Možnosti zabezpečení vzdáleného přístupu

Bc. Jiří Běhal

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Jiří Běhal**
Osobní číslo:	**A20218**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Možnosti zabezpečení vzdáleného přístupu**
Téma práce anglicky:	**Posibilities of Securing Remote Access**

Zásady pro vypracování

1. Specifikujte nejčastěji používané služby/protokoly pro zabezpečení vzdáleného přístupu.
2. Stanovte omezující parametry pro zajištění bezpečného přístupu.
3. Navrhněte vhodné řešení pro bezpečný vzdálený přístup.
4. Proveďte implementaci návrhu v testovacím prostředí.
5. Ověřte funkcni a bezpečnostní prvku řešení, test proveďte s využitím nejčastějších útoku.

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

Seznam doporučené literatury:

1. JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8.
2. POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 8086898385.
3. KOSTOPOULOS, George K. Cyberspace and cybersecurity. 1rd ed. Boca Raton: CRC Press, 2013. ISBN 9781466501331.
4. KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 9788025138250.
5. MATOUŠEK, Petr. Síťové aplikace a jejich architektura. Brno: VUTIUM, 2014. ISBN 9788021437661.
6. LEWIS, Mark. Comparing, designing, and deploying VPNs. Indianapolis: Cisco Press, 2006. ISBN 1587051796.
7. KOSTOPOULOS, George K. Cyberspace and cybersecurity. 1rd ed. Boca Raton: CRC Press, 2013. ISBN 9781466501331.

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

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

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

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN

prof. Mgr. Roman Jašek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 6.5.2021 Jiří Běhal, v.r.

ABSTRAKT

Diplomová práce se zabývá možnostmi zabezpečení vzdáleného přístupu. Cílem práce je navržení vhodného řešení pro bezpečný vzdálený přístup a následná implementace v testovacím prostředí. Funkčnost a bezpečnost navrženého řešení byly otestovány proti nejčastějším útokům. Součástí práce je specifikace nejvíce používaných služeb a protokolů pro zabezpečení vzdáleného přístupu.

Klíčová slova: vzdálený přístup, kyberbezpečnost, zabezpečení

ABSTRACT

This diploma thesis deals with possibilities of secure remote connection. The aim of the diploma thesis is to design optimal solution for securing remote connection and then implementation in testing environment. Functionality and security of designed solution were tested againts most often cyberattacks. One part of thesis is dedicated to specification of most using services and protocols for secure remote connection.

Keywords: Remote connection, Cybersecurity, security

Nejprve bych chtěl poděkovat svému vedoucímu diplomové práce Ing. Davidu Malaníkovi, Ph.D. za odborné vedení, podnětné rady a připomínky, které mi poskytoval během zpracovávání mé diplomové práce. Dále bych chtěl poděkovat své rodině a blízkým za podporu, kterou se mi dostávalo během mého studia.

OBSAH

ÚVOD

Home office byl před nástupem epidemie COVID-19 pro spoustu zaměstnanců příjemný benefit, v jejím průběhu se již stával nutným zlem a s přibývajícími měsíci už to je jen nekonečná rutina a problémy. Pro mnoho IT oddělení však byly tyto měsíce nejnáročnější v historii. Rychlý a většinou nedostatečně připravený přesun do čistě on-line prostředí byl a stále je příležitostí pro kyberzločince. Hlavním problémem, který bylo nutné vyřešit, je, jak budou všichni tito zaměstnanci pracovat z domova? Jak bude možné zajistit co nejvyšší možnou úroveň kyberbezpečnosti, tak jako tomu bylo dříve za „běžných" pracovních podmínek? Jednou z možností je zajistit jim bezpečný vzdálený přístup k interním systémům a počítačům tak, jako by byli fyzicky přítomni v zaměstnání.

Vzdálený přístup je metoda, jak ovládat zařízení, případně práci na něm z jiného vzdáleného místa. Pro určitý typ činností v informatice se tato metoda využívá již dlouhodobě, avšak v dnešní době je stále více používána i pro běžnou práci. Možností a postupů, jak na bezpečný vzdálený přístup, je mnoho, avšak ne vždy jsou ideální.

V teoretické části své diplomové práce se věnuji specifikaci nejčastěji používaných služeb a protokolů pro zabezpečení vzdáleného přístupu. Dále jsou stanoveny obecné omezující parametry, které mohou ovlivnit zajištění bezpečného přístupu.

Návrh vhodného řešení pro bezpečný vzdálený přístup je součástí praktické části diplomové práce. Tento návrh reflektuje zjištěné informace, které jsou popsané v předchozích částech práce. Následuje část věnující se implementaci navrženého řešení v testovacím prostředí. Implementované řešení je ověřeno jak z funkčního, tak také z bezpečnostního hlediska. Testování je provedeno s využitím nejčastějších útoků.

Dílčím cílem této práce je specifikovat služby a protokoly používané pro vzdálený přístup a jejich omezující parametry. Hlavním cílem je však návrh, implementace a otestování vhodného bezpečného a funkčního řešení pro zabezpečený vzdálený přístup.

I. TEORETICKÁ ČÁST

1 SPECIFIKACE SLUŽEB A PROTOKOLŮ

Pro realizaci vzdáleného přístupu lze využít rozdílných služeb a protokolů. Všechny tyto služby a protokoly mají jednu společnou vlastnost, a tou je nutnost připojení na Internet. Z této společné vlastnosti však vyplývá jeden velký problém a tím je bezpečnost. Připojením a komunikací na Internetu se tyto služby a protokoly vystavují riziku napadení. Tak jako jiné IT systémy, i tyto služby a protokoly mají své zranitelnosti. Minulá i současná doba je plná kybernetických útoků, které vyústily v ovládnutí koncových stanic nebo systému, kdy byly k těmto útokům využity zranitelnosti služeb a protokolů pro vzdálený přístup.

V první kapitole teoretické části práce jsou specifikovány nejčastější služby a protokoly, používané pro realizaci vzdáleného přístupu. V rámci specifikace je popsáno také zabezpečení dané služby a protokolu, nejznámější zranitelnosti a pokud jsou známé tak také úspěšné útoky.

Specifikované služby a protokoly:

- RDP,
- VPN,
- TeamViewer,
- NoMachine,
- SSH,
- VNC.

1.1 RDP

RDP neboli Remote Desktop Protocol je protokol, který byl vyvinut firmou Microsoft a který poskytuje uživateli grafické rozhraní pro připojení a ovládání vzdáleného počítače skrze počítačovou síť. Připojení funguje jako klient-server, kde na serveru není oficiálně přidělen TCP port, ale ve výchozím nastavení se používá port 3389 [1].

Obrázek 1. Přihlašovací okno [2]

1.1.1 Základní architektura

Základní architektura Remote Desktop Protocolu je založena na rozšíření rodiny protokolů T.120. Jedná se o vícekanálový protokol, který umožňuje přenášet různé typy informací. RDP je schopný přenášet data až 64 000 oddělenými kanály, nicméně pro aktuální přenos se používá pouze jeden samostatný kanál [3].

Typ přenášených informací:

- Přenos obrazu,
- Šifrovaná data z klávesnice a myši,
- Přenos zvuku.

1.1.1.1 Princip činnosti

Na straně serveru RDP použije vlastní video ovladač pro převedení obrazu z monitoru na síťové pakety, které poté pošle skrze síť klientovi. Na straně klienta RDP obdrží tyto pakety a převede je do GDI pro zobrazení na monitoru. Zajištění vstupních dat od klienta skrze klávesnici a myš je realizováno přímým přesměrováním na server. Na straně serveru RDP používá vlastní ovladače pro klávesnici a myš pro zachycení těchto vstupních dat [1].

1.1.2 Zabezpečení protokolu

Pro zabezpečení přenášených dat přes síť RDP používá RSA šifru spolu s proudovou šifrou RC4. Délka klíče se dá zvolit jako 56 nebo 128-bitová. RDP podporuje také protokol TLS. Zvýšení zabezpečení lze dosáhnout implementací NLA, která vyžaduje před připojením klienta k serveru jeho ověření.

1.1.2.1 Počty RDP a útoků

Výše je uveden jen základní výčet možností, jak zabezpečit RDP. Bohužel žádný systém a jeho zabezpečení není bezchybné a historicky je známo mnoho typů útoků a zranitelností na RDP. Během první vlny epidemie došlo k logickému nárůstu práce z domova, a tedy i častější použití RDP. Dle analýzy internetové vyhledávače Shodan se v březnu 2020 zvýšil počet RDP koncových stanic na internetu o 41 % [4].

Obrázek 2. Počty RDP portů[1] [23]

V korelaci s tímto nárůstem používání RDP byl zaznamenán i vyšší výskyt kyberútoků. Antivirová společnost Kaspersky v této době zachytila nárůst útoků hrubou silou až čtyřnásobně vyšší než v běžných měsících, kdy např. během dubna 2020 došlo v USA až k 1,4 miliónu útoků [5].

1.1.2.2 BlueKeep

BlueKeep (CVE-2019-0708) je označení pro zranitelnost objevenou v RDP protokolu v roce 2019, která existuje v starších operačních systémech (Windows Vista, XP, Server 2003) tak i v „novějších“ (Windows 7, Server 2008). Útočník může využít tuto zranitelnost pro převzetí kontroly nad napadeným systémem a vykonání RCE [6].

[1] Platnost k 15.3.2021

Dopady způsobené tímto typem útoků mohou být velmi vysoké, jelikož útočník v případě úspěchu získá systémová oprávnění nad daným zařízením. S těmito oprávněními útočník ovládá celé zařízení a může přidávat další účty, prohlížet, upravovat a mazat soubory, instalovat programy apod. [6]

Doporučené opatření pro snížení možnosti napadení:

- Instalace dostupných záplat,
- Blokace portu 3389,
- Zablokování RDP jako služby,
- Zavést NLA,
- Přechod na novější OS.

1.2 VPN

Virtuální privátní síť, známá více pod zkratkou VPN, je označení pro privátní síť, která využívá veřejnou síť (většinou Internet) pro propojení vzdálených zařízení uživatelů a sítí. Tento typ propojení zaručuje vyšší stupeň soukromí, anonymity a zabezpečení [7].

Existují dva základní typy VPN:

- Vzdálený přístup (Remote-Access),
- Site-to-site.

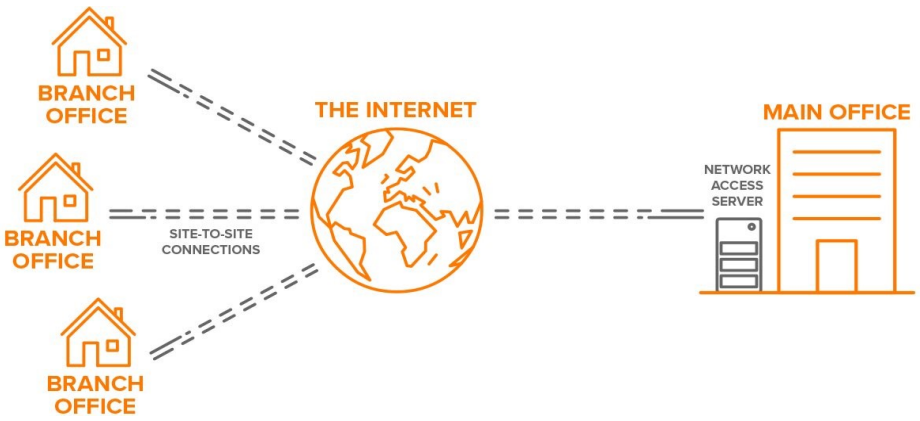
1.2.1 Remote Access

Jedná se o připojení, které je nejčastěji využíváno individuálními uživateli. Tento typ připojení je možné označit také jako host-to-network, kde se připojuje jedno zařízení (počítač) do sítě [8].

Obrázek 3. Remote Access VPN [8]

1.2.2 Site-to-site

Site-to-site VPN je využívána nejčastěji v institucích, které sídlí na různých místech. Pro připojení z těchto míst site-to-site VPN vytvoří uzavřenou interní síť, někdy nazývanou také jako intranet [8].



Obrázek 4. Site-to-site VPN [8]

1.2.3 Zabezpečení

Bohužel služby VPN nelze realizovat kompletně anonymně a bezpečně tak, jak bychom si v ideálním světě přáli, ale existují mechanismy, jak míru anonymity a zabezpečení zvýšit na co nejvyšší úroveň. Proti úniku informací během vzdáleného přenosu s využitím VPN se používají tunelovací protokoly a šifrování.

1.2.3.1 Zabezpečení dle CIA

Jednou z možností, jak na zabezpečení vzdáleného přístupu s využitím VPN lze pohlížet, je zabezpečení informační bezpečnosti dle CIA triády.

Konkrétně se jedná o tyto opatření:

- Důvěrnost (Confidentiality) – pokud by útočník odposlouchával síťový provoz na úrovni paketů, viděl by pouze zašifrovaná data.
- Integrita (Integrity) – používání metod k zajištění integrity, např. hash otisk.
- Dostupnost (Availability) – pouze autentizovaní uživatelé mají přístup do VPN klienta.

1.2.3.2 Bezpečnostní protokoly

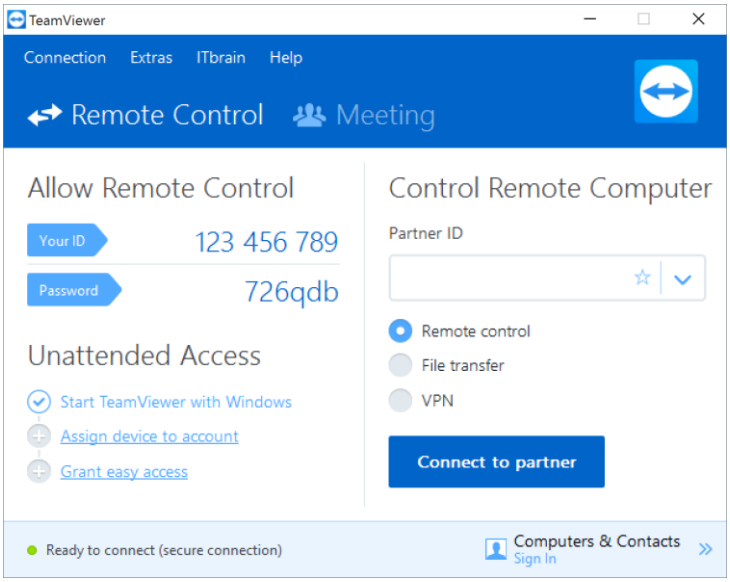
- IPsec – je zkratka pro Internet Protocol Security, což je soubor protokolů využívaných pro zajištění bezpečné výměny paketů skrze nezabezpečené sítě např. Internet. Pro autentizaci jsou podporovány algoritmy SHA-1 a SHA-2. Algoritmus SHA-1 o délce 160 bitů a algoritmus SHA-2 o délce 256 a 512 bitů. Pro šifrování se používá šifra AES s délkou klíče 128, 192 nebo 256 bitů [9].
- SSL/TLS – pomocí tohoto protokolu lze šifrovat celou síť nebo pouze individuálně připojeného uživatele. SSL VPN se používá tam, kde protokol IPsec má problémy s nastavením firewallu a NAT [7].
- PPTP – pro zabezpečení používá 40-bitový a 128-bitový šifrovací protokol Microsoft Point-to-Point Encryption (MPPE)[2] [7].
- L2TP – je zabezpečený tunelovací protokol pro přenos IP provozu s využitím PPP. Nejlepší možnou volbou, jak bezpečně používat L2TP protokol, je zašifrování dat pomocí IPsec. Standart L2TP uvádí jako nejlepší bezpečnou možnost pro zašifrování a přenos dat použít L2TP skrze IPsec [10].

