuje virtuální zařízení Windows Server 2016 Standart Edition běžící v programu VMware Workstation 14 Player, připojení do domény na Domain Controller serveru, které je stejným virtuálním zařízením jako RADIUS server.

4.1 Příprava konfigurace

Připojení do zkušební domény bude probíhat z testovacího počítače, který vytvoří VPN tunel na zařízení MikroTik, který se dotáže RADIUS serveru na ověření přístupových údajů zadané ve zkušebním počítači. RADIUS serveru tyto údaje ověří na Domain Controller serveru v adresářové službě běžící na serveru a odpoví MikroTik zařízení.

Z fyzického pohledu se jedná o model:

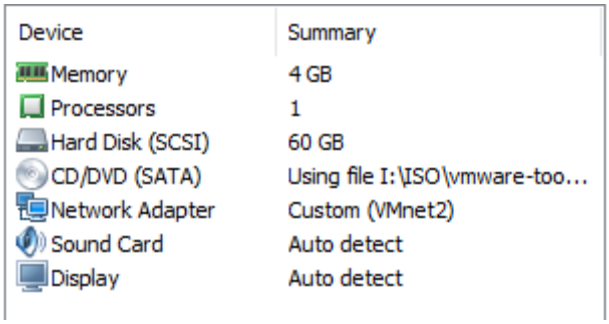


Obrázek 2 Fyzické rozložení zařízení, zdroj: vlastní

4.2 Konfigurace Domain Controller serveru

4.2.1 Základní konfigurace

Jako Domain Controller server slouží Windows Server 2016 Standart Edition ve virtuálním programu VMware Workstation. Server je síťově napojen na specifickou virtuální síť VMnet2.



Obrázek 3 Hardwarové nastavení virtuálního zařízení, zdroj: vlastní

Po nainstalování operačního systému a vytvoření administrátorského účtu s heslem „FimUhkSakac23“ proběhla aktivace dočasné licence a změna výchozího anglického jazyka na češtinu. Server získal jméno AmariaHW a byla mu přidělena statická IP adresa 172.16.0.1 s prefixem /24. Následně proběhlo stahování a instalace potřebných služeb, konkrétně šlo o:

- Active Directory Domain Services (AD DS)
- Domain Name Services (DNS)
- Distributed File System (DFS Namespace)

4.2.2 Active Directory Domain Services (AD DS)

Active Directory Domain Services (AD DS) jsou základní funkce služby Active Directory. Umožňují spravovat jednotlivé uživatele a počítače i zároveň organizovat data do logických hierarchií. Služba AD DS může poskytovat například bezpečnostní certifikáty, správu dat a jednotné přihlášení do služeb SSO (Single Sign-On). [57]

Server AmariaHW byl povýšen na řadič domény **amaria.local**, a tuto doménu rovněž spravuje. Heslo do domény bylo nastaveno na „Barabora2001“. V „Uživatelé a počítače služby Active Directory“ byli vytvořeny uživatelské profily pro vzdálený přístup uživatelům „sakac“ (Jan Sakač) a „mariska“ (Jan Mariška) se společným heslem „Heslovka1397“. Uživatelé mají v profilech povolený přístup do sítě. Společně s uživatelskými účty byla vytvořena skupina „RADIUSgroup“ sloužící jako oprávnění pro vzdálené uživatele v nastavení typu skupin na „Zabezpečení“. Oběma uživatelům byl přiděl přístup do této skupiny.

4.2.3 Domain Name Services (DNS)

DNS služba se vytvořila společně s AD DS kvůli vzájemné integraci služeb. Služba slouží pro překlad adres na doménová jména a je integrovaná do AD DS.

Pro funkčnost DNS v doméně jsou nastaveny Zóny dopředného a zpětného vyhledávání. V zóně dopředného vyhledávání je nastavena nová primární zóna na doménu **amaria.local**. Zóna zpětného vyhledávání je nastavena na adresy 0.16.172. Do DNS serveru jsou vneseny statické IP adresy obou serverů AmariaHW (172.16.0.1) a Kassandra (172.16.0.2).

4.2.4 Distributed File System (DFS Namespace)

DFS Namespace je služba, která umožňuje seskupovat sdílené složky umístěné na různých fyzických serverech do jednoho nebo více logických názvů a poskytnout jednotný virtuální pohled na sdílené složky.

Tato služba bude poskytovat sdílené soubory pro vzdálené uživatele a bude sloužit jako kontrola funkčnosti VPN služby. Sdílené složky byly vytvořeny dvě – „Veřejné“, ke které mají přístup všichni uživatelé v doméně a „Vzdálení pracovníci“, kam můžou uživatelé s oprávněním „RADIUSgroup“.

4.3 Konfigurace RADIUS serveru

4.3.1 Základní konfigurace

Základní konfigurace na RADIUS serveru proběhla stejně jako konfigurace Domain Controller (DC) serveru. Rozdíl je ve dvou síťových kartách, kdy jedna je ve VMware Player nastavena na Bridge (kopíruje síťové rozhraní fyzického počítače) a druhá je nastavená stejně jako DC serveru (VMnet2), a službách, který RADIUS server poskytuje:

- Network Policy Server (NPSA)

RADIUS server získal jméno Kassandra, a byl přidělen do domény **amaria.local** pro komunikace s DC serverem.

