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

Technologie NAT traversal

NAT Traversal Technology

2017 Bc. Daniel Boháč

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

Zadání diplomové práce

Student: **Bc. Daniel Boháč**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T059 Mobilní technologie

Téma: Technologie NAT traversal
NAT Traversal Technology

Jazyk vypracování: čeština

Zásady pro vypracování:

Cílem diplomové práce je návrh, realizace a testování sítě využívající technologii NAT traversal v laboratorním prostředí s využitím směrovačů Huawei a Cisco.

Osnova práce:
1. Popište různé způsoby vyžití technologie NAT traversal se zaměřením na její použití ve virtuálních privátních sítích.
2. Navrhněte a v laboratorních podmínkách realizujte alespoň tři druhy sítí VPN za současného použití technologie NAT traversal. Sítě sestavte pomocí směrovačů Huawei a Cisco. Ověřte funkčnost navržených řešení.
3. Ověřte kompatibilitu směrovačů Huawei a Cisco v těchto sítích.

Seznam doporučené odborné literatury:

[1] CARMOUCHE, James Henry. *IPsec Virtual Private Network Fundamentals.* Indianapolis: Cisco Press, 2006. ISBN 1-58705-207-5.
[2] Dokumentace k směrovačům Huawei a Cisco.

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: 28.04.2017

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

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA Fakulta elektrotechniky a informatiky ID16 OSTRAVA

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

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

V Ostravě 26. dubna 2017

.....

Velmi rád bych poděkoval vedoucímu své diplomové práce, panu Ing. Petru Machníkovi, Ph.D. za odbornou pomoc a cenné rady při tvorbě této práce.

Abstrakt

V současnosti dochází společně s rozvojem Internetu také k nedostatku veřejných IP adres, které jsou využívány jako jedinečný identifikátor zařízení v počítačových sítích. Z tohoto důvodu byla iniciována snaha tento problém řešit. Jedním z možných řešení je využití překladu adres, označovaného jako NAT. S rozvojem Internetu a moderních počítačových sítí vznikla také potřeba pro bezpečné propojení jednotlivých sítí a bezpečné připojení vzdáleného uživatele do sítě. K tomuto účelu lze využít technologii VPN. Teoretická část této práce se proto zabývá technologiemi NAT, VPN a také mechanismy řešícími problémy, které NAT způsobuje.

Cílem praktické části této práce je konfigurace VPN technologií v síti využívající překlad adres. Záměrně byly vybrány VPN technologie, na které má překlad adres negativní vliv a je tedy nutné aplikovat metody řešící vzniklé potíže. Testované topologie jsou sestaveny ze směrovačů značky Cisco a Huawei. Je tedy také ověřena kompatibilita mezi zařízeními obou výrobců, aby bylo umožněno jejich bezproblémové nasazení v praxi.

Klíčová slova: Cisco, DMVPN, DSVPN, Huawei, IPSec, L2TP, NAT, NAT-T, PAT, PPTP, VPN

Abstract

Nowadays, in connection with the growth of the Internet, there is also a shortage of public IP addresses, which are used as unique identifiers of the devices in a computer network. For this reason, an effort has been initiated to address this problem. One possible solution is the use of network address translation, known as NAT. With the developing Internet and modern computer networks, demand for secure interconnection of individual networks and secure connection for the remote users raised. For this purpose, VPN technology can be used. The theoretical part of this thesis, therefore, deals with NAT, VPN technology and mechanisms that deal with problems caused by NAT.

The practical part of the thesis aims to the configuration of the VPN technologies in a network that uses NAT. VPN technologies which are negatively affected by network address translation has been intentionally chosen so it is necessary to apply the methods solving the arisen problems. Tested topologies are composed of Cisco and Huawei routers. Therefore, also compatibility between the devices of both manufacturers has been tested to enable their easy usage in practice.

Key Words: Cisco, DMVPN, DSVPN, Huawei, IPSec, L2TP, NAT, NAT-T, PAT, PPTP, VPN

Obsah

Seznam použitých zkratek a symbolů

AAA	–	Authentication, Authorization and Accounting
AH	–	Authentication Header
BDR	–	Backup Designated Router
CIE	–	Client Information Entry
DES	–	Data Encryption Standard
DMVPN	–	Dynamic Multipoint VPN
DPD	–	Dead Peer Detection
DR	–	Designated Router
DSVPN	–	Dynamic Smart VPN
EAP	–	Extensible Authentication Protocol
ESP	–	Encapsulating Security Payload
FTP	–	File Transfer Protocol
GRE	–	Generic Routing Encapsulation
HMAC	–	Keyed-Hash Message Authentication Code
HTTP	–	Hypertext Transfer Protocol
CHAP	–	Challenge-Handshake Authentication Protocol
IANA	–	Internet Assigned Numbers Authority
ICMP	–	Internet Control Message Protocol
ID	–	Identification
IKE	–	Internet Key Exchange
IOS	–	Internetwork Operating System
IP	–	Internet Protocol
IPCP	–	Internet Protocol Control Protocol
IPSec	–	Internet Protocol Security
IPX	–	Internetwork Packet eXchange
ISAKMP	–	Internet Security Association and Key Management Protocol
ISO	–	International Standards Organization
ISP	–	Internet Service Provider
L2F	–	Layer 2 Forwarding Protocol
L2TP	–	Layer 2 Tunneling Protocol
LAC	–	L2TP Access Concentrator
LAN	–	Local Area Network
LAS	–	L2TP Access Server
LNS	–	L2TP Network Server
mGRE	–	Multipoint GRE
MOBIKE	–	Mobile IKE

MTU	–	Maximum Transmission Unit
NAS	–	Network Access Server
NAT	–	Network Address Translation
NAT-D	–	Network Address Translation Discovery
NAT-T	–	Network Address Translation Traversal
NBMA	–	Non-Broadcast Multiple-Access
NHRP	–	Next Hop Resolution Protocol
OS	–	Operating System
OSI	–	Open System Interconnection
OSPF	–	Open Shortest Path First
PAP	–	Password Authentication Protocol
PAT	–	Port Address Translation
PEAP	–	Protected Extensible Authentication Protocol
PPP	–	Point-to-Point Protocol
PPPoE	–	Point-to-Point Protocol over Ethernet
PPTP	–	Point-to-Point Tunneling Protocol
RFC	–	Request For Comment
RTT	–	Round-Trip Time
SA	–	Security Associations
SADB	–	Security Association Database
SHA	–	Secure Hash Algorithm
SIP	–	Session Initiation Protocol
SPI	–	Security Parameter Index
TCP	–	Transmission Control Protocol
TLS	–	Transport Layer Security
TTL	–	Time To Live
UDP	–	User Datagram Protocol
VPDN	–	Virtual Private Dialup Network
VPN	–	Virtual Private Network
VRP	–	Versatile Routing Platform

Seznam obrázků

Seznam tabulek

1 Úvod

Se zvyšující se dostupností připojení k Internetu se jeho využívání stalo nedílnou součástí života značného množství uživatelů na Zemi. S rostoucím počtem uživatelů Internetu ovšem nastal problém nedostatku veřejných IP (Internet Protocol) adres. Za účelem eliminace tohoto problému existuje více řešení, jedním z nich je využití překladu adres označovaného jako NAT (Network Address Translation). V kapitole č. 2 jsou proto popsány vlastnosti technologie NAT, rozdělení této technologie a také znázorněn princip její funkce.

V současnosti prakticky každá větší organizace využívá pro svou činnost informační systémy, nebo jiné informační technologie, které značně zvyšují efektivitu práce. Pro propojení jednotlivých technologických zařízení, jsou využívány počítačové sítě, které umožňují jejich vzájemnou komunikaci. Často je také potřeba, aby měl do těchto síti uživatel přístup i z jiných lokalit, než z kanceláře určité organizace. Tato situace nastává, pokud zaměstnanec společnosti pracuje z domova, nebo je na cestách, přičemž pro získání potřebných informací vyžaduje přístup do lokální sítě společnosti. Obdobná situace nastává, když se podnik rozrůstá a za účelem přístupu k informacím je třeba propojit jednotlivé vzdálené pobočky společnosti. V minulosti se k tomuto účelu využívaly např. pronajaté linky, které ovšem byly velmi nákladné. S rozvojem Internetu již není využívání pronajatých linek třeba, jelikož lze s využitím technologie VPN (Virtual Private Network) vytvořit bezpečnou virtuální privátní síť přes sdílenou infrastrukturu, jako je právě Internet. To umožňuje značné snížení nákladů, ale také řadu dalších výhod i nevýhod, které jsou popsány v kapitole č. 3. V této kapitole jsou také uvedeny základní principy funkce VPN, jejich rozdělení, bezpečnostní požadavky a také detailnější popis vybraných typů VPN.

Technologie NAT zamezuje některým protokolům, včetně těch umožňujících tvorbu VPN, v jejich správné funkci. Proto byly vytvořeny mechanismy, jak těmto protokolům umožnit funkci v síti využívající NAT. Tyto mechanismy jsou označovány jako NAT-T (NAT Traversal) a pojednává o nich kapitola č. 4.

Navazující kapitoly jsou věnovány praktické implementaci sítí využívajících technologii VPN a NAT. Implementace je zdokumentována a rovněž je ověřena funkčnost navržených řešení. Vzhledem k použití zařízení výrobce Cisco i Huawei v navržených topologiích, je také ověřena jejich vzájemná kompatibilita.

2 Překlad síťových adres

Technologie překladu síťových adres označována také jako NAT uskutečňuje proces přepisu zdrojových a cílových adres, případně také TCP (Transmission Control Protocol) / UDP (User Datagram Protocol) portů segmentů procházejících přes zařízení realizující NAT. Cílem této technologie je především zamezení vyčerpání IP adres. Toho je docíleno prostřednictvím sdílení určitého rozsahu veřejných IP adres vyšším počtem hostů s privátními adresami. Koncept je založen na skutečnosti, že každé zařízení odesílající data ze své LAN (Local Area Network) sítě do Internetu musí mít přiřazenu veřejnou IP adresu. Ovšem pro zamezení vyčerpání veřejných IP adres se v lokálních sítích standardně využívají privátní adresy, které jsou směrovatelné pouze v místní síti. V případě, kdy je potřeba odeslat data ze zařízení s privátní adresou do veřejné sítě, lze využít technologii NAT, která provede překlad privátní adresy na adresu veřejnou, čímž umožní komunikaci. Funkci NAT obvykle realizuje hraniční směrovač, nebo firewall.

