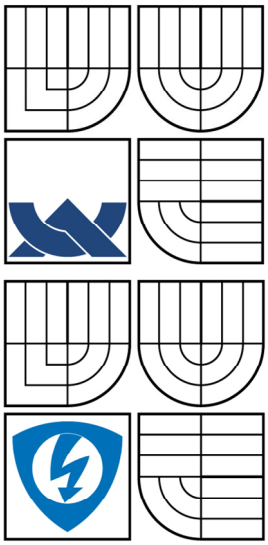


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FAKULTA ELEKTROTECHNIKY A
KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV AUTOMATIZACE A MĚŘÍCÍ TECHNIKY

ZABEZPEČENÁ SÍŤ ZALOŽENÁ NA ZAŘÍZENÍCH FIRMY CISCO

DIPLOMOVÁ PRÁCE

AUTOR PRÁCE ZDENĚK WAGNER

VEDOUCÍ PRÁCE Ing. TOMÁŠ MACHO , Ph.D.

BRNO 2008

Anotace

V práci je řešena problematika Virtuálních privátních sítí (VPN) na současných i starších protokolech a uvedené různé možnosti jejich využití. Mezi nejzajímavější by mohly patřit části věnované různým způsobům využití VPN technologie, protokolu IPSec, IOS SSLVPN a RSA serveru s HW tokenem pro zajištění dvoufaktorové autentizace uživatele.

Klíčová slova:

Cisco, VPN, SSLVPN, IPSEC, GRE, autentifikační mechanismy, AAA, RADIUS, TACACS+, RSA server

Annotation

This work deals with the matter of Virtual Private Network (VPN) utilizing both contemporary and older protocols and the possibilities of their use. Among the most interesting parts there are those presenting various ways of use of the VPN technology, IPSec protocol, IOS SSLVPN and RSA server with HW token ensuring the two-factor user authentication

Key words:

Cisco, VPN, SSLVPN, IPSEC, GRE, auhtentication mechanism, AAA, RADIUS, TACACS+, RSA server

Abstrakt

Práce se zabývá problematikou vytváření Virtuálních privátních sítí (VPN). V úvodu a následné analýze je popsán současný stav a požadavek na rozšíření možností používaných technologií pro vytváření VPN u mého zaměstnavatele Magistrátu Města Brna. Pro lepší pochopení celé problematiky jsou v práci uvedeny současné i starší protokoly a metody vytváření VPN. Cílem bylo za použití současných protokolů a technologií navrhnout zabezpečené řešení připojení mobilních uživatelů do sítě MMB. Jako hlavní stavební prvky pro realizaci takového připojení je použito směšovače Cisco 3845 jako IOS SLLVPN brány a RADIUS serveru od společnosti RSA ve verzi s HW tokenem. Cílové řešení postavené na těchto prvcích je dostatečně bezpečné a umožňuje jednoduché připojení do sítě MMB.

Abstract

The work is focused on the matter of creating Virtual Private Networks (VPN). The introduction and the following analysis describes the actual status and the demand for the expansion of potential of the technologies used for creating VPN within my employer – Brno City Municipality (BCM). For the better understanding of the matter the work describes the older protocols and methods of creating VPN as well. The main objective was to design a secured solution of connecting mobile users in the BCM network using current protocols and technologies. Cisco 3845 as an IOS SLLVPN gateway and RSA´s RADIUS server (HW token version) are used as the main construction elements of this connection. The final solution based on these elements is safe enough and guarantees a simple connection to the BCM network.

Bibliografická citace

WAGNER, Zdeněk. Zabezpečená síť založená na zařízeních firmy Cisco. Brno: Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, 2008. 3, přílohy. Ing. Tomáš Macho Ph.D..

P r o h l á š e n í

„Prohlašuji, že svou diplomovou práci na téma "Zabezpečená síť založená na zařízeních firmy Cisco" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené diplomové práce dále prohlašuji, že v souvislosti s vytvořením této diplomové práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne : 21.5.2008 Podpis:

P o ď ě k o v á n í

Děkuji tímto …Ing. Tomáši Machovi Ph.D. ... za cenné připomínky a rady při vypracování diplomové práce.

V Brně dne : 27.5.2008 Podpis:

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

Zkratka/Symbol	Popis
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
URL	Uniform Resource Locators
WWW	World Wide Web
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ISAKMP	Internet Security Association and Key Management Protocol
AH	Authentication Header
ESP	Encapsulating Security Payload
SA	Security Association
IKE	Internet Key Exchange
GRE	Generic Routing Encapsulation
PPTP	Point-to-Point Tunneling Protocol

L2TP	Layer Two Tunnel Protocol
IPSEC	Internet Protocol Security protocol
NIST	Institute of Standards and Technology
NAT	Network Address Translator
VPN	Virtual Private Network
VI'DN	Virtual Private Dial-up Network
AES	Advanced Encryption Standard
DES	Data Encryption Standard
MD5	Message Digest 5
RFC	Request For Comments
IOS	Internetwork Operating System
CSD	Cisco Secure Desktop
SVC	SSL VPN Client
NAC	Network Admission Control
PIN	Personal Identification Number
SSH	Secure Shell
POP3	Post Office Protocol - Version 3
IMAP	Internet Message Access Protocol
SMTP	Simple Mail Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
SUN JRE	Sun Java Runtime Enviroment

1. ÚVOD

Internet se stal symbolem 20. a 21. století. Stále rostoucí poptávka po datových přenosech nás vede k vytváření stále dokonalejších, rychlejších, a také bezpečnějších sítí. Dostáváme se od přenosu informací v podobě textu (webový prohlížeč), až po přenos zvuku či obrazu. S rostoucí poptávkou se bohužel zvyšuje i riziko odposlechu citlivých údajů, hrozby internetových virů, neoprávněných přístupů a kriminalita všeobecně páchána prostřednictvím internetu. Všechny instituce a firmy musejí nakládat stále více finančních prostředků pro zabezpečení jejich služeb poskytovaných prostřednictvím internetu. (internetové bankovnictví, a jiné aplikace, vzdálené přístupy mobilních zaměstnanců, …). Na druhou stranu je dnes požadována 100% spolehlivost a hlavně bezpečnost. Z tohoto důvodu vznikají záložní datové cesty a budují se VPN (virtual private network)

Stejně jako asi v každé větší společnosti využívající sítí WAN tak i v instituci Magistrátu Města Brna, kde pracuji jako správce sítě se setkáme s nějakou formou využívání VPN. V našem prostředí je VPN založená na protokolu IPSec využívána celkem hojně, zejména k propojení s úřady městských částí (UMČ). Tento způsob připojení však nevyhovuje požadavku na jednoduchou konfiguraci vzdálené (klientské) části připojení. Byl jsem proto postaven před úkol navrhnout a realizovat řešení, které by bylo dostatečně zabezpečené, spolehlivé a zároveň nenáročné na konfiguraci na straně uživatele. Řešení navíc musí umožňovat snadné připojení kdykoliv a odkudkoliv.

Snahou této bakalářské práce tedy bude analyzovat problémy spojené s budováním VPN založených na současných protokolech a technologiích. Vzhledem k tomu že celá infrastruktura MMB je postavena na prvcích firmy Cisco bude i tato práce zaměřena na využití řešení od této společnosti kvůli zajištění kompatibility a možnosti maximálně využít vlastností nabízené jejími technologiemi. Cílem je navrhnout řešení vzdáleného přístupu zaměstnanců či administrátorů pro instituci Magistrát Města Brna.

1.1 ANALÝZA SOUČASNÉHO STAVU SÍŤOVÉ INFRASTRUKTURY MAGISTRÁTU MĚSTA BRNA

Současný stav síťové infrastruktury Magistrátu Města Brna (MMB):

Z hlediska síťové topologie je vybudována síť WAN v níž se nacházejí budovy (uzly) v rámci kterých je realizována síť LAN. Jednotlivé uzly jsou propojeny optickými kabely, takže je možno na celek pohlížet jako na rozsáhlou síť LAN včetně globálního zabezpečení a přístupových politik platným pro všechny uzly. Do této sítě LAN je realizováno připojení pro úřady městských částí (UMČ) několika způsoby:

- UMČ využívají připojení pomocí VPN pracujících s protokolem IPSec, **využívají** vybudovanou infrastrukturu MMB pro připojení k internetu (antivir, antispam, firewall,..) včetně emailových služeb, mají omezený k aplikacím intranetu (zápisy z jednání, jídelna…)
- UMČ využívají připojení pomocí VPN pracujících s protokolem IPSec, **nevyužívají** vybudovanou infrastrukturu MMB pro připojení k internetu ale využívají jen emailových služeb a mají omezený k aplikacím intranetu (zápisy z jednání, jídelna…)
- UMČ využívají pouze SMTP nebo POP3 respektive SPOP3 služby kde je na firewallu MMB nastavena jejich IP adresa jako důvěryhodná pro komunikaci na určitých portech.

Z uvedeného vyplývá, že není realizováno řešení, pomocí kterého by bylo možno se připojit k infrastruktuře MMB, bez nutnosti být vybaven hardwarem nebo softwarem, schopným realizovat IPSec nebo ekvivalentní náhradu VPN spojení. Bez znalosti informací o nastavení od ISP a informací potřebných pro konfiguraci IPSec z čehož vyplývající náročnější konfigurace klientské části.

V této práci se budu zabývat právě řešením tohoto úkolu, tedy realizací VPN spojení kdykoliv a odkudkoliv bez náročné konfigurace, pomocí zařízení a technologie Cisco IOS SSL VPN od firmy Cisco.

2. VIRTUÁLNÍ PRIVÁTNÍ SÍTĚ (VPN)

2.1 VPN (VIRTUAL PRIVATE NETWORK)

Úplně obecná definice virtuální privátní sítě by mohla znít:

VPN je privátní sít, kde privátnost je vytvořena nějakou metodou virtualizace. VPN může být vytvořena v mnoha variantách - mezi dvěma koncovými systémy, mezi dvěma organizacemi, mezi několika koncovými systémy v rámci jedné organizace nebo mezi více organizacemi pomocí např. globální sítě Internet. Může být vytvořena také přímo mezi aplikacemi a samozřejmě také libovolnou kombinací všech uvedených možností.

Jednodušší, tedy jen přibližná, ale zato mnohem méně formální definice by mohla znít:

VPN je privátní síť, vybudovaná v rámci veřejné síťové infrastruktury, jakou je např. globální Internet.

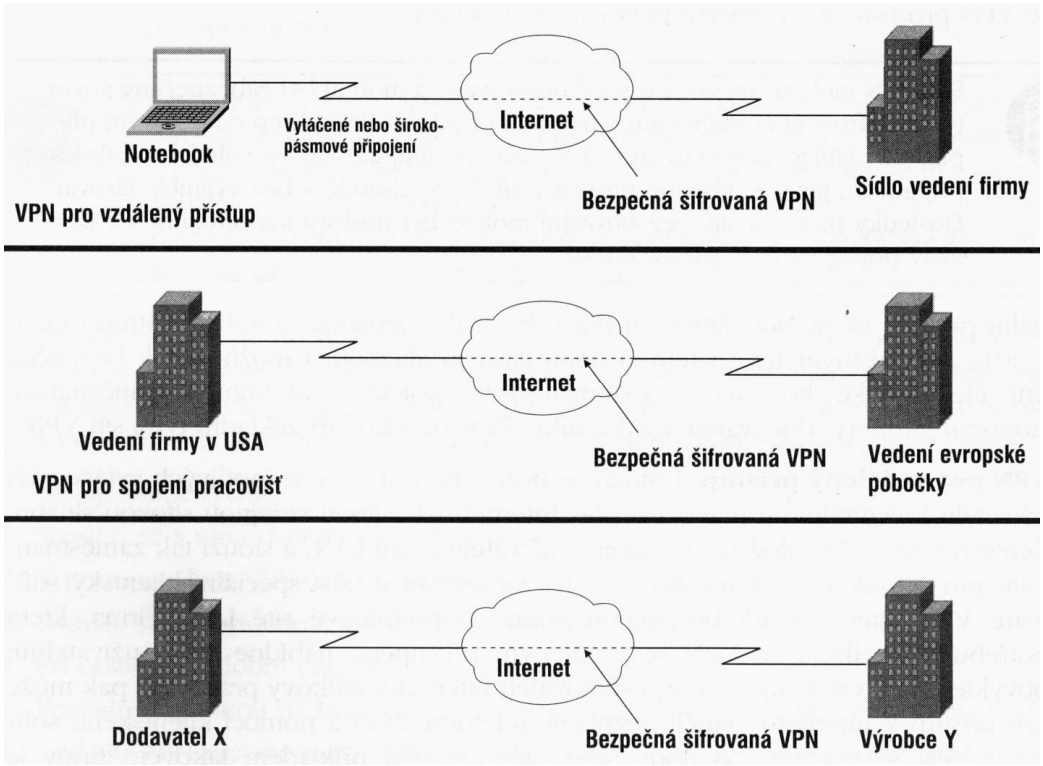
2.2 ÚČEL VPN

Bezpečnost komunikace ve VPN má dvě nedílné složky. Autentizaci uživatelů a utajení přenášených dat. Autentizace ověřuje totožnost dvou koncových bodu VPN (klient VPN, brána VPN nebo směrovač či ‚firewall) a uživatelů posílajících zprávy přes VPN.

VPN lze použít pro řešení různých požadavků, jež v sobě zahrnují potřebu bezpečně komunikovat přes veřejnou síť, které lze kategorizovat následovně:

- **VPN pro spojení pracovišť**. Tyto sítě rozšiřují stávající síť LAN ve firmě do dalších budov a pracovišť pomocí určitého specializovaného vybavení; vzdálení zaměstnanci pak mohou využívat stejné síťové služby jako pracovníci v ústředí. Uvedený typ sítě VPN bývá trvale aktivně propojený; někdy se označují také jako hardwarové VPN, intranetové VPN nebo jako VPN mezi sítěmi LAN (LAN-to-LAN, site-to-site).
- **VPN pro vzdálený přístup**. Umožňuje bezpečné připojení jednotlivých vytáčených uživatelů k centrálnímu pracovišti přes Internet nebo jinou veřejnou síťovou službu. Tento typ sítě VPN představuje spojení uživatele a sítě LAN, a slouží tak zaměstnancům pro připojení z terénu. Na počítači zaměstnance běží speciální klientský software VPN, který zavádí bezpečnou linku do podnikové sítě LAN. Firma, která potřebuje rozsáhlou síť VPN se vzdáleným přístupem, nabídne svým uživatelům obvykle určitý vytáčený účet k poskytovateli Internetu; dálkový pracovník pak může pro přístup k Internetu vytočit bezplatné telefonní číslo a pomocí klientského softwaru VPN se dostane do podnikové sítě. Dobrým příkladem takovéto firmy je obchodní společnost se stovkami obchodních zástupců v terénu. Sítě VPN pro vzdálený přístup se někdy označují jako softwarové VPN, virtuální privátní vytáčené sítě (Virtual Private Dial-up Network, VI'DN), nebo zkráceně vytáčené VPN. Uživatel platí malý „paušální" poplatek místnímu poskytovateli (nebo telekomunikační společnosti) a nemusí tím pádem pro připojení do firemní sítě vést podstatně dražší dálkový, meziměstský hovor. Nad spojením k místnímu poskytovateli pak vytvoří tunel VPN. VPN pro vzdálený přístup kladou nároky na řešení autentizace klientů, protože se uživatelé mohou připojovat opravdu odkudkoli a kdykoli
- **Extranetové VPN**. Poslední typ poskytuje bezpečné spojení s obchodními partnery, dodavateli a zákazníky za účelem vedení elektronické komerce. Extranetové sítě VPN jsou rozšířením intranetových VPN a vnitřní síť je v nich navíc chráněna pomocí firewallů. Dobrým příkladem může být firma, která natolik úzce spolupracuje s dodavateli a partnery, že vzájemné

potřeby zajišťuje přímým propojením informačních systémů - je to tedy vyšší forma dodavatelsko-odběratelských vztahů. Extranet umožňuje rychlejší výměnu informací.



Obrázek 2.1: Tři základní typy sítí VPN

Privátní IP datagramy se posílají přes VPN prostřednictvím bran VPN a klientů VPN. Ti mají nakonfigurované privátní adresy ostatních míst propojených VPN. Datagram určený na některou z těchto privátních adres se zabalí do datagramu s veřejnou IP adresou. Zapouzdřený datagram se směruje podle informace ve vnějším záhlaví přes IP' síť až k cílové bráně VPN, ta jej rozbalí a předá cílové stanici podle privátní adresy specifikované v záhlaví původního datagramu.

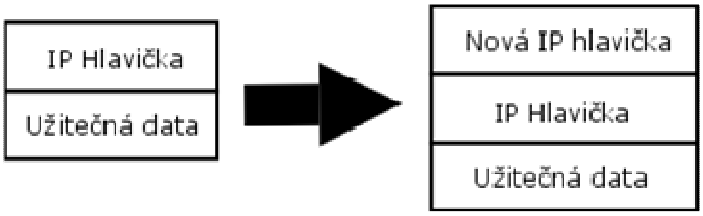
3. BEZPEČNOSTNÍ PROTOKOLY

3.1 IPOVERIP

Protokol IPoverIP patří mezi základní protokoly pro budování VPN. Pro svojí jednoduchost je vhodný pro budování záložní datové cesty.

IPoverIP je protokol, který umožňuje budovat VPN. Pomocí tohoto protokolu lze dosáhnout komunikace na úrovni vnitřní sítě přes sítě rozsáhlé (např.internet). Tento způsob komunikace si lze představit jako běžnou poštu, tedy zabalíme dopis do obálky, napíšeme adresu platnou pro Českou republiku. Tato obálka je později vložena ještě do jedné obálky a napsána nová adresa, která nemusí být platná pouze pro Českou republiku, tato obálka dorazí k příjemci, ten obálku rozbalí a předá dál. Tímto způsobem dosáhneme komunikace, kdy obě strany bydlí virtuálně v České republice. IPoverIP je zajímavý svojí jednoduchostí, která mu dodává robustnost. Původní paket je obalen novou IP hlavičkou viz obrázek 3.1. Z tohoto důvodu zůstane původní IP hlavička nezměněna a nemusí se přepočítávat kontrolní součet hlavičky. Nová IP hlavička má novou IP adresu odesílatele i příjemce. Důležité je převzít z původní hlavičky příznak DF (Don't Fragment), jeli nastaven na hodnotu 1 je zakázána fragmentace. Fragmentace je asi největším problémem IPoverIP, jelikož přidáním nové IP hlavičky vzroste celková velikost IP paketu o 20bytů. Pro doplnění MTU (Maximum Transfer Unit) Ethernet II je standardně 1500bytů. Pokud odesílatel vytvoří IP paket o celkové velikosti 1500bytů a kdekoli po cestě k příjemci je použit protokol IPoverIP, musí dojít k fragmentaci IP paketu. Některé aplikace z důvodu bezpečnosti právě fragmentaci zakazují. V tomto případě je paket zahozen a odesílateli je poslán paket ICMP Typ 3, Kód 4 (Fragmentation needed but don't fragment bit set). Nová IP hlavička má vlastní TTL, TOS, jako protokol vyšší vrstvy je vyplněn IPoverIP. TTL dekrementováno o 1 při vybalení paketu z nadřazeného, tj. v cílovém místě, takže z pohledu paketu pak přeskočil jen jednou , fyzicky mohl urazit vícero přeskoků. U protokolu se vyskytuje hrozba zacyklení ,protože při každém zabalení je znovu nastavena hodnota TTL. Provádí se proto kontrola, zda se zdrojová IP adresa paketu náhodou nerovná mé vlastní IP adrese, případně zda cílová

IP adresa neodpovídá uzlu, který paket odeslal. Protokol obsahuje zabezpečení, že paket dorazí na určené místo Nová IP hlavička má také svůj kontrolní součet. Obrázek 3.1.



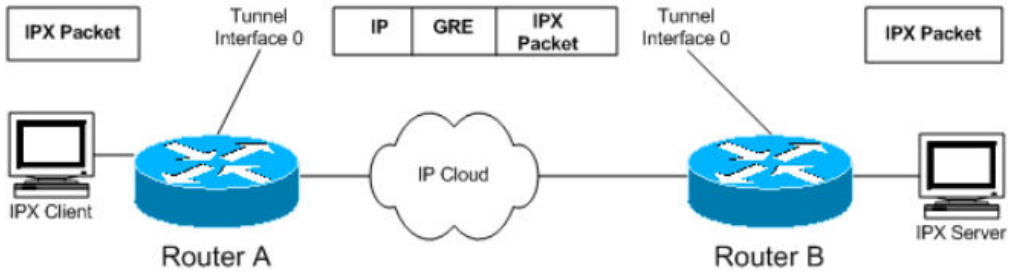
Obrázek 3.1: IPoverIP

Zhodnocení:

Díky absenci jakéhokoliv zabezpečení není vhodný kandidát na implementaci řešení přes nezabezpečený kanál.

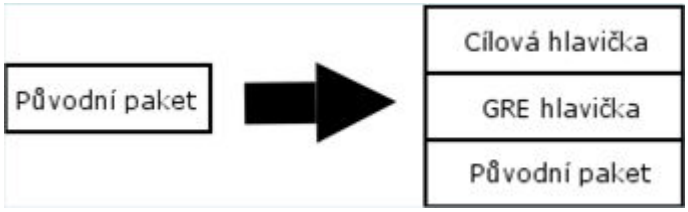
3.2 GRE

GRE (generic routing encapsulation) je tunelovací protokol vyvinutý firmou Cisco. Obecně definuje, jakým způsobem by měly být zabaleny pakety širokého spektra protokolů a předány transportnímu protokolu. Nevyžaduje, aby přenášeným, případně přenašitelským protokolem byl IP protokol kterékoli verze. Cílem je umožnit vytváření tunelů, které budou uzpůsobené pro přenos paketů jednoho protokolu skrze jiný protokol. Z toho plyne, že je nezávislý na transportních a přenášených protokolech. Typické použití je na obrázku 3.2.



