UNIVERZITA PARDUBICE
Fakulta elektrotechniky a informatiky

Technologie OpenVPN

Lukáš Liška

Bakalářská práce
2013

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Lukáš Liška**
Osobní číslo:	**I10121**
Studijní program:	**B2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Technologie OpenVPN**
Zadávající katedra:	**Katedra informačních technologií**

Zásady pro vypracování:

Autor v bakalářské práci popíše princip virtuálních privátních sítí (VPN) a technologie využívané při jejich tvorbě. Specifikace požadavků kladené na VPN, výhody použití, popíše VPN na spojové, síťové vrstvě, transportní a aplikační vrstvě. Praktická realizace bude provedena v síťové laboratoři pomocí technologie OpenVPN a Cisco VPN.

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

***STEINBERG, Joseph. SSL VPN: understanding, evoluating and planning secure, web-based remote access. Vyd. 1. Birmingham: Packt Publishing, 2005, 195 s. ISBN 19-048-1107-8.**

***OPPLIGER, Rolf. SSL and TLS: theory and practice. Vyd. 1. Boston: Artech House, c2009, xxi, 257 p. Artech House information security and privacy series. ISBN 15-969-3447-6.**

Vedoucí bakalářské práce: **Ing. Soňa Neradová**
Katedra softwarových technologií

Datum zadání bakalářské práce: **21. prosince 2012**
Termín odevzdání bakalářské práce: **10. května 2013**

L.S.

prof. Ing. Simeon Karamazov, Dr.
děkan

Ing. Lukáš Čegan, Ph.D.
vedoucí katedry

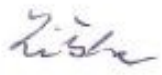
V Pardubicích dne 29. března 2013

Prohlášení autora

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.



V Pardubicích dne 15. 8. 2013 Lukáš Liška

Poděkování

Na tomto místě bych chtěl poděkovat své vedoucí práce, Ing. Soně Neradové, za vstřícnost, ochotu a cenné rady poskytnuté v průběhu zpracování bakalářské práce.

Anotace

Tato bakalářská práce v teoretické části popisuje základní rozdělení virtuálních privátních sítí a jejich princip na spojové, síťové, transportní a aplikační vrstvě. Praktická část je zaměřena na popis konfigurace virtuální privátní sítě pomocí technologie Cisco VPN a OpenVPN.

Klíčová slova

VPN, konfigurace, Clientless SSL VPN, SSL VPN Client, OpenVPN

Title

Technologies OpenVPN

Annotation

This bachelor's work in theoretical part describes the basic division of private networks and their principle to network access, internet, transport and application layer. The practical part is focused on how to configure a virtual private network using Cisco VPN and OpenVPN.

Keywords

VPN, configuration, Clientless SSL VPN, SSL VPN Client, OpenVPN

Obsah

Seznam zkratek

3DES	Triple Data Encryption Standard
AAA	Autentizace, Autorizace a Accounting
AES	Advanced Encryption Standard
AH	Authentication Header
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CA	Certifikační autorita
CUG	Closed User Group identifier
DES	Data Encryption Standard
DH	Diffie–Hellman
EAP	Extensible Authentication Protocol
ELAN	emulation Local Area Network
ESP	Encapsulating Security Payload
FR	Frame Relay
GRE	Generic Routing Encapsulation
IKE	Internet Key Exchange
L2F	Layer 2 Forwarding Protocol
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LEC	Local Area Network emulation client
LES	Local Area Network emulation server
LSP	Label Switch Path
MD5	Message-Digest Algorithm
MPOA	Multiprotocol over Asynchronous Transfer Mode
MPLS	Multiprotocol Label Switching
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network
WAN	Wide Area Network

Seznam obrázků

Seznam tabulek

Úvod

Ve světě protkaném datovými spoji vzniká potřeba, aby spolu lidé a organizace komunikovali bezpečně. Cena pronájmu soukromých linek nebo WAN spojů je vysoká, takže běžnému uživateli je tato technologie nedostupná. Řešením těchto problémů jsou právě virtuální privátní sítě, kterými se tato bakalářská práce zabývá.

Cílem této práce je tedy přiblížit čtenáři technologii virtuálních privátních sítí. Tato technologie a její problematika je náplní úvodní kapitoly. Zde se popisuje její základní rozdělení, princip fungování a výhody či požadavky přinášející její používání.

V další části je charakteristika virtuálních privátních sítí detailněji popsána na jednotlivých vrstvách síťového modelu TCP/IP.

Praktická část práce pomocí navrženého simulačního schématu poskytuje způsob realizace virtuální privátní sítě s popsanými jednotlivými kroky, které vedou k její tvorbě.

1 Úvod do VPN

Virtuální privátní sítě, pro které se vžila zkratka VPN, jsou základním prvkem bezpečné komunikace mezi sítěmi. Jak již samotný název napovídá, jedná se o sítě, jejichž zabezpečení soukromí je umožněno či zajištěno pomocí určité formy virtualizace. VPN lze tedy považovat za způsob určité simulace soukromé sítě ve veřejné síti, jakou je například Internet. Nazývá se „virtuální“ protože závisí na použití virtuálního propojení, to je dočasné spojení, které může být vytvořeno za použití příslušného softwaru, hardwaru nebo kombinací obojího. Virtuální okruhy, které takto vzniknou, jsou privátní datovou sítí propojující jednotlivé uživatele nebo lokality s pomocí tunelovacích a šifrovacích protokolů.

Ohledně výrazu VPN lze nalézt několik různých definicí, bohužel některé jsou poněkud hůře pochopitelné. Jednoduchá a srozumitelná definice by tedy mohla znít takto. VPN je síť umožňující vytvořit zabezpečené spojení na veřejné komunikační infrastruktuře.

1.1 Základní typy sítí VPN

Rozlišují se tři základní druhy VPN, které vznikly postupem času s rozvojem technologií a nároky uživatelů.

1.1.1 Důvěrné (Trusted) VPN

První sítě VPN vznikaly nad privátními pronajatými telefonními linkami. Teprve později se začaly budovat přes veřejné sítě typu Internet. Prvotní sítě tohoto druhu se nazývaly důvěryhodné VPN a jejich bezpečnost byla závislá čistě na ochraně privátní linky. Bylo možné skrz ně dopravovat data mnoha zařízení souběžně, a tato zařízení se spoléhala na bezpečnost, kterou v systému zajišťoval pouze poskytovatel privátního datového spoje.

Důvěryhodné sítě VPN používají následující technologie linkové a síťové vrstvy:

- Virtuální okruhy ATM druhé vrstvy.
- Virtuální okruhy Frame Relay druhé vrstvy.
- Transport rámců protokolem druhé vrstvy MPLS.
- Směrování MPLS řízené protokolem třetí vrstvy BGP, který se používá na Internetu. [1]

1.1.2 Bezpečné (Secure) VPN

Problematiku bezpečnosti však zkomplikoval rozvoj Internetu. Na technologii důvěryhodných VPN sítí se najednou nedalo spoléhat, protože kombinováním více VPN linek u poskytovatelů vzniká nebezpečí možnosti odposlouchávání na trase. Do sféry bezpečnosti VPN proniklo šifrování, které se uplatňuje na koncových bodech VPN linek. Data přenášená po Internetu jsou tedy zašifrována. Koncovými body, které na jedné straně linky přidávají šifrování a na druhé straně jej odstraňují, jsou často hraniční směrovače nebo podobná zařízení. Tento typ VPN se tedy nazývá bezpečné VPN.

V bezpečných VPN se využívají následující technologie a šifrovací protokoly:

- Šifrování IPsec v transportním nebo tunelovém režimu.
- Kombinace L2TP/IPsec.
- MPLS LSP – Protokol LSP propojuje směrovače v síti MPLS.
- SSL verze 3.0 nebo TLS spolu se šifrováním. [1]

1.1.3 Hybridní

Jedná se o sítě, které kombinují vlastnosti obou výše zmíněných a snaží se těžit z jejich výhod. Internet se v tomto případě pokládá za rozlehlou síť WAN a zabezpečená VPN část pokrývá právě tuto veřejnou část sítě VPN. Zbývající díl sítě na obou stranách linky může, ale nemusí být zabezpečen pomocí šifrování. Poskytují se v něm však minimálně služby důvěryhodné VPN sítě. Zpravidla se jedná o kombinaci lokálních bezpečných sítí s důvěrnými sítěmi poskytovatelů.

V hybridních VPN se mohou využívat technologie z libovolné kombinace technologií používaných pro bezpečné a důvěryhodné VPN sítě. [1]

1.2 Požadavky kladené na VPN

Existuje jeden velmi důležitý požadavek, který je společný pro bezpečné, důvěryhodné a hybridní VPN. Administrátor VPN musí znát celý rozsah sítě VPN a bez ohledu na použitý typ sítě VPN by měla mít VPN schopnost, které normální síť nemá.

Konkrétní požadavky pro důvěrnou VPN jsou:

- Směrování a adresace používaná v síti musí být stanovena před vytvořením VPN.
- Nikdo jiný než poskytovatel důvěrné VPN nesmí měnit, vkládat a mazat data nebo vymazat údaje o vlastnostech VPN.
- Nikdo jiný než poskytovatel důvěrné VPN nesmí vytvářet nebo měnit cesty uvnitř sítě VPN.

Konkrétní požadavky pro bezpečnou VPN jsou:

- Veškerý provoz na zabezpečené VPN, musí být šifrován a autentizován. Mnoho protokolů, které se používají pro vytvoření zabezpečené VPN umožňují vytvoření VPN, které využívají autentizace, ale bez šifrování. I když takové sítě jsou bezpečnější, než sítě bez autentizace, nejedná se o bezpečnou VPN, protože neexistuje žádné soukromí.
- Bezpečnostní vlastnosti VPN musí být odsouhlaseny všemi stranami v rámci VPN. Bezpečná VPN má jeden nebo více tunelů, a každý tunel má dva koncové body. Administrátoři obou konců každého tunelu musí být schopny se dohodnout na společných vlastnostech tunelu.
- Nikdo mimo VPN nesmí ovlivnit bezpečnostní vlastnosti VPN. Nesmí být možné, aby útočník změnil bezpečnostní vlastnosti kterékoli části sítě VPN, například oslabit šifrování nebo ovlivnit šifrovací klíče, které jsou používány.

Konkrétní požadavky pro hybridní VPN jsou:

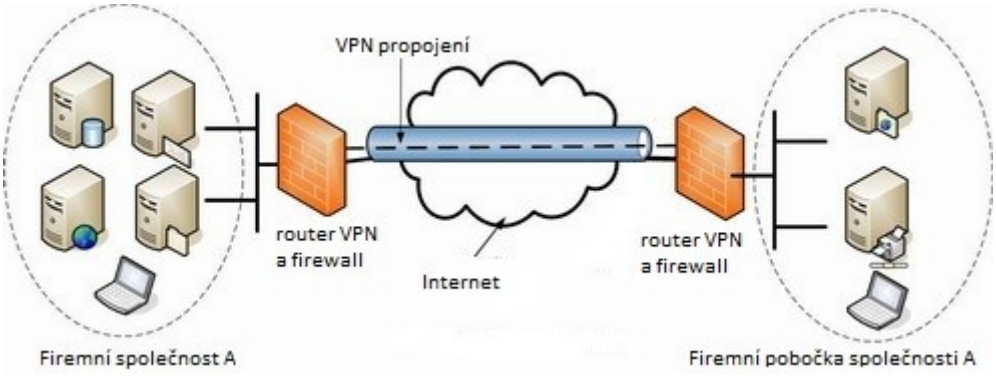
- Hranice zabezpečené VPN v rámci důvěrné VPN musí být zcela jasná, protože hybridní VPN může být jen z určité části zabezpečená VPN, jelikož je tvořena v rámci důvěrné VPN sítě.
- Administrátor VPN musí vědět, jestli provoz mezi dvěma určitými adresami v hybridní VPN je součástí bezpečného VPN či nikoliv. [1]

1.3 Topologie VPN

Z hlediska topologie sítě rozlišujeme dva typy základních propojení site-to-site a klient-to-site neboli vzdálený přístup. Topologie se od sebe odlišují především v tom, k jakému účelu se využívají.