2.1 Terminologie překladu adres

Organizace IANA (Internet Assigned Numbers Authority) vyčlenila určité rozsahy adres, které jsou určeny pro užití v privátní síti a nejsou globálně směrovatelné. Tyto adresy jsou označovány jako neregistrované a žádná společnost si nemůže nárokovat jejich vlastnictví. S využitím těchto adres není možná přímá komunikace se zařízeními z veřejné sítě, jako je např. Internet, jelikož směrovače ve veřejné síti jsou nakonfigurovány k zahazování všech paketů, obsahujících neregistrovanou IP adresu. Rozsahy privátních IPv4 adres jsou vyobrazeny v tabulce č. 2.1:

Tabulka 2.1: Rozsahy privátních IPv4 adres

Třída adres	**Rozsah adres**
A	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.255.255
C	192.168.0.0 - 192.168.255.255

Tyto adresy jsou v terminologii NAT označovány jako vnitřní adresy. Všechen datový provoz pocházející z těchto privátních adres, který směřuje do jiné veřejné sítě, mimo privátní rozsah adres, musí být přeložen na směrovatelnou adresu označovanou jako vnější adresa. Pojem vnější a vnitřní adresa je použit pro identifikaci polohy zařízení z hlediska překladu adres. Vnitřní adresy identifikují zařízení v rámci privátní sítě určité organizace, zatímco vnější adresy identifikují zařízení z hlediska vnější sítě.

Dále lze adresy rozdělit na globální a lokální. Po provedení překladu adres jsou adresy označovány jako globální. Naopak adresy použité před uskutečněním překladu jsou označovány jako lokální. Lokální adresy jsou tedy využívány v privátní síti organizace, zatímco globální adresy jsou využívány ve veřejné síti. Celkový přehled zmíněné terminologie je vyobrazen v tabulce č. 2.2.

Tabulka 2.2: Přehled terminologie NAT [1]

Název adresy	**Význam**
Vnitřní lokální	Vnitřní host před překladem adresy
Vnitřní globální	Vnitřní host po překladu adresy
Vnější lokální	Cílový host před překladem adresy
Vnější globální	Cílový host po překladu adresy

2.2 Využití překladu adres

Hlavním důvodem vzniku technologie NAT je snaha o zpomalení vyčerpávání adresního prostoru, který nabízí protokol IPv4. Toho je dosaženo umožněním reprezentace určitého počtu privátních IP adres menším počtem veřejných IP adres.

Překlad adres lze ale také využít při slučování dvou společností s duplicitními schématy interního adresování, nebo v případě změny ISP (Internet Service Provider), která by vyžadovala změnu interního adresování. S využitím technologie NAT je v takovém případě potřeba přečíslovat pouze veřejné IP adresy. Další výhodou je také zvýšená bezpečnost. Ta je způsobena skrytím struktury vnitřní sítě a identity hostů, jelikož je tato síť zvenčí reprezentována nižším počtem sdílených vnitřních globální adres. Tato skutečnost je ovšem i jednou z nevýhod, jelikož z ní také plyne nemožnost zahájení komunikace z vnější sítě se zařízením ve vnitřní síti, dokud není vytvořen záznam v NAT tabulce. Navíc NAT způsobuje zpoždění přenosu a snížení výkonu zařízení, uskutečňujícího překlad, jelikož kromě samotného překladu je potřeba rovněž opakovaně provést přepočet kontrolního součtu z důvodu změny paketu.

Další problém překladu adres je skutečnost, že některé protokoly odesílají i informace o síťové adrese a případně také o portu transportní vrstvy ISO (International Standards Organization) / OSI (Open System Interconnection) modelu. Mezi tyto protokoly patří např. FTP (File Transfer Protocol) a SIP (Session Initiation Protocol). V případě využití překladu adres dojde k odeslání nesprávné informace a bez použití technik NAT-T může dojít k selhání komunikace. Překlad adres činí problémy rovněž bezpečnostnímu protokolu IPSec (Internet Protocol Security). Protokol AH (Authentication Header) i ESP (Encapsulating Security Payload) využívají kontrolu integrity dat. Pokud NAT změní data v IP záhlaví a případně také port TCP/UDP protokolu, dojde k porušení integrity dat a narušení správné funkce protokolu. S využitím technik NAT traversal a protokolu ESP je ovšem možné IPSec VPN v síti využívající NAT sestavit.

2.3 Typy překladů adres

Techniky překladu síťových adres lze podle principu jejich funkce rozdělit do tří základních kategorií [1]:

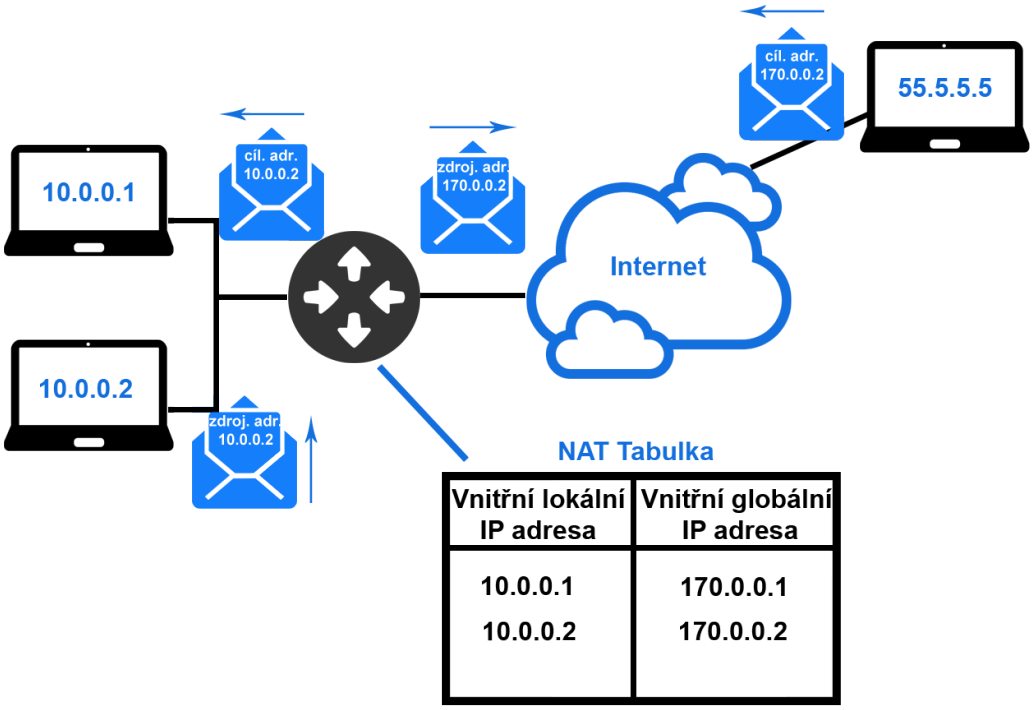
- **Statický NAT** – Nejjednodušší kategorie překladu adres. Poskytuje asociaci adres 1 : 1 mezi neregistrovanou a registrovanou adresou z čehož vyplývá, že každý host v síti musí mít vyhrazenu jednu směrovatelnou IP adresu. Záznamy v překladové tabulce jsou u tohoto typu NAT vytvořeny okamžitě po konfiguraci asociací a zůstávají zde, dokud nejsou manuálně odstraněny.

- **Dynamický NAT** – Umožňuje asociaci M : N mezi neregistrovanými a registrovanými adresami ze specifikovaného rozsahu. Asociace je ovšem na rozdíl od statického typu NAT uskutečňována dynamicky na základě předkonfigurovaných kritérií definujících, které konkrétní IP adresy budou překládány. Záznamy v překladové tabulce jsou vytvářeny až v případě, kdy je komunikace vyžaduje. Tyto záznamy jsou zachovány po dobu komunikace. Po ukončení komunikace je nastaven časovač, po jehož vypršení dojde k vymazání záznamu z překladové tabulky.

- **PAT (Port Address Translation)** – Varianta překladu adres, která je často také označována jako „přetížení NAT“, jelikož umožnuje asociaci několika neregistrovaných IP adres na jedinou registrovanou IP adresu, tzn. umožnuje asociaci 1 : N. Jedná se o určitou variantu dynamického překladu adres, která využívá k překladu kromě IP adres také porty. S využitím jediné registrované IP adresy tak lze umožnit komunikaci s vnější sítí, teoreticky až 65536 uživatelům. V praxi ovšem bude maximální možný počet položek v překladové tabulce omezen s ohledem na systémové zásady, množství volných portů, či velikost operační paměti zařízení, které překlad adres uskutečňuje [1]. Existuje také statická varianta PAT, která funguje obdobně jako statický NAT s tím rozdílem, že v rámci překladu umožňuje specifikovat také porty transportního protokolu. Tím je umožněno vytvoření několika statických záznamů se stejnou asociovanou adresou. Výše zmíněné techniky statického i dynamického překladu mají své výhody i nevýhody. Dynamický překlad je obvykle využíván pro běžné klienty, kteří nepotřebují permanentně přidělenou veřejnou IP adresu, ale mohou ji sdílet, což je ekonomicky výhodnější. Naopak statický NAT je vhodný pro zařízení, která vyžadují, aby byla z vnější sítě vždy dostupná pod stejnou veřejnou adresou. Statický překlad rovněž umožňuje bezproblémové započetí komunikace z vnější sítě. Nevýhodou je ovšem potřeba manuální konfigurace asociací a potřeba trvalého vyhrazení dané IP adresy.

2.4 Princip funkce

Praktický příklad funkce mechanismu NAT je zobrazen na obrázku č. 2.1.