Obrázek 3.2: Použití protokolu GRE

Vytvoření paketu



Obrázek 3.3: GRE paket

Nedochází k přiložení původních dat ihned za hlavičku transportního protokolu, ale data jsou nejprve zabalena do GRE protokolu a ten je teprve předán transportnímu protokolu k přenosu. Specifikace nepožaduje žádné specifické vlastnosti původního, nebo transportního protokolu. Definuje pouze jakým způsobem má vypadat GRE hlavička. Podle toho lze zjistit, jaký protokol je v GRE paketu zabalen. Nastavení TTL a identifikace zacyklení řešeno stejně jako u protokolu IPoverIP

Zhodnocení:

Opět chybí implementován mechanismus ochrany přenášených dat.

3.3 PPTP

Point-to-Point Tunneling Protocol (PPTP) byl vyvinut společně firmami Microsoft, U.S. Robotics a několika dalšími společnostmi zabývající se vzdáleným přístupem. Protokol využívá ke své činnosti protokolu PPP (point-to-point protocol). Pomocí PPTP se uživatelé můžou připojovat do svých korporátních sítí.

Protokol je postaven na modelu klient-server kdy jedna strana nejprve vždy spojení sestavuje. Sestavování spojení je realizováno pomocí tzv. kontrolní datového spoje, což je TCP spojení iniciované klientem směrem k serveru. Po navázání toho spojení je možné mezi klientem a serverem obousměrně přeposílat IP pakety.

Vytvoření paketu

Obrázek 3.5: PPTP paket

Paket je nejprve obalen do PPP, po té zabalen do upravené verze GRE protokolu a teprve po té předán protokolu IP, který okolo něho vytvoří ještě jednu hlavičku, aby mohl cestovat v IP síti.

Zhodnocení:

Nedefinuje žádné zabezpečení nad přenášenými daty. Vše je totiž na PPP protokolu jehož šifrovací klíče jsou odvozeny přímo z uživatelova hesla, z toho plyne slabší implementace zabezpečení. Je tedy náchylný na offline útoky na uživatelovo heslo. PPTP je obsažen v produktech firmy Microsoft a podporuje jen 255 současných spojení a pouze jeden vytvořený tunel na uživatele.

3.4 L2TP

Layer 2 Tunneling Protocol (L2TP) byl publikovaný v roce 1999 a navržený jako standard RFC 2661. L2TP vznikal primárně ze dvou starších tunelovacích protokolů pro PPP: Cisco's Layer 2 Forwarding (L2F) a Microsoft's Point-to-Point Tunneling Protocol (PPTP) jejichž vlastnosti kombinuje. Nová verze tohoto protokolu, L2TPv3 byla publikována a navržena jako standard RFC 3931 v roce 2005. L2TPv3 poskytuje přídavné bezpečnostní vlastnosti, vylepšené zapouzdřování (enkapsulaci). Data jsou přenášena v zapouzdřených PPP rámcích datové části UDP paketů. Podporuje tvorbu vícenásobných tunelů mezi koncovými uzly v tranzitních sítích internet (IP), Frame Relay a ATM. Dále umožňuje autorizaci uzlů v rámci

tunelu, šifrování a kompresi přenášených rámců. V rámci protokolu L2TP jsou využívány dva základní druhy uzlů:

- **LAS** (L2TP Access Concentrator) – klient protokolu L2TP, přístupový koncentrátor sítě. Vytváří tunel mezi serverem a uzly koncentrátoru LAS pro přenos PPP rámců jednotlivých uzlů do vzdálené sítě. Zabezpečuje autentifikaci a přístup a po úspěšné autentifikaci je uživatel přesměrován na LNS
- **LNS** (L2TP Network Server) – je server protokolu L2TP, který v rámci tunelů zřizuje relace pro jednotlivá koncová zařízení připojená k přístupovému koncentrátoru. Zabezpečí vlastní přístup do vnitřní sítě

Zhodnocení:

Podporován společností Microsoft od produktové řady Windows2000. Plně podporuje protokol IPSec

3.5 IPSEC

IPSec (IP security) je bezpečnostní rozšíření IP protokolu. V architektuře OSI se jedná o zabezpečení již na síťové vrstvě. Toto rozšíření je tak nezávislé na dalších (vyšších) protokolech TCP/UDP. Je definován v několika desítkách RFC, ale základní jsou 2401 a 2411. Vytváří logické kanály - security associations (SA) – bezpečnostní asociace, které jsou vždy jednosměrné, pro duplex se používají dva SA.

Balík IPSec používá tři vzájemně se doplňující protokoly, které společně tvoří ucelený a bezpečný systém standardů, jež se ideálně hodí i pro sítě VPN. Podívejme se na ně podrobněji:

- **ISAKMP** (Internet Security Association and Key Management Protocol). Popisuje fázi dohody o spojení v IPSec, ve které se navazuje spojení sítě VPN; protokol Oaklev pak definuje metodu navázání výměny autentizovaného klíče. Uvedená metoda může mít několik různých režimů činnosti a výchozí údaje pro

klíče („klíčový materiál") může odvozovat pomocí speciálních algoritmů jako je Diffie-Helhnan. Součástí protokolu ISAKMP je také standard IKE (Internet Key Exchange), jenž definuje postup pro dohodu bezpečnostních parametrů (například doba života bezpečnostních asociací SA, typ šifrování atd.) a pro potvrzení věrohodnosti klíčů.

- **AH** (Authentication Header). Poskytuje autentizaci a volitelně také ochranu proti opakování relace. Zajišťuje ověření integrity přenášených dat. Jeho služby jsou však omezené jen na část hlavičky IP a rozšířené hlavičky, ale nezajišťuje již šifrování dat - pomocí jednosměrného haše vytváří z paketu pouze otisk zprávy. Autentizační hlavička AH se vkládá do samotných chráněných dat (například do úplného datagramu IP). Protokol AH můžeme používat samostatně, nebo ve spojení s ESP, kterým byl dnes již ale v podstatě překonán. Podrobněji je AH popsán v RFC 2402

- **ESP** (Encapsulating Security Payload). Umí to co protokol AH, navíc však umí i šifrovat. Lze jej použít jen jako AH protokol nebo jen jako šifrovací protokol proto se používá spojení těchto dvou dohromady. ESP zajišťuje důvěrnost a ochranu dat s volitelnými službami autentizace. detekce opakování relace. Protokol ESP definuje úplné zapouzdření uživatelských dat; můžeme jej používat samostatně, nebo ve spojení s AH. Běží nad protokolem TCP s porty 50 a 51 a blíže je popsán v dokumentu RFC 2406.

3.5.1 Bezpečnostní asociace SA

Bezpečnostní asociace (Security Association, SA) zavádějí vztah důvěry mezi dvěma partnerskými zařízeními a koncové body sítě VPN se tak pomocí nich mohou dohodnout na množině přenosových pravidel, kdy si vzájemně potvrzují takzvané zásady (politiky) s potenciálním partnerem. Bezpečnostní asociaci tak můžeme považovat za jakousi „smlouvu", v níž se potvrdí a závazně nastaví různé parametry navazovaného spojení. Určitou bezpečnostní asociaci popisuje IP adresa, identifikátor bezpečnostního protokolu a jedinečná hodnota indexu bezpečnostního

parametru SPI (security parameter index). Index SPI je přitom 32bitové číslo, zapisované do hlavičky paketu. Rozlišujeme dva typy bezpečnostních asociací:

- **IKE** (Internet Key Exchange). Zajišťuje dohodu klíčů, autentizaci partnerů, správu klíčů a jejich výměnu. Je to obousměrný protokol a jako takový vytváří bezpečný komunikační kanál mezi oběma zařízeními, která se dohodnou na šifrovacím algoritmu, hašovacím algoritmu, autentizační metodě a případných informacích o skupině. Výměna klíčů zde vychází z algoritmů Diffie-Hellman, přičemž síťoví administrátoři mohou IKE úzce svázat se systémy pro správu zásad. Jako ochrana proti útoku s mužem uprostřed (kdy útočník odposlouchává pakety v síti, upravuje je a v pozměněné podobě je vkládá zpět do komunikačního proudu) slouží zdokonalená verze algoritmu Diffie-Hellman s označením STS (Station-To-Station); tento protokol provádí vzájemnou autentizaci obou zařízení pomocí digitálních podpisů a certifikátů s veřejným klíčem
- **IPSec SA** (bezpečnostní asociace IPSec). Protokol IPSec SA je jednosměrný, a proto je nutné v každém směru komunikace zavádět samostatné asociace. Celý proces probíhá ve dvou fázích a třech režimech: fáze 1 nabízí dva režimy, a sice hlavní režim a agresivní režim, zatímco fáze 2 má jediný, takzvaný rychlý režim. Koncový uživatel nemá nad výběrem konkrétního režimu žádnou kontrolu; volba probíhá automaticky a je závislá na konfiguračních parametrech obou partnerů

Bezpečnostní asociace se využívají v protokolech IKE i IPSec, i když obě asociace jsou pak vzájemně nezávislé. Asociace IPSec SA jsou navíc jednosměrné a v každém z bezpečnostních protokolů (AH a/nebo ESP) jsou jedinečné. Úlohou bezpečnostních asociací je definovat, které protokoly a algoritmy se budou aplikovat na citlivé pakety a jaké výchozí údaje pro klíče se budou mezi oběma partnery používat. Asociace IPSec SA je možné zavést dvěma různými způsoby:

- **Ruční bezpečnostní asociace s předem sdílenými klíči**. U této metody se musí nejprve dohodnout administrátor PIX Firewallu a příslušného partnera IPSec. Neprobíhá zde žádná dohoda o asociacích, takže oba systémy musí mít stejnou

konfiguraci, jinak se síťový provoz pod IPSec nemůže správně přenášet. Ruční konfigurace není nijak obtížná; na druhé straně se ale předem sdílené klíče dosti těžko mění, protože tunel po jednostranné změně přestane fungovat - předem sdílené klíče se proto obvykle nikdy nemění.

- **Asociace zaváděné pomocí IKE.** Jestliže bezpečnostní asociace zavádíme pomocí protokolu IKE, mohou se oba partneři na parametrech nových bezpečnostních asociací dohodnout. To znamená, že určíme seznam povolených parametrů (například přípustných transformací příkazem crypto map.

3.5.2 Přehled činnosti protokolu IPSec

Hlavním úkolem IPSec je umožnit výměnu privátních informací přes nezabezpečené spojení; k tomu bezpečně provádí dohodu o spojení a přenos klíčů. Pomocí šifrování chrání protokol IPSec zasílané informace před zadržováním a odposlechem. Aby ale bylo celé šifrování účinné, musí obě strany používat stejné, společné heslo (neboli tajný klíč), kterým šifrují a dešifrují veškeré informace na vstupu a na výstupu z tunelu VPN. IPSec zavádí pomocí IKE bezpečné spojení, nad nímž pak síť VPN může formovat a propojovat vlastní data. Na nejvyšší úrovni můžeme posloupnost událostí v transakci IPSec popsat následovně:

1. Jeden z partnerů IPSec přijme nebo vygeneruje „zajímavý" provoz, a to nad rozhraním, které má podle platné konfigurace zahajovat vytvoření tunelu IPSec.
2. Pomocí dohody v hlavním nebo agresivním režimu IKE se mezi oběma partnery IPSec vytvoří bezpečnostní asociace IKE SA.
3. Nyní nastoupí dohoda v rychlém režimu, která z výsledků IKE vytvoří mezi oběma partnery IPSec dvě bezpečnostní asociace IPSec SA.
4. Přes šifrovaný tunel se prostřednictvím obalových protokolů ESP nebo AH začnou přenášet vlastní data.

Tyto čtyři zdánlivě jednoduché kroky si ale žádají trochu podrobnější výklad. Protokol IPSec pracuje ve dvou hlavních fázích, jejichž úkolem je zajistit důvěrnou výměnu společného tajného klíče (1).

3.5.3 Režimy šifrování protokolem IPSec

Protokol IPSec má dva režimy šifrování, a sice tunelovací a přenosový (transportní) režim. Oba se liší svým uplatněním a také objemem režie, doplněným k nesenému (přenášenému) paketu. Tunelovací režim šifruje se zátěží paketu i jeho hlavičku, zatímco přenosový režim provádí jen šifrování datové zátěže.

Tunelovací režim

Při propojení dvou PIX Firewallů (nebo jiných bezpečnostních bran) přes nedůvěryhodnou síť, jakou je veřejný Internet, se IPSec normálně implementuje v tunelovacím režimu; bude z něj vycházet i veškerý náš další výklad IPSec.

Přenosový režim

Tato metoda implementace protokolu IPSec se zpravidla používá ve spojení s protokolem L2TP, a to pro autentizaci vzdálených klientů VPN pod Windows 2000.

Zhodnocení:

IPSec je díky svým vlastnostem dnes nejrozšířenější standard na budování VPN sítí. Hash funkce u AH protokolu je vypočítávána právě i z některých "statických" částí samotného IP transportního paketu, čímž je bohužel znemožněno provozu IPSecu na sítích, kde dochází k překladu adres (NAT)

3.6 SSL

Na vyšších vrstvách než IPSec působí ještě další bezpečnostní mechanismy. SSL (Secure Sockets Layer) je firemní mechanismus, který se používá na aplikační vrstvě. Nezabezpečuje veškerou komunikaci, ale pouze některé aplikace. nejznámější uplatnění SSL je u zabezpečeného HTTP (HTTPS) podporovaného většinou webových prohlížečů. SSL se využívá u aplikací e-business nebo pro vzdálený

přístup, včetně virtuálních privátních sítí (SSL VPN). Třetí verze SSL se stala základem otevřené specifikace řešení TLS (Transport layer Security, RFC 2246).

SSL zajišťuje autenticitu odesílatele, integritu a šifrování aplikačních dat při jejich přenosu přes veřejnou IP síť. SSL vyžaduje spolehlivý transportní protokol, tedy TCP. SSL používá kombinaci šifrování veřejným a soukromým klíčem: asymetrické šifrování se používá v průběhu počáteční fáze pro autentizaci a generování klíčů dané relace, soukromý klíč se pak využívá pro šifrování zpráv.

SSL podporuje obousměrnou autentizaci, ale používá se většinou pouze jednosměrně. Lze využít jak jména a hesla (RADIUS), jména a token (RSA SecurelD), nebo digitální certifikáty X.509. Klient SSL spoléhá na digitální certifikát od vzdáleného serveru, k němuž se chce připojit. Útočník může ale certifikát zfalšovat a tak provést útok typu man-in-the-middle. Tomu lze zabránit dvoustupňovou autentizaci za použití jak hesla, tak tokenu.

3.6.1 SSL versus IP SEC

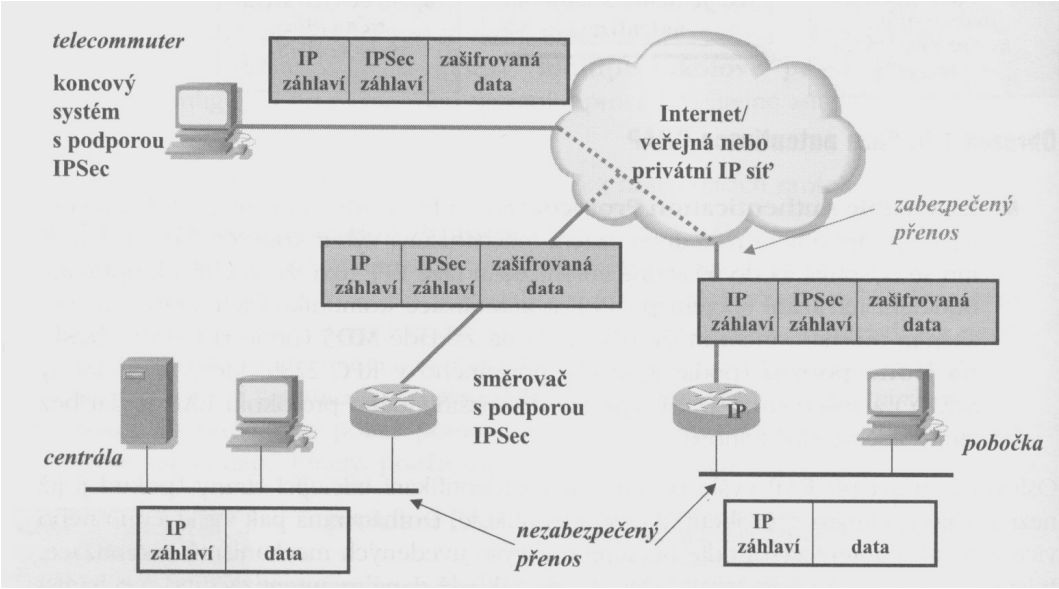
SSL podobně jako IPSec umožňuje bezpečnou komunikaci vzdáleného uživatele (i mobilního) se serverem přes veřejnou IP síť. IPSec, jak bylo řečeno výše, se stará o bezpečný komunikační kanál po IP mezi klientem a cílovým systémem na síťové vrstvě, takže nijak neomezuje podporované aplikace. Naproti tomu SSL slouží k zabezpečení samotné aplikace typu klient-server, ale ne všech aplikací. Bezpečný klient SSL je implementován na základě prohlížeče a všechny aplikace pak musí být individuálně podpořeny SSL. Nicméně pro mnoho podniků jsou právě zmiňované aplikace jediné, k nimž budou potřebovat vzdálení uživatelé přístup.

Úroveň SSL šifrování se dohaduje při komunikaci tak, že většinou se strany shodnou na nejnižším možném stupni, tedy s 40bitovým klíčem. U IPSec je úroveň šifrování přednastavená administrativně, takže běžně Lze použít 128bitový klíč. SSL šifruje nad transportní vrstvou, takže chrání aplikační data. IPSec, s použitím protokolu ESP, chrání šifrováním navíc původní záhlaví IP a TCP. IPSec chrání před nechtěnou analýzou provozu, a to SSL neumí. SSL není chráněno před některými útoky typu DoS (Denial of Service).

Jak SSL, tak IPSec podporuje bezpečnostní algoritmy pro zajištění integrity zpráv, jako MD5 nebo SHA1, ale implementace IPSec podporují silné šifrování typu 3DES nebo AES. SSL se hodí i pro připojování mobilních uživatelů z veřejných přístupových sítí (např. bezdrátových LAN, tzv. hot spots), i když právě v těchto případech vyžadují silné zabezpečení na ochranu před útoky zvnějšku. IPSec je naproti tomu vhodné pro pevné připojení vzdálených uživatelů.

3.6.2 SSL VPN versus IPSec VPN

IPSec představuje vysoce bezpečnou metodu pro budování VPN (obrázek 1.1), ale je současně také složité na implementaci. Vyžaduje speciální klientský software (a jeho instalaci na klientském systému) a komplexní konfiguraci všech potřebných parametrů IPSec včetně konfigurace podpory tunelů.



Obrázek 4.1: IP VPN s IPSec

IPSec trend vede k řešení bezpečnosti koncových bodů. Tunely totiž mohou být narušeny trojskými koni, viry, nebo spyware na klientském zařízení. VPN klienti proto potřebují implementovat osobní firewall. Nicméně vzdálená zařízení často nejsou vybavena posledními bezpečnostními záplatami (AV soubory). Centrální bezpečnostní politika špatně dosáhne na vzdálené uživatele, centralizovaný upgrade

proto není většinou možný. Řešením je integrovat VPN klienty a bezpečnostní pravidla na počítačích a tento trend neplatí pouze pro VPN na bázi IPSec, ale i pro SSL VPN.

