VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Virtuální privátní sítě IPsec se vzdáleným přístupem

IPsec Remote Access Virtual Private Networks

2016 **Bc. Vojtěch Bazgier**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

Zadání diplomové práce

Student: **Bc. Vojtěch Bazgier**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2601T013 Telekomunikační technika

Téma: Virtuální privátní sítě IPsec se vzdáleným přístupem
IPsec Remote Access Virtual Private Networks

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování různých řešení virtuálních privátních sítí IPsec se vzdáleným přístupem v laboratorním prostředí s využitím směrovačů Cisco a Huawei.

Osnova práce:
1. Popište různá řešení sítí IPsec VPN se zaměřením na sítě se vzdáleným přístupem.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň tři druhy sítí IPsec VPN se vzdáleným přístupem a podporou PKI (Public Key Infrastructure). Použijte k tomu směrovače Cisco a Huawei. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu směrovačů Cisco a Huawei v těchto sítích.
4. Srovnejte jednotlivá řešení. Zhodnoťte výhody a nevýhody jejich použití.

Seznam doporučené odborné literatury:

[1] CARMOUCHE, James Henry. *IPsec Virtual Private Network Fundamentals.* Indianapolis: Cisco Press, 2006. ISBN 1-58705-207-5.
[2] DEAL Richard. *The Complete Cisco VPN Configuration Guide.* Indianapolis: Cisco Press, 2006. ISBN 1-58705-204-0.
[3] Dokumentace k směrovačům Cisco a Huawei.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Machník, Ph.D.**

Datum zadání: 01.09.2015
Datum odevzdání: 29.04.2016

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky OSTRAVA

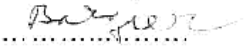
doc. Ing. Miroslav Vozňák, Ph.D.
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *28. června 2016*



podpis studenta

Poděkování

Rád bych poděkoval Ing. Petru Machníkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této diplomové práce.

Abstrakt

Tato diplomová práce se zabývá řešením zabezpečené komunikace mezi uživatelem a VPN bránou, umístěnou ve vzdálené síti. Na straně klienta je nainstalován VPN klient, který poskytuje zabezpečené spojení pomocí protokolu IPSec. V současnosti je vzdálený přístup hojně používán k připojení do firem a dalších instituci, a umožňuje například práci z domova. V diplomové práci budou jako VPN brány použita tří zařízení. Jedná se o zařízení Cisco ASA, směrovač Cisco řady 2800 a směrovač Huawei řady AR2200. Autentizace uživatelů je provedena pomocí certifikátů, které vydává certifikační autorita provozována na směrovači Cisco řady 2901.

Klíčová slova

VPN, VPN koncentrátor, VPN klient, IPSec, IKE protokol, certifikát, PKI

Abstract

This thesis deals with the solution of secure communication between the user and the VPN gateway which is located on a remote network. On the client side is installed VPN client that provides secure connections using IPSec. At present, remote access is widely used to connect to companies and other institutions, and allows, for example, work from home. In this thesis will be used as a VPN gateway three devices. The devices are the Cisco ASA appliance, Cisco 2800 Series Router and Huawei AR2200 series router. User authentication is performed using certificates issued by a Certification Authority operated on a Cisco 2901 series router.

Key words

VPN, VPN concentrator, VPN klient, IPSec, IKE protocol, certificates, PKI

Obsah

Seznam použitých zkratek

Zkratka	Význam
AAA	Authentication, Authorization and Accounting protocol
ACL	Access Control List
ACS	Access Control Server
AES	Advanced Encryption Standart
AH	Authentification Header
ASA	Adaptive Security Appliance
CA	Certificate Authority
CRL	Certificate Revocation List
DES	Data Encryption Standart
DMZ	Demilitarized Zone
DoS	Denial of Service
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol Security
ISAKMP	Internet Security Assosiation and Key Management Protocol
LDAP	Lightweight Direcotry Access Protocol
L3	Layer 3
MD5	Message Digest 5
MPLS	Multiprotocol Label Switching
MTU	Maimum Transmission unit
NIDS	Intrusion Detection Systém
OTP	One-Time Password

OSI	Open Systém Interconnection
PKI	Public Key Infrastructure
PSK	Pre-shared key
RA	Registration Authority
RAVPN	Remote Access VPN
RSA	Rivest, Shamir, Adleman
SA	Security Asociation
SCEP	Simple Certificate Enrollment Protocol
SHA	Secure Hash Algorithm
SOHO	Small Office, Home Office
SPI	Security Parameter Index
SSL	Security Sockets Layer
TLS	Transport Layer Security
VLAN	Virtual Loacal Area Network
VPN	Virtual Private Network

Seznam ilustrací a seznam tabulek

Úvod

Cílem této diplomové práce je realizace a testování virtuálních privátních sítí IPsec se vzdáleným přístupem. Účelem těchto sítí je zabezpečit přenos dat od uživatele, který se připojuje ke vzdálené síti, přes veřejnou nezabezpečenou infrastrukturu jako je Internet. K realizaci těchto virtuálních privátních sítí bude použito zařízení od firem Cisco a Huawei. Jako autentizační metoda pro připojení do vnitřní privátní sítě bude sloužit ověřování pomocí certifikátů, které budou vydávány certifikační autoritou.

Celkově se práce skládá z devíti kapitol. V prvních čtyřech kapitolách je popsána teoretická stránka řešeného problému. V první kapitole je popsáno dělení virtuálních privátních sítí, jejich typy a možné výhody vyplývající z jejich nasazení do síťové infrastruktury. Druhá kapitola se zabývá protokolem IPsec. Je vysvětleno, jak protokol funguje, jsou popsány jeho vlastnosti, módy a další protokoly, které protokol IPsec využívá k vytvoření bezpečného tunelu. Třetí kapitola nese název Remote access VPN a popisuje architekturu sítí se vzdáleným přístupem. V další kapitole jsou popsány části PKI (Public Key Infrastructure) a je vysvětlen princip podepisování certifikátů.

Následující kapitoly jsou již zaměřeny na praktickou část řešení zadání diplomové práce. V šesté kapitole je popsáno, jak vytvořit virtuální privátní síť se vzdáleným přístupem se zařízením Cisco ASA, které slouží jako VPN koncentrátor. Podrobně je popsán každý krok konfigurace a jsou vysvětleny jednotlivé příkazy, kterými se zařízení konfiguruje. Taktéž je popsána konfigurace certifikační autority, získání certifikátů pro VPN koncentrátor i pro vzdáleného uživatele. Na jeho straně je nainstalován VPN klient, jehož nastavení je také popsáno. Funkčnost vytvořeného zabezpečeného tunelu je poté ověřena pomocí příkazů na VPN koncentrátoru a pomocí paketového analyzátoru Wireshark, který je nainstalován na dvou počítačích, sledujících provoz ve vnitřní a vnější síti. Celý tento popis konfigurace a ověření funkčnosti je poté proveden i se směrovačem Cisco řady 2800 a směrovačem Huawei AR2200, které postupně nahradí zařízení Cisco ASA. Vzniknou tedy tři topologie sítí, kde budou tyto tři zařízení vystupovat jako VPN koncentrátor. Grafické znázornění těchto topologii je vyobrazeno pro každé zařízení zvlášť.

V závěru práce je popsán výsledek celého řešení IPsec virtuálních privátních sítí se vzdáleným přístupem. Je shrnuto, jakým způsobem lze realizovat tato řešení na jednotlivých zařízeních, jsou srovnány jejich konfigurace, popsány jejich vzájemné odlišnosti a vylíčeny jejich výhody a nevýhody pro realizaci IPsec virtuálních privátních sítí.

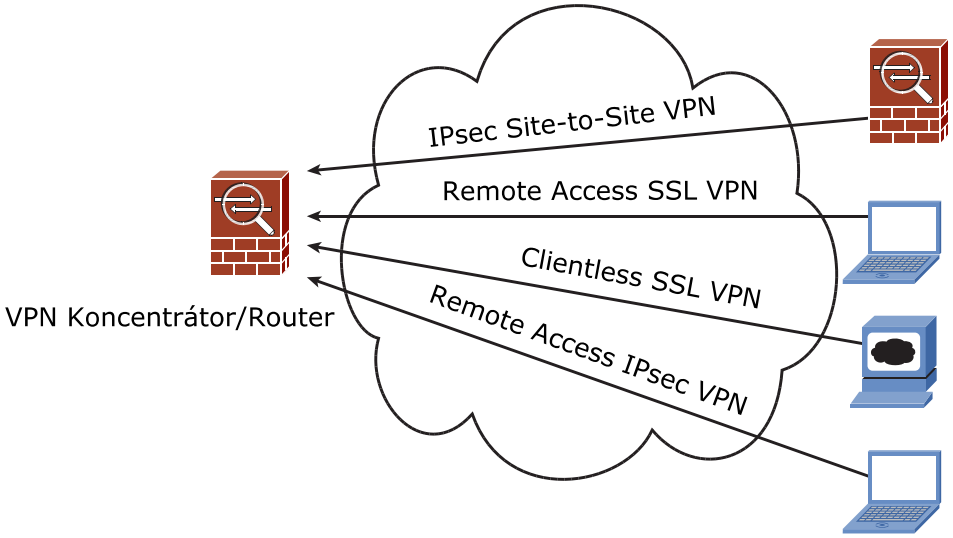
1 Virtuální privátní sítě

Virtuální privátní sítě (VPN) zajišťují zabezpečený a privátní přenos dat přes nezabezpečenou síťovou infrastrukturu. Zabezpečení přenášených dat je docíleno použitím zapouzdření, tzv. enkapsulace nebo šifrováním. Případně jsou data pro přenos přes nezabezpečenou síť zapouzdřena a následně i zašifrována[1].

Virtuální privátní sítě tedy můžeme rozčlenit do dvou skupin: ty které nabízí privátní přenos dat s využitím zapouzdření dat či přidáním značky k datovému paketu (například: VLAN - Virtual local area networks , MPLS VPN - Multiprotocol Label Switching VPN) a ty, které nabízejí zabezpečení a privátní přenos dat (IPsec/ Secure Sockets Layer (SSL)VPN). Zabezpečení je docíleno aplikací kryptografického protokolu (například IPsec, SSL, TLS - Transport Layer Security)[2].

1.1 Dělení sítí VPN

Výše zmíněných VPN metod můžeme využít k zajištění zabezpečeného přenosu dat mezi dvěma vzdálenými sítěmi (viz obrázek 1.1). Jedná se o tzv.: virtuální privátní sítě síť-síť (Site - to - Site VPN), nebo k realizaci spojení vzdáleného uživatele s centrálním bodem (například firma, škola, …), tzv.: virtuální privátní sítě se vzdáleným přístupem (Remote access VPN). Právě na posledně zmiňovanou VPN síť bude tato práce zaměřena.



Obrázek 1.1: *Virtuální privátní sítě[2]*

1.2 Základní výhody sítí VPN

Poslední dva výše zmiňované typy VPN sítí poskytují čtyři základní výhody pro přenos dat mezi vzdálenými sítěmi či uživateli: Jsou jimi[1]:

- Autentičnost: Této vlastnosti je dosaženo použitím hesel (pre-shared keys - PSK), one-time passwords (OTP), tokenů, infrastrukturou veřejných klíčů (public key infrastrukture - PKI). Hlavním účelem autentifikace je ověření identity komunikujících stran.

- Důvěrnost: Je zajištěna zašifrováním uživatelských dat před jejím vysláním přes vytvořený VPN tunel s cílem zabránit komukoli tato data zachytit.

- Integrita dat: Poskytuje záruku, že mezi zdrojem a cílovou destinací nebylo nijak s přenášenými daty manipulováno (například útočník snažící se provádět útok man in the middle).

- Antireplay ochrana: Zařízení posílající data může ke každému paketu přidat sekvenční číslo, které zajistí, že paket nebyl například duplikován.

2 Internet Protokol Security

Internet Protokol Security (IPsec)[1], definován v RFC 2401, poskytuje prostředky pro zajištění autenticity, integrity a důvěrnosti dat na síťové vrstvě OSI modelu. IPsec je tvořen sadou protokolů, které definují standardy pro čtyři klíčové prvky, potřebné pro vytvoření robustní virtuální privátní sítě (VPN).

- Bezpečnostní protokoly
- Mechanizmus výměny klíčů
- Algoritmy potřebné pro šifrování a bezpečnou výměnu klíčů
- Definici SA a její údržbu

Efektivní VPN tunel tedy musí zajišťovat autenticitu, integritu, důvěrnost dat a jejich nezaměnitelnost. Čím více těchto podmínek šifrovaná komunikace splňuje, tím je komunikační kanál považován za bezpečnější.

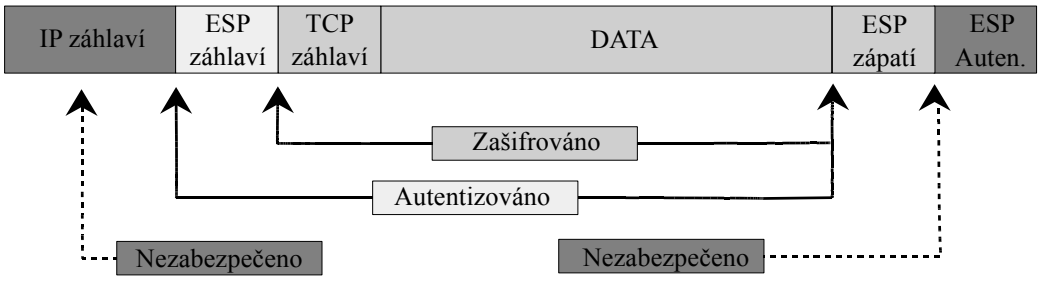
IPsec VPN šifruje data na třetí vrstvě OSI modelu a nabízí komplexní VPN řešení poskytující autentizaci dat, antireplay ochranu, důvěrnost dat a jejich integritu. IPsec je jednou z nejrozšířenějších VPN technologii v dnešních sítích. Jedná se o otevřený standard, může proto bez problému pracovat v sítích postavených na technologiích od různých výrobců.

2.1 Módy protokolu IPsec

IPsec používá dva různé módy k vytvoření zabezpečeného komunikačního kanálu. Jedná se o transportní a tunelovací mód. Zabezpečený komunikační kanál, který IPsec poskytuje, se nazývá IPsec SA (IPsec Security Association).

2.1.1 Transportní mód

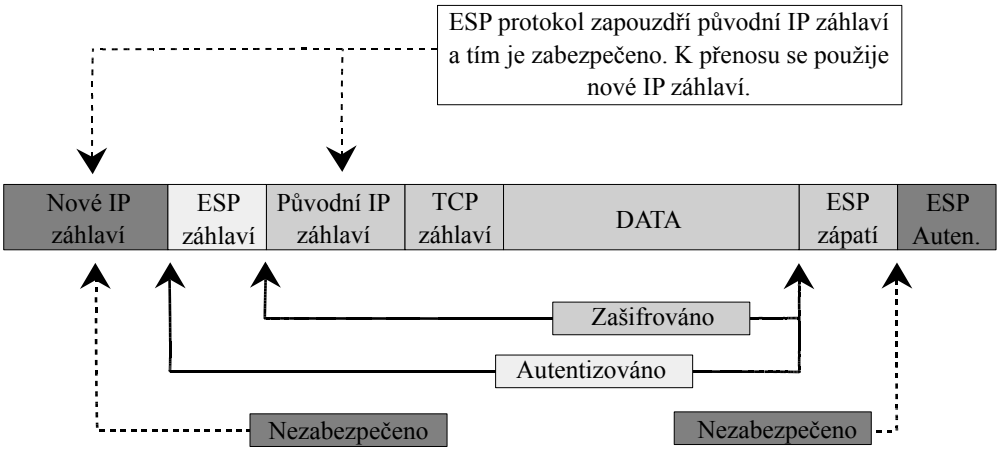
RFC 2401 definuje transportní mód SA jako spojení dvou IPsec hostů dohromady. V transportním módu (viz Obrázek 2.1) se používá ESP (Encapsulating Security Payload). Pouze protokoly vyšších vrstev jsou považované za důvěrné. Je to dáno tím, že do ESP paketu není začleněna hlavička IP.



Obrázek 2.1: Zapouzdření IP paketu pomocí ESP protokolu v transportním módu[1]

2.1.2 Tunelovací mód

Tunelovací mód má oproti módu transportnímu, chráněnou i IP hlavičku, nejsou tedy zabezpečeny pouze protokoly z vyšších vrstev. Je to docíleno vytvořením nové IP hlavičky, která je připojena k ESP paketu (viz Obrázek 2.2).



Obrázek 2.2: Zapouzdření IP paketu pomocí ESP protokolu v tunelovacím módu[1]

Tunelovací mód tedy zakrývá užitečné atributy IP hlavičky dvou koncových komunikujících stran.

2.2 Protokol ESP

Protokol ESP [1] poskytuje kombinaci bezpečnostních prvků pro IP pakety, které jsou zpracovány pomocí IPsecu. Jako příklad takovýchto prvků si můžeme představit důvěrnost dat, autenticitu nebo mechanizmy pro zachování integrity dat. Tyto prvky mohou být použity dohromady nebo zvlášť. Vše určuje administrátor před dohodnutím SA. ESP může být použit jak v tunelovacím, tak i v transportním módu. Taktéž může být nasazen samostatně nebo dohromady s hlavičkou AH.

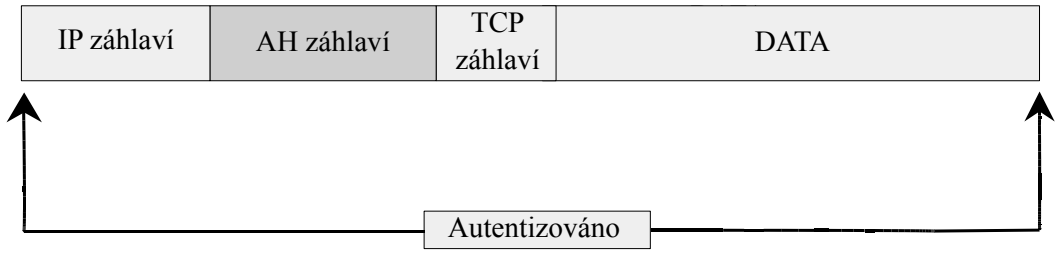
Každý ESP paket je označen pomocí SPI (Security Parametr Index). SPI poskytuje zařízením informace, ke kterému SA ESP paket patří. Jedná se o 32bitové číslo, odvozené cílovým zařízením během IKE fáze. Kromě čísla SPI je každý ESP paket označen sekvenčním číslem, které zajišťuje antireplay ochranu.

K zajištění integrity a autentifikace dat se používá HMAC (Hashed Message Authentication Code), který je přidán do ESP hlavičky. Tento kód je vytvořen pomocí hashovací funkce (MD5, SHA), sdíleného tajného klíče (vytvořeného pomocí Diffie-Hellmanova algoritmu) a vstupní zprávy.

2.3 Protokol AH

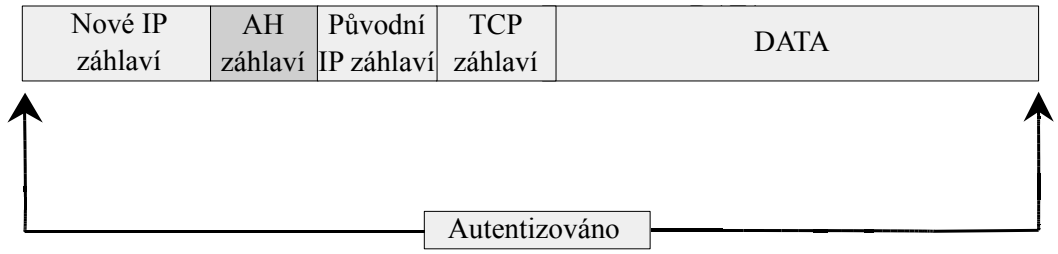
Pokud není vyžadována důvěrnost dat, je možné použít IPsec s hlavičkou AH místo ESP hlavičky. AH protokol[1] poskytuje autentifikaci, antireplay ochranu a integritu dat. To je zajištěno přidáním hlavičky do paketu s názvem authentication header (viz Obrázek 2.3). Jak už bylo zmíněno,

protokol AH na rozdíl od protokolu ESP nezajišťuje důvěrnost dat. Jelikož ale autentizuje části IP hlavičky, poskytuje lepší ochranu pro protokoly vyšších i nižších vrstev, zatímco ESP protokol v transportním módu pouze pro protokoly vyšších vrstev.



Obrázek 2.3:Zapouzdření IP paketu pomocí AH protokolu v transportním módu[1]

Stejně jako protokol ESP, také protokol AH může fungovat v transportním i tunelovacím módu. V tunelovacím módu AH kopíruje část vnitřní IP hlavičky a použije jí k vytvoření nové vnější IP hlavičky. AH v tunelovacím módu (viz Obrázek 2.4) poskytuje celému paketu autenticitu a integritu, včetně nové IP adresy.



Obrázek 2.4:Zapouzdření IP paketu pomocí AH protokolu v tunelovacím módu[1]

Stejně jako ESP zapouzdření, i zapouzdření pomocí AH protokolu používá identifikátory SPI k určení, do které příslušné SA paket patří.

2.4 IPsec SA

Pokud chtějí dvě zařízení vytvořit mezi sebou IPsec spojení, musí se dohodnout na řadě parametrů. Těchto parametrů, na kterých se zařízení domlouvají, je několik. Aby byl IPsec tunel vytvořen a správně fungoval, je nutné je nastavit. Vyjednávání těchto parametrů má na starosti IPsec SA[1]. Mezi tyto parametry můžeme zařadit:

- Mód – Jedná se buď o transportní, nebo tunelovací mód.
- Zapouzdření paketů – Způsob zapouzdření paketů a typ šifrovacího algoritmu. Lze nastavit protokoly ESP, AH nebo obojí. Šifrovací algoritmus je symetrický. Můžeme vybírat mezi DES,3DES,AES.
- Koncový bod tunelu – Specifikuje koncové zařízení, se kterým chceme vytvořit IPsec tunel. Používá se, pokud nepoužíváme dynamické vytváření tunelu
- Zabezpečovaný provoz – Koncová zařízení IPsec tunelu musí mít nastavený stejný provoz, který se má šifrovat či dešifrovat. Pokud toto není splněno, tunel se nevytvoří

- MTU – Koncová zařízení se musí domluvit na MTU ve vytvořeném tunelu
- SPI

IPsec vyžaduje vytvoření jedinečného IPsec SA pro každý směr IPsec tunelu a pro každý protokol (ESP,AH, nebo jejich kombinace). Taktéž se vytváří další typ SA a to IKE SA. IKE SA se vytváří ještě před vytvořením IPsec SA a slouží k vytvoření zabezpečeného kanálu k přenosu parametrů k vytvoření IPsec SA.

Postup vytváření jednotlivých SA je zobrazen na následujícím obrázku (viz obrázek 2.5).

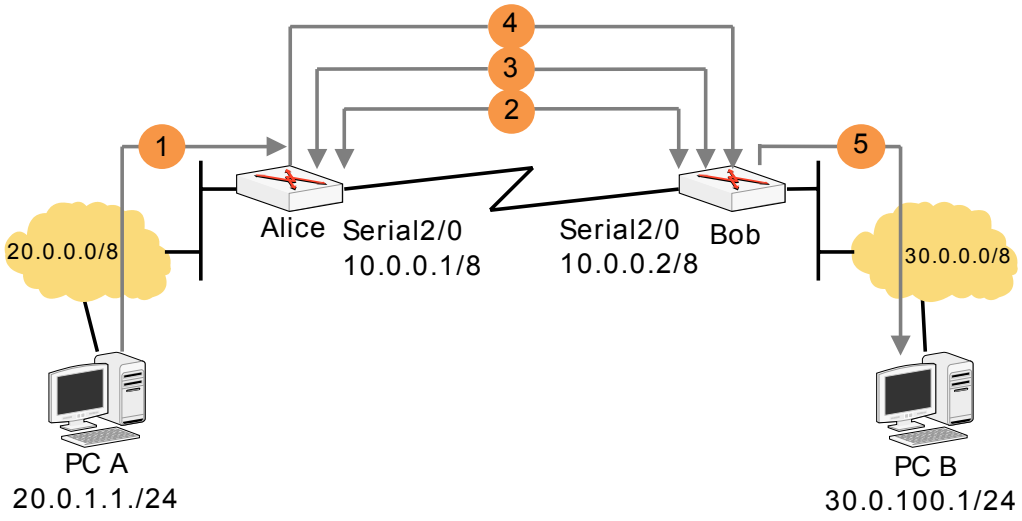
1) Alice příjme paket, který splňuje podmínky pro šifrování provozu a započne vyjednávání IKE SA.

2) Alice a Bob se vzájemně autentizují, buď pomocí předsdílených klíčů nebo certifikátů. IKE SA je nyní vytvořen.

3) Jakmile je IKE aktivní, směrovače mohou použít tento zabezpečený kanál k vyjednávání IPsec SA. Dohodnou se na použitém šifrovacím algoritmu (DES, 3DES, AES), hashovacím algoritmu (MD5, SHA), a pomocí Diffie–Hellmanova algoritmu se vymění sdílený symetrický klíč. Také se vzájemně domluví na unikátním čísle SPI, kterým se budou označovat pakety ve vytvořených SPI.

4) Pakety nyní mohou být šifrovány domluveným symetrickým klíčem, vyjednaným v kroku 3, a poslány Bobovi.

5) Bob příjme paket, podívá se na hodnotu SPI,a zjistí, jak dešifrovat paket. Paket dešifruje a použije vnitřní IP hlavičku k poslání nezašifrovaného paketu k cílovému místu.



Obrázek 2.5: Postup vytváření SA[5]

Další pakety se přenáší od bodu čtyři, protože SA již byly vytvořeny. Až po uplynutí doby, kdy je tunel aktivní nebo po přenesení určitého množství dat, je SA zrušeno a dalším paketem začne vyjednávání SA znovu.

2.5 Protokol ISAKMP

ISAKMP[1] (Internet Security Association and Key Management Protocol) byl původně definován jako protokol, který implementoval dvě důležité služby do stále více používaného IPsec protokolu. Jedná se o dynamické vytváření SA a dynamické vyměňování kryptografického klíče přes zabezpečený kanál.

ISAKMP definuje následující procedury:

- Autentizace konců IPsec tunelu
- Vyjednávaní, údržba a ukončení IPsec SA
- Generace kryptografického klíče a jejich výměna (DH)
- Prevence před útoky na komunikaci (antireplay, ochrana před útoky DoS)

V podstatě ISAKMP slouží k poskytování těchto služeb, ale nedefinuje, jaký protokol by měl tyto služby řešit. Je tedy nezávislý na používaném protokolu pro výměnu klíče. V případě IPsec VPN, je k vyjednávání parametrů nejvíce používán IKE protokol.

Výhodou používání ISAKMP/IKE je také možnost nastavit životnost vytvořeného IPsec tunelu, což při použití manuálních klíčů není možné. To umožňuje administrátorům zbytečně nezatěžovat prostředky a automaticky ukončovat IPsec tunel po vypršení jeho životnosti.

2.6 Typy autentizace IKE protokolu

V IPsec VPN, která používá ISAKMP, je IKE protokol kanálem, přes který se vymění parametry pro vyjednání IPsec SA. Důležité je, aby se IKE SA vytvořily naprosto bezpečně. Z tohoto důvodu nabízí IKE mnoho robustních autentifikačních mechanizmů k zajištění autenticity obou konců IPsec tunelů. VPN koncová zařízení mohou podporovat následující typy autentizace:

- Předsdílené klíče
- RSA šifrování
- RSA podpisy (certifikáty X.509)

2.6.1 Předsdílené klíče

Předsdílené klíče je možno využít v menších sítích, kde mohou být klíče zadány ručně. Využívá se IKE předsdílených klíčů. Klíče jsou ručně nastaveny na koncích tunelu, které se vzájemně autentizují posláním vypočítaného hash kódu z dat obsahující předsdílený klíč. Jestliže přijímající strana vypočítá stejný hash kód za pomocí svého předsdíleného hesla, je jasné, že jsou hesla stejná a koncové zařízení IPsec tunelu jsou autentizována[3].

2.6.2 Šifrování RSA

IKE použije RSA kryptografický algoritmus k ověření identity konců tunelů, před vyjednáváním IKE fáze I. Využívá se náhodnosti čísel, k dosažení větší bezpečnosti.

2.6.3 Podpisy RSA a certifikáty standardu X.509

RSA podpisy jsou formou digitálních podpisů. Jedná se o kombinaci šifrovacího algoritmu RSA a vlastností digitálních podpisů. RSA podpisy jsou hlavně využívány v kombinaci s X.509 certifikáty a certifikačními autoritami (CA).

X.509 certifikáty a CA byly vyvinuty k snížení administrativní zátěže v sítích, kde se používá asymetrické šifrování. Vznikl tedy centrální bod administrace nebo CA jehož prostřednictvím koncová zařízení registrují své veřejné klíče a získávají veřejné klíče svých protějšků. Aby se zabránilo neefektivním výměnám informací, CA musí komunikovat pomocí certifikátů, které jsou standardizovány. Pro tento účel je určen standard X.509, který podporuje kryptosystém založeny na veřejném klíči.

2.7 Fáze protokolu IKE

2.7.1 IKE fáze I

Jak už bylo řečeno, hlavním smyslem IKE protokolu je vytvoření zabezpečeného kanálu, přes který se vymění bezpečnostní parametry pro vytvoření IPsec SA. Toto vyjednávání parametrů IKE kanálu je nazýváno jako fáze I. Pro úspěšné dokončení vyjednávání IKE fáze I se musí obě komunikující strany dohodnout na následujících parametrech[1]:

- Autentifikační metoda
- Autentifikační hashovací algoritmus
- Šifra
- Číslo skupiny Diffie-Hellmanova algoritmu

Jakmile jsou tyto metody jednou dohodnuty, komunikující strany začnou s vyjednávacím procesem. Výsledkem IKE fáze I je vytvoření ISAKMP SA. Po jeho vzniku mezi kryptografickými koncovými zařízeními může být vytvořen autentizovaný kanál pro důvěrné vytvoření IPsec SA.

2.7.1.1 Hlavní mód

Hlavní mód [1] pro IKE vyjednávání, provádí ochranu identity mezi dvěma kryptografickými zařízeními. Na rozdíl od agresivního módu spotřebuje vetší množství výpočetního výkonu, což je dáno tím, že hlavní mód zahrnuje více komplikované vyjednávání než v případě agresivního módu. Hlavní mód umožňuje bezpečné vytvoření ISAKMP SA, aniž by byly vyměňovány identity koncových stran jako běžný text. Toho je v IKE hlavním módu docíleno výměnou zpráv mezi komunikujícími stranami ve třech krocích.

2.7.1.2 Agresivní mód

Na rozdíl od vyjednávání IKE v hlavním módu, který zahrnuje výměnu zpráv ve třech krocích, agresivní mód[1] zahrnuje pouze dva kroky výměny zpráv. Stejně jako v případě hlavního módu, agresivní mód zahrnuje zprávy pro dohodnutí šifry, hashovacího algoritmu, autentifikační metody a číslo skupiny Diffie-Hellmanova algoritmu. V agresivním módu jsou identity obou komunikujících stran nezašifrovány, protože jsou současně poslány s kryptografickými prvky, které jsou potřebné pro šifrování v první výměně zpráv. Hlavní výhodou agresivního módu je, že je méně výpočetně náročný.

2.7.2 IKE fáze II

Cílem vyjednávání IKE fáze II [1]je zřízení IPsec SA kanálů mezi dvěma koncovými zařízeními. IKE využívá Diffie-Hellmanova algoritmu k výměně sdíleného tajného hesla, které bude sloužit k šifrování přenášených dat. Je možné také použít klíč vytvořený v IKE fázi I.

2.7.2.1 ***Rychlý mód***

IKE fáze II se používá pouze v jednom módu. Jedná se o rychlý mód[1]. Vzhledem k tomu, že hlavním smyslem fáze II je vytvořit IPsec SA, výměna zpráv v rychlém módu musí obsahovat informace o vytvářeném IPsec SA (ESP nebo AH, například šifry DES, 3DES, AES, hashovaní algoritmy MD5 nebo SHA a provoz, který má být šifrován). Pro vyjednání se použije dvou kroků, které obsahují celkem čtyři zprávy.

Podrobný popis zpráv a jejich průběh v hlavním módu, agresivním módu a rychlém módu je možné se dočíst v [1].