Obrázek 2.1: Princip funkce NAT

V tomto příkladu je odeslán paket od hosta s IP adresou 10.0.0.2 mimo vnitřní síť a paket prochází přes hraniční směrovač, který uskutečňuje překlad adres. Směrovač rozpozná, že se jedná o vnitřní lokální IP adresu, ze které jsou odeslány data do vnější sítě. Adresa je proto na směrovači přeložena na vnitřní globální adresu a záznam o tomto překladu je uložen do NAT tabulky. Následně je paket obsahující přeloženou zdrojovou adresu odeslán na vnější rozhraní směrovače. Externí host pak odešle odpověď na vnitřní globální adresu cílového hosta a směrovač prostřednictvím NAT tabulky provede překlad z vnitřní globální adresy na adresu vnitřní lokální. Poté je paket odeslán na výstupní rozhraní.

V případě využití přetížení PAT se princip funkce mírně liší, jelikož IP adresy všech vnitřních hostů se mohou překládat na jedinou vnitřní globální IP adresu. Z tohoto důvodu jsou v NAT tabulce obsaženy také čísla portů, jejichž prostřednictvím je umožněno rozlišení více hostů využívajících stejnou globální IP adresu.

3 Virtuální privátní síť

Síťová technologie VPN umožňuje vytvoření bezpečného spojení přes veřejnou infrastrukturu, nebo přes privátní infrastrukturu vlastněnou jinou organizací. S využitím VPN je možné zajistit, aby veškerý datový provoz procházel přes zabezpečený virtuální tunel, na který jsou aplikovány bezpečnostní mechanismy za účelem zabezpečení spojení k privátní síti a k ochraně identity uživatelů.

Vzhledem k tomu, že VPN umožňuje využití veřejné infrastruktury, jsou virtuální privátní sítě cenově výhodné a odpadá tak potřeba vlastních, nebo pronajatých linek, které jsou pro menší organizace cenově nedostupné. Typicky lze VPN využít pro bezpečné připojení vzdálených uživatelů do firemní sítě nebo propojení několika geograficky oddělených poboček společnosti prostřednictvím Internetu a tak sjednotit jednotlivé sítě dohromady.

3.1 Zabezpečení virtuálních privátních sítí

Zajištění bezpečnosti dat je hlavním cílem této technologie, a proto dobře navržené VPN poskytují[2, 4]:

- **Důvěrnost dat** – Důvěrnost znamená, že k citlivým údajům mají přístup pouze autorizovaní uživatelé. Vzhledem k tomu, že jsou soukromá data přenášena přes veřejnou síť, je důvěrnost dat klíčová a může být dosažena prostřednictvím šifrování dat.

- **Integrita dat** – Zajištění správnosti a konzistence přenášených dat. Data jsou při přenosu chráněna proti neautorizované modifikaci, ale také proti následkům chybného spojení. Pokud dojde k porušení integrity dat, musí být tato skutečnost detekována. Za účelem zajištění integrity dat jsou využívány hašovací funkce a opravné či detekční kódy.

- **Autentizace původu dat** – Ověření, zda data pocházejí od určitého subjektu. Toto ověření je důležité pro zajištění ochrany před útoky využívajícími tzv. spoofing. K tomuto ověření se využívá např. digitální podpis.

- **Anti-Replay** – Ověřuje, zda je každý paket unikátní a není duplikován. Cílem je zamezit útočníkům zachycení paketů a následné vložení modifikovaných paketů do datového toku mezi zdrojem a cílem. Toho je docíleno prostřednictvím sekvenčních čísel, které se inkrementují při každé odeslané zprávě. Pokud cílové zařízení obdrží zprávu s nižším sekvenčním číslem, než je očekáváno, jsou pakety zahozeny.

- **Tunelování toku dat** – Tunelování je proces zapouzdřování celého paketu do paketu jiného a odeslání jej přes síť. Tunelování je užitečné v případech, kdy je žádoucí, aby byla utajena identita zařízení, ze kterého datový provoz pochází. V případě odeslání dat zařízením, využívající např. protokol IPSec, je k původním datům přidáno další záhlaví. Zašifrováním původních paketů včetně jejich originálního záhlaví je pak skryt skutečný zdroj dat. Pouze

důvěryhodný partner je schopen určit skutečný zdroj dat poté, co oddělí přidané záhlaví od paketu a dešifruje původní záhlaví. Tunelování však samo o sobě neposkytuje bezpečnost dat. Původní paket je pouze zapouzdřen do jiného paketu a pokud není zašifrován, může jej kdokoli odchytit a analyzovat[2].

- **AAA** – Zkratka vyjadřující autentizaci, autorizaci a účtování (authentication, authorization, accounting). Tyto operace jsou využívány pro zajištění vyšší úrovně bezpečnosti přístupu v prostředí VPN pro vzdálený přístup a mohou být zajištěny zařízením poskytujícím funkci VPN, nebo prostřednictvím externího AAA serveru.
  - Autentizace – Proces ověření platné identity uživatele síťových služeb. Autentizace je dosažena prostřednictvím představení identity a určitého pověření, kterým je obvykle heslo.
  - Autorizace – Proces udělování souhlasu s provedením určité operace uživateli na základě autentizace. Výsledkem tohoto procesu je udělení souhlasu k provedení operace, nebo odmítnutí požadavku.
  - Účtování – Monitorování a sběr informací o využívání síťových služeb uživatelem. Získané informace lze využít např. za účelem správy, účtování nebo plánování.
- **Nepopiratelnost** – Tato služba zajišťuje, aby mohl příjemce prokázat přijetí zprávy od komunikačního partnera a tím také zamezit případnému popření odeslání této zprávy jejím odesílatelem. Z tohoto důvodu je nepopiratelnost velmi žádoucí např. v oblasti finančních transakcí. Za účelem dosažení nepopiratelnosti se využívá digitálních certifikátů, které se připojují k odeslaným zprávám.

3.2 Klady a zápory VPN

Využití technologie VPN znamená pro řadu organizací značný přínos, jelikož jim umožňuje vytvoření virtuální privátní sítě nad sdílenou infrastrukturou, což znamená snížení finančních nákladů, jelikož již není třeba využívat nákladné vyhrazené linky. Další nespornou výhodou je krátká doba vytvoření takovéto virtuální sítě, jelikož využívaná sdílená infrastruktura již existuje a není třeba ji budovat jako je tomu u privátních linek vlastněných samotnou organizací. Navíc je tato sdílená infrastruktura pod správou ISP, který je za její funkčnost odpovědný. Virtuální privátní sítě také zajišťují vysokou úroveň bezpečnosti prostřednictvím metod popsaných v kapitole 3.1 a rovněž poskytují vysokou úroveň rozšiřitelnosti a flexibility, protože je tato virtuální topologie definována pouze na základě konfigurace.

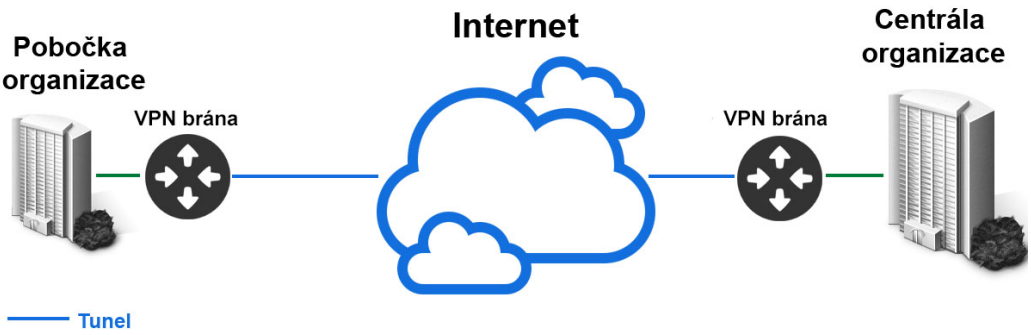
Technologie VPN má ovšem také své stinné stránky. Návrh a implementace VPN může být velmi komplexní záležitostí, a proto je potřeba profesionála s odbornými znalostmi z oblasti počítačových sítí, síťové bezpečnosti a VPN technologií. Spolehlivost, propustnost a jiné parametry části sítě využívající VPN nejsou pod kontrolou organizace, ale závisí na poskytovateli internetového připojení, navíc některé VPN produkty různých dodavatelů nejsou vzájemně

kompatibilní, a proto jejich kombinace může způsobovat technické potíže. Další nevýhodou je skutečnost, že šifrování znamená zátěž na výkon bezpečnostní brány, jelikož je třeba provádět matematicky náročné výpočty. Vzhledem k tomu, že se v rámci této technologie využívá rovněž princip tunelování, znamená to také vyšší režii z důvodu přenosu dodatečných dat v přídavném záhlaví. V případě, kdy velikost paketů přesáhne MTU (Maximum Transmission Unit), dojde navíc k potřebě fragmentace těchto paketů, čímž se negativně ovlivní výkon sítě. Dalším problémem je technologie NAT, která může narušit správnou funkci VPN.

3.3 Rozdělení VPN

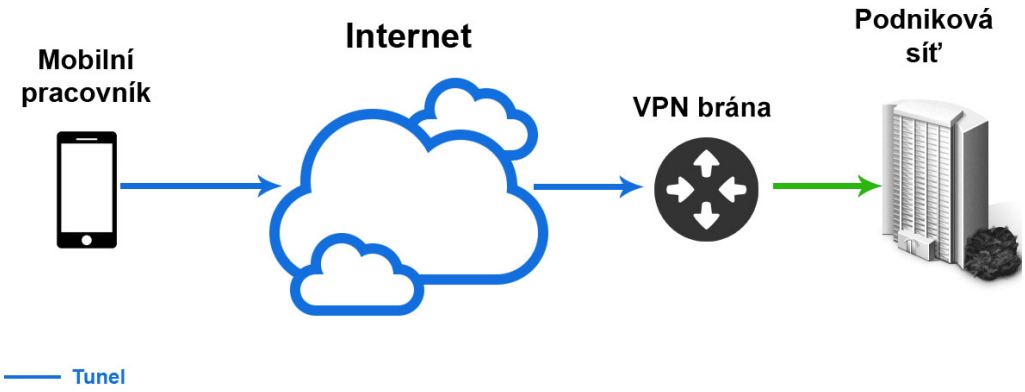
Sítě VPN lze rozdělit na dva základní typy [3]:

- **VPN mezi lokalitami (Site-to-Site)** – Jedná se o typ VPN sloužící ke vzájemnému propojení celých sítí prostřednictvím veřejné infrastruktury. Příkladem může být propojení sítě určité pobočky organizace s centrálou, viz obr. č. 3.1. Uživatelé v tomto případě nepotřebují klientský VPN software, ale jednoduše přijímají a odesílají datový provoz skrz VPN bránu. Jako VPN brána pak může sloužit např. směrovač, firewall, nebo VPN koncentrátor. Daná VPN brána zajišťuje zapouzdřování a šifrování odchozího síťového provozu a odesílání tohoto provozu skrz VPN tunel na VPN bránu v cílové destinaci. Při přijetí dat VPN brána oddělí záhlaví paketu, dešifruje obsah a odešle paket cílovému hostu v privátní síti [2].