SSL jako alternativa k IPSec pro budování VPN je slabší z hlediska bezpečnosti, ale je méně náročná na implementaci. Nepotřebuje nový klientský software, protože běží na standardních webových prohlížečích, a nevyžaduje tedy od uživatele žádnou instalaci. SSL ale nepodporuje všechny aplikace: hodí se pro zabezpečení komunikace webové, elektronické pošty nebo sdílení souborů. Naproti tomu se nehodí pro relačně orientované aplikace. Porovnání IPSec a SSL pro budování VPN je uvedeno v tabulce 1.1

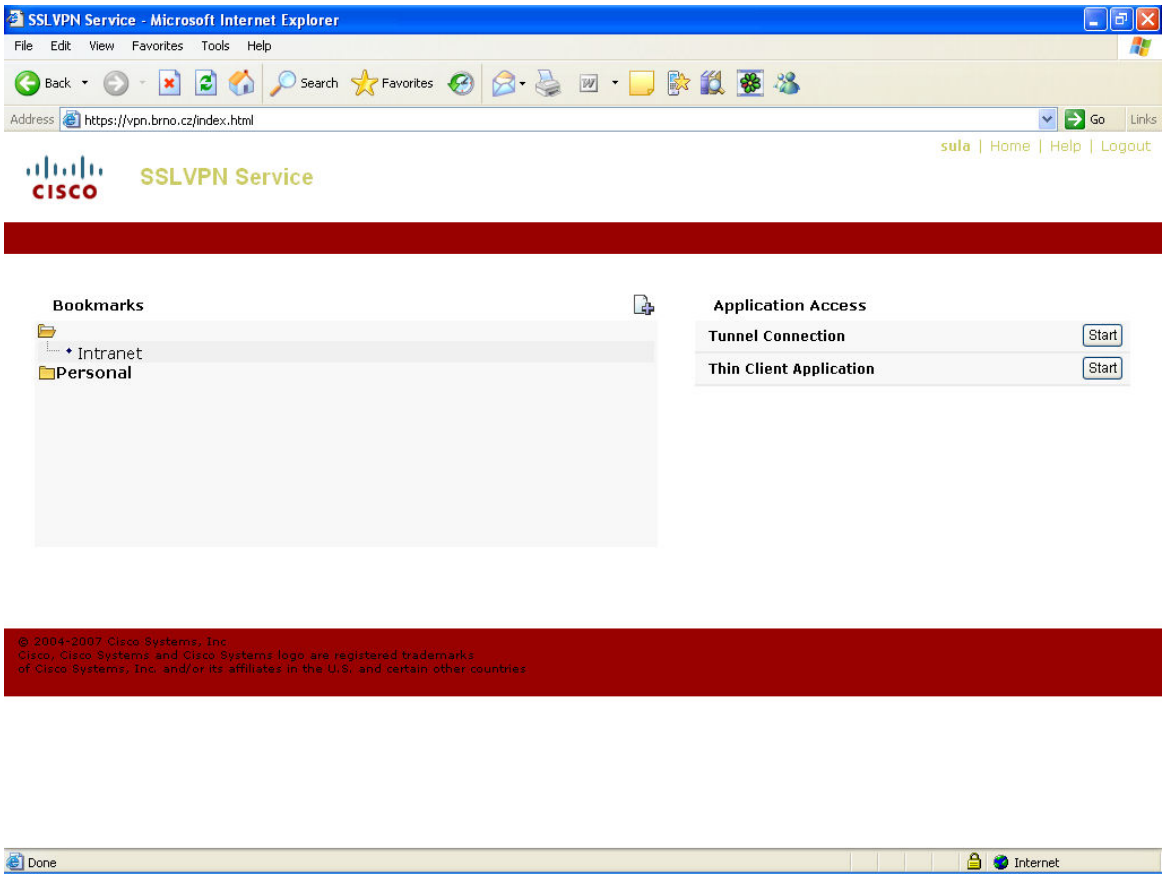
Tabulka 1.1: Porovnání VPN na bázi IPSec a SSL

	SSL	**IPSec**
Aplikace	webové aplikace, sdílení souborů a elektronická pošta	všechny aplikace TCP/IP
Šifrování	různě silné v závislosti na webovém prohlížeči	konzistentně silné, závisí na dané implementaci
Autentizace	různě silná (jednosměrná nebo obousměrná, za použití hesel, tokenu nebo certifikátů)	silná (obousměrná za použití tokenu nebo certifikátu)
Celková bezpečnost	středně silná	velmi silná

.

3.7 CISCO IOS SSL VPN (CISCO WEB VPN)

Tento způsob přístupu do vnitřní sítě je pro klienta velice jednoduchý a přívětivý. Klient přistoupí pomocí prohlížeče na WWW stránku (HTTPS), kde se přihlásí a ocitne se na výchozí stránce brány. Zde si volí typ přístupu do vnitřní sítě ze tří možností. Záleží na klientovi který typ si zvolí a pomocí které aplikace bude přistupovat do vnitřní sítě.



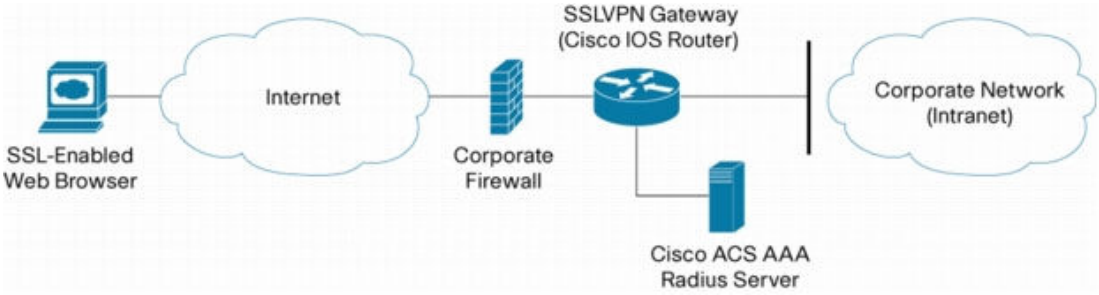
Obrázek 4.2: Výběr přístupu na bráně

- přístup na službu HTTP nebo HTTPS - klient používá pro přístup k této službě pouze prohlížeč a na bráně se vyspecifikují servery ke kterým bude mít daný uživatel přístup.
- přístup na služby využívající pouze protokol TCP. Klient používá pro přístup tenkého klienta, kterého si spustí přímo z brány. Dojde ke spuštění Java

aplikace, která zpřístupní přes lokální loopback klienta a vybraný port aplikace z vnitřní sítě.

- přístup do vnitřní LAN pomocí SSL VPN klienta (tlustý klient). Jedná se o plnohodnotný přístup do vnitřní sítě. Tímto způsobem jsou dostupné všechny povolené služby.

Koncepce připojeni pomocí Cisco IOS SSL VPN



Obrázek 4.3: Koncepční schéma připojení přes Cisco IOS SSL VPN

Odlišností oproti připojení například pomocí IPSec tunelem kde dochází k vytváření tunelu již mezi firewallem nebo prvkem na jeho úrovni je, že komunikace prochází skrze firewall a je navazována proti SSL VPN bráně, kde dochází k ověření uživatele a povolení přístupu k aplikacím a službám definovaným způsobem.

4. ŠIFROVACÍ A HASHOVACÍ ALGORITMY

4.1 ŠIFROVÁNÍ DES

Dne 23. listopadu 1976 přijal úřad NIST (National Institute of Standards and Technology) upravený (zkrácení 128bitového klíče na pouhých 56 bitů) algoritmus Lucifer za americký federální standard a současně změnil jeho název na Data Encryption Standard (DES). Algoritmus, jehož specifikace byla zveřejněna následně v lednu 1977, se díky silné oficiální podpoře vlády zanedlouho rychle rozšířil.

Na přelomu sedmdesátých a osmdesátých let, kdy nejlepší „stolní" počítače byly 8bitové Atari a Commodore, byla míra bezpečnosti v algoritmu DES docela ideální. Nové počítače byly ale stále rychlejší, a také se k nim dostávalo stále více lidí, kteří se v algoritmu různě „vrtali"; brzy proto narazil na své hranice a 56bitový klíč se zkrátka pro důkladné zabezpečení ukázal jako nedostatečný.

V roce 1997 přestal úřad NIST podporovat algoritmus DES a začal pracovat na jeho náhradě, která byla označena jako Advanced Encryption Standard (AES). (1)

4.1.1 Omezení algoritmu DES

Dejme tomu, že někdo zašifruje důležitá data pomocí klíče složeného jen z běžných znaků, třeba jen z normálních velkých písmen anglické abecedy od A do Z (za heslo má například jméno manželky, oblíbeného fotbalového klubu, nebo svého bydliště). Při omezení znaků na obyčejná písmena je ale prolomení či uhodnutí hesla (klíče) stotisíckrát jednodušší.

Takovéto heslo složené jen z písmen se už tedy dá prolomit relativně pohodlně; navíc, pokud lidé mají heslo složené jen z písmen, můžeme vsadit, že to bude jednoduché slovo ze slovníku - a takové heslo zjistíme během pár minut.

4.2 ŠIFROVÁNÍ TRIPLE DES (3DES)

Ve své době, tedy v sedmdesátých letech, byl algoritmus DES přímo fantastickou odpovědí na problém šifrování dat; jeho autoři si ale ani ve snu nedokázali představit, nakolik se svět dokáže za pouhých 30 roků změnit. Především si neuvědomovali, že se nacházejí v předvoji samotné informační revoluce. Díky technickému pokroku se ale algoritmus DES se svojí úrovní ochrany stal pouhou popelkou a celý obor jednoznačně žádal jiné řešení.

Algoritmus DES byl překonaný, nicméně později byl vyvinut algoritmus Triple DES (3DES); protože byl odvozen z původního DES, proběhl vývoj poměrně rychle. Na první pohled by se ze zkratky mohlo zdát, že prolomení šifry 3DES je třikrát obtížnější než u algoritmu DES - ve skutečnosti je ale rozdíl řádový, $5*10^{33}$krát.

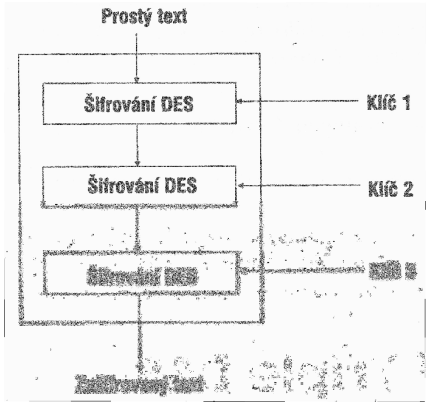
„Trojitý" algoritmus 3DES používá při šifrování a dalších souvisejících výpočtech hned tři samostatné klíče a efektivní délku výsledného klíče tak prodlužuje z 8 na 24 znaků, tedy na 168 bitů (24*7). Matematicky vzato můžeme počet různých kombinací vyjádřit jako:

$2^{168} = 3,7 * 10^{50}$ kombinací

Algoritmus 3DES se považuje již za velmi silnou šifru.

Síla šifrovacího mechanismu

Algoritmus 3DES je v podstatě rozšířením původního DES, přičemž data postupně šifruje pomocí tří klíčů, jak vidíme na obrázku 4.1:



Obrázek 4.1: Kroky při šifrování algoritmem 3DES

Vlastní postup šifrování dat je v algoritmu 3DES stejný jako v DES, zde se ale třikrát opakuje - původní data (například dokument Microsoft word) se zašifrují pomocí prvního klíče, výsledek pomocí druhého klíče, a tento výsledek vstoupí do šifrování se třetím klíčem. Odtud také označení 3DES.

4.2.1 Omezení algoritmu 3DES

Protože každý blok dat ve formátu prostého textu je nutné zašifrovat třikrát po sobě, je zřejmé, že algoritmus 3DES běží pomaleji než obyčejný DES. Pokud do něj ale správně zadáme tři různé klíče, je výsledné šifrování o několik řádů silnější než u původního DES. Používat u všech tří kroků šifrování stejný klíč je velmi nevhodné - výsledkem je pak pouze jakási pomalá varianta běžného algoritmu DES. Jak jsme si již řekli, plný algoritmus 3DES je oproti původnímu DES podstatně silnější metodou šifrování a dnes se používá velmi často.

4.3 ALGORITMUS OTISKU ZPRÁVY MD5

S vývojem Internetu jako takového a se změnou orientace celého světa na práci s daty a s počítačovými sítěmi jsme si museli postupně zvyknout také na to, že se „tu a tam" setkáme s hackery. To znamená, že se musíme zabývat mimo jiné i bezpečností, autenticitou (neboli pravostí při komunikaci) a integritou dat..

Zmíněné otázky jsou velmi důležité pro každého - od tajných vojenských či státních institucí, přes lékařské osobní záznamy, až po finanční údaje. Každá organizace potřebuje tajná či privátní data uchránit před cizími osobami, které k nim nemají mít přístup. Pokud jsme v souvislosti s bezpečností hovořili o autenticitě a integritě dat, můžeme je blíže charakterizovat takto:

- **Autenticita** (pravost, hodnověrnost) osvědčuje, že osoba nebo skupina osob, která odesílá data, je skutečně tím, za koho se vydává. Příkladem zajištění autenticity dat je digitální podpis.

- **Integrita** (celistvost) prokazuje, že se data během přenosu nezměnila a že jsme je přijali ve stejné podobě, v jaké byla odeslána. Stahovali jste si někdy nějakou softwarovou aplikaci nebo záplatu do operačního systému? V takovém případě je důležité, aby si stažený soubor zachoval integritu.

Algoritmus otisku zprávy Message Digest 5 (MD5 je jednou z nejlepších metod zajištění těchto potřeb zabezpečení datové komunikace. Takovýto algoritmus v principu generuje ze vstupních dat jistý výstup o pevné délce, který se nazývá haš (hash), otisk, či „otisk prstu" (message digest, fingerprint) a je klíčem k bezpečnosti MD5. (Oficiální popis algoritmu MD5 je uveden v dokumentu RFC 1321.) (1)

Je důležité poznamenat, že algoritmus MD5 žádná data nijak nešifruje ani je nepozměňuje; namísto toho z nich vytvoří jistý otisk, podle něhož je možné poznat autenticitu a integritu přijatých dat.

5. NÁVRH ROZŠÍŘENÍ SÍŤOVÉ INFRASTRUKTURY MAGISTRÁTU MĚSTA BRNA

Informace pro vytvoření možných variant řešení vzdáleného přístupu do vnitřní sítě MMB a využívání definovaných zdrojů byly získány při jednáních s vedoucími a uživateli kteří o toto rozšíření usilovali.

Kritéria byla stanovena na až 100 současně připojených uživatelů, dvoufaktorovou autentikaci a integrovatelost do současné infrastruktury MMB.

5.1 KOMPONENTY PRO ROZŠÍŘENÍ INFRASTRUKTURY

Jednotlivé komponenty jsem volil s ohledem na dostatečný výkon pro uvažovaný počet uživatelů a možnou další rozšiřitelnost o nové funkční moduly v případě potřeby dalších služeb.

Základní komponenty jsou:

- VPN koncentrátor (včetně SW nástavby)
- Autentikační manažer
- CiscoSecureDesktop (CSD)

VPN Koncentrátor

Jako VPN koncentrátor jsem zvolil kvalitní z hlediska uvažovaného počtu uživatelů (do 100 uživatelů) i výkonnostně dostačující **Cisco 3845**, které je ideální platformou pro SSL-Based remote access VPN řešení, které je realizováno technologií **Cisco IOS WebVPN**. Toto integrované řešení je tzv. „single box“ řešení, kdy veškeré potřebné záležitosti spojené s konfigurací, správou a dostupností se řeší v rámci jednoho zařízení. Řešení založené na produktech Cisco navíc zapadá do koncepce stávajících aktivních prvků na MMB

Z hlediska požadovaného počtu uživatelů a umístění VPN koncentrátoru do stávající infrastruktury bude Cisco 3845 vybaveno hardwarově v základní konfiguraci se dvěmi 10/100/1000 LAN porty s tím, že licence na SSL VPN bude do 100 uživatelů.

Poznámka:
Cisco 3845 má dostatečný počet slotů pro další rozšíření portů, které mohou být využity v rámci redundance popřípadě jiného začlenění v rámci infrastruktury, popřípadě dalších vlastností souvisejících s technologií NAC

Autentikační manažer

Pro autentikaci jednotlivých „vzdálených“ uživatelů jsem vybral řešení od společnosti **RSA – SecureID Authentication,** protože jako jedno z mála řešení na trhu nabízí dvoufaktorovou autentizaci která je založena na něčem, co znáte (heslo nebo PIN) a něčem, co máte (autentizační předmět - token), což poskytuje mnohem spolehlivější úroveň uživatelské autentizace než pouhá hesla. Řešení RSA je jediné řešení, které mění automaticky heslo každých 60 vteřin. RSA je de-facto průmyslový standard pro autentikace uživatelů. Dalším důvodem bylo, že korektně probíhala komunikace s VPN koncentrátorem s verzí IOS 12.4. Například se směrovačem řady PIX se komunikaci nepodařilo korektně zprovoznit.

RSA Authentiacation manager bude implementován na stávajících technologiích serverů SUN/Solaris a bude poskytovat spolehlivou a evidovatelnou autentikaci pro všechny „vzdálené“ uživatele.

Poznámka:
Stejně jako v případě licenci SSL VPN bude i zde licence pro 100 uživatelů včetně 100 ks HW tokenů pro autentikaci.

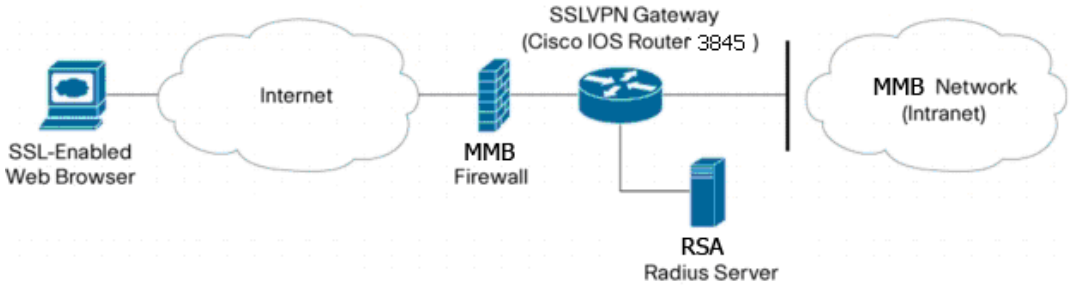
CiscoSecureDesktop (CSD)

CiscoSecureDesktop zajišťuje kontrolu integrity a správnosti hosta (vzdálené PC) tím, že kontroluje, zda-li má host správné a aktuální antiviry, service packy, firewally. CSD je schopen detekovat také „malware“ a povolit přístup pouze v případech, kdy je vše v pořádku.

CSD vytvoří virtuální desktop s CSD oddílem na disku, do kterého se ukládají veškerá data daného spojení včetně cookies, dočasných souborů, historie atd.- tato data jsou uložena kryptovaně (administrátor – 3DES, ostatní RC4), po odpojení je tento obsah smazán (splňuje pravidla U.S.Department of Defense – DoD)

5.2 POPIS KOMUNIKACE MEZI JEDNOTLIVÝMI PRVKY ŘEŠENÍ

Blokové schéma řešení



Obrázek 6.1: Blokové schéma rozšíření

Inicializace připojení se realizuje navštívením stránky se vzdáleného počítače vybaveného prohlížečem podporujícím SSL komunikaci. Navštívená stránka bude např. HTTPS://www.test.cz/ssl, na tento dotaz se vrátí okno s výzvou k přihlášení. Autentikace je zajištěna pomocí **uživatelského jména, PINu a tokenu.** Ověření se provádí na RSA serveru, kam VPN koncentrátor (SSLVPN Gateway) odesílá přihlašovací údaje s prázdnými dynamicky přidělovanými radius parametry pomocí RADIUS protokolu a očekává návrat údajů včetně doplnění o dynamické parametry.

Dynamické parametry jsou např. IP adresa, která bude přidělena při spuštění SVC, zda má uživatel právo ke spuštění tenkého (mapování portů) / tlustého klienta a na jaké služby bude mít přístup , jaké mu budou zobrazeny odkazy pro přístup na HTTP /HTTPS.

Zabezpečení lze zvýšit omezením zdrojových veřejných IP adres, ze kterých se inicializuje toto spojení. (Pokud je to žádoucí pro zvýšení bezpečnosti a pokud mají zamýšlené vzdálené strany statické adresy.)

5.3 NÁVRHY ŘEŠENÍ

5.3.1 Varianta vzdáleného přístupu 1 – přístup na port TCP 80, 443

Jedná se o vzdálený přístup pouze na port TCP 80, 443 (webové služby). Základními komponentami řešení je Cisco WebVPN technologie ve spolupráci s autentikačními technologie RSA (dvoufaktorová autentikace).

Řešení obsahuje:

Cisco WebVPN v konfiguraci „clietless SSL VPN“. Po úspěšném zalogování má uživatel k dispozici stránku s odkazy na servery z vnitřní sítě, které smí takto na dálku navštívit.

Zhodnocení:

Výhody:

Řešení je jednoduché, a přitom bezpečné, protože je zajištěna obousměrná kryptovaná komunikace a pro jednoznačnou autentikaci se používá HW token. Není vyžadováno žádné instalace a konfigurace na straně klienta neboť je využíván pouze webový prohlížeč - zvládne obsloužit každý, kdo používá Internet. Mezi další kladné vlastnosti patří rychlost, škálovatelnost a nízké náklady na řešení. Řešení zapadá do stávajících technologií na MMB a je možné ho kombinovat s Variantou vzdáleného přístupu 2,3 a 4 .

Nevýhody:

Řešení neprovádí kontrolu vzdálené stanice nicméně tímto typem přístupu nehrozí nákaza. Přístup je omezen jen na HTTP a HTTPS služby.

5.3.2 Varianta vzdáleného přístupu 2 – Přístup na služby nad TCP používající statické porty

Jedná se o vzdálený přístup pouze pro služby nad TCP protokolem a používající statické porty (například Telnet, SSH, POP3, IMAP nebo SMTP). Základními komponentami řešení je Cisco WebVPN technologie ve spolupráci s autentikační technologií RSA (dvoufaktorová autentikace).

Řešení obsahuje:

Cisco WebVPN v konfiguraci „thin-client SSL VPN“. Po úspěšném zalogování a kliknutí na odkaz „Thin Client Application“ se stáhne na klientskou stanici javovský applet, který umožní zabezpečený vzdálený přístup na TCP aplikace. Dále se uživateli zobrazí úvodní stránka s odkazem „Start Application Access“. Tento odkaz zobrazí uživateli tabulku překladu vnitřních adres a portů na lokální loopback a port. Samotné navštívení daného serveru a služby je potom realizováno právě přes lokální loopbackovou adresu a lokální port, o což se stará právě javovský applet.

Příklad: jeden řádek překladové tabulky může vypadat takto:

Intranet	127.0.0.1:3000	10.0.99.48:80

Samotné navštívení intranetu potom bude realizováno zadáním do prohlížeče 127.0.0.1:3000.