1.3 TeamViewer

Další možností pro vzdálený přístup je program TeamViewer, který je díky snadnému a přehlednému uživatelskému rozhraní u veřejnosti velmi populární. Jedná se o multiplatformní program, který běží na OS Windows, macOS i na Linux. Další výhodou je možnost připojení z mobilního zařízení na koncové stanice. TeamViewer je taktéž kompatibilní s mobilními zařízeními běžícími na odlišných OS, a to na Android, iOS, Windows 10 Mobile nebo BlackBerry [11].

Program TeamViewer umožňuje vytvořit VPN spojení, kdy na obou propojených koncových stanicích musí být nainstalovaný speciální typ TeamVieweru [11].

[2] Tento protokol není považován za bezpečný a neměl by se tedy již používat.



Obrázek 5. Hlavní okno TeamViewer [12]

1.3.1 Zabezpečení

K zajištění co nejvyšší úrovně zabezpečení vzdáleného přístupu TeamViewer využívá šifrování, dvou faktorovou autentizaci, ochranu proti útokům hrubou silou a další.

TeamViewer pro výměnu privátních a veřejných klíčů využívá šifru RSA o délce 4096 bitů. Přenášená data jsou zašifrována pomocí AES o délce 256 bitů. Pro dvou faktorovou autentizaci je nutné zadat kód z mobilního telefonu, kdy tento kód je vygenerován pomocí TOTP algoritmu. Při snaze o útok hrubou silou TeamViewer jako protiopatření exponenciálně zvyšuje latenci mezi přihlašovacími pokusy [13].

Mezi další dílčí prvky zvyšující zabezpečení je v programu TeamViewer implementována ochrana přenosu souborů, potvrzení důvěryhodného zařízení při prvním propojení, detekce neobvyklého chování uživatelských účtů (např. připojení z jiné nebo neobvyklé lokality).

1.4 NoMachine

NoMachine je označení pro NX technologii, která nám umožňuje se vzdáleně připojovat ke koncovým stanicím, sdílet plochu, posílat soubory a další. V současné době je NX technologie a produkt NoMachine dostupný pro všechny nejpoužívanější typy OS (Windows, Mac, Linux) a také pro mobilní zařízení (iOS, Android, Raspberry). Podobně jako ostatní služby používané pro vzdálený přístup NoMachine využívá pro autentizaci několik odlišných metod. Samozřejmostí je potom šifrování všech přenášených dat. Jedná se o řešení, které je pro individuální uživatele zdarma, což poskytuje NoMachine výhodu oproti konkurentům [14].

1.4.1 Zabezpečení

Autentizace je jednou ze základních a běžně používaných variant, jak zvýšit zabezpečení. NoMachine od verze 4.0, kde už je defaultně používán NX protokol, umožňuje tyto autentizační metody:

- Heslo,
- Privátní klíč,
- Kerberos protokol.

Jednou z možností, kterou protokol NX umožňuje u verze Enterprise, je posílat data skrze SSH. Pokud je tento protokol použit, tak se autentizační metody rozšíří ještě o použití klíče od SSH agenta a čipové karty, které mají v sobě nahrán SSH privátní klíč. Dnes již běžná metoda ověření pomocí dvou faktorové autentizace je v tomto řešení také obsažena [15].

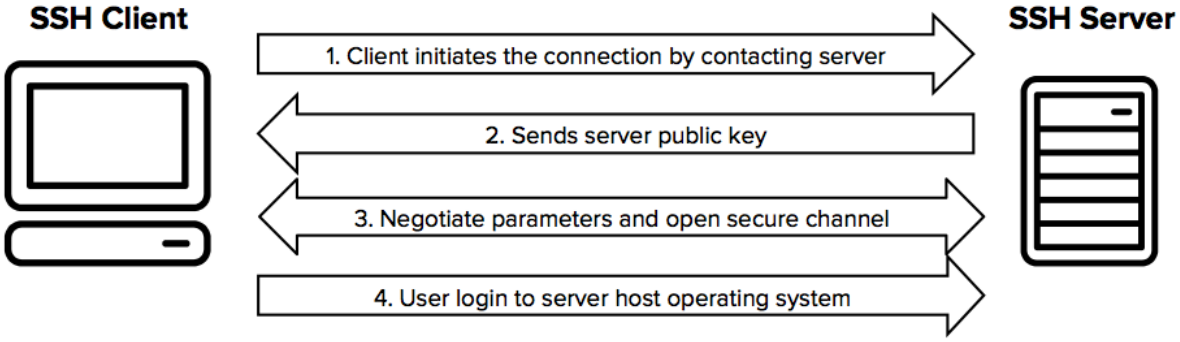
Pro šifrování dat je již od zmiňované verze 4.0 použitá šifra AES s 128bitovým klíčem. Pro zpětnou kompatibilitu s nižšími verzemi je použita šifra RC4. Placená verze NoMachine Enterprise umožňuje tunelování skrze SSH protokol [16].

1.5 SSH

SSH protokol je metoda pro zabezpečený vzdálený přístup mezi koncovými stanicemi. Impulsem pro vznik tohoto protokolu bylo nahradit dříve používané nezabezpečené protokoly (např. Telnet, rlogin). Pro zabezpečení používá SSH protokol autentizaci uživatele a šifrování.

1.5.1 Princip činnosti

Princip činnosti protokolu je založen na modelu klient-server, tedy kdy připojení je navázáno ze strany SSH klienta připojením na SSH server. Pro autentizaci klienta na serveru je využíván veřejný šifrovací klíč, případně heslo. Jakmile je navázáno spojení, SSH protokol používá pro ochranu přenášených dat symetrické šifrování a hashovací algoritmy [17].



Obrázek 6. Spojení klient-server SSH protokol [17]

Pro šifrování přenášených dat SSH protokol používá šifrovací algoritmus AES. K zajištění integrity je použito standardních hashovacích algoritmů, které patří do skupiny SHA-2 [17].

1.5.2 Bezpečnost a útoky

I přes maximální možnou snahu zabezpečit SSH protokol co nejlépe, existují hackovací nástroje, útoky a další možnosti, jak toto zabezpečení prolomit.

BothanSpy a Gyrfalcon jsou hackovací nástroje, které cílí na různé typy implementací SSH protokolu a snaží se ukrást přihlašovací jména, hesla a SSH klíče. Dle série dokumentů zveřejněných serverem Wikileaks v roce 2017 (označované jako Vault 7) byly tyto nástroje vyvinuty a používány CIA [18].

Z principu fungování je SSH náchylné vůči MITM útoku. Pro zamezení těchto typů útoků musí být mezi klientem a serverem určitý typ sdíleného tajemství. Nejvíce běžně používané metody jsou:

- X.509 certifikát,
- Proprietární certifikační mechanismus,
- Veřejný klíč na straně klienta, privátní na straně serveru,
- Sdílené tajná hodnota, např. předem sdílené klíče [19].

1.6 VNC

Posledním specifikovaným protokolem pro vzdálený přístup je Virtual Network Computing, který umožňuje grafické sdílení obrazovky vzdáleného počítače. K tomuto sdílení VNC využívá RFB protokol. Jedná se o multiplatformní protokol, který funguje na principu klient-server. Ve výchozím stavu je použit port 5900 [20].

Momentálně existuje velké množství upravených variant VNC, kdy některé jsou optimalizované pro Windows, jiné umožňují sdílet soubory apod. Společnosti, které umožňují vzdálený přístup s využitím VNC protokolu, jsou např. RealVNC nebo UltraVNC.

1.6.1 Zabezpečení

Zabezpečení VNC je ve výchozím stavu nedostatečné, kdy se zejména RFB protokol nedá považovat za bezpečný. V některých případech RFB protokol nevyžaduje ani autentizaci. V ostatních případech při použití autentizace klient musí zadat heslo, které je šifrované šifrou DES a má pouze 8 znaků. Tento typ autentizace je ale považován za kryptograficky slabý a nedoporučuje se využívat v nedůvěryhodných sítích [21].

Tyto nedostatky jsou však v dnešní době již vyřešeny, kdy např. společnost RealVNC používá šifru AES o délce klíče 128 nebo 256 bitů v závislosti na zvoleném produktu [22].

Pro zvýšení zabezpečení se používá také tunelování skrze VPN nebo SSH.

2 OMEZUJÍCÍ PARAMETRY

Během implementace nových technologií, postupů a procesů se vždy objeví problémy, ať už menšího či vážnějšího charakteru a nejinak je tomu i při realizaci řešení pro vzdálený přístup. Častějším problémům nahrává i rychlý přesun mimo firemní prostředí, na který mnoho organizací nebylo připraveno. Nepřipravenost se může projevit v různých oblastech od HW a SW vybavení až po aplikaci a dodržování interních bezpečnostních procesů, např. bezpečnostních politik.

Obsahem této kapitoly je stanovení omezujících parametrů, které mohou ovlivnit zajištění bezpečného přístupu. Jedná se o tyto omezující parametry:

- Roztříštěnost OS,
- End-of-life OS,
- Domácí počítač,
- Síť mimo pracoviště,
- Cena,
- Možnosti monitoringu,
- Doba realizace.

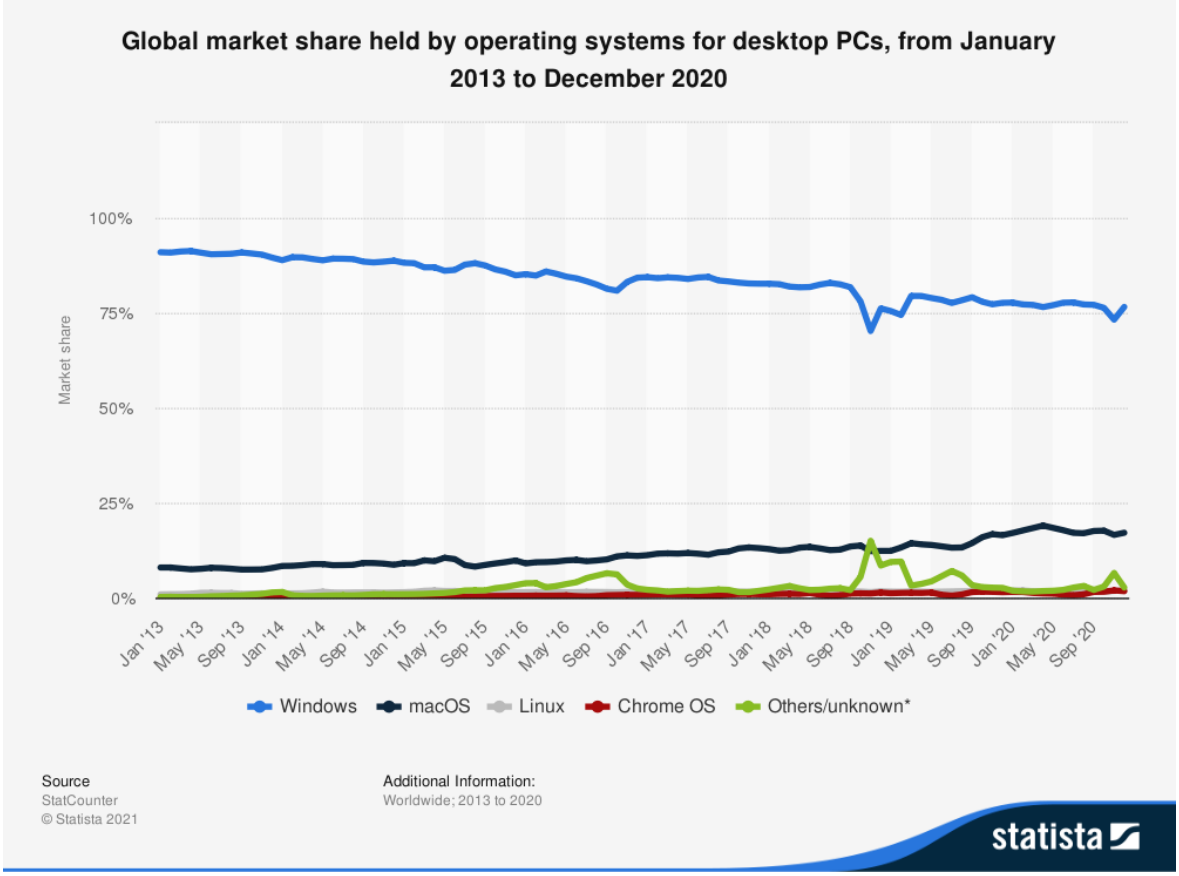
2.1 Roztříštěnost OS

Jedním z omezujících parametrů pro zajištění bezpečného přístupu je roztříštěnost OS v rámci organizace. Tato roztříštěnost velmi komplikuje výběr správného a bezpečného řešení pro vzdálený přístup. Jedná se zde nejen o rozdílné OS pracovních stanic, ale také mobilních telefonů a dalších zařízení. Omezujícím parametrem jsou také pravidelně neaktualizované OS, v nejhorším případě OS po konci podpory ze strany výrobce.

2.1.1 Přehled OS

Roztříštěnost OS je ovlivněna mnoha faktory, např. o jaký typ organizace se jedná, zdali o státní nebo soukromou, na její velikosti, jestli umožňují BYOD a další. Charakter vykonávané práce také ovlivňuje výběr používaných OS.

Přehled výskytu nejpoužívanějších OS běžících na koncových stanicích v období od roku 2013 do roku 2020 je zobrazen na následujícím obrázku.



Obrázek 7. Přehled OS [24]

Z výše uvedeného grafického zobrazení používaných OS (*Obrázek 7.)* lze jasně vidět, že dominance OS Windows již není tak vysoká jako v minulosti. V souvislosti s tímto trendem je zřejmé, že omezující parametr roztříštěnost OS bude mít v budoucnu stále větší váhu.

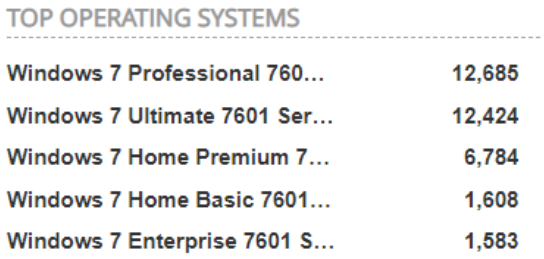
2.2 End-of-life OS

End-of-life neboli také konec podpory OS je velmi omezujícím parametrem pro zajištění bezpečného přístupu. Ukončením podpory ze strany poskytovatele již dále není dostupná technická podpora při potížích a aktualizace software. Nejrizikovějším omezujícím parametrem je ale ukončení vydávání bezpečnostních aktualizací a oprav proti objeveným zranitelnostem a chybám. Pro kyberzločince jsou poté stanice s těmito OS častým a snadným terčem.