Obrázek 3.1: Site-to-Site VPN

- **VPN pro vzdálený přístup (Remote-Access)** – Jedná se o spojení typu uživatel-síť, které umožňuje bezpečné spojení jednotlivých hostů s privátní sítí organizace prostřednictvím veřejné sítě, kterou obvykle představuje Internet. Z tohoto důvodu je tento typ VPN využíván zejména organizacemi, jejichž zaměstnanci pracují z domova, nebo vyžadují připojení k privátní síti, když se nachází mimo prostory organizace. V remote-access VPN má typicky každý uživatel klientský VPN software, který uskutečňuje zapouzdření a šifrování dat. Na straně VPN brány jsou pak opět odděleny záhlaví paketů, obsah dešifrován a odeslán cílovému uživateli. Princip remote-access VPN je zobrazen na obr. č. 3.2.



Obrázek 3.2: Remote-Access VPN

VPN lze dále klasifikovat podle mnoha kritérií, mezi které patří zejména:

- Protokol použitý pro tunelování datového provozu.
- Umístění koncového bodu tunelu.
- Vrstva ISO/OSI modelu, na které daná VPN funguje.
- Poskytovaná úroveň bezpečnosti.

V rámci této práce jsou popsány následující VPN technologie, které jsou rovněž konfigurovány v praktické části práce:

- IPSec VPN.
- GRE (Generic Routing Encapsulation) over IPSec VPN.
- DMVPN (Dynamic Multipoint VPN) zabezpečena technologií IPSec.
- L2TP (Layer 2 Tunneling Protocol) over IPSec VPN.
- PPTP (Point-to-Point Tunneling Protocol) VPN.
- IPSec IKEv2 VPN.

Jedná se tedy převážně o kombinace různých VPN technologií společně s technologií IPSec pro zajištění bezpečnosti. Tato kombinace je použita také proto, že IPSec VPN je v současnosti převládající VPN technologie, jež je negativně ovlivněna překladem adres. Ten je v této práci použit pro testování technologie NAT-T.

3.4 Internet Protocol Security

Jedná se o sadu protokolů. Jejich hlavním účelem je zabezpečení dat přenášených prostřednictvím sítí založených na IP protokolu. IPSec se řadí mezi protokoly síťové vrsty ISO/OSI modelu. Není svázán se specifickými šiframi, metodami autentizace nebo jinými bezpečnostními technologiemi. Z tohoto důvodů umožňuje, aby byly nové algoritmy implementovány bez potřeby změn IPSec standardu. IPSec zabezpečuje spojení mezi dvěma VPN bránami, dvěma hosty, nebo mezi bránou a hostem. Poskytovány jsou následující bezpečnostní funkce:

- **Důvěrnost** – Zajištěno algoritmy šifrujícími data (DES, 3DES, AES, RSA, SEAL ...).
- **Integrita** – Využití hašovacích algoritmů – obvykle HMAC-MD5, nebo HMAC-SHA-1.
- **Autentizace** – IPSec k tomuto účelu využívá metodu výměny klíčů IKE (Internet Key Exchange).
- **Anti-Replay** – Dosaženo prostřednictvím porovnání sekvenčních čísel přijatých paketů v tzv. klouzavém okně.

Velkou výhodou protokolu IPSec je jeho implementace na síťové vrstvě ISO/OSI modelu. Z tohoto důvodu lze prostřednictvím tohoto protokolu zabezpečit prakticky všechen provoz nezávisle na protokolech vyšších vrstev ISO/OSI modelu a rovněž může být použit se všemi standardními protokoly druhé vrstvy ISO/OSI modelu, jedná se tedy o velice univerzální protokol.

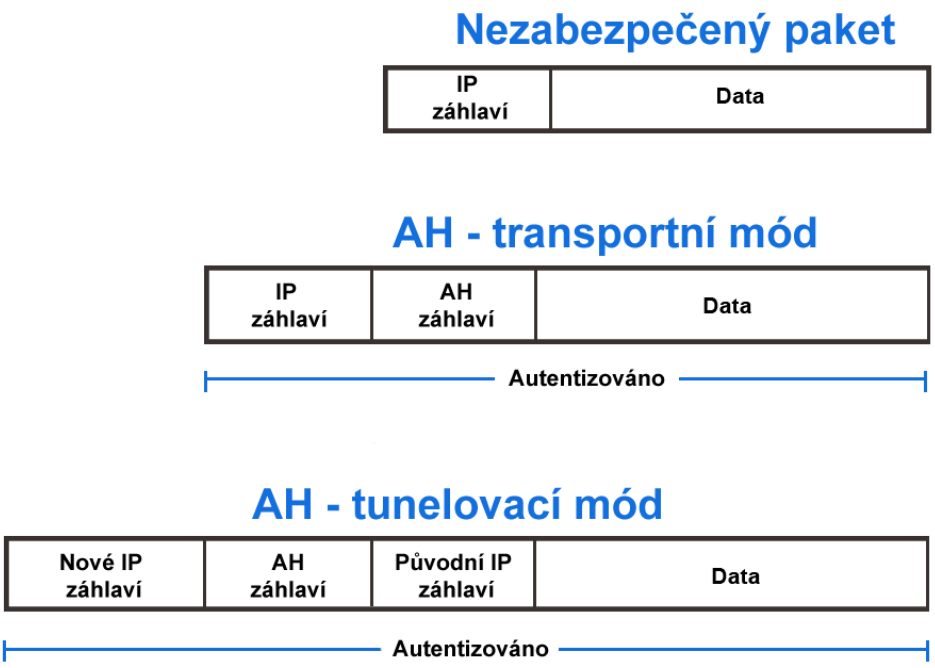
Pro svou funkci IPSec využívá dva základní protokoly:

- **AH** – Poskytuje autentizaci a integritu dat, ale neumožňuje šifrování paketů. Integrita je dosažena využitím jednosměrné hašovací funkce. Výsledný haš je zkombinován s obsahem zprávy a odeslán. Příjemce pak může odhalit případné změny provedením totožné hašovací funkce na přijatém paketu a porovnáním hašů. Vzhledem k tomu, že je v hašovací funkci rovněž zahrnuto využití sdíleného klíče, je zajištěna autentizace. Funkcionalita AH je aplikována na celý datagram, kromě polí v IP hlavičce, které se modifikují při přenosu. Proces zapouzdření dat s využitím AH je ilustrován na obrázku č. 3.3. Jelikož AH zabezpečuje IP paket včetně jeho záhlaví, je tento mechanismus nekompatibilní s technologií NAT, která modifikuje IP záhlaví. To má za následek vytvoření nesouhlasného výsledku hašovací funkce a zahození paketu.

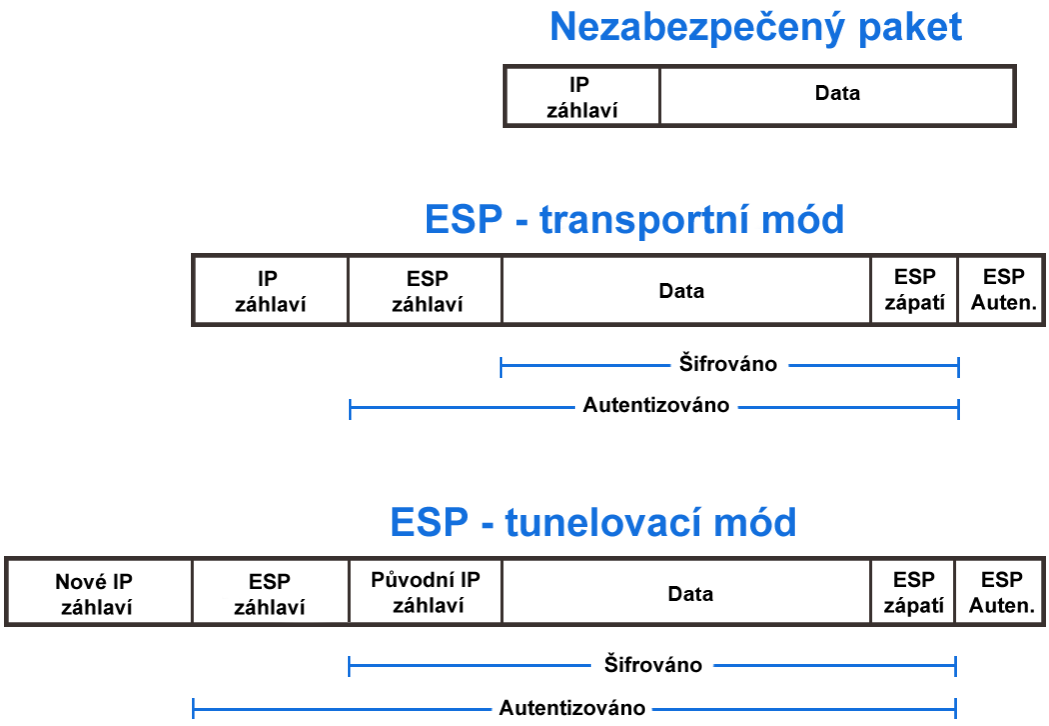
- **ESP** – Poskytuje důvěrnost, autentizaci zdroje i kontrolu integrity. Nejprve jsou užitečná data uvnitř paketu šifrována, poté je na tyto data aplikován hašovací algoritmus – obvykle HMAC-MD5, nebo HMAC-SHA-1. Prostřednictvím haše je ověřena integrita a autentizace zdroje dat. Volitelně je možná také anti-replay ochrana. Původní data jsou mechanismem ESP dobře chráněna, jelikož při použití tunelovacího módu je zašifrován celý originální paket, k němuž je přidáno ESP záhlaví i zápatí. V hašovacím procesu je zahrnut šifrovaný paket, a také ESP záhlaví se zápatím. Nakonec je na začátek těchto dat vloženo nové IP záhlaví, na základě kterého je paket směrován sítí. Proces zapouzdření dat prostřednictvím ESP je znázorněn na obr. č. 3.4.