Stejně fungují další služby – Telnet, SSH, POP3, …

Zhodnocení:

Výhody:

Řešení je jednoduché, a přitom bezpečné, protože je zajištěna obousměrná kryptovaná komunikace a pro jednoznačnou autentikaci se používá HW token. Není

vyžadováno žádné instalace a konfigurace na straně klienta neboť je využíván pouze webový prohlížeč - zvládne obsloužit, kdo používá Internet. **Je však nutné mít nainstalováno SUN JRE 1.4 nebo vyšší a podporované OS jsou Win2000 a WinXP.** Mezi další kladné vlastnosti patří rychlost, škálovatelnost a nízké náklady na řešení. Řešení zapadá do stávajících technologií na MMB a je možné ho kombinovat s Variantou vzdáleného přístupu 1,3 a 4 .

Nevýhody:

Řešení neprovádí kontrolu vzdálené stanice nicméně tímto typem přístupu nehrozí nákaza. Uživatel stanice musí mít administrátorská práva. Připojení je omezené pouze pro TCP aplikace se statickými porty (UDP nepodporuje, nefunguje např. pro většinu FTP)

5.3.3 Varinata vzdáleného přístupu 3 – plnohodnotný přístup

Jedná se o plnohodnotný vzdálený přístup do vnitřní sítě MMB (na libovolného hosta z vnitřní sítě, na libovolnou povolenou službu. Základními komponentami řešení je Cisco WebVPN technologie ve spolupráci s autentikační technologií RSA (dvoufaktorová autentikace).

Řešení obsahuje:

Cisco WebVPN s použitím „SSL VPN Client“ (SVC). Po úspěšném zalogování a kliknutí na odkaz „Tunnel Connection“ se automaticky na klientskou stanici nainstaluje SVC a dojde k vytvoření SSL tunelu pro provoz, který se vyspecifikuje v konfiguraci tunelu. Ostatní provoz jde mimo SSL tunel. Uživatel dostane IP adresu z rozsahu VPN připojení s určitými právy. **V závislosti na typu uživatele se na tento rozsah navážou omezení, aby uživatel využíval pouze dovolené zdroje.**

Zhodnocení

Výhody

Řešení je jednoduché, a přitom bezpečné, protože je zajištěna obousměrná kryptovaná komunikace a pro jednoznačnou autentikaci se používá HW token. Není vyžadováno žádné instalace a konfigurace na straně klienta neboť je využíván pouze webový prohlížeč - zvládne obsloužit, kdo používá Internet. **Je však nutné mít nainstalováno ActiveX, podporované OS jsou Win2000 a WinXP.** Mezi další kladné vlastnosti patří rychlost, škálovatelnost a nízké náklady na řešení. Řešení zapadá do stávajících technologií na MMB a je možné ho kombinovat s Variantou vzdáleného přístupu 1,2 a 4 .

Nevýhody:

Řešení neprovádí kontrolu vzdálené stanice, při tomto způsobu připojení již může dojít k nákaze.

5.3.4 Varianta vzdáleného přístupu 4 - plnohodnotný přístup s ověřením klienta

Jedná se o plnohodnotný vzdálený přístup do vnitřní sítě MMB (na libovolného hosta z vnitřní sítě, na libovolnou povolenou službu. Na rozdíl od Variant 1-3 dochází k určitému ověřování klienta, čímž se zvyšuje bezpečnost propojení. Základními komponentami řešení je Cisco WebVPN technologie ve spolupráci s autentikační technologií RSA (dvoufaktorová autentikace) a dále Cisco Secure Desktop (CSD), který zajistí ověření a ochranu klienta. CSD lze chápat jako doplnění technologie WebVPN o metodu charakterizování klienta z hlediska důvěryhodnosti a na základě výsledku je tomuto klientovi umožněn vzdálený přístup metodou 1, 2 nebo 3.

Řešení obsahuje

Cisco WebVPN s použitím „SSL VPN Client“ (SVC) a Cisco Secure Desktop (CSD). Podporované OS na klientských stanicích jsou Win 2000 nebo XP. Stanice si po nastartování SSL relace a zprovoznění SVC klienta automaticky stáhne a nainstaluje CSD a použije IP adresu, specifické soubory, registrové klíče a

certifikáty k určení typu lokality, odkud se klient připojuje. Následuje autentikace CSD, která používá různá kritéria pro přidělování přístupových práv. Prověřuje se operační systém, antivirus (například datum posledního skenování), antispyware, personální firewall. Po připojení se vytvoří virtuální desktop s CSD oddílem na disku, do kterého se ukládají veškerá data daného spojení včetně cookies, dočasných souborů, historie atd.- tato data jsou uložena kryptovaně (administrátor – 3DES, ostatní RC4), po odpojení je tento obsah smazán. Je možné nastavit aby byl CSD po odpojení z PC automaticky odinstalován. Další z nastavení je, že uživatel smí používat pouze SW nainstalovaný v defaultní cestě OS Microsoft Windows – Program Files.

Instalace CSD na klientské straně je automatická a transparentní pro uživatele, zkouší se tyto způsoby (první, na který má uživatel oprávnění se použije): ActiveX, Microsoft, JVM Sun JVM, EXE

Podporované komponenty:

Prohlížeče:

- IE 6.0 – 7 (Beta)
- Netscape 7.x – 8
- Mozilla 1.7.x
- Mozilla Firefox 1.0.x – 1.5

E-mail klienti:

- Microsoft Outlook
- Microsoft Outlook Express
- Eudora
- Lotus Notes

Detekce systému pro:

- Antivirus
    - Avast AntiVirus (4.0)
    - AVG AntiVirus (7.1)

- eTrust Antivirus (7.0 to 2005)
- F-Secure Antivirus (2003 to 2005)
- McAfee VirusScan (8.0 to 10.0, Enterprise 7.0 to 8.0)
- Norton AntiVirus For Windows (Corporate 8.0 to 9.0, Professional 2004 to 2005)
- Panda AntiVirus (Titanium 2004 or Platinum 7.0 to 8.0)
- PC-cillin 2003 or 2004
- Trend Micro OfficeScan 7.0

- Antispyware
  - Microsoft Anti-Spyware
  - Anonymizer AntiSpyware
- Personální firewall
  - Cisco Security Agent (4.0 to 4.5)
  - Internet Connection Firewall (ICF) (Windows XP to XP SP2)
  - ISS BlackICE PC Protection (3.6)
  - McAfee Personal Firewall (4.0 to 5.0), Plus 2006 Version 7.0
  - Norton Personal Firewall (2003 to 2006)
  - Sygate Personal Firewall (5.0 to 5.6)
  - ZoneAlarm Personal Firewall (4.0 to 6.0)
- Service Pack
  - Windows XP Service Pack 2
  - Windows XP Service Pack 1
  - Windows XP (no service pack)
  - Windows 2000 Service Pack 4
  - Windows 2000 Service Pack 3
  - Windows 2000 Service Pack 2
  - Windows 2000 Service Pack 1
  - Windows 2000 (no service pack)

- Windows NT Service Pack 6
- Windows Millennium Edition
- Windows 98 Second Edition

Výhody:

Je zajištěna obousměrná kryptovaná komunikace a pro jednoznačnou autentikaci se používá HW token. Je prováděno prověření klientů a lze rozlišit typ a původ klientského HW Na základě ohodnocení klienta lze omezit přístup klienta do sítě – (pouze http přístup, omezený přístup přístupovými pravidly, plný přístup pomocí klienta). Přístup lze kombinovat s variantou 1,2 a 3.

Nevýhody:

Nevýhodami tohoto způsobu připojení je složitější práce. Dále prověření klientů není příliš dokonalé a je zde omezená podpora pro SW produkty

Toto řešení nebylo použito.

5.3.5 Varianta vzdáleného přístupu 5 - Cisco Network Admission Control

Toto řešení spadá do technologie Cisco Self-Defending Networks (CSDN). Její rozvedení a podrobné vysvětlení by bylo značně obsáhlé a je v této práci uvedeno spíše jako možný směr dalšího rozšíření zabezpečení vzdálených připojení.

Jedná se o komplexní „technologii“, která řeší bezpečný přístup ke zdrojům na celé síťové infrastruktuře (LAN,WAN, WLAN). Velmi zjednodušeně se dá říci, že NAC zajišťuje autentikaci, autorizaci, vyhodnocení a opravení klientské stanice tak, aby byl zajištěn bezpečný přistup do sítě. NAC mimo jiné zajišťuje:

- Kontrolu zabezpečení na základě uživatele, zařízení, operačního systému
- Blokuje, izoluje (karanténa), napravuje klienty

NAC se skládá ze 3 základních komponent:

- **Cisco Clean Access Server** – vynucuje ohodnocování klientů, dokud je neprověří, blokuje jejich provoz. Dimenzován dle počtu paralelně připojených uživatelů – 100, 250, 500, 1500, 2500
- **Cisco Clean Access Manager** – centralizovaná konsole (webová) pro správu rolí, pravidel, politik, pro nastavení Cisco Clean Access Serverů (dimenzováno dle počtu serverů – pro 3, 20, 40 serverů)
- **Cisco Clean Access Agent** – read-only agent, informuje Cisco Clean Access Server o stavu klienta, zdarma

NAC představuje v síťové problematice relativně novou dimenzi, která by měla zjednodušit a zabezpečit celou síťovou infrastrukturu. I když je NAC v současné době doménou Cisco Systems, podporu tomuto „průmyslovému standardu“ již ohlásili i další velcí výrobci.

V současné době je podporován pouze Cisco HW. Připravují se nové NAC appliance a také modul do Cisco IOS routeru (Cisco 3800).

Výhody:

Tento způsob představuje komplexní řešení a má smysl ho nasadit jen v plném rozsahu. Zahrnuje online komunikaci a zjišťování verzí virových databází, … Nabízí vysokou úroveň zabezpečení a je dobře škálovatelné

Nevýhody:

Nevýhodou je složité nasazení. Vyžaduje velké změny i v interní síti MMB (zavedení 802.1x, řešení nových problémů pro správce). Řešení je nákladné.

6. IMPLEMENTACE

Pro náš případ kdy potřebujeme vyřešit přístup mobilních zaměstnanců do vnitřní sítě MMB s přihlédnutím na požadované zajištění bezpečnosti a pravidel pro přístup k aplikačním prostředkům intranetu se ukázala být nejvhodnější právě kombinace navrhované varianty jedna a dva. Na uživatele jsou kladeny minimální nároky jak po stránce vědomostní tak na zásah na klientskou stanici. Tato varianta navíc umožňuje velice dobře rozdělovat kam a jakým způsobem bude mít daný uživatel přístup.

Před samotným postupem konfigurace jednotlivých prvků je nutné zmínit ještě některé názvosloví a technologie.

6.1 TECHNOLOGIE AAA

V dnešním světě musíme prakticky všechno chránit před zneužitím - a zároveň nic není zadarmo. Nezáleží přitom, jestli vystupujeme v roli systémového administrátora, manažera, studenta, nebo třeba konstruktéra sítí. Při přístupu k určitým službám přes počítačovou síť potřebujeme vždy tři věci:

- Autentizaci (ověření totožnosti)
- Autorizaci (stanovení oprávnění)
- Účtování (sběr informací)

Tyto komponenty se společně označují zkratkou AAA, která v angličtině vychází z výrazu *authentication, authorization and accounting* a často se zde vyslovuje jako „triple A". Každá z nich hraje v bezpečnosti sítě velmi důležitou roli, jak si nyní řekneme podrobněji.

6.1.1 Autentizace

Úkolem autentizace je zajistit, že daný uživatel sítě je skutečně tím, za koho se vydává. To je důležité, protože neoprávněným osobám samozřejmě přístup k síti nepovolujeme. Autentizaci zajišťuje obvykle sdílená (společná) tajná informace nebo důvěryhodná softwarová aplikace od jiného výrobce.

Pomocí autentizace může síťový administrátor také snadno poznat, kdo se přihlásil k síťovému zařízení či do Internetu, protože každý musí zadat své uživatelské jméno a heslo. Při vzdáleném připojení ke směrovači prostřednictvím služby telnet zadává uživatel normálně jen heslo do samotného směrovače; toto řešení je sice funkční, ale rozhodně není bezpečné, protože pokud je směrovač připojen k Internetu, může se o připojení pokoušet také útočník - a často si toho ani nevšimneme. Tomuto útočníkovi stačí totiž uhodnout jediné heslo; a myslíte si, že je to tak těžké, když má k dispozici tolik času?

jak se dozvíte, kdo to byl a jakou změnu provedl? S autentizací AAA musí každý uživatel při přihlášení zadat platné uživatelské jméno a heslo, přidělené od síťového administrátora. Následující ukázka tak podává příklad přihlášení vzdáleného uživatele ke směrovači Cisco pod autentizací AAA:

```
User Access Uerification
Username: tom thomas
Password: xxxxxxxx
MyCiscoRouter>
```

Jak vidíme, uživatel zde musel napsat platné uživatelské jméno a heslo. Databáze platných uživatelských jmen bývá zpravidla umístěna lokálně, na samotném směrovači, nebo na vzdáleném serveru zabezpečení.

6.1.2 Autrizace

S mechanismem autentizace souvisí také autorizace, která nastupuje po jejím úspěšném dokončení. U autentizovaného uživatele musíme totiž rozhodnout, jestli má oprávnění k provedení požadovaných operací. Jako běžný uživatel nebudeme mít například možnost přístupu ke všem souborům v systému. Autorizaci zajišťují přístupové seznamy (ACL) nebo zásady (politiky).

Pomocí autorizace tak administrátor kontroluje úroveň přístupu, kterou má uživatel po úspěšném přihlášení (získání přístupu) ke směrovači. Systém Cisco IOS Software zná určité úrovně přístupu neboli úrovně oprávnění (privilegií), které uživateli vymezují množinu povolených příkazů; uživatel s úrovní oprávnění 0 nemůže zadávat žádné příkazy systému Cisco IOS, zatímco uživatel s úrovní 15 může provádět naprosto všechny platné příkazy. Jednotlivé úrovně oprávnění může přidělovat místní (lokální) nebo vzdálený server zabezpečení. Aktuální úroveň oprávnění ve směrovači Cisco zobrazíme příkazem show privilege:

```
MyCiscoRouter>show privilege
Current privilege level is 15
MyCiscoRouter>
```

Autorizace může stanovovat také typy komunikačních aktivit a protokolů, které má uživatel povoleny; takto je například možné povolit jen provoz FTP, telnet nebo HTTP. Pamatujte si, že čím vyšší je úroveň oprávnění, tím více možností daný uživatel systému Cisco IOS má.

6.1.3 Účtování

Procesy účtování nastupují až po úspěšném dokončení autentizace a autorizace daného uživatele. Administrátor pomocí nich shromažduje informace o uživatelích, přihlášených k síťovým zařízením, a o jimi provedených operacích. Tyto informace pak mohou mimo jiné sloužit i jako právoplatný důkaz falšování, odposlechu či nabourání sítě, protože dostáváme jasnou „mapu" časových okamžiků vstupu uživatelů a jejich činnosti. Konkrétně se tak administrátor dozví, kdy se který uživatel přihlásil ke kterému směrovači, které příkazy systému IOS v něm zadával a kolik bajtů během své relace přenesl. Díky účtování může administrátor sledovat i změny konfigurace směrovačů. Zjištěné účetní informace se shromažďují přímo ve směrovači nebo ve vzdáleném serveru zabezpečení.

Pokud se k Internetu připojujete přes vytáčenou linku, dostanete se do styku s mechanismy AAA v okamžiku přihlášení (autentizace) a přijetí souhlasu (autorizace) v síti poskytovatele služeb. Účtování je pak proces, v němž poskytovatel sbírá informace o využití sítě; ty tvoří podklad nejen pro fakturaci, ale také pro plánování kapacit a další účely.

Po konfiguraci mechanismů AAA může v neoprávněném přístupu k síti bránit vhodný externí server zabezpečení, který pracuje nad externím bezpečnostním protokolem, jako je RADIUS nebo TACACS. Ve směrovačích Cisco je možné spustit oba zmíněné protokoly které si nyní popíšeme.

Rozhodneme-li se používat protokoly RADIUS či TACACS, určené pro servery zabezpečení, musíme také spustit mechanismy AAA. Na server zabezpečení se totiž odesílají právě informace, zjištěné v procesech AAA; v něm pak podléhají dalšímu zpracování.

6.2 PROTOKOL RADIUS (REMOTE AUTHENTICATION DIAL-IN USER SERVICE)

RADIUS je systém typu klient/server, jehož úkolem je zabezpečení sítě proti vetřelcům. Protokol RADIUS je implementován v systému Cisco IOS Software, kde odesílá autentizační požadavky na server RADIUS; tímto serverem je pak zařízení, na němž běží démon či aplikace RADIUS. Protokol RADIUS zajišťuje autentizaci, autorizaci a účtování vzdálených uživatelů vždy ve spojení s mechanismy AAA. Autentizace uživatele prostřednictvím serveru RADIUS probíhá následujícím způsobem:

1. Vzdálenému uživateli se vypíše výzva k zadání uživatelského jména a hesla.
2. Zadané uživatelské jméno a heslo se zašifruje a odešle se po datové síti.
3. Server RADIUS přečte uživatelské jméno a heslo, a buďto je přijme, nebo zamítne.

V některých případech může uživatele požádat o doplnění dalších informací (jedná se o takzvanou odpověď s výzvou); pokud například uživateli vypršela platnost hesla, vyzve jej server RADIUS k zadání nového.

Provoz mezi síťovým přístupovým serverem (Network Access Server, NAS) a serverem RADIUS není šifrován - na rozdíl od protokolu TACACS, který, přenos autentizačních zpráv šifruje

Server RADIUS je obvykle softwarová komponenta, která pracuje nad různými platformami, tedy například i na hostitelských systémech s MicrosoftWindows NT nebo s Unixem. Server RADIUS dokáže autentizovat uživatele směrovačů, autentizovat externí dodavatele, a dokonce ověřovat platnost cest v IP.

Takto zapneme protokol RADIUS na směrovači Cisco:

- Krok 1: Zadáme příkaz aaa new-model. Protokol RADIUS musí pracovat vždy ve spojení s AAA.
- Krok 2: Příkazem radius-server host určíme příslušný server RADIUS, jak vidíme v příkladu.

- Krok 3: Nakonec určíme heslo pro komunikaci mezi směrovačem a serverem RADIUS

Před aktivací služby RADIUS musíme samozřejmě také do serveru RADIUS zadat příslušná uživatelská jména a hesla

V příkladu vidíme konfiguraci směrovače Cisco, který bude uživatele autentizovat pomocí serveru RADIUS s hostitelskou adresou 10.99.34.50

Ukázka konfigurace protokolu RADIUS:

```
radius-server host 10.99.34.50
radius-server key <heslo>
```

6.3 PROTOKOL TACACS+ (TERMINAL ACCESS CONTROLLER ACCESS CONTROL SYSTÉM)

Protokol TACACS, který také spolupracuje s mechanismy AAA a je alternativou k protokolu RADIUS.

Systém Cisco IOS podporuje celkem tři verze protokolu TACACS: je to TACACS, rozšířený (extended) TACACS a TACACS+. Všechny tři metody zajišťují autentizaci uživatelů a odepírají přístup uživatelům, kteří nezadají platné uživatelské jméno a heslo.

První verze protokolu TACACS definuje jen jednoduchou verifikaci hesla a jednoduchou autentizaci. Účtování je zde omezeno jen na záznam požadavků a jejich odmítnutí. Druhá, rozšířená verze TACACS je náhradou této první verze. A konečně TACACS+ neboli TACACS plus poskytuje podrobné účtování a pracuje pouze s mechanismy AAA (jinými slovy, nejprve u něj musíme zapnout příkaz aaa new-model). TACACS+ tak svými funkcemi nahrazuje starší verze TACACS. Obecně tak TACACS představuje centralizovaný systém zabezpečení, který ověřuje uživatele při přihlášení z libovolného vzdáleného místa. Autentizace uživatele nad serverem TACACS probíhá následovně:

1. Vzdálenému uživateli se vypíše výzva k zadání uživatelského jména a hesla.
2. Zadané uživatelské jméno a heslo se odešle po datové síti a provede se jejich autentizace.
3. Server TACACS přečte uživatelské jméno a heslo, a buďto je přijme, nebo zamítne. V některých případech může uživatele požádat o doplnění dalších informací (jedná se o takzvanou odpověď s výzvou).

Odpověď s výzvou se může vypisovat například při chybách během autentizace. Verze TACACS+ vyžaduje ke své činnosti mechanismus AAA, ale původní TACACS ani rozšířený TACACS zapnuté AAA nevyžadují.

Postup při konfiguraci protokolu TACACS+ na směrovači Cisco:

- Krok 1: Zadáme příkaz **aaa new-model**. Protokol TACACS+ musí pracovat vždy ve spojení s AAA.
- Krok 2: Příkazem **tacacs-server host** určíme příslušný server TACACS.
- Krok 3: Určíme autentizační klíč pro komunikaci mezi směrovačem a serverem TACACS+.
- Krok 4: Protože protokol TACACS+ může pracovat jen ve spojení s mechanismy AAA, musíme zadat autentizaci, autorizaci a účtování TACACS+.

Ukázka konfigurace protokolu TACACS:

```
aaa new-model
aaa authentication enable default tacacs+

! Směrovač bude heslo oprávněného režimu autentizovat
! pomocí serveru TACACS

aaa authorization exec tacacs+

! Autorizace příkazů režimu EXEC v lokálním směrovači bude probíhat
```

! nad protokolem TACACS+

```
aaa accounting exec start-stop tacacs+
```

! K příkazům režimu EXEC se budou shromažďovat účetní informace

```
tacacs-server host 10.99.34.50
tacacs-server key <heslo>
```

Tento příklad uvádí jen základní konfiguraci protokolu TACACS+ pomocí dalších konfiguračních voleb můžeme zadat také složitější příkazy mechanismu AAA.

