

Využití virtuálních privátních sítí pro vzdálenou správu aktivních prvků

The Use of Virtual Private Networks for Remote Management of
Active Network Elements

Adam Viktorin

Bakalářská práce
2013



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Adam VIKTORIN**
Osobní číslo: **A10067**
Studijní program: **B3902 Inženýrská informatika**
Studijní obor: **Informační a řídicí technologie**
Forma studia: **prezenční**

Téma práce: **Využití virtuálních privátních sítí pro vzdálenou správu aktivních prvků**

Zásady pro vypracování:

1. Zpracujte literární rešerši na dané téma.
2. Navrhněte univerzální konfiguraci VPN pro propojení 2 LAN oddělených Internetem pomocí směrovačů CISCO.
3. Konfiguraci VPN ověřte na směrovačích CISCO akademie FAI.
4. Ověřte na takto vytvořené VPN vzdálenou správu aktivních prvků.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. PUŽMANOVÁ, Rita. TCP/IP v kostce. 2. upr. a rozš. vyd. České Budějovice: Kopp, 2009, 619 s. ISBN 978-80-7232-388-3.
2. MASON, Andrew G. Cisco secure virtual private networks. Indianapolis: Cisco Press, 2002, 388 p. ISBN 1-58705-033-1.
3. LEWIS, Mark. Comparing, designing, and deploying VPNs. Indianapolis: Cisco Press, 2006, 1043 p. ISBN 1-58705-179-6.
4. Seriál Tuneluji, tuneluješ, tunelujeme - Root.cz [online]. 2003 [cit. 2013-02-04]. Dostupné z: <http://www.root.cz/serialy/tuneluji-tunelujes-tunelujeme/>
5. OpenVPN - Open Source VPN [online]. 2002 - 2013 [cit. 2013-02-04]. Dostupné z: <http://openvpn.net/>

Vedoucí bakalářské práce:

Ing. Miroslav Matýsek, Ph.D.

Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce:

24. února 2013

Termín odevzdání bakalářské práce:

14. června 2013

Ve Zlíně dne 24. února 2013

prof. Ing. Vladimír Vašek, CSc.
děkan



prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato práce představuje technologie virtuálních privátních sítí a poskytuje návod na jednoduché zprovoznění IPsec VPN. V první části, se práce věnuje rozdělení a vlastnostem jednotlivých technologií. Dále je do detailu rozebrána a popsána IPsec VPN, která je ve druhé části použita pro praktické řešení zabezpečeného propojení dvou LAN oddělených Internetem. Konfigurace aktivních síťových prvků jsou navrženy a vytvořeny v software Cisco Packet Tracer 5.3.3 a následně ověřeny na směrovačích Cisco akademie FAI.

Klíčová slova: Virtuální privátní síť, směrovač, konfigurace, IPsec, Cisco Packet Tracer.

ABSTRACT

This thesis is presenting virtual private network technologies and providing easy step – by – step manual for deploying IPsec VPN. The first part is aimed to dividing and describing VPN technologies. The IPsec VPN technology is than examined in detail and it's used in the second part of the thesis for deployment of secure connection of two LANs separated by Internet. The configuration of active network elements is designed and made in Cisco Packet Tracer 5.3.3 software and subsequently tested on FAI Cisco Networking Academy routers.

Keywords: Virtual private network, router, configuration, IPsec, Cisco Packet Tracer.

Chtěl bych poděkovat Ing. Miroslavu Matýskovi Ph.D. za kvalitní vedení a pomoc při vytváření této práce, Ing. Jiřímu Korbelovi Ph.D. za jeho znalost vybavení laboratoře a dobré cvičení kurzů Cisco akademie FAI. A také bych chtěl poděkovat své rodině, přítelkyni a přátelům, kteří mě podporují po celou dobu mého studia.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně

.....
podpis diplomanta

OBSAH

ÚVOD	10
I TEORETICKÁ ČÁST	11
1 VIRTUÁLNÍ PRIVÁTNÍ SÍŤ	12
1.1 VPN ZAŘÍZENÍ.....	12
1.2 TECHNOLOGIE A PROTOKOLY VPN.....	13
1.2.1 Technologie a protokoly VPN typu síť – síť.....	13
1.2.2 Technologie a protokoly VPN pro vzdálený přístup.....	13
1.3 ROZDĚLENÍ VPN.....	14
1.3.1 VPN zajištěné poskytovatelem a VPN zajištěné uživatelem	14
1.3.2 VPN typu síť – síť a VPN pro vzdálený přístup	15
1.3.3 L2VPN a L3VPN	15
1.3.4 Povinný a nepovinný tunel.....	15
1.3.5 Důvěryhodné VPN a zabezpečené VPN	16
1.4 PŘEHLED A POROVNÁNÍ VPN	16
1.4.1 VPN typu síť – síť	16
1.4.1.1 Poskytovatelem zajištěné L2VPN.....	16
1.4.1.2 Poskytovatelem zajištěné L3VPN.....	17
1.4.1.3 Uživatelem zajištěné VPN	17
1.4.2 VPN pro vzdálený přístup.....	17
1.4.2.1 VPN s dobrovolným tunelem	17
1.4.2.2 VPN s povinným tunelem.....	18
2 IPSEC VE VPN TYPU SÍŤ – SÍŤ	19
2.1 VÝHODY A NEVÝHODY	19
2.2 BEZPEČNOST IPSEC	20
2.2.1 Kryptografické algoritmy	21
2.2.1.1 Ověřovací algoritmy	21
2.2.1.2 Šifrovací algoritmy	22
2.2.1.3 Kryptografické algoritmy veřejných klíčů	23
2.2.2 Protokoly AH a ESP.....	25
2.2.2.1 AH.....	25
2.2.2.2 ESP.....	25
2.2.2.3 AH a ESP	26
2.2.3 Bezpečnostní asociace.....	26
2.2.4 IPsec databáze	27
2.2.5 Techniky správy klíčů a SA	27
2.2.6 IKEv1	27
2.2.6.1 Fáze 1 IKE vyjednávání v hlavním módu.....	28
2.2.6.2 Fáze 1 IKE vyjednávání v agresivním módu	29
2.2.6.3 Fáze 2 IKE vyjednávání v rychlém módu.....	29
2.2.7 IKEv2	30
2.2.8 Zpracování IPsec paketu	31
II PRAKTICKÁ ČÁST	33

3	KONVENCE.....	34
4	NASAZENÍ IPSEC VPN	35
4.1	VÝBĚR A KONFIGURACE IKE POLITIKY	35
4.1.1	Výběr vhodné IKE metody ověřování.....	35
4.1.2	Výběr kryptografických parametrů IKE politiky	37
4.1.2.1	Konfigurace šifrovacího algoritmu	38
4.1.2.2	Konfigurace Diffie – Hellman skupiny.....	38
4.1.2.3	Konfigurace Hash algoritmu	38
4.1.2.4	Konfigurace ověřovací metody	39
4.1.2.5	Konfigurace životnosti IKE SA	39
4.2	VÝBĚR A KONFIGURACE IPSEC TRANSFORMACÍ.....	40
4.2.1	Výběr bezpečnostního protokolu	40
4.2.2	Výběr hash algoritmu	40
4.2.3	Výběr šifrovacího algoritmu	40
4.2.4	Výběr kompresního algoritmu	41
4.2.5	Konfigurace IPsec transformačního setu.....	41
4.3	TVORBA A KONFIGURACE KRYPTOVACÍHO PŘÍSTUPOVÉHO SEZNAMU	43
4.4	SPOJENÍ POMOCÍ KRYPTOVACÍ MAPY	44
5	SIMULACE IPSEC VPN	46
5.1	KONFIGURACE SMĚROVAČE INTERNET	46
5.2	KONFIGURACE VPN BRAN	47
5.2.1	Předsdílený klíč	47
5.2.2	IKE politika	47
5.2.3	IPsec transformační set.....	48
5.2.4	Kryptovací přístupový seznam.....	48
5.2.5	Kryptovací mapa	49
5.2.6	Vnitřní rozhraní	49
5.2.7	Vnější rozhraní	50
5.2.8	Statické směrování	50
5.3	KONFIGURACE PRACOVNÍCH STANIC	51
5.4	FUNKCIONALITA SIMULACE	51
5.4.1	Ping z PC1	52
5.4.2	Ping z PC3.....	54
5.4.3	Vytvoření IPsec SA	56
6	FYZICKÁ REALIZACE NA SMĚROVAČÍCH CISCO AKADEMIE FAI	57
6.1	VYTVOŘENÍ IPSEC SA	57
6.2	PŘÍSTUP NA FTP SERVER.....	59
6.3	TELNET PŘEPÍNAČE.....	60
	ZÁVĚR	62
	CONCLUSION	63
	SEZNAM POUŽITÉ LITERATURY.....	64

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	65
SEZNAM OBRÁZKŮ	68
SEZNAM PŘÍLOH.....	69

ÚVOD

Na vývoj moderních technologií je navázán i vzrůstající počet jejich aplikací, které mnohdy přinášejí velké výhody v úspoře času. Protože s lidmi dnešní doby je spjato tvrzení, že čas jsou peníze, jsou tyto aplikace velmi oblíbené.

Jednou z oblastí, které do této kategorie spadají, jsou technologie virtuálních privátních sítí. Díky těmto technologiím je člověk schopen využívat firemních dat i z pohodlí svého domova či v podstatě kterékoliv části světa. Stejně tak je možné, aby oddělené pobočky jedné nebo skupiny organizací, sdílely skladovací, logistické a marketingové informace. Dalším velmi vhodným využitím virtuálních privátních sítí je jejich využití ve vzdálené správě aktivních síťových prvků. Administrátor už nemusí kvůli každé úpravě konfigurace do serverovny, může využít zabezpečeného vzdáleného připojení a provést nápravu za zlomek původně potřebného času.

Právě pro širokou škálu využití byla jako téma této práce vybrána technologie virtuálních privátních sítí.

I. TEORETICKÁ ČÁST

1 VIRTUÁLNÍ PRIVÁTNÍ SÍTĚ

Za historického předchůdce VPN (Virtual Private Network) je možné považovat virtuální síť spojené s přepínači, tzv. VLAN (Virtual Local Area Network). Tato technologie na jedné fyzické infrastruktuře umožňuje existenci několika autonomních VLAN. Rozšířením z fyzické infrastruktury na síť DSP (Data Service Provider) vzniká VPN [1].

Definice VPN:

VPN poskytuje organizaci nebo organizacím funkcionalitu privátní sítě na veřejné nebo sdílené infrastruktuře jako je třeba Internet [2].

1.1 VPN zařízení

Předtím, než bude možné popsat jednotlivé VPN technologie a protokoly, je nutné rozdělit síťová zařízení do skupin, které později poslouží pro jednoduchou orientaci.

Zařízení v síti uživatele můžeme rozdělit do dvou kategorií:

- **C (Customer) zařízení** – C zařízení jsou zařízení jako směrovače nebo přepínače v uživatelské síti. Tato zařízení nemají přímé propojení do sítě poskytovatele datových služeb. Stejně tak nemají povědomí o VPN.
- **CE (Customer Edge) zařízení** – CE zařízení jsou zařízení, která jsou na hranici uživatelské sítě a připojují se k síti poskytovatele datových služeb přes PE (Provider Edge) zařízení.

Ve VPN založených na CE zařízeních mají tato zařízení povědomí o VPN. Naopak ve VPN založených na PE zařízeních, CE zařízení toto povědomí nemají.

Ve VPN typu síť – síť se zařízení v síti DSP taktéž rozdělují do dvou kategorií:

- **P (Provider) zařízení** – P zařízení jsou zařízení jako směrovače nebo přepínače v síti DSP, která nejsou přímo propojena se síti uživatele. Rovněž tato zařízení nemají povědomí o uživatelských VPN.
- **PE (Provider Edge) zařízení** – Zařízení přímo připojená k síti uživatele přes CE zařízení.

Ve VPN založených na PE zařízeních mají tato zařízení povědomí o VPN. Naopak ve VPN založených na CE zařízeních, PE zařízení toto povědomí nemají.

Další zařízení používaná ve VPN jsou NAS (Network Access Server) a VPN brány.

NAS je zařízení, které vytváří rozhraní mezi přístupovou sítí a sítí poskytovatele. U VPN pro vzdálený přístup může NAS sloužit jako koncový bod VPN tunelu.

VPN brána slouží jako koncový bod VPN tunelu a to zvláště ve VPN pro vzdálený přístup nebo u VPN sítí založených na CE zařízeních typu síť – síť [2].

1.2 Technologie a protokoly VPN

1.2.1 Technologie a protokoly VPN typu síť – síť

Ve VPN typu síť – síť jsou uživatelská data tunelována mezi CE nebo PE zařízeními.

- **IPsec (Internet Protocol security)** – IPsec sestává ze skupiny protokolů navržených k ochraně komunikace mezi bezpečnostními bránami nebo uživateli. IPsec tunely jsou často tvořeny ve VPN typu síť – síť mezi CE zařízeními [2].
- **GRE (Generic Routing Encapsulation)** – GRE je možné použít na vytvoření tunelů a přenos paketů jednoho protokolu skrze jiný protokol. GRE v základu nemá žádnou úroveň zabezpečení, té lze dosáhnout kombinací s protokolem IPsec [2, 3].
- **Draft Martini** – Jakýkoliv přenos v sítích MPLS (MultiProtocol Layer Switching).
- **L2TPv3 (Layer 2 Tunneling Protocol)** – Představuje hlavní řídicí a zapouzdřovací protokol pro tunelování mnohonásobné komunikace mezi dvěma IP (Internet Protocol) uzly na spojové vrstvě [4].
- **IEEE 802.1Q tunelování (tzv. VLAN ve VLAN)** – 802.1Q protokol používaný u VLAN. Umožňuje poskytovateli služeb tunelování tagovaných ethernetových rámců uživatelské komunikace přes páteřní síť poskytovatele přidáním dalšího tagu.
- **MPLS LSP (Link State Protocol)** – Pakety jsou směrovány na základě označení připojeného k paketu [2].

1.2.2 Technologie a protokoly VPN pro vzdálený přístup

Ve VPN pro vzdálený přístup jsou data tunelována mezi mobilním uživatelem a VPN bránou.

- **L2F (Layer 2 Forwarding) protokol** – Cisco proprietární protokol vytvořený pro tunelování PPP (Point – to – Point Protocol) rámců mezi NAS a VPN bránou. Mobilní uživatelé se připojují k NAS a jejich PPP rámce jsou tunelovány na VPN bránu.
- **PPTP (Point – to – Point Tunneling Protocol)** – Jedná se v podstatě o stejný protokol jako L2F protokol, ale byl vyvinut konsorciem prodejců. PPP zapouzdřené pakety přenášené přes PPTP tunely jsou často zabezpečeny pomocí MPPE (Microsoft Point-to-Point Encryption).
- **L2TPv2/L2TPv3** – Jedná se o IETF (Internet Engineering Task Force) standard, který kombinuje nejlepší vlastnosti L2F protokolu a PPTP.
- **IPsec** – Tuto technologii je možné použít jak u VPN typu síť – síť, tak i u VPN pro vzdálený přístup.
- **SSL (Secure Sockets Layer)** – SSL je bezpečnostní protokol původně vyvinutý společností Netscape Communications.

Byl vytvořen ve třech verzích a jeho třetí verze SSLv3 je podobná IETF standardu TLS (Transport Layer Security).

SSL má jednu velkou výhodu – je zabudován téměř v každém webovém prohlížeči. Proto použití SSL VPN nevyžaduje žádný další speciální klientský software [2].

1.3 Rozdělení VPN

Jelikož v minulosti neexistovala koordinace mezi jednotlivými vývojáři VPN protokolů a technologií, vznikla spousta metod jejich rozdělení a odlišení.

1.3.1 VPN zajištěné poskytovatelem a VPN zajištěné uživatelem

- **VPN zajištěné poskytovatelem** – VPN konfigurované a provozované poskytovatelem nebo poskytovateli.
- **VPN zajištěné uživatelem** – konfigurované a provozované uživatelem.

Uživatelé může být často myšlena organizace nebo jiný poskytovatel [2].

1.3.2 VPN typu síť – síť a VPN pro vzdálený přístup

- **VPN typu síť – síť** – Poskytuje propojení mezi jednotlivými geograficky oddělenými sítěmi organizace (Intranet VPN) nebo mezi jednotlivými organizacemi (Extranet VPN).
- **VPN pro vzdálený přístup** – Poskytuje připojení k síti organizace pro mobilní uživatele [2].

