Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Využití VNC pro automatizaci diagnostiky specializovaných zařízení Siemens

Bakalářská práce

Autor: Tomáš Antoš
Studijní obor: Aplikovaná informatika

Vedoucí práce: Mgr. Josef Horálek, Ph.D.

Hradec Králové březen 2022

Prohlášení:

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

V Hradci Králové dne 12.8.2022 Tomáš Antoš

Poděkování:
Děkuji vedoucímu bakalářské práce, Mgr. Josefu Horálkovi, Ph.D. za metodické vedení práce, připomínky a rady poskytnuté na konzultacích.

Anotace

V práci je představen způsob využití VNC protokolu pro připojení analyzátorů – specializovaných zdravotnických zařízení firmy Siemens k dálkové správě.

Práce je rozdělena do dvou částí. V teoretické části jsou představeny obecné principy a možnosti využití VNC včetně využívaného protokolu RFB. Dále je představen způsob zabezpečení a přenosu dat. Následně je představen a popsán aktuální používaný model vzdálené správy, který se již používá pro komunikaci se zdravotnickými zařízeními. Další část práce je zaměřena na analýzu nedostatků stávajícího řešení. V praktické části je pak navržena inovace modelu a využití VNC jako hlavního systému pro vzdálenou komunikaci. Navrženy jsou také systémové kroky pro jeho možnou realizaci.

Annotation

Title: Using VNC to automate the diagnostics of specialized devices

The thesis presents how to use the VNC protocol to connect analyzers – specialized medical devices from Siemens for remote management. The work is divided into two parts. In the theoretical part, the author will present the general principles and possibilities of using the VNC, including the RFB protocol used. The method of security and data transfer will also be presented. Furthermore, presentation and description of the current remote management model already used in communication with medical facilities. The next part of the thesis will focus on analyzing the shortcomings of the current solution. In the practical part, the author will propose an innovation of the model and the use of the VNC as the main system for remote communication. It will also propose systemic steps for its possible implementation.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Laboratoře ve zdravotnických zařízeních využívají analyzátory – specializované zdravotnické přístroje analyzují odebrané vzorky pacientovy krve a následně vydají výsledek doktorem požadovaného testu. Analyzátory hrají zásadní roli v moderní medicíně. Bez výsledků jednotlivých analýz se dnes již neobejde žádný doktor.
Proto je vynakládáno velké úsilí na zajištění bezporuchového provozu jednotlivých přístrojů. To je řešeno ze strany pracovišť např. nastavením nepřetržitého provozu, audity a školením obsluhy, tak i ze strany servisních organizací.
Jednou z firem je i společnost Siemens Healthcare, která zajišťuje instalaci a servis přístrojů napříč medicínskými obory. Zajištění servisu v režimu 24/7 je tedy nezbytnou nutností, včetně zajištění kvalifikovaných techniků a aplikačních specialistů.
Jedním z možných řešení je i zřízení dohledového centra s vlastní infrastrukturou, které dokáže zajistit vzdálenou správu všech nainstalovaných přístrojů v regionu.
Hlavní motivací pro zavedení vzdálené správy v servisní organizaci je omezení fyzické přítomnosti servisních pracovníků u zákazníků.
Aplikační specialisté se dokážou z kteréhokoli místa připojit na obrazovku řídícího počítače analyzátoru. Pomohou tak obsluze přístroje s ovládáním aplikace řídícího PC a s řešením problémů. Technici pak dokážou odhalit problém spuštěním diagnostiky v prostředí servisní aplikace. Může tak být vyřešen jen banální problém bez nutnosti výjezdu a provoz stroje není přerušen na dlouhou dobu.
Technik či aplikační specialista se může na budoucí fyzický zásah lépe připravit.
Výhody vzdálené správy ocení všichni. Moderní ekonomicky postavený servis si vyžaduje minimalizaci nákladů spojených s výjezdy techniků k závadám zařízení.
Zákazník pak ocení rychlost reakce na ohlášenou závadu.

Cílem této bakalářské práce je tedy ukázat možnosti použití VNC pro vzdálenou správu. Analyzovat výhody a nevýhody jeho současné použití ve stávajícím řešení firmy Siemens.
V praktické části je cílem představit vylepšený model řešení vzdálené správy.

2 Úvod do problematiky

Pro realizaci vzdálené správy lze použít několik platforem tzv. tenkých klientů, využívajících různých protokolů.

Jedním z nich je RDP, jehož protokol umožňuje přenos souborů, audia. Pomocí RDP je možné připojení jednoho uživatele v daný okamžik. Možnost připojení více uživatelů vyžaduje instalaci Terminálového serveru a zakoupení patřičných licencí. Jako server může být provozován pouze na Microsoft Windows systémech. Další z možností můžeme zmínit platformu Teamviewer, jež obsahuje ještě větší množství funkcionalit, včetně chatu. Služba používá cloudové servery a úložiště, vyžaduje tedy přístup do veřejné sítě – internetu. To omezuje použitelnost této platformy v čistě lokální sítích, z nichž není prostup do internetu povolen. Další z možností je VNC, pracuje na všech platformách, přenáší bitmapový obrázek a je nenáročný na procesor klientského počítače. Umožňuje připojení více uživatelů v jednom okamžiku. [15]

Využití VNC je ideální při odstraňování problémů na koncových stanicích. Může zároveň plnit funkci dohledu nad chováním uživatele koncové stanice, aniž by o tom uživatel věděl. V porovnání s jinými programy a protokoly vychází VNC jako bezkonkurenčně nejrychlejší a nákladově nejpřívětivější. [7]

Tenký klient

Je program, který obsahuje pouze prezentační vrstvu aplikace. Všechna data, procesní algoritmy a logiku aplikace má na starosti server. Pracuje v režimu klient-server, to znamená že se skládá jak ze softwaru serveru, tak klienta. Při navazování spojení nejčastěji iniciuje relaci klient. Klient se dotazuje serveru, server naopak čeká na požadavky od klienta. [5]

Tencí klienti

Pojem tenký klient se používá pro různé počítače. Tenký klient může být označen takový počítač, který nutně potřebuje veliký centrální server. Nebo je tenký klient takový počítač, který používá centrální server jen jako datové úložiště aplikací, které na samotném tenkém klientovi chybí. Tenkým klientem může být i pracovní stanice, která používá vzdálené připojení, třeba jen občas nebo jen pro něco. Zjednodušeně by se dalo říct, že tenký klient je počítač bez pevného disku.

Technologie tenkých klientů byla běžným modelem v letech 1960-80. Tehdy se používaly robustní sálové počítače, ke kterým se uživatelé připojovali pomocí takzvaných hloupých terminálů.

Po příchodu systému X Window, byla část těchto terminálů nahrazena X terminály. To byly vlastně hloupé terminály, na kterých bylo možné provozovat grafický X server. [12]

Ultratenký klient

Je taková aplikace, která pouze zobrazuje pracovní plochu jiného systému, který je spuštěn na serveru. Taková aplikace může zobrazovat jiný systém i prostřednictvím HTTP prohlížeče.

Systém X

X Window je vhodný pro použití na centrálním serveru, kde je instalován Linux nebo jiný unixový systém. Jako tenkého klienta pro Linux lze použít X Window nebo X terminál. Protokol X nelze ale použít pro připojení k Windows.[15]

VNC

VNC a jeho protokol RFB (Remote Frame Buffer) jsou pro tenké klienty velmi užitečným nástrojem. Pro spuštění VNC klienta lze použít systémy Linux i Windows. Na VNC serveru pak umožňují současnou práci více uživatelů. Podporu VNC obsahují i některé specializované terminály a operační systémy mobilních zařízení. VNC klienti jsou tencí, to znamená že nejsou nenároční na prostředky, protože neukládají svoje data v hostovaném počítači. Odlišují se tím od systémů jako jsou X

Windows. Klienta VNC je možné kdykoli odpojit od serveru a znovu zase připojit, aniž by to nějak ovlivnilo chování serveru.[16]

RDP

RDP (Remote Desktop Protocol) je protokol firmy Microsoft, využívá se v terminálových službách Windows. V Linuxu se RDP implementuje například pomocí programu rdcskrop (hup;/' / wwn:rdesktrnorg/), ke kterému lze z linuxové stanice snadno udělat tenkého klienta pro spojení s Windows serverem.[15]

3 Představení principu VNC

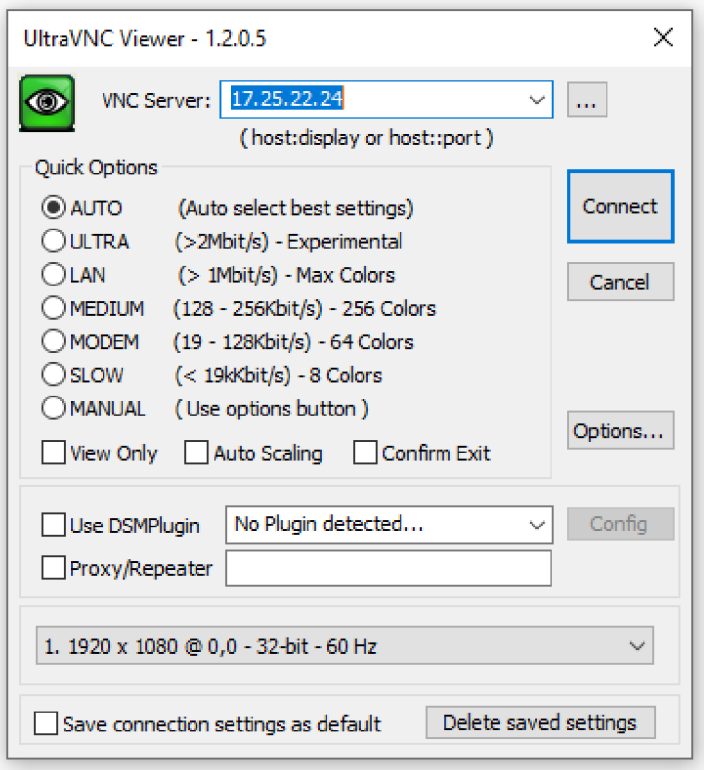
VNC (Virtual Network Computing) je program tenkého klienta, který se umí připojit ke vzdálenému počítači a zobrazit jeho pracovní plochu. Program disponuje i možností sdílet také tuto pracovní plochu s dalšími uživateli.

VNC technologie stojí na využití jednoduchého RFB protokolu vzdálené plochy. Ten je zcela nezávislý na operačním systému, můžeme ho například aplikovat na linuxový VNC server a připojovat se k němu Windows VNC klientem. Jiné, než v Linuxu je řešení účtů v architektuře Windows, ta neumožňuje, aby na jednom počítači pracovalo více uživatelů najednou, tak aby měl každý svojí pracovní plochu. Windows sice umožnuje připojení více VNC klientů, ale všichni jsou připojeni na stejný VNC server, z tohoto důvodu pak sdílejí jednu stejnou pracovní plochu. VNC server je možné ve systémech Windows spouštět jako službu ale i jako uživatelskou aplikaci. V případě, že bude VNC server spuštěný jako služba, je možné ho nastavit tak, aby k němu mohl být v jeden moment přihlášený pouze jeden jediný uživatel. [2][15]

3.1 UltraVNC

VNC je systémem tenkého klienta na obrázku 1. Jde o variantu systému VNC, která využívá také protokol RFB. VNC server je spuštěný jako daemon, tzn. permanentní služba spuštěná na pozadí.

UltraVNC obsahuje integrovaný Java Vieweru, pomocí něj ten zajišťuje připojení a zároveň díky němu lze provést přenos dat z jednoduché aplikace na UltraVNC server. K šifrování komunikace je možné využít SecureVNCPlugin. Ten umožňuje zvolit druh šifrování a délku klíče. Na straně klienta se generuje veřejný klíč pro stranu serveru a na straně serveru je vygenerován privátní klíč. Pro správnou funkci pluginu je nezbytně důležité, aby byl povolen na straně serveru a stejně tak nastavený i na straně klienta. Použití pluginu UltraVNC v případě že použijeme jinou variantu VNC není možné. [9]



Obr. 1 VNC klient.
Zdroj: UltraVNC: UltraVNC remote access tools. UltraVNC Team [Online]. 2020 [cit. 15.07.2021.]. Dostupné z: https://www.uvnc.com

Program je dostupný na domovské stránce ve 2 verzích:

- **Stable** je verze, která je odzkoušená a plně funkční.
- **RC** je testovací verze, kde jsou přidané doplňky a funkce k programu. Tato verze je funkční, ale může být za určitých podmínek nestabilní. [9]

Siemens používá modifikovanou variantu UltraVNC a nazývá ji i2iVNC.

Další funkce programu jsou:

- **File transfer** umožňuje přenos souborů mezi klientem a serverem.
- **Video driver** je externí ovladač, který zabezpečuje rychlou změnu obrazu. Tento driver umožňuje přímé spojení s video pamětí na grafické kartě framebufferu a UltraVNC serveru. Takový způsob použití grafického framebufferu zrychluje změnu obrazu na obrazovce a snižuje zatížení procesoru.

- **Encryption Plugin** je plugin doplněk s nástroji na kryptování a zabezpečení spojení.
- **Text chat** je zabudovaný textový chat pro komunikaci mezi klientem a serverem.
- Podpora více monitorů – program je možné používat na více monitorech najednou.
- **Repeater/Proxy-support** je podpora průchodnosti přes opakovače a proxy servery.
- **Auto reconnection** zajišťuje, že spojení se sekundárním počítačem je automaticky obnovováno.
- **Java Viewer** je prohlížeč, který podporuje Java aplikace a umožňuje i přenos souborů.

4 Představení protokolu VNC

Využití protokolu VNC

Pomocí komunikačního schématu klient – server na jehož principu pracuje VNC lze přenášet stav obrazovky serveru na display mobilního telefonu. Mobilní telefon obsahuje VNC klienta a na serveru je nainstalovaný VNC server. Vlastní mobilní telefon nemá dostatečně robustní hardware pro běh VNC serveru. Proto se všechny výpočetní operace provádí na serveru a nedochází tak k přetěžování CPU mobilního telefonu. [6]

Integrováním VNC do aplikace zabývající se inventarizací, je umožněna kontrola průběhu operací na koncových stanicích. Propojení obou koncových bodů je pak zabezpečeno SSH tunelem. [20]

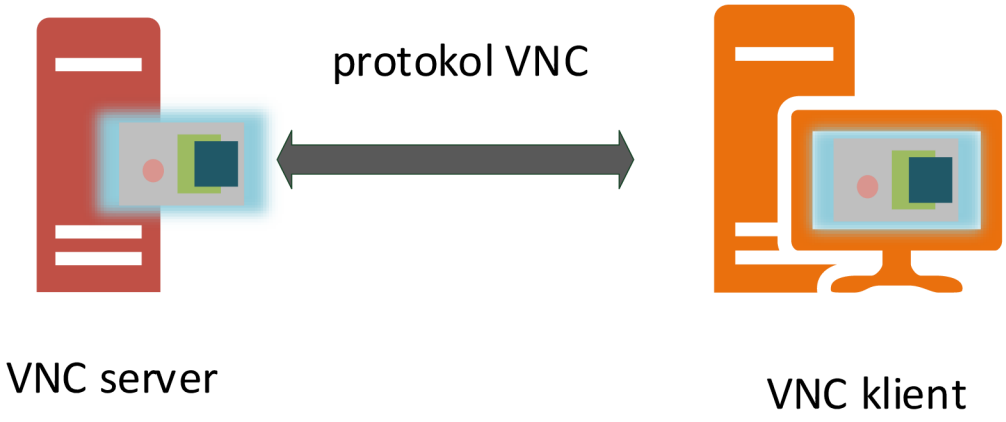
Evidentní výhodou všech řešení s VNC je skutečnost, že klientská aplikace nezatěžuje jeho CPU a operace probíhají na serveru. Zmiňovanou nevýhodou všech řešení je pak slabé zabezpečení VNC protokolu, které je třeba řešit nějakou formou bezpečného SSH nebo VPN spojení.[14][15]

VNC protokol

VNC protokol je totožný s protokolem RFB.

Tato technologie je základem systému VNC. Jedná se o jednoduchý protokol pro vzdálený přístup s grafickým uživatelským rozhraním. Pracuje na úrovni framebufferu, a proto je funkční ve všech operačních systémech a aplikacích. Připojení je možné k jakémukoli zařízení komunikujícím protokolem TCP/IP.

Jeden koncový bod, se kterým uživatel interaguje, je VNC klient. Druhý koncový bod, je VNC server. Zde dochází ke změně obsahu obrazovky a ten je ukládán do framebufferu na obrázku 2.



Obr. 2 VNC architektura.
Zdroj: RICHARDSON, T., Q. STAFFORD-FRASER, K.R. WOOD a. HOPPER. Virtual network computing. IEEE Internet Computing [online]. 1998 [cit. 2021-8-9]. ISSN 10897801. Dostupné z: doi:10.1109/4236.656066

Počátky VNC

Společnost ORL rozšířila X Window Systém, který umožňoval, aby aplikace pro zobrazení uživatelského rozhraní běžela na vzdáleném počítači. Zavedla tzv. teleportaci tzn. teleportoval se systém, kde běželo uživatelské rozhraní aplikace X, dynamicky na jiný displej. Nevýhodou tohoto způsobu přenosu obrazu bylo, že Systém X vyžadoval, aby program X server byl spuštěn na počítači, který řídí grafickou kartu. Ke spuštění tohoto softwaru byly třeba značné prostředky, které zařízení NCS nebo osobní digitální asistenty (PDA), neobsahovaly. [9]

Vývoj ultratenkého klienta

V roce 1994 společnost ORL vytvořila Videotile systém. Jednalo se o zobrazovací zařízení s LCD obrazovkou, perem a připojením k ATM síti. Videotile byl experiment v oblasti technologií ultratenkých klientů. Byl navržen pro zobrazování kvalitního videa, a měl být použit k interakci s aplikacemi. V prvním experimentu k tomuto účelu byla zvolena obrazovka vzdáleného počítače jako zdroj videa, které se jednoduše odeslalo na uživatelské rozhraní. Experiment fungoval, ale při přenosu se využívala velká šířka pásma. Reakcí na tuto skutečnost bylo, že se přestaly přenášet celá videa a začaly se posílat pouze ty části obrazovky, které se měnily. Tím se

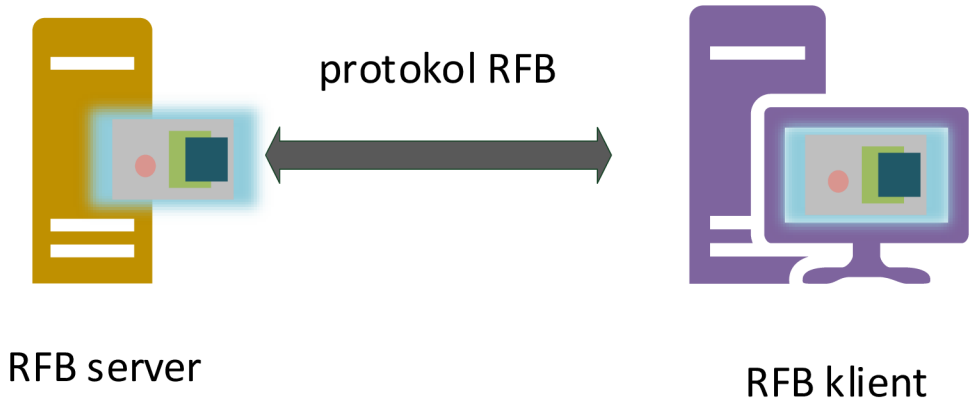
omezilo množství přenášených dat a následně se tato myšlenka promítla do protokolu VNC.