Pozn:

Po zapnutí mechanismu AAA můžete při troše neopatrnosti velice snadno "vyhodit" sebe sama; jestliže třeba zadáte nějaký příkaz narychlo a vyskočíte z konfigurace, nemusí se vám už podařit znovu vstoupit do stejného režimu.

6.4 TACACS+ NEBO RADIUS?

Porovnáme-li oba výše popisované serverové protokoly, RADIUS a TACACS+, snadno zjistíme, že oba ke své činnosti vyžadují na směrovači Cisco zapnutí mechanismů AAA (s výjimkou starších verzí TACACS a rozšířeného TACACS), a oba vyžadují od uživatele zadání platného uživatelského jména a hesla. Rozdíl spočívá jednak v samotné konstrukci protokolu, a jednak v tom, že TACACS+ představuje centralizovanou ověřovací neboli validační službu, zatímco RADIUS je postaven na technologiích klient/server.

6.5 KONFIGURACE JEDNOTLIVÝCH KOMPONENT ŘEŠENÍ

Konfigurace WEB VPN brány realizované Cisco směrovačem 3845
Viz. Příloha 1

Konfigurace RADIUS serveru – verze od RSA pro konfiguraci RSA tokenů
Viz. Příloha 2

Konfigurace klientské části s návaodem k použití
Viz Příloha 3

7. ZÁVĚR

Úkolem práce bylo realizovat zabezpečené připojení mobilních uživatelů do sítě MMB bez nutnosti složité konfigurace klientských počítačů. Pro pochopení celé problematiky a porozumění možným konfiguracím a způsobům nasazení Virtual Private Network (VPN) jsem se v první části práce věnoval seznámení s jednotlivými protokoly, algoritmy a způsoby nasazení VPN. V další části se už zabývám přímo komponenty a SSLVPN technologií použitou pro vyřešení daného úkolu. Jsou zde uvedeny jednotlivé způsoby přístupu do sítě MMB přičemž každý nabízí specifické vlastnosti využití, které se dají velice dobře aplikovat na různé okruhy uživatelů. Jejich kombinací lze dosáhnout optimálního výsledku podle potřeb administrátorů na zabezpečení, zručnosti uživatelů a jim nabízených možností. V mém případě je používána kombinace prvních tří variant čemuž odpovídá i konfigurace a nastavení uvedené v poslední části práce.

Mezi jednu z nejnáročnější části celého řešení patřilo nalezení vhodného hardwaru korektně komunikujícího s RSA serverem. Při řešení daného úkolu vyvstal problém ve vzájemné spolupráci mezi směrovači řady PIX a RSA serverem. Místo směrovače řady PIX bylo třeba použít směrovače Cisco řady 1800 s verzí IOS 12.4. Další náročnou částí bylo odzkoušení a nalezení způsobu, jakým předávat radius parametry mezi RSA serverem a SSLVPN bránou, protože tvar syntaxe a přiřazování jednotlivých parametrů je velice špatně dokumentován.

Pro úspěšné zvládnutí úkolu jsem tedy musel najít vhodný směrovač a provést jeho konfiguraci ve funkci SSLVPN brány. Při konfiguraci se vyskytly potíže s webovým nástrojem pro konfiguraci, a bylo ji nutné provést přes konsolový interface. Následně jsem provedl konfiguraci RSA serveru a našel vhodný formát radius parametrů pro komunikaci se směrovačem. V poslední fázi implementace byly umístěny jednotlivé tokeny na RSA server a přiřazeny uživatelům. Po dokončení implementace VPN sítě bylo provedeno zaškolení uživatelů jak s novým nástrojem pracovat.

8. SEZNAM POUŽITÉ LITERATURY

[1] THOMAS, M. *Zabezpečení počítačových sítí bez předchozích znalostí*, 2005, ISBN: 80-251-0417-6

[2] PUŽMANOVÁ, R. *Bezpečnost bezdrátové komunikace Jak zabezpečit Wi-Fi, Bluetooth, GPRS či 3G*, 2005, ISBN: 80-251-0791-4

[3] ONDŘEJ, Š. *Don´t find fault, find a remedy* [online], 2007, poslední revize 18.05.2007. Dostupné z: <http://www.sevecek.com/index.php?id=15>.

[4] *Webopedia* [online], 2007, poslední revize 27.06.2001. Dostupné z: <http://www.webopedia.com/TERM/P/PPTP.html>

[5] HABRMAN, R. *Síťové protokoly (XXV. část), Protokol L2TP* [online], 2007, poslední revize 25.04.2008. Dostupné z: <http://www.owebu.cz/pc-site/vypis.php?clanek=1600>

[6] PRůCHA, O. *Vše co jste chtěli vědět o VPN, ale báli jste se zeptat* [online]. 2005, Dostupné z: <http://home.zcu.cz/~ondrous/>

[7] *SVĚT SÍTÍ* [online].2007. Dostupné z: <http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=219>

[8] *SVĚT SÍTÍ* [online].2007. Dostupné z: <http://www.svetsiti.cz>

[9] *CISCO* [online].2007. Dostupné z: <http://www.cisco.com>

[10] *WIKIPEDIA.COM, The Free Encyklopedia* [online].2007. Dostupné z: <http://en.wikipedia.org/wiki/Main_Page>

[11] *WIKIPEDIA.CZ, Otevřená encyklopedie* –[online].2007. Dostupné z: <http://cs.wikipedia.org/wiki/Hlavn%C3%AD_strana>

SEZNAM PŘÍLOH

Příloha 1

Konfigurace WEB VPN brány – realizovaná Cisco směrovačem 3845

Pro autentifikaci uživatelů je použita varianta vzdálené autentifikace s využitím protokolu RADIUS. Autorizace je v konfiguraci Cisco směrovače nedílnou součástí AAA, což v sobě navíc zahrnuje i autentifikaci a účtování. Konfigurace takové autorizace je uvedena níže:

```
aaa new-model

aaa group server radius AAA_SRV
server-private 192.168.99.8 auth-port 1812 acct-port
1813 key 7 095A5E07260E1B1B08090F
!
aaa group server tacacs+ ACCOUNTING
 server 192.168.88.11
!
tacacs-server host 192.168.88.11 key 7 010703174F
!
ip radius source-interface GigabitEthernet0/1
 ip tacacs source-interface Loopback100
!
aaa authentication login default local
aaa authentication login SSLVPN group AAA_SRV
aaa authentication login IPSECVPN local
aaa authorization network IPSEC_AUTHOR local
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo
aaa accounting exec default start-stop group ACCOUNTING
aaa accounting commands 1 default start-stop group
ACCOUNTING
aaa accounting commands 15 default start-stop group
ACCOUNTING
```

```
aaa accounting network default start-stop group
ACCOUNTING
aaa accounting connection default start-stop group
ACCOUNTING
aaa accounting system default start-stop group
ACCOUNTING
```

Jelikož se jedná o komunikaci na bázi SSL, tak je nutné vygenerovat certifikát a nebo navést certifikát vygenerovaný a podepsaný certifikační autoritou. Zde je ukázáno navedení certifikátu:

```
crypto pki trustpoint brno_ca
enrollment terminal pem
fqdn vpn.test.cz
subject-name CN=vpn.test.cz
revocation-check none
rsakeypair VPN_KEY_2007_10_09
!
crypto pki certificate chain brno_ca
certificate 1888B0959386921A
308203A7 3082028F A0030201 02020818 88B09593 86921A30
0D06092A 864886F7 …
     … 0D010105 05003031 31133011 06035504 03130A4D
96CEEDCE 003D6068 BA9C3039 BAC79196 AB19314F 7D606221
DA36C751 CAD81B20
81EFCF48 05B22D85 836D6C
     quit
```

Pro připojení plným klientem je potřeba klientovi přiřadit IP adresu z tzv. IP poolu, který je nakonfigurován na směrovači:

```
ip local pool omi_wagner 192.168.30.13 -
```
pouze pro 1 uživatele

```
ip local pool dais 192.168.50.1 192.168.50.7-
```
až pro 7 užovatelů

Po připojení uživatele plným klientem lze omezit jejich provoz access-listem. Ten se přiřazuje dynamicky po přihlášení - RADIUS serverem příslušným atributem.:

```
ip access-list extended omi_wagner
permit tcp host 192.168.30.13 host 192.168.53.82 eq 3389
permit igmp host 192.168.30.13 host 224.0.0.22
deny   ip any any log


ip access-list extended dais
permit ip 192.168.50.0 0.0.0.7 192.168.10.0 0.0.0.255
permit udp 192.168.50.0 0.0.0.7 host 192.168.88.11 eq
domain
permit udp 192.168.50.0 0.0.0.7 host 192.168.88.15 eq
domain
permit igmp 192.168.50.0 0.0.0.7 host 224.0.0.22
deny   ip any any log
```

Samotná konfigurace brány je realizovaná těmito příkazy:

`webvpn gateway MMB_Gateway`	-	pojmenování brány
`hostname vpn.test.cz`	-	jméno, uvedené v certifikátu
`ip address 192.168.34.11 port 443`	-	adresa a port brány
`ssl trustpoint brno_ca`	-	přiřazení (profilu) certifikátu
`logging enable`	-	zapnutí logování
`inservice`	-	zapnutí brány

V rámci jedné brány lze konfigurovat více kontextů – lze si pod tím představit něco, jako doménu. Každý kontext má svůj vlastní design stránky pro přihlášení a do každému kontextu spadají uživatelé. Ti jsou na RADIUS serveru zavedeni včetně kontextu. Podle toho RADIUS server rozpoznává, který uživatel se může přihlásit do kterého kontextu. Následuje ukázka konfigurace dvou kontextů s příslušnými politikami.

```
webvpn context omi                    -    název kontextu
login-photo file flash:Petrov.jpg          - obrázek na
                                             přihlašovací stránce

color #990000
secondary-color white
title-color #CCCC66
text-color black
ssl authenticate verify all
```

Nachystání zpřístupnění lokálního http / https serveru z přístupové brány – po přihlášení uživatele. Typickým příkladem použití může být intranet.

```
url-list "omi_wagner"
url-text "Intranet" url-value "http://intranet.brno.cz"
```

Nachystáni konfigurace pro tenkého klienta, jeho použití je konfigurováno v rámci politiky daného kontextu.

```
port-forward "omi_wagner"
local-port 3000 remote-server "192.168.53.82" remote-
port 3389 description "RDP"
local-port 3001 remote-server "192.168.53.82" remote-
port 22 description "SSH"
local-port 3002 remote-server "192.168.53.82" remote-
port 80 description "E-Mail"
```

```
policy group omi_wagner
  url-list "omi_wagner"          -   použít předkonfigurovaný url list
  port-forward "omi_wagner"      -   použít tuto konfiguraci tenkého
                                     klienta
  functions svc-enabled          -   povolit možnost přístupu
                                     plným klientem (SVC)
  hide-url-bar                   -   zakázání prohlížení internetových
                                     stránek z brány
  timeout idle 0
  timeout session 86400          -   timeout spojení
  svc address-pool "omi_wagner"  -   IP adresa, kterou dostane
                                     klient po připojení SVC
  svc keep-client-installed      -   zachovat instalaci SVC po
                                     odpojení
  svc split include 192.168.53.82 255.255.255.255-
                                     směrovací tabulka pro SVC –
                                     přidání cesty do směrovací
                                     tabulky, po připojení SVC bude
                                     do tunelu směrován pouze tento
                                     provoz

webvpn context dais
 login-photo file flash:Petrov.jpg
 color #990000
 secondary-color white
 title-color #CCCC66
 text-color black
 ssl authenticate verify all

policy group dais
```

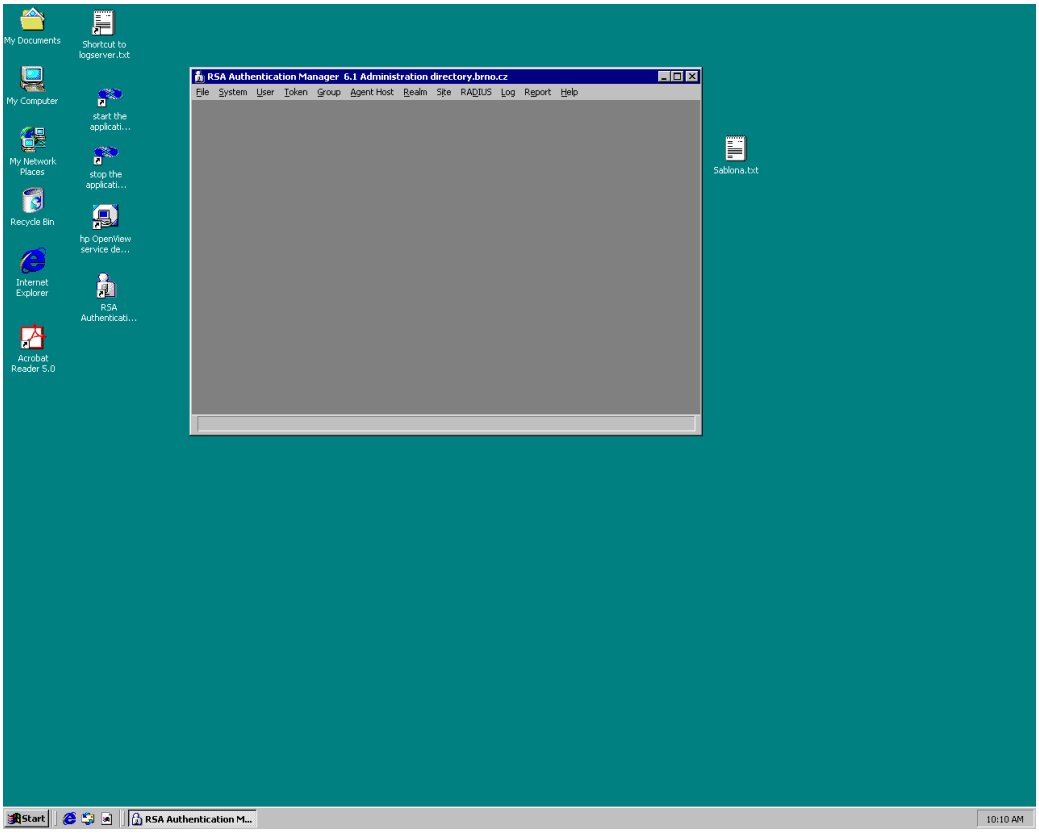
```
functions svc-enabled
hide-url-bar
timeout idle 0
timeout session 86400
svc address-pool "dais"
svc keep-client-installed
svc split dns "brno.cz"
svc split include 192.168.88.15 255.255.255.255
svc split include 192.168.88.11 255.255.255.255
svc split include 192.168.10.0 255.255.255.0
svc dns-server primary 192.168.88.11
svc dns-server secondary 192.168.88.15
default-group-policy dais_default
aaa authentication list SSLVPN
aaa authentication domain @dais
aaa accounting list ACCOUNTING
gateway MMB_Gateway domain dais
logging enable
inservice
```

Příloha 2

Konfigurace RADIUS serveru – verze od RSA pro konfiguraci RSA tokenů

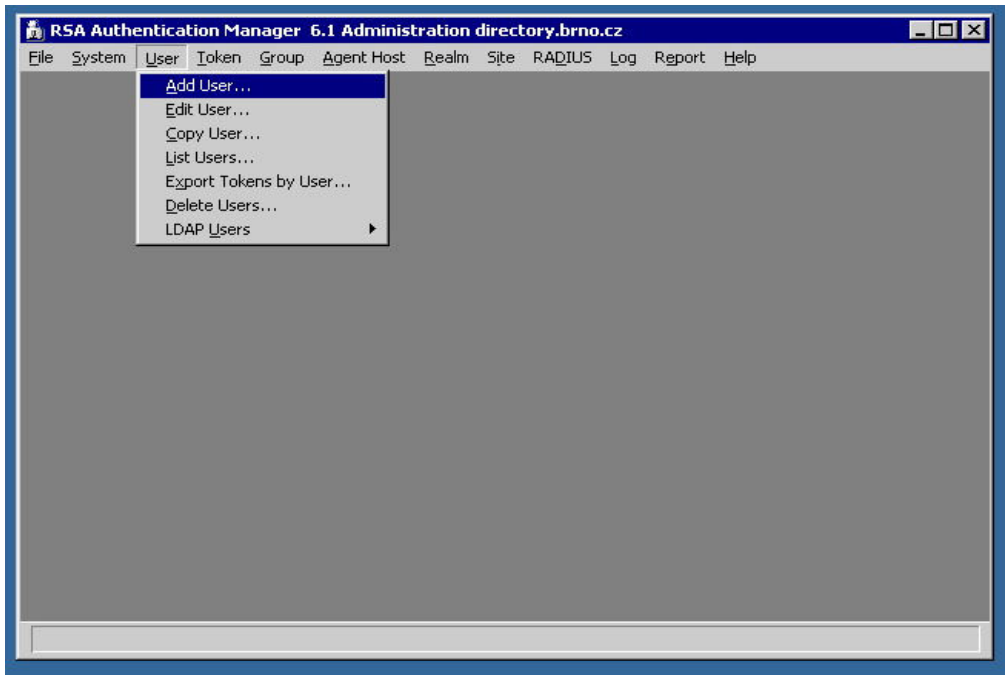
Celý management RSA serveru je realizován pomocí RSA Authentication Manageru ve verzi 6.1. Tento poskytuje kromě základních funkcí jako administrace uživatelů, tokenů a konfigurace s tím spojené i některé další užitečné informace statistického charakteru. Nejdůležitější funkce si nyní ukážeme:

Spuštění RSA Authentication Manageru 6.1



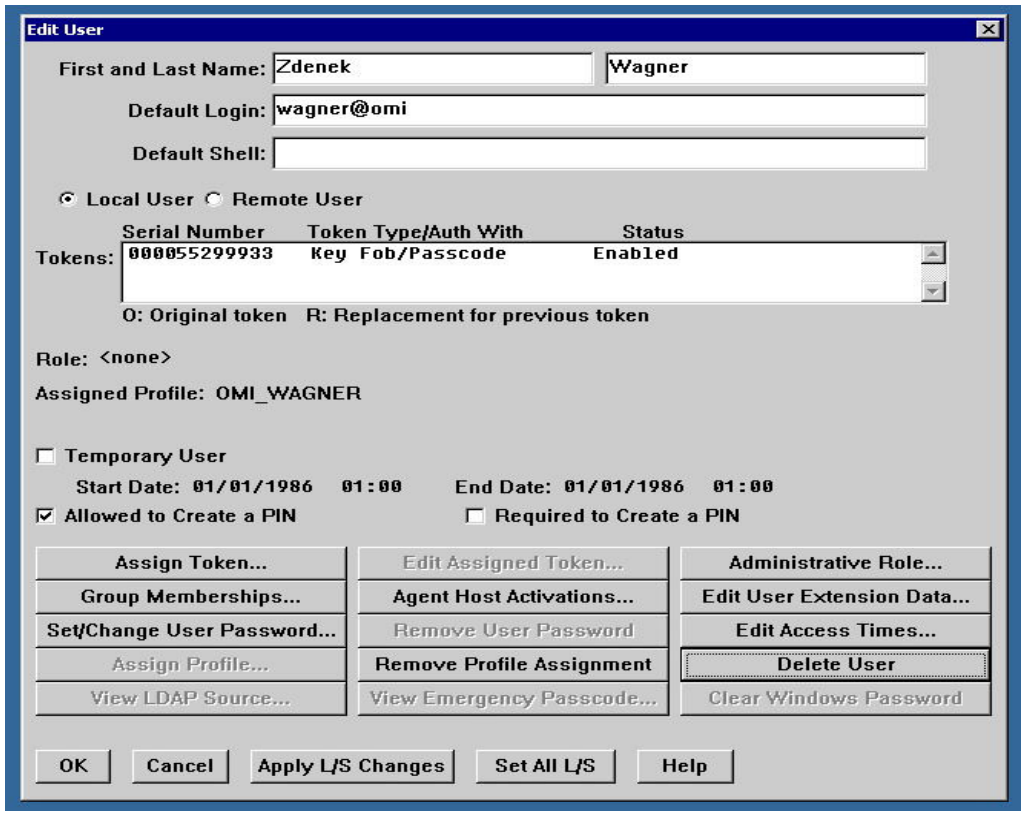
Obrázek 9.1: Úvodní obrazovka RSA Authentication Manager

Vytvoření uživatele:



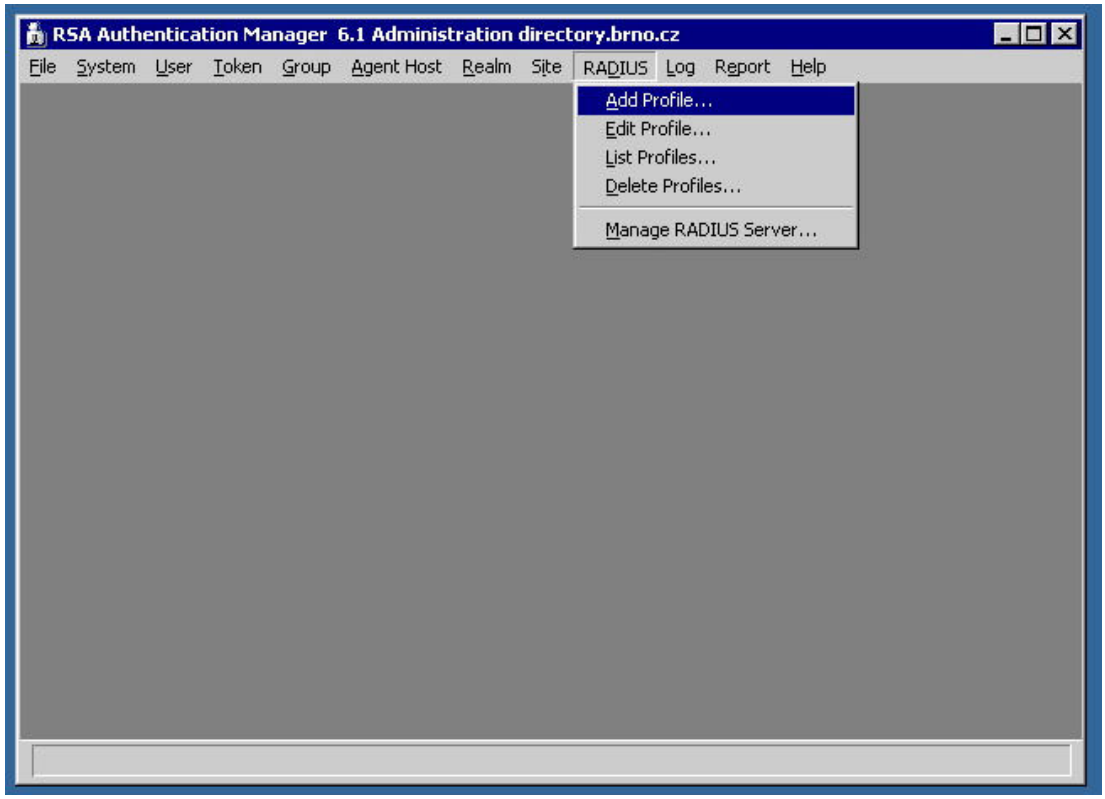
Obrázek 9.2: Vytváření uživatele

Vyplnění informací o uživateli:

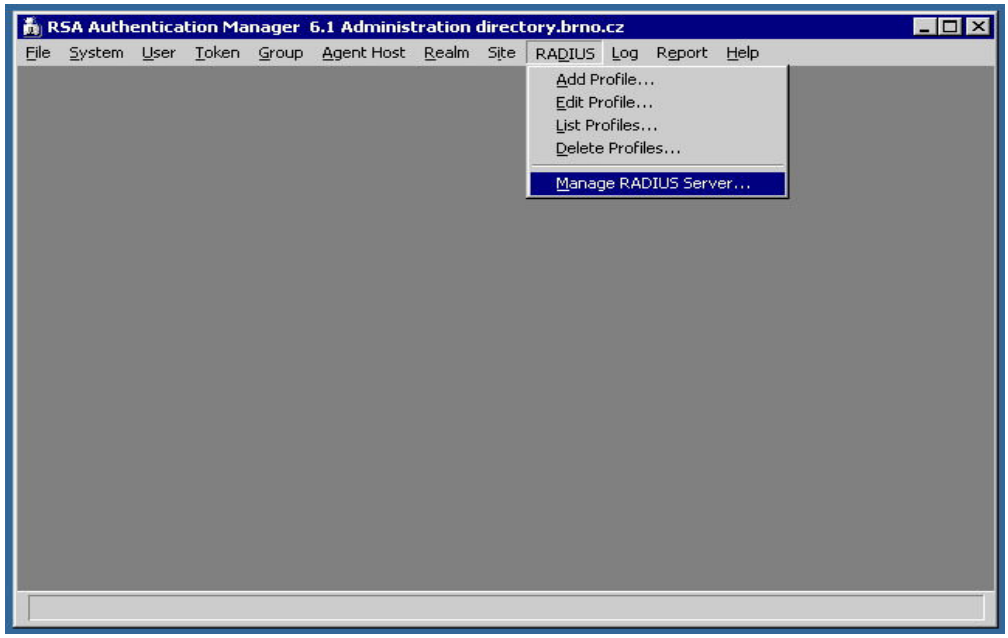


Obrázek 9.3: Vytváření uživatele - detail

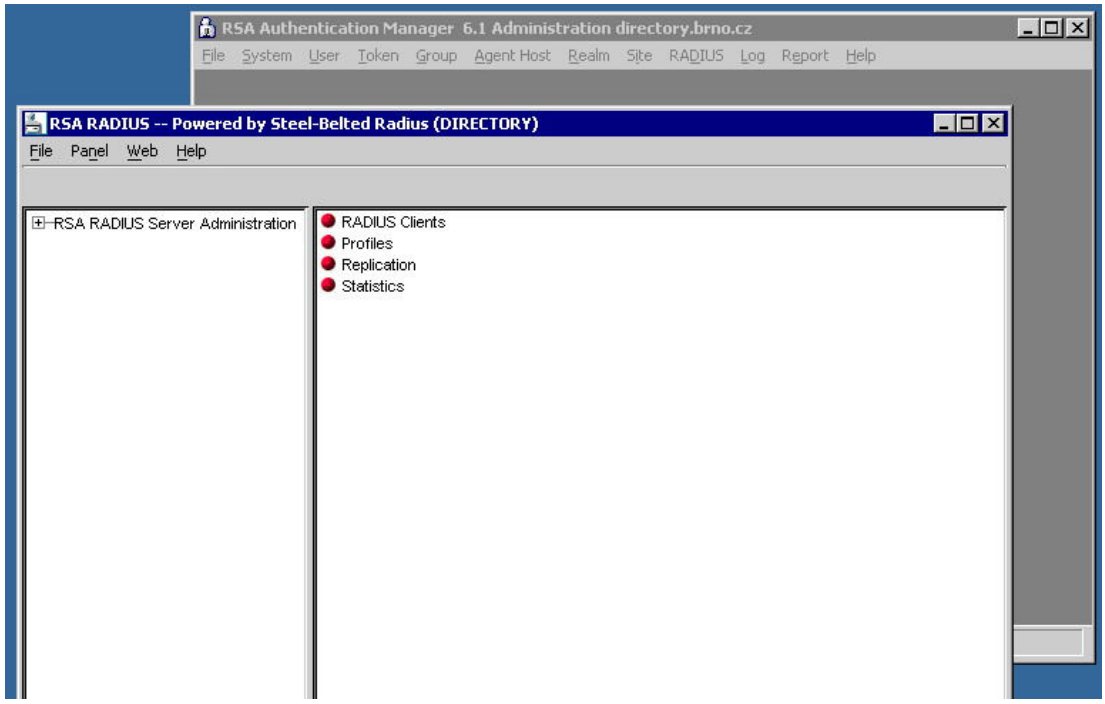
Vytvoření profilu – je potřeba jakoby vytvořit profil na dvakrát ale v tomto menu se vytváří jen názvy. K provázání dojde až po vytvoření profilu shodného jména v menu Manage RADIUS Server.



Obrázek 9.4: Vytváření profilu

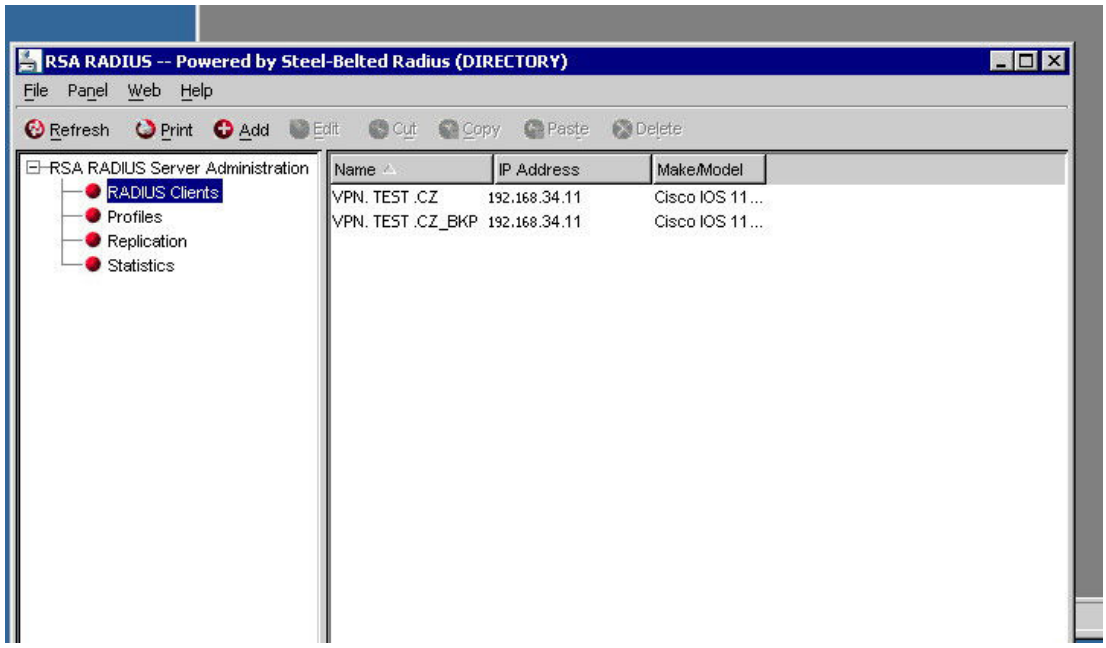


Obrázek 9.5: Vytváření profilů_Manage



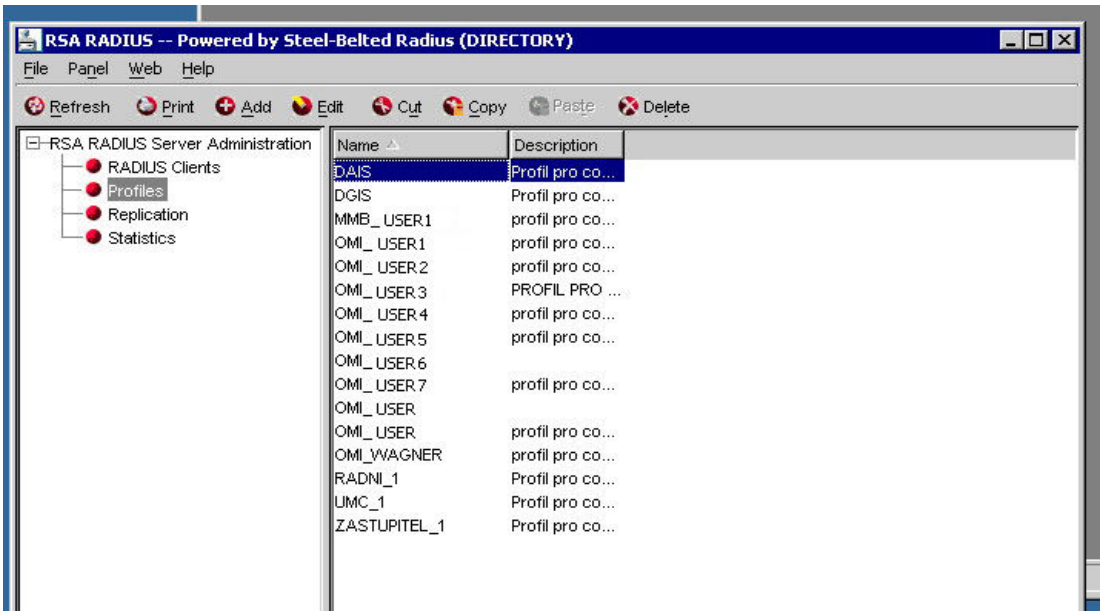
Obrázek 9.6: Menu-Manage RADIUS Server

Radius clients – definice kdo se může doptat radius serveru na autorizaci. (S jinymi směrovači tento radius nekomunikuje – neodpoví na dotaz.)



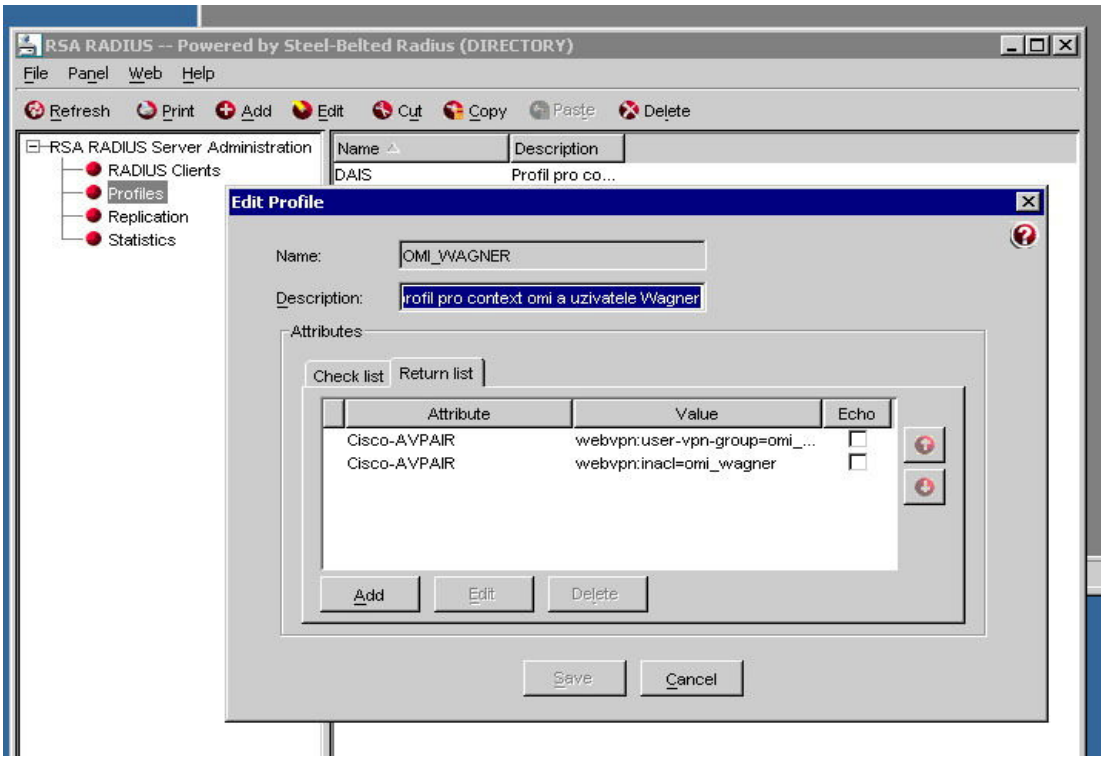
Obrázek 9.7: RADIUS Clients

Zmiňované opětovné vytváření profilu se shodným názvem.



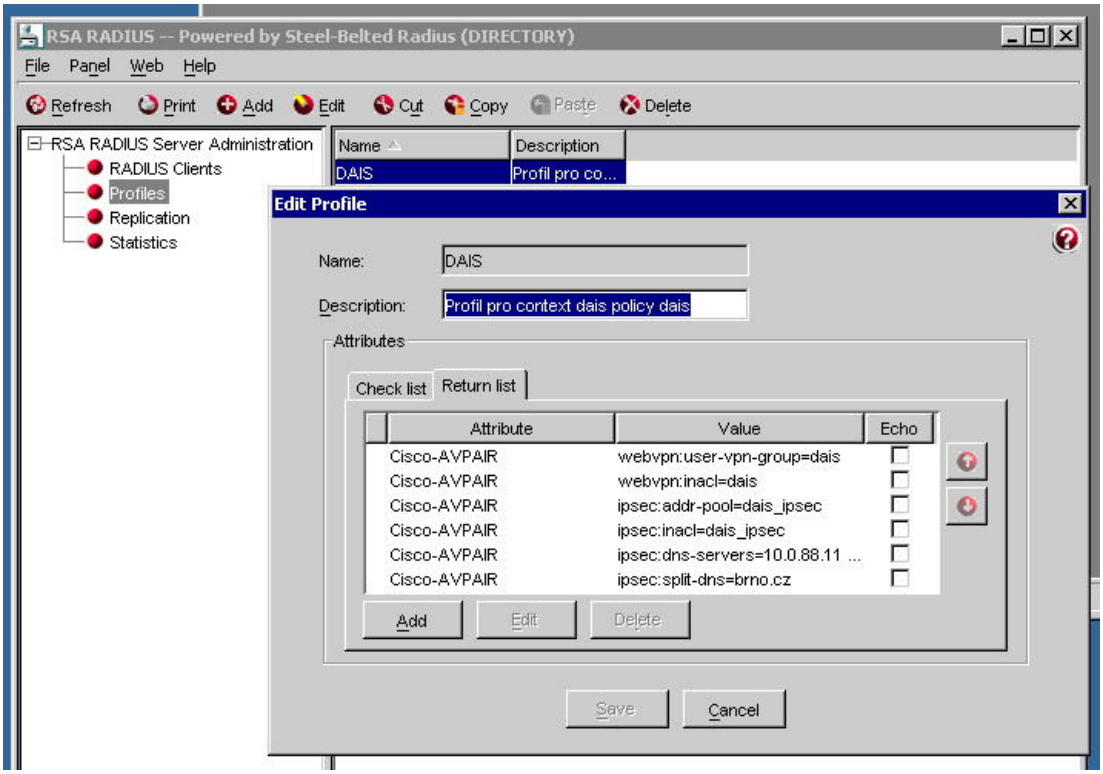
Obrázek 9.8: Vytváření profilu k provázání

Při vytváření profilu se zadávají RADIUS parametry (kontext, ACL) které mají být vráceny na bránu při úspěšném ověření uživatele.



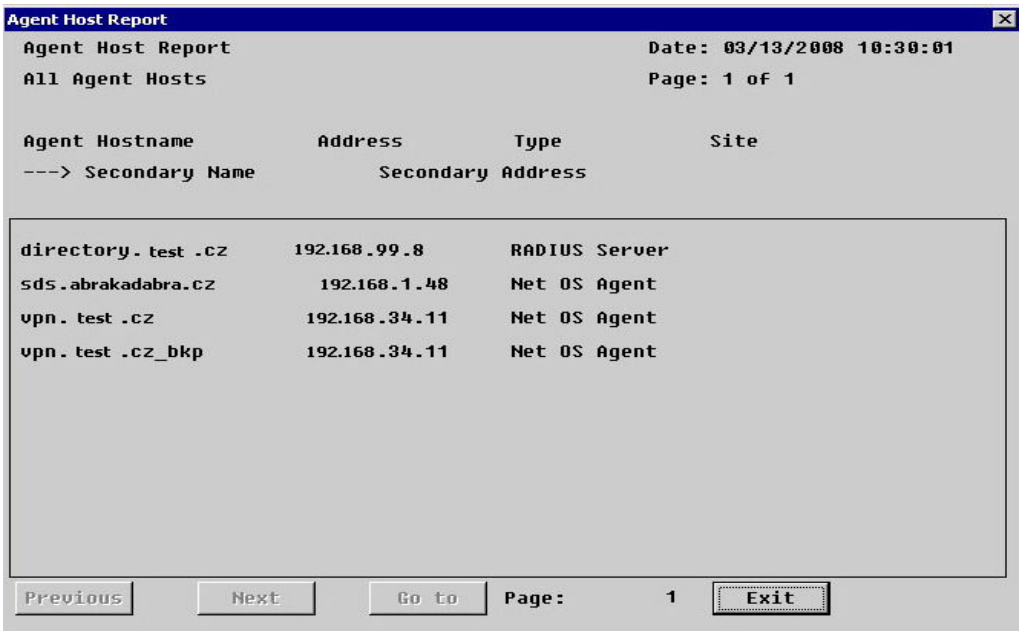
Obrázek 9.9: Editace profilu uživatele

Opět vytváření profilu uživatele s větším množstvím parametrů – skupina uživatelů, více nastavení...