Protokol ESP lze dále provozovat ve dvou odlišných módech:

- **Transportní mód** – V tomto módu je bezpečnost zajišťována od transportní vrstvy výše. Užitečná data jsou uvnitř paketu chráněna, ale původní IP záhlaví je ponecháno nezabezpečeno a použito ke směrování.
- **Tunelovací mód** – Zajišťuje ochranu nad celým původním paketem, který je zašifrován, a poté zapouzdřen do dalšího paketu.



Obrázek 3.3: Struktura zapouzdření dat v AH módu



Obrázek 3.4: Struktura zapouzdření dat v ESP módu

3.4.1 Protokol Internet Key Exchange

Za účelem autentizace a generování šifrovacích klíčů se v rámci IPSec využívá protokol IKE. Ten vyjednává tzv. security associations (SA), prostřednictvím kterých si účastníci vyměňují parametry potřebné pro sestavení spojení. Bezpečnostní asociace (SA) jsou uchovávány v databází SADB (Security Association DataBase) společně s indexy SPI (Security Parameter Index), které slouží k identifikaci položek v databázi. V rámci IPSec je protokol IKE využíván k vyjednávání SA, generování klíčů a také k jejich obnově. Praktický princip funkce je rozdělen do dvou následujících fází:

- **IKE fáze č. 1** - V průběhu této fáze dochází k autentizaci a vyjednání parametrů pro vytvoření zabezpečeného spojení, které je následně použito pro druhou IKE fázi. Součástí vyjednávaných parametrů jsou např. algoritmy použité pro šifrování, autentizaci a kontrolu integrity dat. IKE SA sestavené v první IKE fázi lze považovat za řídící kanál, přes který nejsou posílána uživatelská data. Vytvořené IKE SA je na rozdíl od později popisovaného IPSec SA obousměrné.
- **IKE fáze č. 2** - Druhá fáze využívá zabezpečeného kanálu vzniklém v první fázi za účelem vytvoření IPSec SA. Po vytvoření IPSec SA je tato bezpečnostní asociace využita pro zabezpečení uživatelských dat.

Protokol IKEv1 využívá pro účely první fáze jeden ze dvou režimů. Těmi jsou hlavní a agresivní režim. Pro vyjednání druhé fáze existuje již pouze jeden režim označován jako rychlý režim. Při použití hlavního režimu je mezi účastníky vyměněno celkem šest zpráv ve třech párech [8]:

- První pár obsahuje bezpečnostní pravidla nastavená na daném zařízení. Iniciátor odešle podporované bezpečnostní pravidla a algoritmy. Z těch si následně odpovídající strana vybere a specifikuje vybraná pravidla v odpovědi.
- Druhý pár slouží pro Diffie-Hellmanovu metodu výměny veřejného klíče. Skupina Diffie-Hellmanova algoritmu již byla vyjednána v prvním páru zpráv.
- Třetí pár je použit pro ISAKMP (Internet Security Association and Key Management Protocol) autentizaci. Každý účastník je autentizován a jeho identita validována prostřednictvím sdíleného klíče nebo digitálního certifikátu. Tyto a všechny následující pakety již jsou šifrovány a autentizovány.

V případě použití agresivního režimu dochází k výměně pouze tří zpráv. Jedná se tedy o rychlejší režim, ve kterém však není zabezpečena přenášená identita účastníků [8]:

- Nejprve iniciátor odešle informace pro účely Diffie-Hellmanova algoritmu včetně kódových slov (nonces). Dále informace o identitě, IKEv1 pravidlech a algoritmech.
- Odpovídající strana daný paket autentizuje a odešle odpověď obsahující vybraná pravidla, kódová slova, informace potřebné pro vytvoření klíče a identifikaci.
- Iniciátor spojení autentizuje přijatý paket a odešle autentizační haš.

V posledním režimu, označovaném jako rychlý režim, jsou vyjednávány následující parametry:

- Autentizační algoritmus.
- Šifrovací algoritmus.
- Protokol AH nebo ESP.
- Tunelovací nebo transportní mód.
- Doba trvání IPSec SA.

Následně již dochází k zabezpečené výměně dat prostřednictvím protokolové sady IPSec.

Protokol IKEv1 z počátku nepodporoval rozšíření, mezi které spadá např. v této práci využívaný NAT-T. To vedlo různé výrobce k implementaci vlastních řešení, přestože později byla standardizována různá IKEv1 rozšíření. Protokol IKEv2 vznikl za účelem zjednodušení a sjednocení procesu protokolu IKEv1. Také došlo k integraci různých rozšíření a nových vlastností do

standardu protokolu IKEv2. Mezi ně patří např. NAT-T, DPD (Dead Peer Detection), MOBIKE (Mobile IKE) a EAP (Extensible Authentication Protocol) autentizace. Přestože obě verze protokolu využívají UDP zapouzdření s portem 500 a formát záhlaví je podobný, nejsou tyto verze kompatibilní.

Protokol IKEv2 zjednodušuje výměnu zpráv v průběhu první a druhé fáze sestavení VPN. V rámci protokolu IKEv1 je k sestavení VPN potřeba přenést šest zpráv v hlavním režimu první fáze a následně další tři zprávy v rychlém režimu pro druhou fázi tunelu. V případě použití agresivního režimu je počet zpráv v první fázi snížen na tři. Je tedy potřeba přenést devět, nebo šest zpráv. Při použití protokolu IKEv2 je potřeba přenést pouze čtyři zprávy. První fáze je v rámci tohoto protokolu pojmenována IKE_SA_INIT a druhá IKE_AUTH [8].

V první fázi jsou vyjednány bezpečnostní parametry včetně protokolu pro šifrování a ověření integrity dat, Diffie-Hellmanovy skupiny a náhodná čísla. Také je v této fázi vygenerována hodnota SKEYSEED, ze které jsou vytvářeny všechny budoucí klíče. Následující zprávy jsou již autentizovány a šifrovány [8].

Druhá fáze využívá IKE SA vytvořené v první fázi a zajišťuje ověření identity ostatních VPN brán nebo klientů a vyjednává protokoly pro účely šifrování, autentizace a ověření integrity, aby mohlo dojít k sestavení CHILD SA pro použití protokolem ESP a AH. Termín CHILD SA je analogií pro IPSec SA z protokolu IKEv1 [8].

3.5 Generic Routing Encapsulation

Protokol GRE je specifikován v RFC2784 a RFC2890 jako protokol umožňující zapouzdření libovolného protokolu jiným protokolem síťové vrstvy ISO/OSI modelu [9]. V případě, kdy je potřeba zapouzdřit a přenést určitý paket, je tento paket nejprve zapouzdřen protokolem GRE. Vytvořený GRE paket je pak možné zapouzdřit do jiného protokolu a následně jej přes vytvořený tunel směrovat k cílovému zařízení. Vnější protokol, který je použit pro zapouzdření GRE paketu a přenos mezi oběma konci tunelu je označován jako transportní či doručovací (delivery) protokol. Síťová zařízení, která se nacházejí v cestě mezi oběma konci GRE tunelu neanalyzují původní paket, ale pouze vzniklý vnější IP paket transportního protokolu. Jakmile je tato datová struktura doručena na zařízení, které zakončuje GRE tunel, dojde k odstranění GRE zapouzdření a původní paket je následně směrován ke svému původnímu cíli. Adresní prostor mezi vnějším a původním vnitřním protokolem je tedy oddělen a dochází zde k jakési simulaci privátní sítě. Graficky znázorněný princip zmíněného zapouzdření lze vidět na obr č. 3.5.

Obrázek 3.5: Struktura GRE zapouzdření

Přestože protokol GRE nezajišťuje bezpečnost dat např. prostřednictvím šifrování jako je tomu u IPSec VPN, jedná se o technologii, která má mnoho výhod a využití, mezi které patří:

- Přenos různých protokolů přes páteřní síť, která je nepodporuje.
- Alternativní řešení pro sítě, které mají problém s omezeným počtem skoků.
- Ve spojení s technologií PPTP je umožněna tvorba VPN.
- Přenos vícesměrového vysílání v IPSec VPN sítích, které jinak umožňují pouze přenos komunikace typu unicast.
- Nízká náročnost z hlediska využitých prostředků oproti alternativním VPN technologiím.

3.6 Dynamic Multipoint VPN

V terminologii Huawei je tato technologie nazývána DSVPN (Dynamic Smart Virtual Private Network). Jedná se o koncept založený na topologii typu hub-and-spoke. Z názvu plyne skutečnost, že se v topologii využívá terminologie pro dva specifické typy uzlů:

- **Hub** – Jedná se o zařízení, které obvykle reprezentuje centrálu či hlavní pobočku společnosti. Uzly typu spoke se v případě konceptu DMVPN k této centrále registrují protokolem NHRP (Next Hop Resolution Protocol) a v případě konceptu hub-and-spoke je přes tento uzel směrována veškerá zabezpečená komunikace mezi uzly typu spoke.
- **Spoke** – Tento typ uzlu představuje pobočku, která využívá služeb uzlu typu hub pro komunikaci s ostatními pobočkami.

Původní topologie hub-and-spoke využívá statických tunelů vytvořených mezi centrálou a uzly typu spoke, které představují pobočky. V případě potřeby přidání nového uzlu typu spoke je vyžadován zásah do konfigurace tohoto uzlu a také do konfigurace centrály. Navíc je veškerá komunikace mezi pobočkami směrována přes tunel na centrálu, kde je tunel zakončen a následně je komunikace směrována přes další tunel na druhou pobočku.