4.3.2 Network Policy Server (NPS)

NPS umožňuje vytvářet a vynucovat zásady přístupu k síti, ověřování a autorizaci v celé podnikové doméně. Server NPS může také sloužit jako proxy server RADIUS pro předávání požadavků na připojení vzdáleného serveru, aby se mohly načíst požadavky na vytváření připojení a předávat je do domény k ověření a autorizaci.

Po instalaci NPS byl server registrován v adresáři Active Directory a vytvořen nový RADIUS klient s odkazem na Mikrotik zařízení na IP adrese 10.0.0.1 se sdíleným klíčem „sakac-radius-client-22“. Dále je definována „Zásada vyžádání nového připojení“ VPNpolices s podmínkami:

- Typ portu serveru NAS – Virtual (VPN)
- Identifikátor serveru NAS – **amaria.local**
- Ověření požadavků tímto serverem

Dále „Zásady sítě“ s názvem VPNnetworkPolicies jsou nastavené tak, že udělí přístup tomu, kdo se snaží přistoupit k síti přes Remote Access Server a kdo splňuje následující podmínku, že je členem skupiny RADIUSgroup. Protokol EPA je nastaven na EAP-MSCHAP v2, MS-CHAP v2 a MS-CHAP. Časový limit nečinnosti je nastaven na

maximálně 60 minut, časový limit relace je nastaven na 1440 minut (24 hodin), a šifrování je ve výchozím stavu nastavené na MPPE 40 bitů a MPEE 56 bitů.

4.4 *Konfigurace routeru Mikrotik* RB493G

4.4.1 Základní nastavení

Mikrotik zařízení leží mezi domácím Wi-Fi routerem TP-Link Archer C1200 s přístupem k internetu a fyzickým počítačem, na kterém běží dvě virtuální zařízení. Je zprostředkovatelem internetu pro virtuální zařízení a přístupovým bodem VPN. Rovněž je klientem RADIUS serveru.

Před prvním použitím je důležité smazat předchozí konfiguraci a zařízení vrátit do výchozího nastavení pomocí příkazu:

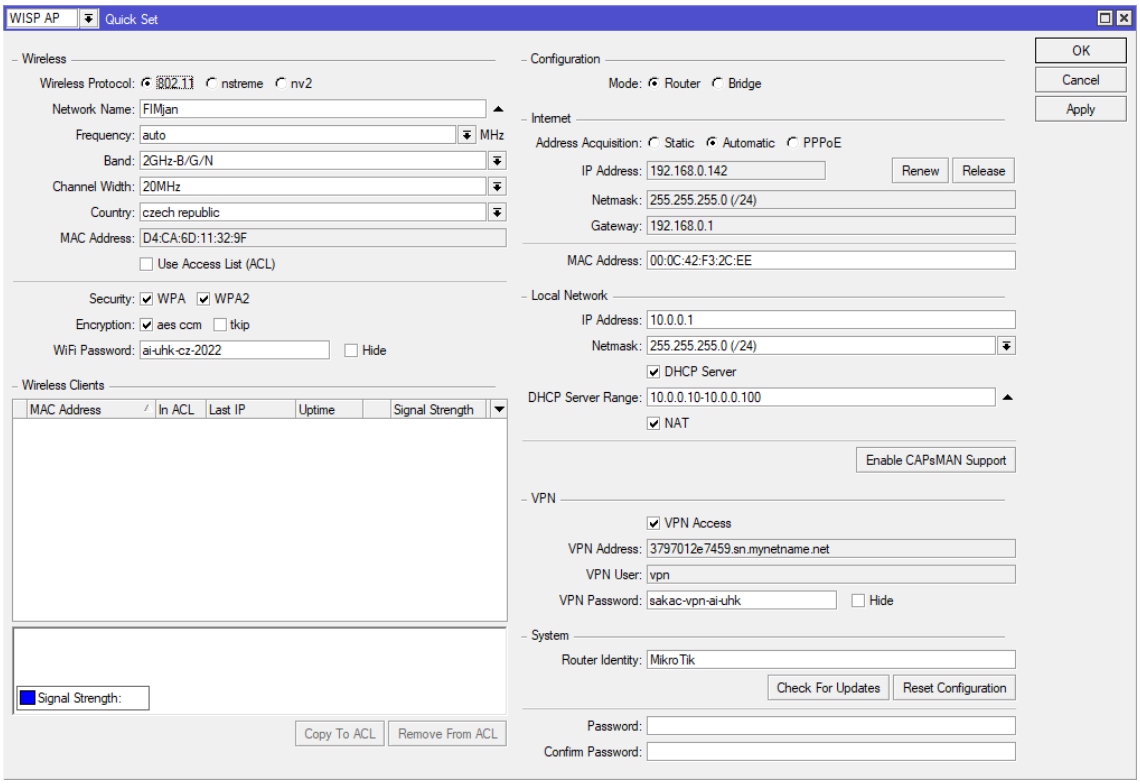
```
[admin@MikroTik] > /system reset-configuration no-defaults=yes skip-backup=yes
```