V roce 1995, kdy byla uvolněna první verze jazyka Java s prohlížečem HotJava od společnosti Sun Microsystems, se objevila myšlenka využít mechanismus Videotile v Javě pro přístup k aplikacím prostřednictvím webového prohlížeče. Vznikl tak Java applet s implementovaným VNC klientem, který umožňuje připojení do jakéhokoliv VNC serveru. [9]

4.1 Protokol RFB

RFB (Remote Framebuffer) na obrázku 3, je jednoduchý protokol používaný pro vzdálený přístup ke grafickému rozhraní uživatele. Je nedílnou součástí VNC aplikací. Protokol je řízen dle požadavků klienta. Data jednotlivých pixelů jsou přenášena pouze je-li klient připojen. I v případě, že se klient odpojí od serveru, stav uživatelského rozhraní zůstává zachován pro jeho opětovné připojení.

Protokol zjišťuje barevnou hloubku pixelů v prostoru vytyčeným souřadnicemi x, y. Framebuffer je složen z dílčích bufferů. Ukládají se do nich informace o barevné hloubce každého pixelu, počtu barev a parametry alfa kanálu. Ten definuje průhlednost daného pixelu. [4]



Obr. 3 RFB architektura.
Zdroj: RICHARDSON, T. and J. Levine. The Remote Framebuffer Protocol RFC 6143. RealVNC Ltd. [online]. March 2011. [cit. 11.08.2021]. Dostupné z: https://www.rfc-editor.org/info/rfc6143. DOI 10.17487/RFC6143

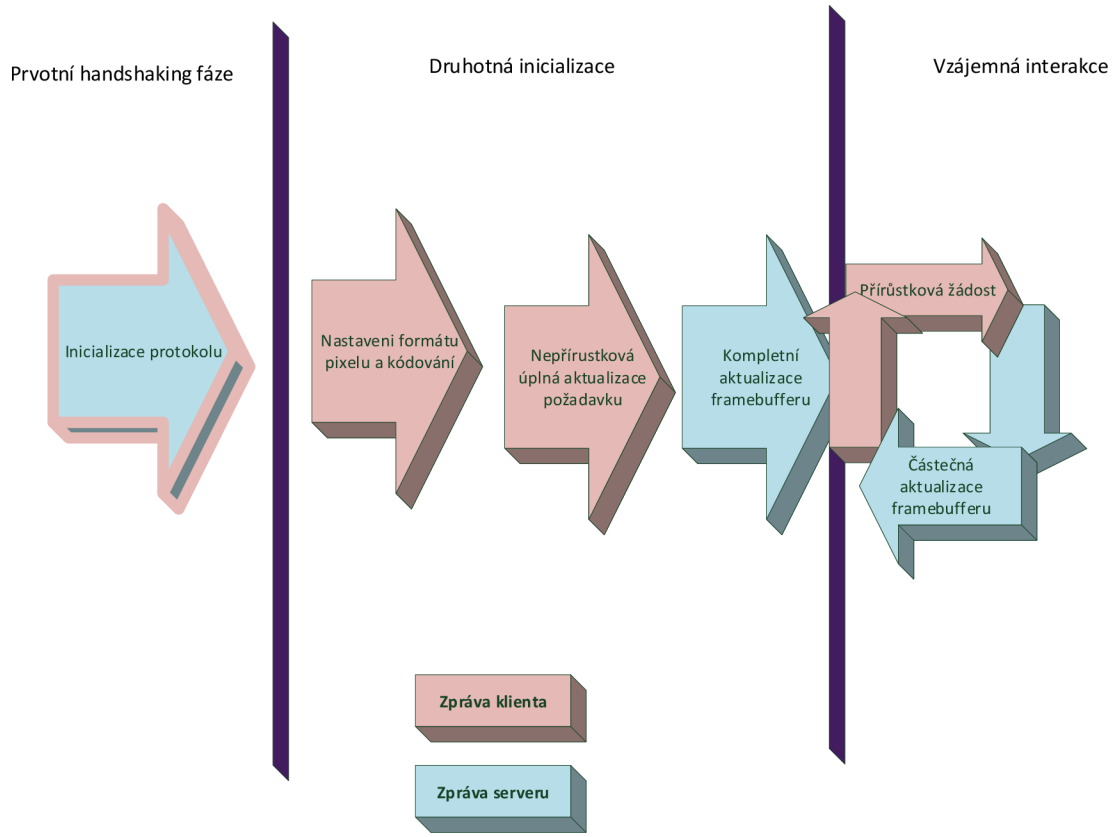
Přenos obrazových dat funguje takto:

- Host odešle obrázek plochy
- Klient odešle události klávesnice a myši hostiteli
- Na serveru se vykreslí obrázek a odešle ho zpět klientovi

Klient se může kdykoli odpojit a připojit znovu. [4]

Princip sestavení spojení

Připojení pomocí protokolu se sestává ze tří fází, jak je vyobrazeno na obrázku 4.



Obr. 4 VNC implementace.
Zdroj: RICHARDSON, T. and J. Levine. The Remote Framebuffer Protocol RFC 6143. RealVNC Ltd. [online]. March 2011. [cit. 11.08.2021]. Dostupné z: https://www.rfc-editor.org/info/rfc6143. DOI 10.17487/RFC6143

První (handshaking) fáze

Jde o prvotní navázaní komunikace. Klient a server si v této fázi vyměňují zprávy o parametrech přenosu, použité verzi protokolu, autorizaci a typu kódování se kterým budou data pixelu posílána. Na výběr je více typů kódování a několik

kódovacích schémat umožňujících komprimaci dat obrazových bodů a dalších parametrů. Parametry pro definici šířky pásma, rychlost vykreslování na straně klienta, rychlost zpracování na serveru. Server musí respektovat možnosti a nastavení parametrů formát pixelu, barevná hloubka a kódování na straně klienta. Spojení klienta se severem je při TCP komunikaci zahájeno tzv. handshakem. Následuje zasílání zpráv v rámci RFB protokolu na přiřazeném portu 5900. [4]

Verze protokolu

Server odesílá zprávu s informací o podporované verzi protokolu. Klient odesílá stejnou zprávu. Následně bude v komunikaci použita verze protokolu klienta, podmínkou však je, že nesmí být vyšší než verze serveru. [4]

Bezpečnost

Následujícím krokem po tom, co je potvrzena verze protokolu je nastavení typu zabezpečení, které bude použité při komunikaci mezi serverem a klientem. Kódy jednotlivých typů zabezpečení jsou uvedeny v tabulce 1.

Tabulka 1 Druhy zabezpečení.

Číslo	Jméno
0	Invalid
1	None
2	VNC Authentification

Zdroj: RICHARDSON, T. and J. Levine. The Remote Framebuffer Protocol RFC 6143. RealVNC Ltd. [online]. March 2011. [cit. 11.08.2021]. Dostupné z: https://www.rfc-editor.org/info/rfc6143. DOI 10.17487/RFC6143

Druhá fáze

Druhou fází je inicializace. Server a klient si pošlou inicializační zprávu. Klient posílá informaci o počtu možných uživatelů připojených najednou. Server informuje klienta o velikosti a parametrech jeho framebufferu:

- Šířka framebufferu
- Výška framebufferu
- Pixel formát serveru

Inicializace klienta

Klient posílá inicializační zprávu s příznakem *shared-flag*. Jestliže má server ponechat připojené dosavadní uživatele ke sdílené obrazovce, pak je tento příznak ve stavu PRAVDA. Stav NEPRAVDA reprezentuje exkluzivitu připojení klienta, tzn. že v tomto stavu dojde k odpojení ostatních klientů. [4]

Inicializace serveru

Po přijetí *ClientInitialisation* zprávy posílá server *ServerInitialistion* zprávu. V ní určuje šířku a výšku framebufferu serveru, typ formátování pixelů a jména spojeného s obrazovkou, jak je uvedeno v tabulce 2.

Tabulka 2 Zprávy serveru.

Počet bytů	Type [Value]	Popis
2	U16	*framebuffer-width*
2	U16	*framebuffer-height*
16	PIXEL_FORMAT	*server-pixel-format*
4	U32	*name-length*
name-length	U8 array	*name-string*

Zdroj: RICHARDSON, T. and J. Levine. The Remote Framebuffer Protocol RFC 6143. RealVNC Ltd. [online]. March 2011. [cit. 11.08.2021]. Dostupné z: https://www.rfc-editor.org/info/rfc6143. DOI 10.17487/RFC6143

Třetí fáze

V této fázi již probíhá normální interakce protokolu, kdy server s klientem vzájemně komunikují pomocí zasílaných zpráv. Protokol RFB definuje *client-to-server* zprávy a *server-to-client* zprávy, pomocí nich se vzájemně informují o událostech na vstupu

i změnách framebufferu. Vstupní parametry RFB protokolu, které představují události na klávesnici nebo myši počítače, jsou odeslány na server. [4]

Parametry zpráv klient-server

SetPixelFormat nastavuje formát hodnot pixelu ve FramebufferUpdate zprávách. Hodnoty zobrazuje tabulka 3. Pokud nepřijde SetPixelFormat zpráva od klienta, bude server posílat pixely dle nastavení ve zprávě ServerInit.

SetEncodings nastavuje druhy kódování.[9]

FramebufferUpdateRequest upozorňuje server na žádost o stavu framebufferu, který je definován x-pozicí, y-pozicí, šířkou a výškou. Server obvykle reaguje na FramebufferUpdateRequest zasláním zprávy FramebufferUpdate.

KeyEvent registruje události na klávesnici, přenáší informace o stisknuté nebo uvolněné klávese

PointerEvent vrací pozice kurzoru.

ClientCutText posílá serveru informace o použité sadě znaků na klávesnici. Podporuje kódování ISO 8859-1.[9]

Zprávy server-klient

FramebufferUpdate je zpráva jako odpověď na FramebufferUpdateRequest. Zpráva se skládá z nové sekvence dat pixelu, které si klient znovu ukládá do jeho framebufferu.

SetColourMapEntries je zpráva, která říká klientovi, které pixely mají být obarveny danou barvou RGB. To platí, pokud je používána mapa barev.

Bell generuje akustický signál na straně klienta

ServerCutText přenáší text mezi klientem a serverem v nastaveném kódování jazyka, podporuje I SO 8859-1.[4]

Tabulka 3 Hodnoty pro PixelFormat.

Počet bytů	Type [Hodnota]	Popis
1	U8	*bits-per-pixel*
1	U8	*depth*
1	U8	*big-endian-flag*
1	U8	*true-colour-flag*
2	U16	*red-max*
2	U16	*green-max*
2	U16	*blue-max*
1	U8	*red-shift*
1	U8	*green-shift*
1	U8	*blue-shift*
3	U8	*padding*

Zdroj: RICHARDSON, T. and J. Levine. The Remote Framebuffer Protocol RFC 6143. RealVNC Ltd. [online]. March 2011. [cit. 11.08.2021]. Dostupné z: https://www.rfc-editor.org/info/rfc6143. DOI 10.17487/RFC6143

Bezpečnost

Protokol nepoužívá bezpečnostní ochranu. Heslo pro VNC autentifikaci je slabé a není proto doporučeno jeho použití v nezabezpečených sítích. Proto se doporučuje přenos v IPSec nebo SSH kanálech. [4]

Schémata kódování

Schéma kódování specifikuje kompresní algoritmus, který se používá pro kódování dat pixelů. Vybrané schéma ovlivňují různé parametry, jako je šířka pásma sítě, rychlost vykreslení na straně klienta a rychlost zpracování na straně serveru.[2]

Všichni klienti a servery VNC musí podporovat tato kódování. Nicméně, výběr kódování, které bude nakonec použito pro dané připojení, záleží na možnostech serveru a klienta a spojení mezi nimi.[4]

Druhy kódování

Všechny dostupné druhy kódování obrazu obsahuje tabulka 4.

Tabulka 4 Druhy kódování.

Číslo	Jméno
0	Raw
1	CopyRect
2	RRE
5	Hextile
15	TRLE
16	ZRLE
-239	Cursor pseudo-encoding
-223	DesktopSize pseudo-encoding

Zdroj: RICHARDSON, T. and J. Levine. The Remote Framebuffer Protocol RFC 6143. RealVNC Ltd. [online]. March 2011. [cit. 11.08.2021]. Dostupné z: https://www.rfc-editor.org/info/rfc6143. DOI 10.17487/RFC6143

Raw

Kódování Raw je nejjednodušším typem, jde o surová data. Reprezentují ho hodnoty pixelu, tj. šířka a výška pixelu při skenování obrazovky v řádku zleva doprava. Nedostatkem tohoto kódování je chybějící komprese. Server i klient zpracují sice data velmi rychle, ale pouze při využití šířky celého pásma. Z toho důvodu je Raw kódování vhodné pro místní připojení ke stejnému počítači s prakticky neomezenou šířkou pásma, ale je nepoužitelné pro připojení přes pomalý modem. [4]

CopyRect

Použití této touto metody kódování je velmi jednoduché a efektivní. Lze ho aplikovat tehdy kdy klient již má k dispozici stejná pixel data uložená jinde ve svém framebufferu. Klient pak může z pozice na souřadnicích XY zkopírovat obdélník s parametry pixelu. Využití této metody se dá v situacích, kdy uživatel pohybuje oknem po obrazovce a obsah okna se neustále posouvá. [4]

RRE

Kódovací metoda RRE pracuje tak, že rozdělí obdélník dat pixelů do menších podoblastí. Každá z nich má optimální velikost a lze ji jednoduše vypočítat. Podoblast obsahuje pixely s jedinou hodnotou. Následným sloučením podoblastí dojde k rekonstrukci celé původní obdélníkové oblasti.

Kódovací metoda využívá hodnotu pixelu pozadí *Vb* (ta představuje nejrozšířenější hodnotu pixelu v obdélníku) a dále počet N. Jednotlivé obdélníky v počtu N jsou deklarovány v seznamu. Každý obdélník je reprezentován čtyřmi parametry *vxywh*. Parametr *v* je hodnota pixelu, parametry *xy* jsou souřadnice obdélníku. Počátek je definován nulovými souřadnicemi v levém horním rohu. Další parametry *wh* představují šířku a výšku obdélníku.

Zobrazení původního obdélníku provede klient, tak že vykreslí obdélník a vyplní ho hodnotou pixelu pozadí.[4]

Hextile

Kódovací metoda Hextile představuje variantu kódování RRE. Metoda spočívá v rozdělení kódovaného obdélníku na menší obdélníky, o rozměrech 16x16 dlaždic. Rozměry každého obdélníku v dlaždici representují 4 bity, celkem 16 bitů (*xy* pozice, šířka a výška). První kódování je aplikováno na dlaždici vlevo nahoře a dále se pokračuje zleva doprava, shora dolů. Dojde-li k situaci, že šířka celého obdélníku není přesný násobek 16, dojde k zmenšení šířky poslední dlaždice v každém řádku. Podobně, pokud výška celého obdélníku není přesný násobek 16, pak výška každé dlaždice v celém řádku bude také menší. [4][2]

4.2 VPN

Virtuální neveřejná síť (Virtual private network) označuje kategorii podnikových sítí, jež propojují koncová zařízení nebo celé sítě přes veřejnou počítačovou síť, viz obrázek 5. [13]

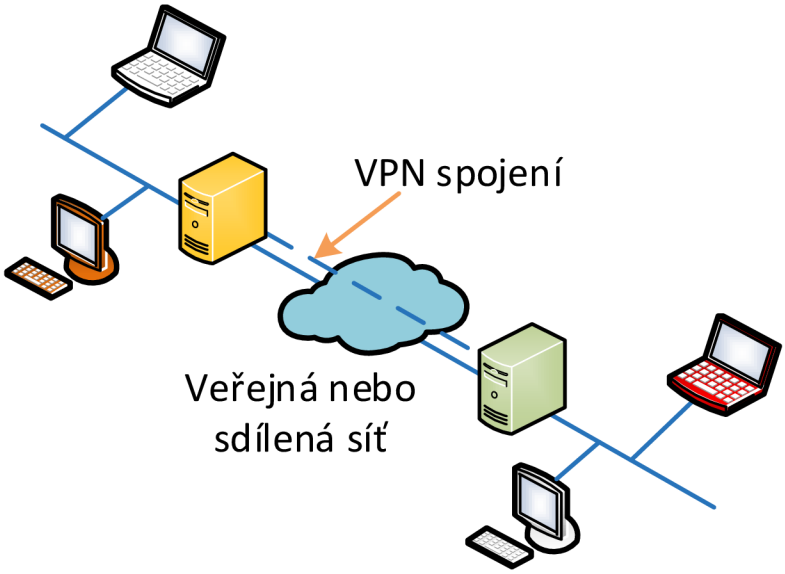
Představení VPN připojení

Pro spojení s cílovým počítačem v zákaznícké síti je potřeba bezpečné propojení přes veřejnou počítačovou síť. Takové, které bude garantovat ochranu a bezpečný přenos dat mezi koncovou stanicí, např. VNC serverem a klientem v řídícím dohledovém centru, se nazývá VPN. [17]

Připojení pomocí VPN vzdáleného přístupu umožňuje uživatelům, kteří pracují doma nebo na cestách, pracovat se serverem v privátní síti pomocí infrastruktury veřejné sítě – internetu. Propojením sítí pomocí VPN vzniká privátní zabezpečená linka ve veřejné nezabezpečené síti. Síťové prostředky mohou uživatelé využívat stejným způsobem jako v rámci jedné lokální sítě. Propojením sítí nebo koncových zařízení VPN pomocí tunelovacích protokolů spojové nebo síťové vrstvy modelu dosáhneme spojení, které odpovídá propojení v jedné lokální síti. VPN je ale virtuální síť. Pouze se zdá že se jedná o síť používanou jednou organizací. Síť ale sdílí ostatní uživatelé veřejné sítě. [13; 21; 22; 23; 24; 18]

Postup připojení

Klient VPN virtuálně volá virtuální port na VPN serveru, pomocí tunelovacích protokolů. Na **VPN serveru** proběhne autentizace volajícího a teprve pak se přenesou data. V hlavičce zapouzdřená data odesílaná do sdílené nebo veřejné sítě jsou zašifrována pomocí šifrovacích klíčů, bez nich nejsou pakety čitelné. Záhlaví obsahuje informace o směrování, díky nimž je umožněn průchod dat sdílenou či veřejnou sítí až k cílovému bodu. Používají se protokoly PPTP, L2TP a SSTP. [3; 21; 22; 23; 24]



Obr. 5 VPN.
Zdroj: What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

4.3 Druhy VPN

Dle zapouzdření:

Tunelovaná linka – zapouzdřený a zašifrovaný je celý paket.