Technologie DMVPN tento koncept vylepšuje s využitím rozhraní mGRE (multipoint GRE) umožňující komunikaci typu bod - více bodů. V případě využití původního hub and spoke konceptu by bylo na hub směrovači nutné vytvořit tunelové rozhraní pro každé spojení s uzlem typu spoke. V případě DMVPN je možné pro všechna tato spojení využít jedno mGRE rozhraní. Navíc není nutné veškerý přenos mezi pobočkami směrovat přes centrální směrovač. Prostřednictvím protokolu NHRP mohou spoke uzly zjistit asociaci mezi logickou IP adresou tunelu a skutečnou IP adresou, čímž je umožněno následné navázání VPN přímo mezi pobočkami bez potřeby centrálního směrovače jako prostředníka.

Ke své funkci DMVPN využívá následujících protokolů:

- Dynamický směrovací protokol.
- GRE nebo mGRE.
- Protokol NHRP.
- Volitelně pro účely zabezpečení také IPsec.

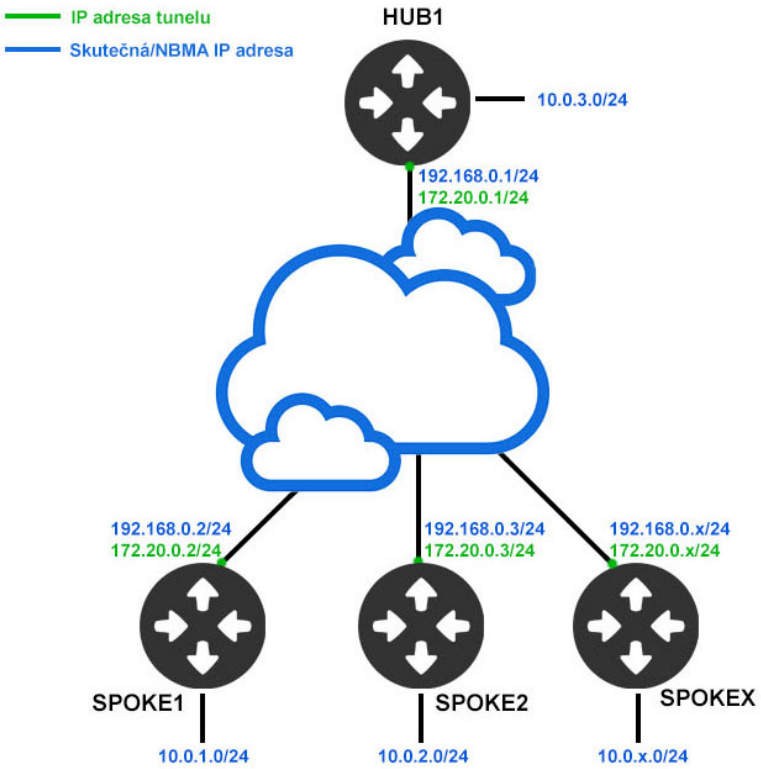
3.6.1 Výhody DMPVN

Technologie DMVPN poskytuje mimo jiné následující výhody a funkce [10]:

- Umožnění přímé komunikace mezi uzly typu spoke, bez potřeby využití centrálního směrovače jako prostředníka. Tím je také eliminována potřeba využití dodatečných zdrojů na centrálním směrovači a sníženo zpoždění v síti.
- Podpora tvorby VPN s uzly, které mají dynamicky přidělovány IP adresy. To je umožněno použitím protokolu NHRP s jehož využitím je IP adresa uzlu typu spoke registrována na centrálním směrovači. Pouze uzel typu hub musí mít předělenou statickou adresu.
- Zjednodušené přidávání VPN uzlů typu spoke do topologie. Při této operaci je nutné provést pouze konfiguraci přidávaného spoke směrovače, ale ostatní uzly typu spoke či hub v topologii mohou být ponechány nedotčeny. Také není třeba vytvářet tunelové rozhraní pro každou nově přidanou pobočku. Toho je docíleno využitím mGRE rozhraní.
- Použitím technologie DMVPN je snížena velikost konfigurace potřebná na jednotlivých směrovačích ve VPN síti.
- Z důvodu využití protokolu GRE je umožněno použití vícesměrového vysílání, a proto je také zajištěna funkce dynamických směrovacích protokolů v rámce VPN sítě.
- Technologie DMVPN podporuje koncept označovaný jako split tunneling umožňující specifikovat komunikaci, která má být směrována přes zabezpečený tunel, zatímco jiná komunikace může využívat nedůvěryhodného spojení.
- Bezproblémová interoperabilita s technologií IPSec umožňující zabezpečení přenášených dat.

3.6.2 Princip funkce

Předpokládejme, že dle schématu č. 3.6 dojde k iniciaci spojení ze stanice s IP adresou 10.0.1.2 na 10.0.2.2. Zdrojová stanice je umístěna za směrovačem SPOKE1 a cílová stanice za SPOKE2.



Obrázek 3.6: Princip funkce DMVPN

Pro účely sestavení dynamického a zabezpečeného tunelu mezi těmito pobočkami, jsou vykonány následující události [10, 11]:

1. Směrovač SPOKE1 obdrží paket s cílovou IP adresou 10.0.2.2. Ze své směrovací tabulky zjistí, že je nutné paket odeslat skrz tunelové rozhraní na adresu dalšího skoku 172.20.0.3. Pokusí se tuto IP adresu nalézt ve své NHRP tabulce, ve které ji nenalezne. Proto vytvoří zprávu NHRP Resolution Request a odešle ji na NHS (Next-Hop Server), který je reprezentován směrovačem typu hub.

2. Hub směrovač nalezne ve své NHRP tabulce IP adresu 172.20.0.3 a s ní asociovanou IP adresu 192.168.0.3. Vytvoří zprávu NHRP Resolution Reply a odešle informace o asociaci mezi zmíněnými IP adresami směrovači SPOKE1. Ten zjištěnou asociaci doplní do své NHRP tabulky a naváže IPSec tunel s IP adresou 192.168.0.3. V novějších implementacích DMVPN lze vidět obměněný princip, kdy hub směrovač deleguje odeslání odpovědi na zprávu Resolution Request směrovači SPOKE2 a sám hub na tuto zprávu nedopovídá.

V tomto případě obdrží zprávu Resolution Request směrovač SPOKE2, ten si z ní zaznamená informace o asociaci mezi NBMA adresou a adresou tunelu směrovače SPOKE1 do NHRP tabulky. Není proto potřeba, aby SPOKE2 vytvářel požadavek Resolution Request v případě, kdy potřebuje zaslat odpověď či novou zprávu směrovači SPOKE1.

3. Po úspěšném sestavení IPSec tunelu jsou veškerá data do sítě 10.0.2.0/24 posílána přímo přes směrovač SPOKE2.

4. Jakmile je paket s cílovou IP adresou 10.0.2.2 doručen do cíle, vygeneruje cílové zařízení odpověď na IP adresu 10.0.1.2. Po obdržení tohoto paketu směrovačem SPOKE2 dojde k prohledání směrovací tabulky. Směrovač zjistí, že má být paket zaslán na adresu dalšího skoku 172.20.0.2 přes tunelové rozhraní. Proto také směrovač zkontroluje svou NHRP tabulku a pokud zjistí že zde není záznam pro adresu 172.20.0.2, tak následují body pět a šest. V opačném případě je již možná přímá komunikace mezi směrovači typu spoke.

5. Opět je zaslána zpráva NHRP Resolution Request na server NHS a situace se opakuje.

6. Směrovač SPOKE2 po obdržení zprávy NHRP Resolution Reply zaznamená danou asociaci do své tabulky a následně může dojít k přímé komunikaci mezi směrovačem SPOKE1 a směrovačem SPOKE2 bez využití hub směrovače jako prostředníka. Je také iniciován pokus o vytvoření IPSec tunelu. Ten je již ovšem sestaven, proto není třeba žádná další akce.

7. V případě, kdy není NHRP asociace po dobu holdtime využita, je daná asociace odstraněna. To také způsobí odstranění IPSec SA pro dané spojení.

3.7 Layer 2 Tunneling Protocol

L2TP je tunelovací protokol operující na druhé vrstvě ISO/OSI modelu, který vznikl kombinací protokolů PPTP a L2F (Layer 2 Forwarding Protocol). Protokol L2TP umožňuje přenos multiprotokolového provozu prostřednictvím zapouzdření PPP (Point-to-Point Protocol) rámců, které pak mohou být odeslány přes IP, X.25, Frame Relay nebo ATM sítě. Pro přenos zpráv za účelem správy tunelu využívá L2TP protokol UDP, který je rovněž využit pro přenos zapouzdřených PPP rámců, nesoucích samotná tunelovaná data. Na obr. č. 3.7 je vyobrazena struktura zapouzdření dat v L2TP.

Obrázek 3.7: Struktura zapouzdření dat protokolem L2TP

Jednou z výhod L2TP je skutečnost, že v tradičních VPN řešeních vzdálený uživatel přistupuje do sítě prostřednictvím NAS (Network Access Server), který zajišťuje ukončení point-to-point relace vzdáleného uživatele, poskytuje autentizaci a řídí přístup uživatele do sítě. V rámci protokolu L2TP jsou tyto funkce odděleny do dvou fyzicky oddělených zařízení, čímž je zvýšena flexibilita:

- **L2TP Access Concentrator (LAC)** – Zajišťuje autentizaci a přístup k síti. Po úspěšné autentizaci je relace vzdáleného uživatele přesměrována na LNS.
- **L2TP Network Server (LNS)** – Umožňuje vzdálenému uživateli přístup do sítě a uskutečňuje logické zakončení PPP relace uživatele, která je tunelována z LAC.

