# Bezpečné připojení zaměstnanců společnosti Povodí Labe, státní podnik, do podnikové sítě

Secure access for employee in company Povodi Labe state corporation to corporate networks.

Bc. Filip Navrátil

Diplomová práce
2011



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

# ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

| | |
|---|---|
| Jméno a příjmení: | **Bc. Filip NAVRÁTIL** |
| Osobní číslo: | **A09711** |
| Studijní program: | **N 3902 Inženýrská informatika** |
| Studijní obor: | **Informační technologie** |
| Téma práce: | **Bezpečné připojení zaměstnanců společnosti Povodí Labe, státní podnik, do podnikové sítě.** |

Zásady pro vypracování:

1. **Proveďte literární rešerši k tématu práce.**
2. **Analyzujte současný stav v organizaci a analyzujte bezpečností rizika.**
3. **Porovnejte varianty možných řešení a navrhněte postup implementace nejvhodnějšího.**
4. **Realizujte implementaci a proveďte diskusi nad řešením problému.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:


1. **LEWIS, Mark. Troubleshooting Virtual Private Networks. US : Cisco Press, 2004. 840 s. ISBN 1587051044.**
2. **HUANG, Qiang; FRAHIM, Jazib. SSL Remote Access VPNs. US : Cisco Press, 2008. 384 s. ISBN 1587052423.**
3. **LEWIS, Mark. Comparing, Designing, and Deploying VPNs. US : Cisco Press, 2006. 1080 s. ISBN 1587051796.**
4. **FEILNER, Markus; GRAF, Norbert. Beginning OpenVPN 2.0.9. UK : Packt Publishing, 2009. 356 s. ISBN 184719706X.**
5. **FRAHIM, Jazib; SANTOS, Omar. Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance. 2nd Edition. USA : Cisco Press, 2010. 1152 s. ISBN 1587058197.**
6. **FEILNER, Markus. OpenVPN : Building and Integrating Virtual Private Networks: Learn how to build secure VPNs using this powerful Open Source application. UK : Packt Publishing, 2006. 258 s. ISBN 190481185X.**
7. **DOSTÁLEK, Libor; VOHNOUTOVÁ, Marta. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. CZ : Computer Press, 2006. 536 s. ISBN 80-251-0828-7.**
8. **KABELOVÁ, Alena; DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP a systémem DNS. 5. aktualizované vydání. CZ : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.**


Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **24. února 2011**

Termín odevzdání diplomové práce: **18. května 2011**

Ve Zlíně dne 24. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
*děkan*

doc. Mgr. Roman Jašek, Ph.D.
*ředitel ústavu*

## ABSTRAKT

V diplomové práci je řešena problematika bezpečného připojení zaměstnanců Povodí Labe, státní podnik, do podnikové sítě. V teoretické části práce je proveden obecný popis možností a trendů, které jsou v současné době k dispozici v této oblasti se zaměřením na využití virtuálních privátních sítí - Virtual Private Network. Popisuje některé z typů virtuálních privátních sítí, technologie a protokoly, které jsou v rámci virtuálních privátních sítí využívány. Jsou zde zmíněny i některé aspekty, které je nutno vzít v úvahu při vytváření virtuálních privátních sítí, jako je například bezpečnost. Praktická část práce popisuje současný stav bezpečného připojení do podnikové sítě a dále se zabývá výběrem, návrhem a popisem implementace nejvhodnějšího nového řešení, které by nejlépe splňovalo požadavky na bezpečné připojení zaměstnanců do podnikové sítě.


Klíčová slova: VPN, SSL VPN, SSL/TLS, IPsec, Firewall, Endpoint Security


## ABSTRACT

The thesis deals with the issue of safe access for employees of Povodí Labe, State Enterprise, to a corporate network. The theoretical part generally describes trends and opportunities that are currently available in this field, focusing on the use of virtual private networks - Virtual Private Network. It describes some of the types of virtual private networks, technologies and protocols which are used within the virtual private network. Some aspects which must be taken into consideration when creating virtual private networks, such as security, are mentioned here. The practical part describes the present state of safe access to corporate networks. It also deals with selecting, designing and implementing the most appropriate description of such a solution that would best fulfil the requirements of safe access for employees to the corporate network.


Keywords: VPN, SSL VPN, SSL/TLS, IPsec, Firewall, Endpoint Security

Tímto bych chtěl poděkovat vedoucímu své diplomové práce panu doc. Mgr. Romanu Jaškovi, Ph.D. za rady a připomínky k řešení této práce. Dále děkuji své rodině za její podporu.

**Prohlašuji, že**

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

**Prohlašuji,**

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

Ve Zlíně ……

podpis diplomanta

# OBSAH

# ÚVOD

Bezpečné připojení zaměstnanců do podnikové sítě se v dřívějších dobách využívalo pouze sporadicky nebo bylo výsadou správců ICT, kteří měli potřebné povědomí o dané problematice. V současné době, kdy je na vzestupu mobilní připojení k Internetu prakticky odkudkoliv a tím umožněno připojení do firemní sítě z libovolného místa, je zajištění bezpečnosti při připojování do firemní sítě prvořadou záležitostí.

Pro manažery společností je výhodné zajistit zaměstnancům vzdálený přístup a tím zajistit (nebo vynutit) jejich maximální pracovní nasazení nezávisle na pracovní době a místě, i když to není v některých případech opětováno nadšením ze strany zaměstnanců. Vše je vynuceno sílícím tlakem na efektivitu a pružnost při plnění zadaných úkolů.

S těmito požadavky ze strany manažerů společnosti jsou spojeny další náklady věnované ochraně perimetru společnosti pro zajištění bezpečnosti IS podniku. Vzdálené připojení do podnikové sítě z prostředí Internet lze realizovat pomocí technologie virtuálních privátních sítí, dále jen VPN.

VPN představuje soubor technik a prostředků, které jsou využívány pro vzdálené bezpečné připojení do podnikové sítě z prostředí Internet. Jelikož zaměstnanci využívají připojení k Internetu z firemních zařízení i ze zcela jiných důvodů než jsou ryze pracovní záležitosti, respektive přistupují kromě podnikové sítě i na místa, kde nelze garantovat bezpečnost, tudíž je možné si při těchto aktivitách pořídit různé typy infekcí a ty následně přenést do podnikového prostředí, je nutné rozšířit a udržet perimetr zabezpečení i při následném přístupu do firemní sítě skrze VPN.

První část práce popisuje obecné a formální poznatky o problematice VPN. V dalších částech této práce budou tyto techniky a prostředky pro zajištění bezpečného využití VPN blíže popsány. Konkrétně se v druhé části práce zaměříme na výběr vhodného řešení pro zajištění požadavků kladených na bezpečné připojení zaměstnanců Povodí Labe, státní podnik, do podnikové sítě a následně návrhu nejvhodnějšího postupu implementace zvoleného řešení.

# I. TEORETICKÁ ČÁST

# 1 DŮVODY A VÝHODY ZAVEDENÍ VPN

Jedním ze základních důvodů zavedení VPN je ekonomická výhodnost tohoto řešení oproti vytváření nebo pronajímání vlastních WAN sítí. To je dáno především menšími náklady na datové připojení k prostředí Internetu, než jsou náklady na pronájem nebo budování vlastní WAN sítě. Další výhodou je pružné přizpůsobení konfigurace VPN dle aktuálních potřeb firmy. Dalším důvodem je nutnost zajistit bezpečné připojení mobilních zaměstnanců do podnikové sítě. V současné době se této možnosti stále více využívá při připojení zaměstnanců pracujících z domova nebo mobilních uživatelů.

Díky technologii VPN je rozšířena geografická konektivita do lokální sítě firmy. Není podstatné, kde a jak jsou umístěny jednotlivé počítače nebo celé lokální sítě (pobočky). Technologie VPN umožní v rámci veřejné sítě Internet nebo v rámci jiného typu sítě zabezpečený přenos dat.

Při vytváření VPN je velmi důležitým faktorem kvalita datového připojení klienta nebo celé lokální sítě, ze které je zprostředkováváno VPN spojení. Dalším důležitým faktorem je zajištění celkového zabezpečení daného řešení. Jedná se především o zabezpečení autentizace například zajištěním využívání dvoufaktorové autentizace.

## 1.1 Obecný popis technologie VPN

Termínem VPN je obecně myšleno bezpečné propojení několika prostředků ICT prostřednictvím nezabezpečené veřejné sítě nebo jiného typu sítě. Jinak řečeno cílem VPN je dosáhnout toho, aby různé prostředky ICT, které jsou připojeny do úplně rozdílných sítí, mezi sebou komunikovaly skrze zabezpečené připojení a byly tak virtuálně propojeny do jedné virtuálně uzavřené sítě tzv. Virtual Private Network. VPN nahrazuje svojí funkcí rozlehlou WAN síť a využívá přitom různých technologií.

# 2 ZÁKLADNÍ PRINCIPY A POŽADAVKY

VPN je, jak popisujeme výše, založeno na vytvoření zabezpečeného přenosového kanálu s využitím nezabezpečeného přenosového média nebo jiného typu sítě. Proto je nutné se podrobněji zaměřit na některé základní principy a požadavky využívané v rámci VPN.

## 2.1 Autentizace

Slouží k ověření identity objektu vstupujícího do VPN spojení. Autentizace je většinou založena na znalosti autentizačních údajů, jako je jméno a heslo nebo vlastnictví bezpečnostního certifikátu. V současné době se stále častěji využívá autentizace pomocí dalšího hardware prvku, například pomocí čipových karet a USB Token, kde je uložen bezpečnostní certifikát. Jedná se o tzv. PKI autentizaci. Tato autentizace je dvoufaktorová – musíme znát PIN a vlastnit bezpečnostní certifikát.

Při autentizaci je nutné, aby obě strany (klient, server), které vstupují do VPN spojení, byly důvěryhodné. To je řešeno pomocí autentizace klienta (PC, směrovač) prostřednictvím PSK (Pre-shared key) nebo PKI (Public-Key Infrastructure). PSK autentizace je založena na manuálním sdílení tajného klíče. Toto má jednu velkou nevýhodu. Je nutné zajistit bezpečnou distribuci tajného klíče mezi uživatele VPN. Autentizace využívající PKI je založena na certifikátech vydávaných certifikační autoritou. V tomto případě není manuálně sdílen tajný klíč, ale pro každý subjekt, který se účastní VPN spojení, je vygenerován certifikát. Tyto certifikáty jsou generovány jednou certifikační autoritou a navzájem si důvěřují. Na základě certifikátu se provádí ověření a následná výměna dat, která je nutná pro zahájení šifrování přenosu. Autentizace s využitím PKI je současné době upřednostňována. Další možností zajištění dvoufaktorové autentizace je využití tzv. jednorázových hesel. Lídrem v těchto technikách autentizace je společnost RSA a její produkt RSA ID. Přesný popis a funkčnost jednorázových hesel bude vysvětlena v dalších částech diplomové práce.

## 2.2 Autorizace

Zajišťuje ověření, zda zvolený objekt má oprávnění k provedení nějaké činnosti, v našem případě k přístupu do vnitřní sítě. Následuje po úspěšné autentizaci.

## 2.3 Šifrování

Jelikož VPN je síť sestavená většinou nad veřejným médiem, konkrétně nad sítí Internet, je základní podmínkou zachování bezpečnosti přenášených dat zajistit dostatečné šifrování. Pomocí šifrování se data zpracují do těžko čitelné podoby s využitím šifrovacího algoritmu a šifrovacího klíče. K šifrování se využívá symetrické šifrovací algoritmy například DES, 3DES, IDEA, Blowfish a další. K výměně šifrovacích klíčů se u PKI autentizace využívá asymetrické šifrování.

## 2.4 Bezpečnost na straně klienta

Síť VPN je nejvíce zranitelná přes VPN klienty respektive uživatele, kteří se do podnikové sítě připojují prostřednictvím VPN klienta. Proto je základní podmínkou dostatečného zabezpečení VPN i zabezpečení klienta.

Doporučuje se instalovat klientský firewall, tedy pokud není součástí VPN klienta. Dále se doporučuje nasadit některý z prostředků vynucující politiku zabezpečení po připojení do sítě. Například pomocí produktové řady NAC (Network Admission Control) od firmy Cisco nebo NAP (Network Access Protection) od firmy Microsoft, případně dalších řešení jiných výrobců. Tyto produkty se zaměřují, jak je popsáno výše, na vynucení politik dle požadavků organizace. Pokud klient, připojený do firemní sítě, nevyhoví nastaveným politikám, je připojen do sítě s patřičnými omezeními.

Další možností je vynucení bezpečnostních politik na straně klienta již v průběhu sestavování VPN spojení, jak umožňují některé produkty popisované v této práci. Například je vyžadována aktuální verze antivirového softwaru instalovaného na klientovi, ze kterého je navazováno VPN spojení. Další možnosti jsou například v testování určitých hodnot na straně klienta, který sestavuje spojení. Například u klientů s operačním systémem Windows se testují hodnoty v registru. Díky těmto možnostem, které výrobci VPN řešení shrnují pod jedno označení Endpoint Security, je umožněno například povolit přístup do VPN pouze z firemních zařízení (PC, Smartphone, atd.).

## 2.5 Integrita

Data, která jsou přenášena skrze VPN, musí být možné získat v takovém stavu (podobě) v jakém byla odeslána. Integrita přenášených dat nám umožní zjistit, zda nebyla data při

přenosu porušena vlivem vadného přenosového prostředí nebo snahou útočníka podvrhnout přenášená data. Integrita dat se zajišťuje pomocí hashovacích algoritmů a opravných kódů.

## 2.6 Rychlost

Dalším klíčovým parametrem VPN spojení je rychlost. Ta je většinou omezena kvalitou a kapacitou datové linky a kvalitou šifrování. Kapacitou datové linky je zde myšlena datová propustnost linky, kterou je subjekt připojen do prostředí Internetu. Rychlost VPN sítě je také ovlivňována kvalitou šifrování. Na rychlost šifrování a tím rychlost celého VPN spojení, má vliv i to, zda je VPN server softwarový nebo hardwarový. Hardwarový VPN server obvykle obsahuje hardwarové akcelerátory šifrování.

# 3 ROZDĚLENÍ VPN PODLE TYPU SPOJENÍ

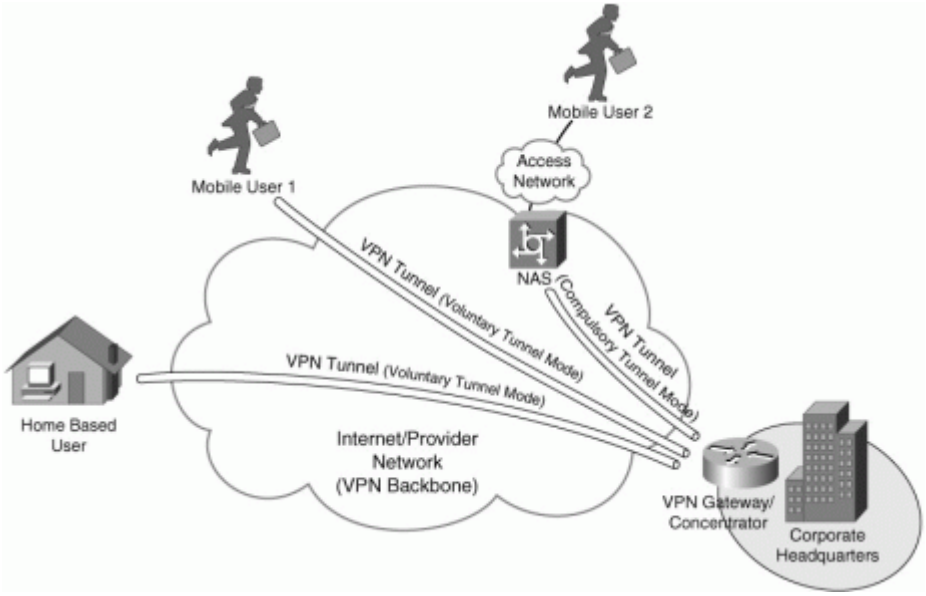
V odborné literatuře jsou typy VPN spojení popisovány rozdílně.[1], [2] Některé odborné publikace popisují rozdělení na: point-to-point, point-to-site, site-to-site. V dalších publikacích je VPN rozděleno na: Remote-Access a Site-to-Site. Tato práce se zaměřuje na popis rozdělení VPN podle posledně jmenovaného rozdělení, tedy Remote-Access a Site-to-Site. Oba typy si dále popíšeme.

## 3.1 Remote-Access

Tento typ VPN připojení využívají mobilní uživatelé nebo uživatelé pracující z domova. Při tomto typu VPN připojení je většinou využíván softwarový VPN klient, nicméně to nemusí být podmínkou. Softwarový VPN klient obsahuje i dodatečné funkcionality jako je například síťový firewall. Některé operační systémy, které jsou využívány pro připojení do sítě, již obsahují základní podporu pro různé druhy VPN spojení.

**Zjednodušený popis průběhu připojení Remote-Access:**

1. Klient musí být připojen k prostředí Internet.
2. Klient naváže zabezpečené spojení pomocí VPN softwaru s VPN serverem. Při navázání spojení dojde k výměně informací nutných k zajištění zabezpečeného připojení a ověření důvěryhodnosti VPN serveru, aby nemohlo dojít k podvržení VPN klienta nebo VPN serveru. K ověření důvěryhodnosti VPN serveru se používají dvě metody - PSK (Pre-shared key) a PKI (Public-Key Infrastructure).
3. Klient se musí ověřit pomocí hesla nebo PKI.
4. VPN server přidělí klientovi IP adresu a v operačním systému klienta je vytvořen virtuální síťový adaptér, přes který je směrován veškerý provoz na VPN server.




Obrázek 1 - Schéma VPN typu Remote-Access [1]

## 3.2 Site-to-Site

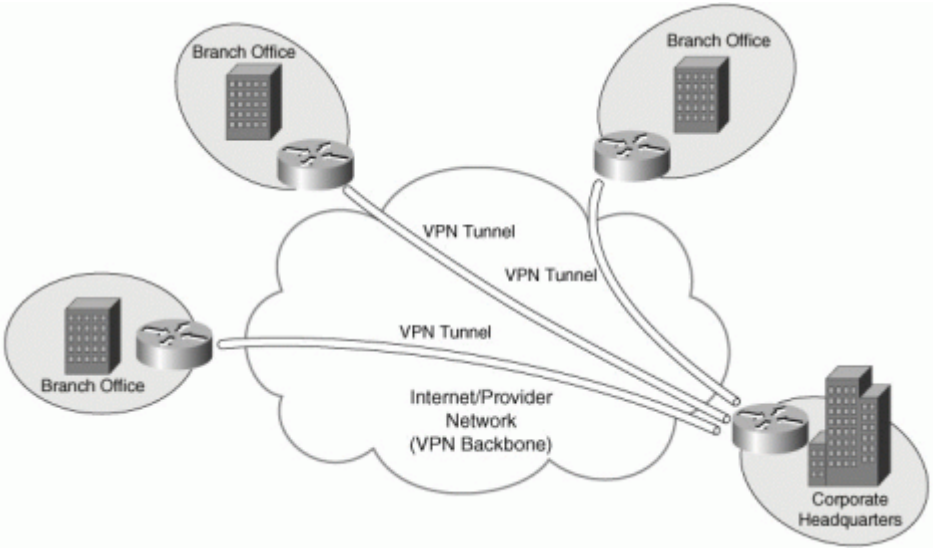
Tento typ VPN je využíván při propojení celých sítí například geograficky oddělených poboček firmy. VPN spojení realizuje firewall nebo směrovač (router) pobočky tzn. pro uživatele na pobočce je VPN spojení naprosto transparentní. Při tomto typu spojení jsou většinou využívány hardwarové prostředky, které mají hardwarovou podporu šifrování. Díky hardwarové podpoře šifrování je dosahováno větší rychlosti.

**VPN site-to-site dále dělíme:**

1. Site-to-site - Intranet

   Je využíváno pro propojení geograficky odlehlých poboček firmy, jak je popsáno výše.
2. Site-to-site – Extranet

   Je využíváno pro kontrolovaný přístup do vnitřní sítě, například pro důvěryhodné partnery, firmy nebo zákazníky.




Obrázek 2 - Schéma VPN typu Site-to-Site [1]

## 3.3 Rozdíly mezi VPN dle typu spojení

Při VPN spojení typu Remote-Access je nutná interakce od uživatele, který navazuje spojení. Naproti tomu u VPN typu Site-to-Site je spojení realizováno na přístupovém bodu (firewall, směrovač) pobočky, tzn. uživatelé nemusejí vyvíjet jakoukoliv aktivitu, aby bylo navázáno VPN spojení. Pro uživatele je toto spojení naprosto transparentní. Dalším rozdílem jsou používané typy protokolů při VPN spojení. Site-to-Site VPN využívá především protokol IPSec, který představuje v současné době bezpečností standard u tohoto typu VPN. Při realizaci VPN typu Remote-Access se v poslední době začal hojně využívat protokol SSL/TLS neboli obecně SSL VPN. Využitím SSL VPN lze teoreticky zaručit přístup do firemní sítě z jakékoliv části sítě Internet, a to díky obvykle standardně povolené SSL/TLS (TCP port 443) u většiny ISP.

# 4 TYPY VPN SÍTÍ

V mnoha různých publikacích či pracích je VPN rozdělováno podle toho, na jaké vrstvě síťového modelu ISO/OSI je provozováno. V této práci se zaměříme na rozdělení dle praktického použití s přihlédnutím na různé protokoly, které jsou v rámci VPN využívány.

## 4.1 VPN s využitím privátních datových sítí

Jsou založené na využívání dedikovaných privátních sítí veřejných poskytovatelů telekomunikačních služeb, a to nejčastěji pomocí ATM, Frame Relay nebo MPLS sítí. Díky možnosti využití dedikovaných datových linek, můžeme vytvořit zcela privátní síť, která je oddělena od veřejné sítě Internet.

VPN v síti MPLS funguje na principu přepínání podle značek (label switching). Přenášená data jsou nejprve označena pomocí speciálních značek. Značky jsou přiděleny na základě různých kritérii, například podle cílové adresy nebo příslušnosti k určité VPN síti. Data v MPLS síti se pak směřují podle těchto značek. Po přenosu na koncový prvek MPLS jsou již data dále směrována klasicky podle cílové adresy.

## 4.2 VPN s využitím tunelování a šifrování

Jedná se o nejčastěji používaný typ VPN sítě. Při vytváření tohoto typu VPN spojení jsou využívány techniky tunelování a šifrování. Technika tunelování představuje proces přenášení dat v zapouzdřené podobě prostřednictvím jiného nebo stejného síťového protokolu. Nevýhodou toho řešení je, že musí být zajištěna patřičná úprava bezpečnostních síťových politik (firewall), jelikož jsou pro tunelování a šifrování obvykle využívány protokoly jako je IPsec nebo GRE. Nicméně to není jediná podmínka pro úspěšné využití těchto protokolů. Například i poskytovatel připojení do Internetu dále jen ISP, skrze kterého je VPN realizováno, musí umožňovat využívání těchto protokolů. V další části jsou popsány některé z protokolů a technik, které jsou pro tento typ VPN typické.

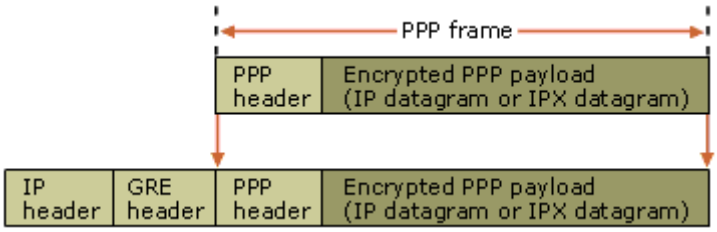
### 4.2.1 Generic Routing Encapsulation (GRE)

Je tunelovací protokol vyvinutý původně společností CISCO. Protokol GRE (Generic Routing Encapsulation) je určený k zapouzdření paketů jednoho protokolu do protokolu jiného - tunelování. Do paketů, které jsou určené pro přenos tunelem, jsou vloženy zvláštní

přídavné hlavičky (GRE header) a cílové adresy, odpovídající směrovači na konci tunelu. Toto "zabalení" (encapsulation) paketu je v cílovém bodu tunelu (firewall, směrovač) odstraněno a paket dále pokračuje ke svému cíli podle informací ve své původní IP hlavičce. [9]

### 4.2.2 Point-to-Point Tunneling Protocol (PPTP)

Je rozšířením protokolu PPP (Point-to-Point Protocol) a slouží ke zdokonalení mechanismů ověřování, komprese a šifrování protokolu PPP. Rámec PPP (datagram IP) je vnořen do hlavičky protokolu GRE (Generic Routing Encapsulation) a hlavičky protokolu IP. V hlavičce protokolu IP je uvedena zdrojová a cílová IP adresa, která odpovídá klientovi a serveru VPN. PPTP podporuje metody autentizace PAP, CHAP, MS-CHAP a MS-CHAPv2 nebo EAP-TLS. V podání firmy Microsoft obsahuje PPTP šifrování MPPE (Microsoft Point to Point Encryption). Přesněji - rámec PPP je šifrován metodou MPPE s využitím šifrovacích klíčů generovaných v průběhu ověřování. Na následujícím obrázku je znázorněno schéma zapouzdření rámce PPP v protokolu PPTP. [5], [8]




Obrázek 3 - Zapouzdření rámce PPP v protokolu PPTP [5]

### 4.2.3 Layer two tunelling protocol (L2TP/IPsec)

Byl uveden jako rozšíření PPP společností CISCO, Microsoft a dalšími. Čerpá z protokolu PPTP a také z tunelovacího protokolu L2F společnosti CISCO. Je podporován operačními systémy Windows 2000 a novějšími. Podporován je také Unix/Linuxovými systémy a zařízeními Cisco. Pro zajištění vysoké míry bezpečnosti musí být doplněn o protokol IPsec. Poté je označován jako L2TP/IPsec.

Při spojení s L2TP Network Server přes IPsec je počítač, ze kterého je inicializované spojení, ověřen pomocí PSK klíčů nebo pomocí certifikátu počítače (PKI) protokolem IKE

(Internet Key Exchange). Protokolem IKE jsou dohodnuty i bezpečnostní parametry spojení jako je například šifrování. Zpráva protokolu L2TP/IPsec je šifrována pomocí standardu DES (Data Encryption Standard) nebo trojnásobného algoritmu DES (3DES) pomocí šifrovacích klíčů generovaných v procesu vyjednávání protokolu IKE (Internet Key Exchange). Ověření uživatele je založeno na autentizačních protokolech protokolu PPP jako je PAP, CHAP, MS-CHAPv2 nebo pomocí certifikátu uživatele s využitím protokolu EAP-TLS (Extensible Authentication Protocol-Transport Level Security) nebo protokol PEAP (Protected Extensible Authentication Protocol). Po úspěšném ověření je uživatel připojen do podnikové sítě.

**Zapouzdření paketů připojení L2TP/IPSec se skládá ze dvou vrstev [6]:**

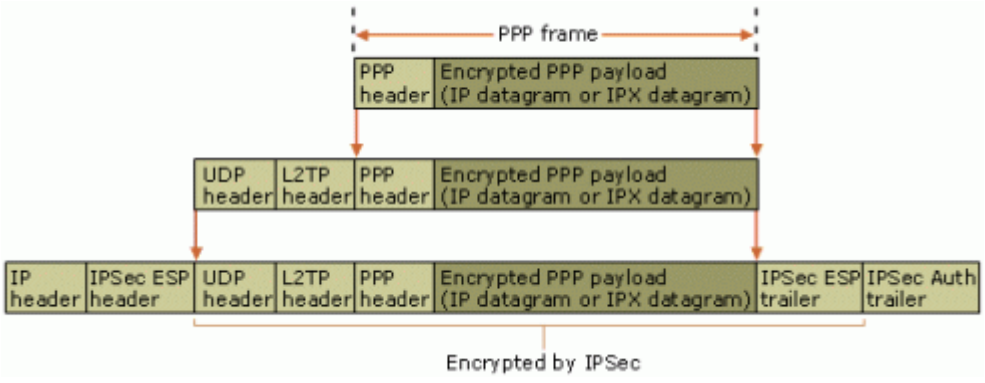
1. Zapouzdření L2TP

   Rámec PPP (datagram IP nebo datagram IPX) je vnořen do hlavičky protokolu L2TP a do hlavičky protokolu UDP.

2. Zapouzdření IPSec

   Výsledná zpráva protokolu L2TP je vnořena do hlavičky a do koncové části protokolu IPSec ESP (Encapsulating Security Payload) a je opatřena koncovou částí zabezpečení IPSec, která zajišťuje integritu a ověření zprávy a dále je opatřena koncovou hlavičkou protokolu IP. V hlavičce protokolu IP je uvedena zdrojová a cílová adresa IP, která odpovídá klientovi a serveru VPN.

Na následujícím obrázku je znázorněno zapouzdření rámce PPP protokolem L2TP/IPSec.[6]




Obrázek 4 - Zapouzdření rámce PPP protokolem L2TP/IPsec [6]

### 4.2.4 Internet Protocol Security (IPsec)

Jedná se o soubor protokolů a technik, které zaručují šifrované spojení v síti TCP/IP. Je často využíván společně s jinými VPN protokoly, jak je popsáno výše, pro zajištění větší bezpečnosti VPN spojení. IPsec může být provozován ve dvou módech – tunelovací a transportní. V tunelovacím módu se zašifrují data včetně záhlaví a je přidáno nové IP záhlaví. V transportním módu se šifrují pouze data a IP záhlaví zůstává nezměněno. IPsec se skládá z dalších dvou nezávislých protokolů AH (Authentication Header) a ESP (Encapsulated Security Payload). Protokol IPSec je založen na modelu koncového zabezpečení a zajišťuje důvěryhodnost a zabezpečení od zdrojové po cílovou adresu IP. Samotnou adresu IP nelze vždy považovat za určitou identitu. V procesu ověřování je ověřována platnost identity systému, který danou adresu IP používá, a to zejména pomocí PSK nebo pomocí PKI s využitím protokolu IKE. Protokol IPSec je nativně podporován v IPv6, což může v blízké době zajistit jeho další rozšíření. Dokonce se vyskytují úvahy, že by mohl vytlačit tzv. SSL VPN tzn. VPN založené na protokolu SSL/TLS.

## 4.3 VPN s využitím SSL/TLS - SSL VPN

Jak již z názvu vyplývá, základním stavebním kamenem pro zajištění bezpečného VPN spojení je protokol SSL/TLS. Tento protokol je využíván ve spojení s technikami tunelování.

Protokol SSL definuje způsob šifrování a autentizaci komunikujících stran. TLS (Transport Layer Security) je nástupcem protokolu SSL a ve verzi TLS 1.0. Jde v podstatě o SSLv3 s některými drobnými opravami a vylepšeními. Proto se často uvádí složený zápis SSL/TLS dále jen SSL. V protokolu SSL jsou využívány asymetrické i symetrické šifrovací algoritmy. Následuje obecný popis principu SSL spojení.