2.8 Protokol IKEv2

Protokol IKEv2 [4][5]je druhá a poslední verze IKE protokolu. Ve verzi IKEv1 při použití hlavního módu ve fázi jedna je vyjednávání parametrů docíleno pomocí šesti zpráv, u fáze II jsou to zprávy čtyři. V protokolu IKEv2 se počty zpráv mohou lišit. Vyjednávání může proběhnout pomocí čtyř nebo i 30 zpráv v závislosti na složitosti autentizace, na počtu atributu použitých u EAP protokolu. U IKEv2 není agresivní ani hlavní mód. Pro vyjednávání se využívají dvě fáze, IKE_SA_INIT Exchange a IKE_AUTH Exchange.

Oproti protokolu IKEv1 nabízí protokol IKEv2 tyto vylepšení

- Podpora mobility pomocí protokolu MOBIKE
- Podpora EAP autentifikace
- Zabudovaná funkce NAT traversal
- Detekce, zda je IPsec tunel aktivní
- Lepší odolnost vůči útokům typu DoS vytvářejících falešné tunely

3 Remote Access VPN

Se stále se zvětšujícím počtem zaměstnanců, kteří pracují mimo svou firmu, je potřeba dynamicky měnit bezpečnost IP sítí. Nasazení Remote Access VPN (RAVPN)[1] se stalo ústředním bodem pro zabezpečení konektivity v podnikových sítích pro vzdáleně připojené uživatele. Princip spočívá v povolení zabezpečené komunikace na třetí vrstvě OSI modelu k jakémukoli VPN koncovému bodu, který má internetové spojení k příslušnému VPN koncentrátoru.

3.1 Přehled architektury RAVPN

Základ RAVPN architektury tvoří dva prvky. Jsou jimi VPN koncentrátory a VPN klienti.

- VPN klienty můžeme rozdělit na hardwarově orientované nebo softwarově orientované. Jako hardwarově založeného klienta si můžeme představit VPN směrovač či VPN modul zprostředkující RAVPN řešení. V případě softwarově založeného klienta, RAVPN spojení zajišťuje klientský software, který běží na uživatelském počítači.
- VPN koncentrátory se používají k ukončení RAVPN spojení přicházející od VPN klientů. VPN koncentrátory mohou v RAVPN řešení nabízet variabilní řešení pro ukončování velkého počtu IPsec spojení od VPN klientů.

VPN koncentrátory a VPN klienti spolu mohou komunikovat přes různá technologická řešení, která podporují komunikaci na třetí vrstvě OSI modelu. Příkladem mohou být vytáčené linky, internetové spojení používající technologii DSL nebo bezdrátový standard 802.11.

3.2 Klienti RAVPN

Jak už bylo řečeno výše, RAVPN klienty můžeme dělit na dva typy[1]. Hardwarově orientované nebo softwarově orientované. Softwarově orientovaní klienti běží lokálně na vzdálené uživatelské pracovní stanici nebo laptopu, které jsou propojené k centrálně řízenému VPN koncentrátoru. Tento VPN koncentrátor je typicky umístěn ve firemním areálu. Hlavní výhoda, kterou softwarově orientovaní VPN klienti poskytují, je jejich velká mobilita. Po jejich nasazení na uživatelský laptop, umožní tento softwarový klient rozšířit zabezpečenou komunikaci z firemního areálu kdekoli do míst, kde má VPN klient přístup ke komunikaci na třetí vrstvě OSI modelu. Použití softwarově orientovaných klientů je proto užitečné pro tunelování dat z centrálně umístěného firemního areálu ke koncovému uživateli. Nicméně jsou tady i některá omezení, která tyto klienty znevýhodňují oproti hardwarově orientovaným VPN klientům. Konkrétně klientům, kteří jsou softwarově orientováni, není umožněno připojení jiného L3 zařízení na vzdálený konec té samé VPN (například připojení hardwarového IP telefonu). Dále neumožňují lokální ukončení GRE tunelu, a proto typicky nepodporují multicastový datový tok. Ačkoli jsou hardwarově orientovaní klienti jednoznačně méně mobilní, jsou řešením pro mnoho funkčních omezení nalezených u VPN IPsec klientů založených na softwarové bázi.

Hardwarově orientované VPN klienty můžeme typicky najít v malých odlehlých místech, která nemají vyhrazené připojení k centrálnímu IPsec směrovači. Tyto zařízení můžeme běžně nalézt v domácích kancelářích, které mají internetové připojení přes technologii DSL nebo přes kabelový modem. Hardwarově orientovaní VPN klienti zajišťují IPsec VPN (taktéž ukončení GRE tunelu)

připojení ke koncentrátoru, přičemž také umožňují místní nezašifrovanou komunikaci v rámci malé domácí sítě. Proto VPN komponenty na hardwarové bázi přidávají síťový prvek do SOHO nebo menších poboček firem a umožňují uživatelům bezpečně šířit hlas, video a data.

Aby bylo možné zajistit mobilitu i šíři služeb pro vzdáleně připojeného uživatele, je velmi běžné provozovat softwarově i hardwarově založené klienty najednou. Pokud máme k dispozici připojení přes hardwarově orientovaného VPN klienta, můžeme využívat všechny IP služby provozované v areálu firmy, ale s omezením pohybu. Toto řeší klient založený na softwarové bázi, který umožňuje komunikaci uživatelům s velkou mobilitou. Všechny tyto služby musí být nastaveny a povoleny na stráně VPN s koncentrátorem. Z tohoto důvodu jsou různé variace RAVPN topologie viděny hlavně na straně sítě, kde je umístěn VPN koncentrátor.

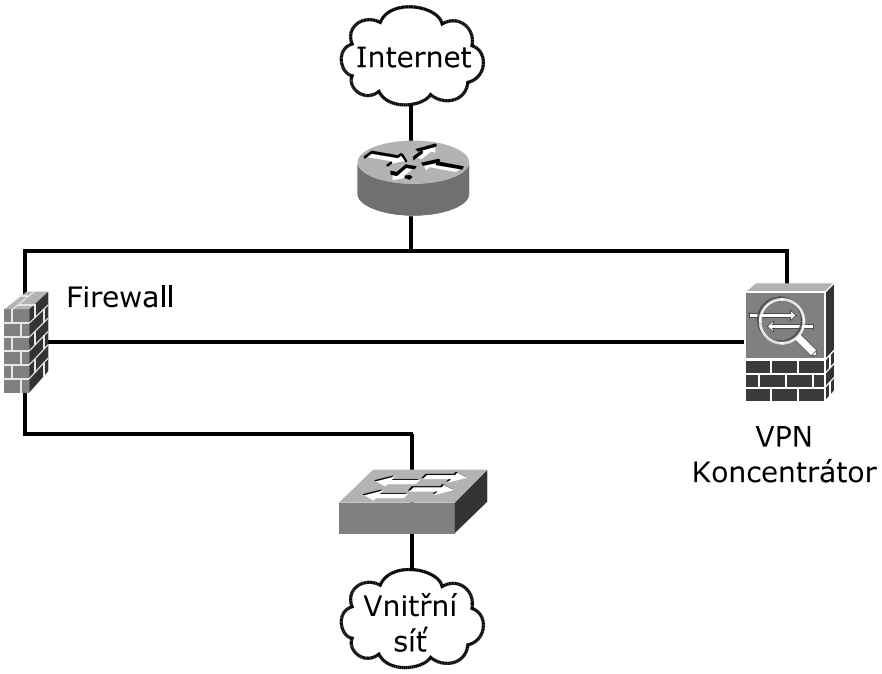
3.3 VPN koncentrátory

Pro ukončení RAVPN spojení přicházejících od VPN klientů je potřeba VPN koncentrátor. Před jeho implementací je nutné promyslet jeho umístění v existující síťové architektuře. Ve většině případů se VPN koncentrátor umisťuje blízko perimetru sítě.

Na obrázcích 3.1 až 3.3 můžeme vidět tři nejběžnější síťové topologie, které jsou doporučovány pro umístění VPN koncentrátoru Každý z těchto návrhu se týká nasazení VPN koncentrátoru v podnikovém prostředí pro efektivní ukončení klientských IPsec VPN tunelů v rámci RAVPN sítí.

3.4 VPN koncentrátor na vnější straně sítě s jednou DMZ

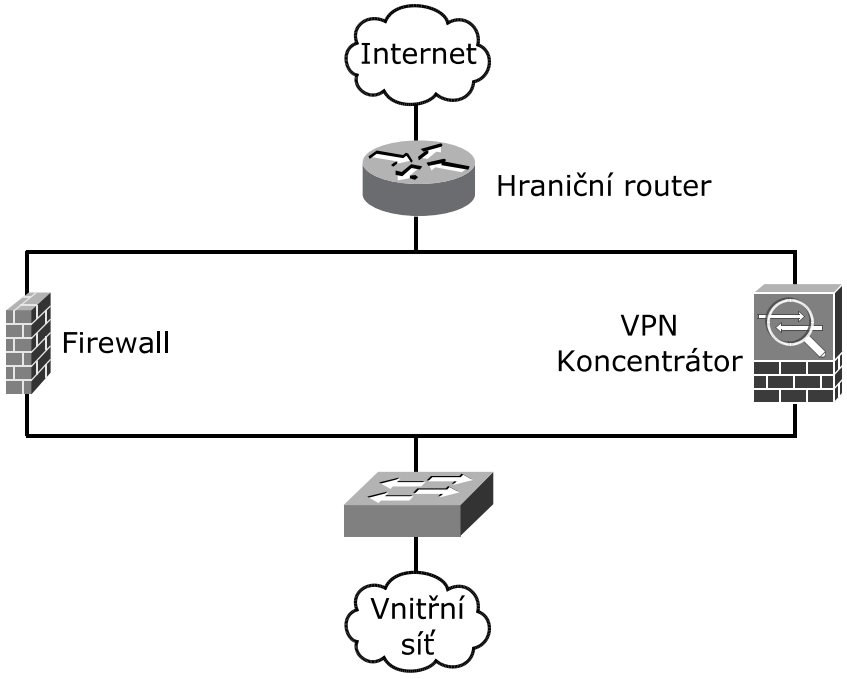
Návrh DMZ na obrázku 3.1, je jedním z nejznámějších a nejefektivnějším návrhem v RAVPN/DMZ implementaci. Návrh umožňuje zvýšenou bezpečnost, jelikož provoz z VPN koncentrátoru směřující do vnitřní sítě je ještě kontrolován firewallem. Taktéž může firewall přidat další bezpečnostní prvky jako je AAA autentizace ve spojení s ACS serverem umístěným na vnitřní straně sítě, který umožní autentizaci, autorizaci a účetní řešení pro různé typy provozu až po sedmou vrstvu OSI modelu. Dále může být zpracování vstupního datového provozu z DMZ hlouběji kontrolováno na síťové útoky pomocí ASA či NIDS zařízení[1].



Obrázek 3.1: VPN koncentrátor v řadě s Firewall bránou[2]

3.5 VPN koncentrátor s paralelním firewallem

Jak můžeme vidět na obrázku 3.2, je možné provést návrh bez jakékoli IPsec modifikace, která by se přidávala do nastavení ACL ve firewallu.

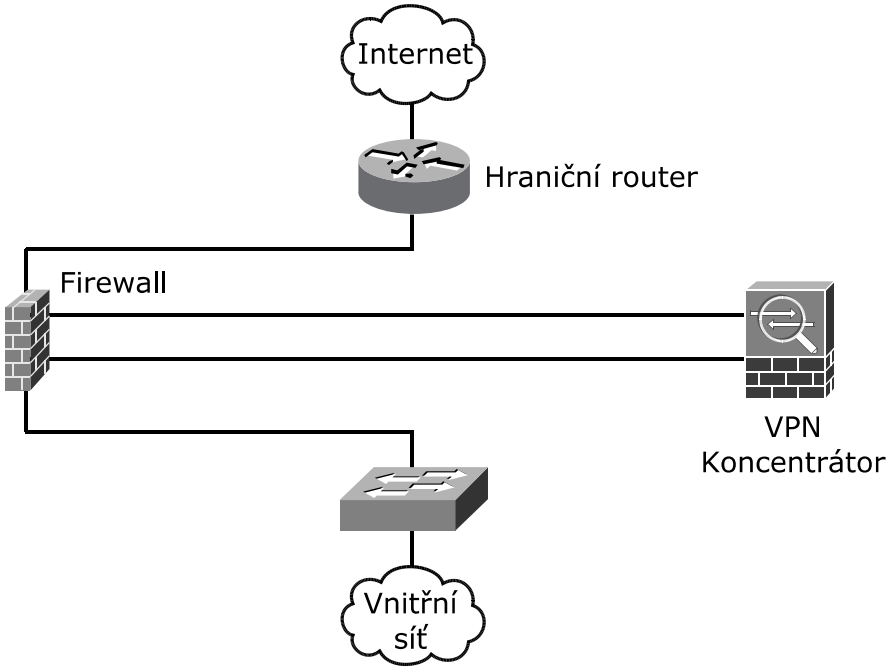


Obrázek 3.2:VPN koncentrátor s paralelním Firewallem[2]

Umístění VPN koncentrátoru paralelně s firewallem eliminuje možnou lidskou chybu, při otevírání děr ve firewallu, jako povolování vstupujícího IPsec provozu od VPN klientů do koncentrátoru. Navíc tato topologie nezatěžuje firewall kontrolou IPsec provozu vstupujícího do VPN koncentrátoru. Namísto toho je tento provoz výhradně soustředěn na VPN koncentrátor. Stejně tak není koncentrátor zatížen provozem, který nepřísluší v k VPN provozu, jak tomu bylo v případě, kdy byl VPN koncentrátor zapojen v sérii s firewallem[1].

3.6 VPN koncentrátor s dvěma DMZ a firewallem

Použití dvou DMZ rozhraní pro vnější a vnitřní VPN provoz můžeme vidět na obrázku 1.9. Tento návrh může být také efektivním způsobem pro integrování VPN koncentrátoru do DMZ. Měl by být nasazen při potřebě zvýšené ochrany VPN koncentrátoru. Jedná se o nejpoužívanější RAVPN architekturu, která na rozdíl od zapojení VPN koncentrátoru s paralelním firewallem (Obrázek 1.8), vylučuje hrozbu přímého přístupu neznámých uživatelů z internetu na VPN koncentrátor, aniž by byl tento provoz kontrolován firewall bránou. Odstraňuje také možné dvojitého kontrolování vstupního provozu firewallem, které mohlo nastat v případě architektury zobrazené na Obrázku 3.3[1].



Obrázek 3.3:VPN koncentrátor umístěn v DMZ[2]

V případě malých a středních podnikových sítí, lze při návrhu RAVPN topologie využít síťového zařízení, které poskytuje možnosti firewall brány a VPN koncentrátoru v jednom fyzickém boxu a minimalizovat tak celkové náklady na implementaci[2].

4 PKI - Public Key Infrastructure

PKI - Public Key Infrastructure neboli Infrastruktura veřejných klíčů[1] je systém kryptografických koncových zařízení, které využívají infrastrukturu důvěryhodných zdrojů. Mezi tyto důvěryhodné zdroje patří certifikační autority (CA) a registrační autority (RA). Hlavním účelem je usnadnění komunikace bezpečným způsobem. Ve velkých podnikových sítích s IPSec VPN přístupem, může být správa klíčů velmi náročná. S rostoucím počtem koncových zařízení komunikujících zabezpečeným způsobem je potřeba zavést centralizovanou metodu pro správu klíčů mezi těmito koncovými zařízeními. V našem případě mezí IPSec VPN koncentrátorem a IPSec VPN klientem. PKI může být použita v různých kryptografických řešení. V případě nasazení v IPSec VPN řešení, PKI zahrnuje následující prvky:

- Koncová zařízení patřící do PKI - VPN brány, koncová zařízení
- Zdroje, kterým důvěřují koncová zařízení patřící do PKI - PKI Certifikační autority
- Výměna veřejných klíčů mezi koncovými zařízeními pro autentizaci a šifrování IKE SA

4.1 Struktura PKI

PKI používá pro bezpečnou správu klíčů několik kryptografických zařízení. Tyto zařízení společně pracují pro zajištění širokého spektra funkci důležitých pro řízení distribuce klíčů. Mezi zmíněné funkce patří:

- Ověření integrity veřejných klíčů
- Autentizování požadavků na uložené veřejné klíče
- Bezpečné vydávání certifikátů veřejných klíčů
- Zrušení veřejných klíčů, které už nejsou nadále platné
- Udržování informace o zrušení veřejného klíče a distribuování této informace
- Bezpečné uložení platného veřejného klíče

4.1.1 Certifikáty veřejných klíčů

Hlavním účelem výměny klíčů v asymetrickém šifrování je bezpečně doručit veřejný klíč straně, která chce šifrovat přenášená data pro přijímací stranu. PKI pomáhá usnadňovat bezpečnou výměnu klíčů se zajištěním autenticity obou komunikujících stran. Prvním krokem této výměny je vytvoření certifikátu veřejného klíče.

Certifikát veřejného klíče je generován certifikační autoritou (CA). K tomu aby CA mohla vytvořit certifikát veřejného klíče pro odpovídající kryptografické koncové zařízení, musí se nejdříve koncové zařízení u CA zapsat. Proces zapsání obsahuje registraci, inicializaci a certifikaci kryptografického koncového zařízení s uzly v PKI, jako jsou registrační autority a certifikační autority.

Proces zapsání koncového zařízení uvnitř PKI infrastruktury vypadá následovně:

- Kryptografické koncové zařízení se zaregistruje u CA nebo RA. Během tohoto procesu dá k dispozici svou identitu certifikační autoritě. CA autentizuje koncové zařízení, vydá svůj veřejný klíč koncovému zařízení.
- Kryptografické koncové zařízení začne inicializaci generováním veřejného a soukromého klíče (pokud již nebyl tento pár klíčů generován dříve). Veřejný klíč je poslán certifikační autoritě.
- CA podepíše certifikát veřejného klíče vlastním soukromým klíčem a vytvoří tak certifikát pro koncové zařízení
- Kryptografická koncová zařízení můžou nyní požádat o certifikát veřejného klíče od koncového zařízení popsaného výše. K získání příslušného veřejného klíče využijí veřejný klíč certifikační autority, kterým dešifrují certifikát a veřejný klíč tím získají.

4.1.2 Registrační autority

Certifikační autorita provádí v mnoha případech všechny PKI služby potřebné k spravování veřejných klíčů v síti. Existují ale případy, kdy může některé úlohy předat certifikační autorita autoritě registrační (RA). Registrační autorita může zajišťovat například následující služby:

- Ověřování identity kryptografických koncových bodů, které se pokouší používat PKI.
- Generování veřejného klíče a soukromého klíče používaného v inicializační fázi procesu zapsání
- Ověřování kryptografického koncového zařízení, pokoušejícího se zapsat svým veřejným klíčem s CA, že má odpovídající soukromý klíč, který je spjat s udávaným veřejným klíčem
- Nepřímé vydávaní CRL

Ačkoli RA je schopna převzít mnoho funkcí od certifikační autority, RA může pouze CA doplňovat. CA je centrální součástí PKI a je jediným zařízením v PKI, které je schopno podepisovat certifikáty veřejných klíčů od kryptografických koncových zařízení.

4.1.3 Revokační seznam

Revokační seznam sděluje kryptografickým koncovým zařízením, které certifikáty veřejných klíčů již nejsou nadále platné. Tato funkce je důležitá k udržování aktuálních veřejných klíčů, které jsou používány koncovými zařízeními. Veřejné klíče, které jsou periodicky obnovovány, přispívají k větší bezpečnosti a neposkytují útočníkovi mnoho času k získání veřejného klíče.

4.1.4 Certifikační autority

Certifikační autorita představuje centrální zdroj důvěry v PKI. To je způsobeno tím, že CA je jediným prvkem v PKI, který je schopný vydávat certifikáty koncovým zařízením. PKI infrastruktura nemusí mít pouze jednu CA. Více CA může být v PKI uspořádáno hierarchicky podle důvěry nebo mohou být v síti redundantní.

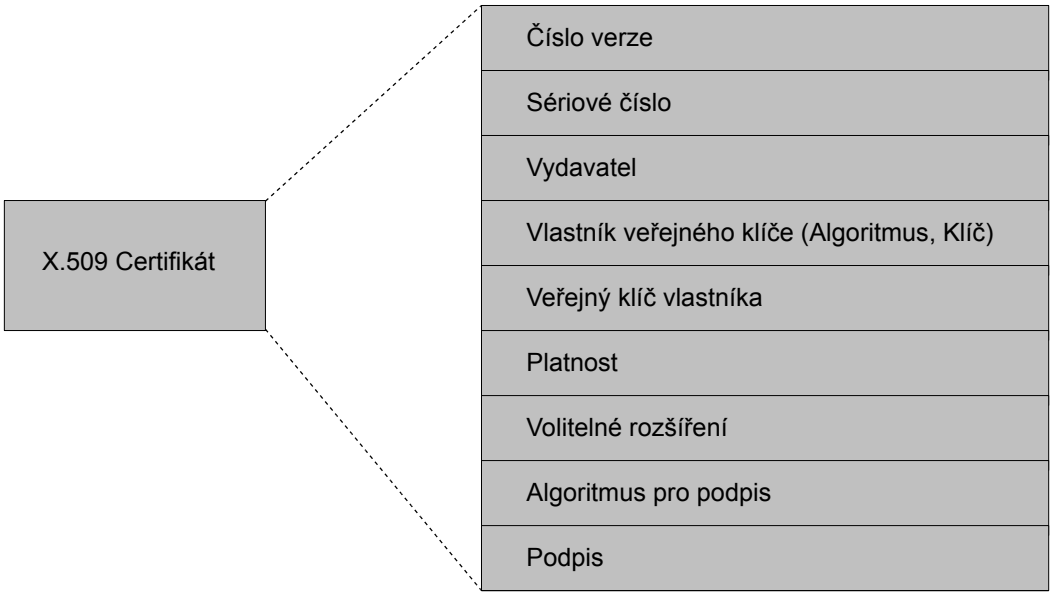
CA je také většinou zodpovědná za udržování CRL a typicky slouží jako CRL vydavatel. Ačkoli může CA vydáváním CRL pověřit jednu nebo více RA, je CA schopna převzít odpovědnost za všechny funkce a RA není v PKI potřeba.

4.1.5 Kryptografická koncová zařízení

PKI byla navržena pro sítě používající asymetrické šifrování a různé druhy kryptografických zařízení. Nejen síťové uzly mohou představovat kryptografické koncové zařízení v PKI. Do této skupiny patří také pracovní stanice, aplikace a další zařízení nacházející se na okraji IP sítě. Tudíž kryptografickým koncovým zařízením může být kterýkoli počítač, server, síťový prvek nebo periferní zařízení, které chce komunikovat s jiným IP kryptografickým zařízením, které je součástí PKI. Taktéž musí být kryptografické koncové zařízení zapsáno u CA v PKI a rovněž je nezbytné, aby bylo schopné získat certifikát veřejného klíče kryptografického koncového zařízení, kterému chce posílat zašifrovaná data.

4.1.6 Certifikáty ITU-T X.509

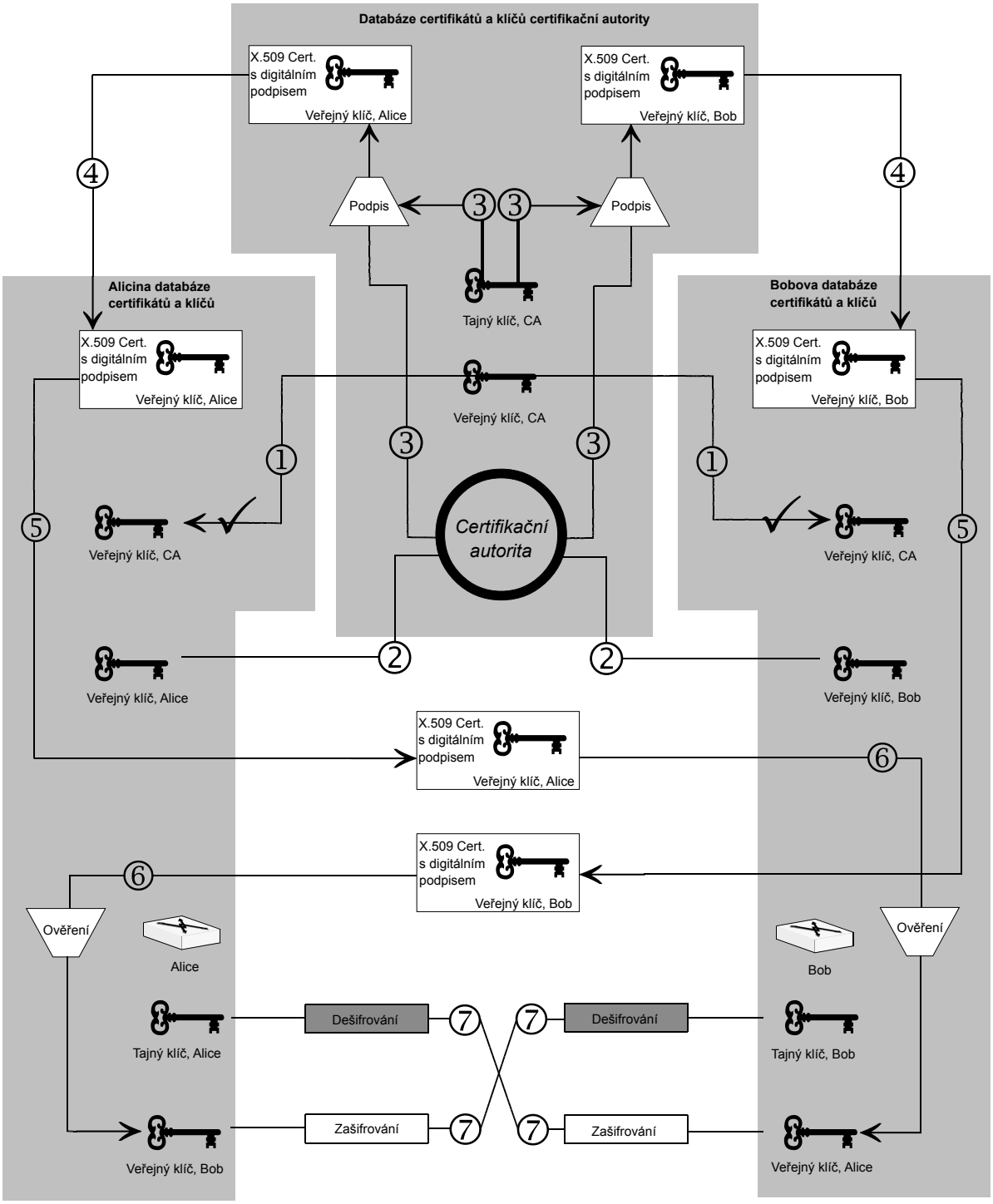
ITU-T X509 certifikáty a certifikační autority byly vyvinuty k zmenšení administrativní zátěže v sítích využívajících asymetrické kryptografie. S využitím centrálního bodu administrace nebo bodu důvěry (Trustpoint - taktéž označovaný jako certifikační autorita) pro registraci veřejných klíčů komunikujících stran. Aby se účinně tyto informace vyměnily, certifikační autorita musí komunikovat certifikáty, které jsou standardizovány. Certifikáty ve formátu ITU-T X509 jsou běžně uznávaným standardem kryptosystému využívající veřejný klíč. Na obrázku 4.1 je vyobrazen certifikát v X. 509 formátu.



Obrázek 4.1:Digitální certifikát[1]

V současné době jsou v sítích využívajících PKI používány certifikáty podle standardu ITU-T X.509v3.

V následujících bodech je popsána komunikace mezi dvěma koncovými zařízeními, využívající pro IKE autentizaci digitálních certifikátů (Obrázek 4.2).

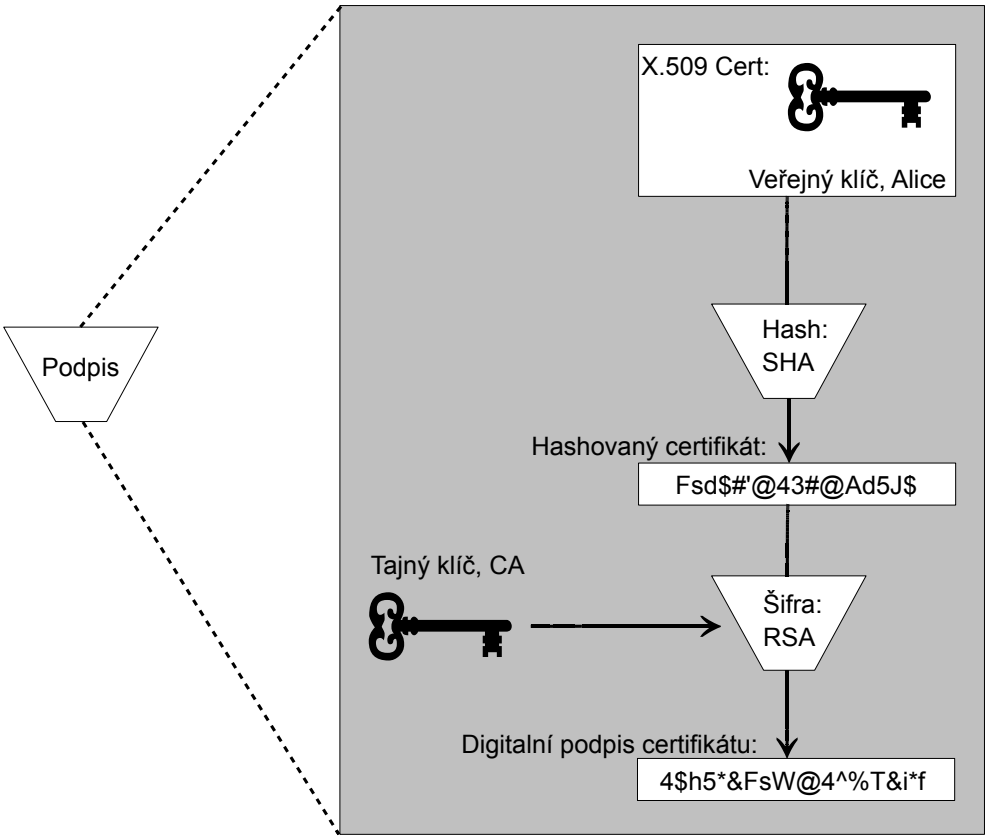


Obrázek 4.2:Funkce certifikační autority[5]

1) Alice a Bob si vyžádají certifikát certifikační autority obsahující její veřejný klíč. Certifikát nainstalují, a taktéž mohou provést kontrolu autenticity certifikační autority.

2) Alice a Bob se zapíši u certifikační autority a pošlou jí své veřejné klíče.

3) Jakmile se Alice a Bob zapíší u certifikační autority, jejich veřejné klíče jsou přijaty a digitálně podepsány soukromým klíčem certifikační autority (Obrázek 4.3). Výsledkem jsou digitální certifikáty veřejných klíčů pro Alici a Boba.

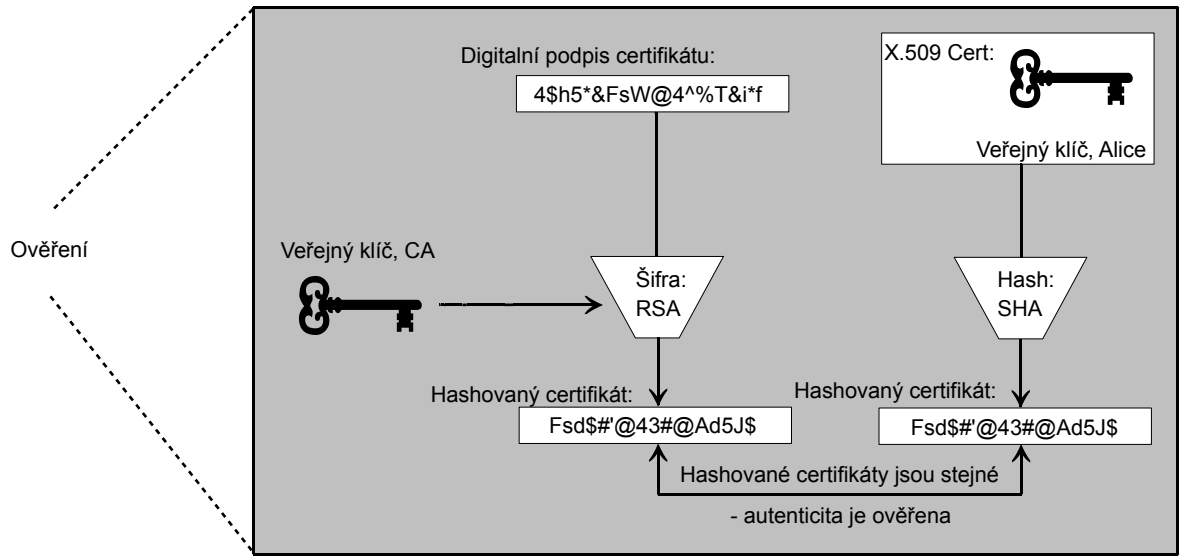


Obrázek 4.3:Digitální podpis [5]

4) CA pošle Alici i Bobovi jejich podepsané certifikáty, které se lokálně uloží u Alice i Boba, a budou později použity pro ISAKMP fázi I.