Obrázek 4 Příkaz na smazání současné konfigurace, zdroj: vlastní

kdy Mikrotik po takto provedeném restartu konfigurace běží v módu router se jménem MikroTik s defaultními nastaveními včetně IP adres. Manuálně je nastaven pro spojení mezi ním a domácím routerem je nastaven na rozhraní ether1 a byla mu definována statická IP adresu 192.168.0.143 s maskou 255.255.255.0 (prefix /24). Pro DNS server a výchozí bránu je nastavena adresa 192.168.0.1 kterou je domácí router. Pro vnitřní rozhraní ether2 až ether9 je nastaven Bridge pro všechny porty, se jménem local, a pro adresaci slouží DHCP server. Adresace na lokání porty je nastavena na IP 10.0.0.1/24 a DHCP server přiděluje adresy v rozmezí 10.0.0.10 – 10.0.0.100. Funkce NAT je povolena pro komunikaci mezi sítěmi. Bezdrátová služba vzhledem ke konfiguraci není potřeba a je zakázaná i přes nastavenou konfiguraci. Pro vzdálenou komunikaci je povolena služba VPN.

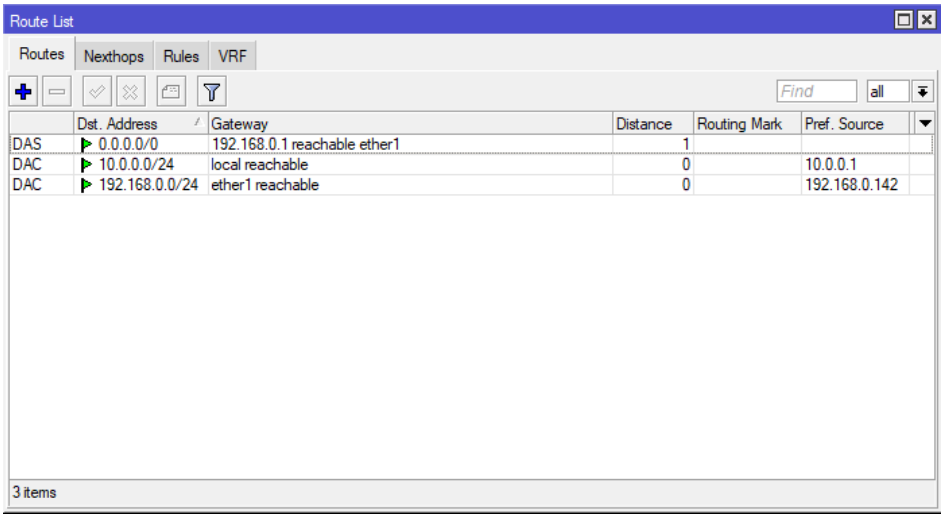
Mikrotik také umožňuje nastavit celou řadu firewallových pravidel na příchozí i odchozí spojení. Nastavením pravidel na připojení je další bezpečnostním vrstvou.

Pro využití v implementační části je možné nastavit například VPN připojení pouze s využitím protokolu L2TP.



Obrázek 5 Základní konfigurace Mikrotik routeru, zdroj: vlastní

Během základního nastavení je vytvořená routovací tabulka na přiloženém obrázku číslo 4 a také byl přidán NTP Client odkazující na domácí router, který bude poskytovat aktuální datum a čas.



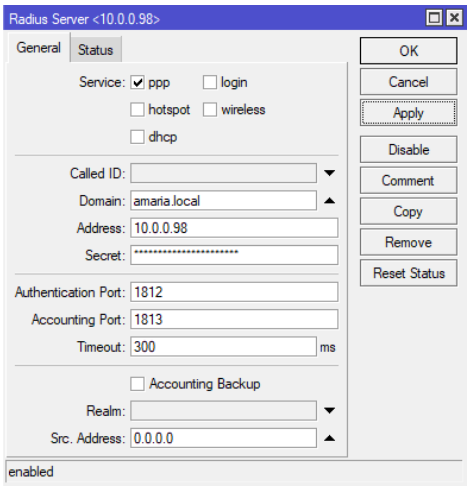
Obrázek 6 Routovací tabulka Mikrotik routeru, zdroj: vlastní

4.4.2 Konfigurace RADIUS klienta

Prvním krokem pro vytvoření RADIUS klienta je definování adres, které se mají přidělovat po autentizaci. Z tohoto důvodu je definován nový rozsah adres 10.0.0.80–10.0.0.89 s názvem „VPNpool“. Tyto adresy budou přidělovány uživatelům, který se připojí přes VPN službu.

Dále je třeba nastavit Point-to-Point Protocol (PPP). Pro využití VPN služby použijeme nový profil s názvem „VPNprofile“, nastavením lokální adresy na 10.0.0.1, vzdálené adresy na „VPNpool“ a server DNS na 10.0.0.98 (adresu zařízení Kassandra). Aktivací L2TP Serveru bude využíván VPN protokol L2TP. Další nastavení serveru zahrnuje nastavení profilu na „VPNprofile“, autentizace proběhne „mschap2“ nebo „mschap1“, a použití IPsec a s heslem „sakac-radius-client-22“ zajistí použití protokolu L2TP/IPsec. L2TP/IPsec protokol je vybrán proto, že je obecně považovaný za bezpečnější oproti například PPP protokolu a je také k dispozici na většině operačních systémech se snadným nastavením. Pro nastavení ověřování RADIUS serveru v části PPP Authentication&Accounting bude použit Radius a Accounting.

