Česká zemědělská univerzita v Praze

Technická fakulta

Analýza SD-WAN sítí v prostředí Internetu

Diplomová práce

Vedoucí diplomové práce: Ing. Zdeněk Votruba, Ph.D.

Autor: Bc. Dominik Čáp

Praha, 2020

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Dominik Čáp

Obchod a podnikání s technikou

Název práce

Analýza SD-WAN sítí v prostředí Internetu

Název anglicky

Software-defined networking in a wide area network

Cíle práce

Cílem práce je posouzení možností a praktického nasazení nových koncepcí tzv. softwarově definovaných sítí na globálními sítěmi. Posouzeny budou jak technická, tak i technologická a organizační hlediska.
V rámci praktické části bude porovnána tato síť se sítí vytvořenou prostřednictvím obvyklé služby VPN a to z pohledu latence, rychlosti a spolehlivosti při různém zatížení sítě. Podle zpracovaných hodnot pak bude formulováno doporučení a závěr.

Metodika

1. Úvod
2. Cíl práce
3. Metodika
4. Virtuální sítě, důvody, řešení a trendy
5. Praktické ověření funkce VPN
6. Praktické ověření funkce SD WAN
7. Zpracování výsledků a shrnutí
8. Závěr a doporučení

Doporučený rozsah práce

50 – 60 stánek včetně obrázků a grafů

Klíčová slova

WAN, LAN, VPN, SD WAN

Doporučené zdroje informací

BURIAN P. Internet inteligentních aktivit, ekniha, Grada, 2014

DOYLE, Jeff a Jennifer CARROLL. Routing TCP/IP. 2nd ed. New Delhi, India: Pearson Education, 2006. ISBN 9788131700426.

HUCABY, David. CCNP BCMSN exam certification guide: CCNP self-study. 1st selling. Indianapolis, IN: Cisco Press, 2004. ISBN 1-58720-077-5

KUROSE, James a Keith ROSS. Počítačové sítě. 1. vyd. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

OREBAUGH, Angela. Wireshark a Ethereal: kompletní průvodce analýzou a diagnostikou sítí. Vyd. 1. Brno: Computer Press, 2008. ISBN 978-80-251-2048-4.

PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z: [technologie pro datovou, hlasovou i multimediální komunikaci]. 2., aktualiz. vyd. Brno: Computer Press, 2006. ISBN 80-251-1278-0.

Předběžný termín obhajoby

2019/2020 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 7. 1. 2019

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 15. 2. 2019

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 16. 12. 2019

Prohlášení

„Prohlašuji, že jsem diplomovou práci na téma: Analýza SD-WAN sítí v prostředí Internetu vypracoval samostatně a použil jen pramenů, které cituji a uvádím v seznamu použitých zdrojů.

Jsem si vědom, že odevzdáním diplomové práce souhlasím s jejím zveřejněním dle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů, ve znění pozdějších předpisů, a to i bez ohledu na výsledek její obhajoby.

Jsem si vědom, že moje diplomová práce bude uložena v elektronické podobě v univerzitní databázi a bude veřejně přístupná k nahlédnutí.

Jsem si vědom, že na moji diplomnovou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů, především ustanovení § 35 odst. 3 tohoto zákona, tj. o užití tohoto díla.“

V Praze dne 30. 3. 2020 ……

Bc. Dominik Čáp

Poděkování

Děkuji Ing. Zdeňkovi Votrubovi, Ph.D. za vedení této diplomové práce, za jeho ochotu, odborné rady a cenné připomínky, které mi během psaní práce poskytoval. Dále bych chtěl poděkovat společnosti Neeco s. r. o. za poskytnutí přístupů k realizaci praktické části práce a v neposlední řadě své rodině za významnou podporu v průběhu celého studia.

Abstrakt: Tato práce se zaměřuje na budoucnost technologií WAN (Wide Area Networking) a zejména na vznikající, vysoce potenciální softwarově definovanou technologii WAN. Technologické principy SD-WAN a jeho dopady na trh WAN budou důkladně analyzovány, aby bylo možné ukázat, jaké jsou scénáře vývoje tohoto trhu. Práce objasňuje vývoj WAN technologií, jejich alternativy a skutečnost, že se vše pohybuje směrem k systémům založeným na cloudu. Práce obsahuje porovnání řešení VPN se softwarově definovanými WAN jak po teoretické stránce, tak i praktické. Došlo se k závěru, že SD-WAN poskytuje stejně kvalitní přenos dat po síti jako technologie VPN, ale zároveň disponuje mnoha dalšími podstatnými výhodami.

Klíčová slova: WAN, LAN, VPN, SD-WAN

Analysis of SD-WAN networks in the Internet environment

Abstract: This work focuses on the future of Wide Area Networking (WAN) technologies and especially on the emerging, high-potential software-defined WAN technology. The technological principles of SD-WAN and its impact on the WAN market will be thoroughly analyzed to show what are possible scenarios for the development of this market. The work explains the development of WAN technologies, their alternatives and the fact that everything is moving towards cloud-based systems. The thesis includes a comparison of VPN solutions with software defined WAN theoretically and also practically. It was concluded that SD-WAN provides the same quality data transmission over the network as VPN technology, but also has many other significant advantages.

Key words: WAN, LAN, VPN, SD-WAN

Obsah

Seznam použitých zkratek

AES	Advanced Encryption Standard, standard pokročilého šifrování
AI	Artificial Intelligence, umělá inteligence
ATM	Asynchronous Transfer Mode, asynchronní přenosový režim
AWS	Amazon Web Services, Amazon webové služby
DIY	Do It Yourself, udělej si sám
DMVPN	Dynamic Multipoint VPN, dynamická VPN
DTLS	Datagram Transport Layer Security
EAP-TLS	Extensible Authentication Protocol
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service, infrastruktura jako služba
IETF	Internet Engineering Task Force, Komise pro technickou stránku
IoT	Internet of Things, internet věcí
IPsec	IP Security Protocol
ISP	Internet Service Provider, poskytovatel internetového připojení
IWAN	Intelligent WAN
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
MPLS	Multiprotocol Label Switching
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol verze 2
NAT	Network Address Translation, překlad síťových adres
NHRP	The Next Hop Resolution Protocol
OMP	Overlay Management Protocol
PaaS	Platform as a Service, platforma jako služba

PfRv3	Performance Routing Version 3
PPP	The Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
QoE	Qoulity of Expierence, kvalita zkušeností
QoS	Quality of Service, kvalita služeb
QUIC	Quick UDP Internet Connections
RFC	Request for Comments
SaaS	Software as a Service, software jako služba
SD-WAN	Software-defined networking in WAN, softwarově-definovaná
SDN	Software-defined Networking
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network, virtuální privátní síť
WAN	Wide Area Network, rozlehlá síť
ZTP	Zero Touch Provisioning

Seznam obrázků

Seznam tabulek

1 Úvod

S příchodem cloudových technologií vznikají v dnešním IT světě nové výzvy. Tradiční funkce WAN (Wide Area Network) jako propojování uživatelů či kampusů s aplikacemi na serverech v datových centrech již nejsou tolik aktuální. Většinou se k zabezpečení a konektivitě využívalo dedikovaných MPLS (Multiprotocol Label Switching) obvodů. Ve světě cloudu toto již nefunguje.

Cloudová řešení odhalila určitou nepřipravenost sítí WAN. Ty byly navrhnuty pro minulé období a nejsou tak připraveny na nárůst provozu WAN, jenž s sebou cloud přinesl. Příkladem může být nepředvídatelný výkon aplikací, složitá správa nebo zranitelnost dat. Pro řešení těchto problémů přichází nový druh rozlehlé sítě SD-WAN (software-defined networking in WAN).

Virtualizační a hypervisorové technologie umožnily mnoha datovým centrům přejít od hardwarových řešení k softwarově řešeným datovým centrům (software-based data centers, SDDCs). Nyní k podobnému přechodu dochází u rozlehlých sítí WAN. Za nejžádanější potřebu se považuje hybridní konektivita právě pro tradiční rozlehlé sítě WAN, které nyní používají metodu jediného připojení. Hybridní síť WAN podporuje veškeré transportní mechanismy, které jsou v dnešní době k dispozici.

Softwarově definované WAN sítě v současné době atakují špičku nejčastěji implementovaných řešení v moderních firmách. Nabízejí totiž významnou obchodní hodnotu pro organizace s distribuovanými pobočkami různě po světě, zejména po finanční stránce. Úspory firmám přináší především výhody jednodušší, pružnější a snadněji spravovatelné síťě.

Počítačové sítě hrají v moderní společnosti rozhodující roli. V dnešní době je v datových centrech hostováno mnoho internetových služeb, jako jsou vyhledávače, sociální sítě a elektronický obchod, kde jsou stovky tisíc počítačů propojeny rozsáhlými sítěmi datových center. Tato datová centra jsou vzájemně propojena širokopásmovými sítěmi, které pokrývají planetu theentire. Koncoví uživatelé používají své osobní počítače, mobilní telefony a tablety k přístupu k internetovým službám prostřednictvím ETHERets, WiFi sítí a celulárních sítí. Správa těchto sítí pro poskytování rychlých, spolehlivých a bezpečných síťových služeb je hlavním problémem ve výzkumu počítačových sítí.

2 Cíl

Cílem práce je analyzovat SD-WAN řešení. Posoudit možnosti jeho nasazení, vysvětlit základní principy a porovnat tuto technologii s řešením VPN. Přiblížena budou technická, technologická i organizační hlediska.

Praktická část se zaměřuje na porovnání dat z provozu datové sítě s VPN technologií a následně technologií SD-WAN. Cílem je zjistit, jestli má nová technologie SD-WAN pozitivní vliv i na rychlost, latenci nebo spolehlivost sítě, nebo zda řešení SD-WAN přináší výhody v jiných aspektech.

Dílčí cíle této práce jsou:

- Vytvořit přehled řešené problematiky.
- Popsat možnosti nasazení technologie SD-WAN.
- Porovnat technologie VPN a SD-WAN.
- Prakticky ověřit technologii VPN.
- Prakticky ověřit technologii SD-WAN.

3 Metodika

Pro vytvoření přehledu řešené problematiky bude čerpáno převážně ze zahraničních online zdrojů. Jelikož téma je stále nové, knižní publikace jsou k dispozici převážně pouze v zahraničí a to je i hlavním důvodem zpracování práce z internetových zdrojů.

Bude vytvořen teoretický základ týkající se témat WAN, VPN a SD-WAN. Práce se zaměřuje na vysvětlení základních principů těchto technologií. Zmíněny budou současná řešení WAN, využití a typy VPN. V části o SD-WAN se zaměří na architekturu, zabezpečení, případy užití a jednotlivé typy řešení. Budou teoreticky srovnána technologie VPN a SD-WAN.

V praktické části budou měřeny hodnoty při běžném provozu na síti. U technologie VPN se vytvoří datový tunel mezi lokálními sítěmi a po dobu 24 hodin bude probíhat měření třech veličin. Ztrátovost paketů při spojení, latenci sítě a přenos dat. Pro měření bude využito programů FortiClient k vytvoření VPN tunelu a OpManager spolu s PRTG Network Monitor k měření údajů provozu na síti. U technologie SD-WAN bude probíhat měření také 24 hodin a zkoumány budou opět zmíněné tři hodnoty. K měření bude použito řešení od společnosti Cisco Systems. Výsledné hodnoty budou na závěr porovnány.

Součástí praktické části práce je ekonomické zhodnocení, ve kterém se bude počítat návratnost investice při přechodu na technologii SD-WAN spolu s výší potenciálních úspor. K tomuto výpočtu bude využito finančního modelu od společnosti ACG Research, který nabízí společnost Silver Peak Systems.

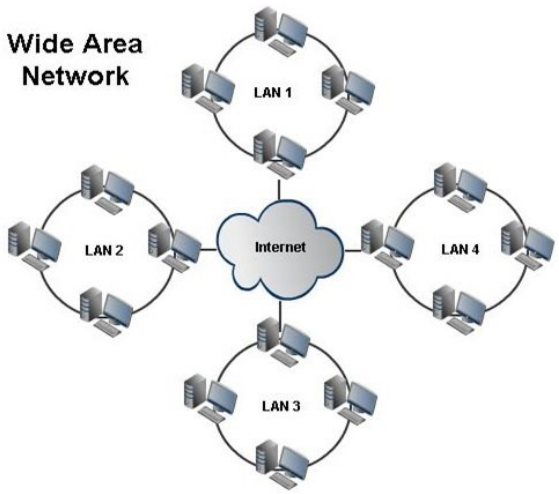
4 Přehled řešené problematiky

Počítačové sítě jsou dnes nezbytné pro maximální využití počítačů a dalších souvisejících zařízení. Jedná se o soubor počítačového vybavení, které je propojeno různými způsoby. Základním přínosem je schopnost výměny dat mezi zařízeními. Pro SD-WAN je nezbytná WAN (Wide Area Network), která pokrývá rozlehlé geografické území. Nejznámějším příkladem WAN je síť internet. [1]

4.1 WAN

Od vzniku ARPANETu v 60. letech minulého století, první výpočetní sítě TCP / IP, se svět stal mimořádně připojeným k jeho moderní verzi - internetu. Existují některé důležité historické události, které jsou zodpovědné za to, jak internet vidíme dnes. Vývoj Ethernetu roku 1974 v Xerox PARC a jeho úspěch jako první široce rozmístěné LAN technologie kolem roku 1980. Vznik přechodu v 90. letech, který nahradil nízkofunkční mosty, jež byly v té době používány. Představení prvního komerčního víceprotokolového routeru v roce 1986 společností Cisco, který změnil svět počítačových sítí. Všichni tito vývojáři výrazně přispěli k výzkumu a vývoji v oblasti počítačových sítí. Později, když se síť stala dostupnou pro komerční účely, po roce 1990 byl potřeba jiný typ technologie, který by mohl spojovat nejen místní, ale také vzdálené počítače. Tato skutečnost vyvolala vznik WAN, jejíž schéma je zobrazeno na obrazku 1. [2]

Obrázek 1 - Schéma Wide Area Network



Zdroj: https://www.mbaskool.com/business-concepts/it-and-systems/13445-wan.html

První formou WAN byly tzv. leased lines (pronajaté linky). Jednalo se o jednoduchá soukromá spojení vyžadující sdílená média, kterými byla multiplexována jednotlivá připojení různých zákazníků. První komerční technologií s přepínáním paketů WAN však byla Frame Relay. Byla navržen tak, aby nahradila řádky a vytvořila protokol nezávislý na paketech s přepínáním WAN. Další důležitou technologií WAN, která začala přecházet od paketových k buňkovým sítím, byl asynchronní přenosový mód (ATM) na konci 80. let. Rivalita trvala desetiletí, dokud se sítě s přepojováním paketů nestaly standardem moderního internetu. [2]

Další technologie WAN, která bude zmíněna, je stále dominantní technologií WAN od jejího vzniku v roce 1999. Tato technologie se jmenuje MPLS a je standardizována IETF v RFC3031 (RFC = označení řady dokumentů popisující internetové protokoly). MPLS je založeno na přepínání značek, patentovaném řešení Cisco, které začalo v roce 1998 a zaměřilo se na označování IP paketů. Všechny výše uvedené technologie WAN mají jednu hlavní podobnost. Vyžadují služby poskytovatele telekomunikačních služeb, který je odpovědný za jejich správu a poskytuje je jako službu potenciálním zákazníkům. Proto jsou zákazníci závislí na konkrétních sítích Frame Relay, ATM nebo MPLS, které jejich ISP (Internet Service Provider) poskytuje. Je důležité si uvědomit, že tyto sítě nejsou připojeny k samotnému internetu a jsou určeny pouze pro soukromou komunikaci mezi podnikovými weby. [3]