Obrázek 9.10: Editace profilu uživatele – skupina

Přehled služeb a zařízení kterými RADIUS server komunikuje

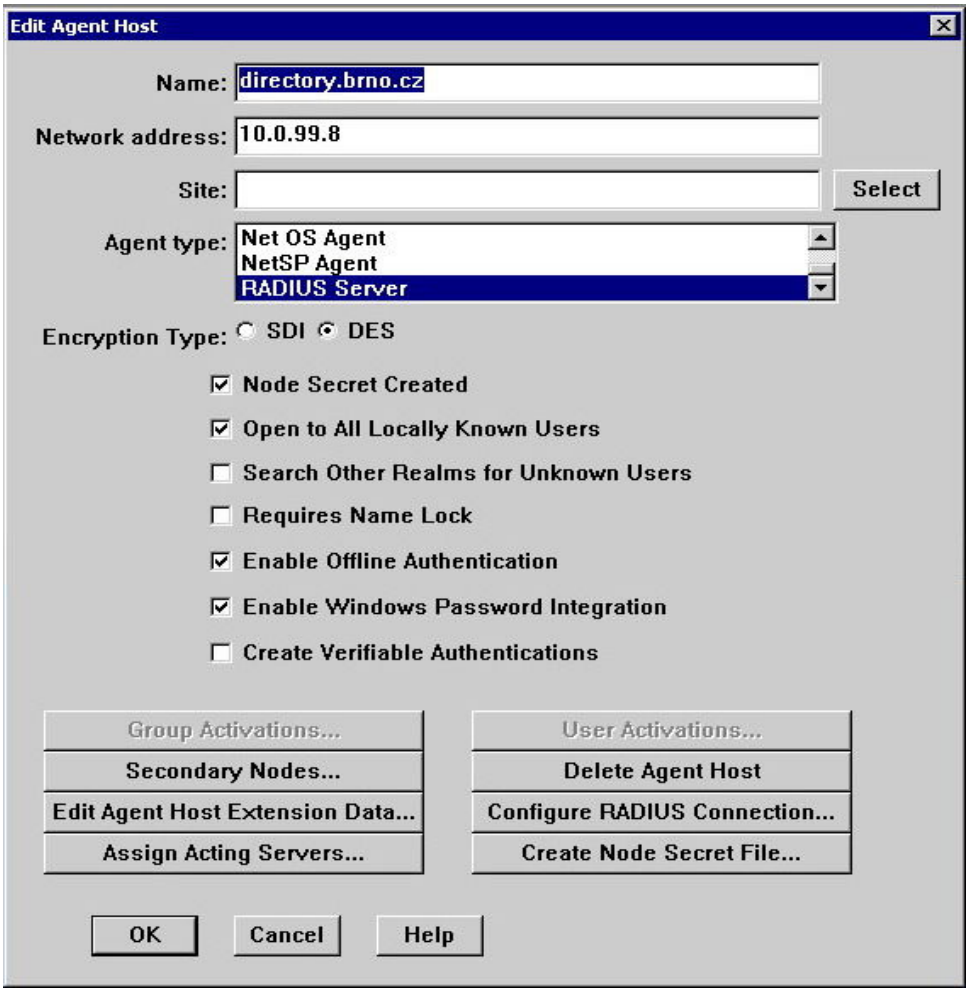


Obrázek 9.11: Přehled služeb a zařízení

Přídání zařízení a služby s kterou bude RADIUS server komunikovat

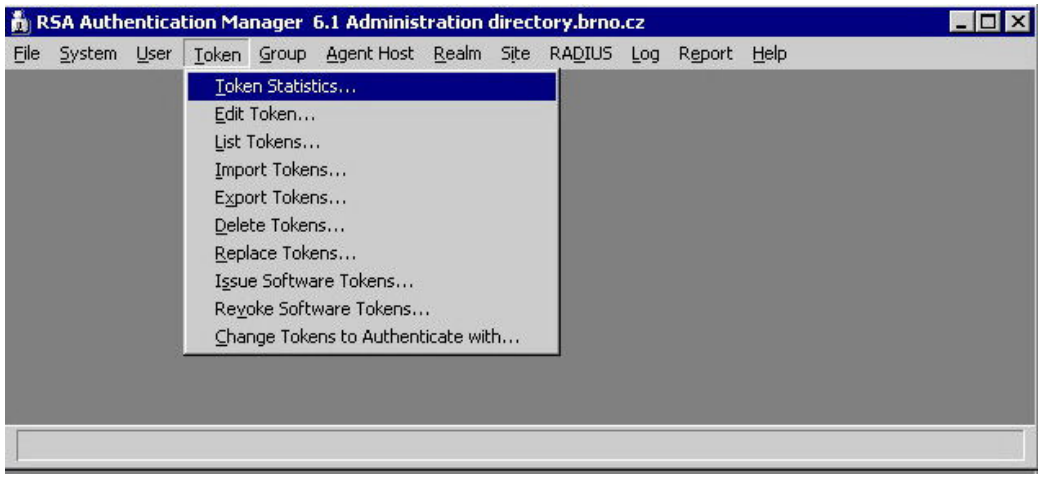
Obrázek 9.12: Přídání zařízení a služby

Detailní pohled na přidání služby a zařízení



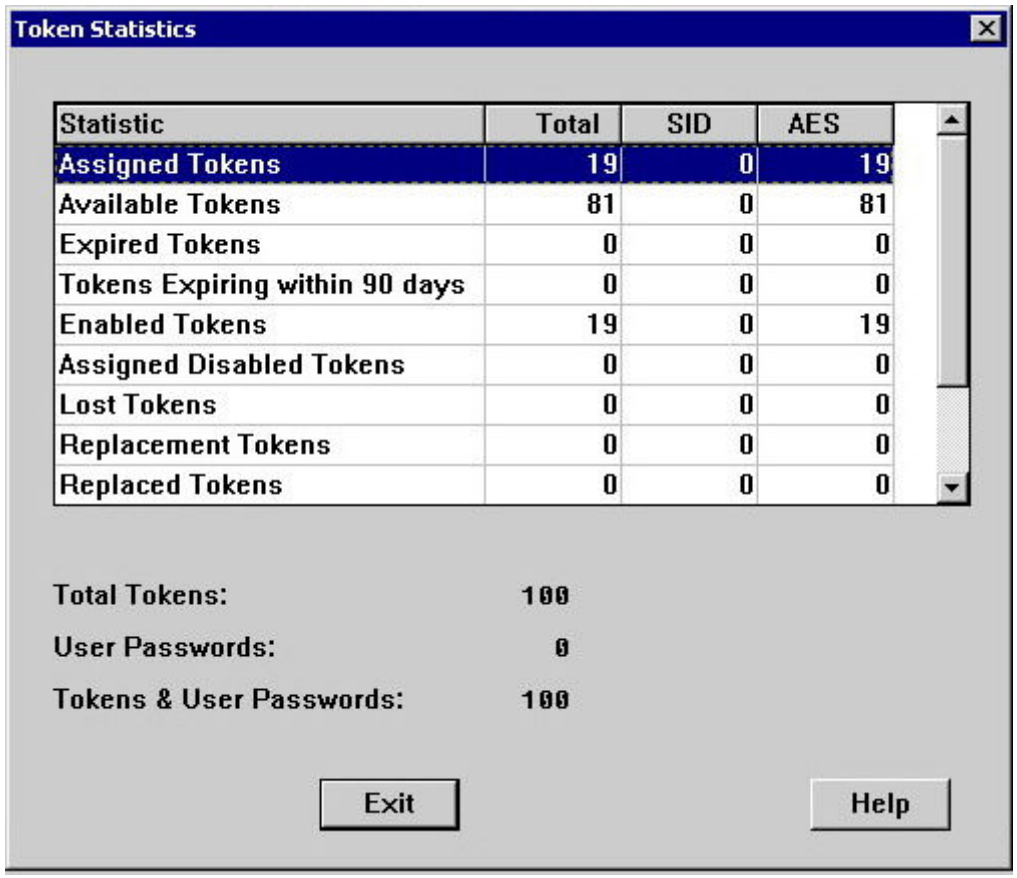
Obrázek 9.13: přídání služby a zařízení – detail

Statistika tokenů



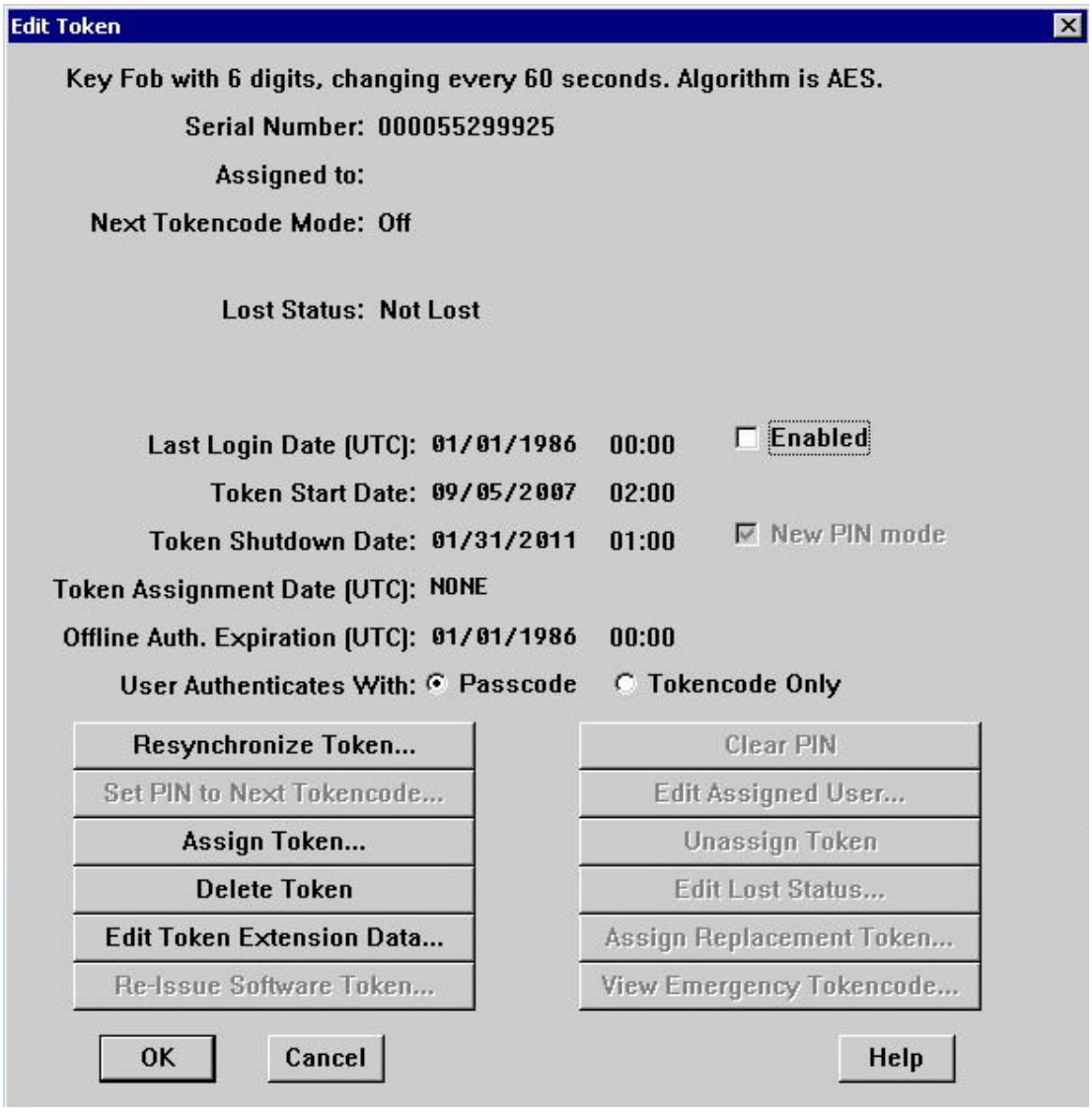
Obrázek 9.14: Statistika tokenů

Statistika tokenů – detail



Obrázek 9.15: Statistika tokenů - detail

Editační okno tokenu

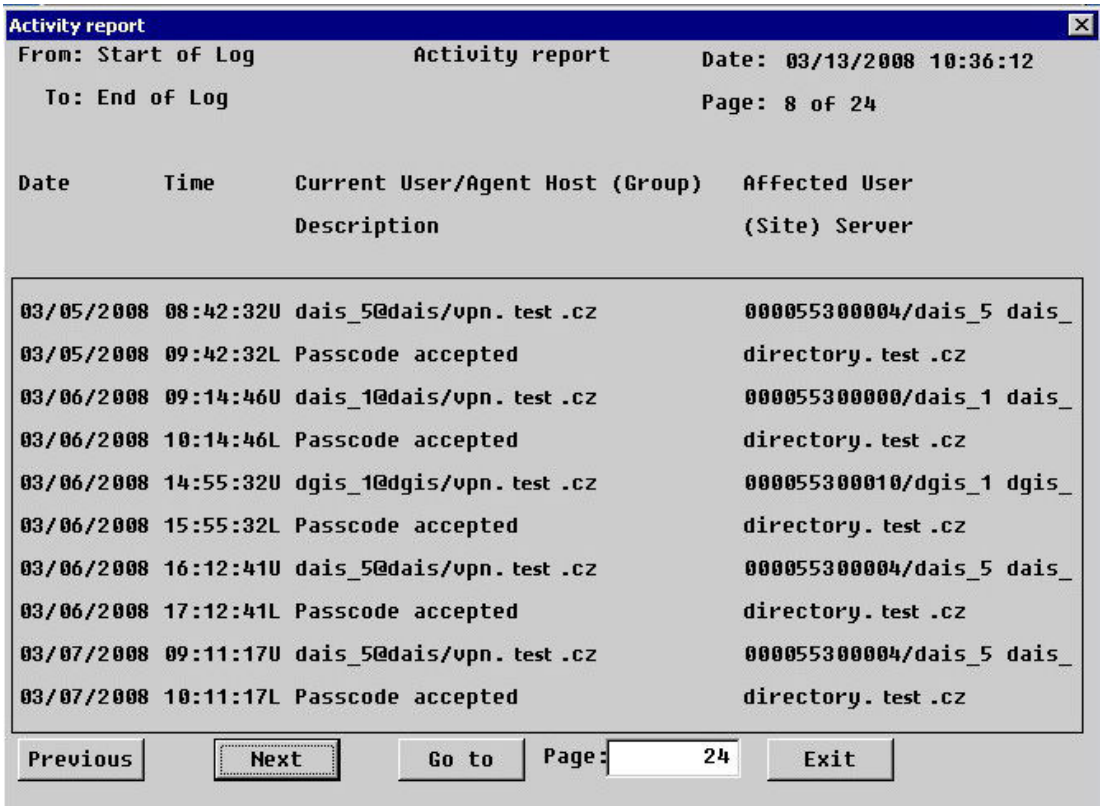


Obrázek 9.16: Editační okno tokenu

Activity log

Obrázek 9.17: Activity log

Activity log detail



Obrázek 9.18: Activity log detail

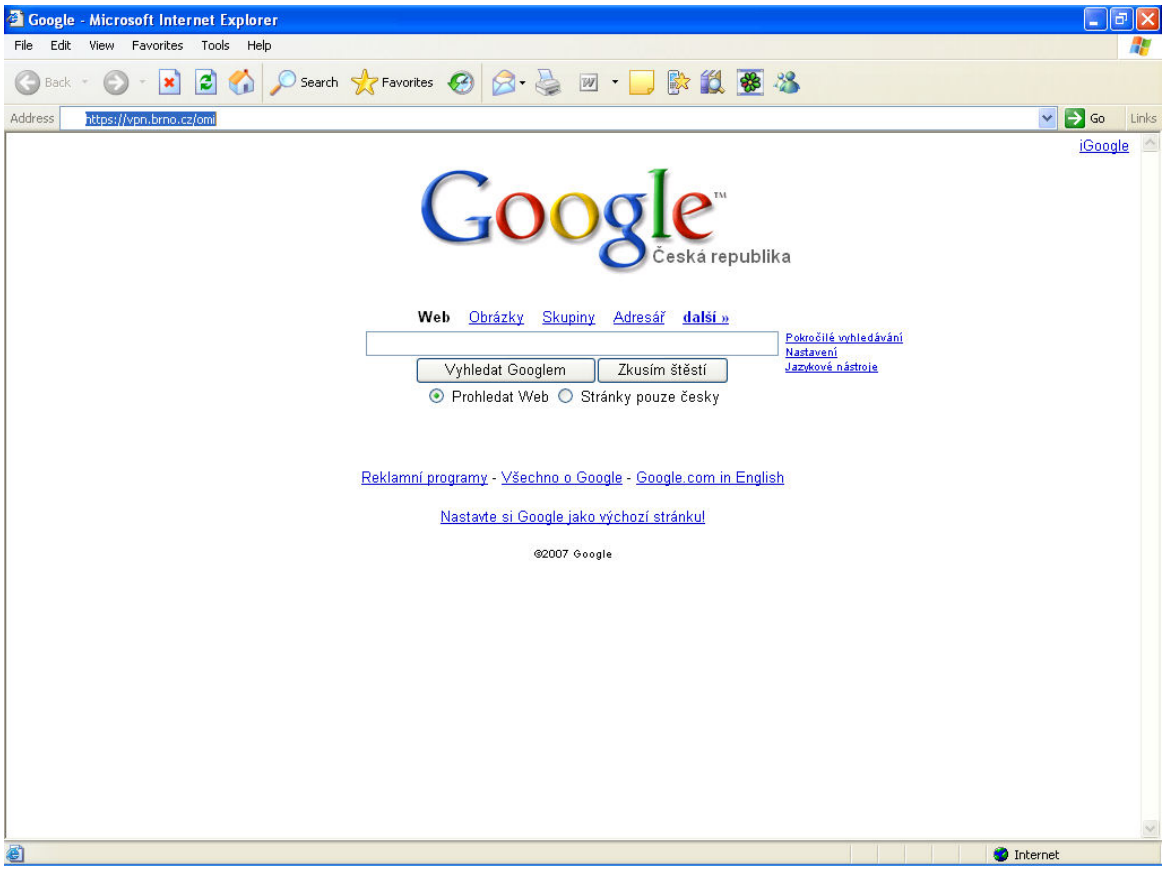
Příloha 3

Konfigurace klientské části – použití

Každý uživatel vzdáleného přístupu do sítě MMB má své uživatelské jméno, PIN, RSA token a spadá do jednoho contextu (například radni, zastupitel, omi, umc, ...).

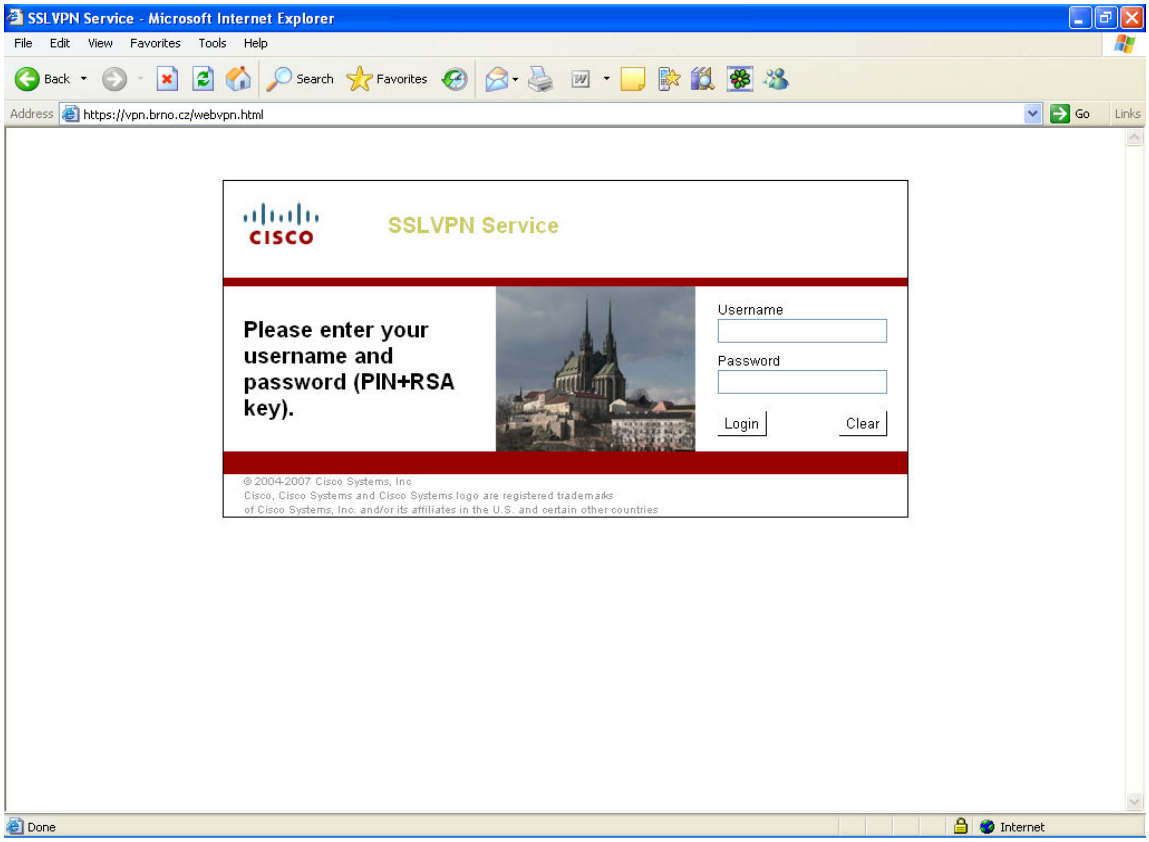
Přihlášení pro přístup do sítě MMB je přes odkaz ve formátu:

https://vpn.test.cz/context (například https://vpn.test.cz/omi)



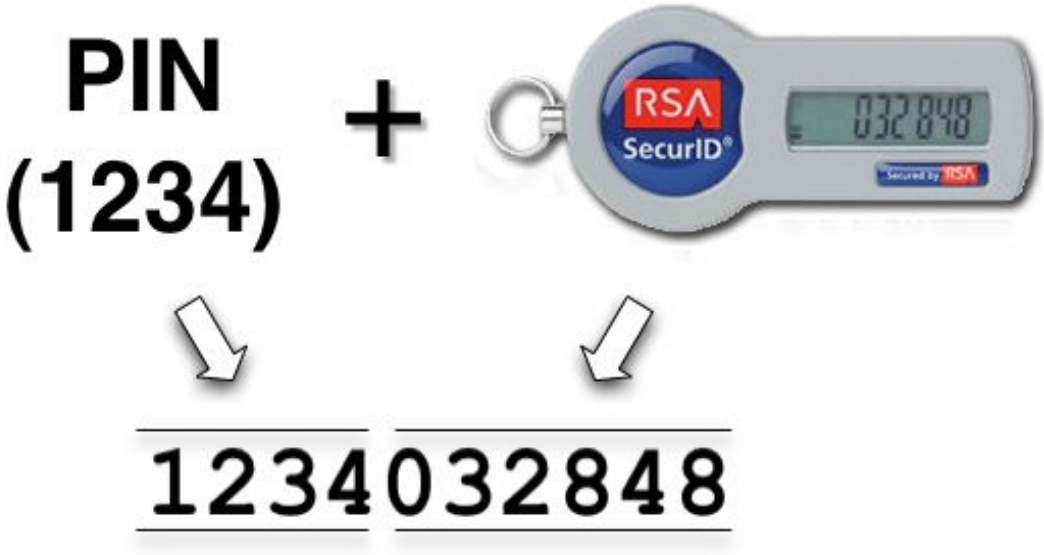
Obrázek 10.1: Odkaz pro vzdálený přístup.

Po zadání odkazu se zobrazí domovská stránka portálu vzdáleného přístupu - obrázek 2. Na této stránce je uživatel vyzván k zalogování.