1.3.1 Site-to-site topologie

Jak již název napovídá, site-to-site propojují dvě a více lokálních sítí. Firemní společnosti používají propojení sítí přes VPN ke spojení rozptýlených míst stejným způsobem, jako kdyby byly propojeny pronajatou linkou nebo jinou WAN technologií (Frame Relay, ATM). Výhodou takového propojení je sdílení podnikového intranetu nebo extranetu s pracovním partnerem. V této topologii, uživatelé posílají a přijímají data skrz VPN bránu, kterou bývá obvykle směrovač nebo server. VPN brána je zodpovědná za šifrování odchozího provozu a posílání jej skrz VPN tunel do internetu k protější VPN bráně cílové sítě. Tato brána odřeže hlavičku paketu, rozšifruje obsah a doručí paket k cílovému uživateli uvnitř cílové sítě. [2]

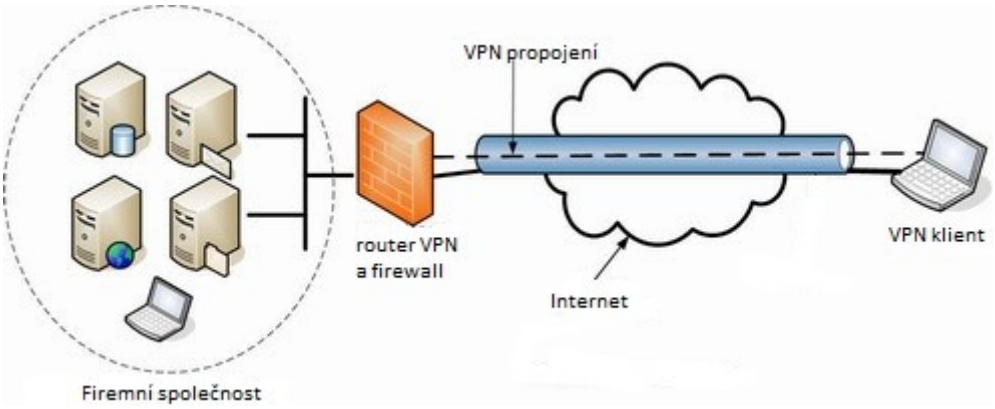


Obrázek 1 – Topologie VPN site-to-site [11]

1.3.2 Client-to-site topologie

Client-to-site, někdy taky označováno jako client-to-server neboli vzdálený přístup slouží pro přístup vzdálených uživatelů k lokální síti. Obvykle se jedná o pracovníky v terénu či domácí uživatele, kteří se potřebují dostat k firemním síťovým aplikacím. Po navázání VPN mají vzdálení uživatelé stejný přístup k síťovým aplikacím, jako kdyby se nacházeli v příslušné lokalitě. Tento druh VPN má dočasný charakter, VPN se aktivuje dle potřeb

vzdálených uživatelů. Každý uživatel má typicky nainstalovaný VPN klient, software, který zabaluje a šifruje pakety předtím, než je odešle přes internet k cílové VPN bráně. Ten usnadňuje připojení, takže uživateli stačí základní znalost k vybudování VPN spojení. [2]



Obrázek 2 – Topologie VPN client-to-site [11]

1.4 Obecný princip navazování spojení VPN

K vytvoření VPN spojení je potřeba určitého softwaru, jehož příkladem může být OpenVPN. V některých případech je potřeba pro realizaci vytvoření VPN i nutný hardware, tím to příkladem je Cisco VPN.

Nejčastější spojení je provozováno jako klient-server aplikace, na kterém je vysvětlen následující princip VPN. VPN server běží přímo na systému s firewallem a při svém spuštění vytvoří virtuální síťové rozhraní (virtuální síťovou kartu) a tím i další podsíť firemní sítě. Server očekává spojení na vnějším rozhraní firewall systému a provádí autentizaci VPN klienta, který se připojuje z vnější sítě pomocí klientské aplikace. Po úspěšném ověření je klientskému systému přidělena IP adresa z virtuální podsítě. Mezi serverem a klientem je následně vytvořen šifrovaný tunel, kterým jsou bezpečně přenášeny všechny pakety směrovány do lokální sítě. Samozřejmě spojení mezi VPN a lokální sítí je možné omezovat pomocí pravidel firewallu a tím jednoduše určit, ke kterému systému či aplikaci se klienti mohou dostat. Takto popsané spojení bude názorně nakonfigurováno v praktické části pomocí OpenVPN a Cisco VPN. [10]

1.5 Výhody VPN používání

VPN má spoustu výhod a přínosů, které přináší ať samotným koncovým uživatelům, tak celým organizacím. Výhody při užívání VPN jsou:

- Zvýšená bezpečnost. – Po připojení k internetu přes VPN tunel jsou síťová data šifrována a zabezpečena VPN standardem. Tímto způsobem jsou tyto informace mimo dosah útočníků.

- Anonymita. – Prostřednictvím připojení VPN můžou lidé surfovat na internetových stránkách v naprosté anonymitě. Ve srovnání s metodou web proxy nebo softwarem na utajení IP je VPN na vyšší úrovni. VPN umožňuje uživatelům přístup k internetu v 100% anonymitě z libovolného softwaru nebo aplikace nainstalované v počítačovém systému.
- Odblokování webové stránky a obejití web filtrů. – V těchto dnech jedním z hlavních použití VPN je přístup k zablokované webové stránce, která je blokována lokálním ISP nebo internetovými autoritami. Využití má zejména v některých zemích, kde se uplatňuje cenzura Internetu.
- Změna IP adresy. – Služba VPN z jiného státu může dát uživatelům sítí VPN adresu IP z tohoto státu. To lze využít na webové stránky například typu on-line bankovnictví nebo webové stránky akciových investic, které vyžadují přístup z domácí země.
- Zlepšení kvality služeb a výkonu sítě. – Zde záleží na tom, jak je nastavena VPN infrastruktura. Někdy v původní síti rychlost stahování a kvalita služeb není dostatečně kvalitní či dochází ke zpoždění paketů, poté VPN připojení může výrazně pomoci.
- Snížení nákladů. – Náklady na vytvoření a údržbu připojení k LAN síti prostřednictvím VPN jsou ve srovnání s jinými bezpečnostními připojeními podstatně levnější.
- Vzdálený přístup. – Společnosti poskytují připojení VPN pro zaměstnance, kteří pracují z domova nebo z vnějšku při obchodních cestách a tak zvyšují produktivitu v podnikatelském prostředí.
- Sdílení souborů. – VPN je často používáno pro připojení více poboček v různých lokalitách nebo v zemích, takto mají soubory zabezpečené a okamžitě k dispozici po celém světě. [8]

2 VPN na síťovém modelu TCP/IP

Síťový model TCP/IP popisuje způsoby, jak vypadá síťové propojení a komunikace. Síťový model je rozdělen na čtyři vrstvy, kde každá vrstva má definované služby a může komunikovat se sousedními vrstvami. Na těchto vrstvách pak rozeznáváme několik typů VPN.

Obrázek 3 – Síťový model TCP/IP [12]

2.1 VPN na spojové vrstvě

Princip technologie vytváření VPN na spojové vrstvě pracuje podobně jako princip vytvoření plně privátních sítí na vlastních nebo pronajatých oddělených přenosových linkách. Vytvořené VPN na spojové vrstvě jsou pak nezávislé na vyšší přenosové vrstvě. Infrastrukturu těchto sítí s virtuálními obvody ve spojové vrstvě tvoří sítě ATM a Frame Relay. Za zvláštní typ VPN tvořených na spojové vrstvě lze považovat i virtuální sítě (VLAN) vytvořené technologií LAN emulace. Technologie virtuálních sítí vznikla původně pro prostředí ethernetových přepínačů, ale používá se i v sítích ATM a Frame Relay. Architektura sítí s virtuálními obvody na spojové vrstvě nabízí vysoce kvalitní alternativu k sítím pevných dedikovaných obvodů.

2.1.1 Virtuální sítě

Virtuální sítě lze aplikovat dvěma způsoby a to:

- Jestliže je ATM technologie používána pouze na páteřní přepínače a ve vlastní síti nejsou žádné koncové uzly ATM, pak je toto prostředí páteře ATM pro virtuální sítě zcela transparentní. Připojené LAN přepínače v dané VLAN komunikují mezi sebou bez toho, že by si byly vědomy existence ATM sítě mezi sebou. V reálných sítích tento jednoduchý případ ale není moc častý.
- Častějším případem je stav, kdy je potřeba použití technologie emulovaných LAN, označováno zkratkou LANE. Jedná se o případ, kdy i sdílené servery jsou

připojeny k páteři přímým ATM připojením a abychom zajistili členství i těmto uzlům v některé VLAN musí se použít právě technologie LANE.

Základní funkcí LANE je emulace LAN nad ATM sítí. LANE protokol definuje rozhraní pro protokoly vyšší vrstvy – síťové vrstvy. Pakety těchto síťových protokolů jsou pak dále posílány přes ATM síť zapouzdřeny v jednom ze dvou možných LANE MAC rámcích. LANE protokol způsobuje, že ATM síť vypadá jako síť typu Token Ring nebo Ethernet.

LANE základními prvky jsou LES – server, poskytující mapování mezi MAC a ATM adresami, a LEC – klientské rozhraní, které musí obsahovat každý člen ELAN. LES podle požadavků jednotlivých LEC poskytuje překlad mezi MAC a ATM adresami, takže LEC mohou komunikovat mezi sebou přímo po ATM síti.

Standard LANE umožňuje vytvoření více překrývajících se virtuálních sítí, tak klient LEC může být členem více ELAN. Tak mohou uzly z různých ELAN přistupovat ke společným síťovým zdrojům bez nutnosti průchodu přes směrovač.

Členy ELAN mohou být jen uzly ATM, zatímco členy VLAN mohou být jak uzly ATM, tak i uzly na standardních segmentech. Na členy ELAN tak můžeme pohlížet jako na podmnožinu VLAN.

V jedné ATM síti může být vytvořeno více ELAN. To vyvolává potřebu jejich propojování - jak mezi sebou, tak se stávajícími LAN a WAN sítěmi. Propojení uskutečnit lze jedině pomocí směrovače, na kterém je implementován vícenásobný LEC, každý pro jednu ELAN. Směrování datových paketů pak probíhá stejným způsobem jako u standardních sítí. Jednotlivým ELAN jsou totiž přiřazeny různá identifikační čísla sítě. Podle adresy cíle LEC pozná, že paket není ve stejné ELAN a pošle jej na svůj defaultní směrovač. Tento směrovač po obdržení paketu určí ze svých směrovacích tabulek cílovou ELAN a přesměruje do ní paket. [3]

2.1.2 MPOA

V sítích MPOA na rozdíl od LAN Emulace je použit úplně jiný přístup ke směrování paketů. Využívá se zde tzv. „virtuální směrovač“, který emuluje funkci tradiční sítě se směrovači a identifikuje datové toky, které mapuje přímo do virtuálních spojení přes ATM síť. Pakety tak již nemusí být na své cestě zpracovávány na každém směrovači a vedle podstatného zvýšení výkonnosti dochází ke zmenšení transportního zpoždění.

Základní principy MPOA standardu vychází z rozdělení funkcí tradičního multiprotokolového směrovače, tedy oddělení výpočetního zpracování směrování od vlastního fyzického směrování paketů mezi jednotlivými podsítěmi. Výpočetní zpracování (správa adres, topologické informace atd.) je prováděno MPOA serverem (MPS), zatímco vlastní fyzické směrování paketů provádí MPOA klient (MPC).

MPS funkce je implementována do ATM přepínače nebo MPS pracuje jako samostatný směrovací server s ATM připojením. Funkce MPC je zabudována do okrajových ATM

přepínačů a do připojených ATM stanic. Tím jsou od sebe fyzicky odděleny zařízení, která provádí směrovací výpočty a zařízení, která provádí vlastní fyzické přenosy.

Výhoda použití MPOA technologie spočívá v dynamickém vytváření virtuálních obvodů mezi koncovými uzly a významného snížení provozních nákladů. Nedostatkem MPOA sítě z pohledu VPN je její výhradní omezení na ATM jako přenosové technologie na spojové vrstvě. [3], [4]

2.1.3 MPLS

MPLS je považováno za hybridní technologii, která integruje dva základní přístupy k tvorbě VPN a to:

- Použití směrování na síťové vrstvě a přepínání paket po paketu.
- Virtuální obvody na spojové vrstvě a přepínání podle datových toků.

MPLS integruje směrování na síťové vrstvě s tzv. přepínáním podle návěští. Toto přepínání podle návěstí umožňuje plynulý přenos dat mezi koncovými uzly. Pro identifikaci dat, která se mají přenést, se používají speciální návěští.