Před vlastním přenosem si obě strany, vstupující do SSL spojení, ověří totožnost s využitím certifikátů a techniky veřejných a privátních klíčů (asymetrické šifrování). Po ověření si vymění bezpečnostní informace, na základě kterých je poté sestaveno SSL spojení. Vlastní SSL přenos je šifrován symetrickými šifrovacími algoritmy, například 3DES, RC4. Integritu přenášených dat zajišťují hashovací funkce SHA nebo MD5.

VPN založené na tomto protokolu má několik výhod. Například není nutné zajišťovat specifické nastavení firewallu a SSL protokol je většinou standardně podporován mnohými ISP. S využitím Java appletů nebo ActiveX komponent, spuštěných

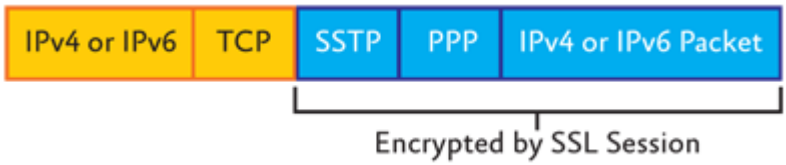
z internetového prohlížeče, může být realizován portforwarding (přesměrování síťových portů).

V současné době SSL VPN začínají nahrazovat VPN typu Remote-Access založené na IPsec. Jelikož SSL VPN využívá pro svůj provoz standardně povolený TCP port 443, není problém s připojením prakticky z jakékoliv části sítě Internet. SSL VPN nabízí taktéž stejné možnosti jako VPN založené na IPsec, například NAC (Network Access Control) nebo dvoufaktorovou autentizaci (certifikáty, jednorázová hesla). SSL VPN neslouží pouze k omezenému přístupu do podnikové sítě skrze webový prohlížeč, jako tomu bylo v dřívějších dobách, ale v současnosti umožňuje plnohodnotný přístup (je zajištěno směrování veškeré síťové komunikace skrze zabezpečený tunel) do podnikové sítě skrze instalovaného SSL VPN klienta.

### 4.3.1 Secure Socket Tunneling Protocol (SSTP)

Jedná se protokol vyvíjený společností Microsoft, který má nahradit VPN protokoly jako je PPTP a L2TP/IPsec. Secure Socket Tunneling Protocol (SSTP) využívá rozšířené protokoly HTTP a SSL. SSTP zajišťuje zapouzdřování IP paketů (tunelování) skrze SSL protokol a tím odpadají problémy s filtrováním GRE nebo IPsec protokolů některými ISP. Toto VPN spojení může být realizováno jenom mezi nejnovějšími verzemi operačního systému Windows. (například mezi Windows Server 2008, Windows Vista SP1 a novějšími). SSTP má integrovanou podporu pro Network Access Protection (NAP), které mohou být použity pro lepší ochranu sítě a vynucování síťových politik. [7]

IP paket je nejprve uzavřen záhlavím PPP a záhlavím SSTP. Kombinace IP paketu, záhlaví PPP a záhlaví SSTP je šifrováno pomocí SSL. Na závěr je přidána hlavička TCP a záhlaví IP. [7]




Obrázek 5 - Struktura SSTP paketu [7]

### 4.3.2 OpenVPN

OpenVPN je open-source VPN řešení, které využívá SSL/TLS protokol. Podporuje mnoho plaforem například Linux, Window, FreeBSD. Běží v takzvaném user-space SSL VPN. User-space označení znamená, že se jedná o aplikaci, která běží ve svém uživatelském prostoru operačního systému na rozdíl od prostoru jádra systému. To zaručuje větší bezpečnost celého VPN řešení. S operačním systémem komunikuje skrze virtuální síťové adaptéry TUN nebo TAP. OpenVPN využívá pro tunelové spojení UDP protokol, který je vhodnější pro tunelování TCP protokolu. OpenVPN, i když využívá SSL/TLS protokol, není provozováno na standardním portu TCP 443, ale je využíván UDP protokol specifický port například 1194. Toto může být problém při sestavování VPN spojení, protože někteří ISP blokují některé porty. Nicméně může být OpenVPN zkonfigurováno k využívání TCP protokolu a portu 443.

**Obecná charakteristika OpenVPN** [3]**:**

- pro zabezpečení se využívá technologie protokolů SSL/TLS
- dostupnost pro řadu OS (Linux, Windows 2000/XP, OpenBSD, FreeBSD, NetBSD, Mac OS X a Solaris)
- podpora režimů 1:1 nebo N:1
- autentizace za použití sdíleného klíče nebo X. 509 certifikátů
- odolnost při použití na nekvalitních linkách
- pro přenos používá UDP protokol, ale lze použít i TCP

# II. PRAKTICKÁ ČÁST

# 5 SOUČASNÝ STAV

V této kapitole bude popsán současný stav ICT prostředků v podniku Povodí Labe, státní podnik dále jen PLA a další technické parametry ICT jako je topologie sítě atd.

## 5.1 Územní členění organizace z pohledu zapojení sítě

Podnik je rozdělen na šest hlavních vzájemně geograficky oddělených lokalit, které jsou propojené pomocí vlastní mikrovlnné WAN sítě, dále jen páteřní síť, vybudované na vlastním zařízení a využívající licenční pásmo dle stanov ČTU. Přenosová kapacita páteřní sítě je 6 Mb/s. Konkrétně se jedná o lokality: Hradec Králové, Pardubice 2, Pardubice 4, Jablonec nad Nisou, Roudnice nad Labem, Vaňov. K této páteřní síti se dále připojuje dalších 65 lokalit (střediska, vodní díla, atd.). Některé z lokalit se připojují k páteřní síti pomocí mikrovlnných pojítek v přenosové kapacitě do 2 Mb/s. Jiné lokality, kde nelze z technických nebo ekonomických důvodů vyřešit připojení k páteřní síti pomocí vlastního mikrovlnného spoje, je využíváno řešení s názvem IPConect od společnosti Telefónica O2 Czech Republic, a.s. dále jen O2 a.s. Jedná se VPN síť postavenou na MPLS technologii využívající síť společnosti O2 a.s.

Každá z lokalit má jiný adresní rozsah, tzn. síť PLA se skládá z 65 podsítí. V horizontu jednoho roku bude nynější řešení páteřní sítě sloužit pouze jako záložní, neboť bude nahrazeno novou páteřní sítí spojující všech šest lokalit pomocí VPN sítě typu Site-to-Site založené na protokolu IPsec využívající akademické optické sítě CESNET s kapacitou cca 30 Mb/s. V rámci vlastní WAN sítě jsou přenášena nejenom data, ale i telefonní hovory.

## 5.2 Aktuálně využívané ICT v organizaci dle zaměření

V této části diplomové práce jsou popsány ICT prostředky organizace z pohledu jejich funkčnosti v IS organizace tzn. z pohledu autentizace, bezpečnosti, zálohování, atd. Je nutné dopředu zmínit, že v PLA je plně využívána VMware virtualizační technologie, která bude podrobněji popsána v další části práce.

### 5.2.1 Bezpečnost

Zajištění ochrany dat a ICT prostředků organizace je jednou z prvořadých priorit v současnosti. V PLA je k zajištění bezpečnostních rizik používáno několik ICT prostředků od předních leaderů na trhu. Jedná se především o firewally, antivirovou a antispamovou ochranu. V následující části je oblast bezpečnosti dat a ICT v PLA popsána podrobněji.

#### *5.2.1.1 Firewall a proxy servery*

Funkce firewallu je zajistit bezpečný perimetr pro ICT prostředky vnitřní sítě. Existuje několik druhů firewallů od jednoduchých paketových filtrů až po speciální stavové nebo aplikační firewally, které kontrolují on-line síťový provoz dle RFC standardů. PLA využívá k zajištění ochrany firewall ASA 5520 (Adaptive Security Appliances) od společnosti Cisco. Toto zařízení v sobě integruje firewall, IPS (Intrusion prevention system) a VPN.

Pro zajištění a kontrolu přístupu k síti Internet z vnitřní sítě organizace je využíván proxy server Novell BorderManager s autentizací založené na adresářové službě Novell eDirectory.

#### *5.2.1.2 Antivirová a antispamová ochrana*

Antivirová ochrana je v PLA zabezpečena z několika směrů. V prvním případě je ochrana zajištěna pomocí antivirového softwaru instalovaného na uživatelských PC. Na PC je instalován Symantec Endpoint Protection antivirus, který zajišťuje jednak antivirovou ochranu, ale nabízí i ochranu pomocí personálního firewall. Tento antivirový programu byl v PLA nasazen na základě výsledků podrobného výběru z mnoha antivirových programů dostupných na trhu. Vyznačuje se vynikající antivirovou detekcí, precizní centrální správou klientů a vynikajícím monitorovacím rozhraním.

V dalším směru je antivirová ochrana spjata s antispamovou ochranou. Jedná se o antivirovou a antispamovou ochranou e-mailové brány PLA v zóně DMZ, která je využívána pro příjem a odesílání e-mailových zpráv do sítě Internet. Jako antivirová a antispamová e-mailová brána je využívána InterScan Messaging Security Virtual Appliance od společnosti TrendMicro. Toto zařízení se vyznačuje vynikající úspěšností v detekci spamu a velice nízkým skórem falešných záchytů tzv. false positive. Zařízení má

velice intuitivní administrátorské rozhraní a jak z názvu vyplývá, jedná se zařízení provozované ve virtuálním prostředí.

### 5.2.2 Zálohování ICT

V PLA je zálohování realizováno pomocí modelu centrálního zálohování. V tomto modelu zálohování je využíván jeden nebo více zálohovacích serverů, na které jsou skrze zálohovací klienty přenášena zálohovaná data. K centrálnímu zálohování je využíván Tivoli Storage Manager od společnosti IBM. Do centrálního zálohování jsou integrovány všechny důležité ICT organizace. Například centrální databáze, souborové servery, poštovní servery. Centrální zálohovací server sestává z HW serveru značky IBM, zálohovací páskové knihovny značky IBM využívající technologii LTO 5 a z diskového pole HP EVA 4000. Všechny tyto části zálohovacího serveru jsou připojeny do SAN sítě.

### 5.2.3 Centrální databáze

V organizaci je využíván databázový server Oracle, konkrétně Real Aplication Cluster 10.2 (RAC). Je tvořen dvěma HW servery HP 360 G4 připojených do SAN sítě, skrze kterou jsou veškerá data všech instancí databází ukládána na centrální datové pole. Zajímavostí RAC technologie je využití Automatic Storage Management (ASM). Jedná se v podstatě o vlastní cluster systém souborů.

### 5.2.4 Centrální datové úložiště

Slouží k bezpečnému ukládání dat celé organizace a skládá se ze dvou zrcadlených diskových polí Hitachi Adaptable Modular Storage 2100 o hrubé diskové kapacitě každého pole 32,3 TB, které je zapojeno do SAN sítě. Většina ICT organizace ukládá data na toto diskové pole. Tím je zajištěna velmi vysoká dostupnost a bezpečnost ukládaných dat.

### 5.2.5 Virtualizace

V organizaci je virtualizační technologie VMware využívána již několik let. Konkrétně se jedná o VMware cluster vSphere 4 Enterprise tvořený šesti ESXi servery, které představují jádro celé virtuální infrastruktury. Na tomto VMware clusteru je v současné době provozována většina serverů organizace, respektive všechny servery s certifikací běhu na virtuálním HW. Konkrétně v současné době je na VMware clusteru provozováno

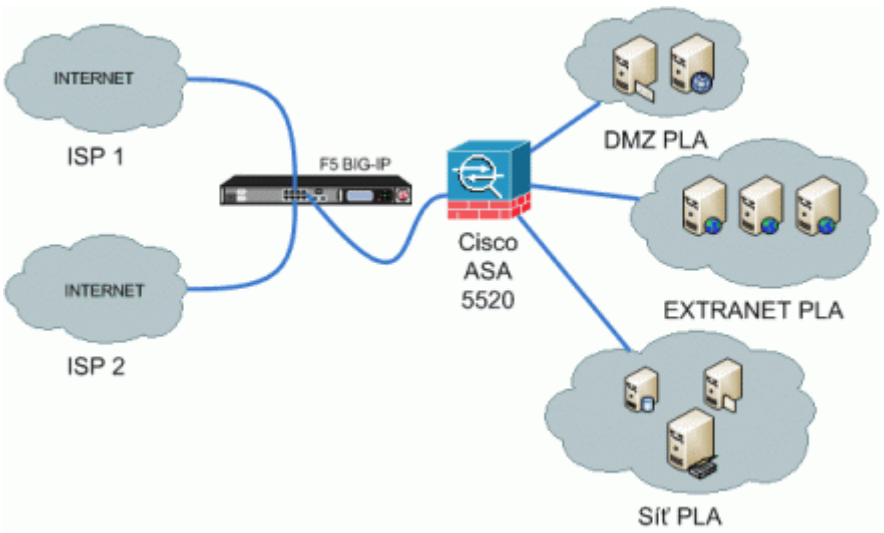
33 virtuálních serverů (8x Linux systém, 2x Novell systém a ostatní jsou Windows systémy v edici 2003 SP2 32bit, 2008 a 2008 R2). Data (virtuální servery) jsou uloženy na centrálním datovém poli a jsou dostupná skrze SAN síť.

### 5.2.6 SAN síť

Organizace využívá SAN síť tvořenou dvěma SAN switch Cisco MDS9124 a dvěma SAN switch Cisco MDS9020. Pomocí této SAN sítě, jak již bylo popisováno výše, jsou propojeny ICT podniku, které využívají centrální datové úložiště.

### 5.2.7 Připojení Internet

Připojení do sítě Internet je realizováno skrze dva ISP tak, aby byla zajištěna redundantní konektivita a zamezilo se výpadkům spojení. Využití redundantního připojení je zajišťováno pomocí ICT prostředku tzv. balanceru od firmy F5. Jelikož jsou rychlosti připojení k sítí Internet rozdílné (ISP 1 – 30 Mb/s, ISP 2 – 5 Mb/s), je balancer nakonfigurován tak, aby 70% datového toku bylo realizováno skrze ISP 1 a 30% bylo realizováno skrze ISP 2. Tímto je zajištěno rovnoměrného rozdělení zátěže.




Obrázek 6 - Schéma připojení k Internetu

### 5.2.8 Síťové prvky využívané v organizaci

K mikrovlnnému propojení v rámci páteřní sítě jsou využívána mikrovlnná (radiová) pojítka značky Alcoma. Organizace využívá v síti WAN a LAN aktivní síťové prvky značek Cisco a F5.

### 5.2.9 Klientské stanice

Na klientských stanicích, dále jen podnikové PC, jsou instalovány operační systémy Windows 2000, XP a v menší míře Windows Vista. Pravidelný upgrade operačních systémů Windows je zajištěn pomocí WSUS (Windows Server Update Services). Pro zajištění přístupu k prostředkům sítě Novell Netware je na podnikových PC instalován Novell klient. Dále je na většině podnikových PC instalován kancelářský balík Microsoft Office.

### 5.2.10 Adresářové služby

Adresářové služby slouží k zajištění správy identit a síťových prostředků. V PLA je využívána adresářová služba eDirectory od firmy Novell. Službu eDirectory lze chápat jako databázi udržující informace o součástech počítačové sítě (tzn. o uživatelích, serverech, tiskárnách, politikách apod.). Tyto informace jsou dále přístupné ostatním prostředkům ICT. Jednou ze základních vlastností eDirectory je autentizace uživatelů. Autentizaci lze provádět skrze nativní prostředí eDirectory například Novell Modular Authentication Service (NMAS) nebo pomocí standardních autentetizačních protokolů například LDAP, RADIUS. Mezi základní rysy eDirectory patří objektovost. Tím je myšlena skutečnost, že informace o součástech sítě jsou udržovány ve formě objektů a jejich vlastností. Množina typů těchto objektů a jim příslušných vlastností neboli schéma eDirectory, je přitom otevřená, lze ji tedy rozšiřovat a upravovat dle potřeby. Vzniklé objekty jsou umísťovány do hierarchické struktury nazývané strom eDirectory.

### 5.2.11 Souborové servery

Zaměstnanci podniku ukládají svoje data primárně na souborový klastr server podniku. Tento server je tvořen dvěma servery s instalovaným operačním systémem Novell NetWare 6.5 SP7 a jsou propojeny v klastr.

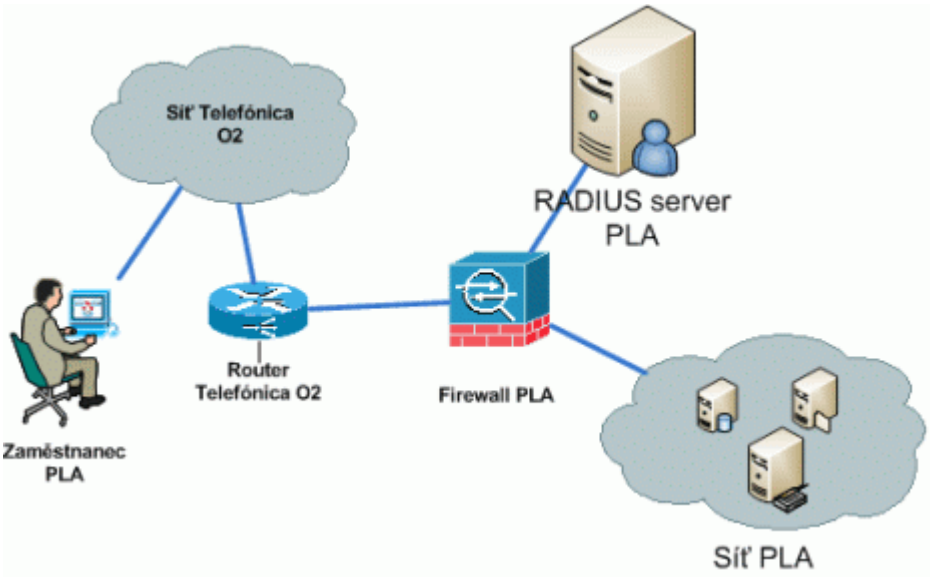
## 5.3 Současné řešení bezpečného připojení do podnikové sítě

V současné době je bezpečné připojení do podnikové sítě řešeno pomocí služby OnePort od společnosti Telefonica O2 a.s. Tato služba nabízí připojení do podnikové sítě s využitím sítě operátora.

### 5.3.1 Technický popis

Každý uživatel, kterému bylo uděleno oprávnění připojovat se vzdáleně do podnikové sítě, obdrží předem nakonfigurovaná CDMA/GPRS modem. Pomocí tohoto modemu se přihlásí do sítě operátora a následně se přihlásí do podnikové sítě pomocí autentizačních údajů s využitím autentizačního RADIUS serveru, který je dále navázán na Novell eDirectory. Technicky je tento přístup řešen ICT zařízením (směrovač) operátora na vnějším perimetru LAN sítě organizace a vlastním firewallem PLA, na kterém probíhá zmíněná autentizace. Celková datová kapacita, pro celou skupinu uživatelů s oprávněním přístupu, je pouhých 512 kbit/s. Toto není důsledkem technického omezení linky, ale je pouze smluvně omezené s vazbou na měsíční paušální poplatek za danou kapacitu linky.

CDMA/GPRS modemy disponují USB rozhraním, nebo je lze připojovat k firemním notebookům skrze rozhraní PCMCIA nebo Express Card. Na následujícím obrázku je schéma současného bezpečného připojení do podnikové sítě.




Obrázek 7 - Schéma aktuálního VPN připojení do podnikové sítě

### 5.3.2 Nevýhody současného řešení

Současné řešení umožňuje připojení do firemní sítě pouze skrze HW zařízení operátora a pouze na území ČR. Mezi další velké nevýhody patří současná velmi malá kapacita daného připojení, konkrétně se jedná o 512 kbit/s pro všechny uživatele služby. Jelikož v současné době službu využívá zhruba 25 zaměstnanců, jedná se v podstatě o datovou linku s agregací 1:25. Na kapacitu datové linky má vliv i to, odkud je realizováno připojení. Pokud budeme realizovat připojení v hustě obydlené části je reálné, že rychlost datového připojení bude nadále klesat dle aktuálního celkového počtu uživatelů připojených na stejnou základovou stanici (BTS).

### 5.3.3 Bezpečnost současného řešení

Jelikož není přístup veřejně dostupný z Internetu, neboť je nutné vlastnit speciální zařízení CDMA/GPRS modem, který je předem nakonfigurován pro členství ve skupině OnePort, tzn. k firemní síti se nelze připojit libovolným CDMA/GPRS modemem, je dané řešení do jisté míry bezpečné. Dalším aspektem bezpečnosti je samotná síť operátora, kde není stoprocentně zajištěno, že přenášená data nebudou v dané síti odposlechnuta či jinak zneužita. Další velkou nevýhodou současného řešení je možné zneužití CDMA/GPRS modemů k připojení se z jiných než firemních ICT podniku. Tato možnost zneužití je omezena pouze vydaným nařízením vedení podniku, které toto jednání přísně zakazuje, ale technicky není omezeno. Není tedy žádným problémem připojit CDMA/GPRS modem pomocí USB rozhraní k domácímu PC zaměstnance podniku a realizovat z něj připojení do podnikové sítě. To s sebou přináší samozřejmě velkou spoustu rizik pro celý IS podniku. Žádný z uživatelů není schopen zajistit srovnatelné podmínky zabezpečení svého domácího PC s podmínkami zabezpečení podnikového ICT prostředku.

## 5.4 Požadavky na nové řešení

Jak již vyplývá z předešlé části, současné řešení bezpečného připojení do podnikové sítě obsahuje některé nedostatky, které by měly být v novém řešení odstraněny. Základním nedostatkem původního řešení je možnost realizovat připojení pouze na území ČR a pouze s využitím datové sítě konkrétního mobilního operátora a možné zneužití CDMA/GPRS modemů pro připojení do podnikové sítě z jiných než podnikových ICT. V následující části je přehled a stručný popis požadavků na nové řešení.

### 5.4.1 Přístup z libovolného místa

Nové řešení by mělo zajistit bezpečný přístup do podnikové sítě z libovolného místa, které bude připojeno k síti Internet s využitím podnikových ICT. Pro zajištění tohoto požadavku je vhodné realizovat nové řešení bezpečného přístupu do podnikové sítě založené na tzv. SSL VPN, které umožňuje přístup i z míst, kde ISP blokuje specifické protokoly nebo porty. Z těchto důvodu povolení, respektive blokace určitých specifických síťových portů za strany ISP, není vhodné VPN typu Remote-Access realizovat pomocí protokolu IPsec. Záměrem celého řešení je zajistit bezpečný přístup do podnikové sítě, ale pouze do podnikové sítě z různých částí sítě Internetu. Toho bude docíleno pomocí personálních firewallů instalovaných na klientských stanicích a v nich definovaných politik, které umožní po připojení se k síti Internet přístup pouze do VPN sítě.

### 5.4.2 Přístup pouze z podnikových ICT

Dalším požadavkem ze strany PLA je zajištění bezpečného připojení do podnikové sítě pouze z podnikových ICT. Tento požadavek je v dnešní době dostupnosti připojení k síti Internet zcela relevantní. Je nutné zajistit, aby se k podnikové síti připojovaly pouze podnikové ICT, a tím byla minimalizována možnost zavlečení jakékoliv formy bezpečnostního rizika (škodlivý kód) do podnikové sítě. Pouze u podnikových ICT jsme schopni vynutit a udržovat dostatečné zabezpečení (aktualizace OS, aktualizovaný antivirus a osobní firewall). Některé z aktuálně dostupných řešení na trhu zajišťující bezpečný přístup do podnikové sítě umožňují tento požadavek zajistit pomocí Network Access Controll, dále jen NAC. Tato funkcionalita umožňuje správcům ICT vynutit politikou konkrétní míru zabezpečení na koncové stanici, která navazuje spojení do VPN. Tyto požadavky se obecně nazývají „Endpoint Security“, neboli zabezpečení na koncovém bodě. Například lze pomocí těchto politik vynutit připojení pouze ICT s aktualizovaným antivirovým softwarem nebo s aktivním osobním firewallem. Dále lze pomocí této funkcionality vynutit přistup pouze podnikových ICT za pomocí vhodně nastavených politik, například pomocí záznamu v registrech u OS Windows, nebo pomocí certifikátu samotného přistupujícího ICT (PC). V současné době při splnění této podmínky není zcela nutné realizovat dvoufaktorovou autentizaci. Variantou může být umožnění přístupu k podnikovým zdrojům ICT v omezené míře s určitou mírou bezpečnosti pomocí SSL VPN portálů.

# 6 ŘEŠENÍ DOSTUPNÁ NA TRHU A JEJICH POROVNÁNÍ

Oblastí bezpečného připojení do podnikové sítě se zabývá bezpočet výrobců ICT. Předem je nutné uvést, že výběrem řešení a jejich následným porovnáním neprošly všechny produkty (zařízení) dostupné v aktuální době na trhu. To není bohužel technicky ani časově možné. Při výběru vhodných produktů se vycházelo ze základních požadavků PLA, jak je již popsáno v předešlé části práce.

## 6.1 Postup výběru

V následující části je popsán postup, jakým způsobem byla vybírána vhodná a dostupná řešení dané problematiky.

### 6.1.1 Prvotní výběr

V prvním kroku byl proveden výběr řešení dostupných aktuálně na trhu a které podle veřejně dostupných informací získaných především ze sítě Internet odpovídají požadavkům PLA. Hlavním požadavkem, který vymezuje danou produktovou skupinu je požadavek na NAC (Network Access Control) na straně klienta, neboli tzv. Endpoint Security, což je kontrola případně vynucení předem daných bezpečnostních parametrů na vzdáleném zařízení, které navazuje zabezpečené připojení do podnikové sítě. Některé produkty byly z důvodu nekompatibility, respektive z důvodu jejich úzce cílenému zaměření na konkrétní operační systém, vyřazeny z výběru. Například produkt společnosti Microsoft Forefront Unified Access Gateway dále jen UAG, který je kompatibilní v plném SSL VPN (zajištěno směrování veškerého síťového provozu do VPN tunelu) s využitím protokolu SSTP, pouze s operačními systémy Windows , a to ještě jenom s nejnovějšími verzemi[1] tohoto operačního systému, konkrétně Windows Vista SP1 nebo Windows 7.

Po prvním kroku výběru a po prvotním odfiltrování produktů dostupných v době psaní práce na trhu, splňuje komplexně požadavky PLA jen několik produktů, které budou dále popsány. Bohužel, produkty dostupné pod OpenSource licencí není možno nasadit z důvodu jejich nekompatibility s požadavkem na zajištění (vynucení) bezpečnostních politik tzv. Endpoint Security na straně vzdáleného klienta.

[1] Zdroj: http://technet.microsoft.com/en-us/library/dd857262.aspx, http://technet.microsoft.com/en-us/library/dd920232.aspx

### 6.1.2 Vybrané řešení dle požadavků PLA

V následující tabulce je seznam produktů dostupných v době psaní práce, které vyhovují požadavkům PLA. Vybrané produkty umožňují shodně až 100 konkurenčních připojení. Produkt Cisco ASA 5520 byl do výběru zahrnut nejen proto, že vyhovuje požadavkům PLA, ale z důvodu jeho současného využívání v PLA. Další porovnání produktů bude popsáno v samostatné kapitole této práce. Někteří z výrobců nabízejí dané produkty i ve virtuálním prostředí. Této možnosti mělo být využito při porovnávání produktů, bohužel jak se ukázalo, využití virtuálních verzí při porovnávání bylo omezené, protože některé virtuální verze jsou omezeny svojí funkčností oproti fyzickým verzím.

Tabulka 1 - Přehled vybraných řešení

| Výrobce | Produkt | Produktové informace | Kontakt |
|---|---|---|---|
| Cisco | ASA 5520 | http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html | E-mail: cz-omg@alefnula.com |
| Juniper Networks | SA 2500 SSL VPN | http://www.juniper.net/us/en/products-services/security/sa-series/sa2500/ | E-mail: info@infinity.cz |
| Barracuda Networks | Barracuda SSL VPN 480 | http://www.barracudanetworks.com/ns/products/sslvpn_features.php | E-mail: barracuda@gestocomm.cz |

### 6.1.3 Oslovení zástupců výrobců

V dalším kroku byli kontaktování zástupci výrobců (prodejci) vybraných třech produktů na našem trhu. Prvotní kontakt proběhl pomocí e-mailové komunikace, popřípadě telefonicky. S některými zástupci byla dohodnuta osobní schůzka, kde byl obecně představen vybraný produkt a nastíněna možnost jeho využití. Při těchto návštěvách byly vzneseny taktéž dotazy ohledně technické specifikace produktů. Díky těmto dotazům bylo možno odvodit některé technické skutečnosti před samotným porovnáním jednotlivých produktů. Osobní

schůzky se ukázaly jako velice přínosné, jelikož na nich došlo k upřesnění technických informací. Na osobních schůzkách mi zástupci výrobců poskytli detailní technické informace, které byly využity při porovnávání vybraných produktů.

## 6.2 Popis vybraných řešení

Řešení vybrané dle požadavků PLA nabízejí do jisté míry obdobné funkcionality zabezpečeného přístupu do podnikové sítě. Jedná se o produkty typu appliance, dále jen zařízení určené k přesně danému účelu vyladěné k co nejvyššímu výkonu. Liší se až v detailech, které budou zhodnoceny v kapitole zabývající se porovnáním. Mezi základní funkce, jak již vyplývá z názvu této práce, je zajištění bezpečného připojení do firemní sítě podniku. Zařízení ASA 5520 od společnosti Cisco nabízí nejenom zajištění bezpečného přístupu do podnikové sítě, ale zajišťuje kompletní ochranu podnikové sítě.

Všechny z popisovaných zařízení nabízejí dva typy Remote-Access VPN přístupu. První typ zajišťuje zabezpečený přístup pouze k aplikacím a prostředkům, které jsou publikovány skrze tzv. VPN portál. Jedná se v podstatě o reverzní proxy server, který zajišťuje autentizovaný přístup k vybraným zdrojům ICT podniku. Je zde umožněn přístup, například na vzdálenou plochu nebo webové rozhraní elektronické pošty, s využitím patřičných Java Appletů nebo ActiveX. Skrze VPN portál lze přistupovat k aplikacím tzv. cloud computingu Cytrix XenApp, atd. Podrobněji budou všechny dostupné funkcionality jednotlivých zařízení vysvětleny při jejich popisu.

