Česká zemědělská univerzita v Praze

Technická fakulta

Katedra technologických zařízení staveb

Diplomová práce

Bezpečnostní a provozní analýza komerčně využívaných VPN

Bc. Lukáš Urban

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Technická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Lukáš Urban

Informační a řídicí technika v agropotravinářském komplexu

Název práce

Bezpečnostní a provozní analýza komerčně využívaných VPN

Název anglicky

Security and operational analysis of commercially used VPNs

Cíle práce

Cílem práce je posouzení možností a praktického nasazení nových koncepcí služeb VPN a porovnat je mezi sebou. Posouzeny budou jak technická, tak i technologická a organizační hlediska. V rámci praktické části bude porovnány různé řešení sítí VPN a ověřeny jejich parametry. Uvedené výsledky se porovnají 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. Zpracování výsledků a shrnutí
7. Závěr a doporučení

Doporučený rozsah práce

50 – 60 stánek včetně obrázků a grafů

Klíčová slova

WAN, LAN, VPN, bezpečnost

Doporučené zdroje informací

Bollapragada, Khalid, Wainner: IPSec VPN Design, Pearson Education (US), 2005, ISBN: 1587051117

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

FEILNER, M.: OpenVPN, Packt Publishing Limited, 2006, ISBN: 9781904811855

Horák, J: Malá počítačová síť doma a ve firmě, Grada, 2003, ISBN: 8024705826

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.

SPORTACK, Mark. Směrování v sítích IP: [autorizovaný výukový průvodce: samostudium: kompletní zdroj informací o směrování a protokolech v sítích IP]. Vyd. 1. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.

Předběžný termín obhajoby

2021/2022 LS – TF

Vedoucí práce

Ing. Zdeněk Votruba, Ph.D.

Garantující pracoviště

Katedra technologických zařízení staveb

Elektronicky schváleno dne 3. 2. 2021

doc. Ing. Jan Malaťák, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 2. 2021

doc. Ing. Jiří Mašek, Ph.D.

Děkan

V Praze dne 08. 10. 2021

Čestné prohlášení

Prohlašuji, že svou diplomovou práci *Bezpečnostní a provozní analýza komerčně využívaných VPN* jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne: 30.3.2022 .....

Bc. Lukáš Urban

Poděkování

Děkuji Ing. Zdeňku Votrubovi, Ph.D., vedoucímu diplomové práce, za odborné vedení a cenné rady, čímž přispěl k vypracování této diplomové práce.

Bezpečnostní a provozní analýza komerčně využívaných VPN

Abstrakt: Cílem práce bylo provedení bezpečnostní a provozní analýzy virtuálních privátních sítí, které jsou komerčně využívané. Součástí byla praktická konfigurace VPN a porovnání stejných typů VPN mezi několika výrobci zařízení, na kterých jsou VPN provozovány. Dále byly jednotlivé typy VPN porovnány mezi sebou z hlediska propustnosti, spolehlivosti a rychlosti. Finální součástí této práce byla konfigurace Microsoft Remote Desktop Services – RemoteApps, jako funkční porovnání možnosti využití a praktického nasazení oproti VPN.

Klíčová slova: LAN, WAN, VPN, Bezpečnost, RemoteApps, Zyxel, Fortinet, SSL, IPsec, Remote Desktop Services

Security and operational analysis of commercially used VPNs

Abstract: The aim of the work was to perform security and operational analysis of virtual private networks that are used commercially. It included a practical VPN configuration and a comparison of the same types of VPNs between several manufacturers of devices on which VPNs are operated. Furthermore, the individual types of VPN were compared with each other in terms of throughput, reliability and speed. Final part of this work was the configuration of Microsoft Remote Desktop Services - RemoteApps, as a functional comparison of usability and practical deployment compared to VPN.

Keywords: LAN, WAN, VPN, Security, RemoteApps, Zyxel, Fortinet, SSL, IPsec, Remote Desktop Services

Obsah

Seznam obrázků

Seznam tabulek

Seznam příloh

Seznam použitých zkratek

NAS – Network Access Storage

VPN – Virtual Private Network

IP – Internet Protocol

IT – Information Technology

SSL – Secure Sockets Layer

IPsec – Internet Protocol Security

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

LAN – Local Area Network

WAN – Wide Area Network

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

FQDN – Fully Qualified Domain Name

URL – Uniform Resource Locator

ISO – International Organization for Standardization

HTTP – Hypertext Transfer Protocol

SMTP – Simple Mail Transfer Protocol

FTP – File Transfer Protocol

MAC – Media Access Control

TCP/IP - Transmission Control Protocol/Internet Protocol

RFC – Request for Comments

UTP – Unshielded Twisted Pair

ARP – Address Resolution Protocol

ICMP – Internet Control Message Protocol

CRC – Cyclic Reduncancy Check

POP3 – Post Office Protocol version 3

IMAP – Internet Message Access Protocol

SSH – Secure Shell

HTTPS – Hypertext Transfer Protocol Secure

SNMP – Simple Network Management Protocol

RADIUS - Remote Authentication Dial In User Service

IGP – Interior Gateway Protocol

QoS – Quality of Service

L2TP – Layer Two Tunneling Protocol

PPTP – Point to Point Tunneling Protocol

DES – Data Encryption Standard

3DES – Triple Data Encryption Standard

AES – Advanced Encryption Standard

MD5 – Message Digest

SHA – Secure Hash Algorithms

IKE – Internet Key Exchange

DH - Diffie Hellman

PPP – Point to Point Protocol

GRE – Generic Routing Encapsulation

PAP – Password Authentication Protocol

CHAP – Challenge Handshake Authentication Protocol

MS-CHAP – Microsoft Challenge Handshake Authentication Protocol

LNS - L2TP Network Server

LAS - L2TP Access Concentrator

PSK – Pre-Shared Key

RSA – Rivest-Shamir-Adleman

SA - Security Associations

ISAKMP - Internet Security Association and Key Management Protocol

AH - Authentication Header

ESP – Encapsulating Security Payload

TLS – Transport Layer Security

RDGW – Remote Desktop Gateway

RDP – Remote Desktop Protocol

RDS – Remote Desktop Services

RDSH – Remote Desktop Session Host

RDCB – Remote Desktop Connection Broker

CAL - Client Access Licence

SD-WAN - Software Defined Wide Area Network

API – Application Programming Interface

SSD - Solid State Disk

HDD – Hard Disk Drive

NAT - Network Adress Translation

SMB - Server Message Block

WWW - World Wide Web

MGMT - Management

PFS - Perfect Forward Secrecy

GPO - Group Policy Objects

OSI - Open Systems Interconnection

CRC - Cyclic Reduncancy Check

1. Úvod

Dnešní nelehká doba si díky pandemii onemocnění Covid-19 žádá moderní přístup k vykonávání práce. Dalo by se říci, že obor informačních technologií je jedním z mála odvětví na pracovním trhu, po jehož službách byla během karanténních opatření zaznamenána vyšší poptávka. Důvodem byl zájem klientů neomezit produktivitu, kreativitu či pracovitost svých zaměstnanců za současného zajištění bezpečného prostředí k práci. Pro firmy, zabývající se informačními technologiemi, to znamenalo zajištění možnosti klientům pracovat ze svých domovů s využitím stejných nebo minimálně rozdílných nástrojů, které mají dostupné v místě výkonu práce.

Konkrétněji se zde primárně hovoří o přístupech na firemní datová úložiště (s přístupy stejnými jako kdyby byl zaměstnanec fyzicky ve firmě), případně o přístupu k aplikacím a programům, které jsou dostupné pouze lokálně z interní počítačové sítě (aplikace nejsou ven do internetu publikované a jsou tedy veřejnosti nepřístupné – většinou z bezpečnostních důvodů). Nemusí se jednat pouze o přístupy, ale také v některých případech o sdílení prostředků či periferií, jako jsou tiskárny, NAS (Network Access Storage – síťové úložiště) či výrobní stroje. Všechny tyto možnosti zajišťuje VPN – Virtuální Privátní Síť.

VPN se nevyužívá pouze k provádění práce z domova a k zajištění přístupů. Ve firemním prostředí lze pomocí VPN zajistit propojení jednotlivých poboček firmy – tyto pobočky jsou poté připojeny do stejné počítačové sítě a komunikují se stejným doménovým řadičem. Výsledkem je to, že počítače všech poboček mohou mít nadiktovánu stejnou doménovou politiku, přestože je každý počítač připojen k jinému poskytovateli internetu.

Další možností použití VPN je připojení počítače do sítě mimo naši republiku, čímž dojde ke změně veřejné IP adresy, pod kterou uživatel vystupuje na internetu. Řada hackerů, ale i běžných uživatelů, této možnosti využívá v internetovém prohlížeči k maskování své skutečné lokace.

VPN sice nabízí možnosti, o kterých řada občanů nemá povědomí, že mohou být realizovány, nicméně v dnešní době, s nástroji, jako jsou například Microsoft RemoteApps, je umožněno některé vlastnosti VPN zajistit jiným, uživatelsky přívětivějším způsobem. Klientská VPN totiž vyžaduje alespoň minimální znalost uživatele o použití. Zaměstnanec není ve firmě fyzicky přítomen, musí proto využít mezikroku – „vytočení“ VPN. V této práci jsou proto popsány také alternativy k VPN, které by pro řadu firem mohly být atraktivní a mnoho IT firem s pokročilejšími znalostmi je pro své klienty nabízí.

2. Cíl práce

Cílem teoretické části této diplomové práce je analýza různých typů VPN (Virtuální Privátní Sítě) a jejich bezpečnostních algoritmů z pohledu bezpečnosti, funkčnosti a složitosti nasazení. VPN jsou dále porovnány s několika alternativami, které jsou v současné době v komerčních firmách velmi rozšířené a předpokládá se jejich další vývoj v nedaleké budoucnosti.

V rámci praktické části je cílem nasazení, tedy konfigurace a zprovoznění, komerčně využívaných VPN na hardwarových zařízeních, která jsou hojně rozšířena a používána v komerčním sektoru. Na vytvořených VPN připojeních poté bude změřena propustnost, šířka pásma a spolehlivost. Naměřené výsledky budou porovnány mezi jednotlivými zařízeními. Výsledkem výzkumu by mělo být zjištění, zdali jsou naměřitelné rozdíly v provozování stejných typů VPN při použití stejných bezpečnostních protokolů a algoritmů, a to na zařízeních od různých výrobců ve srovnatelné cenové relaci.

V práci je dále cílem také zanalyzování alternativního řešení k VPN sítím, které může funkčností i bezpečností pro mnoho firem být vítanou alternativou oproti používání VPN.

3. Metodika

Konfigurace VPN bude provedena na dvou zařízeních od dvou různých výrobců dle doporučení výrobce, manuálů a technické dokumentace. Zařízení budou zapůjčena od společnosti NWS s.r.o. Na zařízeních budou nakonfigurovány SSL a IPsec typy VPN, které jsou k dispozici na obou zařízeních. Konfigurace bude provedena pro remote access VPN, tedy VPN, která slouží k připojení z osobního počítače nebo mobilního zařízení. VPN budou nakonfigurovány na obou zařízeních se stejným zabezpečením, tedy při použití stejných šifrovacích a hashovacích algoritmů, pro co nejspravedlivější porovnání obou výrobců. Měření VPN poté bude prováděno přes počítačové aplikace, které se na analýzu rychlosti, propustnosti a spolehlivosti počítačových sítí specializují. Měřeny budou jak TCP packety, tak UDP packety, porovnány budou také různé velikosti zasílaných packetů (jak pro propustnost, tak pro odezvu (ping). Měření budou prováděna několikrát za sebou, aby bylo vyloučeno momentální vytížení sítě. Měřící aplikace v režimu klienta budou nainstalovány a spuštěny na virtualizovaném počítači s operačním systémem Windows 10 Enterprise (virtuální stroj bude obsluhován hypervisorem VMWare ESXi) v kanceláři Praha 9 – Kbely, měřící aplikace v režimu serveru budou spuštěny na počítači Dell Optiplex s operačním systémem Windows 10 Pro v rodinném bytě v Novém Strašecí. Vzdušná vzdálenost mezi počítači bude cca 50 km. Před provedením konfigurace a měření bude třeba u poskytovatele internetu v Novém Strašecí zajistit pevnou IP adresu a NAT 1:1. Na počátku měření bude přes portál speedtest.net změřena aktuální rychlost na obou přípojkách. Předpokládá se, že rychlost internetu nebude žádným způsobem limitace pro VPN.

Předpokladem je, že budou naměřeny nejen rozdíly mezi jednotlivými typy VPN, ale také se předpokládá nalezení rozdílu ve spolehlivosti či funkčnosti mezi výrobci testovaných zařízení. Posuzována bude také náročnost nasazení a nastavení VPN jak ze strany administrátora, který VPN konfiguruje, tak ze strany uživatele, který si VPN připojení konfiguruje ve svém klientském softwaru.

Pro realizaci alternativního řešení k VPN bude využito prostředí firmy z Hodonína, kde bude nasazena Remote Desktop Gateway, pomocí které bude zajištěno připojení do vnitřní firemní sítě. Na Microsoft Windows Server budou přidány role Remote Desktop services a bude nakonfigurována kolekce aplikací RemoteApps. RemoteApps budou nasazeny do uživatelských počítačů pomocí doménové politiky.

4. Teoretický rozbor

V teoretickém rozboru k diplomové práci Bezpečnostní a provozní analýza komerčně využívaných VPN jsou popsány a vysvětleny základní pojmy, které jsou potřebné k samotnému pochopení toho, co jsou a k čemu se VPN – Virtuální Privátní Sítě používají. Z teoretického hlediska jsou popsány bezpečnostní algoritmy, které jsou využívány v rámci VPN protokolů. Závěrem jsou v této práci rozebrány funkční alternativy, které jsou v současnosti velmi využívané ve firemním sektoru, jelikož nesou stejné vlastnosti, pro které si firmy nechávají zprovozňovat VPN připojení pro své zaměstnance nebo pro své pobočky.

Jak již bylo naznačeno, VPN protokoly popsané v této práci jsou ty VPN protokoly, které jsou používány v komerčním sektoru a patří mezi ty nejčastěji dostupné ke konfiguraci na současných routerech či firewallech, jež jsou nabízeny firmám a organizacím po celém světě.

4.1. Základní pojmy

Následující základní pojmy slouží jako podklad k vysvětlení funkce VPN a zároveň se tyto pojmy vyskytují v praktické části při konfiguraci síťových zařízení. Bez znalosti a pochopení těchto pojmů by nebylo možné zařízení korektně a funkčně nastavit.

LAN

Local Area Network, neboli lokální síť, je počítačová síť, ve které jsou mezi sebou propojovány koncové body na malou vzdálenost (většinou v rámci jedné budovy), za účelem sdílení periferií (tiskáren, skenerů) a k přístupu na interní sdílená úložiště (servery) nebo aplikace. Tato lokální síť je oddělena od dalších počítačových sítí směrovačem (routerem). [40] [41]

WAN

Wide area network, v dnešní době nazývaná Internet, je počítačová síť, pomocí které jsou propojeny koncové body na velkou vzdálenost. Tato počítačová síť překračuje možnosti, které nabízí lokální síť. [40] [41]

Router

Router, neboli směrovač, je fyzické zařízení zapojené do počítačové sítě, pomocí kterého dochází k zjišťování cest v interní síti a k přesměrovávání packetů ze vstupních portů na výstupní porty. [28] [41]

Gateway

Gateway je fyzické zařízení (nejčastěji router nebo firewall), které odděluje lokální síť LAN od externí sítě – další LAN sítě, nebo internetu (WAN). Data z lokální sítě jsou přetvářena do formy, ve které jsou dostupné a čitelné v externích počítačových sítích. Pomocí gateway je tedy možné, aby zařízení z jedné počítačové sítě komunikovala se zařízeními v jiné počítačové síti, a to i pomocí rozdílných protokolů. [40]

Firewall

Firewall je síťové bezpečnostní zařízení, pomocí kterého je monitorována komunikace (jak příchozí, tak odchozí). Pomocí Firewallu je na základě pravidel rozhodováno, zdali bude datový provoz povolen nebo zamítnut. Firewallem je tedy tvořena bariéra mezi zabezpečenou sítí a nedůvěryhodnou externí sítí. [42]

Hlavním rozdílem mezi routerem a firewallem je to, že routerem jsou slepě směrovány (routovány) datové provozy mezi počítačovými sítěmi, kdežto pomocí firewallu je monitorován celý provoz, který se řídí firewallovými pravidly a na základě těchto pravidel je provoz povolen nebo blokován. Mezi další vlastnosti a funkce, které firewally nabízí, patří například Webfilter (filtrování které webové stránky budou povoleny a které zakázány), Quality of Service / bandwidth management (nastavení šířky pásma pro konkrétní klienty), antivirová inspekce a další. [43]

DHCP

Dynamic Host Configuration Protocol je protokol, pomocí kterého je klientovi automaticky poskytnuta unikátní lokální IP adresa, maska sítě a výchozí brána. Pomocí DHCP mohou být klientovi nadiktovány i DNS servery, které má používat. Adresy jsou přidělovány dynamicky, nicméně konkrétním zařízením lze vytvořit rezervaci na konkrétní IP adresu. [60]

DNS

Domain Name System je sada protokolů, pomocí které jsou konkrétním zařízením s IP adresou přiřazovány názvy (hostname). IP adresy jsou pro člověka obtížně zapamatovatelné, a proto jsou doménová jména často upřednostňována před IP adresami. Konkrétní IP adresa může mít přiřazeno i více doménových jmen, nebo také žádné. [2]

FQDN

Fully qualified domain name (plně kvalifikovaný doménový název) je kompletní název zařízení v doméně. Skládá se ze dvou částí - z hostname (jména) a z jména domény. [61]

URL

Uniform Resource Locator je soubor znaků sloužící k identifikaci umístění dat na internetu. Hlavním důvodem používání URL adres je snadná dohledatelnost informace na webu. Každá URL adresa by teoreticky měla odkazovat na unikátní zdroj. [15]

4.2. Referenční model ISO/OSI

Referenční model, značený jako norma 7498, byl vytvořen ISO (International Organization for Standardization – mezinárodní standardizační organizací) roku 1979. [24] Model OSI (Open Systems Interconnection) je možné rozdělit na 7 vrstev (aplikační, prezentační, relační, transportní, síťová, linková a fyzická vrstva) podle jednotlivých kroků v síťovém komunikačním procesu. Tyto vrstvy, po splnění konkrétních úloh, postupně předávají data dalším vrstvám podle toho, zdali se jedná o odesílání či příjem dat – dolů nebo nahoru. Průchozí data tak získávají dodatečně informace, které jsou vkládány každou vrstvou před původní data. [25]

Nejvyšší (sedmou) vrstvou architektury je **aplikační vrstva** [24], do které patří protokoly – např. HTTP (webové dokumenty), SMTP (přenos e-mailových zpráv), FTP (přenos souborů). [26] Hlavním smyslem této vrstvy je interakce mezi aplikacemi a sítí, ale nikoli tvorba uživatelské aplikace. [25] Data jsou z této vrstvy předávána protokolem z uživatelské aplikace dolů – do prezentační vrstvy.