4.1.1 Možnosti WAN

Existuje však další způsob jak vytvořit spojení WAN mezi podniky. Využívá stávající internetovou infrastrukturu a nezávisí na konkrétní službě. Tato metoda se nazývá Virtual Private Networking. VPN jsou extrémně nákladově efektivní, škálovatelné a flexibilní řešení, která lze použít jako alternativu k výše uvedeným technologiím WAN. VPN využívají dostupnou veřejnou infrastrukturu – internet, k realizaci virtuální sítě WAN mezi podnikovými weby. Vzhledem k tomu, že internet je globální síť, tak poskytuje možnost připojení webů z celého světa. Sítě VPN také nabízejí jednu další možnost, než tradiční řešení WAN. To je příležitost pro vzdálený přístup k firemní infrastruktuře, kterou lze inicializovat z jakéhokoli místa s přístupem na internet. Existují také nevýhody této technologie. Neexistují žádné současné standardy pro řešení VPN, takže výběr mezi mnoha možnými variantami je poměrně složitý. Největší výhodou pro podniky v používání řešení VPN oproti tradičním WAN je jejich cena, avšak výhody jako spolehlivost provozu a efektivní QoS (quality of service) jsou nabízeny pouze z tradičních řešení WAN. [4]

Jedním z druhů VPN připojení je IPsec. Jedná se o sadu protokolů, které se používají k vytvoření zabezpečeného kanálu přes internetovou vrstvu IP a většinou se používají pro vytváření VPN. Protokol IPsec lze použít s protokolem IPv4 i IPv6 k zajištění vysoce kvalitního zabezpečení provozu na internetu. Druhým řešením VPN je DMVPN. Dynamic Multipoint VPN je patentované řešení Cisca, které nabízí vysoce škálovatelné a automatizované služby VPN. [4]

4.1.2 Současná řešení

V dnešní době je jasné, že digitální svět se ubírá zejména směrem ke cloudovým řešením. Od aplikací po síťovou komunikaci cloud rychle předhání své soupeře. Obzvláště zajímavé je, jak cloud transformuje trh WAN se vznikem SD-WAN - cloudového síťového přístupu využívajícího zásady softwarového definování síťových sítí. SD-WAN je jedním z nejžhavějších témat dnešních diskuzí o sítích, a to díky skutečnosti, že kombinuje softwarově definované sítě, cloud a WAN tržní sektory. [5]

S rostoucí poptávkou po vysokorychlostním síťovém provozu, který se očekává od technologií, jako je umělá inteligence (AI), internet věcí (IoT) a 5G, se předpokládá, že do roku 2020 budou digitální podniky potřebovat více než 5 000 terabitů propojení. Toto množství provozu bude vyžadovat více škálovatelný a cloud-friendly model pro podnikání než současný lídr na trhu - MPLS. Podniky budou vyžadovat flexibilní, snadno použitelnou a snadno spravovanou síťovou komunikační službu, která je vysoce škálovatelná a levná. SD-WAN je navržen tak, aby umožnil podnikům nejen propojit své pobočky jako tradiční MPLS WAN, ale také zajistit rychlé připojení ke všem potřebným aplikacím. [6]

Dalším důležitým bodem SD-WAN je nepříliš složitá konfigurace. Oddělení řídicí roviny od datové roviny, která je hlavním principem SDN (software-defined networking), umožňuje zajistit centralizovaný konfigurační model, který lze snadno spravovat. SD-WAN je schopen využívat jak internet, tak existující síť MPLS, aby nabídl nejlepší možnou optimalizaci WAN pro podnikání. SD-WAN a MPLS jsou tedy za určitých podmínek schopny koexistovat, což je dalším důležitým aspektem, jak tato nová technologie ovlivní současný trh WAN. ISPsare bývalo hlavním hráčem ve hře WAN a s příchodem SD-WAN je nyní na ústupu. [6]

4.1.3 Motivace

Po desetiletích opakujících se konfigurací se síťoví inženýři těší na přístup, který usnadní proces správy sítě a přinese do něj více automatizace. Softwarově definovaný přístup je dosud tou nejlepší myšlenkou. Umožňuje oddělení mozků a svalů sítě a přináší vysokou úroveň programovatelnosti. Aplikace softwarově definovaných principů v sektoru WAN je realizováno pomocí technologie SD-WAN. Od nástupu nové technologie v roce 2017 se SD-WAN v roce 2018 přiblížil k vůdčím postavení v tomto odvětví. Tento rychlý přechod je největší změnou na trhu WAN za své existence a zaslouží si analýzu. Jelikož prodejci SD-WAN jsou nezávislí na telekomunikačních společnostech a jejich řešení funguje výhradně jen na internetu, očekává se výrazný posun na trhu. Potřeba výzkumu v této oblasti je pro odborníky na vytváření sítí velmi důležitá a přispěje k lepšímu pochopení vývoje WAN. Již existují úspěchy s přijetím SD-WAN, které směřují k dalšímu výzkumu v této oblasti. Společnost City and Guilds Group oznámila, že po zavedení řešení SD-WAN zaznamenala trojnásobné zlepšení výkonu svých aplikací Office 365 v rámci své globální síťové infrastruktury. [6][7][8]

4.2 VPN

V současné době lze hovořit o krizi WAN na úrovni technické vrstvy s ohledem na obtížnost konfigurace ve vrstvě aplikační. Jedna ze služeb s jednoduchou formou aplikace se skrývá pod zkratkou VPN (virtuální privátní síť).

4.2.1 Vysvětlení VPN

Virtuální privátní síť slouží k šifrovanému propojení zařízení přes veřejnou síť jako je internet. V zásadě slouží k vytvoření zabezpečeného soukromého síťového tunelu, jenž je znázorněn na obrázku 1. VPN bezpečně přenášejí informace přes internet spojující vzdálené uživatele, pobočky a obchodní partnery do rozšířené podnikové sítě. [9]

Obrázek 2 - Virtuální privátní síť

Zdroj: https://sites.google.com/site/virtualprivatenetworks/website-builder

VPN je virtuální, což znamená, že fyzická infrastruktura sítě musí být transparentní pro jakékoli další připojení. Ve většině případů to znamená, že síť není vlastněná jedním uživatelem, ale je veřejnou sítí sdílenou s mnoha dalšími uživateli. Pro usnadnění nezbytné transparentnosti horních vrstev se používá síťové tunelování. K překonání skutečnosti, že uživatel nevlastní fyzickou síť, se uzavírají dohody o úrovni služeb s poskytovateli sítí tak, aby co nejlépe splňovaly požadavky na výkon a dostupnost, které VPN vyžaduje. [9]

Z názvu vyplývá, že provoz na síti je soukromý. Vzhledem k častému proudění na veřejných sítí se využívá preventivních opatření k zajištění nezbytného zabezpečení, které je vyžadováno pro jakýkoli konkrétní profil provozu na síti. Mezi tyto bezpečnostní požadavky se řadí šifrování dat, autentizace původu dat, bezpečné generování a včasná aktualizace kryptografických klíčů potřebných pro šifrování a autentizaci, ochrana před přehráváním paketů a spoofingem adres. [9]

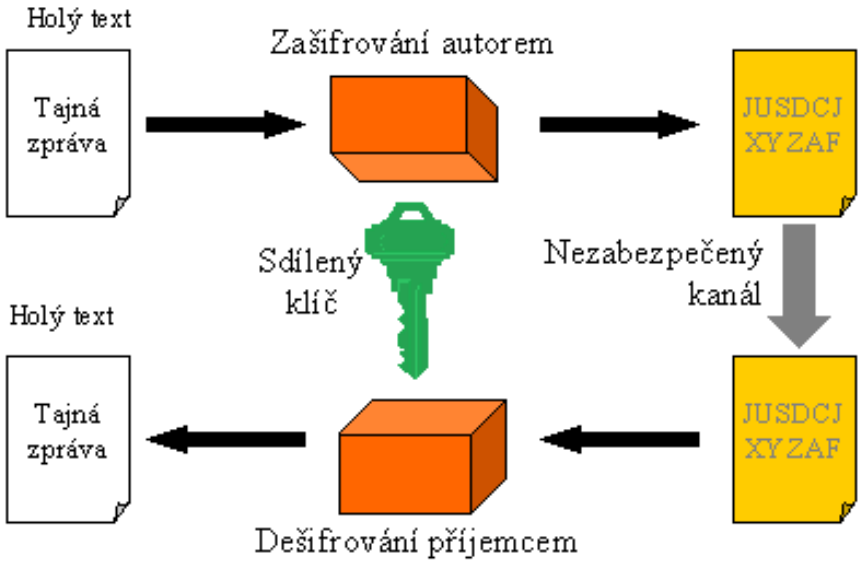
4.2.2 Princip VPN

Virtuální privátní sítí lze nasimulovat privátní síť přes síť veřejnou – internet. Zašifrované připojení chrání uživatele před případným sledováním. O zašifrování se postará VPN klient na jedné straně a vybraný VPN server na straně druhé. Server data rozluští a následně odešle na cílový server, např. webové stránce. Opačný provoz funguje shodně. Tato architektura zajišťuje, že poskytovatel připojení nevidí procházené webové stránky a jejich provozovatelé zase neznají skutečnou IP adresu uživatele, ale pouze adresu VPN serveru. [10][11]

Data uživatelů nejsou šifrováním komplexně ochráněna, jelikož jsou rozšifrovaná na serveru, který k nim má úplný přístup. Kompletního zašifrování lze dosáhnout při použití HTTPS. Tento protokol, který zajišťuje zabezpečenou komunikaci v počítačové síti se považuje za vhodný doplněk ke službě VPN. V případě, kdy je využíváno nezabezpečeného HTTP jsou data od VPN až k cílovému serveru běžně čitelná. Šifrování se uskutečňuje pouze v tunelu mezi uživatelským počítačem a příslušným VPN serverem. Naopak je-li využitý protokol HTTPS, tak jsou data šifrovaná na celé trase od počítače až ke koncovému serveru. V tomto případě se považuje za nejcitlivější informaci soupis navštívených IP adres. [10]

Šifrování, čili metoda, kterou se upravuje čitelný text na nečitelnou změť znaků je při provozu VPN hojně využívané. Asymetrické šifrování, symetrické šifrování a hashování jsou tři nejčastější způsoby šifrování. Princip symetrického šifrování je zobrazen na obrázku 3. Další metodou ochrany hackery jsou vlastní systémy DNS, které většina VPN nabízí. [11]

Obrázek 3 - Princip symetrického šifrování



Zdroj: https://kore.fi.muni.cz/wiki/index.php?title=Soubor:Symetric_crypto.png

4.2.3 Využití VPN

Ochrana soukromí, mixování provozu či obejití geoblokace jsou jedny z mnoha důvodů jak VPN využít. Mezi další se řadí obejití lokální cenzury nebo obejití blokace protokolů. Původně byla roku 1996 technologie vyvinuta společností Microsoft pro bezpečný vzdálený přístup zaměstnanců k podnikovým sítím. Od té doby se stala VPN standartním řešením

pro většinu firem. Dnes se převážně využívá ke skrytí internetových aktivit či jako ochrana proti kybernetickým zločincům. [11][12]

4.2.4 Typy VPN

Při výběru vhodné VPN je nutné vymezit, který druh zabezpečení je třeba použít. Pokud se uvažuje student, pracovník menší firmy nebo zaměstananec velké společnosti, pro každý tento příklad se hodí jiný typ technologie VPN. Při výběru záleží na požadované úrovni zabezpečení a složitosti řešení, případně ceně. [13]

PPTP VPN

Point-to-Point Tunneling Protocol je nejčastěji využívaný druh VPN sítě. Klient PPTP v zásadě navazuje tunelové připojení k serveru PPTP, který prostřednictvím něj přenáší všechna online data a provoz a zároveň zajišťuje jeho šifrování. PPTP zapouzdřuje síťová data a vkládá do ‚IP obálky". Od té doby pokaždé, když router nebo jakékoli jiné zařízení narazí na tato data, zachází s nimi jako s IP paketem. Jakmile jsou data přijata serverem PPTP, jsou přeposlána na web nebo do cílového zařízení. K zajištění šifrování jsou používány dva protokoly. První z nich, MS-CHAPv2 byl v roce 2012 prolomen a od té doby již připojení skrze něj není považováno za bezpečné. Druhým využívaným protokolem zůstává certifikový EAP-TLS. [13][14][15]

Site-to-site VPN

Korporacemi hojně využívaná VPN site-to-site je také nazývána router-to-router. Velké společnosti tuto síť používají hlavně k vzájemnému propojení vlastních kanceláří, ať už na národní či mezinárodní úrovni. VPN mezi sítěmi umožňuje pobočkám na několika pevných místech navázat bezpečné vzájemné spojení prostřednictvím veřejné sítě jako je internet. VPN mezi sítěmi rozšiřuje síť společnosti a zpřístupňuje zaměstnancům počítačové zdroje z jednoho místa na další. [13][16]

Existují dva typy site-to-site VPN. První je na bázi intranetu - má-li společnost jedno nebo více vzdálených míst, ke kterým se chtějí připojit v jediné soukromé síti, může vytvořit intranetovou VPN pro připojení každé samostatné LAN k jediné WAN. Druhým typem je extranet.

Ten se využívá v případě, pokud má společnost úzký vztah s jinou společností k vytvoření bezpečného sdíleného síťového prostředí a zároveň omezení přístupu k jejich samostatným intranetům. [15][16]

L2TP

Layer 2 Tunneling Protocol vyvinutý roku 1998 společnostmi Cisco a Microsoft patří mezi nejrozšířenější ve světě. Používá se k relizaci virtuálních privátních sítí. Tento typ VPN slučuje protokoly PPTP a L2F, právě od Microsoftu a Cisca. Samostatně neposkytuje žádné šifrování ani důvěrnost. Spíše se spoléhá na šifrovací protokol, který prochází v tunelu, aby poskytl soukromí. [17]

Tunelování L2TP začíná zahájením spojení mezi LAC (L2TP Access Concentrator) a LNS (L2TP Network Server) - dvěma koncovými body protokolu - na internetu. Jakmile je toho dosaženo, vrstva propojení PPP (Point-to-point protocol) je aktivována a zapouzdřena a poté je přenášena přes web. Připojení PPP je pak zahájeno koncovým uživatelem s poskytovatelem internetových služeb. Jakmile LAC přijme připojení, naváže se spojení PPP. Poté je přidělen volný slot v síťovém tunelu a požadavek je předán LNS. Nakonec, jakmile je připojení plně ověřeno a přijato, je vytvořeno virtuální rozhraní PPP. V tu chvíli mohou linkové rámce volně procházet tunelem. Rámce jsou přijímány LNS, který poté odstraní zapouzdření L2TP a pokračuje ve zpracování jako normálního rámce. [17]

IPsec

Internet Protocol Security je VPN protokol využívaný pro vytvoření zabezpečené komunikace skrze internet přes IP síť. Tunel umožňuje připojit se k centrální síti ze vzdálené lokality. Bezpečnost je zabezpečena tak, že každá relace musí být ověřena a zároveň jsou pakety jednotlivě zašifrovány napříč celým spojením. IPsec funguje ve dvou režimech – mód přenosu a mód tunelování. Oba z režimů zabezpečují přenos dat mezi různými sítěmi. V přenosovém módu je datový paket šifrován, v tunelovém kódován. Výhodou tohoto typu připojení je možnost implementace dalších bezpečnostních protokolů pro zvýšení ochrany systému. Za nevýhodu se považuje finanční náročnost a časově náročná instalace před použitím. [13]

SSL a TLS

Secure Sockets Layer a Transport Layer Security pracují jako jeden protokol k vytvoření VPN spojení. V tomto připojení se využívá webový prohlížeč jako klient a místo celé sítě

jsou zpřístupněny pouze konkrétní aplikace. Tento protokol je využíván například e-shopy nebo poskytovateli služeb. Relace jsou zabezpečeny, jelikož webové prohlížeč nevyžadují žádnou akci uživatele k přepnutí do SSL. [13]