1.3.3 L2VPN a L3VPN

- **L2VPN (Layer 2 VPN)** – VPN typu síť – síť na druhé vrstvě ISO / OSI (International Organization for Standardization / Open Systems Interconnection) modelu zajišťující komunikaci mezi směrovači, prepínači a koncovými zařízeními. PE zařízení přeposílají data na základě MAC (Media Access Control) adresy uvedené v hlavičce rámce.

Tyto VPN se dále dají rozdělit do dvou kategorií:

- P2P (Point – to – Point) okruhové VPN – Jsou také známy jako VPWS (Virtual Private Wire Service) VPN.
- MP (MultiPoint) VPN – Existují ve dvou variantách: VPLS (Virtual Private LAN Service) VPN a IPLS (IP – Only LAN Service) VPN.
- **L3VPN (Layer 3 VPN)** – VPN typu síť – síť na třetí vrstvě ISO / OSI modelu. Propojuje koncová zařízení a směrovače na oddělených uživatelských sítích. PE zařízení přeposílají data na základě IP adresy uvedené v hlavičce IP paketu [2].

1.3.4 Povinný a nepovinný tunel

- **Povinný tunel (nebo také NAS iniciovaná VPN)** – V tomto módu VPN pro vzdálený přístup fungují tak, že se mobilní uživatel připojuje na NAS, který tuneluje uživatelská data na a z VPN brány. Jedná se o poskytovatelem zajištěnou VPN a použité protokoly jsou: L2F, PPTP a L2TP.
- **Nepovinný tunel (nebo také uživatelem iniciovaná VPN)** – VPN v tomto módu mohou být jak poskytovatelem, tak uživatelem zajištěné a uživatelská data jsou tunelována přímo mezi mobilním uživatelem a VPN bránou [2].

1.3.5 Důvěryhodné VPN a zabezpečené VPN

- **Důvěryhodné VPN** – Zajištěné poskytovatelem, uživatelská data jsou nešifrovaná přenášena přes páteřní síť poskytovatele.
- **Zabezpečené VPN** – Uživatelská data jsou přes páteřní síť poskytovatele přenášena ověřená a šifrovaná.

1.4 Přehled a porovnání VPN

1.4.1 VPN typu síť – síť

Do porovnání jednotlivých VPN typu síť – síť je možné zařadit velké množství faktorů, v této práci byly jednotlivé technologie porovnány z hledisek:

- Spojení dvou bodů, nebo spojení vícebodové.
- Rozšiřitelnosti.
- Geografického dosahu.
- Bezpečnosti.
- Vestavěné podpory multicast paketů / rámců.
- Vestavěné podpory více protokolů.

1.4.1.1 Poskytovatelem zajištěné L2VPN

VPWS – P2P spojení s dobrou rozšiřitelností. Geografický dosah je limitovaný u nasazení Draft Martini na MPLS páteřní síti, u L2TPv3 může přecházet jakoukoliv IP – podporující páteřní síť. Zabezpečení je dobré, obsahuje vestavěnou podporu multicast a podporuje více protokolů.

VPLS – MP spojení, ostatní vlastnosti stejné jako VPWS.

IPLS – Stejně jako VPLS, ale podporuje pouze protokol IP.

1.4.1.2 Poskytovatelem zajištěné L3VPN

BGP (Border Gateway Protocol) / MPLS – MP spojení s výbornou rozšiřitelností. Geografický dosah je limitován na MPLS páteřní síť. Zabezpečení je dobré, nepodporuje multicast ani více protokolů.

IPsec – P2P spojení s dobrou rozšiřitelností. Může být nasazeno na jakoukoliv IP – podporující páteřní síť. Má excelentní zabezpečení a nepodporuje ani multicast ani více protokolů.

GRE – P2P spojení s dobrou rozšiřitelností. Může být nasazeno na jakoukoliv IP – podporující páteřní síť. Zabezpečení je slabé, ale podporuje multicast i více protokolů.

1.4.1.3 Uživatelem zajištěné VPN

IPsec – Stejně vlastnosti jako poskytovatelem zajištěné IPsec.

GRE – Stejně vlastnosti jako poskytovatelem zajištěné GRE [2].

1.4.2 VPN pro vzdálený přístup

Jednotlivé technologie VPN pro vzdálený přístup byly porovnány z hlediska:

- Funkcionality – Kolik je jí poskytnuto mobilním uživatelům oproti uživatelům v místní síti.
- Bezpečnosti.
- Rozšiřitelnosti.
- Vestavěné podpory více protokolů.
- Vestavěné podpory multicast paketů / rámců.

1.4.2.1 VPN s dobrovolným tunelem

L2F – Funkcionalita je srovnatelná s uživateli v místní síti. Bezpečnost je limitována pouze na ověření tunelu, rozšiřitelnost je velmi dobrá a L2F obsahuje vestavěnou podporu více protokolů i multicasu.

PPTP – Stejně vlastnosti jako L2F, pouze bezpečnost je lepší s použitím MPPE.

L2TPv2/3 – Stejně vlastnosti jako L2F.

1.4.2.2 VPN s povinným tunelem

PPTP – Stejné vlastnosti jako s dobrovolným tunelem.

L2TPv2/3 – Stejné vlastnosti jako s dobrovolným tunelem.

IPsec – Funkcionalita je srovnatelná s uživateli v místní síti. Zabezpečení je excelentní a rozšiřitelnost je velmi dobrá. Nepodporuje více protokolů, ale podporuje multicast.

SSL / TLS – Funkcionalita je limitována pokud nepoužíváme specifický klientský software. Zabezpečení je excelentní a rozšiřitelnost je dobrá. Nepodporuje však více protokolů ani multicast [2].

2 IPSEC VE VPN TYPU SÍŤ – SÍŤ

Jedná se o bezpečnostní rozšíření protokolu IP, které poskytuje ověřování a / nebo šifrování komunikace. V poslední době se toto rozšíření stalo velmi populárním pro zajištění jak VPN typu síť – síť, tak VPN pro vzdálený přístup.

2.1 Výhody a nevýhody

Předtím, než je nasazeno IPsec pro VPN typu síť – síť, je potřeba zvážit všechny klady a zápory, které přináší.

- IPsec přináší velmi vysokou úroveň zabezpečení.
- IPsec VPN typu síť – síť může být nasazena organizací, která jej chce využívat, ale stejně tak se může jednat o službu poskytovanou a spravovanou DSP.
- IPsec mohou být nasazeny na jakoukoliv IP – podporující páteřní síť včetně Internetu. Tahle vlastnost může být velmi výhodná v rámci úspory nákladů.
- Organizace, které nasadí IPsec VPN typu síť – síť mají plnou kontrolu nad směrováním ve své WAN (Wide Area Network) síti. To je velký rozdíl oproti MPLS L3VPN, kde je nutné, aby si CE a PE směrovače vyměňovali směrovací informace (dynamické směrování).
- IPsec VPN typu síť – síť využívající standardní IPsec tunely mohou být obtížně rozšiřitelné. Musí být zformován IPsec tunel mezi každým párem VPN bran, což je náročné hlavně u sítí, kde je vyžadováno propojení každý s každým.
- Pro zvýšenou bezpečnost IPsec VPN je potřeba ověřování digitálním certifikátem. Použití digitálních certifikátů nařizuje nasazení PKI (Public Key Infrastructure).
- Dynamické směrování v IPsec VPN, používající standardní P2P IPsec tunelování, je často komplexnější než v MPLS L3VPN. Každá IPsec VPN brána musí být směrovacím partnerem všech dalších IPsec VPN bran.
- IPsec neposkytuje podporu více protokolů ani posílání multicast paketů. Nicméně tyto dvě vlastnosti je možné změnit, pokud použijeme kombinaci IPsec / GRE a VTI (Virtual Tunnel Interface).

- IPsec může způsobit vysoké zatížení CPU (Central Processing Unit) na VPN branách. To je způsobeno náročností výpočtů šifrovacího / dešifrovacího procesu a ověřování. Zatížení může být sníženo použitím hardware akceleratorů na směrovačích [2].

2.2 Bezpečnost IPsec

Velkou výhodou IPsec je možné použití jak u IPv4, tak u IPv6 sítí. Zde poskytuje zabezpečení přenosu mezi uživateli nebo VPN branami.

IPsec je tvořeno několika částmi:

- **Kryptografické algoritmy.**
- **Bezpečnostní protokoly.**
- **Bezpečnostní asociace.**
- **IPsec databáze.**
- **Techniky správy SA (Security Association) a klíčů.**

Tyto části dohromady poskytují následující bezpečnostní prvky:

- **Kontrola přístupu** – IPsec dokáže kontrolovat přístup ke zdrojům v síti za bezpečnostní bránou.
- **Integrita dat** – IPsec dokáže detekovat změny v paketech, nezávisle na pořadí v jakém přijdou. Pokud by byl paket při přenosu mezi bezpečnostními branami pozměněn, bude zahozen.
- **Ověření původu dat** – IPsec potvrzuje, že obdržené zprávy jsou od uživatele, který je zároveň odesílatelem, nikoliv od někoho, kdo se za něj vydává. Pakety, které jsou odeslány potencionálním útočníkem, jsou zahozeny.

Integrita dat a ověření původu dat dohromady tvoří autentizaci IPsec.

- **Ochrana přeposílání** – Zajišťuje, že každý duplikovaný paket je zahozen.
- **Zabezpečení dat** – Bezpečnostní prvek, který má na starosti skrývání dat a zabezpečení proti možnosti je přečíst. K tomuto se používá šifrovacích algoritmů.

- **Limitované zabezpečení přenosu** – V některých případech, i když útočník nedokáže získat data, je možné z přenosu získat identity komunikujících zařízení, frekvenci komunikace a velikost paketů. IPsec částečně zabezpečuje přenos i proti tomuto možnému útoku [2].

2.2.1 Kryptografické algoritmy

Šifrování a ověřování uživatelských dat je v IPsec zajištěno kryptografickými algoritmy.

- **Ověřovací algoritmy.**
- **Šifrovací algoritmy.**
- **Kryptografické algoritmy veřejných klíčů.**

2.2.1.1 Ověřovací algoritmy

IPsec používá několik hashovacích algoritmů pro autentizaci dat.

- **Hash algoritmy.**

Hash algoritmus je kryptografický algoritmus, který slouží k vygenerování hash pevné délky ze zadaného klíče libovolné délky. Základem těchto algoritmů je fakt, že není možné z hash hodnoty zpětně získat originální zprávu. Vhodný algoritmus dokáže z malé změny klíče vygenerovat absolutně odlišnou hodnotu hash a tím je možné zjišťovat i malé změny v rozsáhlých souborech relativně snadno. Kvalitní algoritmus rovněž dokáže zajistit, že neexistují dva různé vstupy se stejnou hodnotou hash a pokud ano, není možné je v reálném čase spočítat.

Nejčastěji používanými hash algoritmy jsou MD5 (Message Digest 5) a SHA – 1 (Secure Hash Algorithm). MD5 generuje hash délky 128 bitů, SHA – 1 generuje 160 bitů dlouhý hash [2, 5].

Je-li poslán hash spolu se zprávou, po přijetí příjemce spočítá hash zprávy a porovná jej s obdrženou hodnotou hash. Když se tyto hodnoty rovnají, zpráva je ověřena, když se nerovná, bude zahozena. Tato bezpečnostní technika ovšem nestačí. Pokud by útočník pouze pozměnil zprávu, paket by byl zahozen, ale pokud útočník změní zprávu a zároveň vymění hash originálu za hash podstrčené zprávy, nová zpráva bude ověřena.

- **MAC (Message Authentication Code) a HMAC (Hashed MAC) algoritmy.**

Protože samotná hodnota hash odeslaná spolu se zprávou nestačí, je potřeba přidat do hash algoritmu něco navíc, něco takového, že pouze bezpečnostní brány a uživatelé budou schopni spočítat správnou hash hodnotu. K tomuto účelu slouží sdílený klíč. Pokud útočník tento klíč nemá, je pro něj nemožné spočítat správnou hodnotu hash své podstrčené zprávy a přijímací brána zprávu zahodí.

Hash algoritmus, který používá jako vstup zprávu a sdílený klíč se nazývá MAC. Další nespornou výhodou tohoto algoritmu oproti klasickému hash algoritmu je to, že je možné jej použít k ověření původu dat, protože pouze odesílatel a příjemce mají správný klíč.

Jelikož bylo prokázáno, že MD5 a SHA – 1 jsou prolomitelné, IPsec používá posílený MAC algoritmus nazývaný HMAC. HMAC používá upravené algoritmy MD5 – HMAC – 96 a SHA – HMAC – 96, které generují hash hodnot o zkrácené délce 96 bitů [2].

2.2.1.2 Šifrovací algoritmy

Šifrování je proces, při kterém z otevřeného textu pomocí klíče vytváříme text bez rozšifrování nečitelný – šifrovaný text. Proces, kterým z šifrovaného textu dostaneme text otevřený, se nazývá dešifrování [2, 6].

IPsec používá symetrického šifrování pro objemové šifrování dat. Symetrické šifrování znamená, že stejný klíč je použit jak k šifrování otevřeného textu, tak k zpětnému dešifrování textu šifrovaného. Takže když jedna VPN brána pomocí klíče zprávu zašifruje, druhá VPN brána vyžaduje stejný klíč k dešifrování. Symetrické algoritmy jsou relativně rychlé a proto je možné je k tomuto objemovému šifrování komunikace použít. Problémem je složitá distribuce a správa klíče v síti s větším počtem VPN bran. Existují dva typy symetrických šifrovacích algoritmů:

- **Blokové šifry.**

Blokové šifry, jak název napovídá, šifrují otevřený text po stejně dlouhých blocích a mohou fungovat v několika módech:

- ECB (Electronic CodeBook) mód.

- CBC (Cipher – Block Chaining) mód.
- CFB (Cipher FeedBack) mód.
- OFB (Output FeedBack) mód.

V módu ECB jsou bloky otevřeného textu šifrovány nezávisle. Nevýhodou je, že dva stejné bloky otevřeného textu vždy generují stejný šifrovaný text. Kvůli tomuto problému je potencionální útočník schopen vyhledávat opakované vzory a pomocí frekvenční analýzy prolomit šifrování.

Módy CBC, CFB a OFB přidávají do šifrování prvek zpětné vazby.

V módu CBC projde blok otevřeného textu před zašifrováním funkcí exkluzivní disjunkce s předchozím blokem šifrovaného textu. U prvního bloku se používá inicializační vektor.

Typickými zástupci CBC blokových šifer jsou DES (Data Encryption Standard) a AES (Advanced Encryption Standard). DES šifruje / dešifruje bloky o velikosti 64 bitů a používá k tomu 64 bitů dlouhý klíč. Protože bylo brzy zjištěno, že DES není dostatečně odolný, vznikl 3DES, což je v podstatě třikrát v řadě použitý DES algoritmus. Nejčastěji se prvním klíčem šifruje, druhým dešifruje a třetím opět šifruje. 3DES je sice stále bezpečný šifrovací algoritmus, ale rychlost šifrování je nízká a proto byl nahrazen Rijndael (AES) algoritmem.

AES šifruje / dešifruje bloky velikosti 128 bitů v jednom cyklu a používá klíče délky 128, 192 nebo 256 bitů [2, 6, 7].

- **Proudové šifry.**

Proudové šifry šifrují otevřený text po bitech a často jsou rychlejší než blokové šifry. Nejčastěji používané proudové šifry jsou RC4 a SEAL (Software Encryption ALgorithm). SEAL je optimalizovaný pro 32 – bit procesory [2].

2.2.1.3 Kryptografické algoritmy veřejných klíčů

Šifrovací algoritmy používaly symetrické šifrování, které používají na šifrování a dešifrování stejný klíč. Kryptografické algoritmy veřejných klíčů používají šifrování asymetrické, které se liší od toho symetrického tak, že je potřeba dvou klíčů (veřejný a soukromý). Kryptografické algoritmy veřejných klíčů mají tyto vlastnosti:

- Jsou výrazně pomalejší, proto se nehodí pro objemové šifrování.
- Šifrovaný text není kompaktní.
- Nemají problémy s distribucí a správou klíčů. Distribuce sestává z publikace veřejných klíčů ke každému zařízení.
- Mohou být použity k šifrování, digitálním podpisům a pro symetrickou výměnu klíčů.