L2TP může být naimplementován ve dvou odlišných topologiích, které se liší na základě toho, zda si je klientské zařízení vědomo, že je spojení tunelováno [17]:

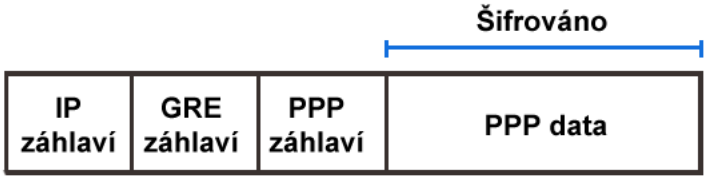
- **Client-aware tunneling** – V tomto případě vzdálený klient iniciuje vytvoření tunelu. Klient vytváří logické spojení v rámci fyzického spojení k LAC. Po celou dobu si je vědom o tunelovaném spojení a může určit datový provoz procházející tunelem.
- **Client-transparent tunneling** – Transparentní tunelování využívá L2TP přístupové koncentrátory (LAC) distribuované poblíž vzdálených uživatelů. Vzdálení uživatelé nemusí podporovat L2TP, ale pouze navazují point-to-point spojení s LAC prostřednictvím PPP protokolu. Přístupový koncentrátor (LAC) zajišťuje výměnu PPP zpráv se vzdáleným uživatelem a vytváří L2TP tunel k LNS, přes který jsou přenášeny PPP zprávy vzdáleného uživatele. LNS představuje pro vzdáleného uživatele bránu do domovské sítě.

Nevýhodou L2TP je skutečnost, že tento protokol nezajišťuje důvěrnost ani silnou autentizaci. Data jsou přenášena pouze v původní podobě a zapouzdřena L2TP a PPP rámci. Dodatečná ochrana poskytující důvěrnost, autentizaci a integritu může být zajištěna využitím protokolu IPSec společně s L2TP. Kombinace těchto protokolů je označována jako L2TP over IPSec a je popsána v RFC3193. Strukturu zapouzdření dat v L2TP over IPSec VPN lze vidět v příloze A.

3.8 Point-to-Point Tunneling Protocol

Point-to-Point Tunneling Protocol je protokol umožňující tvorbu VPN sítí na druhé vrstvě ISO/OSI modelu, který je specifikován v RFC 2637. Umožňuje, aby byl multiprotokolový datový provoz zašifrován, zapouzdřen do IP datagramu a následně odeslán skrz nedůvěryhodnou veřejnou infrastrukturu. Využívá zapouzdření PPP rámců do IP datagramů pro následný přenos přes sít, založenou na IP protokolu. Protokol PPTP lze využít k tvorbě remote-access i site-to-site VPN. Využívá kontrolního TCP spojení na portu 1723 za účelem správy tunelu a modifikovanou verzi protokolu GRE k zapouzdření PPP rámců. Nicméně obdobně jako u standardního GRE spojení jsou tyto GRE pakety zapouzdřeny do IP paketů a identifikovány jako IP protokol s číslem 47. GRE tunel je využíván za účelem přenosu zapouzdřených PPP paketů, čímž je umožněno tunelování libovolného protokolu, který lze přenášet prostřednictvím PPP jako je např. protokol IP či IPX (Internetwork Packet eXchange).

Samotná PPTP specifikace nepopisuje způsob šifrování, ani autentizace a spoléhá na tunelování protokolu PPP. Nicméně množství PPTP implementací nabízí různé úrovně šifrování a autentizace jako jejich standardní součást. V implementacích společnosti Microsoft lze tunelovaný PPP provoz autentizovat např. prostřednictvím mechanismů PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol), MS-CHAP v1/v2, PEAP (Protected Extensible Authentication Protocol) / EAP-MSCHAPv2, nebo PEAP-TLS. Za účelem šifrování dat lze také volitelně využít MPPE šifrování. Na obr. č. 3.8 je vyobrazena struktura zapouzdření dat v PPTP [7].



Obrázek 3.8: Struktura zapouzdření dat protokolem PPTP

Výhodou tohoto protokolu je zejména jeho podpora ve všech verzích OS (Operating system) Microsoft Windows od Windows 95 výše.

4 Technologie NAT-T

Překlad adres obvykle nezpůsobuje žádné potíže v typické komunikaci klient-server, při které je spojení inicializováno klientem a server využívá unikátní veřejnou IP adresu. Existují ovšem také situace, ve kterých NAT způsobuje problémy v komunikaci. Prvním problémem je skutečnost, že z principu funkce technologie NAT plyne nemožnost navázání spojení mezi dvěma uživateli využívajícími privátní IP adresy a NAT. Uživatelé spolu nemohou komunikovat, dokud nejsou vytvořeny potřebné záznamy v tabulce překladů. Další problémy vznikají např. u protokolů, které v obsahu svých zpráv odesílají také informace o IP adrese a portu. Tyto informace jsou nesprávné, jelikož po průchodu přes NAT dochází ke změně IP adresy, případně také portu. Potíže jsou způsobeny také některým protokolům, využívající hašovací funkce za účelem ověření integrity dat. Překlad adres pozmění některé informace, a proto haš vypočtený odesílatelem neodpovídá haši příjemce, který z tohoto důvodu přijatý paket zahodí.

Mezi představitele protokolů, kterým činí NAT potíže patří např. SIP, FTP a VPN založené na technologii IPSec. Patřičné korekční akce je třeba provést i u PPTP VPN či DMVPN. Za účelem vyřešení problémů technologie NAT došlo ke specifikaci mechanismů NAT-T, jejichž cílem je umožnit bezproblémovou komunikaci skrz tuto technologii. Mezi NAT-T mechanismy využívané v této práci lze zařadit:

- IPSec VPN NAT-T.
- PPTP NAT-T.
- DMVPN NAT-T.

Jednotlivé mechanismy jsou dále popsány. Záměrně jsou zvoleny VPN NAT-T technologie, jelikož cílem praktické části je zejména testování kompatibility VPN technologií mezi směrovači značky Cisco a Huawei, a také ověření NAT-T technologií mezi oběma výrobci v rámci VPN sítí.

4.1 IPSec VPN NAT-T

IPSec v ESP módu šifruje veškeré citlivé informace a zapouzdřuje celý TCP/UDP datagram v rámci ESP záhlaví. Problémem ESP je skutečnost, že neobsahuje informace o portech, jako je tomu u TCP/UDP protokolu. Ovšem PAT za účelem umožnění přístupu hostů do veřejné sítě vytváří databázi, do které ukládá informace o asociaci mezi interní IP adresou, externí IP adresou a také portem. Protože ale ESP záhlaví neobsahuje žádné informace o portech, nemůže se při asociaci IP adres do databáze přiřadit unikátní port daného paketu. Z tohoto důvodu není tento překlad dokončen a tak není možné určit, který host z vnitřní sítě paket odeslal. Proto není možné, aby u zpětného datového provozu došlo k úspěšnému překladu. Aby bylo možné zajistit úspěšnou komunikaci skrz PAT, lze využít technologii NAT-T. Přenos zpráv umožňující IPSec NAT-T je uskutečňován následovně. Nejprve je nutné identifikovat, jestli oba

účastníci komunikace podporují technologii NAT-T. To je zjištěno výměnou zpráv obsahujících tzv. vendor ID (Identification) v prvních dvou ISAKMP zprávách hlavního nebo agresivního režimu. V případě, kdy oba účastníci potvrdí podporu této technologie v poli vendor ID, dojde k detekci překladu adres ve třetí a čtvrté zprávě hlavního režimu případně ve druhé a třetí zprávě agresivního režimu. Detekce překladu adres je zajištěna prostřednictvím dat v poli NAT-D. Tato data jsou tvořena hašem cílové nebo zdrojové adresy a použitého portu.

Jakmile účastník obdrží zprávu se zmíněným hašem, vygeneruje z použitých IP adres a portů vlastní haš. Pokud se tyto dva haše neshodují, dochází mezi účastníky k překladu adres a případně také portů. Proto je aktivována funkce NAT-T a ESP paket je zapouzdřen do UDP záhlaví s portem 4500 [12]. V případě použití protokolu IKEv2 dochází k analogickému postupu. Účastníci podporující technologii NAT-T odesílají v prvních dvou zprávách IKEv2 fáze č. 1 pole NAT_DETECTION_SOURCE_IP a NAT_DETECTION_DESTINATION_IP obsahující haše z IP adres a portů. Ty jsou opět porovnány s hašem, vygenerovaném na přijímajícím účastníkovi stejně jako tomu bylo u protokolu IKEv1. Také je zde aplikováno stejně řešení NAT-T prostřednictvím UDP zapouzdření. Tímto zapouzdřením získá zařízení uskutečňující PAT přístup k UDP portům a překlad lze úspěšně dokončit.

Kromě této metody IPSec NAT-T lze také využít alternativu IPSec-over-UDP, která funguje na obdobném principu. Rozdílem je, že standardní IPSec NAT-T zapouzdřuje ESP pakety do UDP datagramů pouze v případě, kdy se v síti nachází zařízení uskutečňující NAT, zatímco IPSec-over-UDP toto zapouzdření uskutečňuje vždy [6]. Existuje i varianta NAT-T, využívající obdobných principů za použití protokolu TCP namísto UDP. Ta ovšem není natolik využívaná.

4.2 PPTP NAT-T

Protokol PPTP využívá GRE za účelem zapouzdření dat a vytvoření VPN tunelu. Protokol GRE ovšem nevyužívá porty, a proto zde nastává obdobný problém jako u dříve zmíněného protokolu IPSec – technologie PAT nemůže bez použití portů úspěšně provádět svou činnost. Tento problém lze řešit technikou zvanou PPTP NAT-T, nebo také PPTP passthrough. Řešení spočívá v nahrazení původního formátu GRE, jeho modifikovanou verzí, ve které je přidáno pole Call ID. Když PPTP klient vytváří spojení, generuje unikátní Call ID a vkládá jej do modifikovaného záhlaví. Pole Call ID je poté použito zařízením uskutečňujícím PAT jako náhrada portů a lze jej tak společně se zdrojovou IP adresou použít za účelem identifikace tunelu [5, 6].

4.3 DMVPN NAT-T

Technologie DMVPN umožňuje vytvoření tunelu typu spoke-to-spoke i v případě, kdy je určitý spoke za zařízením uskutečňujícím překlad adres. Toho je docíleno NAT rozšířením, které je umístěno do CIE (Client Information Entry) záznamu NHRP zprávy. Rozšíření obsahuje logickou IP adresu použitou pro účely tunelu, ale také skutečnou NBMA adresu po jejím překladu. Jelikož je tato informace přenášena v NHRP zprávách, je zařízení, které tuto zprávu obdrží schopné

zjistit, že dochází k překladu adresy. Také je schopno zjistit IP adresu, se kterou má komunikovat. V případě, kdy dojde k selhání sestavení spoke-to-spoke tunelu nedochází ke ztrátě dat. Data jsou posílána skrz hub směrovač. Toho je docíleno následovně. Jakmile hub směrovač příjme zprávu NHRP Resolution Request pro zjištění NBMA adresy určitého směrovače typu spoke, odešle svou vlastní adresu, namísto hledané adresy jiného spoke směrovače. Tím je zajištěno, že bude zmíněná komunikace směrovaná skrz hub směrovač a nedojde k vytvoření spoke-to-spoke tunelu.