Po nastavení pravidel VPN služby je nastaven nový RADIUS server. Server poskytuje službu „ppp“ na adrese 10.0.0.98 (zařízení Kassandra) v doméně **amaria.local**. Heslo je nastavené na „sakac-radius-client-22“ s výchozími porty 1812 pro autentizaci, a 1813 pro účetnictví (Accounting).



Obrázek 7 Nastavení RADIUS serveru, zdroj: vlastní

4.5 Konfigurace VPN připojení ze vzdáleného počítače

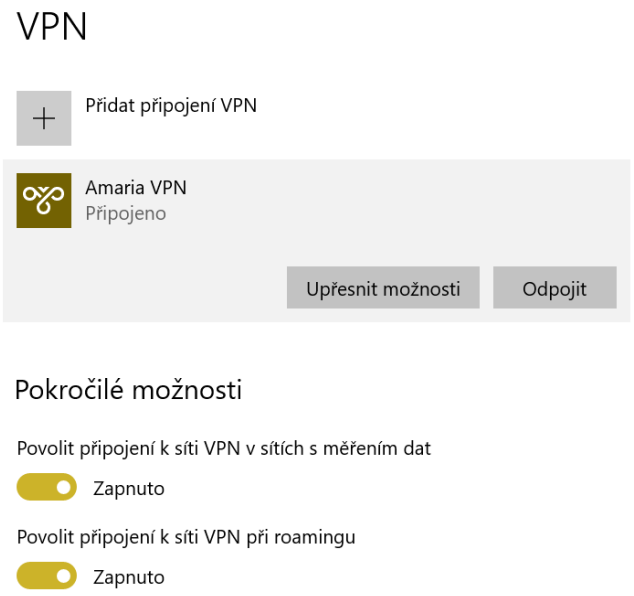
4.5.1 Konfigurace VPN připojení

Pro připojení pomocí služby VPN do doménové sítě **amaria.local** se použije zabudovaný nástroj v operačních systémech Windows 10. VPN připojení je nadefinováno na adresu zařízení Mikrotik se šifrováním L2TP/IPsec s předem definovaným klíčem.

Obrázek 8 Nastavení VPN připojení, zdroj: vlastní

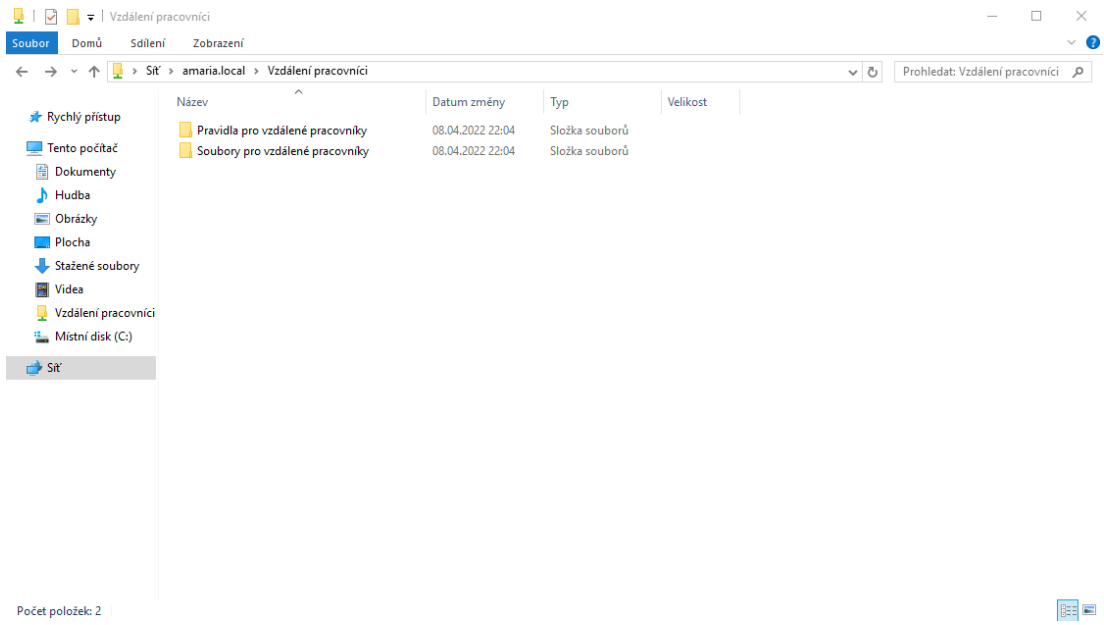
4.5.2 Ověření připojení

Po konfiguraci VPN připojení přichází na řadu připojení do sítě **amaria.local** pomocí zabudované VPN služby v operačních systémech Windows 10.