Prezentační vrstva rozbaluje, dekóduje a překládá data do formátů tak, aby jim aplikační vrstva přijímacího počítači rozuměla. Jako příklady je možné uvést kompresi dat

(různé způsoby snížení velikosti dat pro rychlejší přenos s rozdílnými výsledky), kódování dat (aby data nebyla dostupná neautorizovaným osobám) a překlad protokolu (pro umožnění přenosu mezi různými operačními systémy a platformami jsou data konvertována z jednoho protokolu do druhého). [25]

Relační vrstva, která bývá také nazývána session vrstvou, vytváří časové intervaly (relace), kde dochází ke komunikaci mezi procesy aplikací. Pro přenosy má relační vrstva velký význam, protože je v ní řízena jejich synchronizace, přidělovány pověření a jsou zde vytvářeny kontrolní body (potřebné při poruše k navázání na přenos). [24]

Další, a také poslední vrstvou ovlivňující komunikaci koncových systémových prvků, je **transportní vrstva**, která rozkládá data přijatá z relační vrstvy na pakety a síťové vrstvě odevzdává potvrzení o správnosti přijetí. Přes síťovou vrstvu jsou také tvořena či rušena spojení (nebo několik spojení současně) a multiplexována či demultiplexována data mezi transportními spoji koncových procesů. Všechny části zprávy jsou díky této vrstvě správně uspořádány a dostanou se v pořádku k příjemci. [24]

Z rámců se stávají pakety přenosem mezi dvěma uzly, které nejsou přímo spojeny. [27] Aby byly pakety poslány na správné místo, zjišťuje **síťová vrstva** architekturu sítě (vzájemné propojení uzlů), [25] ale také zabezpečuje routování (adresování a směrování) paketů v síti od zdroje k cíli přes několik mezilehlých prvků. [24]

Díky **linkové vrstvě**, která bývá také nazývána spojovou vrstvou, je možné přenášet více rámců. Rámce jsou bity, neboli bloky dat a linková vrstva správně určuje jejich jednotlivé části (včetně začátku a konce) za pomoci služeb fyzické vrstvy. V případě, že dojde k chybě (přijatá podoba rámce není taková, jaká byla vysílána), linková vrstva tuto skutečnost pozná a zažádá o opětovné zaslání rámce. [27] Komunikace na linkové vrstvě probíhá na základě fyzických MAC adres (media access control), které jsou hexadecimálním číslem. Toto číslo má každá síťová karta už od výrobce, většinou se nedá změnit uživatelem, je unikátní a MAC adresy jsou recyklovány výrobci, takže je jen malá šance, že by se v jedné síti mohly nacházet dvě stejné MAC adresy. O jakou konkrétní síťovou kartu se jedná, určují až poslední 3 bajty zadané výrobcem, protože první 3 bajty jsou kódem výrobce (přiděleno organizací IEEE). [25]

Nejnižší vrstvou je **fyzická vrstva**, která jako jediná podporuje fyzickou komunikaci dat mezi systémy – aktivuje, udržuje v aktivním stavu a deaktivuje fyzická spojení přenášející bity. [28] K přenosu bitů komunikačním kanálem dochází v této vrstvě bez ohledu na jejich význam, [25] při zachování jejich posloupnosti (jako při vstupu do vrstvy) – díky identifikátorům k přesnému určení datových okruhů mezi dvěma systémy. [28]

Podstatnými technickými záležitostmi této vrstvy jsou hodnoty napětí (reprezentují logické stavy), délka impulsů (časová délka 1 bitu), význam vysílaných signálů, kontakty a tvary konektorů. [27]

4.3. TCP/IP Protokol

Následující kapitola je důležitá k pochopení, na jakých vrstvách TCP/IP pracují dále popsané VPN protokoly a k pochopení principu zapouzdřování dat.

Protokol TCP/IP (Transmission Control Protocol / Internet Protocol) je sada komunikačních protokolů používána k síťové komunikaci po celém světě. Sada protokolů vznikla v sedmdesátých letech pro ministerstvo obrany USA za účelem sjednocení komunikace v rámci projektu ARPANET. Popsána je ve standardu RCF (Requests For Comment). [2]

Protokol TCP/IP je používán jak v lokálních sítích (LAN), tak na internetu (síti WAN) a není závislý na použitém přenosovém médiu – lze ho používat po UTP kabelu, optickém kabelu, koaxiálním kabelu a dalších. [3]

TCP/IP se skládá ze čtyř vrstev, mezi které patří aplikační vrstva, transportní vrstva, síťová vrstva a vrstva síťového rozhraní. [3] TCP/IP je praktický model vytvořený na základě teoretického modelu ISO/OSI. Rozdíl ve vrstvách TCP/IP protokolu oproti modelu ISO/OSI je tedy v tom, že TCP/IP je složen pouze ze 4 vrstev. [2] Porovnání vrstev TCP/IP s referenčním modelem ISO/OSI je znázorněno v tabulce 1.

<table>
<tr><th>ISO / OSI</th><th>TCP / IP</th></tr>
<tr><td>Aplikační vrstva</td><td rowspan="3">Aplikační vrstva</td></tr>
<tr><td>Prezentační vrstva</td></tr>
<tr><td>Relační vrstva</td></tr>
<tr><td>Transportní vrstva</td><td>Transportní vrstva</td></tr>
<tr><td>Síťová vrstva</td><td>Síťová vrstva</td></tr>
<tr><td>Linková vrstva</td><td rowspan="2">Vrstva síťového rozhraní</td></tr>
<tr><td>Fyzická vrstva</td></tr>
</table>

Tabulka 1 Porovnání ISO / OSI a TCP / IP [2]

4.3.1. Vrstva síťového rozhraní

Jedná se o nejnižší vrstvu TCP/IP modelu. V této vrstvě je sloučena linková vrstva a vrstva fyzická z referenčního modelu ISO/OSI. Vrstva definuje, jakým způsobem jsou data fyzicky odesílána skrze počítačovou síť. Vrstva síťového rozhraní tedy zodpovídá za zapouzdření packetů (dále v kapitole Zapouzdření) do jednotlivých rámců a za zjištění fyzických MAC adres podle IP adres v hlavičce packetu. Mezi protokoly, pracující na 1. vrstvě TCP/IP patří ethernet, token ring a další [8]

4.3.2. Síťová vrstva

Druhá vrstva TCP/IP modelu (též nazývána internetovou vrstvou) je zodpovědná za odeslání dat příjemci z konkrétní sítě, bez ohledu na cestu, kterou packety budou putovat. Vrstva pracuje s IP adresami, díky kterým je schopna identifikovat zařízení na internetu. [8]

Mezi protokoly, které pracují na síťové vrstvě patří IP protokol, ARP protokol (protokol ke zjištění fyzické adresy z IP adresy) a ICMP protokol, který zajišťuje předání informace o úspěchu či neúspěchu v doručení požadovaných dat – pokud je cíl nedosažitelný, dočasně nedostupný nebo jsou data ztracena (timeoutem – vypršením časového limitu, aj.). [8]

4.3.3. Transportní vrstva

Třetí vrstva je zodpovědná za spolehlivost a rychlost doručování dat skrze počítačovou síť. Součástí této vrstvy jsou 2 protokoly: UDP a TCP. [8]

UDP protokol (User datagram protocol)

Transportní protokol UDP umožňuje komunikaci po síti bez nutnosti nastavení komunikačního kanálu předtím, než byla započata komunikace. [13]

Jedná se o jednoduchý protokol, který nedokáže garantovat spolehlivost v doručení zasílaných packetů. Protokol nedokáže zaručit, zdali se přenášená data neztratí, zdali nedorazí do cíle v jiném pořadí, nebo zdali nebudou některá data doručena ve větším množství. [14]

Data jsou posílána v celých blocích, nejsou nijak dělena do menších celků. UDP protokol je využíván v případech, kdy je upřednostňován požadavek na rychlost doručení oproti spolehlivosti doručení. Při užívání transportního protokolu UDP dochází

k zapouzdření dat. Po zapouzdření se UDP packet (datagram) skládá z hlavičky a přenášených dat. Následně jsou datagramy předány síťové vrstvě k přenosu. [13]

Integrita packetů je kontrolována pomocí CRC (Cyclic reduncancy check). Pokud je integrita packetu narušena, packet je vyhodnocen jako ztracený. [13]

UDP protokol se nejčastěji používá pro přenos hlasu a obrazu. Zvukové a obrazové streamovací protokoly jsou navrženy tak, aby při ztrátě packetů došlo pouze k nepatrnému zhoršení kvality. [13]

TCP protokol (Transmission control protocol)

Transportní protokol TCP navazuje spojení mezi dvěma uzly a data posílá po menších celcích. Jeho velkou výhodou je záruka doručení dat, a to i doručení ve správném pořadí. Cílový uzel po doručení dat potvrdí přijetí odesílateli zasláním potvrzovací zprávy. V protokolu TCP tedy probíhá obousměrná komunikace. Další vlastností TCP protokolu je rozlišení dat na aplikační vrstvě – lze z něj snadno určit pro kterou aplikaci jsou data určena. [14] . Vhodná využití transportního protokolu TCP (pro aplikační protokoly) jsou:

- File transfer protocol (FTP) – protokol přenosu dat
- Hypertext transfer protocol (http) – protokol k přenosu webových stránek
- E-mailové protokoly pro příjímání zpráv POP3 (Post office protocol), IMAP (Interactive mail access protocol) a emalový protokol pro odesílání zpráv SMTP (Simple mail transfer protocol)
- Secure shell (SSH) – vzdálené připojení na počítač/zařízení formou konzole. [13]

Z výše uvedeného popisu transportního protokolu TCP je patrné, že UDP obsahuje menší hlavičku a díky tomu je také UDP mnohem rychlejší – bez záruky doručení všech dat ve správném pořadí, protože u UDP neprobíhá zpětná vazba od příjemce k odesílateli, dokonce ani neprobíhá navázání spojení před započetím zasílání dat. [14]

4.3.4. Aplikační vrstva

Aplikační vrstva TCP/IP využívá nižší vrstvu (transportní vrstvu) k přenesení aplikačních dat. Protokoly, které pracují na aplikační vrstvě, lze rozdělit na uživatelské a služební protokoly. [2]

Uživatelské protokoly jsou využívány koncovými uživateli. Mezi tyto protokoly patří protokoly http (hypertext transfer protocol), HTTPS (secure hypertext transfer protocol),

SMTP (simple mail transfer protocol), Telnet, FTP (file transfer protocol), IMAP (Interactive mail access protocol), nebo POP 3 (post office procotol). [2]

Služební protokoly slouží ke komunikaci mezi síťovými prvky (předávání dat, hlášení stavu) a dalšími internetovými protokoly, které podporují jeho funkci. Mezi tyto protokoly patří například SNMP (Simple Network Management Protocol) – protokol, který je používán ke sběru dat z IP zařízení, RADIUS (Remote Authentication Dial-In User Service) – protokol, který je používán k centralizovanému ověření na síti a směrovací protokoly jako IGP (Interior gateway protocol) – protokol, který slouží k výměně informací mezi směrovači. [2]

4.3.5. Zapouzdření

Předtím, než jsou data odeslána ze zdroje k příjemci, dochází k takzvanému zapouzdřování (encapsuling). Aby mohla data putovat skrze IP síť, zapouzdřování je prováděno od nejvyšší vrstvy k vrstvě nejnižší. [7]

Prakticky zapouzdření probíhá tím způsobem, že aplikační data – protokoly HTTPS, e-mailové protokoly jako POP (Post Office Protocol), IMAP (Internet Message Access Protocol), Exchange, protokol pro přenos souborů FTP (File Transfer Protocol) a další, jsou doplněna o aplikační hlavičku a dále jsou zaslána nižší vrstvě – transportní vrstvě. Transportní vrstva rozdělí tato data na více částí, znovu je zabalí a přidá před ně svoji hlavičku – TCP nebo UDP. Tato data se nazývají TCP (nebo UDP) segmenty. Dále jsou data předána síťové vrstvě, která data zapouzdří a doplní je o IP hlavičku – tím vzniká packet (IP datagram). V závěru jsou data předána první vrstvě TCP/IP – vrstvě fyzického rozhraní, kterou jsou před data přidána ethernetová hlavička a patička na konci. V této chvíli se mluví o rámcích a lze říci, že data jsou připravena k odeslání. [7]

Při přijetí dat příjemcem jsou data opět rozbalena směrem od nejnižší vrstvy k vrstvě nejvyšší (tedy od vrstvy síťového rozhraní k aplikační vrstvě). [7]

4.4. Definice VPN a tunnelingu

Virtual private network (virtuální privátní síť) je privátní (zabezpečená) síť zkonstruovaná skrze veřejnou síťovou infrastrukturu (internet). VPN je komunikační prostředí, ve kterém je přístup řízen takovým způsobem, kdy umožňuje spojení mezi uzly pouze pro účastníky, kterým jsou přenášená data určena. K zřízení VPN spojení je využíváno běžné komunikační médium, na kterém je vytvořen šifrovaný tunel (vysvětleno dále) čímž zajišťuje soukromí a bezpečnou komunikaci po internetu. [16]

Mezi výhody uživání VPN patří pro korporátní využití to, že zaměstnanci mohou být připojeni vzdáleně do korporátní počítačové sítě skrze jejich vlastního poskytovatele internetu. Bezpečnost je poté ve VPN zajišťována pomocí šifrovacích a autentikačních protokolů. [39]

Nevýhodou VPN je nemožnost zajištění QoS – quality of service (kvalitu služby). VPN je závislá na internetovém připojení jak serveru, ke kterému se připojuje klient, tak samotného klienta. Je velmi náročné zajistit konkrétní šířku pásma, propustnost mezi komunikujícími stranami není garantována a může docházet k doručení packetů ve špatném pořadí, nebo i ke ztrátám packetů. [39]

4.4.1. Tunneling

Každý VPN protokol potřebuje proces, při kterém je snaha přenést data z jedné interní sítě do druhé interní sítě skrze internet. Tento proces se nazývá tunneling. Součástí tunnelingového protokolu je zapouzdření, rozbalení a přenos dat. [4]

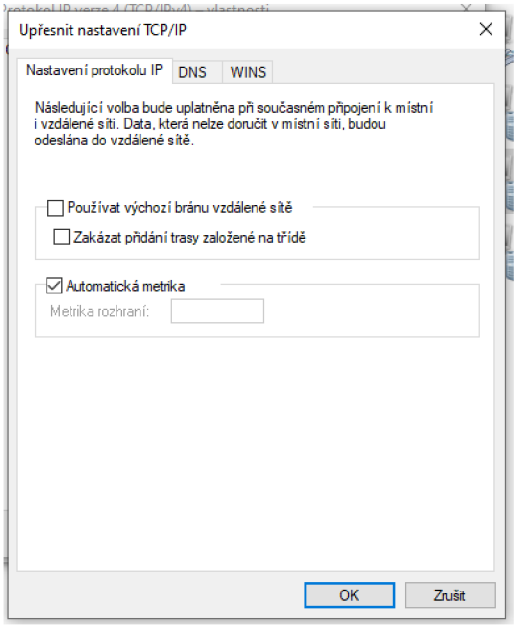
Tunnelingový protokol zapouzdřuje rámce dat a přidává k nim další (vlastní) hlavičku. Zapouzdřená data jsou díky tunnellingovému protokolu dle přidané hlavičky směrována mezi koncovými body po internetu až po směrovač příjemce (ve většině případů končí na WAN adrese routeru/firewallu). Ve chvíli, kdy zapouzdřená data dorazí do cíle, jsou opět rozbalena a dále jsou směrována pomocí originální hlavičky (už v rámci LAN sítě příjemce). Tímto způsobem jsou z nich získána originální data. Logická cesta, která je vytvořena pro cestu dat se nazývá tunel**.** [4]

4.4.2. Split tunneling

Díky split tunnelingu je při vytvoření VPN tunelu umožněno rozhodnout, zdali skrze VPN tunel putují všechna data, nebo pouze část. Při vytvoření VPN tunelu je možné využívat k veškeré komunikaci směrovač (gateway) vzdálené sítě, včetně služeb jako např. DNS (domain name server – překlad síťových adres). Se split tunnelingem je spojována řada bezpečnostních rizik. Hlavním důvodem je to, že uživatel pracuje na nezabezpečené síti a vystavuje tím firemní data nebezpečí. Pokud by byla napadena síť uživatele při zapnutém split tunnelingu, je zde šance ovlivnění i firemní sítě. [36]

Mezi výhody split tunnelingu patří větší výkon sítě pro uživatele, jelikož na komunikaci putující skrze VPN je ve většině případů aplikováno omezení šířky pásma (bandwidth restrictions) nebo i technické omezení rychlosti VPN. [36]

Nastavení split tunnelingu (používat výchozí bránu vzdálené sítě) lze vidět na obrázku 1.



Obrázek 1 Nastavení split tunnelingu na virtuálním adaptéru ve Windows 10 [Zdroj: Vlastní]

4.5. Rozdělení VPN

Virtuální privátní sítě lze podle způsobu použití rozdělit na osobní VPN a firemní VPN. [64] Firemní VPN lze dále dělit podle toho, zda je tunel tvořen mezi dvěma sítěmi, nebo pouze mezi klientským počítačem, na Síť-Síť a Klient-Síť. [65]

4.5.1. Osobní VPN

Osobní VPN jsou nabízeny jako služba, která slouží pro počítačové uživatele k ochraně dat a soukromí při vystupování na internetu. Primárně jde o zajištění anonymity formou skrytí skutečné IP adresy. Tyto VPN jsou používány jak na veřejných sítích (knihovny, restaurace, kavárny atd.), tak i na domácích sítích uživatelů. [64]

Mezi poskytovatele VPN služeb patří ExpressVPN, NordVPN, ProtonVPN a další. [64]

4.5.2. Firemní VPN

Firemní VPN jsou nastavovány pro propojení (na úrovni počítačové sítě) několika poboček firmy, nebo slouží k připojení zaměstnanců z domova (nebo z jiné lokality) do firemní počítačové sítě za účelem přístupu k datům, periferiím, aplikacím, které jsou dostupné pouze z vnitřní firemní sítě. [65]

Klient – Síť (Remote access VPN / Site-Client)

Klient-síť VPN připojení umožňuje bezpečné připojení do lokální sítě z konkrétní klientské stanice – počítače. [1]

VPN klient-síť umožňuje pro organizace a firmy připojení mobilních uživatelů ze vzdálených lokací, jako jsou domovy, hotely, letiště, kavárny tak, jako kdyby byla jejich zařízení fyzicky připojena přímo do firemní sítě. Firmy nemusí přidělovat každému zaměstnanci pracujícímu na home office firemní router, který by byl nakonfigurovaný pro propojení dvou lokálních sítí. Mezi technologie Remote Access patří VPN protokoly L2TP, IPsec, SSL, PPTP a další. [23]

Využívání remote access VPN výrazně snižuje náklady na pořízení hardwaru a také náklady spojené s nastavováním routerů a modemů. [23]

Síť – Síť (Site to Site / Gateway-Gateway)

Site-to-site VPN lze chápat jako VPN mezi routerem a routerem. Nejčastěji se používá k propojení jednotlivých poboček firem. Všechny pobočky mohou být připojeny do jedné a té samé interní sítě – toto se nazývá intranet. V případě, že se site-to-site VPN používá k připojení do sítě jiné společnosti, mluvíme o extranetu. U site-to-site VPN uživatelé na svých stanicích nepotřebují žádnou konfiguraci, o vytočení VPN tunelu se stará jejich router. [1]

Jelikož je Site-to-site VPN založena na komunikaci mezi dvěma routery, jeden router je nakonfigurován jako VPN server a druhý jako klient. Z toho plyne, že router s VPN serverem musí mít pevnou veřejnou IP adresu, aby byl VPN tunel realizovatelný, router klient může mít adresu dynamickou. Komunikace mezi těmito routery začne po autentikaci. [1]

4.6. Bezpečnost VPN

Následující kapitola popisuje šifrovací, hashovací algoritmy a algoritmus výměny bezpečnostních klíčů, které jsou využívány napříč tunnelingovými VPN protokoly, jež jsou popsány dále v této diplomové práci. Tyto algoritmy jsou nezbytnou součástí VPN protokolů k zajištění bezpečnosti přenosu dat a autentikace komunikujících stran.