Transportní linka – je zapouzdřená a zašifrovaná je pouze datová část paketu.

Dle připojení:

Site-to-site

Je takové spojení VPN, jímž je možné realizovat vzájemné propojení dvou sítí nebo většího počtu privátních sítí. [6; 21; 22; 23; 24]

VPN server, umístěný v jedné ze sítí, umožňuje připojení VPN klientovi z jiných sítí. Klient VPN, který žádá o připojení se ověřuje jako první na straně dotazovaného serveru VPN. Teprve poté co je úspěšně ověřen klient následuje ověření serveru na straně klienta. [13; 21; 22; 23; 24]

Remote Access

Je takové spojení VPN, které zajistí možnost vzdáleného přístupu na server z domácí sítě přes internet. Jako příklad si lze představit připojení klienta, který se připojí do firemní privátní sítě. [3; 21; 22; 23; 24]

4.4 Zabezpečení připojení VPN

Přenášená data je třeba zabezpečit, k tomu účelu slouží tzv. tunelovací protokoly PPTP, L2TP/IPSec a SSTP. Ty používají rozličné způsoby šifrování a různé druhy ověření. Data jsou zapouzdřena hlavičkou, která obsahuje směrovací informace. Takto se data posílají vytvořeným tunelem. [3; 21; 22; 23; 24]

Typy ověřování:

1. **pomocí protokolu PPP** je možné bezpečně ověřit uživatele. Ověřování začíná na straně VPN serveru, ten nejprve začne s ověřováním VPN klienta, který se zkouší pomocí Point-to-Point protokolu (PPP) připojit. Klient VPN poté začne ověřovat server VPN. Metoda vzájemného ověřování poskytuje ochranu vůči počítačům, které by se pouze vydávaly za VPN servery. [3; 21; 22; 23; 24; 19]
2. **pomocí Internet Key Exchange (IKE)** protokol využívá ověřovací mechanismus, který porovnává certifikáty klienta a serveru. Metody, kterými IKE protokol řeší výměnu počítačových certifikátů nebo předsdíleného klíče, se spouští při první fázi vytváření připojení L2TP/IPSec. Novější varianta protokolu nazvaná IKEv2 již dokáže sestavit spojení výrazně rychleji. [3; 21; 22; 23; 24]
3. **pomocí původu dat a neporušenosti dat** tato metoda ověřuje u připojení L2TP/IPSec, zda data, která byla pomocí připojení VPN odeslána, opravdu pochází, tzn. byla vytvořena na druhém konci připojení a zda nebyla během přenosu změněna. Data obsahují kontrolní součet založený na šifrovacím klíči, který je zná pouze odesílatel a příjemce. [19; 3; 21; 22; 23; 24]

Šifrování dat

Aby bylo zajištěno utajení dat při průchodu sdílenou nebo veřejnou tranzitní sítí, odesílatel data zašifruje a příjemce je dešifruje. V tabulce 5 jsou uvedeny tyto šifrovací a dešifrovací procesy, ty probíhají u odesílatele i příjemce a používají společný šifrovací klíč. [13; 21; 22; 23; 3; 19]

Zachycené pakety odeslané prostřednictvím připojení VPN v tranzitní síti nejsou srozumitelné pro toho, kdo nemá společný šifrovací klíč. Důležitým parametrem zabezpečení je délka šifrovacího klíče. Šifrovací klíč lze určit pomocí výpočetních technik. Tyto techniky však vyžadují větší výpočetní výkon a delší výpočetní čas v závislosti na velikosti klíče. Aby byla zajištěna co možná největší bezpečnost a důvěryhodnost dat používá se co největší možná velikost klíče. [3; 21; 22; 23; 19]

Tabulka 5 Druhy šifrovacích protokolů.

Protokol	Protokol šifrování	Šifrování rámců	Klíče
PPTP	PPP	MPPE	MS-CHAPv2, EAP-TLS
SSTP	HTTPS	SSL	EAP-TLS
L2TP	IPSec	DES, Triple DES	

Zdroj: What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

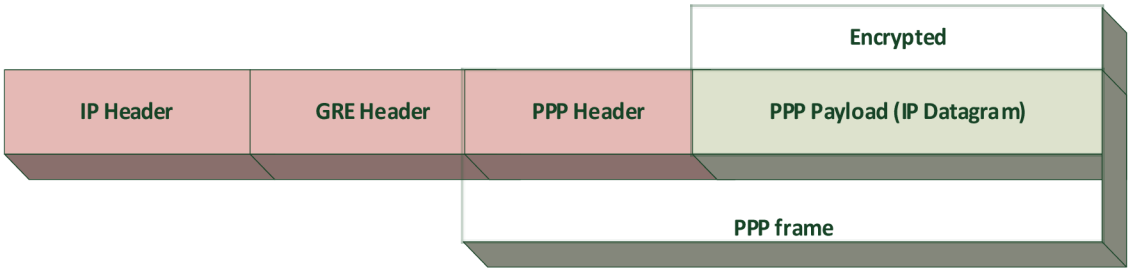
Protokoly tunelování

Tunelování zajišťuje zapouzdření paketu z jednoho typu protokolu do datagramu jiného protokolu. Využití PPTP k zapouzdření IP paketů používá VPN sestavování spojení. Řešení VPN lze nakonfigurovat na protokolu PPT (Point-to-Point Tunelování Protocol), protokolu L2TP (Layer Two Tunneling Protocol) nebo protokolu SSTP (Secure Socket Tunneling Protocol). Možnosti jednotlivých protokolů PPTP, L2TP a SSTP závisí na vlastnostech původně určených pro protokol PPP (Point-to-Point Protocol). Protokol PPP zapouzdřuje IP pakety v rámci PPP rámců a poté přenáší zapouzdřené PPP pakety přes spojení point-to-point. [19; 3; 21; 22; 23; 24]

PPTP

PPTP umožňuje šifrování provozu s více protokoly a jejich zapouzdření do hlavičky IP. Protokol PPTP lze použít pro vzdálený přístup a připojení VPN mezi servery. Zapouzdření PPTP na obrázku 6, zapouzdřuje PPP rámce v IP datagramech pro přenos po síti. PPTP používá připojení TCP pro správu tunelů a upravenou verzi Generic Routing Encapsulation. [20; 21; 22; 23; 24; 19]

Protokol PPTP nepoužívá metodu veřejných klíčů (PKI), tím se liší od protokolu L2TP/IPSec. Nezabrání tedy přečtení odchycených paketů, k tomu by byl nutný šifrovací klíč. Protokol neobsahuje informace o integritě dat, nelze tak deklarovat, že data nebyla během přenosu změněna. Není možné ani ověřit, že data odeslal ověřený uživatel, a tak zjistit jejich původ. [3; 21; 22; 23; 24]



Obr. 6 Ukázka šifrování PPTP.
Zdroj: What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

SSTP

Secure Socket Tunneling Protocol (SSTP) je nový protokol tunelového propojení, který používá protokol HTTPS. Přes TCP port 443 zprostředkovává přenos skrz bránu firewall a webové proxy servery. Ty obyčejně blokují PPTP a L2TP/IPSec přenos. Protokol SSTP používá mechanismus pro zapouzdření přenosu protokolu PPP prostřednictvím kanálu Secure Sockets Layer (SSL) na protokolu HTTPS. VPN připojení začíná nejdříve vytvořením obousměrného spojení se serverem SSTP, teprve pak jsou přenášena data. [3; 19; 22; 23; 13]

Zapouzdření

SSTP zapouzdřuje rámce protokolu PPP v datagramech IP pro přenos v síti. SSTP využívá pro připojení port 443, ten používá jak pro tunel, tak i datové rámce protokolu PPP. Zpráva SSTP je šifrována pomocí kanálu SSL protokolu HTTPS. [3; 19; 22; 23; 13]

Protokol L2TP

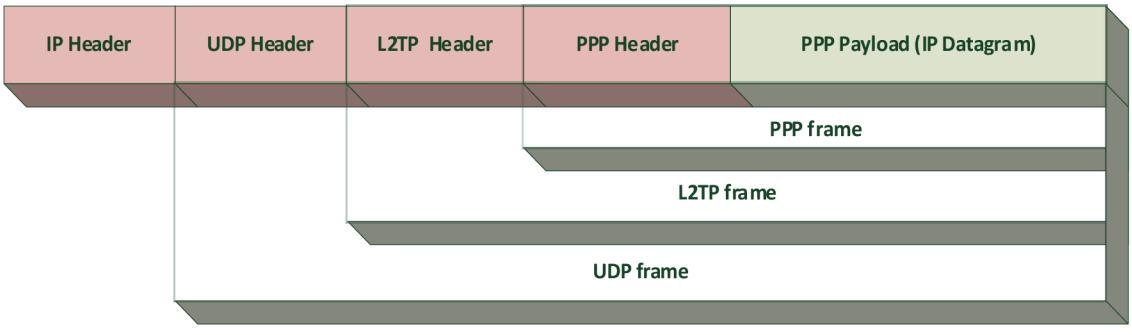
L2TP umožňuje šifrování přenosů s více protokoly, pracuje tak že částečně používá jak PPTP, tak i Layer 2 Forwarding (L2F) a nabízí tak to nejlepší z funkcí obou protokolů. L2TP k šifrování datagramů protokolu PPP nepoužívá šifrování MPPE, ale používá protokol IPSec. Kombinace protokolu L2TP a zabezpečení IPSec se nazývá L2TP/IPSec. Klient VPN i VPN server musí podporovat protokol L2TP a IPSec. [3; 19; 22; 23; 24]

Připojení L2TP/IPSec umožňuje ověřování počítačů ve vrstvě protokolu IPSec a ověřování uživatelů ve vrstvě protokolu PPP, to je rozdíl oproti protokolu PPTP a SSTP. Z důvodu ověřování a vydávání počítačových certifikátů pro počítač serveru VPN a všechny klientské počítače VPN je nutné zavést infrastrukturu veřejných klíčů. Při použití protokolu IPSec, zabezpečuje připojení L2TP/IPSec utajení, integritu a ověřování dat. [3; 13; 19; 21; 22; 23]

Vrstvy zapouzdření paketů protokolu L2TP/IPSec

První vrstva: L2TP zapouzdření rámce

PPP (IP datagram) se zapouzdřuje nejdříve do hlavičky protokolu L2TP a dále pak do hlavičky protokolu UDP, jak ukazuje obrázek 7.

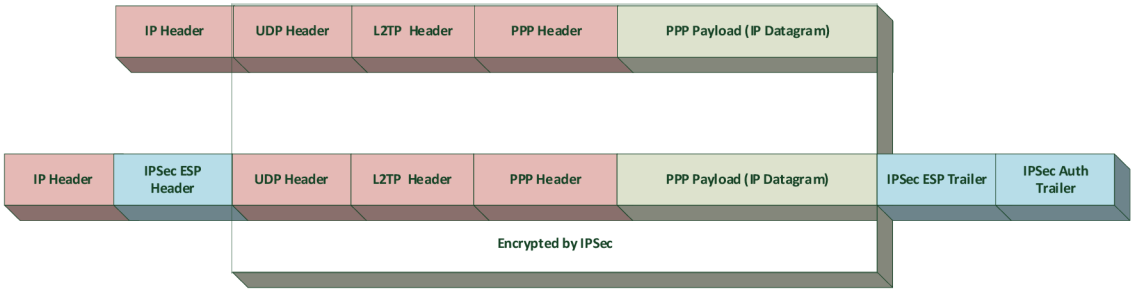


Obr. 7 Rozložený paket L2TP s IP Datagramem.

Zdroj: What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

Druhá vrstva: IPSec zapouzdření

Trailerem IPSec Encapsulating Security Payload (ESP) zabalená zpráva L2TP se spolu s hlavičkou zabezpečuje lepší integritu a ověřování zpráv. IP adresy strany klienta VPN a serveru VPN jsou definovány v hlavičce, viz. obrázek 8. [3; 21; 22; 23]



Obr. 8 IPSec zapouzdření.
Zdroj: What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

VPN realizovaná v transportní a aplikační vrstvě

SSL/TLS (Secure Socket Layer/Transport Layer Security)

Vytvořený tunel používá šifrování protokolu SSL, kdy dochází ke změně hlavičky IP nebo TCP hlavičky paketu. Vlastní SSL protokol využívá několik dílčích protokolů. Zabezpečení uživatelů a jejich identifikačních údajů zajišťuje technologie asymetrického šifrování soukromého a sdíleného klíče. Data, která se přenáší mezi koncovými zařízeními jsou protokolem **SSL/TLS** zašifrovaná. [3; 18; 21; 22; 23]

Hlavní protokoly SSL/TLS

HP (Handshake Protocol) protokol umožňuje, aby se účastníci komunikace dohodli na způsobu šifrování a zabezpečení. [3; 21; 22; 23; 24]

RLP (Record Layer Protocol) je protokol, který pracuje s daty, provádí kontrolní výpočty, provádí šifrování při odesílání dat a dešifruje data při příjmu. Zajišťuje přenos Handshake protokolu. [19; 3; 21; 22; 23]

CCSP (Change Cipher Specification Protocol) má na starosti pravidla podle kterých bude probíhat komunikace, informuje o tom prostřednictvím Handshake protokolu. [3; 19; 22]

AP (Alert Protocol) má starosti chyby vzniklé při komunikaci o nich pak informuje protější strany spojení. [11; 21; 22; 23; 24]

VPN na síťové vrstvě obsahuje směrovací informace potřebné ke směrování IP protokolu. Stupeň zabezpečení, s kterým bylo VPN vytvořeno záleží na použitém protokolu, který, definuje typ šifrování atd. [3]

IPSec

Protokol IPSec (Internet Protocol SECurity) poskytuje potřebné zabezpečení pro protokol IPv4. Protokol IPv4 totiž neobsahuje spolehlivou ochranu přenášených dat a negarantuje ani pravost odesílatele. IPSec ovládá jak vytvoření tunelu, tak i zabezpečení autenticity a šifrování přenášených dat. IPSec zahrnuje skupinu protokolů, které spolupracují na bezpečnosti jednotlivých IP datagramů. Protokol zajišťuje vytvoření VPN spojení s vysokým stupněm zabezpečení. Výhodou systémů IPSec VPN je že nejsou běžně zachyceny při skenování portů a samotná složitost protokolů odrazuje útočníky. [11; 21; 22; 23; 24]

Hlavní protokoly IPSec

IKE (Internet Key Exchange) – Protokol, který má na starosti ověřování pravosti klíčů a jejich výměnu mezi systémy. Dále zprostředkovává šifrovací algoritmy. [21; 22; 23; 11]

AH (Authentication Header) – Protokol integrity a autentizace dat. Zabraňuje útokům, které využívají zopakování přenášených dat. [11; 21; 22; 23]

ESP (Encapsulating Security Payload) – Protokol, který také zajišťuje integritu a autentizaci dat nebo může být zvolen pro šifrování dat.[13][11]

Režimy IPSec

Transportní režim zabalí data do IP paketu, ta obsahuje adresy strany přijímané a také strany odesílané. Použití transportního režim se uplatňuje zejména při komunikaci Uživatel – Uživatel. [21; 22; 23; 24; 11]

Tunelový režim pracuje pouze s daty a IP hlavička zůstává. Tunelový režim je uplatňován při komunikaci Server – Server u spojování celých sítí. [6; 21; 22; 23; 24]

Porovnání bezpečnosti IPSec a SSL

Oba modely podporují bezpečnostní algoritmy MD5 nebo SHA1. Bezpečná komunikace vzdáleného uživatele a serveru přes veřejnou síť je tak zajištěna oběma modely. [6; 21; 22; 23; 24; 11]

SSL se používá k zabezpečení některých aplikací typu klient-server. SSL šifruje pomocí 40bitového klíče, a to nad transportní vrstvou, tím jsou ochráněna data aplikací. Ochrana před útoky typu DoS, ale není dostatečná. Jeho nasazení může být realizováno pro připojení mobilních koncových zařízení ve veřejných přístupových sítích. [11; 21; 22; 23; 24]