Pro navázání zabezpečeného připojení SSL / TLS používají prohlížeč a server certifikát SSL. Jedná se o typ digitálního certifikátu vyžadovaného během procesu handshake SSL / TLS k ověření identity webu a povolení šifrovaného připojení. Protokoly SSL / TLS proto používají kombinaci asymetrického a symetrického šifrování. Handshake SSL / TLS umožňuje prohlížeči ověřit webový server, získat veřejný klíč a nastavit zabezpečené připojení před zahájením skutečného přenosu dat. [18]

MPLS

Multi-Protocol Label Switching je považován za nejvhodnější připojení typu Site-to-Site. Důvodem je především flexibilita a adaptabilita. V připojení se obvykle využívá více protokolů, jelikož MPLS je založen na zdroji, který se využívá ke zrychlení distribuce síťových paketů. Princip spočívá v tom, že při přenosu dat se před každý paket směřující do páteřní sítě předřadí krátké označení, které je využito pro další distribuci datové jednotky. Za nejvýznamnější výhodu je považována schopnost implementace kontroly, na základě které lze sledovat datový provoz. V porovnáním s dalšími typy VPN jsou konfigurace i případné úpravy poměrně složité, a tak realizace tohoto typu připojení je značně finančně nákladná. [13][19]

Hybrid VPN

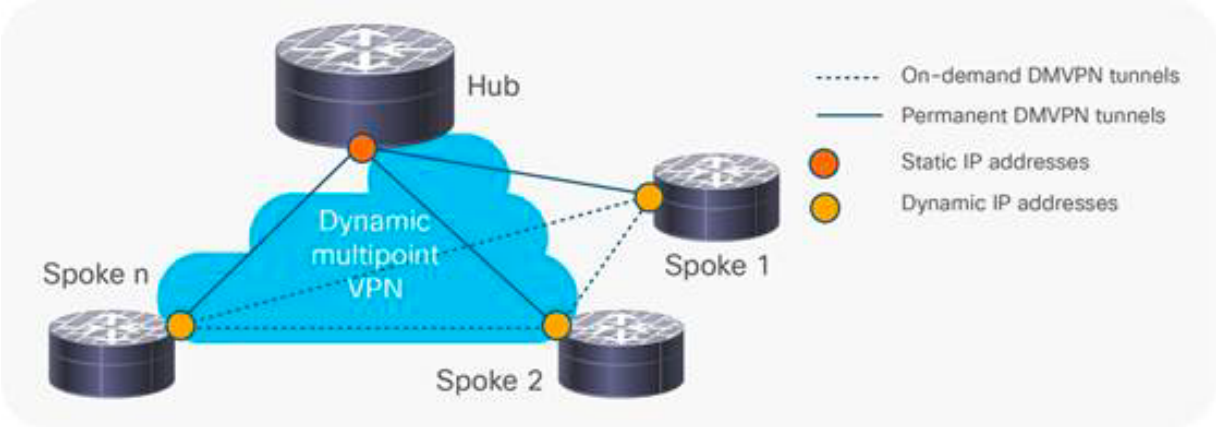
Kombinací Multi-Protocol Label Switching a Internet Protocol Security vzniká hybridní VPN. Tyto dva typy připojení se využívají odděleně na odlišných místech. V případě použití připojení i na stejném místě může být záměrem využití IPsec VPN jako záložního připojení. IPsec vyžaduje zařízení většinou ve formě směrovače, který data šifruje a tvoří VPN tunel. MPLS VPN jsou využívány operátorem skrze jeho zařízení v síti. Pro propojení těchto dvou VPN je vytvořena speciální brána z důvodu zachování bezpečnosti a eliminace tunelu IPsec. Hybridní VPN jsou finančně náročná řešení v porovnání s dalšími typy, ovšem nabízejí na oplátku vysokou fleixbilitu. [13]

4.2.5 Dynamická vícebodová VPN

Dynamic Multipoint VPN (DMVPN) je patentované řešení VPN společnosti Cisco, které je navrženo pro flexibilní nasazení ve velkém měřítku s minimální složitostí a nízkými

náklady na implementaci ve srovnání s VPN MPLS. DMVPN pracuje s konceptem rozbočovače a paprsků (hub and spoke). V architektuře je jeden hlavní směrovač, který se označuje jako rozbočovač a více směrovačů pobočkových kanceláří - paprsky. Pobočkové směrovače mají trvalé připojení pouze k centrálnímu rozbočovači a v případě potřeby inicializují připojení na vyžádání k dalším paprskovým směrovačům. Technologie je pro představu znázorněna na obrázku 4. Řešení DMVPN se pro jeho realizaci opírá o tři hlavní technologie - Generic Routing Encapsulation (GRE), IPsec a Protokol Next-Hop Resolution (NHRP). DMVPN může poskytnout volitelné šifrování dat VPN pomocí protokolu IPsec. [20][21]

Obrázek 4 - Cisco dynamická vícebodová VPN



Zdroj: https://www.cisco.com/c/en/us/products/collateral/security/dynamic-multipoint-vpn-dmvpn/data_sheet_c78-468520.html

4.3 SD-WAN

Je výzvou pro síť, aby vyhověla současným vyvíjejícím se aplikačním požadavkům. Zejména v sektoru WAN, kde kvůli cloudovým aplikacím roste potřeba určitého frekvenčního pásma a nízké latence. Zatímco podniky vynakládají miliardy na virtualizaci a modernizaci infrastruktury datového centra, je také doporučováno upgradovat WAN. Existují tři formy cloudových služeb - Software jako služba (SaaS), Platforma jako služba (PaaS) a Infrastruktura jako služba (IaaS). [22]

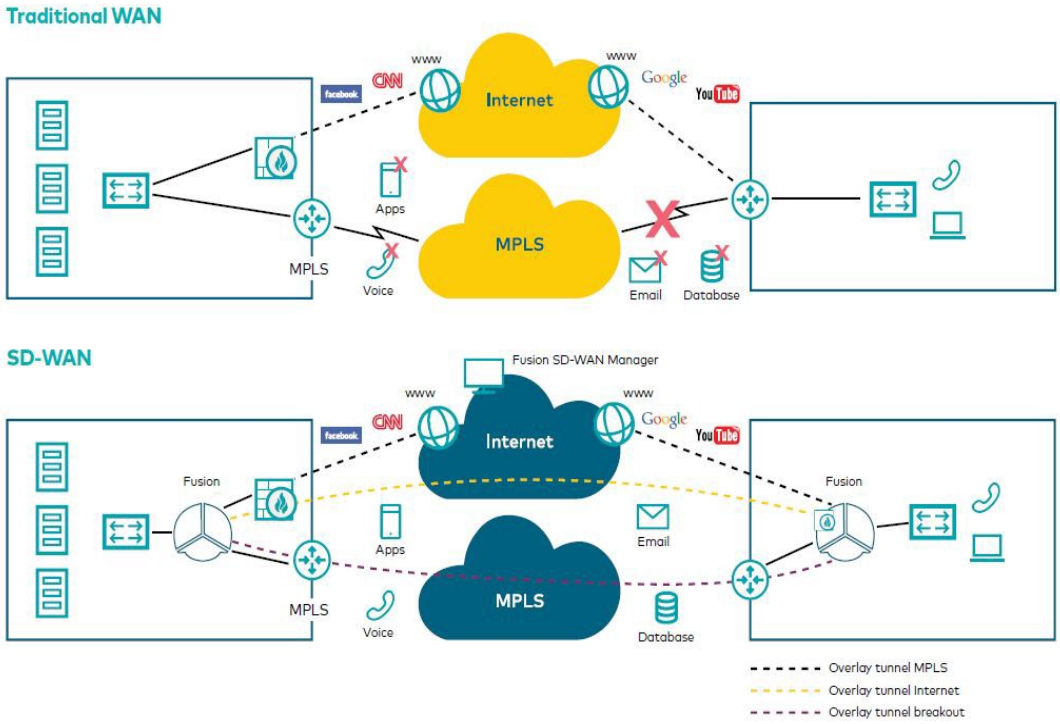
Vzhledem k tomu, že v České republice již cloudové služby využívá třetina všech firem, je možné konstatovat, že jsou lépe připravené na případnou implementaci SD-WAN řešení. Výdaje na cloudové řešení rostou už třetí rok po sobě. V případě srovnání výdajů v roce 2019 a odhadu pro rok 2020, očekává se dvouciferné procento zvýšení. Tomu napomáhá přechod

podniků do moderního IT prostředí, obměna programového vybavení a především právě přechod na cloudové technologie. [23]

Je to síť WAN, která slepuje všechny oddělené cloudové infrastruktury a vytváří holistickou síť pro podnikání. K tomuto efektu také dochází paralelně s rostoucím přijetím SDN. Možná kombinace těchto událostí není náhoda. Možná je to právě softwarově definovaná síť, která se chystá transformovat sektor WAN. Očekává se, že k nejpravděpodobnějšímu rozsáhlému přijetí zásad SDN dojde právě na trhu WAN. [24]

SD-WAN je technologie, která má potenciál provést evoluci v odvětví sítí v oblasti WAN. Přináší nový koncept pro síťový sektor - aplikačně řízené sítě, u nichž se očekává, že se síť přizpůsobí potřebám aplikace. Tato koncepce umožňuje, aby se SD-WAN stala náhradou optimalizačních služeb WAN, drahých MPLS VPN a dalších nákladů na automatizaci a správu sítě. Tento nový koncept WAN je vidět na obrázku 5 v porovnání s tradiční variantou. Obvykle se označuje jako hybridní WAN. Spodní část obrázku znázorňuje kombinaci všech funkcí do jednoho centralizovaného řešení. [25]

Obrázek 5 - Porovnání SD-WAN a tradiční WAN



Zdroj: https://codeburst.io/sd-wan-for-business-a-new-wan-is-here-6fe8e198df4d

4.3.1 Architektura

Fungování technologie je vysvětleno na řešení SD-WAN od společnosti Cisco. Existuje více vendorů zabávajících se SD-WAN technologií a všechny jsou založené na obdobných principech. Jedná se o překryvnou architekturu WAN dodávanou v cloudu, která rozšiřuje principy softwarově definovaných sítí (SDN) do sítě WAN. Řešení je rozděleno do čtyř rovin: data, kontrola, správa a orchestrace. [26]

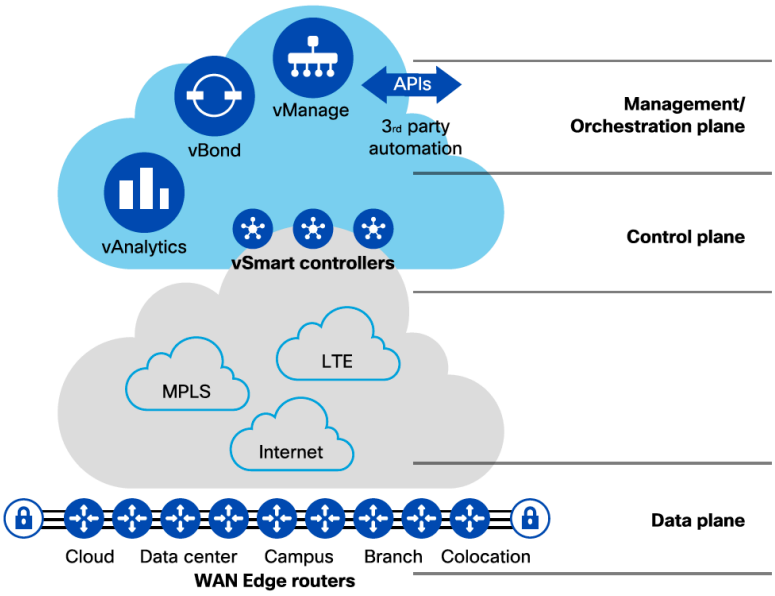
Řešení Cisco SD-WAN obsahuje čtyři klíčové komponenty zodpovědné za každou úroveň organizace:

- Cisco vManage
- Cisco vBond
- Cisco vSmart
- Cisco WAN Edge routery.

Z obrázku 6 vyplývá, že v rovině pro orchestraci figurují zařízení vBond a vManage. Do kontrolní roviny spadá vSmart a do datové WAN Edge routery. Cisco SD-WAN je architektura v cloudu navržená tak, aby vyhověla komplexním potřebám moderních rozsáhlých sítí prostřednictvím tří klíčových oblastí:

- Pokročilá optimalizace aplikací, která přináší předvídatelný aplikační zážitek s vývojem obchodní aplikační strategie.
- Vícevrstvé zabezpečení, které poskytuje flexibilitu pro nasazení správného zabezpečení na správném místě.
- Jednoduchost v podnikovém měřítku, která umožňuje politiku typu end-to-end od uživatele k aplikaci na tisících webů. [26]

Obrázek 6 - Aplikace SDN pricipů



Zdroj: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

vManage

Cisco vManage zajišťuje uživatelské rozhraní v rovině pro správu. Správci sítě a operátoři zde provádějí konfiguraci, odstraňování problémů a monitorování. vManage nabízí základní zobrazení pro jeden i více tenantů a různou variaci rozmístění zákazníků a poskytovatelů služeb. [26]

Klíčovými výhodami řešení Cisco SD-WAN jsou automatizovaná správa a zjednodušené operace. Cisco vManage nabízí jediný panel skla pro všechny aspekty správy, monitorování a řešení problémů řešení Cisco SD-WAN. Cisco vManage umožňuje správcům poskytovat nové weby, zavádět zásady, poskytovat hluboký přehled o viditelnosti a výkonu aplikací, kontrolovat stav zařízení, provádět aktualizace softwaru a mnoho dalšího. Aplikace Cisco vManage využívá řízení přístupu na základě rolí k oddělení úkolů přiřazením různých přístupových oprávnění. [26]

vBond

Cisco vBond sídlí v rovině orchestrace. Řadič vBond je z velké části zodpovědný za proces Zero-Touch Provisioning, autentizaci v první linii, distribuci informací o správě a za usnadnění procházení síťových adres (NAT). Když se router poprvé spustí v nenakonfigurovaném stavu,

je vBond zodpovědný za zabudování zařízení do struktury SD-WAN. Úkolem vBond je porozumět tomu, jak je síť konstruována, a poté sdílet tyto informace mezi ostatními komponenty. [26]

vAnalytics

Cisco vAnalytics nabízí další službu založenou na SaaS, která poskytuje více informací o stavu a dostupnosti sítě, výkonu aplikací a anomáliích a předpovídání využití sítě a aplikací pro lepší plánování kapacit. [26]

vSmart

Cisco vSmart je považován za mozek řešení a existuje v kontrolní rovině. Jelikož jsou zásady vytvářeny ve službě vManage, je vSmart komponentou odpovědnou za prosazování těchto zásad centrálně. Když se pobočky připojí online, jejich směrovací informace se vyměňují s řadičem vSmart a nikoli přímo s ostatními pobočkami. Pomocí zásad je směrovací informace ovlivňována a sdílena s dalšími místy, která určují, jak budou jednotlivé pobočky spolu komunikovat. Protože trasy jsou přijímány prostřednictvím protokolu Overlay Management Protocol (OMP) z umístění poboček, může řadič vSmart vyvolat politiku vytvořenou ve službě vManage proti těmto trasám a řídit, jak provoz prochází látkou SD-WAN. [26]

WAN Edge routery

Routery Cisco WAN Edge jsou zodpovědné za vytvoření síťové struktury a předávání provozu. Směrovače Cisco WAN Edge přicházejí v různých formách, virtuálních i fyzických, a jsou vybírány na základě konektivity, propustnosti a funkčních potřeb webu. [26]

Směrovače WAN Edge tvoří tunely Internet Protocol Security (IPSec) a vytvářejí překryv SD-WAN. Kromě toho je mezi směrovači WAN Edge a každým z řídících prvků vytvořen řídicí kanál. Prostřednictvím tohoto řídícího kanálu obdrží každá součást informace o konfiguraci, zajištění a směrování. Do řídicí infrastruktury není předáván žádný datový provoz. [26]