4.6.1. Šifrovací algoritmy

Šifrovací algoritmus je dvoucestná kryptografická funkce, která má za cíl znemožnit neautorizovaným osobám přístup k datům. Data, která byla zašifrována šifrovacím algoritmem mohou být odšifrována pouze příjemcem, který zná klíč. [32]

DES

DES (Data Encryption Standard – Standard datového šifrování) je algoritmus, který slouží k zašifrování digitálních dat. V algoritmu je využívána 56bitová délka klíče. [47]

3DES

Triple DES je algoritmus, který funguje stejně jako algoritmus DES (tedy 56bitová délka klíče), ale každý blok dat je zašifrován třikrát, přičemž pokaždé jde o nezávislý 56bitový klíč. [47]

AES

AES (Advanced Encryption Standard – Pokročilý šifrovací standard) je šifrovací algoritmus, který rozděluje data po 128 bitech a k jejich šifrování používá 128, 192 nebo 256bitové klíče. [48]

4.6.2. Hashovací algoritmy

Hashovací funkce je kryptografický algoritmus, pomocí kterého je vypočítána hodnota, která je jedinečná pro daný řetězec či zprávu. Z konkrétní zprávy je vždy vypočítána stejná hash. Při hashích tedy nevznikají kolize a nelze vytvořit zprávu, která by poskytla konkrétní hodnotu hashe. [5]

Pomocí hashovací funkce je vytvořen unikátní identifikátor pro konkrétní informaci. Při hashovacím procesu je z čistého textu o libovolné délce provedena konverze do bitové hodnoty o specifické délce. Hashovací funkce je jednosměrný kryptografický algoritmus. [32]

Hashovací funkce jsou používány primárně k zabezpečení informací (například v certifikátech, či ve VPN protokolech). [5]

MD5

Message Digest 5 je hashovací algoritmus, který je používán k autentizaci dat, či ke kontrole integrity dat. Výsledkem MD5 výpočtu je 128bitový řetězec. Typicky je řetězec reprezentován jako 32číslicové hexadecimální (v šestnáctkové soustavě) číslo. [17]

SHA1

Secure Hash Algorithm – Bezpečností Hashovací Algoritmus 1 je algoritmus tvořící 160bitový řetězec. [33] SHA1 je pro svou délku považován za bezpečnější algoritmus než MD5. [23]

Výzkum čínských kryptografů (Xiaoyun Wang a další) dokázal, že MD5 a SHA1 nejsou bezkolizní algoritmy. Díky tomuto zjištění byl vyvinut nový bezpečnější hashovací algoritmus **SHA2.** [23] Secure Hash Algorithm 2 je hashovací algoritmus, který používá různé délky (SHA-256, SHA-384, SHA-512). Jedná se tedy o rodinu hashů s různými délkami generovaného řetezce. [33]

4.6.3. Výměna bezpečnostních klíčů

Diffie-Hellman Key Exchange je algoritmus sloužící k výměně klíčů skrze nezabezpečený kanál. Algoritmus je použit během IKE (Internet Key Exchange). Jde o metodu, která je používána k vytvoření sdíleného šifrovacího klíče, který je dále použit v šifrovacích a hashovacích algoritmech (DES, MD5 atd.). Pouze dvě strany, které jsou součástí DH key Exchange (výměny klíčů algoritmem Diffie-Hellman) mohou odvodit sdílený klíč, ale klíč sám o sobě není nikdy zaslán skrze internet. [47]

4.7. VPN a tunnelingové protokoly

VPN a tunnelingové protokoly jsou tvořeny z různých přenosových protokolů a šifrovacích algoritmů, které se od sebe liší mírou zabezpečení a způsobem, jakým pracují a jakým vytvářejí zabezpečený tunel mezi klientem a serverem. [23]

4.7.1. PPTP

Point to Point Tunneling Protocol je protokol, který umožňuje PPP protokolu (Point-To-Point protocol), aby byl tunelován skrze IP síť. [6] Jedná se o protokol, který pracuje na druhé vrstvě ISO/OSI modelu. [1]

Protokol zajišťuje zabezpečený tunel mezi PPTP klientem a PPTP serverem. Tento klient potřebuje mít nainstalovaný PPTP klientský software, skrz který se nakonfiguruje připojení. PPTP ke své funkci používá Generic Routing Encapsulation (GRE), jako transportní protokol pracující na portu 47. GRE zajišťuje zapouzdření dalších síťových vrstev tak, že je možné je přenášet po internetu. PPTP dále ke své funkci používá TCP port 1723. [1]

Původní verze protokolu PPTP obsahovala vážné bezpečnostní nedostatky, které byly pouze částečně odstraněny v druhé verzi tohoto protokolu. PPTP by tedy z bezpečnostních důvodů měl být používán velmi obezřetně. [1]

Point to Point protokol (**PPP**) je TCP/IP protokol, který slouží k propojení jednoho počítače s druhým skrze lokální síť, nebo také internet. Ke komunikaci mezi dvěma počítači, které jsou propojeny síťovým kabelem, je vždy použit protokol PPP. Mezi autentikační protokoly PPP se řadí protokoly PAP, CHAP a MS-CHAP. [49]

PAP

Password Authentication Protocol (protokol autentikace hesel) slouží k ověření identity (handshake) mezi komunikujícími stranami (peery). Při vytváření připojení je autentikačním systémem rozhodnuto, zdali bude pokračovat v připojení nebo jej ukončí, a to na základě uživatelského ID a hesla, které je mu zasláno vzdálenou stranou. Uživatelské ID a heslo je odesíláno v čistě textové podobě – v žádné fázi nejsou tato data šifrována. Z tohoto důvodu je protokol PAP velmi náchylný na útoky hackerů. [21]

CHAP

Challenge Handshake protocol (protokol výzvy k podání ruky) je protokol, pomocí kterého je periodicky ověřována identita komunikující strany. Po navázání spojení je z autentikačního systému odeslána výzva komunikující straně, aby prokázala svou totožnost. Komunikující strana (peer) odpovídá odesláním hodnoty hashe (vytvořena hashovací funkcí MD5 – Message Digest 5). Autentikačním systémem je dále ověřena hodnota hashe a pokud hodnota nesedí, komunikace je ukončena. Identita je nadále ověřována v náhodných intervalech po celou dobu spojení. [22]

MS-CHAP

Microsoft Challenge Handshake Protocol (Microsoft verze protokolu CHAP) je protokol, který je podporován protokolem PPP (Point to Point protocol) a využíván ve VPN protokolu PPTP. Funkčně je protokol podobný protokolu CHAP, ale liší se ve formátu packetu, který je ve formátu, který byl specificky vytvořen tak, aby vyhovoval operačním systémům Microsoft Windows. [37]

V protokolu MS-CHAP verze 2 je podporována dvousměrná autentikace, a také oddělení kryptografických klíčů pro data, která byla přijata a pro data, která byla vysílána. [37]

4.7.2. L2TP

L2TP (Layer 2 Tunneling Protocol – Tunnelingový protokol na druhé vrstvě) je protokol, který vznikl z PPTP a (jak z názvu vyplývá) pracuje na druhé vrstvě ISO/OSI modelu – linkové vrstvě. V modelu TCP/IP pracuje na vrstvě první – vrstvě síťového rozhraní. K funkci L2TP je využíván UDP port 1701. Tento protokol umožňuje více připojení skrze stejný tunel, na rozdíl od protokolu PPTP. [1]

Protokol sám o sobě v sobě nemá zahrnuto naprosto žádné zabezpečení. Proto se ve většině případů používá společně s IPSec (Internet Protocol Security), které umožňuje chránit IP komunikaci na síťové vrstvě TCP/IP – popisuje se jako L2TP/IPsec (L2TP over IPsec). [38]

Mezi nevýhody L2TP patří fakt, že poskytovatel internetu nemusí mít ve své infrastruktuře L2TP povolený. Od operačního systému Microsoft Windows 2000 má L2TP nativní podporu jako remote access protokol. [23]

L2TP je možné provozovat ve dvou modelech. V nuceném modelu (compulsory tunnel model) a v dobrovolném modelu (voluntary tunnel model). [23]

U **voluntary tunnel** modelu je spojení vyvoláno ze vzdálené uživatelské stanice, použitím L2TP klientského softwaru. Uživatelské L2TP packety jsou zaslány poskytovateli internetu a jím jsou přesměrovány do vzdálené počítačové sítě. Poskytovatel internetu nemusí přímo podporovat L2TP. [23] U voluntary tunnel modelu tunel začíná u klientského počítače a končí u korporátní sítě. [34]

U **compulsory tunnel** modelu je vzdáleným počítačem inicializováno připojení k poskytovateli internetu. L2TP spojení mezi vzdálenou sítí (korporátní sítí) a počítačem uživatele je poté vytvořeno poskytovatelem internetu. [23] Poskytovatel internetu musí L2TP podporovat, tunel zde začíná u korporátní sítě a je ukončen u poskytovatele internetu. Uživatel tedy navazuje PPP komunikaci s poskytovatelem internetu a L2TP komunikaci zajišťuje poskytovatel (LAC) s LNS – síťovým serverem korporátu. [34]

L2TP v compulsory (nuceném) tunnel modelu

LAC (L2TP access concentrator) – L2TP koncentrátor přístupu se nachází mezi LNS (L2TP network server) a uživatelským počítačem. Úkolem LAC je přenos packetů mezi LNS a uživatelem formou zapouzdření packetů, které získal od uživatele a rozbalení packetů pro uživatele, které získal od LNS. Z logického hlediska je LAC koncovým bodem pro LNS, kde jsou data zasílána skrze L2TP tunel. [35]

LNS (L2TP network server) – L2TP síťový server je koncovým bodem L2TP tunelu a je jednou z komunikačních stran pro LAC. LNS je tedy vlastněný organizací do které je prováděno připojení. Koncový uživatel nemusí vědět, že existuje tunel mezi LAC a LNS serverem jeho firmy. [35]

L2TP over IPsec

Jak již bylo zmíněno, součástí Microsoft Windows je vestavěný VPN klient, který umí podporovat L2TP. Ve většině případů je k zabezpečení dat použit IPsec. V L2TP over IPsec (psáno také jako L2TP/IPsec) je připojení mezi klientskou stanicí a cílovým směrovačem zajištěno v následujících sedmi krocích:

1. Uživatel je připojen k směrovači poskytovatele internetu a získává od něj IP adresu.
2. L2TP klient je spuštěn uživatelem a nakonfigurován k použití IPsecu
3. Pro klientskou stanici je vynuceno spojení a je prováděno vyjednávání zabezpečeného kanálu k výměně klíčů (dále popsáno v kapitole 4.7.3.4 Fáze protokolu IKE: Fáze 1)
4. Jsou vytvořeny dva zabezpečené kanály za účelem šifrování dat a autentifikaci (dále popsáno v kapitole 4.7.3.4 Fáze protokolu IKE: Fáze 2).
5. V pátém kroku je inicializováno L2TP spojení uvnitř IPsecu.
6. Uživatelské ověřovací údaje jsou použity k validaci L2TP spojení.
7. L2TP uživatelské packety jsou zapouzdřovány L2TP a šifrovány pomocí IPsecu.

[23]

4.7.3. IPsec

IPsec, Internet Protocol Security (Internetový bezpečnostní protokol) je sada protokolů, která slouží k zabezpečení komunikace na síťové vrstvě TCP/IP (třetí vrstva referenčního modelu ISO/OSI). Součástí sady protokolů IPsec jsou protokoly, které slouží k autentizaci (navzájem mezi komunikačními body) a vyjednání/domluvení se na formě šifrování (domluvení se na šifrovacím algoritmu). [54] IPsec tedy zajišťuje:

- Výměnu šifrovacích klíčů
- Přidání hlaviček a patiček k packetům
- Autentifikaci komunikačních stran (PSK, RSA)
- Šifrování (DES, 3DES, AES)
- Zajištění integrity přenášených dat (MD5, SHA)
- Přenos packetů
- Dešifrování na konci komunikace

[50]

Před vytvořením bezpečného tunelu se obě strany musí dohodnout na parametrech přenosu – tzn. na protokolech, které budou použity. [50]

4.7.3.1. Security Associations (SA)

Zabezpečená komunikace je založena na konceptu zvaném Security Associations (bezpečnostní asociace). SA specifikuje bezpečnostní nastavení, které je určené komunikujícím stranám. Každá komunikující strana má dvě IPsecové SA – pro odchozí packety a pro příchozí packety. Navíc si každá komunikující strana uchovává databázi aktivních SA (pro odchozí i příchozí směry) a na základě této databáze je při odesílání nebo přijímání packetů rozhodnuto, jaké autentikační a šifrovací parametry budou aplikovány. [39]

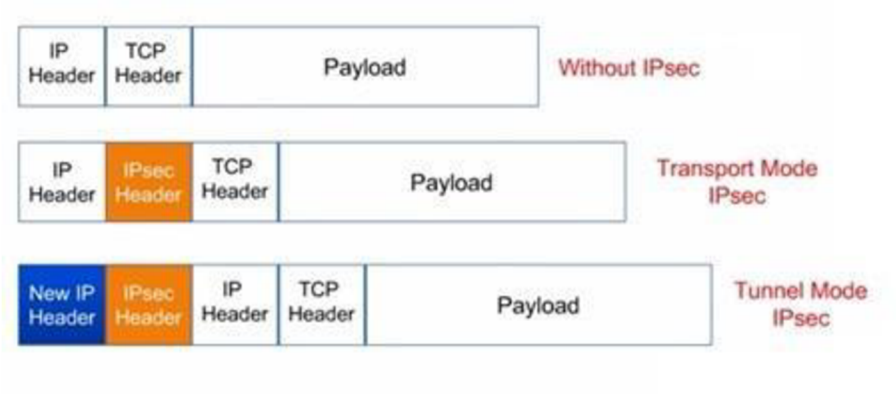
4.7.3.2. Režimy IPsecu

Režim přenosu (Transport mode)

V transportním módu jsou zapouzdřena pouze přenášená data. Používá se k propojení dvou bodů (dvou počítačů) nebo k propojení počítače a směrovače (end-station – gateway). Mezi IP hlavičku a TCP hlavičku se vloží ESP nebo AH hlavička. Původní IP hlavička je tedy použita pro směrování. V transportním módu jsou šifrována data již od zdroje – již od počítače, který se zůčastnil vytváření tunelu. [18]

Režim tunelu (Tunnel mode)

Tunelový mód je používán častěji, než transportní mód. Používá se převážně k propojení dvou směrovačů (gateway to gateway VPN/ Site-to-site VPN). V tunelovém režimu je zapouzdřen celý původní paket, je před něj přidána ESP nebo AH hlavička a dále nová IP hlavička, podle které je paket směrován. Šifrování dat je zajištěno pouze v tunelu, tzn. že dokud se data nedostanou ke směrovači, nejsou šifrována. [18] Režimy IPsec jsou znázorněny na obrázku 2.



Obrázek 2 Režimy IPSec [Zdroj: rfwireless-world.com]

4.7.3.3. IKE (Internet Key Exchange)

IKE je jedním z primárních protokolů použitým v IPSec. V IPSecu zajišťuje bezpečnostní vyjednání mezi dvěma body (**peery**) formou výměny klíčů, pomáhá vyjednat SA (**Security Association**). Protokol IKE ke své funkci používá aplikační rámec, tedy framework **ISAKMP** – Internet Security Association and Key Management Protokol. Protokol IKE využívá dvou bezpečnostních protokolů, a to Authentication Header a Encapsulating Security Payload. [19]

Authentication Header (AH)

Protokol zajišťuje autentizaci zdroje dat a integritu dat, ale nezajišťuje žádné šifrování. Funkcí tohoto protokolu je, že před zasílaná data přidává AH hlavičku a po zaslání packetu skrze internet je na druhé straně kontrolována nejen AH hlavička, ale také vnější IP hlavička – veřejná IP adresa zdroje. [51]

Encapsulating Security Payload (ESP)

Protokol ESP, stejně jako Authentication header, zajišťuje integritu dat, autentifikaci, ale také šifrování. Jak plyne z názvu – protokol ESP zajišťuje zapouzdření dat (tedy zapouzdření IP hlavičky třetí vrstvy ISO/OSI) do ESP hlavičky, díky čemuž jsou originální data i originální IP hlavička bezpečně zapouzdřeny a na druhé straně je kontrolována pouze ESP hlavička. Vnější IP hlavička je při kontrole vynechávána, což znamená, že pokud packet přijde z jiné veřejné IP adresy, protokol ESP tento fakt ignoruje. [52]

V mnoha případech jsou použity oba protokoly (AH a ESP) zároveň – Integrita dat a autentizace je zajišťována protokolem AH a šifrování je zajištěno protokolem ESP. [52]

4.7.3.4. Fáze protokolu IKE

Protokol IKE se skládá ze dvou vyjednávacích fází – takzvaně IKE fáze 1 a fáze 2. IKE fáze 1 využívá dva módy, a to Main mode a Agressive mode. IKE fáze 2 používá pouze jeden mód, který se nazývá Quick mode. [19]

IKE fáze 1

První fáze slouží k autentikaci účastnících se stran, vyjednání jaké protokoly budou použity a k vytvoření bezpečného kanálu.V této fázi IKE dochází k vyjednání pěti parametrů: Hashovací funkce, Autentikaci, Skupinu klíčů Diffie-Hellman, Dobu života vytvořeného kanálu (lifetime) a Šifrování. Výsledkem fáze 1 je vytvořený tunel, který slouží k vyjednání fáze 2, a jsou vytvořeny IKE Security Associations. Komunikace mezi dvěma body je na konci této fáze zajištěna na UDP portu 500. [19]. IKE fáze jedna má dva módy: Main mode a Agressive mode. [19]

Main mode zahrnuje tři dvoucestné výměny mezi iniciátorem a příjemcem. Celkově je tedy vytvořeno 6 zpráv. V první výměně dochází k výměně algoritmů a hashí použitých k zabezpečení další komunikace. Po odsouhlasení IKE SA oběma stranami se přechází k druhé výměně. V druhé výměně se používá Diffie-Hellman k vygenerování sdílených klíčů. Ve třetí výměně dochází k potvrzení identity obou stran. Potvrzovaným parametrem je IP adresa v šifrované formě. [19]

V Agressive módu jsou celkově zaslány 3 zprávy. V první výměně dojde k zaslání téměř všeho z IKE SA. Příjemce zašle vše zpět iniciátorovi a ten potvrdí, že došlo k výměně. Slabinou Agressive módu IKE je to, že dojde k výměně informací ještě předtím, než byl vytvořen zabezpečený kanál. Výhodou oproti Main módu je rychlost. [19]

IKE fáze 2

Cílem druhé fáze IKE je vyjednání IPSec Security Associations za účelem vytvoření tunelu. V druhé fázi probíhají následující procesy:

- Vyjednávání IPSecových SA, které jsou chráněny již existujícími IKE SA
- Vytvoření IPSecových SA
- Cyklické znovu-vyjednávání IPSecových SA za účelem neustálé bezpečnosti
- Občasná výměna Diffie-Hellman klíčů

[19]

IKE fáze 2 má mód, který se nazývá rychlý (quick mode). Quick mode, po vytvoření tunelu v IKE fázi 1, vyjednává sdílené IPSecové pravidla, odvozuje sdílené klíče použité pro bezpečnostní algoritmy a vytváří IPSecové Security Associations. [19]

Quick mode je také používán k vyjednání nových IPsecových SA, pokud současným vyprší životnost (expirují). [19]

4.7.4. SSL VPN

SSL VPN poskytuje nejen bezpečnou komunikaci díky šifrování pro jakékoliv typy zařízení, ale také téměř nulovou nutnost konfigurace. Tento typ VPN využívá webový prohlížeč (typicky port 443) k připojení do vzdálené sítě a k aplikacím, které mohou, ale nemusí být webové. [12]

Z teoretického hlediska se SSL VPN nachází mezi transportní a aplikační vrstvou OSI modelu. [23]

Administrátoři mohou pro klienty omezit využití VPN – připravit prostředí, které běží v prohlížeči a uživatelé mohou používat webové aplikace, které nejsou volně dostupné z internetu, pouze ze vzdálené lokální sítě. [12]

Další možností připojení je využívání aplikace (softwaru) poskytnutého výrobcem. Uživatel se poté ověří jménem a heslem, bez nutnosti jakékoliv další konfigurace na straně klientského počítače. [12]

SSL VPN tedy nese výhodu v jednoduchosti konfigurace, nezávislosti na zařízení. Další velkou výhodou je, že pro svou funkci vyžaduje pouze port 443 (HTTPS) – tzn. Port, který je na straně směrovače/firewallu, či na straně poskytovatele, blokován ve velmi málo případech. Jediným rizikem používání SSL VPN je právě internetový prohlížeč. Neustále je zde riziko malwaru a dalších útoků. [12]

Protokol SSL/TLS

Secure Sockets Layer (vrstva bezpečných socketů) je kryptografický protokol, který zajišťuje zabezpečenou komunikaci na internetu. Nejčastěji je využíván na zabezpečených webových stránkách (HTTPS). Je vložený mezi transportní a aplikační vrstvu TCP/IP, lze jej tedy také nazvat vrstvou. [9]

Protokol využívá asymetrickou šifru, kdy klient i server mají veřejný a privátní klíč. Odeslané zprávy jsou zašifrovány pomocí veřejného šifrovacího klíče, příjemce poté zprávu rozšifruje pomocí svého privátního klíče. [11]

Následovníkem protokolu SSL je protokol TLS (Transport Layer Security – zabezpečení vrstvy transportní), který má nyní již verzi 1.3. [9]

Verze TLS 1.1 již není považována za bezpečnou, nicméně starší multifunkční zařízení (jako starší síťové tiskárny) novější protokol nepodporují. [9] Například firma Microsoft v prostředí Office 365 pro zasílání e-mailů z multifunkčních zařízení vyžaduje TLS verzi 1.2. [10]

5. Komerčně využívané alternativy k VPN

V následující kapitole jsou popsány podnikově využívané alternativy, které umí plně nahradit požadavky na VPN, a to jak po funkční stránce, tak po uživatelské stránce (jednoduchost a pochopitelnost uživatelů při užívání).