Druhým typem Remote-Access VPN je přístup do podnikové sítě realizovaný pomocí speciálního softwaru dále jen VPN klienta. Pomocí tohoto VPN klienta je sestaven SSL VPN tunel, skrze který je směrován veškerý síťový provoz a tím je zprostředkován plnohodnotný přístup do podnikové sítě. Při sestavování SSL VPN tunelu je vzdálenému ICT prostředku přidělena IP adresa z vnitřního rozsahu sítě. Tedy skrze VPN klienta je vytvořen plnohodnotný přístup do podnikové sítě.

Výhodou SSL VPN je, že i v případě plného VPN přístupu jsme schopni detailněji definovat přístup do jednotlivých částí podnikové sítě. Při VPN přístupu využívající IPsec není možnost, jak přesněji určit, kdo kam má přístup, tedy pokud zanedbáme nastavení směrovacích pravidel. Všechna zařízení z níže popisovaných umožňují připojení v jednom okamžiku až sta uživatelů.

### 6.2.1 Barracuda SSL VPN 480

Zařízení Barracuda SSL VPN společnosti Barracuda Networks je zařízení, které v sobě integruje softwarový i hardwarový bezpečný přístup do podnikové sítě. Zařízení podporuje klastrové zapojení, což zajišťuje velmi vysokou dostupnost VPN řešení. Díky zařízení lze přistupovat k interním ICT z libovolného místa v sítí Internet. Pro přístup lze využít webový prohlížeč nebo plnohodnotného VPN klienta (Barracuda Network Connector). Konfiguraci a správu zařízení lze provádět skrze integrované webové rozhraní. Barracuda SSL VPN nabízí vysokou míru detailního rozdělení bezpečnostní politiky a řízení zdrojů. Správce systému je schopen uživatelům Barracuda SSL VPN delegovat různou míru bezpečného přístupu k zdrojům ICT. Zařízení umožňuje dva typy Remote-Access VPN, a to s využitím instalovaného VPN klienta (Barracuda Network Connector) nebo využitím pouze webového prohlížeče. S využitím webového prohlížeče mají uživatelé zajištěn přístup k webovým aplikacím, které jsou jim nabízeny dle aktuální konfigurace. V tomto případě funguje Barracuda jako reverzní proxy server. Další možností využití webového prohlížeče je ke spouštění speciálně definovaných aplikaci, jako je RDP klient, VNC klient, atd. Tato možnost je podmíněna pouze instalovaným JRE (Java Runtime Environment) v klientském počítači, jelikož všechny výše popisované aplikace se spouštějí formou Java Appletu. Skrze webový prohlížeč probíhá i kontrola klientské stanice, zda vyhovuje nastaveným podmínkám pro Endpoint Security. Pokud nelze kontrolu provést, je uživateli odepřen přístup, nebo jsou mu zpřístupněny jen některé funkce. Například je uživateli povolen pouze přistup k webovému rozhraní elektronické pošty. Při připojení pomocí instalovaného VPN klienta (Barracuda Network Connector) je zajištěn plnohodnotný přístup do podnikové sítě, připojovanému klientovi je přidělena IP adresa z vnitřního rozsahu sítě. Při využití instalovaného VPN klienta je taktéž prováděna kontrola Endpoint Security, tedy kontrola, zda uživatel vyhovuje přednastaveným pravidlům. Barracuda SSL VPN umožňuje úplnou kontrolu nad prostředky určenými pro externí přístup jako jsou vnitřní webové aplikace, souborové systémy a další aplikace. Jak již je popsáno výše, podpora pro SSL tunelování přímo z webového prohlížeče je řešena prostřednictvím Barracuda SSL VPN Agent, což je Java klient, který podporuje několik aplikací, včetně služby Vzdálená plocha, Citrix XenApp, VNC, NX, SSH a Telnet. Robustní zabezpečení a funkce auditování umožňuje administrátorům definovat vlastní politiky, které budou upravovat a monitorovat přístup k vnitřním zdrojům pro určité

uživatele nebo skupiny. Pro zvýšení bezpečnosti jsou data nahrávána v průběhu relace VPN na interní zdroje ICT, testována na viry a další malware, aby se zabránilo infekci interních zdrojů. Pro bezpečné připojení z veřejně dostupných míst pomocí webového prohlížeče, jako je například knihovna, internetová kavárna a tak podobně, je využívána funkce „Cache cleanig“. Tato funkce zajistí, že veškerá data uložená během probíhající relace budou po odhlášení uživatele smazána.

#### *6.2.1.1 Základní popis konfigurační logiky*

Pro jasnější představu o možnostech konfigurace zařízení je nutné popsat logiku konfigurace daného zařízení. Respektive základní konfigurační moduly, ze kterých se při konfiguraci vychází.

Konfigurace zařízení se provádí skrze webové rozhraní a rozděluje se na čtyři základní moduly:

- BASIC
- RESOURCE
- ACCESS CONTROL
- ADVANCE

BASIC

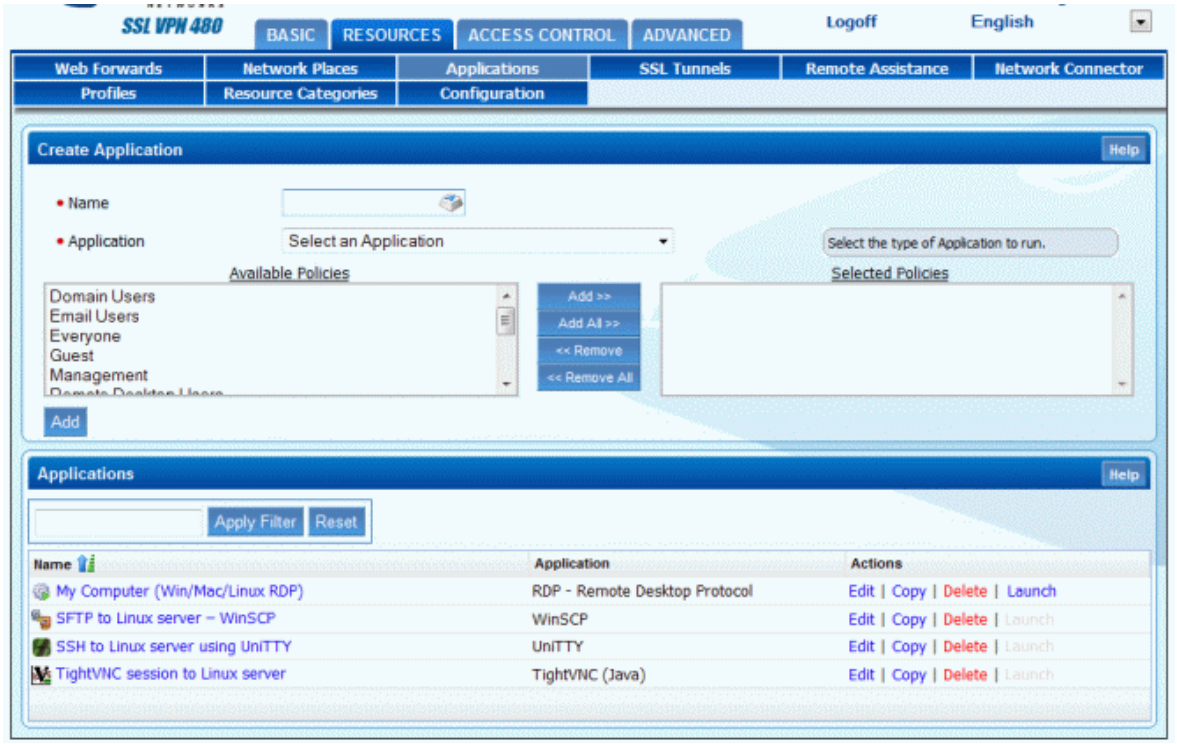
Slouží k zajištění a konfiguraci všech dostupných informací, které jsou v průběhu provozu logovány. Jsou zde přehledně zobrazeny statistické informace o vytížení serveru, o realizovaných spojeních a například detailní audit logy jednotlivých uživatelů, kteří zařízení využívají.

RESOURCES

Základním konfiguračním modulem zařízení jsou tzv. Resources (zdroje). Jak již z názvu vyplývá, jedná se o část systému, který obsluhuje dostupné zdroje neboli dostupné prostředky ICT z vnitřní sítě podniku. Přístup k definovaným zdrojům je na základě nastaveného oprávnění. Zdroje lze dále kategorizovat [14].

Dále je uveden seznam použitelných zdrojů:

- Web Forwards – umožňuje definovat vzdálené webové zdroje, jako je například přístup k webovému rozhraní elektronické pošty
- Network Places - přístup k sdíleným prostředkům ve vnitřní síti
- Application – umožňují spouštět definované a podporované aplikace, podmínkou je instalace ActiveX nebo Java apletu na webovém prohlížeči
- SSL Tunnels – Vytvoří zabezpečené spojení se specifickým zařízením ve vnitřní síti podniku
- Network Connector – Získání plného přístupu do vnitřní sítě.

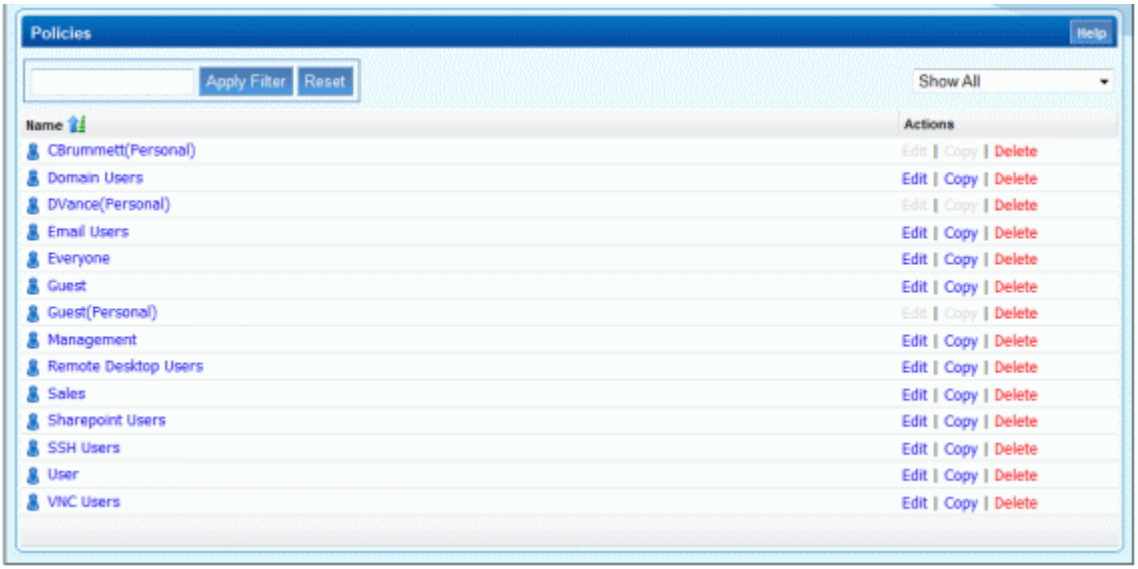



Obrázek 8 - Barracuda Resouces - Applications

ACCESS CONTROL

Řízení a definování oprávnění je v zařízení propracováno do nejmenších detailů. Zařízení umožňuje velmi vysokou míru škálovatelnosti v oblasti řízení přístupových práv. Přístupová práva lze definovat na objekty tzv. Polices (politiky). Díky politikám lze přidělovat oprávnění na další části systému, konkrétně třeba na zdroje [14].

Zařízení podporuje autentizaci s využitím Active Directory, LDAP, RADIUS. Podporuje dvoufaktorové autentizační mechanismy včetně technologie OTP (One-Time Password) RSA SecurID a VASCO Digipass s využitím RADIUS serveru.




Obrázek 9 - Barracuda Policy

ADVANCE

Slouží ke konfiguraci, jak již z názvu vyplývá, rozšířených nastavení zařízení, jako je například konfigurace použité verze šifrování (AES, 3DES) a síly šifrování. Dále slouží k podrobné konfiguraci logování.

#### *6.2.1.2 Parametry*

Následující tabulka obsahuje souhrnný přehled parametrů[2] daného zařízení.

[2] Zdroj: http://www.barracudanetworks.cz/barracuda-networks-produkt-barracuda-networks-ssl-vpn.htm .

Tabulka 2 - Přehled parametrů Barracuda SSL VPN 480

| **Barracuda SSL VPN 480** | |
|---|---|
| | |
| Počet současně pracujících uživatelů | 100 |
| | |
| Ethernet rozhraní | 1 x 10/100 |
| | |
| Zabezpečený SSL tunel | ANO |
| Instalovatelný klient Barracuda Network Connector | ANO |
| Zpřístupnění interní webové aplikace | ANO |
| Zpřístupnění interních sdílených disků | ANO |
| Sdílení pomocí Windows Explorer | ANO |
| Aplikace VNC, NX, Telnet, SSH a RDP (vzdálená plocha) | ANO |
| Jednotné přihlašování jedním heslem | ANO |
| Ochrana proti viru | ANO |
| Virtuální klávesnice | ANO |
| Integrace s Active Directory/LDAP | ANO |
| Vícevrstvá schémata přihlášení | ANO |
| Víceuživatelský realm | ANO |
| Barracuda SSL VPN Server Agent | ANO |
| Podpora hardware Token zabezpečení | ANO |
| Autorizace pomocí RADIUS | ANO |
| Aplikační rozhraní/SNMP | ANO |
| Systémové logování SYSLOG | ANO |
| Konfigurace s redundantními disky (RAID) | ANO |

#### *6.2.1.3 Podporované typy autentizace podrobněji*

V následující tabulce je seznam podporovaných metod autentizace [14]. U každé z metod autentizace je uvedeno, zda autentizace může být použita jako primární, nebo sekundární. Pokud má autentizační metoda oba typy, tedy primární/sekundární, může být použita v obou případech.

Tabulka 3 - Podporované typy autentizace

| Autentizace | Typ |
|---|---|
| Klientský certifikát | Primary/Secondary |
| IP Adresa | Primary/Secondary |
| Heslo | Primary/Secondary |
| PIN | Primary/Secondary |
| Veřejný klíč | Primary/Secondary |
| RADIUS | Primary/Secondary |
| OTP (One-Time Password) | Secondary |
| Osobní otázka | Secondary |

#### *6.2.1.4 Endpoint Security*

Jak již bylo popisováno výše, zařízení umožňuje provádět kontrolu na koncovém zařízení, a to konkrétně kontrolu na verzi operačního systému, přítomnosti konkrétní záplaty operačního systému a mnoho dalších. Bohužel nepodporuje kontrolu hodnot v registrech OS Windows.

#### *6.2.1.5 Pořizovací náklady*

Tabulka níže uvedená obsahuje přehled nákladů za jeden rok na dané zařízení. Veškeré ceny jsou bez DPH. Cena zařízení je včetně licencí pro 25 uživatelů, kteří se mohou připojovat ve stejný okamžik tzv. Concurrent User License. Licence Energize Update slouží pro aktualizaci interního antivirového softwaru. Licence Instant Replacement představují servis na HW. Veškeré informace k licencím a cenám jsou dle podkladů od distributorů daného zařízení v ČR.

Tabulka 4 - Pořizovací náklady Barracuda SSL VPN 480

| Zařízení | Náklady |
|---|---|
| Barracuda SSL VPN 480 | 119 999,00 Kč |
| **Licence** | |
| Barracuda Energize Updates na 1 rok | 33 499,00 Kč |
| Barracuda Instant Replacement na 1 rok | 26 499,00 Kč |
| **Náklady celkem** | **179 997,00 Kč** |

### 6.2.2 Juniper SA 2500 SSL VPN

Jako v předešlém případě se jedná o HW zařízení, které pro zajištění bezpečného připojení do podnikové sítě využívá svých softwarových a hardwarových prostředků. Konfigurace se provádí pomocí velice přehledného intuitivního webového rozhraní. Zařízení umožňuje bezpečné připojení typu Remote-Access VPN do podnikové sítě. Umožňuje klastrové zapojení, což zajišťuje velice vysokou dostupnost VPN řešení. Jako v předešlém případě je umožněno využít k vytvoření bezpečného připojení do podnikové sítě dvou metod. První metodou je připojení skrze webový prohlížeč. Druhá metoda je založena na využití instalovaného VPN klienta a vytvoření plného VPN připojení do podnikové sítě. Využití pouze webového prohlížeče má opět některé výhody, ale i nevýhody. Skrze webový prohlížeč, bez instalovaného Java Appletu nebo ActiveX prvků, můžeme získat přístup pouze k interním zdrojům ICT, především aplikace s webovým rozhraním. V tomto případě se opět jedná o zprostředkování zdrojů formou reverzní proxy. Výhodou tohoto řešení je, že ho lze realizovat z jakéhokoliv ICT prostředku s podporovaným webovým prohlížečem. Nevýhodou toho způsobu připojení je to, že uživatelé mají povolen přístup jen k „nevýznamným“ částem ICT podniku, respektive takto bývá standardně konfigurováno. To je celkem logické, jelikož při připojení bez podpory Java Appletu nebo ActiveX není možné provést Endpoint Security prověření a není tedy zaručeno, že se jedná o zabezpečené PC, či jiný ICT prostředek. Využitím připojení skrze webový prohlížeč s podporou Java Appletu nebo ActiveX můžeme jednak provádět kontrolu Endpoint Security a zároveň lze využívat některé aplikace, jako jsou například RDP a VNC, případně spouštět aplikace Citrix XenApp. Zařízení disponuje funkcionalitou zvanou Secure Virtual Workspace. Jedná se o virtuální pracovní plochu, která se vytváří na základě definovaných pravidel. Uživateli, který se připojuje z nezabezpečeného místa (knihovna, internetová kavárna) nebo nevyhoví pravidlům nastavených v konfiguraci Endpoint Security, v tomto případě se jedná o funkci Host Check, je vnuceno spuštění virtuální pracovní plochy Secure Virtual Workspace. V této virtuální pracovní ploše může uživatel bezpečně vykonávat veškeré potřebné aktivity a je zaručeno, že jakékoliv informace týkající se dané relace nemohou být logovány nebo jinak zneužity skrze hostitelské PC. Po ukončení SSL VPN relace je virtuální plocha kompletně odstraněna. Správce SSL VPN může detailně definovat, jaké prostředky umožní virtuální plocha převzít z hostitelského

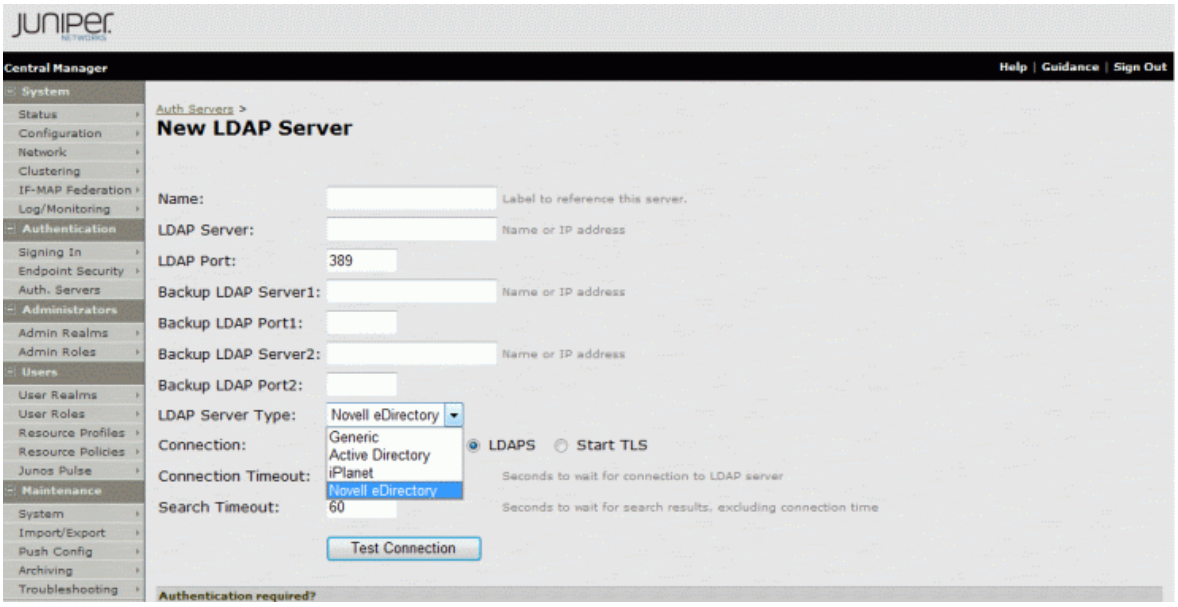
PC. Například lze definovat, zda budou přístupny lokální disky ve virtuální ploše, zakázán konkrétní software, atd.

#### *6.2.2.1 Základní konfigurační logika*

Pro vytvoření obecné představy o konfiguračních možnostech zařízení je nutné opět nejprve popsat některé základní konfigurační objekty zařízení.

Authentication Servers

Autentizační servery jsou základním konfiguračním objektem, určují typ a druh autentizace. Například může při vytváření autentizačního serveru využít jako zdroj autentizačních údajů lokální uživatelskou databázi nebo LDAP server, RADIUS server, atd.




Obrázek 10 - Vytvoření autentizačního serveru

User Roles

Uživatelské role umožňují definovat parametry uživatelské relace. Definujeme, zda daná role umožňuje využívat zdroje (RDP, Telnet/SSH) nabízené zařízením. Uživatelské role jsou následně přiřazovány k uživatelským účtům v uživatelských doménách (oblastech). Samotné uživatelské role nedefinují zdroje zařízení, pouze nastavují, zda daný uživatel může zdroje využívat.

Resource Profile

Pomocí tohoto konfiguračního objektu definujeme zdroje, které jsou dále poskytovány uživatelům.

User Authentication Realms

Uživatelské autentizační domény (oblasti) přiřazují uživatelské role a autentizační schéma (autentizační server) daným uživatelům. Díky tomu může podrobněji rozdělit autentizaci a nabízené zdroje pro jednotlivé domény. Toho lze využít při plánování poskytovaných zdrojů uživatelům zařízení. Příkladem by mohlo být rozdělení podle pozice v podniku. Například obchodní oddělení bude mít přístupné jiné zdroje (jinou doménu) než management podniku.

#### *6.2.2.2 Podporované typy autentizace*

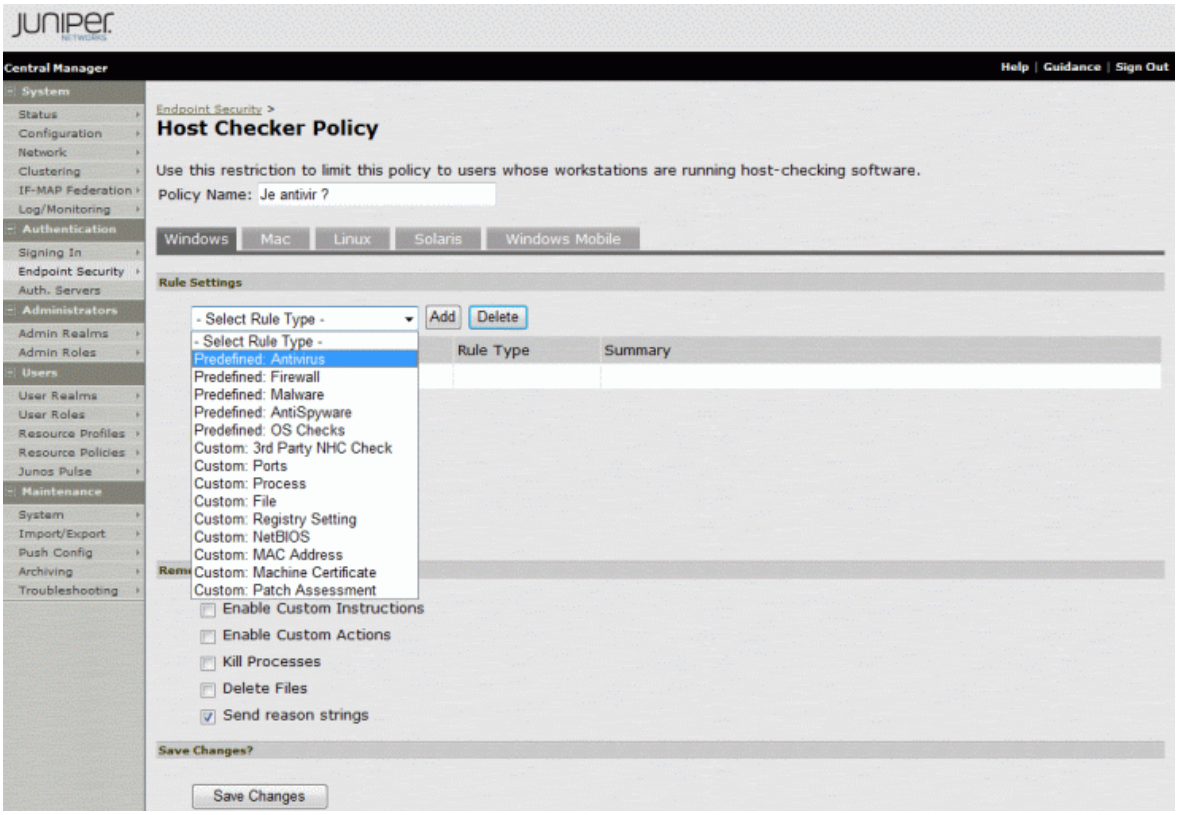
Zařízení podporuje mnoho autentizačních metod, dále jen AAA (Authentization, Authorization, Accounting) schémata. Podporována je dvoufaktorová autentizace založená na OTP (One-Time Password), eToken. Zařízení využívá pro podporu dvoufaktorové autentizace dvě metody, a to ACE (RSA ACE server) a využití RADIUS server autentizace [16].

Celkový přehled podporovaných typů autentizace:

- LDAP
    - Microsoft Active Directory
    - Sun ONE (iPlanet)
    - Novell eDirectory
    - OpenLDAP
- NIS
- ACE
- RADIUS
- Active Directory/NT
- SiteMinder
- SAML

#### 6.2.2.3 *Endpoint Security*

Kontrola zabezpečení připojujícího se koncového zařízení je velice propracovaná. Funkce kontroly zabezpečení koncové stanice se nazývá „Host Checker“. Při kontrole lze nastavit velice mnoho různých druhů kontrolních prvků. Můžeme nastavit kontrolu na konkrétní verzi antivirového programu s přesnou dobou stáří virových definic [12]. Na základě této kontroly můžeme vyvodit další postup, například umožnit přístup k omezeným zdrojům nebo vynutit spuštění Secure Virtual Workspace, popřípadě vynutit jiné akce. Tato kontrola je zajištěna pomocí ActiveX nebo Java Appletu, popřípadě speciální aplikací, která se nabízí k instalaci při přihlášení.




Obrázek 11 - Juniper SA 2500 SSL VPN - Host Checker

#### 6.2.2.4 *Pořizovací náklady*

Tabulka č. 5 obsahuje informace o nákladech spojených s daným zařízením. Veškeré ceny jsou bez DPH. Veškeré informace k licencím a cenám jsou dle podkladů od distributorů daného zařízení v ČR.

Tabulka 5 - Pořizovací náklady Juniper SA 2500 SSL VPN

| Zařízení | Náklady |
|---|---|
| Juniper SA 2500 SSL VPN | 34 000,00 Kč |
| **Licence** | |
| Add 25 simultaneous users to SA 2500 | 67 252,00 Kč |
| Juniper Care NextDay Support for SA2.5K-L (10-49U) na 1 rok | 8 704,00 Kč |
| **Náklady celkem** | **109 956,00 Kč** |

### 6.2.3 Cisco ASA 5520

Zařízení Adaptive Security Appliances společnosti Cisco se od výše jmenovaných liší svojí funkčností. Neslouží výhradně jenom k vytváření zabezpečeného SSL VPN připojení do firemní sítě, ale zajišťuje komplexní ochranu vnitřní sítě. Integruje v sobě firewall, IPS (Intrusion prevention system) a SSL VPN. Jak již bylo zmíněno v předešlé části, toto zařízení je již integrováno do stávající infrastruktury PLA, kde zajišťuje ochranu vnitřních ICT zdrojů podniku. Zařízení, stejně jako dříve popisovaná zařízení, podporuje dva typy Remote-Access VPN založené na SSL VPN. Opět jako u předcházejících dvou zařízení lze k přístupu do podnikové sítě využít pouze webový prohlížeč nebo plnohodnotného VPN klienta.

Při využití webového klienta využíváme dva módy, a to tzv. „Clientless“ a „Thin client“. V módu „Clientless“ potřebuje uživatel pro přístup k vnitřním zdrojům sítě pouze webový prohlížeč, ale jeho přístup je omezen pouze ke zdrojům, které využívají pro komunikaci HTTPS nebo HTTPS protokol [13]. Mód „Clientless“ je v podstatě přístup k interním zdrojům pomocí reverzní proxy. V módu „Thin client“ je taktéž využíván webový prohlížeč, do kterého je doinstalován Java Applet popřípadě ActiveX. Díky přítomnosti Java Appletu nebo ActiveX lze využívat přístup k interním zdrojům skrze tunelování protokolu TCP, popřípadě lze využívat předefinované aplikace založené na Java Appletu nebo ActiveX (RDP, VNC, atd.). Oba módy, tedy jak Clientless“ tak „Thin client“, jsou pro přehlednost v dalších částech práce sjednoceny pod jeden název, a to Clientless. Pokud je vyžadován plný VPN přístup do podnikové sítě, je nutné využít Cisco AnyConnect VPN klient, který je nutné instalovat na klientské PC nebo jiný podporovaný ICT prostředek.

Stejně tak jako předešlé popisované zařízení umožňuje i toto zařízení provádět kontrolu bezpečnosti na zdrojovém ICT zařízeni (PC), ze kterého je navazováno spojení tzv. Endpoint Security. Lze kontrolovat obsah registrů, soubor na disku, spouštěný proces, verzi antivirového softwaru a mnoho dalších parametrů. Na tuto kontrolu opět navazují politiky přiděleného oprávnění k vnitřním zdrojům podniku. Na základě Endpoint Security lze rozpoznat, z jakého místa se uživatel připojuje. V režimu Clientless (využití webového prohlížeče) umožňuje zařízení vytvořit po provedené autorizaci bezpečný šifrovaný prostor tzv. Secure Desktop [13], do kterého jsou ukládána všechna citlivá data během trvající relace. S využitím funkce Endpoint Security a tohoto šifrovaného prostoru (Secure Desktop), jsme schopni zajistit zabezpečený přístup k interním zdrojům z jakéhokoliv místa sítě Internet.

#### *6.2.3.1 Základní konfigurační logika*

Ke konfiguraci slouží software Adaptive Security Device Manager, dále jen ASDM společnosti Cisco nebo lze využít CLI (Command-line interface). Konfigurace zařízení, respektive jeho části zajišťujících SSL VPN, lze přibližně popsat několika základními objekty konfigurace. V další části textu si některé z konfiguračních objektů popíšeme. Upozorňuji, že se nejedná o kompletní výčet všech konfiguračních objektů.