Nejčastěji používané algoritmy veřejných klíčů jsou Diffie – Hellman, RSA (Rivest, Shamir, Adleman), DSA (Digital Signature Algorithm) a ElGamal. Diffie – Hellman se používá pro výměnu klíčů, RSA a ElGamal mohou být použity na šifrování digitálních podpisů a DSA se používá pro vytváření digitálních podpisů [2].

- **Šifrování používající algoritmy veřejných klíčů.**

Šifrovací algoritmy veřejných klíčů používají jeden klíč pro šifrování a druhý pro dešifrování. Jedná se o dvojici veřejného klíče a s ním matematicky asociovaného soukromého klíče. Jakákoliv data šifrovaná veřejným klíčem, mohou být dešifrována soukromým klíčem, nikoliv opět veřejným. Podobně to funguje i opačně. Data šifrovaná soukromým klíčem mohou být dešifrována pouze klíčem veřejným.

- **Digitální podpis.**

Jedná se o šifrovanou hash hodnotu, která značí, že určitá organizace posílá, ověřuje nebo ručí za danou komunikaci.

Uživatel A, který chce odeslat zprávu, nejprve spočítá její hash hodnotu a zašifruje s pomocí svého soukromého klíče, čímž dostane digitální podpis. Podpis připojí k originálu zprávy a odešle vše příjemci B. Příjemce spočítá hash hodnotu zprávy a dešifruje hash příchozí zprávy pomocí veřejného klíče. Pokud se hash hodnoty rovnají, zpráva je přijata a příjemce ví, že zpráva nebyla upravena a že ji odeslal uživatel A.

- **Výměna klíčů s Diffie – Hellman**

Diffie – Hellman je algoritmus veřejných klíčů, který se používá pro domluvu dvou uživatelů na bezpečném klíči, přes nezabezpečený komunikační kanál. Využívá při tom výpočetní složitosti diskrétního logaritmu [2, 8].

2.2.2 Protokoly AH a ESP

IPsec používá dva různé bezpečnostní protokoly, AH (Authentication Header) a ESP (Encapsulating Security Payload).

2.2.2.1 AH

Jedná se o protokol sady IP s identifikátorem 51. AH je přídatná hlavička paketu, která poskytuje tyto bezpečnostní prvky:

- **Integrita dat.**
- **Ověření původu dat.**
- **Volitelná ochrana proti opakování paketů.**

AH může operovat ve dvou módech:

- **Transportní mód** – AH hlavička je vložena mezi originální IP hlavičku a hlavičku protokolu transportní vrstvy. V tomto módu je ověřen celý paket vyjma polí v IP hlavičce, které mohou měnit svou hodnotu při přenosu – TTL (Time – To – Live), ToS (Type of Service) a kontrolní součet hlavičky. Běžně se tento mód používá pro ochranu uživatelských paketů mezi koncovými zařízeními.
- **Tunelový mód** – AH hlavička je spolu s novou IP hlavičkou připojena k paketu určenému k ochraně. Opět je zabezpečen celý paket včetně nové IP hlavičky vyjma polí, které mohou měnit svou hodnotu při přenosu. Běžně se tento mód používá při přenosu paketů mezi bezpečnostními bránami [2].

2.2.2.2 ESP

Jedná se o protokol sady IP s identifikátorem 50. ESP je hlavička paketu, která poskytuje následující bezpečnostní prvky:

- **Integrita dat.**

- **Ověření původu dat.**
- **Volitelná ochrana proti opakování paketů.**
- **Zabezpečení dat.**
- **Limitované zabezpečení přenosu (pouze v tunelovém módu).**

ESP poskytuje stejné bezpečnostní prvky jako AH a ještě přidává další, což je důvod, proč už je AH používáno jenom zřídka.

ESP taktéž operuje ve dvou módech:

- **Transportní mód** – ESP hlavička je vložena mezi IP hlavičku paketu určeného k ochraně a mezi hlavičku protokolu transportní vrstvy. Na konec paketu je připojena ESP patička a volitelné pole ESP ICV (Integrity Check Value). Na rozdíl od AH, je u ESP zabezpečen celý paket vyjma IP hlavičky. Pokud je ESP nakonfigurováno k šifrování, šifruje opět celý paket vyjma IP hlavičky a ESP hlavičky. Běžně se tento mód používá pro ochranu uživatelských paketů mezi koncovými zařízeními.
- **Tunelový mód** – Stejně jako u AH v tunelovém módu je vytvořena nová IP hlavička a ESP hlavička, které jsou připojeny k paketu. ESP patička a pole ESP ICV jsou připojeny na konec paketu. Stejně jako v transportním módu je zabezpečen celý paket, nyní včetně originální IP hlavičky, vyjma nové IP hlavičky. Pokud je ESP nakonfigurováno k šifrování, šifruje se stejně jako v transportním módu, ale i s originální IP hlavičkou [2].

2.2.2.3 AH a ESP

Pro ochranu přenosu dat je možné použít obě technologie zároveň. Opět máme možnost transportního a tunelového módu a hlavičky jsou nyní řazeny za sebe, prve AH, potom ESP.

2.2.3 Bezpečnostní asociace

IPsec SA je jednosměrná a definuje jakým způsobem je provoz zabezpečen. Je identifikována pomocí SPI (Security Parameter Index) a obsahuje informace o bezpečnostním protokolu, jeho módu, kryptografickém algoritmu a SA životnosti.

Konkrétní provoz může být zabezpečen jednou nebo více SA. Pokud používáme AH pro ověření a ESP pro šifrování, provoz bude zahrnovat dvě SA. Protože jsou SA jednosměrné, pro zajištění provozu mezi dvěma VPN branami jsou potřeba minimálně dvě [2].

2.2.4 IPsec databáze

IPsec pro správné zpracování IP provozu definuje tři databáze:

- **SPD (Security Policy Database)** – Specifikuje, který provoz by měl být zabezpečen IPsec a který ne.
- **SAD (Security Association Database)** – Položky obsahují informace ke každé IPsec SA a rozhraní v SPD.
- **PAD (Peer Authorization Database)** – Tato databáze poskytuje spojení mezi IKE (Internet Key Exchange) protokolem a SPD. PAD specifikuje například rozsah adres, ze kterých je možno vytvořit IPsec spojení [2].

2.2.5 Techniky správy klíčů a SA

IPsec podporuje dvě různé techniky:

- **Manuální správa klíčů a SA** – Tato technika je velmi podobná manuálnímu udržování směrovací tabulky. Stejně tak je i těžko rozšiřitelná.
- **Automatizovaná správa klíčů a SA s IKE protokolem** – IKE protokol dovoluje, aby se IPsec uživatelé dynamicky ověřovali, generuje klíče a vyjednává IPsec SA.

2.2.6 IKEv1

IKEv1 (IKE verze 1) se skládá ze skupiny protokolů:

- **SKEME (Secure Key Exchange MEchanism)** – Popisuje univerzální techniku k výměně klíče, poskytující anonymitu a rychlou obnovu klíče.
- **Oakley protokol** – Popisuje sérii technik k výměně klíče nazývaných módy. Zároveň detailně popisuje PFS (Perfect Forward Secrecy), ochranu identity a ověření.
- **ISAKMP (Internet Security Association and Key Management Protocol)** – Poskytuje framework pro ověření a výměnu klíče, ale nedefinuje je. ISAKMP byl

vytvořen tak, aby byl nezávislý na technice výměny klíče. Díky tomu podporuje velké množství těchto technik.

Vyjednávání IKEv1 je rozděleno do dvou fází a tří módů. Ve fázi jedna IPsec uživatelé vytvoří IKE SA. Tato IKE SA je použita k ochraně vyjednávání fáze dvě. Fáze dvě se stará o vyjednání IPsec SA. Fáze jedna IKEv1 může vyjednávat v hlavním, nebo agresivním módu. Fáze dvě vyjednává v rychlém módu. IKE SA vyjednané ve fázi jedna jsou obousměrné. Jak už bylo zmíněno dříve, IPsec SA jsou jednosměrné a tak tomu je i ve fázi dvě IKEv1.

K ověření mezi IPsec uživateli při IKE vyjednávání mohou být použity tři metody:

- **Předsdílené klíče** – Staticky konfigurovaný klíč musí být stejný na obou branách IPsec uživatelů.
- **Šifrované nonce** – Nonce je zašifrována veřejným klíčem na VPN branách IPsec uživatelů. Každý uživatel musí vlastnit veřejný klíč protistrany před IKE vyjednáním.
- **Digitální podpisy** – Je vytvořen digitální podpis konkrétní části informace a vyměněn mezi IPsec uživateli. Každý uživatel poté verifikuje digitální podpis informace použitím veřejného klíče protistrany. Nejen, že každý uživatel musí před začátkem IKE vyjednávání vlastnit veřejný klíč protistrany, zároveň musí být ověřeno, že tento klíč opravdu patří protistraně. Toho je možné docílit použitím certifikační autority, která uděluje digitální certifikáty IPsec uživatelům. Digitální certifikát je asociací mezi identitou a veřejným klíčem uživatele. Certifikační autorita je třetí strana, která je důvěryhodná pro obě strany IPsec komunikace.

2.2.6.1 Fáze 1 IKE vyjednávání v hlavním módu

Účel fáze jedna je vytvoření IKE SA mezi dvěma IPsec uživateli. Během této fáze si uživatelé vymění tři páry zpráv:

- **První pár (zprávy 1 a 2)** – Tento pár zpráv je použit k vyjednání parametrů IKE politiky, jako jsou – hash algoritmus, šifrovací algoritmus a metoda ověření.
- **Druhý pár (zprávy 3 a 4)** – Tento pár je použit k výměně veřejných hodnot a nonce (náhodných čísel) Diffie – Hellman algoritmu. Diffie – Hellman výměna

umožňuje IPsec uživatelům dohodu na tajném sdíleném klíči. Náhodná čísla jsou použita jako klíčovací část ve výpočtu relačních klíčů IPsec uživatelů.

IPsec uživatelé v této fázi vygenerují první ze čtyř relačních klíčů SKEYID. Z tohoto klíče jsou dále vypočítány zbývající tři: SKEYID_d, SKEYID_a a SKEYID_e. IPsec uživatelé ověřují a šifrují zbývající zprávy IKE fáze 1 a 2 pomocí klíčů SKEYID_a a SKEYID_e.

- **Třetí pár (zprávy 5 a 6)** – Tento pár je použit pro výměnu a ověření identity IPsec uživatelů mezi sebou.

Fáze jedna je dokončena a mezi IPsec uživateli byla vytvořena IKE SA.

2.2.6.2 Fáze 1 IKE vyjednávání v agresivním módu

Jedná se o alternativu k hlavnímu módu, která používá tři zprávy namísto původních šesti. Agresivní mód je rychlejší, ale nezajišťuje takovou bezpečnost jako mód hlavní. Bezpečnost je snížena, protože IPsec identity jsou posílány nešifrovány.

Tři zprávy použité v agresivním módu jsou tyto:

- **Zpráva 1** – Zprávu odesílá iniciátor IKE vyjednávání a obsahuje všechny informace, které iniciátor posílá v prvních dvou zprávách v hlavnímu módu (parametry IKE politiky, Diffie – Hellman veřejné hodnoty a nonce) a zároveň obsahuje identitu iniciátora.
- **Zpráva 2** – Zprávu odesílá respondér a obsahuje stejné informace jako všechny tři zprávy respondéra v hlavnímu módu (přijetí parametrů IKE politiky, Diffie – Hellman veřejné hodnoty a nonce a respondérovu identitu). Zpráva zároveň slouží k ověření identity respondéra na straně iniciátora.
- **Zpráva 3** – Zprávu odesílá iniciátor a slouží k ověření jeho identity na straně respondéra.

2.2.6.3 Fáze 2 IKE vyjednávání v rychlém módu

Po dokončení první fáze IKE vyjednávání začíná fáze dvě, jejíž účel je vytvoření IPsec SA. Tyto IPsec SA jsou použity k ochraně uživatelského provozu při přenosu přes síť mezi IPsec uživateli.

IKE fáze dvě sestává ze tří zpráv:

- **Zpráva 1** – Zpráva odeslaná iniciátorem obsahující IPsec SA návrhy. Těmito návrhy jsou: šifrovací algoritmus, hash algoritmus a životnost IPsec.
- **Zpráva 2** – Zpráva odeslaná respondérem, která přijímá jeden z IPsec návrhů ze zprávy 1.
- **Zpráva 3** – Zpráva slouží jako potvrzení zprávy 2.

Zprávy jedna a dvě navíc obsahují klíčovací materiál (nonce). Tento materiál může být použit pro ověření AH SA nebo pro ověření a šifrování ESP SA. Pokud je navíc povolena funkce PFS, jsou zde přeposílány i speciální veřejné hodnoty Diffie – Hellman algoritmu.

Běžně se klíčový materiál pro IPsec SA získává z Diffie – Hellman veřejných hodnot přeposlaných ve fázi jedna IKE vyjednávání. Pokud je ale požadována vyšší bezpečnost, je povolena funkce PFS a je zajištěno, že IPsec klíčovací materiál je založen na hodnotách Diffie – Hellman algoritmu přenesených během fáze dvě.

Pokud jsou IPsec uživatelé VPN brány vyjednávající SA pro koncové uživatele, zprávy 1 a 2 obsahují navíc proxy identity. Tyto identity jsou odlišné od identit použitých ve fázi jedna. Identity fáze jedna slouží k identifikování IPsec uživatelů mezi sebou, naopak identity fáze dvě popisují provoz, jež má být chráněn IPsec SA.

Všechny zprávy IKE vyjednávání fáze dvě jsou zabezpečeny relačními klíči SKEYID_e a SKEYID_a vygenerovanými ve fázi jedna [2, 9].

2.2.7 IKEv2

Základní specifikace IKEv2 (IKE verze 2) zahrnuje všechny funkcionality IKEv1, stejně jako funkcionality, které byly k IKEv1 přidány – průchod NAT (Native Address Translation) a starší formy ověřování. IKEv2 navíc zahrnuje zlepšení v celkové efektivitě a bezpečnosti.

IKEv2 zachovává většinu vlastností IKEv1, včetně dvoufázového vyjednávání. Ve fázi jedna IKEv2 vyjednávání se vyjednají algoritmy, vytvoří se tajný relační klíč, ověří se uživatelé a vytvoří se IKE SA. Navíc ovšem IKEv2 ve fázi jedna vytvoří i první IPsec SA, tyto SA se označují jako SA potomci. V první fázi iniciátor odesílá požadavky 1 a 2 a respondér posílá odpovědi 1 a 2. Ve druhé fázi jsou pomocí páru žádost / odpověď

vytvoření všichni další potřební SA potomci. Pár žádost / odpověď IKEv2 používá i pro posílání informačních zpráv jako je například zpráva, která informuje protistranu o ukončení IPsec SA [2, 10].

2.2.8 Zpracování IPsec paketu

Tato část popisuje jakým způsobem je zpracován paket na VPN bráně.

- **Zpracování odchozího paketu** – IPsec VPN brána obdrží uživatelský paket na vnitřním rozhraní a zkontroluje paket proti SPD, aby zjistila, jestli má být paket zahozen, přeposlán mimo IPsec nebo zabezpečen IPsec. Pokud má být paket přeposlán mimo IPsec, je odeslán z vnějšího rozhraní.

Pokud je v SPD definováno, že má být paket zabezpečen IPsec, zkontroluje se SAD, jestli pro paket existuje SA. Pokud není nalezena žádná IPsec SA, je s protistranou inicializováno IKE vyjednávání (za předpokladu, že jsou povoleny automatizované SA a výměny klíče a že je IKE vyjednávání ověřeno v PAD). Když je IKE vyjednávání úspěšné, do SAD je přidána jedna nebo více SA.

Paket je zapouzdřen podle SA parametrů v SAD (AH nebo ESP). Pokud paketu odpovídá jen jedna SA (jen AH nebo ESP), paket je odeslán z vnějšího rozhraní.

Jestliže paketu odpovídá více záznamů v SAD (kombinace AH a ESP), je paket zapouzdřen znovu podle parametrů další SA. Jakmile jsou zpracovány všechny SA odpovídající paketu, je paket odeslán z vnějšího rozhraní na IPsec bránu protistrany.

- **Zpracování příchozího paketu** – IPsec VPN brána obdrží paket na vnějším rozhraní a pokud není zabezpečen IPsec, tak je zpracován podle záznamu v SPD. Jestliže je v SPD, že paket by měl jít mimo IPsec, je odeslán z vnitřního rozhraní. Když se jedná o ICMP (Internet Control Message Protocol) paket adresovaný VPN bráně, tak se předá ICMP procesu. Pokud se nejedná o ICMP paket a SPD nespécifikuje, že by paket měl jít mimo IPsec, pak je zahozen.