2.2.1 EOL Windows 7

Aktuálním bezpečnostním rizikem je používání OS Windows 7 i po ukončení podpory. Společnost Microsoft ukončila podporu tohoto OS po 10 letech dne 14. ledna 2020. Dle

dostupných zdrojů však stále existuje velké množství uživatelů a stanic, které používají tuto verzi OS Windows.



Obrázek 8. Počet stanic s OS Windows 7 [3] [25]

2.3 Domácí počítač

Dalším omezujícím parametrem jsou domácí soukromé počítače, kdy v některých případech je uživatel nucen jej využívat i pro pracovní účely. Jednou z forem práce je možnost BYOD do firemního prostředí a poté i domů. Ačkoli BYOD může mít pro zaměstnavatele velké výhody, tak z pohledu kyberbezpečnosti je většinou problematické.

2.3.1 Problémy

Při využívání domácích nebo vlastních zařízení se mohou vyskytnout problémy a omezení různého typu, které se v běžném firemním prostředí a zařízeních vyskytují jen zřídka. Jedná se např. o tyto:

- Pravidelnost aktualizací,
- Aplikace a vynucení dodržování bezpečnostních politik a interních procesů,
- HW a SW požadavky,
- Oddělení soukromých a pracovních účtů,
- Bezpečnostní monitoring,
- Dostupnost služeb a dat.

[3] Platnost k 15.3.2021.

2.4 Síť mimo pracoviště

Omezující parametr, který do určité míry souvisí i s předchozím bodem, je připojení na síť mimo pracoviště (např. doma, co-working). Z provozního hlediska se jedná o problémy s poskytovateli, kteří mohou být různí, a také s rychlostí a spolehlivostí připojení.

Z bezpečnostního hlediska je zde mnoho parametrů, které je nutné vzít v potaz. Jedná se např. o tyto:

- Zabezpečení Wifi routeru,
- Bezpečnostní monitoring (IoC),
- Ochrana perimetru (Firewall, DDOS),
- Ochrana a monitoring zařízení,
- Dostupnost služeb.

2.5 Cena

Nejenom v rámci řešení vzdáleného přístupu je cena jedním z hlavních omezujících parametrů. Ekonomická návratnost a nezbytná finanční investice je všudypřítomný faktor u všech typů projektů. Názory a náhled na výši investice se také liší typem společnosti, oblastí, ve které působí anebo s jakými daty pracují (např. osobní údaje, know-how, utajované informace apod.). V některých případech by při úniku dat následné pokuty od regulačních úřadů výrazně převyšovaly vstupní investice do zabezpečení vzdáleného přístupu. Je tedy důležité pro každou společnost si hned v počátku projektu stanovit, kolik peněz jsou ochotny investovat. V návaznosti na toto rozhodnutí totiž poté mohou být některé technologie a řešení vynechány z finančních důvodů hned od začátku řešení projektů.

Cena za adekvátní zabezpečení vzdáleného přístupu může být ovlivněna více faktory. Konkrétně se jedná o tyto:

- Nutnost nákupu nového software,
- Počet licencí k tomuto software,
- Nákup specializovaného hardware,
- Cena za implementaci do stávající IT infrastruktury,
- Platba za podporu.

2.6 Možnosti monitoringu

Jedním z důležitých prvků pro zajištění kyberbezpečnosti ve společnostech je monitoring provozních a bezpečnostních událostí v infrastruktuře. Tento monitoring se využívá nejen pro zajištění kyberbezpečnosti v reálném čase, ale také jako důležitý zdroj informací pro vyšetřování bezpečnostních incidentů. Problém nastává, pokud je nutné zajistit tento monitoring i při vzdáleném přístupu, např. z domácího počítače, sítě atd. V některých případech je dokonce zákonná povinnost zajistit tento monitoring a případné důležité informace, pokud by se vyskytl bezpečnostní incident předat příslušným orgánům. V ČR se této oblasti věnuje NÚKIB, kde se zákonná povinnost vztahuje na organizace patřící mezi Kritickou informační infrastrukturu. Při řešení anebo vyšetřování bezpečnostních incidentů je povinnost spolupracovat s tímto orgánem a dodat mu všechny podklady (např. logy).

2.7 Doba realizace

Pro společnosti, které potřebují vyřešit vzdálený přístup v krátkém časovém intervalu, je dopad tohoto omezujícího parametru významný. Doba realizace se odvíjí od náročnosti zvoleného řešení a použitých technologií.

Významně ji může ovlivnit vhodné nastavení vnitřních procesů a typ organizace, kdy je z praxe známé, že soukromé firmy se dokážou s tímto problémem vypořádat efektivněji než státní sféra. Naopak negativně ji mohou ovlivnit používané technologie a nastavení vnitřní infrastruktury společností, která není vhodná pro realizování vzdáleného přístupu bez jakýchkoliv úprav. Při realizaci vzdáleného přístupu je nutné počítat nejen s řešením po technologické stránce, ale i s administrativními a právními omezeními, které mohou celkovou dobu velmi výrazně prodloužit.

2.8 Určení důležitosti omezujících parametrů

Škálování hodnot

Váha byla přidělena podle toho, jaký má omezující parametr dopad na běh společnost. Rozmezí vah je od 1 do 5, kde jednička znamená nejnižší a pětka značí nejvyšší váhu.

Podle závažnosti dělíme omezující parametry do tří skupin s označením nízká, střední a vysoká vážnost. Číselný převod je následující:

- Nízká – 1 bod,

- Střední – 2 body,
- Vysoká – 3 body.

Výsledek vzniká vynásobením váhy a vážnosti, kde čím vyšší výsledek pro omezující parametr vyjde, tím je pro nás tento parametr důležitější.

Tabulka 1. Určení důležitosti omezujících parametrů

Omezující parametr	Váha	Vážnost	Výsledek
Roztříštěnost OS	3	střední	6
EOL OS	4	vysoká	12
Domácí počítač	2	nízká	2
Síť mimo pracoviště	1	nízká	1
Cena	3	střední	6
Monitoring	2	střední	4
Doba realizace	3	vysoká	9

Dle výsledků z *Tabulky 1.* byl jako nejdůležitější omezující parametr určen používaní EOL systémů. Dalším důležitým omezujícím parametrem je doba realizace, kdy organizace potřebují rychle a pružně reagovat na přesuny na home-office. Na stejné úrovni z pohledu důležitosti je poté omezující parametr roztříštěnost OS spolu s cenou za realizaci bezpečného vzdáleného přístupu.

II. PRAKTICKÁ ČÁST

3 NÁVRH ŘEŠENÍ

Možností, vhodných technologií a přístupů, jak navrhnout řešení pro bezpečný vzdálený přístup, je mnoho, vždy ale záleží na okolnostech, které toto řešení omezují. Obsahem této kapitoly tedy je návrh řešení, které reflektuje nejdůležitější omezující parametry pro zajištění bezpečného vzdáleného přístupu. Tyto omezující parametry jsou stanoveny a popsány v druhé kapitole této práce.

3.1 Výběr vhodné technologie

Výběr vhodné technologie pro návrh řešení byl realizován vícekriteriálním hodnocením nejpoužívanějších technologií pro bezpečný vzdálený přístup. Jako vstupní kritéria pro vyhodnocení, které technologie jsou nejvhodnější, byly použity nejdůležitější omezující parametry doplněné o další vhodná kritéria.

Konkrétně se jedná o tyto:

- Podpora pro EOL OS,
- Access listy,
- Multiplatformnost,
- Náročnost konfigurace,
- Cena.

Škálování hodnot:

Pokud technologie podporuje EOL OS, tak získá jeden bod, pokud tomu tak není, bodů je nula.

Jestliže je možnost řešení přístupu přes Access listy přímo integrována do použité technologie, tak získá jeden bod, pokud tomu tak není, tak nula bodů.

Za podporu multiplatformních OS je zisk jednoho bodu, jinak je bodů nula.

Jestli lze pro konfiguraci využít GUI, tak daná technologie získá jeden bod, pokud ne, tak nula bodů.

Pokud se jedná o open-source technologii, tak je udělen jeden bod. V některých případech záleží od konkrétního typu, zdali je technologie zdarma či nikoliv, a proto je v tomto případě přiděleno nula bodů.

Výsledek vzniká sečtením všech bodů u dané technologie.

Tabulka 2. Vícekriteriální hodnocení technologií

	Kritérium					
Technologie	Podpora EOL systémů	Access listy	Multiplatformnost	Konfigurace	Cena	Výsledek
IPsec	1	0	1	0	1	3
L2TP	1	0	1	0	1	3
SoftEther	1	1	1	1	1	5
Wireguard	1	0	1	0	1	3

Na základě výsledků získaných z vícekriteriálního hodnocení vhodných technologií (*Tabulka 2.*) byla vybrána jako nejlepší technologie SoftEther. Jedná se o technologii SoftEther VPN, která nejlépe řeší omezující parametry a která byla použita pro návrh řešení. Jako záložní varianta při nedostupnosti VPN bude sloužit SSH.

3.2 SoftEther VPN

Pro zabezpečení přístupu do interní sítě organizace byla zvolena technologie SoftEther VPN. Toto vybrané VPN řešení splňuje všechny nejdůležitější omezující parametry (*viz. Tabulka 1.*).

SoftEther VPN je open-source akademický projekt japonské univerzity Tsukuba.

Omezující parametry splňuje následovně:

- Pro organizace, ve kterých se i přes snahu o aktualizaci či výměnu starších OS za novější stále vyskytují EOL OS, nabízí SoftEther VPN řešení. Tato VPN podporuje Microsoft SSTP VPN pro OS Windows ve verzi Vista/7/8.
- Doba realizace je závislá čistě od schopností IT pracovníků implementovat, nakonfigurovat a uvést do provozu řešení SoftEther VPN.
- Plná multiplatformnost je zajištěna, kdy podporuje OS Windows, Linux, Mac, Android, iPad a Windows Mobile.

- Jedná se o bezplatnou verzi VPN, takže celková suma za toto řešení se po technické stránce odvíjí od pořizovacích nákladů na hardwarové prvky.

Pro zvýšení zabezpečení byl přidán další omezující parametr, který bude řešit úroveň přístupů přes VPN. Přístupy se budou definovat podle rozsahů IP adres (*viz Tabulka 3.*). Konkrétně se jedná o přístupy definované v těchto rolích:

- Uživatel,
- Privilegovaný uživatel,
- Správce.

První definovaná role je běžný uživatel, který bude mít základní přístup k systémům nutným pro výkon jeho pracovních úkolů. K ostatním částem sítě a systémům nebude mít přístup.

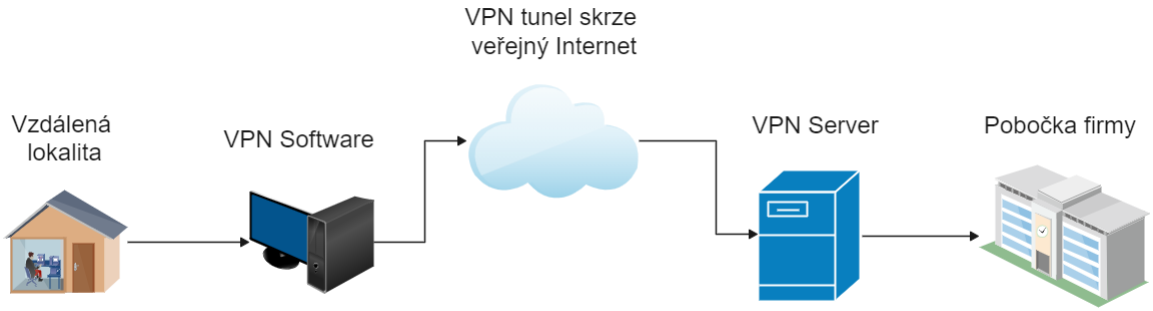
Role privilegovaného uživatele lze chápat jako nadřízené běžných uživatelů, kteří potřebují mít přehled nad celým fungováním organizace. Typicky se jedná o vyšší management, ředitele, CEO, majitele apod.

Správce je role pro pracovníky IT oddělení dané organizace, kteří se starají o provozní záležitosti a dostupnost služeb.

Tabulka 3. Rozsahy IP adres

Role	Rozsah IP
Uživatel	192.168.1.1 – 192.168.1.254
Privilegovaný uživatel	192.168.10.1. – 192.168.10.254
Správce	192.168.20.1 – 192.168.20.254

3.3 Schéma



Obrázek 9. Schéma navrženého řešení

4 IMPLEMENTACE

Tato kapitola čtenáře provede implementací navrženého řešení v testovacím prostředí. Každá část navrženého řešení zde bude detailněji popsána. Součástí této kapitoly jsou také screenshoty z průběhu implementace řešení spolu s nezbytným vysvětlením nejdůležitějších kroků a fází implementace. Pro účely testovacího prostředí je využita univerzitní infrastruktura v laboratoři výpočetní techniky.

Testovací prostředí se skládá konkrétně z těchto prvků:

- Virtuální server s OS Ubuntu,
- Virtuální počítače s OS Windows 10,
- Fyzický počítač s OS Windows 10.

4.1 Konfigurace serveru

Jako první krok při implementaci navrženého řešení je nutné správně nakonfigurovat server. Tato konfigurace spočívá především ve stažení softwaru SoftEther VPN server. Tento software je vybaven vším, co je nezbytné pro funkční implementaci navrženého VPN řešení, kde nás zajímá zejména dostatečný výkon, funkcionality, zabezpečení, škálování a přenositelnost. Jedná se o stěžejní část SoftEther VPN systému, jelikož pouze prostřednictvím tohoto softwaru je možné se poté přes VPN Client Managera vzdáleně připojit.

4.1.1 Postup konfigurace

V této části práce bude definován postup konfigurace serveru krok za krokem, tedy jak správně implementovat software SoftEther VPN server.

Vzhledem k tomu, že se jedná o open-source řešení, tak lze tento software stáhnout z oficiálních stránek výrobce, které se nachází na adrese https://www.softether.org/. Stránky jsou dostupné pouze v angličtině, proto pro větší přehlednost nebudou některé pojmy přeloženy do češtiny.