5.1. Remote Desktop Gateway (RD Gateway)

Jak je dále vysvětleno v kapitole 5.1.1 níže, protokol Remote Desktop (RDP) je používán pro ovládání grafického rozhraní počítače ze vzdálené lokace. V operačním systému Windows Server 2008 R2 bylo poprvé zahrnuto řešení Remote Desktop Gateway. Toto řešení využívá protokolu HTTPS (port 443) k vytvoření zabezpečeného šifrovaného připojení. Remote Desktop Gateway zajišťuje směrování provozu z klienta, skrze zmíněný port 443 do vnitřní sítě, ve které je zajištěn přístup k prostředkům a počítačům pomocí protokolu RDP – port 3389. Komunikace mezi klientem a RD Gateway je po celou dobu připojení šifrována díky protokolu HTTPS. [45]

Nevýhodou VPN oproti RD Gateway je to, že ve výchozím nastavení VPN umožňuje přístup k jakémukoli zařízení či aplikaci na úrovni síťové infrastruktury. RD Gateway pro přístup užívá autorizační pravidla a bezpečnostní skupiny, pomocí kterých je specifikováno, k jakému zařízení a aplikaci má konkrétní uživatel přístup. V případě, že je uživatel ověřen vůči RD Gateway, ale není autorizován k využívání prostředků za RD Gateway, zabezpečený tunel mezi klientem a RD Gateway není vytvořen, uživateli je zamítnut přístup a spojení je ukončeno. [45]

Útočník by tedy při útoku na RD Gateway musel znát práva a přístupy konkrétního uživatele, aby se naskytla příležitost k prolomení zabezpečení, které je zabezpečené a šifrované pomocí SSL (Secure Sockets Layer) v rámci HTTPS protokolu. [45]

Další nevýhodou VPN oproti RD Gateway je to, že v rámci VPN mohou nastat kolize IP rozsahů. Množství lokálních IP adres je omezené a je zde značná šance, že adresa vzdálené sítě, do které se klient připojuje, bude kolidovat s adresami v interní síti klienta. [46]

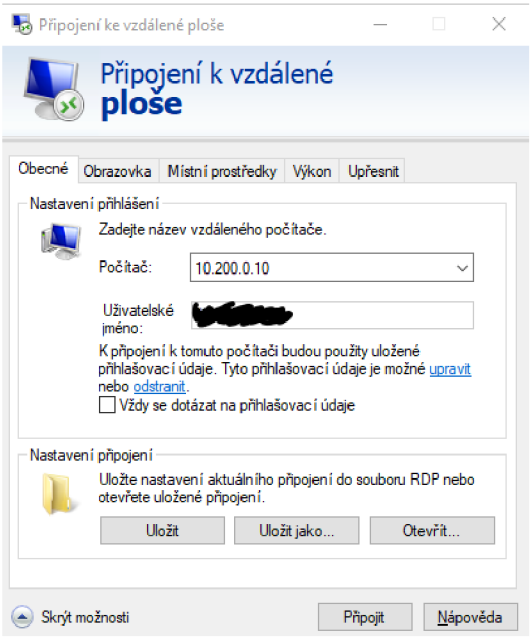
5.1.1. Remote desktop protokol (RDP)

Protokol vzdálené plochy je protokol vyvinutý firmou Microsoft, který umožňuje připojení na jiný počítač skrze počítačovou síť. Součástí RDP protokolu je grafické rozhraní, díky kterému je užívání protokolu i neznalému uživateli velmi blízké. [14]

Protokol RDP mimo jiné zajišťuje přenos dat, sériovou komunikaci mezi zařízeními (i periferiemi – na vzdáleném PC se mohou zobrazovat jako „redirected“ – tedy přesměrované z počítače, který vyvolal připojení) a šifrování dat (včetně šifrování aktivity klávesnice a myši). [14]

Protokol ve výchozím nastavení pracuje na TCP a UDP portu 3389. K chodu protokolu (k připojení na vzdálený počítač/plochu) je zapotřebí software – na straně klienta i serveru. Klientský software existuje pro celou řadu operačních systémů – Windows, Linux, Unix, Mac OS, iOS, Android a další. [14]

RDP protokol je stále rozvíjen a historicky se nachází v několika verzích. Novější verze nabízí větší možnosti zabezpečení, či sdílení (kupříkladu právě zmíněných periferií). Např. verze 6.0 je možné využívat Network Level Auhentication – Autentifikaci na úrovni sítě, díky čemuž lze ověřit klienta ještě předtím, než je na server/vzdálený počítač připojen. [53] V současné době je aktuální verze protokolu Remote Desktop 10.0. [57] Aplikace (klienta) protokolu Remote Desktop v operačním systému Windows 10 je zobrazena na obrázku 3.



Obrázek 3 Připojení k vzdálené ploše – klient Windows 10 [Zdroj: vlastní]

5.1.2. Remote desktop services

Remote Desktop Services jsou technologie, které umožňují uživatelům připojení na virtuální plochu, k RemoteApps, a nebo na session-based plochu (vysvětleno dále). [58]

5.1.2.1. Session-based desktop

Session-based plocha je zajišťována operačním systémem Windows Server. Tato technologie se chová stejně, jako více uživatelských účtů na jednom a tom samém počítači. V této technologie tedy nemá každý uživatel vlastní virtuální operační systém, ale pouze svou instanci plochy, ke které se připojuje skrze počítačovou síť. Všichni připojení uživatelé pracují na stejném operačním systému, tedy na jednom konkrétním Windows serveru, tím pádem uživatelé mají přístup ke stejnému systému souborů. [55]

Součástí session-based desktop jsou RemoteApps, které umožňují nasazení aplikace na uživatelská zařízení. Tato aplikace není spuštěna na uživatelském zařízení, ale na vzdáleném serveru (na serveru, na kterém je aplikace nainstalována) jako session-based desktop aplikace, nicméně uživatel vidí a ovládá pouze konkrétní aplikaci. Uživatel tedy nemusí vědět, že aplikace není nainstalována u něj v počítači. Kromě toho, uživatel nemusí řešit žádné vytáčení VPN či konfiguraci na routeru/firewallu, pouze aplikačním zástupcem spustí aplikaci a ta se pro uživatele tváří jako kdyby byla lokálně nainstalována na jeho počítači. [58]

5.1.2.2. Virtual desktop

Virtuální plocha umožňuje vytvoření virtuálního operačního systému pro každého připojeného uživatele. Výsledkem je striktní izolace systémů souborů mezi uživateli – každý virtuální operační systém má svůj vlastní souborový systém, přidělenou paměť, přidělené úložiště, virtuální procesor a další. Chování virtual desktop je tedy velmi podobné tomu, jako když každý uživatel má vlastní počítač, na kterém pracuje. Hlavním rozdílem je ale to, že uživatel může tento operační systém i s aplikacemi užívat odkudkoliv ze světa – bez fyzické přítomnosti u konkrétního počítače. [55]

Výhody a nevýhody Session-based desktop

Hlavní výhodou session-based plochy je jednoduchost konfigurace a nasazení. To s sebou přináší řadu nevýhod:

- Nižší bezpečnost, jelikož uživatelé sdílí jeden a tentýž operační systém. Uživatelé tedy nejsou od sebe striktně odděleni, hackeři či viry se mohou skrze jeden uživatelský účet dostat k datům dalších účtů.
- Nelze vytvořit zálohovací image (kopii disku) pro konkrétního uživatele. V případě nutnosti přenosu session-based desktopu z jednoho serveru na druhý je nutné buď kopírovat celý server, nebo remote desktop services nastavit znovu.
- Uživatelé sdílí stejné systémové prostředky, tzn. že pokud jeden uživatel vytíží svou prací procesor (nebo jinou část počítače), jsou jím ovlivněni i ostatní uživatelé. [55]

Obecně se doporučuje užití session-based desktop v prostředích, kde je používáno pouze několik aplikací, které mají být dosažitelné skrze počítačovou síť. [55]

Výhody a nevýhody Virtual desktop

Virtuální plocha přináší řadu výhod, ale také složitější nastavení a konfiguraci. Mezi tyto výhody patří to, že každý uživatel má přidělené vlastní systémové prostředky a virtual desktop se poté tváří a chová jako fyzický počítač. To znamená, že jeden uživatel svým užíváním neovlivňuje počítačový výkon druhého uživatele, a to i v případě, že vyčerpá všechny jemu přidělené systémové prostředky. [55]

Bezpečnost je výrazně zvýšena, jelikož uživatelé pracují v separovaných (či oddělených) prostředích – nemůže dojít k neautorizovanému přístupu k datům jiného uživatele. [55]

Každou virtuální plochu lze zálohovat zálohovacím softwarem, lze vytvářet image konkrétní plochy stejně jako při zálohování operačního systému. [55]

Mezi nevýhody patří náročnější licencování – je třeba zalicencovat jednotlivé instance virtuálních ploch podobně jako operační systém. [56]

5.1.2.3. Role Remote Desktop Services

K zajištění funkčnosti Remote Apps je třeba nainstalovat na jeden nebo na více serverů následující role.

Remote Desktop Session Host (RDSH)

RDSH zastává roli terminálového serveru. Jsou na něm nainstalovány aplikace a virtuální plochy, které využívají připojení uživatelé. Uživatelé se k těmto plochám a aplikacím připojují pomocí Remote desktop klientů (tedy aplikací), které běží na jejich vlastním počítači, nebo mobilním zařízení. Operační systémy Microsoft Windows, MAC OS, iOS a Android mají v sobě integrované takovéto aplikace, nebo jdou jednoduše doinstalovat. Další možností je připojení je skrze internetový prohlížeč – remote aplikace je vyvolána skrze internetový prohlížeč, ale poté se jeví, jako kdyby běžela přímo v operačním systému uživatele. [20]

Aplikace a plochy mohou být organizovány do celků mezi několika servery. Tyto celky se nazývají kolekce (Collections). Kolekce v sobě obsahují jednotlivé aplikace, kdy přístupy k nim jsou řízeny konkrétními bezpečnostními skupinami uživatelů v doméně. [20]

Remote Desktop Connection Broker (RDCB)

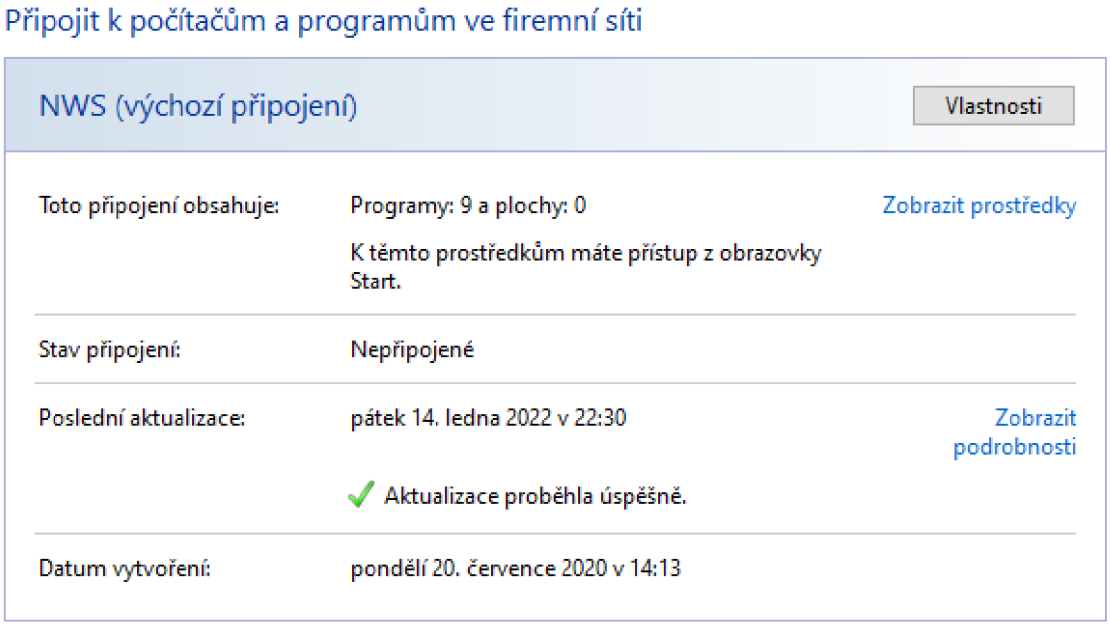
RDCB směruje přicházející žádosti o vzdálené připojení na konkrétní RDSH servery. Pomocí RDCB je rozhodnuto, ke které kolekci má být uživatel nasměrován. Nelze opomenout důležitou vlastnost, že RDCB zajišťuje také vyvážené vytížení (load balancing) RDSH serverů (v případě, že se používá více RDSH serverů najednou). Pro jednotné přihlášení uživatelů k vzdáleným aplikacím a plochám (single sign on) je třeba, aby RDCB server i klient měli nainstalovaný certifikát. [20]

Remote Desktop Gateway (RDGW)

RDGW zajišťuje připojení k vzdáleným aplikacím a plochám z veřejné sítě – z internetu. K šifrování komunikačního kanálu mezi klientem a serverem je využíván protokol SSL – Secure Sockets Layer. Remote Desktop Gateway je takový server, který musí být dosažitelný z internetu skrze veřejnou IP adresu a musí umožňovat TCP připojení na portu 443 (SSL) a UDP připojení na portu 3391. K funkčnosti je opět za potřebí, aby server i klient měli nainstalovaný digitální certifikát. [20]

Připojení k aplikacím a k firemním prostředům, které má konkrétní uživatel podle svých práv k dispozici, lze do počítače přidat pomocí RDP feedu (někdy psaný jako RDS feed) – lze vidět na obrázku 4 níže. [59]

RDP Feed je URL adresa, která vede k souboru, který má ve výchozím nastavení Remote desktop services cestu https://rdweb.contoso.com/RDWeb/Feed/webfeed.aspx (namísto contoso je název domény). [59]



Obrázek 4 Připojení k firemním aplikacím ve Windows 10 [Zdroj: vlastní]

5.1.2.4. Licencování RDS

Licencování je řešeno buď na úrovni uživatelů, nebo na úrovni zařízení (počítačů, které se připojují). Každý uživatel, který využívá služby Remote Desktop, tedy vytváří session se serverem, potřebuje Client Access licenci (CAL). Během připojování uživatele k RDSH serveru, RDSH server si vyžádá RDS CAL licenci z Remote Desktop licenčního serveru. [68]

V rámci licencování je k dispozici 120 dní bezúročné období, během kterého není žádná RDS licence potřebná. [68]

RDS CAL licence jsou kompatibilní pouze od novější verze ke starší, starší verze CAL licencí nelze na nových serverech používat. [68]

5.2. Citrix Files, Citrix Virtual Apps

Firma Citrix Systems nabízí cloudovou službu, která poskytuje firemní aplikace skrze internet. Citrix server používá Microsoft Remote Desktop Services infrastrukturu k nasazení virtuálních aplikací uživatelům. Aplikace jsou tedy pro uživatele dostupné online a pro firmy to znamená ušetření finančních prostředků, jelikož poté není potřeba centralizace ve vnitřním firemním prostředí a ve specifických případech i k zvýšení bezpečnosti. [67]

5.3. SD-WAN

Díky Software Defined Wide Area Network – softwarově definovaným WAN byla nastíněna nová perspektiva k budování počítačových sítí. Formou SD-WAN je zjednodušeno budování spojení mezi pobočkami stejné organizace. Skrze SD-WAN je možné centrálně nastavit síťové politiky (network policies), bez nutnosti manuální konfigurace každého směrovače či firewallu na síti. [29] V neposlední řadě je umožněno zajistit požadovanou QoS (Quality of Service – kvalitu služby) pro konkrétní aplikace, uživatele nebo lokace [29], snazší propojení data center s nižší latencí. [31]

Síť může být spravována správci sítě skrze standardizované aplikační rozhraní (API) nehledě na výrobce síťového zařízení. [30]

SD-WAN dokáže řídit několik připojení a dynamicky směrovat určitou komunikaci tou nejrychlejší a nejbezpečnější cestou. Díky tomu dokáže zajistit redundanci a snížit náklady na propojení v síti. [31]

Bezpečnost je u SD-WAN řešena jak pro administraci, tak pro komunikaci s cloudovým kontrolorem a také na úrovni dat. Routery, které jsou součástí SD-WAN, mají v sobě zabudované ochranné mechanismy, pomocí kterých je řešena bezpečnost jednotlivých poboček při přistupování na internet. [66]

Mezi tyto ochranné mechanismy patří firewall, ochrana a detekce narušení, filtrování obsahu a další. Před připojením zařízení do SD-WAN se každé zařízení musí ověř vůči cloudovému kontroloru. Přístupy jsou vázané na role a uživatelské skupiny, řešena je politika hesel, pravidelné aktualizace softwaru. [66]

6. Praktická část

V praktické části bylo realizováno měření dvou typů VPN na dvou různých zařízeních. Na závěr bylo provedeno nakonfigurování Microsoft Remote Desktop Gateway a RemoteApps.

6.1. Realizace měření VPN

V technické dokumentaci, na školeních či ve výukových videích výrobců routerů a firewallů se představují návody na to, jak nakonfigurovat konkrétní VPN. Cílem praktického měření bylo porovnat VPN řešení od několika výrobců firewallů (routerů), které je standartně používané v komerčních firmách a najít, zdali jsou naměřitelné rozdíly v provedení nebo kvalitě mezi stejnými VPN technologiemi od různých výrobců, kteří nabízejí produkty ve srovnatelné cenové relaci.

Zařízení, na kterých bylo nakonfigurováno několik typů VPN, byla od firmy Fortinet (Fortigate) a od firmy Zyxel.

Výsledkem praktické části byly naměřené rychlosti a odezvy, díky kterým lze říci, zdali řešení některého výrobce je vhodnější a jaké jsou rychlostní a provozní rozdíly mezi dvěma typy VPN. Cílem bylo nasimulovat prostředí tak, jako se zaměstnanec připojuje vzdáleně ze svého domova (nebo z jiného místa) do interní sítě svého zaměstnání. Nakonfigurovány tedy byly remote access VPN (VPN typu client-server, tedy připojení uživatelského počítače do firemní sítě), které vybrané firewally nabízejí. Měření bylo prováděno mezi dvěma koncovými body ve dvou různých lokalitách s dvěma různými konektivitami. Strana, na které byla spuštěna měřící aplikace v klientském režimu je dále nazvána Client a strana, na které byla měřící aplikace spuštěna v serverovém režimu je dále nazývána Server. Měření rychlosti a propustnosti tedy probíhalo směrem od klienta k serveru, kdy klient je počítač, který se chová jako osobní nebo služební počítač zaměstnance, který se připojuje do interní sítě své firmy a přistupuje k firemním datům nebo prostředkům na straně serveru.