Jakmile je na vnějším rozhraní obdržen IPsec paket, tak je odstraněno IPsec zabezpečení podle správné SA v SAD za použití SPI v AH / ESP hlavičce paketu. Když je paket zabezpečen více než jednou IPsec hlavičkou (kombinace AH a ESP), opět se vyhledá správná SA v SAD a zabezpečení je znovu odstraněno.

Poté, co jsou odstraněna veškerá IPsec zabezpečení, paket je odeslán z vnitřního rozhraní VPN brány ke koncovému uživateli [2].

II. PRAKTICKÁ ČÁST

3 KONVENCE

Tato část se věnuje konfiguraci IPsec VPN na referenčním modelu. Příkazy použité v této části mají následující tvar:

Část příkazu tučným písmem je povinná a daná Cisco IOS (Internetwork Operating System). *Povinná uživatelsky volitelná část příkazu je psána kurzívou. Nepovinné uživatelské parametry jsou opět psány kurzívou, ale uzavřeny do hranatých [závorek]. Povinné parametry příkazu jsou uzavřeny do složených {závorek} a jednotlivé možnosti jsou takto | odděleny. Nepovinné parametry příkazu jsou uzavřeny do hranatých [závorek].*

Příklady:

crypto isakmp key *keystring* address *peer-address* [*mask*]

encryption {des | 3des | aes | aes 192 | aes 256}

4 NASAZENÍ IPSEC VPN

Před nasazením IPsec VPN je potřeba promyslet a zvážit následující parametry:

- **IKE politika** – Pouze za předpokladu, že je povolena automatizovaná tvorba SA a výměna klíčů.
- **IPsec transformace (transformační set)** – Jedná se IPsec návrhy zabezpečení.
- **Kryptovací přístupový seznam (Crypto access list)** – Popisuje provoz, který má být zabezpečen IPsec SA.
- **Kryptovací mapa (Crypto map)** – Spojuje IKE politiku, IPsec transformace a kryptovací přístupový seznam.
- **Potřeba přenosu více protokolů a multicast.**
- **Speciální parametry** – Například, zda budou IPsec tunely přecházet NAT zařízení nebo firewall [2].

4.1 Výběr a konfigurace IKE politiky

Při nasazení IPsec VPN s IKE je potřeba vhodně zvolit parametry tak, aby výsledná síť byla jak zabezpečená, tak rozšiřitelná. Mezi parametry IKE patří metoda ověřování a šifrovací algoritmus.

4.1.1 Výběr vhodné IKE metody ověřování

Cisco směrovače podporují tři metody:

- **Ověření pomocí předsdíleného klíče** – Tato metoda může být nastavena na všech Cisco zařízeních podporujících IPsec. Příkaz pro nastavení předsdíleného klíče je zadáván v globálním konfiguračním módu a má následující tvar:

crypto isakmp key *keystring* address *peer-address* [*mask*]

Keystring je alfanumerický řetězec rozlišující velká a malá písmena. Pro správnou funkci spojení musí být identicky nastaven na obou VPN branách a měl by být dostatečně složitý, protože je často nejslabším článkem zabezpečení.

Peer – address je adresa protistrany a *mask* je její maska.

Běžně se používá pro každou dvojici VPN bran rozdílný klíč, pokud chce administrátor z nějakého důvodu použít stejný klíč pro více VPN bran, zadá tzv. wildcard adresu (doplněk masky) místo adresy protistrany.

Bezpečnostní rizika u použití předsdílených klíčů jsou velká a to hlavně kvůli možnosti útoku hrubou silou (zkoušení všech různých řetězců jako klíče). Riziko se zároveň zvyšuje s použitím agresivního módu vyjednávání ve fázi jedna, proto lze tento mód zakázat v globálním konfiguračním módu použitím příkazu:

crypto isakmp aggressive-mode disable

Problém je v tom, že tento příkaz je dostupný až od Cisco IOS verze 12.3. Navíc Cisco VPN a Cisco Easy VPN klienti mohou vyžadovat agresivní mód vyjednávání.

Dalším bezpečnostním rizikem je fakt, že předsdílené klíče jsou v konfiguračním souboru uloženy v nešifrovaném tvaru, proto když se někdo dostane ke konfiguraci VPN brány, získá i klíče. Od Cisco IOS verze 12.3 je možné tyto klíče šifrovat pomocí skupiny příkazů v globálním konfiguračním módu:

key config-key password-encrypt [*master-key*]

Master – key je klíč, který se použije k šifrování a není uložen v konfiguračním souboru.

password encryption aes

- **Ověření pomocí šifrované nonce** – Tato verze ověřování se skládá ze tří kroků:
 - Konfigurace jména IPsec VPN bran a jména domény.
 - Vygenerování RSA klíčů.
 - Konfigurace veřejných klíčů.

Ve výsledku je toto ověřování bezpečnější než předsdílené klíče, ale použití pro větší množství VPN bran je zbytečně složité a proto se spíše používá ověřování pomocí digitálních podpisů, které zároveň poskytuje i vyšší bezpečnost.

- **Ověření pomocí digitálního podpisu** – Tato metoda je velmi vhodná v rozsáhlejších sítích a poskytuje vysokou úroveň zabezpečení. Její nasazení se skládá z šesti kroků:

- Nastavení času na VPN branách.
- Konfigurace jména IPsec VPN bran a jména domény.
- Vygenerování RSA klíčů.
- Určení certifikační autority.
- Ověření certifikační autority.
- Přihlášení IPsec VPN bran k certifikační autoritě [2].

Tato práce se věnuje pouze propojení dvou LAN oddělených Internetem, proto není nezbytně nutné používat ověření pomocí digitálních podpisů. To je důvod, proč není toto ověřování rozebráno do detailu.

4.1.2 Výběr kryptografických parametrů IKE politiky

Dalším krokem po výběru a konfiguraci ověřovací metody je konfigurace IKE politiky. IKE politika je tvořena kryptografickými parametry a je konfigurována příkazem v globálním konfiguračním módu:

crypto isakmp policy priority

Tento příkaz otevře konfigurační mód konkrétní IKE politiky. *Priority* určuje prioritu IKE politiky a jedná se o číslo v rozsahu 1 – 10000, kde nižší číslo značí vyšší prioritu. Na jednom zařízení může být nastaveno několik IKE politik s různou prioritou. Ve fázi jedna IKE vyjednávání se hledá vhodná politika ze seznamu, ten se prochází od nejnižšího čísla priority. Pokud je nalezena, IKE vyjednávání je úspěšné, pokud ne, vyjednávání skončí.

IKE politika je určena těmito parametry:

- **Šifrovací algoritmus.**
- **Diffie – Hellman skupina.**
- **Hash algoritmus.**
- **Ověřovací metoda.**
- **Životnost IKE SA.**

4.1.2.1 Konfigurace šifrovacího algoritmu

Mohou být specifikovány tři druhy šifrovacího algoritmu:

- DES 56 – bit šifrování (základní volba).
- 3DES 168 – bit šifrování.
- AES 128 – bit, 192 – bit, 256 – bit šifrování.

Pro zvolení šifrovacího algoritmu slouží tento příkaz zadaný v konfiguraci IKE politiky:

```
encryption {des | 3des | aes | aes 192 | aes 256}
```

Základní volba DES algoritmu už se dnes nedoporučuje používat, protože jeho ochrana je jednoduše prolomitelná.

4.1.2.2 Konfigurace Diffie – Hellman skupiny

K dispozici jsou tři Diffie – Hellman skupiny:

- Skupina 1 – 768 – bit primární modul (základní volba).
- Skupina 2 – 1024 – bit primární modul.
- Skupina 5 – 1536 – bit primární modul.

Diffie – Hellman skupina 5 je tou nejbezpečnější, ale má nejvyšší procesní nároky. Naopak skupina 1 je nejméně bezpečná, ale nároky má nejnižší.

Ke zvolení Diffie – Hellman skupiny slouží tento příkaz zadaný v konfiguraci IKE politiky:

```
group {1 | 2 | 5}
```

Základní volba, skupina 1, už se dnes taktéž nedoporučuje.

4.1.2.3 Konfigurace Hash algoritmu

Dále je potřeba zvolit hash algoritmus používaný k ověření IKE zpráv, k dispozici jsou dvě varianty:

- MD5 HMAC verze.
- SHA – 1 HMAC verze (základní volba).

Ke zvolení hash algoritmu slouží tento příkaz zadaný v konfiguraci IKE politiky:

hash {sha | md5}

Algoritmus SHA – 1 je o něco pomalejší než MD5.

4.1.2.4 Konfigurace ověřovací metody

Konfigurovat lze tři různé metody:

- Předsdílené klíče.
- Šifrované nonce.
- Digitální podpisy (základní volba).

Pro nastavení ověřovací metody se používá tento příkaz zadaný v konfiguraci IKE:

authentication {rsa-sig | rsa-encr | pre-share}

Při použití předsdílených klíčů je potřeba použít složitý klíč, aby byla zajištěna alespoň minimální úroveň ochrany. Ověření pomocí předsdílených klíčů a šifrovaných nonce je špatně rozšiřitelné. Ověření s využitím digitálních certifikátů je dobře rozšiřitelné a bezpečné, ale vyžaduje existenci certifikační autority.

4.1.2.5 Konfigurace životnosti IKE SA

Posledním parametrem, který je třeba nakonfigurovat, je životnost IKE SA. Když tato životnost vyprší, IPsec partneři znovu vyjednájí IKE fázi jedna. K nastavení životnosti IKE SA se používá tento příkaz zadaný v konfiguraci IKE:

lifetime *seconds*

Parametr *seconds* udává životnost v rozsahu 60 – 86400 sekund se základní volbou 86400 (24 hodin). Čím vyšší je životnost IKE SA, tím se snižuje bezpečnost, protože potencionální útočník má více materiálu na kryptoanalýzu.

Pro správnou funkci IKE vyjednávání je potřeba, aby byla životnost IKE SA na obou stranách komunikace nastavená na stejnou hodnotu [2].

4.2 Výběr a konfigurace IPsec transformací

Dalším krokem v konfiguraci IPsec VPN je konfigurace IPsec transformačního setu. Ten specifikuje kryptografické parametry použité k vyjednání IPsec SA v IKE fázi dvě. Parametry, které je možné specifikovat IPsec transformačním setem jsou:

- **Bezpečnostní protokol a mód.**
- **Hash algoritmus.**
- **Šifrovací algoritmus.**
- **Kompresní algoritmus.**

4.2.1 Výběr bezpečnostního protokolu

Na výběr jsou dva protokoly, které byly dříve popsány v první části této práce:

- AH
- ESP

AH poskytuje ověření zprávy, ESP může poskytovat i šifrování.

4.2.2 Výběr hash algoritmu

Opět je možné zvolit ze dvou dříve popsaných variant:

- MD5 HMAC verze.
- SHA – 1 HMAC verze.

SHA – 1 HMAC je sice pomalejší, ale bezpečnější.

4.2.3 Výběr šifrovacího algoritmu

Šifrovací algoritmus lze zvolit pouze, pokud je zvolen bezpečnostní protokol ESP. Na výběr máme několik variant:

- DES (56 bit)
- 3DES (168 bit)
- AES (128 bit, 192 bit a 256 bit)

- SEAL (160 bit)

DES, 3DES a AES jsou blokové šifry, SEAL je šifra proudová. DES šifrování bylo úspěšně prolomeno v roce 1999, 3DES je bezpečný, ale pomalý algoritmus, AES je z blokových šifer nejrychlejší a zároveň bezpečný. SEAL se používá pouze v nestandardním rozšíření ESP.

4.2.4 Výběr kompresního algoritmu

Po šifrování otevřeného textu vznikne na pohled náhodný šifrovaný text. Protože kompresní algoritmy většinou hledají v datech opakující se vzory, může při kompresi šifrovaného textu dojít k záporné kompresi – komprimovaná data jsou rozsáhlejší než originál. Jediná možnost využití kompresních algoritmů u IPsec VPN je tedy ještě před šifrováním.

Proto byl vytvořen PCP (IP Payload Compression Protocol). Ten komprimuje data ještě před šifrováním. PCP je stejně jako AH a ESP samostatným IP protokolem s identifikátorem 108. Na Cisco směrovačích se používá PCP s LZS (Lempel – Ziv – Stac) kompresním algoritmem. Tento algoritmus má maximální kompresní poměr 2:1.

Kompresní algoritmus použitý mezi IPsec partnery je vyjednáán pomocí IKE a informace o něm je uložena jako PCP SA.

LZS způsobuje relativně vysoké zatížení CPU na IPsec VPN branách, zároveň však snižuje celkový objem dat, takže se dá použít na méně propustných linkách.

4.2.5 Konfigurace IPsec transformačního setu

Ke konfiguraci transformačního setu slouží tento příkaz zadaný v globálním konfiguračním módu:

```
crypto ipsec transform-set transform-set-name transform1 [transform2] [transform3] [transform4]
```

Kde *transform-set-name* je jméno transformačního setu a *transform1* a další jsou jednotlivé transformace. Maximálním možným počtem transformací jsou čtyři:

- Jedna pro AH.
- Dvě pro ESP (ověřování a šifrování).

- Jedna pro kompresi.

Taková konfigurace je však zbytečná, protože dvakrát ověřujeme stejný paket (AH a ESP ověřování). Proto je praktický limit stanoven na tři transformace:

- Jedna pro ověřování (AH nebo ESP).
- Jedna pro šifrování.
- Jedna pro kompresi.

Možnosti transformací:

- **AH – Hash:**
 - *Ah-md5-hmac* – MD5 HMAC hash algoritmus.
 - *Ah-sha-hmac* – SHA – 1 HMAC hash algoritmus.
- **ESP – Hash:**
 - *Esp-md5-hmac* – MD5 HMAC hash algoritmus.
 - *Esp-sha-hmac* – SHA – 1 HMAC hash algoritmus.
- **ESP – Šifrování:**
 - *Esp-null* – Žádné šifrování.
 - *Esp-des* – DES šifrování.
 - *Esp-3des* – 3DES šifrování.
 - *Esp-aes* – AES šifrování se 128 bit klíčem.
 - *Esp-aes 192* – AES šifrování se 192 bit klíčem.
 - *Esp-aes 256* – AES šifrování se 256 bit klíčem.
 - *Esp-seal* – SEAL šifrování.
- **PCP – Kompresi:**
 - *Comp-lzs* – LZS komprese.

Příklady možného použití transformací:

- Pouze AH ověřování.

- Pouze ESP, DES nebo AES šifrování.
- AH ověřování s ESP šifrováním.
- ESP ověřování s ESP šifrováním (nejpoužívanější model).

Ke všem těmto variantám je možné použít LZS kompresi.

Některé transformace nelze použít samostatně:

- ESP ověřování.
- SEAL šifrování.

Při konfiguraci IPsec transformačního setu je možné zvolit mód bezpečnostního protokolu pomocí příkazu zadaného v konfiguraci transformačního setu:

mode {tunnel | transport}

Pokud mód nezvolíme, je základní volbou tunelovací mód. Ten se používá běžně, ale jednou z výjimek je použití GRE tunelů [2].

4.3 Tvorba a konfigurace kryptovacího přístupového seznamu

Selektory určují, který provoz má být chráněn SA a skládají se z několika elementů:

- Zdrojová a cílová IP adresa.
- Protokol následující vrstvy (například ICMP, GRE, TCP, UDP).
- Zdrojový a cílový port (pokud jsou k dispozici).

Selektory se na Cisco směrovačích konfiguruji pomocí kryptovacích přístupových seznamů. Ty jsou rozšířením přístupových seznamů, které se specifikují v kryptovací mapě.

Přístupový seznam pro účely kryptovací mapy se dá nastavit v globálním konfiguračním módu příkazem:

access-list *access-list-number* **{permit | deny}** **{ip | icmp | tcp | udp}** *source-wildcard-ip*
source-mask destination-ip destination-wildcard-mask

Access-list-number je identifikátor přístupového seznamu, **{permit | deny}** slouží jako výběr mezi možnostmi: Povolit a zakázat, **{ip | icmp | tcp | udp}** určuje protokol. *Source-*

ip a *source-wildcard-mask* definují zdrojovou síť, stejně jako *destination-ip* a *destination-wildcard-mask* definují cílovou síť.