IPSec řešení vede k většímu zabezpečení komunikace mezi koncovými body.
Pracuje na síťové vrstvě mezi klientem a serverem a neomezuje podporované aplikace. K šifrování používá 128bitový klíč, podporuje silné šifrování typu 3DES nebo AES. Protokol ESP, který používá šifruje původní záhlaví IP a TCP. Výhodou IPSec je ochrana před analýzou provozu, to je něco, co SSL nepodporuje. [13; 21; 22; 23; 24]

5 Aktuální stav a přístupy vzdálené správy zdravotnické techniky

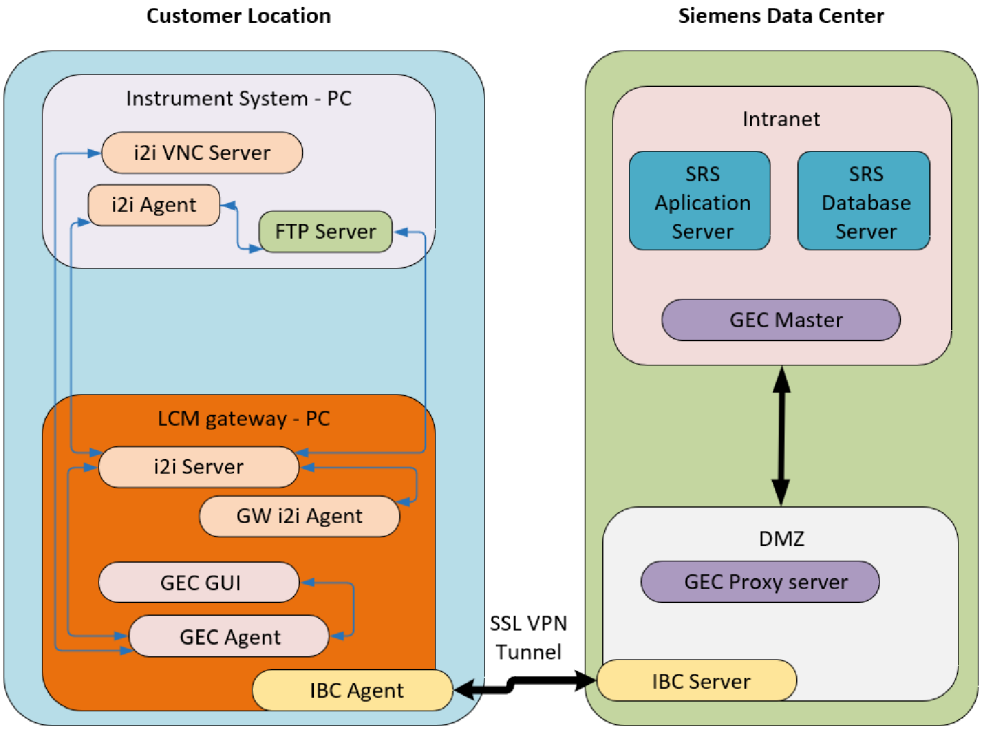
Dosavadní řešení reprezentuje schéma na obrázku 9.

Customer Location – Strana zákazníka

V zákazníkově síti je umístěn řídící PC analyzátoru a PC gateway (LCM), který udržuje s PC analyzátoru obousměrnou komunikaci. Počítač brány LCM je propojen se SRS serverem Siemens data centra ve vzdálené DMZ zóně. Toto spojení je vytvořeno pomocí VPN tunelu s SSL šifrováním. [1]

Siemens Data Center

Obslužná aplikace Siemens data centra je realizována jako SaaS (Software as a Service) aplikace. Jde o webového klienta využívající platformu Java. Obsahuje databázi jednotlivých koncových stanic tzn. řídících PC analyzátorů a PC gateway (LCM). Umožňuje jejich správu a vzdálenou kontrolu.



Obr. 9 Blokové schéma současného stavu.
Zdroj: Document Library – Siemens Healthineers. Document Library – Siemens Healthineers [online]. Dostupné z: https://doclib.siemens-healthineers.com/home

Strana zákazníka obsahuje

Řídící PC analyzátoru je koncová stanice a má spuštěny tyto služby

- I2i agent
- VNC server

PC gateway LCM je počítač, v něm instalované podpůrné služby zajišťují spojení s analyzátory a zprostředkovává připojení se Siemens Data Centrem (SRS). Instalované aplikace jsou:

- I2i server
- GW i2i Agent
- GEC GUI
- GEC agent
- IBC agent

GEC GUI je grafické prostředí aplikace, která obsahuje databázi všech připojených strojů v lokální síti zákazníka

GEC agent je klient aplikace GEC, adresuje žádosti VNC klienta z SRS na počítač analyzátoru, kde je i2i Server.

IBC agent je klient aplikace IBC, posílá zprávu na IBC server a iniciuje sestavení VPN tunelu

Strana SRS serveru obsahuje

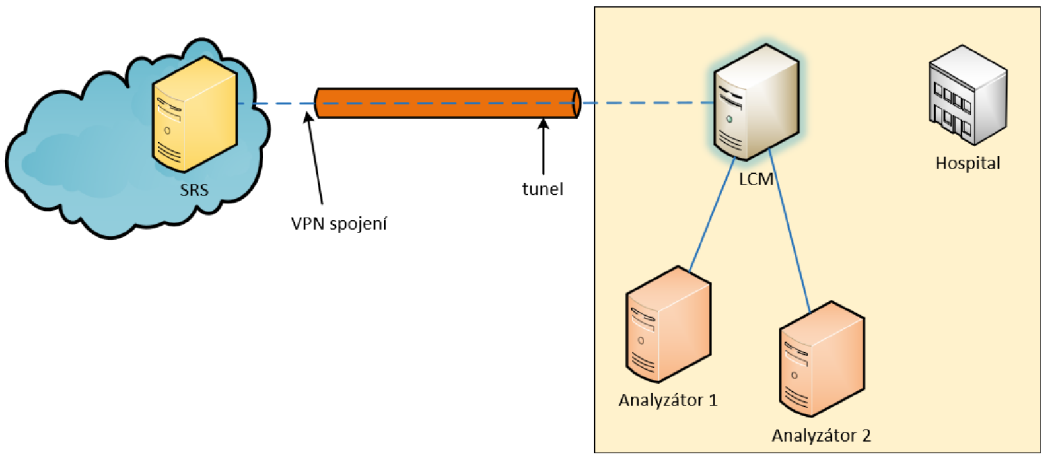
IBC server čeká na přihlášení IBC klienta, následně sestavuje VPN tunel

GEC proxy server překládá adresy připojených klientů

SRS application server jedná se o SaaS aplikaci s integrovaným VNC klientem

SRS database server je databáze používaná SaaS aplikací

[1]



Obr. 10 Schéma připojení VPN.
Zdroj: Document Library – Siemens Healthineers. Document Library – Siemens Healthineers [online]. Dostupné z: https://doclib.siemens-healthineers.com/home

Popis spojení k analyzátoru

i2i Agent instalovaný v PC analyzátoru inicializuje spojení vysláním dotazu na portu 20001. I2i server na LCM akceptuje dotaz a sestaví spojení.[1]

Popis spojení k serveru SRS

Siemens používá VPN klienta cRSP SSL VPN verze 1.5.2 RC1. Připojení VPN probíhá na transportní a aplikační vrstvě pomocí protokolů SSL/TLS. Pokud zákazníkova síť používá proxy server pro přístup ven, je možné jeho parametry nadefinovat v nastavení LCM. Služba na straně Siemens serveru poslouchá na portu 443, obrázek 10.

Vznik relace vzdáleného přístupu

Pokud má zákazník problémy s funkcí analyzátoru vyžádá si vzdálenou Siemens podporu. Pracovník Siemens podpory se přihlásí do obslužné aplikace SRS a vyhledá zákazníkův přístroj v databázi a iniciuje připojení k tomuto přístroji. VNC klient na straně SRS portálu vysílá dotaz na VNC server řídícího počítače analyzátoru. Na jeho obrazovce se objeví žádost v podobě informačního okna k povolení přístupu. Ta musí být přijata zákazníkem během 30 sekund jinak bude relace ukončena. Jakmile

zákazník povolí přístup je veškerá aktivita připojeného pracovníka podpory viditelná na monitoru řídícího počítače analyzátoru. [1]

Struktura dat

Všechna data jsou při datovém přenosu do SRS zašifrovaná a jedná se o následující typy dat:

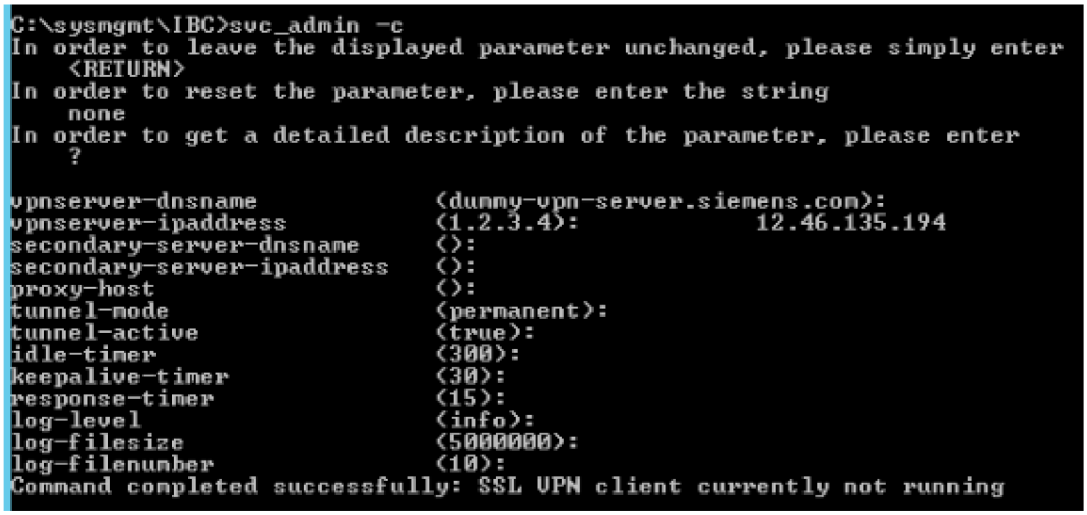
• Chyby systému (software, data ze senzorů)

• Soubory (přenesené automaticky nebo na požádání)

• Výsledky testu

Sestavení VPN připojení

V aplikaci cmd z příkazového řádku spustíme batch file Register.cmd, jak je vidět na obrázku 11. Ten aktivuje cRSP_SSL_VPN_klienta příkazem C:\SYSMGMT\IBC\svc_admin.exe -m–f "svc_request.xml"



Obr. 11 připojení pomocí VPN.
Zdroj: Vlastní zpracování

Příkazy VPN klienta

Následující funkce vyvoláme doplněním parametru za příkaz svc_admin

Change Configuration (option – c) Příkaz nastaví parametry spojení IP VPN serveru

Registration (option – r) Zadáním hesla a parametrů spojení příkaz zaregistruje klienta na serveru

Deregistration (option – d) Příkaz provede zrušení registrace na SRS portálu

Connectivity Test (option – t) testuje dosažitelnost serveru

Status Information (option – s s) vrací informaci o stavu spojení

Current Configuration (option – s c) vypíše konfiguraci spojení

Version Information (option – v) vrací verzi klienta a operačního systému

Help (option – h) zobrazí nápovědu

Navázání spojení

Na obrázku 12 je nastavení parametrů VPN klienta, to provedeme na příkazovém řádku pomocí příkazu C:\sysmgmt\IBC>svc_admin – c

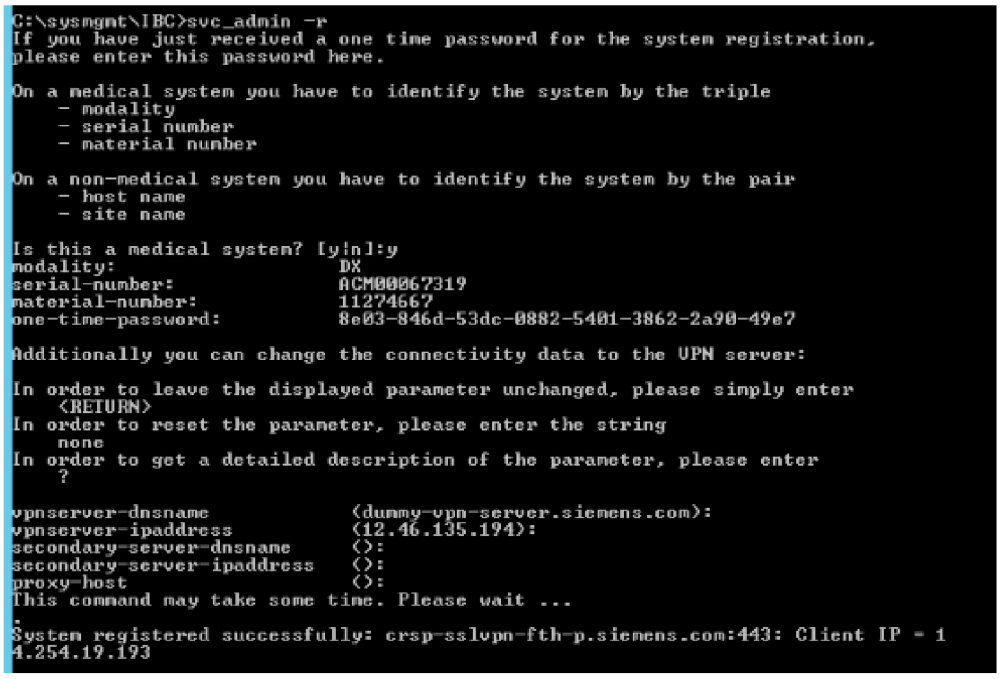
```
C:\sysmgmt\IBC>svc_admin -c
In order to leave the displayed parameter unchanged, please simply enter
    <RETURN>
In order to reset the parameter, please enter the string
    none
In order to get a detailed description of the parameter, please enter
    ?

vpnserver-dnsname            (dummy-vpn-server.siemens.com):
vpnserver-ipaddress          (1.2.3.4):            12.46.135.194
secondary-server-dnsname     ():
secondary-server-ipaddress   ():
proxy-host                   ():
tunnel-mode                  (permanent):
tunnel-active                (true):
idle-timer                   (300):
keepalive-timer              (30):
response-timer               (15):
log-level                    (info):
log-filesize                 (5000000):
log-filenumber               (10):
Command completed successfully: SSL VPN client currently not running
```

Obr. 12 Spojení VPN.
Zdroj: Vlastní zpracování

Registrace a spuštění VPN tunelu

Registraci a sestavení VPN tunelu provádíme pomocí příkazu svc_admin – r



Obr. 13 Spuštění VPN.
Zdroj: Vlastní zpracování

Tímto došlo k sestavení VPN tunelu, pomocí protokolu TLS 1.2 a šifrováním AES256:
2020-05-01 20:09:12.494 DEBUG svcevent vpnSrvConcf: SSL connection established with ciphers 'ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM (256) Mac=AEAD'
2020-05-01 20:09:12.495 DEBUG svctimer stopConnectRetryTimer(conn=022E6610)

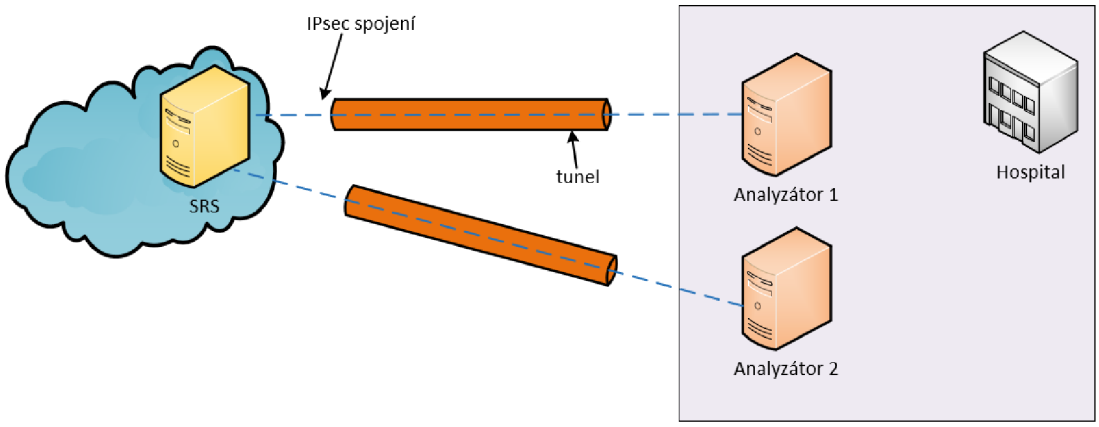
Následuje fáze registrace LCM na sCRP:
2020-05-01 20:09:12.495 DEBUG svcevent vpnSrvConcf(): Generate request to register server on current connection.

Přidělení IP adresy ve vytvořené VLAN:
2020-05-01 20:09:16.736 INFO svcevent Virtual LAN device configured: IP=14.254.19.193, MAC=00: ff:63:15:77:7 b, MTU=1500

6 Návrh modelu systému využití VNC jako hlavního systému pro vzdálenou komunikaci s možností automatické diagnostiky specializovaných zdravotnických zařízení firmy Siemens

Cílem vlastního modelu je ukázat řešení vyznačující se časovou úsporou při připojování k analyzátorům, rychlejší odezvou při práci na vzdálené obrazovce. Řešení, které se bude vyznačovat vyšší bezpečností a ochranou přenášených dat. Zajistí také průběžné monitorování chodu stroje pomocí přenosu souborů s chybovými hláškami.

Řešení na obrázku 14, předpokládá změnu schématu propojení koncového počítače s SRS portálem na Siemens serveru. Spojení tedy propojí přímo obě koncové stanice pomocí IPSec tunelu.



Obr. 14 Schéma připojení pomocí IPSec.
Zdroj: Vlastní zpracování

6.1 Výběr technologie

Výběr tenkého klienta

Výčet možných klientů zobrazuje tabulka 6.

Tabulka 6 Druhy klientů.

typ	Vlastní user account	Platforma	Cloud server
RDP	Ano	Win, Linux	ne
Teamviewer	ano	Win, Linux	ano
VNC	ne	Win, Linux	ne

Zdroj: What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

Pro řešení přenosu souborů a rychlejší odezvu by bylo vhodnější použít RDP připojení. Při přihlášení přes RDP však dojde k odhlášení současného uživatele. To není žádoucí z pohledu zákazníka, který by neviděl právě probíhající aktivitu vzdáleně připojeného pracovníka podpory, ale pouze přihlašovací obrazovku.