4.3.2 Zabezpečení

Hlavní součástí cloudové síťové vrstvy je její zabezpečení. Vzhledem k tomu, že SD-WAN využívá veřejnou internetovou infrastrukturu jako dopravní síť, je bezpečnost klíčovou součástí jejího fungování. [27]

Architektura Cisco SD-WAN poskytuje silné zabezpečení pro operace v ovládací rovině, datové rovině a při správě. Aby větve SD-WAN mohly mít přímý přístup k internetu bez závislosti na jiném zařízení nebo řešení z hlediska zabezpečení, jsou do routeru WAN Edge zabudovány mechanismy ochrany před hrozbami. To zajišťuje ochranu provozu uživatelů v pobočkových sítích před internetovými hrozbami a také zlepšuje výkon aplikací, což umožňuje provozu bezpečně využívat přímého přístupu k internetu, pokud je to optimální cesta. Níže jsou uvedeny funkce ochrany před hrozbami, které jsou k dispozici na routeru WAN Edge:

- stavový aplikační firewall
- ochrana a detekce narušení (IPS / IDS)
- filtrování URL, Cisco Advanced Malware Protection (AMP) a ThreatGRID
- Cisco Umbrella DNS
- tunelování pro zabezpečení internetových bran v cloudu (třetí strany). [26]

Obecné doporučené postupy pro zabezpečení komunikačních kanálů:

- fyzická bezpečnost - zákaz neomezeného fyzického přístupu, monitorování spotřebiče, ovládání poplachu, ochrana fyzických rozhraní, ochrana napájení.
- zabezpečení zařízení - řízení přístupu založené na rolích, silná správa hesel, pravidelné aktualizace zabezpečení, úplné vymazání dat po vyřazení z provozu.
- zabezpečení sítě - šifrování AES, ověřování SHA, zabezpečení transportní vrstvy (TLS), služby RADIUS a TACACS +, SNMPv3. [28]

Od každého zařízení SD-WAN je vyžadováno, aby se autentizovalo k řadiči, než se může zapojit do zabezpečené cloudové sítě. Autorizace zařízení je řízena pomocí zásad. Tyto zásady jsou řízeny řídicí rovinou a lze je použít k manipulaci s provozem. [28]

4.3.3 Možnosti nasazení SD-WANu

Nasazení architektury SD-WAN může přinést úspory nákladů, lepší výkon a snadnější správu. Tato digitální transformace obsahuje posuny, kterými podnik prochází při digitalizaci a automatizací operací. Digitální transformace integruje technologii pro řešení tradičních obchodních problémů s automatizací, digitalizovanými procesy a umělou inteligencí. [29]

Jednou z podmínek potřebných k nasazení SD-WAN je virtualizace IT infrastruktury, zejména virtualizace sítě. Pro většinu podnikových IT oddělení je nejjednodušším místem, kde začít s virtualizací sítě právě WAN. Softwarově definované WAN přinášejí relativně rychlé úspory nákladů a výhody výkonu. Virtualizace eliminuje hardware, umožňuje flexibilnější správu a další. [29]

Po splnění nezbytné virtualizace lze uvažovat o této digitální transformaci. Žádné dvě architektury SD-WAN nebudou navrženy, postaveny a spravovány identicky. Rozhodnutí o nasazení změní několik faktorů, včetně vzhledu vzdálené sítě, požadavků koncových uživatelů a omezení rozpočtu. Následujících sedm kroků je nutné projít při uvažování o nasazení SD-WAN:

- vypočítání maximálního počtu vzdálených webů
- správné nasazení na základě počtu uživatelů a předpokládaného využití WAN
- analýza aplikací, služeb, pracovního vytížení
- analýza možnosti připojení WAN
- výběr modelu nasazení
- naplánování sběru datového toku WAN po nasazení
- nepřetržitá snaha o zlepšování založená na analytice. [29]

Každý podnik si musí vybrat, zda implementovat SD-WAN jako řešení „udělej si sám“ (DIY), nebo si najmout poskytovatele spravovaných služeb pro jeho realizaci (Managed SD-WAN). Některé důležité výhody obou přístupů jsou uvedeny v tabulce 1. [29]

Tabulka 1 - Výhody řešení od poskytovatele a DIY

Výhody „Udělej si sám“ (DIY)	Výhody řešení od poskytovatele
Úspora nákladů	Funkčnost
Úplná kontrola	Škálovatelnost
Nezávislost	Kvalifikovaná podpora

Zdroj: Vlastní

Mezi hlavní výhody přístupu DIY patří úspora nákladů, úplná kontrola a nezávislost. Očekává se, že řešení DIY bude stát méně než přidané poplatky za předplatné poskytovatele. Důvodem je skutečnost, že největší náklady na SD-WAN jsou vynaloženy jeho nasazením. Řešení pro kutily nabízí úplnou kontrolu nad podnikovou IT infrastrukturou, aniž by do některého z procesů byly zapojeny třetí strany. To je zvláště důležité pro podniky, které mají citlivé informace a jsou proti zapojení cizích společností. Nezávislost je klíčovým faktorem flexibility a neměla by být podceňována. Jedná se o schopnost podniku samostatně provádět významné změny ve své IT infrastruktuře, aniž by čekal na složité a časově náročné postupy od společností, jako jsou poskytovatelé internetových služeb. Výše uvedené výhody jsou silným bodem pro přijetí SD-WAN jako DIY řešení, ale přicházejí s náklady. Aby podnik mohl nasazovat řešení DIY, musí mít v této oblasti značné zdroje a odborné znalosti. To formuje strategii DIY jako nejvýznamnější pro velké podniky. [30][31]

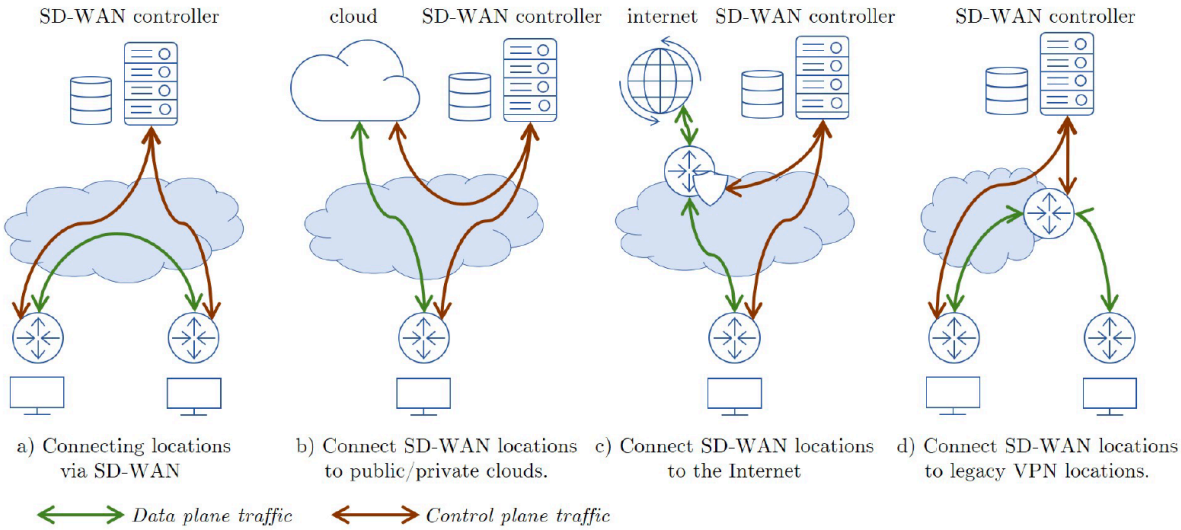
K dispozici je také třetí možnost nasazení služby SD-WAN. Nazývá se „SD-WAN-as-a-Service“. Tato možnost využívá funkčnost cloudu, aby umožnila použití SD-WAN jako služby a poskytla důležité výhody, jako je flexibilita, rychlé nasazení a nízké náklady. Některé společnosti, se zaměřují na vytváření vysoce výkonných řešení SD-WAN-as-a-Service zaměřených na poskytovatele internetových služeb. Tímto způsobem přichází do hry strategie dalšího prodeje, která poskytovatelům služeb umožňuje nakupovat službu SD-WAN jako cloudové řešení a dále ji prodávat jako samostatnou službu svým zákazníkům. [32]

4.3.4 Případy užití

SD-WAN se obvykle používá k navázání zabezpečeného spojení mezi geograficky oddělenými místy podniku. Rozlišují se různé případy přípojení. Čtyři z nich jsou níže přiblíženy a následně vyobrazeny na obrázku 7. [33]

1) Propojení místních sítí několika poboček, všechny propojené prostřednictvím SD-WAN.
2) Propojení s veřejným nebo soukromým prostředím pro cloudové služby. Podniky v současné době využívají cloudová řešení pro své obchodní procesy a toto spojení jim umožňuje bezpečně se připojit ke vzdáleným cloudům.
3) Propojení pobočky prostřednictvím SD-WAN s veřejným internetem. V tomto případě musí být zajištěna zvláštní opatření, která zaručí bezpečný provoz mezi pobočkami přes SD-WAN.
4) Propojení poboček pomocí SD-WAN s místy využívajícími tradiční VPN. Po zavedení SD-WAN musí koexistovat s pobočkami, které jsou stále připojeny prostřednictvím VPN technologie. U tohoto případu je vyžadováno nastavení monitoringu na controlleru k mapování spojení od SD-WAN k VPN a naopak. [33]

Obrázek 7 - Čtyři možnosti připojení SD-WAN



Zdroj: https://www.csacademy.nl/images/scripties/2018/A_security_architecture_for_software_defined_wide_area_networks---final.pdf

4.3.5 Typy služeb

Existují tři typy scénářů služeb SD-WAN – on-premise (prem-only), cloud a hybrid. On-premise řešení znamená provoz služby lokálně na vlastněných zařízeních, hybrid potom kombinací této a cloudové možnosti. Tyto tři varianty se týkají konkrétní služby, kterou je možno používat prostřednictvím řešení SD-WAN, spíše než možností nasazení. Typ on-premise je nejzákladnějším typem služby SD-WAN. Zahrnuje pouze plné propojení mezi geograficky oddělenými pobočkami. Tento typ řešení je určen pro podniky, které nevyžadují používání cloudových služeb, a proto nemusí platit dodatečné náklady

za cloudové řešení SD-WAN. Nejdůležitější výhodou řešení typu prem-only je formování provozu v reálném čase, které využívá mechanismus QoS (quality of service) orientovaný na aplikaci. Typ cloudové služby je určen pro podniky, které chtějí optimalizovat svůj přístup ke cloudu. Poskytuje stejnou QoS architekturu založenou na aplikacích jako řešení typu on-premise, avšak speciálně navrženou pro výkon cloudových aplikací. Funkčnost tohoto řešení závisí na konceptu cloudové brány. Cloudovou bránu lze považovat za bránu poslední instance pro všechny hlavní cloudové aplikace, jako jsou Office 365, Salesforce, AWS atd. Poskytuje přímý přístup k těmto aplikacím, zlepšuje jejich výkon a spolehlivost. Toto řešení je určeno pro podniky, které přijaly cloudovou IT infrastrukturu. Posledním typem služby SD-WAN je hybridní řešení. Zahrnuje on-premise a cloudová řešení do jedné hybridní služby SD-WAN, která je schopna poskytnout jak spolehlivou infrastrukturu WAN, tak vysoce výkonné cloudové připojení. Toto řešení je určeno pro podniky, které chtějí zcela nahradit své současné služby MPLS koncepcí WAN nové generace, zaměřenou na aplikace. Nebo pro podniky, které chtějí využívat řešení SD-WAN společně s MPLS VPN. Hybridní služba SD-WAN je nejflexibilnějším, škálovatelným a výkonem orientovaným řešením WAN, které dnes na trhu WAN existuje. [34][35]

4.3.6 Vendoři

Je obtížné najít jiný sektor podnikového IT průmyslu, který zaznamenal rychlejší růst než softwarově definovaná síť WAN. Analytici předpovídají, že trh SD-WAN poroste o 40,4 % ročně od roku 2017 do roku 2022, kdy dosáhne 4,5 miliardy dolarů. Mezi další předpoklady patří, že tempo růstu během pěti let dosáhne 35 % ročně. [36]

Největším síťovým dodavatelem SD-WAN řešení je společnost Cisco Systems z USA. V roce 2019 vlastnila největší podíl na trhu a byla považována za největšího výrobce na světě dle objemu a výnosů. Za největší událost na trhu SD-WAN se považuje obchod, kdy společnost Cisco koupila za 610 milionů USD řešení pureplay Viptela. Rozšířila tím svou produktovou řadu, kam jsou řazeny i další SD-WAN řešení – iWAN a Meraki. Na základě toho je tak schopna nabízet zákazníkům větší množsví alternativ. [36][37]

Dalším zajímavým jménem na trhu je firma Nuage Networks, která je podporována svou mateřskou společností Nokia, známým prodejcem telefonů. Do nejúspěšnější desítky se řadí také firmy Oracle, Juniper Networks, Citrix Systems, Aryaka Networks nebo například

Silver Peak Systems. Každá ze společností nabízí svoje vlastní řešení, které se principialně neliší od Cisco Systems, které je však stále jednoznačným leadrem na tomto trhu. [36]

4.3.7 Budoucí příležitosti a výzvy

Již se začíná uvažovat o možném použití nových technik jako například strojové účení pro vytváření sítí a virtualizaci síťových funkcí. Dalším předmětem uvažování jsou nové transportní protokoly pro usnadnění rozvoje víceúčelového vytváření sítí založených na SD-WAN. [38]

S rozvojem internetu se zvyšují požadavky na sítě jako vysoká propustnost, nízká latence a vysoká stabilita. Jedním z druhů víceúčelových sítí jsou sítě s nízkou latencí, jelikož nové aplikace a operační scénáře kladou na latenci náročné požadavky. Jedním z příkladů mohou být sítě pro hráče cloudových her, kde se očekává přenos dat s nízkou latencí na síti. Nízkou latenci lze dosáhnout eliminováním dlouhé zpáteční cesty dat a dostat cloud „blíže“ k uživatelům, což je nezbytné pro realizaci víceúčelových sítí. [38]

V posledních letech byly metody strojového učení použity k řešení problémů se sítí a ukázaly velký příslib. Byl vytvořen systém pro generování adaptivních bitrate algoritmů za použití technik posilování učení, které překonávají nejlepší a nejmodernější schéma, se zlepšením průměrné QoE (Quality of expierence) o 12-25%. [38]

Virtualizace síťových funkcí poskytuje novou metodu vytváření IT aplikací. Spojení virtualizace síťových funkcí a SD-WAN má několik výhod jako například snížení kapitálových výdajů, snížení provozních nákladů nebo rychlost a flexibilitu služeb. [38]

Nové transportní protokoly se vyvijí kvůli dosažení nízké latence bez obětování zabezpečení a spolehlivosti. Patří mezi ně například protokol QUIC (Quick UDP Internet Connections). Jeho cílem je snížit latenci připojení odesláním dat přímo při navazování spojení. QUIC lze snadno implementovat a aktualizovat v uživatelském prostoru. Protože většina aplikací je vyvíjena na základě starších přenosových protokolů a tyto protokoly jsou v praxi široce využívány, existuje ještě dlouhá cesta k jejich nahrazení novými přenosovými protokoly. [38]

4.3.8 Srovnání SD-WAN a VPN technologie

SD-WAN je sice ve srovnání s VPN novější technologií, ovšem není nejlepším řešením pro každou síťovou infrastrukturu. Zaléží na požadavcích zahrnující například výkon sítě, přístup ke cloudu nebo vlastní kontrolu WAN. [39]

SD-WAN versus VPN MPLS

Technologie SD-WAN ve srovnání s VPN MPLS poskytuje výhodu ve správě sítě. Principy definované softwarem umožňují centralizovaný systém správy a za pomocí webového rozhraní lze zajistit kontrolu nad celou sítí WAN. U technologie VPN MPLS musí být každý router nakonfigurován samostatně a to skrze příkazový řádek. [40][41]