Každý takto vytvořený seznam znamená jednu SA v IKE vyjednávání.

Kryptovací přístupový seznam by měl být vždy zrcadlený i na protistraně. Kdyby nebyl, vznikne situace, kdy je pouze jedna strana schopná vyvolat IPsec VPN tunel [2, 11].

4.4 Spojení pomocí kryptovací mapy

Kryptovací mapa slouží ke spojení IKE politik, IPsec transformačních setů a kryptovacích přístupových seznamů do formy, která je použitelná pro jednotlivé rozhraní VPN bran. Příkaz pro vytvoření kryptovací mapy se zadává v globálním konfiguračním módu a má následující tvar:

```
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name] [discover]
```

Map-name je jméno kryptovací mapy, *seq-num* slouží pro připojení více partnerů na jeden vnější interface (každý má různé nastavení). Další možnosti slouží pro použití dynamických kryptovacích map.

Po vytvoření kryptovací mapy je jí potřeba přiřadit IPsec partnera, transformační set a přístupový seznam, to vše se nastavuje v konfiguračním módu kryptovací mapy pomocí příkazů:

```
set peer [hostname | ip-address]
```

Hostname nebo *ip-address* slouží k určení IPsec partnera.

```
set transform-set transform-set-name [transform-set-2] ... [transform-set-6]
```

Tento příkaz umožňuje přiřadit až šest transformačních setů na jednu kryptovací mapu.

```
match address {access-list-number | name}
```

Access-list-number nebo *name* specifikují přístupový seznam.

Pokud existují bezpečnostní rizika, možností jak je odstranit je použití PFS, které se také nastavuje v konfiguračním módu kryptovací mapy pomocí příkazu:

```
set pfs [group1 | group2 | group 5]
```

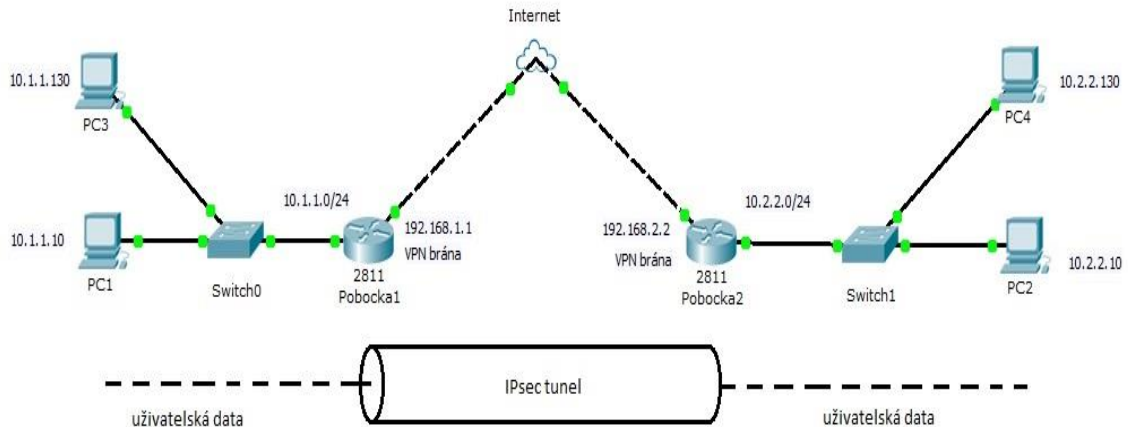
Po vytvoření a konfiguraci kryptovací mapy je potřeba ji ještě přiřadit konkrétnímu vnějšímu rozhraní, k tomu slouží příkaz v konfiguračním módu rozhraní:

crypto map *map-name*

Tím je konfigurace jednoduché IPsec VPN dokončena.

5 SIMULACE IPSEC VPN

K vytvoření simulace byl použit software Cisco Packet Tracer 5.3.3 a zmíněná simulace vypadala následovně:



Obr. 1. Simulace IPsec VPN v software Cisco Packet Tracer 5.3.3.

Jako směrovače byly použity zařízení Cisco Integrated Services Router 2811, toto zařízení bylo použito i jako Internetový cloud, pouze byla změněna ikona. Jako přepínače jsou použity Cisco Catalyst 2960, ty nejsou pro simulaci příliš podstatné, mají tovární nastavení.

5.1 Konfigurace směrovače Internet

Kompletní konfiguraci je možno najít na příloženém CD, zde je uveden podstatný výtah.

Na tomto směrovači jsou nakonfigurovány pouze adresy rozhraní:

1. *!Konfigurace rozhrani*
2. *!*
3. *interface FastEthernet0/0*
4. *ip address 192.168.1.2 255.255.255.0*
5. *duplex auto*
6. *speed auto*
7. *!*
8. *interface FastEthernet0/1*
9. *ip address 192.168.2.1 255.255.255.0*
10. *duplex auto*
11. *speed auto*

Rozhraní FastEthernet0/0 má IP adresu 192.168.1.2 a masku 255.255.255.0 (řádek 4) a rozhraní FastEthernet0/1 má IP adresu 192.168.2.1 a masku 255.255.255.0 (řádek 9).

5.2 Konfigurace VPN bran

Konfigurace obou VPN bran se liší pouze v detailech, proto jsou vždy tyto detaily popsány v následujících částech. Jednotlivé části konfigurací jsou číslovány. Uvedeny jsou pouze výtahy z jednotlivých konfigurací, kompletní konfigurace je možno najít na příloženém CD.

5.2.1 Předsdílený klíč

Konfigurace na VPN bráně Pobočka1:

1. *!Sifrovaci predsdileny klic*
2. *!*
3. *crypto isakmp key HodneSlozityKlic address 192.168.2.2*

Jako předsdílený klíč je použit řetězec HodneSlozityKlic (nejedná se o dostatečně silný klíč) a IP adresa protistrany je 192.168.2.2 (řádek 3).

Konfigurace na VPN bráně Pobočka2:

1. *!Sifrovaci predsdileny klic*
2. *!*
3. *crypto isakmp key HodneSlozityKlic address 192.168.1.1*

Konfigurace na této VPN bráně se liší pouze v IP adrese protistrany (192.168.1.1), klíče musejí být stejné.

5.2.2 IKE politika

Konfigurace na VPN bráně Pobočka1:

1. *!IKE politika*
2. *!*
3. *crypto isakmp policy 10*
4. *encr aes*
5. *hash md5*
6. *authentication pre-share*
7. *group 2*
8. *lifetime 43200*

Na řádce 3 je vidět identifikátor politiky – 10. Jako šifrovací algoritmus je použit AES (řádek 4), jako hash algoritmus je použit MD5 HMAC verze (řádek 5), k ověření je použit

předsdílený klíč (řádek 6), u Diffie – Hellman algoritmu je použit 1024 – bit dlouhý primární modul (řádek 7) a životnost IKE SA je 43200 sekund (řádek 8).

Konfigurace na VPN bráně Pobočka2 je totožná:

1. *!IKE politika*
2. *!*
3. *crypto isakmp policy 10*
4. *encr aes*
5. *hash md5*
6. *authentication pre-share*
7. *group 2*
8. *lifetime 43200*

5.2.3 IPsec transformační set

Konfigurace na VPN bráně Pobočka1:

1. *!Transformacni set*
2. *!*
3. *crypto ipsec transform-set set1 esp-aes esp-md5-hmac*

Transformační set má název set1, používá ESP protokol s AES šifrováním a MD5 HMAC hash algoritmus (řádek 3).

Konfigurace na VPN bráně Pobočka2 je totožná:

1. *!Transformacni set*
2. *!*
3. *crypto ipsec transform-set set1 esp-aes esp-md5-hmac*

5.2.4 Kryptovací přístupový seznam

Konfigurace na VPN bráně Pobočka1:

1. *!Pristupovy seznam*
2. *!*
3. *access-list 101 permit ip 10.1.1.0 0.0.0.127 10.2.2.0 0.0.0.127*

Přístupový seznam má identifikátor 101. Určuje, že do IPsec SA má být zahrnuta veškerá IP komunikace ze zdrojů s IP adresou v rozsahu: 10.1.1.1 – 10.1.1.126 (10.1.1.127 je všesměrová adresa) na cílový rozsah IP adres: 10.2.2.1 – 10.2.2.126 (řádek 3).

Konfigurace na VPN bráně Pobočka2:

1. *!Pristupovy seznam*

2. !
3. *access-list 101 permit ip 10.2.2.0 0.0.0.127 10.1.1.0 0.0.0.127*

Konfigurace na této bráně je zrcadlová – adresy jsou prohozeny.

5.2.5 Kryptovací mapa

Konfigurace na VPN bráně Pobočka1:

1. *!Kryptovaci mapa*
2. !
3. *crypto map map1 10 ipsec-isakmp*
4. *set peer 192.168.2.2*
5. *set transform-set set1*
6. *match address 101*

Název kryptovací mapy je map1 a její sekvenční číslo je 10 (řádek 3), IP adresa IPsec partnera je 192.168.2.2 (řádek 4), jako transformační set je zvolen set1 (řádek 5) a přístupový seznam má identifikátor 101 (řádek 6).

Konfigurace na VPN bráně Pobočka2:

1. *!Kryptovaci mapa*
2. !
3. *crypto map map1 10 ipsec-isakmp*
4. *set peer 192.168.1.1*
5. *set transform-set set1*
6. *match address 101*

Zde je konfigurace téměř totožná, rozdíl je pouze v IP adrese IPsec partnera – 192.168.1.1 (řádek 4).

5.2.6 Vnitřní rozhraní

Konfigurace na VPN bráně Pobočka1:

1. *!Vnitřni rozhrani*
2. !
3. *interface FastEthernet0/1*
4. *ip address 10.1.1.1 255.255.255.0*
5. *duplex auto*
6. *speed auto*

Vnitřní rozhraní má IP adresu 10.1.1.1 a masku 255.255.255.0 (řádek 4).

Konfigurace na VPN bráně Pobočka2:

1. *!Vnitřní rozhraní*
2. *!*
3. *interface FastEthernet0/1*
4. *ip address 10.2.2.1 255.255.255.0*
5. *duplex auto*
6. *speed auto*

Vnitřní rozhraní má IP adresu 10.2.2.1 a masku 255.255.255.0 (řádek 4).

5.2.7 Vnější rozhraní

Konfigurace na VPN bráně Pobočka1:

1. *!Vnější rozhraní*
2. *!*
3. *interface FastEthernet0/0*
4. *ip address 192.168.1.1 255.255.255.0*
5. *duplex auto*
6. *speed auto*
7. *crypto map map1*

Vnější rozhraní má IP adresu 192.168.1.1 a masku 255.255.255.0 (řádek 4), Kryptovací mapa je mapa s označením map1 (řádek 7).

Konfigurace na VPN bráně Pobočka2:

1. *!Vnější rozhraní*
2. *!*
3. *interface FastEthernet0/0*
4. *ip address 192.168.2.2 255.255.255.0*
5. *duplex auto*
6. *speed auto*
7. *crypto map map1*

Vnější rozhraní má IP adresu 192.168.2.2 a masku 255.255.255.0 (řádek 4), Kryptovací mapa je mapa s označením map1 (řádek 7).

5.2.8 Statické směrování

Konfigurace na VPN bráně Pobočka1:

1. *!Směrování na základní branu*
2. *!*
3. *ip classless*
4. *ip route 0.0.0.0 0.0.0.0 192.168.1.2*

Statická konfigurace základní brány na IP adresu 192.168.1.2 (adresa rozhraní FastEthernet0/0 směrovače Internet – řádek 4).

Konfigurace na VPN bráně Pobočka2:

1. *!Smerovani na zakladni branu*
2. *!*
3. *ip classless*
4. *ip route 0.0.0.0 0.0.0.0 192.168.2.1*

Statická konfigurace základní brány na IP adresu 192.168.2.1 (adresa rozhraní FastEthernet0/1 směrovače Internet – řádek 4).

5.3 Konfigurace pracovních stanic

Každá pracovní stanice (PC1 – PC4) má nakonfigurovanou pouze IP adresu, masku sítě a základní bránu.

PC1: IP adresa 10.1.1.10, maska 255.255.255.0 a základní brána 10.1.1.1.

PC2: IP adresa 10.2.2.10, maska 255.255.255.0 a základní brána 10.2.2.1.

PC3: IP adresa 10.1.1.130, maska 255.255.255.0 a základní brána 10.1.1.1.

PC4: IP adresa 10.2.2.130, maska 255.255.255.0 a základní brána 10.2.2.1.

5.4 Funkcionalita simulace

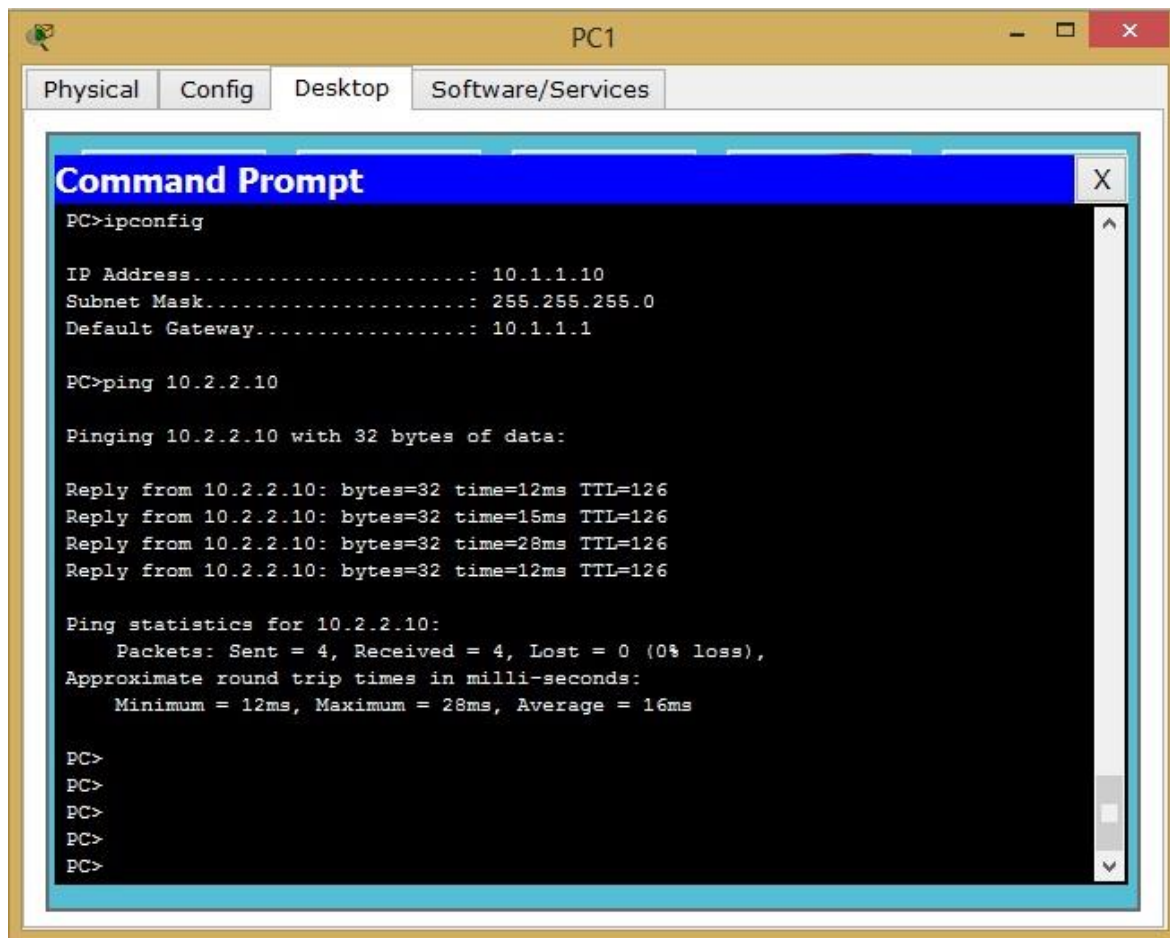
Podle nastavení přístupových seznamů na VPN branách je zřejmé, že do IPsec komunikace by měly být zahrnuty pouze pracovní stanice PC1 a PC2. PC3 a PC4 nemají IP adresy z daného rozsahu a proto je komunikace mezi nimi, stejně jako komunikace s pracovní stanicí PC1 nebo PC2, nezabezpečena.