Obrázek 9 VPN připojení do domény amaria.local, zdroj: vlastní

Po připojení do sítě **amaria.local** z testovacího počítače má uživatel umožněný přístup ke sdíleným složkám služby DFS Namespace. Dle nastavených pravidel skupiny „RADIUSgroup“ se pro vzdálené pracovníky připojí složka s názvem „Vzdálení pracovníci“, kteří mohou tito uživatelé dále pracovat s potřebnými soubory.



Obrázek 10 Přístup ke sdíleným složkám z domény amaria.local, zdroj: vlastní

4.6 Shrnutí výsledků

Pro implementační část byla navržena síťová architektura založená na doméně **amaria.local**, ke které se měl vzdálený uživatel připojit skrze VPN tunel s použitím bezpečného protokolu L2PT/IPSec. Vzdálený uživatel by měl mít po připojení do sítě přístup ke složkám služby DFS.

Hardwarovou část tvořily Mikrotik RB493G spolu s fyzickým a testovacím počítačem. Virtuální zařízení tvořila dvojice serverů spuštěná v programu VMware na fyzickém počítači. Jeden ze serverů (AmariaHW) se stal Domain Controller serverem a druhý (Kassandra) se stal RADIUS serverem pro ověřování připojovaných klientů. Společně servery poskytují vzdáleným uživatelům přístup do vnitřní sítě **amaria.local**.

Po realizaci připojení a konfiguraci všech zařízení podle „Návrhu a realizace připojení“ se úspěšně naváže spojení mezi vnitřní sítí a vnějším zařízením. VPN klient spustí proces ověřování, kde se Mikrotik zařízení dotáže RADIUS serveru na autentizaci přihlašovacích údajů. RADIUS server se na pravost údajů následně dotáže Domain Controller serveru, který odpoví kladně, či záporně. Výsledek procesu putuje zpět k VPN klientovi, který se na základě odpovědi serveru bude připojen do vnitřní sítě, nebo bude připojení odmítnuto na základě chybných údajů. Implementovaný způsob řešení je vhodný zejména pro střední až velké podniky, které mají finanční prostředky pro realizaci takové implementace.

Během konfigurace nastával problém při ověřování RADIUS serverem. Ve zdrojích dokumentace je uvedena chybná aktualizace od společnosti Microsoft, která znemožňovala připojení VPN k cílovému serveru pro protokoly L2TP a IPSec IKE. Řešením se stal až nově instalovaný operační systém Windows 10 Home ve starší verzi na testovacím počítači ve virtuálním prostředí VMware. Počítač bez nainstalované aktualizace se bez potíží připojil do vnitřní sítě.

5 Závěry a doporučení

Podniky již delší dobu umožňují svým zaměstnancům pracovat vzdáleně, ale doba COVID-19 tento trend výrazně umocnila. Zaměstnanci firem se během pandemie potýkali s novou pracovní formou, která byla záhy vystavena nebezpečí z řad útočníků. Ochrana dat pro uživatele v této nové formě je zásadní pro bezpečný chod podniků. Práce prokázala, že bezpečný vzdálený přístup k podnikovým datům pomocí virtuální privátní sítě VPN, jako jednoho z nejdůležitějších aspektů zabezpečení pro vzdálené připojení do podnikové sítě, je zásadní pro ochranu podnikových dat a přístup zaměstnanců do vnitřní podnikové sítě. Při realizaci vzdáleného přístupu do vnitřní sítě je kladen důraz zvláště na konzistenci a spolehlivost datové sítě každého podniku. Zabezpečení a efektivnost protokolů virtuálních privátních sítí se neustále vyvíjí a nabízí možnosti pro nízkonákladové připojení jednotlivých poboček i zaměstnancům do jedné sítě a zároveň přístup k podnikovým datům. Bez ohledu na způsob nasazení VPN (vlastní, či využití dodavatele), existují různé možnosti implementace zabezpečení na různé vrstvy. Technologie se s dobou neustále vyvíjejí, stejně tak jako důmyslné útoky na podnikovou infrastrukturu. Mění se i filozofie infrastruktury a podniková úložiště jsou umisťována mimo firemní sítě do cloudů. Bezpečný přístup pak dostává jiný rozměr. Podniky musí na tuto realitu neustále reagovat a zvyšovat úroveň zabezpečení svých dat. Současné dostatečné řešení bezpečnosti v budoucnu nebude stačit, ale implementace dnešních pokročilých technologií jako běžný standard zajistí bezpečný a plynulý provoz podniků.

6 Seznam použité literatury

[1] BUREŠOVÁ, Karla. *VPN (1) - historie, definice a důvody budování* [online]. [cit. 2022-03-31]. Dostupné z: https://adoc.pub/vpn-1-historie-definice-a-dvody-budovani.html. Akademická práce.

[2] *THE HISTORY OF VPN*. Le-VPN [online]. 2018 [cit. 2022-03-31]. Dostupné z: https://www.le-vpn.com/history-of-vpn/.

[3] TYSON, Jeff, Chris POLLETTE a Stephanie CRAWFORD. *How a VPN (Virtual Private Network) Works*. Computer.howstuffworks.com [online]. 2011 [cit. 2022-03-31]. Dostupné z: https://computer.howstuffworks.com/vpn.htm.