5) Jestliže chtějí Alice a Bob zahájit navzájem vyjednávání ISAKMP fáze I, vymění si své podepsané certifikáty veřejných klíčů.

6) Oba poté použijí veřejný klíč certifikační autority (obdržený v kroku 1) k ověření digitálního podpisu (vypočítaného v bodě 3) vzájemně vyměněných certifikátů v bodě 5. (Obrázek 4.4)



Obrázek 4.4:Ověření digitálního podpisu[5]

7) Nyní může Alice použít Bobův veřejný klíč a Bob Alicin veřejný klíč k vzájemné šifrované komunikaci. Soukromé klíče zůstaly po celou dobu této výměny v utajení.

Šifrování pomocí RSA podpisů se využívá pouze v případě vytvoření IKE kanálu. V IPSec SA se využívá k šifrování sdíleného tajného hesla vyjednaného přes IKE kanál pomocí Diffie-Hellmanova algoritmu.

Ve výše popsané výměně klíčů, používali Alice s Bobem k zapsání se u CA Simple Certificate Enrollment Protocol (SCEP) definovaný ve standartu X. 509. K distribuování certifikátu je používána klient/server aplikace jako HTTP, FTP nebo LDAP.

5 RAVPN na zařízení Cisco ASA

Platforma Cisco nabízí pro řešení virtuální privátní IPsec sítě se vzdáleným přístupem zařízení, které v sobě spojuje několik síťových prvků (firewall, Intrusion Prevention System, síťové služby - směrování, VPN koncentrátor). Jedná se o model typu ASA, který se vyskytuje v různých označeních v závislosti na jejich výkonu. V našem případě použijeme model typu ASA 5505 [6].

Konfiguraci ASA zařízení je možné provést klasicky přes příkazovou řádku - CLI nebo využít grafického uživatelského rozhraní, které je dostupné přes webové rozhraní. V druhém případě se jedná o Java aplikaci s názvem Cisco Adaptive Security Device Manager (ASDM) [6].

5.1 Topologie sítě

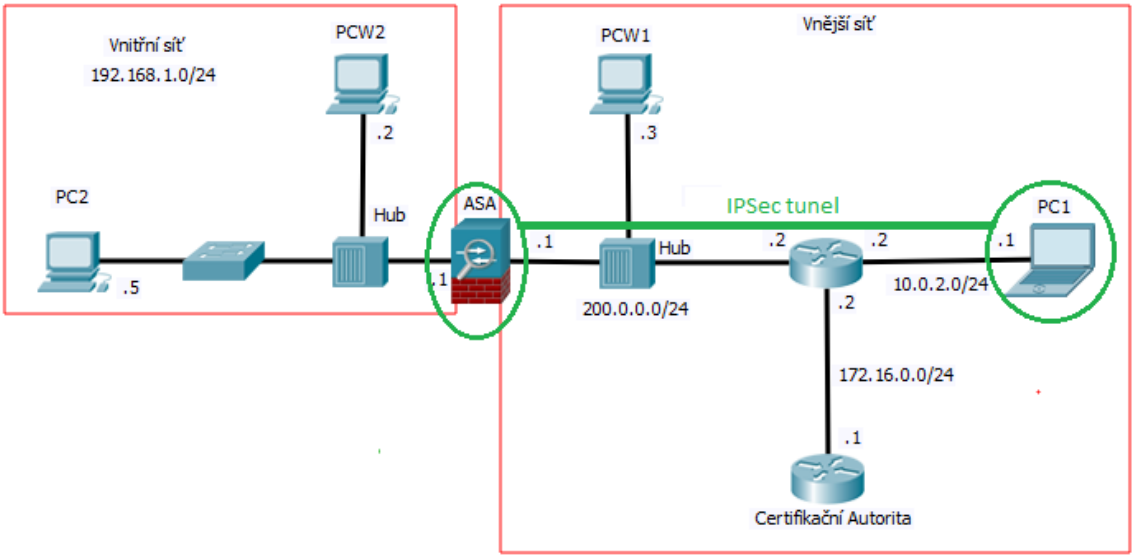
Zapojení síťových zařízení s Cisco VPN koncentrátorem, můžeme vidět na obrázku 5.1. Jedná se o topologii dvou sítí. Vnější sítě a vnitřní sítě, které rozděluje Cisco ASA zařízení. Pracuje jednak jako firewall, ochraňující vnitřní síť před hrozbami přicházejícími z vnější sítě a taktéž umožňuje vzdáleným uživatelům bezpečný přístup do vnitřní sítě.

Pro otestování funkčnosti je ve vnitřní síti umístěn počítač PC2, který bude odpovídat na příkaz ping vzdáleně připojených uživatelů přes Cisco ASA zařízení.

Taktéž je pro funkčnost PKI nakonfigurován Cisco směrovač jako certifikační autorita, vydávající certifikáty pro uživatelé, kteří se chtějí do vnitřní sítě připojit.

Uživatelé mají na svých zařízeních nainstalovaného VPN klienta. V našem případě se jedná konkrétně o aplikaci Cisco VPN Client.

.



Obrázek 5.1: Topologie sítě

5.2 Konfigurace certifikační autority

Pro účely certifikační autority je použit směrovač Cisco řady 2901, na kterém je certifikační autorita nakonfigurovaná a poskytuje ostatním síťovým zařízením své služby, v podobě vydávání digitálních certifikátů [9].

Konfigurace CA s názvem CASERVER

```
Router (config)# crypto pki server CASERVER
```

Specifikace, kde bude databáze certifikační autority uložena a jestli se budou vydávané certifikáty ukládat:

```
Router(cs-server)#database url nvram:
Router(cs-server)#database level minimum
```

Následuje pojmenování vydavatele certifikátu

```
Router(cs-server)#issuer-name CN=CertifikacniAutorita
```

Povolení automatického udělování certifikátů:

```
Router(cs-server)#grant auto
```

Zapnutí certifikační autority:

```
Router(cs-server)#no shutdown
```

A Povolení http serveru:

```
Router (config)# ip http server
```

Pomocí příkazu show crypto pki server CASERVER můžeme provést kontrolu nakonfigurované certifikační autority:

```
CASERVER#show crypto pki server CASERVER
Certificate Server CASERVER:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=CertifikacniAutorita
    CA cert fingerprint: A09773E4 BBD6E324 2EADE7F9 5DDDB0C8
    Granting mode is: auto
    Last certificate issued serial number (hex): 3
    CA certificate expiration timer: 10:09:28 UTC Jun 8 2019
    CRL NextUpdate timer: 16:09:29 UTC Jun 8 2016
    Current primary storage dir: nvram
```

```
    Database Level: Minimum - no cert data written to storage
```

Z výpisu můžeme vyčíst fingerprint (hash), který se shoduje s otiskem při získávání certifikátu pro ASA koncentrátor.

Můžeme také zobrazit certifikát certifikační autority:

```
CASERVER#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CertifikacniAutorita
  Subject:
    cn=CertifikacniAutorita
  Validity Date:
    start date: 10:09:28 UTC Jun 8 2016
    end   date: 10:09:28 UTC Jun 8 2019
  Associated Trustpoints: CASERVER
```

5.3 Konfigurace Cisco ASA 5505

Konfigurace Cisco ASA zařízení v sobě zahrnuje několik nezbytných části. Jedná se o nastavení IP adres na rozhraní, registrace u certifikační autority a nastavení IPsec VPN koncentrátoru.

5.3.1 Nastavení IP adres rozhraní

Cisco ASA disponuje celkem osmi porty. Port 0 slouží k připojení ASA zařízení do vnější sítě. Portů 1-7 se využívá k připojení síťových zařízení ve vnitřní síť. Nastavení IP adres rozhraní se provádí přiřazením určitě VLAN na dané rozhraní [7]. Konfigurace rozhraní je zobrazena na následujících řádcích.

```
ASA (config)#int Vlan1
ASA (config-if)#ip address 192.168.1.1 255.255.255.0
ASA (config-if)#no shutdown
ASA (config-if)#nameif inside
ASA (config)#int Vlan2
ASA (config-if)#ip address 200.0.0.1 255.255.255.0
```

```
ASA (config-if)#no shutdown
ASA (config-if)#nameif outside
ASA (config)#int ethernet 0/0
ASA(config-if)#switchport access Vlan2
ASA (config)#int ethernet 0/1
ASA(config-if)#switchport access Vlan1
```

5.3.2 Registrace u certifikační autority

Aby byla komunikace mezi uživatel z vnější sítě a VPN koncentrátorem úspěšná, musí i Cisco ASA patřit do PKI infrastruktury. Je potřeba tedy provést registraci u certifikační autority a získat podepsaný certifikát, který se využije při sestavování spojení [8, 9, 10].

V prvním kroku je potřeba vygenerovat soukromý a veřejný klíč:

```
ASA (config)# crypto key generate rsa label NovyPar
```

Dále definujeme název certifikační autority, kterou ASA zařízení použije:

```
ASA (config)# crypto ca trustpoint CASERVER
```

Použijeme vytvořený klíč:

```
ASA (config-ca-trustpoint)# keypair NovyPar
```

Pokračujeme nastavením SSL nebo IPsec spojení:

```
ASA (config-ca-trustpoint)# id-usage ssl-ipsec
```

Nastavení specifického jména Cisco ASA zařízení, které bude obsaženo v certifikátu:

```
ASA (config-ca-trustpoint)# subject-name CN=ASA
```

Nastavení IP adresy certifikační autority a portu (Pro použití SCEP protokolu)

```
ASA (config-ca-trustpoint)# enrollment url http://172.16.0.1:80
```

Autentizování certifikační autority (získání certifikátu a veřejného klíče certifikační autority):

```
ASA (config)# crypto ca authentificate CASERVER
```

Zobrazí se nám následující text, kde potvrdíme, že se jedná o správnou certifikační autoritu a přijmeme certifikát. Identifikace certifikační autority je provedena pomoci fingerprintu (hashe) jejího certifikátu.

```
INFO: Certificate has the following attributes:
Fingerprint:     a09773e4 bbd6e324 2eade7f9 5dddb0c8
Do you accept this certificate? [yes/no]: Y
Trustpoint CA certificate accepted.
```

Získání certifikátu pro Cisco ASA zařízení provedeme následujícím příkazem:

```
ASA (config)# crypto ca enroll CA_Server

%
% Start certificate enrollment ..

% The subject name in the certificate will be: CN=ASA

% The fully-qualified domain name in the certificate will be: ASA

% Include the device serial number in the subject name? [yes/no]: n
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
```

Pokud vše proběhne v pořádku, obdržíme potvrzení o získání certifikátu.

```
ASA(config)# The certificate has been granted by CA!
```

Pro ověření a zobrazení certifikátů použijeme následující příkaz:

```
ASA# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 02
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: MD5 with RSA Encryption
  Issuer Name:
    cn=CertifikacniAutorita
  Subject Name:
    hostname=ASA
    cn=ASA
  Validity Date:
    start date: 12:16:50 UTC Jun 8 2016
```

```
    end   date: 12:16:50 UTC Jun 8 2017
  Associated Trustpoints: CASERVER


CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: MD5 with RSA Encryption
  Issuer Name:
    cn=CertifikacniAutorita
  Subject Name:
    cn=CertifikacniAutorita
  Validity Date:
    start date: 10:09:28 UTC Jun 8 2016
    end   date: 10:09:28 UTC Jun 8 2019
  Associated Trustpoints: CASERVER
```

5.3.3 Nastavení VPN koncentrátoru

K úspěšnému vytvoření tunelu mezi ASA zařízením a vzdáleným uživatelem je nutné nastavit několik parametrů, které se využijí k sestavení zabezpečeného spojení.

V prvním kroku je potřeba nastavit parametry IKEv1 protokolu, které se použijí k jeho sestavování. Specifikujeme autentizační metodu, šifrovací algoritmus, hashovací algoritmus, Diffie-Hellmanovu skupinu a životnost tunelu [11]:

```
ASA (config)# crypto ikev1 policy 1
ASA (config-ikev1-policy)# authentication rsa-sig
ASA (config-ikev1-policy)# encryption 3des
ASA (config-ikev1-policy)# hash sha
ASA (config-ikev1-policy)# group 2
ASA (config-ikev1-policy)# lifetime 43200
```

Dále tuto politiku přiřadíme na odchozí rozhraní:

```
ASA(config)# crypto ikev1 outside
```

Následuje nastavení rozsahu adres, které budou dostupné pro vzdáleně připojené uživatele:

```
ASA(config)# ip local pool Adresy 192.168.2.1-192.168.2.20
```

Vytvoření vzdáleného uživatele, kterému bude umožněn přístup do vnitřní sítě:

```
ASA(config)# username baz0007 password 123456
```

Důležité je také nastavit druh šifrovací a autentizační metody pro fázi 2 IKE protokolu:

```
ASA(config)# crypto ipsec ikev1 transform set Prvni esp-3des esp-
          md5-hmac
```

V dalších bodech je nastavena tzv.: tunnel-group (connection profile), kde se definuji politiky a parametry spojení. Typ spojení je nastaven jako vzdálený přístup, je použit námi nakonfigurovaný rozsah adres označený jako Adresy a pro autentizování konců tunelu jsou v protokolu IKEv1 použity digitální certifikáty.

```
ASA(config)# tunnel-group Profil type remote-access
ASA(config)# tunnel-group Profil general-attributes
ASA(config-general)# address-pool Adresy
ASA(config)# tunnel-group Profil ipsec-attributes
ASA (config-ipsec)# ikev1 trust-point CASERVER
```

Aby se mohli do vnitřní sítě připojovat i uživatelé, u kterých neznáme jejich IP adresy, je potřeba vytvořit dynamickou krypto mapu se specifikovanými IKEv1 parametry:

```
ASA (config)# crypto dynamic-map Mapa1 1 set ikev1 transform-set
          Prvni
```

Následuje vytvoření krypto mapy, která umožní VPN koncentrátoru použití vytvořené dynamické krypto mapy a její umístění na rozhraní:

```
ASA (config)# crypto map Mapa2 1 ipsec-isakmp dynamic Mapa1
ASA (config)# crypto map Mapa2 interface outside
```

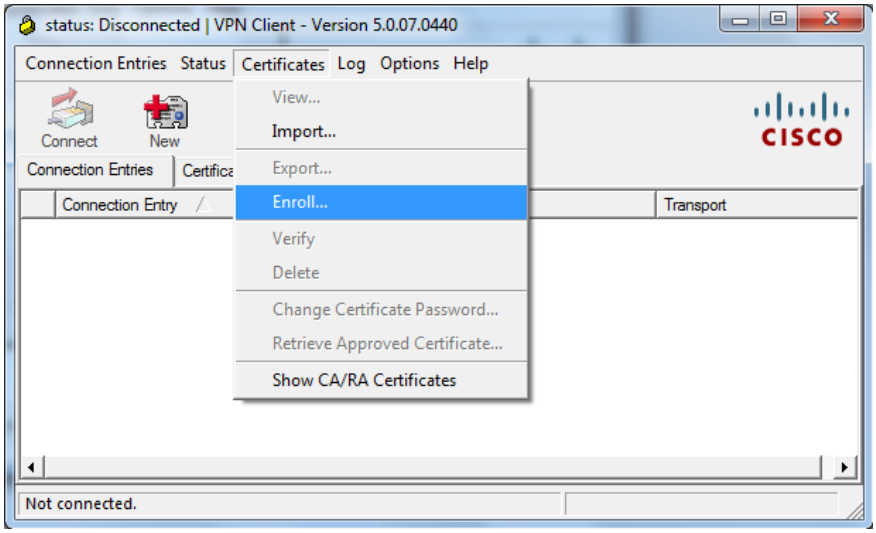
Jelikož používáme k autentizování digitální certifikáty, je potřeba vytvořit pravidla pro mapování certifikátu vzdáleného uživatele na správnou tunnel-group s využitím atributů položek v certifikátu. Pokud by nebyla vytvořena, použila by se defaultní pravidla DefaultCertificateMap [12].

```
ASA (config)#crypto ca certificate map CertMap 1
ASA (ca-certificate-map)# subject-name attr o eq vsb
ASA (config)#tunnel-group-map enable rules
ASA (config)#tunnel-group-map CertMap 1Profil
```

5.4 Nastavení Cisco VPN klienta

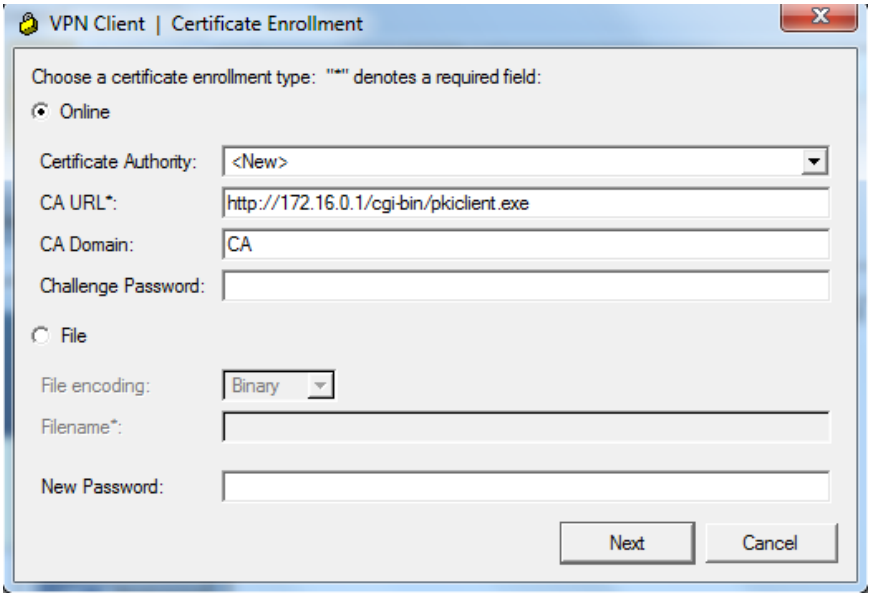
K připojení se na Cisco ASA zařízení a k vytvoření tunelu je použit VPN Cisco Client verze 5.0.07.0290 [13]. V následujících krocích je popsána konfigurace zmiňovaného klienta.

V prvním kroku je potřeba získat certifikát od certifikační autority. Postup je vyobrazen na obrázcích 5.2 až 5.4:



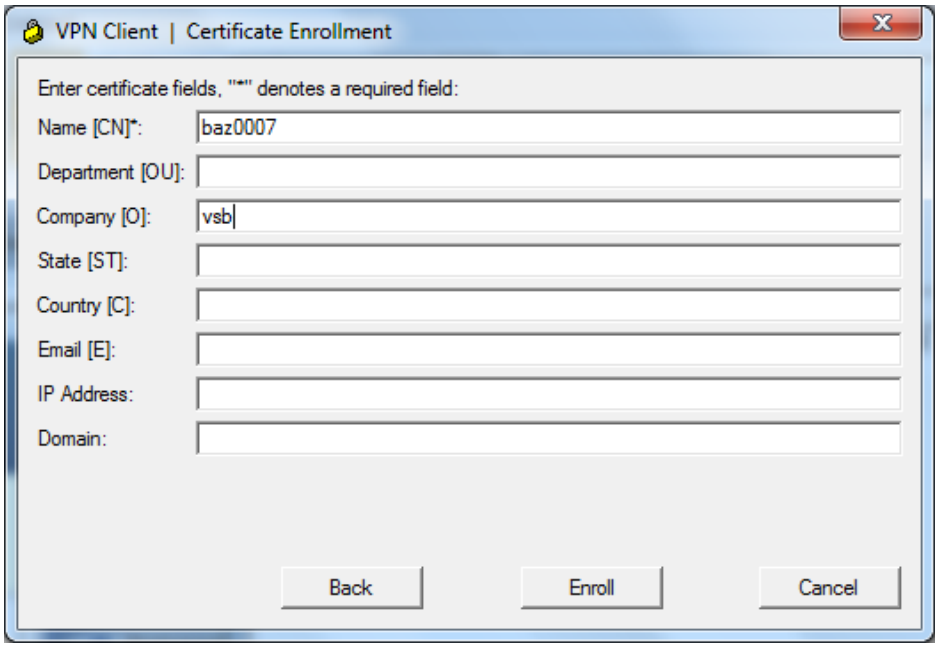
Obrázek 5.2:Získání certifikátů pomocí SCEP protokolu, krok 1

V tomto kroku je potřeba nastavit příslušnou adresu CA serveru a jeho doménu:



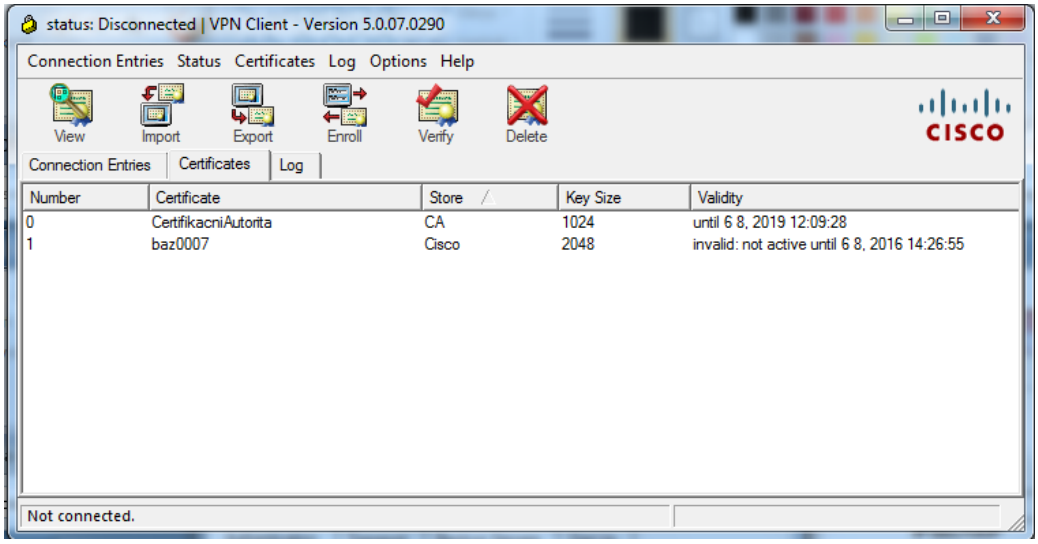
Obrázek 5.3:Získání certifikátů pomocí SCEP protokolu, krok 2

Následuje vypsání položek certifikátů. Není povinné vyplňovat všechny atributy, avšak je potřeba vyplnit jméno. V našem případě je ještě nastavena položka firma, která se kontroluje v ASA zařízení při realizaci tunelu:



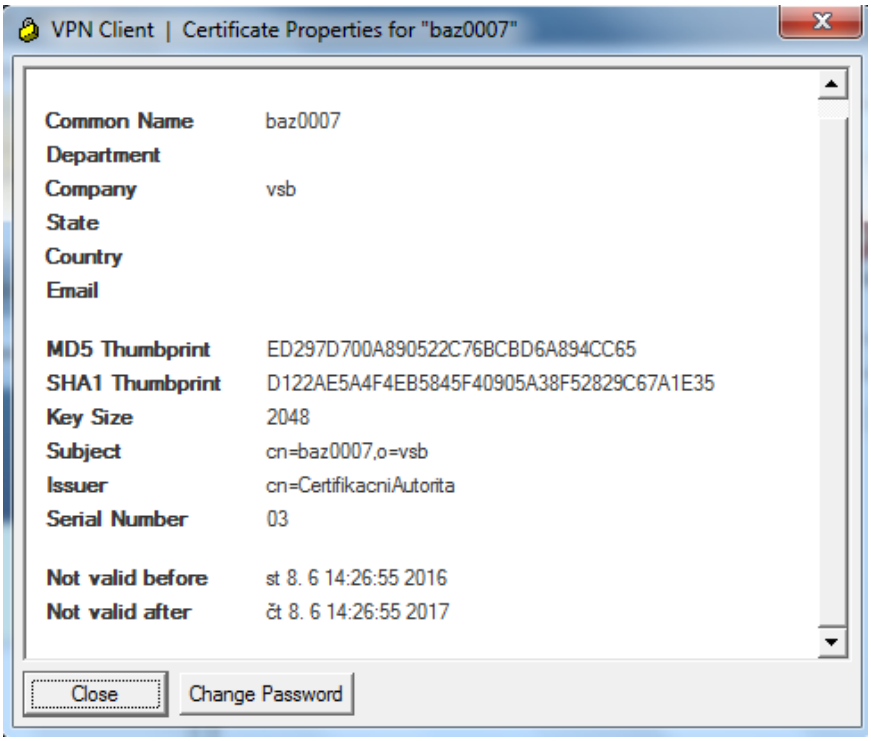
Obrázek 5.4:Získání certifikátů pomocí SCEP protokolu, krok 3

V záložce Certificates můžeme poté vidět udělené certifikáty (Obrázek 5.5). Konkrétně certifikát certifikační autority a osobní certifikát:



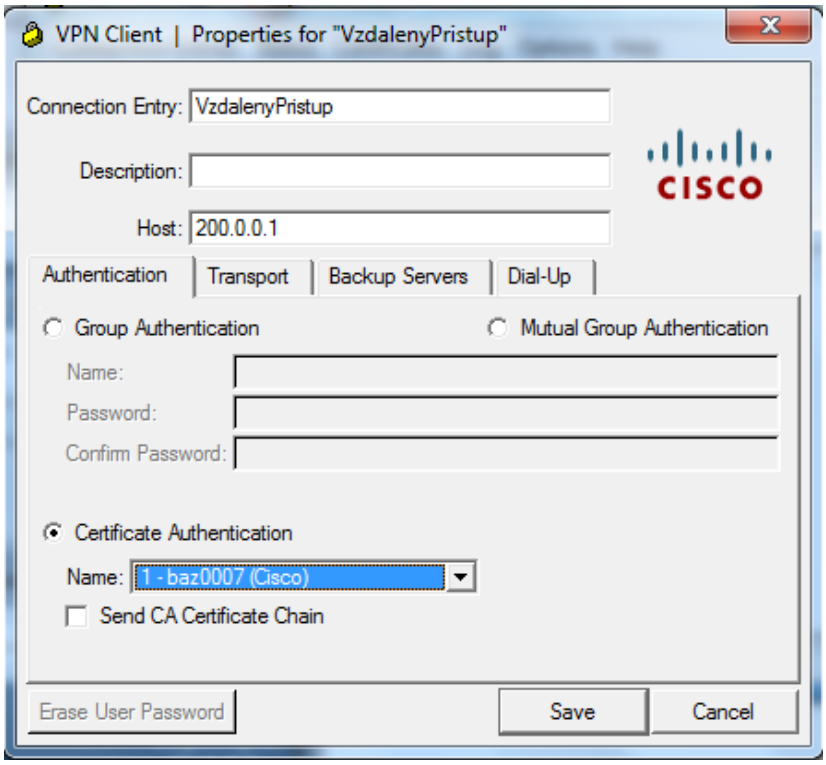
Obrázek 5.5:Dostupné certifikáty

Po rozkliknutí jednotlivých položek, můžeme vidět detaily dílčích certifikátů (viz Obrázek 5.6).



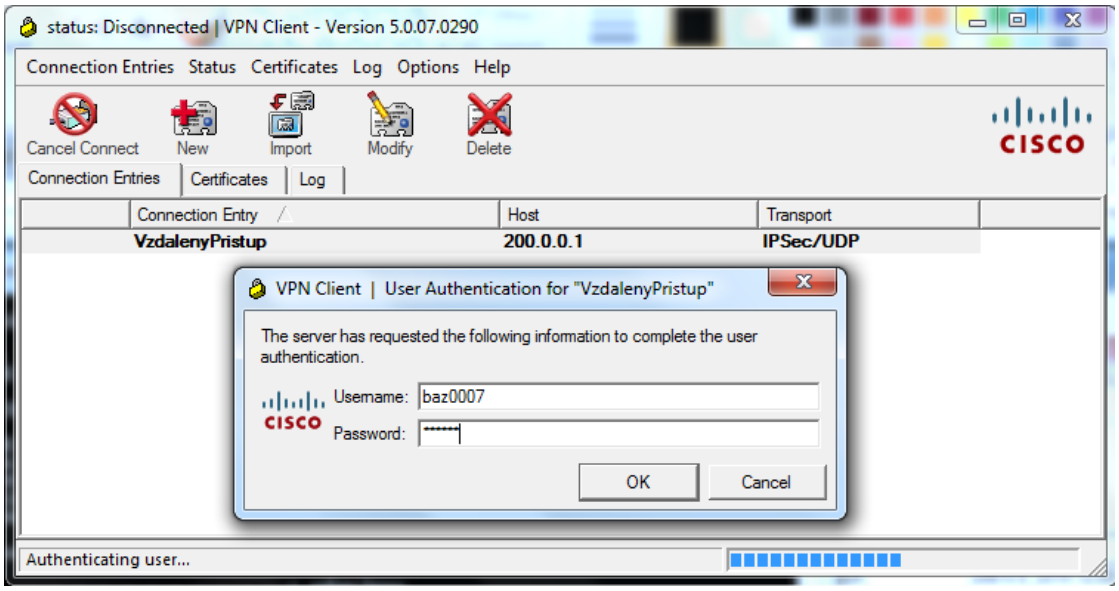
Obrázek 5.6: Udělený osobní certifikát

A poté již následuje vytvoření nového spojení. Je potřeba vyplnit IP adresu rozhraní Cisco ASA připojeného do vnější sítě a vybrat ověřování pomocí certifikátu. V rolovacím seznamu vybereme získaný osobní certifikát udělený certifikační autoritou (viz Obrázek 5.7).



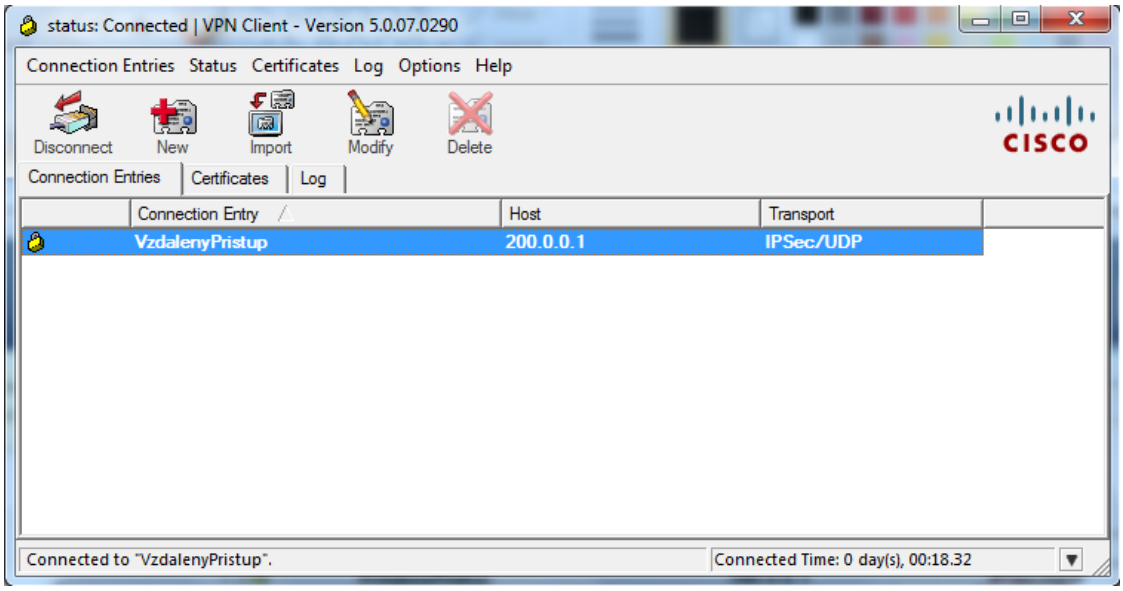
Obrázek 5.7: Vytvoření spojení

Pro úspěšné připojení je ještě potřeba se autentizovat vůči databázi uživatelů ve VPN koncentrátoru (viz Obrázek 5.8).