Group Policies

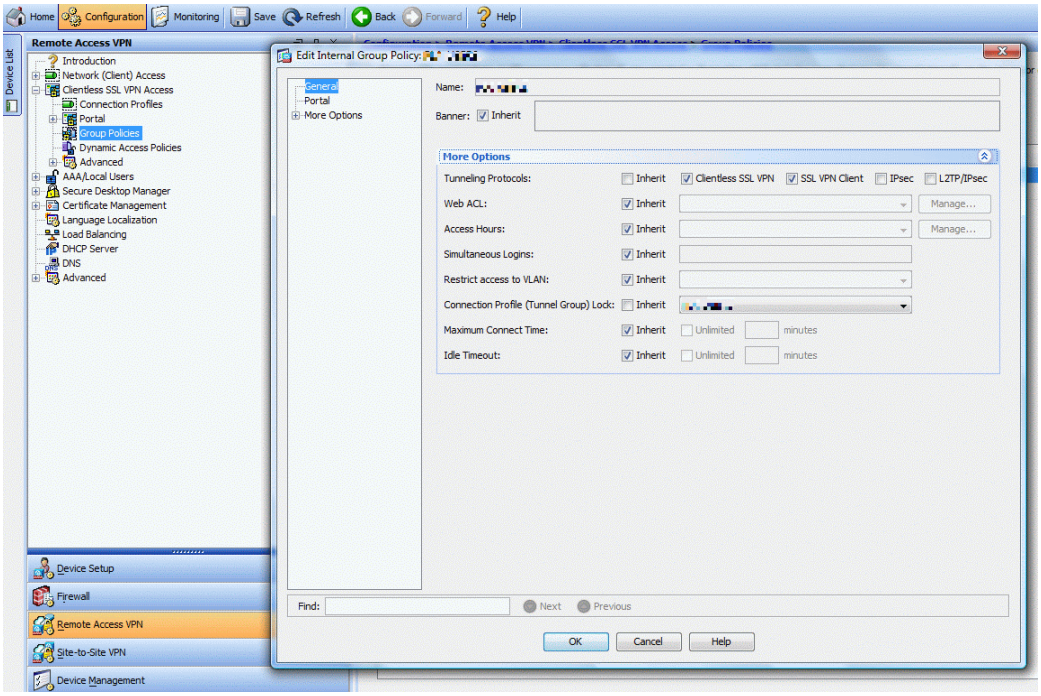
Jedná se o kolekci uživatelských atributů a hodnot uložených v interní databázi nebo externě, například v RADIUS nebo LDAP serveru. Slouží k nastavování síťových a bezpečnostních politik na vytvořenou uživatelskou relaci.

Group Policies jsou založeny na sdíleném modelu a lze je rozdělit do tříd:

- Default Group Policy
- Group Policy
- User Policy

Ve sdíleném modelu dědí uživatelská relace atributy a politiky z uživatelských politik, které je dědí z nadřazených skupinových politik a ty je dědí z nadřazených defaultních skupinových politik. Pokud jsou politiky nadefinovány, jsou navázány na tzv. Tunnel Group. Pokud uživatel naváže VPN relaci na daný Tunnel Goup, neboli VPN

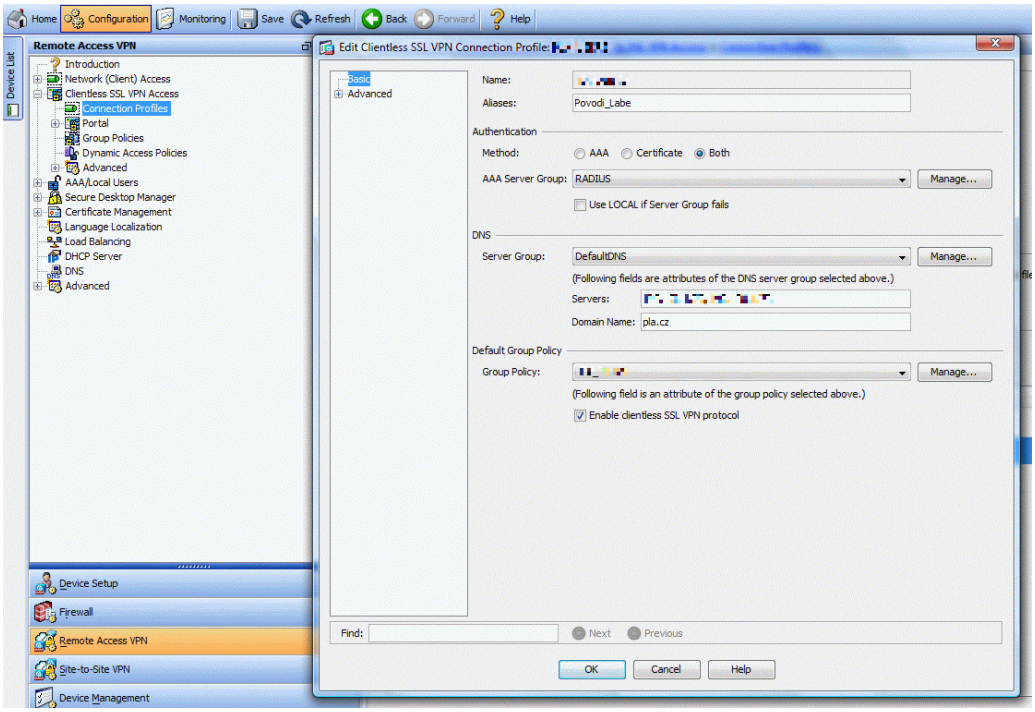
Connection Profile, jsou mu automaticky přiděleny všechny politiky dle nastavené Group Policy, která je k danému Connection Profile přidělena.




Obrázek 12 - Group Policies

Tunnel Group

Definuje typ použité autentizace, rozhraní očekávající připojení, DNS server a mnohé další parametry. Dále zde definuje, na jaké URL se budou uživatelé připojovat, aby mohli využívat daný Connection Profile.




Obrázek 13 - Connection Profile (Tunnel Group)

Dynamic access policies

Pomocí dynamických přístupových politik konfigurujeme přístupová práva k vnitřním síťovým zdrojům na základě kolekce atributů získaných z klientské relace. Konkrétně atributy klientské relace, podle kterých konfigurujeme přístupová práva, získáváme pomocí Cisco Secure Desktopu, který si popíšeme v další části diplomové práce.

### *6.2.3.2 Podporované typy autentizace*

Zařízení podporuje následující typy autentizací:

- RADIUS
- LDAP
- Kerberos
- NT Domain
- TACACS+
- SDI

#### *6.2.3.3 Endpoint Security*

Zajištění kontroly koncové stanice při vytváření relace tzv. Endpoin Security v rámci řešení Cisco ASA se nazývá Cisco Secure Desktop, dále jen CSD. Funkci CSD lze popsat následovně. Při prvním navazování spojení do podnikové sítě je stažena klientská komponenta ActiveX nebo Java Applet. Tato komponenta provede sken vzdáleného PC, aby zjistila informace, například verzi operačního systému, instalované servis packy, instalovaného antivirového softwaru, přítomnost specifického klíče v registru a mnoho dalších parametrů. Takto lze prověřil nejenom koncové stanice s operačním systémem Windows, ale i s jinými operačními systémy například Linux, Mac OS a další. U koncových stanic s operačním systémem jiným než Microsoft Windows, lze využít modul CSD tzv. Host Scan. Pomocí tohoto modulu lze provádět kontrolu na spuštěné procesy a specifické síťové porty, přítomnost souboru na disku.

CSD se skládá z více modulů, jak již je popsáno výše, neobsahuje pouze nástroje k prověření koncové stanice. Dalším modulem CSD je tzv. Secure Desktop. Jedná se šifrovanou část, která se vytváří na vzdáleném systému, ze kterého bylo vytvořeno VPN připojení skrze webový prohlížeč (Clientless) a slouží k ukládání citlivých dat vytvořených během relace. Příkladem může být zaměstnanec, který se připojuje do podnikové sítě z hotelového PC. Jelikož nevyhoví nastavené politice CSD, je mu vynucen přístup s využitím Secure Desktop. Tím je zajištěno, že citlivá data vytvářená během vzniklé relace jsou dostatečně zabezpečena. Po ukončení relace se celá šifrovaná část vymaže. Správci CSD je umožněno nastavovat, jaký software může být v průběhu Secure Desktop na vzdáleném klientovi spouštěn, popřípadě jaké zdroje vzdáleného klienta (hostitelského PC) budou povoleny (tiskárny, lokální disky). CSD modul Secure Desktop lze využít pouze na koncových stanicích s operačním systémem Windows [13].

Dalším modulem CSD je Cache Cleaner. Tento modul slouží k vymazání citlivých dat uložených na koncové stanici po ukončení relace připojení. Využití tohoto modulu je i na operačních systémech Linux a Mac OS.

#### *6.2.3.4 Pořizovací náklady*

Tabulka č. 6 obsahuje informace o nákladech na dané zařízení. Veškeré ceny jsou bez DPH. Cena samotného zařízení není započtena, protože dané zařízení je již ve vlastnictví podniku. Pro realizaci SSL VPN je nutné zakoupit pouze patřičné licence.

Tabulka 6 - Pořizovací náklady Cisco ASA 5520

| Zařízení | Náklady |
|---|---|
| Cisco ASA 5520 | 0,00 Kč |
| **Licence** | |
| ASA 5500 SSL VPN 25 Premium User License | 33 580,00 Kč |
| ASA 5500 Advanced Endpoint Assessment License for SSL VPN | 10 795,00 Kč |
| **Náklady celkem** | **44 375,00 Kč** |

## 6.3 Porovnání vybraných řešení

Jak již bylo popsáno výše, k porovnání řešení byly použity jejich detailní technické specifikace a jejich virtuální verze. Aby nebylo porovnání provedeno pouze v teoretické rovině a pomocí virtuálních verzí, které jak již bylo upozorněno, nejsou funkčností plně srovnatelné s fyzickými verzemi, byli zástupci výrobců požádáni o předvedení zařízení v produkčním prostředí. To se ukázalo jako velice přínosné, jelikož mohli být dotázáni i správci jednotlivých zařízení v produkčním prostředí, kteří popsali přednosti daného zařízení, ale zároveň upozornili na jeho nedostatky.

Někteří výrobci nabízejí zapůjčení vybraného řešení na testování, ale čekací lhůty na zápůjčku u některých zařízení jsou v řádech týdnů a je s tím spojena i veškerá zodpovědnost za zapůjčené zařízení. V případě jeho poškození nebo ztráty musí být vyrovnány veškeré náklady spojené s případnou opravou, či náhradou. Po zjištění těchto skutečností byly k porovnání daných zařízení použity z části reference od správců daných zařízení, technické detaily a dále pak z části porovnání virtuálních verzí některých zařízení.

Porovnání zařízení bylo rozděleno do několika etap. První etapa byla zahájena už při prvotním výběru, kdy byl kladen důraz na to, aby zařízení splňovala požadavky PLA, jak bylo popisováno v přecházejících částech práce a tím došlo k vyfiltrování některých vhodných VPN řešení dostupných v současné době na trhu.

V druhé etapě byla zařízení porovnána z pohledu jejich technické funkcionality například možné typy autentizací, jak podrobně lze specifikovat politiky NAC respektive Endpoint

Security, z pohledu jejich administrace a ovládání a dále pak jaké nároky jsou kladeny na integraci do stávajícího informačního systému PLA.

Ve třetí etapě byla zařízení porovnávána z ekonomického pohledu včetně všech případných investic do zařízení při jeho nasazení do produkčního prostředí, což byl jeden z nejvíce hodnotících parametrů.

### 6.3.1 Správa a konfigurace

V následující části se zaměříme na porovnání popsaných zařízení z pohledu jejich správy. Zařízení společnosti Barracuda Networks a Juniper Networks disponují velice propracovaným webovým konfiguračním rozhraním, které umožňuje detailní konfiguraci daného zařízení. Třetí popisované zařízení od společnosti Cisco lze konfigurovat skrze Win32 aplikaci s názvem ASDM. Tato aplikace slouží ke konfiguraci nejenom VPN části zařízení ASA, ale i ke konfiguraci ostatních funkčních celků daného zařízení. Pokud budeme porovnávat dané zařízení i z pohledu intuitivnosti jejích ovládání, lze jednoznačně říci, že zařízení společností Barracuda Networks a Juniper Networks svojí intuitivností ovládání vynikají nad zařízením společnosti Cisco. U obou získáte hned v úvodní stránce webového konfiguračního rozhraní přehled o celkové provozní situaci. Dále jsou zde sumárně zobrazeny informace o kritických stavech, které se vyskytly během provozu. Celkově lze říci, že webové konfigurační rozhraní obou zařízení je velice povedené a z pohledu správy a konfigurace jsou srovnatelné. Nicméně zřízení společnosti Barracuda Networks vyniká další funkcionalitou, a to velice propracovanou koncepcí přidělování zdrojů SSL VPN portálu pro konkrétní uživatele.

### 6.3.2 Zajištění funkce Endpoint Security

Dalším požadavkem na funkcionalitu, který byl ze strany PLA vyžadován, bylo zajištění kontroly bezpečnosti koncových přístupových bodů, respektive PC, ze kterých je navazována relace a případné vynucení bezpečnostních politik. Konkrétně povolení přístupu pouze z podnikových ICT, a pokud bude přístup z jiného než podnikového PC, zajistit dostatečnou míru bezpečnosti. Všechna popisovaná zařízení umožňují zajistit kontrolu přistupujících zařízení. Nejméně vhodným, z pohledu zajištění kontroly přístupu pouze podnikových ICT a případně zajištění větší bezpečnosti při přístupu z jiných než podnikových ICT, se ukázalo řešení od společnosti Barracuda Networks. Toto zařízení

nedokáže provádět kontrolu hodnot databáze registrů vzdáleného přístupového bodu provozovaného na platformě Windows. V případě zajištění větší míry bezpečnosti při přístupu z jiných než podnikových ICT, nabízí pouze funkci „Cache Cleaner“, která odstraní všechny uložené citlivé informace po ukončení relace. Nicméně jako jediný z porovnávaných zařízení nabízí antivirovou kontrolu dat, která jsou skrze SSL VPN tunel přenášena.

Zařízení od společností Juniper Networks a Cisco umožňují velice detailní kontrolu zabezpečení na straně klienta. Zařízení od společnosti Cisco dokáže dokonce na základě nastavených politik vynutit akce na vzdáleném přístupovém bodu, například aktualizaci antivirového softwaru.

Zařízení od společnosti Cisco a od společnosti Juniper Networks umožňují zajistit větší míru zabezpečení při přístupu z jiného než podnikového ICT, a to pomocí speciální technologie tzv. vault (trezor) technologie. Jedná se o systém, který dokáže na hostitelském zařízení před sestavením vlastní VPN relace při využití webového prohlížeče vytvořit bezpečně oddělené prostředí. V takto bezpečně odděleném prostředí od hostitelského systému můžeme přistupovat k interním zdrojům podniku. Díky tomuto „trezoru“ nemůže dojít ke zneužití interních dat ze strany hostitelského systému. Dále obě zařízení umožňují použít další funkcionalitu tzv. Cache Cleaner, obdobně jako řešení od Barracuda Networks. Z pohledu kontroly zajištění bezpečnosti na straně vzdáleného VPN klienta je jednoznačně na prvním místě zařízení společnosti Cisco, dále pak zařízení společnosti Juniper Networks a na posledním místě zařízení společnosti Barracuda Networks.

### 6.3.3 Nároky na integraci do stávajícího IS podniku

Výběr zařízení k porovnání byl i z pohledu nároků na integraci do stávajícího IS podniku. Byl kladen důraz na zajištění kompatibility v hlavních funkčních částech porovnávaných zařízení, jako je autentizace, síťové protokoly a mnoho dalších. Z těchto důvodů jsou všechna porovnávaná zařízení srovnatelná. Nespornou výhodu má zařízení společnosti Cisco, které je do IS podniku již integrováno a plní zde funkci firewallu. Výhodou porovnávaných zařízení je jejich provedení ve formě tzv. appliance, tedy určené k přesně danému účelu, vyladěné k co nejvyššímu výkonu. Díky této skutečností odpadají nároky na instalaci případného softwaru a další vícepráce při instalaci. Všechna zmíněná zařízení jsou uzpůsobena na montáž do speciálních skříní tzv. racků. Z pohledu nároků kladených na

integraci do podnikové sítě, vychází nejlépe ASA 5520 společnosti Cisco, jelikož je v IS podniku již provozováno.

### 6.3.4 Zhodnocení pořizovacích nákladů

V následující tabulce jsou informace týkající se nákladů na pořízení zařízení, 25 ks konkurenčních licencí a následné roční náklady na licence případně HW servis. Z tabulky vyplývá, že řešení založené na Cisco ASA 5520 představuje nejmenší náklady na pořízení a případný provoz. Nulové hodnoty u tohoto zařízení týkající se pořizovacích a ročních nákladů, jsou způsobeny tím, že zařízení je již v IS podniku provozováno a veškeré tyto náklady jsou již pravidelně hrazeny a nepředstavují tak nové zatížení rozpočtu podniku.

Tabulka 7 - Celkové náklady na zařízení

| Zařízení | Pořizovací cena zařízení | Cena licencí | Roční náklady | Náklady celkem |
|---|---|---|---|---|
| **Cisco ASA 5520** | 0,00 Kč | 44 375,00 Kč | 0,00 Kč | **44 375,00 Kč** |
| **Barracuda SSL VPN 480** | 119 999,00 Kč | 0,00 Kč | 59 998,00 Kč | **179 997,00 Kč** |
| **Juniper SA 2500 SSL VPN** | 34 000,00 Kč | 67 252,00 Kč | 8 704,00 Kč | **109 956,00 Kč** |

## 6.4 Řešení vybrané k implementaci

Jak již bylo popsáno v úvodu této části, všechna zařízení představující řešení bezpečného připojení do podnikové sítě, jsou do jisté míry vybavena stejnými funkcionalitami a liší se až v detailních technických vlastnostech. Po pečlivém zhodnocení všech vlastností a funkcionalit jednotlivých zařízení, jsem dospěl k závěru, že nejvhodnějším řešením pro bezpečné připojení zaměstnanců podniku Povodí Labe, státní podnik, do podnikové sítě je řešení založené na zařízení ASA 5520 od společnosti Cisco.

Jedním z důvodu tohoto rozhodnutí jsou nejlépe propracované možnosti kontroly a vynucení bezpečnostních pravidel (Endpoint Security) na koncových stanicích, které se připojují do firemní sítě ze všech porovnávaných zařízení. Dalším důvodem tohoto rozhodnutí jsou náklady spojené s implementací, které jsou nejnižší ze všech porovnávaných zařízení. Výsledné náklady jsou ovlivněny i tím, že dané zařízení je již zcela integrováno do stávajícího IS podniku. Což představuje jistou výhodu, jelikož odpadají nejenom náklady na školení stávajících správců IS podniku, ale i ostatní případné náklady.

# 7 NÁVRH A POPIS IMPLEMENTACE ZVOLENÉHO ŘEŠENÍ

V této části práce popisuji návrh implementace (konfigurace) zvoleného řešení založeného na zařízení Cisco ASA 5520 tak, jak by měla být realizována v produkčním prostředí s přihlédnutím na všechny požadavky PLA. Návrh a poté samotnou implementaci jsem prováděl na základě svých zkušeností s touto problematikou a s využitím odborné literatury dostupné na trhu [13], popřípadě dalších dostupných materiálů [20].

## 7.1 Nutné předpoklady pro implementaci

Před samotným návrhem postupu implementace zvoleného řešení, je nutno se zmínit o některých předpokladech pro zdárnou implementaci.

### 7.1.1 Internetové spojení

K zajištění bezpečného připojení do podnikové sítě je nutné zajistit vhodné připojení k síti Internet. K tomuto účelu lze využít stávající CDMA/GPRS modemy s přednastaveným datovým tarifem, které jsou součástí nahrazovaného připojení do podnikové sítě. Dále bude umožněno zaměstnancům využívat vlastních možností k připojení do Internetu, například pomocí privátního připojení k Internetu skrze jejich ISP. Jelikož je celé řešení postaveno na SSL VPN, čímž je zajištěna komunikace výhradně pomocí protokolu SSL tzn. TCP port 443, připojení skrze různorodé ISP by nemělo být překážkou.

### 7.1.2 Zajištění ochrany na straně klientů

Jelikož budou zaměstnanci v rámci tohoto řešení využívat nezabezpečenou celosvětovou síť Internet, je nutné zajistit u všech podnikových ICT, které budou využívat tento přístup, instalaci softwarového firewallu a antivirového softwaru a konfigurace příslušných firewallových pravidel.

## 7.2 Návrh implementace

Z důvodu aktuálně rozpracovávaného projektu zabývajícího se náhradou centrálního adresářového a autentizačního serveru (Novell eDirectory) a výběrem vhodného řešení interní certifikační autority v podniku Povodí Labe, státní podnik, není zcela jasně dané budoucí řešení adresářového, autentizačního serveru a interní certifikační autority. S tím je

spojena vazba na případný výběr vhodného řešení zajišťující dvoufaktorovou autentizaci. Z toho vyplývá, že by bylo neekonomické a nesystémové v současné době připravovat řešení bezpečného připojení do podnikové sítě s využitím dvoufaktorové autentizace.

Proto je implementace zaměřena na zajištění bezpečného připojení do podnikové sítě pouze uživatelům využívající podnikové ICT, tzn. zatím bez nutnosti dvoufaktorové autentizace. Tato podmínka připojení uživatelů pouze z podnikových ICT, bude zajištěna využitím funkce Cisco Secure Desktop a nastavených specifických pravidel. Nicméně v průběhu implementace bude pro ověření funkčnosti využito dvoufaktorové autentizace založené na uživatelském certifikátu.

Implementaci zvoleného řešení lze rozdělit do několika dílčích kroků, které by měly zajistit co největší míru komplexnosti a bezpečnosti při implementaci, a to následovně:

1. Implementace SSL VPN části Cisco ASA 5520 včetně zajištění Endpoin Security nastavení
2. Implementace klientských firewallových pravidel
3. Testování daného řešení

### 7.2.1 Návrh implementace SSL VPN části Cisco ASA 5520

Před samotnou konfigurací SSL VPN části bude nutné vytvořit popřípadě upravit současnou konfiguraci zařízení Cisco ASA. Konkrétně upravit, popřípadě přidat firewallová pravidla. Je nutné vypnout NAT na odchozím VPN spojení, aby z vnitřní sítě mohl být průchod zpět do VPN sítě. Dále je nutné na firewallu povolit přístup do vnitřní sítě z VPN sítě. K firewallovým pravidlům se vrátíme podrobněji při popisu implementace.

Jako první krok při implementaci bude nutné vygenerovat SSL certifikát pro zajištění samotné SSL VPN. Můžeme vygenerovat self-signed certifikát nebo využít služeb certifikační autority. Pro zajištění dvoufaktorové autentizace založené na uživatelském certifikátu je nutné využít služeb certifikační autority, v našem případě lokální certifikační autority provozované jako součást eDirectory. Při implementaci bude otestována dvoufaktorová autentizace založená na uživatelských certifikátech, nicméně nasazení této formy autentizace do provozního prostředí bude až v návaznosti na připravovaný projekt certifikační autority v Povodí Labe.

Pro zajištění požadavků na nové řešení je nutné správně nakonfigurovat Prelogin Policies, Group Policies, Dynamic Access Policies obecně tzv. Endpoint Security, které jsou součástí Cisco Secure Desktop [13], [20]. Cílem implementace je zajistit bezpečné připojení do podnikové sítě pouze zaměstnancům z podnikových PC. Toho bude docíleno pomocí Prelogin Policy kontroly speciální hodnoty klíče registru systémů Windows. U jiných než Windows systémů, lze požadavek na připojení podnikových PC realizovat taktéž pomocí Prelogin Policies s využitím kontroly, například určitého běžícího procesu nebo souboru na disku. Podrobněji bude vše popsáno při implementaci. Dalším cílem bude zajistit kontrolu bezpečnosti koncové stanice, která realizuje připojení. Díky funkcionalitě Advance Edpoint Assessment [13] lze kontrolovat například verze virových definic a na základě výsledku vyvolat akce, například zakázat VPN připojení.

### 7.2.2 Návrh implementace klientských firewallů

Na všech podnikových ICT (PC) je v současné době instalován software Symantec Endopint Protection. Jedná se o software, který zajišťuje funkce antiviru a personálního firewallu. V podniku byla prozatím využívána pouze antivirová funkce daného produktu. Pomocí tohoto personálního firewallu a patřičných pravidel zajistíme dostatečnou ochranu podnikových PC, které musejí být pro sestavení VPN spojení připojeny do nezabezpečené sítě Internet.

Tato firewallová pravidla jsou definována centrálně skrze administrační server Symantec Endpoint Protection Manager server a na klienty jsou dále automaticky distribuována [19]. Tento server slouží ke kompletní správě antivirových a firewallových klientů. Na administračním serveru jsou ukládány veškeré konfigurace jednotlivých klientů a další informace týkající se jejich správy a provozu. Software Symantec Endopint Protection bude dále využit k distribuci speciální hodnoty klíče registru systémů Windows. Díky této speciální hodnotě dojde k rozlišení podnikových PC od jiných PC, které nejsou v majetku podniku (PC v knihovně, domácí PC), a to na základě prováděné kontroly před autentizaci uživatele pomocí Prelogin Policies.

## 7.3 Popis implementace Cisco ASA 5520 SSL VPN

V následující části budou detailně popsány konfigurační kroky, které byly provedeny při implementaci řešení bezpečného připojení do podnikové sítě s využitím zařízení Cisco

ASA 5520 v podniku Povodí Labe, státní podnik. Je nutné upozornit, že některé detailní části konfigurace nebudou z důvodu bezpečnosti zcela přesně odpovídat provozní konfiguraci, respektive budou obsahovat fiktivní data. To je celkem pochopitelné, jelikož diplomová práce je veřejně dostupný dokument a zveřejněním provozní konfigurace by mohlo dojít k ohrožení bezpečnosti realizovaného řešení.

Konfiguraci ASA 5520 lze provádět skrze ASDM software nebo pomocí CLI (Command Line Inerface). Při implementaci byly využity obě varianty, protože některé části SSL VPN nelze konfigurovat pomocí CLI, jako například Cisco Secure Desktop (CSD). Nicméně většina konfigurací byla prováděna pomocí konfiguračního softwaru ASDM. Tento software na základě vytvořené grafické konfigurace generuje CLI příkazy.

Pro přehlednost bylo u popisu některých konfiguračních kroků vypuštěno vkládání sejmutých obrazovek (printscreen) grafické konfigurace a v následujícím textu diplomové práce jsou pouze CLI výstupy z ASDM aplikace. Aby nebyl čtenář ochuzen o náhled na konfiguraci pomoci konfigurační aplikace ASDM, budou v jednotlivých částech konfigurace kromě CLI příkazů i odkazy na sejmuté obrazovky z ASDM, které jsou uloženy v příloze diplomové práce. Pro přehlednost jsou CLI příkazy vizuelně odlišeny jiným fontem písma a stínováním. U většiny kroků konfigurace je formou textového postupu proveden popis jednotlivých úkonů v ASDM aplikaci.

Dále je nutné připomenout, že Cisco ASA 5520 umožňuje využít dvou typů VPN připojení. Prvním je ClientLess, což je připojení skrze zabezpečený VPN portál, kde se pro VPN přístup využívá pouze webový prohlížeč s instalovaným ActiveX nebo Java Appletem. V případě Clientless je SSL relace vytvořena mezi klientem a zařízením Cisco ASA. Cisco ASA následně otvírá svoje vlastní spojení do vnitřní sítě. Druhým typem je plný VPN přístup tzv. AnyConnect klient, kde je využíván speciální software, neboli VPN klient. V tomto typu VPN je spojení vytvářeno napřímo skrze SSL VPN tunel mezi VPN klientem a dostupnými zdroji vnitřní sítě s využitím Cisco ASA jako prostředníkem, který udržuje SSL VPN tunel. Veškeré konfigurace, které jsou popisovány níže, se vztahují na oba typy VPN přístupů.

### 7.3.1 Prvotní konfigurace

Před samotnou konfigurací SSL VPN části je nutné nejprve provést základní konfiguraci Cisco ASA 5520, jako je povolení konfigurace zařízení pomocí ASDM softwaru a vytvoření uživatelského účtu pro ASDM software.

#### *7.3.1.1 Povoleni přístupu pro ASDM*

Před konfigurací pomocí ASDM je nutné zapnout http server na zařízení.

```
http server enable
```

#### *7.3.1.2 Definování přístupu pomocí ASDM*

Musí být nadefinováno, odkud je povolen přístup na http server, respektive odkud je povolen přístup pomocí ASDM aplikace.

```
http 192.168.1.0 255.255.255.0 Inside
```

#### *7.3.1.3 Přidání konfiguračního uživatele*

Vytvoření lokálního uživatelského účtu, který bude využíván pří konfiguraci pomocí ASDM aplikace.

```
username admin_asdm password privilege 15
```

#### *7.3.1.4 ASDM image konfigurace*

Pro zajištění podpory konfigurační aplikace ASDM je nutné nadefinovat, kde je ASDM na zařízení umístěno.

```
asdm image disk0:/asdm-621.bin
```

#### *7.3.1.5 Upgrade CSD a AnyConnect Client*

Před konfigurací je nutné provést upgrade zdrojových balíčku (package) Cisco Secure Desktop, AnyConnectClient, které jsou uloženy ve flash paměti Cisco ASA 5520. (Příloha I Obr. 1)

```
webvpn
svc image disk0:/anyconnect-win-2.5.2019-k9.pkg 1
 svc image disk0:/anyconnect-linux-64-2.5.2019-k9.pkg 2
 svc image disk0:/anyconnect-linux-2.5.2019-k9.pkg 3
 svc image disk0:/anyconnect-wince-ARMv4I-2.5.2019-k9.pkg 4
```

```
 svc enable
```

### 7.3.2 Nutné úpravy Firewall a NAT pravidel

Při konfiguraci SSL VPN je nutné konfigurovat firewallové politiky. Při realizaci VPN SSL je nutné například vypnout NAT na odchozím spojení z vnitřních sítí, aby mohl být proveden průchod zpět do VPN sítě.