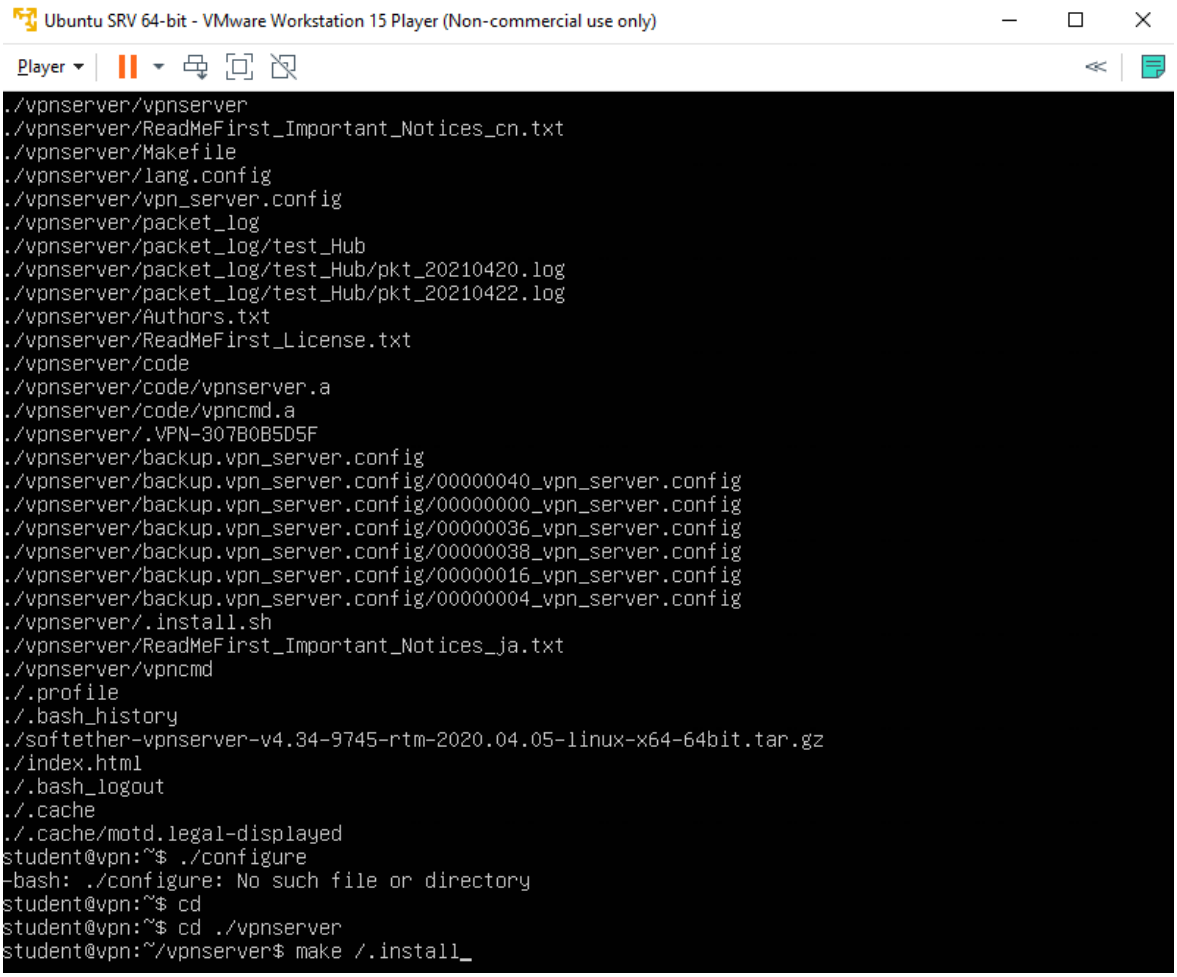
Na stránkách výrobce si najdeme záložku Download a zde vybereme požadovaný software. Vzhledem k použitému typu serveru je nutné vybrat tyto možnosti:

- Select Component – SoftEther VPN Server,
- Select Platform – Linux,
- Select CPU – Intel x64 / AMD64 (64bit).

Použita byla poslední dostupná verze:

SoftEther VPN Server (Ver 4.34, Build 9745, rtm), softether-vpnserver-v4.34-9745-rtm-2020.04.05-linux-x64-64bit.tar.gz (7.16 MB)

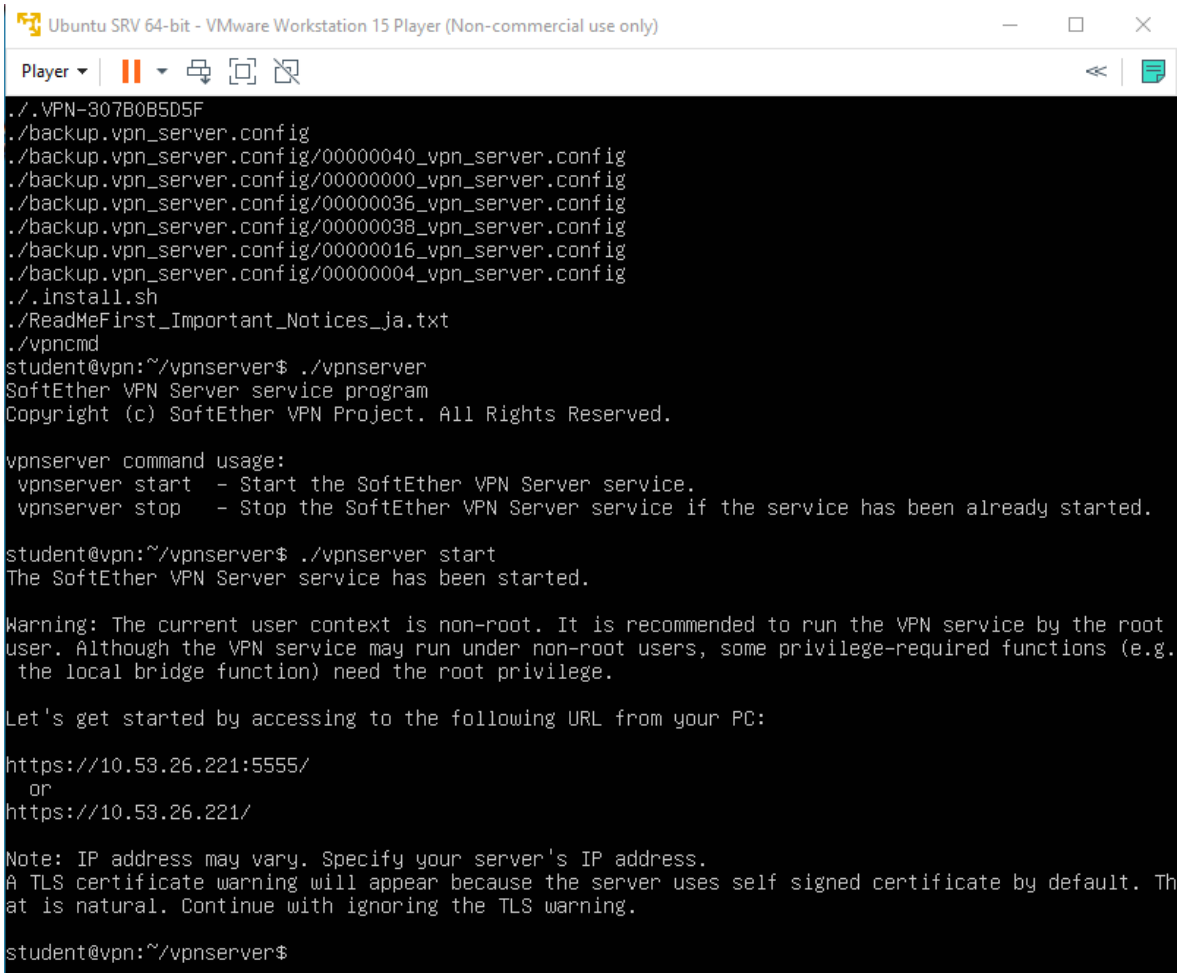
Tak jako je to u serverů běžné, nedisponují grafickým rozhraním, ale komunikace probíhá pouze prostřednictvím příkazového řádku, takže pro stažení byl použit příkaz *wget.* Stažené soubory je poté nutné extrahovat a naistalovat.



Obrázek 10. Obsah staženého souboru

Pro instalaci je nutné se nacházet ve správné složce a následně spustit příkaz *make /.install*. Dále musíme odpovědět na otázky, které se obecně vyskytují při instalacích, např. že jsme si přečetli a rozumíme licenčním podmínkám, souhlasíme s podmínkami užívání apod. Po zodpovězení těchto otázek dojde k instalaci softwaru SoftEther VPN server.

Na závěr je příkazem *./vpnserver start* nastartována služba SoftEther VPN server.



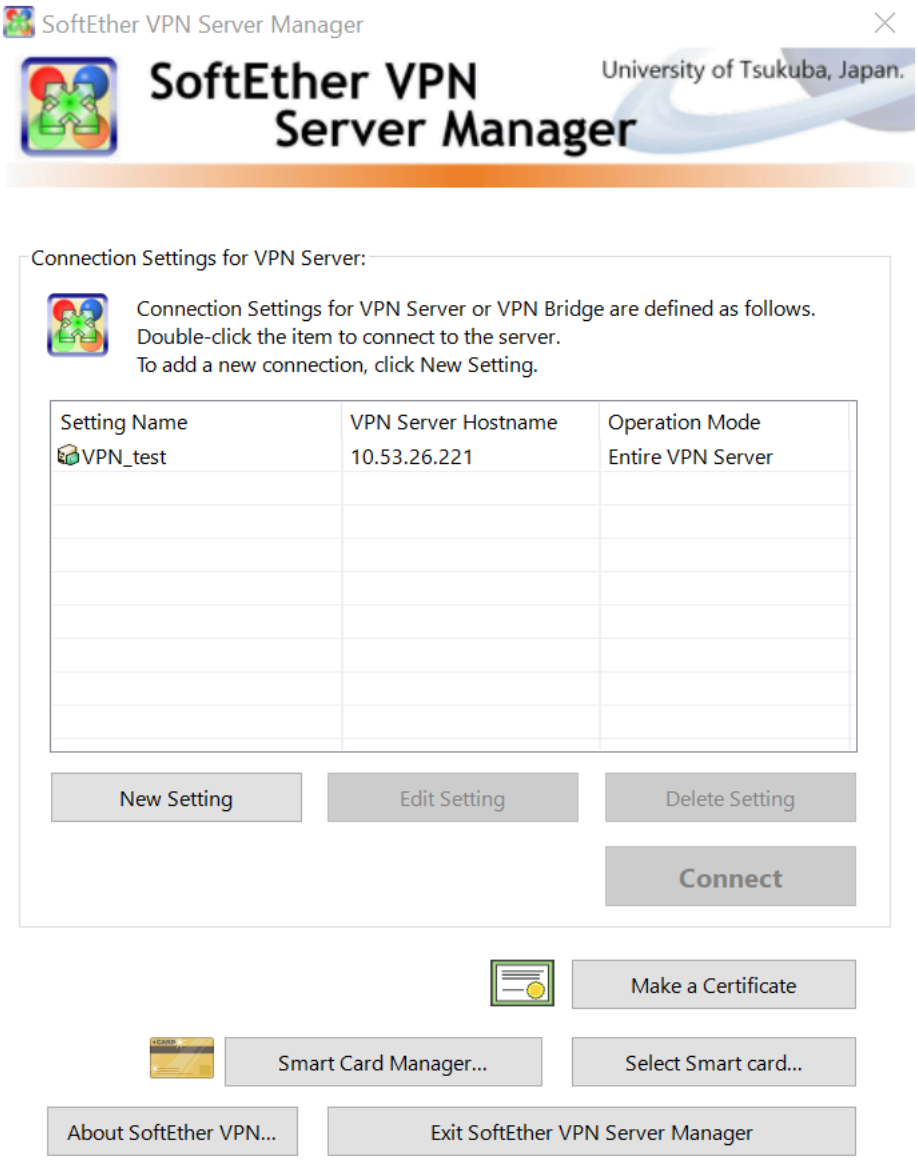
Obrázek 11. Start SoftEther VPN server

Služba SoftEther VPN server byla nastartována a pro informace o tom, jaké jsou další možnosti administrace, je vhodné přistoupit na link *https://10.53.26.221:5555/*. Link je složen z IP adresy, na které se server nachází, a z otevřeného portu.

Pro následující administraci serveru byl použit SoftEther VPN Server Manager.

4.2 SoftEther VPN Server Manager

Jakmile je na serveru správně naistalován a spuštěn software SoftEther VPN Server, tak pro správu tohoto serveru využijeme SoftEther VPN Server Manager. Tento styl správy serveru je také doporučovaný výrobcem. SoftEther VPN Server Manager je dostupný pouze pro zařízení s OS Windows a macOS.



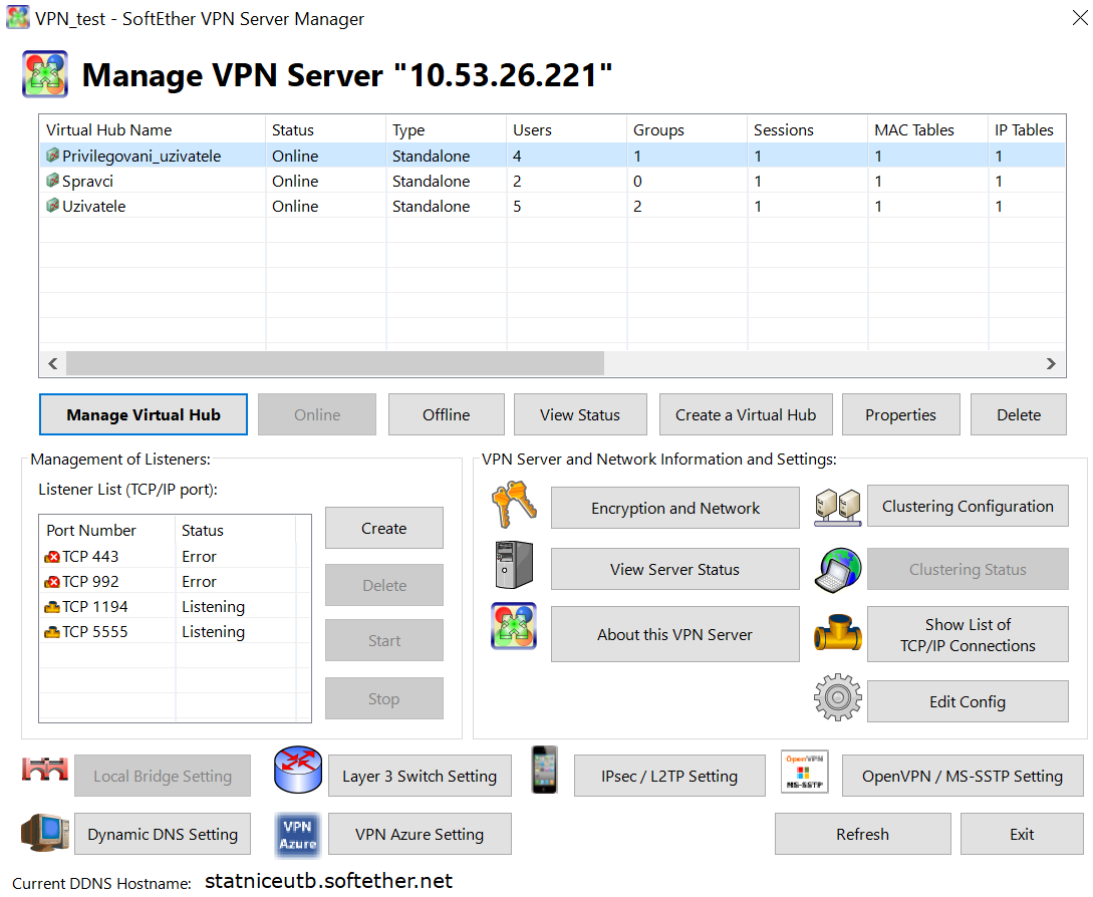
Obrázek 12. SoftEther VPN Server Manager

Jak lze vidět na *Obrázku 12.*, tak rozhraní pro správu serveru je uživatelsky velmi přehledné. Přes New Setting je možné připojit nový server, kde je nutné vyplnit jméno, ale především destinaci VPN serveru, tedy host name nebo IP adresu a číslo portu. Pomocí Edit Setting je možné stávající nastavení změnit nebo poupravit. Delete Setting slouží k odstranění nastavení.