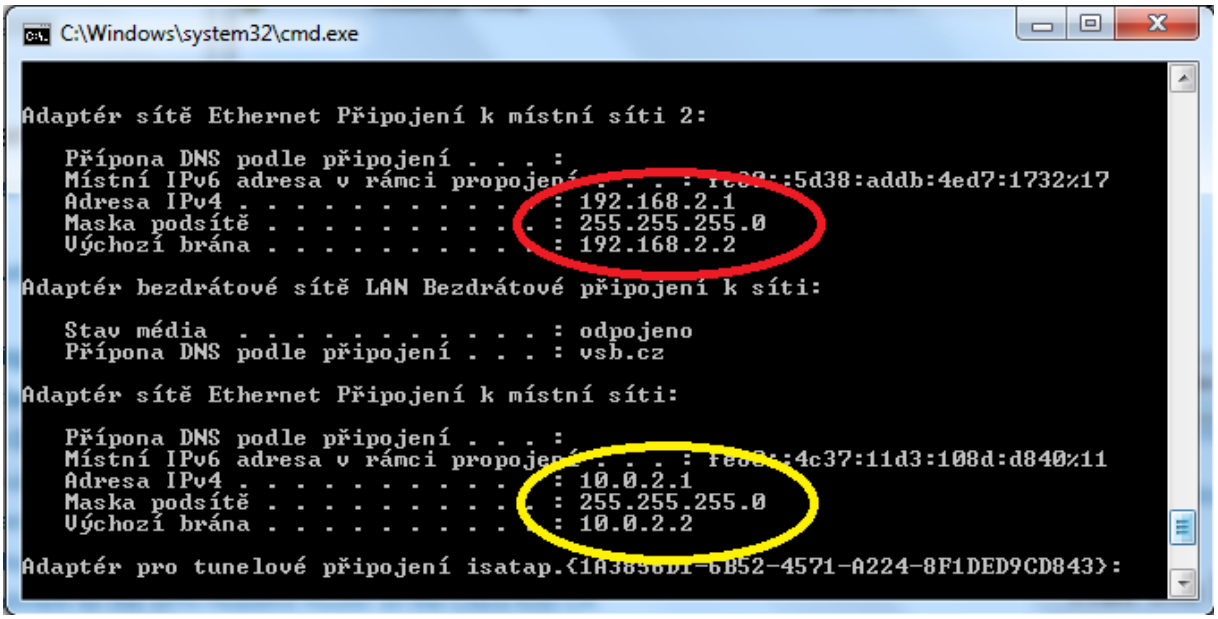
Obrázek 5.8:Autentizace uživatele

Po úspěšném připojení ke koncentrátoru se nám zobrazí následující okno (viz Obrázek 5.9) a bezpečné připojení do privátní sítě je uskutečněno.



Obrázek 5.9:Úspěšné připojení do vzdálené sítě

Kontrolu přirazené adresy provedeme pomocí příkazu ipconfig v příkazové řádce. Červeně je označená IP adresa přidělená VPN koncentrátorem po připojení do privátní sítě. Žlutě je označena fyzická IP adresa PC1(viz Obrázek 5.10).



Obrázek 5.10: IP adresy PC1

5.5 Kontrola IPsec tunelu v zařízení Cisco ASA

Na následujících výpisech můžeme vidět výpisy vlastností vytvořeného IPsec tunelu v zařízení Cisco ASA. K jejím zobrazením je použito několik příkazů v Cisco IOS.

Na zkráceném výpisu pomocí příkazu `show ipsec sa` (celý výpis lze vidět v příloze C diplomové práce), můžeme vidět vlastnosti vytvořeného IPsec tunelu. Lze vyčíst IP adresu vzdáleného uživatele - 10.0.2.1, jemu přiřazenou IP adresu od VPN koncentrátoru - 192.168.2.1, označení SPI příchozího a odchozího SA. Taktéž je možné vidět typ zapouzdření.

```
interface: outside
    Crypto map tag: Mapa1, seq num: 1, local addr: 200.0.0.1
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port):
(192.168.2.1/255.255.255.255/0/0)
      current_peer: 10.0.2.1, username: baz0007
      dynamic allocated peer ip: 192.168.2.1
      dynamic allocated peer ip(ipv6): 0.0.0.0
      local crypto endpt.: 200.0.0.1/0, remote crypto endpt.:
10.0.2.1/0
    inbound esp sas:
      spi: 0x665BED98 (1717300632)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel, IKEv1, }
```

```
         slot: 0, conn_id: 61440, crypto-map: Mapa1
    outbound esp sas:
      spi: 0x47680B75 (1198001013)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel, IKEv1, }
```

V následujícím výpisu pomocí příkazu `show isakmp` si můžeme povšimnout počtu připojených uživatelů (počet vytvořených IKEv1 spojení k VPN koncentrátoru), jejich IP adresy a zkrácený výpis informací o vytvořeném tunelu.

```
ASA(config)# show isakmp
IKEv1 SAs:

   Active SA: 1
Total IKE SA: 1

1   IKE Peer: 10.0.2.1
    Type    : user            Role    : responder
    Rekey   : no              State   : MM_ACTIVE
Global IKEv1 Statistics
  Active Tunnels:              1
  Previous Tunnels:           12
  In Octets:               69372
  In Packets:                377
  In Drop Packets:            14
  In Notifys:                243
  In P2 Exchanges:            12
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    8
  Out Octets:              42936
  Out Packets:               344
  Out Drop Packets:            0
```

5.6 Analýza IPsec provozu v aplikaci Wireshark

Pomocí protokolového síťového analyzátoru Wireshark, které je spuštěn na PCW1 a PCW2 (viz Obrázek 5.1), je zachycen provoz mezi VPN klientem a VPN koncentrátorem. Na odchyceném provozu v PCW1 je zobrazen průběh vytváření IPsec tunelu (viz Obrázek 5.11)

No.	Time	Source	Destination	Protocol	Length	Info
4	1.755467000	10.0.2.1	200.0.0.1	ISAKMP	1202	Identity Protection (Main Mode)
5	1.757362000	200.0.0.1	10.0.2.1	ISAKMP	170	Identity Protection (Main Mode)
6	1.773877000	10.0.2.1	200.0.0.1	ISAKMP	330	Identity Protection (Main Mode)
7	1.777024000	200.0.0.1	10.0.2.1	ISAKMP	384	Identity Protection (Main Mode)
8	1.835394000	10.0.2.1	200.0.0.1	ISAKMP	590	Identity Protection (Main Mode) (Message fragment 1)
9	1.835411000	10.0.2.1	200.0.0.1	ISAKMP	590	Identity Protection (Main Mode) (Message fragment 2)
10	1.835413000	10.0.2.1	200.0.0.1	ISAKMP	98	Identity Protection (Main Mode) (Message fragment 3 - last)
11	1.875855000	200.0.0.1	10.0.2.1	ISAKMP	338	Identity Protection (Main Mode) (Message fragment 2 - last)
12	1.875872000	200.0.0.1	10.0.2.1	ISAKMP	590	Identity Protection (Main Mode) (Message fragment 1)
13	2.869588000	200.0.0.1	10.0.2.1	ISAKMP	118	Transaction (Config Mode)
14	7.342794000	10.0.2.1	200.0.0.1	ISAKMP	134	Transaction (Config Mode)
15	7.345772000	200.0.0.1	10.0.2.1	ISAKMP	110	Transaction (Config Mode)
16	7.348881000	10.0.2.1	200.0.0.1	ISAKMP	102	Transaction (Config Mode)
17	7.359839000	10.0.2.1	200.0.0.1	ISAKMP	230	Transaction (Config Mode)
18	7.361664000	200.0.0.1	10.0.2.1	ISAKMP	214	Transaction (Config Mode)
19	7.377093000	10.0.2.1	200.0.0.1	ISAKMP	1070	Quick Mode
20	7.377103000	200.0.0.1	10.0.2.1	ISAKMP	134	Informational
21	7.380929000	200.0.0.1	10.0.2.1	ISAKMP	238	Quick Mode
22	7.380946000	10.0.2.1	200.0.0.1	ISAKMP	94	Quick Mode

Obrázek 5.11: Vytváření IPsec tunelu

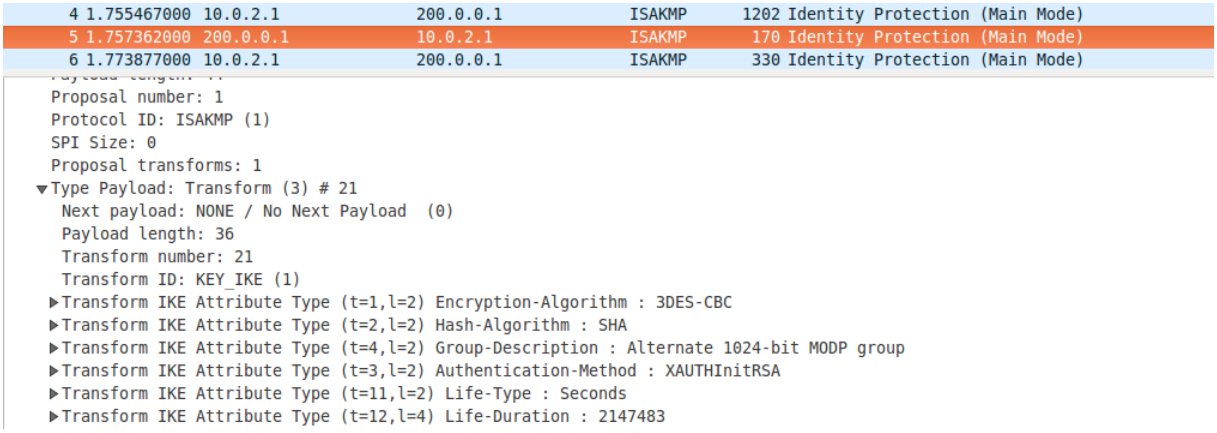
Pokud provedeme analýzu první zprávy vytváření IPSec tunelu, kterou iniciuje Cisco VPN klient, povšimneme si, že klient nabízí až 26 různých kombinací pro zabezpečení komunikace (viz Obrázek 5.12).

```
    4 1.755467000 10.0.2.1          200.0.0.1          ISAKMP    1202 Identity Protection (Main Mode)
    5 1.757362000 200.0.0.1         10.0.2.1           ISAKMP     170 Identity Protection (Main Mode)
    6 1.773877000 10.0.2.1          200.0.0.1          ISAKMP     330 Identity Protection (Main Mode)

  ▶ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ▶ Transform IKE Attribute Type (t=12,l=4) Life-Duration : 2147483
  ▼ Type Payload: Transform (3) # 26
      Next payload: NONE / No Next Payload  (0)
      Payload length: 36
      Transform number: 26
      Transform ID: KEY_IKE (1)
    ▶ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : DES-CBC
    ▶ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
    ▶ Transform IKE Attribute Type (t=4,l=2) Group-Description : Default 768-bit MODP group
    ▶ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : RSA-SIG
    ▶ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
    ▶ Transform IKE Attribute Type (t=12,l=4) Life-Duration : 2147483
▼ Type Payload: Vendor ID (13) : XAUTH
    Next payload: Vendor ID (13)
    Payload length: 12
```

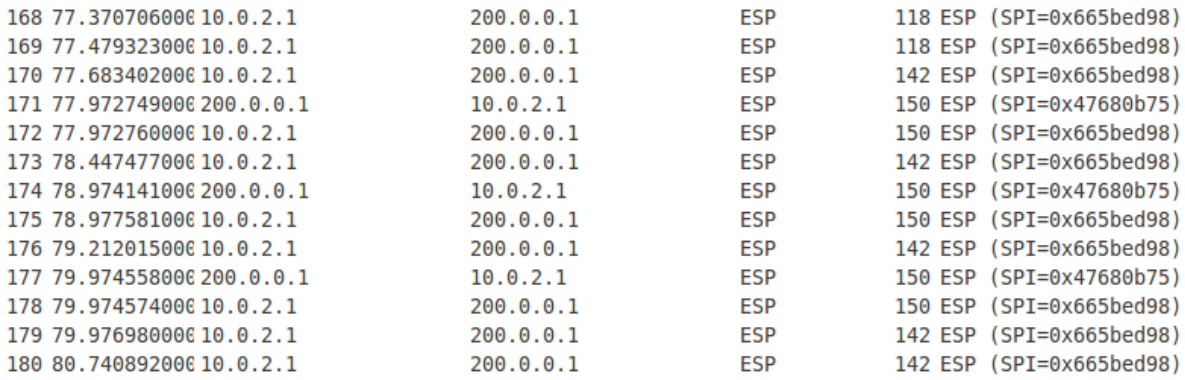
Obrázek 5.12: Analýza vytváření IPSec spojení

ASA zařízení si vybere odpovídající zabezpečení (viz Obrázek 5.13) podle toho, jak je nastavena bezpečnostní politika v kapitole 5.3.3. Vidíme tedy, že je vybrána kombinace číslo 21 a odpovídá námi nastavené bezpečnostní politice.



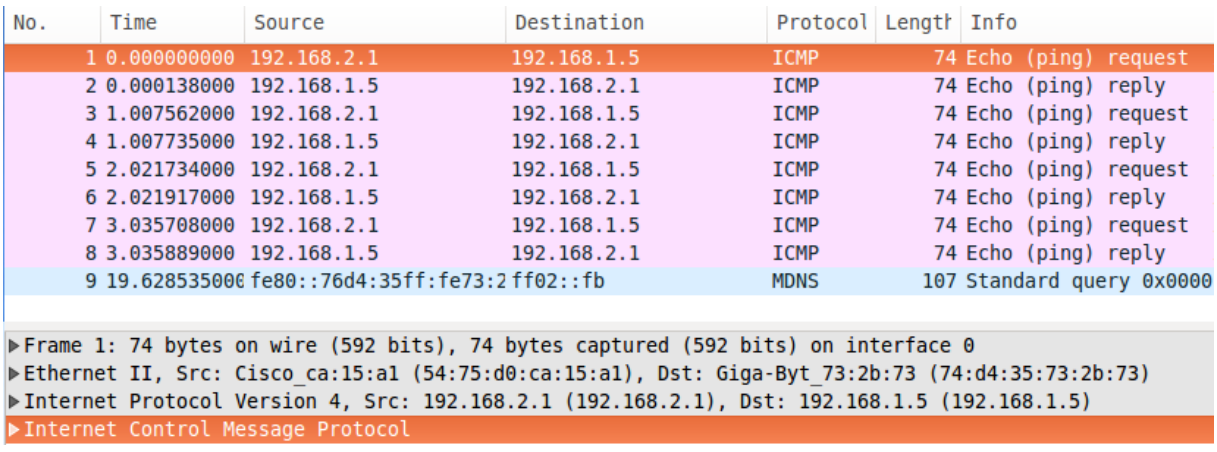
Obrázek 5.13: Analýza vytváření IPSec spojení

Vygenerujeme-li nějaký provoz z PC1 do privátní sítě za VPN koncentrátorem, uvidíme, že provoz je zabezpečený ESP protokolem a označení SPI odpovídá označením ve výpisu z kapitoly 5.5. (viz Obrázek 5.14).



Obrázek 5.14: Zachycený šifrovaný provoz

Provedením analýzy paketů na PCW2 uvidíme, pod jakou adresou probíhá komunikace ve vnitřní sítí po odšifrování paketů. Z výpisu lze vidět IP adresu 192.168.2.1, kterou přidělil VPN koncentrátor VPN klientu (viz Obrázek 5.15).



Obrázek 5.15: Provoz ve vnitřní síti

6 RAVPN na směrovači Cisco řady 2800

Vzdálené bezpečné připojení do privátní sítě přes nedůvěryhodnou síťovou infrastrukturu, lze realizovat taktéž pomocí směrovače, který vystupuje v roli VPN koncentrátoru. V tomto případě bude jako VPN koncentrátor sloužit směrovač firmy Cisco řady 2800.

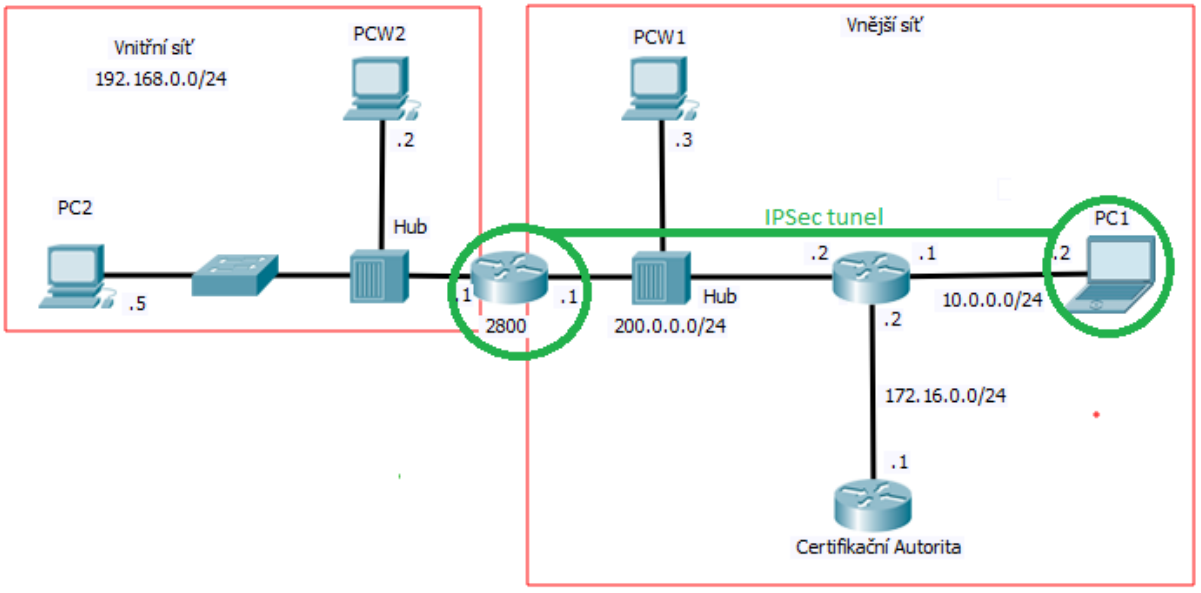
Jako v případě Cisco ASA zařízení, i v tomto případě můžeme provést konfiguraci pomocí příkazové řádky nebo využít možnosti grafického rozhraní a použít Security Device Manager (SDM).

6.1 Topologie sítě

Topologie testované sítě se podobá konfiguraci sítě v prvním případě, kdy jako VPN brána sloužilo ASA zařízení. V tomto řešení vystupuje jako VPN koncentrátor směrovač Cisco řady 2800, rozdělující vnitřní a vnější síť. Ostatní části sítě zůstávají stejné. K vydávání certifikátů je k dispozici certifikační autorita provozována na směrovači Cisco řady 2901 a sledování provozu je k dispozici pomocí počítačů PCW1 a PCW2 připojených do hubů (Obrázek 6.1).

Uživatelé, konkrétně uživatel na PC1 má na svém zařízení nainstalovaného VPN klienta. V našem případě se opět jedná o VPN klienta firmy Cisco.

Pro kontrolu vytvořeného IPSec tunelu je proveden příkaz ping z počítače PC1 na počítač PC2, který je umístěn v privátní síti.



Obrázek 6.1:Schéma zapojení se směrovačem Cisco řady 2800

6.2 Konfigurace certifikační autority

Stejné jako v minulém případě, i zde je nakonfigurována certifikační autorita na směrovači Cisco řady 2901. Konfigurace je totožná s konfigurací z minulého případu s tím rozdílem, že se liší její certifikát a fingerprint, kvůli nového spuštění certifikační autority.

Fingerprint neboli otisk vypadá tedy následovně:

```
CASERVER#show crypto pki server CASERVER
Issuer name: CN=CertifikacniAutorita
    CA cert fingerprint: 408B8E88 EE2B4C3C 87CBAC39 AA236268
```

Certifikát se příliš nezměnil. Změny doznala pouze platnost certifikátu:

```
CASERVER#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CertifikacniAutorita
  Subject:
    cn=CertifikacniAutorita
  Validity Date:
    start date: 10:23:55 UTC Jun 20 2016
    end   date: 10:23:55 UTC Jun 20 2019
  Associated Trustpoints: CASERVER
```

6.3 Konfigurace směrovače Cisco 2800

Pro úspěšné vytvoření zabezpečeného tunelu, je potřeba několik kroků k nastavení směrovače Cisco. Do určité míry je konfigurace podobná s konfigurací Cisco ASA zařízení, nicméně jsou při nastavovaní směrovače řady 2800 patrné odlišnosti.

6.3.1 Nastavení autentizace uživatele

Pro autentizování a autorizaci uživatelů bude použita místní databáze ve směrovači. V první řadě je potřeba vytvořit nový 'aaa model' (autentizace, autorizace, účtování), který poskytuje metodu pro identifikování uživatelů přihlašujících se do směrovače a následně jim umožňuje přístup k různým síťovým zdrojům.

```
Cisco_2800(config)#aaa new-model
Cisco_2800(config)#aaa authentication login VPN local
Cisco_2800(config)#aaa authorization network VPN local
```

Vytvoříme i uživatele, kterému bude dovolen přístup do vnitřní sítě:

```
Cisco_2800(config)#username baz0007 password 0 cisco
```

6.3.2 Registrace u certifikační autority a získání certifikátů

Podobně jako v případě ASA zařízení, je potřeba i u směrovače provést konfiguraci certifikační autority, od které získáme potřebné certifikáty.

Nejprve je tedy potřeba vygenerovat soukromý a veřejný klíč:

```
Cisco_2800(config)# crypto key generate rsa label NovyPar
```

V dalším kroku nakonfigurujeme důvěrnou certifikační autoritu pojmenovanou CASERVER, se kterou bude směrovač komunikovat:

```
Cisco_2800 (config)#crypto pki trustpoint CASERVER
```

Nastavíme port a IP adresu certifikační autority, na které s ní budeme pomocí SCEP protokolu komunikovat:

```
Cisco_2800 (ca-trustpoint)# enrollment url http://172.16.0.2:80
```

Dále nastavíme název směrovače Cisco, který bude zahrnut ve vydaném certifikátu:

```
Cisco_2800 (ca-trustpoint)# subject-name CN=Cisco
```

Umožníme použití klíčů s názvem NovyPar, které jsme vytvořili:

```
Cisco_2800 (ca-trustpoint)# rsakeypair NovyPar
```

V posledním případě specifikujeme použití certifikátu, v našem případě bude certifikát sloužit pro IKE protokol

```
Cisco_2800 (ca-trustpoint)# usage ike
```

Nyní už můžeme požádat certifikační autoritu o osobní certifikát a certifikát certifikační autority. Posledně jmenovaný získáme pomocí příkazu `crypto ca authenticate <název certifikační autority>`:

```
Cisco_2800 (config)#crypto ca authenticate CASERVER

Certificate has the following attributes:
       Fingerprint MD5: 408B8E88 EE2B4C3C 87CBAC39 AA236268
      Fingerprint SHA1: 4FEB3E75 9C8F0B5E 0778AE55 096623AE 31DCDBD1
```

Zkontrolujeme, zda souhlasí vypsaný fingerprint s otiskem certifikátu certifikační autority (viz. kapitola 6.2) a certifikát přijmeme:

```
% Do you accept this certificate? [yes/no]: y
```

Následuje již hláška o uspěšném získání certifikátu:

```
Trustpoint CA certificate accepted.
```

O osobní certifikát požádáme příkazem `crypto ca enroll <název certifikační autority>:`

```
Cisco_2800 (config)#crypto ca enroll CASERVER
%
% Start certificate enrollment ..
Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
Jun 20 13:54:02.811: %PKI-6-CERTRET: Certificate received from
Certificate Authority
```

Po úspěšném získání certifikátů můžeme opět provést jejich výpis příkazem `show crypto pki certificates`. Certifikáty se příliš neliší od certifikátů v ASA zařízení a jsou dostupné v příloze D diplomové práce.

6.3.3 Nastavení VPN brány

V této podkapitole bude ukázáno už samotné nastavení VPN brány, nastavení parametrů tunelu, politik a konfigurace dalších nezbytných součástí pro úspěšné vytvoření zabezpečeného tunelu.

V prvním kroku definujeme bezpečnosti politiku ISAKMP, nebo-li parametrů, které se použijí při fázi 1 IKE protokolu. Provedeme nastavení šifrování (AES), hashovacího algoritmu (SHA), způsobu autentizace (digitální certifikáty) a skupiny Diffie-Hellmanova algoritmu:

```
Cisco_2800 (config)#crypto isakmp policy 1
Cisco_2800 (config-isakmp)#encryption   aes
Cisco_2800 (config-isakmp)#authentication rsa-sig
Cisco_2800 (config-isakmp)#hash sha
Cisco_2800 (config-isakmp)#group 2
```

Pro vzdáleně připojené uživatele definujeme IP adresy, které jim budou automaticky přiděleny. Nakonfigurujeme tedy rozsah adres pomocí následujícího příkazu:

```
Cisco_2800 (config)#ip local pool VPNAdresy 192.168.2.1 192.168.2.30
```

Dále definujeme Access list, který nám zajistí dostupnost sítě za VPN bránou:

```
Cisco_2800(config)# ip access-list extended VPNACL
Cisco_2800(config-ext-nacl)#permit ip 192.168.0.0 0.0.0.255
192.168.2.0 0.0.0.255
```

Nyní nakonfigurujeme zapouzdření, šifrování a hashovací algoritmus, který se využije u fáze 2 IKE protokolu. V tomto případě šifra AES a hash SHA :

```
Cisco_2800(config)# crypto ipsec transform-set T1 esp-aes 256 esp-
sha-hmac
```

Vytvoříme dynamickou krypto mapu, které přiřadíme námi vytvořené parametry pro fázi 2 IKE protokolu a parametr reverse-route, který přidá statickou cestu k vzdálené síti do směrovací tabulky:

```
Cisco_2800(config)# crypto dynamic-map DYNMAP 10
Cisco_2800 (config-crypto-map)# set transform-set T1
Cisco_2800 (config-crypto-map)# reverse-route
```

Dále vytvoříme krypto mapu, kde povolíme dotazování IKE protokolu pro autentizaci, povolíme směrovači přijímání požadavku o IP adresu od kteréhokoliv uzlu a přiřadíme dynamickou kryptomapu:

```
Cisco_2800(config)# crypto map VPN client authentication list VPN
Cisco_2800(config)# crypto map VPN isakmp authorization list VPN
Cisco_2800(config)# crypto map VPN client configuration address
respond
Cisco_2800(config)# crypto map VPN 10 ipsec-isakmp dynamic DYNMAP
```

V dalším kroku definujeme skupinu s názvem VPNSKUPINA, kde nakonfigurujeme rozsah adres přidělovaný vzdáleným uživatelům a access control list, zajišťující přístup do vnitřní sítě:

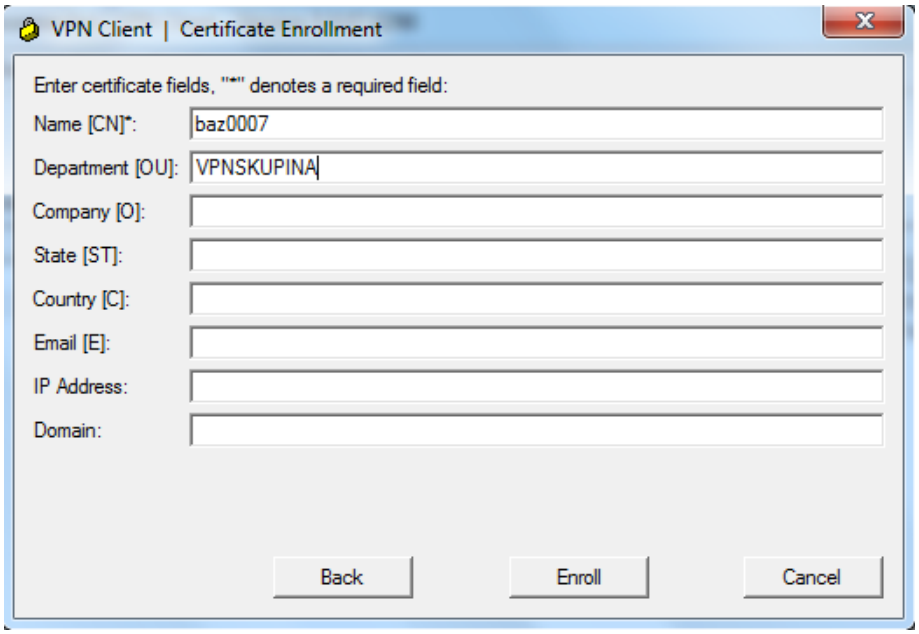
```
Cisco_2800(config)# crypto isakmp client configuration group
VPNSKUPINA
 Cisco_2800 (config-isakmp-group)#pool VPNAdresy
 Cisco_2800 (config-isakmp-group)#acl VPNACL
```

V posledním kroku přiřadíme vytvořenou krypto mapu na rozhraní ve vnější síti:

```
Cisco_2800(config)#  interface FastEthernet0/1
Cisco_2800(config-if)#crypto map VPN
```

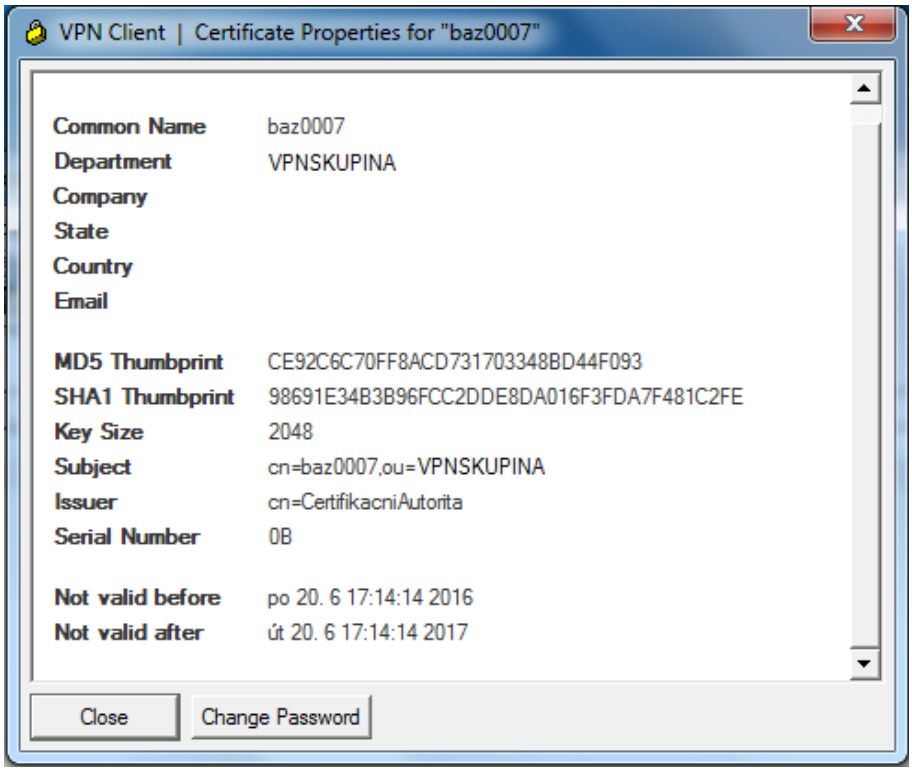
6.4 Nastavení Cisco VPN klienta

Nastavení Cisco VPN klienta probíhá ve stejných krocích jako v případě nastavení pro připojení k ASA zařízení. Získáme certifikáty pomocí SCEP protokolu, nastavíme adresu VPN koncentrátoru, povolíme autentizaci pomocí certifikátu a vyplníme přihlašovací údaje (viz Obrázek 5.7). Jediná změna se nachází při vyplňování údajů, které budou obsaženy v certifikátu. Do kolonky ou vepíšeme název skupiny, kterou jsme vytvořili na směrovači Cisco 2800 a to VPNSKUPINA (viz Obrázek 6.2)



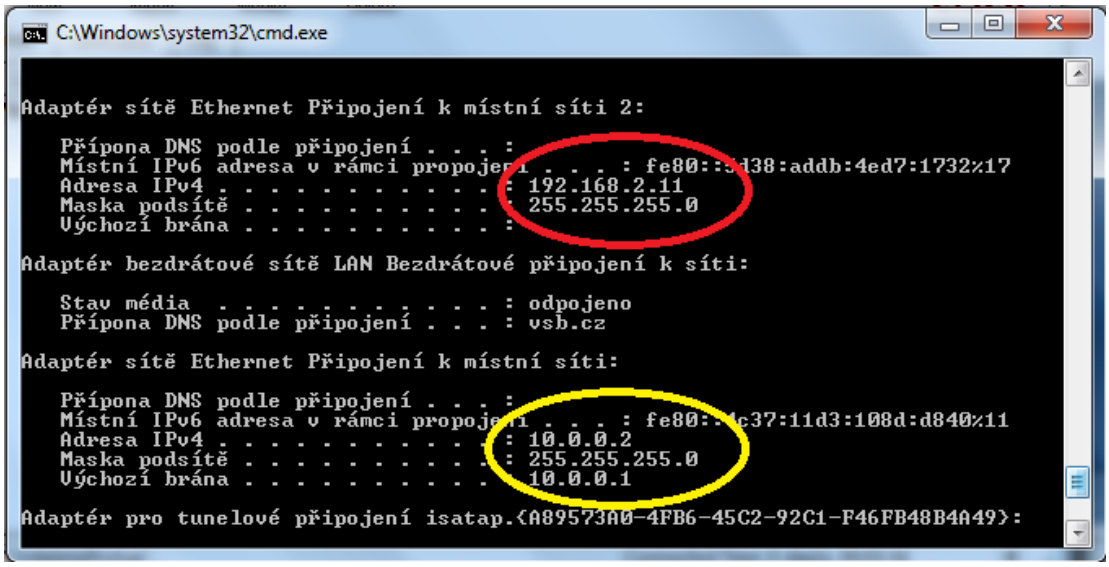
Obrázek 6.2:Nastavení položek osobního certifikátu

Udělený osobní certifikát bude vypadat následovně (viz Obrázek 6.3):



Obrázek 6.3: Udělený certifikát

Kontrolu přirazené adresy provedeme pomocí příkazu ipconfig v příkazové řádce (viz Obrázek 6.4). Červeně je označená IP adresa přidělená VPN koncentrátorem po připojení do privátní sítě. Žlutě je označena fyzická IP adresa PC1.