#### *7.3.2.1 Vypnutí NAT pro VPN síť*

Vypnutí NAT na odchozím spojení, aby z vnitřní sítě mohl být průchod zpět do VPN sítě.

```
nat (Inside) 0 access-list NO_NAT_PLA
access-list NO_NAT_PLA line 13 extended permit ip 192.168.0.0 255.255.0.0
172.16.248.0 255.255.255.0
```

#### *7.3.2.2 Přidání pravidla pro odchozí spojení z VPN sítě*

Aby mohli klienti připojení skrze VPN realizovat spojení do sítě Internet na stejném interfacu, na kterém je zakončeno připojení VPN, je nutné vytvořit NAT následujícím pravidlem.

```
nat (Outside) 1 172.16.248.0 255.255.255.0
```

#### *7.3.2.3 Řízení přístupu uživatelů*

Přístup uživatelů VPN je řízen pomocí Access listu XXX_XXX_USERS, který je přiřazen do Group Policy VPN_VPN

```
Access-list XXX_XXX_USERS permit IP 172.16.248.0 255.255.255.0 any
```

#### *7.3.2.4 Nastaveni Security Level*

Povoleni provozu mezi dvěma nebo více hosty připojených na stejném interfacu.

```
same-security-traffic permit intra-interface
```

### 7.3.3 Vytvoření SSL certifikátu

Prvním krokem v konfiguraci SSL VPN by mělo být vytvoření SSL certifikátu [13]. Tento SSL certifikát slouží k ověření totožnosti vzdáleného serveru, v našem případě konfigurovaného Cisco ASA 5520. S využitím techniky veřejných a privátních klíčů

(asymetrické šifrování) je certifikát také využíván při výměně bezpečnostních informací nutných pro sestavení SSL relace. Vlastní SSL přenos je šifrován pomocí symetrických šifrovacích algoritmů například AES256-SHA1, AES128-SHA1.

Při vytváření SSL certifikátu můžeme postupovat dvojím způsobem. Může vygenerovat self-signed certifikát nebo využít služeb certifikační autority. Self-signed certifikát je podepsán zařízením, které certifikát vygenerovalo, což není považováno za důvěryhodné, protože pravost certifikátu nemůže být ověřena. Pokud využijeme služeb kvalifikované certifikační autority, je tento certifikát považován za důvěryhodný a ověřený.

Při implementaci byl zvolen postup vytvoření certifikátu s využitím lokální certifikační autority.

#### *7.3.3.1 Instalce CA certifkatu*

Pro využívání certifikátů podepsaných lokální certifikační autoritou je nutné přidat veřejný klíč dané certifikační autority do úložiště certifikátů. (Příloha I Obr. 2)

**Postup:**

**ASDM -> Configuration -> Device Management -> CA Certificates -> Add**

```
crypto ca trustpoint CA_Povodi_Labe
no id-usage
enrollment terminal
crypto ca authenticate CA_Povodi_Labe nointeractive
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
AAAAAAAAADAYMBACAQACCH//////////AQEAAgQR8tz2MBgwEAIBAAIIf///////
//8BAQACBBHy3PaiTjBMAgECAgIA/wIBAAMNAID//////////////wMJAID/////
////MBIwEAIBAAIIf/////////8BAf8wEjAQAgEAAgh/////////wEB/zANBgkq
hkiG9w0BAQUFAAOBgQAyB4oSswowF/5w5fONFF7EHUtdznYeV5wGXzp1ho98Li2j
3u9Pw0sl1OIdNlNDfUxpuYGjskdfjh6767Asdsdfjkhj78787686ASDdfsjdfnhj
IGm8yo3gZjMgiLqpWwKaFYP1JHRVTvGDzJczCVoDLKhq3ILlInDQ6fsRHObA
GA==
quit
```

#### *7.3.3.2 Vygenerování identity certifikátu*

Tento SSL certifikát slouží k ověření totožnosti vzdáleného serveru. Certifikát je také využíván při výměně bezpečnostních informací nutných pro sestavení SSL relace. Generování certifikátu lze provádět skrze konfigurační aplikaci ASDM nebo pomocí CLI. Při vytváření certifikátu je nejdříve vygenerován klíčový pár tj. privátní a veřejný klíč. Následně je vytvořen CSR (Certificate Signing Request), který musí lokální CA zpracovat, respektive podepsat. Vzniklý certifikát následně spárujeme s privátním klíčem a tím je proces vytváření SSL certifikátu dokončen. (Příloha I Obr. 3, Obr. 4)

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Certificate Management ->
Identity Certificates -> Add -> nechat podepsat CA -> Install
```

```
crypto key generate rsa label LB_CA_KEY modulus 2048 noconfirm

crypto ca trustpoint LB_CA_TrustPoint
keypair LB_CA_KEY
id-usage ssl-ipsec
fqdn lb.pla.cz
subject-name CN=lb.pla.cz,O=Povodi Labe,C=CZ,L=Hradec Kralove
enrollment terminal
crypto ca enroll LB_CA_TrustPoint noconfirm
```

```
crypto ca import LB_CA_TrustPoint certificate nointeractive
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Z6pJzA9qtSbdm7UCkUxsd3yANn28QefyYuYecsUjd/T6IqSbtTF06ulT/1mOl9To
TKTre87ng8GEH6NaSCFNGDjBdv66MROW8Q2BZf238YLTsVM7JDJUDilD2siJBwiO
BJJU33l2Fqd75kb+KrWPFVqzvpLiLWft+UnpxkE/FjiESxzt86dNiOCP1FDwDhdB
yAb2UM/D8c1SbcuepWlS3sr0M0I9Y5yT8iqldTMRSQ4F7RdX6Tp9yFbsnl3X64kA
aXhOarXMK5Z+eso80KpgX1/8Q+iq7Aplq4xLNhoTrm7eGVlMpOzhx/0hu5CZVBOk
yAyetIepkrDv
Gec=
Quit¨
```

Po přidání CA certifikátu a vytvoření identity certifikátu podepsaného CA je nutné nastavit příslušný certifikát na daný interface. (Příloha I Obr. 5)

**Postup:**

```
ASDM -> Configuration -> Device Management -> Advanced -> SSL Settings ->
Vybereme Interface -> Přiřadíme certifikát
```

```
ssl trust-point LB_CA_TrustPoint Outside
```

### 7.3.4 Definování AAA serveru - autentizace

Zařízení nabízí celou škálu autentizačních metod, jak bylo popsáno v předcházejících částech diplomové práce. K připojení do SSL VPN bude využita autentizace založená na RADIUS serveru. Uživatelé využívající bezpečné připojení do podnikové sítě budou autentizovány pomocí RADIUS serveru, který je součástí eDirectory. V eDirectory lze navíc přesně určit, kterým uživatelů je autentizace skrze RADIUS server povolena. Autentizace s využitím RADIUS serveru je v IS podniku již provozována. V konfiguraci ASA 5520 bude vytvořen tzv. AAA server využívající k ověření RADIUS server. Tento AAA server se dále napojí na danou Tunnel Group neboli Connection Profile [13]. Konfigurace autentizace lze provést skrze ASDM klienta nebo pomocí CLI (Command Line Inerface). Na RADIUS serveru je nutné nastavit tzv. klient neboli definovat, kdo se může RADIUS serveru dotazovat.

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> AAA/Local Users-> AAA
Server Groups -> Add - > Přidáme RADIUS server
```

```
aaa-server RADIUS (Inside) host server1
timeout 1
retry-interval 1
key **********
radius-common-pw **********
aaa-server RADIUS (Inside) host server2
timeout 1
retry-interval 1
key **********
radius-common-pw **********
```

### 7.3.5 Základní konfigurace SSL VPN

Při vytváření základní konfigurace SSL VPN byl použit ASDM průvodce, díky kterému lze v několika krocích zprovoznit základní konfiguraci SSL VPN. Tuto základní konfiguraci je

nutné posléze jemněji doladit. Pomocí konfiguračního průvodce (Příloha I Obr. 6, Obr. 7, Obr. 8) jsou vytvořena některá základní nastavení, jako například:

- Connection Profile (Tunnel Group)
- Policy Group
- IP Pool - neboli rozsah IP adres přidělovaných vrámci SSL VPN
- Interface - zakončení VPN spojení
- AAA server
- Bookmarky

**Postup:**

**Menu ASDM -> Wizards -> SSL VPN Wizard -> provedeme konfiguraci**

```
webvpn
enable Outside
import webvpn url-list VPN_VPN disk0:/tmpAsdmImportFile1880362373
delete /noconfirm disk0:/tmpAsdmImportFile1880362373
webvpn
tunnel-group-list enable
svc image disk0:/anyconnect-win-2.5.2019-k9.pkg 1
svc enable
ssl trust-point PLA_CERT_SSL Outside
ip local pool VPN_VPN 172.16.248.100-172.16.248.199 mask 255.255.255.0
group-policy VPN_VPN internal
group-policy VPN_VPN attributes
vpn-tunnel-protocol svc webvpn
webvpn
url-list value VPN_VPN
svc   enable
tunnel-group VPN_VPN type remote-access
tunnel-group VPN_VPN general-attributes
default-group-policy VPN_VPN
authentication-server-group  RADIUS
address-pool  VPN_VPN
tunnel-group VPN_VPN webvpn-attributes
group-alias Povodi_Labe enable
group-url https://192.168.100.3/Povodi_Labe enable
```

#### *7.3.5.1 Konfigurování Policy Rules*

Po základní konfiguraci SSL VPN pomocí průvodce je nutné provést jemnější doladění vytvořené konfigurace. Například nastavení parametru split-tunnel-policy. Pomocí tohoto parametru definujeme, zda má být veškerý síťový provoz směrován do VPN tunelu, nebo zda má být některá část směrována jinou cestou [13]. V tomto případě bylo nastaveno

směrování veškerého provozu na vzdáleném hostu do SSL VPN tunelu, tedy volba Tunnel All Networks. (Příloha I obr. Obr. 9)

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Clientless -> Group
Policies -> Vybereme požadovanou skupinu -> Edit
```

```
group-policy VPN_VPN attributes
vpn-filter none
webvpn
svc keep-installer installed
group-policy VPN_VPN attributes
split-tunnel-policy   tunnelall
dns-server value 192.168.1.10
wins-server value 192.168.1.20
default-domain value pla.cz
group-policy VPN_VPN attributes
vpn-filter value XXX_XXX_USERS
group-lock value VPN_VPN
webvpn
svc ask enable default webvpn
```

### 7.3.6 Konfigurace CSD a Prelogin Policy

CSD (Cisco Secure Desktop) zajišťuje několik funkcionalit, které nám umožní kontrolu případné vynucení bezpečnostních politik na připojovaném zařízení. Jednou z funkcí CSD je Prelogin Policy. Tato funkce je využívána k prověření vzdáleného klienta před vlastní autentizací uživatele a lze využít pro zjištění přístupu pouze ze ICT prostředků (PC), které vyhoví dané Prelogin Politicy, například pouze firemní PC. Konfigurace Prelogin Policy probíhá pomocí ASDM konfiguračního softwaru. Pomocí tohoto softwaru je vytvořen XML soubor, kde jsou uloženy konfigurační parametry CSD a tento soubor je uložen ve flash paměti Cisco ASA 5520.

#### *7.3.6.1 Aktivace CSD*

Před samotnou konfigurací musí být nejprve aktivován CSD [20]. Touto aktivací je zajištěno, že při přístupu skrze webové rozhraní VPN dále jen VPN portál, bude zajištěno stažení a následné spuštění CSD na straně vzdáleného klienta.

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Secure Desktop Manager->
Setup -> Vybereme z flash disku konkrétní CSD image -> Zaškrtneme volbu
Enable Secure Desktop
```

```
webvpn
csd image disk0:/csd_3.5.2008-k9.pkg
csd enable
```

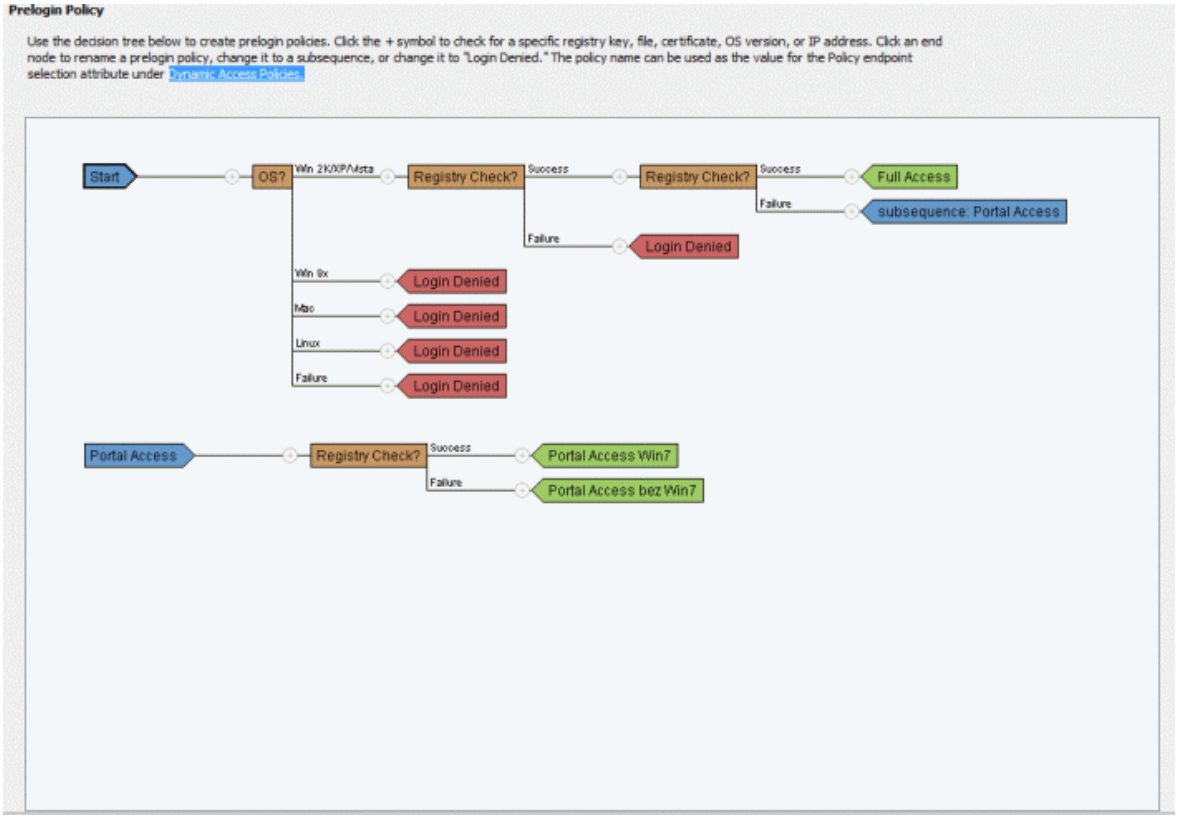
#### *7.3.6.2 Popis konfigurace Prelogin Policies*

Jsou nastaveny tři Prelogin Policies, které zajistí připojení pouze podnikových zařízení s OS Windows 2K, XP, Vista a Windows 7, a to pomocí kontroly výskytu specifického klíče v registru OS Windows. Prelogin Policy kontrola je prováděna v obou typech VPN přístupu. Tedy jak v Clientless, tak v plném VPN přístupu, kdy je využíván instalovaný AnyConnect klient. Samotná kontrola je prováděna v několika krocích. Dále si popíšeme postup při připojení skrze VPN portál.

V prvním kroku provádíme kontrolu OS připojovaného zařízení (Příloha I Obr. 20). Pokud je zařízení typu OS Windows 2K, XP, Vista nebo Windows 7, pokračujeme v dalším prověření, pokud nevyhoví, je zakázán přístup k přihlašovacímu dialogu (Příloha I Obr. 19). V druhém kroku je prováděna kontrola, zda se připojuje podnikové zařízení, a to na základě výskytu specifického klíče v registru OS Windows. Pokud nevyhoví, je zakázán přístup k přihlašovacímu dialogu VPN portálu. Pokud vyhoví, přechází do třetího kroku, kde se prověřuje, zda má již instalovaného AnyConnect klienta. Pokud je klient již instalován, je přidělena politika Full Access tzn. plný přístup do VPN sítě. Pokud není klient AnyConnect instalován, pokračuje se do dalšího kroku, kde je prováděna kontrola zda se jedná o zařízení s OS Windows 7 nebo jiné OS Windows. Pokud se jedná o zařízení s OS Windows 7, je mu přidělena politika Portal Acces Win7, která vynutí vymazání všech dočasně uložených dat při ukončení VPN portálu. Pokud se nejedná o zařízení s OS Windows 7, je mu přidělena politika Portal Access bez Win7 a vzdálenému uživateli je vnuceno spuštění Secure Desktop, neboli virtuální zabezpečené pracovní plochy.

Prelogin Policy:

- Full Access - Nemá žádná omezení, jedná se o plný přístup do podnikové LAN.
- Portall Access bez Win7 – Vzdálenému klientovi je vnuceno spuštění Secure Desktop, neboli virtuální zabezpečené pracovní plochy.
- Portall Access Win7 - V současné verzi CSD není podporována Secure Desktop pro OS Windows 7, a proto je vzdálenému uživateli vnucen tzv. Cache Cleaner, který vynutí vymazání všech dočasně uložených dat při ukončení VPN portálu.




Obrázek 14 - Schéma Prelogin Policy

### 7.3.7 Dynamic Access Policies

Jedná se o politiky, které jsou aplikovány po Group Policies. Slouží k prověření Endpoint Security na straně klienta. Můžeme prověřovat například přítomnost nainstalovaného antivirového softwaru, dokonce lze prověřit, jak zastaralé jsou antivirové definice na straně klienta. Na základě výsledků z provedeného prověření může provést další akce, například zakázat připojení. Pro využití funkce Dynamic Access Policies dále jen DAP, je nejprve nutné zapnout volbu Endpoint Assesment.

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Secure Desktop Manager ->
Host Scan -> Zaškrtneme Endpoint Assessment
```

Pomocí DAP (Dynamic Access Policies) je provedeno prověření, zda je na připojovaném PC spuštěn proces antivirového systému. K tomu bude využita další z funkcionalit CSD,

což je tzv. Host Scan. Ten slouží k vytvoření vlastních prověřovacích pravidel, které lze dále používat v DAP. Následuje popis konkrétního nastavení DAP.

#### *7.3.7.1 Vytvoření Host Scan*

Před vlastní konfigurací DAP je přidán Host Scan, který prověří přítomnost spuštěného procesu na vzdáleném PC [20]. V tomto případě spuštění procesu Rtvscan.exe, který vypovídá o funkčním antivirovém programu Symantec (Příloha I Obr. 10).

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Secure Desktop Manager->
Host Scan -> ADD -> Vybereme Process Scan -> Vyplnime Endpoint ID a
Process Name
```

#### *7.3.7.2 Vytvoření Dynamic Access Policies*

Při vytváření DAP nemusí být využito pouze vlastní prověřovací pravidlo vytvořené pomocí Host Scan, ale můžeme použít velkou škálu již předdefinovaných prověřovacích pravidel, například pravidlo prověřující přítomnost osobního firewallu a mnoho dalších.

Při vytváření DAP je rozlišována jejich priorita podle čísla priority, které bylo vloženo při definici DAP a to tak, že čím je číslo vyšší, má daná DAP politika vyšší prioritu.

V našem případě byla přidána DAP na prověření přítomnosti antiviru s využitím vlastního prověřovacího pravidla definovaného pomocí Host Scan. (Příloha I Obr. 11)

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Network (Client) Access ->
Dynamic Access Policies -> ADD -> Vyplníme název politiky a prioritu ->
Add Endpoint Attribute -> Vybereme typ Process -> Vybereme námi
definovaná Host Scan   -> Zvolime akce, které se mají provést
```

```
dynamic-access-policy-record "Symantec AutoProtect"
priority 100
description "Kontrola funkcniho antiviru Symantec"
user-message "Nemas funkcni antivirovy software. Kontaktuj sveho
informatika."
action terminate
```

### 7.3.8 Konfigurace VPN portálu

Po prvotní konfinaci SSL VPN je nutné provést konfiguraci VPN portálu. Je vhodné vypnout některé volby, které uživatelé nevyužijí, a naopak zapnout například virtuální klávesnici (OnScreen Keyboard), která představuje větší bezpečí při zadávání citlivých údajů skrze VPN portál.

#### *7.3.8.1 Vypnutí výchozích voleb VPN portálu*

Některé z voleb VPN portálu je vhodné vypnout. To lze provést v konfiguraci Group Policies. (Příloha I Obr. 12).

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Clientless SSL VPN Access -
> Group Policies -> Vybereme politiku -> Edit -> More Options ->
Customization -> Portal Customization -> Manage
```

```
group-policy VPN_VPN attributes
webvpn
customization value DfltCustomization
```

#### *7.3.8.2 Zapnutí OnScreen klávesnice*

Pro zajištění větší bezpečnosti při vkládání citlivých dat, jako je například uživatelské jméno a heslo, je vhodné zapnout funkci OnScreen klávesnice. Tuto klávesnici můžeme vyžadovat na všech stránkách VPN portálu nebo jenom na přihlašovací stránce.

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Clientless SSL VPN Access
-> Portal -> Customization -> Vybrat volbu Show only for the login page
```

```
webvpn
onscreen-Keyboard logon
```

#### *7.3.8.3 Konfigurace port forwardingu*

Po přihlášení k VPN portálu můžeme využívat přesměrování portů (portforwarding). Jedná se o funkci, která umožní aplikacím spouštěných z připojeného PC komunikovat se zdroji vnitřní sítě. V případě této implementace bylo přesměrování portů využito pro komunikaci

lokálně spuštěného RDP klienta s terminálovým serverem ve vnitřní síti. (Příloha I Obr. 13)

**Postup:**

**ASDM -> Configuration -> Remote Access VPN -> Clientless SSL VPN Access -> Portal -> Port Forwarding -> Add -> Vyplníme parametry Port Forwardingu**

```
webvpn
port-forward Server_v_LAN_PLA 55555 terminal-server.pla.cz 3389
```

### 7.3.9 Monitoring SSL VPN

Po implementaci je vhodné provádět monitoring VPN spojení. K tomu lze využít CLI nebo můžeme monitoring provádět pomocí konfigurační aplikace ASDM.

**Postup:**

**ASDM -> Monitoring -> VPN -> VPN Statistic**

```
vpn-sessiondb detail webvpn

Session Type: WebVPN Detailed

Username     : .nekdo.nekde.pla
Index        : 45
Public IP    : 185.165.84.96
Protocol     : Clientless
License      : SSL VPN
Encryption   : AES256                Hashing      : SHA1
Bytes Tx     : 139864                Bytes Rx     : 24825
Pkts Tx      : 6                     Pkts Rx      : 2
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : VPN_VPN              Tunnel Group : VPN_VPN
Login Time   : 15:03:06 MET Fri Apr 8 2011
Duration     : 0h:02m:14s
NAC Result   : Unknown
VLAN Mapping : N/A                   VLAN         : none

Clientless Tunnels: 1

Clientless:
  Tunnel ID    : 45.1
  Public IP    : 185.165.84.96
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: TLSv1.0               TCP Dst Port : 443
  Auth Mode    : userPassword
  Idle Time Out: 30 Minutes            Idle TO Left : 27 Minutes
  Client Type  : Web Browser
```

```
  Client Ver   : Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0;
SLCC1; .NET CLR 2.0.50727; .N
  Bytes Tx     : 139864                Bytes Rx     : 24825

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 134 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

### 7.3.10 Autentizace pomocí AAA a certifikátu

Jak již bylo popsáno v návrhu implementace, byla otestována dvoufaktorová autentizace založená na uživatelském certifikátu. Zapnutí této funkcionality se provádí v Connection Profilu, a to pomocí CLI nebo pomocí ASDM. (Příloha I Obr. 14)

**Postup:**

```
ASDM -> Configuration -> Remote Access VPN -> Clientless SSL VPN Access
-> Connection Profiles -> Vybereme profil -> Edit -> Basic ->
Authentication -> Vybereme Both
```

```
tunnel-group VPN_VPN webvpn-attributes
no authentication aaa
authentication certificate aaa
```

## 7.4 Implementace - personální firewall

Na úvod je nutné zmínit, že veškeré konfigurace pravidel personálního firewallu jsme prováděli skrze Symantec Endpoint Protection Manager server s využitím konzole Symantec Endpoint Protection Console [19], přes niž jsme schopni spravovat veškeré nastavení klientů. Samotnou implementaci lze rozdělit do dvou kroků. V prvním kroku jsou definována firewall pravidla, která zaručí zabezpečení podnikových PC připojených do sítě Internet. V druhém kroku bude pomocí personálního firewallu vynucen zápis do registrů Windows u všech PC, které se budou připojovat do podnikové sítě pomocí nového řešení.

### 7.4.1 Definice firewall pravidel

Před samotným definováním pravidel je nutné vytvořit novou skupinu (Group Policy) s názvem VPN. Veškeré konfigurační kroky se budou dále odvíjet nad touto skupinou.

Všechny podnikové PC, které budou využívány pro připojení pomocí nově realizovaného bezpečného připojení do podnikové sítě, musejí být členem této skupiny. To nám zajistí, že na všechny PC dané skupiny budou aplikována jednotná pravidla.

Při vytváření pravidel firewallu je nutné rozlišit, zda je PC připojené ve vnitřní (lokální) síti podniku nebo zda se připojuje do lokální sítě ze sítě Internet s vyžitím VPN. Tímto prvotním rozdělením zajistíme možnost kontrolovat, jaká firewall pravidla se budou nastavovat. Pokud bude PC připojeno do lokální sítě, nebude jeho síťová komunikace nijak omezena. Pokud bude PC připojeno skrze VPN síť, tedy skrze síť Internet, bude na daném PC zakázána jakákoliv jiná komunikace kromě VPN tunelu. Pokud bude chtít zaměstnanec přistupovat k síti Internet, bude muset využít sestaveného VPN spojení a k síti Internet se připojovat skrze zabezpečenou infrastrukturu podniku.

Začneme přidáním další tzv. „Location“ [19], kde stanovíme, za jakých podmínek bude klient součástí této Location (Příloha I Obr. 15). Díky tomuto rozdělení jsme schopni aplikovat různá firewall pravidla při různém zapojení do sítě. Tedy pokud bude PC zapojeno přímo do lokální sítě, jsme schopni mu nastavit jiná firewall pravidla, než když bude PC připojeno skrze VPN síť. Definice firewall. pravidel je pomocí grafického rozhraní skrze Symantec Endpoint Protection Manager. (Příloha I Obr. 16)

### 7.4.2 Definice Host Integrity

Díky funkci Host Integrity [19], která je součástí personálního firewallu, jsme schopni provádět kontrolu uživatelských PC na přítomnost instalovaného service packu, přítomnost určité hodnoty v registru Windows a mnoho dalších. Na základě provedené kontroly můžeme spouštět různé akce na daném PC. Například zapsat nějaké hodnoty do registrů Windows, a tak podobně. V našem případě tuto funkci využijeme k distribuci (zápisu) specifické hodnoty do registrů Windows na PC, které jsou ve skupině VPN. Tímto zajistíme splnění jedné z Prelogin Policies podmínek, které jsou vyžadovány při sestavování VPN spojení.

Host Integrity se definuje přidáním konkrétní politiky skrze grafickou konzoli Symantec Endpoint Protection Console. Byla přidána politika, která testuje výskyt určitého registr klíče Windows a pokud klíč není zapsán, tak jej vytvoří znovu. (Příloha I Obr. 17, Obr. 18)

## 7.5 Testování a popis implementovaného řešení

Na závěr celé implementace je nutné provést otestování zvoleného řešení, čímž bude zároveň implementované řešení představeno.

Testování bylo rozděleno do dvou kroků. V první kroku byla testována funkčnost Prelogin Policies, Group Policies a DAP včetně dalších implementovaných funkcí CSD. Ve druhém kroku byla testována funkčnost vytvořeného VPN spojení se zaměřením na ověření dostupnosti interních zdrojů podniku v rámci sestaveného spojení.

### 7.5.1 Ověření funkčnosti definovaných podmínek přístupu

Definované podmínky přístupu do podnikové sítě, konkrétně Prelogin Policies, Group Policies a DAP, byly testovány jak při přístupu k VPN portálu tedy v režimu Clientless, tak při plném VPN přístupu pomocí AnyConnect klienta.

Nejprve otestujeme přístup pouze s využitím webového prohlížeče (Clientless), a to tak, že do webového prohlížeče zadáme URL https://lb.pla.cz. Nutnou podmínkou kontroly je instalované Java (JRE) rozšíření webového prohlížeče, případně zapnutá podpora pro ActiveX. Před zobrazením přihlašovacího dialogu je na pozadí prováděno CSD skenování, které zajistí kontrolu nastavených Prelogin Policies. Pokud nastaveným Prelogin Policies daný PC nevyhoví, je mu odepřen přístup (Příloha I obr. Obr. 19). V opačném případě je zobrazena přihlašovací stránka a po úspěšné autorizaci je uživatel přesměrován na VPN portál. (Příloha I Obr. 20, Obr. 21, Obr. 22)

Ve druhém kroku otestujeme plný VPN přístup do podnikové sítě. Po instalaci a spuštění AnyConnect klienta zadáme do pole „Connect to:“ lb.pla.cz. Opět je před samotným procesem autentizace prověřen systém, ze kterého je navázáno VPN spojení podle konfigurovaných Prelogin Policies a pokud nevyhoví, je zakázáno přihlášení (Příloha I Obr. 23). V opačném případě jsme po úspěšné autentizaci připojeni do lokální sítě (Příloha I Obr. 24, Obr. 25).

Lze konstatovat, že v obou případech byla potvrzena funkčnost kontroly a vynucení přístupových podmínek, které zaručují bezpečné připojení do podnikové sítě.

### 7.5.2 Ověření dostupnosti interních ICT zdrojů

V předešlé části byla testována kontrola funkčnosti definovaných podmínek přístupu. Nyní se zaměříme na testování dostupnosti interních ICT zdrojů podniku v obou VPN režimech, tedy v režimu VPN portálu (Clientless) a v plném VPN režimu, tedy s využitím AnyConnect VPN klienta.

V režimu Clientless byl testován přístup k webovému rozhraní elektronické pošty a přístup do intranetu podniku, a to následovně. Do webového prohlížeče byla zadána URL https://lb.pla.cz, po provedeném Prelogin skenu a úspěšné autentizaci byl zpřístupněn VPN portál (Příloha I Obr. 26). Ve VPN portálu bylo kliknuto na odkaz pro přístup do webového prostředí elektronické pošty (Příloha I Obr. 27) a dále na odkaz intranetového serveru podniku. Vše proběhlo bez zjevných problémů.

V plném VPN režimu byl testován přístup k síťovým prostředkům podniku, konkrétně přístup na souborový server podniku, a to následovně. Po spuštění a přihlášení do VPN sítě pomocí AnyConnect klienta, bylo provedeno připojení síťového adresáře ze souborového serveru. (Příloha I Obr. 28, Obr. 29, Obr. 30)

Při testech nebyly zjištěny nedostatky, všechny požadované vnitřní ICT zdroje podniku byly přístupné.