6.1.1. Client

První strana, VPN Client, se nacházela v Praze 9 – Kbely. Před měřením proběhla instalace operačního systému Windows 10 Enterprise na serverovém počítači Dell PowerEdge T440 s následujícími parametry:

- Procesor Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
- Operační paměť 128 GB
- Pevné disky 2x 480 GB SSD RAID1
  2x 1,2 TB HDD RAID1
  2x 1,2 TB HDD RAID1

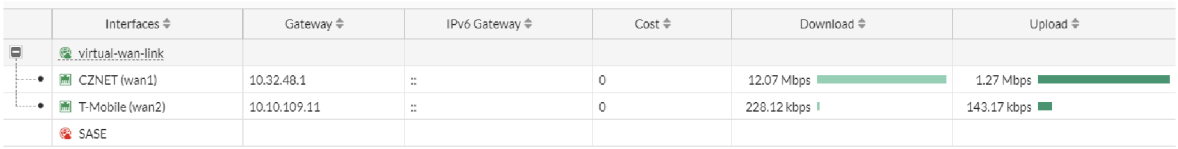
Zmíněný operační systém Windows 10 byl nainstalován jako virtuální zařízení v prostředí VMWare ESXi. Byly mu přiděleny 2 jádra procesoru, 8 GB operační paměti a 50GB místa na pevném disku. Jako síťový adaptér byl přidělen adaptér VMXNET 3, který dovoluje rychlost 10GBit.

Klientský počítač se nacházel za Firewallem Fortinet 40F, do kterého byly přivedeny dvě konektivity dvou různých poskytovatelů internetu – T-Mobile a CZNET.

T-Mobile na klientské straně zajišťuje připojení přes optický kabel. Na počátku měření, byla skrze webovou stránku speedtest.net naměřena rychlost 281,80 Mbit/s rychlost stahování a 87,56 Mbit/s rychlost nahrávání. Odezva od serverů, proti kterým se měřila rychlost, byla 18 ms a proto byla pro účely měření zvolena primárně druhá konektivita.

CZNET na straně klienta zajišťuje připojení k internetu bezdrátově. Na počátku měření byla přes stránku speedtest.net naměřena 85,81 Mbit/s rychlost stahování a 75,67 Mbit/s rychlost nahrávání. Připojení přes CZNET je výrazně pomalejší, nicméně odezva od serveru, proti kterému byla měřena rychlost, byla pouze 1 ms.

Konektivita byla skrze SD-WAN (Softwarově definované WAN) nastavena takovým způsobem, že firewall Fortinet 40F sám volí nejstabilnější a nejrychlejší konektivitu (internetové připojení) k dosažení požadovaného cíle. Nicméně právě pro vyšší odezvu připojení přes T-Mobile (18 ms) bylo k porovnání využito připojení přes CZNET, které je sice více jak trojnásobně pomalejší, ale jeho nižší odezva přinesla jasnější výsledky. Internetový připojení T-Mobile bylo tedy pomocí SD-WAN pravidla zakázáno. Virtuální WAN-link lze vidět na obrázku 5.



Obrázek 5 Konfigurace SD-WAN na Fortinet 40F v Praha 9 – Kbely [Zdroj: Vlastní]

6.1.2. Server

Druhá strana měření, strana VPN serveru, se nacházela v Novém Strašecí v panelovém domě. Připojení k internetu je zde zajištěno přes místního poskytovatele internetu Bubakov.net. Připojení je zajišťováno pomocí optického kabelu. Na počátku měření byla skrze internetovou stránku speedtest.net naměřena 381 Mbit/s rychlost stahování a 321,72 Mbit/s rychlost nahrávání.

Poskytovatel internetu Bubakov.net přiděluje svým zákazníkům interní LAN rozsah (poskytovatel tedy v Novém Strašecí vytváří jednu velkou LAN síť), proto bylo nutné zajistit u poskytovatele NAT 1:1 (Network Adress Translation – překlad síťových adres), tedy IP adrese, která se nacházela na WAN portu testovaných firewallů byla na straně poskytovatele internetu přidělena jedna konkrétní statická IP adresa, kterou nesdílí s žádným dalším zákazníkem nebo sousedem v domě.

Počítač, na kterém byla spuštěna měřící aplikace v režimu server byl Dell Optiplex 3080 s následujícími parametry:

- Procesor Intel Core i3 10105
- Operační paměť 4 GB
- Pevný disk SSD 128 GB
- Operační systém Windows 10 Pro

6.2. Měřící aplikace

K měření odezvy byly použity dvě aplikace. První byl nástroj Iperf (iperf.fr) od francouzských vývojářů.

iPerf

iPerf je nástroj sloužící k aktivnímu měření maximální využitelné šířky pásma na počítačových sítích. Spouštění a ovládání probíhá z příkazové řádky (command line), nástroj nemá sám o sobě žádné grafické rozhraní. Součástí nástroje je možnost specifikovat řadu

parametrů, které se týkají velikosti zasílaných packetů nebo specifikace použitého transportního protokolu. Při měření nástroj vypisuje šířku pásma, míru ztráty packetů a další parametry. Nástroj již podlehl několika změnám, současná verze je iPerf3.1.3, verze mezi sebou nejsou zpětně kompatibilní – zdrojový kód aplikace iPerf3 se od iPerf2 zásadně liší. Aplikace je funkční jako cross-platform, tedy lze měřit například systém Windows oproti systému Linux atd. [62]

Mezi podporované operační systémy a platformy patří: Microsoft Windows, Linux, Android, MacOS X, FreeBSD, OpenBSD, VxWorks, Solaris. [62]

Pro spuštění nástroje iPerf je třeba spustit příkazovou řádku (cmd.exe) a otevřít adresář ve kterém se nachází spouštěcí soubor iperf3.exe. Toto se provede pomocí příkazu „cd“ (change directory) – například. pokud se soubor iperf3.exe nachází v dokumentech ve složce „iperf“, je třeba zadat příklaz „cd C:\Users\jméno uživatele\Documents\iperf“. [62]

Ve chvíli, kdy se nacházíme ve správné složce spustíme nástroj zadáním „iperf3.exe“, zároveň je ale třeba nástroji před některé parametry, které se definují znakem „-„ (pomlčka). Pro měření, je tedy na straně klienta třeba zadat příkaz „iperf3.exe -c ip-adresa-serveru“, kdy parametrem „-c“ specifikujeme že spouštíme iPerf v režimu client. Na straně serveru spustíme iPerf pomocí parametru -s, dále už nespecifikujeme žádnou IP adresu, iPerf se přepne do režimu serveru a poslouchá na výchozím portu 520, tedy „iperf3.exe -s“. [62]

NetIO-GUI

Druhou aplikací, která byla při měření použita jako doplněk byla NetIO-GUI. Aplikace je open source (volně šiřitelná) a je podporována pouze na operačním systému Microsoft Windows. Aplikace je továrně nastavena tak, že směrem k serveru se pokusí odeslat packety o velikosti 1k až 32k a následně rychlosti zaslaných packetů zprůměruje. Neopomenutelnou součástí aplikace je také odezva (PING), kdy se aplikace pokusí odeslat packety o velikosti 32b až 1024b a následně opět zprůměruje naměřené výsledky. [63]

Vlastní měření probíhá tak, že se aplikace spustí na dvou počítačích, kdy na jednom se spustí v Client-Mode a na druhém v Server-Mode. Na počítači s client-mode je poté nutné specifikovat IP adresu serverové části – druhého počítače. IP adresu lze na počítači zjistit například pomocí příkazu „ipconfig“, který zadáme do příkazové řádky (cmd.exe na systému Microsoft Windows). Na závěr je nutné vybrat, zdali chceme k měření využít protokol TCP nebo UDP. [63]

Přenos dat protokolem SMB

Pro podložení a kontrolu naměřených výsledků byl dále skrze VPN tunel zaslán soubor o velikosti 236 MB. Odesílaným souborem byl instalační soubor VMware VMvisor 5.5.0. Odeslání probíhalo skrze protokol SMB (Server Message Block – protokol umožňující sdílený přístup k souborům a složkám). Na počítači v Novém Strašecí byla na disku C: vytvořena složka, na které bylo zapnuto sdílení pro všechny uživatele. Z klientského počítače ve Kbelích byl poté zapnut průzkumník souborů Windows (proces explorer.exe) a do adresního řádku byla zadána lokální IP adresa počítače, na kterém se nachází sdílená složka ve tvaru „\\ip adresa počítače“. Ověření proti sdílené složce poté proběhlo jménem a heslem lokálního uživatele počítače v Novém Strašecí.

6.3. Konfigurace SSL VPN na Fortinet 40F

Jako první byla provedena konfigurace na zařízení značky Fortinet. Jedná se o firewall Fortinet 40F s firmwarem 7.0.5, který byl zapůjčen od firmy NWS s.r.o. Firewally Fortinet jsou dodávany s operačním systémem FortiOS, který umožňuje vytvoření SSL VPN a IPsec VPN. V rámci IPsecu umožňuje vytvoření tunelu jak site-to-site tak client-site. Připojení ke client-site IPsec VPN probíhá (stejně jako u SSL VPN) přes aplikaci s výstižným názvem FortiClient, která je zdarma stažitelná ze stránek výrobce. Firewall dále nabízí využití SD-WAN.

Konfigurace SSL VPN byla provedena přes grafické rozhraní, které je dostupné z webového prohlížeče po zadání IP adresy. Veškeré nastavení bylo provedeno dle dokumentace a návodů firmy Fortinet a dle vlastní logiky a uvážení na základě nabytých informací z teoretické části. Firewall byl před vlastním měřením využívaný pro internetové připojení bytu v Novém Strašecí, a proto nebylo třeba nastavovat WAN a LAN, DHCP protokol a další.

Do nastavení VPN se administrátor dostane skrze menu v levé části – SSL-VPN Settings. Zde bylo třeba vybrat na jakém rozhraní VPN naslouchá, specifikovat port na kterém naslouchá, dále zvolit server certifikát, specifikovat parametry pro připojené klienty, jako jsou DNS servery a přiřazování IP adresy (DHCP) a vybrat pro které uživatele, nebo skupiny uživatelů je VPN povolena. Nastavení bylo provedeno následujícím způsobem:

- **Connection settings**
  - **Listen on Interface:** WAN
  - **Listen on Port:** 10443 (náhrada za HTTPS port 443 – dobře zapamatovatelné)
  - **Server Certificate:** FortiNet Factory
  - **Restrict Access:** Allow access from any host (možnost limitovat připojení pro konkrétní IP adresy)
- **Tunnel mode client settings**
  - **Address Range:** Automatically assign adresses (Byl využit výchozí předdefinovaný adresní rozsah 10.212.134.200 – 10.212.134.210)
  - **DNS server:** Specify (Vynucení klientovi využít námi specifikované DNS servery)
  - **DNS Server #1:** 1.1.1.1 (DNS server Cloudflare)
  - **DNS Server #2:** 1.0.0.1 (opět DNS server Cloudflare – lze využít i Google, NIC.CZ nebo další DNS servery)

Authentication/Portal Mapping

V této části byla vytvořena nová uživatelská skupina, které bylo umožněno tunelové připojení. Skupina byla nazvána „SSL VPN“ a byl do ní přidán testovací uživatel Urban.

Již během nastavování firewall Fortinet 40F vypisuje upozorňovací textová pole, která jsou barevně odlišena a administrátorovi vysvětlují co bude znamenat nastavení, které právě provedl. Webové rozhraní tedy v tuto chvíli upozornilo na to, že neexistují žádná SSL-VPN politiky (pravidla). Klikem na toto upozornění jsme byli přeneseni do Policy & Objects/Firewall Policy.

Dle návodu pro nastavení SSL-VPN na Fortinet firewallu je třeba vytvořit firewallové pravidlo, pomocí kterého je směrována komunikace z SSL-VPN tunelového rozhraní směrem do interní LAN sítě, která je za firewallem. Nastavení bylo provedeno následujícím způsobem:

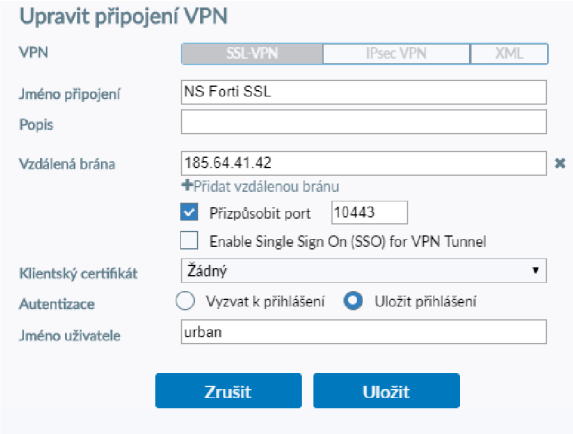
- **Name:** SSL VPN > LAN
- **Incoming Interface:** SSL-VPN tunnel interface
- **Outgoing Interface:** LAN
- **Source:** All adresses, SSL VPN uživatelská skupina
- **Destination:** LAN adresses

- **Service:** All (možnost limitovat použití SSL VPN na určité služby)
- **Action:** Accept
- **Options**
    - **Firewall / Network Options - NAT:** Povoleno (Nutnost, jelikož firewall je zapojen za NAT 1:1)
    - **Logging Options - Log Allowed Traffic:** All Sessions (Druhou možností je Security Events)

Ostatní nastavení jako IP Pool Configuration a bezpečnostní profily bylo ponecháno ve výchozím stavu.

Po provedeném nastavení byla ze stránek výrobce stažena aplikace FortiClient VPN a provedena instalace do operačního systému Windows 10. Aplikace ihned nabízí jedinou možnost – konfigurovat VPN.

V menu byla zvolena SSL-VPN a do Vzdálené brány zadána veřejná IP adresa a specifikován port 10443 viz Obrázek 6.



Obrázek 6 Nastavení SSL VPN v aplikaci FortiClient VPN [Zdroj: Vlastní]

Veřejnou IP adresu (Vzdálená brána) lze zjistit na straně serveru přes webovou stránku https://www.mojeip.cz/, nebo je viditelná v System Information ve Statusu firewallu Fortinet 40F.

6.4. Konfigurace SSL VPN na Zywall USG300

Firewall Zywall USG300 byl opět zapůjčen od firmy NWS s.r.o.. Šlo o zařízení, které ještě před několika dny obsluhovalo kancelář poměrně významné pražské advokátní kanceláře. V dobu měření byl tento Firewall nahrazen právě zařízením značky Fortinet – Fortinet 80F. Zařízení mělo nahráno firmware 3.30(AQE.7) z roku 2015 (poslední aktualizace). Konfigurace, stejně jako u Fortinet, probíhala přes webové rozhraní. Zywall USG300 byl nicméně před prvotní konfigurací resetován do továrního nastavení. Po převezení do Nového Strašecí a po připojení počítače, ze kterého probíhala konfigurace, do portu 1 bylo třeba zadat výchozí URL adresu 192.168.1.1.

Před zprovozněním VPN na zařízení Zywall USG300 bylo nejprve nutné kompletně nakonfigurovat celý firewall tak, aby fungoval stejným způsobem jako Fortinet 40F – tedy nakonfigurovat WAN a LAN, tak aby byla vytvořena lokální síť s přístupem do internetu, ve které si připojené zařízení nastavují konfiguraci podle nastavení DHCP serveru běžícího na firewallu.

Dle nastavení WAN na firewallu Fortinet 40F je připojení k internetu Bubakov limitováno na konkrétní MAC adresu. Z toho důvodu bylo nutné zkopírovat WAN MAC adresu z Fortinet 40F na Zywall USG300. Přepsání MAC adresy lze provést na záložce Edit Ethernet na Portu 2 (zvolen jako WAN port) po rozbalení pokročilých vlastností (show advanced settings). V části MAC Adress Setting bylo zvoleno overwrite default MAC address a vložena adresa bc:ee:7b:97:3d:xx (konkrétní MAC adresa z bezpečnostních důvodů není uvedena). IP adresa byla ponechána na dynamické IP adrese (přidělení z DHCP serveru poskytovatele internetu). Na straně LAN dále vystupoval firewall pod jinou MAC adresou, kterou nelze jednoduše změnit.

Po nastavení WAN bylo třeba nastavit interní síť – LAN. Na záložce Network/Interface/Ethernet proběhlo nastavení LAN1 následujícím způsobem:

- **IP address:** 192.168.113.1 (IP adresa default gateway na LAN síti)
- **Subnet Mask**: 255.255.255.0
- **DHCP:** DHCP server (další možností je DHCP relay a nebo vypnutí DHCP)
- **IP Pool Start Address:** 192.168.113.20
- **Pool Size:** 200
- **First DNS server:** ZyWALL
- **Second DNS server:** Custom Defined – 1.1.1.1

Po nastavení LAN bylo třeba povolit web management, na záložce Systém/WWW, aby bylo webové rozhraní dostupné i z internetu. Proto bylo zaškrtnuto povolení HTTPS a výchozí port, přes který se provádí konfigurace routeru byl z bezpečnostních důvodů změněn na 10443. Dále bylo zaškrtnuto „Redirect http to HTTPS“, kdy se při vyvolání webového managementu vždy uskuteční šifrovaná komunikace.

Jelikož byl výchozí port web managementu 443 změněn na port 10443, bylo nutné provést nastavení Service (služby) na záložce Object/Service. Služba byla nazvána „Remote_MGMT“, IP protokol byl zvolen TCP a jako starting port byl vyplněn port 10443. Ending port byl ponechán prázdný. Po vytvoření služby bylo nutné službu přidat do skupiny služeb (záložka Service Group) – „Default_Allow_WAN_To_ZyWALL“ a zde byl do objektů přidán objekt „Remote_MGMT“, tedy služba, která byla před chvílí vytvořena.

V této chvíli firewall Zywall USG300 fungoval jako bezpečný směrovač pro připojení do internetu a bylo možné přejít na nastavení samotné SSL VPN.

Nejprve byl vytvořen uživatel, pomocí kterého bylo provedeno měření a samotné připojení na VPN. Uživatele lze vytvořit na záložce Object/(User/Group). Stejně jako na Fortinet 40F, zde byl pro účely měření vytvořen uživatel „urban“. Tento uživatel byl poté zařazen do nově vytvořené uživatelské skupiny „VPN_Users“.

Další v pořadí bylo vytvoření SSL VPN na záložce VPN/SSL VPN. Kliknutím na Add se otevře okno Access Policy.. Policy bylo nazváno „SSL_VPN_Urban“ a jako zóna byla vybrána SSL_VPN. Ze skupinových objektů byli vybráni VPN_Users. Níže v nastavení Access Policy bylo povoleno „Enable network extension (Full Tunnel Mode)“ – pro povolení toho, aby veškerý datový provoz mohl být posílán skrze VPN tunel (nemusí být použito) a dále bylo přidáno adresní pravidlo, tedy adresní rozsah pro uživatele SSL_VPN. Tento adresní rozsah byl nazván „SSL_VPN“, address type byl vybrán typu RANGE (tedy specifikace rozsahu). V tuto chvíli byla SSL VPN nastavena a dostupná na portu 10443. Rozsah byl nastaven jednoduchým způsobem:

- **Starting IP Address:** 10.12.14.1
- **End IP Address:** 10.12.14.10

Společnost Zyxel nabízí pro připojení SSL VPN klientský software – Zywall Secuextender. Tento software je pro uživatele operačního systému Windows zdarma stažitelný, verze pro MAC OS potřebuje placenou licenci, nicméně nabízí na 30 dní zkušební verzi.

Nastavení aplikace SecuExtender je velice přímočaré a jednoduché. Do pole server byla zadána veřejná WAN adresa Zywallu (IP adresa přidělená poskytovatelem internetu) a port 10443 byl od ní oddělen pomocí znaku „:“ (dvojtečka). Dále již stačilo pouze vyplnit uživatele a zadat heslo. Po vytočení VPN je nutné odsouhlasit certifikát Zywallu a tímto je tunel spojen.