Obrázek 6.4:Kontrola IP adres

6.5 Kontrola IPsec tunelu v zařízení Cisco řady 2800

Stejné jako v Cisco ASA zařízení, jsou i ve směrovači Cisco řady 2800 dostupné příkazy pro zobrazení parametrů vytvořených IPsec spojení.

Ve zkráceném výpisu příkazu `show crypto ipsec sa` (celý výpis je zobrazen v příloze D diplomové práce), lze vyčíst název krypto mapy, rozhraní, na které je přiřazená, IP adresu rozhraní a IP adresy vzdáleného uživatele, označení SPI, nastavení šifrování a také že je tunel aktivní.

```
Cisco_2800#show crypto ipsec sa

interface: FastEthernet0/1

    Crypto map tag: VPN, local addr 200.0.0.1

   remote ident (addr/mask/prot/port):
(192.168.2.11/255.255.255.255/0/0)

   current_peer 10.0.0.2 port 57740

     local crypto endpt.: 200.0.0.1, remote crypto endpt.: 10.0.0.2

     inbound esp sas:

      spi: 0x14C4BE97(348438167)

        transform: esp-256-aes esp-sha-hmac ,

        in use settings ={Tunnel, }

        sa timing: remaining key lifetime (k/sec): (4396297/3398)

        Status: ACTIVE

      outbound esp sas:
```

```
spi: 0x150D4AC0(353192640)
  transform: esp-256-aes esp-sha-hmac ,
  in use settings ={Tunnel, }
  sa timing: remaining key lifetime (k/sec): (4396297/3398)
  Status: ACTIVE
```

Výpis pomocí příkazu `show crypto isakmp sa`, nám poskytuje informaci o vytvořeném tunelu.

```
Cisco_2800#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
200.0.0.1       10.0.0.2        QM_IDLE           1043 ACTIVE
```

6.6 Analýza IPsec provozu v aplikaci Wireshark

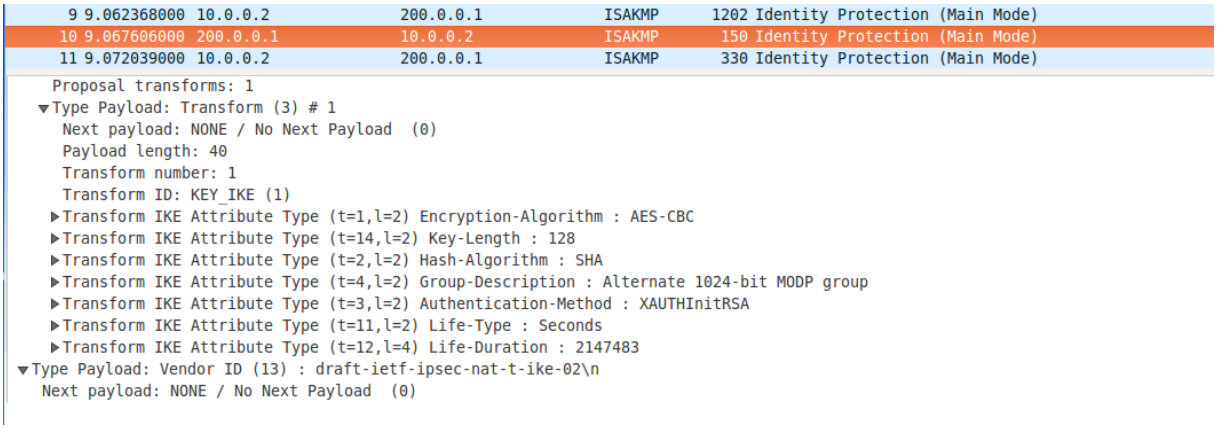
Obdobně jako v případě analýzy IPSec provozu s ASA zařízením, i tady analyzujeme provoz na dvou místech. Na PCW1 je analyzován šifrovaný provoz ve vnější síti a PCW2 analyzuje již dešifrovaný provoz ve vnitřní síti.

Na obrázku 6.5 můžeme vidět průběh spojení mezi směrovačem Cisco 2800 a Cisco VPN klientem. Můžeme si povšimnout paketu označených jako Config Mode. Tyto pakety zajišťují ověření identity uživatele, který se chce připojit k zařízení Cisco. Jeho identita je ověřená vůči lokalní databázi v zařízení Cisco. Rovněž je pomocí těchto paketů nastavena IP adresa vzdáleného uživatele [14, 15]. Taktéž si můžeme prohlédnout šifrovaný provoz ESP protokolem a označení SPI, které odpovídá označením ve výpisech na směrovači.

```
 9 9.062368000 10.0.0.2        200.0.0.1        ISAKMP    1202 Identity Protection (Main Mode)
10 9.067606000 200.0.0.1       10.0.0.2         ISAKMP     150 Identity Protection (Main Mode)
11 9.072039000 10.0.0.2        200.0.0.1        ISAKMP     330 Identity Protection (Main Mode)
12 9.143896000 200.0.0.1       10.0.0.2         ISAKMP     384 Identity Protection (Main Mode)
13 9.199732000 10.0.0.2        200.0.0.1        ISAKMP    1094 Identity Protection (Main Mode)
14 9.350472000 200.0.0.1       10.0.0.2         ISAKMP     806 Identity Protection (Main Mode)
15 9.350489000 200.0.0.1       10.0.0.2         ISAKMP     150 Informational
16 9.351565000 200.0.0.1       10.0.0.2         ISAKMP     118 Transaction (Config Mode)
17 11.223296006 10.0.0.2       200.0.0.1        ISAKMP     134 Transaction (Config Mode)
18 11.226042006 200.0.0.1      10.0.0.2         ISAKMP     118 Transaction (Config Mode)
19 11.226802006 10.0.0.2       200.0.0.1        ISAKMP     102 Transaction (Config Mode)
20 12.234941006 10.0.0.2       200.0.0.1        ISAKMP     230 Transaction (Config Mode)
21 12.240446006 200.0.0.1      10.0.0.2         ISAKMP     406 Transaction (Config Mode)
22 12.251163006 10.0.0.2       200.0.0.1        ISAKMP    1078 Quick Mode
23 12.258011006 200.0.0.1      10.0.0.2         ISAKMP     246 Quick Mode
24 12.258028006 10.0.0.2       200.0.0.1        ISAKMP     102 Quick Mode
25 12.874072006 Cisco_4b:53:59 Cisco_4b:53:59   LOOP        60 Reply
26 22.873463006 Cisco_4b:53:59 Cisco_4b:53:59   LOOP        60 Reply
27 22.933402006 10.0.0.2       200.0.0.1        ESP        134 ESP (SPI=0x14c4be97)
28 22.933418006 200.0.0.1      10.0.0.2         ESP        134 ESP (SPI=0x150d4ac0)
29 23.929585006 10.0.0.2       200.0.0.1        ESP        134 ESP (SPI=0x14c4be97)
30 23.929602006 200.0.0.1      10.0.0.2         ESP        134 ESP (SPI=0x150d4ac0)
```

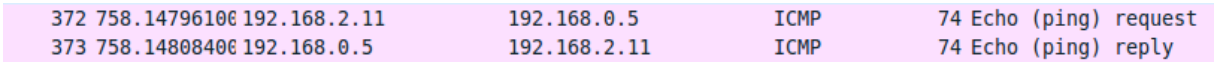
Obrázek 6.5: Vytvoření spojení a šifrovaný provoz

I v tomto případě nabízí Cisco VPN klient 26 různých kombinací zabezpečení pro fázi 1 IKE protokolu. Na dalším obrázku (Obrázek 6.6) se můžeme podívat, jakou kombinaci zabezpečení si Cisco směrovač řady 2800 vybral. Jedná se hned o první nabízenou možnost. Lze vidět, že zabezpečení odpovídá námi nastaveným bezpečnostním politikám na směrovači.



Obrázek 6.6: Vybraný bezpečnostní návrh

Analýzu dešifrovaných paketů provedeme na počítači PCW2. Na obrázku 6.7 se lze přesvědčit, že ve vnitřní síti se již komunikuje pomocí přidělené IP adresy, kterou přidělil směrovač počítači PC1.



Obrázek 6.7: Analýza dešifrovaných paketů

7 RAVPN na směrovači Huawei AR2200

V této kapitole bude ukázáno, jak vytvořit virtuální privátní síť se vzdáleným přístup pomocí směrovače Huawei řady AR2200. Směrovač bude začleněn do topologie jako VPN brána, která bude vytvářet šifrované spojení se vzdáleným klientem, který poté bude bezpečně komunikovat se zařízeními ve vnitřní síti.

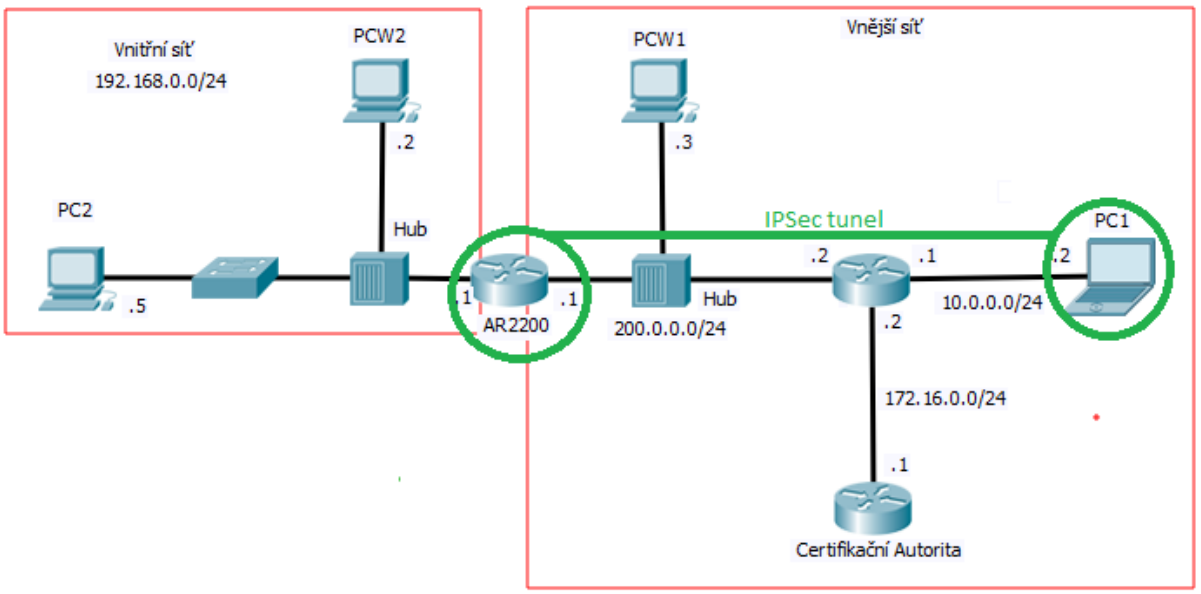
Nastavení směrovače huawei AR2200 je provedeno pomocí příkazové řádky.

7.1 Topologie sítě

I v tomto případě je topologie sítě stejná jako v předchozích případech. Jako VPN brána vystupuje směrovač Huawei řady AR2200, který je umístěn na pomezí vnitřní a vnější sítě. Pro potřebu vydávání certifikátu slouží certifikační autorita spuštěna na směrovači Cisco řady 2901. K analýze provozu slouží dva počítače PCW1 a PCW2, které jsou připojeny do hubů a na kterých je spuštěn síťový analyzátor Wireshark.

Pro kontrolu zabezpečeného spojení je poté proveden příkaz ping z počítače PC1 na počítač PC2, který je umístěn ve vnitřní síti.

Na počítači PC1 je nainstalován Shrew Soft VPN Client verze 2.2.2 [14].



Obrázek 7.1: Topologie sítě

7.2 Konfigurace certifikační autority

Nastavení certifikační autority se neliší od konfigurací v předchozích případech, kdy jako VPN braná vystupovala ASA nebo směrovač Cisco řady 2800. Lze si ji tedy prohlédnout v minulých kapitolách. Zobrazíme si pouze fingerprint certifikátu certifikační autority, který budeme později potřebovat.

```
CASERVER#show crypto pki server CASERVER
Issuer name: CN=CertifikacniAutorita
    CA cert fingerprint: 68DF385D BC56A542 12E3B564 BA534B26
```

7.3 Konfigurace směrovače Huawei AR2200

Nastavení směrovače Huawei provedeme v několika krocích. Je potřeba získat certifikáty od certifikační autority, nastavit politiku pro vytvoření zabezpečeného tunelu, vytvořit access control list a přiřadit politiku na vnější rozhraní.

7.3.1 Registrace u certifikační autority a získání certifikátů

Předtím, než provedeme požadavek na získání certifikátů od certifikační autority je nutné na směrovači nakonfigurovat potřebné části. V prvním kroku vytvoříme takzvanou entitu, která identifikuje žadatele o certifikát. Je potřebné vyplnit atribut common-name, čili název subjektu pro který bude certifikát vydán. Ostatní atributy jsou volitelné.

```
[Huawei]pki entity AR2200
[Huawei-pki-entity-AR2200]  common-name 2200
```

Dále vytvoříme takzvaný realm, ve kterém pro získání certifikátů nastavíme entitu, certifikační autoritu, její IP adresu, otisk certifikátu certifikační autority. Tento realm bude taktéž použit pro nastavení autentizace pomocí certifikátu u IKE protokolu.

```
[AR2200]pki realm VPN
[AR2200-pki-realm-VPN]ca id CASERVER
[AR2200-pki-realm-VPN]entity 2200
[AR2200-pki-realm-VPN]enrollment-url http://172.16.0.1:80
[AR2200-pki-realm-VPN]fingerprint md5 68DF385D BC56A542 12E3B564
BA534B26
```

Pokud se rozhodneme pro získání certifikátů pomocí SCEP protokolu použijeme následující příkazy. První příkaz slouží k získání certifikátu certifikační autority, druhý z nich, k získání certifikátu pro směrovač Huawei.

```
[AR2200]pki get-certificate ca VPN
[AR2200]pki get-certificate local VPN
```

V našem případě využijeme manuální metody pro získání obou certifikátů. Na směrovači si následujícím příkazem vygenerujeme požadavek na certifikát, kde VPN je název realmu.

```
[AR2200]pki enroll-certificate VPN pkcs10
```

Zobrazí se nám vygenerovaný požadavek:

```
-----BEGIN PKCS10 REQUEST-----
```

```
MIICajCCAVICAQAwDzENMAsGA1UEAxMEMjIwMDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAOKvePO4MsHrbO0OJASx8QMXaXVdYvme/zPXttg9xhNZIVlh
S2ZwbL/34jBFClXfM6mb6yL7ymwcmDyfah+sHC/7Yz+Bm5xShyjLad0ITTjkB5TY
kqf7SEVka7dkO/smACyAHwUQTFpx+YN7NvMId/OH/+Wbmc3SmtboduBnjuvVj/M1
Y3onnrwjx+jUM+yb/zzP7WT6F9hesoDRSofvqijFtFDpbk7CpEaWnFbqGsrQHlbv
v66zezxzihHyQYXjlMWhcrW8tX7YPLbDPjNIBPKVePeTUVLcXAhupz52on7Ze4qG
8ms2MnnVnl77d/ilxjMwUgUfdYKP6wJLWPSKBBkCAwEAAaAWMBQGCSqGSIb3DQEJ
BzEHEwVjaXNjbzANBgkqhkiG9w0BAQQFAAOCAQEAuh9BMzYeUqv7qYraWgcUlD51
sXLI6NeRkxtYcfhiGFmVCs+WvDQXRoRQ/Bn5Ha4GCoxc2fgiIDEfdAjD+k9Rk+Ut
AcJOFjYNj7dvCj+OW73ETRIn0YRDIH+SMdXxu+Qb7vCfj9CMdYWWmH3j01CpJ993
wE4c0B8m7+TDGF2Kcdbl91O+2LfTFGgZ3jHp3QQt7vx2Yr2Oi6NUm/WNeSALu/cr
6DUg/J3aqOsnPSAsDBWwWQfK6mcP+27qut/skBChkxdiklwmwr+zdNznEpONWNkV
e4pOSkstg8QBQG+Vo3oxZPcNHdgmPUIT4gqbszxPryoT8VyotNqLTbP5HM8kSw==
-----END PKCS10 REQUEST-----
```

Tento požadavek doručíme certifikační autoritě, kde vygenerujeme certifikát pro směrovač Huawei. Na směrovači Cisco tak učiníme podle následujícího příkazu v privilegovaném módu, kde CASERVER je název certifikační autority a pkcs10 formát požadavku.

```
CASERVER#crypto pki server CASERVER request pkcs10 terminal
PKCS10 request in base64 or pem
```

Následovně jsme vyzvání k vložení požadavku, který ukončíme na novém řádku slovem quit. Pokud vše proběhne v pořádku, ihned se vygeneruje certifikát pro směrovač Huawei.

```
% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN PKCS10 REQUEST-----
MIICajCCAVICAQAwDzENMAsGA1UEAxMEMjIwMDCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAOKvePO4MsHrbO0OJASx8QMXaXVdYvme/zPXttg9xhNZIVlh
S2ZwbL/34jBFClXfM6mb6yL7ymwcmDyfah+sHC/7Yz+Bm5xShyjLad0ITTjkB5TY
kqf7SEVka7dkO/smACyAHwUQTFpx+YN7NvMId/OH/+Wbmc3SmtboduBnjuvVj/M1
Y3onnrwjx+jUM+yb/zzP7WT6F9hesoDRSofvqijFtFDpbk7CpEaWnFbqGsrQHlbv
v66zezxzihHyQYXjlMWhcrW8tX7YPLbDPjNIBPKVePeTUVLcXAhupz52on7Ze4qG
8ms2MnnVnl77d/ilxjMwUgUfdYKP6wJLWPSKBBkCAwEAAaAWMBQGCSqGSIb3DQEJ
BzEHEwVjaXNjbzANBgkqhkiG9w0BAQQFAAOCAQEAuh9BMzYeUqv7qYraWgcUlD51
sXLI6NeRkxtYcfhiGFmVCs+WvDQXRoRQ/Bn5Ha4GCoxc2fgiIDEfdAjD+k9Rk+Ut
```

```
AcJOFjYNj7dvCj+OW73ETRIn0YRDIH+SMdXxu+Qb7vCfj9CMdYWWmH3j01CpJ993
wE4c0B8m7+TDGF2Kcdbl91O+2LfTFGgZ3jHp3QQt7vx2Yr2Oi6NUm/WNeSALu/cr
6DUg/J3aqOsnPSAsDBWwWQfK6mcP+27qut/skBChkxdiklwmwr+zdNznEpONWNkV
e4pOSkstg8QBQG+Vo3oxZPcNHdgmPUIT4gqbszxPryoT8VyotNqLTbP5HM8kSw==
-----END PKCS10 REQUEST-----
quit
% Granted certificate:
-----BEGIN CERTIFICATE-----
MIICajCCAdOgAwIBAgIBAjANBgkqhkiG9w0BAQQFADAfMR0wGwYDVQQDExRDZXJ0
aWZpa2FjbmlBdXRvcml0YTAeFw0xNjA2MTcxMTU0MzlaFw0xNzA2MTcxMTU0Mzla
MA8xDTALBgNVBAMTBDIyMDAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDir3jzuDLB62ztDiQEsfEDF2l1XWL5nv8z17bYPcYTWSFZYUtmcGy/9+IwRQpV
3zOpm+si+8psHJg8n2ofrBwv+2M/gZucUocoy2ndCE045AeU2JKn+0hFZGu3ZDv7
JgAsgB8FEExacfmDezbzCHfzh//lm5nN0prW6HbgZ47r1Y/zNWN6J568I8fo1DPs
m/88z+1k+hfYXrKA0UqH76ooxbRQ6W5OwqRGlpxW6hrK0B5W77+us3s8c4oR8kGF
45TFoXK1vLV+2Dy2wz4zSATylXj3k1FS3FwIbqc+dqJ+2XuKhvJrNjJ51Z5e+3f4
pcYzMFIFH3WCj+sCS1j0igQZAgMBAAGjQjBAMB8GA1UdIwQYMBaAFLUoBbU/PyZu
9uZJNqU7u1gzQYbnMB0GA1UdDgQWBBTorU9pLNKFz77hHVhx2hIgoSFlCTANBgkq
hkiG9w0BAQQFAAOBgQCLXZQ7pnv5CzaEToQi5TQ8iPTpTDh0n9Y8RWc0OO0qrxYW
mt9Hu7s8njAQmmVomXsTa2PFUjKoh75a693FjPqVk4/yoAOd83H0Ut3x5MNxtN84
yOmhXCve07Ad8/B2Sd1aX1DKz/xhzOlfhcRcJNtFnrQZVEDOjRAJYQLFu8CINw==
-----END CERTIFICATE-----
```

Taktéž je potřeba certifikát certifikační autority, který vygenerujeme následujícím příkazem v konfiguračním módu:

```
CASERVER(config)#crypto pki export CASERVER pem terminal
% The specified trustpoint is not enrolled (CASERVER).
% Only export the CA certificate in PEM format.
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICFzCCAYCgAwIBAgIBATANBgkqhkiG9w0BAQQFADAfMR0wGwYDVQQDExRDZXJ0
aWZpa2FjbmlBdXRvcml0YTAeFw0xNjA2MTcwOTI2MTlaFw0xOTA2MTcwOTI2MTla
MB8xHTAbBgNVBAMTFENlcnRpZmlrYWNuaUF1dG9yaXRhMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQC47alM3rYEPgB3NSUtoyExpB2ogdk8dccuMKHUu92aUFSG
```

```
5faEoz37LT9/P9v+6JXaQbsR5ALNHC0Mt4+clpNBY96hD0hf23AjrowRwLHU91PC
dlRRcpJWPp2u58PnjIsLD9AwjSetKT74LuULumNbW5PVzqsHTwq62qZgnbKACQID
AQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBhjAfBgNVHSME
GDAWgBS1KAW1Pz8mbvbmSTalO7tYM0GG5zAdBgNVHQ4EFgQUtSgFtT8/Jm725kk2
pTu7WDNBhucwDQYJKoZIhvcNAQEEBQADgYEASdng8pPesaEfFZVqRo4YzVQD1kH3
OkZBxuOEwP98C8rYXFcL94Vb/PgSqOOP5YNQb2jda/DzK+BI4gTxqGX4vX/OAerF
HEFsYLaJ4WYFXijUvL1kYKcMU3UeEmmmLMfQzKGcCzTA7Wz1D2qoz9NWLi2i+Coi
LNsotfTTzrSmPa8=
-----END CERTIFICATE-----
```

Takto získané certifikáty si uložíme do dvou souborů. Certifikát certifikační autority s příponou pem, certifikát pro směrovač Huawei bez přípony. Oba soubory překopírujeme na USB flash disk, který vložíme do Huawei směrovače. Soubory poté překopírujeme do úložiště sd1 ve směrovači Huawei a to následujícími příkazy:

```
<AR2200>copy usb0:/ca.pem sd1:/
<AR2200>copy usb0:/hcert sd1:/
```

Poté certifikáty importujeme do směrovače k budoucímu použití k vytvoření IPSec tunelu. Prvně importujeme certifikát určený pro směrovač:

```
[AR2200]pki import-certificate local VPN pem
Please enter the name of certificate file <length 1-127>: hcert
 You are importing a local certificate.
Please enter the name of private key file <length 1-127>:
```

Zmačkneme klávesu ENTER a certifikát bude úspěšně importován.

```
Successfully imported the certificate.
```

Import certifikátu certifikační autority vypadá obdobně:

```
[AR2200]pki import-certificate ca VPN pem
 Please enter the name of certificate file <length 1-127>: CA.pem
 Successfully imported the certificate.
```

Kontrolu importovaných certifikátů můžeme provést pomocí příkazu display pki certificate:

```
<AR2200>display pki certificate local VPN
Certificate
  Status : Available
  Version: 3
  Serial Number: 02
```

```
  Subject:  CN=2200

  Associated Pki Realm : VPN

Total Number: 1

<AR2200>display pki certificate ca VPN
CA certificate
  Status : Available
  Version: 3
  Serial Number: 01
  Subject:  CN=CertifikacniAutorita
  Associated Pki Realm : VPN

Total Number: 1
```

7.3.2 Vytvoření bezpečnostních politik

Pro vytvoření IPSec tunelu je nutné vytvořit bezpečnostní politiku, pro vyjednání vlastností tunelu. Nastavíme tedy bezpečnostní parametry pro fázi 1 IKE protokolu. Jedná se o hashovací algoritmus, šifru, autentizační metodu a číslo Diffie-Hellmanovy skupiny. Vybraný šifrovací algoritmus a hashovací algoritmus je pouze demonstrační, v praxi je doporučené použit novějších algoritmů jako AES a SHA.

```
[AR2200]ike proposal 5
[AR2200-ike-proposal-5] authentication-algorithm md5
[AR2200-ike-proposal-5] encryption-algorithm 3des-cbc
[AR2200-ike-proposal-5]  authentication-method rsa-signature
[AR2200-ike-proposal-5] dh group5
```

Dále definujeme parametry pro fázi 2 IKE protokolu:

```
[AR2200]ipsec proposal Faze2
[AR2200-ipsec-proposal-Faze2] esp encryption-algorithm 3des
[AR2200-ipsec-proposal-Faze2]esp authentication-algorithm md5
```

Následuje nastavení pro vzdáleného uživatele. Definujeme zde vytvořený realm a bezpečnostní parametry pro fázi 1 IKE protokolu:

```
[AR2200]ike peer peer1 v1
[AR2200-ike-peer-peer1] ike-proposal 5
[AR2200-ike-peer-peer1] pki realm VPN
```

Taktéž je potřeba vytvořit ACL pro povolení vzdáleného přístupu do vnitřní sítě. Adresa 10.10.10.10 odpovídá adrese, která bude později nastavena ve VPN klientu:

```
[AR2200]acl number 3000
[AR2200-acl-adv-3000] rule 5 permit ip source 192.168.0.0 0.0.0.255
destination 10.10.10.10 0
```

Nyní vytvoříme šablonu, ve které spojíme vytvořené parametry tunelu.

```
[AR2200]ipsec policy-template Sablona 10
[AR2200-ipsec-policy-templet-Sablona-10] ike-peer peer1
[AR2200-ipsec-policy-templet-Sablona-10] proposal Faze2
[AR2200-ipsec-policy-templet-Sablona-10] security acl 3000
```

Nakonec nakonfigurujeme celkovou IPSec politiku, které přiřadíme vytvořenou šablonu. Poté vytvořenou IPSec politiku přiřadíme na rozhraní ležící ve vnější síti.

```
[AR2200] ipsec policy Politika1 1 isakmp template Sablona
[AR2200]int GigabitEthernet 0/0/1
 [AR2200-GigabitEthernet0/0/1]ipsec policy Politika1
```

7.4 Získání certifikátu pro PC1

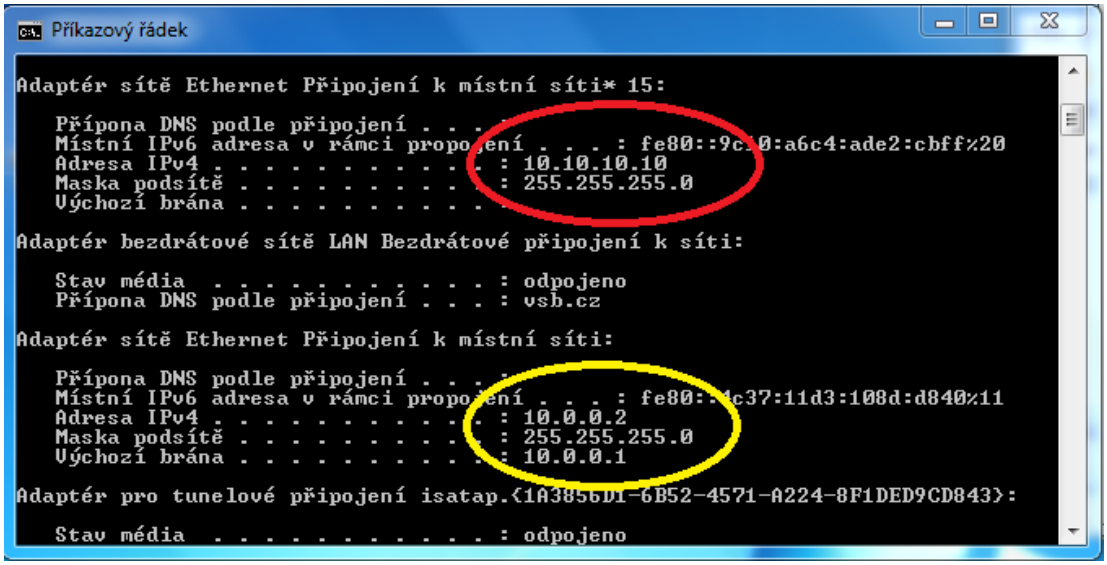
Aby bylo možné vytvořit zabezpečený tunel mezi počítačem PC1 a VPN bránou, je potřeba získat certifikát i pro počítač PC1. Jelikož Shrew Soft VPN klient nepodporuje SCEP protokol, je potřeba certifikát získat manuálně. Vytvoříme tedy nejprve požadavek na certifikát.

To se provádí v několika krocích. V systému Windows zapneme Managmentovou konzoli příkazem mmc. Otevře se nám následující okno (viz Obrázek 0.1 v příloze A diplomové práce), klikneme na soubor a vybereme Přidat nebo odebrat modul snap-in. Celý postup je vyobrazen v příloze A diplomové práce.

7.5 Nastavení Shrew Soft VPN Klienta

Na rozdíl od Cisco VPN klienta lze Shrew Soft VPN klienta nastavovat podle vlastního uvážení a definovat vlastnosti vytvářeného tunelu. Nastavování klienta začneme přidáním nového spojení pomocí tlačítka Add. Vyskočí následující okno (viz Obrázek 0.17 v příloze B diplomové práce), kde nastavíme IP adresu VPN brány, vypneme auto konfiguraci a použijeme virtuální adapter s IP adresou, kterou ručně vepíšeme. V záložce Client vypneme Nat Traversal (viz Obrázek 0.18 v příloze B diplomové práce). Celý postup je znázorněn v příloze B diplomové práce.

Kontrolu přirazené adresy provedeme pomocí příkazu ipconfig v příkazové řádce (viz Obrázek 7.2). Červeně je označená IP adresa, kterou jsme nastavili v klientu VPN. Žlutě je označena fyzická IP adresa PC1.



Obrázek 7.2: Kontrola IP adres

7.6 Kontrola IPsec tunelu v zařízení Huawei AR2200

Kontrolu vytvořeného IPSec tunelu mezi směrovačem Huawei AR2200 a VPN klientem můžeme stejně jako u Cisco zařízení, provést pomocí příkazu na zobrazení aktivních IPSec tunelů.