Dalším faktem je, že směrovač Internet nemá povědomí o lokálních sítích za jednotlivými VPN branami a proto nedokáže směrovat pakety mezi jednotlivými pracovními stanicemi, pokud nejsou IPsec tunelovány.

Jednoduchým testem funkcionality simulace je ping mezi jednotlivými pracovními stanicemi.

5.4.1 Ping z PC1

Protože je simulace zrcadlová, stačí poslat ping pouze z jedné strany. Ping z pracovní stanice PC1 by měl projít přes IPsec tunel na pracovní stanici PC2, pracovní stanice PC4 by měla být nedostupná, protože nemáme kompletní směrovací tabulky a ping na pracovní stanici PC3 by měl projít bez problémů, protože se jedná o lokální síť a pakety jsou přepínány na lokálním přepínači.



```
PC1
Physical Config Desktop Software/Services
Command Prompt
PC>ipconfig

IP Address. . . . . : 10.1.1.10
Subnet Mask. . . . . : 255.255.255.0
Default Gateway. . . . . : 10.1.1.1

PC>ping 10.2.2.10

Pinging 10.2.2.10 with 32 bytes of data:

Reply from 10.2.2.10: bytes=32 time=12ms TTL=126
Reply from 10.2.2.10: bytes=32 time=15ms TTL=126
Reply from 10.2.2.10: bytes=32 time=28ms TTL=126
Reply from 10.2.2.10: bytes=32 time=12ms TTL=126

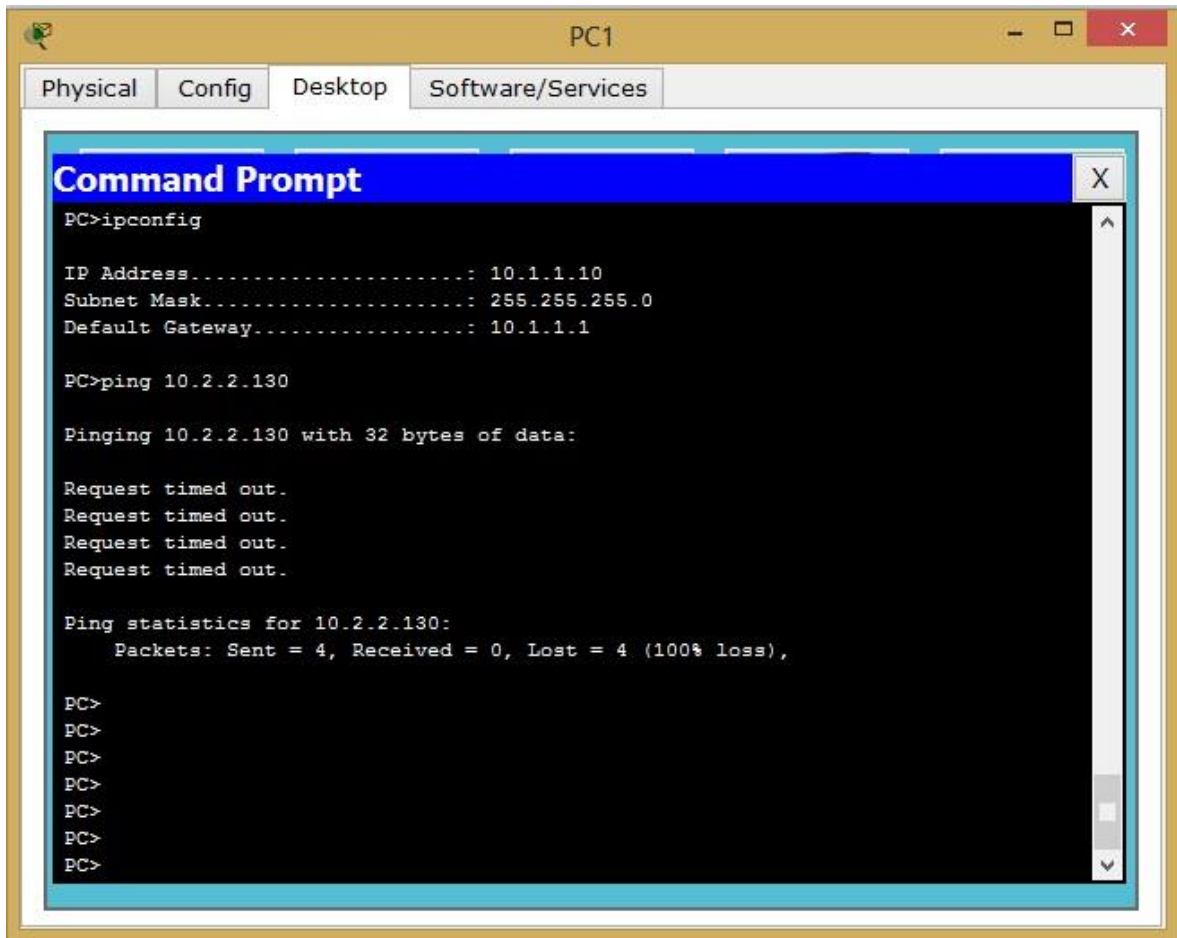
Ping statistics for 10.2.2.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 28ms, Average = 16ms

PC>
PC>
PC>
PC>
PC>
```

Obr. 2. Ping z PC1 na PC2.

Na obrázku 2 je patrné, že ping mezi pracovními stanicemi PC1 a PC2 prošel bez problémů, tento obrázek je pořízen v době, kdy už je vytvořena IPsec SA pro tuto komunikaci.

Na obrázku 3 je naopak vyobrazen ping mezi PC1 a PC4. PC4 neleží v rozsahu IP adres určenému k IPsec tunelování. Protože nemáme kompletní směrovací tabulky, ping podle předpokladů neprošel a vypršel mu TTL.



The image shows a screenshot of a virtual PC environment. The window title is "PC1" and it has tabs for "Physical", "Config", "Desktop", and "Software/Services". The "Software/Services" tab is active, displaying a "Command Prompt" window. The command prompt shows the following text:

```
PC>ipconfig

IP Address.....: 10.1.1.10
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.1.1.1

PC>ping 10.2.2.130

Pinging 10.2.2.130 with 32 bytes of data:

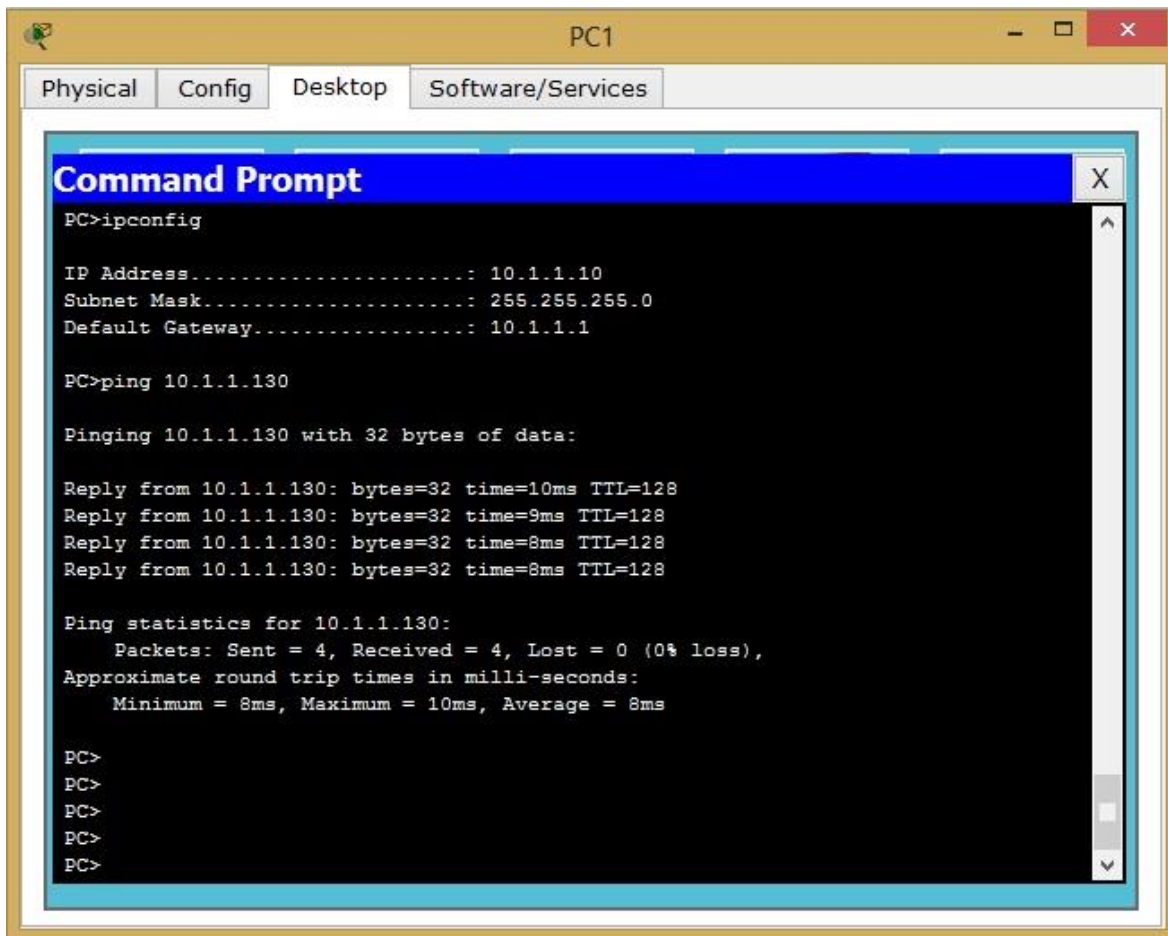
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.2.2.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
PC>
PC>
PC>
PC>
PC>
PC>
```

Obr. 3. Ping z PC1 na PC4.

Na obrázku 4 je znázorněn ping mezi pracovními stanicemi PC1 a PC3, které jsou ve stejné lokální síti, proto komunikace mezi nimi nejde přes VPN bránu – směrovač, ale pouze přes lokální přepínač. Je možné vysledovat, že průměrný čas v milisekundách potřebný k dosažení cíle je nižší, než u obrázku 2, kde pakety procházejí přes tři směrovače a dva přepínače.



```
PC1
Physical Config Desktop Software/Services
Command Prompt
PC>ipconfig

IP Address. . . . . : 10.1.1.10
Subnet Mask. . . . . : 255.255.255.0
Default Gateway. . . . . : 10.1.1.1

PC>ping 10.1.1.130

Pinging 10.1.1.130 with 32 bytes of data:

Reply from 10.1.1.130: bytes=32 time=10ms TTL=128
Reply from 10.1.1.130: bytes=32 time=9ms TTL=128
Reply from 10.1.1.130: bytes=32 time=8ms TTL=128
Reply from 10.1.1.130: bytes=32 time=8ms TTL=128

Ping statistics for 10.1.1.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 8ms, Maximum = 10ms, Average = 8ms

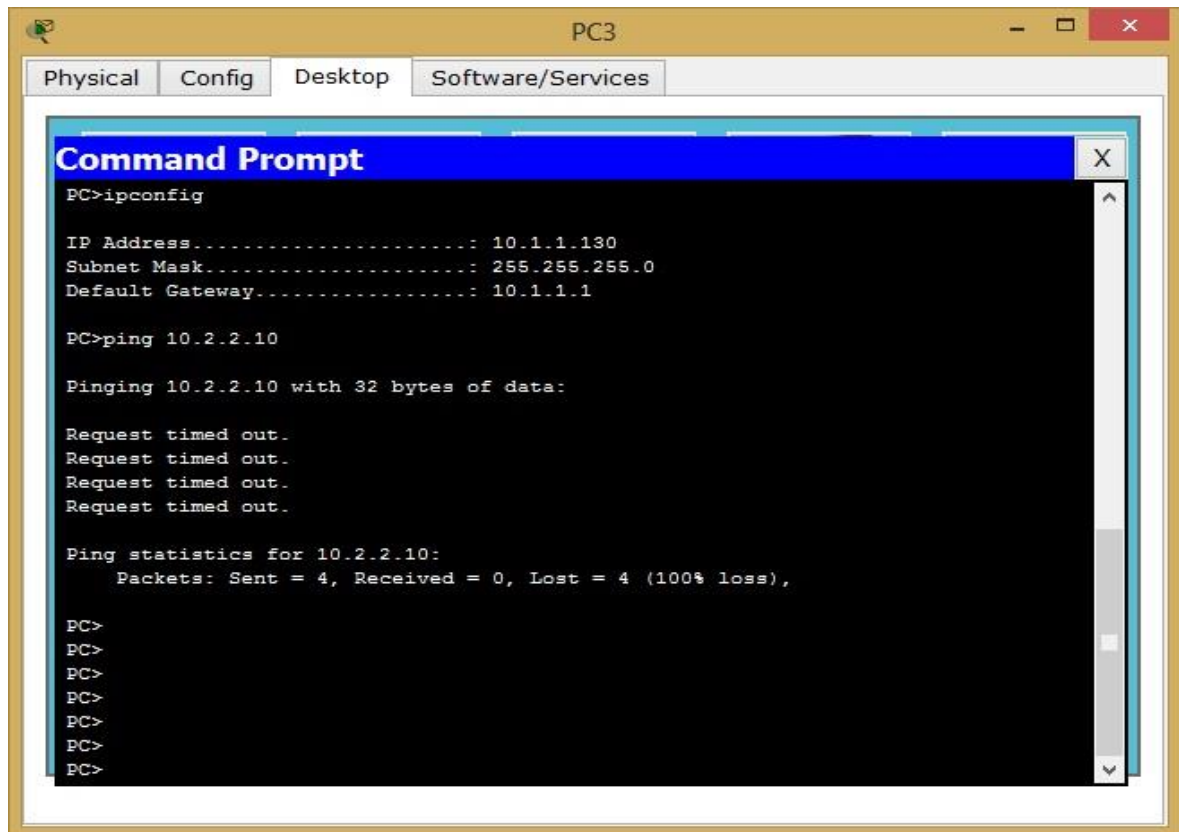
PC>
PC>
PC>
PC>
PC>
```

Obr. 4. Ping z PC1 na PC3.

5.4.2 Ping z PC3

Pracovní stanice PC3 leží mimo rozsah IP adres určených k IPsec tunelování a proto je veškerá komunikace z této stanice nechráněna. Protože nemáme kompletní směrovací tabulky, ping na pracovní stanice PC2 a PC4 by měl být neúspěšný.

Jednotlivé výsledky příkazů ping jsou na obrázcích 5 a 6.



The screenshot shows a Command Prompt window titled "Command Prompt" with a blue header bar. The window is open on a PC3 desktop environment, with tabs for "Physical", "Config", "Desktop", and "Software/Services". The command prompt shows the following text:

```
PC>ipconfig

IP Address.....: 10.1.1.130
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.1.1.1

PC>ping 10.2.2.10

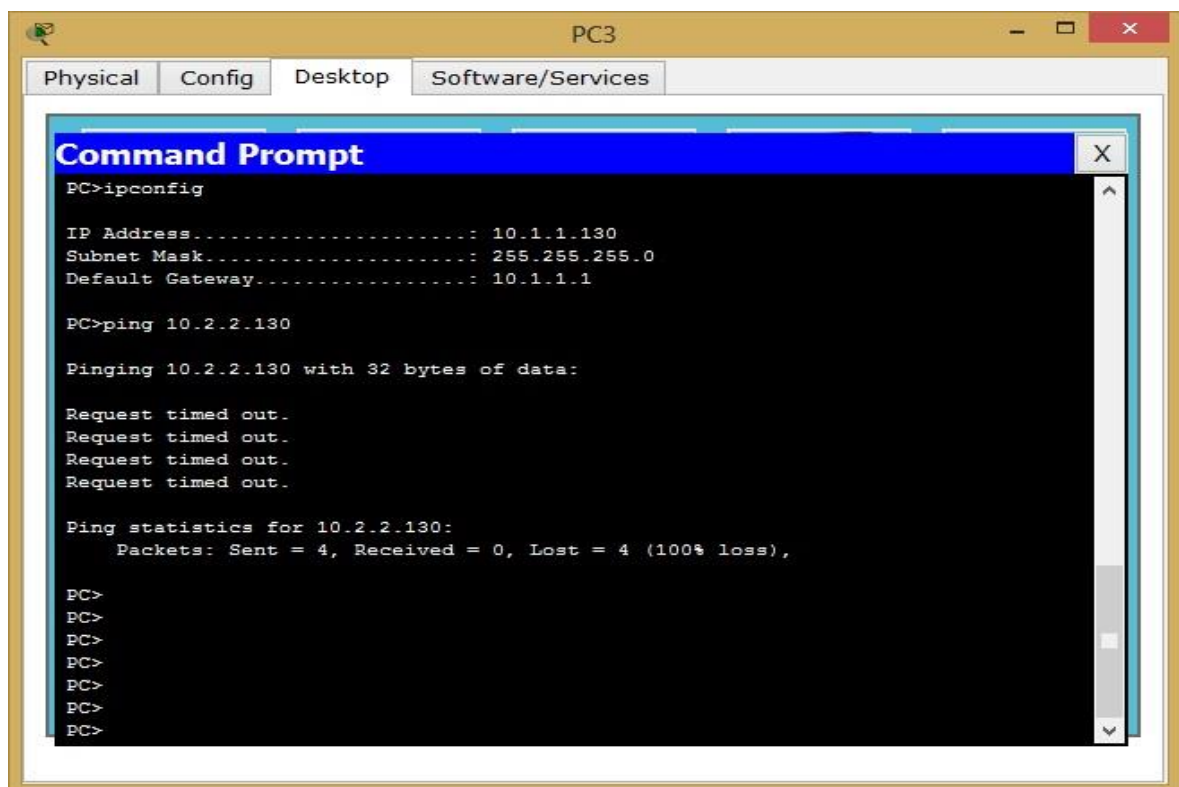
Pinging 10.2.2.10 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.2.2.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
PC>
PC>
PC>
PC>
PC>
PC>
```

Obr. 5. Ping z PC3 na PC2.