MPLS může pracovat s libovolným médiem, po kterém se dají přenášet síťové pakety mezi uzly, definovanými svými síťovými adresami. MPLS poskytuje jen základní mechanismy, které zahrnují:

- Přidělování krátkých návěští pevné délky specifikovaným datovým tokům.
- Pomocí identifikace těchto návěští zjednodušení přenosu paketů.
- Možnost přímého využití přenosových mechanismů, které poskytují spojově orientované technologie jako ATM a Frame Relay.
- Procedury a protokoly pro přidělování návěští jednotlivým datovým tokům a distribuci těchto informací mezi jednotlivými zúčastněnými uzly.

Vytvořená VPN technologií MPLS má tři základní složky:

- Řízenou distribuci směrovacích informací jako způsob vytvoření VPN a řízení vzájemného propojení mezi nimi.
- Použití identifikátorů pro jednotlivé virtuální sítě (VPN ID) a obzvláště jejich provázanost s IP adresami k jejich případné změně na unikátní adresy.
- Použití přepínání podle návěstí na směrování paketů.

MPLS architektura je založena na aplikaci návěští na paket, vstupující do sítě MPLS. Tím je pro daný paket určena sekvence přepínačů, kterými musí projít na své cestě mezi okrajovými uzly sítě, a také výstupní směrovač. Rozšířením této architektury z hlediska VPN je globální identifikátor CUG. Tento globální identifikátor může být přiřazen paketu při vstupu do MPLS sítě a pak použit jako index ve směrovací tabulce pro VPN k určení počátečního návěští. CUG je na výstupu ze sítě MPLS dále znovu použit jako index v globální tabulce VPN k určení výstupního směrovače. [3], [4]

2.2 VPN na síťové vrstvě

Informace v síťové vrstvě slouží pro směrování protokolu IP a práce se směrovacími informacemi je základem pro vytvoření VPN na této vrstvě.

2.2.1 Filtrování směrových informací

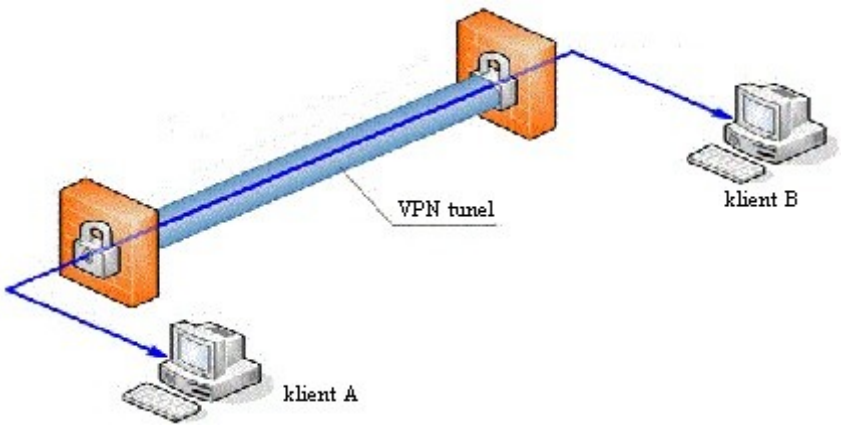
Vytváření VPN je založeno na poměrně jednoduchém principu o omezení poskytování směrovacích informací. Informace o dosažitelnosti vybraných sítí, které jsou v jedné VPN, tak nejsou poskytována okolním sítím, které do dané VPN nenáleží. To samé platí i v obráceném směru.

Takový způsob vytváření VPN má ale své nedostatky. Největším z nich je obtížné zabránění přístupu z jednotlivých částí VPN na nejbližší implicitní směrovač, sloužící k externí komunikaci se sítěmi mimo danou vlastní VPN. Implicitní směrovač dané sítě pro vnější komunikaci s ostatními částmi dané VPN musí být přístupný, proto na tomto směrovači je nutná řádná implementace komunikačních filtrů k zablokování veškeré komunikace, směřující mimo danou VPN. [3]

2.2.2 Tunelování

Tunelování se vztahuje na zapouzdření a směrování, stejně jako na odstranění zapouzdření. Tunely nevyžadují, aby vložená data byla nutně zašifrována, i když tomu tak většinou bývá. Tunel je logickou trasou, ale jeví se jako bodové (point-to-point) spojení v síti. Zařízení, která komunikují uvnitř tunelu, ať už se jedná o přepínače, brány, směrovače nebo proxy servery, jsou zdrojovému i cílovému systému neviditelná.

Pokud se zašifruje celý paket (data i záhlaví) a takto zašifrovaný paket je obalen novým záhlavím a odeslán na druhý konec VPN spojení, jedná se o VPN tunel. Tunelování je tedy proces, při čemž se celý paket ocitá zapouzdřený uvnitř jiného paketu. Zašifrovaný paket se nazývá „pasažérský paket“ a jeho obalující paket „přepravní paket“ není zašifrován, protože obsahuje informace o adresaci. Koncové body tunelu se nazývají „tunelová rozhraní“, přičemž místní konec tunelu je pro nás zdrojový a vzdálený konec je cílem komunikace. [4], [5]



Obrázek 4 – VPN tunelování [11]

Tunely se všeobecně považují za bezpečnější způsob přenosu dat z důvodu ukrytí více informací. Vyžadují však ke svému fungování více zdrojů a režijní náklady navíc.

Jako obálka pro zapouzdření paketů mohou sloužit protokoly GRE, IPsec, PPTP a L2TP. Protokol IPsec je jednou z metod používaných pro zašifrování VPN provozu. Pokud se pro tunelování použije jeden z protokolů GRE, PPTP nebo L2TP, tzv. nosné protokoly, a jejich data mezi koncovými body spojení pak ještě zašifruje IPsec, říká se tomuto mechanismu IPsec transport.

2.2.3 GRE

Jedná se čistě o směrovací protokol, sám o sobě nedokáže zajistit šifrování paketů. GRE tunely jsou obecně typu bod-bod, tzn., že pro tunel existuje jen jedna zdrojová a také jen jedna cílová adresa. Hraniční směrovač v síti odesílatele uplatní GRE protokol na pasažérský paket. Na koncové straně si pak hraniční směrovač přečte informace z GRE záhlaví, vyjme pasažérský paket a vyšle jej dále ke svému cíli. Tunely GRE jsou často vkládány dovnitř VPN tunelů, které pak poskytují nezbytné kryptografické funkce.

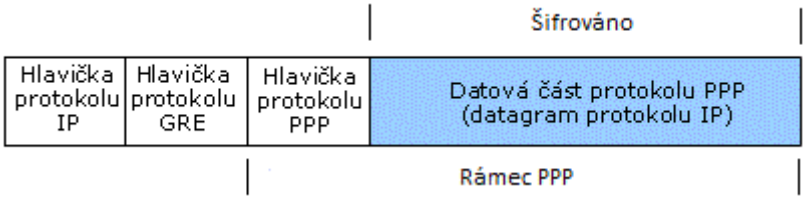
Protokol GRE podporuje jak fyzické IP adresy, tak platné logické nebo virtuální IP adresy. Když se tedy například vytvoří VPN spojení mezi dvěma sítěmi LAN, může k založení GRE tunelu být použita buď adresa fyzického rozhraní směrem ke klientovi nebo adresa rozhraní zpětné smyčky (loopback) směrovače. [5]

2.2.4 PPTP

PPTP pro svou činnost využívá protokol PPP, který zajišťuje vzdálený přístup mezi dvěma body. PPTP tunel lze nastavit i tak, že přístup je umožněn celému vzdálenému síťovému segmentu.

V rámci PPTP existuje možnost využívání šifrování o síle 40 nebo 128 bitů. Vzdálení klienti protokolu PPTP se autentizují mechanismy CHAP nebo EAP. PPTP spojení umožňuje pouze autentizaci uživatelů, protože v protokolu PPP to ani jinak není možné. Vzdálené počítače tak autentizovat nelze, což představuje jisté omezení.

Při procesu zapouzdření je zašifrovaný paket nejprve obalen do PPP, dále pak do upravené verze GRE protokolu a nakonec předán protokolu IP, který okolo něho vytvoří ještě jednu hlavičku, aby mohl být správně přenesen. Z pohledu směrovače se takový paket jeví jako každý jiný IP paket, přičemž celý rámec PPP představuje v tomto případě data paketu. [5]



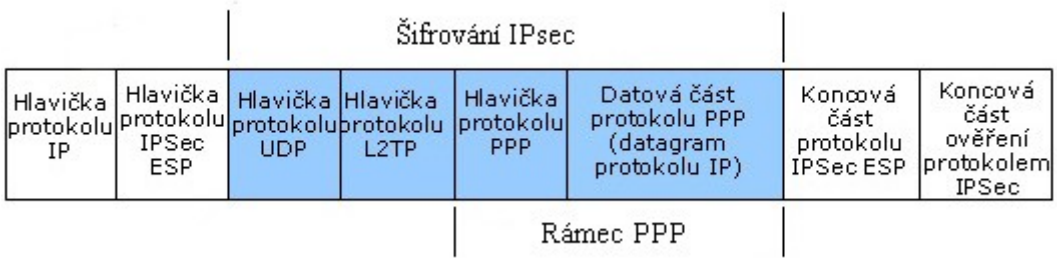
Obrázek 5 – Formát paketu PPTP pro zapouzdření dat [13]

2.2.5 L2TP

Model L2TP vychází ze staršího standardu L2F od společnosti Cisco Systems. L2TP ve verzi 3 umožňuje vzdálená připojení serveru NAS, tunelovaná na bránu nebo koncentrátor. Do L2TP se vkládají zapouzdřené rámce PPP. Tunel může být i rozšířen tak, aby se mohly vzdáleně připojovat celé sítě.

L2TP protokol nemá žádné nástroje na zabezpečení, proto se obvykle kombinuje s IPsecem. Data lze přepravovat přes sítě ATM, Frame Relay, PPP, VLAN nebo PPP nad IP. L2TPv3 vytváří z rámců PPP standardní pakety, které jsou zašifrované protokolem IPsec. Kombinace L2TP/IPsec může využívat nejen autentizační metody jako PPP, ale i autentizaci počítačů prostřednictvím certifikátů nebo sdíleného klíče.

Princip vytvoření paketu L2TP probíhá tak, že se k pasažérskému paketu připojí nejdříve hlavička L2TP a UDP spolu se zakončením Ipsec ESP. Modul IPsec data zašifruje a přidá k nosnému paketu ještě hlavičku IPsec ESP a autentizací zakončení IPsec. Nakonec obdrží hlavičku IP, aby mohl být vyslán do VPN tunelu. [4], [5]



Obrázek 6 – Formát paketu L2TP pro zapouzdření dat [13]

2.2.6 IPsec

IPsec je komplexní sada protokolů podporována jak IPv4, tak i IPv6 a nabízí tunelování, šifrování a autentizaci. IPsec nejprve zařídí to, že se obě strany navzájem autentizují a následně šifruje veškerou komunikaci pomocí domluveného algoritmu. Tunel mezi dvěma servery nebo mezi serverem a uživatelem pak zabezpečuje provoz jakéhokoli typu.

IPsec může pracovat ve dvou módech:

- Tunelovací mód. - Šifruje celý paket a doplňuje novou hlavičku. Tento mód lze použít pro IPsec proxy, klient vysílá data, směrovač je šifruje a posílá dál, tudíž se nedá z komunikace odhalit adresa klienta.
- Transportní mód. - Šifruje pouze data, IP hlavička se ponechá a doplní se pouze IPsec hlavička.

IPsec využívá dva hlavní protokoly a to:

- AH - Zajišťuje integritu a autentizaci zdroje dat ve formě autentizačního záhlaví vloženého za původní IP záhlaví. Používá hashovací funkce MD5 či SHA1 a

společný klíč, který si na začátku domluví. V hlavičce obsahuje pořadové číslo paketu.

- ESP – Zajišťuje utajení zprávy šifrováním datového obsahu i záhlaví, a kromě toho poskytuje obdobné autentizační služby jako AH. Standardně šifruje pomocí DES, ale protože je tento algoritmus již zastaralý, využívá se častěji jeho vylepšená varianta 3DES.

Aby bylo možné zapouzdření a vybalení paketu s AH nebo ESP je potřeba tajný klíč, algoritmus a další údaje. Tyto informace jsou uloženy v bezpečnostní asociaci (SA). SA zavádějí vztah důvěry mezi dvěma partnerskými zařízeními a koncové body sítě VPN se pomocí nich dohodnou na přenosových pravidlech. SA si vzájemně potvrzují zásady s potenciálním partnerem, jaké parametry bude navazované spojení mít.