## 7.6 Zhodnocení implementovaného řešení

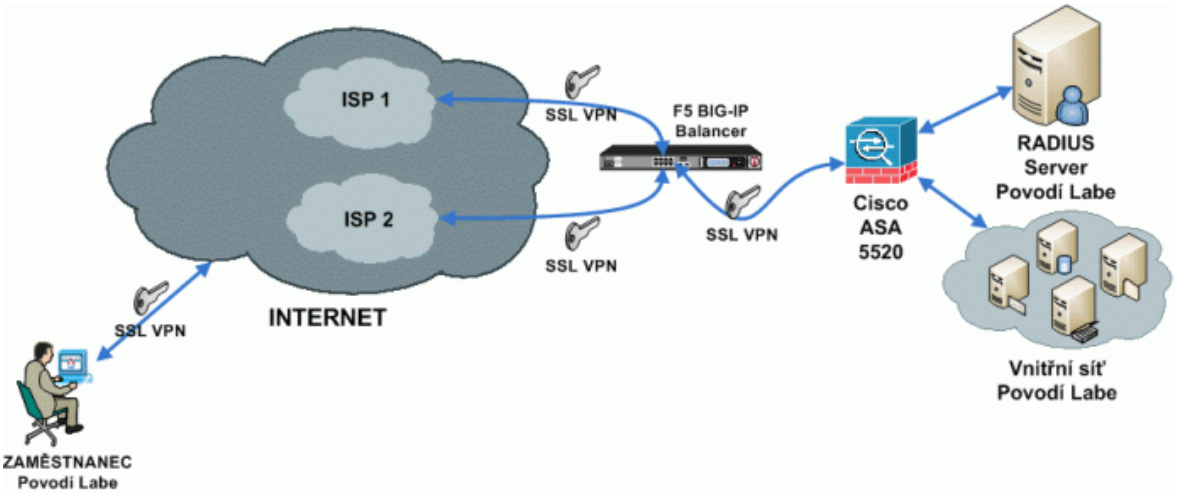
Řešení, které jsem implementoval, zaručuje připojení zaměstnanců podniku Povodí Labe, státní podnik, do podnikové sítě z prostředí Internet se zajištěním maximálního bezpečí a uživatelského komfortu.

Největší předností zvoleného a implementovaného řešení je nezávislost na konkrétním typu internetového připojení a celková bezpečnost. Zaměstnancům je umožněn přístup do podnikové sítě z libovolné části sítě Internet. Jedinou podmínkou je realizovat VPN spojení z podnikového ICT. Důvodem tohoto požadavku je bezpečnost kladená na celé řešení. Jedině u podnikových ICT jsme schopni zajistit, případně vynutit, jak pomocí technických, tak organizačních prostředků, vysokou míru bezpečnosti. K zajištění této základní podmínky jsou využívány pokročilé funkce zvoleného zařízení, které představuje implementované řešení.

Konkrétně se jedná o soubor funkcí s názvem Cisco Secure Desktop, díky kterým jsme schopni na vzdáleném zařízení nejenom ověřit, zda odpovídá nastaveným bezpečnostním zásadám, ale jsem schopni na základě tohoto ověření vyvolat další akce, například vynucení aktualizace antivirových definic.

### 7.6.1 Schéma implementovaného řešení

Následující schéma odpovídá implementovanému řešení bezpečného připojení zaměstnanců Povodí Labe, státní podnik, do podnikové sítě.




Obrázek 15 - Schéma implementovaného řešení

# ZÁVĚR

Cílem této diplomové práce bylo vybrat a následně implementovat nejvhodnější řešení dostupné v danou dobu na trhu, které by nejlépe splňovalo požadavky kladené na bezpečné připojení zaměstnanců do podnikové sítě Povodí Labe, státní podnik. V teoretické části práce byly popisovány obecné a technické informace týkající se problematiky bezpečného připojení do podnikové sítě tak, aby čtenář získal obecné povědomí v dané problematice. Následující praktická část je zaměřena na výběr, návrh a popis implementace nejvhodnějšího řešení, které by nejlépe splňovalo dané požadavky.

Pro zajištění maximální dostupnosti bezpečného připojení do podnikové sítě bylo celé řešení postaveno na využití SSL VPN. Důvodů pro toto rozhodnutí bylo několik, jak již bylo v této práci popsáno. Byly představeny některé z možných řešení dostupných v danou dobu na trhu. Posléze bylo jedno z představovaných řešení vybráno na základě porovnání, kde bylo přihlédnuto k současnému stavu IS podniku, požadavkům kladeným na nové řešení a k celkovým nákladům na implementaci nového řešení.

Poté následoval návrh a vlastní implementace daného řešení do IS podniku. Popis implementace je v diplomové práci dokumentován. Po implementaci bylo testováním ověřeno splnění všech požadavků, které byly na nové řešení kladeny. Je nutné znovu připomenout, že při výběru vhodného řešení byl kladen důraz na bezpečnost, nenáročnost a na nízké náklady spojené s integrací nového řešení do stávající IS podniku.

Lze konstatovat, že vybrané řešení splňuje všechny požadavky, které byly vyžadovány. Dále je nutné poznamenat, že vybrané řešení je nejméně ekonomicky nákladné, a to jak v nákladech na provoz, tak v nákladech na správu a konfiguraci. Je to dáno tím, že vybrané řešení je založeno na zařízení, které je již v IS podniku zcela integrováno a obsluhováno proškolenou obsluhou a nevznikají tak vícenáklady na případné školení obsluhy, či za vzdálenou správu nového zařízení, nebo jiné náklady.

Implementované řešení lze po dokončení právě probíhajících projektů zabývajících se náhradou centrálního adresářového a autentizačního serveru a výběrem vhodného řešení interní certifikační autority v podniku Povodí Labe, státní podnik, rozšířit o zavedení dvoufaktorové autentizace založené na uživatelských certifikátech nebo na technologii One Time Password. Po zavedení dvoufaktorové autentizace do běžného provozu a dodržením

patřičných bezpečnostních pravidel, lze uvažovat o zpřístupnění interním zdrojům podniku s využitím pouze VPN portálu i zaměstnancům z jiných než podnikových PC.

Implementované řešení je v současné době v podniku provozováno v testovacím režimu, při kterém dochází k jemnějšímu dolaďování konfiguračních parametrů dle konkrétních požadavků ze strany zaměstnanců podniku.

# ZÁVĚR V ANGLIČTINĚ

The aim of this thesis was to select and then implement the best solution available on the market that would best fulfil the requirements of safe access for employees to the corporate network of Povodí Labe, State Enterprise. The theoretical part of the thesis described the general and technical information related to the issue of safe access to corporate networks, so that the reader was generally aware of the issue. The following practical part focuses on the selection, suggestion and description of a solution that would best fulfil the requirements.

To ensure maximum availability of safe connections to corporate networks, the entire solution was based on the use of SSL VPNs. There were a few reasons to choose this particular solution as they have already been described in the thesis. Some other possible solutions available on the market have been introduced. Then one of those solutions was selected on the basis of comparison considering the present state of the enterprise IS, the demand for a new solution, and to the overall cost of its implementing.

Then the suggested solution and implementation of this solution to the IS followed. Description of the implementation has been documented in the thesis. After the implementation, the satisfaction of all stressed requirements has been tested. It should be recalled that when selecting an appropriate solution the emphasis was supposed to be given on security, compactness and low cost associated with integrating new solutions into existing enterprise IS.

It can be concluded that the chosen solution meets all requirements. It should also be stated that the chosen solution is the least expensive both in the cost of operations and the cost of administration and configuration. This is due to the fact that the chosen solution is based on the apparatus which has already been fully integrated to the enterprise IS and operated by a trained staff. This means that no additional costs (e.g. staff training or management of the new equipment) have appeared.

After the completion of ongoing projects dealing with the replacement of the central directory and authentication server and the selection of a suitable internal certification authority in Povodí Labe, State Enterprise, the implemented solution can be expanded to the introduction of a two-factor authentication based on user certificates or One Time Password technology. After introducing a two-factor authentication into normal operation,

and observation of appropriate security arrangements, disclosure of internal company resources using only the VPN portal may be considered. Other than the PC company staff may take the advantage too.

The implemented solution is currently being tested in the company. During the testing a finer tuning of configuration parameters according to specific requests of the employees is being dealt with.

# SEZNAM POUŽITÉ LITERATURY


[1] LEWIS, Mark. *Comparing, Designing, and Deploying VPNs*. [s.l.] : Cisco Press, 2006. 1080 s. ISBN 978-1-58705-179-1.

[2] SCOTT, Charlie; WOLFE, Paul; ERWIN, Mike. *Virtual Private Networks, Second Edition*. [s.l.] : O'Reilly, 1999. 225 s. ISBN 1-56592-529-7.

[3] HLADÍK, Radek. *ROOT.CZ* [online]. 2004 [cit. 2011-02-14]. OpenVPN - VPN jednoduše. Dostupné z WWW: <http://www.root.cz/clanky/openvpn-vpn-jednoduse>.

[4] DOSTÁLEK, Libor; VOHNOUTOVÁ, Marta. *Velký průvodce infrastrukturou PKI a technologií elektronického podpisu*. [s.l.] : Computer Press, 2006. 534 s. ISBN 80-251-0828-7.

[5] *MICROSOFT TECHNET* [online]. 2003 [cit. 2011-02-14]. PPTP (Point-to-Point Tunneling Protocol). Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc738852%28WS.10%29.aspx>.

[6] *MICROSOFT TECHNET* [online]. 2003 [cit. 2011-02-16]. L2TP (Layer Two Tunneling Protocol). Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc759432%28WS.10%29.aspx>.

[7] DAVIES, Joseph. *TechNet Magazine : The Secure Socket Tunneling Protocol* [online]. 2008 [cit. 2011-04-17]. The Cable Guy. Dostupné z WWW: <http://technet.microsoft.com/en-us/magazine/2007.06.cableguy.aspx>.

[8] *MICROSOFT TECHNET* [online]. 2003 [cit. 2011-03-07]. Protokol PPTP (Point-to-Point Tunneling Protocol. Dostupné z WWW: <http://technet.microsoft.com/cs-cz/library/cc739465%28WS.10%29.aspx>.

[9] LUHOVÝ, Karel. *Svět sítí : Tradiční model tunelování* [online]. 2003 [cit. 2011-03-19]. Seriál o VPN. Dostupné z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Tutorialy&temaID=219&clanekID=224>

[10] LEWIS, Mark. *Troubleshooting Virtual Private Networks*. 2nd edition. [s.l.] : Cisco Press, 2004. 840 s. ISBN 978-1587051043.

[11] HUANG, Qiang; FRAHIM, Jazib. *SSL Remote Access VPNs*. 1 edition. [s.l.] : Cisco Press, 2008. 384 s. ISBN 978-1587052422.

[12] WYLER, Neil, et al. *Juniper Networks Secure Access SSL VPN Configuration Guide*. [s.l.] : Syngress, 2007. 582 s. ISBN 978-1597492003.

[13] FRAHIM, Jazib; SANTOS, Omar. *Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*. 2nd edition. [s.l.] : Cisco Press, 2010. 1152 s. ISBN 978-1587058196.

[14] *Barracuda SSL VPN Administrator's Guide* [online]. Documentation version v17-110214 Barracuda Networks, Inc., 2011 [cit. 2011-04-10]. 129 s. Dostupné z WWW: <http://www.barracudanetworks.com/ns/downloads/Admin_Guides/Barracuda_SSLVPN_AG_US.pdf>.

[15] FEILNER, Markus; GRAF, Norbert. *Beginning OpenVPN 2.0.9*. [s.l.] : Packt Publishing, 2009. 356 s. ISBN 978-1847197061.

[16] *Secure Access Administration Guide* [online]. Sunnyvale : Juniper Networks, Inc., 2011 [cit. 2011-04-15]. 1078 s. Dostupné z WWW: <http://www.juniper.net/techpubs/software/ive/admin/j-sa-sslvpn-7.0-adminguide.pdf>.

[17] FEILNER, Markus. *OpenVPN : Building and Integrating Virtual Private Networks*. [s.l.] : Packt Publishing, 2006. 258 s. ISBN 978-1904811855.

[18] KABELOVÁ, , Alena; DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP a systém DNS*. [s.l.] : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.

[19] *Administration Guide for Symantec™ Endpoint Protection and Symantec Network Access Control* [online]. Documentation version 11.00.00.00.03. Cupertino : Symantec Corporation, 2007 [cit. 2011-04-20]. 697 s. Dostupné z WWW: <ftp://ftp.symantec.com/public/english_us_canada/products/symantec_endpoint_protection/11.0/manuals/administration_guide.pdf>.

[20] *Cisco Secure Desktop Configuration Guide, Release 3.5 : for Cisco ASA 5500 Series Administrators* [online]. San Jose : Cisco Systems, Inc., 2010 [cit. 2011-04-20]. 118 s. Dostupné z WWW: <http://www.cisco.com/en/US/docs/security/csd/csd35/configuration/guide/CSD35cfg.pdf>.

# SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

| | |
|---|---|
| 3DES | Triple Data Encryption Standard |
| AAA | Authentization, Authorization, Accounting server |
| AH | Authentication Header |
| Blowfish | Symetrická bloková šifra |
| BTS | Base transceiver station |
| CLI | Command-line interface |
| CSD | Cisco Secure Desktop |
| ČTU | Český telekomunikační úřad |
| DAP | Dynamic Access Policies |
| DES | Data Encryption Standard |
| DMZ | Demilitarized Zone |
| EAP-TLS | Extensible Authentication Protocol-Transport Layer Security |
| ESP | Encapsulating Security Payload |
| GRE | Generic Routing Encapsulation |
| HW | Hardware |
| CHAP | Challenge-handshake authentication protokol |
| ICT | Informační a komunikační technologie |
| IS | Informační systém |
| ISP | Internet service provider |
| IDEA | International Data Encryption Algorithm |
| IKE | Internet Key Exchange |
| IP | Internet Protocol |
| IPsec | Internet Protocol Security protokol |
| JRE | Java Runtime Environment |

| | |
|---|---|
| L2F | Layer Two Forwarding |
| L2TP | Layer Two Tunneling Protocol |
| L2TP/IPsec | Layer Two Tunneling Protocol s ochranou IPsec |
| MD5 | Message-Digest algorithm |
| MPPE | Microsoft Point to Point Encryption |
| MS-CHAP | Microsoft Challenge-handshake authentication protokol |
| MS-CHAP2 | Microsoft Challenge-handshake authentication protokol ver. 2 |
| NAC | Network Access Control |
| NAP | Network Access Protection |
| NAT | Network Address Translation |
| NX | NoMachine - NX server |
| OTP | One-Time Password |
| PAP | Password Authentication Protocol |
| PC | Personal Computer |
| PEAP | Protected Extensible Authentication Protocol |
| PKI | Public-Key Infrastructure |
| PLA | Povodí Labe, státní podnik |
| PPP | Point-to-Point Protocol |
| PPTP | Point-to-Point Tunneling Protocol |
| PSK | Pre-shared key |
| RDP | Remote Desktop Protocol |
| RFC | Request for Comments |
| SAN | Storage area network |
| SHA | Secure Hash Algorithm |
| SSH | Secure Shell |

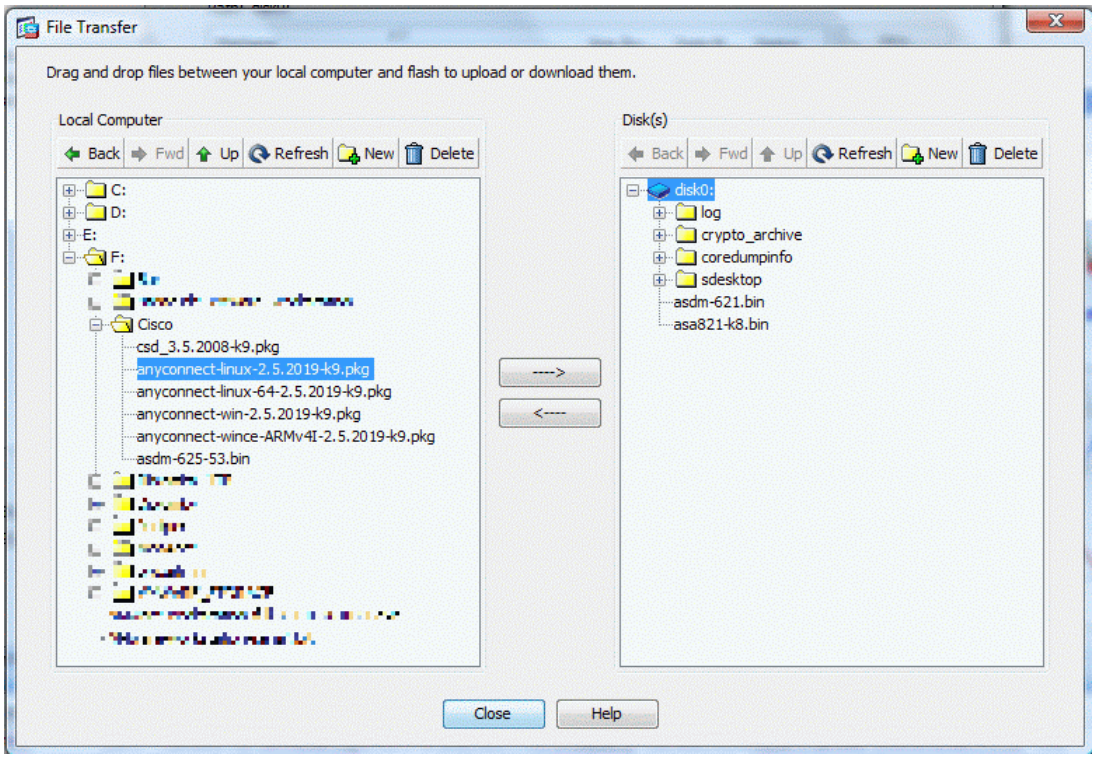
| | |
|---|---|
| SSL/TLS | Secure Sockets Layer/Transport Layer Security |
| SSTP | Secure Socket Tunneling Protocol |
| TCP | Transmission Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| UDP | User Datagram Protocol |
| URL | Unique Resource Locator |
| VNC | Virtual Network Computing |
| VPN | Virtual Private Network |
| WAN | Wide Area Network - Rozlehlá síť |
| WSUS | Windows Server Update Services |
| XML | Extensible Markup Language |