6.5. Konfigurace IPsec VPN na Fortinet 40F

Konfigurace IPsec VPN na Fortinet je poměrně jednoduchá, vzhledem ke složitosti tohoto tunnelingového protokolu. Ke konfiguraci lze totiž použít IPsec Creation Wizard, který je dostupný ve webovém rozhraní pod VPN / IPsec Wizard.

V první části VPN Wizard bylo třeba dát název IPsecové VPN a zvolit o jaký typ se bude jednat (Site-to-Site, Remote Access, Custom). V této části tedy bylo zvoleno Remote Access a jako název bylo přiřazeno „Urban IPsec Forti“.

Další část IPsec Wizard byla zaměřena na autentikaci. Jako Incoming Interface byla vybrána WAN1 (komunikace přichází z internetu), authentication method má možnost buď Signature, nebo Pre-shared Key. Bylo tedy zvoleno pre-shared key a zadán náhodně vygenerovaný řetězec GroDKd849gsdgshrsda3. Nakonec je třeba zvolit uživatelskou skupinu, pro kterou bude IPsec VPN určena. Tu je možné vytvořit při vybírání User Group (uživatelské skupiny). Proto byla vytvořena skupina IPSEC_VPN a do ní byl přidán uživatel „Urban“.

Třetí částí IPsec Wizard bylo Policy &Routing. Tato část byla nakonfigurována následujícím způsobem:

- **Local interface:** LAN
- **Local address:** LOCAL_LAN
- **Client Address Range:** 10.10.10.10-10.10.10.50
- **Subnet Mask:** 255.255.255.255 (výchozí nastavení)
- **DNS Server:** Use System DNS (V síti nejsou žádné DNS servery)
- **Enable IPv4 Split Tunnel:** Povoleno (není požadováno, aby veškerý provoz šel skrze VPN tunel)

Poslední částí IPsec Wizard byly Client Options, kde bylo veškeré nastavení ponecháno na výchozích hodnotách – save password, auto connect, always up (keep alive).

Po dokončení IPsec Wizard bylo možné na záložce IPsec Tunnels zkontrolovat jaké zabezpečení a nastavení bylo wizardem použito. Před zobrazením těchto informací je třeba kliknout na „convert to custom tunnel“, abychom toto nastavení mohli vůbec zobrazit.

IPsec wizard svým nastavením vytvořil celé množství kombinací šifrovacích a hashovacích algoritmů ve fázi 1 a fázi 2. Pro účely měření byly všechny tyto algoritmy smazány a byly použity pouze šifrovací algoritmy AES128 s hashovací funkcí SHA256, pro následující porovnání s Zywall USG300. Jako Diffie Hellman skupina klíčů byla zvolena DH5.

Připojení k VPN probíhalo opět přes aplikaci FortiClient, která umožňuje jak SSL tak IPsec VPN připojení. Aplikace je kompletně zdarma a je stažitelná z webových stránek výrobce. Konfigurace připojení byla mírně složitější oproti SSL. Po výběru IPsec VPN bylo třeba zadat Jméno připojení, kde byl zvolen název „Urban IPsec“, jako vzdálená brána byla vyplněna veřejná IP adresa VPN serveru na který se připojovalo, způsob autentizace byl zvolen pomocí předběžně sdíleného klíče. Dále bylo nutné rozkliknout pokročilá nastavení, aby se zobrazily možnosti nastavení fáze 1 a fáze 2. Ve fázi 1 i ve fázi 2 byly zvoleny šifrovací algoritmy AES128 a autentizace SHA256, DH skupina klíčů 5.

Detekce neaktivních peerů, NAT Traversal i povolení PFS (perfect forward secrecy) zůstalo zaškrtnuto.

6.6. Konfigurace IPsec VPN na Zywall USG300

Nastavení IPsec VPN probíhalo, stejně jako u SSL, z webového rozhraní. Požadavkem bylo vytvořit a nakonfigurovat IPsec VPN, včetně obou IKE fází, jako site-to-client, tedy VPN pro obyčejného uživatele bez nutnosti konfigurace uživatelské sítě. Site-to-site VPN (VPN mezi dvěma firewally) tedy nebyla vytvářena.

Na záložce VPN/IPsec VPN se nacházelo několik stránek. První stránkou je VPN Connection, která slouží ke konfiguraci IKE fáze 2, druhou stránkou je VPN Gateway, která nese nastavení IKE fáze 1.

Na stránce byla tedy přidána nová VPN Gateway a nakonfigurována následujícím způsobem:

- **VPN Gateway Name**: VPN_GW
- **Gateway Settings**
  - **Interface:** wan1
  - **Peer Gateway Address:** Dynamic Address
  - **Pre-Shared Key:** GroDKd849gsdgshrsda3 (náhodně vygenerovaný řetězec – stejný jako u Fortinet)

Po rozkliknutí Show Advanced Settings bylo nastaveno dále:

- **Phase 1 Settings**
  - **SA Life Time:** 86400 seconds
  - **Negotiation Mode:** Aggressive
  - **Proposal: Encryption:** AES128, **Authentication:** SHA256
  - **Key Group:** DH5 (Diffie-Hellman skupina klíčů)
  - **NAT Traversal:** povoleno (výchozí nastavení)
  - **Dead Peer Detection:** povoleno (výchozí nastavení)

Ostatní nastavení VPN Gateway byla ponechána na výchozích hodnotách.

Po nastavení VPN Gateway byla nakonfigurována druhá fáze – na stránce VPN connection.

- **Connection Name:** IPSec_VPN_Urban
- **Enable Replay Detection, Enable NetBIOS broadcast over IPSec:** zakázáno
- **VPN Gateway**
- **Application Scenario:** Remote Access
- **VPN Gateway:** vybrána VPN_GW
- **Local policy:** LAN_SUBNET
- **Phase 2 Setting**
  - **SA Life Time:** 86400
  - **Active Protocol:** ESP
  - **Encapsulation:** Tunnel
  - **Proposal: Encryption:** AES128, **Authentication:** SHA256

Pro připojení k IPSec VPN není možné využít aplikaci Zywall Secuextender, ani výchozí VPN aplikaci v operačním systému Microsoft Windows, jelikož IPSec VPN do ní není implementována (pouze kombinace L2TP over IPsec). Společnost Zyxel nabízí aplikaci Zywall IPSec VPN Client, která je bohužel ve všech případech placená, nicméně pro účely této diplomové práce bylo využito zkušební verze na 30 dní.

Aplikace je opět dostupná ke stažení na webových stránkách výrobce. Konfigurace Zywall IPSec VPN Client není tak jednoduchá, jako je tomu u Zywall Secuextender – SSL VPN.

Nejprve bylo třeba v IKE V1 vytvořit nové připojení VPN. Připojení automaticky dostane název Ikev1Gateway. Do vzdálené brány bylo nutné doplnit veřejnou IP adresu VPN serveru, na který se připojujeme. Dále bylo třeba vyplnit 2x za sebou předsdílený klíč (pre-shared key) a v kryptografii nastavit šifrování na AES128, Autentizaci na SHA-256 a Skupinů klíčů na DH5 (1536). Toto veškeré nastavení koresponduje s nastavení, které bylo navoleno na Zywall USG300 během konfigurace.

IPsec fáze 2 je nastavována na Ikev1Tunnel (výchozí název). Adresa VPN klienta zůstala nastavena na 0.0.0.0 , Adresa vzdálené LAN byla 192.168.113.0 (adresa vzdálené lokální sítě), maska podsítě 255.255.255.0 (stejná jako vzdálená LAN síť). V části ESP bylo zvoleno opět šifrování AES128. autentizace SHA-256 a režim ESP: Tunel. Ostatní nastavení bylo ponecháno na výchozích hodnotách.

6.7. Naměřené výsledky

Veškeré výsledky měření jsou dostupné v přílohách k této diplomové práci. V rámci porovnání řešení stejné VPN od různých výrobců jsou v následujících podkapitolách zobrazeny pouze výsledky měření rychlosti TCP a UDP packetů pomocí nástroje iPerf3, jelikož právě v těchto měřeních byly zjištěny nejvýraznější rozdíly. Samotná měření pomocí nástroje iPerf3 byla provedena několikrát za sebou, ale mezi jednotlivými měřeními na stejném zařízení nebyly zaznamenány výraznější rozdíly. Oproti tomu rozdíly mezi SSL VPN Fortinet 40F a SSL VPN Zywall USG300 byly patrné již od první chvíle.

6.7.1. SSL VPN

Měření rychlosti TCP packetů skrze SSL VPN Fortinet 40F

Tabulka 2 zobrazuje průběh měření pomocí nástroje iPerf3. Na počátku měření docházelo k přenosu většího množství dat (megabajtů) díky vyšší rychlosti a v průběhu

měření se rychlost měnila, nikdy už ale nedosáhla rychlosti jako v první sekundě od počátku měření. Jak již bylo zmíněno výše, měření bylo zopakováno několikrát po sobě a toto chování se nijak významně nezměnilo mezi jednotlivými pokusy.

Interval [sekundy]	Přenos [MB]	Rychlost
0,00 - 1,01	7,12	59,2 Mbit/s
1,01 - 2,01	3,25	27,4 Mbit/s
2,01 - 3,01	3	25,2 Mbit/s
3,01 - 4,01	3,5	29,1 Mbit/s
4,01 - 5,01	3,38	28,3 Mbit/s
5,01 - 6,01	3,75	31,5 Mbit/s
6,01 - 7,01	3,25	27,2 Mbit/s
7,01 - 8,01	3,62	30,6 Mbit/s
8,01 - 9,01	3,62	30,1 Mbit/s
9,01 - 10,0	3,5	29,5 Mbit/s

Tabulka 2 TCP packety skrze SSL VPN Fortinet [Zdroj: vlastní]

Tabulka 3 uvádí, že skrze SSL VPN Fortinet 40F byla naměřena průměrná rychlost 38,7 Mbit/s a žádné packety nebyly ztraceny (Celkem odesláno = Celkem přijato).

Celkem odesláno	**46,1 MB**
Celkem přijato	**46,1 MB**
Průměrná rychlost	**38,7 Mbit/s**

Tabulka 3 TCP packety skrze SSL VPN Fortinet – výsledné hodnoty [Zdroj: vlastní]

Měření rychlosti TCP packetů skrze SSL VPN Zywall USG 300

Již v průběhu měření TCP packetů bylo patrné, že rychlost u Zywall USG 300 je výrazně nižší. Jak je zobrazeno v tabulce 4, i po několika zopakovaných měřeních rychlost nikdy nepřesáhla hodnotu 10 Mbit/s. Průměrná rychlost se vždy pohybovala v okolí zobrazených 8,49 Mbit/s z prvního měření.

Z těchto skutečností plyne, že v rámci SSL VPN Zywall USG 300 nebylo možné odeslat či přijmout TCP packety vyšší rychlostí než 10 Mbit/s. Naopak u SSL VPN Fortinet 40F byla na počátku měření zjištěna až šestinásobně vyšší rychlost, která se v průběhu měření snížila na trojnásobnou.

Při měření na Zywall USG300 vždy došlo ke ztrátě menšího množství TCP packetů (celkem bylo odesláno 10,1 MB, ale přijato bylo pouze 9,96 MB). U SSL VPN Fortinet 40F se ztrátovost TCP packetů nepodařila naměřit.

Pro vysvětlení chování UDP packetů zaslaných skrze VPN jsou v tabulkách níže (tabulky 5 a 6) zobrazeny pouze výsledky měření, průběhy měření jsou zaznamenány v přílohách k této diplomové práci (příloha 1 a 2).

Interval [sekundy]	Přenos [MB]	Rychlost
0,00 - 1,01	1,1	9,32 Mbit/s
1,01 - 2,01	1	8,47 Mbit/s
2,01 - 3,01	1,12	9,40 Mbit/s
3,01 - 4,01	1,12	9,42 Mbit/s
4,01 - 5,01	1	8,39 Mbit/s
5,01 - 6,01	1	8,35 Mbit/s
6,01 - 7,01	0,896	7,42 Mbit/s
7,01 - 8,01	1	8,34 Mbit/s
8,01 - 9,01	0,768	6,32 Mbit/s
9,01 - 10,0	1,12	9,38 Mbit/s
Celkem odesláno	**10,1 MB**	
Celkem přijato	**9,96 MB**	
Průměrná rychlost	**8,49 Mbit/s**	

Tabulka 4 TCP packety skrze SSL VPN Zywall [Zdroj: vlastní]

Měření rychlosti a propustnosti UDP packetů SSL VPN Fortinet 40F a Zywall USG300

Z tabulek 5 a 6 lze vyčíst, že rychlost se v rámci UDP packetů mezi zařízeními nijak neliší. V rámci SSL VPN Fortinet 40F byla u UDP packetů naměřena průměrná rychlost podobná, jako maximální rychlost u TCP packetů, při minimální procentuální ztrátě. Nicméně, u Zywall USG 300 docházelo k téměř maximální ztrátě.

Fortinet 40F UDP	
Celkem odesláno	82,7 MB
Průměrná rychlost	69,3 Mbit/s
Ztráta datagramů	3/10583
Procentuelní ztráta	0,03 %
Zpoždění v odesílání	0,949 ms

Tabulka 5 UDP packety SSL Fortinet 40F [Zdroj: vlastní]

Zywall USG300 UDP	
Celkem odesláno	82,7 MB
Průměrná rychlost	69,3 Mbit/s
Ztráta datagramů	9324/10588
Procentuelní ztráta	88 %
Zpoždění v odesílání	13,676 ms

Tabulka 6 UDP packety SSL Zywall USG300 [Zdroj: vlastní]

6.7.2. IPSec VPN

Měření rychlosti a propustnosti TCP packetů na Fortinet 40F

Naměřené výsledky jsou zaznamenány v tabulce 7. Měření bylo provedeno opět několikrát v krátkém časovém intervalu, ale naměřené hodnoty se mezi sebou nijak zásadně nelišily.

Z naměřených výsledků je patrné, že remote access IPsec VPN se chovala daleko stabilněji než SSL VPN, tedy udržovala téměř konstantní rychlost a přenos. IPsec se tedy jeví jako rychlejší varianta při výběru VPN oproti SSL, nicméně administrátor nesmí opomenout fakt, že konfigurace IPsec je poměrně značně náročná (jak na serveru, tak na klientském softwaru) a vyžaduje znalost počítačových sítí, bezpečnosti a routování.

SSL VPN při své konfiguraci nenabízí žádné bezpečnostní volby, k šifrování a autentizaci je zde využíván protokol TLS. Lze tedy předpokládat, že nižší rychlost SSL VPN je způsobena právě protokolem TLS.

IPsec a SSL mimo jiné pracují na jiné vrstvě. IPsec pracuje na síťové vrstvě modelu ISO/OSI, kdežto SSL VPN pracuje na aplikační vrstvě ISO modelu – šifruje tedy HTTPS provoz, namísto šifrování konkrétních IP packetů.

Interval [sekundy]	Přenos [MB]	Rychlost
0,00 - 1,01	7,5	62,5 Mbit/s
1,01 - 2,01	6,62	56,0 Mbit/s
2,01 - 3,01	7,62	63,5 Mbit/s
3,01 - 4,01	7,38	61,9 Mbit/s
4,01 - 5,01	7	58,7 Mbit/s
5,01 - 6,01	7,5	63,2 Mbit/s
6,01 - 7,01	7,62	63,8 Mbit/s
7,01 - 8,01	7	58,7 Mbit/s
8,01 - 9,01	7	59,0 Mbit/s
9,01 - 10,0	7,5	62,4 Mbit/s
Celkem odesláno	**72,8 MB**	
Celkem přijato	**72,6 MB**	
Průměrná rychlost	**61 Mbit/s**	

Tabulka 7 TCP packety skrze IPsec VPN Fortinet [Zdroj: vlastní]

Měření rychlosti a propustnosti TCP packetů na Zywall USG300

V tabulce 8 jsou zaznamenány naměřené hodnoty pro TCP packety zaslané skrze IPsec VPN vytvořené na Zywall USG300. Z hodnot je patrné, že byla dosažena rychlost téměř 40 Mbit/s, což se blížilo chování IPsec VPN skrze Fortinet 40F. IPsec VPN na Zywall USG300 byla tedy stabilitou a propustností podobná stejnému typu VPN na Fortinet 40F, nicméně maximální rychlost byla opět nižší.

Interval [sekundy]	Přenos [MB]	Rychlost
0,00 - 1,01	4,75	39,4 Mbit/s
1,01 - 2,01	4,38	36,8 Mbit/s
2,01 - 3,01	4,75	39,9 Mbit/s
3,01 - 4,01	4,5	37,7 Mbit/s
4,01 - 5,01	4,62	38,8 Mbit/s
5,01 - 6,01	4,62	38,8 Mbit/s
6,01 - 7,01	4,62	39,1 Mbit/s
7,01 - 8,01	4,62	38,5 Mbit/s
8,01 - 9,01	4,5	38 Mbit/s
9,01 - 10,0	4,25	35,4 Mbit/s
Celkem odesláno	**45,6 MB**	
Celkem přijato	**45,5 MB**	
Průměrná rychlost	**38,2 Mbit/s**	

Tabulka 8 TCP packety skrze IPsec VPN Zywall [Zdroj: vlastní]

Porovnání rychlosti a spolehlivosti IPsec VPN při zasílání UDP packetů je znázorněno v tabulkách 9 a 10.

Fortinet 40F UDP	
Celkem odesláno	82,9 MB
Průměrná rychlost	69,4 Mbit/s
Ztráta datagramů	610/10606
Procentuelní ztráta	5,80 %
Zpoždění v odesílání	0,148 ms

Tabulka 9 UDP packety IPsec Fortinet 40F [Zdroj: vlastní]

Zywall USG300 UDP	
Celkem odesláno	83,1 MB
Průměrná rychlost	69,7 Mbit/s
Ztráta datagramů	4175/10634
Procentuelní ztráta	39 %
Zpoždění v odesílání	1,665 ms

Tabulka 10 UDP packety IPsec Zywall USG300 [Zdroj: vlastní]

Tabulky s měřením UDP packetů (tabulky 9 a 10) uvádí, že průměrné rychlosti se téměř shodují u obou firewallů. Nicméně bylo zjištěno, že u firewallu Zywall USG300 docházelo k velké ztrátě packetů – tedy 39% zaslaný packetů nebylo vůbec doručeno.

Naměřené výsledky provedené nástrojem NetIO GUI jsou k dispozici v přílohách ke každému typu VPN. Při měření IPsec VPN na Zywall USG300 a SSL VPN na Fortinet 40F se nepodařilo z nespecifikovaných důvodů naměřit rychlost odesílání a přijímání UDP packetů. V průběhu odesílání UDP packetů skrze IPsec tunel vytvořený na Fortinet 40F docházelo k timeoutu (vypršení časového limitu) při 32KB velikosti packetů. Toto chování, pomocí nástroje iPerf3, nebylo zaznamenáno. Jelikož je iPerf3 stále vyvíjený a podporovaný software s detailnější dokumentací, než NetIO GUI, byl v této práci kladen větší důraz na naměřené výsledky právě nástrojem iPerf3, který se choval stabilněji a předvídatelněji.

6.8. Porovnání Zywall USG300 a ATP500

Jelikož bylo měření prováděno na zařízení Zyxel USG 300, které již není nabízeno (jedná se tedy o starší zařízení), bylo navíc provedeno kontrolní přeměření na jiném zařízení společnosti Zyxel. Tímto zařízením byl Zywall ATP500, který pracuje jako firewall v jedné z největších realitních kanceláří v Praze. Firewall měl v sobě nahraný firmware V5.02 (ABFU.0), který byl vydán 4.7.2021 – je tedy možné toto zařízení považovat za velmi aktuální. Měření bylo provedeno opět skrze nástroj iPerf3. Naměřené výsledky je možné vidět v tabulce 11.