Nastavení serveru:

- Name – VPN_test,
- Host Name – 10.53.26.221,
- Port Number – 5555.

Po dokončení nastavení se přes Connect připojíme k našemu serveru.



Obrázek 13. Manage VPN Server

Pokud je vše správně nastaveno, dojde k připojení k serveru (*viz Obrázek 13.*). Zde můžeme vytvářet, spravovat a dále pracovat s Virtual Huby. Najdeme zde také detailní informace o VPN serveru a o jeho aktuálním stavu. Aktivní připojení k serveru lze vidět pod položkou Show List of TCP/IP Connections, kde, pokud je to nutné, lze také připojení druhé strany zrušit. Další položky v tomto okně nebyly při implementaci využity.

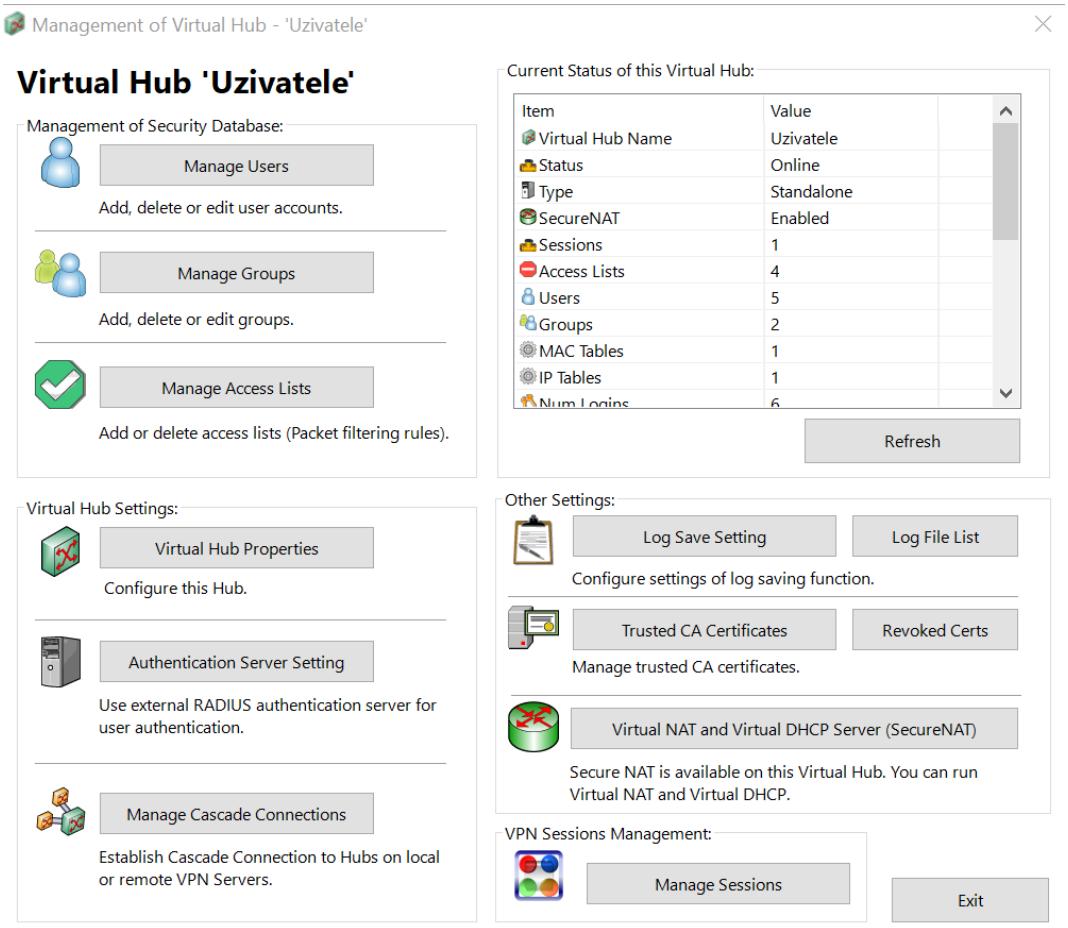
4.2.1 Virtual Hub

SoftEther VPN Server umožňuje vytvářet neomezený počet Virtual Hubs, kdy lze pomocí této komponenty řídit úroveň přístupů. Dle navrženého řešení byly vytvořeny tři Virtual Hubs. Konkrétně se jedná o tyto:

- Uzivatele,
- Privilegovani_uzivatele,
- Spravci.

Pro vytvoření nového Virtual Hubu je nutné zvolit položku Create a Virtual Hub a v novém okně vyplnit Name, Password a jako status zvolit Online, případně zvolit Limit Max VPN Sessions.

Jakmile je vytvořen nový Virtual Hub, tak pomocí položky Manage Virtual Hub jej můžeme začít spravovat.



Obrázek 14. Management of Virtual Hub

4.2.1.1 Manage Users

Prvním krokem při správě Virtual Hub **Uzivatele** je přidání uživatelů. Tato akce bude realizována zvolením položky Manage Users a poté New. Tímto dojde k vytvoření dalšího okna Create New User, kde je nutné zadat všechny důležité informace jako User Name, Group Name, Expiration Date a zvolit typ autentizace. Typ autentizace byl zvolen pomocí hesla, takže posledním krokem při vytváření nového uživatele je nastavení hesla. V okně Manage Users jsou poté přehledně vidět všichni uživatelé spolu s doplňujícími informacemi (např. počet připojení přes VPN, datum posledního připojení, přenesené bajty a pakety).

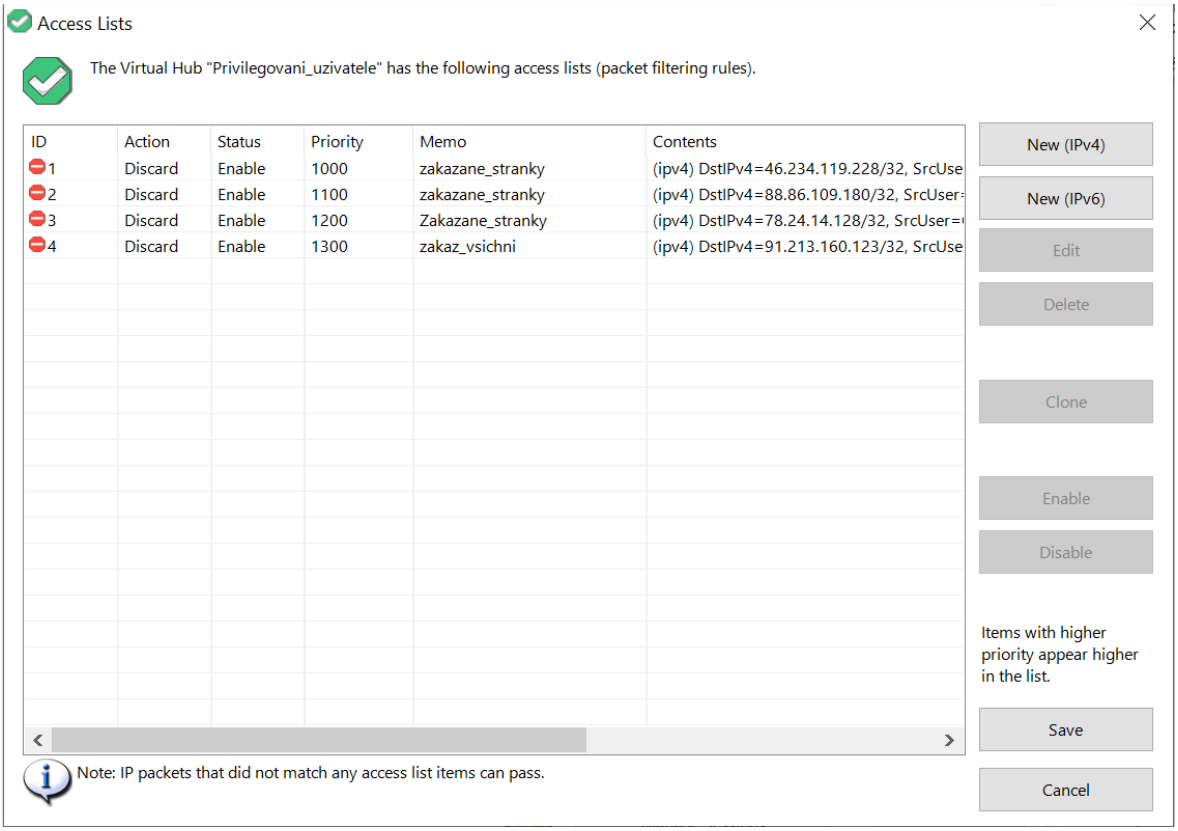
Při implementaci navrženého řešení bylo vytvořeno 5 uživatelů.

4.2.1.2 Manage Groups

Po vytvoření uživatelů je můžeme rozdělit do různých skupin, např. dle oddělení ve firmě. Uživatelé vytvoření ve Virtual Hubu **Uzivatele** byli rozděleni do dvou skupin. Rozdělení uživatelů do skupin je výhodné tehdy, pokud chceme aplikovat nějaké omezující pravidlo nejen pro jednoho uživatele, ale i pro celou skupinu.

4.2.1.3 Manage Access Lists

Access List slouží k filtraci IP paketů podle předem definovaných pravidel. Při vytváření Access Listu je důležité správně nastavit hodnoty Priority, kdy se jednotlivá pravidla vyhodnocují odshora.



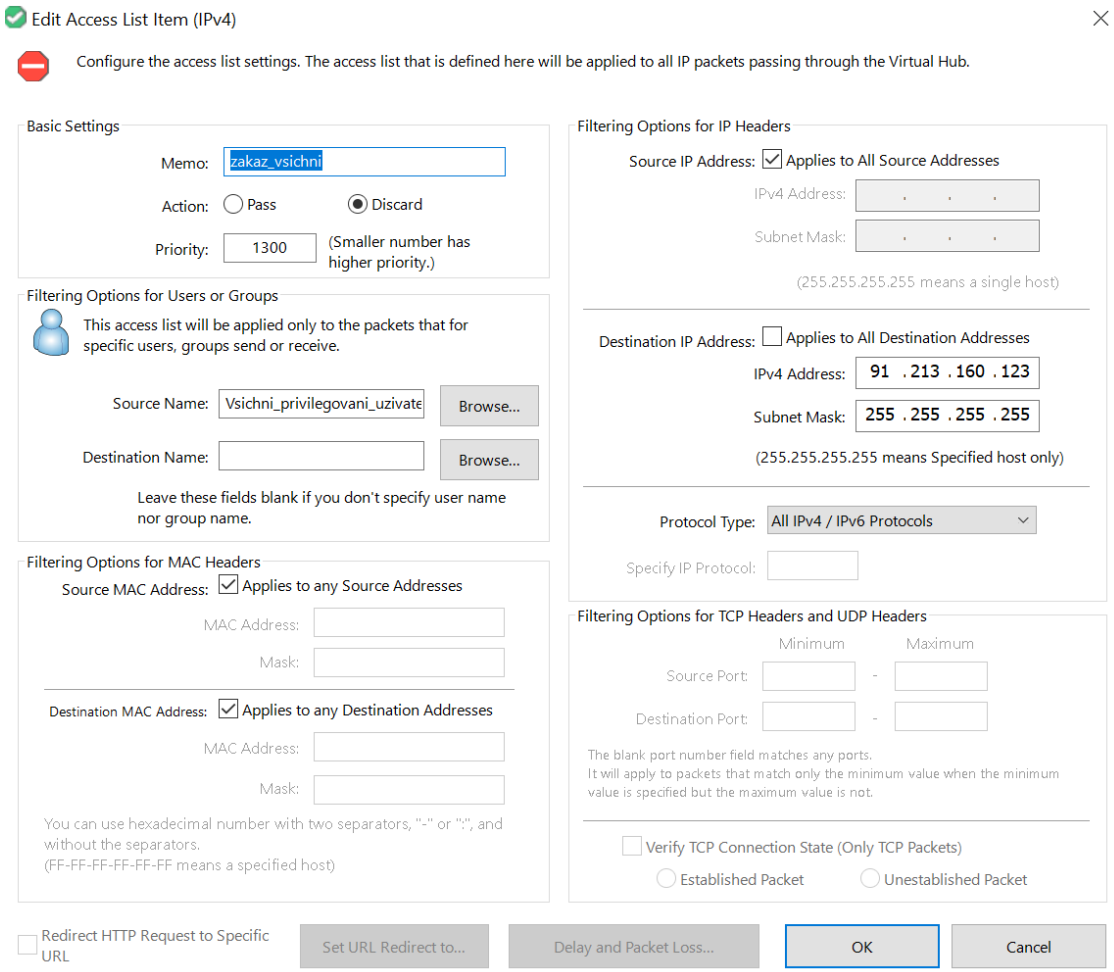
Obrázek 15. Access Lists

U Access Listu se nastavují tyto pravidla:

- Memo – popis access listu,
- Action – nastavení na Pass nebo Discard,
- Priority – nižší číslo má vyšší prioritu,

- Source a Destination name – výběr uživatele nebo skupiny, pro kterou bude Access list nastaven,
- Source IP address – definice zdrojové IP adresy,
- Destination IP address – definice cílové IP adresy,
- Další pravidla – Protocol type, filtrování MAC adresy, source/destination port number range.

Pokud nejsou nastaveny žádné Access listy anebo pokud se IP pakety neshodují s žádnými pravidly obsaženými v Access listu, tak Action je defaultně nastaveno na Pass. Samozřejmostí je poté možnost přidávání, mazání a úprava Access listu.



Obrázek 16. Edit Access List Item

Na *Obrázku 16.* lze vidět příklad nastavení Access Listu pro skupinu *Vsichni_privilegovani_uzivatele*.

Tabulka 4. Access List

Virtual Hub	Privilegovani uzivatele	
User/Group	Status	IP
Vyrobni_reditel	Discard	46.234.119.228/32
Vyrobni_reditel	Discard	88.86.109.180/32
Obchodni_reditel	Discard	78.24.14.128/32
Všichni_privilegovani_ uživatele	Discard	91.213.160.123/32
	Uzivatele	
Uzivatele_Administrativa	Discard	195.178.88.109/32
Uzivatele_Vyroba	Discard	91.239.200.58/32
	Spravci	
Přístup pro uživatele ve Virtual Hubu Spravci je bez omezení.		