# SEZNAM OBRÁZKŮ

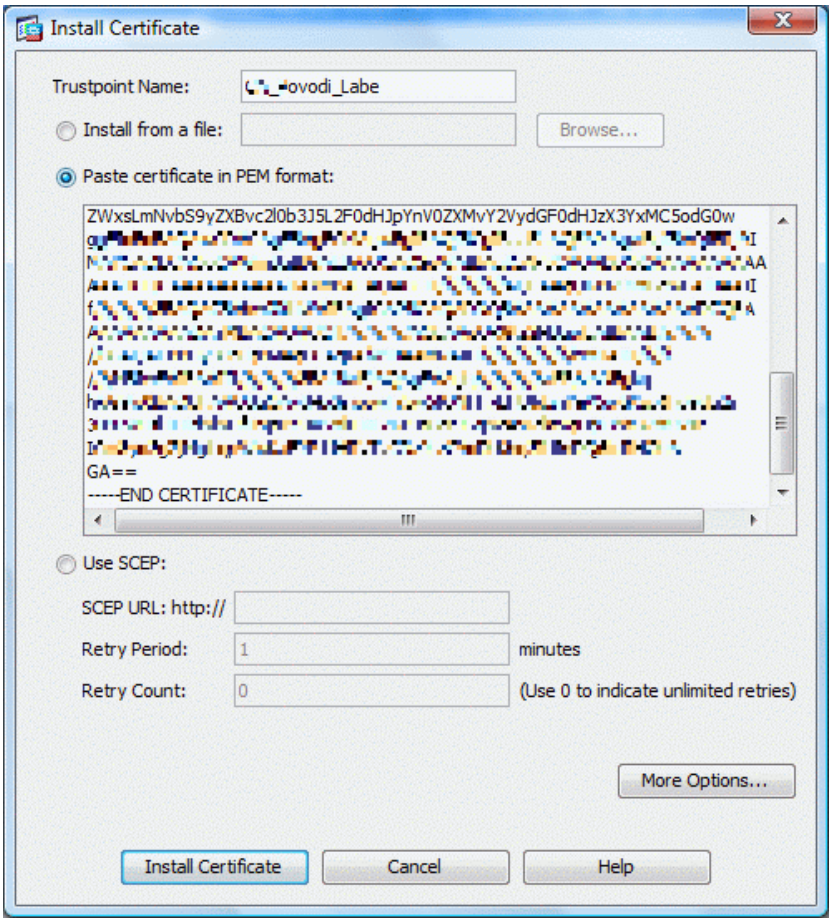
# SEZNAM TABULEK

# SEZNAM PŘÍLOH

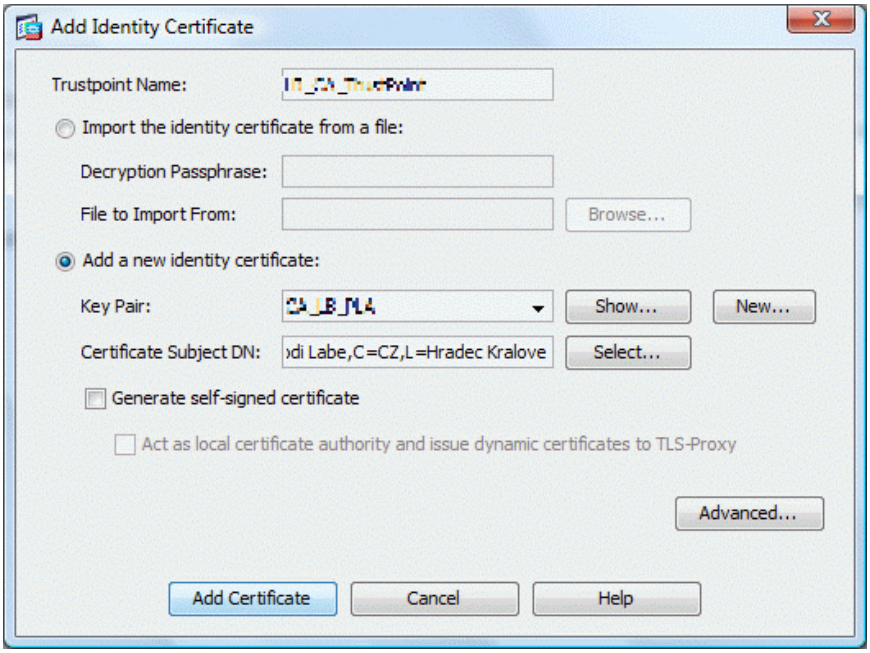
# PŘÍLOHA P I: OBRÁZKY



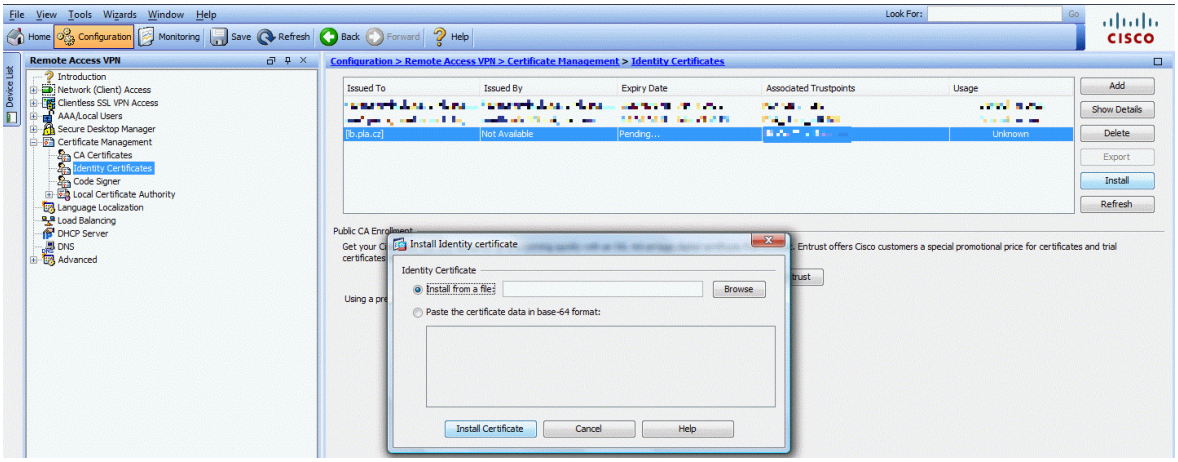

Obr. 1 - Upgrade CSD a AnyConnectClient



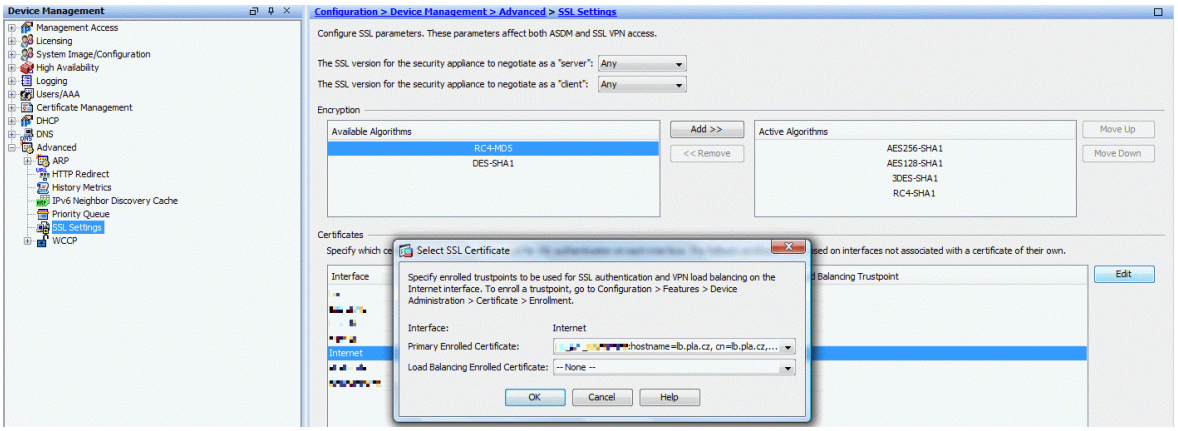

Obr. 2 - Instalace CA certifikátu



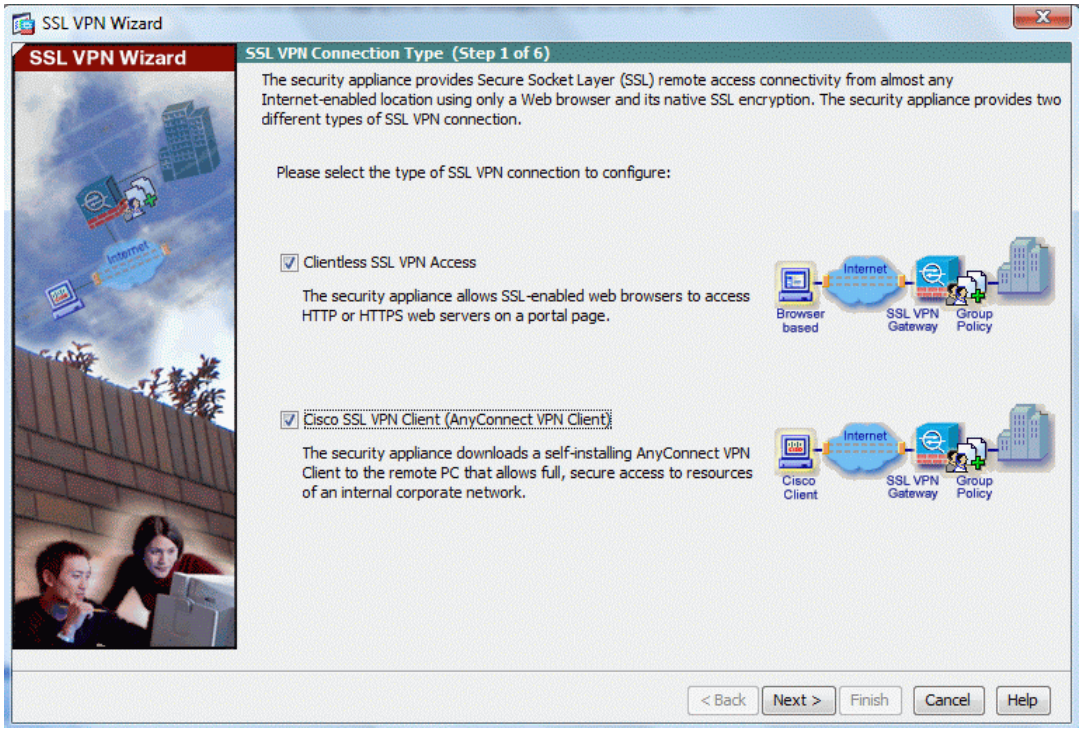

Obr. 3 - Vytvoření Identity certifikátu



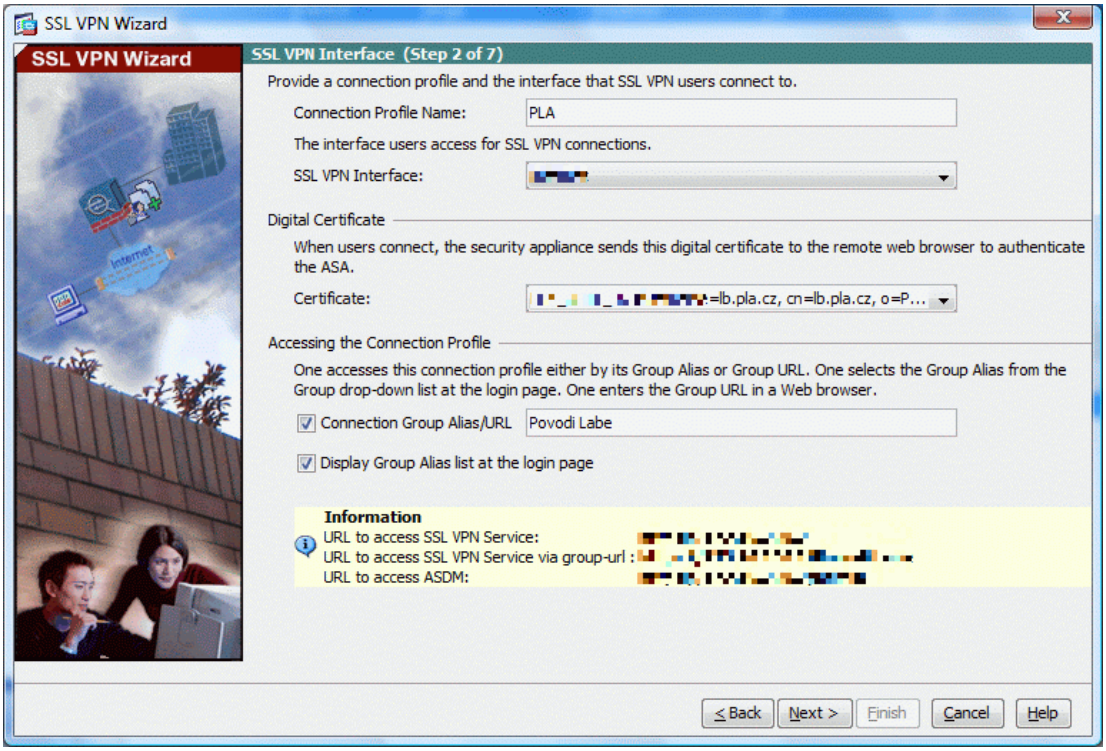

Obr. 4 – Instalace podepsaného certifikátu



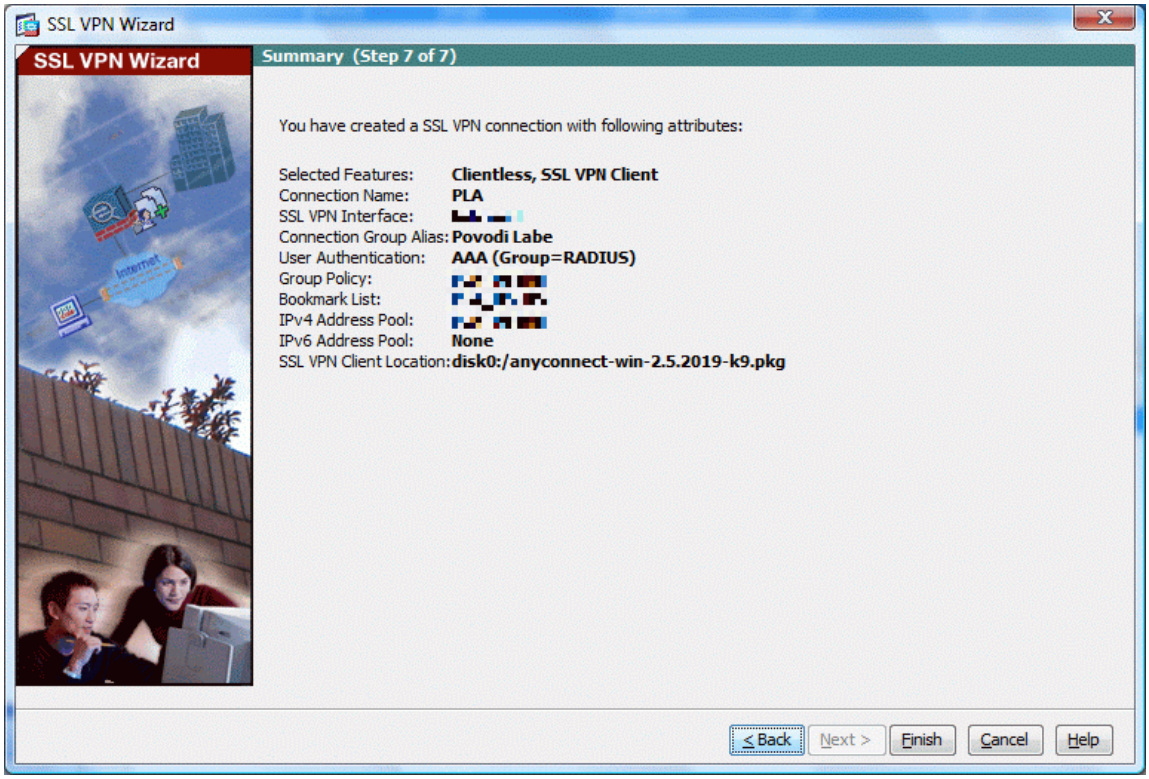

Obr. 5 - Přiřazení SSL certifikátu na daný interface



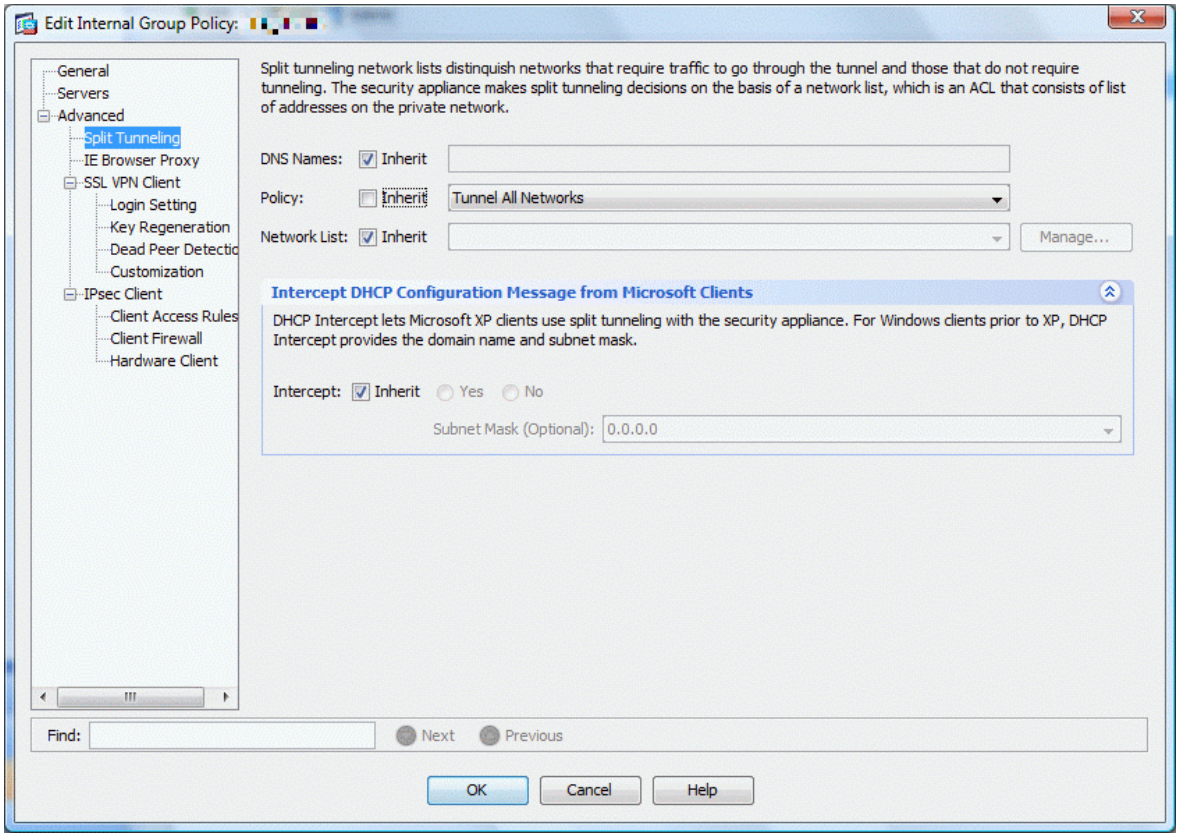

Obr. 6 - Úvodní obrazovka průvodce vytvoření SSL VPN



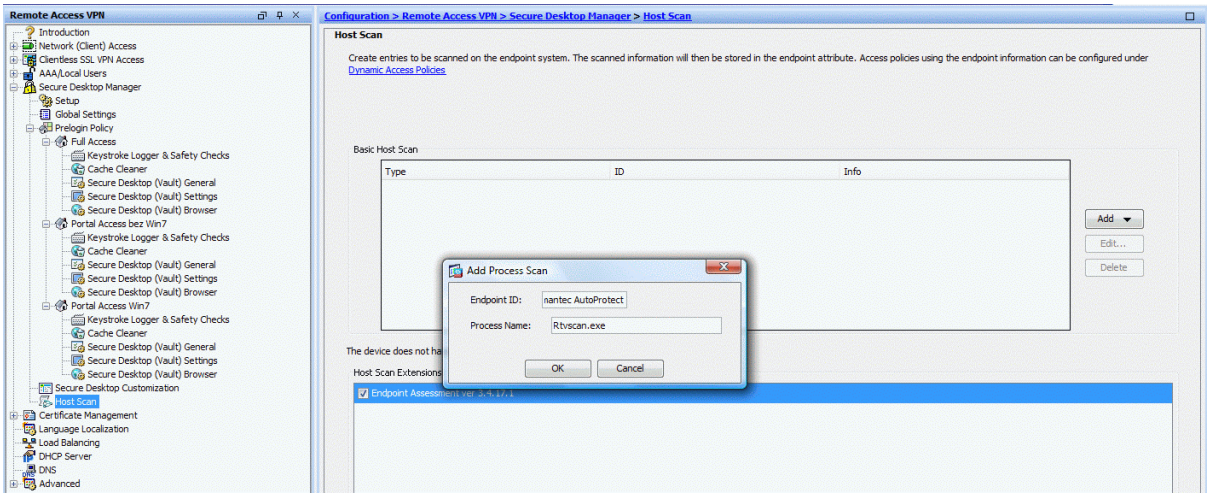

Obr. 7 - Konfigurace SSL VPN pomocí průvodce



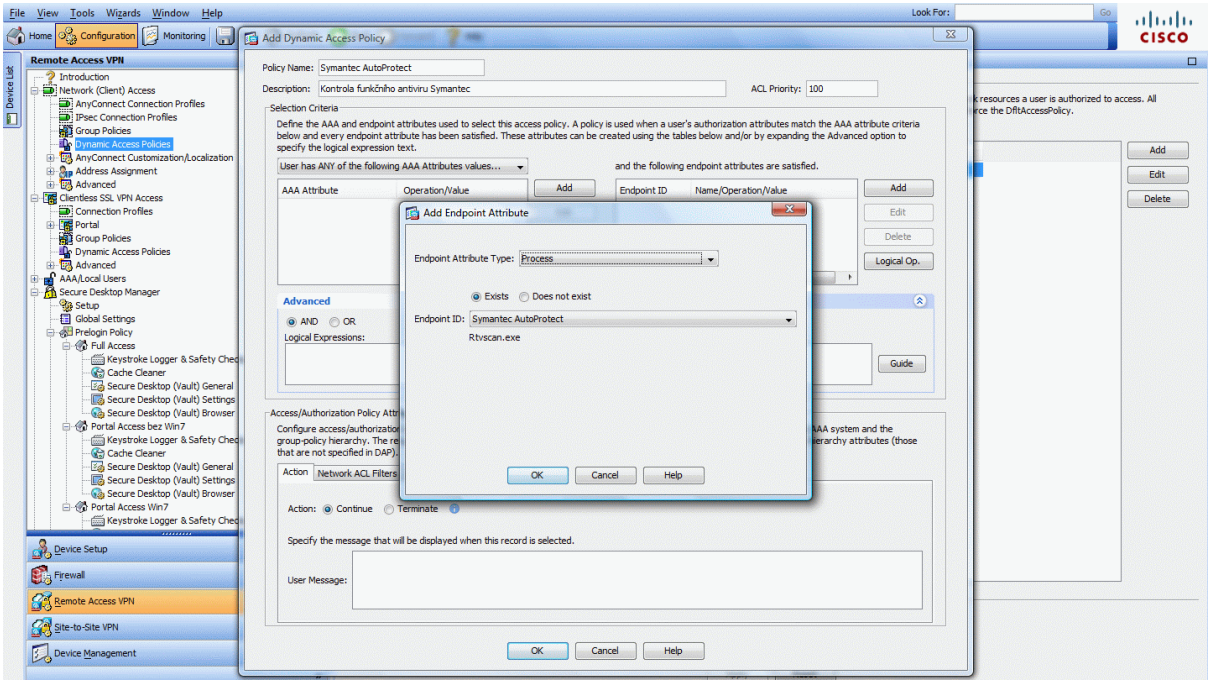

Obr. 8 - Dokončení konfigurace SSL VPN pomocí průvodce



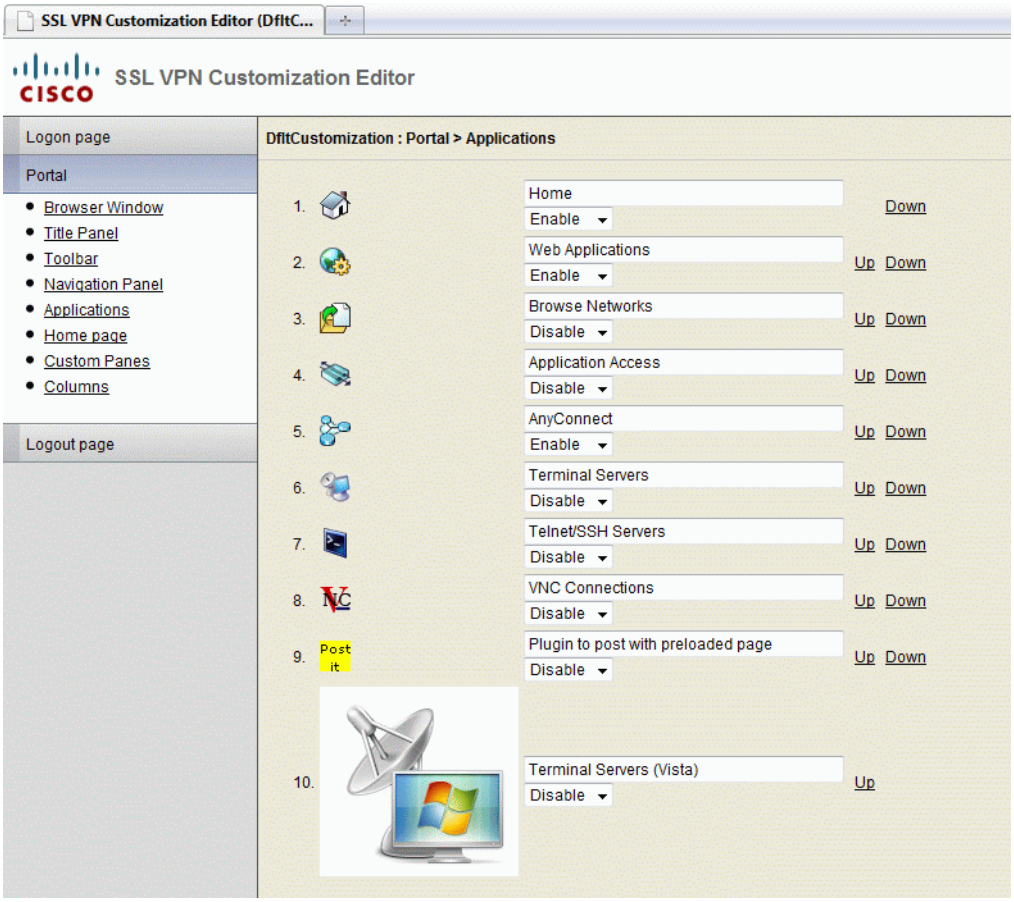

Obr. 9 - Úprava Group Policy



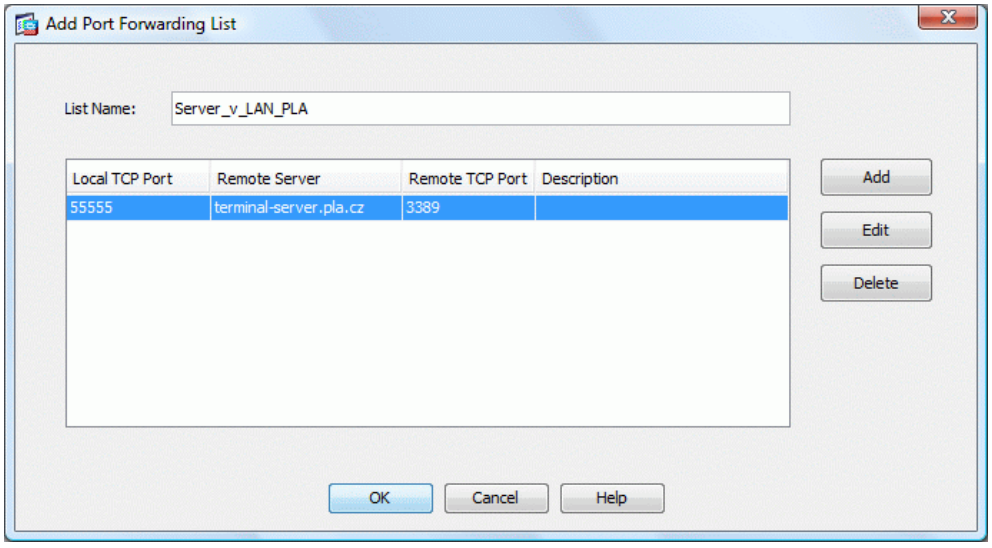

Obr. 10 - Vytvoření Host Scan



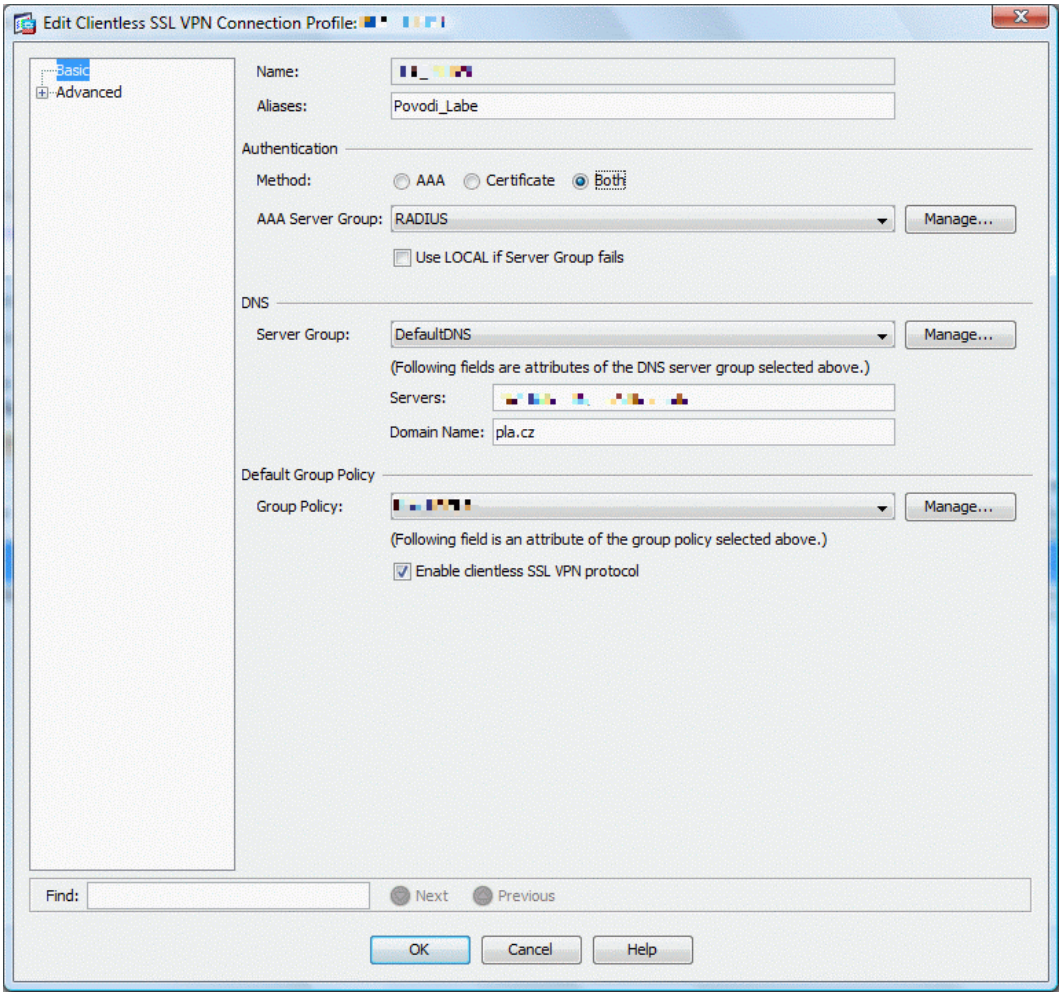

Obr. 11 - Konfigurace DAP



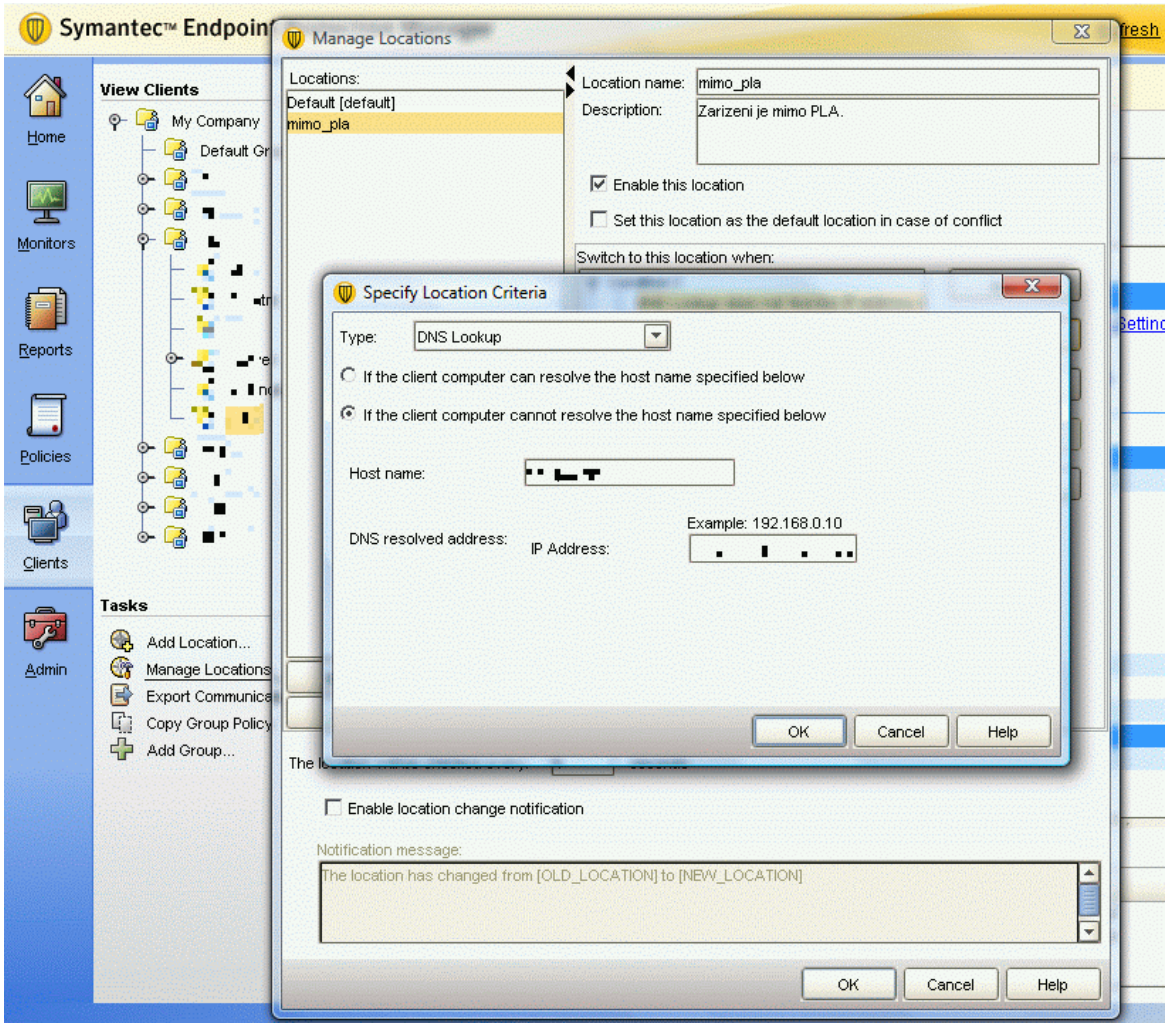

Obr. 12 - Úprava portálu



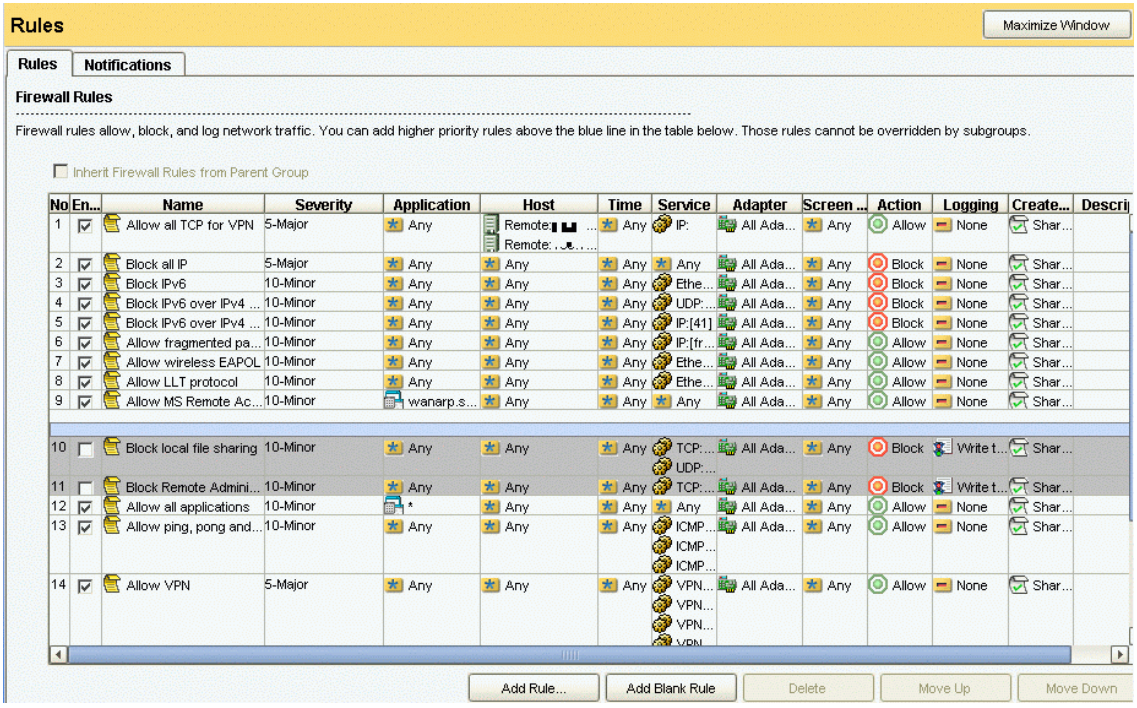

Obr. 13 - Konfigurace Port Forwardingu



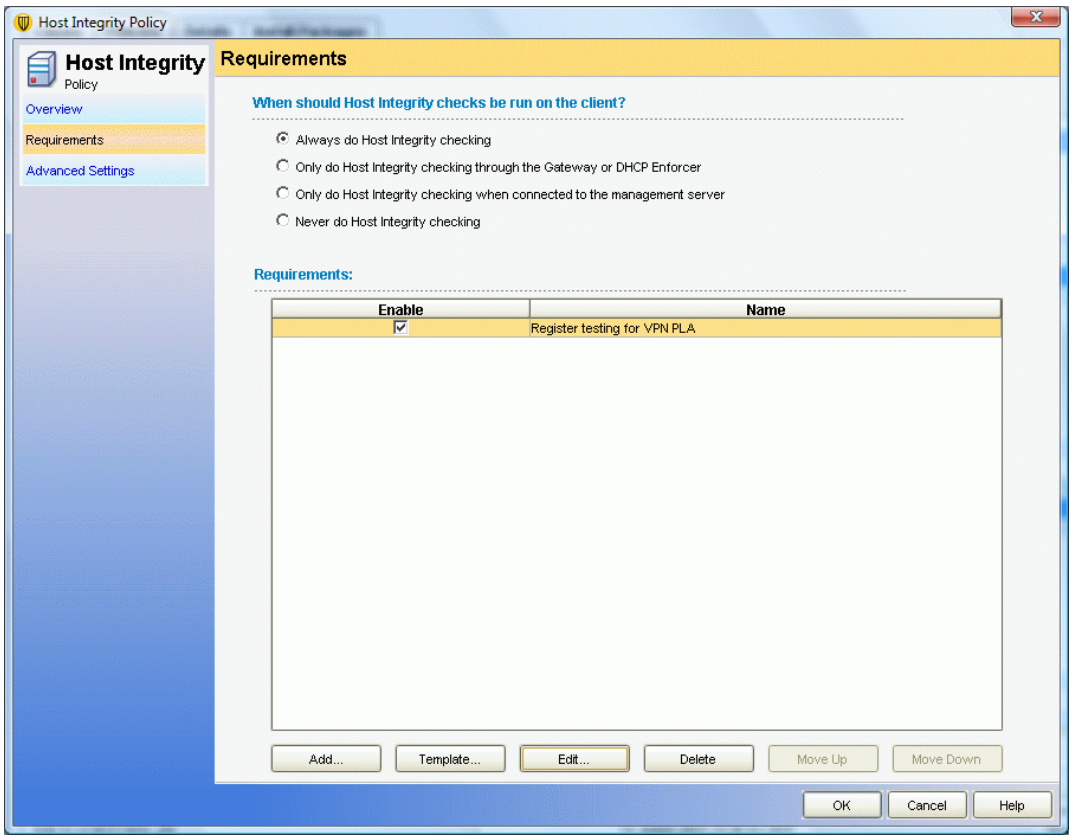