Za další výhodu se považuje škálovatelnost sítě SD-WAN. Zařízení fungují na principu plug-and-play, což podporuje rychlou a snadnou implementaci dalších součástí síťové architektury. U MPLS je šířka pásma komunikačního kanálu přímo spojena s jeho náklady. Z toho důvodu jsou používány přenosové kanály s nízkou kapacitou a aplikována mechanika QoS (quality of service) pro co nejefektivnější využití služby, což pro SD-WAN neplatí. SD-WAN používá základní připojení k internetu a jeho služba nezávisí na šířce pásma. Uživatelé mají možnost snadno upgradovat nebo downgradovat své internetové předplatné podle svých potřeb. [42][43]

Za jednu z hlavních výhod SD-WANu oproti MPLS je považována také bezpečnost. MPLS poskytuje určitou úroveň zabezpečení oddělením provozu VPN, ovšem přenos nešifruje. Od poskytovatele internetu tedy provoz chráněn není. SD-WAN poskytuje úplné šifrování všech připojení a to buď prostřednictvím DTLS, nebo Ipsec. Sice existuje možnost na stávající MPLS využít Ipsec, ovšem následkem toho se může zdvojnásobit velikost paketu a to může vést k neefektivnímu využití šířky pásma. [3][43]

Pokud se uvažuje cloudový nebo hybridní typ SD-WAN, výhodou je i přítomnost cloudového řešení, které MPLS nenabízí. Výhoda tkví v aplikačně orientovaném QoS mechanismu, který SD-WAN řešení poskytuje. Tento koncept se v oblasti tvoření sítí objevil po přijetí modelu SDN. [44]

Porovnání nákladů na tato dvě řešení vychází také ve prospěch SD-WAN. Spravovaná služba SD-WAN představuje pro uživatele nižší měsíční náklady než u MPLS. Při nasazení DIY řešení SD-WAN do velkého podniku s mnoha pobočkami budou náklady vysoké. Pokud se ovšem

tyto náklady časově rozpočítají a vezme-li se v úvahu schopnost úplné kontroly nad sítí, v porovnání s MPLS budou opět nižší, jelikož poplatek za předplatné služby zůstane faktorem po celou dobu životnosti podniku. [45]

Největší a nejdůležitější výhodou MPLS je její spolehlivost. Používá mechanismus orientovaný na připojení, který poskytuje virtuální privátní kanál pro VPN každého zákazníka. To znamená, že řešení MPLS VPN je vysoce spolehlivé. To je důležité zejména pro podniky, které neustále používají aplikace v reálném čase, jako jsou VoIP nebo streamingové služby. SD-WAN bohužel nemůže poskytnout stejnou úroveň spolehlivosti jako MPLS, protože používá veřejnou internetovou infrastrukturu jako dopravní síť. [40]

SD-WAN versus VPN Ipsec

Ipsec je sice součástí SD-WAN, ovšem jelikož je to otevřený standart, který lze kombinovat i například s MPLS VPN nebo DMVPN, na trhu WAN není považován za hlavní konkurenční produkt. Důvodem je to, že Ipsec je schopen poskytovat prostřednictvím veřejné internetové infrastruktury pouze čistou tunelovou službu VPN. Neexistuje žádná spolehlivost provozu jako u MPLS, žádná WAN nebo optimalizace cloudu jako u SD-WAN a žádná automatizace typu peer jako u DMVPN. Místo toho se Ipsec považuje za doplňkový produkt k ostatním řešením WAN. [46][47]

SD-WAN versus dynamická VPN

DMVPN je řešení, které nabízí pouze jeden dodavatel v síťovém sektoru – Cisco. SD-WAN naopak nabízí téměř všechny hlavní společnosti, včetně společnosti Cisco. První strategií společnosti Cisco bylo pro SD-WAN použití technologie DMVPN jako jádra pro řešení IWAN. Cílem DMVPN bylo spolu s další patentovanou technologií Cisco PfRv3 poskytnout hybridní řešení WAN, které bylo schopno využívat jak MPLS, tak veřejné internetové infrastruktury. Později se akvizicí společnosti Viptela rozhodla společnost Cisco vytvořit tři různé nabídky SD-WAN založené na řešeních Viptela, Meraki a IWAN, zaměřených na různé typy požadavků zákazníků. Tento přístup se liší od většiny ostatních dodavatelů SD-WAN, protože ti poskytují pouze jedno řešení SD-WAN. [48][49]

V případě technologie DMVPN je potřeba fyzických zařízení, kdežto u SD-WAN se v tomto projevuje výhoda cloudu, kde se jedná o virtuální zařízení. Práce s virtuálními zařízeními se považuje za jednodušší a více flexibilní. [50]

Hlavní výhodou SD-WAN je jednodušší možnost správy, než je tomu u DMVPN. Design, počet překryvů, konfigurace šifrování či práce s certifikáty, to vše hovoří pro SD-WAN. U Cisco SD-WAN je přítomen Zero Touch Provisioning (ZTP), kdežto u DMVPN je třeba složitější konfigurace. V technologii DMVPN chybí nástroj pro správu WAN, v SD-WAN je implementace různých zásad méně náročná. [50]

5 Praktická část

Cílem praktické části bylo stanoveno porovnání technologie SD-WAN s řešením VPN. Pro srovnání byly změřeny tři základní veličiny – ztráty paketů při spojení, rychlost přenosu dat a latence. U měření VPN technologie se vytvořil datový tunel a při použití speciálních monitorovacích programů byly měřeny zmíněné veličiny.

U řešení SD-WAN se využilo základních monitorovacích funkcí obsažených přímo v prvku umístěném v rovině pro správu. Naměřené hodnoty byly následně porovnány a na základě výsledků bylo možné posoudit, jestli má nová technologie SD-WAN pozitivní vliv i na rychlost, latenci či spolehlivost sítě, nebo řešení SD-WAN přináší výhody v jiných aspektech.

Bylo provedeno ekonomické zhodnocení nasazení technologie SD-WAN. K tomu byl využit kalkulátor pro výpočet výnosnosti investice pro co nejpřesnější odhad. Výsledkem byly možné úspory a výnosnost investice.

5.1 Praktické ověření funkce VPN

Praktické ověření funkce VPN bylo realizováno třemi různými programy. Byl vytvořen datový tunel, na kterém byla následně měřena ztrátovost paketů, latence a rychlost přenosu dat. VPN tunel spojoval dvě lokální počítačové sítě.

5.1.1 Použitý software

K vytvoření datového tunelu VPN byl použit software FortiClient od společnosti Fortinet. Program FortiClient zabezpečuje all-in-one ochranu koncových stanic, antivir, antispam, firewall nebo právě funkci VPN klienta.

K měření ztrát paketů a latence byl použit program OpManager od společnosti ManageEngine. Software umožňuje komplexně monitorovat a spravovat sítě. Nabízí mimo jiné možnosti správy síťových zařízení, WAN, serverů i monitoring VPN tunelů.

Pro větší vzorek byl k měření ztráty paketů a latence použit ještě software PRTG Network Monitor od společnosti Paessler. Program je využíván k monitoringu všech běžných operačních systémů a nabízí velkou řadu nastavitelných senzorů, dle kterých lze sledovat provoz na síti.

5.1.2 Měření spolehlivosti VPN

Byla provedena měření spolehlivosti spojení datového VPN tunelu. Změřena byla ztrátovost paketů a hodnota latence. Na vytvořeném datovém tunelu byly hodnoty měřeny 24 hodin. Pro ověření naměřených hodnot byly využity dva různé programy – PRTG Network Monitor a OpManager.

Ztrátovost paketů

Pro změření ztrátovosti paketů byl využit software PRTG Network Monitor. Změny v provozu byly vyhodnocovány každou jednu minutu. Postup, kterým byly hodnoty získány je následující: Do monitoringu nainstalovaném na tunelem propojeném zařízení bylo přidáno koncové zařízení v jiné LAN síti. Pro naměření ztrátovosti paketů se nastavily dva senzory, které monitorovaly ztrátovost paketů. Jednalo se o senzory QoS a ping.

Druhým využitým softwarem byl OpManager. Postup byl podobný jako u PRTG. Na jednom z propojených zařízení byl nainstalován tento monitoring a v něm bylo přidáno zařízení na druhém konci datového tunelu. Jednou ze základních měřených veličin je právě ztrátovost paketů, proto nebylo potřeba nastavovat customatizované senzory. Výsledky obou měření jsou zaznamenány v tabulce 2.

Tabulka 2 – Naměřená ztrátovost u VPN

Software	Ztrátovost v procentech
PRTG Network Monitor	0,98
OpManager	1,02
Průměrná hodnota	1,00

Zdroj: Vlastní

Latence

Pro získání hodnoty latence VPN datového tunelu byly použity opět programy PRTG a OpManager. Stejně jako u ztrátovosti paketů byl monitoring nainstalovaný na zařízení, ze kterého byl vytvořen datový tunel. Zařízení na druhém konci spojení bylo přidáno manuálně. U software PRTG byl využit senzor QoS, program OpManager opět tuto hodnotu měří defaultně a nebylo potřeba konfigurovat žádný senzor. Výsledky obou měření

jsou zaznamenány v tabulce 3. Ani v jednom z programů nebyla možnost naměřit hodnoty s přesností na dvě desetinná místa jako u SD-WAN řešení.

Tabulka 3 – Naměřená latence u VPN

Software	Latence v ms
PRTG Network Monitor	4
OpManager	4
Průměrná hodnota	4

Zdroj: Vlastní

Přenos dat a rychlost

Poslední veličinou určenou k porovnání byla stanovena rychlost. Využity byly hodnoty naměřené na stejném datovém tunelu jako v případě ztrátovosti a latence. V průběhu jednoho dne bylo přeneseno celkem 34,77 GB dat, což by odpovídalo rychlosti 3,22 Mb/s. Tuto rychlost nelze považovat za maximální možnou a to vzhledem k internetovému připojení jednotlivých sítí LAN, na kterém je rychlost závislá. Dat bylo odesláno podobné množství jako při měření rychlosti SD-WAN kvůli závěrečnému porovnání.

5.2 Praktické ověření funkce SD-WAN

Praktické ověření funkce SD-WAN bylo provedeno na řešení společnosti Cisco. Popsána byla topologie sítě s geografickým popisem pro představení vzdálenosti mezi síťovými prvky. Zmíněny byly výhody uživatelského rozhraní a základní funkce kontroly jednotlivých prvků v síti. Byly změřeny tři základní parametry pro pozdější porovnání s VPN řešením. Jedná se o spolehlivost, latenci a zkoumán byl i přenos dat v rámci sítě.

5.2.1 Topologie SD-WAN

Síť se skladála z prvku vManage, který zajišťuje uživatelské rozhraní v rovině pro správu. Dále ze dvou vSmart zařízení, která jsou považována za mozek Cisco řešení a jsou odpovědnými komponenty za prosazování zásad. V rovině orchestrace bylo využito dvou prvků vBond a zbytek sítě tvořilo osm WAN Edge routerů.

5.2.2 Geografie

Všechny prvky byly umístěny v USA a přistupovalo se k nim skrze webové rozhraní. V San Jose byl umístěn vManage a v San Franciscu vSmart. Zařízení vBond se nacházely v Chicagu a v San Jose. Nejrozmanitější umístění měly WAN Edge routery, které fungovaly ze San Jose, Portlandu, Dallasu, státu Kentucky a z Chicaga.

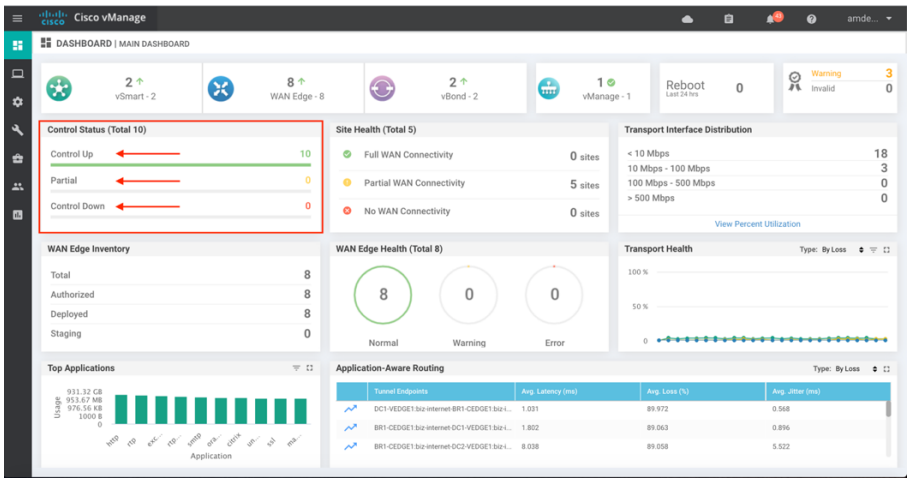
5.2.3 Použitelnost

SD-WAN řešení lze monitorovat a nastavovat skrze webové rozhraní. Níže si představíme, které základní funkce a vymoženosti toto prostředí nabízí. Ke konfiguraci či kontrole není vždy třeba znát konzolové příkazy, jak tomu bývá u klasických routerů. Připojení skrze webové prostředí nabízí přehledné uživatelské rozhraní, kde tyto činnosti lze provozovat.

Kontrola připojení

Na obrázku 8 je zobrazena hlavní obrazovka po přihlášení do kontrolního prvku vManage v SD-WAN síti. Připojení lze zkontrolovat v okně zvýrazněném červeným rámečkem. Řádek Control UP znázorňuje celkový počet zařízení s požadovaným počtem připojení provozní řídicí roviny k řadiči vSmart. Partial monitoruje celkový počet zařízení s některými provozními ovládacími rovinami připojení k řadičům vSmart. Možnost Control Down značí celkový počet zařízení bez připojení řídicí roviny k řadiči vSmart.

Obrázek 8 - Kontrola připojení

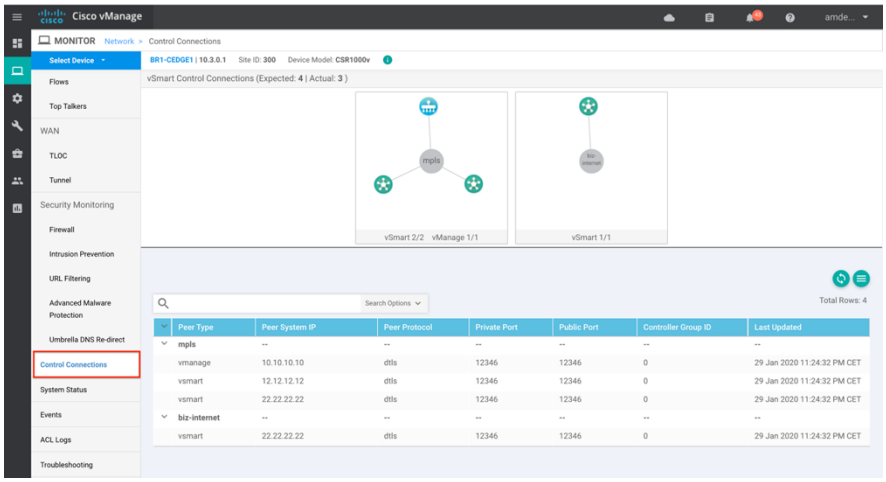


Zdroj: Snímek z uživatelského rozhraní SD-WAN (vlastní zpracování autora)

Kontrola připojení určitého zařízení

Pokud má zařízení více rozhraní, vManage zobrazí grafickou topologii všech řídících připojení pro každý typ jako je na obrázku 9. Lze zobrazit spojení pro daný typ transportu či vybrat nebo zrušit výběr kontrolních připojení.