[4] *Is your company properly securing data wherever it lives?*. Www.spirion.com [online]. 2022 [cit. 2022-03-31]. Dostupné z: https://www.spirion.com/blog/is-your-company-properly-securing-data-wherever-it-lives/.

[5] *Why is data security important?*. Ibm.com [online]. [cit. 2022-03-31]. Dostupné z: https://www.ibm.com/topics/data-security.

[6] HUNKO, Mykhailo, Igor RUBAN a Kateryna HVOZDETSKA. *Securing the Internet of Things via VPN technology* [online]. 2021 [cit. 2022-03-31]. Dostupné z: https://doi.org/10.30837/csitic52021232903. Akademická práce. Kharkiv National University of Radio Electronics, Ukraine.

[7] YASAR, Kinza. *Security Challenges During the COVID-19 Pandemic and How to Protect Yourself.* Makeuseof.com [online]. 2021 [cit. 2022-03-31]. Dostupné z: https://www.makeuseof.com/security-challenges-covid-pandemic/.

[8] VANEČKOVÁ, Šárka. *Počítačová síť a internet.* Filozofická-přírodovědecká fakulta v Opavě, Slezská univerzita v Opavě, 2017. ISBM 978-80-7510-245-4. Dostupné také z: http://vavreckova.zam.slu.cz/obsahy/pocsit/skripta/sitebc.pdf.

[9] *Personal Area Network*. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2021 [cit. 2021-6-12]. Dostupné z: https://cs.wikipedia.org/wiki/Personal_Area_Network.

[10] PETERKA, Jiří. *Privátní vs. veřejné sítě* [online]. 17/96. 1994 [cit. 2021-6-12]. Dostupné z: http://www.earchiv.cz/a96/a617k150.php3.

[11] *Internal Network definition*. Lawinsider.com [online]. [cit. 2022-03-31]. Dostupné z: https://www.lawinsider.com/dictionary/internal-network.

[12] *Privátní síť*. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2021-6-12]. Dostupné z:

https://cs.wikipedia.org/wiki/Priv%C3%A1tn%C3%AD_s%C3%AD%C5%A5.

[13] *Co je VPN a jak funguje? Váš základní průvodce* [online]. Avast, 2019 [cit. 2021-6-12]. Dostupné z: https://blog.avast.com/cs/co-je-vpn-a-jak-funguje.

[14] CertBros, 2021, VPNs Explained | Site-to-Site + Remote Access, YouTube video. [cit. 2021-6-12]. Dostupné z: https://www.youtube.com/watch?v=CWy3x3Wux6o.

[15] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika*. Třetí vydání. Praha: Grada Publishing, 2015, 240 s. ISBN 9788024799186.

[16] *IaaS, PaaS a SaaS aneb V čem se liší služby „as a Service".* Master.cz [online]. 2022 [cit. 2022-04-10]. Dostupné z: https://www.master.cz/blog/iaas-paas-a-saas-aneb-v-cem-se-lisi-sluzby-as-a-service/.

[17] ŠTRÁFELDA, Jan. *Intranet*. Strafelda.cz [online]. 2016 [cit. 2022-03-31]. Dostupné z: https://www.strafelda.cz/intranet.

[18] *Firemní počítačová síť a související technologie* [online]. 2017, 2017, , 1-3 [cit. 2021-12-02]. Dostupné z: https://www.czso.cz/documents/10180/46014804/06200517k01.pdf/18852f0a-9847-440a-936b-36da780d570c?version=1.0.

[19] DASU, Tamraparni, Yaron KANZA a Divesh SRIVASTAVA. *Geotagging IP Packets for Location-Aware Software-Defined Networking in the Presence of Virtual Network Functions* [online]. researchgate, 2017 [cit. 2022-03-31]. Dostupné z: https://www.researchgate.net/profile/Yaron-Kanza/publication/323993472_Geotagging_IP_Packets_for_Location-Aware_Software-Defined_Networking_in_the_Presence_of_Virtual_Network_Functions/links/5ab6d837aca2722b97ce01e7/Geotagging-IP-Packets-for-Location-Aware-Software-Defined-Networking-in-the-Presence-of-Virtual-Network-Functions.pdf.

[20] ALI, Fawad. *Everything You Need to Know About Geo-Blocking*. Makeuseof [online]. 2022 [cit. 2022-03-31]. Dostupné z: https://www.makeuseof.com/geo-blocking-everything-you-need-to-know/.

[21] SPADAFORA, Anthony. *Remote access VPN: what are they, how do they work and which are the best* [online]. 2020 [cit. 2022-03-31]. Dostupné z: https://www.techradar.com/vpn/remote-access-vpn.

[22] *Site-to-Site VPN* [online]. [cit. 2022-03-31]. Dostupné z: https://www.perimeter81.com/glossary/site-to-site-vpn.

[23] *What Is a Site-to-Site VPN?* Https://www.paloaltonetworks.com/ [online]. [cit. 2021-6-12]. Dostupné z: https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn.