The screenshot shows a Command Prompt window titled "Command Prompt" with a blue header bar. The window is open on a PC3 desktop environment, with tabs for "Physical", "Config", "Desktop", and "Software/Services". The command prompt shows the following text:

```
PC>ipconfig

IP Address.....: 10.1.1.130
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 10.1.1.1

PC>ping 10.2.2.130

Pinging 10.2.2.130 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

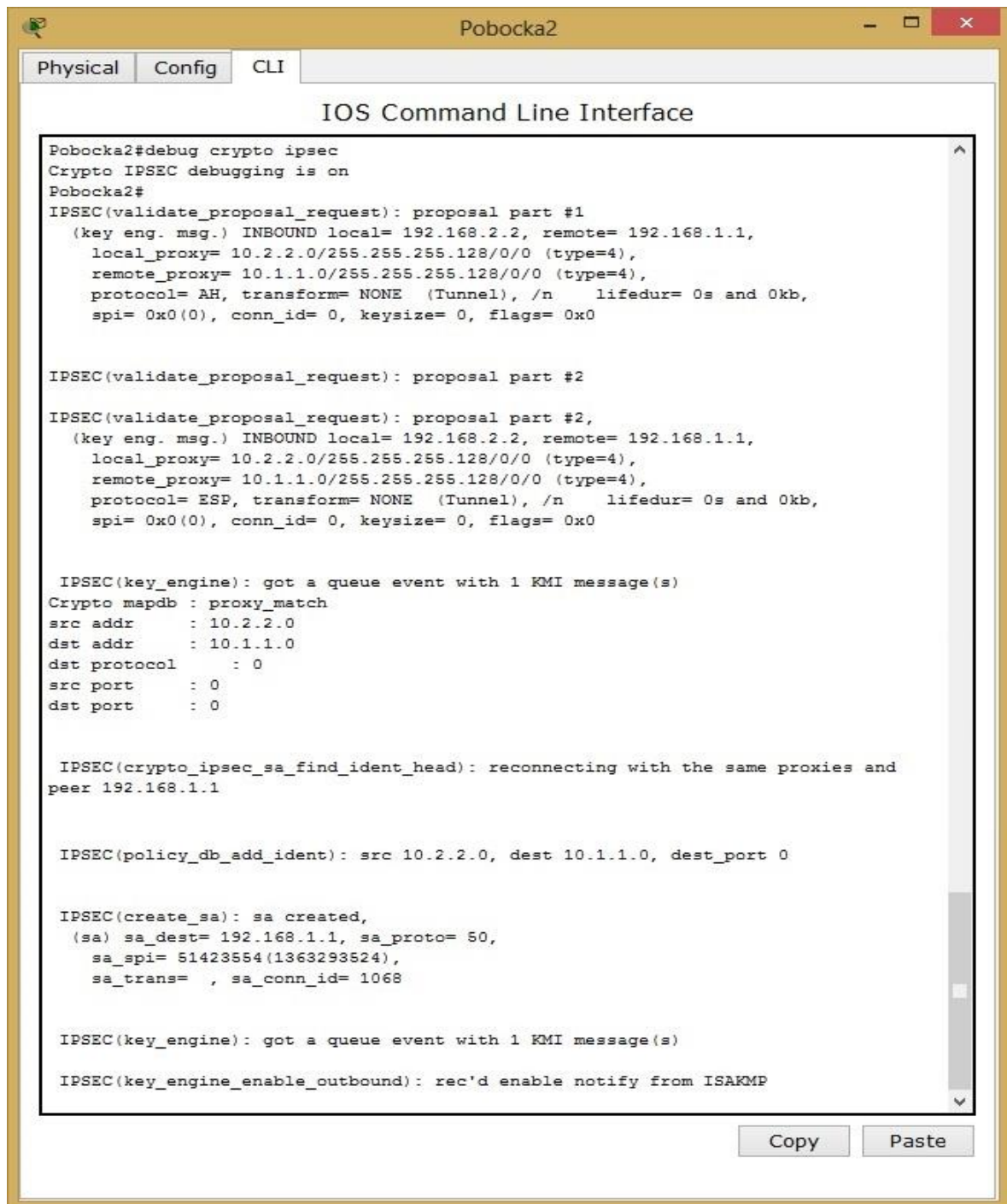
Ping statistics for 10.2.2.130:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

PC>
PC>
PC>
PC>
PC>
PC>
PC>
```

Obr. 6. Ping z PC3 na PC4.

5.4.3 Vytvoření IPsec SA

Před navázáním komunikace mezi pracovními stanicemi PC1 a PC2 musí dojít k IKE vyjednávání a k vytvoření IPsec SA na VPN branách pro tuto komunikaci. Vyjednávání a vytvoření IPsec SA bylo zachyceno pomocí příkazu **debug crypto ipsec** na VPN bráně Pobočka2 – obrázek 7.



```
Pobočka2#debug crypto ipsec
Crypto IPSEC debugging is on
Pobočka2#
IPSEC(validate_proposal_request): proposal part #1
(key eng. msg.) INBOUND local= 192.168.2.2, remote= 192.168.1.1,
local_proxy= 10.2.2.0/255.255.255.128/0/0 (type=4),
remote_proxy= 10.1.1.0/255.255.255.128/0/0 (type=4),
protocol= AH, transform= NONE (Tunnel), /n lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0

IPSEC(validate_proposal_request): proposal part #2

IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) INBOUND local= 192.168.2.2, remote= 192.168.1.1,
local_proxy= 10.2.2.0/255.255.255.128/0/0 (type=4),
remote_proxy= 10.1.1.0/255.255.255.128/0/0 (type=4),
protocol= ESP, transform= NONE (Tunnel), /n lifedur= 0s and 0kb,
spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x0

IPSEC(key_engine): got a queue event with 1 KMI message(s)
Crypto mapdb : proxy_match
src addr      : 10.2.2.0
dst addr      : 10.1.1.0
dst protocol   : 0
src port      : 0
dst port      : 0

IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with the same proxies and
peer 192.168.1.1

IPSEC(policy_db_add_ident): src 10.2.2.0, dest 10.1.1.0, dest_port 0

IPSEC(create_sa): sa created,
(sa) sa_dest= 192.168.1.1, sa_proto= 50,
sa_spi= 51423554(1363293524),
sa_trans= , sa_conn_id= 1068

IPSEC(key_engine): got a queue event with 1 KMI message(s)

IPSEC(key_engine_enable_outbound): rec'd enable notify from ISAKMP
```

Obr. 7. IKE vyjednávání a tvorba IPsec SA.


```

COM1 - PuTTY
Pobočka2#debug crypto ipsec
Crypto IPSEC debugging is on
Pobočka2#
*May 22 12:13:03.127: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*May 22 12:13:03.135: IPSEC(validate_proposal_request): proposal part #1
*May 22 12:13:03.135: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) INBOUND local= 192.168.2.2, remote= 192.168.1.1,
  local_proxy= 10.2.2.0/255.255.255.128/0/0 (type=4),
  remote_proxy= 10.1.1.0/255.255.255.128/0/0 (type=4),
  protocol= ESP, transform= NONE (Tunnel),
  lifedur= 0s and 0kb,
  spi= 0x0(0), conn_id= 0, keysize= 128, flags= 0x0
*May 22 12:13:03.135: Crypto mapdb : proxy_match
  src addr      : 10.2.2.0
  dst addr      : 10.1.1.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*May 22 12:13:03.139: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*May 22 12:13:03.143: Crypto mapdb : proxy_match
  src addr      : 10.2.2.0
  dst addr      : 10.1.1.0
  protocol      : 0
  src port      : 0
  dst port      : 0
*May 22 12:13:03.143: IPSEC(crypto_ipsec_sa_find_ident_head): reconnecting with
the same proxies and peer 192.168.1.1
*May 22 12:13:03.143: IPSEC(policy_db_add_ident): src 10.2.2.0, dest 10.1.1.0, d
est_port 0

*May 22 12:13:03.143: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.2.2, sa_proto= 50,
  sa_spi= 0x5EC24D81(1589792129),
  sa_trans= esp-aes esp-md5-hmac , sa_conn_id= 2001
  sa_lifetime(k/sec)= (4455017/3600)
*May 22 12:13:03.143: IPSEC(create_sa): sa created,
  (sa) sa_dest= 192.168.1.1, sa_proto= 50,
  sa_spi= 0x96636ADC(2523097820),
  sa_trans= esp-aes esp-md5-hmac , sa_conn_id= 2002
  sa_lifetime(k/sec)= (4455017/3600)
*May 22 12:13:03.147: IPSEC(key_engine): got a queue event with 1 KMI message(s)
*May 22 12:13:03.147: IPSEC(key_engine_enable_outbound): rec'd enable notify fro
m ISAKMP
*May 22 12:13:03.147: IPSEC(key_engine_enable_outbound): enable SA with spi 2523
097820/50
*May 22 12:13:03.147: IPSEC(update_current_outbound_sa): updated peer 192.168.1.
1 current outbound sa to SPI 96636ADC

```

Obr. 10. IKE vyjednávání a tvorba IPsec SA.

```

COM1 - PuTTY
Pobočka2#sh crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
192.168.2.2  192.168.1.1  QM_IDLE       1001 ACTIVE

IPv6 Crypto ISAKMP SA
Pobočka2#

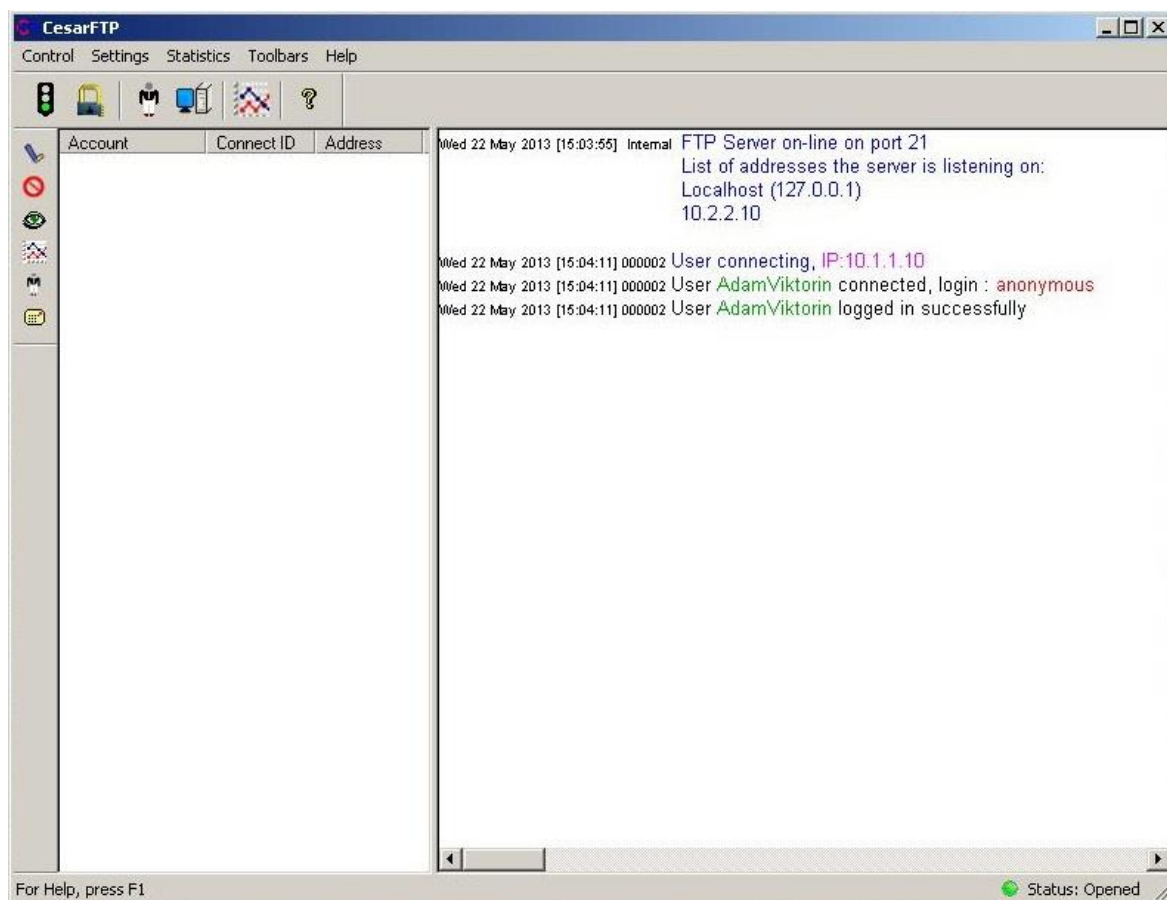
```

Obr. 11. IPsec SA mezi VPN branami po navázání komunikace.

Obrázky 9 až 11 znázorňují navázání IPsec komunikace, vyjednávání a vytvoření IPsec SA a výpis existujících SA po navázání komunikace.

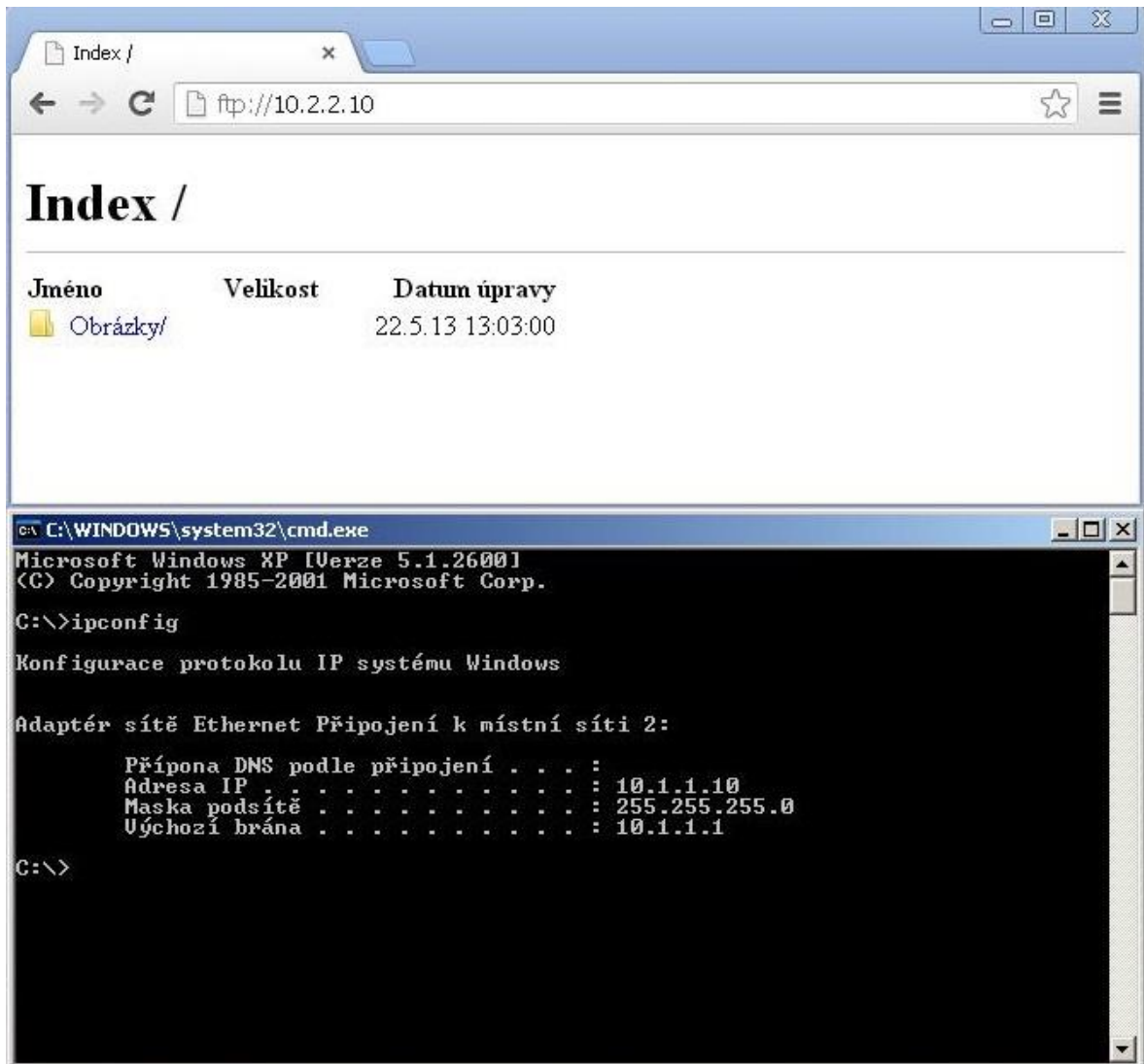
6.2 Přístup na FTP server

K vytvoření FTP serveru byla použita freeware aplikace CesarFTP společnosti ACLogic. FTP server byl spuštěn na pracovní stanici PC2 (IP 10.2.2.10) a spojení bylo navázáno z pracovní stanice PC1 (IP 10.1.1.10).