Interval [sekundy]	Přenos [MB]	Rychlost
0,00 - 1,01	0,992	8,11 Mbit/s
1,01 - 2,01	1,12	9,35 Mbit/s
2,01 - 3,01	0,647	5,30 Mbit/s
3,01 - 4,01	0,094	0,765 Mbit/s
4,01 - 5,01	0,573	4,68 Mbit/s
5,01 - 6,01	0,345	2,82 Mbit/s
6,01 - 7,01	0,057	0,465 Mbit/s
7,01 - 8,01	0,052	0,425 Mbit/s
8,01 - 9,01	0,732	6,05 Mbit/s
9,01 - 10,0	0,857	6,94 Mbit/s

Tabulka 11 Porovnání Zywall USG300 a ATP500 – SSL VPN [Zdroj: vlastní]

Průměrná naměřená rychlost byla vypočtena na 4,48 Mbit/s, přičemž po celou dobu měření nebyla naměřena rychlost vyšší, než 10 Mbit/s.

Měření bylo prováděno na jiné konektivitě, nicméně konektivita jak na straně serveru, tak na straně klienta byla rychlejší než při původním měření. Z naměřených výsledků vyplívá, že zařízení firmy Zyxel mají patrné potíže s propustností a rychlostí

u VPN typu SSL, v porovnání s jinými výrobci firewallů a routerů, jako je například Fortinet.

Pro úplnost bylo provedeno také měření skrze IPsec VPN, kde byly naměřeny podobné výsledky, jako u Zywall USG300. Průměrná rychlost zde byla vypočítána na 52,1 Mbit/s.

Měření bylo prováděno na starším zařízení Zywall USG300 a na novějším zařízení Zywall ATP500, ale výsledky byly velmi podobné. Z těchto zjištěných faktorů vyplívá, že problém s rychlostí SSL u zařízení Zyxel není vázaný na konkrétní hardwarový prvek nebo na stáří výrobku, ani nejde o aktuální chybu firmwaru. Problémy tedy způsobuje vlastnost, nebo nepopsaná chyba, která je u firewallů Zywall přítomna již řadu let.

6.9. Realizace alternativního řešení – Microsoft Remote Apps a RDGW

Nasazení a konfigurace remote aplikací proběhla v nejmenované firmy z Hodonína. Firmu jsem se rozhodl nejmenovat, přestože byl získán souhlas k použití do této diplomové práce, a to z důvodu neustále rostoucího počtu kybernetických útoků. Informace získané v této kapitole diplomové práce by mohli pomoci potenciálnímu útočníkovi ve specifikovaní jeho pokusů penetrovat kybernetickou ochranu a získat tak přístup k datům firmy. Z tohoto důvodu je v této diplomové práci nadále místo skutečného názvu firmy použito „firma X“.

Firma se specializuje na prodej a výrobu kancelářských potřeb. Jako remote server byl použit virtuální server s doménovým názvem KOS-RDS (Fully qualified domain name poté bylo kos-rds.firmaXYZ.local). **Technické údaje o serveru:**

- Procesor Intel Xeon Silver 4214 2,20GHz (4 jádra)
- Nainstalovaná paměť RAM 8 GB
- Operační systém Windows Server 2019 Standard
- Přiřazené místo pevného disku 45 GB
- Server je virtualizovaný v prostředí VMWare – hypervizor ESXi verze 7.0.3
- Hardwarové prostředky jsou přidělovány skrze hypervizor

6.9.1. Konfigurace RDS rolí

Instalace a nastavení bylo provedeno skrze grafické rozhraní Windows Serveru. Na počátku konfigurace bylo třeba nainstalovat do serveru novou roli skrze Windows Server managera. Při nasazování role Remote Desktop Services, bylo třeba zvolit z několika možností a scénářů, které průvodce přidáním role nabízí.

Tato rozhodnutí byla uskutečněna na základě komunikace s firmou – dle jejich požadavků na funkčnost a užívání.

Bylo tedy rozhodnuto, že tento RDS server bude nastaven v režimu Session-based, tedy každý přihlášený uživatel bude mít na serveru svou vlastní běžící **session** (spojení se serverem) a všichni uživatelé budou sdílet stejné systémové prostředky i stejný souborový systém (omezení přístupů pouze právy). Další možností bylo zvolit virtual desktop, kdy by každý uživatel měl svou vlastní plochu.

Veškeré role Remote Desktop services jsou instalovány na jeden jediný server a proto průvodce upozorňuje na to, že na server budou nainstalovány tyto 3 role:

- Remote Desktop Connection Broker
- Remote Desktop Web Access
- Remote Desktop Session Host

Dále bylo rozhodnuto že bude nainstalována i role RD Web Access, pro připojení k remote aplikacím skrze internetový prohlížeč. Po nainstalování Remote Desktop rolí na server následovalo vytvoření kolekce aplikací.

6.9.2. Vytváření kolekcí:

Kolekce byla vytvořena pouze jedna, jako název kolekce byl zvolen název firmy „Firma X“. Při vytváření kolekce je nutné vybrat Remote Desktop Session Hots (v tomto případě byl pouze jeden – kos-rds.firmaXYZ.local). Následně je nutné vybrat uživatelskou skupinu, která má možnost připojit se ke kolekcím – v základu je předvolena bezpečnostní skupina „Domain Users“ (doménový uživatelé). Tato skupina však byla nahrazena bezpečnostní skupinou „RDS_users“, která byla vytvořena za účelem přidělení práv k remote aplikacím.

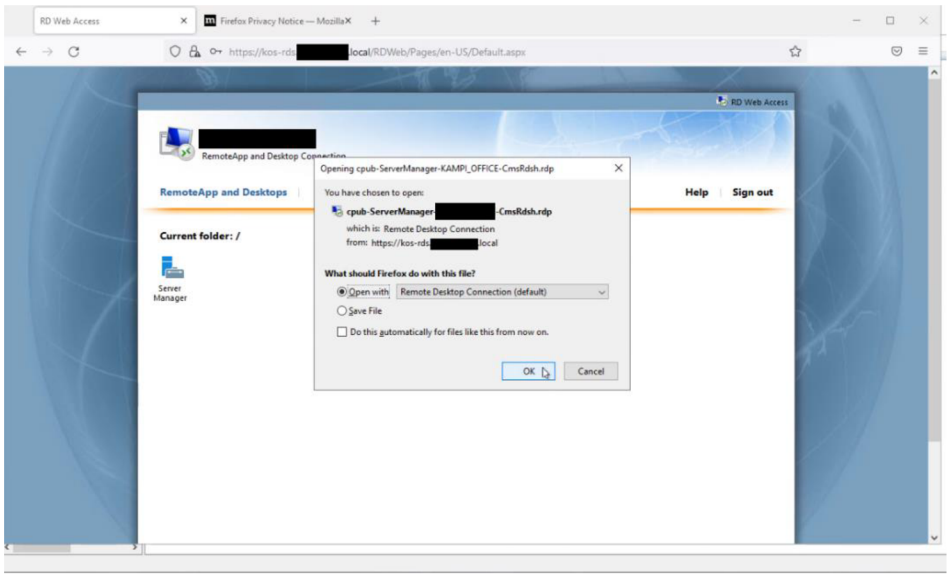
Poslední položkou k výběru byla možnost „Enable user profile disks“ – povolení disků uživatelských profilů. Průvodce upozorňuje, že přihlášený uživatel by musel být

členem skupiny lokálních administrátorů, což by nebylo z hlediska doménové bezpečnosti žádoucí. Proto byla možnost povolení uživatelských disků zneaktivněna.

Po vytvoření kolekce je třeba zvolit remote aplikace, které budou součástí kolekce. K prvotním testům byla do kolekce přidána aplikace Server Manager, po otestování a zprovoznění byly nadále přidány aplikace Altus Vario a další.

Po vytvoření kolekce bylo nutné pomocí aplikace Windows PowerShell s administrátorským ověřením (elevated powershell) spustit příkaz Set-RDworkspace -name „Firma X“ (název kolekce), pomocí kterého byl přiřazen název, který uvidí uživatelé ve webovém prostředí (Remote Desktop Web Access) a v jejich remote aplikacích.

V tuto chvíli se staly remote aplikace dostupné skrze webový prohlížeč na adrese https://kos.rds.firmaxyz.local/rdweb - výchozí adresa po provedení předchozího nastavení. Webový přístup lze vidět na obrázku 7.

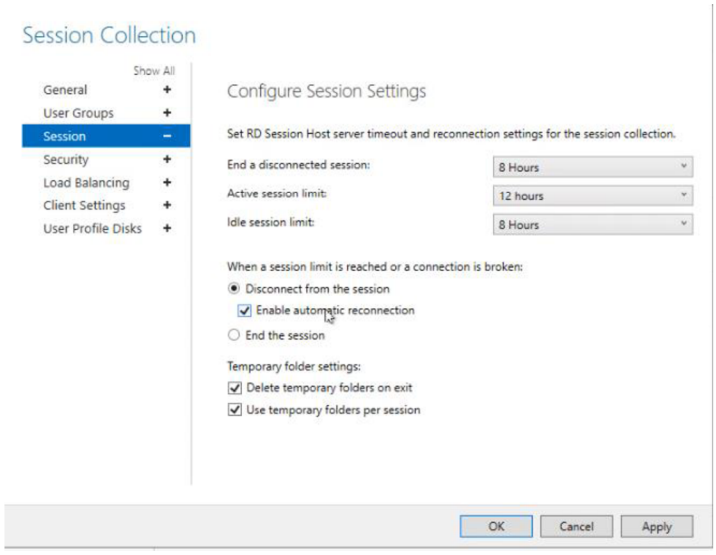


Obrázek 7 Webový přístup k nasdíleným RemoteApps [zdroj: vlastní]

Po otestování funkčnosti následovalo nastavení časových limitů a opětovného připojení. To bylo třeba nastavit ve vlastnostech kolekce (Properties of the collection), kliknutím na „Tasks“ a „Edit properties“. Zde je v nastavení možné specifikovat za jaký čas se ukončí odpojená session (ukončení spojení se serverem – End a disconnected session), časový limit aktivního session spojení (Active session limit) a limit nečinného spojení (Idle session limit). Ve výchozím nastavení jsou všechny hodnoty nastaveny na hodnotu „never“ (nikdy), nicméně dle doporučení a zkušenosti server specialistů z firmy NWS s.r.o. bylo

nastaveno End a disconnected session na 8 hodin, Active session limit na 12 hodin a Idle session limit na 8 hodin.

Vlastnosti kolekcí lze vidět na obrázku 8 níže. Mezi další vlastnosti kolekce patří specifikace, jak se Remote Desktop Server má zachovat v případě, že je překročen limit spojení, nebo pokud dojde k poruše připojení. V těchto vlastnostech můžeme zvolit buď ukončení spojení, nebo odpojení spojení, které dále umožňuje povolit možnost automatického opětovného připojení (enable automatic reconnection). Poslední vlastností v nastavení spojení (session) pro kolekci je povolení mazání dočasných souborů při ukončení spojení a povolení používání dočasných souborů pro každé spojení zvlášť.



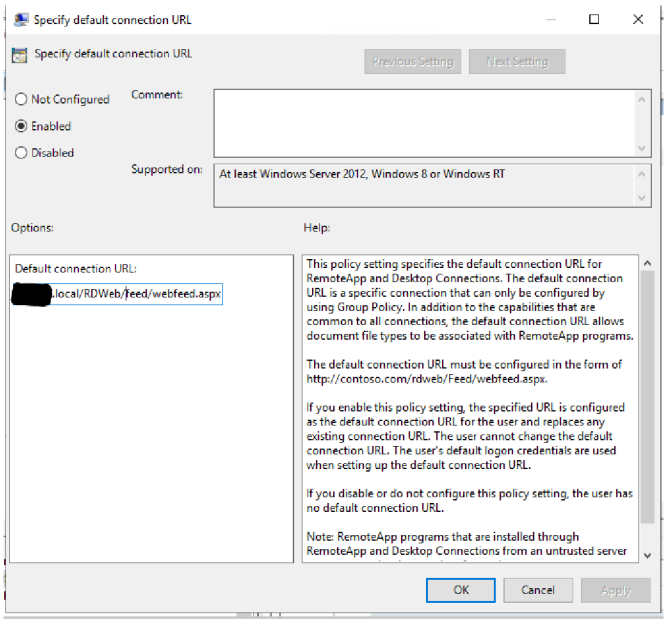
Obrázek 8 Nastavení vlastností kolekce [zdroj: vlastní]

V nastavení kolekcí je dále možné například povolit nebo zakázat přesměrování systémových a hardwarových prostředků z klientského počítače do virtuální session-based plochy. Tato zařízení se poté v operačním systému, ke kterému je uživatel připojen pomocí remote desktop protokolu zobrazují jako „redirected“. Je tedy možné uživateli zakázat například přesměrování systémových disků jeho počítače a naopak povolit přesměrování tiskárny, kterou má uživatel u sebe doma a tím pádem je uživateli umožněno tisknout na ni z aplikace, která běží na vzdáleném serveru a po síťové stránce není se serverem nijak spojena. V tomto konkrétním případě je možné nastavit, aby se primárně používal Remote Desktop Easy Print ovladač tisku. Ostatní nastavení vlastností kolekcí byla ponechána na výchozích hodnotách.

6.9.3. Nasazení RDS Feedu

RemoteApps jsou do osobních počítačů připojovány pomocí RDS feedu, což je URL adresa, specifikující konkrétní pracovní prostředí. Uživateli jsou pomocí této adresy, kterou zadá do konfigurace vzdáleného připojení, přiřazeny aplikace podle oprávnění uživatele, kterým se proti RDS feedu ověří. V operačním systému Windows se RDS feed připojuje skrze „Ovládací panely\Všechny položky Ovládacích panelů\Připojení k aplikacím RemoteApp a vzdáleným plochám“.

Aby každý uživatel nemusel RDS feed do počítače zadávat ručně, nebo aby administrátor nemusel osobně obcházet počítač po počítači, byl RDS feed uživatelům namapován pomocí doménových politik – Group policy (GPO). Doménové politiky jsou spravovatelné na doménovém kontroloru (Domain Controller), což je server, který zajišťuje v doménový síti autentizaci. [44] Doménová politika byla vytvořena přes výchozí nástroj Group Policy Management, kdy byl vytvořen nový Group Policy Object. Objektu byl dán výstižný název „USER – RDS feed“ (politika určená uživatelům). V jeho nastavení byla dále specifikována konkrétní URL adresa ve stromu Uživatelské konfigurace – politiky – administrativní šablony – Windows komponenty – Remote Desktop Services – RemoteApp and Desktop Connections v politice s názvem „Specify default connection URL“ - tedy specifikace výchozího URL spojení. Jako URL adresa byla vložena adresa RDS Feedu, jež je ve výchozím nastavení „ https://název serveru.plně kvalifikovaný název domény/RDweb/feed/webfeed.aspx “, tedy v tomto konkrétním případě byla zadána URL adresa „ https://kos-rds.firmaXYZ.local/RDweb/feed/webfeed.aspx “. Doménová politika k nasazení RDS Feedu je zobrazena na obrázku 9.



Obrázek 9 Nastavení výchozího RDS Feedu v doménové politice [zdroj: vlastní]

6.9.4. Připojení k aplikacím z internetu

Nastavení Remote Desktop Gateway (RDGW)

Pro zpřístupnění aplikací pro uživatele z internetu bez nutnosti používání VPN bylo třeba nakonfigurovat roli Remote Desktop Gateway. V Server Manager byly vybrány Remote Desktop Services / Overwier / Deployment Overview a zde rozbaleny Tasks – Edit Deployment Properties. Zde v nastavení RD Gateway bylo zvoleno „Use these RD Gateway server settings:“, jako Server name bylo zadáno „intranet.firmaXYZ.cz a zaškrnuto „Use RD Gateway credentials for remote computers“ a Bypass RD Gateway server for local adresses“. K právě provedenému nastavení se váže několik náležitostí, které bylo třeba zajistit. První z nich je zakoupení SSL certifikátu, který bude vystaven na hostname (server name) Remote Desktop Gateway a pomocí kterého se bude ověřovat identita serveru, ke kterému se klienti připojují. Certifikát byl zakoupen u certifikační autority Sectigo firmou, pro kterou byly RemoteApps konfigurovány. Druhou náležitostí bylo upravení DNS záznamů vlastníkem, nebo správcem domény. Správce domény proto nastavil veřejný DNS záznam jako nameserver odkazující na intranet.firmaXYZ.cz.

Nastavení routeru/firewallu

Klientské zařízení je schopno připojit se a ověřit se vůči serveru Remote Desktop Gateway (RDGW) na portu 443 (HTTPS). Proto je třeba na routeru či firewallu nastavit port forwarding (v případě nastavení jiného než výchozího portu 443 – překlad portů), nebo virtual server. Smyslem je to, aby v případě, že se klient bude snažit ověřit vůči veřejné IP adrese přes HTTPS, tak bude přesměrován na interní server s interní IP adresou.

Na firewallu Fortinet konfigurace probíhá na záložce Policy & Objects / Virtual IPs. Zde bylo třeba vytvořit pravidlo s následujícím nastavením:

- **Name:** WAN_to_RDS (Dobře popisný název)
- **Interface:** WAN1
- **Type:** Static NAT
- **External IP address/range:** 193.179.32.xxx (veřejná IP adresa firewallu)
- **Map to: IPv4 address/range:** 192.168.101.23 (interní IP adresa RDGW serveru)
- **Optional filters:** povoleno
- **Services:** Jako služba vybrána služba RDS, která napovídá, že bude povoleno na TCP portu pravdilo any > 443 a UDP > 3391.

Před nasazením RemoteApps uživatelům se nesmělo opomenout, že aby byly aplikace dostupné z internetu, musela se adresa RDS feedu v jejich počítačích doménovou politikou, nebo ručně, změnit na https://intranet.firmaXYZ.cz/rdweb//feed/webfeed.aspx.

Funkčnost řešení

Díky předchozímu nastavení jsou doménoví uživatelé schopni spustit vzdáleně ze svého počítače firemní aplikace, běžící pod jejich uživatelským profilem bez nutnosti používání jakékoliv VPN. K připojení je využita Remote Desktop Gateway, která po ověření uživatele zajistí z internetu připojení na Remote Desktop Connection Broker a připojení skončí na Remote Desktop Session Host, kde se uživateli spustí aplikace. Veškerá komunikace probíhá přes protokol HTTPS na portu 443 a aplikace jsou dostupné odkudkoli z internetu. Uživatelé mají aplikace přidané do operační systému pomocí RDS feedu a z uživatelského pohledu se zdá, jako kdyby aplikace běžely lokálně na jejich počítači.

7. Závěr

V diplomové práci byla popsána bezpečnostní řešení a jednotlivé typy VPN – Virtuálních Privátních Sítí, včetně bezpečnostních algoritmů, které tyto VPN využívají. Dále byly v teoretické části popsány některé alternativy, které mohou plně nahradit užívání VPN pro komerční účely. V rámci praktické části byly nakonfigurovány dvě zařízení od dvou různých výrobců pro otestování dvou typů komerčně často využívaných VPN – SSL a IPsec. Zařízení, na kterých byly VPN nakonfigurovány, byly firewally od výrobce Zyxel a od výrobce Fortinet. Oba firewally a obě VPN byly nakonfigurovány se stejným zabezpečením (šifrování, autentikace). Při měření rychlosti, propustnosti a stability nakonfigurovaného Na VPN připojení, pomocí nástroje iPerf3 proti serveru ve vnitřní síti za firewallem, byly zjištěny významné rozdíly v kvalitě spojení mezi firewally dvou zmíněných výrobců. Firewall značky Zyxel – Zywall USG300, skrze SSL typ VPN, nebyl schopen při zasílání TCP packetů dosáhnout vyšší rychlosti než 10 Mbit/s, v porovnání s firewallem Fortinet 40F, na kterém byla naměřena rychlost až 6x vyšší – v průměru čtyřnásobná. Při zasílání UDP packetů byla na Zywall USG300 zaznamenána téměř maximální (88 %) ztrátovost packetů.