4.2.1.4 Virtual NAT and Virtual DHCP Server

Součástí SoftEther VPN Server je i funkce SecureNAT. Jedná se o proprietární technologii, která byla vyvinuta přímo pro SoftEther VPN a její použití zvyšuje zabezpečení sítě. Secure-NAT řešení je rozděleno na tyto dvě části:

- Virtual NAT function,
- Virtual DHCP server function.

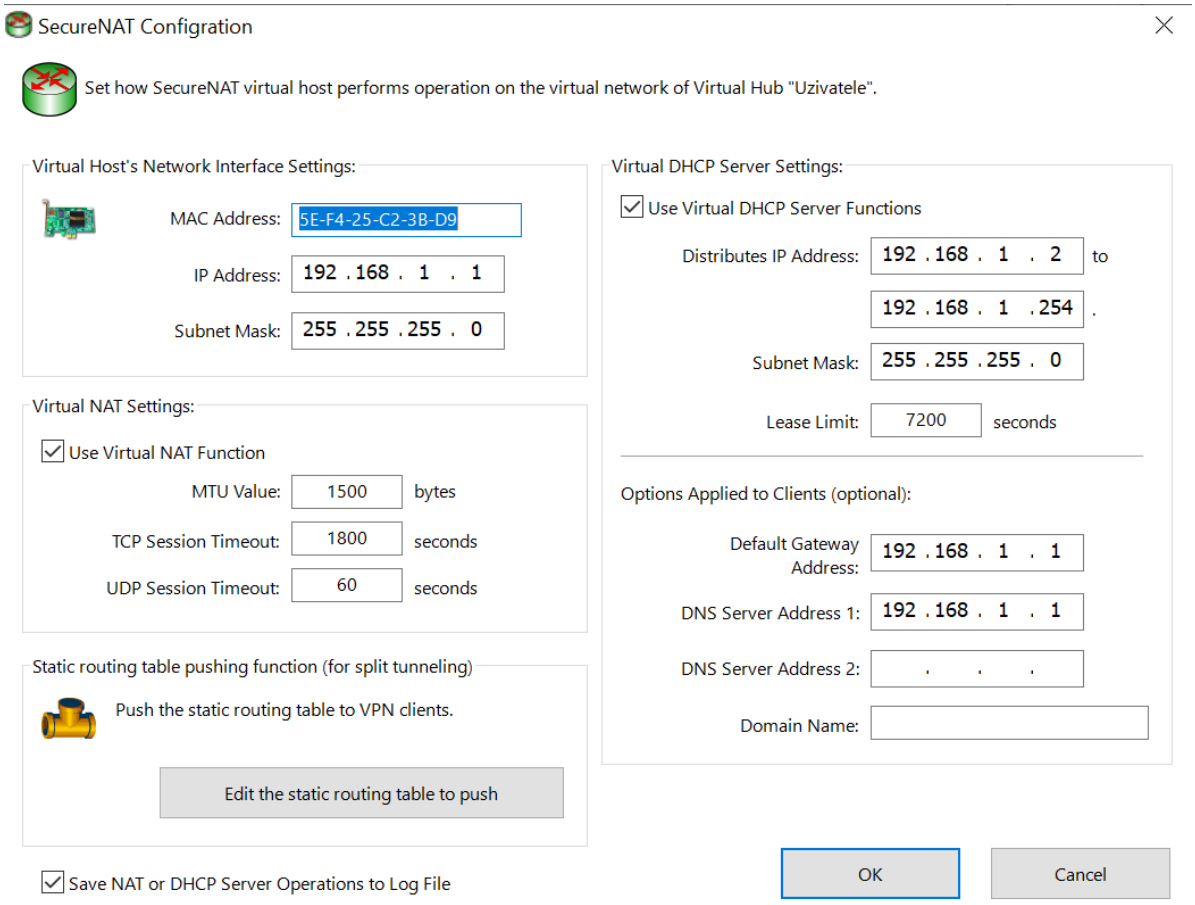
Nastavení a konfigurace SecureNAT do implementovaného řešení je následující.

Ve výchozím stavu je tato funkce zablokována a je tedy nutné ji nejdříve povolit. V okně management of Virtual Hub vybereme položku Virtual NAT and Virtual DHCP Server (SecureNAT), zde zvolíme Enable SecureNAT a vše potvrdíme. Následně zvolíme položku SecureNAT Configuration.

Při konfiguraci SecureNAT je nutné zadat tyto informace:

- Virtual Hosts Network Interface Settings – nastavení MAC adresy, IP adresy a masky podsítě,
- Virtual DHCP Server Settings – nastavení rozsahu distribuovaných IP adres a masky podsítě,

- Options Applied to Clients – nastavení výchozí Gateway adresy a adresy DNS serveru.



Obrázek 17. SecureNAT Configuration pro Virtual Hub Uzivatele

4.3 SoftEther VPN Client

Jakmile je server, Virtual Hubs a celkové prostředí správně nastaveno, je čas na připojení uživatele ze vzdáleného místa. SoftEther VPN řešení pro toto připojení používá software SoftEther VPN Client, které je nutné naistalovat do počítače, ze kterého se uživatel připojuje. VPN Client umožňuje uživateli vyřizovat téměř všechny operace, které jsou nutné vykonat pro připojení. Tento VPN Client má přehledné grafické uživatelské rozhraní, takže i méně zkušení uživatelé nemají s nastavením větší problém. Pomocí tohoto VPN klientského softwaru je možné se připojit na Virtual Hub, který běží na serveru ve vzdálené lokalitě.

Stažení softwaru SoftEther VPN Client proběhne stejně jako stahování softwaru pro server ze stránek výrobce. Pro stažení správného typu byly vybrány tyto možnosti:

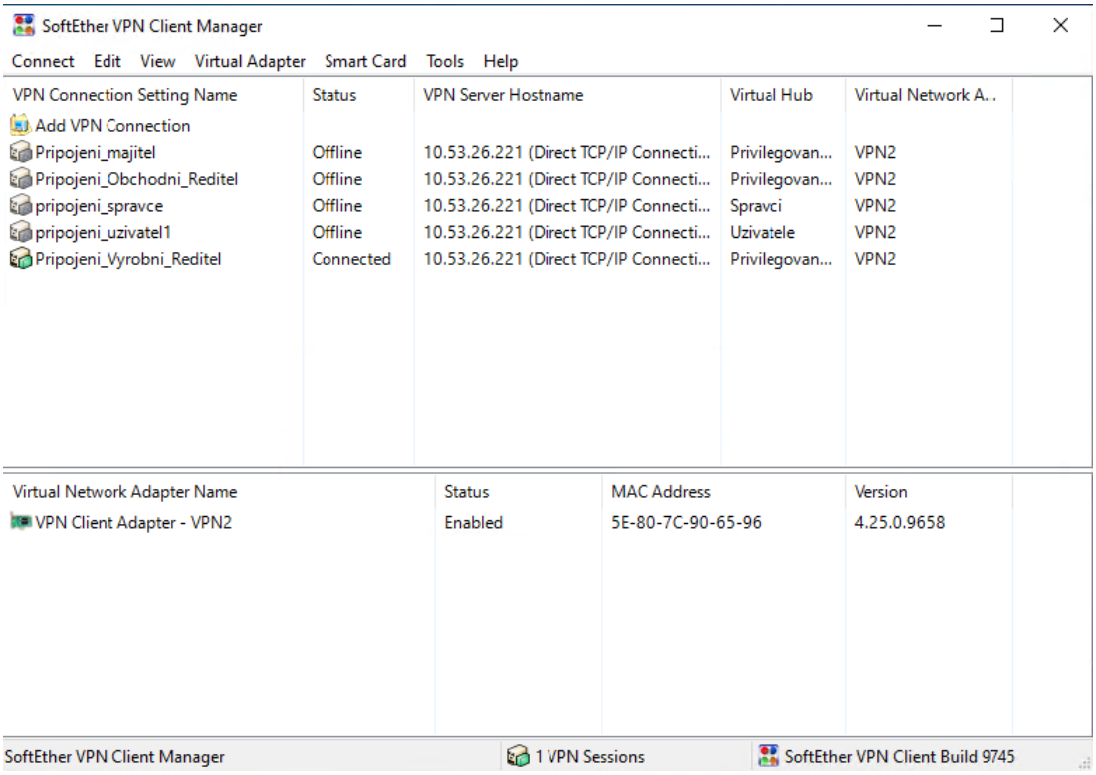
- Component – SoftEther VPN Client,

- Platform – Windows,
- CPU – Intel (x86 and x64).

Stažena byla poslední dostupná verze:

SoftEther VPN Client (Ver 4.34, Build 9745, rtm) softether-vpnclient-v4.34-9745-rtm-2020.04.05-windows-x86_x64-intel.exe (48.90 MB)

Po stažení je nutné nainstalovat tohoto Clienta a spustit jej.



Obrázek 18. SoftEther VPN Client

4.3.1 Virtual Network Adapter

SoftEther VPN Client komunikuje přes VPN vytvořením Virtual Network Adapter v zařízení. OS Windows a na něm běžící aplikace rozpoznají Virtual Network Adapter jako síťové zařízení stejně tak, jako by se jednalo o fyzický síťový adaptér. Toto řešení umožňuje uživateli využívat Virtual Network Adapter s TCP/IP protokolem.

Po spuštění SoftEther VPN Clienta jsou všechna okna prázdná. Jako první krok je tedy nutné vytvořit Virtual Network Adapter. Počet vytvořených adaptérů není nijak omezen.

Vytvoření nového Virtual Network Adapteru je možné v záložce Virtual Adapter -> New Virtual Network Adapter. Následně je nutné zadat jméno, které musí být ve tvaru

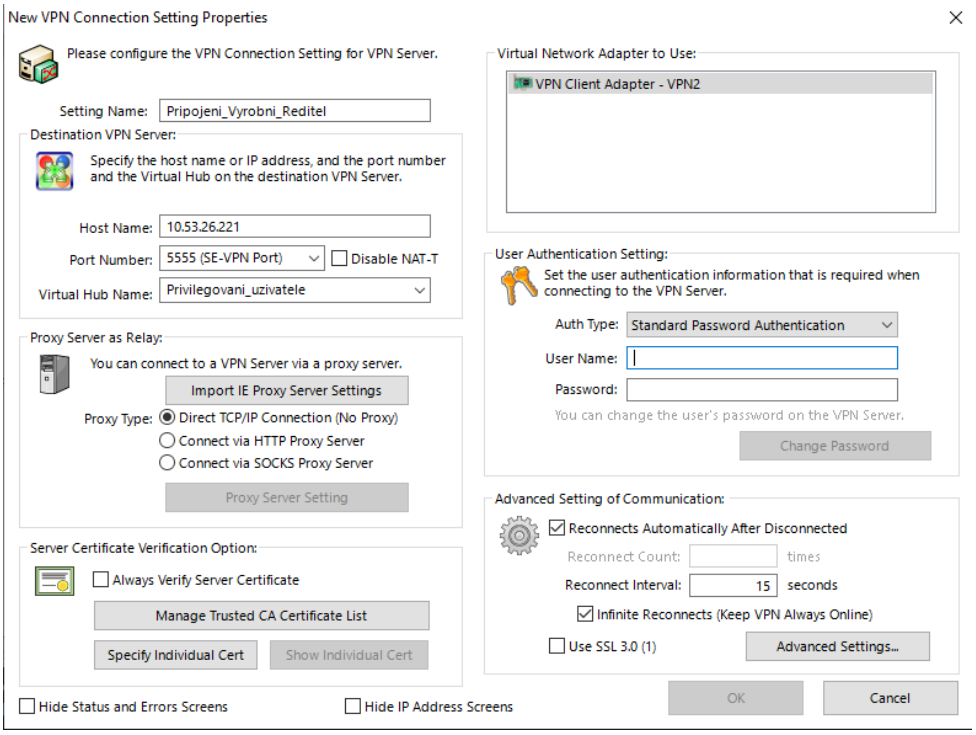
„VPNčíslo“. Tlačítkem Create a dalším potvrzení dojde k vytvoření Virtual Network Adapteru. Při implementaci řešení byl vytvořen jeden adapter s označením „VPN2“.

4.3.2 Connection Setting

Jakmile je vytvořen Virtual Network Adapter, tak dalším nezbytným úkonem je konfigurace nastavení pro připojení k Virtual Hubu na SoftEther VPN Serveru.

Stejně jako u předchozího kroku po instalaci nejsou nastavena žádná existující spojení. Musí se tedy nastavit podmínky pro připojení. V záložce Connect zvolíme New VPN Connection Setting Properties. Otevře se nové okno, kde bude možnost konfigurace. Konkrétně je nutné vyplnit tyto položky:

- Setting Name – zvolit jméno pro toto nastavení,
- Destination VPN Server – stanovit Host Name nebo IP adresu, číslo portu a Virtual Hub na VPN serveru,
- Proxy Server as Relay – zvolit Proxy type,
- Server Certifikace Verification Options – volitelné nastavení,
- Virtual Network Adapter to Use – pokud je vytvořeno více Virtual Network Adapter, tak zvolit, jaký chci použít pro toto nastavení,
- User Authentication Settings – zvolit typ autentizace,
- Advanced Setting of Communication – rozšířené možnosti nastavení.



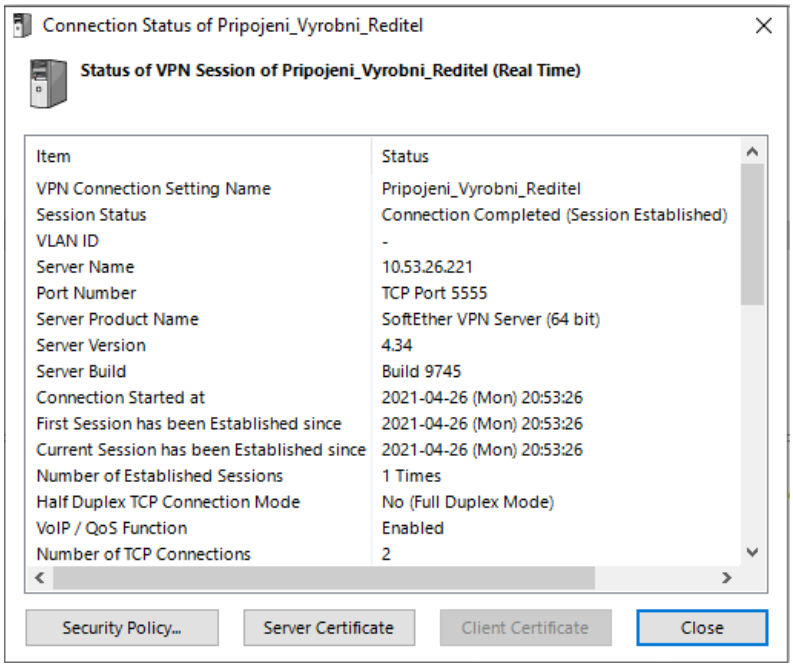
Obrázek 19. New VPN Connection Setting Properties

Jak lze vidět na *Obrázku 19.,* takto vypadá konkrétní případ konfigurace nastavení pro připojení uživatele **Vyrobni_Reditel**, který je součástí Virtual Hubu **Privilegovani_uzivatele**.