Příkaz `display ipsec sa` je obdobou příkazu `show crypto ipsec sa` u zařízení Cisco. Ze zkráceného výpisu můžeme vyčíst typ zapouzdření, použité šifrování, hashovací algoritmus, konce tunelu nebo použitou bezpečnostní politiku. Celý výpis je k dispozici v příloze E diplomové práce.

```
===============================
Interface: GigabitEthernet0/0/1
 Path MTU: 1500
===============================
  -----------------------------
  IPSec policy name: "Politika1"
  Sequence number   : 1
  Acl group         : 3000
  Acl rule          : 5
  Mode              : ISAKMP
  -----------------------------
```

```
    Connection ID     : 251
    Encapsulation mode: Tunnel
    Tunnel local      : 200.0.0.1
    Tunnel remote     : 10.0.0.2
    Flow source       : 192.168.0.0/255.255.255.0 0/0
    Flow destination  : 10.10.10.10/255.255.255.255 0/0

    [Outbound ESP SAs]
      SPI: 3257253873 (0xc225bff1)
      Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-MD5

    [Inbound ESP SAs]
      SPI: 1276174260 (0x4c10dfb4)
      Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-MD5
```

Příkaz `display ike sa` nám umožní vidět aktuální vytvořené SA pomocí IKE protokolu. Lze vidět, že fáze 1 i fáze 2 proběhly v pořádku a jsou připraveny.

```
<AR2200>display ike sa
    Conn-ID  Peer            VPN   Flag(s)                 Phase
  -----------------------------------------------------------------
      242    10.0.0.2        0     RD|ST                     2
      232    10.0.0.2        0     RD                        1
```

Příkaz `display ike proposal` nám zobrazí dostupné bezpečnostní návrhy pro první fázi IKE protokolu. Vidíme námi vytvořený návrh s označením číslo 5.

```
<AR2200>display ike proposal
-----------------------------------------
 IKE Proposal: 5
   Authentication method      : rsa-signature
   Authentication algorithm   : MD5
   Encryption algorithm       : 3DES-CBC
   DH group                   : MODP-1536
   SA duration                : 86400
   PRF                        : PRF-HMAC-SHA
-----------------------------------------
```

7.7 Analýza IPsec provozu v aplikaci Wireshark

Obdobně jako v předchozích případech, i zde monitorujeme provoz na dvou místech: V PCW1 je monitorován šifrovaný provoz a provoz ve vnitřní síti je monitorován v počítači PCW2. Sestavení tunelu tedy pozorujeme na PCW1 a je zobrazeno na obrázku 7.3.

13	33.647040000	10.0.0.2	200.0.0.1	ISAKMP	274	Identity Protection (Main Mode)
14	33.654440000	200.0.0.1	10.0.0.2	ISAKMP	186	Identity Protection (Main Mode)
15	33.659683000	10.0.0.2	200.0.0.1	ISAKMP	295	Identity Protection (Main Mode)
16	33.783126000	200.0.0.1	10.0.0.2	ISAKMP	328	Identity Protection (Main Mode)
17	33.797009000	10.0.0.2	200.0.0.1	ISAKMP	734	Identity Protection (Main Mode)
18	33.949063000	200.0.0.1	10.0.0.2	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0384)
19	33.949080000	200.0.0.1	10.0.0.2	ISAKMP	60	Identity Protection (Main Mode)
20	33.952776000	10.0.0.2	200.0.0.1	ISAKMP	118	Informational
21	35.085797000	10.0.0.2	200.0.0.1	ISAKMP	198	Quick Mode
22	35.089768000	200.0.0.1	10.0.0.2	ISAKMP	102	Informational
23	35.119350000	HP_75:a9:d4	CDP/VTP/DTP/PAgP/UDLD	CDP	185	Device ID: HUB-CVT-20060B0 75A9D4 Port ID: Ethernet0
24	38.291108000	Cisco_4b:53:58	CDP/VTP/DTP/PAgP/UDLD	CDP	359	Device ID: Router Port ID: FastEthernet0/0
25	38.291124000	Cisco_4b:53:58	CDP/VTP/DTP/PAgP/UDLD	CDP	354	Device ID: Router Port ID: FastEthernet0/0
26	39.997614000	Cisco_4b:53:58	Cisco_4b:53:58	LOOP	60	Reply
27	40.121751000	10.0.0.2	200.0.0.1	ISAKMP	198	Quick Mode
28	40.125593000	200.0.0.1	10.0.0.2	ISAKMP	102	Informational
29	44.268482000	200.0.0.1	10.0.0.2	ISAKMP	206	Quick Mode
30	44.270010000	10.0.0.2	200.0.0.1	ISAKMP	198	Quick Mode
31	44.274996000	200.0.0.1	10.0.0.2	ISAKMP	94	Quick Mode
32	45.129396000	10.0.0.2	200.0.0.1	ISAKMP	198	Quick Mode
33	45.133447000	200.0.0.1	10.0.0.2	ISAKMP	102	Informational
34	48.982782000	10.0.0.2	200.0.0.1	ISAKMP	126	Informational
35	48.987988000	200.0.0.1	10.0.0.2	ISAKMP	126	Informational
36	49.996988000	Cisco_4b:53:58	Cisco_4b:53:58	LOOP	60	Reply
37	50.137005000	10.0.0.2	200.0.0.1	ISAKMP	198	Quick Mode
38	50.140891000	200.0.0.1	10.0.0.2	ISAKMP	102	Informational
39	56.720483000	10.0.0.2	200.0.0.1	ESP	126	ESP (SPI=0x4c10dfb4)
40	56.720499000	200.0.0.1	10.0.0.2	ESP	126	ESP (SPI=0xc225bff1)
41	57.703555000	10.0.0.2	200.0.0.1	ESP	126	ESP (SPI=0x4c10dfb4)
42	57.703571000	200.0.0.1	10.0.0.2	ESP	126	ESP (SPI=0xc225bff1)
43	58.717824000	10.0.0.2	200.0.0.1	ESP	126	ESP (SPI=0x4c10dfb4)

Obrázek 7.3: Sestavení spojení a šifrovaný provoz

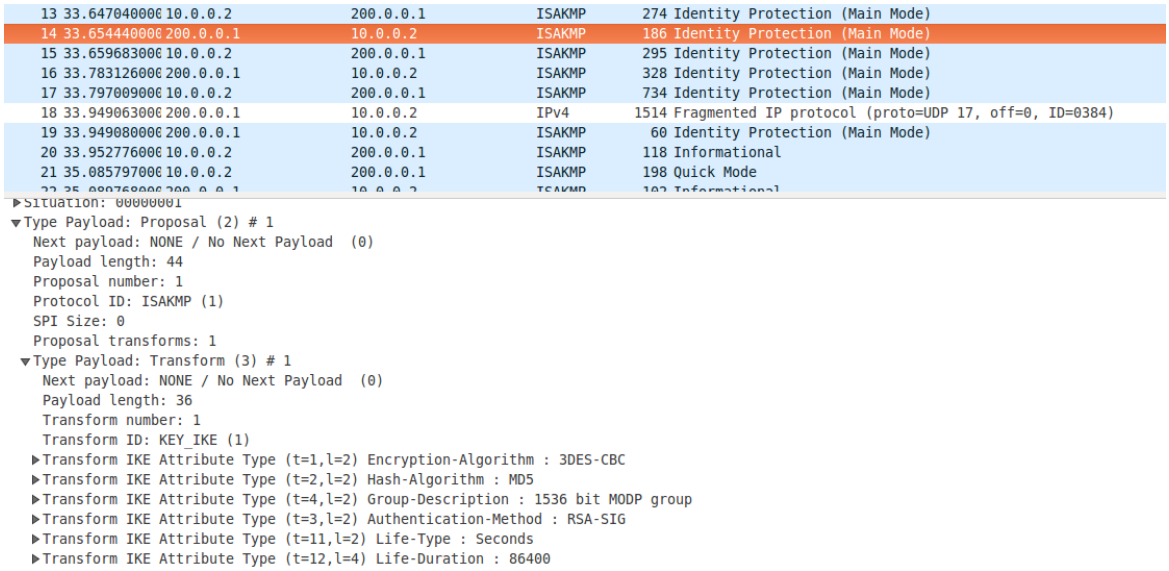
Taktéž můžeme vidět provoz šifrovaný ESP protokolem a označení SPI, které odpovídá označením SPI z výpisu `display ipsec sa`, ve směrovači Huawei.

Nabízené zabezpečení tunelu, které poskytuje VPN klient je zobrazeno na obrázku 7.4. Vidíme, že odpovídá nastavení VPN klienta.

```
▼Type Payload: Transform (3) # 1
    Next payload: NONE / No Next Payload  (0)
    Payload length: 36
    Transform number: 1
    Transform ID: KEY_IKE (1)
  ▶Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
  ▶Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
  ▶Transform IKE Attribute Type (t=4,l=2) Group-Description : 1536 bit MODP group
  ▶Transform IKE Attribute Type (t=3,l=2) Authentication-Method : RSA-SIG
  ▶Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
  ▶Transform IKE Attribute Type (t=12,l=4) Life-Duration : 86400
▼Type Payload: Vendor ID (13) : Microsoft L2TP/IPSec VPN Client
  Next payload: Vendor ID (13)
  Payload length: 24
  Vendor ID: 4048b7d56ebce88525e7de7f00d6c2d380000000
```

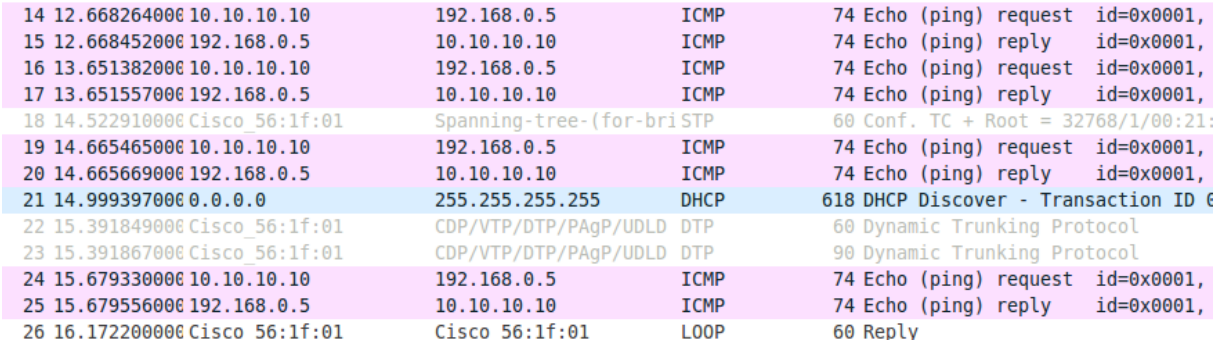
Obrázek 7.4: Nabízený bezpečnostní návrh

Na rozdíl od Cisco VPN klienta, zde VPN klient nenabízí více možných bezpečnostních návrhů. Je nabízen pouze námi nastavený návrh. VPN brána si ho tedy vybere (viz Obrázek 7.5), jelikož jsou stejné parametry nastaveny i ve VPN bráně.



Obrázek 7.5: Vybraný bezpečnostní návrh

V počítači PCW2, na kterém je také spuštěn Wireshark, monitorujeme provoz ve vnitřní síti, za VPN bránou. Vidíme, že paket je dešifrován a jako zdrojová adresa je použita adresa nastavena ve VPN klientu (viz Obrázek 7.6).



Obrázek 7.6: Dešifrovaný provoz

8 Kompatibilita směrovačů Cisco, Huawei a zhodnocení výhod jednotlivých řešení

Nastavení VPN koncentrátoru je zhruba podobné na všech třech zařízeních. Je potřeba nastavit bezpečnostní politiky IPsec tunelu, získat certifikát od certifikační autority a přiřadit bezpečnostní politiku na rozhraní vnější sítě. Nejlépe vybavené zařízení na vytvoření virtuální privátní sítě se vzdáleným přístupem je Cisco ASA zařízení, které v sobě již má defaultní nastavení pro vytvoření tohoto typu sítě a usnadňuje konfiguraci. Taktéž disponuje firewallem, což může být výhoda pro menší podnikové sítě, které by se rozhodly ušetřit a mít dvě zařízení v jednom fyzickém přístroji. V případě směrovače Cisco řady 2800 a směrovače Huawei řady AR2200, je nutné zařadit do podnikové sítě ještě firewall, popřípadě je vhodně včlenit do již vybudované podnikové sítě nejlépe tak, jak je popsáno v teoretické části této diplomové práce. U nastavení směrovače Cisco řady 2800 a Huawei AR2200 je ještě nutné definoval ACL, které umožní přístup do vnitřní privátní podnikové sítě. Nastavení směrovače Huawei se liší také v tom, že nebylo možné přiřadit IP adresu z vytvořeného rozsahu IP adres, vzdáleným uživatelům. Proto je potřeba ručně vyplnit IP adresu ve VPN klientu, což Shrew Soft VPN klient na rozdíl od Cisco VPN kienta umožňuje. Taktéž nastavení rozšířeného ověřování uživatele vůči lokalní databázi nebylo ve VPN koncentrátoru Huawei dostupné.

Jako vydavatel certifikátů je využita certifikační autorita realizovaná na Cisco směrovači řady 2901. Certifikační autorita může přijímat požadavky na certifikáty pomocí SCEP protokolu nebo vydávat certifikáty manuální formou, pokud SCEP protokol selže. V případě Cisco VPN klienta, směrovače Cisco či zařízení ASA, která SCEP protokol podporují, nebyl problém s komunikací a certifikáty bylo možné pomoci tohoto protokolu získat. Shrew Soft VPN klient tento protokol nepodporuje, proto bylo nutné požádat o certifikáty manuálně. Stejně tomu bylo i v případě Huawei směrovače, který sice SCEP protokol podporuje, nicméně k úspěšné komunikaci s certifikační autoritou spuštěnou na zařízení Cisco nedošlo. Certifikační autoritu lze tedy využívat na Cisco směrovačích, ovšem s verzi IOSu, která tuto službu podporuje. V našem případě se jednalo o IOS verze 15.5. Směrovače Huawei v době psaní této práce možností nastavení certifikační autority nedisponují.

Závěr

Tato diplomová práce demonstrovala jak vytvořit zabezpečený komunikační kanál přes nedůvěryhodnou síťovou infrastrukturu, jakou je například Internet. V roli VPN koncentrátoru vystupovala tři zařízení: Cisco ASA, směrovač Cisco řady 2800 a směrovač Huawei řady AR2200. Všechna tři zmíněná zařízení podporují možnost vytvořit IPsec tunel a ověřit autenticitu uživatelů pomocí certifikátů. U Cisco zařízení je nejvhodnější použít Cisco VPN klienta, který sice nedisponuje velkou možností nastavení, za to komunikace se směrovači Cisco funguje bez jakýchkoliv problému. U směrovače Huawei je vhodné použít VPN klienta, kde je možné nastavit parametry spojení a který není orientován pouze na jeden typ VPN brány jako v případě Cisco VPN klienta. Jelikož Huawei v době psaní této práce nedisponuje žádným vlastním VPN klientem, který by podporoval IPsec protokol, je vhodné použit volně dostupný Shrew Soft VPN klient.

Certifikační autorita byla spuštěna na směrovači Cisco řady 2901 a vydávála certifikáty zařízením, které chtějí spolu zabezpečeně komunikovat. Certifikační autorita je schopná vydávat certifikáty jednak manuálním způsobem, kdy je potřeba nejprve vytvořit požadavek na certifikát, zkopírovat ho certifikační autoritě a poté vytvořit certifikát z onoho požadavku a nebo využít automatický způsob získávání certifikátů pomocí protokolu SCEP, kdy je do směrovače zadaná IP adresa certifikační autority a certifikáty jsou automaticky staženy, například pomocí protokolu HTTP.

V současné době Cisco i Huawei prosazují virtuální privátní sítě se vzdáleným přístupem pomocí SSL protokolu. V případě firmy Cisco je k dispozici AnyConnect Secure Mobility Client, který podporuje SSL protokol a protokol IKEv2. Nepodporuje však protokol IKEv1, který je podporován v diplomové práci použitým Cisco VPN klientem nebo klientem od firmy Shrew Soft.

Použitá literatura

[1] CARMOUCHE, James Henry. IPsec Virtual Private Network Fundamentals. Cisco Press, 2006. ISBN 1-58705-207-5.

[2] HOOPER, Howard. CCNP Security VPN 642-648 Official Cert Guide. Cisco Press, 2012. ISBN 1-58720-447-9.

[3] IPSec Overview Part Four: Internet Key Exchange (IKE). Ciscopress [online]. Cisco Press, 2002 [cit.2016-01-15].Dostupné z:http://www.ciscopress.com/articles/article.asp?p=25474&seqNum=3

[4] IKEv2 Packet Exchange and Protocol Level Debugging. Cisco [online]. 2013 [cit. 2016-01-15]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/115936-understanding-ikev2-packet-exch-debug.html

[5] MACHNÍK, Petr. Širokopásmové sítě pro integrovanou výuku VUT a VŠB-TUO [online]. Ostrava, 2014 [cit. 2016-01-15]. VYSOKÁ ŠKOLA BÁŇSKÁ–TECHNICKÁ UNIVERZITA OSTRAVA.

[6] Úvod do Cisco ASA a možnosti VPN. Www.samuraj-cz.com [online]. 2011 [cit. 2016-01-26]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-2-uvod-do-cisco-asa-a-moznosti-vpn/

[7] Starting Interface Configuration (ASA 5505). Www.cisco.com [online]. [cit. 2016-01-26]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa84/configuration/guide/asa_84_cli_config/interface_start_5505.html

[8] Configuring Certificates. Www.cisco.com [online]. [cit. 2016-01-26]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa80/configuration/guide/conf_gd/cert_cfg.html

[9] Configuring PKI. Www.cisco.com [online]. [cit. 2016-01-26]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/vspa/configuration/guide/ivmsw_book/ivmvpn4.html

[10] Crypto ca authenticate through crypto ca trustpoint. Commands A to C, Cisco IOS XE Release 3SE [online]. [cit. 2016-01-26]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-xe-3se-5700-cr-book/sec-a1-xe-3se-5700-cr-book_chapter_0101.pdf

[11] Configuring Remote Access VPNs. Cisco [online]. [cit. 2016-01-26]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/vpn_remote_access.html

[12] Understanding how ASA Firewall matches Tunnel-Group Names. Http://blog.ine.com [online]. [cit. 2016-01-26]. Dostupné z: http://blog.ine.com/2009/04/19/understanding-how-asa-firewall-matches-tunnel-group-names/

[13] *Cisco: Download Software* [online]. [cit. 2016-06-28]. Dostupné z: https://software.cisco.com/download/navigator.html?mdfid=270636499&i=rm

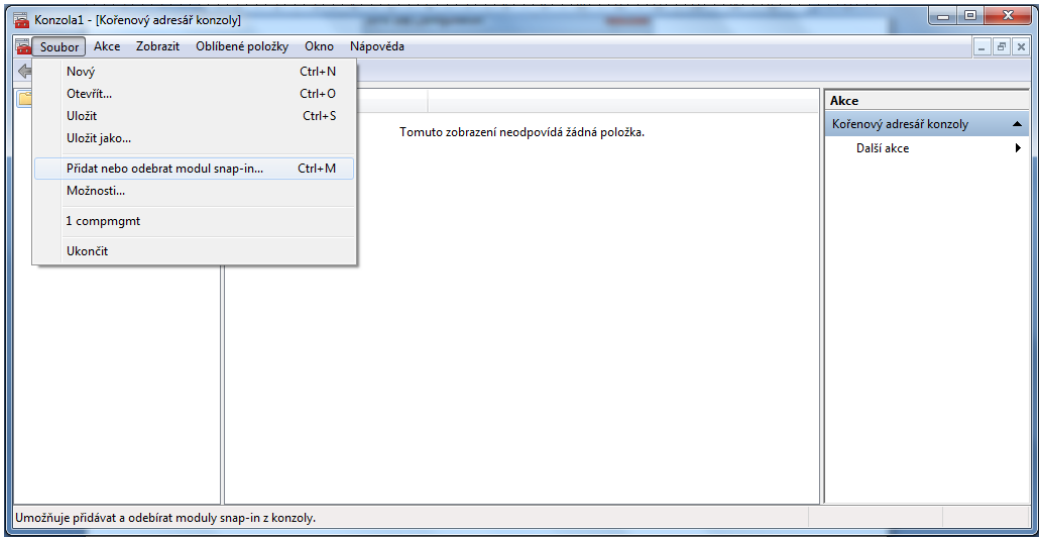
[14] *Shrew Soft: Download* [online]. [cit. 2016-06-28]. Dostupné z: https://www.shrew.net/download

[15] Extended Authentication within ISAKMP/Oakley (XAUTH). *Http://ietf.org/* [online]. [cit. 2016-06-28]. Dostupné z: https://tools.ietf.org/html/draft-ietf-ipsec-isakmp-xauth-06#page-6

[16] The ISAKMP Configuration Method. *Http://ietf.org/* [online]. [cit. 2016-06-28]. Dostupné z: https://www.ietf.org/proceedings/46/I-D/draft-ietf-ipsec-isakmp-mode-cfg-05.txt

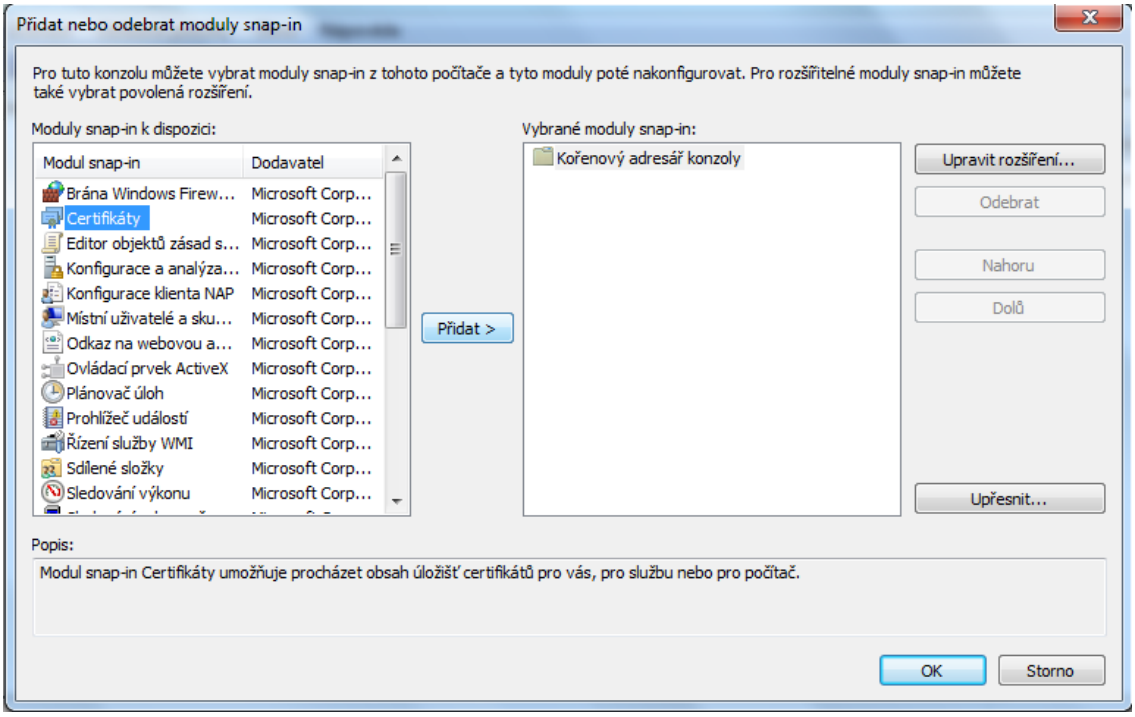
Seznam příloh

Příloha A: *Získání certifikátů pro PC1*



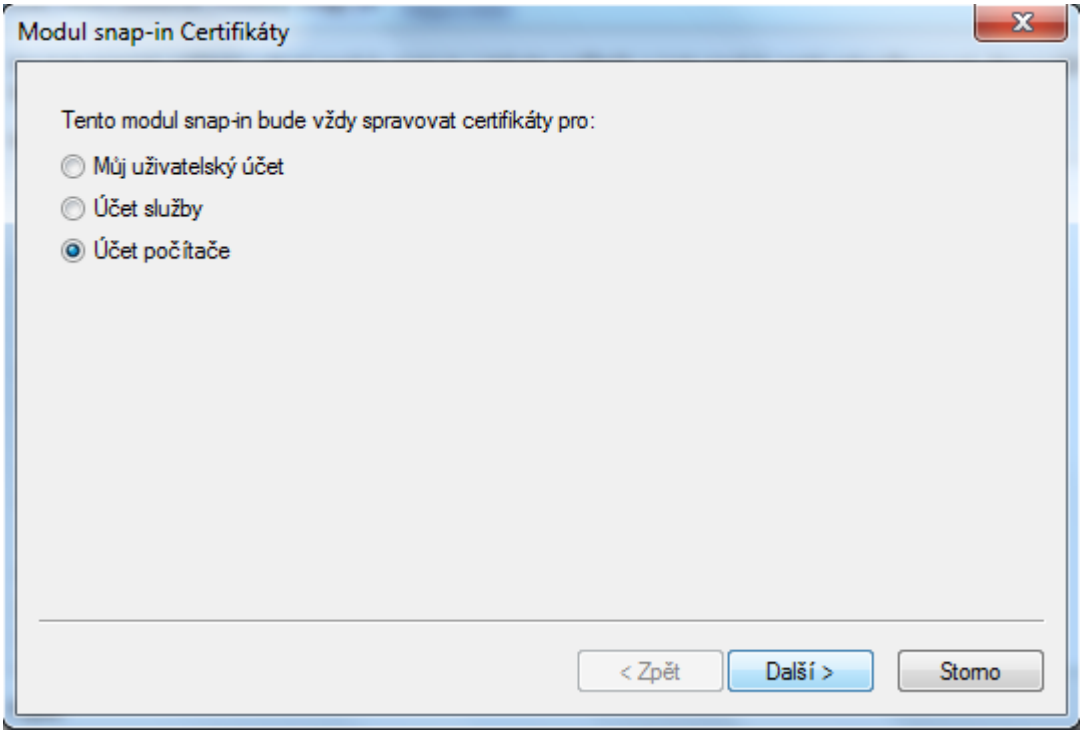
Obrázek 0.1 : Získání certifikátu, krok 1

Klikneme na položku Certifikáty a dáme přidat (viz Obrázek 0.2).

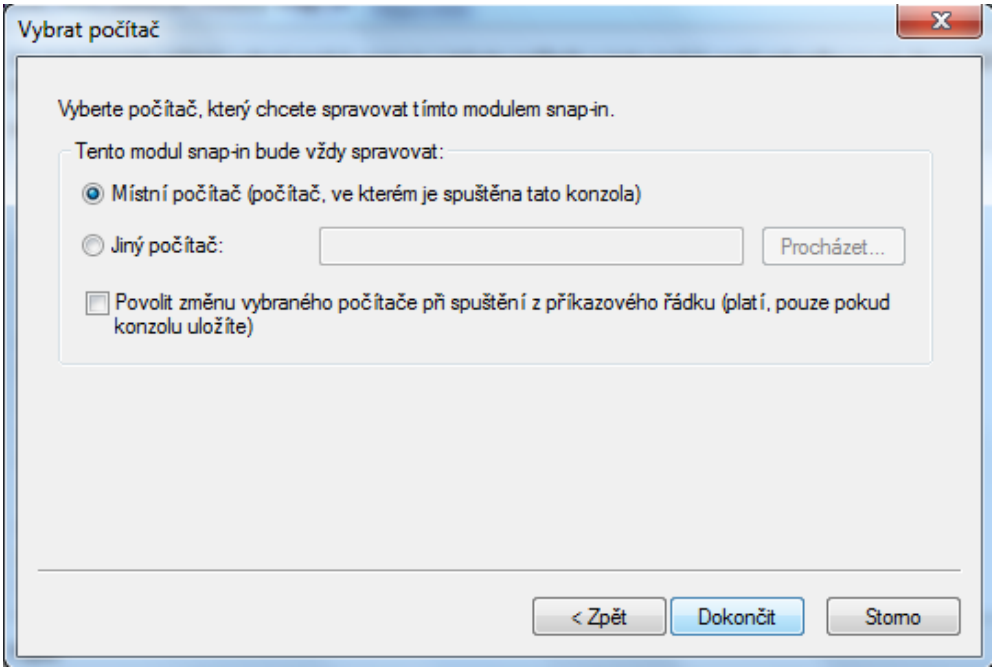


Obrázek 0.2: Získání certifikátu, krok 2

Zaškrtneme Účet počítače a dáme další (viz Obrázek 0.3) a dokončit (viz Obrázek 0.4).

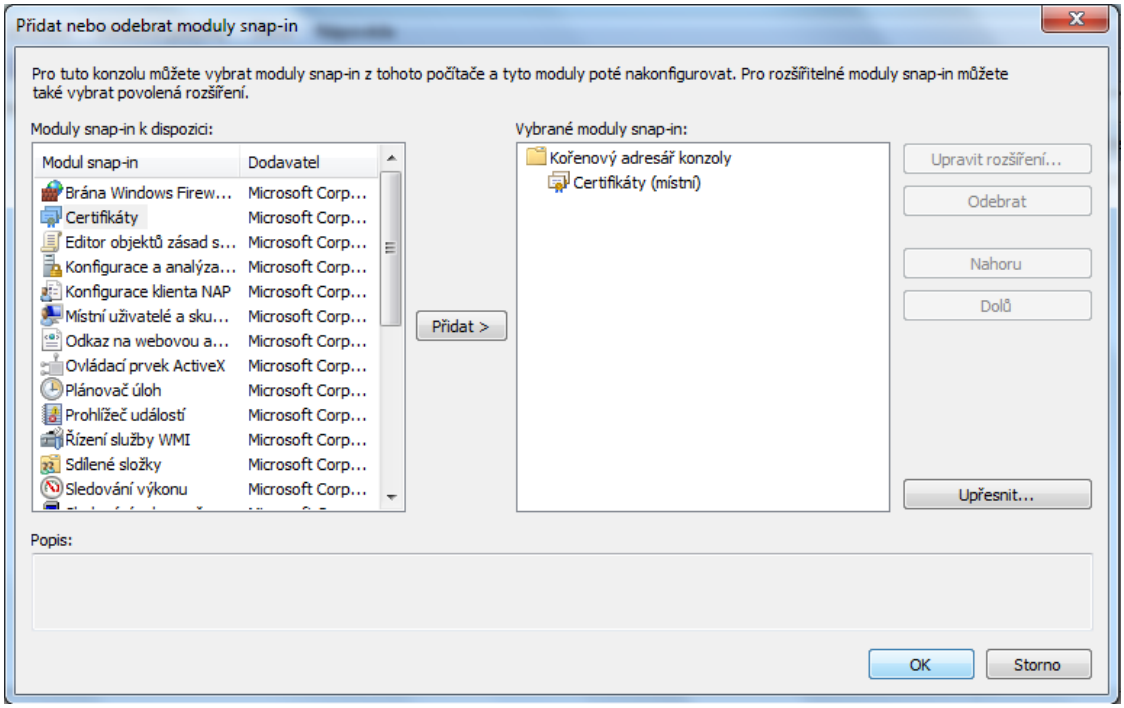


Obrázek 0.3: Získání certifikátu, krok 3



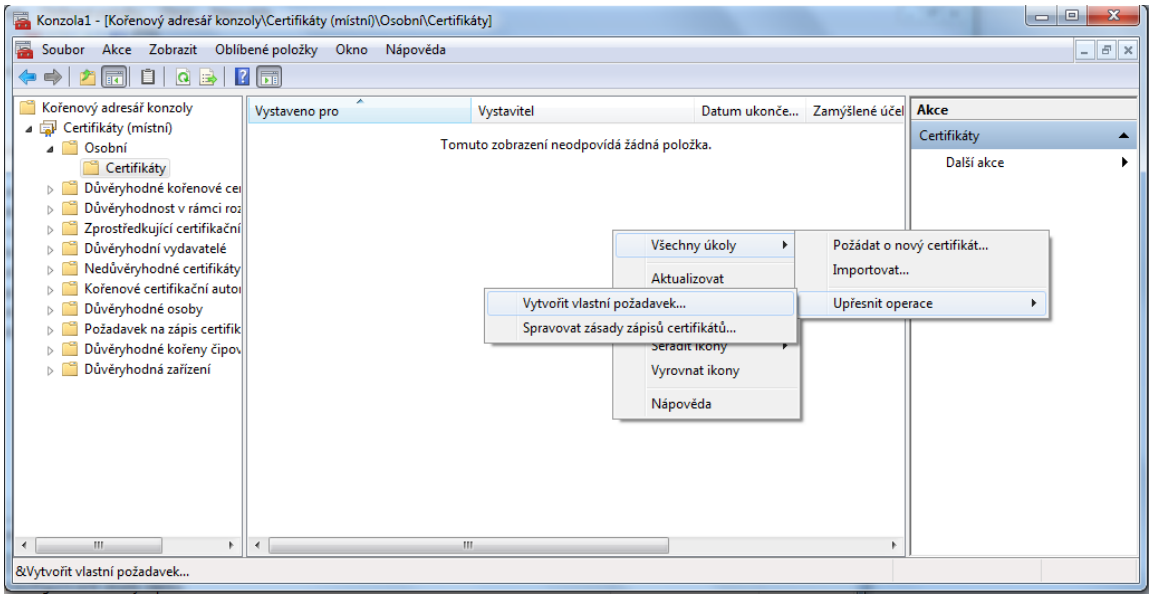
Obrázek 0.4: Získání certifikátu, krok 4

Modul snap-in Certifikáty je vybrán a můžeme dát OK. (viz Obrázek 0.5)



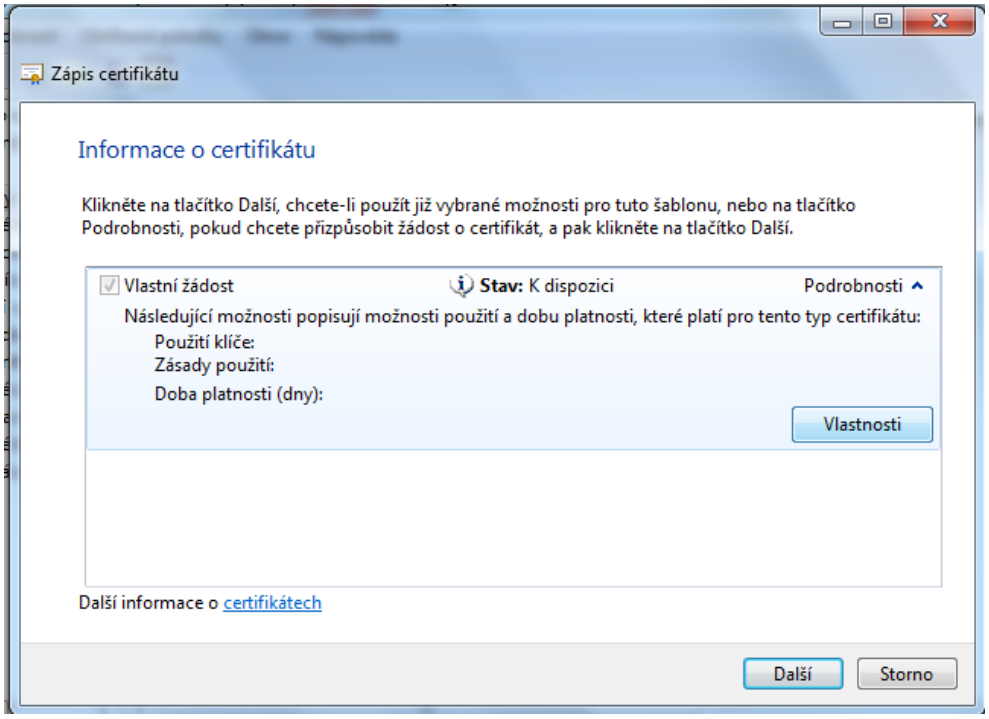
Obrázek 0.5: Získání certifikátu, krok 5

Nyní rozklikneme položku Certifikáty, dále složku Osobní a Certifikáty. Klikneme na Další akce, Všechny úkoly, Upřesnit operace a Vytvořit vlastní požadavek (viz Obrázek 0.6).