[24] SCHNEIER, Bruce a Bruce MUDGE. *Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)* [online]. 1999 [cit. 2021-6-12]. Dostupné z: https://www.schneier.com/academic/archives/1999/09/cryptanalysis_of_mic_1.html.

[25] VARVELLO, Matteo, Iñigo AZURMENDI, Antonio NAPPA, Panagiotis PAPADOPOULOS, Goncalo PESTANA a Ben LIVSHITS. *VPN0: A Privacy-Preserving Decentralized Virtual Private Network* [online]. Cornell University, 2019 [cit. 2022-03-31]. Dostupné z: https://arxiv.org/pdf/1910.00159.pdf. Cornell University, New York.

[26] JANE, Megan Mary. *Internet privacy and security: Do you need a decentralized VPN?* [online]. 2018 [cit. 2022-03-31]. Dostupné z: https://bigdata-madesimple.com/internet-privacy-and-security-do-you-need-a-decentralized-vpn/.

[27] HILEY, Catherine. *What is VPN split tunneling?* [online]. 2022 [cit. 2022-03-31]. Dostupné z: https://cybernews.com/what-is-vpn/split-tunneling/.

[28] *What Is VPN Split Tunneling?*. Perimeter 81 [online]. 2020 [cit. 2022-03-31]. Dostupné z: https://www.perimeter81.com/glossary/vpn-split-tunneling.

[29] CRIST, Eric F. , KEIJSER, Jan J. *Mastering OpenVPN*. 28.08.2015. Packt Publishing Limited, 2015. ISBN 978-1-78355-313-6.

[30] BENNET, John. WIZCASE. Bezpečnostní protokoly VPN vysvětleny: Vysvětlení PPTP [online]. 2021 [cit. 2021-6-12]. Dostupné z: https://cs.wizcase.com/blog/bezpecnostni-protokoly-vpn-vysvetleny-vysvetleni-pptp/.

[31] ŠOPÍK, Bronislav. *IPSEC* [online]. Antonínská 548/1, 601 90 Brno, 2005 [cit. 2022-04-14]. Dostupné z: https://www.fekt.vut.cz/conf/EEICT/archiv/sborniky/EEICT_2005_sbornik/02-Magisterske_projekty/10-Inteligentni_systemy/05-xsopik00.pdf. Akademická práce. Vysoké učení technické v Brně. Vedoucí práce Dr. Cvrček Daniel.

[32] ANGELO, Raymond. *SECURE PROTOCOLS AND VIRTUAL PRIVATE NETWORKS: AN EVALUATION* [online]. Quinnipiac University, 2019 [cit. 2022-04-23]. Dostupné z: https://iacis.org/iis/2019/3_iis_2019_37-46.pdf. Quinnipiac University.

[33] *IPsec*. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2021 [cit. 2021-6-12]. Dostupné z: https://en.wikipedia.org/wiki/IPsec#Tunnel_mode

[34] *Protokol ESP (Encapsulating Security Payload)* [online]. IBM [cit. 2021-6-12]. Dostupné z: https://www.ibm.com/docs/cs/i/7.1?topic=protocols-encapsulating-security-payload.
[35] *Protokol AH (Authentication Header)* [online]. IBM [cit. 2021-6-12]. Dostupné z: https://www.ibm.com/docs/cs/i/7.1?topic=protocols-authentication-header.
[36] *Sloučení protokolů AH a ESP* [online]. IBM [cit. 2021-6-12]. Dostupné z: https://www.ibm.com/docs/cs/i/7.3?topic=protocols-ah-esp-combined.
[37] *Secure Sockets Layer*. Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2021 [cit. 2021-6-12]. Dostupné z: https://cs.wikipedia.org/wiki/Secure_Sockets_Layer.
[38] *SSL /TLS a zabezpečené prohlížení webu* [online]. SSL.com, 2019 [cit. 2021-6-12]. Dostupné z: https://www.ssl.com/cs/Nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-dotazy/faq-co-je-ssl/.
[39] *What is a VPN?* [online]. NordVPN [cit. 2021-6-12]. Dostupné z: https://nordvpn.com/what-is-a-vpn/.
[40] Stackpole, B.. (2007). Centralized authentication services (RADIUS, TACACS, DIAMETER).