4.3.3 Connect to VPN Server

Podmínky pro připojení jsou nastaveny a můžeme přejít k poslednímu finálnímu kroku a tím je připojení k VPN Serveru. Potvrdit žádost o připojení můžeme pomocí dvojkliku na jméno connection settings, které jsme si v předchozím bodě nakonfigurovali. Tuto akci lze realizovat také stisknutím pravého tlačítka a vybrat Connect. Jakmile začne připojování, uživatel je o tom informován zobrazením okna „Connecting to název_serveru“.

Pokud se podaří navázat VPN spojení, tak se změní status připojení na Connected. Uživatel je o této změně informován vyskočením okna „Virtual Network Adapter VPN status“ a zobrazením přidělené IP adresy.



Obrázek 20. Connection Status

Jak lze vidět na *Obrázku 20.* pod položkou Session Status, VPN spojení je úspěšně navázáno (Connection Completed – Session Established).

4.4 SSH

Pokud by se vyskytly jakékoliv komplikace s připojením přes VPN a byla by tato služba nedostupná, tak jako záložní varianta bude připojení přes SSH. Autentizace uživatelů bude probíhat pomocí veřejného a privátního klíče. SSH bude implementováno na jiném serveru, než je VPN řešení. Důvod oddělení na dva odlišné servery je zejména ten, že pokud by VPN server byl nedostupný, tak by bylo nedostupné i toto záložní řešení a tím by ztratilo smysl jej realizovat.

5 OVĚŘENÍ

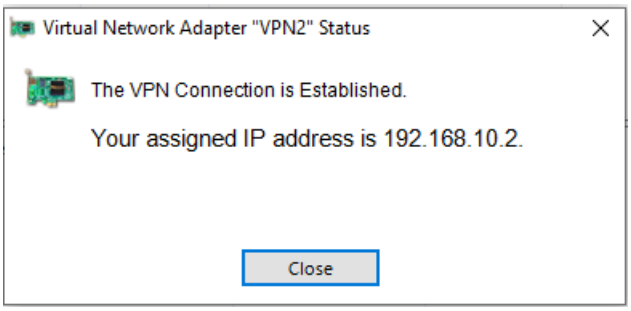
Ověření implementovaného řešení jak z funkčního, tak i z bezpečnostního hlediska, je nezbytnou součástí každého podobného projektu. Co se týče funkčnosti implementovaného řešení, tak bylo ověřeno zejména samotné VPN připojení. Ověřeny byly také jednotlivé úrovně přístupu, které byly omezeny v Access listech. Bezpečnost řešení byla ověřena rozdílnými způsoby od typově jednodušších až po běžně užívané útoky. Jedním z možných narušení bezpečnosti, které bylo ověřeno, je ruční změna IP adresy uživatelem mimo předem definovaný rozsah IP adres. Z pokročilejších technik byl využit nástroj Wireshark pro zachycení komunikace v síti. Bezpečnost implementovaného řešení byla také otestována na možnou obfuskaci IP adres.

5.1 Funkčnost řešení

Jako první bylo ověřeno celkové fungování implementovaného řešení. Pokud by tato primární část řešení nefungovala, tak by ani následné další ověřování nebylo realizovatelné. Tedy prvotně bylo ověřeno VPN připojení, zejména zdali funguje správně a připojeným uživatelům jsou přidělovány IP adresy z požadovaných rozsahů. Druhá část funkčního ověření, která však má i bezpečnostní přesah, je ověření pravidel Access listu.

5.1.1 Ověření VPN připojení

Prvním a základním ověřením implementovaného řešení je ověření připojení přes VPN. Pro toto ověření byl zvolen Virtual Hub **Privilegovani_uzivatele** a konkrétně uživatel definovaný jako **Majitel**.



Obrázek 21. Ověření VPN připojení

VPN připojení bylo navázáno (*Obrázek 21.*), kdy uživateli byla přidělena IP adresa z definovaného rozsahu (*viz. Tabulka 3.*).

```
Unknown adapter VPN2 - VPN Client:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e3:c3ba:b2ac:9250%13
   IPv4 Address. . . . . . . . . . . : 192.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
```

Obrázek 22. Výpis příkazu ipconfig

Dle informací obsažených na *Obrázku 21. a 22*. tedy můžeme konstatovat, že VPN připojení je funkční.

5.1.2 Ověření Access listu

Je nezbytné ověřit také to, zda nastavená pravidla Access listu jsou funkční a plní správně svou roli. Pro ověření byl náhodně vybrán uživatel **Vyrobni_reditel**, pro kterého byla zablokována stránka s IP adresou 88.86.109.180/32. Pro ověření bude využit příkaz ping.

Pro ověření byl nejdříve proveden ping na IP adresu bez VPN připojení. Jak lze vidět na *Obrázku 23.,* je tato adresa dostupná.

```
C:\Users\student>ping 88.86.109.180

Pinging 88.86.109.180 with 32 bytes of data:
Reply from 88.86.109.180: bytes=32 time=6ms TTL=58
Reply from 88.86.109.180: bytes=32 time=6ms TTL=58
Reply from 88.86.109.180: bytes=32 time=5ms TTL=58
Reply from 88.86.109.180: bytes=32 time=5ms TTL=58

Ping statistics for 88.86.109.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 6ms, Average = 5ms
```

Obrázek 23. Ověření Access listu

Následně se připojíme pomocí VPN, kdy z výpisu příkazu *ipconfig* zkontrolujeme, že je VPN připojení realizováno a znovu provedeme ping na stejnou IP adresu.

```
C:\Users\student>ipconfig

Windows IP Configuration


Unknown adapter VPN2 - VPN Client:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e3:c3ba:b2ac:9250%13
   IPv4 Address. . . . . . . . . . . : 192.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : utb.cz
   Link-local IPv6 Address . . . . . : fe80::e841:ab73:47d7:62f7%4
   IPv4 Address. . . . . . . . . . . : 10.53.26.225
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 10.53.24.1

C:\Users\student>ping 88.86.109.180

Pinging 88.86.109.180 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 88.86.109.180:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Obrázek 24. Ověření Access listu

Na *Obrázku 24.* je vidět výpis z příkazového řádku po provedení těchto akcí. Po připojení přes VPN Clienta je však již cíl nedostupný.

Na základě těchto informací tedy můžeme říct, že omezení přístupu pomocí pravidel definovaných v Access listu funguje správně.

5.1.3 Chování VPN v síti

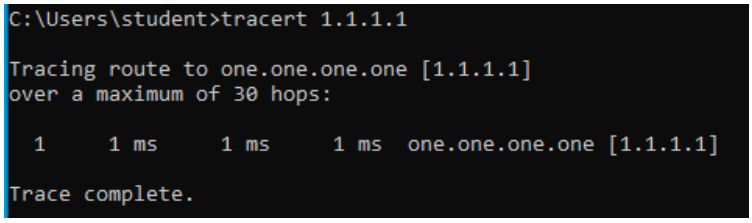
Chování SoftEther VPN v síti bylo analyzováno nástrojem traceroute. Tento nástroj vypisuje uzly v síti, přes které proudí datagramy od zdroje k cíli.

```
C:\Users\student>tracert 1.1.1.1

Tracing route to one.one.one.one [1.1.1.1]
over a maximum of 30 hops:

  1     *        *        *     Request timed out.
  2     *        *        *     Request timed out.
  3     *        *        *     Request timed out.
  4     6 ms     5 ms     5 ms  one.one.one.one [1.1.1.1]

Trace complete.
```

Obrázek 25. Tracert 1.1.1.1

Na *Obrázku 25.* lze vidět výpis příkazu tracert 1.1.1.1 bez připojení přes VPN, kde lze vidět, že cesta datagramů vedla přes čtyři uzly.

Jednou z vlastností SoftEther VPN je to, že tyto uzly či aktivní prvky skrývá.



Obrázek 26. Tracert 1.1.1.1

Jak lze vidět na *Obrázku 26.,* tak po připojení přes VPN je cesta datagramů skrytá, což je jednou z vlastností, kterou SoftEther VPN řešení obsahuje.

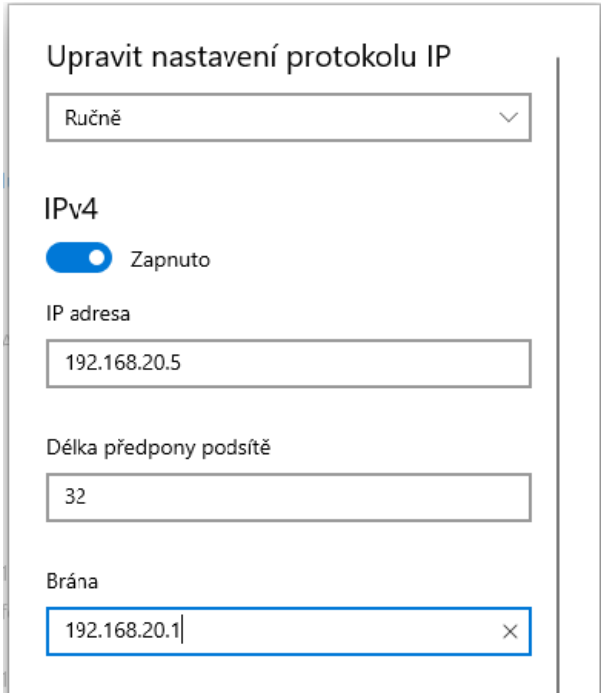
5.2 Bezpečnost řešení

Jakmile je dostatečně ověřena funkčnost řešení, tak je nutné ověřit i jeho bezpečnost. Prvním typem ověření, o který by se mohl pokusit jakýkoliv útočník nebo uživatel, je ruční změna IP adresy mimo předem definovaný rozsah. Pokud by implementované řešení nedokázalo tuto změnu detekovat, tak by mohlo dojít k navýšení přístupových práv a následnému potencionálnímu zneužití těchto vyšších práv. Následujícím typem útoku, který byl ověřen, je zachytávání komunikace s využitím aplikace Wireshark. Znalý a zkušený útočník by takto mohl odposlouchávat komunikaci dalších připojených uživatelů. Posledním typem bezpečnostního ověření je obrana proti obfuskování IP adres. Pomocí tohoto typu útoku je možné zmást a následně obejít obranné mechanismy.

5.2.1 Ruční změna IP adresy

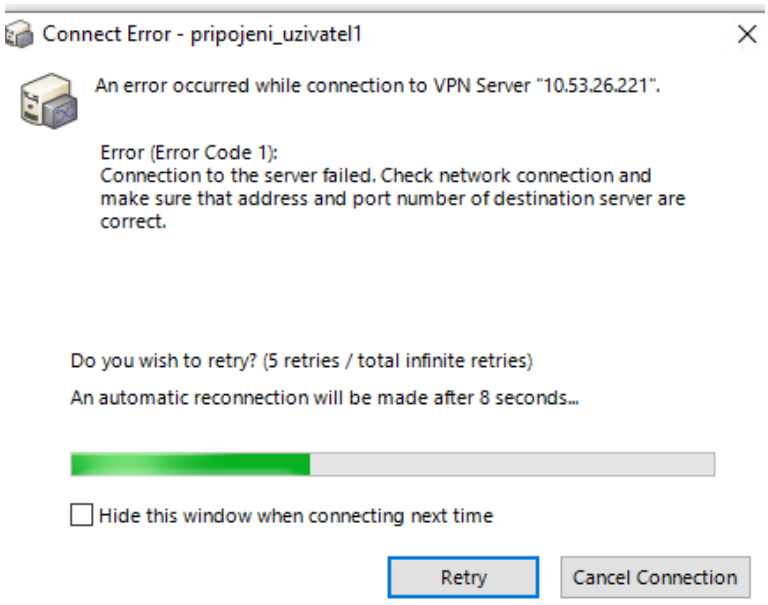
Pro zvýšení zabezpečení byli uživatelé rozděleni do několika tříd, kdy každá z těchto tříd má nastavena rozdílná přístupová práva a omezení. Připojený uživatel by se tedy mohl snažit tato omezení obejít a změnit svou IP adresu. Jedna z možností, jak realizovat tuto akci, je ruční nastavení IP adresy.

Konkrétní ověření bylo provedeno tak, že byl připojen uživatel ze skupiny **Uživatel**. Tomuto uživateli byla přidělena IP adresa z předem definovaného rozsahu - 192.168.1.2. Tento uživatel chce změnit svoje oprávnění a omezení tak, jako by patřil do skupiny **Správce**. Ručně tedy byla nastavena IP adresa z rozsahu definovaného pro správce a konkrétně to byla IP adresa 192.168.20.5.



Obrázek 27. Ruční nastavení IP adresy

Jakmile je ruční nastavení IP adresy potvrzeno, tak došlo k detekci změny IP adresy mimo definovaný rozsah a došlo k okamžitému odpojení od VPN (viz. *Obrázek 27.*).



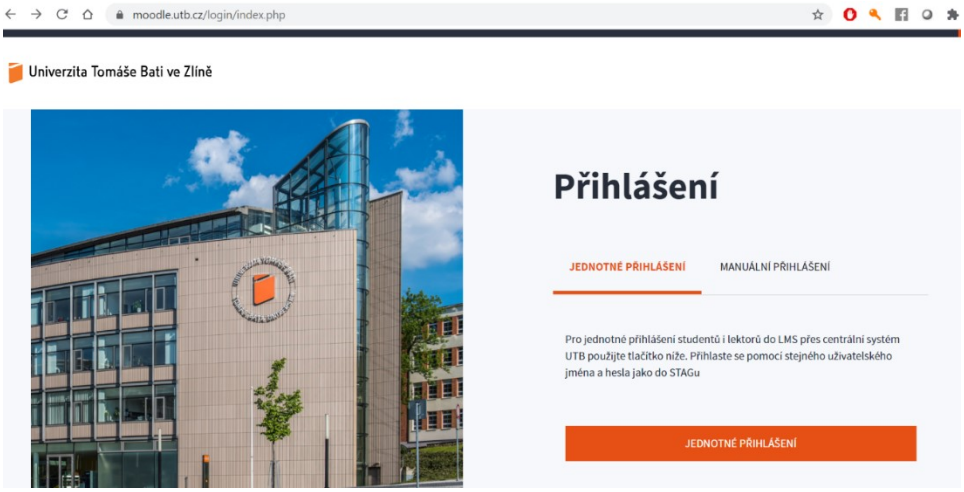
Obrázek 28. Connect Error

5.2.2 Wireshark

Pro další ověření bezpečnosti připojení přes SoftEther VPN byla využita aplikace Wireshark.

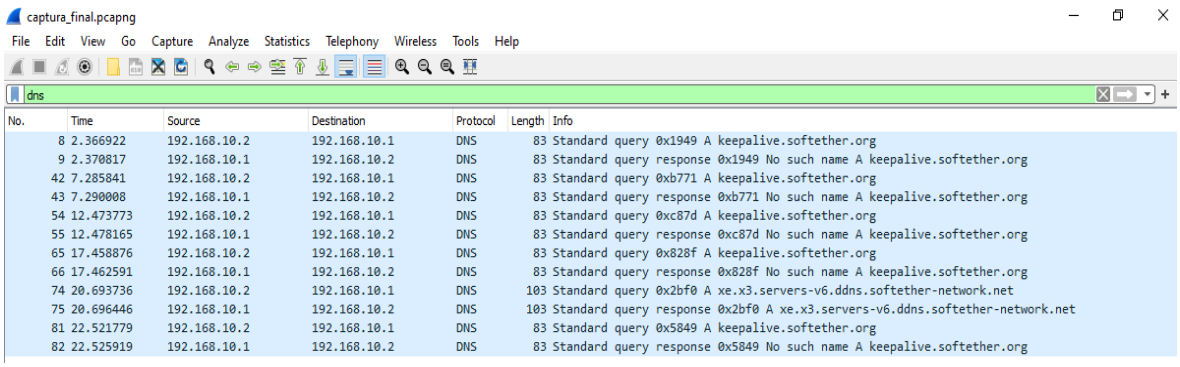
Pro tento test byl vytvořen druhý virtuální PC a stejným způsobem byl stažen a nakonfigurován VPN Client. Připojení z tohoto PC bylo nastaveno pro uživatele **Generalni_reditel** a byla mu přidělena IP adresa 192.168.10.3 Na prvním virtuálním PC byl připojen uživatel **Vyrobni_reditel**, kterému byla přidělena IP adresa 192.168.10.3. Na tomto PC byla stažena a nainstalována aplikace Wireshark.

Pro ověření bezpečnosti bude na prvním PC v aplikaci Wireshark zachytávána komunikace na připojené VPN. Ve stejném čase byl na druhém PC otevřen webový prohlížeč a uživatel přistupuje na stránku www.moodle.utb.cz, kde se poté pomocí jména a hesla se přihlásil.



Obrázek 29. Přístup na moodle

Ve stejný okamžik byl na prvním PC v aplikaci Wireshark spuštěno zachytávání paketů. Zachycená data byla podrobena analýze, zdali lze odposlouchávat komunikaci připojených uživatelů. V tomto konkrétním případě, jestli lze určit, na jaké webové stránky přistupuje.



Obrázek 30. Zachycená data Wireshark

Analýzou zachycených dat nebyly zjištěny žádné informace o aktivitě připojených uživatelů a lze tedy konstatovat, že implementované řešení je z tohoto úhlu pohledu bezpečné.

5.2.3 Obfuskace IP adresy

Bezpečnost navrženého řešení byla ověřena také proti obfuskaci IP adres. Jedná se o změnu či zamaskování IP adresy tak, aby bylo možné obejít bezpečnostní mechanismy.

Pro generaci obfuskovaných IP adres byl použit skript napsaný v jazyce Python. Tento skript byl stažen ze zdroje: https://github.com/C-REMO/Obscure-IP-Obfuscator

Pro obfuskaci byla zvolena IP adresa **88.86.109.180**. Generování obfuskovaných IP adres bylo spuštěno příkazem: *py IP-Obfuscator.py –ip 88.86.109.180*