Obr. 12. CesarFTP server.

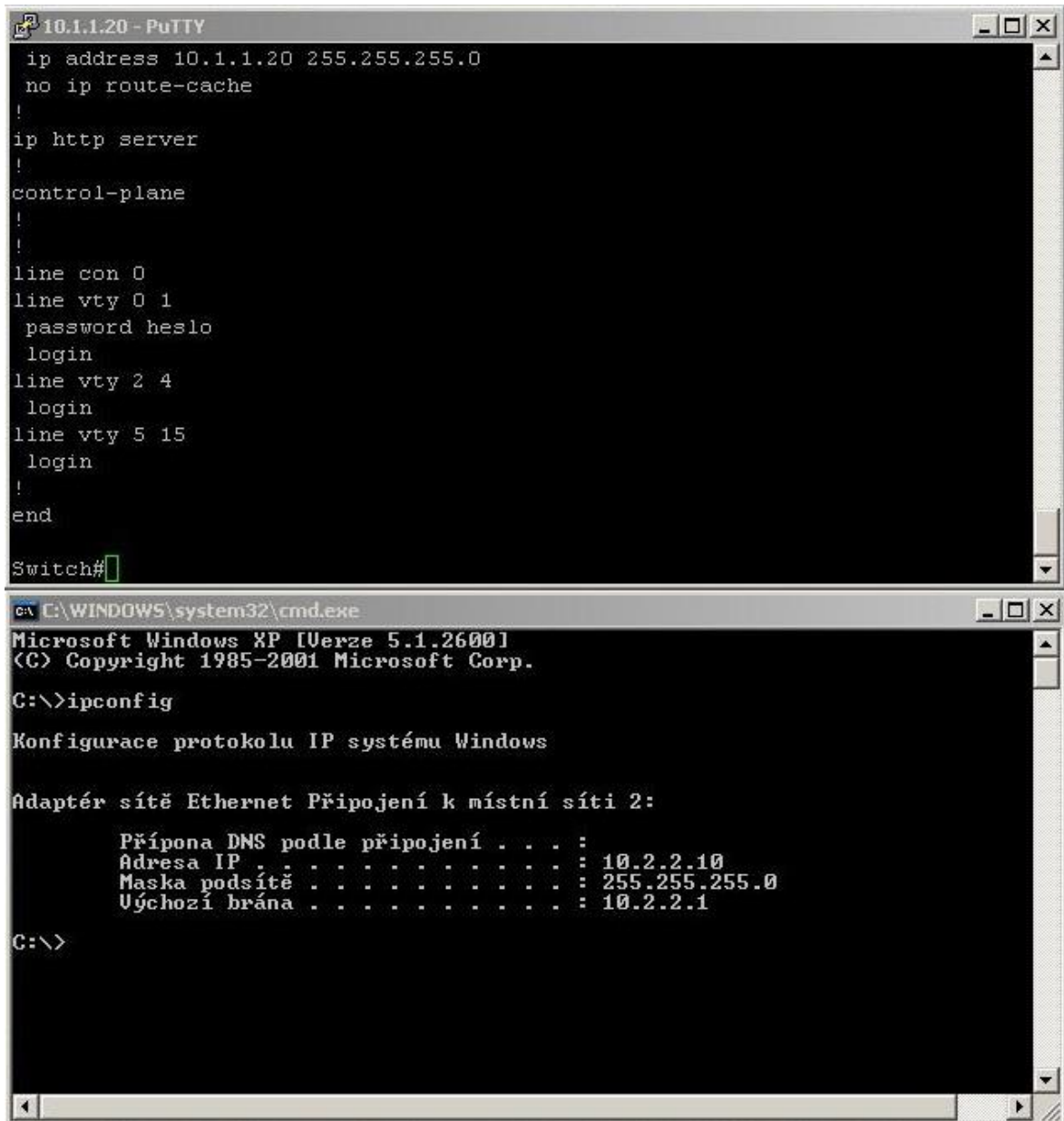
Na obrázku 12 je vidět, že server naslouchá na IP adresách 127.0.0.1 (localhost) a 10.2.2.10. Před spuštěním serveru byl vytvořen uživatel AdamViktorin s možností anonymního přihlášení (bez uživatelského jména a hesla). Dále je v logu serveru vidět, že se tento uživatel přihlásil z IP adresy 10.1.1.10, což je pracovní stanice PC1. Na obrázku 13 je tato situace zachycena ze strany PC1. K připojení byl použit internetový prohlížeč Google Chrome.



Obr. 13. Připojení k FTP serveru z pracovní stanice PC1.

6.3 Telnet přepínače

Pro vzdálené připojení byl použit starší a nezabezpečený telnet protokol, který ovšem zabezpečuje IPsec tunel. Aby bylo vzdálené připojení na přepínač možné, byla mu nastavena IP adresa 10.1.1.20. Telnet připojení bylo navázáno z pracovní stanice PC2 a je znázorněno na obrázku 14. V horní části obrázku lze vidět konec výpisu aktuální konfigurace přepínače a ve spodní části konfiguraci PC2.



```
10.1.1.20 - PuTTY
ip address 10.1.1.20 255.255.255.0
no ip route-cache
!
ip http server
!
control-plane
!
!
line con 0
line vty 0 1
  password heslo
  login
line vty 2 4
  login
line vty 5 15
  login
!
end
Switch#

C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Verze 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ipconfig

Konfigurace protokolu IP systému Windows

Adaptér sítě Ethernet Připojení k místní síti 2:

    Přípona DNS podle připojení . . . . :
    Adresa IP . . . . . : 10.2.2.10
    Maska podsítě . . . . . : 255.255.255.0
    Účchozí brána . . . . . : 10.2.2.1

C:\>
```

Obr. 14. Telnet přepínače.

ZÁVĚR

V této práci byla navržena jednoduchá konfigurace IPsec VPN pro propojení dvou LAN oddělených Internetem. Byla prokázána funkčnost této konfigurace jak v simulačním software Cisco Packet Tracer 5.3.3, tak v laboratořích na zařízeních Cisco akademie FAI. Dále byly naznačeny způsoby využití takové konfigurace v praxi – vzdálená správa aktivních prvků (telnet, SSH), FTP server a komunikace mezi jednotlivými pracovními stanicemi.

Pokračování této práce by se mohlo zaměřit na jiné tunelovací protokoly, jejich využití v praxi a případně jejich porovnání z hledisek rychlosti, bezpečnosti a jednoduchosti implementace.

CONCLUSION

In this thesis, simple IPsec VPN between two LANs separated by Internet was designed and implemented. Its functionality was proved in Cisco Packet Tracer 5.3.3 software and also in laboratory environment on Cisco academy devices. Ways of practical use were pointed out – remote management (telnet, SSH), FTP server and communication between separated workstations.

Continuation of this thesis can focus on other tunnelling protocols, their practical use and compare them in speed, safety and simplicity of implementation.

SEZNAM POUŽITÉ LITERATURY

- [1] LUHOVÝ, Karel. VPN (1) - historie, definice a důvody budování. In: *Svět sítí - informace ze světa počítačových sítí* [online]. 2003 [cit. 2013-05-28]. Dostupné z: <http://www.svetsiti.cz/clanek.asp?cid=VPN-1-historie-definice-a-duvody-budovani-612003>
- [2] LEWIS, Mark. Comparing, designing, and deploying VPNs. Indianapolis: Cisco Press, 2006, 1043 p. ISBN 1-58705-179-6.
- [3] PRŮCHA, Ondřej. *Vše kolem VPN* [online]. 2005 [cit. 2013-05-14]. Dostupné z: <http://home.zcu.cz/~ondrous/>
- [4] RFC 3931 - Layer Two Tunneling Protocol - Version 3 (L2TPv3). In: *IETF Tools* [online]. 2005 [cit. 2013-05-28]. Dostupné z: <http://tools.ietf.org/html/rfc3931>
- [5] TN Algoritmy hash. In: *TN Microsoft TechNet: Materiály pro IT odborníky* [online]. 2013 [cit. 2013-05-28]. Dostupné z: [http://technet.microsoft.com/cs-cz/library/cc726061\(v=ws.10\).aspx](http://technet.microsoft.com/cs-cz/library/cc726061(v=ws.10).aspx)
- [6] ŠTRÁFELDA, Jan. Šifrování a signalizace. In: ŠTRÁFELDA, Jan. *Shaman.cz* [online]. 2001 [cit. 2013-05-28]. Dostupné z: <http://www.shaman.cz/sifrovani/>
- [7] KREJBICHOVÁ, Barbora. *Šifrování*. [online]. [cit. 2013-05-14]. Dostupné z: <http://home.zcu.cz/~barkrej/>
- [8] MIČKA, Pavel. Diffie-Hellman - Algoritmy.net. In: MIČKA, Pavel. *Algoritmy.net* [online]. 2012 [cit. 2013-05-28]. Dostupné z: <http://www.algoritmy.net/article/84/Diffie-Hellman>
- [9] RFC 2409 - The Internet Key Exchange (IKE). In: *IETF Tools* [online]. 1998 [cit. 2013-05-14]. Dostupné z: <http://tools.ietf.org/html/rfc2409>
- [10] RFC 4306 - Internet Key Exchange (IKEv2 Protocol). In: *IETF Tools* [online]. 2005 [cit. 2013-05-14]. Dostupné z: <http://tools.ietf.org/html/rfc4306>
- [11] Configuring IP Access List. In: *Cisco Systems, Inc* [online]. 2007 [cit. 2013-05-28]. Dostupné z: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml#standacl

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard.
AH	Authentication Header.
BGP	Border Gateway Protocol.
C	Customer.
CBC	Cipher – Block Chaining.
CE	Customer Edge.
CFB	Cipher FeedBack.
CPU	Central Processing Unit.
DES	Data Encryption Standard.
DSA	Digital Signature Algorithm.
DSP	Data Service Provider.
ECB	Electronic CodeBook.
ESP	Encapsulating Security Payload.
FAI	Fakulta Aplikované Informatiky.
FTP	File Transfer Protocol.
GRE	Generic Routing Protocol.
HMAC	Hash Message Authentication Code.
ICMP	Internet Control Message Protocol.
ICV	Integrity Check Value.
IEEE	Institute of Electrical and Electronics Engineers.
IETF	Internet Engineering Task Force.
IKE	Internet Key Exchange.
IOS	Internetwork Operating System.
IP	Internet Protocol.

IPLS	Internet protocol – Only Local are network Service.
IPsec	Internet Protocol security.
ISAKMP	Internet Security Association and Key Management Protocol.
ISO / OSI	International Organization for Standardization / Open Systems Interconnection.
L2F	Layer 2 Forwarding.
L2TP	Layer 2 Tunneling Protocol.
L2VPN	Layer 2 Virtual Private Network.
L3VPN	Layer 3 Virtual Private Network.
LAN	Local Area Network.
LSP	Link State Protocol.
LZS	Lempel – Ziv – Stac.
MAC	Media Access Control.
MAC	Message Authentication Code.
MD5	Message Digest 5.
MP	MultiPoint.
MPLS	MultiProtocol Layer Switching.
MPPE	Microsoft Point – to – Point Encryption.
NAS	Network Access Server.
NAT	Native Address Translation.
OFB	Output FeedBack.
P	Provdier.
P2P	Point – to – Point.
PAD	Peer Authorization Database.
PCP	IP Payload Compression Protocol.

PE	Provider Edge.
PFS	Perfect Forward Secrecy.
PKI	Public Key Infrastructure.
PPP	Point – to – Point Protocol.
PPTP	Point – to – Point Tunneling Protocol.
RSA	Rivest, Shamir, Addleman.
SA	Security Association.
SAD	Security Association Database.
SEAL	Software Encryption ALgorithm.
SHA – 1	Secure Hash Algorithm.
SKEME	Secure Key Exchange MEchanism.
SPD	Security Policy Database.
SPI	Security Parameter Index.
SSL	Secure Sockets Layer.
ToS	Type of Service.
TSL	Transport Layer Security.
TTL	Time – To – Live.
VLAN	Virtual Local Area Network.
VPLS	Virtual Private Local area network Service.
VPN	Virtual Private Network.
VPWS	Vitual Private Wire Service.
VTI	Virtual Tunnel Interface.
WAN	Wide Area Network.

SEZNAM OBRÁZKŮ

<i>Obr. 1. Simulace IPsec VPN v software Cisco Packet Tracer 5.3.3.....</i>	<i>46</i>
<i>Obr. 2. Ping z PC1 na PC2.....</i>	<i>52</i>
<i>Obr. 3. Ping z PC1 na PC4.....</i>	<i>53</i>
<i>Obr. 4. Ping z PC1 na PC3.....</i>	<i>54</i>
<i>Obr. 5. Ping z PC3 na PC2.....</i>	<i>55</i>
<i>Obr. 6. Ping z PC3 na PC4.....</i>	<i>55</i>
<i>Obr. 7. IKE vyjednávání a tvorba IPsec SA.....</i>	<i>56</i>
<i>Obr. 8. IPsec SA mezi VPN branami před zahájením komunikace.</i>	<i>57</i>
<i>Obr. 9. Ping z PC1 na PC2.....</i>	<i>57</i>
<i>Obr. 10. IKE vyjednávání a tvorba IPsec SA.....</i>	<i>58</i>
<i>Obr. 11. IPsec SA mezi VPN branami po navázání komunikace.....</i>	<i>58</i>
<i>Obr. 12. CesarFTP server.</i>	<i>59</i>
<i>Obr. 13. Připojení k FTP serveru z pracovní stanice PC1.....</i>	<i>60</i>
<i>Obr. 14. Telnet přepínače.</i>	<i>61</i>

SEZNAM PŘÍLOH

P I Schéma zapojení simulace IPsec VPN.

Uloženo na CD. Cesta: CD\schemata\schemaIPsec.jpg

P II Konfigurační soubory simulace IPsec VPN.

Uloženo na CD. Cesta: CD\konfigurace\IPsec

P III Simulace zapojení IPsec VPN (Cisco Packet Tracer 5.3.3).

Uloženo na CD. Cesta: CD\simulace\IPsec.pkt

P IV Schéma zapojení simulace GRE VPN.

Uloženo na CD. Cesta: CD\schemata\schemaGRE.jpg

P V Konfigurační soubory simulace GRE VPN.

Uloženo na CD. Cesta: CD\konfigurace\GRE

P VI Simulace zapojení GRE VPN (Cisco Packet Tracer 5.3.3).

Uloženo na CD. Cesta: CD\simulace\GRE.pkt