Použití **Teamvieweru** by zase ve většině případů odporovalo bezpečností politice zákazníka.

Použití **VNC** se jeví jako nadále nejvhodnější pro zajištění pomoci pro zákazníka přístupem přímo na obrazovku počítače analyzátoru právě přihlášeného uživatele. Vzhledem k tomu že řídící počítače analyzátorů používají operační systém různých platformách Windows, Apple, Linux, byl znovu zvolen VNC jako multiplatformní protokol. Uživatelé servisní organizace totiž používají k přístupu zařízení – počítače, tablety s operačním systémem různých platforem.

Výběr tenkého klienta

Porovnání VPN protokolů z hlediska bezpečnosti zobrazuje tabulka 7. Díky slabému šifrování hesla ve VNC bude výhodnější použít IPSec tunel a přídavná zabezpečení.

Tabulka 7 Porovnání bezpečnosti VPN.

	IPSec	SSL
Použití	TCP/IP protokol	Web, mail, sdílení souborů
Šifrování	Silná, 128bitovým klíčem	Různě silná, 40bitovým klíčem
Autentizace	Silná(obousměrná)	Různě silná
Míra zabezpečení	Velmi silná	Střední

Zdroj: PUŽMANOVÁ, Rita. TCP/IP v kostce. České Budějovice: Kopp, 2004. 611 stran. ISBN 8072322362.

Výběr VPN serveru

Stěžejní částí řešení je VPN server. Protože však není možné zasáhnout do nastavení Siemens infrastruktury na straně Siemens a vytvořit tak IPSec spojení. Není tak možné testování v reálných podmínkách. Pro testovací účely bude vybrán jeden z open source VPN systémů, tabulka 8.

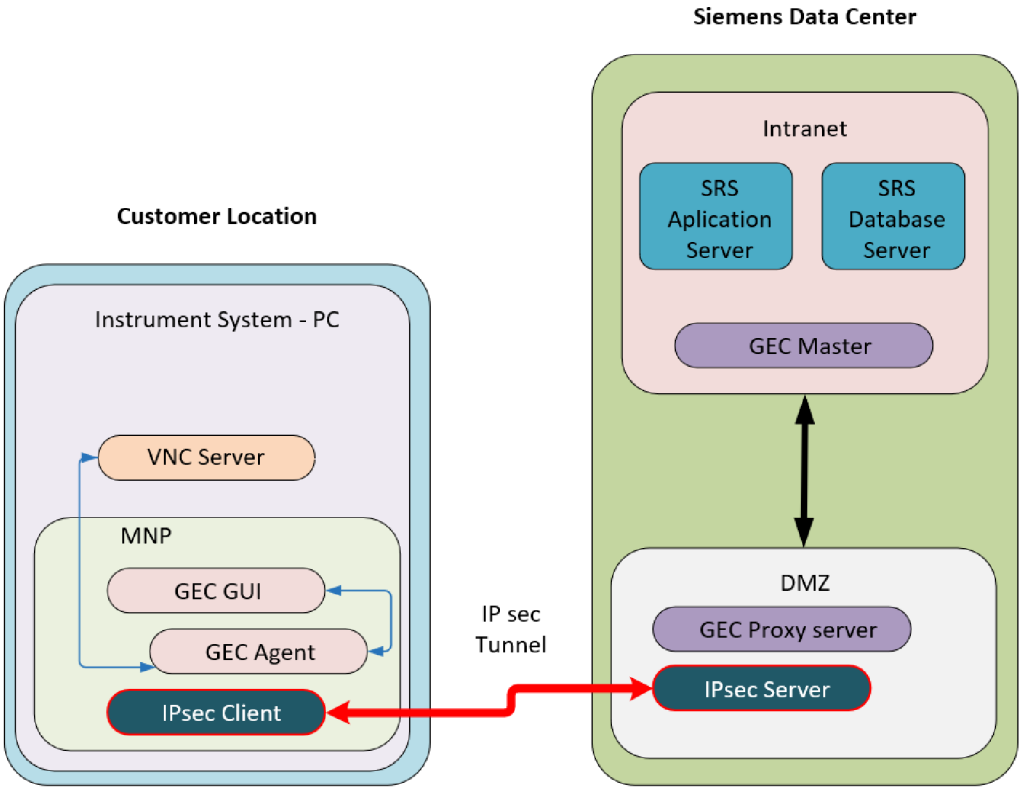
Tabulka 8 Druhy VPN.

Typ	IPSec	Platforma	opensource
LiberSwan	ano	Linux	ano
OpenVPN	ne	Win, Linux	ne
SoftEther	ano	Win, Linux	ano

Zdroj: vlastní zpracování

Sestavení IPSec tunelu

Aplikace IBC Agent sestavuje, na straně PC analyzátoru, chráněné připojení k SRS portálu, obrázek 15. Místo dosavadního VPN SSL tunelu bude vytvořeno připojení pomocí protokolu L2TP/IPSec. Ten pracuje na 3. síťové vrstvě a nabízí lepší parametry pro zabezpečení komunikace.



Obr. 15 Blokové schéma řešení.
Zdroj: Vlastní zpracování

Strana zákazníka

Řešení předpokládá, že jako koncové zařízení bude využit PC analyzátoru, na který se nainstalují tyto aplikace:

- **VNC server** bude použit derivát UltraVNC v nejnovější verzi 1.3.2.0
- **GEC GUI** grafické prostředí aplikace pro připojení k SRS
- **GEC agent** je klientská aplikace GEC, eviduje řídící počítač analyzátoru jako localhost zprostředkovává komunikaci s VNC Serverem
- **IPSec klient** je klientská aplikace VPN serveru

Strana SRS (VPN) serveru

- **GEC proxy server** překládá adresy připojených klientů
- **SRS application server** jedná se o SaaS aplikaci s integrovaným VNC klientem

- **SRS database server** databáze používaná SaaS aplikací SRS portálu
- **IPSec server** – sestavuje IPSec tunel

6.2 Analýza nedostatků stávajícího řešení

Během provozu dohledového centra se ale projevují i nedostatky. Nižší úroveň zabezpečení SSL. Slabé zabezpečení VNC protokolu, snadné odposlechnutí hesla při přihlašování. Dlouhá odezva VNC serveru, ta se projevuje tak, že načítání obrázku obrazovky vzdálené plochy trvá dlouho. Zatuhnutí obrazu, přerušení spojení klient – server. Náklady spojené s pořízením a provozem LCM počítače.
Komplikovaný tok dat z koncové stanice na SaaS přes gateway LCM. GEC aplikace zajišťující komunikaci se SRS serverem používá vlastní databázi. LCM zaznamenává komunikaci s SRS, ukládá přenášené logy, je dalším článkem v komunikační cestě a tím roste pravděpodobnost poruchy. Data odeslaná z SRS se vždy musí uložit nejdříve do LCM až následně jsou transportována do koncového počítače analyzátoru. Přenosy selhávají a data zůstanou v LCM, pak je nutné je vyhledat a dokončit transfer ručně. GEC aplikace také vyžaduje časté restarty, často je ve stavu, kdy je ztraceno spojení s koncovou stanicí.

6.3 Návrh systémových kroků pro jeho realizaci

V této části bude popsána instalace VPN serveru a klienta, jeho konfigurace, dále bude popsána konfigurace a nastavení VNC serveru a klienta. V další kapitole bude následovat ověření funkce.

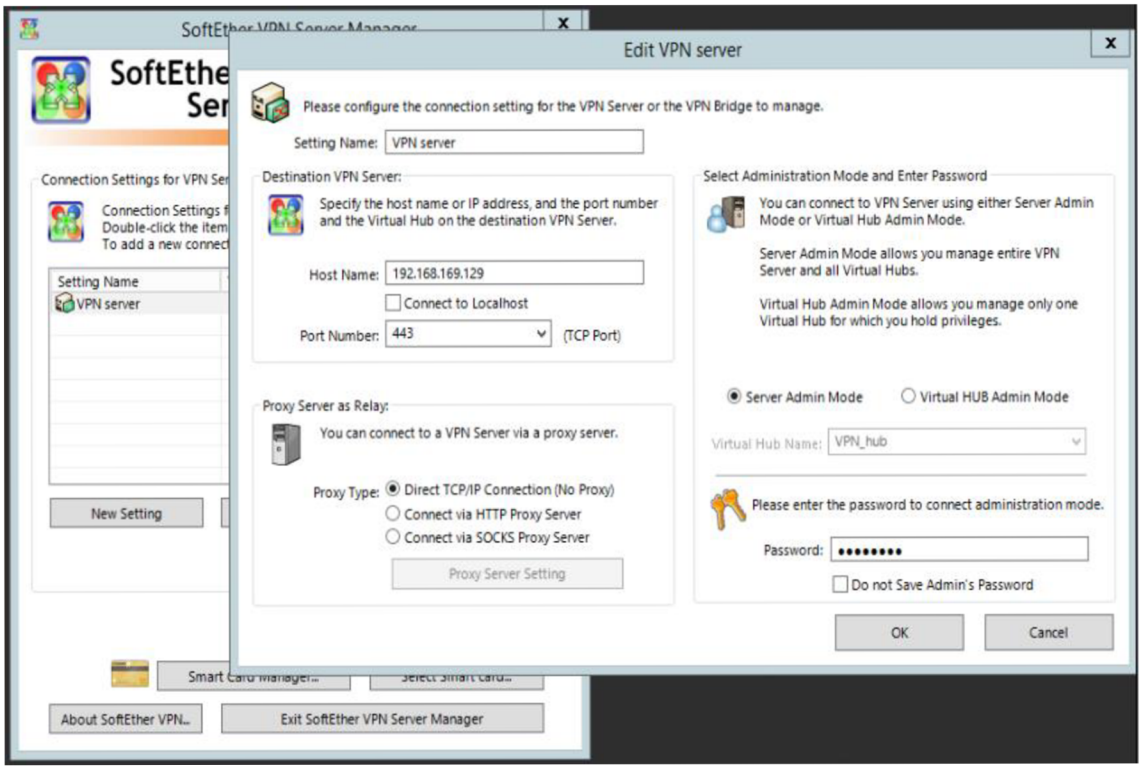
6.3.1 Instalace a konfigurace VPN

Instalace VPN serveru

Pro instalaci VPN serveru je třeba stáhnout instalační balíček z internetové stránky https://www.softether.org/5-download.
Vlastní instalaci spustíme dvojklikem na soubor *softether-vpnserver_vpnbridge-v4.38-9760-rtm-2021.08.17-windows-x86_x64-intel.exe*

Vytvoření VPN serveru

Nainstalovaný VPN server spustíme pomocí zástupce *SoftEther VPN Server Manager.* Na úvodní obrazovce zvolíme *New Settings* a vytvoříme nový server. Zvolíme jméno a IP adresu serveru, zvolíme TCP komunikaci a port 443, obrázek 16.



Obr. 16 Konfigurace VPN serveru.
Zdroj: Vlastní zpracování

Konfigurace VPN serveru

V záložce IPSec / L2TP povolíme funkci *L2TP over IPSec* a definujeme předsdílený klíč, který bude použit při sestavování tunelu, obrázek 17.

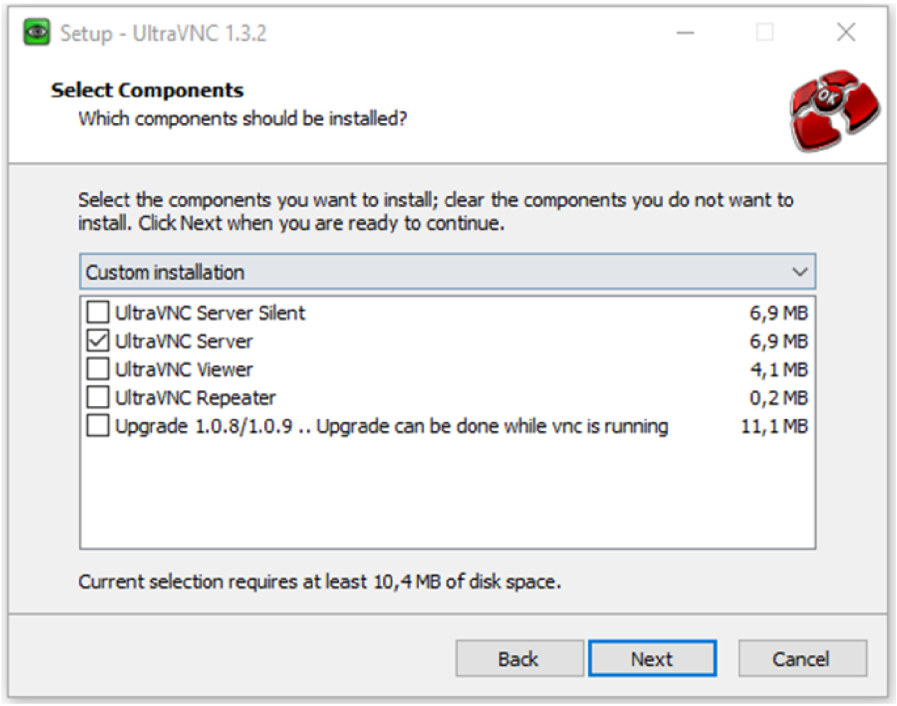
Obr. 17 VPN server – IPSec parametry.
Zdroj: Vlastní zpracování

6.3.2 Instalace a konfigurace VNC

Instalace VNC serveru

Následující postup popisuje instalaci do řídícího PC analyzátoru na platformě Windows.

- Nainstalujeme balíček MNP dodaný firmou Siemens z CD-ROM, případně USB. Současně se při instalaci automaticky nainstalují a zaregistrují služby GEC GUI, GEC agent a IBC agent.
- Nainstalujeme VNC server ze souboru UltraVNC_1_3_2_X64_Setup.exe, zvolíme

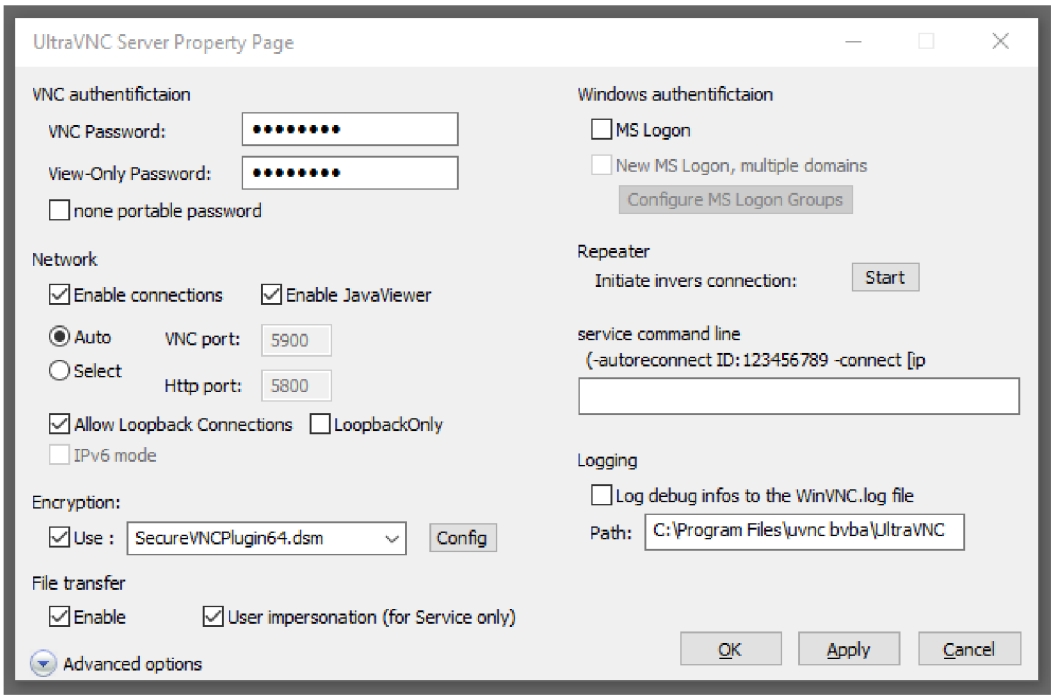


Obr. 18 Instalace VNC serveru.
Zdroj: Vlastní zpracování

Konfigurace VNC serveru

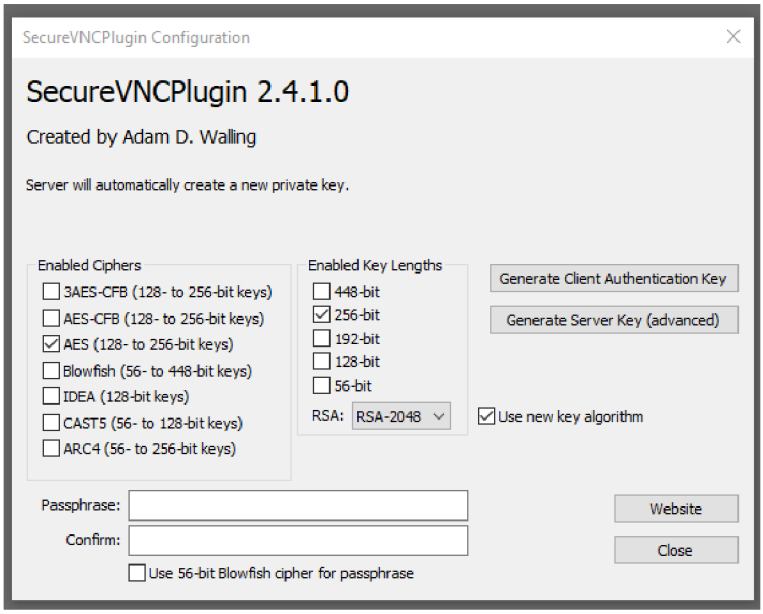
Pravím tlačítkem na ikoně VNC serveru zvolíme *Admin properties* objeví se okno na obrázku 19 a zvolíme

- V sekci VNC autentification definujeme heslo
- V sekci Network vybereme *Enable connection* a *JavaViewer*, číslo portu 5900 (Auto)
- V sekci File transfer zvolíme *Enable* nastavíme parametr *FTUserImpersonation=0* tím bude mít uživatel administrátorské oprávnění a uvidí i namapované disky



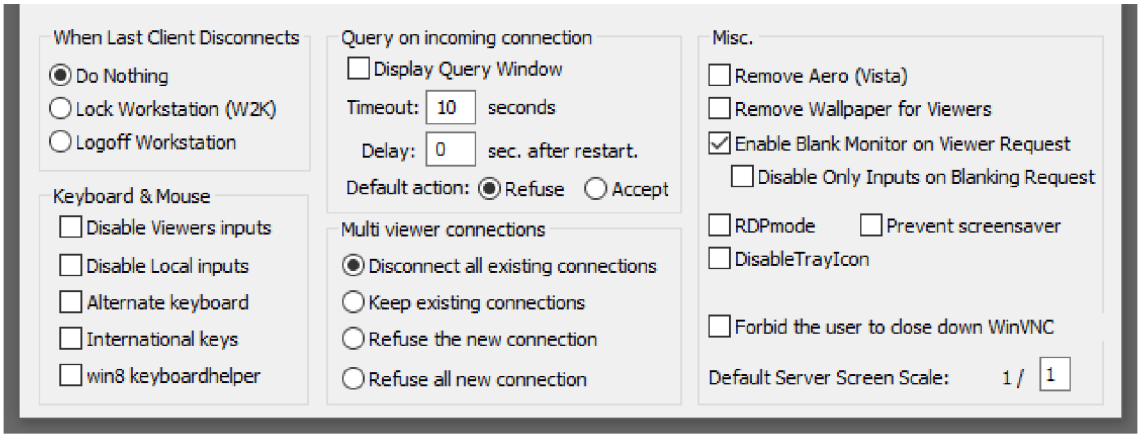
Obr. 19 Nastavení VNC serveru.
Zdroj: Vlastní zpracování

V sekci Encryption zvolíme *Use a SecureVNCPlugin64.dms* a kliknutím přejdeme do Config. Zvolíme variantu kódovaní a vepíšeme heslo pro přihlášení do pole Passphrase. Plugin zajistí šifrovaní hesla v průběhu navazování spojení mezi klientem a serverem, obrázek 20.