Obrázek 9 - Kontrola připojení určitého zařízení



Zdroj: Snímek z uživatelského rozhraní SD-WAN (vlastní zpracování autora)

5.2.4 Měření spolehlivosti SD-WAN

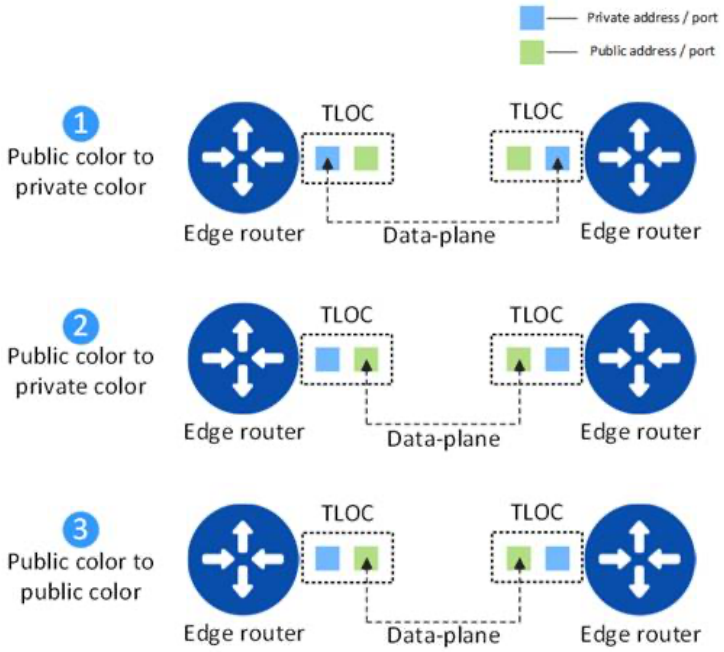
Existuje více možností jak zjistit spolehlivost, respektive ztráty a latenci sítě. První je naměřená průměrná hodnota pro celý TLOC (= Transport Locator). Transportní lokace, které TLOC cesty identifikují, se připojují k fyzickému přenosu jako je například bod, ve kterém se rozhraní WAN připojuje k nosiči. TLOC je tedy souhrn parametrů, které identifikují konkrétní typ transportu, nad kterým SD-WAN transportuje data.

TLOC se skládá ze systémové IP adresy na podobném principu jako Router ID v tradičním networkingu. Unikátně identifikuje celý vEdge router v SD-WAN překryvné síti. Dále z enkapsulace v souvislosti s IPsec nebo GRE, což je protokol ze skupiny TCP/IP určený k zapouzdření paketů jednoho protokolu do protokolu jiného. Dále z barvy, která reprezentuje některý konkrétní transport a může být použita pouze jednou na jednom vEdge routeru. Jsou známé dva typy barev v SD-WAN – privátní a veřejné. Další částí je privátní/veřejná IP adresa fyzického interface, kde transport končí.

Proces prvního provisioningu začíná tak, že se každý vEdge router připojí na kontroler vBond a ten detekuje IP adresu, ze které komunikuje daný vEdge router. Pokud je vEdge router

za NATom, tzn. překladem adres, vBond to rozpozná. To znamená, že pokud vSmart kontroler bude orchestrovat otevírání data-plane komunikace (IPsec nebo GRE tunelů) mezi vEdge routery, tak právě barva vEdge routeru napoví, kterou adresu je nutno použít na takovou komunikaci. Schéma komunikace mezi Edge routery je znázorněno na obrázku 10.

Obrázek 10 - Schéma komunikace mezi Edge routery



Zdroj: Vlastní

Měření tohoto parametru může mít mnoho různých výsledků vzhledem k počtu vytvořených data-plane tunelů. Z toho důvodu bylo pro měření využito měření konkrétních datových tunelů namísto TLOC.

Ztrátovost paketů

Postup, kterým byly získány naměřené hodnoty je následující: Ze základního dashboardu uživatelského rozhraní se zvolila v levém menu položka monitor a v podmenu network. Pro měření se zvolil Edge router označen jako DC1-VEDGE1 a všechna jeho tunelová spojení. Hodnoty byly měřeny 24 hodin provozu zvoleného vEdge routeru. U tunelů je využíván protokol IPsec. Jednotlivé tunely a naměřené hodnoty ztrát v procentech jsou uvedené v tabulce 4.

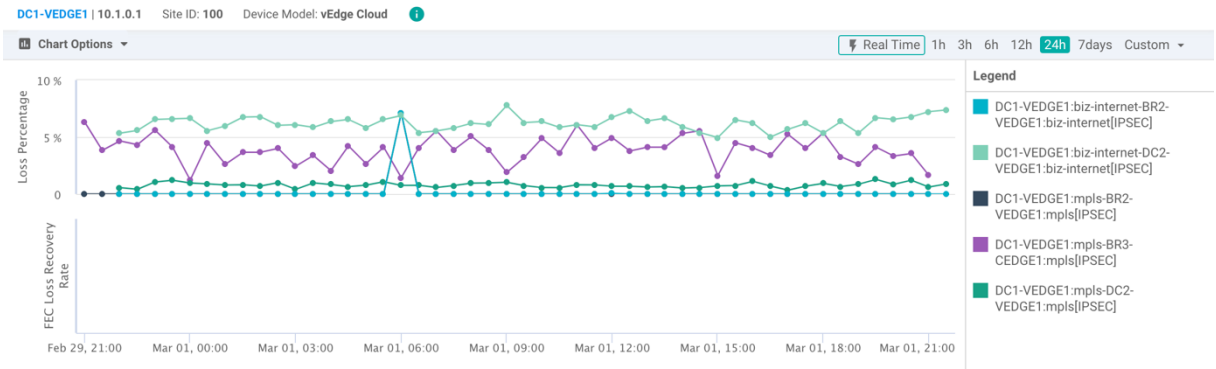
Tabulka 4 – Naměřené hodnoty ztrátovosti SD-WAN

Tunely	Ztrátovost v procentech
DC1-VEDGE1:mpls-DC2-VEDGE1:mpls	0,78
DC1-VEDGE1:mpls-DC2-VEDGE2:mpls	0,00
DC1-VEDGE1:mpls-BR1-CEDGE1:mpls	0,00
DC1-VEDGE1:mpls-BR3-CEDGE1:mpls	3,88
DC1-VEDGE1:mpls-BR2-VEDGE1:mpls	0,15
DC1-VEDGE1:mpls-BR1-CEDGE2:mpls	0,00
DC1-VEDGE1:biz-internet-BR1-CEDGE1:biz-internet	0,00
DC1-VEDGE1:biz-internet-BR1-CEDGE2:biz-internet	0,00
DC1-VEDGE1:biz-internet-BR2-VEDGE1:biz-internet	0,15
DC1-VEDGE1:biz-internet-BR3-CEDGE1:biz-internet	0,00
DC1-VEDGE1:biz-internet-DC2-VEDGE1:biz-internet	6,17
DC1-VEDGE1:biz-internet-DC2-VEDGE2:biz-internet	0,00
Průměrná hodnota	0,93

Zdroj: Vlastní

Průběh a kolísání ztrátovosti v průběhu 24 hodinového měření jsou zobrazeny v grafu na obrázku č. 11, který je pořízen přímo z uživatelského rozhraní Cisco vManage. V grafu byly vynechány tunely s naměřenou hodnotou 0,00 %. Průměrná hodnota ztrát vyšla 0,93 %.

Obrázek 11 - Graf průběhu ztrátovosti u SD-WAN



Zdroj: snímek z uživatelského rozhraní SD-WAN (vlastní zpracování autora)

Latence

Jako druhá veličina byla měřena velikost latence, což je zpoždění mezi příjmutím a vykonáním požadavku. Stejně jako u měření spolehlivosti bylo využito hodnot pro konkrétní tunely. Postup je velmi podobný jako u spolehlivosti. Ze základního dashboardu uživatelského rozhraní se zvolila v levém menu položka monitor, v podmenu network a upravilo se zobrazení pro latenci. Pro měření se zvolil vEdge router označen jako DC1-VEDGE1. Hodnoty byly měřeny 24 hodin provozu zvoleného vEdge routeru.

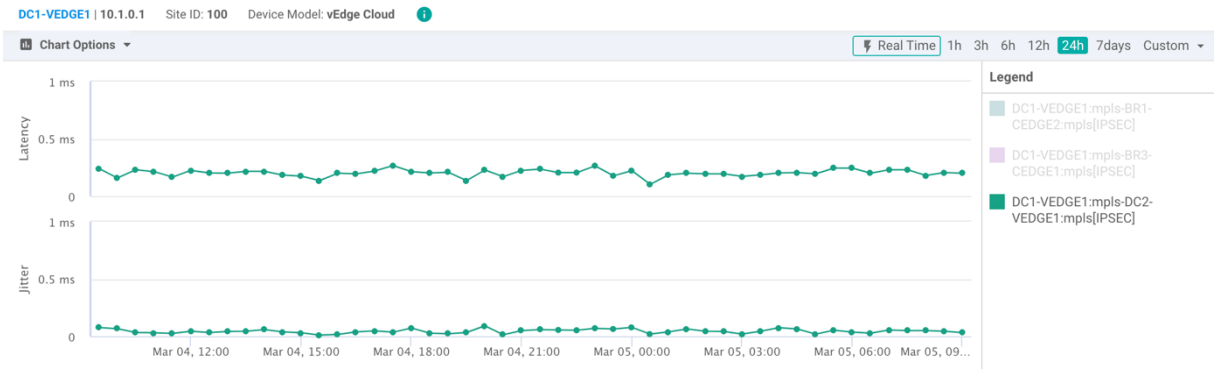
Tabulka 5 – Naměřené hodnoty latence u SD-WAN

Tunely	**Latence v ms**
DC1-VEDGE1:mpls-DC2-VEDGE1:mpls	0,20
DC1-VEDGE1:mpls-DC2-VEDGE2:mpls	0,00
DC1-VEDGE1:mpls-BR1-CEDGE1:mpls	0,00
DC1-VEDGE1:mpls-BR3-CEDGE1:mpls	19,89
DC1-VEDGE1:mpls-BR2-VEDGE1:mpls	0,00
DC1-VEDGE1:mpls-BR1-CEDGE2:mpls	0,02
DC1-VEDGE1:biz-internet-BR1-CEDGE1:biz-internet	1,79
DC1-VEDGE1:biz-internet-BR1-CEDGE2:biz-internet	0,69
DC1-VEDGE1:biz-internet-BR2-VEDGE1:biz-internet	1,49
DC1-VEDGE1:biz-internet-BR3-CEDGE1:biz-internet	0,99
DC1-VEDGE1:biz-internet-DC2-VEDGE1:biz-internet	12,72
DC1-VEDGE1:biz-internet-DC2-VEDGE2:biz-internet	11,47
Průměrná hodnota	4,11

Zdroj: Vlastní

Průběh hodnot latence je vyobrazen na horním grafu na snímku z prostředí vManage na obrázku 12. Pro přehlednost byl vybrán pouze jeden tunel DC1-VEDGE1:mpls-DC2-VEDGE1:mpls. Samotné měření probíhalo 24 hodin provozu zvoleného vEdge routeru. Průměrná hodnota latence vyšla 4,11 ms. Spodní graf na snímku znázorňuje Jitter, což znamená kolísání velikosti zpoždění paketů při průchodu sítí.

Obrázek 12 - Graf průběhu latence u SD-WAN



Zdroj: snímek z uživatelského rozhraní SD-WAN (vlastní zpracování autora)

Přenos dat a rychlost

Poslední veličinou určenou k porovnání byla stanovena rychlost. Bylo využito hodnot pro jeden konkrétní tunel a postup je obdobný jako u předchozích měření ztrát a latence. V uživatelském rozhraní vManage se zvolila v levém menu položka monitor, v podmenu network a upravilo se zobrazení pro přenos dat. Pro měření se zvolil opět vEdge router označen jako DC1-VEDGE1 a jeho spojení s vEdge routerem označeným BR3-CEDGE1. Hodnoty byly měřeny 24 hodin provozu zvoleného tunelu.

V průběhu jednoho dne bylo přeneseno celkem 37,59 GB dat, což by odpovídalo rychlosti 3,48 Mb/s. Tato rychlost ovšem neprezentuje maximální možnou rychlost přenosu dat. V průběhu měření nebylo možno nijak úmyslně ovlivňovat zatížení sítě a jedná se tedy o hodnotu z běžného využití daného tunelu. SD-WAN využívá internetového připojení a záleží tedy na rychlosti připojení od poskytovatelů v obou lokacích umístění routerů.

5.3 Náklady a návratnost investice při přechodu na SD-WAN

Přechod na řešení SD-WAN může způsobit značné úspory, vzhledem k vysoké ceně a složitosti udržování současných sítí WAN. Jejich rigidita a nutnost manuální konfigurace jednotlivých zařízení je v porovnání s SD-WAN provozně neefektivní. WAN jsou náročné na zdroje a často vyžadují specializované IT pracovníky, s čímž jsou spojeny další náklady.

Pro objasnění možných úspor jsou rozebrány jednotlivé faktory, které jsou nezbytné pro analýzu při uvažování o přechodu na technologii SD-WAN. Otestovány byly také kalkulátory nabízené jednotlivými SD-WAN vendory a byla popsána metoda, ze které kalkulátory vycházejí.

5.3.1 Faktory

Při výpočtu návratnosti investice do řešení SD-WAN záleží na několika níže uvedených faktorech:

1) hrubé úspory na datový okruh
2) náklady na předčasné ukončení stávajícího datového okruhu
3) náklady na instalaci nového datového okruhu
4) náklady na upgrade hardwaru
5) náklady na pronájem / odpisy hardwaru
6) časový rámec nasazení. [51]

Hrubé úspory na datový okruh

Vypočítají se jako „aktuální náklady na datový okruh mínus budoucí náklady na datový okruh“. Jedná se o klíčovou položku pro počátek analýzy návratnosti investice. Tyto náklady v podniku analyzují týmy pro správu IT infrastruktury, alternativou je zisk čísel od finančního týmu na základě proběhlých plateb. [51]

Náklady na předčasné ukončení stávajícího datového okruhu

Někdy má smysl zaplatit poplatky za předčasné zrušení a přejít na SD-WAN, ale pouze pokud matematicky vyjde kladně . Například obvod za 1 000 $/měsíc má tří- měsíční poplatek za předčasné ukončení, ale také ušetří 300 $/měsíc ve variantě DIY. Návratnost investic pro konverzi má návratnost 10 měsíců, takže může mít smysl zaplatit pokutu a postupovat vpřed. Sankční poplatky za předčasné ukončení smluvního vztahu jsou uvedeny vždy ve Smlouvě o datových okruzích., Z tohoto důvodu je nutné smlouvy pečlivě prostudovat a vyvolat jednání se současným poskytovatelem, vždy za účasti právníků, buď podnikových a nebo externích. [51]

Náklady na instalaci nového datového okruhu

Vypočítají se jako „náklady na instalaci od nového dodavatele + náklady na interní instalaci“. Jedná se tedy o jednorázové náklady na přechod na SD-WAN technologii. Výše interních nákladů by měla být v podniku předložena vždy odpovědným odborným týmem. [51]

Náklady na upgrade hardwaru

Některé již zakoupené a nasazené směrovače mohou podporovat SD-WAN pouze na základě jednoduché aktualizace softwaru, zatímco jiné bude nutné vyměnit. U těchto technologií se často využívá trvalého obnovovacího programu, na základě kterého se routery nahrazují po určité době za nové. [51]

Náklady na pronájem / odpisy hardwaru

Tyto náklady lze nejefektivněji vysvětlit na příkladu. Podnik vlastní router, který nepodporuje SD-WAN, byl zakoupen před třemi lety a jeho životnost činí pět let. V případě, že router stojí například 4000 $, ztratí dva roky před koncem životnosti hodnotu odpovídající 24 měsícům. To lze vypočítat pomocí vzorce (4000 $/60 měsíců) * 24 měsíců. Výsledek je 1600 $ prohospodařených odpisů. Obdobný koncept platí i pro zařízení v pronájmu. [51]

Časový rámec nasazení

Jednou z možností je urychlit nasazení a rozmístění jednotlivých zařízení, další například nasazení oddálit nebo k němu vůbec nepřistoupit. Výpočet by měl být proveden pro každý datový okruh s přihlédnutím k výše uvedeným metrikám. Příkladem může být datový okruh, u kterého je nutnost uhradit poplatek spjatý s předčasným ukončením a vyžaduje navíc instalaci nového hardwaru. Takový okruh je rozumné převést k datu, kdy poplatek za ukončení neovlivní návratnost investice. [51]

5.3.2 Výpočet

Vzhledem k náročnosti určení výše uvedených faktorů a enormního množství různých podfakorů a možných odlišností, nabízí řada SD-WAN vendorů vlastní kalkulátor pro výpočet výnosnosti investice. Výsledky vychází ze základní rovnice návratnosti investice:

$$Návratnost\ investice = \frac{čistý\ zisk - počáteční\ investice}{počáteční\ investice} * 100\ [\%]$$

Je-li výsledek návratnosti investice nad 100 %, pak je návratnost ekonomicky výhodná a dochází k výdělku. Pokud je výsledek pod 100 %, investice se považuje za ekonomicky nevýhodnou a dochází ke ztrátě.