[41] METZ, Christopher. *AAA PROTOCOLS: Authentication, Authorization, and Accounting for the Internet* [online]. Cisco Systems, 1999 [cit. 2022-04-23]. Dostupné z: https://www.scss.tcd.ie/~htewari/bib_files/met99.pdf.
[42] TANENBAUM, Andrew S. a David J. WETHERALL. *Computer Networks.* Fifth Edition. Pearspm, 2013. ISBN 978-1-29202-422-6.
[43] STANKUŠ, Martin. *Autentizace, autorizace a accounting v prostředí IEEE 802.1X / RADIUS20.* 2007, 15 s. Dostupné také z: http://docplayer.cz/19452620-Autentizace-autorizace-a-accounting-v-prostredi-ieee-802-1x-radius.html.
[44] *Přehled o protokolu RADIUS (Remote Authentication Dial In User Service)* [online]. IMB, 2012 [cit. 2021-9-13]. Dostupné z: https://www.ibm.com/docs/cs/i/7.1?topic=authentication-remote-dial-in-user-service-overview.
[45] *RADIUS. Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2021 [cit. 2021-9-13]. Dostupné z: https://cs.wikipedia.org/wiki/RADIUS.
[46] HASSELL, Jonathan. *Radius: Securing Public Access to Private Resources*. New York: O´Reilly, 2003. ISBN 978-0596003227.
[47] *10 pravidel pro silné heslo: Opravdu máte dobře zabezpečené účty? BlueGhost* [online]. 2018, 27. 03. 2018 [cit. 2021-9-23]. Dostupné z: https://www.blueghost.cz/clanek/10-pravidel-bezpecnost-hesel/.
[48] *Password entropy*. WhatIs.com [online]. 2014 [cit. 2021-9-23]. Dostupné z: https://whatis.techtarget.com/definition/password-entropy.
[49] DASGUPTA, D., Arunava ROY a Abhijit NAG. *Advances in user authentication*. Cham, Switzerland: Springer, [2017]. *Infosys science foundation series* (Springer). ISBN 978-3-319-58806-3.

[50] *What is Multi-Factor Authentication (MFA) and How Does it Work?* [online]. [cit. 2021-9-23]. Dostupné z: https://www.onelogin.com/learn/what-is-mfa.
[51] *Bezpečnostní doporučení NÚKIB pro administrátory v4.0 [online]. NÚKIB*, 2020 [cit. 2021-9-27]. Dostupné z: https://www.nukib.cz/download/publikace/vzdelavani/Admin%204.0%20brozura.pdf.
[52] PAPAKONSTANTINOU, Nikolaos, Douglas L. VAN BOSSUYT, Joonas LINNOSMAA, Britta HALE a Bryan O'HALLORAN. *A Zero Trust Hybrid Security and Safety Risk Analysis Method* [online]. ResearchGate, 2021 [cit. 2022-03-31]. Dostupné z: https://www.researchgate.net/publication/350440983_A_Zero_Trust_Hybrid_Security_and_Safety_Risk_Analysis_Method. VTT Technical Research Centre of Finland.
[53] *THE ULTIMATE GUIDE TO ZERO TRUST SECURITY* [online]. CyberTalk.org, 2021, 13 [cit. 2022-03-31]. Dostupné z: https://resources.checkpoint.com/cyber-security-resources/the-ultimate-guide-to-zero-trust-security.
[54] *What is a Zero Trust network?*. Cloudflare [online]. [cit. 2022-03-31]. Dostupné z: https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/.
[55] BHALLA, Wini. *What Is a Zero Trust Network and How Does It Protect Your Data?* [online]. 2021 [cit. 2022-03-31]. Dostupné z: https://www.makeuseof.com/what-is-zero-trust-network/.
[56] *What is Zero Trust Network Access (ZTNA)?* [online]. [cit. 2022-03-31]. Dostupné z: https://www.cloudflare.com/learning/access-management/what-is-ztna/.
[57] PETTERS, Jeff. *Active Directory Domain Services (AD DS): Overview and Functions.* Varonis [online]. 2020 [cit. 2022-04-20]. Dostupné z: https://www.varonis.com/blog/active-directory-domain-services.

UNIVERZITA HRADEC KRÁLOVÉ
Fakulta informatiky a managementu
Akademický rok: 2020/2021

Studijní program: Aplikovaná informatika
Forma studia: Prezenční
Obor/kombinace: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

Jméno a příjmení:	**Jan Sakač**
Osobní číslo:	**I1900249**
Adresa:	Palackého 380, Trutnov – Horní Předměstí, 54101 Trutnov 1, Česká republika
Téma práce:	Metody bezpečného připojení k podnikovým datovým zdrojům
Téma práce anglicky:	Methods of a secure connection to corporate data sources
Vedoucí práce:	Ing. Pavel Blažek, Ph.D. Katedra informačních technologií

Zásady pro vypracování:

Práce je zaměřena na zabezpečený a bezpečný přístup k datovým zdrojům pomocí VPN. Zabývá se používanými protokoly, jejich porovnáním s důrazem na bezpečnost a implementací v různých případech.
Osnova:
úvod do problematiky geograficky rozdělených sítí
možnosti propojení sítí a připojení k nim
bezpečnostní aspekty připojení
Návrh a implementace řešení připojení
Souhrn realizačních poznatků
Závěr

Seznam doporučené literatury:

1, Jazib Frahim, Omar Santos; Cisco ASA : all-in-one firewall, IPS, Anti-X, and VPN adaptive security appliance, Indianapolis : Cisco Press, 2010
2, Nayan B. Ruparelia; Cloud computing, Cambridge, Massachusetts : MIT Press, [2016]
3, Anthony T. Velte, Robert C. Elsenpeter, Jakub Goner; Cloud Computing : praktický průvodce, Brno : Computer Press ; 2011
4, Barrie A. Sosinsky ;Mistrovství – počítačové sítě, Brno : Computer Press, 2010

Podpis studenta: Jan Sakač Datum: 21. 4. 22

Podpis vedoucího práce: Datum: 21. 4. 22