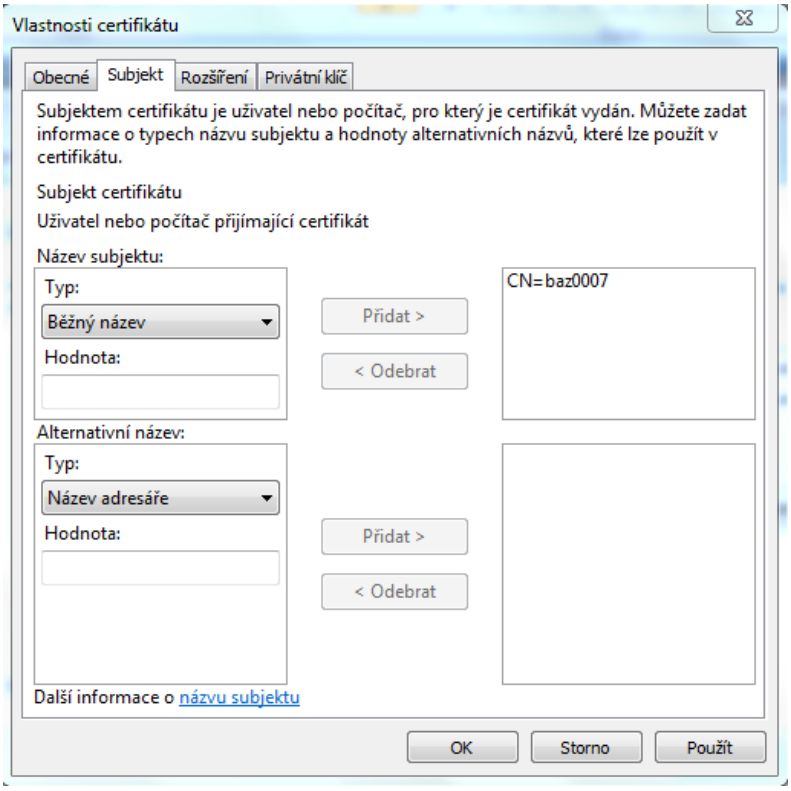
Obrázek 0.6: Získání certifikátu, krok 6

Po otevření postupujeme tlačítkem Další, až narazíme na následující okno (viz Obrázek 0.7), kde klikneme na vlastnosti:



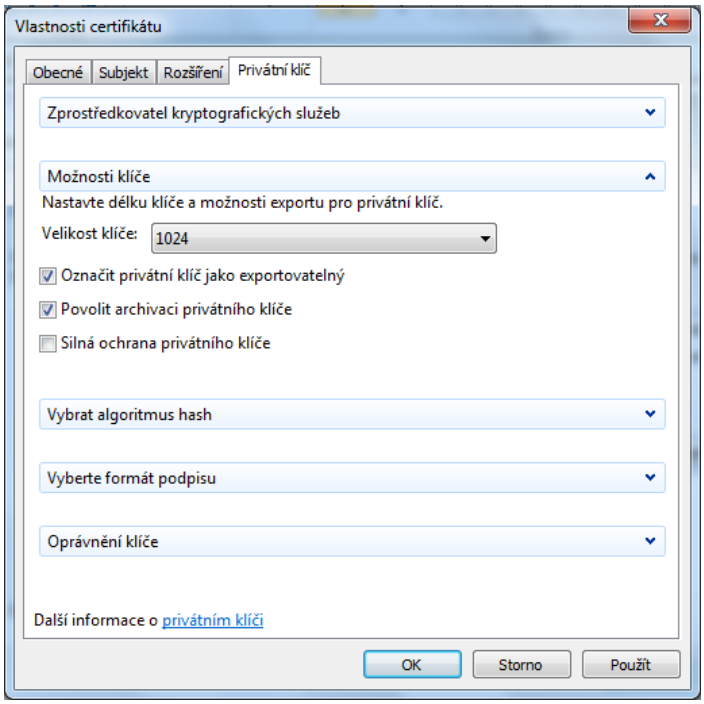
Obrázek 0.7: Získání certifikátu, krok 7

Ve vlastnostech, v záložce subjekt, vybereme typ běžný název, vepíšeme baz0007 a dáme přidat (viz Obrázek 0.8).



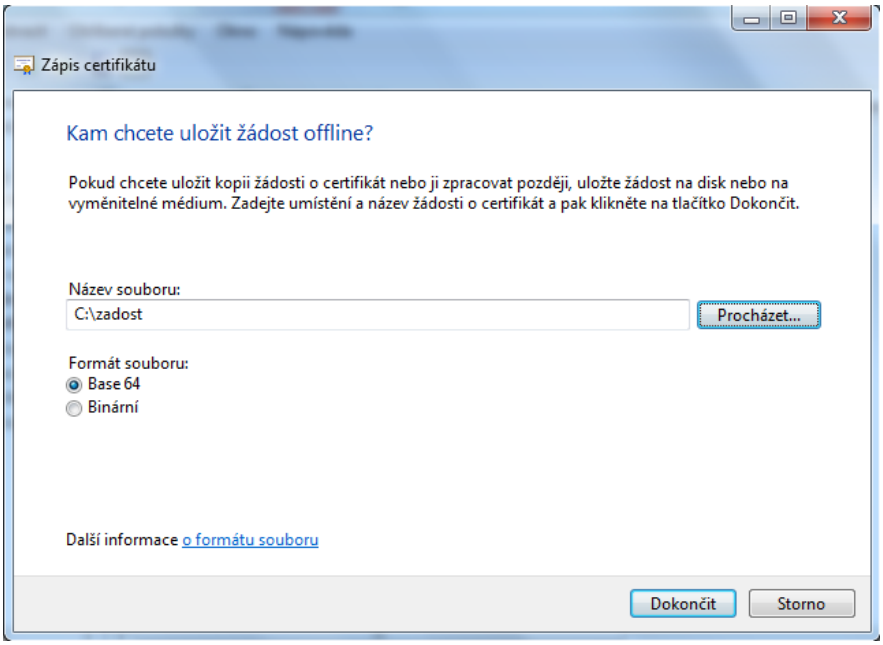
Obrázek 0.8: Získání certifikátu, krok 8

V záložce Privátní klíč klikneme na Možnosti klíče, vybereme privátní klíč jako exportovatelný a povolíme jeho archivaci. Dále klikneme na OK (viz Obrázek 0.9).



Obrázek 0.9: Získání certifikátu, krok 9

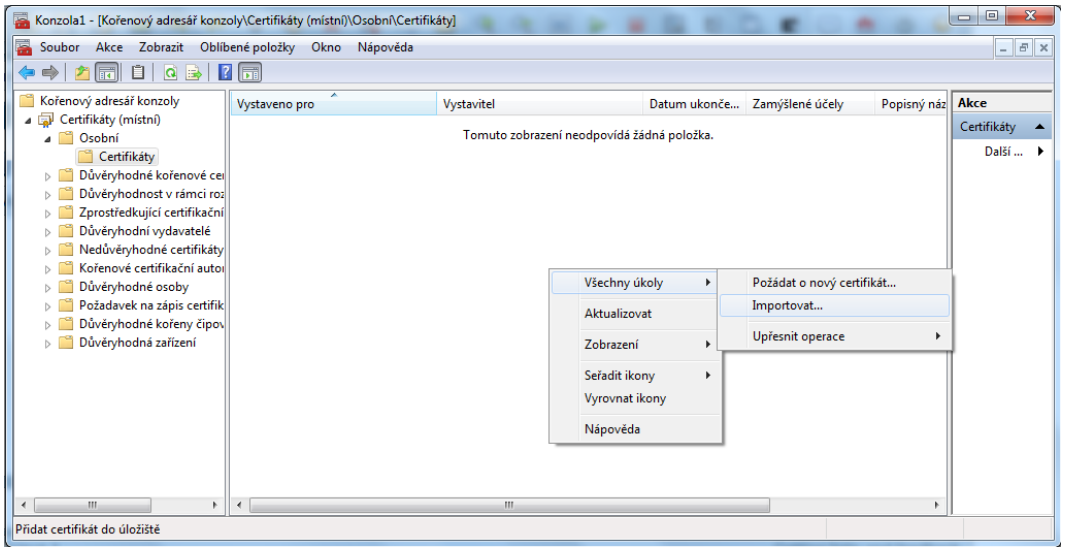
V posledním kroku žádost pojmenujeme a vybereme, kam se má uložit (viz Obrázek 0.10).



Obrázek 0.10: Získání certifikátu, krok 10

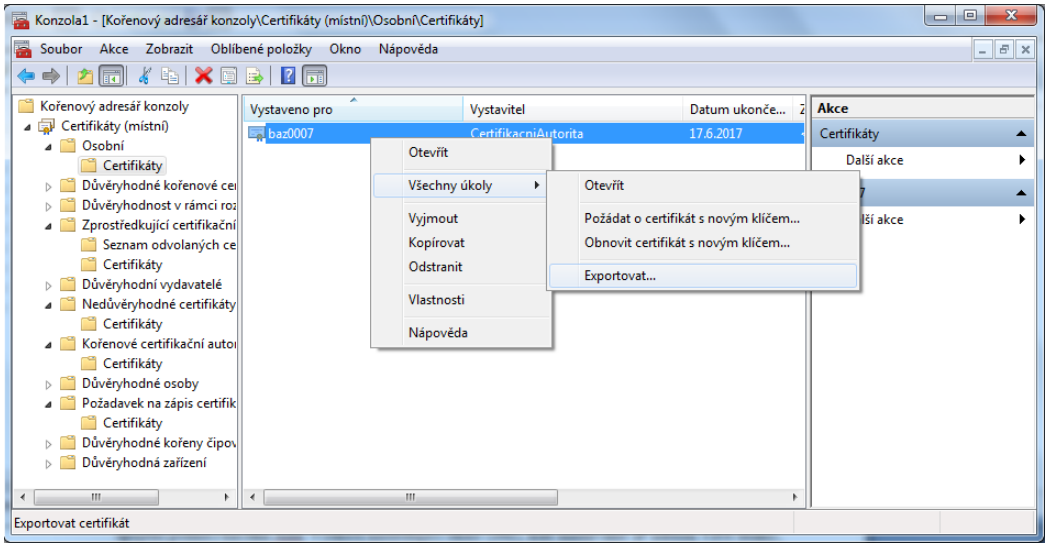
Získaný požadavek zkopírujeme a vytvoříme z něho osobní certifikát stejným způsobem, jako v kapitole 7.3.1. Stejně si uložíme i certifikát certifikační autority.

Obdržíme-li získaný certifikát, importujeme ho způsobem zobrazeným na obrázku 0.11. Klikneme na položku Další, Všechny úkoly a Importovat, kde vybereme osobní certifikát vydaný certifikační autoritou.



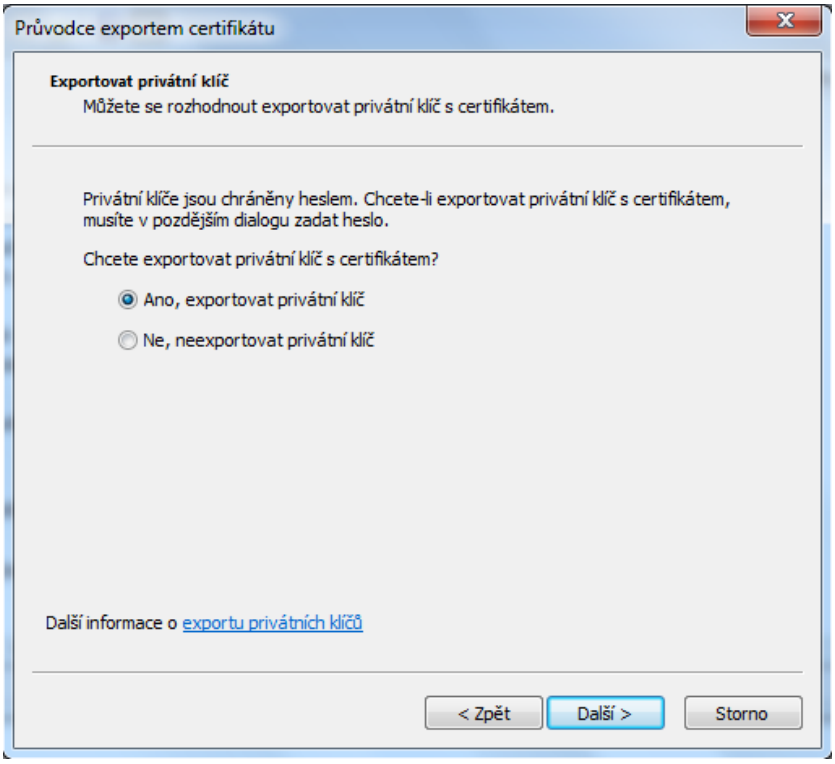
Obrázek 0.11: Import certifikátu

Máme-li importovaný certifikát, můžeme z něho exportovat privátní klíč, který bude potřebný při nastavení VPN klienta (viz Obrázek 0.12).



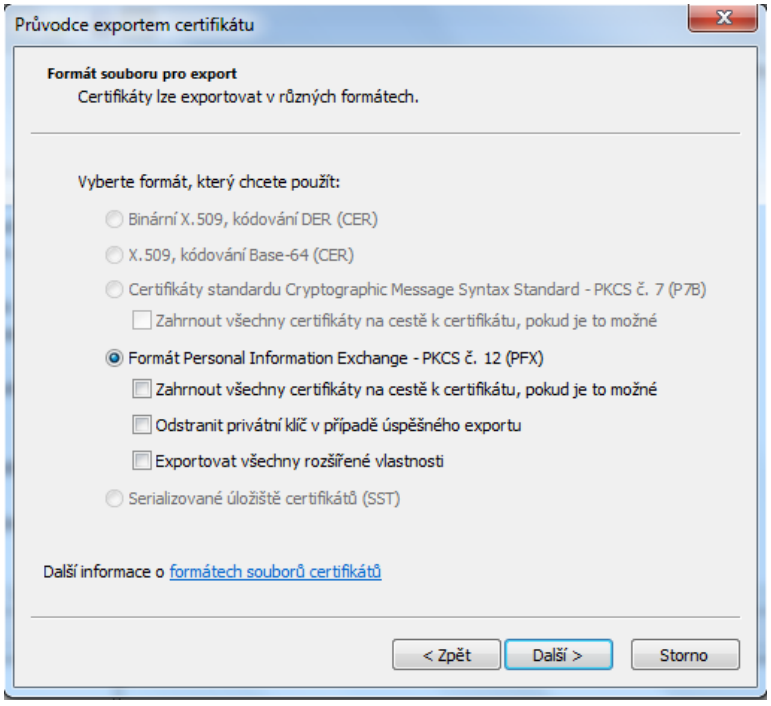
Obrázek 0.12: Export privátního klíče, krok 1

Označíme, že chceme exportovat privátní klíč a poté klikneme na další (viz Obrázek 0.13).



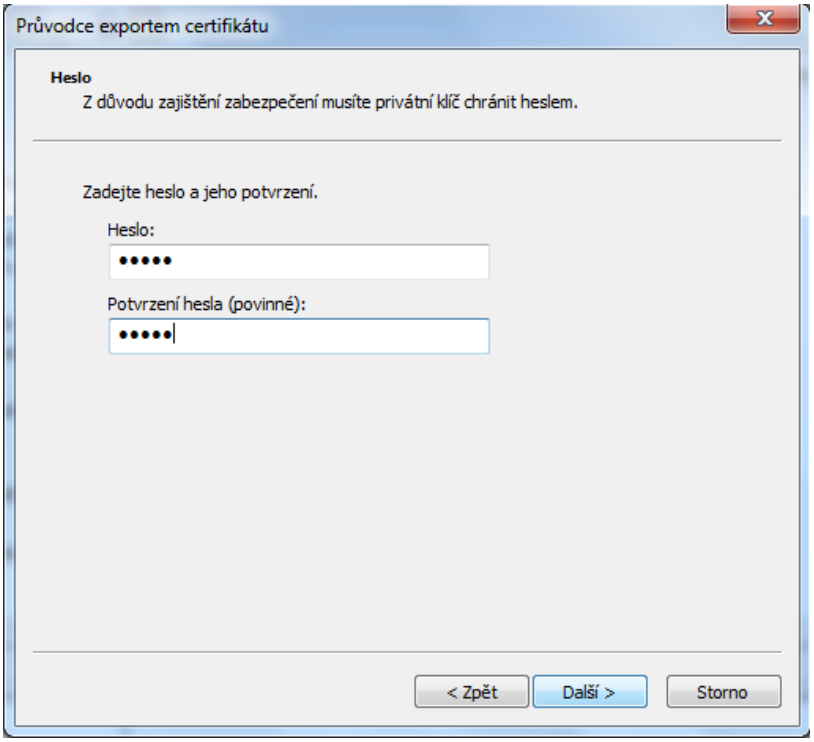
Obrázek 0.13: Export privátního klíče, krok 2

Dále označíme formát PKCS č. 12 a pokračujeme tlačítkem Další (viz Obrázek 0.14).



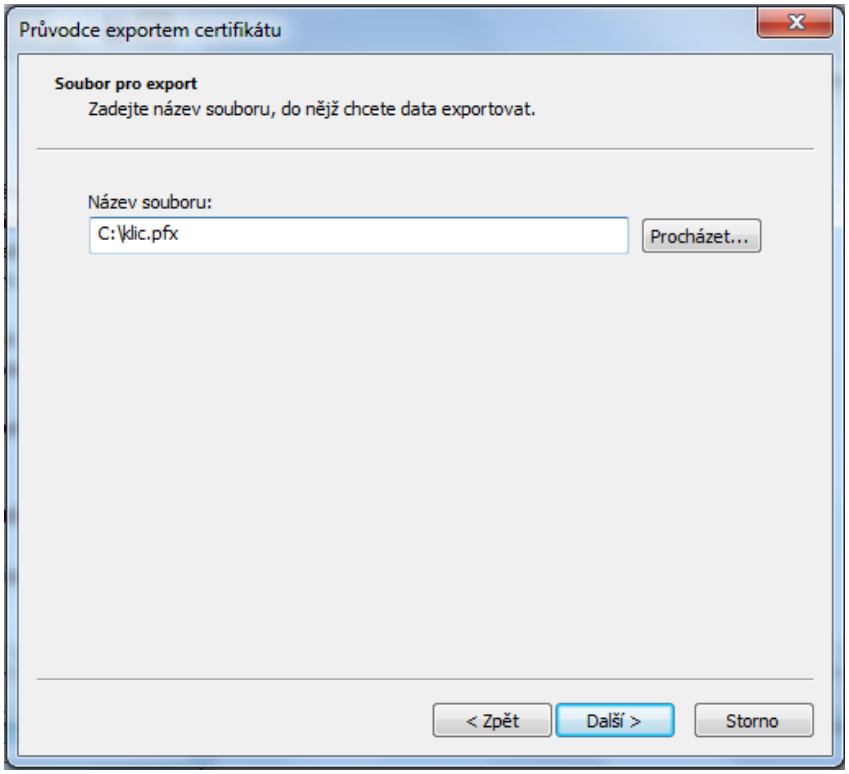
Obrázek 0.14: Export privátního klíče, krok 3

Z důvodu zajištění zabezpečení privátního klíče, zadáme heslo. V našem případě heslo 12345 (viz Obrázek 0.15)



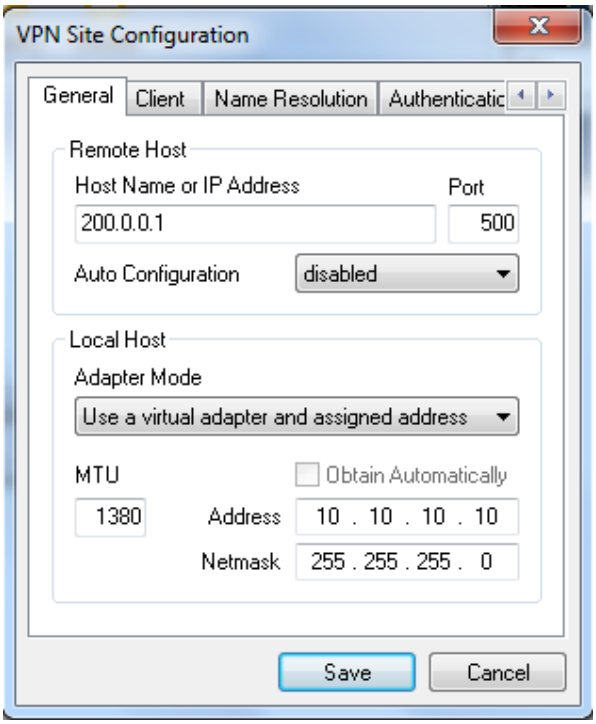
Obrázek 0.15: Export privátního klíče, krok 4

V posledním kroku nastavíme cestu, kam se má privátní klíč uložit a dokončíme jeho export (viz Obrázek 0.16)

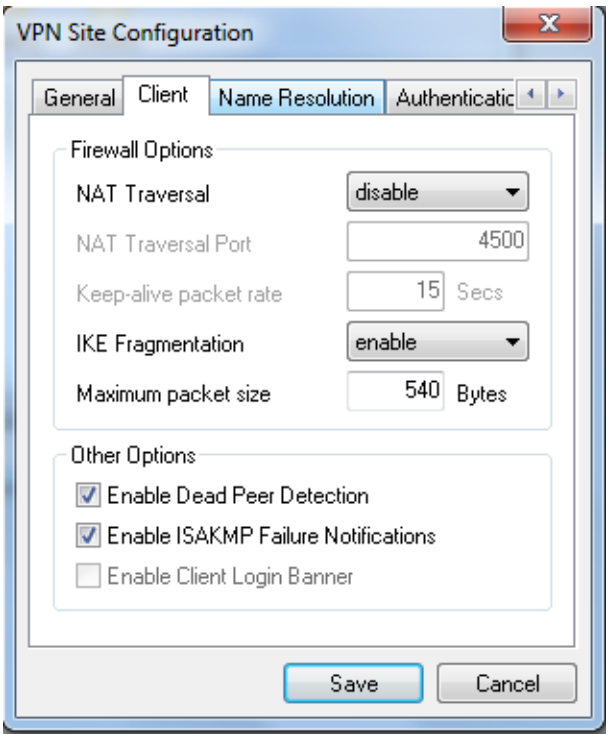


Obrázek 0.16: Export privátního klíče, krok 5

Příloha B: *Nastavení Shrew Soft VPN klienta*

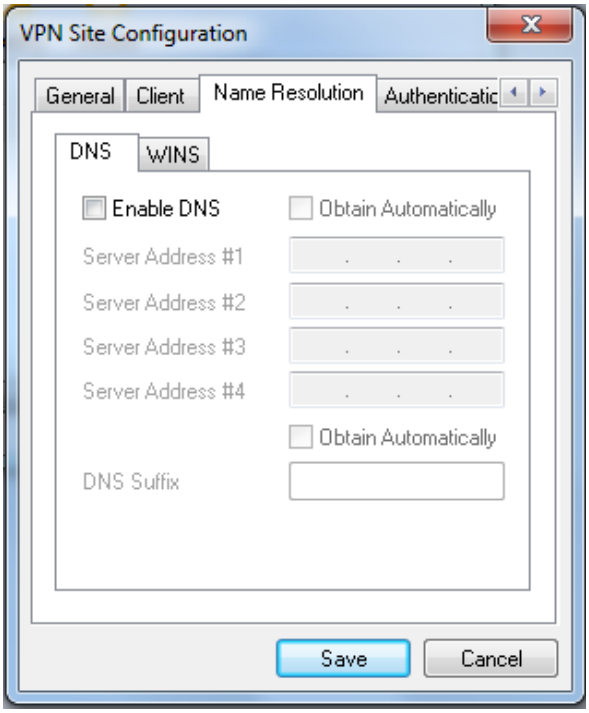


Obrázek 0.17: Nastaveni VPN klienta, krok 1



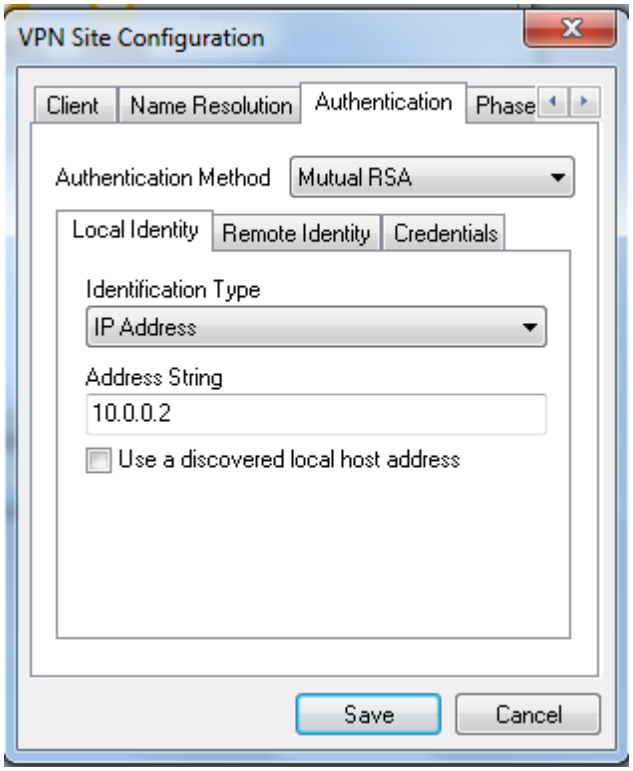
Obrázek 0.18: Nastaveni VPN klienta, krok 2

V záložce Name Resolution vše odškrtneme (viz Obrázek 0.19)

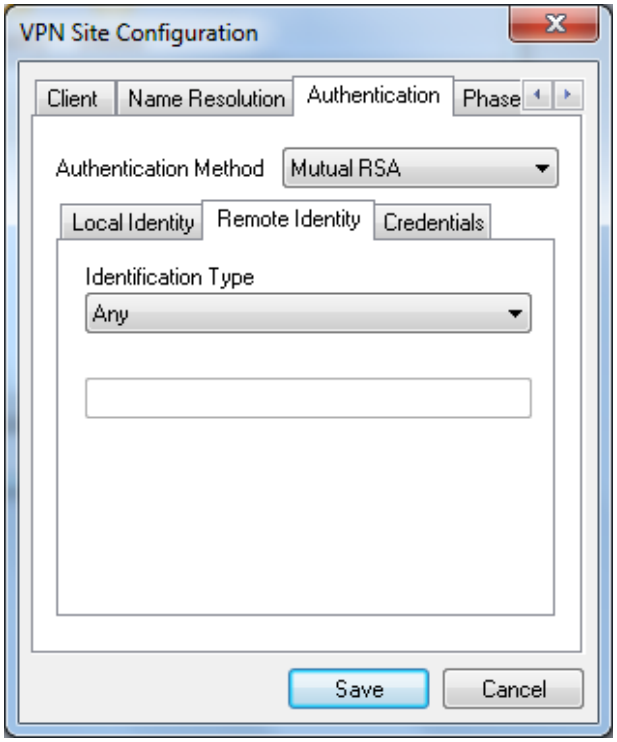


Obrázek 0.19: Nastaveni VPN klienta, krok 3

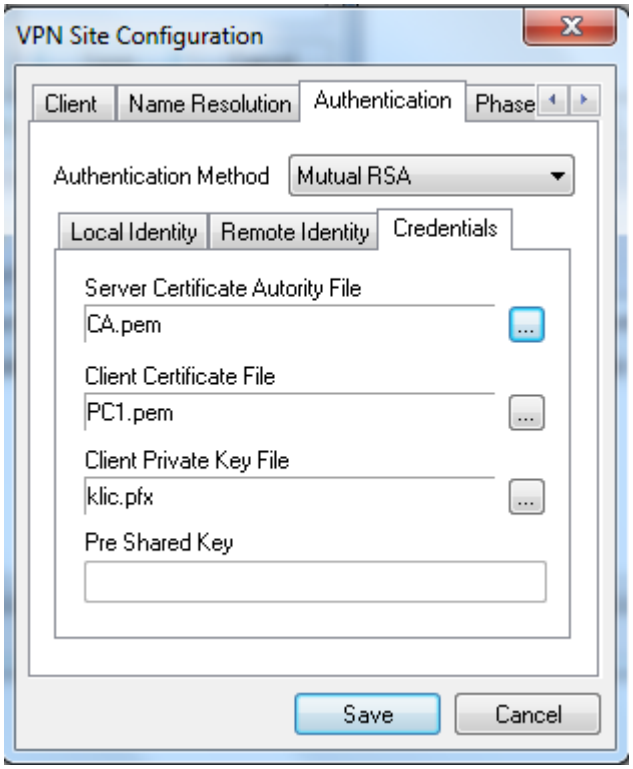
V Záložce Authentication nastavíme metodu ověřování pomocí certifikátů, Místní identitu (viz Obrázek 0.20) jako IP adresu počítače PC1, vzdálenou identitu nastavíme na Any (viz Obrázek 0.21) a v záložce Credentials (viz Obrázek 0.22) vybereme příslušné certifikáty.