5.3.3 Kalkulátor

Pro výpočet byl využit kalkulátor od společnosti Silver Peak Systems, která se řadí mezi leadery v poskytování SD-WAN řešení. Parametry zadané do kalkulátoru jsou obsaženy v tabulce 6. Do kalkulátoru jsou předvyplněny průměrné hodnoty, které lze upravit podle požadavků. Pro toto testování nebyly hodnoty nijak změněny.

Tabulka 6 - Vstupní hodnoty do kalkulátoru

Kalkulátor Silver Peak		
Podrobnosti o podniku	Roční tržby z prodeje	0–100 milionů $
	Počet stanovišť	10
	Výměna dosavadních routerů	Ano
Měsíční náklady na připojení WAN	Průměrná šířka pásma na web	50 Mb/s
	Cena MPLS za 1 Mb/s	75 $
	Náklady na širokopásmové připojení za 1 Mb/s	40 $
Měsíční provozní náklady	Náklady na routery na jedno stanoviště	1300 $
	Náklady na firewall na jedno stanoviště	90 $
	Náklady na optimalizaci WAN na jedno stanoviště	260 $
Zvolená doba	3 roky	

Zdroj: Vlastní

V sekci podrobnosti o podniku byly zvoleny nejnižší možné roční tržby z prodeje. Tento údaj je spíše informativního charakteru pro společnost Silver Peak pro případ, kdy na základě využití kalkulátoru mohou zpětně kontaktovat zákazníka s lepší nabídkou. Počet stanovišť udává například kolik poboček je potřeba propojit. Výměna routerů byla zvolena vzhledem k tomu, že vždy nestačí pouze aktualizace softwaru pro možnost využití některých routerů pro SD-WAN řešení. Měsíční náklady na připojení WAN byly ponechány defaultní, stejně jako měsíční provozní náklady. Výpočet byl zvolen na dobu tří let.

Finanční model pro výpočet potencionálních úspor při nasazení infrastruktury SD-WAN byl vyvinut společností ACG Research. Předpokládá se přechod ze současné technologie „router-centric“, kde se využívají tradiční směrovače na řešení SD-WAN. Souhrn současných řešení byl založen na reprezentativních produktech jednotlivých předních prodejců. U routerů se předpokládala možnost využití MPLS, širokopásmového internetu nebo podpora 4G LTE sítí. MPLS byla vnímána jako hlavní cesta pro přenos a další zmíněné technologie byly považovány za záložní.

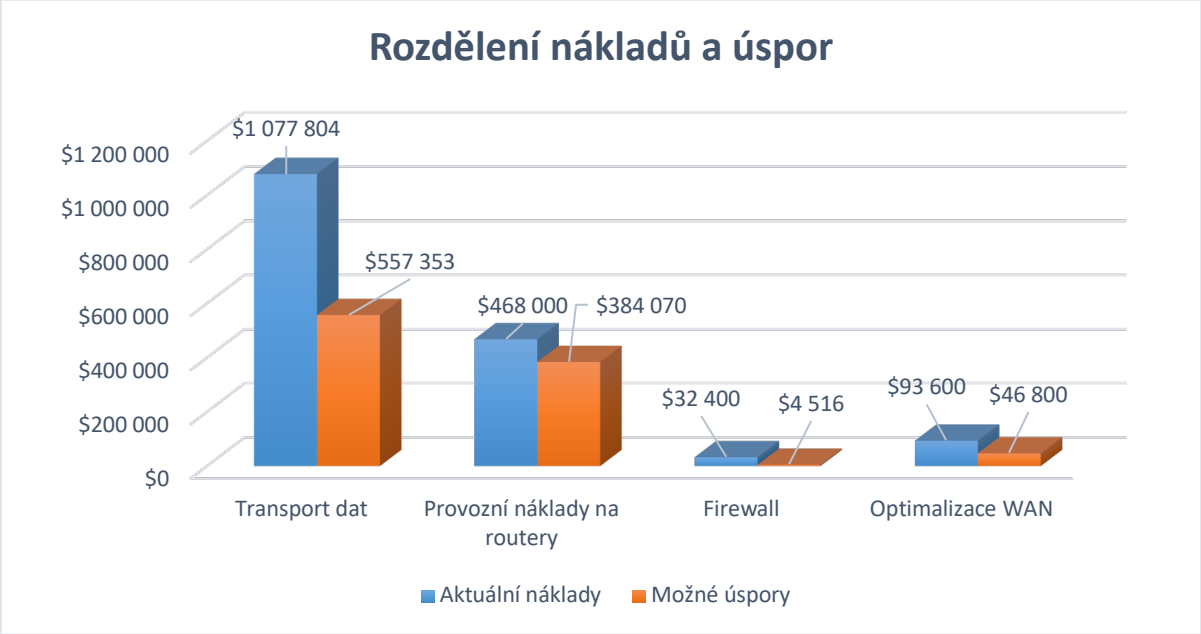
Při výpočtu návratnosti investic byly použity následující předpoklady:

1) Provozní náklady rostou ročně o 20 %.
2) Předpokládá se, že přenos cloudových aplikací jako procento z celkového provozu v prvním roce přesáhne 35 % se složenou roční mírou růstu 27 % a v roce 2022 již dosáhne na 95 %.
3) V prvním roce nejsou realizovány žádné úspory MPLS z důvodu možné existující smluvní dohody. [52]

5.3.4 Výsledné úspory a návratnost investice

Výsledné hodnoty aktuálních nákladů a možných úspor při přechodu na řešení SD-WAN jsou podrobněji zobrazeny a vyčísleny v grafu 1. Nejvýznamnějším artiklem jsou náklady na transport, čili širokopásmové připojení a MPLS. V tomto bodě umožňuje nasazení SD-WAN uspořit kolem poloviny nákladů. Provozní úspory na routery dle výpočtu činí 384 070 $, což je podstatná částka z aktuálních nákladů. Stejně významnou hodnotu úspor v porovnání s náklady přináší i firewall. Na optimalizaci WAN lze ušetřit zhruba polovinu celkových nákladů.

Graf 1 - Výsledné náklady a úspory



Zdroj: Vlastní

Složka provozních nákladů routeru porovnává kapitálové a provozní výdaje pro stávající routery. Předpokládalo se, že routery jsou plně odepisovány. Na základě vstupní šířky pásma byly pro optimalizaci celého provozu použity základní licence. I když existuje počáteční investice do nákupu SD-WAN zařízení, výhody provozních nákladů daleko převažují nad počáteční investicí do kapitálu. Snížení nákladů na operační systém je přičítáno centralizovaným a automatizovaným politikám založeným na aplikacích, rychlejšímu řešení závad, zajišťování nulovým dotykem a inteligentnímu a dynamickému řízení provozu na bázi aplikace po aplikaci.

Podobně jako v případě routerů byly kapitálové náklady existujících firewallů považovány za utopenou cenu. Kvůli růstu provozu a přesunu provozních vzorů do cloudu je nutná další kapacita brány firewall. Integrovaný stavový firewall nabízí ochranu důvěryhodného cloudového provozu, jako jsou aplikace SaaS a IaaS, a umožňuje bezpečné připojení k síti založené na zásadách zabezpečení organizace. Integrovaný stavový firewall minimalizuje množství dalšího méně důvěryhodného cloudového provozu, který je odeslán do externího zařízení firewall pro další úspory nákladů.

Jednou z největších úspor při zavádění SD-WAN jsou celkové měsíční náklady na transport. Díky úpravě trasy a inteligentnímu řízení provozu na základě aplikace umožňuje SD-WAN bezpečně a spolehlivě aktivní využívání levnějších širokopásmových připojení k internetu

a minimalizuje objem provozu, který musí procházet přes nákladnější propojení MPLS. Úspory za první rok se považují za nulové, protože většina podniků je povinna plnit své současné smlouvy o síti MPLS se svým poskytovatelem služeb. Jak je uvedeno výše, analýza také předpokládá roční tempo růstu provozu 20% (meziročně) po dobu trvání analýzy návratnosti investic.

Výsledná hodnota návratnosti investice při zadaných hodnotách z tabulky 6 při přechodu na SD-WAN technologii činí 151 %. Na základě této hodnoty lze usoudit, že přechod na novější technologii SD-WAN se obecně vyplatí.

6 Zhodnocení výsledků

Byly změřeny tři různé veličiny u dvou různých řešení. Prakticky ověřeny byly technologie SD-WAN a technologie VPN. Měřily se veličiny ztrát paketů při spojení, rychlosti přenosu dat a latence. Bylo provedeno ekonomické zhodnocení výpočtem návratnosti investice při přechodu na technologii SD-WAN.

6.1 Ztrátovost paketů

U této měřené veličiny se výsledky obou technologií nijak výrazně nelišily. Porovnány byly průměrné hodnoty měření, které jsou obsaženy v tabulce 7. Rozdíl průměrných hodnot ztrátovosti je 0,07 % ve prospěch SD-WAN.

Tabulka 7 – Výsledky měření ztrátovosti paketů

Technologie	Průměrná hodnota ztrátovosti v procentech
VPN	1,00
SD-WAN	0,93
Rozdíl hodnot	0,07

Zdroj: Vlastní

Ztráta paketů je dobrým měřítkem kvality pro mnoho aplikací založených na protokolu TCP. Ztráta je obvykle způsobena přetížením. Může být také způsobena tím, že síť doručuje nedokonalou kopii paketu. To je obvykle způsobeno bitovými chybami dat nebo v síťových zařízeních.

Úrovně, které popisují kvalitu spojení jsou následující:

- 0 – 1 % ztrát = dobré
- 1 – 2,5 % ztrát = přijatelné
- 2,5 – 5 % ztrát = špatné
- 5 – 12 % ztrát = velmi špatné
- 12 a více % = neakceptovatelné. [53]

Výsledek měření tedy spadá do první z kategorií, která vypovídá o dobré kvalitě spojení a tedy i kvalitním přenosu dat po síti. Rozdíl výsledných průměrných hodnot je zanedbatelný a nemá

na provoz sítě takřka žádný vliv. Z měření lze usoudit, že přenos dat přes VPN je stejně kvalitní jako přenos dat v rámci SD-WAN.

6.2 Latence

Měření latence přineslo stejné výsledky u obou technologií. U měření latence u vytvořeného VPN tunelu nebyla možnost změřit hodnoty s přesností na dvě desetinná místa. Z toho důvodu byla pro toto porovnání naměřená hodnota u SD-WAN zaokrouhlena na celé číslo. Výsledky jsou obsaženy v tabulce 8.

Tabulka 8 - Výsledky měření latence

Technologie	Průměrná hodnota latence v ms
VPN	4
SD-WAN	4
Rozdíl hodnot	0

Zdroj: Vlastní

Latence ovlivňuje zpoždění reakce aplikací na zařízeních. Do celkového zpoždění se sčítá rychlost internetového připojení, odezva vnitřní sítě i práce aplikace. Dle výzkumů trpělivosti se uvádí, že člověk latenci do 100 ms vůbec nevnímá. Průměrná latence pro kabelové připojení přes Ethernet se uvádí méně než 1 ms, průměrná hodnota pro Wifi je méně než 10 ms. [54]

Hodnota latence byla naměřena pro obě dvě technologie stejná. Výsledná hodnota 4 ms je vzhledem k obecným průměrným hodnotám latence pro připojení přes Ethernet nebo Wifi velice solidní. Při interpretaci výsledku je nutno zmínit, že ani jedna síť nebyla cíleně přetěžována a jedná se o hodnotu z běžného provozu.

6.3 Přenos dat a rychlost

Naměření přenosu dat a rychlosti přineslo také podobné výsledky, které jsou obsaženy v tabulce 9. Vzhledem k nemožnosti cíleného zatížení SD-WAN sítě, byla naměřena hodnota přenesených dat, ze které pak následně byla vypočítána průměrná přenosová rychlost. Při měření rychlosti skrze VPN tunel bylo přeneseno o něco méně dat a vzhledem k tomu vyšla přenosová rychlost nižší.

Tabulka 9 - Výsledky měření přenosu dat

Technologie	Rychlost přenosu dat v Mb/s
VPN	3,22
SD-WAN	3,48
Rozdíl hodnot	0,26

Zdroj: Vlastní

Rychlost přenosu dat po síti ovlivňuje rychlost internetového připojení, kvalita vnitřní sítě a jejich zařízení. V měření bylo dosaženo velice podobných hodnot, a tak nelze tvrdit, že některá z technologií vyšla v testování lépe.

6.4 Silné stránky SD-WAN a ekonomické zhodnocení

Naměřené veličiny ztrátovosti paketů, latence nebo rychlosti přenosu dat neodhalily skutečné silné stránky řešení SD-WAN. Síla tohoto řešení spočívá v jiných kvalitách a to zejména v:

- rychlosti nasazení
- rychlosti provisioningu nových WAN Edge routerů
- větší inteligenci sítě při změnách parametrů transportních linek
- větší viditelnosti aplikací na síti
- lepších integrovaných bezpečnostních modelech
- jednodušším integrovánícloudových služeb (IaaS, SaaS)
- lepší programovatelnosti a automatizaci.

Spolu s tím souvisí i možné ekonomické úspory, které technologie SD-WAN přináší. Pro jejich potvrzení se provedl výpočet s využitím kalkulátoru návratnosti investice související s přechodem na tuto technologii. Výsledky jsou uvedeny v tabulce č. 10.

Tabulka 10 - Výsledek možných úspor a návratnosti investice

Možné úspory	Návratnost investice
$ 1 017 826	151 %

Zdroj: Vlastní

Možné úspory spojené s přechodem na novější technologii jsou markantní. Je nutné ovšem podotknout, že se jedná pouze o vypočítaný odhad. Skutečné úspory se mohou lišit v závislosti na jedinečných charakteristikách řešení. Návratnost investice vyšla také velmi pozitivně, ovšem i v tomto případě se jedná o vypočítaný odhad. I přes to, že se jedná pouze o odhad, je možno přechod na SD-WAN obecně doporučit i vzhledem k počtu silných stránek, které tato technolgie přináší na rozdíl od ostatních tradičních možností.

7 Závěr

Cílem práce bylo analyzovat SD-WAN řešení v prostředí internetu. Byla vysvětlena možnost jeho nasazení spolu se základními principy. Zmíněna byla technická, technologická i organizační hlediska. SD-WAN byl porovnán s jednotlivými druhy VPN a následně byly obě technologie prakticky ověřeny.

Byly měřeny hodnoty při běžném provozu v rámci SD-WAN řešení a při tunelovém spojení technologií VPN. Zkoumány byly konkrétně hodnoty ztrátovosti paketů na síti, latence sítě a práce obsáhla i přenos dat a jeho rychlost. Naměřené hodnoty u obou technologií byly následně porovnány.