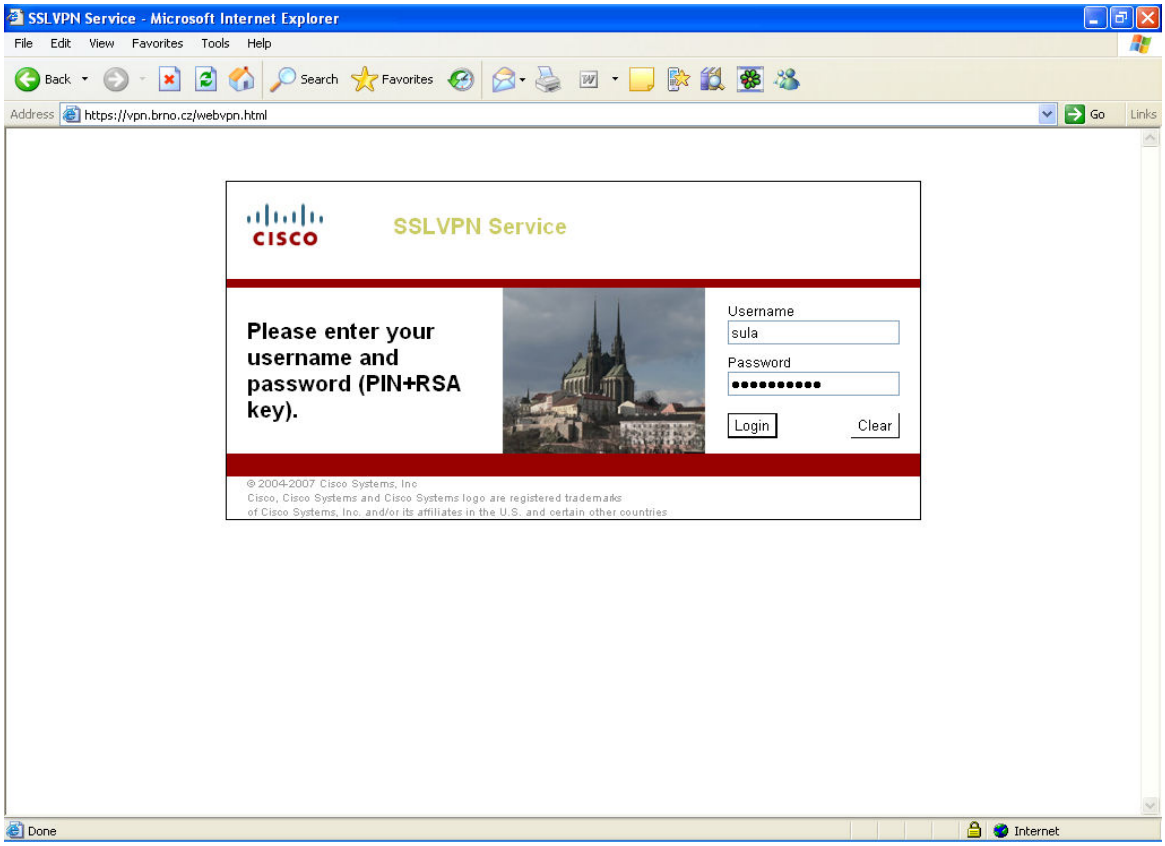


Obrázek 10.2: Portál vzdáleného přístupu – přihlášení.

Pro přihlášení slouží přidělené uživatelské jméno. Heslo je desetimístné číslo složené ze čtyř číslic PIN následovanými šesti čísly opsanými vždy aktuálně z klíčenky viz obrázek 3.



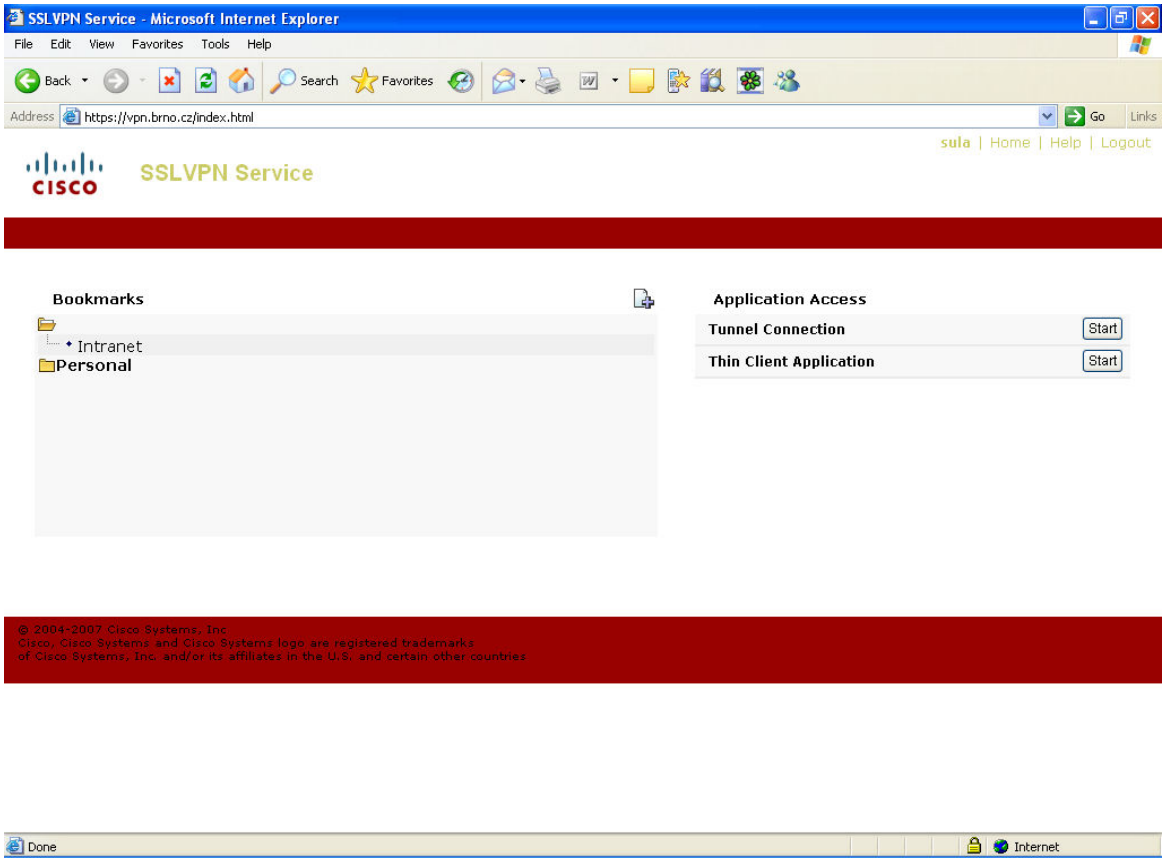
Obrázek 10.3: Heslo



Obrázek 10.4: Přihlášení.

Po úspěšném přihlášení uživatele je zobrazena domovská stránka portálu daného uživatele. Zde si uživatel volí typ přístupu do sítě MMB v závislosti na povoleném oprávnění. (Záleží na druhu uživatele, jaký přístup má povolen. V závislosti na tom má nebo nemá daný typ přístupu k dispozici.) Existují 3 možnosti přístupu:

1. Využití přístupu na webové služby běžící ve vnitřní síti. Servery komunikující HTTP / HTTPS protokolem z vnitřní sítě lze zpřístupnit přímo na domovské portálové stránce daného uživatele. Typickým příkladem je přístup na intranetový server.

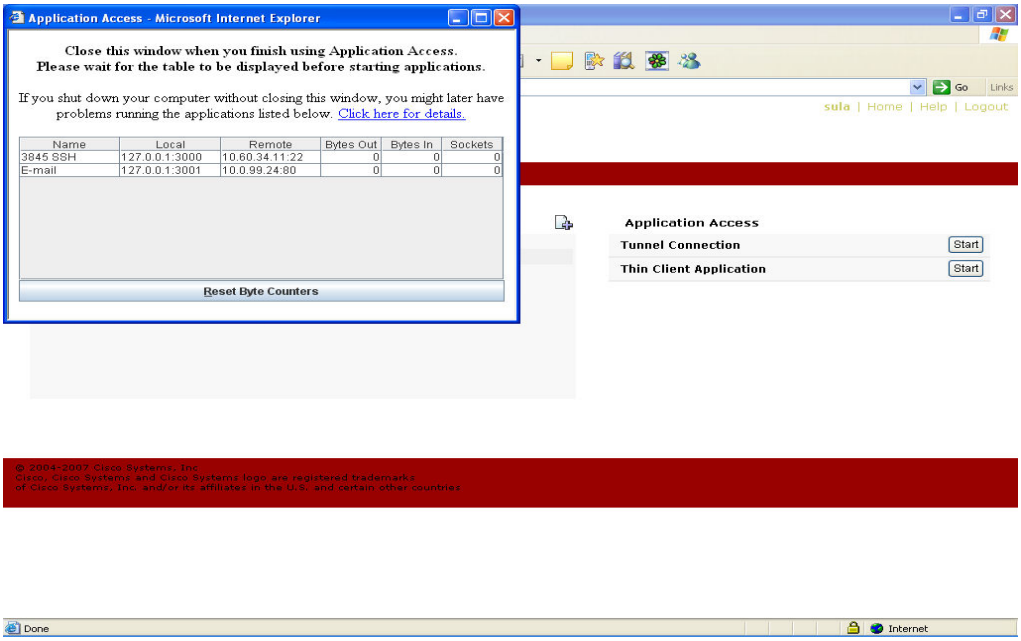


Obrázek 10.5: Zpřístupnění WWW služeb.

2. Tenký klient. Aplikace běžící na libovolném TCP portu lze zpřístupnit tenkým klientem (volba Thin Client Application). Po kliknutí na tuto volbu se vytvoří spojení, při kterém se na lokální loopback klientského stroje přemapují porty vybraných serverů z vnitřní sítě. Tímto způsobem lze přistupovat například na vzdálenou pracovní plochu nebo používat webového mailového klienta.

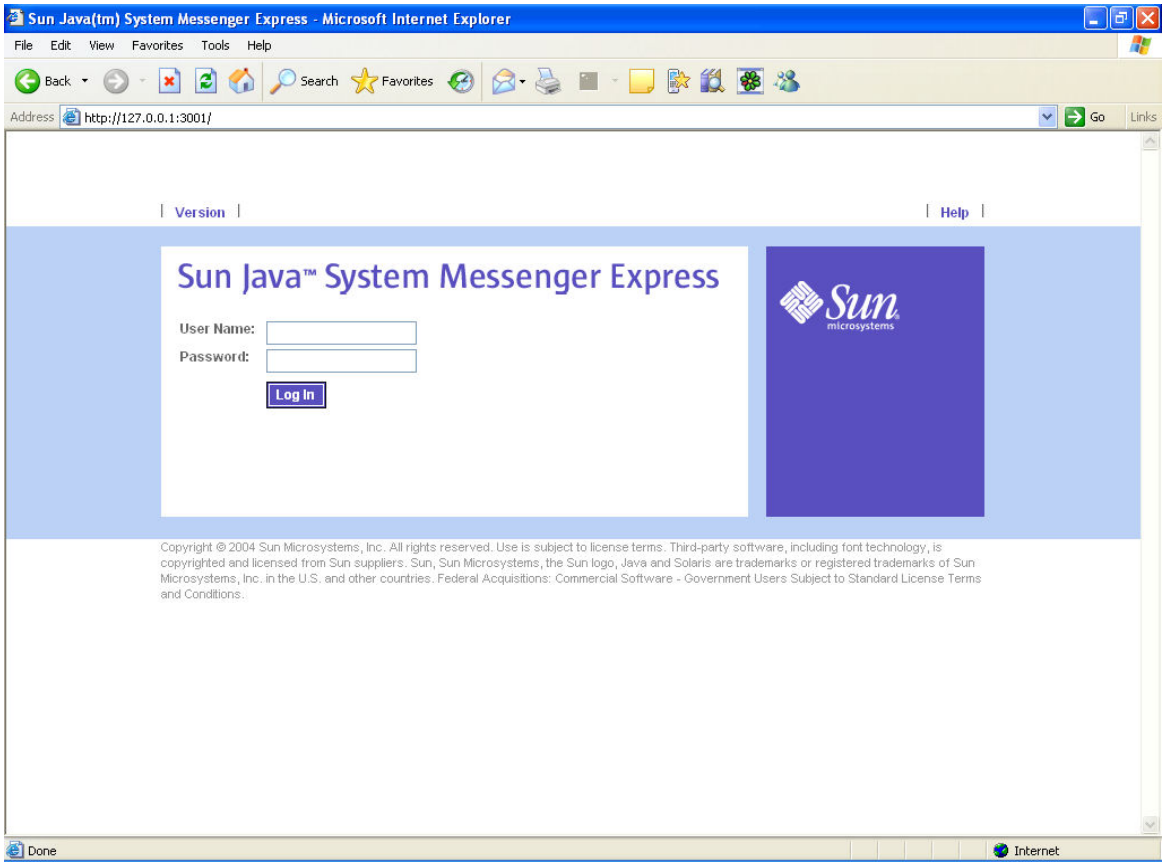
   Po inicializaci tenkého klienta se uživateli zobrazí okno s tabulkou, která popisuje možný přístup tenkým klientem daného uživatele. Na obrázku 6 je tato tabulka ukázána. Jeden řádek reprezentuje jednu službu. Atributy tabulky mají tento význam:

   - Name - popis zpřístupněné služby
   - Local - adresa a port zpřístupněné služby na lokálním počítači klienta, tuto adresaci služby použije uživatel pro přístup
   - Remote - adresa a port vzdálené služby
   - Bytes Out - odeslaný počet bajtů
   - Bytes In - přijatý počet bajtů
   - Sockets - počet používaných TCP spojení



Obrázek 10.6: Spuštění tenkého klienta.

Pro příklad druhý řádek reprezentuje přístup na webové rozhraní mailového klienta. Pro jeho spuštění uživatel zadá do webového prohlížeče lokální adresu služby, čili http://127.0.0.1:3001 – obrázek 10.7.

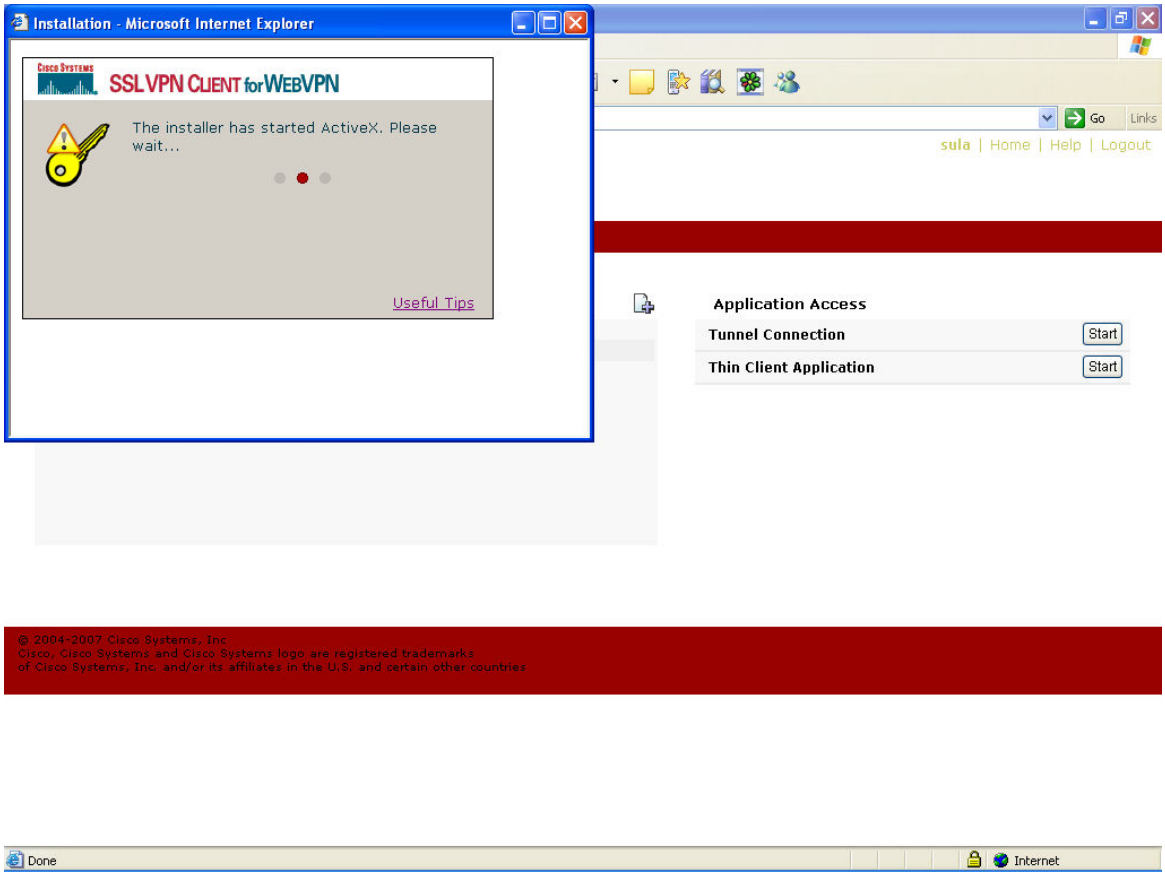


Obrázek 10.7: Použití přístupu přes tenkého klienta.

Ukončení přístupu do sítě MMB tenkým klientem se provede zavřením webového okna s tabulkou.

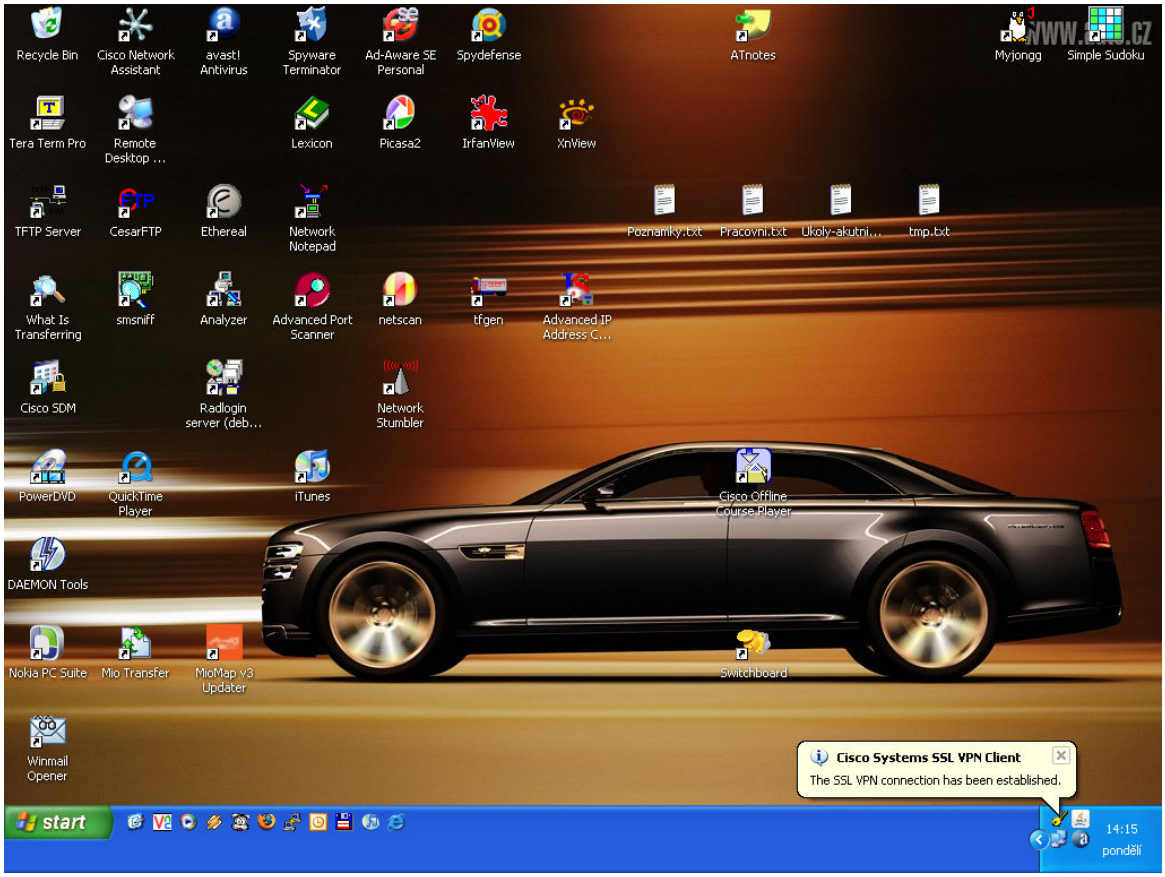
Pro správné ukončení vzdáleného přístupu slouží tlačítko Logout v levém horním rohu domovské stránky portálu vzdáleného přístupu.

3. Plný přístup do sítě MMB (volba Tunnel Connection). Je realizována SSL VPN Clietem (SVC), který se automaticky stáhne a nainstaluje na klientské PC. Po úspěšném navázání tunelu je směrován příslušný provoz klienta do sítě MMB.



Obrázek 10.8: Inicializace SVC.

Pokud vyhovuje alespoň jedna možnost automatického nainstalování a spuštění SVC, tak dojde k plnohodnotnému připojení do sítě. Domovská stránka portálu vzdáleného přístupu daného uživatele se automaticky zavře a zobrazí se ikona žlutého klíče ve spuštěných službách – obrázek 10.9.



Obrázek 10.9: Úspěšné připojení SVC do sítě.

Po úspěšném připojení SVC do sítě MMB jsou přístupné všechny povolené služby na příslušných serverech. Přístup na ně je identický jako v lokální síti MMB.

Pro ukončení tunelu klikne uživatel pravým tlačítkem na ikonu klíče a zvolí nabídku Disconnect.