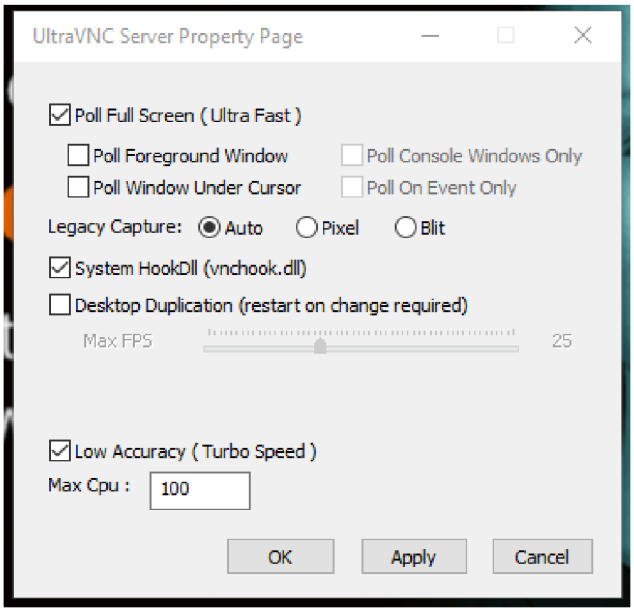
Obr. 20 Nastavení šifrování VNC serveru.
Zdroj: Vlastní zpracování

V rozšířené nabídce Advance option nastavíme *Do nothing*, která zajistí, aby se stanice neodhlašovala z Windows účtu po ukončení relace vzdálené správy. V sekci Query pak zvolíme volbu *Refuse,* ta způsobí automatické ukončení relace po uplynutí časového limitu při přihlašování, obrázek 21.



Obr. 21 Rozšířené nastavení VNC serveru.
Zdroj: Vlastní zpracování

Pravým tlačítkem myši nad ikonou VNC serveru vyvoláme nabídku a vybereme Prosperities. Otevře se okně s nastavením grafiky, zde vybereme *Poll screen* a aktivujeme *Hook driver*. Díky použití služby *Hook* je možné využít funkcí ovladače grafiky a zrychlit vykreslování bitmap, obrázek 22.



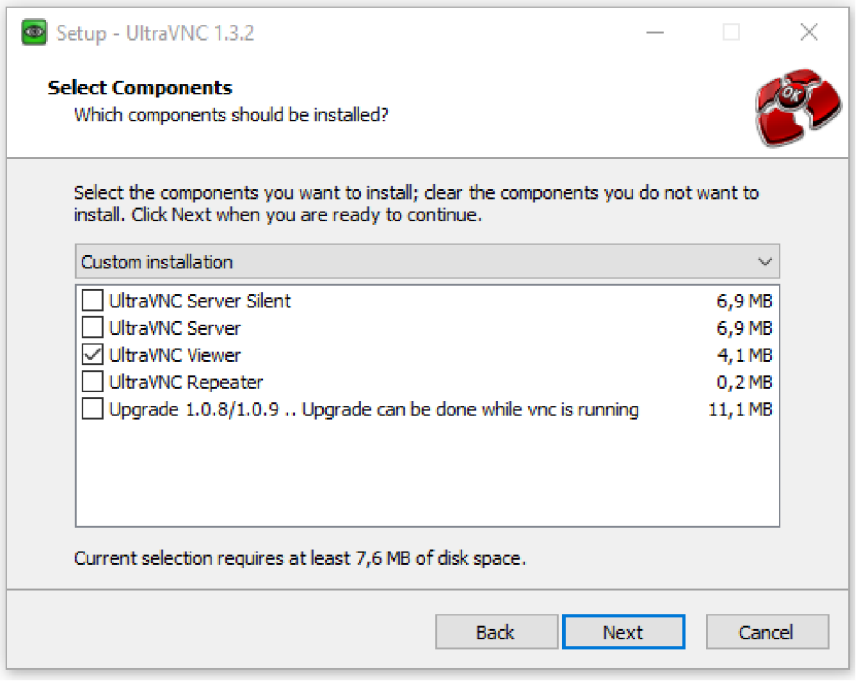
Obr. 22 Obrazovka nastavení grafiky.
Zdroj: Vlastní zpracování

Nastavení VNC serveru je definované souborem *ultravnc.ini* viz Příloha č.1

Instalace VNC klienta

Následující postup a obrázek 23 popisují instalaci VNC klienta do PC představujícího stranu Siemens serveru

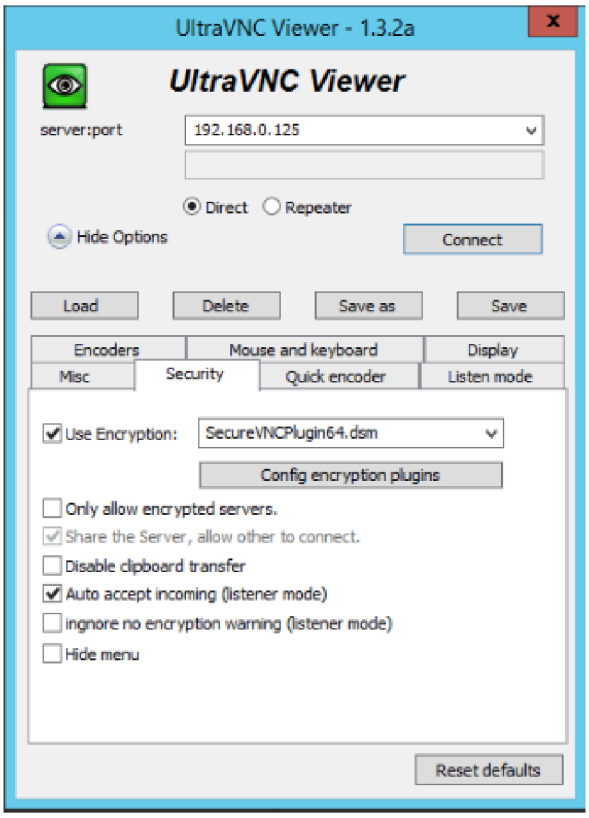
- Rozklikneme soubor UltraVNC_1_3_2_X64_Setup.exe
- Zaškrtneme VNC Viewer v kartě Select Components, tím nainstalujeme VNC klienta
- Zástupce VNC Viewer je umístěn na ploše



Obr. 23 Instalace VNC klienta.
Zdroj: Vlastní zpracování

Konfigurace VNC klienta

Spustíme zástupce aplikace VNC Viewer na ploše. Nastavíme dle obrázku 24 v záložce *Security* použití šifrovacího skriptu *SecureVNCPlugin64.dms*.

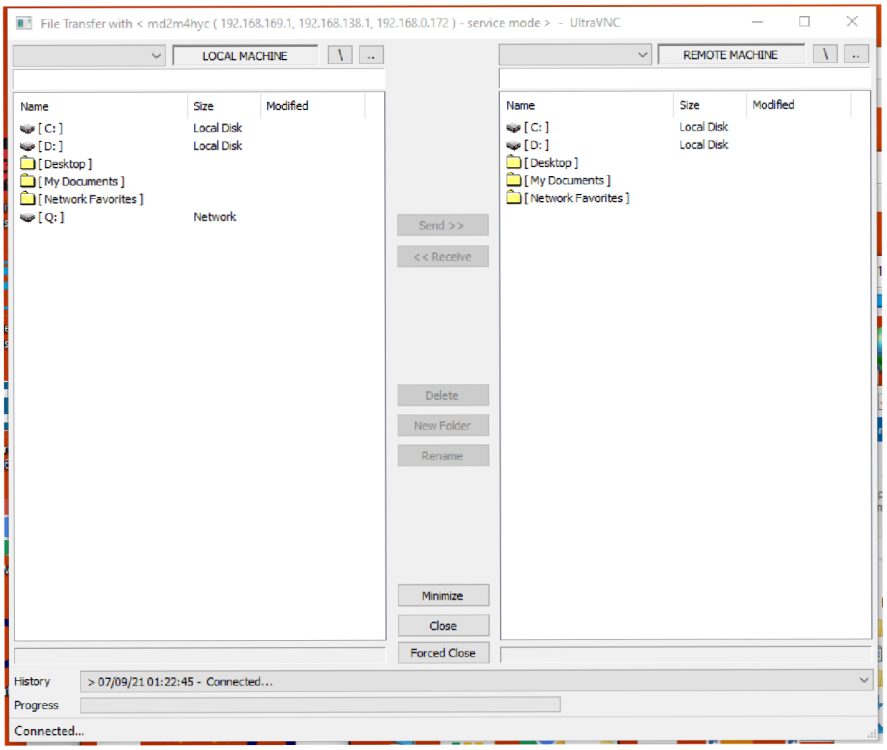


Obr. 24 Konfigurace VNC klienta.
Zdroj: Vlastní zpracování

6.3.3 Přenos souborů

Pro povolení přenosu souborů zapneme tuto funkcionalitu v sekci *File transfer* konfigurační aplikace, případně přímo v konfiguračním souboru *vnc.props.ini*, nastavením parametru *FileTransferEnabled* na hodnotu 1, viz příloha 1.

Vlastní přenos souborů je umožněn přesouváním mezi diskovým prostorem klienta a serveru v okně File transfer, obrázek 25.



Obr. 25 Okno přenosu souborů.
Zdroj: Vlastní zpracování

Pro zautomatizování přenosu dat bude vhodné nadefinovat skripty pro kopírování a shromažďování logů v koncovém PC. Definování a nastavení scheduleru ve Windows pro spouštění skriptů.

6.4 Ověření funkce

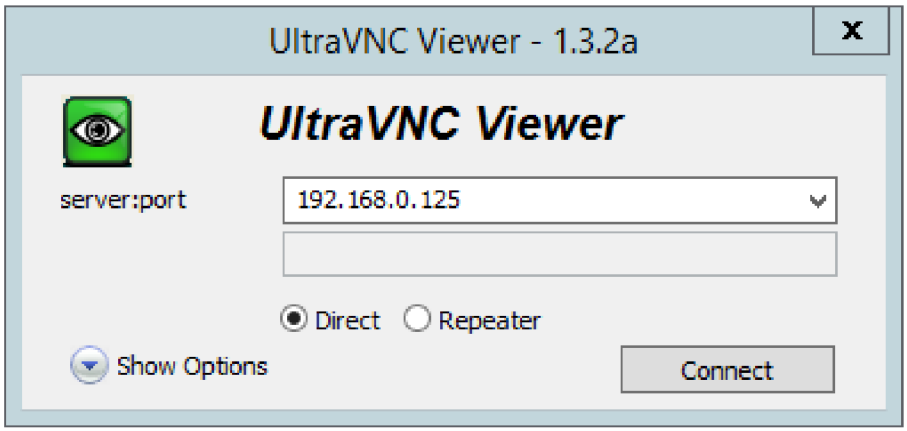
Pro účely ověření funkčnosti řešení budou použity dva virtuální počítače

- virtuální server, Windows server 2012, IP adresa 192.168.169.129 bude představovat stranu Siemens serveru
- virtuální server, Windows 10, IP adresa 192.168.0.125 bude reprezentovat stranu koncového řídícího PC u zákazníka

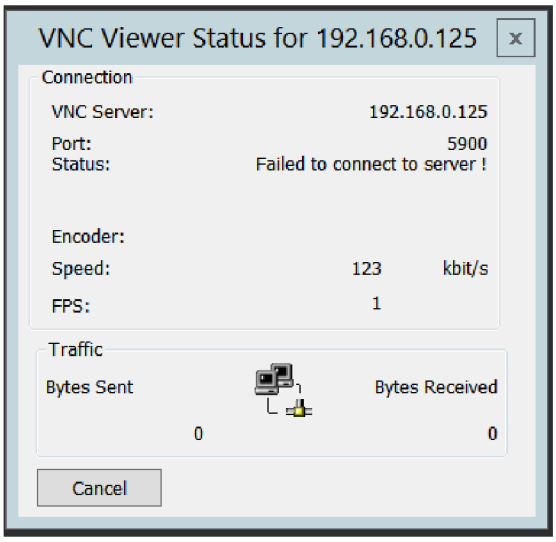
Budeme ověřovat sestavení IPSec tunelu, metodou předsdíleného klíče. Existenci tunelu dokážeme pomocí testu spojení na pomocí protokolu VNC. Na začátku ověříme že IPSec neexistuje tak, že VNC spojení není možné. Vytvoříme IPSec tunel a v dalším kroku pak ověříme vlastní VNC spojení, to zároveň bude sloužit jako ověření existence IPSec tunelu jenž byl vytvořen v předchozím kroku. Nakonec otestujeme rychlost spojení.

Ověření nedostupnosti

Spustíme VNC Viewer na straně VPN serveru a vepíšeme IP adresu VNC serveru, obrázek 26. Při pokusu o spojení dojde k selhání na obrázku 27. Proto můžeme konstatovat, že spojení mezi oběma koncovými body neexistuje.



Obr. 26 Pokus o VNC spojení.
Zdroj: Vlastní zpracování



Obr. 27 Negativní výsledek při pokusu o VNC spojení.
Zdroj: Vlastní zpracování

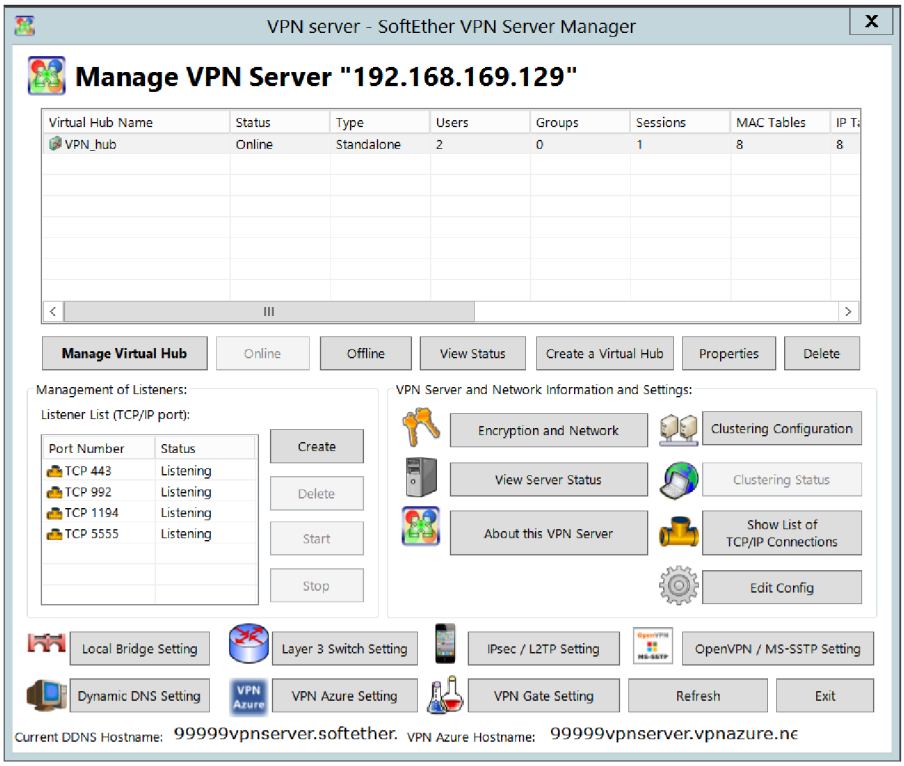
Vytvoření IPSec tunelu

Postupujeme tak, že nejdříve aktivujeme VPN server a poté spouštíme VPN klienta

Spuštění VPN serveru

Na počítači s IP adresou 192.168.169.129, který představuje stranu serveru spustíme aplikaci SoftEther VPN Server Managera, obrázek 28. Na hlavní obrazovce najedeme nad jméno serveru a pomocí volby **Connect** aktivujeme VPN server. Status VPN serveru se změní na Online, došlo tedy k jeho spuštění. Nyní budeme pokračovat spuštěním VPN klienta, obrázek 29.