VPN musí mít tajné klíče a šifrovací algoritmy sdílené mezi všemi účastníky komunikace. Bezpečnou výměnu mezi nimi obstarává protokol IKE, který představuje mechanizmus pro dojednání bezpečnostních služeb mezi koncovými prvky IPsec, autentizování jejich relací a šifrovacích klíčů. Také se stará o výměnu klíčů, která vychází z algoritmu Diffie-Hellman. [3], [4], [9]

2.3 VPN na transportní a aplikační vrstvě

Bezpečnost na vyšších vrstvách TCP/IP modelu lze realizovat rozšířením firemním řešením SSL, na němž je postaveno otevřené řešení TLS.

2.3.1 SSL/TLS

Protokol SSL verze 3 zakládá bezpečná spojení na aplikační vrstvě pro vzdálený přístup uživatelů. Jeho novější verzí je protokol TLS, který byl z SSLv3 odvozen a je s ním zpětně kompatibilní. Oba protokoly jsou proto v mnoha ohledech velmi podobné a často se používají ve spojení SSL/TLS.

Jelikož SSL/TLS je součástí všech moderních webových prohlížečů, jsou VPN spojení založená na webovém přístupu velmi populární. Před vlastním přenosem si obě strany ověří totožnost pomocí asymetrické kryptografie (za pomoci veřejných a soukromých klíčů). Samotná komunikace potom probíhá pomocí symetricky šifrovaných zpráv (např. 3DES, RC4). Integrita přenášených dat pak bývá zajištěna pomocí hashovacích funkcí, podobně jako u protokolu AH. (např. SHA-1, MD5).

Úroveň bezpečnosti SSL/TLS není vysoká jako v případě protokolů IPsec, L2TP či dokonce PPTP. SSL/TLS šifruje pouze data přenášená samotnou aplikací, která SSL/TLS implementuje. Zabezpečení se dá však posílit speciálním klientským softwarem, který podporuje tyto protokoly. [4], [6]

3 Konfigurace Cisco VPN

Cisco VPN nabízí několik druhů vytvoření VPN, tato část se zabývá popisem konfigurace vzdáleného přístupu pomocí Clientless SSL VPN a SSL VPN klient.

Clientless SSL VPN je mód, který nabízí omezený bezpečný přístup na vnitřní zdroje uvnitř firemních sítí. Uživatel přistupuje pomocí internetového prohlížeče na webovou stránku tzv. portál. Přístup je přes šifrovaný protokol HTTPS standardně na portu 443. Nejprve je nutné provést autentizaci uživatele a pak je přístupný portál s nastavenými možnostmi. Přenos dat mezi vzdálenými uživateli a vnitřní sítí je zajištěn tím, že cestuje přes SSL tunel.

SSL VPN klient je mód, který poskytuje uživateli nejvíce možností. Nabízí rozsáhlejší podporu aplikací přes dynamicky stažitelného klienta Cisco AnyConnect VPN. Poté, co klient VPN je ověřen, mohou vzdálení uživatelé přistupovat do vnitřních sítí nebo aplikací, jako kdyby byli na místě. Přenos dat mezi vzdálenými uživateli a vnitřní sítí je zajištěn tím, že je šifrován. [9]

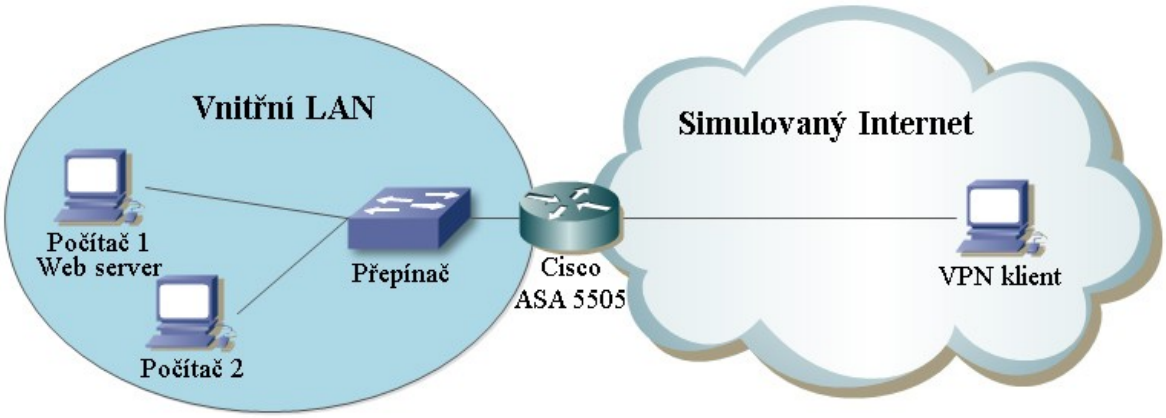
3.1 Návrh testovacího scénáře

Nejprve je popsána konfigurace Clientless SSL VPN, kde je vyžadována autentizace uživatelů kombinací certifikátu a uživatelského jména a hesla. Portálová stránka poskytuje seznam URL webových serverů, které může vzdálený uživatel po úspěšné autentizaci ve vnitřní síti prohlížet. Jiné aktivity ve vnitřní síti vzdálenému uživateli nejsou povoleny.

Poté bude mód Clientless SSL VPN rozšířen o možnost stáhnutí Cisco AnyConnect VPN klienta, dále jen nazýván jako AnyConnect klient a nakonfigurován druhý mód SSL VPN klient. Zde bude nakonec vzdálený uživatel ACL listy omezen pouze také na přístup k web serveru, ale s tím rozdílem, že k němu bude moci přistupovat jakoby byl v jedné lokální síti.

Navrhovaná konfigurace obsahuje dva počítače ve vnitřní síti a bezpečnostní zařízení Cisco Adaptive Security Appliance 5505 (ASA). Na jednom vnitřním počítači je nainstalovaná služba web server. Další počítač slouží k simulaci vzdáleného uživatele. VPN tunel se tvoří mezi zařízením ASA, které slouží jako VPN brána a VPN klientem.

Topologii zapojení znázorňuje následující obrázek.



Obrázek 7 – Schéma testovací topologie

Použité adresní rozsahy a IP adresaci zobrazují následující dvě tabulky.

Tabulka 1 – Adresní rozsahy

Adresní rozsah	Použití
192.168.1.0/24	Vnitřní LAN
192.168.0.0/24	Simulovaný Internet
10.10.10.0/24	VPN tunel

Tabulka 2 – IP adresy zařízení

Zařízení	Rozhraní	I P adresa	Popis
ASA 5505	Fa0/1 (Vlan 1)	192.168.1.1	Vnitřní rozhraní
ASA 5505	Fa0/0 (Vlan 2)	192.168.0.0	Vnější rozhraní
Počítač 1	Fa0/0	192.168.1.5	
Počítač 2	Fa0/0	192.168.1.6	
VPN klient	Fa0/0	192.168.0.5	

3.2 Realizace konfigurace scénáře

Před realizací zařízení ASA nejprve restartujeme, abychom získali počáteční defaultní nastavení od výrobce. Samotná realizace obsahuje všechny příkazy zadávané do příkazového řádku zařízení ASA. Kompletní konfiguraci spolu s konfigurací klientského softwaru lze také shlédnout na přiloženém CD.

3.2.1 Konfigurace rozhraní zařízení ASA

ASA nedovoluje konfigurovat IP přímo na jednotlivá fyzická rozhraní, ale musí se konfigurovat pomocí VLAN rozhraní. Po defaultním nastavení ASA je automaticky nastavena Vlan 1 s nejvyšší bezpečnostní hodnotou 100 a Vlan 2 s nejnižší bezpečnostní hodnotou 0. Pouze zařízení na rozhraní s vyšší bezpečnostní úrovní může navázat spojení se zařízením na nižší bezpečnostní úrovni, ne naopak. V uváděném případě

to znamená, že z outside rozhraní tak nelze navázat spojení s nikým za inside rozhraním. Nutné je tedy nastavit IP adresy VLAN rozhraním a ty pak přiřadit fyzickým rozhraním, konfigurační příkazy jsou:

```
ciscoasa(config)# interface Vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config)# interface Vlan 2
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 192.168.0.1 255.255.255.0

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access Vlan 2
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport access Vlan 1
```

3.2.2 Konfigurace směrování

Zde pro testovanou topologii stačí pouze jeden příkaz a to nastavit defaultní směrování pro vnější rozhraní. Příkaz je následující:

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.0.1 1
```

3.2.3 Konfigurace certifikátů a šifrování

Nejdříve je nutné vyrobit certifikační autoritu, která se stará o vydávání certifikátů a poté samotný certifikát, který bude sloužit k ověření přístupu. Pak se certifikát spolu s vybraným šifrováním uvede do platnosti. Příkazy jsou následující:

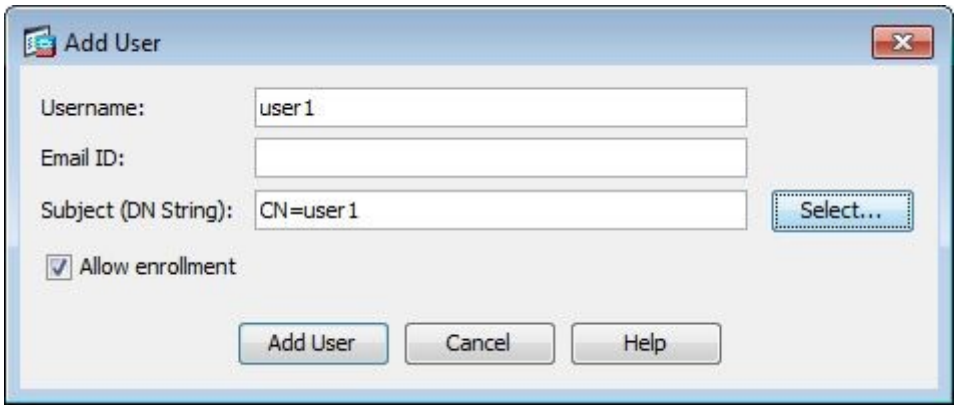
```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp from-address admin@ciscoasa.mynetwork.net
ciscoasa(config-ca-server)# no shutdown passphrase 12345678

ciscoasa(config)# crypto ca trustpoint IdentityCertifikat
ciscoasa(config-ca-trustpoint)# id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)# no fqdn
ciscoasa(config-ca-trustpoint)# subject-name CN=ciscoasa
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# crypto ca enroll IdentityCertifikat noconfirm

ciscoasa(config)# ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ciscoasa(config)# ssl trust-point IdentityCertifikat inside
```

Do databáze certifikační autority na zařízení ASA je ještě potřeba přidat testovacího uživatele. V této databázi je vidět zdali daný uživatel vlastní certifikát k přístupu nebo ne, lze mu i přístup zablokovat. Protože uživatele nelze přidat do certifikační databáze přes

příkazovou řádku, musí se přidat přes ASDM, jenž je konfigurační grafické rozhraní zařízení ASA. Přidání uživatele do certifikační databáze a samotná databáze, kde je znázorněno, že vyrobený uživatel certifikát ještě nevlastní je vidět na přiložených obrázcích.



Obrázek 8 – Přidání uživatele do certifikační databáze

Obrázek 9 – Certifikační databáze

3.2.4 Konfigurace přístupové politiky

V Clientless SSL VPN módu je potřeba nastavit k čemu bude mít vzdálený uživatel po autentizaci k portálu přístup. V tomto případě je to služba web server s IP adresou 192.168.1.5 umístěný na počítači 1. Nejprve se vytvoří tzv. Bookmark List, který danou službu zpřístupní. Bookmark list opět nelze vytvořit přes příkazovou řádku, tak je tvorba v ASDM uvedena na obrázku.

Obrázek 10 – Tvorba Bookmark List

Poté se vytvoří bezpečnostní politika s názvem MyPolicy, kde se povolí tunelový protokol pro Clientless SSL VPN mód a přiřadí se vyrobený Bookmark List, v tomto případě MyBookmark. Konfigurační příkazy jsou:

```
ciscoasa(config)# group-policy MyPolicy internal
ciscoasa(config)# group-policy MyPolicy attributes
ciscoasa(config-group-policy)# vpn-tunnel-protocol webvpn
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# url-list value MyBookmark
```

3.2.5 Tvorba uživatele

Tvorba uživatele s přihlašovacím jménem a heslem. Použití uživatelského účtu je omezeno pouze pro vzdálený přístup. Příkazy jsou:

```
ciscoasa(config)# username user1 password 123456
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type remote-access
```

3.2.6 Konfigurace VPN profilu

Nakonec je potřeba vytvořit VPN profil, zde se jmenuje ClientlessAndAnyConnect. Vytvořený profil je nastaven na vzdálený přístup a autentizaci kombinací certifikátu a uživatelského jména a hesla. Také je mu přidělena bezpečnostní politika MyPolicy a poté už jen stačí povolit vnější rozhraní pro Clientless SSL VPN mód. Vše provedou následující příkazy:

```
ciscoasa(config)# tunnel-group ClientlessAndAnyConnect type remote-access
ciscoasa(config)# tunnel-group ClientlessAndAnyConnect general-attributes
ciscoasa(config-tunnel-general)# default-group-policy MyPolicy
ciscoasa(config-tunnel-general)# tunnel-group ClientlessAndAnyConnect webvpn-
attributes
ciscoasa(config-tunnel-webvpn)# group-alias ClientlessAndAnyConnect enable
ciscoasa(config-tunnel-webvpn)# authentication certificate aaa

ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable outside
ciscoasa(config-webvpn)# tunnel-group-list enable
```

Přesto že zde náš vytvořený VPN profil obsahuje AnyConnect v názvu mohlo by to být pro někoho matoucí, zatím ale podporuje jen Clientless SSL VPN mód. O mód SSL VPN klient s AnyConnect klientem bude rozšířen až později.

3.2.7 Přístup vzdáleného uživatele na portál

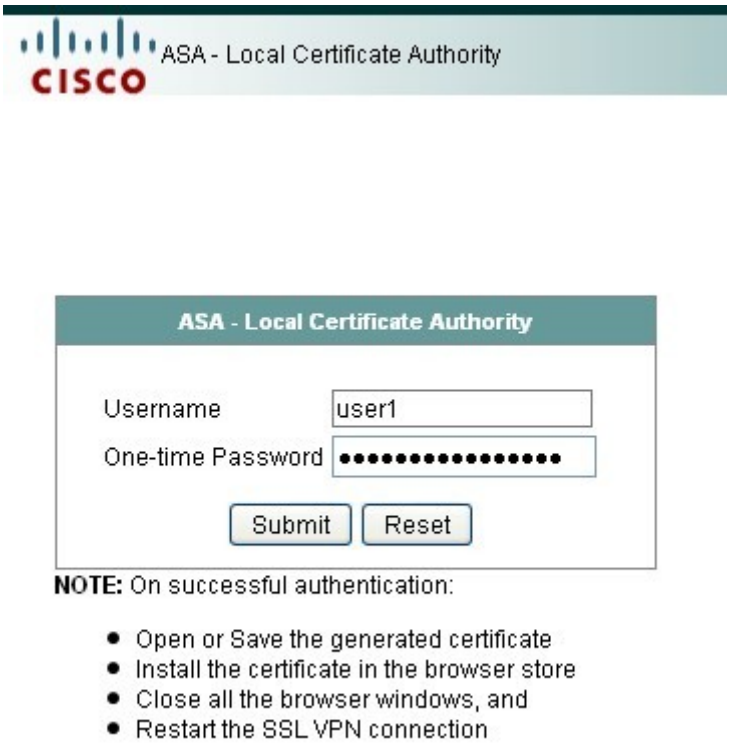
Vzdálený uživatel po zadání IP adresy vnějšího rozhraní, tedy 192.168.0.1 do webového prohlížeče se dostane na přihlašovací obrazovku, kde je vyzván k ověření. Ověření je samozřejmě neúspěšné, protože uživatel stále nevlastní certifikát a je vyzván k jeho získání. To lze vidět na následujících obrázcích.

Obrázek 11 – Přihlášení do portálu

Obrázek 12 – Výzva k získání nového certifikátu

Po kliknutí na získání certifikátu se zobrazí obrazovka od certifikační autority, kde pro získání certifikátu je nutné zadat tzv. jednorázové heslo. Certifikační autorita na ASA

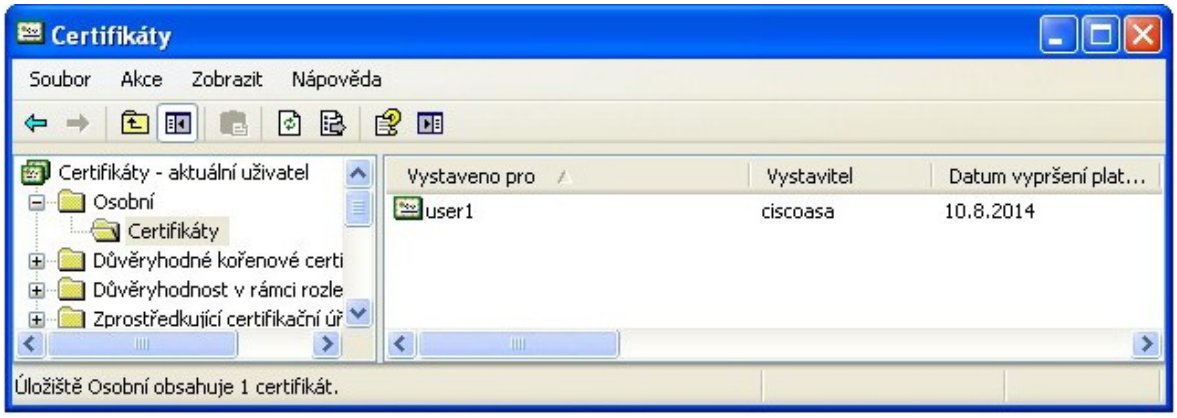
umožňuje jednorázová hesla automaticky zasílat nově registrovaným uživatelům na e-mail. Jednorázové heslo pro daného uživatele také lze zobrazit v ASDM. Ukázky jsou vidět na obrázcích.



Obrázek 13 – Vložení jednorázového hesla

Obrázek 14 – Zobrazení jednorázového hesla

Po zadání jednorázového hesla se do uživatelského počítače importuje jeho přístupový certifikát a v databázi certifikační autority se zobrazí, že daný uživatel už vlastní svůj certifikát. Vše je zobrazeno na následujících obrázcích.

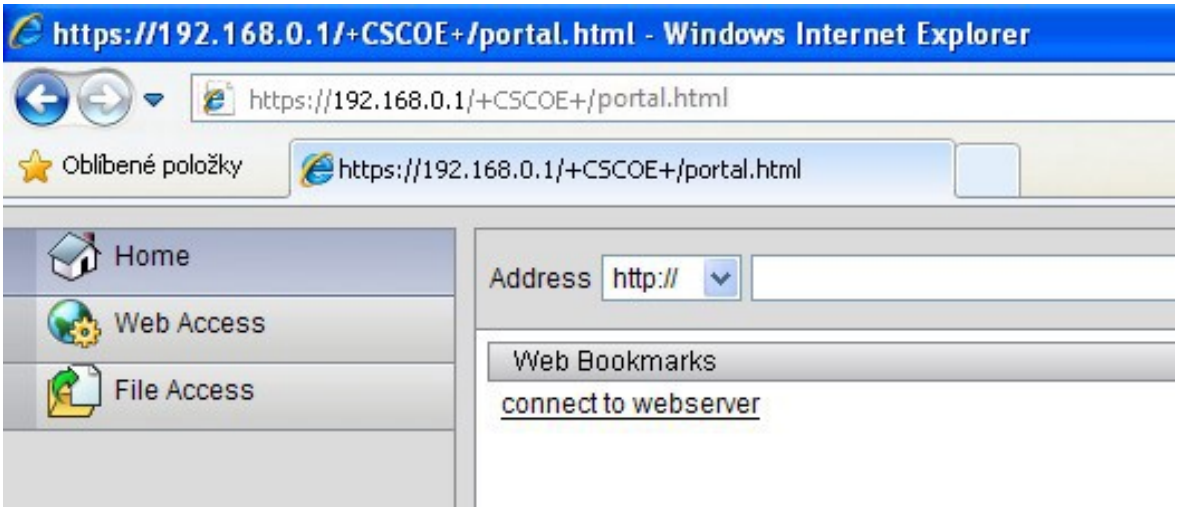


Obrázek 15 – Naimportovaný certifikát na straně klienta

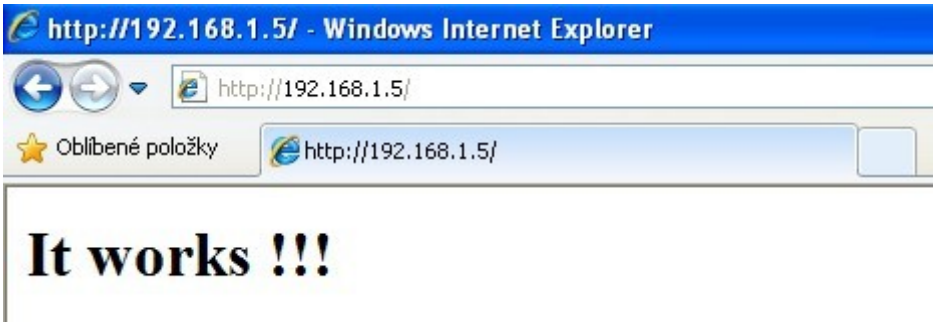
Obrázek 16 – Certifikační databáze s potvrzeným certifikátem

3.2.8 Ověření funkčnosti Clientless SSL VPN módu

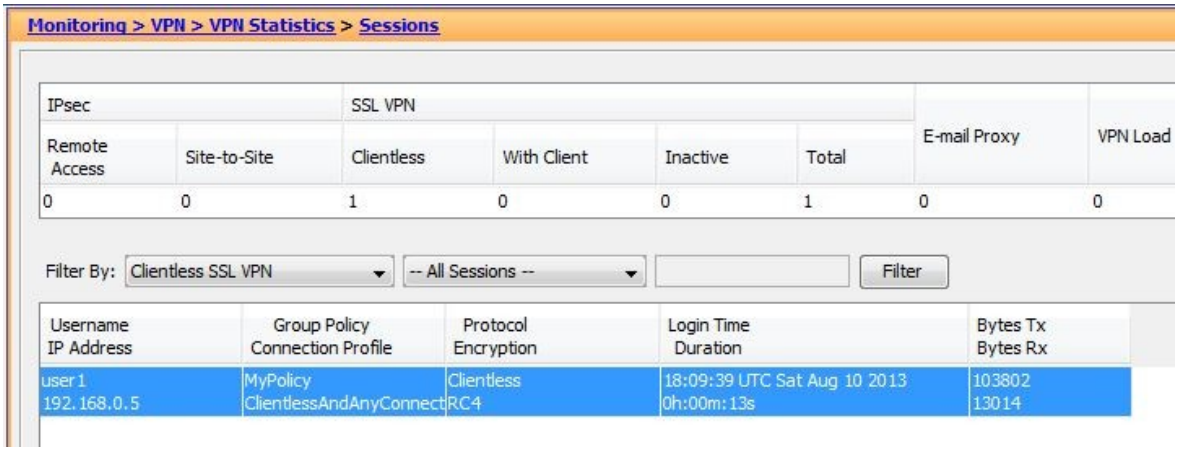
Funkčnost lze ověřit několika způsoby. Prvním znakem je úspěšná autentizace vzdáleného uživatele kombinací certifikátu a uživatelského jména a hesla na portál. Další znak funkčnosti je úspěšné připojení přes vytvořený Bookmark List na web server. Nejprůkaznější ověření funkčnosti poskytuje ASDM, kde je k dispozici použitá politika, šifrování a počet přenesených bajtů přes VPN spojení.



Obrázek 17 – Úspěšná autentizace na portál



Obrázek 18 – Připojení na Web server přes portál



Obrázek 19 – Clientless spojení, použitá politika a šifrování, počet přenesených bajtů

3.2.9 Rozšíření konfigurace na SSL VPN Client mód

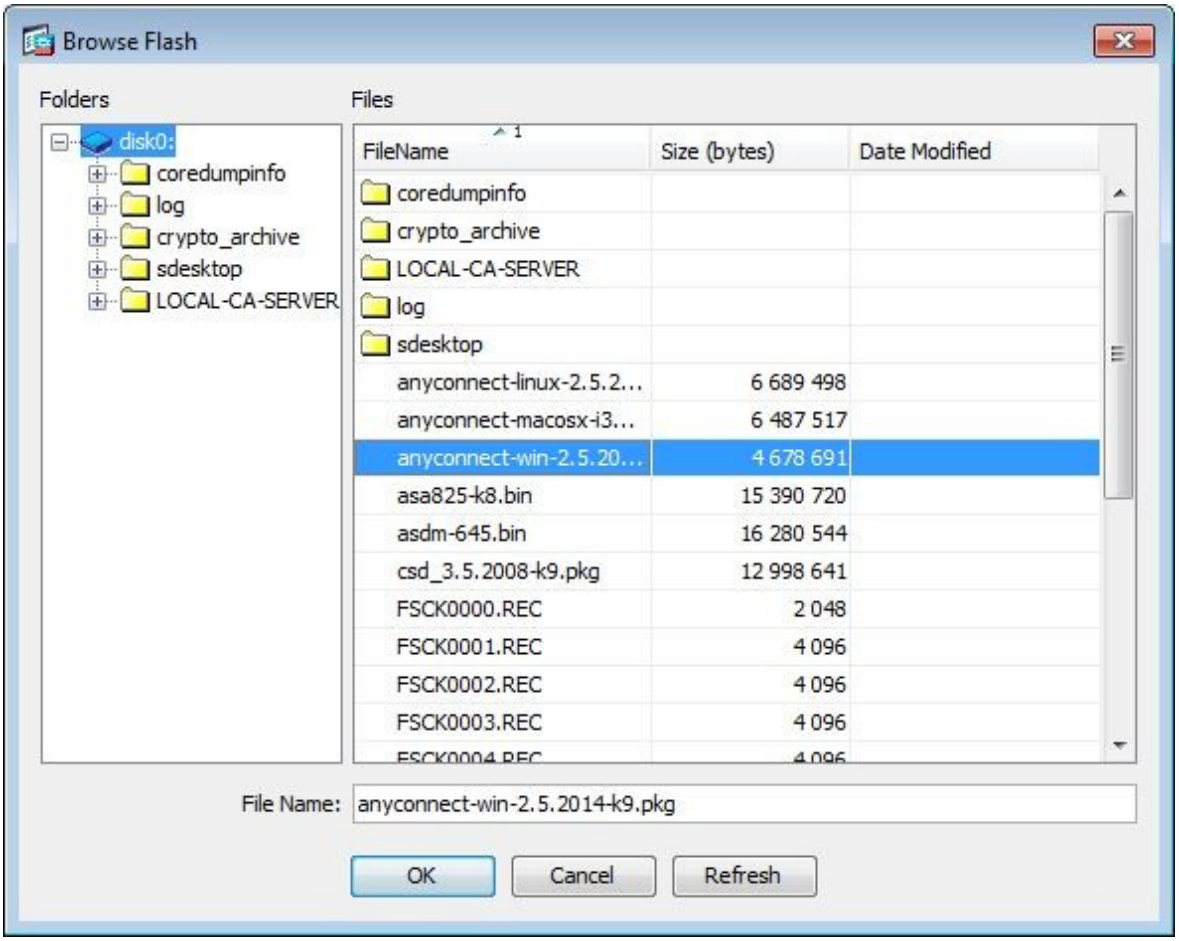
Pro rozšíření na SSL VPN klient mód je využit již nakonfigurovaný VPN profil ClientlessAndAnyConnect. Tento profil je potřeba rozšířit o rozsah adres tzv. IP pool. Z tohoto rozsahu se přidělují jednotlivým uživatelům připojeným přes AnyConnect klienta nové IP adresy. Příkazy na tvorbu a přiřazení rozsahu adres jsou:

```
ciscoasa(config)# ip local pool IpPoolVPN 10.10.10.1-10.10.10.254 mask 255.255.255.0
ciscoasa(config)# tunnel-group ClientlessAndAnyConnect general-attributes
ciscoasa(config-tunnel-general)# address-pool  IpPoolVPN
```

Bezpečnostní politika MyPolicy je rozšířena o povolení tunelového protokolu pro SSL VPN klient mód následujícími příkazy:

```
ciscoasa(config)# group-policy MyPolicy attributes
ciscoasa(config-group-policy)# vpn-tunnel-protocol webvpn svc
```

K VPN profilu ClientlessAndAnyConnect je připojen soubor image anyconnect-win-2.5.2014-k9.pkg z flash paměti na zařízení ASA. Připojení image souboru s AnyConnect klientem umožní, že bude dostupný ke stažení z portálu. Připojení image je nutno udělat přes ASDM, jak lze vidět na obrázku.



Obrázek 20 – Připojení image AnyConnect klient

Nastavení výjimky překlad adres z vnitřní sítě do adresního rozsahu určeného pro VPN klienty se provede následovně:

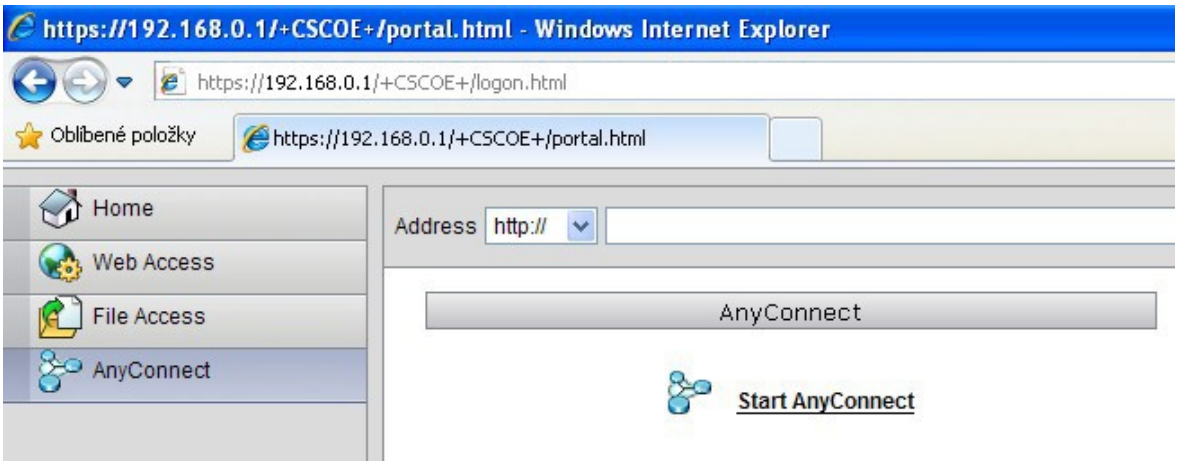
```
ciscoasa(config)# access-list inside_nat0_outbound line 1 extended permit ip 192.168.1.0
255.255.255.0 10.10.10.0 255.255.255.0
ciscoasa(config)# nat (inside) 0 access-list inside_nat0_outbound  tcp 0 0 udp 0
```

Tvorba vlastního přístupového listu MyACL, který dovoluje přístup pouze na IP adresu 192.168.1.5, tedy na počítač 1, kde je služba web server. Přístup kamkoliv jinam do vnitřní sítě je zakázán, tedy počítač 2 je nedostupný. Do politiky MyPolicy je přiřazen přístupový list MyACL. Ten tak vstoupil v platnost pro uživatele VPN profilu ClientlessAndAnyConnect.