Pro ověření, zda se tento problém, či vlastnost, neváže pouze na konkrétní zařízení a konkrétní firmware, bylo stejné měření ověřeno na jiném zařízení výrobce Zyxel, a to na firewallu ATP500. Po naměření SSL VPN, oproti serveru na druhé straně firewallu Zywall ATP500, bylo potvrzeno, že velmi nízká rychlost SSL VPN není závislá na aktuálně nahraném firmwaru, ani na konkrétním hardwaru. Stejné výsledky byly naměřeny na naprosto jiném zařízení, v jiné lokalitě a s jiným připojením k internetu. IPSec VPN se při testování TCP packetů na všech zařízeních (jak zařízení Zyxel, tak zařízení Fortinet) chovala velmi podobně a byly naměřeny srovnatelné rychlosti, odezvy a propustnost. V zasílání UDP packetů přes IPsec VPN byla u zařízení Zyxel zaznamenána značná ztrátovost packetů. Firmě Zyxel je z toho důvodu možné doporučit zanalyzování problému s SSL VPN, jelikož jde o komerčně nejvyužívanější typ VPN, který lze na jejich zařízení nastavit, nebo vydat prohlášení s vysvětlením této vlastnosti, která se na firewally Zywall váže již minimálně 5 let.

Měření pomocí nástroje NetIO GUI zaznamenalo neschopnost doručit UDP packety skrze IPsec VPN Zywall USG300 a skrze SSL VPN Fortinet 40F. U IPsec VPN Fortinet 40F docházelo k timeoutu při odesílání 32KB packetů. Toto chování lze přisoudit aplikaci NetIO

GUI, ke které není dostatečná dokumentace. Nástroj iPerf3 toto chování u UDP packetů nezaznamenával.

Pro důkaz toho, že užívání VPN pro práci z domova či jiné lokality není nutné, byly v rámci praktické části nakonfigurovány Microsoft RemoteApps – aplikace běžící na vzdáleném serveru, na který je připojení zajištěno pomocí Remote Desktop Gateway. Celá konfigurace byla nastavena tak, aby uživatel (zaměstnanec firmy) neměl potřebu cokoliv konfigurovat a aby firemní aplikace, které jsou nainstalovány na firemním interním serveru, byly pro uživatele dostupné odkudkoliv z internetu s neopomenutelným důrazem na bezpečnost řešení. Uživatelům byly do počítače automaticky přidány Remote Desktop připojení k aplikacím, které se neznalému uživateli jeví jako aplikace lokálně nainstalované do jeho počítače.

Nastavení a konfigurace Remote Desktop Gateway a RemoteApps je poměrně složitá a vyžaduje značné zkušenosti administrátora. Administrátor se musí řídit dokumentací společnosti Microsoft nebo diskuzními fóry. Jak bylo vysvětleno v praktické části, Remote Desktop Gateway nabízí vyšší stupeň zabezpečení díky omezení práv každého uživatele, který se skrze Remote Desktop Gateway připojuje na konkrétní aplikaci nebo službu, na kterou má nastavena přístupová práva. V případě, že uživatel nespadá do bezpečnostní skupiny, která má oprávnění přistupovat k dané aplikaci, spojení není vytvořeno. Nutno dodat, že Remote Desktop Gateway neskrývá IP adresu klienta a nedokáže tedy plně nahradit VPN pro všechny případy jejího využití.

Dle naměřených a ověřených informací se IPsec VPN stále jeví rychlostí a stabilitou jako nejvhodnější protokol používaný ve virtuálních privátních sítích (VPN). Svou komplexností a složitostí nastavení, na straně serveru i klienta, je vhodnější k použití pro site-to-site VPN, tedy pro propojení například několika poboček jedné firmy. Pro uživatele je jako firemní VPN vhodnější SSL, která je svou konfigurací značně jednodušší a vyžaduje i pro administrátora minimální znalost tunnelingových (VPN) protokolů.

Pokud jde o výběr hardwaru k provozování VPN, produkty značky Zyxel (řada Zywall) se jeví jako špatná volba pro SSL VPN. K produktům Zywall se vážou vážné nedostatky v propustnosti, které byly zjištěny v této práci. Produkty Fortinet nabízí mnohonásobně lepší a spolehlivější výkon. V neposlední řadě firmware a software FortiOS, který je na všech zařízeních Fortinet naprosto totožný, je velmi intuitivní grafické prostředí. FortiOS administrátorovi při konfiguraci automaticky napovídá a vede ho v krocích k nastavení bezpečného VPN tunelu.

8. Použitá literatura

[1] Frankel a spol., Guide to IPsec VPN, NIST – National Institute of Standards and Technology, revision 1, 2020

[2] KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008. ISBN 9788025122365.

[3] DOYLE, Jeff a Jennifer CARROLL. CCIE professional development routing TCP/IP. 2nd ed. Indianapolis: Cisco Press, 2006. ISBN 9781587052026.

[4] Comparison of VPN Protocols – IPSec, PPTP, and L2TP, Poonam Arora, Prem R. Vemuganti, Praveen Allani, Department of Ecelctrical and Computer Engineering, George Mason University, Fairfax, VA 2202

[5] SSL Certificate & Digital Certificate Authority - SSL.com [online]. [Citace 2. únor 2022] Dostupné z: https://www.ssl.com/cs/Nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-dotazy/co-je-kryptografick%C3%A1-hashovac%C3%AD-funkce/

[6] MS-PTPT: Introduction | Microsoft Docs. [online]. Copyright © Microsoft 2022 [cit. 18. únor 2022]. Dostupné z: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-ptpt/e2eada2f-de4a-4c4a-a543-a90165393521

[7] TCP/IP model encapsulace paketu vs rámec – samuraj-cz.com [online] [citace 5. leden 2022]. Dostupné z: https://www.samuraj-cz.com/clanek/tcpip-model-encapsulace-paketu-vs-ramec

[8] Computer Network | TCP/IP model - javatpoint. Tutorials List - Javatpoint [online]. Copyright © Copyright 2011 [cit. 09.03.2022]. Dostupné z: https://www.javatpoint.com/computer-network-tcp-ip-model

[9] SSL Certificate & Digital Certificate Authority - SSL.com [online]. [cit. 10. leden 2022] Dostupné z: https://www.ssl.com/cs/Nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-dotazy/faq-co-je-ssl/

[10] How to set up a multifunction device or application to send email using Microsoft 365 or Office 365 | Microsoft Docs. [online]. Copyright © Microsoft 2022 [cit. 5. únor 2022].

Dostupné z: https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/how-to-set-up-a-multifunction-device-or-application-to-send-email-using-microsoft-365-or-office-365

[11] SSL protokol :: Informace o certifikátech - SSL certifikáty. SSL Certifikáty - Rapid SSL, GeoTrust, QuickSSL profesionálně [online]. Copyright ©2008 [cit. 3 leden 2022]. Dostupné z: https://www.ssl-certifikaty.cz/o-certifikatech/ssl-protokol/

[12] What Is an SSL VPN? | Fortinet. Fortinet | Enterprise Security Without Compromise [online]. Copyright © 2022 Fortinet, Inc. All Rights Reserved. [cit. 6 prosinec 2021]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/ssl-vpn

[13] Santosh Kumar. Survey on Transport Layer Protocols: TCP & UDP. Sonam Rai Graphic Era University, Dehradun (India) , International Journal of Computer Applications (0975 – 8887)

[14] Přednášky Ing. Zdeněk Votruba – Elektronické instalace budov I. Dostupné z: https://slideplayer.cz/slide/13660558/

[15] Co je URL? | ANT studio. ANT studio | online marketingová agentura [online]. Copyright © 2006 [cit. 14.03.2022]. Dostupné z: https://www.antstudio.cz/slovnik/co-je-url.htm

[16] Paul Ferguson, Geoff Huston – What is a VPN? Cisco Systems, 1998

[17] Rivest, R. The MD5 Message-Digest Algorithm. *ietf.org*. [Online] 1. Duben 1992. [Citace: 20. Únor 2022.] Dostupné z: https://tools.ietf.org/html/rfc1321.

[18] IPSec Overview Part Two: Modes and Transforms > Tunnel and Transport Modes | Cisco Press . Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press [online]. Copyright © 2022 Pearson Education, [cit. 08 leden 2022]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=25477

[19] How IPSec Works > IPSec Overview Part Four: Internet Key Exchange (IKE) | Cisco Press . Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press [online]. Copyright © 2022 Pearson Education, [cit. 08 leden 2022]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=25474&seqNum=7

[20] Remote Desktop Services roles | Microsoft Docs. [online]. Copyright © Microsoft 2022 [cit. 1 březen 2022]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-roles

[21] Authentication Password Protocol | IBM Docs. [online]. Copyright © Copyright IBM Corporation 1998, 2015 [cit. 15. prosinec 2021]. Dostupné z: https://www.ibm.com/docs/en/i/7.4?topic=authentication-password-protocol

[22] PPP Challenge Handshake Authentication Protocol | IETF | Internet Engineering Task Force [online]. [citováno 18. prosinec 2021]. Dostupné z: https://www.ietf.org/rfc/rfc1994.txt

[23] Jazib Frahim, Qiang Huang, SSL remote access VPNs, Ciscopress 2008

[24] Fedor Kállay, Peter Peniak. Počítačové sítě LAN/MAN/WAN a jejich aplikace, Granda publishing, a.s., 2003

[25] Debra Littlejohn Shinder. Počítačové sítě, SoftPress s.r.o.

[26] Kurose, James a Keith Ross. Počítačové sítě, Computer Press, 2014

[27] Jiří Peterka, Referenční model ISO/OSI, Computerworld č. 13/92 1992 Dostupné z: http://www.earchiv.cz/a92/a213c110.php3

[28] Pružmanová, Rita: Moderní komunikační sítě od A do Z, 1998, Computer Press

[29] Zhenjie Yang, Yong Cui, Baochun Li, Yadong Liu and Yi Xu, Software-Defined Wide Area Network (SD-WAN): Architecture, Advances and Opportunities

[30] Oliver Michel, Eric Keller, University of Colorado Boulder, SDN in Wide-Area Networks: A Survey. IEEE. DOI: 10.1109/SDS.2017.7939138

[31] What is SD-WAN? Software-Defined WAN Explained | Fortinet | Enterprise Security Without Compromise [online]. Copyright © 2022 Fortinet, Inc. All Rights Reserved. [cit. 20 únor 2022]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/sd-wan-explained

[32] What Is a Hash Function in Cryptography? A Beginner's Guide - Hashed Out by The SSL Store™. SSL Certificates Provider - Symantec DigiCert Thawte GeoTrust RapidSSL

& Comodo [online]. Copyright © 2022 The SSL Store [cit. 19 únor 2022]. Dostupné z: https://www.thesslstore.com/blog/what-is-a-hash-function-in-cryptography-a-beginners-guide/

[33] The Difference Between SHA-1, SHA-2 and SHA-256 Hash Algorithms. SSL Certificates Provider - Symantec DigiCert Thawte GeoTrust RapidSSL & Comodo [online]. Copyright © 2022 The SSL Store [cit. 19 únor 2022]. Dostupné z: https://www.thesslstore.com/blog/difference-sha-1-sha-2-sha-256-hash-algorithms/

[34] Concepts Layer 2 Tunnel Protocol | IBM Docs. [online]. Copyright © Copyright IBM Corporation 1998, 2014 [cit. 15 únor 2022]. Dostupné z: https://www.ibm.com/docs/en/i/7.3?topic=concepts-layer-2-tunnel-protocol

[35] Understanding VPDN - Cisco. Cisco - Networking, Cloud, and Cybersecurity Solutions [online]. Copyright © [cit. 5 leden 2022]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/dial-access/virtual-private-dialup-network-vpdn/20980-vpdn-20980.html

[36] What is VPN Split Tunneling? | Fortinet. Fortinet | Enterprise Security Without Compromise [online]. Copyright © 2022 Fortinet, Inc. All Rights Reserved. [cit. 3 leden 2022]. Dostupné z: https://www.fortinet.com/resources/cyberglossary/vpn-split-tunneling

[37] Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) - Network Encyclopedia. Network Encyclopedia | Explore, Learn, Master it! [online]. Copyright © 2022 Copyright Network Encyclopedia [cit. 3 leden 2022]. Dostupné z: https://networkencyclopedia.com/microsoft-challenge-handshake-authentication-protocol-ms-chap/

[38] CCIE Routing and Switching v5.1 Foundations: Bridging the Gap Between CCNP and CCIE, Narbik Kocharians, Cisco Press

[39] Firewall policies and VPN configurations, Anne Henmi, Mark Lucas, Abhishek Singh, Chris Cantrell, Syngress 2006

[40] Pete Loshin - TCP/IP Clearly Explained. Internet-Standard.com. Morgan Kaufmann Publishers 2003. ISBN: 1-55860-782-X

[41] Lukáš Urban - Analýza a návrh počítačové sítě komerční firmy dle zásad strukturované kabaláže. ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE, 2020. Bakalářská práce

[42] What Is a Firewall? - Cisco. Cisco - Networking, Cloud, and Cybersecurity Solutions [online]. Copyright © [cit. 2 březen 2022]. Dostupné z: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

[43] What's the Difference between a Switch, a Router, and a Firewall?. IT Support & Outsourced IT Services for Businesses in NH-MA [online]. Copyright © 2022 RMON Networks, Inc. [cit. 2 březen 2022]. Dostupné z: https://rmonnetworks.com/whats-the-difference-between-a-switch-a-router-and-a-firewall/#:~:text=Unlike%20routers%20and%20switches%2C%20firewalls,to%20get%20into%20your%20network.

[44] What Is a Domain Controller?. Purchase Intent Data for Enterprise Tech Sales and Marketing - TechTarget [online]. [Cit. 2 březen 2022] Dostupné z: https://www.techtarget.com/searchwindowsserver/definition/domain-controller

[45] Sucuri WebSite Firewall - Access Denied. Sucuri WebSite Firewall - Access Denied [online]. Copyright © 2019 Sucuri Inc. All rights reserved. [cit. 11.03.2022]. Dostupné z: https://commissum.com/blog-articles/remote-desktop-gateways-a-forgotten-security-feature/

[46] VPNs with Overlapping Subnets Problem Scenario - TechLibrary - Juniper Networks. 301 Moved Permanently [online]. Dostupné z: https://www.juniper.net/documentation/en_US/release-independent/nce/topics/concept/lan2lan-vpn-jseries-srx-series-overview.html

[47] IPSec Overview Part One: General IPSec Standards | Cisco Press . Cisco Press: Source for Cisco Technology, CCNA, CCNP, CCIE Self-Study | Cisco Press [online]. Copyright © 2022 Pearson Education, [cit. 14.03.2022]. Dostupné z: https://www.ciscopress.com/articles/article.asp?p=25470

[48] Advanced Encryption Standard. Tutorialspoint.com [online]. Copyright © Copyright 2021. All Rights Reserved. [cit. 14.03.2022]. Dostupné z: https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

[49] Concepts what is PPP. IBM Docs. [online]. Copyright © Copyright IBM Corporation 1998, 2010 [cit. 20.01.2022]. Dostupné z: https://www.ibm.com/docs/en/i/7.2?topic=concepts-what-is-ppp

[50] What is ipsec | Cloudflare. Cloudflare - The Web Performance & Security Company | Cloudflare [online]. [citováno 5 leden 2022] Dostupné z: https://www.cloudflare.com/learning/network-layer/what-is-ipsec/

[51] Protocols authentication header. IBM Docs. [online]. Copyright © Copyright IBM Corporation 2000, 2010 [cit. 6 prosinec 2021]. Dostupné z: https://www.ibm.com/docs/en/i/7.1?topic=protocols-authentication-header

[52] Difference between AH and ESP protocols. IBM Docs. [online]. Copyright © Copyright IBM Corporation 2000, 2010 [cit. 6 prosinec 2021]. Dostupné z: https://www.ibm.com/support/pages/what-difference-between-ah-and-esp-protocols-ipsec

[53] Alternativní (lepší) klienti pro Windows Remote Desktop < články -> SAMURAJ-cz.com. SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. Copyright © 2005 [cit. 26 listopad 2021]. Dostupné z: https://www.samuraj-cz.com/clanek/alternativni-lepsi-klienti-pro-windows-remote-desktop/

[54] VPN 1 - IPsec VPN a Cisco < články -> SAMURAJ-cz.com. SAMURAJ-cz.com - počítačové sítě, Cisco, Microsoft, VMware, administrace [online]. Copyright © 2005 [cit. 7 listopad 2021]. Dostupné z: https://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/

[55] Remote Desktop Options - Virtual Desktop vs Session-Based Desktop. DesktopReady by Anunta | The Desktop as a Service Solution [online]. Copyright © 2022 Anunta Desktop Inc [cit. 15 listopad 2021]. Dostupné z: https://www.desktopready.com/blog/virtual-desktops-vs-session-based-desktop-what-to-use-when

[56] Understanding How Microsoft VDI Licensing Works. Parallels: Mac & Windows Virtualization, Remote Application Server, Mac Management Solutions [online]. Copyright © 2022 Parallels International GmbH. For more info, please check [cit. 16 listopad 2021]. Dostupné z: https://www.parallels.com/blogs/ras/microsoft-vdi-licensing/

[57] Remote Desktop Protocol (RDP) - Network Encyclopedia. Network Encyclopedia [online]. Copyright © 2022 Copyright Network Encyclopedia [cit. 17 listopad 2021]. Dostupné z: https://networkencyclopedia.com/remote-desktop-protocol-rdp/

[58] Remote Desktop Services Overview | Microsoft Docs. [online]. Copyright © Microsoft 2022 [cit. 16 listopad 2021]. Dostupné z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831447(v=ws.11)

[59] Set up email discovery to subscribe to your RDS feed | Microsoft Docs. [online]. Copyright © Microsoft 2022 [cit. 14 březen 2022]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-email-discovery

[60] Dynamic Host Configuration Protocol (DHCP) | Microsoft Docs. [online]. Copyright © Microsoft 2022 [cit. 14.03.2022]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/networking/technologies/dhcp/dhcp-top

[61] About fully qualified domain names (FQDNs). Indiana University Knowledge Base [online]. Copyright © [cit. 14.03.2022]. Dostupné z: https://kb.iu.edu/d/aiuv#:~:text=A%20fully%20qualified%20domain%20name,be%20mymail.somecollege.edu%20.

[62] iPerf - iPerf3 and iPerf2 user documentation. iPerf - The TCP, UDP and SCTP network bandwidth measurement tool [online]. [Cit 21 únor 2022] Dostupné z: https://iperf.fr/iperf-doc.php

[63] Three More Ways To Measure Network Speed - SmallNetBuilder - Results from #1. Home - SmallNetBuilder [online]. Copyright © 2006 [cit. 26 únor 2022]. Dostupné z: https://www.smallnetbuilder.com/archives/lanwan/lanwan-basics/32252-three-more-ways-to-measure-network-speed?start=1

[64] Co je to VPN? Získejte nejnovější McAfee VPN | McAfee. McAfee | Antivirus, VPN, Identity Protection - Download Free [online]. Copyright © 2022 McAfee, LLC [cit. 17.03.2022]. Dostupné z: https://www.mcafee.com/cs-cz/vpn.html

[65] Co je VPN a jak funguje? Váš základní průvodce.. Avast Blog [online]. Copyright © Avast Software s.r.o. [cit. 17.03.2022]. Dostupné z: https://blog.avast.com/cs/co-je-vpn-a-jak-funguje

[66] Dominik Čáp – Analýza SD-WAN sítí v prostředí Internetu, Česká Zemědělská Univerzita v Praze, 2020, Diplomová práce

[67] What Is Citrix Server and How Does It Work? | Parallels Insights. Parallels: Mac & Windows Virtualization, Remote Application Server, Mac Management Solutions [online]. Copyright © Parallels International GmbH. All rights reserved. [cit. 17.03.2022]. Dostupné z: https://www.parallels.com/what-is-citrix-server/#:~:text=Citrix%20Virtual%20Apps%20isolate%20the,server%20and%20receives%20screen%20updates.

[68] License your RDS deployment with client access licenses (CALs) | Microsoft Docs. [online]. Copyright © Microsoft 2022 [cit. 17.03.2022]. Dostupné z: https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license