```
C:\Users\19jir\Obscure-IP-Obfuscator-master\Obscure-IP-Obfuscator-master>py IP-Obfuscator.py --ip 88.86.109.180

IP Obfuscator   #v0.1f
  Author: Omer Ramić <@sp_omer>

[~] Obfuscated IPs:

[+] http://1482059188
[+] http://0x58566db4
[+] http://013025466664

[+] http://0130.0126.0155.0264
[+] http://00000000130.00000000126.00000000155.00000000264
[+] http://0x58.0x56.0x6d.0xb4
[+] http://0x0000000058.0x0000000056.0x000000006d.0x00000000b4

[+] http://0x58.0x56.0x6d.180
[+] http://0x58.0x56.109.180
[+] http://0x58.86.109.180
[+] http://88.0x56.0x6d.0xb4
[+] http://88.86.0x6d.0xb4
[+] http://88.86.109.0xb4

[+] http://0130.0126.0155.180
[+] http://0130.0126.109.180
[+] http://0130.86.109.180
[+] http://88.0126.0155.0264
[+] http://88.86.0155.0264
[+] http://88.86.109.0264

[+] http://0x58.0x56.28084
[+] http://0x58.5664180
[+] http://0130.0126.28084
[+] http://0130.5664180
[+] http://0x58.0126.28084
[+] http://0130.0x56.28084
```

Obrázek 31. Obfuskované IP adresy

Výše uvedená IP adresa nebyla zvolena nahodile, ale jelikož je obsažena v Access listu pro uživatele **Vyrobni_reditel** jako zakázaná, tak ji lze snadno otestovat.

Ověření bezpečnosti tedy spočívá v připojení tohoto uživatele přes VPN a testování, zdali je možné přistoupit na obfuskované IP adresy. Access list by měl toto připojení zamítnout.

Náhodně vybrány a otestovány byly tyto tři obfuskované IP adresy:

- 1482059188,
- 0130.0126.0155.180,
- 0x58.0x56.0x6d.0xb4.

Jako první byl otestováno spojení na obfuskovanou IP adresu *1482059188,* kdy byl proveden ping na tuto adresu bez připojení k VPN. Jak lze vidět na *Obrázku 32.,* tak tato adresa je za normálního stavu dostupná.

```
C:\Users\student>ping 1482059188

Pinging 88.86.109.180 with 32 bytes of data:
Reply from 88.86.109.180: bytes=32 time=5ms TTL=58
Reply from 88.86.109.180: bytes=32 time=5ms TTL=58
Reply from 88.86.109.180: bytes=32 time=5ms TTL=58
Reply from 88.86.109.180: bytes=32 time=130ms TTL=58

Ping statistics for 88.86.109.180:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 130ms, Average = 36ms
```

Obrázek 32. Ping 1482059188

Po tomto prvotním ověření bylo provedeno připojení na VPN a pomocí příkazu *ipconfig* zkontrolováno, že je připojení navázáno. Následně byl proveden znovu ping na tuto IP adresu. Access list však detekoval toto spojení na obfuskovanou IP adresu a ta se již stává nedostupnou *(viz Obrázek 33.).*

```
C:\Users\student>ipconfig

Windows IP Configuration


Unknown adapter VPN2 - VPN Client:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e3:c3ba:b2ac:9250%13
   IPv4 Address. . . . . . . . . . . : 192.168.10.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : utb.cz
   Link-local IPv6 Address . . . . . : fe80::e841:ab73:47d7:62f7%4
   IPv4 Address. . . . . . . . . . . : 10.53.26.225
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Default Gateway . . . . . . . . . : 10.53.24.1

C:\Users\student>ping 1482059188

Pinging 88.86.109.180 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 88.86.109.180:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Obrázek 33. Ping 1482059188

Stejným způsobem bylo otestováno i spojení na další dvě obfuskované IP adresy *0130.0126.0155.180* a *0x58.0x56.0x6d.0xb4*. Výsledek testu dopadl stejně, tedy že Access list správně detekoval obfuskované IP adresy a zablokoval je.

ZÁVĚR

Zajištění bezpečného vzdáleného přístupu je významná a pro uživatele velmi důležitá oblast. S nárůstem digitalizace a stále významnějším postavením informačních technologií v běžném životě bude významně narůstat na důležitosti i oblast spojená se vzdáleným přístupem. Tento nárůst bohužel nebude jen v pozitivním smyslu, ale souběžně s ním bude narůstat i počet kybernetických útoků a incidentů.

V úvodní kapitole byla provedena specifikace nejčastěji používaných služeb a protokolů pro zabezpečení vzdáleného přístupu. Specifikace spočívala zejména v popisu a principu činnosti dané služby či protokolu. Zaměření na bezpečnost, nejznámější zranitelnosti a útoky je také součástí této specifikace. Současně byly stanoveny i omezující parametry, které ovlivňují zajištění bezpečného přístupu. V závěru této kapitoly byly určeny nejdůležitější omezující parametry, které byly následně promítnuty i do návrhu řešení v praktické části.

Jeden z cílů práce byl splněn návrhem řešení pro zajištění bezpečného vzdáleného přístupu. Základním stavebním prvkem tohoto řešení je SoftEther VPN. Navržené řešení postavené na této technologii bylo následně implementováno v testovacím prostředí. Pro potřeby testování byla využita laboratorní univerzitní infrastruktura. Součástí implementace je detailní popis jednotlivých částí navrženého řešení, které jsou doplněny také o grafické zobrazení.

Na závěr bylo provedeno ověření implementovaného řešení. Toto ověření bylo provedeno jak z funkčního, tak i z bezpečnostního hlediska.

Diplomová práce seznamuje čtenáře s problematikou řešení bezpečného vzdáleného přístupu. V praktické části je uvedeno konkrétní řešení, jak lze realizovat bezpečný vzdálený přístup. Celá tato práce tedy může být využita jako podklad k návrhu, implementaci a otestování řešení pro zajištění bezpečného vzdáleného přístupu.

SEZNAM POUŽITÉ LITERATURY

[1] Remote Desktop Protocol. *Microsoft Documentation* [online]. 2018 [cit. 2021-02-26]. Dostupné z: https://docs.microsoft.com/cs-cz/windows/win32/termserv/remote-desktop-protocol?redirectedfrom=MSDN

[2] Remote Desktop Protocol. *Munchkin press* [online]. 2020 [cit. 2021-02-26]. Dostupné z: https://munchkinpress.com/remote-desktop-protocol-rdp/https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

[3] Understanding Remote Desktop Protocol. *Microsoft Documentation* [online]. 2020 [cit. 2021-02-26]. Dostupné z: https://docs.microsoft.com/en-us/troubleshoot/windows-server/remote/understanding-remote-desktop-protocol

[4] Trends in Internet Exposure. *Shodan blog* [online]. 2020 [cit. 2021-02-26]. Dostupné z: https://blog.shodan.io/trends-in-internet-exposure/

[5] Kaspersky: RDP brute-force attacks have gone up since start of COVID-19. *ZDnet* [online]. 2020 [cit. 2021-02-26]. Dostupné z: https://www.zdnet.com/article/kaspersky-rdp-brute-force-attacks-have-gone-up-since-start-of-covid-19/

[6] Microsoft Operating Systems BlueKeep Vulnerability. *Cybersecurity & Infrastructure Security Agency* [online]. 2019 [cit. 2021-02-26]. Dostupné z: https://us-cert.cisa.gov/ncas/alerts/AA19-168A

[7] https:// How Virtual Private Networks Work. *Cisco* [online]. 2008 [cit. 2021-03-03]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.pdf

[8] Co je VPN a jak funguje? *Avast blog* [online]. 2019 [cit. 2021-02-26]. Dostupné z: https://blog.avast.com/cs/co-je-vpn-a-jak-funguje

[9] Manual:IP/IPsec. *MikroTik documentation* [online]. 2021 [cit. 2021-03-03]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:IP/IPsec

[10] Manual:Interface/L2TP. *MikroTik documentation* [online]. 2021 [cit. 2021-03-03]. Dostupné z: https://wiki.mikrotik.com/wiki/Manual:Interface/L2TP

[11] TeamViewer 13 Manual. *TeamViewer* [online]. 2021 [cit. 2021-03-03]. Dostupné z: https://dl.teamviewer.com/docs/en/v13/TeamViewer13-Manual-Remote-Control-en.pdf?p=17641

[12] TeamViewer Portable. *Download crew* [online]. 2021 [cit. 2021-02-26]. Dostupné z: https://www.downloadcrew.com/article/33872/teamviewer_portable

[13] Security Overview. *TeamViewer* [online]. 2021 [cit. 2021-02-26]. Dostupné z: https://www.teamviewer.com/en/trust-center/security/

[14] NoMachine for everybody. *NoMachine* [online]. 2021 [cit. 2021-03-02]. Dostupné z: https://www.nomachine.com/everybody

[15] Integrating NoMachine with Various Authentication Methods. *NoMachine* [online]. 2021 [cit. 2021-03-02]. Dostupné z: https://www.nomachine.com/DT11R00187

[16] Encryption in NoMachine 4 or later. *NoMachine* [online]. 2021 [cit. 2021-03-02]. Dostupné z: https://www.nomachine.com/AR10K00705

[17] SSH protocol. *SSH* [online]. 2021 [cit. 2021-02-27]. Dostupné z: https://www.ssh.com/ssh/protocol/

[18] BothanSpy & Gyrfalcon - Analysis of CIA hacking tools for SSH. *SSH* [online]. 2021 [cit. 2021-02-27]. Dostupné z: https://www.ssh.com/ssh/cia-bothanspy-gyrfalcon

[19] Man-in-the-Middle Attack. *SSH* [online]. 2021 [cit. 2021-02-27]. Dostupné z: https://www.ssh.com/attack/man-in-the-middle

[20] Virtual Network Computing. *Quentin Stafford-Fraser* [online]. 1998 [cit. 2021-03-03]. Dostupné z: https://quentinsf.com/publications/virtual-network-computing/vnc-ieee.pdf

[21] *The Remote Framebuffer Protocol* [online]. 2011 [cit. 2021-03-02]. ISSN 2070-1721.

[22] VNC connect. *RealVNC* [online]. 2020 [cit. 2021-03-03]. Dostupné z: https://static.realvnc.com/media/documents/vnc-connect-product-brochure.pdf

[23] Remote Desktop. *Shodan* [online]. 2021 [cit. 2021-03-15]. Dostupné z: https://www.shodan.io/report/D6QnJgcO

[24] Global market share held by operating systems for desktop PCs, from January 2013 to December 2020. *Statista* [online]. 2021 [cit. 2021-03-30]. Dostupné z: https://www.statista.com/statistics/218089/global-market-share-of-windows-7/

[25] Windows 7. *Shodan* [online]. 2021 [cit. 2021-03-15]. Dostupné z: https://www.shodan.io/search?query=Windows+7

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

RDP	Remote Desktop Protocol
VPN	Virtual Private Network
SSH	Secure Shell
VNC	Virtual Network Computing
TCP	Transmission Control Protocol
GDI	Graphics Device Interface
RSA	Rivest, Shamir, Adleman (iniciály autorů)
TLS	Transport Layer Security
NLA	Network Level Authentication
USA	United States of America
CVE	Common Vulnerabilities and Exposures
RCE	Remote Code Execution
OS	Operační systém
CIA	Confidentiality, Integrity, Availability
SSL	Secure Sockets Layer
TLS	Transport Layer Security
NAT	Network Adress Translation
IT	Informační technologie
AES	Advanced Encryption Standard
TOTP	Time-based One-time Password
SSH	Secure Shell
SHA-2	Secure Hash Algorithm
CIA	Central Intelligence Agency
MITM	Man-in-the-middle

RFB	Remote Frame Buffer
DES	Data Encryption Standard
PPP	Point-to-Point Protocol
BYOD	Bring-Your-Own-Device
IoC	Indicator of compromise
EOL	End-of-Life
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
CEO	Chief executive officer

SEZNAM OBRÁZKŮ

SEZNAM TABULEK