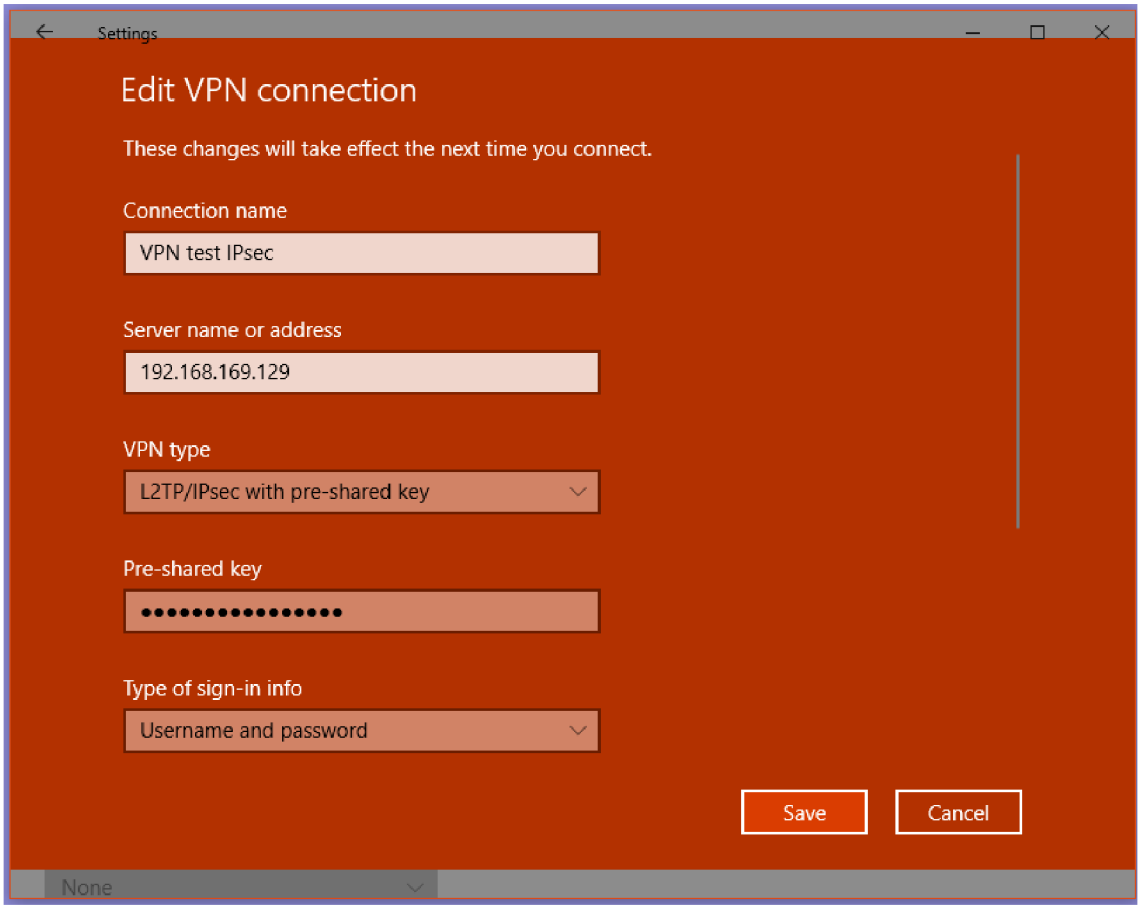
Obr. 28 Start VPN serveru.
Zdroj: Vlastní zpracování



Obr. 29 Server VPN je online.
Zdroj: Vlastní zpracování

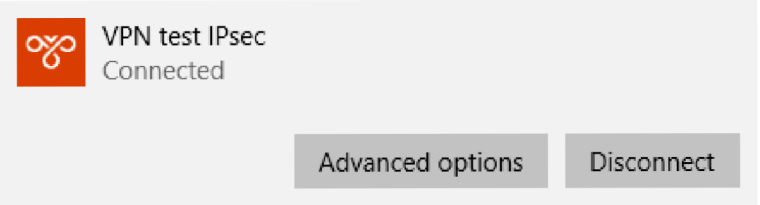
Spuštění VPN klienta

Na počítači s IP adresou 192.168.0.125, který reprezentuje VPN klienta, vytvoříme nové IPSec připojení ve Windows v nabídce Nastavení>> Síť>> VPN. Zadáme IP adresu VPN serveru a předsdílený klíč, obrázek 30.



Obr. 30 VNP klient – IPSec parametry.
Zdroj: Vlastní zpracování

Proběhlo vzájemné ověření klíče a obě stanice se spojili chráněným IPSec tunelem, viz obrázek 31.



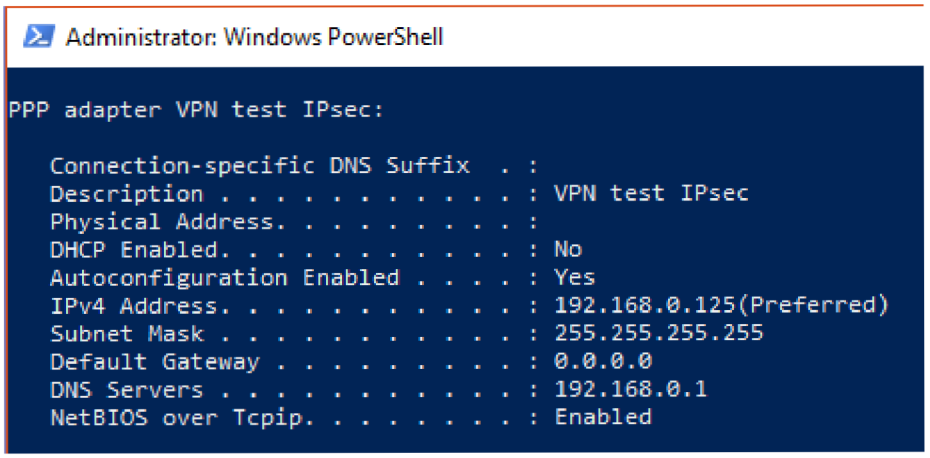
Obr. 31 Sestavené spojení IPSec na straně klienta.
Zdroj: Vlastní zpracování

Ověření VPN tunelu

V logu VPN serveru v Příloze č.2, najdeme záznam o vytvoření L2TP PPP relace a přidělení následujících parametrů klientovi:

- IP adresa: 192.168.0.125
- Maska podsítě: 255.255.255.0
- Výchozí brána: 192.168.0.1

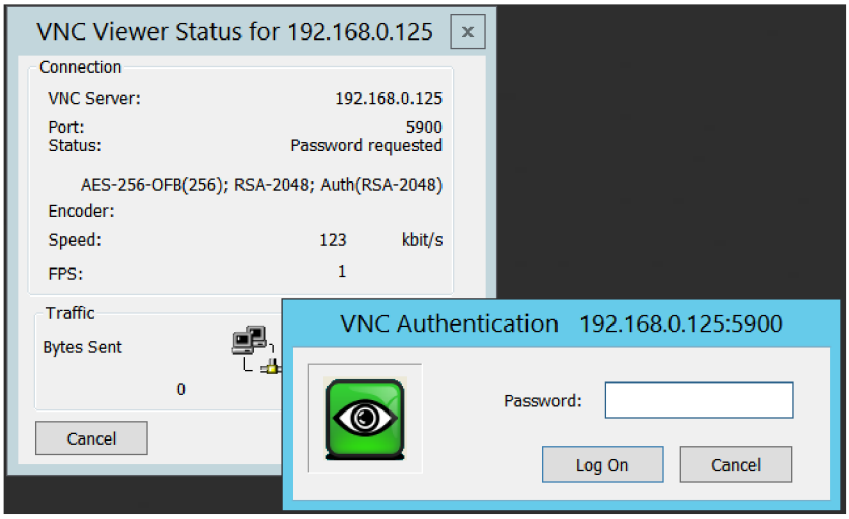
Příkazem *ipconfig /all,* v konzolovém okně aplikace Windows PowerShell na obrázku 32, ověříme stav síťového rozhraní, jež bylo vytvořeno.



Obr. 32 Ověření spojení IPSec klienta.
Zdroj: Vlastní zpracování

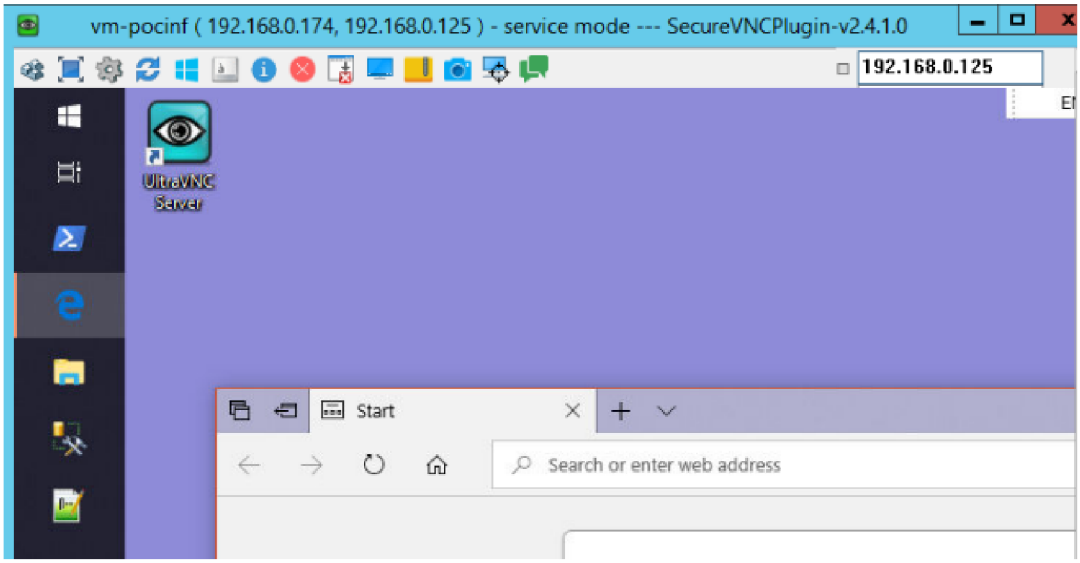
Ověření bezpečného přihlášení do VNC

Na straně VPN klienta spustíme VNC server pomocí souboru *C:\Program Files\uvnc bvba\UltraVNC\winvnc.exe*. Zkopírujeme vygenerovaný klíč z VNC serveru do adresáře VNC klienta. IP adresu 192.168.0.125 testovaného VNC serveru vepíšeme do pole server a stiskem tlačítka Connect spustíme připojování.



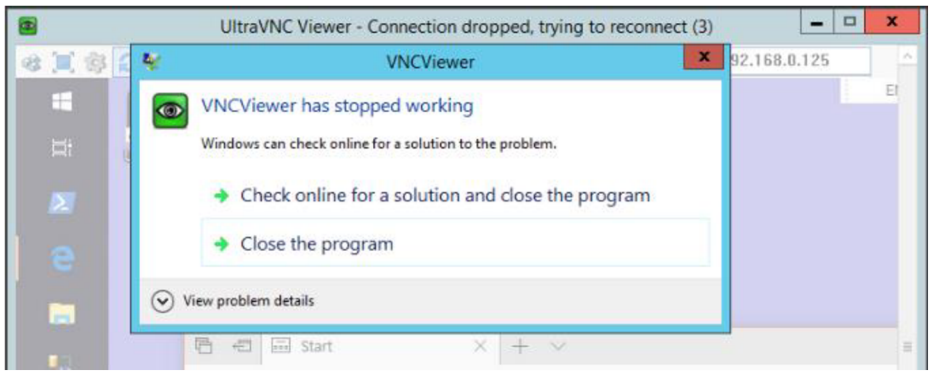
Obr. 33 Přihlášení VNC klienta.
Zdroj: Vlastní zpracování

Následuje ověření heslem, které jsme definovali na VNC serveru. Po zadání správného hesla na obrázku 33 a potvrzením klávesou Log On je spojení navázáno a oznámeno hláškou Connected. Otevře se nové okno s obrazovkou vzdáleného počítače, viz obrázek 34.



Obr. 34 Sestavené VNC spojení.
Zdroj: Vlastní zpracování

Nyní ověříme, zda je VNC komunikace vedena pouze v IPSec tunelu. Ukončíme VPN IPSec spojení pomocí tlačítka Disconnect v aplikaci SoftEther a můžeme na obrázku 35 sledovat, že se zavřelo okno vzdálené obrazovky. Okno s chybovou hláškou nám oznamuje, že došlo k rozpadu VNC spojení. Tímto jsme ověřili že vzdálené spojení na portu 5900 je realizováno pouze pokud existuje IPSec tunel.

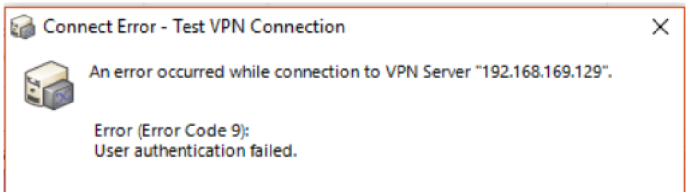


Obr. 35 Rozpad VNC komunikace.
Zdroj: Vlastní zpracování

Pro ověření dalších funkcí nainstalujeme na stranu VPN klienta program SoftEther Client ze souboru *softether-vpnclient-v4.34-9745-rtm-2020.04.05-windows-x86_x64-intel.exe*

Ověření bezpečnosti

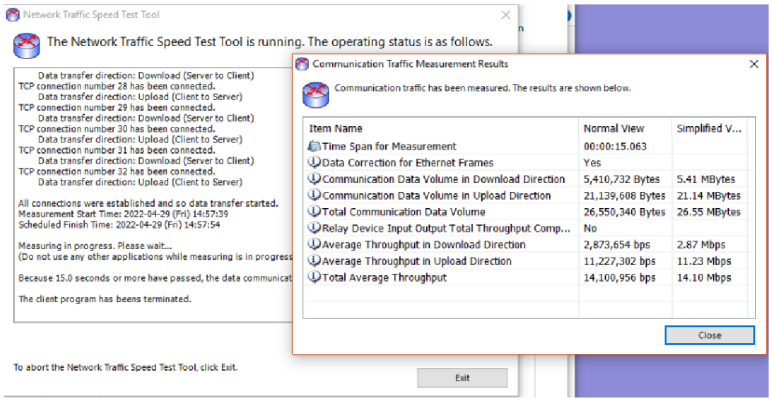
Při navazování spojení ověřuje server a klient certifikát, proto provedeme test, při kterém ověříme tuto funkci. Nejprve ve VPN serveru SoftEther v nastavení uživatele vygenerujeme certifikát. Ten přeneseme do VPN klienta a jako způsob autentizace vybereme *Client certificate.* Při použití tohoto certifikátu dojde k bezproblémovému spojení klienta se serverem. Nyní nahrajeme certifikát jiného uživatele, než který byl vygenerován na VPN serveru a při pokusu o spojení z VPN klienta se objeví chybová hláška autentizace, obrázek 36 a tak není možné sestavit IPSec.



Obr. 36 Výsledek použití špatného certifikátu.
Zdroj: Vlastní zpracování

Ověření rychlosti

Pomocí nástroje Network Traffic Speed Test na obrázku 37, provedeme test rychlosti obousměrného přenosu dat



Obr. 37 Test rychlosti.
Zdroj: Vlastní zpracování

6.5 Sada doporučení pro zajištění bezpečnosti

Vzhledem ke skutečnosti, že je bezpečná komunikace a zabezpečení sítě důležitým aspektem pro organizace zaštiťující zdravotní péči i firmu Siemens, je zde navrženo několik doporučení.

Řídící PC analyzátoru – koncová stanice

Operační systém

Instalace operačního systém Windows 10 včetně dalších aplikací potřebných pro fungování řídícího PC, bude provedena pomocí image disku dodaného fy Siemens. Nastavení ochrany BIOSu heslem.

Antivirový software

Ochranu proti virům, skenování disku zajišťuje Symantec software. Tento software také monitoruje bezpečnostní rizika jako je adware a spyware. Antivirus software je používá heuristickou analýzu k identifikaci nových nebo neznámých virů. Dále použití McAfee softwaru na principu metody whitelisting, která udržuje seznam aktuálně nainstalovaných aplikací a zabrání instalaci či spuštění jiných softwarů.

Firewall

Nasazení pravidel firewallu. Nastavení výjimek pouze pro GEC aplikaci a jí používané porty. Vypnutí ICMP echo dotazů, systém nebude reagovat na ping. HTTP komunikace bude omezená pouze pro místní podsítě. Port pro HTTPS komunikaci je povolen pro všechny sítě.

VNC server

Použití šifrovací pluginu pro přihlášení. Nastavení časového limitu pro automatické odhlášení, ukončení relace a odpojení po nečinnosti. Natavení automatického odmítnutí připojení klienta po uplynutí časového limitu.

Uživatelé koncové stanice

Vytvoření po jednom uživatelském účtu v operačním systému Windows ve skupinách:

- **Users**, účet v této skupině bude určen pro obsluhu, tzn. laboratorní zaměstnance. Tento účet nemá žádná administrativní oprávnění, nemá oprávnění k systémovým změnám a může spouštět většinu aplikací.
- **Administrators**, účet v této skupině bude určen pro uživatele Siemens podpory. Účet bude mít plná administrátorská oprávnění. Aby se předešlo neautorizovanému přístupu k počítači, pokud zůstane bez dozoru je třeba nastavit automatické odhlášení standardně na 15 minut.

Ověření Siemens uživatele

Na straně SRS serveru (SaaS aplikace) realizovat dvoufázové ověření při přihlášení do aplikace. Registrovanému uživateli SRS portálu bude při přihlášení zaslán kód na mobilní telefon. Ten zadá při přihlašování do aplikace. Po výběru požadovaného analyzátoru, bude volbou **Remote control** spuštěn klient UltraVNC.

6.6 Vyhodnocení výsledků

Silné stránky

Použitím bezpečnostního pluginu při logování uživatele dochází k zvýšení ochrany před odposlechem hesla. Realizováním spojení pomocí IPSec se šifrováním a ověřením klíčů pomocí IKEv2 je realizováno. Klient a server se vzájemně ověřují. Ověřování pomocí digitálních certifikátu je velice silnou metodou ověřování.