```
ciscoasa(config)# access-list MyACL line 1 extended permit ip 10.10.10.0 255.255.255.0
host 192.168.1.5
ciscoasa(config)# access-list MyACL line 2 extended deny ip any any
ciscoasa(config)# group-policy MyPolicy attributes
ciscoasa(config-group-policy)# vpn-filter value MyACL
```

3.2.10 Přístup přes AnyConnect Client

Po uživatelské autentizaci do portálu je nyní k dispozici možnost instalace AnyConnect klienta. Po úspěšné instalaci AnyConnect klienta do počítače uživatele se uživatel může okamžitě přihlásit, protože certifikát již vlastní. Kdyby certifikát nevlastnil, stačí kliknout na Get Certificate a poté bude vyzván k zadání jednorázového hesla. Případný postup získání certifikátu je již popsán v kapitole 3.2.7.

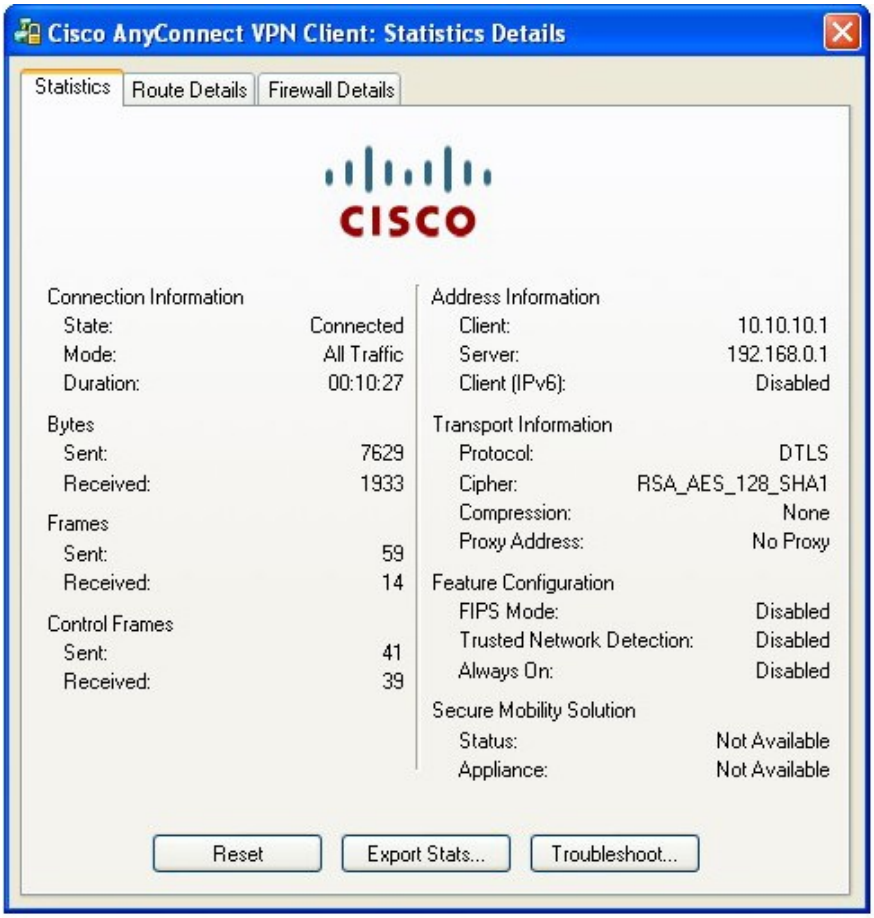


Obrázek 21 – Portál s AnyConnect klientem

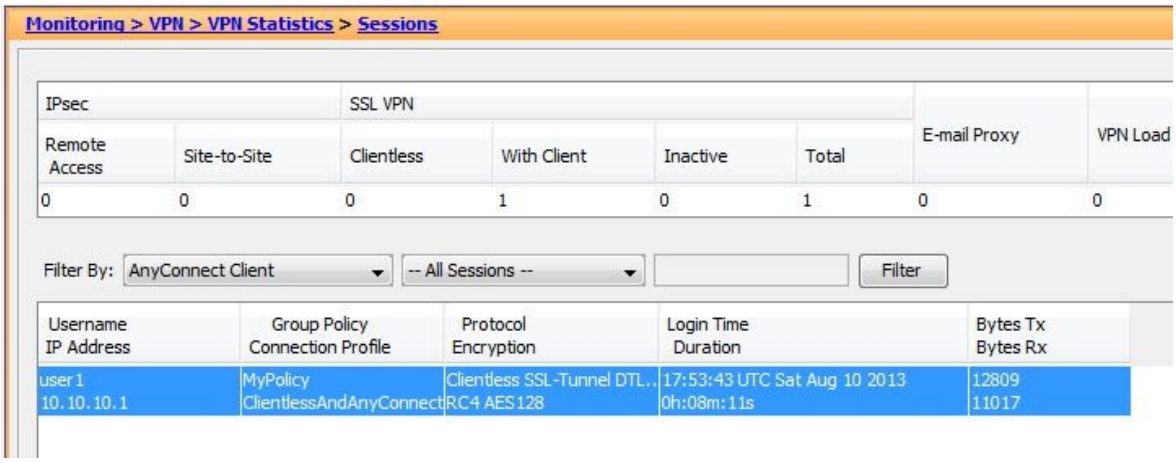
Obrázek 22 – Přihlášení přes AnyConnect klient

3.2.11 Ověření funkčnosti SSL VPN klient módu

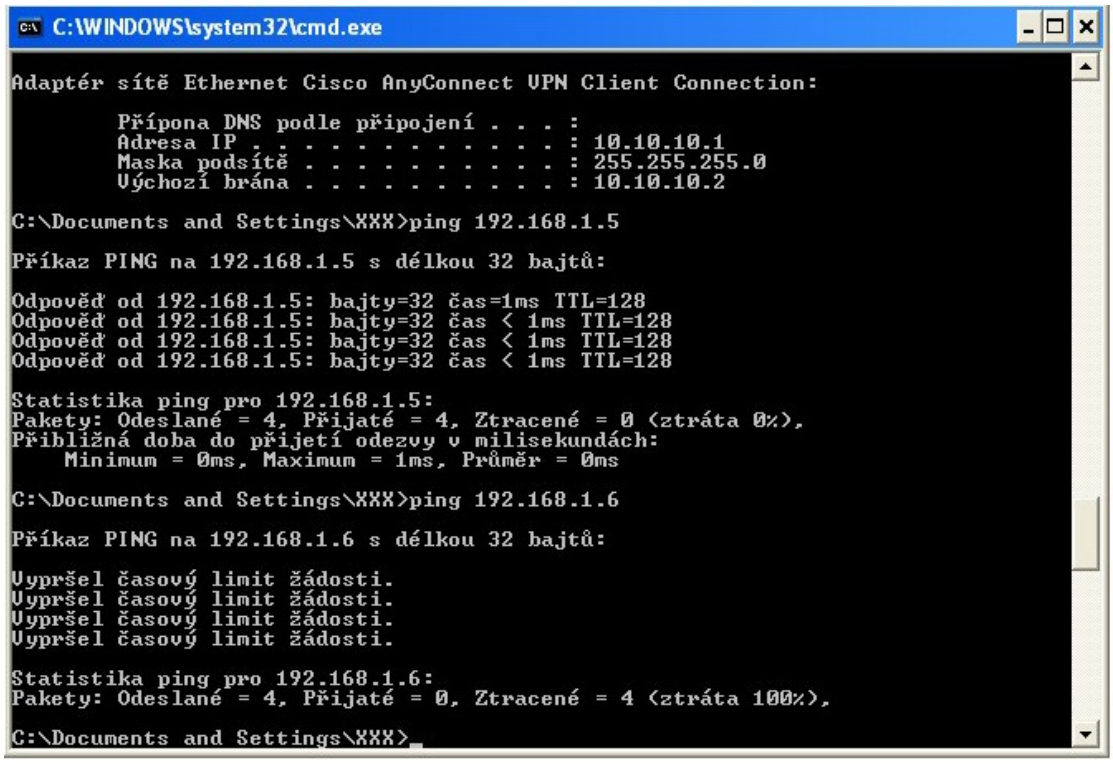
Funkčnost lze opět ověřit několika způsoby. Jako u Clientless SSL VPN módu, tak i tady je prvním znakem úspěšná autentizace vzdáleného uživatele kombinací certifikátu a uživatelského jména a hesla. V AnyConnect klientovi po rozkliknutí záložky Statistic jsou k dispozici údaje o používaném šifrování, přenesených bajtech přes VPN spojení či obdržené IP adresy od ASA 5505. Podobné údaje jsou k dispozici i v ASDM. Přístup k webovému serveru je teď nyní možný i bez využití portálu, což demonstruje příkaz ping na počítač 1 s IP adresou 192.168.1.5. Funkčnost zabránění přístupu kamkoliv jinam ve vnitřní síti poskytuje příkaz ping na počítač 2 s IP adresou 192.168.1.6. Tyto informace lze vyčíst z následujících obrázků.



Obrázek 23 – AnyConnect klient Statistic



Obrázek 24 – Client spojení, použitá politika a šifrování, počet přenesených bajtů



Obrázek 25 – VPN síťové rozhraní, ping na počítač 1 a 2

4 Konfigurace OpenVPN

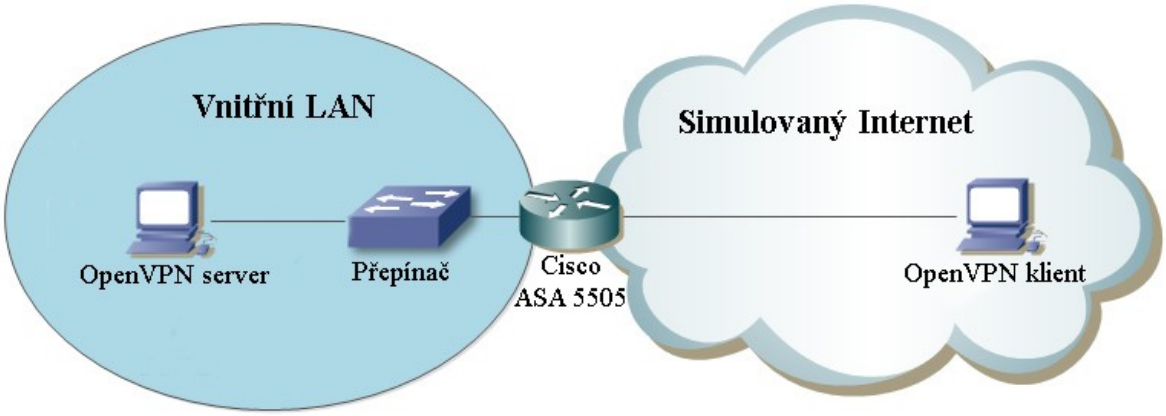
OpenVPN patří do skupiny opensource VPN, standardně používá protokol UDP, ale lze použít i TCP. Veškerá komunikace probíhá na jediném portu, a tak tedy snadno nakonfigurovat firewall, aby propouštěl pouze pakety na tomto portu. Ve chvíli, kdy OpenVPN obdrží nějaký paket, pokusí se pomocí UDP spojení navázat SSL/TLS komunikaci a ověřit druhou stranu. Ověření probíhá pomocí sdíleného klíče nebo certifikáty. Celý OpenVPN program běží v uživatelském režimu a komunikuje prostřednictvím síťového rozhraní TAP nebo TUN. Chování většiny těchto kroků je možno ovlivnit pomocí konfiguračních skriptů. [7]

4.1 Návrh testovacího scénáře

Pro testovací scénář byl vybrán režim client-server. Autentizace uživatele je certifikáty. Veškerá komunikace mezi klientem a serverem probíhá na UDP portu 1194. Komunikace je šifrována a komprimována.

Navrhovaná konfigurace obsahuje jeden počítač ve vnitřní síti, který bude sloužit jako OpenVPN server. Dále bezpečnostní zařízení Cisco Adaptive Security Appliance 5505 (ASA) a počítač k simulaci vzdáleného uživatele.

Topologii zapojení znázorňuje obrázek.



Použité adresní rozsahy a IP adresy na zařízeních:

Tabulka 3 – Adresní rozsahy

Adresní rozsah	Použití
192.168.1.0/24	Vnitřní LAN
192.168.0.0/24	Simulovaný Internet

Tabulka 4 – IP adresy zařízení

Zařízení	Rozhraní	I P adresa	Popis
ASA 5505	Fa0/1 (Vlan 1)	192.168.1.1	Vnitřní rozhraní
ASA 5505	Fa0/0 (Vlan 2)	192.168.0.0	Vnější rozhraní
OpenVPN server	Fa0/0	192.168.1.5	
OpenVPN klient	Fa0/0	192.168.0.5	

4.2 Realizace testovacího scénáře

Před realizací zařízení ASA nejprve restartujeme, abychom získali počáteční defaultní nastavení od výrobce. Samotná realizace obsahuje konfigurační soubor serveru a klienta, a také všechny příkazy zadávané do příkazového řádku zařízení ASA. Na počítačích je nainstalováno OpenVPN 2.3.2 pro operační systém Windows. Kompletní konfiguraci spolu s konfiguračními soubory serveru a klienta lze také shlédnout na přiloženém CD.

4.2.1 Konfigurace zařízení ASA

Po defaultním nastavení ASA je nutné jako bylo u realizace Cisco VPN nastavit IP adresy VLAN rozhraním a ty pak přiřadit fyzickým rozhraním, konfigurační příkazy jsou:

```
ciscoasa(config)# interface Vlan 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config)# interface Vlan 2
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 192.168.0.1 255.255.255.0

ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access Vlan 2
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport access Vlan 1
```

Protože OpenVPN server je umístěn ve vnitřní síti a z outside rozhraní nelze navázat spojení s nikým za inside rozhraním je potřeba povolit na zařízení ASA komunikaci na UDP portu 1194 k cíli s IP adresou 192.168.1.5. Poté vzdálený klient může na tomto portu navázat spojení s OpenVPN serverem. To lze docílit osvobozením překladu adresy 192.168.1.5 do vnější sítě a ACL listem. Příkazy jsou následující:

```
ciscoasa(config)# access-list inside_nat0_outbound line 1 extended permit ip host
192.168.1.5 192.168.0.0 255.255.255.0
ciscoasa(config)# nat (inside) 0 access-list inside_nat0_outbound  tcp 0 0 udp 0

ciscoasa(config)# access-list outside_access_in_1 line 1 extended permit udp 192.168.0.0
255.255.255.0 host 192.168.1.5 eq 1194
ciscoasa(config)# access-group outside_access_in_1 in interface outside
```

4.2.2 Generování certifikátů na OpenVPN serveru

Nejprve se vytvoří certifikační autorita, která se stará o vydávání certifikátů. Pak samotný certifikáty jak pro server, tak pro klienta a Diffie – Hellman. Tvorba v operačním systému ve Windows je přes příkazovou řádku. V příkazové řádce je potřeba přejít do složky EASY-RSA, jenž je součástí instalace OpenVPN. Pokud se při instalaci neměnila cesta uložení, defaultně se nachází zde \ Program Files \ OpenVPN \ EASY-RSA. Poté jsou příkazy následující:

```
C:\Program Files\OpenVPN\EASY-RSA>build-ca

C:\Program Files\OpenVPN\EASY-RSA>build-key-server server

C:\Program Files\OpenVPN\EASY-RSA>build-key client1

C:\Program Files\OpenVPN\EASY-RSA>build-dh
```

Vygenerované certifikáty a klíče je nejlépe přemístit pro pozdější usnadnění práce do složky \ Program Files \ OpenVPN \ config. Jaké soubory patří na OpenVPN server a jaké na OpenVPN klienta poskytuje obrázek.

Filename	Needed By	Purpose	Secret
ca.crt	server + all clients	Root CA certificate	NO
ca.key	key signing machine only	Root CA key	YES
dh{n}.pem	server only	Diffie Hellman parameters	NO
server.crt	server only	Server Certificate	NO
server.key	server only	Server Key	YES
client1.crt	client1 only	Client1 Certificate	NO
client1.key	client1 only	Client1 Key	YES
client2.crt	client2 only	Client2 Certificate	NO
client2.key	client2 only	Client2 Key	YES
client3.crt	client3 only	Client3 Certificate	NO
client3.key	client3 only	Client3 Key	YES

Obrázek 26 – Rozdělení umístění souborů [7]

4.2.3 Konfigurace OpenVPN serveru

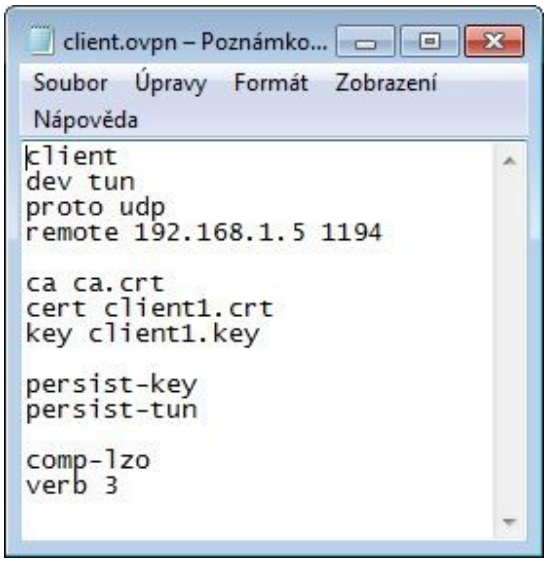
Na straně serveru je potřeba vytvořit konfigurační soubor s názvem server.ovpn a ten umístit do \ Program Files \ OpenVPN \ config. Veškerá nastavení se vytvářejí v tomto konfiguračním souboru.

Obrázek 27 – Konfigurační soubor server.ovpn

Z konfiguračního souboru serveru lze vyčíst informace jako je komunikace na protokolu UDP s portem 1194. Zařízení pro komunikaci je síťový adaptér tun. Direktivy k certifikátům, klíči a souboru s parametry k Diffie-Hellman. Adresní rozsah 10.8.0.0/24 z kterého se budou klientům přidělovat IP adresy. Ping v pravidelných intervalech na klienta pro udržení spojení. Kompresi dat. Zajištění, že v případě automatického restartu tunelu se nebude znovu konfigurovat virtuální síťové rozhraní a číst šifrovací klíč. Ukládání informací o průběhu spojení do logovacího souboru s upřesněním míry „ukecanosti“.

4.2.4 Konfigurace OpenVPN klient

Na straně klienta je potřeba vytvořit konfigurační soubor s názvem klient.ovpn a ten umístit do \ Program Files \ OpenVPN \ config. Veškerá nastavení se vytvářejí v tomto konfiguračním souboru.



Obrázek 28 – Konfigurační soubor client.ovpn

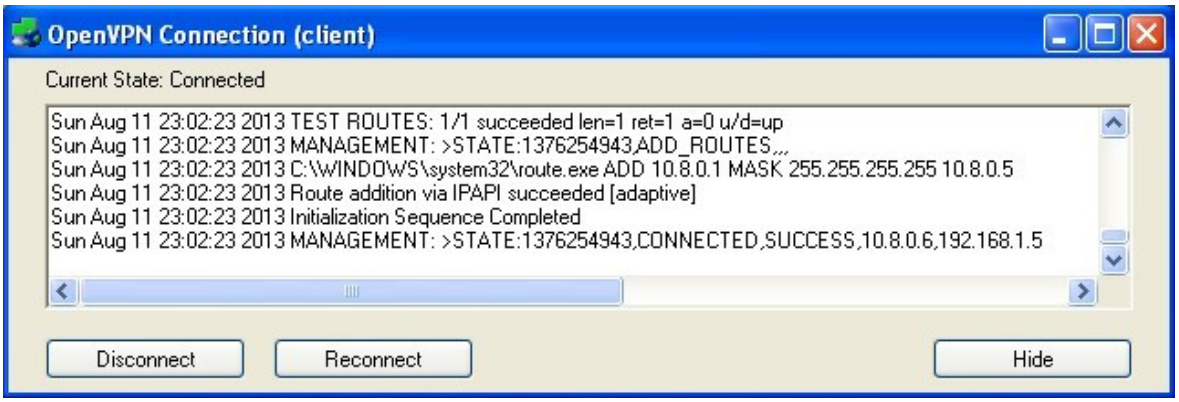
Z konfiguračního souboru klienta lze vyčíst informace, že se jedná o klienta. Zařízení pro komunikaci je síťový adaptér tun. Komunikace probíhá nad portem UDP. Nastavení reálné IP adresy a výchozí port VPN serveru, na který se má klient připojit. V tomto případě to je 192.168.1.5 a výchozí port 1194/UDP. Direktivy k certifikátům a klíči. Kompresi dat a zajištění, že v případě automatického restartu tunelu se nebude znovu konfigurovat virtuální síťové rozhraní a číst šifrovací klíč.

4.2.5 Připojení klienta na server a ověření funkčnosti

OpenVPN server se aktivuje v grafickém rozhraní programu kliknutím na tlačítko Connect. Po úspěšném spuštění OpenVPN server obdrží novou IP adresu 10.0.8.1, jak lze vidět na obrázku.

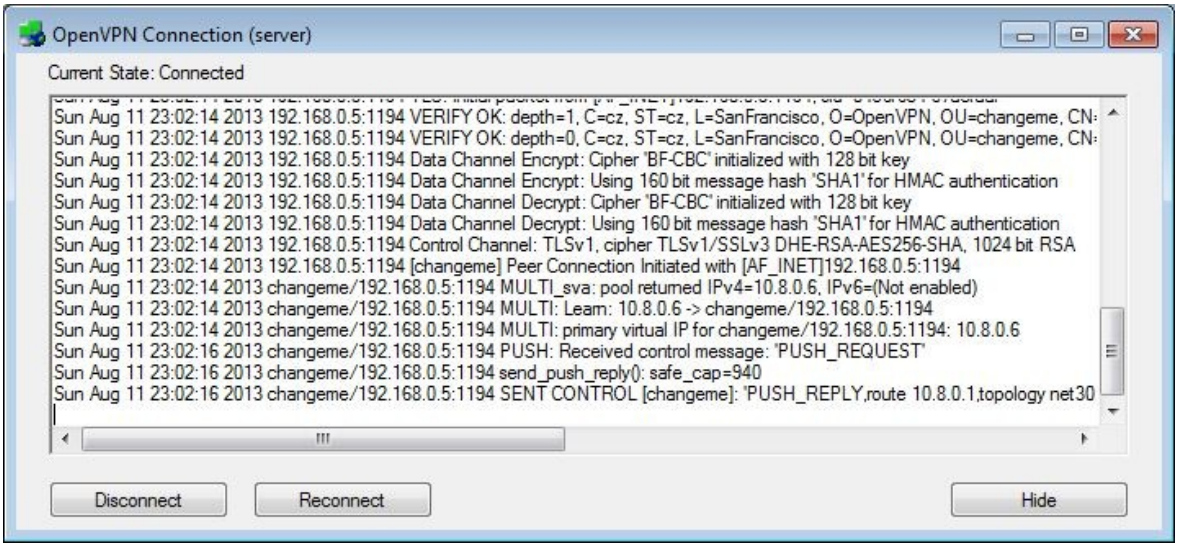
Obrázek 29 – Aktivace OpenVPN serveru

Na straně OpenVPN klienta stačí také kliknout v grafickém rozhraní programu na Connect a uživatel se úspěšně přihlásí k serveru, od kterého získá novou IP adresu 10.8.0.6.

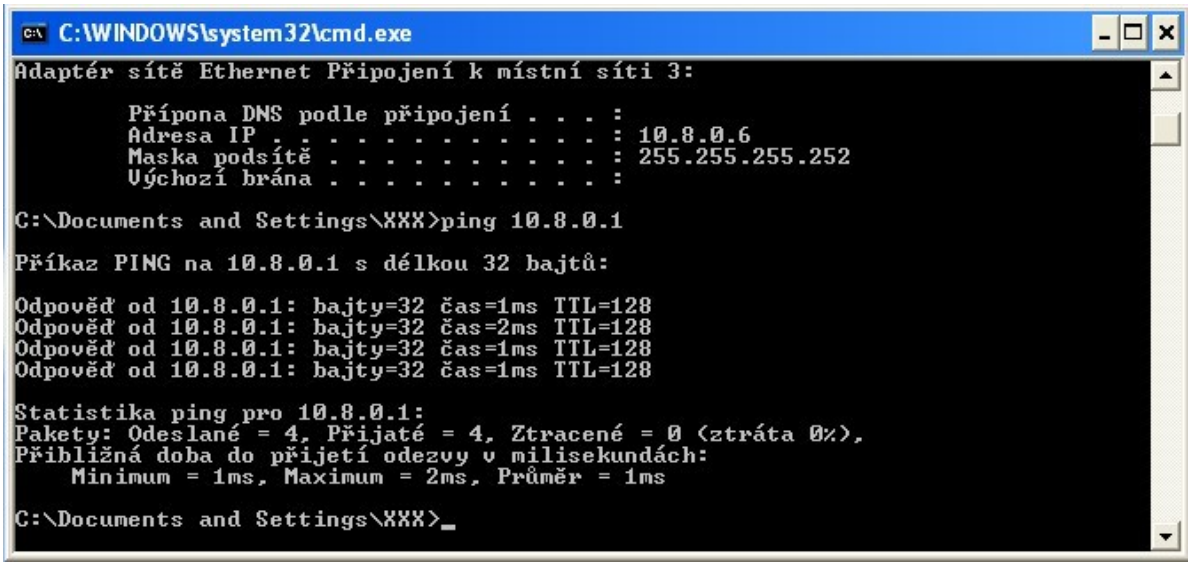


Obrázek 30 – Připojení OpenVPN klienta

Po připojení klienta k serveru je vidět na následujícím obrázku, že komunikace probíhá přes port 1194 a je šifrována. Případně celé záznamy logovacích souborů klienta a serveru jsou k dispozici na přiloženém CD.



Funkční příkaz ping od klienta na IP adresu 10.8.0.1 demonstruje úspěšné připojení na vnitřní počítač do zabezpečené sítě.



Obrázek 31 – Příkaz ping na vnitřní počítač

Závěr

Cílem této bakalářské práce bylo popsat teoretické poznatky o principu fungování VPN a využívání technologií při jeho tvorbě na spojové, síťové, transportní a aplikační vrstvě síťového modelu TCP/IP. V praktické realizaci bylo úkolem demonstrovat řešení VPN za použití technologie Cisco VPN a OpenVPN. Cíle práce byly splněny ve všech bodech.

V úvodní kapitole práce bylo charakterizováno VPN, jeho možné typy provedení a požadavky na jeho vytvoření. Byl popsán obecný princip fungování navazování spojení a výhody používání této technologie.

V další kapitole bylo detailně rozebráno VPN na jednotlivých vrstvách síťového modelu TCP/IP modelu se zaměřením na technologie a protokoly, které na jednotlivých vrstvách využívá.

Třetí kapitola popisuje konfiguraci vytvoření dvou různých typů VPN za použití bezpečnostního zařízení ASA 5505 od společnosti Cisco Systems. Popisovaná konfigurace obsahuje také ukázku omezení přístupu vzdálených uživatelů na jednotlivé vnitřní zdroje sítě.

Čtvrtá kapitola popisuje konfiguraci vytvoření VPN na aplikační vrstvě prostřednictvím programu OpenVPN.

Výsledná práce by mohla sloužit uživatelům, kteří se chtějí o technologii VPN dozvědět více a také jako praktická příručka tvorby OpenVPN a Cisco VPN.

Literatura

[1] VPN Technologies: Definitions and Requirements. *Virtual Private Network Consortium -- VPNC* [online]. 2008 [cit. 2013-08-12]. Dostupné z: http://www.vpnc.org/vpn-technologies.html

[2] Virtuální privátní síť, druhy propojení (2.díl). *Owebu.cz* [online]. 2009 [cit. 2013-08-12]. Dostupné z: http://owebu.bloger.cz/PC-site/Virtualni-privatni-sit-druhy-propojeni-2-dil

[3] LUHOVÝ, Karel. Seriál o VPN. In: *Svět sítí* [online]. 2003 [cit. 2013-8-11]. Dostupné z: http://www.svetsiti.cz/rubrika.asp?rid=17&tid=219.

[4] PUŽMANOVÁ, Rita. *TCP/IP v kostce*. Vyd. 1. České Budějovice: Kopp, 2004, 607 s. ISBN 80-723-2236-2.

[5] SOSINSKY, Barrie. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.

[6] OPPLIGER, Rolf. *SSL and TLS: theory and practise.* Vyd. 1. Boston: Artech House, c2009, xxi, 259 p. Artech House informatic security and privacy series. ISBN 15-969-3447-6.

[7] HOWTO. *OpenVPN* [online]. 2013 [cit. 2013-08-12]. Dostupné z: https://openvpn.net/index.php/open-source/documentation/howto.html

[8] 8 advantages of using VPN. *Invisible Browsing VPN* [online]. 2010 [cit. 2013-08-12]. Dostupné z: http://www.ibvpn.com/blog/2010/02/8-advantages-of-using-vpn/

[9] SSL VPN. In: *Cisco Systems* [online]. 2012 [cit. 2013-08-012]. Dostupné z: http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_sslvpn/configuration/15-2mt/sec-conn-sslvpn-ssl-vpn.html

[10] IMRICH, Jaroslav. VPN sítě s OpenVPN (1). *I15.cz - Vše podstatné za 15 minut* [online]. 2008 [cit. 2013-08-12]. Dostupné z: http://www.i15.cz/vpn-site-s-openvpn-1/

[11] Secure Remote Access (SSL VPN). *Technology, Life and other sutff that come along* [online]. 2006 [cit. 2013-08-12]. Dostupné z: http://nirlog.com/2006/01/23/secure-remote-access-ssl-vpn/

[12] The TCP/IP Networking Model. *Abigail Abanilla - Daily Sojournings* [online]. 2010 [cit. 2013-08-12]. Dostupné z: http://abigailabanilla.com/blogs/networking/the-tcpip-networking-model/

[13] Protokoly tunelového propojení VPN. *Windows Server | Deploy, Manage, Troubleshoot* [online]. 2013 [cit. 2013-08-12]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc771298%28v=ws.10%29.aspx

Příloha A – CD ROM

Obsah CD:

- Konfigurační soubory k Clientless SSL VPN a SLL VPN Client,
- konfigurační soubory k OpenVPN,
- textová část ve formátu pdf.