K měření hodnot u VPN byly použity programy FortiClient, OpManager a PRTG Network Monitor. Hodnoty byly sbírány po dobu 24 hodin kvůli závěrečnému porovnání. Měřeny byly také hodnoty u řešení SD-WAN. K získání těchto hodnot bylo využito řešení od společnosti Cisco Systems.

Z porovnání naměřených veličin nelze určit, že některá z technologií vyšla v testování lépe. Rozdíl průměrných hodnot ztrátovosti paketů při běžném provozu sítě byl zanedbatelný. Měření latence sítě přineslo u obou technologií totožný výsledek. Vzhledem k nemožnosti ovlivnění zatížení SD-WAN při měření byly i hodnoty rychlosti přenosu dat na síti velmi podobné. Pokud by byly sítě realizované technologií SD-WAN i VPN maximálně zatížené, nastalo by pravděpodobně zahlcení sítí, které by se projevovalo zvýšením latence a ztrátou datagramů.

Součástí praktické části práce je i ekonomické zhodnocení možnosti přechodu na technologii SD-WAN. Bylo využito finančního modelu od společnosti ACG Research, který nabízí jeden z předních vendorů SD-WAN společnost Silver Peak Systems. Rozebrány byly hlavní faktory, které při analýze hrají důležitou roli. Byly vypočítány možné úspory v jednotlivých segmentech technologie a spolu s tím i hodnota návratnosti investice spjatá s přechodem na řešení SD-WAN.

SD-WAN je stále poměrně nová a velmi rychle se rozvíjející technologie. Současné architektury WAN již leckdy nestačí dnešním požadavkům vzhledem k nedostatečné rychlosti, nedostatečným možnostem zabezpečení či větší složitosti systému. Z toho důvodu se dá předpokládat, že technologie SD-WAN bude zanedlouho naprosto běžným řešením.

Dle výsledků této práce nepřináší SD-WAN odlišné výkony z hlediska rychlosti přenosu dat, ztrátovosti paketů nebo latence na síti. Přednosti této technologie jsou například v monitoringu sítě, možnosti rozšíření sítě, lepší programovatelnosti nebo bezpečnosti sítě.

Jelikož se jedná o jednu z prvních vypracovaných závěrečných prací na území České republiky na téma týkající se SD-WAN, tak věřím, že pomůže dalším studentům či komukoli jinému k seznámení se s tímto novým řešením a i na základě toho se technologie SD-WAN dostane více do povědomí.

8 Seznam použitých zdrojů

[1] WOODFORD, Ch. Computer Networks [online]. Explainthatstuff.com, 2018. [cit. 5. 3. 2020] Dostupné z: https://www.explainthatstuff.com/howcomputernetworkswork.html

[2] OPPITZ, M. – TOMSU, P. Inventing the Cloud Century. Springer; 1st ed., 2018. 609 s. ISBN 978-3319611600

[3] DE GHEIN, L. MPLS Fundamentals. Cisco Press, 2017. 651 s. ISBN 1-58705-197-4

[4] FOWLER, D. Virtual Private Networks – Making the Right Connection. Morgan Kaufmann Publishers, 1999. 350 s. ISBN 978-1558605756

[5] BLOOMBERG, J. SD-WAN: Entry Point For Software-Defined Everything [online]. Forbes, 2017. [cit. 2. 12. 2019]. Dostupné z: https://www.forbes.com/sites/jasonbloomberg/2017/03/20/sd-wan-entry-point-for-software-defined-everything/#51f781846ee4

[6] POOLE, J. Software-defined everything [online]. Network World IDG Communications, Inc., 2018. [cit. 2. 12. 2019] Dostupné z: https://www.networkworld.com/article/3262993/software-defined-everything.html

[7] BUTLER, B. Why 2018 will be the year of the WAN [online]. Network World IDG Communications, Inc., 2018. [cit. 4. 12. 2019] Dostupné z: https://www.networkworld.com/article/3237691/why-2018-will-be-the-year-of-the-wan.html

[8] KERRAVALA, Z. City & Guilds Group deploys SD-WAN to improve Office 365 performance [online]. Network World IDG Communications, Inc., 2018. [cit. 4. 12. 2019] Dostupné z: https://www.networkworld.com/article/3269049/city-guilds-group-deploys-sd-wan-to-improve-office-365-performance.html

[9] SCOTT, Ch. a kolektiv. Virtual Private Network. USA: O'Reilly Media, Inc., 1999. 211 s. ISBN: 978-1565925298

[10] BOŘÁNEK, R. VPN pro začátečníky: princip fungování, výhody a nevýhody [online]. Root.cz, 2017. [cit. 8. 12. 2019] Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

[11] EMPEY, Ch. Co je VPN a jak funguje? [online]. Avast blog – Avast software s.r.o., 2019. [cit. 8. 12. 2019] Dostupné z: https://blog.avast.com/cs/co-je-vpn-a-jak-funguje

[12] BOŘÁNEK, R. VPN pro začátečníky: princip fungování, výhody a nevýhody [online]. Root.cz, 2017. [cit. 8. 12. 2019] Dostupné z: https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/

[13] FRENKEL, A. Různé typy VPN sítí a kdy je použít [online]. VpnMentor, 2019. [cit. 8. 12. 2019] Dostupné z: https://cs.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/

[14] MOCAN, T. What Is PPTP? [online]. CactusVPN, 2019. [cit. 9. 12. 2019] Dostupné z https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-pptp/

[15] CHIRGWIN, R. Marlinspike demos MS-CHAPv2 crack [online]. The Register, 2012. [cit. 9. 12. 2019] Dostupné z: https://www.theregister.co.uk/2012/07/31/ms_chapv2_crack/

[16] TYSON, J. a kolektiv. How VPNs Work [online]. HowStuffWorks.com, 2011. [cit. 10. 12. 2019] Dostupné z: https://computer.howstuffworks.com/vpn4.htm

[17] TOWNSLEY, W. a kolektiv. Layer Two Tunneling Protocol "L2TP" [online]. Redback Networks, 1999. [cit. 11. 12. 2019] Dostupné z: https://tools.ietf.org/html/rfc2661

[18] Let's Talk about Cybersecurity: TLS vs SSL, HTTPS, and Secure Browsing, 2019 [online]. VPN Unlimited App. [cit. 12. 12. 2019]. Dostupné z: https://www.vpnunlimitedapp.com/blog/tls-vs-ssl-and-secure-browsing/

[19] ROSEN, E. a kolektiv. Multiprotocol Label Switching Architecture [online]. The Internet Society, 2001. [cit. 27. 12. 2019]. Dostupné z: https://tools.ietf.org/html/rfc3031

[20] Understanding Cisco Dynamic Multipoint VPN – DMVPN, MGRE, NHRP [online]. Firewall.cx, [cit. 28. 12. 2019]. Dostupné z: http://www.firewall.cx/cisco-technical-knowledgebase/cisco-services-tech/896-cisco-dmvpn-intro.html

[21] Dynamic Multipoint VPN Configuration Guide, Cisco IOS Release 15M&T [online]. Cisco Systems, Inc., 2018. [cit. 28. 12. 2019]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html

[22] GHAJ, R. – GREENE, N. SD-WAN: Enhancing the Traditional WAN for the Future [online]. International Data Corporation, 2017. [cit. 28. 12. 2019] Dostupné z: https://www.business.att.com/content/dam/attbusiness/reports/enhancing-the-traditional-wan-white-paper.pdf

[23]] DUCHOSLAV, P. Data do cloudu už ukládá třetina českých firem. Není to ovšem řešení vhodné pro všechny [online]. Security Media, s.r.o., 2019. [cit. 28. 12. 2019] Dostupné z: https://www.securitymagazin.cz/security/data-do-cloudu-uz-uklada-tretina-ceskych-firem-neni-to-ovsem-reseni-vhodne-pro-vsechny-1404064436.html

[24] The SoftwareDefined WAN [online]. Silver Peak Systems, Inc. [cit. 28. 12. 2019] Dostupné z: https://www.silver-peak.com/sites/default/files/infoctr/idg-sd-wan-whitepaper.pdf

[25] CHANDRAVAN, P. What Is SD-WAN & Why You Should Care? [online]. Codeburst.io, 2018. [cit. 29. 12. 2019] Dostupné z: https://codeburst.io/sd-wan-for-business-a-new-wan-is-here-6fe8e198df4d

[26] AZIZ, Z. a kolektiv. Cisco SD-WAN Cloud scale architecture [online]. Cisco Systems, Inc., 2019. [cit. 29. 12. 2019] Dostupné z: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-cisco-sd-wan-ebook-cte-en.pdf

[27] UPPAL, S. a kolektiv. Software-defined WAN for Dummies – Velocloud Special Edition. West Sussex: John Wiley & Sons, Ltd., 2015. 61 s. ISBN 978-1-119-10148-2

[28] NetScaler SD-WAN 9.2 [online]. Citrix Systems, Inc., 2017. [cit. 29. 12. 2019] Dostupné z: https://docs.citrix.com/en-us/legacy-archive/downloads/netscaler-sd-wan-9-2.pdf

[29] FROEHLICH, A. Seven steps in deploying SD-WAN architecture [online]. Cisco Systems, Inc., 2018. [cit. 31. 12. 2019] Dostupné z: https://www.cisco.com/c/en/us/solutions/enterprise-networks/sd-wan/seven-steps-deploy-sd-wan-architecture.html

[30] KARKHANAWALA, S. What is SDWAN and Which One is Right for Your Business? [online]. Aryaka Networks, Inc., 2018. [cit. 31. 12. 2019] Dostupné z: https://www.aryaka.com/blog/what-is-sd-wan-which-one-right-for-your-business/

[31] WOOD, M. – LONGO, R. Webinar: SD-WAN The Power to Declare Network Independence [online]. VeloCloud. [cit. 31. 12. 2019] Dostupné z: https://www.velocloud.com/sd-wan-resources/webinars/power-to-declare-network-independence

[32] ARAS, Ch. SD-WAN-as-a-Service: Delivering More Value to Our Service Provider Partners [online]. Citrix, 2018. [cit. 1. 1. 2020] Dostupné z: https://www.citrix.com/blogs/2018/02/21/sd-wan-as-a-service-delivering-more-value-to-our-service-provider-partners/

[33] DIRKSEN, M. A security architecture for software-defined wide area networks [online]. Cyber Security Academy, 2017. [cit. 28. 3. 2020] Dostupné z: https://www.csacademy.nl/images/scripties/2018/A_security_architecture_for_software_defined_wide_area_networks---final.pdf

[34] HOLMES, K. SD-WAN Explained: The 3 Flavors of Software Defined WAN [online]. MatrixNetworks, 2017. [cit. 1. 1. 2020] Dostupné z: https://www.mtrx.com/blog/sd-wan-explained-the-3-flavors-of-software-defined-wan-what-is-sdwan

[35] SMITH, M. The 3 types of SD-WAN architecture [online]. IDG Communications, Inc., 2017. [cit. 1. 1. 2020] Dostupné z: https://www.networkworld.com/article/3219653/the-3-types-of-sd-wan-architecture.html

[36] BURT, J. Top 10 SD-WAN Vendors [online]. eWeek, 2019. [cit. 4. 1. 2020] Dostupné z: https://www.eweek.com/networking/top-10-sd-wan-vendors

[37] KERRAVALA, Z. Why Cisco needs SD-WAN vendor Viptela [online]. NetworkWorld, 2017. [cit. 4. 1. 2020] Dostupné z: http://ezproxy.techlib.cz/login?url=https://search-proquest-com.ezproxy.techlib.cz/docview/1894083944?accountid=119841

[38] YANG, Z. a kolektiv. Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities, 28th International Conference on Computer Communication and Networks (ICCCN), Valencia, Spain, 2019, pp. 1-9.

[39] Get a Clear Understanding of SD-WAN vs. VPN [online]. Simplewan.com, 2018. [cit. 4. 1. 2020] Dostupné z: https://www.simplewan.com/get-clear-understanding-sd-wan-vs-vpn/

[40] SHAH, N. SD-WAN vs. MPLS: Why SD-WAN is a Better Choice in 2019 [online]. Fortinet, Inc., 2019. [cit. 4. 1. 2020] Dostupné z: https://www.fortinet.com/blog/business-and-technology/advantage-of-sdwan-over-mpls.html

[41] SD-WAN vs MPLS vs Internet: What's the Difference? Which is Right for Your Organization? Palo Alto Networks, Inc. [cit. 4. 1. 2020] Dostupné z: https://www.paloaltonetworks.com/cyberpedia/sd-wan-vs-mpls-vs-internet

[42] BOND, R. The 5 Benefits of Moving to SD-WAN from MPLS [online]. Secureops, 2018. [cit. 4. 1. 2020] Dostupné z: https://secureops.com/security/5-benefits-of-sd-wan-from-mpls/

[43] SANTITORO, R. Understanding SD-WAN Managed Services [online]. MEF Forum, 2017. [cit. 4. 1. 2020] Dostupné z: https://www.linkedin.com/pulse/understanding-sd-wan-managed-services-haresh-rane/

[44] GINTERT, J. How Software Defined Wide Area Networking (SD-WAN) Provides Reliable Voice and Video Services Over the Internet [online]. WAN Dynamics, 2018. [cit. 4. 1. 2020] Dostupné z: https://sdn.ieee.org/newsletter/march-2018/how-software-defined-wide-area-networking-sd-wan-provides-reliable-voice-and-video-services-over-the-internet

[45] AKIN, C. What is the cost of MPLS network? [online]. Mushroom Networks Inc. [cit. 4. 1. 2020] Dostupné z: https://www.mushroomnetworks.com/blog/what-is-the-cost-of-mpls/

[46] TAYLOR, S. – WEXLER, J. The pros and cons of IPSec [online]. Network World IDG Communications, Inc., 2004. [cit. 18. 1. 2020] Dostupné z: https://www.networkworld.com/article/2326793/the-pros-and-cons-of-ipsec.html

[47] BEHRINGER, M. – MORROW, M. How IPSec Complements MPLS [online]. Network World IDG Communications, Inc., 2007. [cit. 18. 1. 2020] Dostupné z: https://www.networkworld.com/article/2297191/chapter-6--how-ipsec-complements-mpls.html

[48] SULLENBERGER, M. a kolektiv. History of Networking – DMVPN [online]. Network Collective Media LLC, 2018. [cit. 20. 1. 2020] Dostupné z: https://networkcollective.com/2018/09/hon-dmvpn/

[49] KERRAVALA, Z. Cisco's IWAN isn't dead [online]. Network World IDG Communications, 2017. [cit. 20. 1. 2020] Dostupné z: https://www.networkworld.com/article/3220989/ciscos-iwan-isnt-dead.html

[50] DIB, D. SD-WAN – Glorified DMVPN? [online]. Daniels Networking Blog, 2018. [cit. 21. 12. 2020] Dostupné z: http://lostintransit.se/2018/12/28/sd-wan-glorified-dmvpn/

[51] Analyzing SD-WAN ROI – Key Metrics to Consider [online]. Life Cycle Management Data Group, 2019. [cit. 20. 3. 2020] Dostupné z: https://lcmdatagroup.com/lcm-trends/f/analyzing-sd-wan-roi-%E2%80%93-key-metrics-to-consider

[52] Calculate Your ROI With SD-WAN [online]. Network World IDG Communications, 2019. [cit. 20. 3. 2020] Dostupné z: https://www.networkworld.com/article/3337180/calculate-your-roi-with-sd-wan.html

[52] Science Dissemination Unit [online]. ICTP – SDU, 2006-2019. [cit. 15. 3. 2020] Dostupné z: https://web.archive.org/web/20131010010244/http://sdu.ictp.it/pinger/pinger.html

[53] Latence [online]. ManagementMania.com, 2017. [cit. 15. 3. 2020] Dostupné z: https://managementmania.com/cs/latence-latency