Obr. 14 - Zapnutí dvoufaktorové autentizace



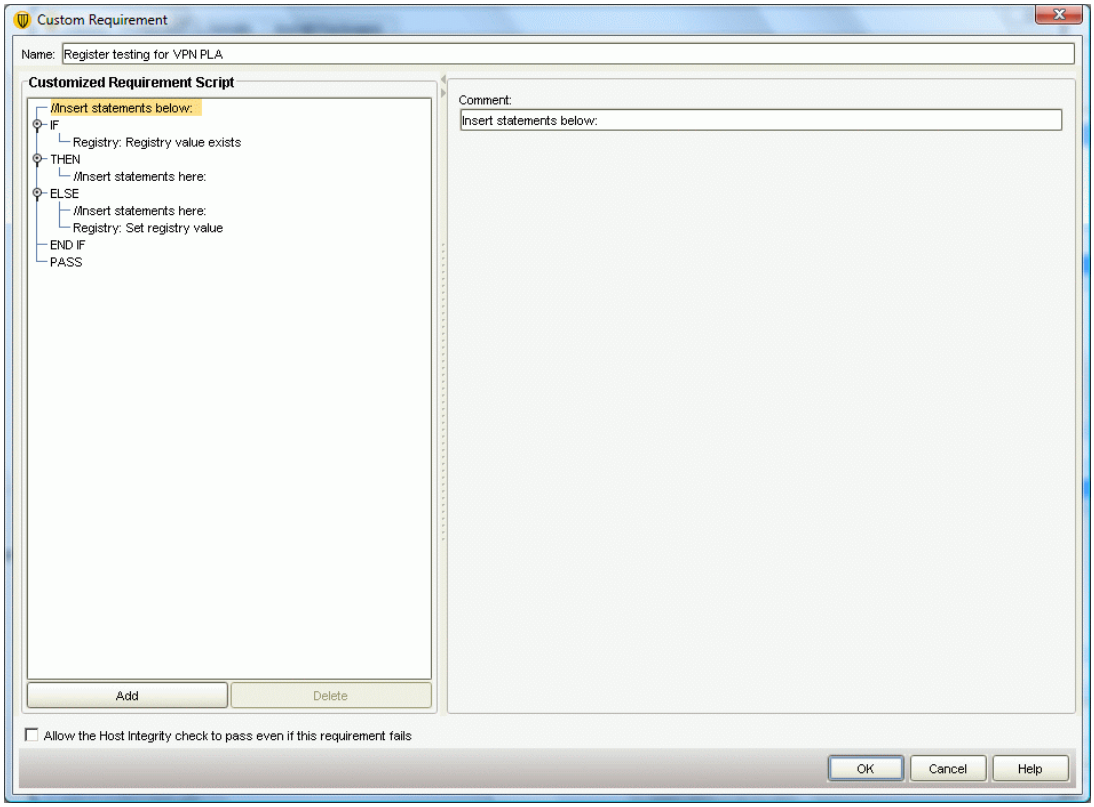

Obr. 15 - Personal firewall -Definice location



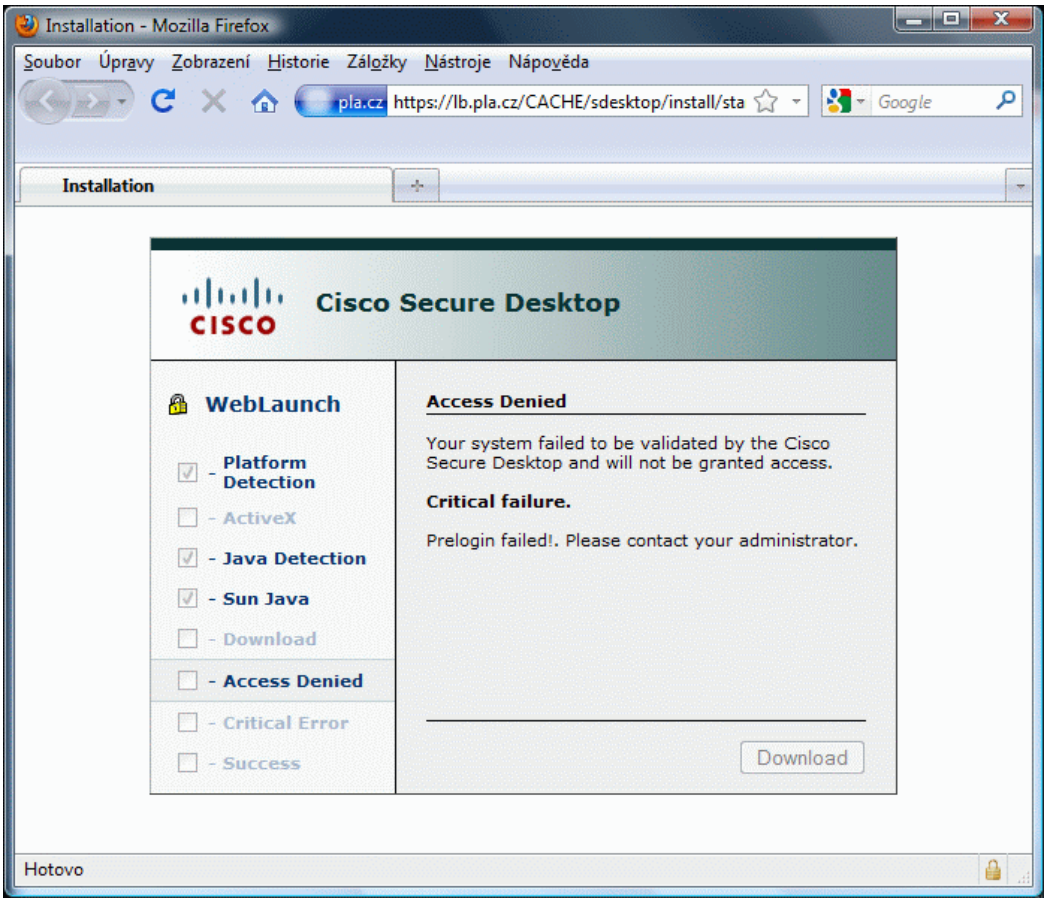

Obr. 16 - Definice firewall politik



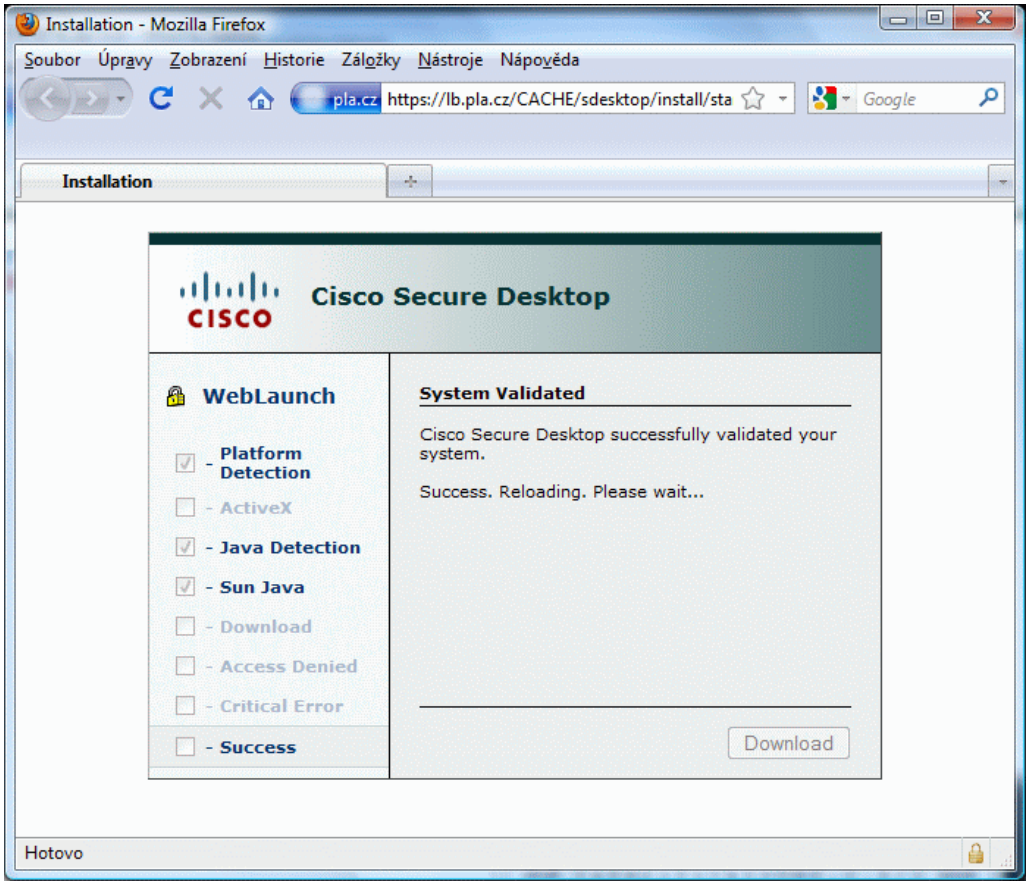

Obr. 17 - Definice Host Integrity politiky



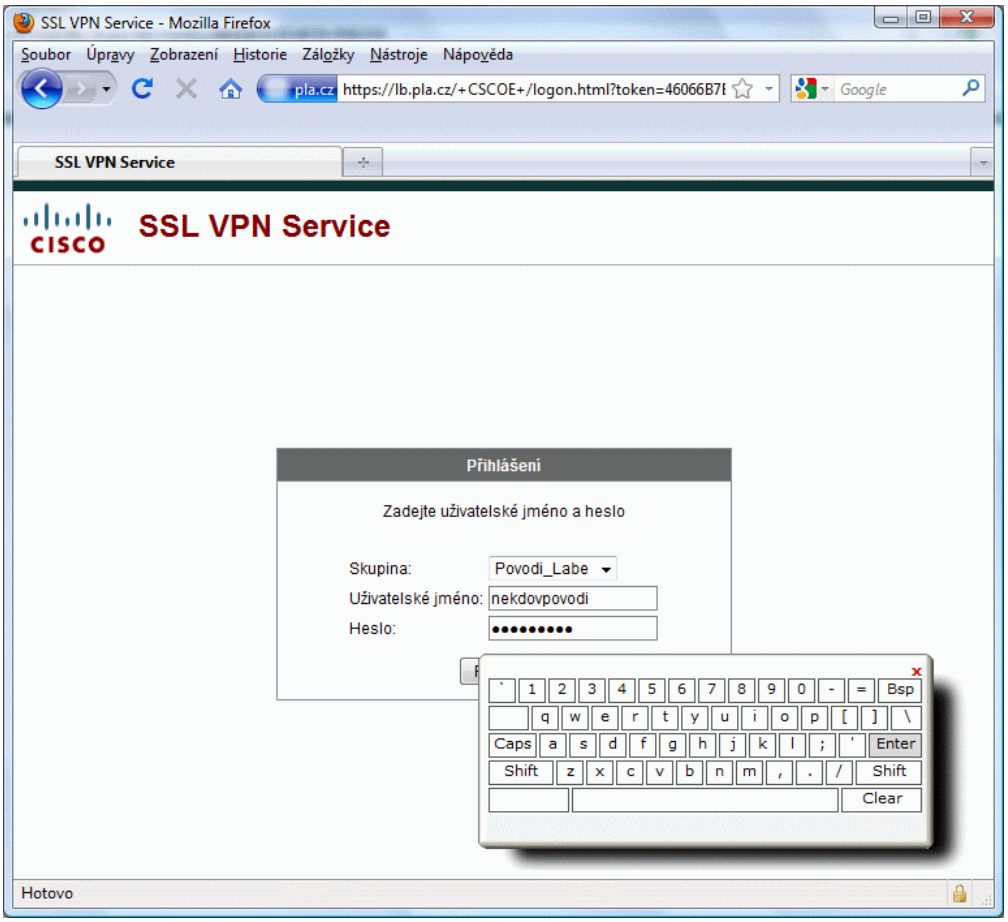

Obr. 18 - Detail - Definice Host Integrity politiky



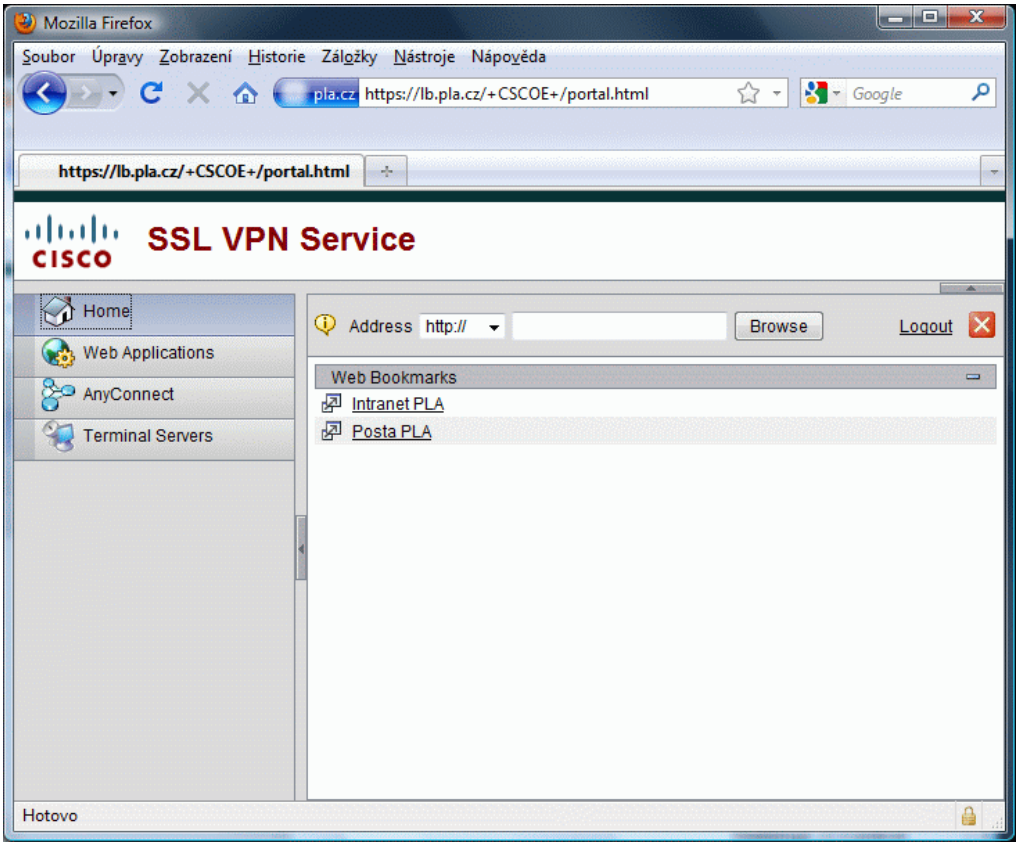

Obr. 19 - Nevyhovění Prelogin Policies



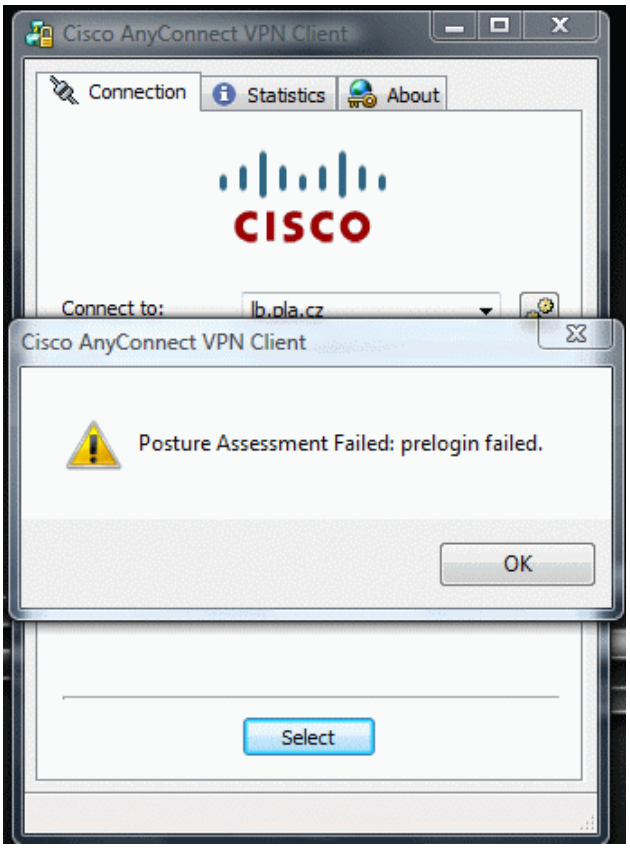

Obr. 20 - Vyhovění Prelogin Policies



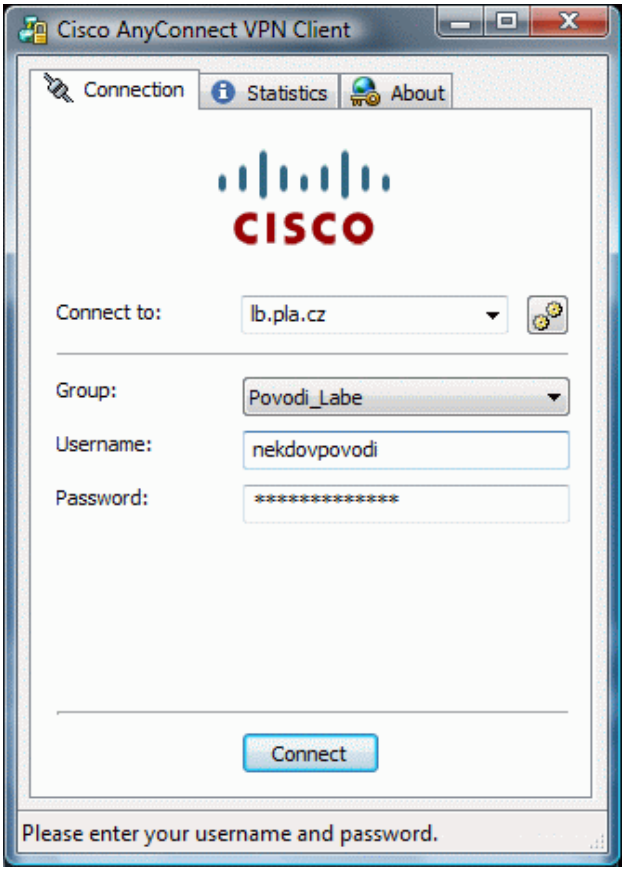

Obr. 21 - Přihlašovací dialog



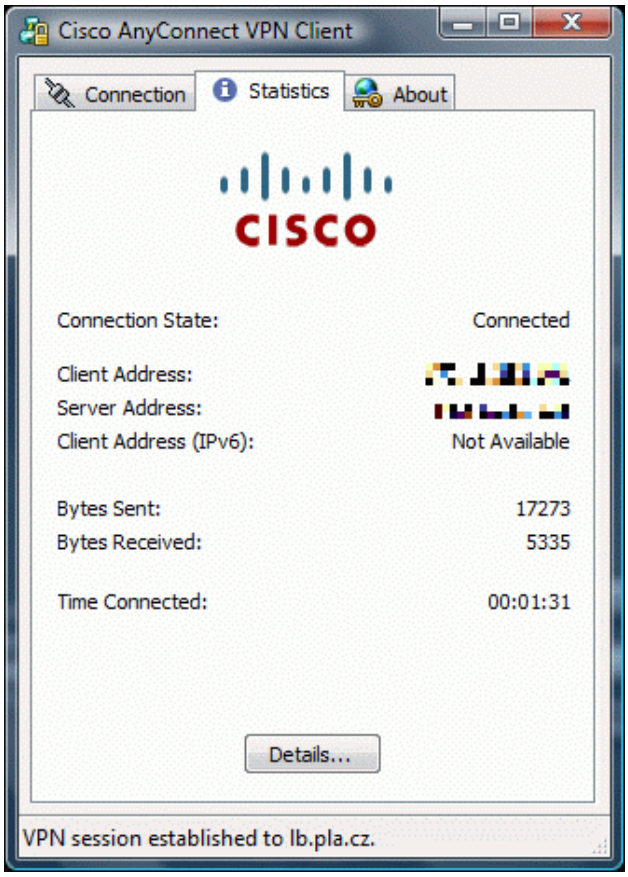

Obr. 22 - Portál SSL VPN



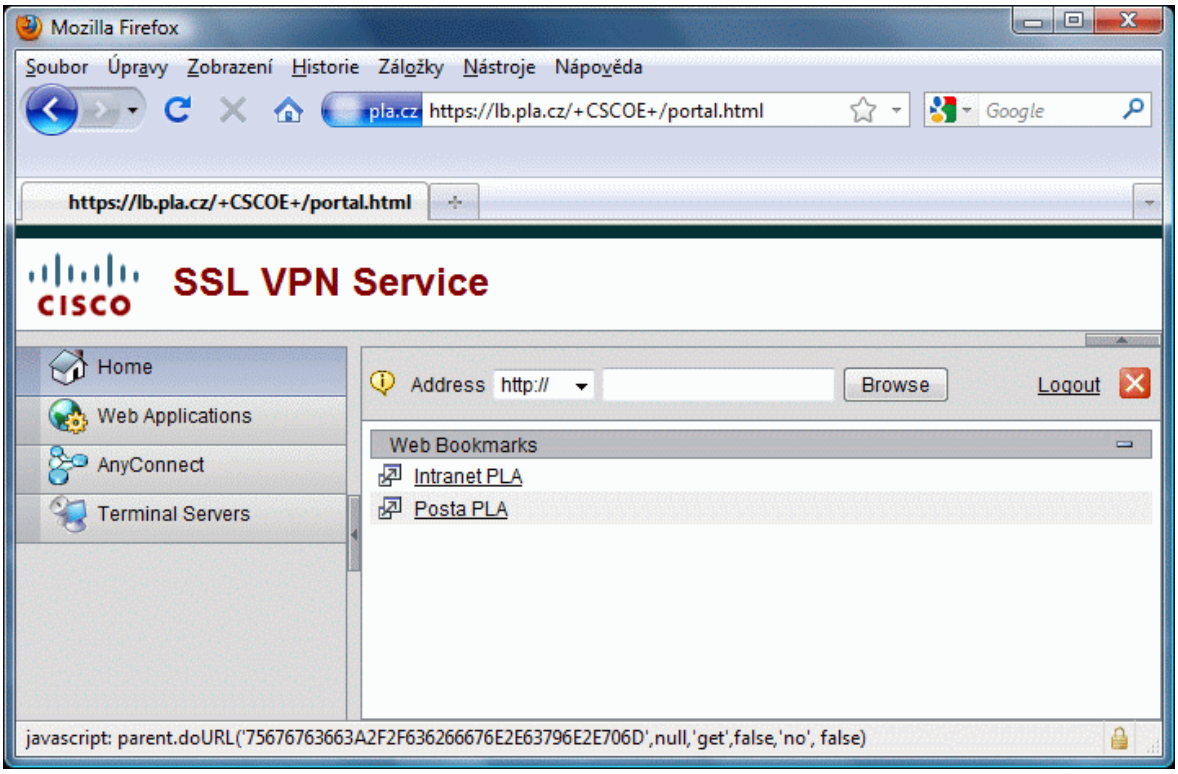

Obr. 23 – Nelze se přihlásit - Prelogin Policies Failed



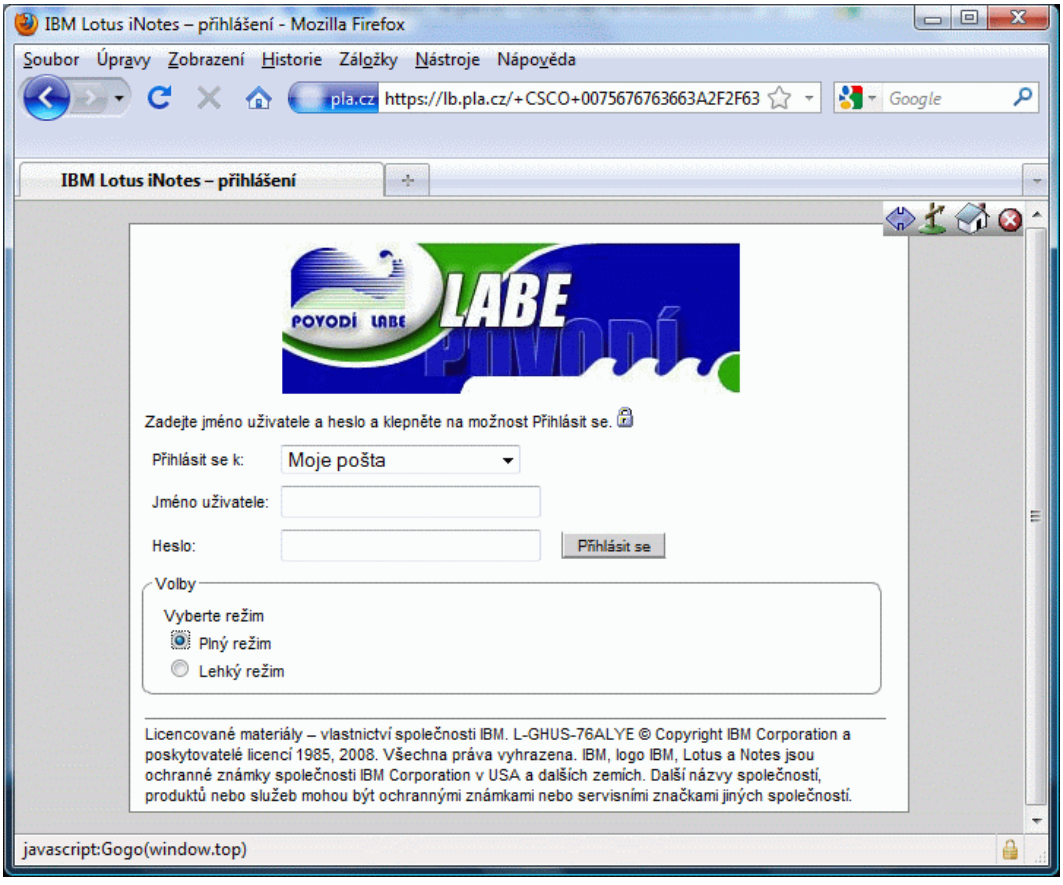

Obr. 24 - Lze se přihlásit - Prelogin Policies OK



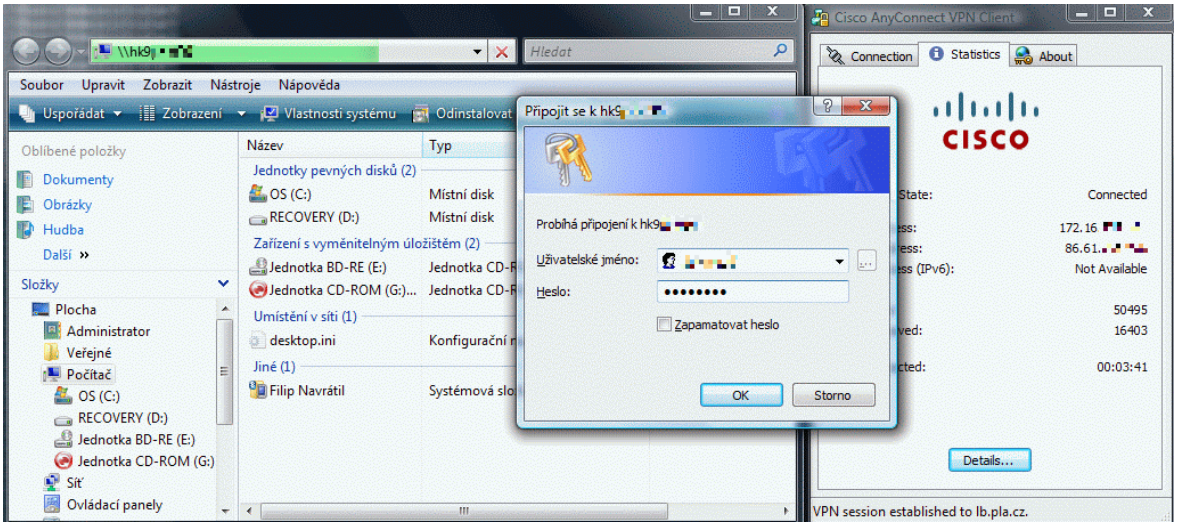

Obr. 25 – Připojený AnyConnect VPN klient



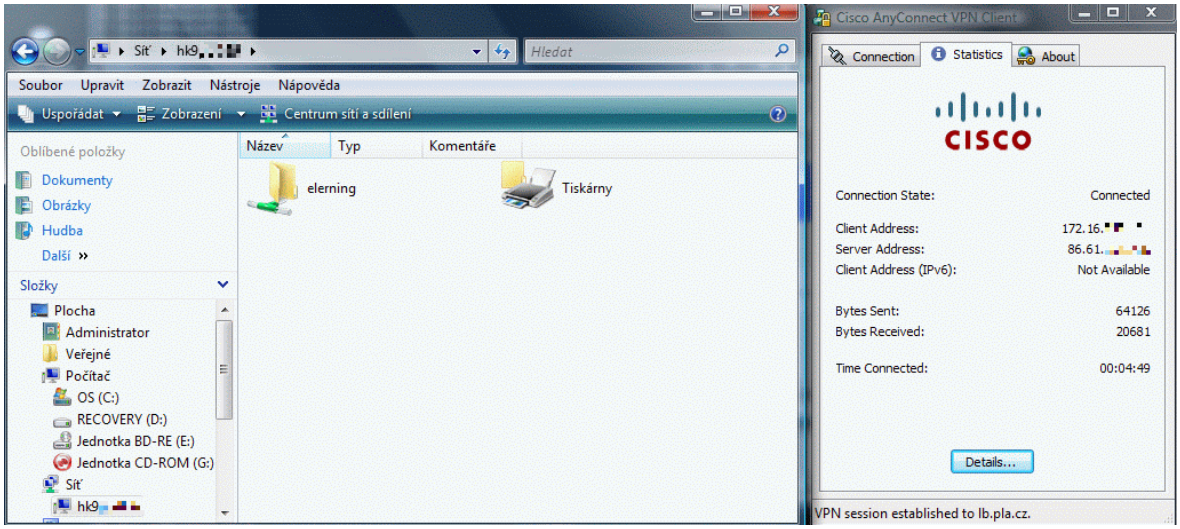

Obr. 26 - VPN portál



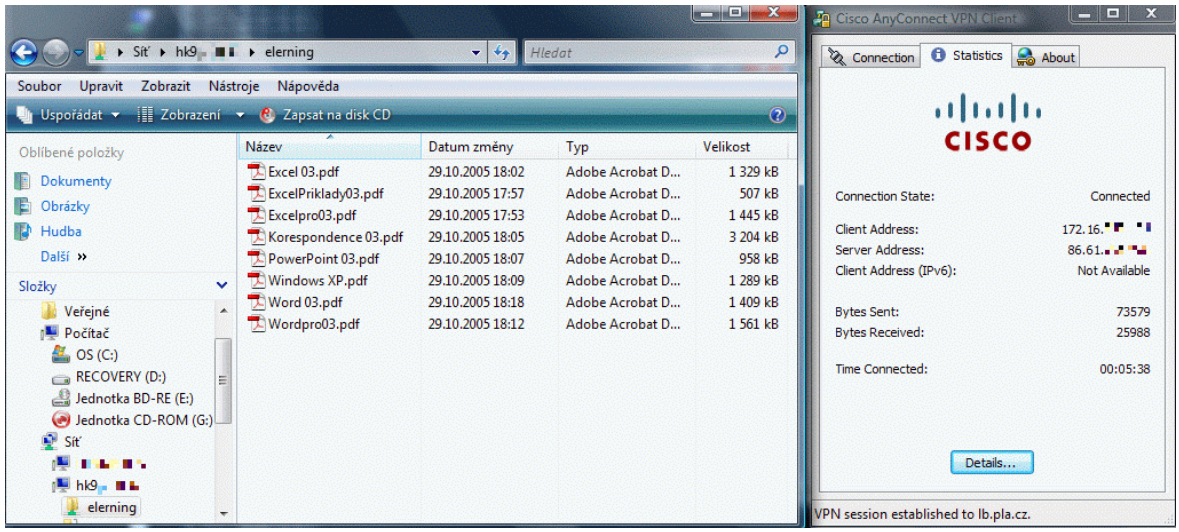

Obr. 27 - Přístup do interní elektronické pošty skrze VPN portál




Obr. 28 - Připojení k souborovému serveru




Obr. 29 - Připojení k souborovému serveru




Obr. 30 – Procházení dat na souborovém serveru