Obrázek 0.20: Nastaveni VPN klienta, krok 4

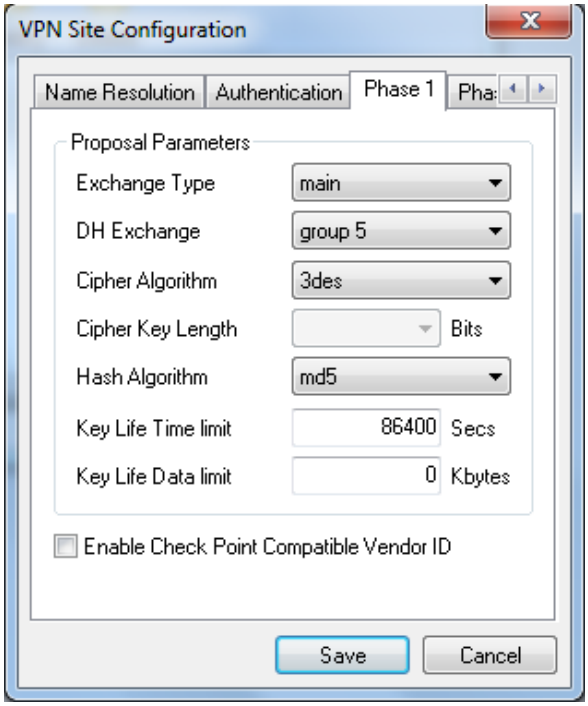


Obrázek 0.21:Nastaveni VPN klienta, krok 5



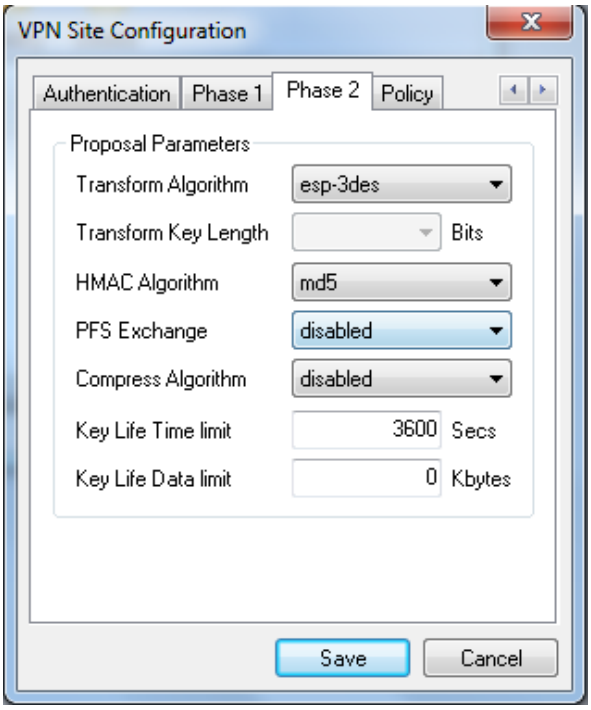
Obrázek 0.22: Nastaveni VPN klienta, krok 6

Následuje již specifikace fáze 1 a fáze 2 IKE protokolu. Nastavíme tady vše stejně tak, jak je nastaveno na směrovači Huawei AR2200. U fáze jedna (viz Obrázek 0.23) se jedna o šifru, hashovací algoritmus a Diffie-Hellmanovu skupinu. Hlavní mód je na směrovači Huawei nastaven defaultně.



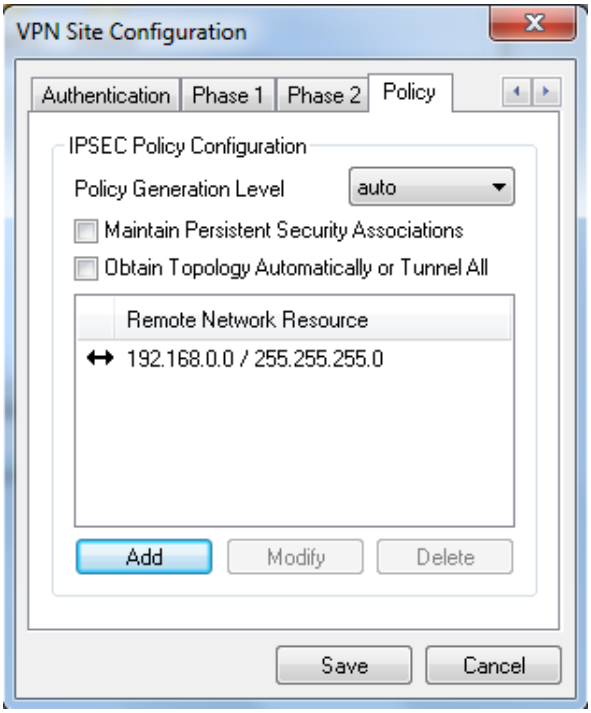
Obrázek 0.23: Nastaveni VPN klienta, krok 7

I u fáze dvě (viz Obrázek 0.24) nastavíme šifrování a hashovaní algoritmus odpovídající nastavením na VPN bráně.



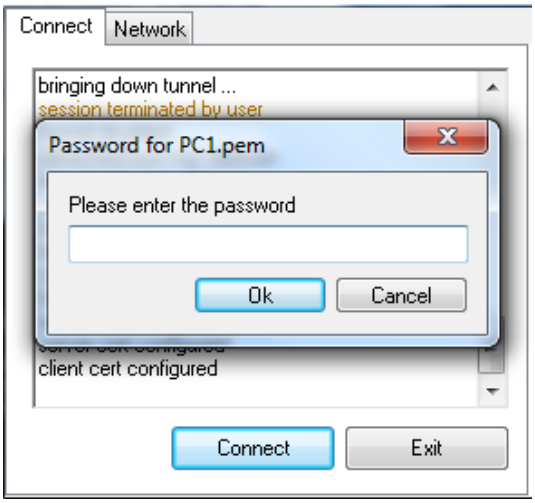
Obrázek 0.24: Nastaveni VPN klienta, krok 8

V poslední záložce (viz Obrázek 0.25) ještě přidáme adresu vzdálené sítě, do které se připojujeme.



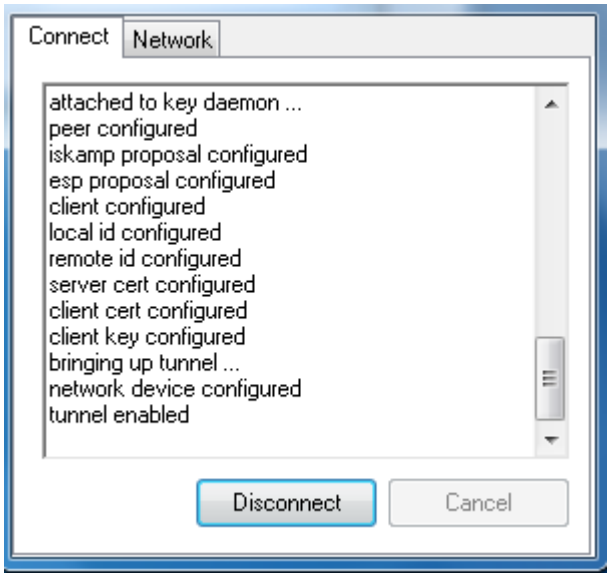
Obrázek 0.25: Nastaveni VPN klienta, krok 9

Následuje již připojení k VPN bráně pomocí tlačítka Connect. VPN klient nás vyzve k zadání hesla pro certifikát počítače PC1(viz Obrázek 0.26). Zadáme heslo 12345 a dáme OK.



Obrázek 0.26: Zadání hesla

Po zadání hesla vyskočí okno, kde můžeme vidět, že všechny konfigurace jsou v pořádku a VPN tunel je aktivní (viz Obrázek 0.27).



Obrázek 0.27: Aktivní tunel

Příloha C: *Konfigurační vypisy použitých síťových zařízení – Cisco ASA*

```
ASA Version 9.1(4)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
ip local pool Adresy 192.168.2.1-192.168.2.20
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 200.0.0.1 255.255.255.0
!
ftp mode passive
object network obj_any
 subnet 0.0.0.0 0.0.0.0
object network obj-vpnpool
 subnet 192.168.2.0 255.255.255.0
pager lines 24
logging asdm informational
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (inside,outside) source static any any destination static obj-vpnpool
obj-vpnpool route-lookup
!
object network obj_any
 nat (inside,outside) dynamic interface
route outside 10.0.2.0 255.255.255.0 10.0.0.2 1
route outside 172.16.0.0 255.255.255.0 10.0.0.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
```

```
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
http server enable
http 192.168.1.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
warmstart
crypto ipsec ikev1 transform-set Prvni esp-3des esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map Mapa1 1 set ikev1 transform-set Prvni
crypto map Mapa2 1 ipsec-isakmp dynamic Mapa1
crypto map Mapa2 interface outside
crypto ca trustpoint CASERVER
 enrollment url http://172.16.0.1:80
 subject-name CN=ASA
 keypair NovyPar
 crl configure
crypto ca trustpool policy
crypto ca certificate map CertMap 1
 subject-name attr o eq vsb
crypto ca certificate chain CASERVER
 certificate 02
    30820219 30820182 a0030201 02020102 300d0609 2a864886 f70d0101 04050030
    1f311d30 1b060355 04031314 43657274 6966696b 61636e69 4175746f 72697461
    301e170d 31363036 30383132 31363530 5a170d31 37303630 38313231 3635305a
    3022310c 300a0603 55040313 03415341 31123010 06092a86 4886f70d 01090216
    03415341 30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181
    00da1b2c 5d68ae35 43d65f22 0e776880 3fc96e7e 573e407e 17881619 5e8883a4
    7e43010e b6edea0f 39723e38 c4db4337 001a9422 10e95674 1caab7b7 ed90d523
    599641fc 5d34b620 d04bee23 2da63876 09a9de8d e135d71d 1330892d f0fd6bdf
    1f9e1a94 6093bbdf 371c0ac7 264f2b93 66996f40 e6031557 0657c035 31bf2f99
    d9020301 0001a362 3060300e 0603551d 11040730 05820341 5341300e 0603551d
    0f0101ff 04040302 05a0301f 0603551d 23041830 168014f5 27cc6c06 3ddaaebd
    ed69e065 24e0bce0 5a6f6730 1d060355 1d0e0416 0414479a 622d1cd1 fa3f78e4
    c749dadd d3bd6c53 ed50300d 06092a86 4886f70d 01010405 00038181 001bdaf4
    c9d1309f 6b8cb287 76de6a53 729341ab ea5277a5 f7b5f84e d2632bb3 011e6ce3
    f11e172d a4af46ae 3ee726f3 ab14120f 5835e7b5 a9eacccb eae7cd9a c8571d14
    11ae507b 5ac66c89 9397769b 74bbc487 49fdd522 6730de16 25e1d499 822b0d90
    25dacd2c f2274a81 32d2a828 bf1679ef 3c5c3a7d 620c283e 418aebdd 6a
  quit
 certificate ca 01
    30820217 30820180 a0030201 02020101 300d0609 2a864886 f70d0101 04050030
    1f311d30 1b060355 04031314 43657274 6966696b 61636e69 4175746f 72697461
    301e170d 31363036 30383130 30393238 5a170d31 39303630 38313030 3932385a
    301f311d 301b0603 55040313 14436572 74696669 6b61636e 69417574 6f726974
    6130819f 300d0609 2a864886 f70d0101 01050003 818d0030 81890281 8100cf10
    aa29e55a d2c4d628 95e2be0d 5eaf0532 0db207e6 8f5f5169 77afcc00 ed791310
    50f8f98c 27ef3413 a0604480 7ba044e4 ce3b3bb0 3f05b92c 4eaa7aa4 b23e8040
    16b62410 28fdd631 af18a1d7 67f4b712 0db2e47e 2793a9d5 c81f1742 fcf1f31c
    abbc05f4 be7b9432 d02092e3 af0a7fd3 d073f40f c3fc310b 2600b939 cfb90203
```

```
    010001a3 63306130 0f060355 1d130101 ff040530 030101ff 300e0603 551d0f01
    01ff0404 03020186 301f0603 551d2304 18301680 14f527cc 6c063dda aebded69
    e06524e0 bce05a6f 67301d06 03551d0e 04160414 f527cc6c 063ddaae bded69e0
    6524e0bc e05a6f67 300d0609 2a864886 f70d0101 04050003 818100c3 a0f9dd53
    67e7d1cd 0742a7f5 cc010911 6767bd63 aba73c65 393512e7 926b6222 c41f9eac
    90e789ff 34320ace 746ca2f7 abdee6f5 50e617ea ab92c4a3 73cb802f ec9c3487
    f751b905 f21f11ca e8aab75d a7467c05 983c62df c1ae890a 9657b1de ac88772c
    ee1016dc 906443a3 3c6a49c2 76084edf 29a79289 1405d086 5999d7
  quit
crypto ikev1 enable outside
crypto ikev1 policy 1
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 43200
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0

dhcpd auto_config outside
!
dhcpd address 192.168.1.5-192.168.1.36 inside
dhcpd enable inside
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
username baz0007 password nCq01dJA2YrB4sT4 encrypted
tunnel-group Profil type remote-access
tunnel-group Profil general-attributes
 address-pool Adresy
tunnel-group Profil ipsec-attributes
 ikev1 trust-point CASERVER
tunnel-group-map enable rules
tunnel-group-map CertMap 1 Profil
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
```

```
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:9c46f4546a90cc60bf225f25c0ce6216
: end

ASA(config)# show isakmp

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.0.2.1
    Type    : user            Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs

Global IKEv1 Statistics
  Active Tunnels:              1
  Previous Tunnels:           12
  In Octets:               69372
  In Packets:                377
  In Drop Packets:            14
  In Notifys:                243
  In P2 Exchanges:            12
  In P2 Exchange Invalids:     0
  In P2 Exchange Rejects:      0
  In P2 Sa Delete Requests:    8
  Out Octets:              42936
  Out Packets:               344
  Out Drop Packets:            0
  Out Notifys:               496
  Out P2 Exchanges:            0
  Out P2 Exchange Invalids:    0
  Out P2 Exchange Rejects:     0
  Out P2 Sa Delete Requests:   3
  Initiator Tunnels:           0
  Initiator Fails:             0
  Responder Fails:             0
  System Capacity Fails:       0
  Auth Fails:                  0
  Decrypt Fails:               0
  Hash Valid Fails:            0
  No Sa Fails:                 0

IKEV1 Call Admission Statistics
  Max In-Negotiation SAs:                 25
  In-Negotiation SAs:                      0
  In-Negotiation SAs Highwater:            1
  In-Negotiation SAs Rejected:             0

Global IKEv2 Statistics
```

```
  Active Tunnels:                         0
  Previous Tunnels:                       0
  In Octets:                              0
  In Packets:                             0
  In Drop Packets:                        0
  In Drop Fragments:                      0
  In Notifys:                             0
  In P2 Exchange:                         0
  In P2 Exchange Invalids:                0
  In P2 Exchange Rejects:                 0
  In IPSEC Delete:                        0
  In IKE Delete:                          0
  Out Octets:                             0
  Out Packets:                            0
  Out Drop Packets:                       0
  Out Drop Fragments:                     0
  Out Notifys:                            0
  Out P2 Exchange:                        0
  Out P2 Exchange Invalids:               0
  Out P2 Exchange Rejects:                0
  Out IPSEC Delete:                       0
  Out IKE Delete:                         0
  SAs Locally Initiated:                  0
  SAs Locally Initiated Failed:           0
  SAs Remotely Initiated:                 0
  SAs Remotely Initiated Failed:          0
  System Capacity Failures:               0
  Authentication Failures:                0
  Decrypt Failures:                       0
  Hash Failures:                          0
  Invalid SPI:                            0
  In Configs:                             0
  Out Configs:                            0
  In Configs Rejects:                     0
  Out Configs Rejects:                    0
  Previous Tunnels:                       0
  Previous Tunnels Wraps:                 0
  In DPD Messages:                        0
  Out DPD Messages:                       0
  Out NAT Keepalives:                     0
  IKE Rekey Locally Initiated:            0
  IKE Rekey Remotely Initiated:           0
  CHILD Rekey Locally Initiated:          0
  CHILD Rekey Remotely Initiated:         0

IKEV2 Call Admission Statistics
  Max Active SAs:                     No Limit
  Max In-Negotiation SAs:                   12
  Cookie Challenge Threshold:                6
  Active SAs:                                0
  In-Negotiation SAs:                        0
  Incoming Requests:                         0
  Incoming Requests Accepted:                0
  Incoming Requests Rejected:                0
  Outgoing Requests:                         0
  Outgoing Requests Accepted:                0
  Outgoing Requests Rejected:                0
  Rejected Requests:                         0
  Rejected Over Max SA limit:                0
```

```
  Rejected Low Resources:                  0
  Rejected Reboot In Progress:             0
  Cookie Challenges:                       0
  Cookie Challenges Passed:                0
  Cookie Challenges Failed:                0

Global IKEv1 IPSec over TCP Statistics
--------------------------------
Embryonic connections: 0
Active connections: 0
Previous connections: 0
Inbound packets: 0
Inbound dropped packets: 0
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 0
Recevied ACK heart-beat packets: 0
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0

ASA(config)# show ipsec sa
interface: outside
    Crypto map tag: Mapa1, seq num: 1, local addr: 200.0.0.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/0/0)
      current_peer: 10.0.2.1, username: baz0007
      dynamic allocated peer ip: 192.168.2.1
      dynamic allocated peer ip(ipv6): 0.0.0.0

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 37, #pkts decrypt: 37, #pkts verify: 37
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing
reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 200.0.0.1/0, remote crypto endpt.: 10.0.2.1/0
      path mtu 1500, ipsec overhead 58(36), media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: 47680B75
      current inbound spi : 665BED98

    inbound esp sas:
      spi: 0x665BED98 (1717300632)
         transform: esp-3des esp-md5-hmac no compression
         in use settings ={RA, Tunnel, IKEv1, }
         slot: 0, conn_id: 61440, crypto-map: Mapa1
         sa timing: remaining key lifetime (sec): 28781
         IV size: 8 bytes
         replay detection support: Y
```

```
        Anti replay bitmap:
         0x000007FF 0xFFFFFFFF
    outbound esp sas:
      spi: 0x47680B75 (1198001013)
        transform: esp-3des esp-md5-hmac no compression
        in use settings ={RA, Tunnel, IKEv1, }
        slot: 0, conn_id: 61440, crypto-map: Mapa1
        sa timing: remaining key lifetime (sec): 28781
        IV size: 8 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001
```

Příloha D: *Konfigurační výpisy použitých síťových zařízení – Cisco 2800*

```
Building configuration...


Current configuration : 4931 bytes
!
! Last configuration change at 16:17:07 UTC Mon Jun 20 2016
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
```

```
no service password-encryption
!
hostname Cisco_2800
!
boot-start-marker
boot system flash:c2801-advipservicesk9-mz.124-22.T.bin
boot-end-marker
!
logging message-counter syslog
enable secret 5 $1$tETF$AA/3hBpteKLe5qAceLB0.0
!
aaa new-model
!
!
aaa authentication login VPN local
aaa authorization network VPN local
!
!
aaa session-id common
dot11 syslog
ip source-route
!
!
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated

!
voice-card 0
!
!
crypto pki trustpoint CASERVER
```

```
 enrollment url http://172.16.0.1:80
 usage ike
 subject-name CN=Cisco
 revocation-check crl
 rsakeypair NovyPar
!
!
crypto pki certificate chain CASERVER
 certificate 0A
  3082020F 30820178 A0030201 0202010A 300D0609 2A864886 F70D0101 04050030
  1F311D30 1B060355 04031314 43657274 6966696B 61636E69 4175746F 72697461
  301E170D 31363036 32303135 31313538 5A170D31 37303632 30313531 3135385A
  302B310E 300C0603 55040313 05436973 636F3119 30170609 2A864886 F70D0109
  02160A43 6973636F 5F323830 3030819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100B7BF CBD61997 DFB65D11 80F078A4 722C6A7F EA543B12
  2AF6F2D1 5DCA8656 8836C6AA 758AA0C8 1BCF8726 92865276 09770EBD D826E0BE
  38D99B19 7FC3E7C1 3495A622 52F1E465 7F6AE6E8 64C8734E CAC051BE 357A050D
  88D58613 C3EEC471 95B7E6E7 E2EDF18B 5493B22F 51C4DA55 3661F56A 8E97AA64
  F9CC03C0 A890139F 29D30203 010001A3 4F304D30 0B060355 1D0F0404 030205A0
  301F0603 551D2304 18301680 1493BBF0 6F92C8AF B7F6CAF1 9DBF353B 1A57F228
  5E301D06 03551D0E 04160414 641DB54B 0A32E172 74EE5FCA 70BE8114 46302FFD
  300D0609 2A864886 F70D0101 04050003 8181003B 591983FC EF7E5999 78328AD4
  11F62F3B 80F1A252 666F5BCC D8F25756 8DB6B853 6305E97C B42D1E2B 16831285
  B66C2C92 20EFCB56 7D14A12C E09C4DE0 D319D246 BB0CDE29 AD7603BE F7AF43F1
  BB387BF0 86E80D6E 311BDBD0 670BD328 62C4988B 78D4319D 60AAB69A F3D41BCB
  EF44EF26 5576D6B2 128E518A E13AFBD2 8B7477
        quit
 certificate ca 01
  30820217 30820180 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  1F311D30 1B060355 04031314 43657274 6966696B 61636E69 4175746F 72697461
  301E170D 31363036 32303130 32333535 5A170D31 39303632 30313032 3335355A
  301F311D 301B0603 55040313 14436572 74696669 6B61636E 69417574 6F726974
  6130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100CF0A
  648DCBC6 03A4D61A 7397AB29 5953E44B 65693622 3FEDCDB0 FDD6C28F 683AE0FB
  A8ECA87F 08002903 935A874E C8386BE1 D169070D 3BFB9814 20897FD5 9D3523A1
```

```
  30660EF9 C52F160A B1760722 198CC118 DC9736CA 6F2C620C 1EB4B211 262BAE8A
  0C0BDB9B E1D3802C 044288D6 4C21AF43 5001A7A1 3511A416 123CD1B9 DD430203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 1493BBF0 6F92C8AF B7F6CAF1
  9DBF353B 1A57F228 5E301D06 03551D0E 04160414 93BBF06F 92C8AFB7 F6CAF19D
  BF353B1A 57F2285E 300D0609 2A864886 F70D0101 04050003 818100C6 CC377BF6
  7432A8B5 43BCA3E2 5F8CC58C 2ADCCC6B AA7DDE3A 6C0184ED 92C7B088 C1B13585
  56667F3E 7F4D3514 B0C01158 0241C48B D7A20E1A 9099161A 1391891A EAAAB817
  25FF7377 82588BDD A0726FDF C811F0B6 57D9702F 63476BA0 390E915A C806B084
  736C9E90 2D0A9441 0BEA9A49 F5E29204 7AED94D6 7F53F1FC 398FEA
        quit
!
!
username baz0007 password 0 cisco
username admin privilege 15 password 0 cisco
archive
 log config
  hidekeys
!
!
crypto isakmp policy 1
 encr aes
 group 2
crypto isakmp identity dn
!
crypto isakmp client configuration group VPNSKUPINA
 pool VPNAdresy
 acl VPNACL
!
!
crypto ipsec transform-set T1 esp-aes 256 esp-sha-hmac
!
crypto dynamic-map DYNMAP 10
 set transform-set T1
 reverse-route
```

```
!
!
!
crypto map VPN client authentication list VPN
crypto map VPN isakmp authorization list VPN
crypto map VPN client configuration address respond
crypto map VPN 10 ipsec-isakmp dynamic DYNMAP
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 200.0.0.1 255.255.255.0
 duplex auto
 speed auto
 crypto map VPN
!
interface Serial0/1/0
 no ip address
 shutdown
 no fair-queue
 clock rate 125000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 125000
```

```
!
interface Serial0/2/0
 no ip address
 shutdown
 clock rate 125000
!
interface Serial0/2/1
 no ip address
 shutdown
 clock rate 125000
!
ip local pool VPNAdresy 192.168.2.1 192.168.2.30
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 200.0.0.2
ip http server
no ip http secure-server
!
!
!
ip access-list extended VPNACL
 permit ip 192.168.0.0 0.0.0.255 192.168.2.0 0.0.0.255
!
!
control-plane
!


!
ccm-manager fax protocol cisco
!
mgcp fax t38 ecm
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
```

```
line aux 0
line vty 0 4
!
scheduler allocate 20000 1000
end
Cisco_2800#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
200.0.0.1       10.0.0.2        QM_IDLE           1043 ACTIVE

IPv6 Crypto ISAKMP SA

Cisco_2800#show crypto ipsec sa
     PFS (Y/N): N, DH group: none

interface: FastEthernet0/1
    Crypto map tag: VPN, local addr 200.0.0.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.2.11/255.255.255.255/0/0)
   current_peer 10.0.0.2 port 57740
     PERMIT, flags={}
    #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 200.0.0.1, remote crypto endpt.: 10.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/1
     current outbound spi: 0x150D4AC0(353192640)
```

```
     inbound esp sas:
      spi: 0x14C4BE97(348438167)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2019, flow_id: FPGA:19, sibling_flags 80000046, crypto
map: VPN
        sa timing: remaining key lifetime (k/sec): (4396297/3398)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x150D4AC0(353192640)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2020, flow_id: FPGA:20, sibling_flags 80000046, crypto
map: VPN
        sa timing: remaining key lifetime (k/sec): (4396297/3398)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:



Cisco_2800#show crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 0A
```

```
  Certificate Usage: General Purpose
  Issuer:
    cn=CertifikacniAutorita
  Subject:
    Name: Cisco_2800
    hostname=Cisco_2800
    cn=Cisco
  Validity Date:
    start date: 15:11:58 UTC Jun 20 2016
    end   date: 15:11:58 UTC Jun 20 2017
  Associated Trustpoints: CASERVER

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=CertifikacniAutorita
  Subject:
    cn=CertifikacniAutorita
  Validity Date:
    start date: 10:23:55 UTC Jun 20 2016
    end   date: 10:23:55 UTC Jun 20 2019
  Associated Trustpoints: CASERVER
```

Příloha E: *Konfigurační výpisy použitých síťových zařízení – Huawei AR2200*

```
[V200R005C20SPC200]
#
 sysname AR2200
#
 drop illegal-mac alarm
#
pki entity AR2200
 common-name 2200
#
pki realm VPN
 ca id CASERVER
 entity AR2200
#
pki realm default
 enrollment self-signed
#
acl number 3000
 rule 5 permit ip source 192.168.0.0 0.0.0.255 destination
10.10.10.10 0
#
ipsec proposal Faze2
 esp encryption-algorithm 3des
#
ike proposal 5
 encryption-algorithm 3des-cbc
 dh group5
 authentication-algorithm md5
 authentication-method rsa-signature
#
ike peer peer1 v1
 ike-proposal 5
 pki realm VPN
#
```

```
ipsec policy-template Sablona 10
 ike-peer peer1
 proposal Faze2
 security acl 3000
#
 ipsec policy Politika1 1 isakmp template Sablona
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password irreversible-cipher %@%@i@@022WH&OJUtb-
'6iWN\9}vu"0DZgQW^U'T]dAN+8v~9}y\%@%@
 local-user admin service-type http
#
firewall zone Local
 priority 64
#
interface GigabitEthernet0/0/0
 ip address 192.168.0.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 ip address 200.0.0.1 255.255.255.0
 ipsec policy Politika1
#
interface GigabitEthernet0/0/2
#
interface Cellular0/0/0
#
interface Cellular0/0/1
#
interface NULL0
#
```

```
 snmp-agent local-engineid 800007DB030819A69B6D4D
#
ip route-static 0.0.0.0 0.0.0.0 200.0.0.2
#
user-interface con 0
 authentication-mode password
 set authentication password cipher %@%@"f4.T]V`i<0Q-
l:WpaHA,.P"6GouOt5GpFnu>4$8.}R+.P%,%@%@
user-interface vty 0 4
#
wlan ac
#
voice
 #
 diagnose
#
Return
<AR2200>display ike sa
    Conn-ID  Peer            VPN   Flag(s)                Phase
  -----------------------------------------------------------------
      242    10.0.0.2        0     RD|ST                  2
      232    10.0.0.2        0     RD                     1

  Flag Description:
  RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
  HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
[AR2200]display ipsec sa

===============================
Interface: GigabitEthernet0/0/1
 Path MTU: 1500
===============================

  ----------------------------
  IPSec policy name: "Politika1"
```

```
  Sequence number  : 1
  Acl group        : 3000
  Acl rule         : 5
  Mode             : ISAKMP
  -----------------------------
    Connection ID     : 251
    Encapsulation mode: Tunnel
    Tunnel local      : 200.0.0.1
    Tunnel remote     : 10.0.0.2
    Flow source       : 192.168.0.0/255.255.255.0 0/0
    Flow destination  : 10.10.10.10/255.255.255.255 0/0
    Qos pre-classify  : Disable
    Qos group         : -

    [Outbound ESP SAs]
      SPI: 3257253873 (0xc225bff1)
      Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-MD5
      SA remaining key duration (bytes/sec): 0/3537
      Max sent sequence-number: 4
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
      SPI: 1276174260 (0x4c10dfb4)
      Proposal: ESP-ENCRYPT-3DES-192 ESP-AUTH-MD5
      SA remaining key duration (bytes/sec): 0/3537
      Max received sequence-number: 4
      Anti-replay window size: 32
      UDP encapsulation used for NAT traversal: N

<AR2200>display ike proposal

Number of IKE Proposals: 2

-----------------------------------------
```

```
 IKE Proposal: 5
   Authentication method      : rsa-signature
   Authentication algorithm   : MD5
   Encryption algorithm       : 3DES-CBC
   DH group                   : MODP-1536
   SA duration                : 86400
   PRF                        : PRF-HMAC-SHA
-----------------------------------------


-----------------------------------------
 IKE Proposal: Default
   Authentication method      : pre-shared
   Authentication algorithm   : SHA1
   Encryption algorithm       : DES-CBC
   DH group                   : MODP-768
   SA duration                : 86400
   PRF                        : PRF-HMAC-SHA
-----------------------------------------
```

Příloha F: *Konfigurační výpisy použitých síťových zařízení – CA Server*

```
Current configuration : 2832 bytes
!
! Last configuration change at 13:49:31 UTC Wed Jun 8 2016
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CASERVER
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
!
!
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
cts logging verbose
!
crypto pki server CASERVER
 no database archive
 issuer-name CN=CertifikacniAutorita
 grant auto
 database url nvram
!
crypto pki trustpoint CASERVER
 revocation-check crl
 rsakeypair CASERVER
!
!
crypto pki certificate chain CASERVER
 certificate ca 01
  30820217 30820180 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  1F311D30 1B060355 04031314 43657274 6966696B 61636E69 4175746F 72697461
  301E170D 31363036 30383130 30393238 5A170D31 39303630 38313030 3932385A
  301F311D 301B0603 55040313 14436572 74696669 6B61636E 69417574 6F726974
  6130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100CF10
  AA29E55A D2C4D628 95E2BE0D 5EAF0532 0DB207E6 8F5F5169 77AFCC00 ED791310
  50F8F98C 27EF3413 A0604480 7BA044E4 CE3B3BB0 3F05B92C 4EAA7AA4 B23E8040
  16B62410 28FDD631 AF18A1D7 67F4B712 0DB2E47E 2793A9D5 C81F1742 FCF1F31C
  ABBC05F4 BE7B9432 D02092E3 AF0A7FD3 D073F40F C3FC310B 2600B939 CFB90203
  010001A3 63306130 0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01
  01FF0404 03020186 301F0603 551D2304 18301680 14F527CC 6C063DDA AEBDED69
  E06524E0 BCE05A6F 67301D06 03551D0E 04160414 F527CC6C 063DDAAE BDED69E0
  6524E0BC E05A6F67 300D0609 2A864886 F70D0101 04050003 818100C3 A0F9DD53
  67E7D1CD 0742A7F5 CC010911 6767BD63 ABA73C65 393512E7 926B6222 C41F9EAC
  90E789FF 34320ACE 746CA2F7 ABDEE6F5 50E617EA AB92C4A3 73CB802F EC9C3487
```

```
  F751B905 F21F11CA E8AAB75D A7467C05 983C62DF C1AE890A 9657B1DE AC88772C
  EE1016DC 906443A3 3C6A49C2 76084EDF 29A79289 1405D086 5999D7
        quit
license udi pid CISCO2901/K9 sn FCZ1937C19F
!
!
!
redundancy
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/1/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/1/1
 no ip address
 shutdown
 clock rate 2000000
!
ip default-gateway 100.0.0.2
ip forward-protocol nd
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 172.16.0.2
!
!
!
!
control-plane
!
!
!
line con 0
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
```

```
line vty 0 4
 login
 transport input none
!
scheduler allocate 20000 1000
!
end
```