Zrychlení a zjednodušení komunikace je dosaženo vyřazením prvku LCM gateway. IPSec tunel je sestaven ze SRS portálu přímo na síťové rozhraní koncového počítače analyzátoru. V tomto případě je aktivita uživatele SRS portálu v zákazníkově síti velice omezena. Jde tak o bezpečnější řešení přístupu do zákazníkovy sítě. Ke zvýšení přenosové rychlosti také přispívá vyřazení aplikace i2i agent, která způsobovala mimo jiné přetěžování sítě broadcast dotazy, a také absence aplikace i2i server. Ke zrychlení přenosu VNC přispívá admin nastavení zapnutím funkce Video Hook driveru.

Přenos souborů nově je nastavena funkce přenosu souborů.

Finanční úspora prostředků v hodnotě cca 1500 euro, představuje nezanedbatelnou částku za hardware a za licence softwaru operačního systému LCM.

Potencionální problémy

Pravděpodobným přetrvávajícím problémem může být rychlost odezvy SaaS aplikace SRS portálu pro Siemens uživatele. To je způsobeno faktem, že aplikace SRS portálu je spuštěna na serverech v DMZ zóně USA. Vhodné by bylo přesunout/zřídit server geograficky blíže uživatelům v Evropě.

7 Závěr

Cílem této práce bylo ukázat protokol VNC a jeho použití pro vzdálenou správu. Popsáno bylo i jeho současné využití při správě analyzátorů – specializovaných zdravotnických zařízení firmy Siemens k dálkové správě.

V teoretické části práce byly představeny obecné principy jednotlivých protokolů vzdálené správy, typy klientů a způsob komunikace. Bylo představen systém VNC a jeho využití včetně protokolu RFB. Dále byl popsán způsob komunikace a zajištění bezpečnosti dat při přenosu přes veřejnou síť. Na bezpečnost je obecně kladen veliký důraz, a proto byly popsány způsoby zabezpečení VPN spojení a typy protokolů tunelování. V kapitole 5 byl prezentován aktuální model vzdálené správy zdravotnických zařízení. Byly analyzovány výhody a nevýhody stávajícího řešení.

V praktické části byl navržen přepracovaný model propojení pro Siemens dohledového centra a koncové stanice – řídícího počítače analyzátoru. V kapitole 6 je navrženo využití novější verze VNC jako hlavního systému pro vzdálenou komunikaci. Zvoleno bylo použití bezpečnějšího typu tunelování pomocí IPSec/L2PT. Bylo provedeno testování a ověření funkce návrhu řešení. Z důvodu nemožnosti ovlivnit nastavení na Siemens backend straně byla provedena simulace připojení pomocí volně dostupného řešení SoftEther VPN.

Byl navržen i soubor systémových kroků a sada doporučení pro zajištění bezpečnosti komunikace jak na straně Siemens, tak na koncové stanici.

Výsledkem Bakalářské práce je návrh inovace současného řešení na základě zkušeností z realizovaných projektů vzdálené správy. Ten by mohl být inspirací pro další zlepšování a vývoj systému vzdálené správy firmy Siemens.

8 Seznam použité literatury

[1] Document Library – Siemens Healthineers. Document Library – Siemens Healthineers [online]. Dostupné z: https://doclib.siemens-healthineers.com/home

[2] RICHARDSON, T., Q. STAFFORD-FRASER, K.R. WOOD a. HOPPER. Virtual network computing. IEEE Internet Computing [online]. 1998 [cit. 2021-8-9]. ISSN 10897801. Dostupné z: doi:10.1109/4236.656066

[3] What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

[4] RICHARDSON, T. and J. Levine. The Remote Framebuffer Protocol RFC 6143. RealVNC Ltd. [online]. March 2011. [cit. 11.08.2021]. Dostupné z: https://www.rfc-editor.org/info/rfc6143. DOI 10.17487/RFC6143

[5] Wikipedia contributors. "Multitier Architecture." *Wikipedia, The Free Encyclopedia* [online]. Dostupné z: https://en.wikipedia.org/wiki/Multitier_architecture

[6] SOJKA, Martin. Optimalizace síťového provozu na mobilním zařízení pomocí Cloudové služby. DSpace VŠB-TUO [online]. 2017 [cit. 11.08.2021]. Dostupné z: https://dspace.vsb.cz/bitstream/handle/10084/119054/SOJ0016_FEI_N2647_2612T059_2017.pdf?sequence=1

[7] BARTOŇ, Jan. Komfortní správa počítačové sítě. Univerzita Tomáše Bati ve Zlíně. [online]. 2011 [cit. 2021-08-11]. Dostupné z: https://theses.cz/id/5277qn/

[8] ZUKAL, Martin. Sdílení plochy při video a audiokonferencích. Vysoké učení technické v Brně [online]. 2010 [cit. 11.08.2021]. Dostupné z: https://www.vutbr.cz/www_base/zav_prace_soubor_verejne.php?file_id=26748

[9] UltraVNC: UltraVNC remote access tools. UltraVNC Team [Online]. 2020 [cit. 15.07.2021.]. Dostupné z: https://www.uvnc.com

[10] [MS-SSTP]: Overview. Microsoft Docs. [online]. 2021 [cit. 13.07.2021]. Dostupné z: https://docs.microsoft.com/cs-cz/openspecs/windows_protocols/ms-sstp/70adc1df-c4fe-4b02-8872-f1d8b9ad806a

[11] PUŽMANOVÁ, Rita. Bezpečnost ve VPN: IPSec versus SSL. DSL.cz [online]. 2006 [cit. 19.07.2021]. Dostupné z: https://www.dsl.cz/clanky/515-bezpecnost-ve-vpn-IPSec-versus-ssl

[12] SMITH, Roderick W. Linux ve světě Windows: průvodce administrátora heterogenních sítí. Praha: Grada, 2006. 446 stran. ISBN 8024714701.

[13] PUŽMANOVÁ, Rita. TCP/IP v kostce. České Budějovice: Kopp, 2004. 611 stran. ISBN 8072322362.

[14] VAŠEK, Jiří. VNC a Vzdálená plocha – kouzlo vzdáleného přístupu. PCTuning [online]. 2009 [cit. 06.08.2021]. Dostupné z: https://pctuning.cz/article/vnc-a-vzdalena-plocha-kouzlo-vzdaleneho-pristupu?chapter=5&scrollTo=article-header

[15] KREJČÍ, Ondřej. Analýza protokolů pro vzdálenou správu. Digitální knihovna UPa [online]. 2014 [cit. 10.08.2021]. Dostupné z: https://dk.upce.cz/bitstream/handle/10195/56020/KrejciO_AnalyzaProtokolu_SN_2014.pdf?sequence=2&isAllowed=y

[16] ROEBUCK, Kevin. Virtual Network Computing (VNC): High-impact Strategies – What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors. Lightning Source Incorporated. 2011. 60 stran. ISBN 1743047398, 9781743047392.

[17] Bc. Filip NAVRÁTIL: Bezpečné připojení zaměstnanců společnosti Povodí Labe, státní podnik, do podnikové sítě,Fakulta aplikované informatiky - Univerzita Tomáše Bati ve Zlíně (2011)

[18] Radek Nezbeda: Virtualní privátní sítě, Provozně ekonomická fakulta – Česká zemědělská univerzita v Praze (2012)

[19] Petr Herdin: Systémy pro anonymní a šifrované přístupy k internetu, Provozně ekonomická fakulta – Česká zemědělská univerzita v Praze (2014)

[20] PAVELEK, Martin. Webová aplikace pro zpracování inventarizačních dat. ČVUT DSpace [online]. 2016 [cit. 12.08.2021]. Dostupné z: https://dspace.cvut.cz/bitstream/handle/10467/66209/F8-BP-2016-Pavelek-Martin-thesis.pdf?sequence=1&isAllowed=y

[21] What Is VPN? Microsoft Docs. [online]. 2012 [cit. 13.07.2021]. Dostupné z: https://technet.microsoft.com/en-us/library/windows-server-2008-R2-and-2008/cc731954(v=ws.10)

[22] BÁRTA, Martin. Bezpečnostní mechanismy protokolů pro zajištěnou komunikaci v síťových modelech [online]. Ústí nad Labem, 2014 [cit. 2022-06-20]. Dostupné z: https://theses.cz/id/zhd3wi

[23] [MS-SSTP]: Overview. Microsoft Docs. [online]. 2021 [cit. 13.07.2021]. Dostupné z: https://technet.microsoft.com/en-us/library/openspecs/windows_protocols/ms-sstp/70adc1df-c4fe-4b02-8872-f1d8b9ad806a

[24] WINTER, Daniel. *Vliv zabezpečení VPN sítí na výkonnost systému*. 2014. Bakalářská práce. Univerzita Karlova, Matematicko-fyzikální fakulta, Katedra softwarového inženýrství. Vedoucí práce Peterka, Jiří.

9 Přílohy

1) Výpis konfiguračního souboru ultravnc.ini
2) Výpis z log souboru VPN serveru SoftEther

Výpis konfiguračního souboru *ultravnc.ini*:

```
[ultravnc]
passwd=952342424890EC8E8E                    / heslo
passwd2=952342424890EC8E8E                   / heslo
[admin]
DSMPluginConfig=SecureVNC;0;0x00104001;
UseRegistry=0
SendExtraMouse=1
Secure=0
MSLogonRequired=0
NewMSLogon=0
DebugMode=0
Avilog=0
path=C:\Program Files\uvnc bvba\UltraVNC
accept_reject_mesg=          / volitelný text zobrazený v oznamovacím okně
DebugLevel=0
DisableTrayIcon=0
rdpmode=1
noscreensaver=0
LoopbackOnly=0
UseDSMPlugin=0                               / použitý šifrovací plugin
AllowLoopback=1
AuthRequired=1                               / vyžadována autentifikace
ConnectPriority=0
DSMPlugin=
AuthHosts=                       / povolení, zakázání IP adresy hosta
AllowShutdown=1
AllowProperties=1
AllowInjection=0
AllowEditClients=1
FileTransferEnabled=1                        / povolen přenos souborů
```

```
FTUserImpersonation=0                    / uživatel jako admin
BlankMonitorEnabled=1
BlankInputsOnly=0
DefaultScale=1
primary=1
secondary=0
SocketConnect=1
HTTPConnect=1
AutoPortSelect=1
PortNumber=5900                          / použitý port pro příjem
HTTPPortNumber=5800                      / port pro webový server
IdleTimeout=0
IdleInputTimeout=0
RemoveWallpaper=0
RemoveAero=0
QuerySetting=2              / odmítnutí přihlášení IP hosta z Authhosts
QueryTimeout=10             / časový interval pro povolení přihlášení hosta
QueryDisableTime=0
QueryAccept=0               / povolení oznamovacího okna připojení hosta
QueryIfNoLogon=1
InputsEnabled=1
LockSetting=0
LocalInputsDisabled=0
EnableJapInput=0
EnableUnicodeInput=0
EnableWin8Helper=0
kickrdp=0
clearconsole=0
[poll]
TurboMode=1
PollUnderCursor=0
PollForeground=0
```

```
PollFullScreen=1
OnlyPollConsole=0
OnlyPollOnEvent=0
MaxCpu2=100                    / povolení použít 100 % CPU
MaxFPS=25
EnableDriver=0
EnableHook=1                   / povolení hardwarové akcelerace
EnableVirtual=0
SingleWindow=0
```

Výpis z log souboru VPN serveru SoftEther:

08:44:40.623 IPsec Client 6 (192.168.0.101:500 -> 192.168.169.129:500): A new IPsec client is created.
08:44:40.624 IPsec IKE Session (IKE SA) 6 (Client: 6) (192.168.0.101:500 -> 192.168.169.129:500): A new IKE SA (Main Mode) is created. Initiator Cookie: 0x2D3BDF11501D439, Responder Cookie: 0x7C4775C730D9303B, DH Group: MODP 2048 (Group 14), Hash Algorithm: SHA-1, Cipher Algorithm: AES-CBC, Cipher Key Size: 256 bits, Lifetime: 4294967295 Kbytes or 28800 seconds
08:44:40.760 IPsec Client 6 (192.168.0.101:4500 -> 192.168.169.129:4500): The port number information of this client is updated.
2022-04-24 08:44:40.760 IPsec Client 6 (192.168.0.101:4500 -> 192.168.169.129:4500):
2022-04-24 08:44:40.760 IPsec IKE Session (IKE SA) 6 (Client: 6) (192.168.0.101:4500 -> 192.168.169.129:4500): This IKE SA is established between the server and the client.
2022-04-24 08:44:40.812 IPsec IKE Session (IKE SA) 6 (Client: 6) (192.168.0.101:4500 -> 192.168.169.129:4500): The client initiates a QuickMode negotiation.
2022-04-24 08:44:40.812 IPsec ESP Session (IPsec SA) 6 (Client: 6) (192.168.0.101:4500 -> 192.168.169.129:4500): A new IPsec SA (Direction: Client -> Server) is created. SPI: 0x701A3CFB, DH Group: (null), Hash Algorithm: SHA-1, Cipher Algorithm: AES-CBC, Cipher Key Size: 256 bits, Lifetime: 250000 Kbytes or 3600 seconds
2022-04-24 08:44:40.812 IPsec ESP Session (IPsec SA) 6 (Client: 6) (192.168.0.101:4500 -> 192.168.169.129:4500): A new IPsec SA (Direction: Server -> Client) is created. SPI: 0x58B5797A, DH Group: (null), Hash Algorithm: SHA-1, Cipher Algorithm: AES-CBC, Cipher Key Size: 256 bits, Lifetime: 250000 Kbytes or 3600 seconds
2022-04-24 08:44:40.815 IPsec ESP Session (IPsec SA) 6 (Client: 6) (192.168.0.101:4500 -> 192.168.169.129:4500): This IPsec SA is established between the server and the client.
2022-04-24 08:44:40.816 IPsec Client 6 (192.168.0.101:4500 -> 192.168.169.129:4500): The L2TP Server Module is started.
2022-04-24 08:44:41.091 L2TP PPP Session [192.168.0.101:1701]: A new PPP session (Upper protocol: L2TP) is started. IP Address of PPP Client: 192.168.0.101 (Hostname: "VM-POCinf"), Port Number of PPP Client: 1701, IP Address of PPP Server: 192.168.169.129, Port Number of PPP Server: 1701, Client Software Name: "L2TP VPN Client - Microsoft", IPv4 TCP MSS (Max Segment Size): 1314 bytes
2022-04-24 08:44:41.108 On the TCP Listener (Port 0), a Client (IP address 192.168.0.101, Host name "VM-POCinf", Port number 1701) has connected.
2022-04-24 08:44:41.108 For the client (IP address: 192.168.0.101, host name: "VM-POCinf", port number: 1701), connection "CID-3-2A92C95D5C" has been created.
2022-04-24 08:44:41.108 SSL communication for connection "CID-3-2A92C95D5C" has been started. The encryption algorithm name is "(null)".
2022-04-24 08:44:41.110 [HUB "VPN_hub"] The connection "CID-3-2A92C95D5C" (IP address: 192.168.0.101, Host name: VM-POCinf, Port number: 1701, Client name: "L2TP VPN Client - Microsoft", Version: 4.38, Build: 9760) is attempting to connect to the Virtual Hub. The auth type provided is "External server authentication" and the user name is "antos".
2022-04-24 08:44:41.111 [HUB "VPN_hub"] Connection "CID-3-2A92C95D5C": Successfully authenticated as user "antos".
2022-04-24 08:44:41.111 [HUB "VPN_hub"] Connection "CID-3-2A92C95D5C": The new session "SID-ANTOS-[L2TP]-6" has been created. (IP address: 192.168.0.101, Port number: 1701, Physical underlying protocol: "Legacy VPN - L2TP")
2022-04-24 08:44:41.111 [HUB "VPN_hub"] Session "SID-ANTOS-[L2TP]-6": The parameter has been set. Max number of TCP connections: 1, Use of encryption: Yes, Use of compression: No, Use of Half duplex communication: No, Timeout: 20 seconds.
2022-04-24 08:44:41.112 [HUB "VPN_hub"] Session "SID-ANTOS-[L2TP]-6": VPN Client details: (Client product name: "L2TP VPN Client - Microsoft", Client version: 438, Client build number: 9760, Server product name: "SoftEther VPN Server (64 bit)", Server version: 438, Server build number: 9760, Client OS name: "L2TP VPN Client - Microsoft", Client OS version: "-", Client product ID: "-", Client host name: "VM-POCinf", Client IP address: "192.168.0.101", Client port number: 1701, Server host name: "192.168.169.129", Server IP address: "192.168.169.129", Server port number: 1701, Proxy host name: "", Proxy IP address: "0.0.0.0", Proxy port number: 0, Virtual Hub name: "VPN_hub", Client unique ID: "4B068C3E7DB01EB6F7D2752A8C6F4216")
2022-04-24 08:44:41.122 L2TP PPP Session [192.168.0.101:1701]: Trying to request an IP address from the DHCP server.

2022-04-24 08:44:41.282 [HUB "VPN_hub"] Session "SID-LOCALBRIDGE-5": The DHCP server of host "D8-07-B6-2B-85-5F" (192.168.0.1) on this session allocated, for host "SID-ANTOS-[L2TP]-6" on another session "CA-D5-F1-55-9C-99", the new IP address 192.168.0.125.

2022-04-24 08:44:41.282 L2TP PPP Session [192.168.0.101:1701]: An IP address is assigned. IP Address of Client: 192.168.0.125, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.0.1, Domain Name: "", DNS Server 1: 192.168.0.1, DNS Server 2: 0.0.0.0, WINS Server 1: 0.0.0.0, WINS Server 2: 0.0.0.0, IP Address of DHCP Server: 192.168.0.1, Lease Lifetime: 7200 seconds

2022-04-24 08:44:41.282 L2TP PPP Session [192.168.0.101:1701]: The IP address and other network information parameters are set successfully. IP Address of Client: 192.168.0.125, Subnet Mask: 255.255.255.0, Default Gateway: 192.168.0.1, DNS Server 1: 192.168.0.1, DNS Server 2: 0.0.0.0, WINS Server 1: 0.0.0.0, WINS Server 2: 0.0.0.0