Proces NHRP registrace je následující [11]:

1. Pobočkový směrovač v roli spoke odešle zprávu NHRP Registration Request s polem NAT-Capability=1 pro signalizaci podpory NHRP NAT rozšíření a zároveň v tomto rozšíření uvede informace o IP adresách centrálního směrovače, které jsou nastaveny na daném směrovači typu spoke. Informace o IP adresách obsahuje logickou adresu tunelu, ale také skutečnou NBMA adresu.

2. Centrální směrovač porovná informace obsažené v NHRP NAT rozšíření se svou vlastní nastavenou NBMA adresou, čímž zjistí, jestli je on sám za zařízením uskutečňujícím překlad adres. Centrální směrovač také zjistí, jestli se daný spoke nachází za NAT zařízením prostřednictvím porovnání zdrojové IP adresy s NBMA adresou uvedenou v NHRP zprávě.

3. Centrální směrovač typu hub pak odpoví zprávou Registration Reply, která v případě detekce překladu adres obsahuje také IP adresu pobočky po zmíněném překladu. Tato informace je opět umístěna do NHRP NAT rozšíření.

4. Pokud spoke obdrží zprávu NHRP Registration reply s rozšířením pro NAT, zaznamená si informaci o své IP adrese po jejím překladu.

Proces výměny zpráv NHRP Resolution [11]:

1. Pokud je spoke za NAT zařízením, odesílá součástí zprávy NHRP Resolution Request také NAT rozšíření.

2. Hub nejprve příjme zprávu Resolution Request. Pokud je spoke za NAT zařízením a původní zpráva neobsahuje NAT rozšíření, tak jej hub přidá před odesláním na další spoke směrovač. V případě, že hub směrovač odesílá tuto zprávu na další směrovač, který nepodporuje NHRP NAT rozšíření, přepíše zdrojovou NBMA adresu tak, aby se zde nyní nacházela daná IP adresa po jejím překladu.

3. Spoke směrovač, který zprávu obdrží pak za účelem sestavení tunelu použije NHRP NAT rozšíření, nebo zdrojovou NBMA adresu v případě, kdy toto rozšíření není nepodporováno. V odpovědi spoke směrovače je opět přenášeno jeho vlastní NAT rozšíření v případě, kdy je směrovač umístěn za zařízením uskutečňujícím NAT.

Samozřejmostí pro správnou funkci tohoto mechanismu je nutnost, aby adresa, na kterou je původní IP adresa překládána, byla vždy stejná pro komunikaci se směrovači v roli spoke i hub.

5 Úvod k praktické části

Za účelem verifikace interoperability mezi zařízeními společnosti Cisco a Huawei jsou v této diplomové práci využity následující směrovače a verze OS:

- Cisco 2900 Series ISR, verze IOS (Internetwork Operating System) 15.5(1)T2
- Cisco 2800 Series ISR, verze IOS 12.4(22)T
- Huawei AR3200, verze VRP (Versatile Routing Platform) 5.120
- Huawei AR2200, verze VRP 5.160

Tato zařízení byla s výjimkou technologie PPTP VPN propojena a nakonfigurována ve dvou topologiích tak, aby se z pohledu zařízení uskutečňujícího překlad adres vždy na opačné straně nacházela VPN brána jiného výrobce. Druhá topologie byla upravena tak, aby se zaměnily strany, na kterých se nacházely VPN brány daných výrobců. Zároveň byl při změně topologie zaměněn také směrovač AR3200 za směrovač AR2200 pro účely verifikace interoperability mezi různými směrovači a verzemi OS. Na vytvořených schématech jsou zařízení, která jsou použita v daných topologiích rozlišena označením T1 nebo T2. To specifikuje zda-li je dané zařízení použito v topologii č. 1 nebo topologii č. 2. Zařízení bez tohoto označení jsou použita v obou topologiích. Označení rozhraní směrovačů je na schématech uváděno pouze pro původní topologii. Označení ve druhé topologii je zřejmé z jeho popisu v konfiguraci. Popis konfigurace a verifikace jednotlivých VPN technologií je v rámci práce postupně stručnější, jelikož řada principů konfigurace je využita vícenásobně, proto není třeba jejich opakovaného detailního popisu. V ukázkách konfigurace také není uváděno základní nastavení fyzických rozhraní směrovačů, pokud se zde nenachází netypická či jinak významná konfigurace. Zpravidla tedy jednotlivé ukázky předpokládají, že konfigurace IP adresy, popis rozhraní a jeho aktivace již byla provedena. Vzhledem k tomu, že se předpokládá odborná znalost čtenáře, nejsou v práci popisovány ani operační módy a přechody mezi nimi, za účelem zajištění lepší čitelnosti, přehlednosti a stručnosti textu. Operační mód je v popisovaných konfiguracích zřejmý ze zobrazeného promptu. Součástí standardního textu práce je pouze konfigurace první topologie. Druhá topologie obvykle neobsahuje žádné výrazné změny. Proto je umístěna do příloh, kde se v případě potřeby nachází také zkrácené konfigurace všech použitých zařízení.

5.1 Konfigurace jmen uzlů

Aby bylo zřejmé, jaké zařízení se nachází na určité pozici v topologii a jaká je jeho funkce, tak byla vytvořena následující konvence ve formátu RX_FUNKCE_MODEL. Jména uzlů v síti začínají písmenem R následovaným číslicí jednoznačně identifikující směrovač v topologii. Následující část označuje hlavní funkci směrovače a v poslední části je specifikován výrobce a model

směrovače. Například označení „R1_VPNGW_C2900“ značí, že se jedná o směrovač č. 1 poskytující funkce VPN brány a jedná se o výrobce Cisco, model 2900 Series. Tato konvence je dodržována v konfiguracích zařízení. Na schématech topologií je konvence zkracována za účelem lepší čitelnosti s ohledem na omezenou velikost schématu.

Nastavení jmen směrovačů v síti je základní operací nevyžadující rozsáhlé znalosti, proto je daná problematika vysvětlena jen v této kapitole. Aby bylo dosaženo vyšší stručnosti a přehlednosti, nebudou příkazy pro změnu jmen směrovačů opakovaně uváděny v kapitolách pojednávajících o konfiguraci VPN technologií. Čtenáři je i nadále umožněno identifikovat konfigurované zařízení dle nadpisu či promptu uváděného ve výstupech konfigurace.

Pojmenování směrovače Cisco je velmi prosté. Po přihlášení operátor vstoupí do konfiguračního módu skrz privilegovaný EXEC mód a příkazem *hostname R1_VPNGW_C2900* změní jméno směrovače z Router na R1_VPNGW_C2900. Pochopitelně je možné zvolit i jiné jméno. Změna názvu ovlivní také prompt jak lze vidět na následujícím výstupu:

```
Router>enable
Router#configure terminal
Router(config)#hostname R1_VPNGW_C2900
R1_VPNGW_C2900(config)#
```

Konfigurace zařízení Huawei je uskutečněna obdobně. Nejprve operátor vstoupí do systémového módu, ve kterém pak příkazem *sysname R3_VPNGW_H3200* změní název na R3_VPNGW_H3200. Tato změna opět ovlivní také prompt:

```
<Huawei>system-view
[Huawei]sysname R3_VPNGW_H3200
[R3_VPNGW_H3200]
```

6 Konfigurace IPSec VPN

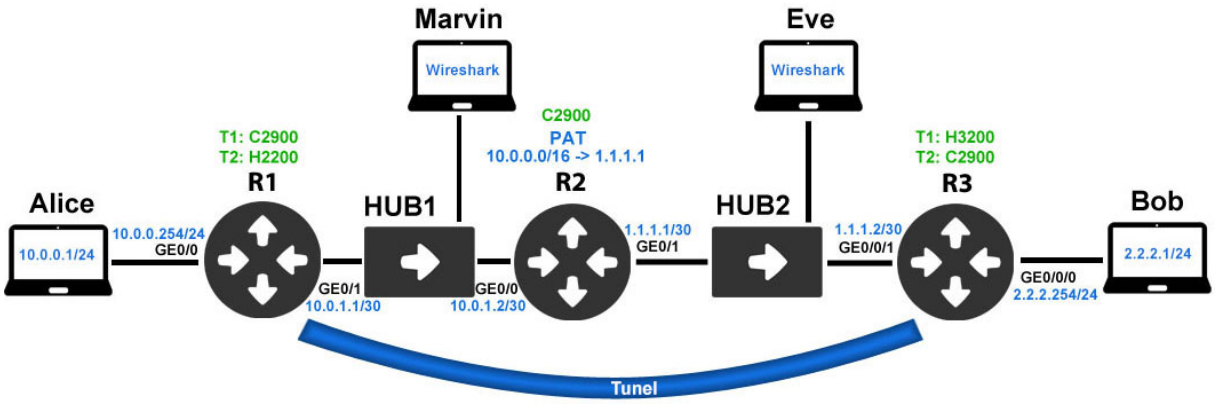
Pro ověření interoperability technologie IPSec VPN NAT traversal mezi zařízeními Cisco a Huawei jsou vytvořeny dvě topologie, ve kterých jsou využity vždy tři směrovače. Dva směrovače umístěné po stranách představují VPN brány, mezi kterými bude sestaven VPN tunel. Rovněž jsou výchozími bránami pro LAN sítě 10.0.0.0/24 resp. 2.2.2.0/24 ve kterých jsou připojeny koncové stanice uživatelů Alice a Boba. Pokud mezi sebou budou chtít zmínění uživatelé komunikovat, jejich zprávy budou směrovány na VPN bránu, kde se pomocí bezpečnostních mechanismů data zabezpečí a odešlou skrz tunel na druhou VPN bránu, která již zprávu odešle na koncovou stanici.

Zmíněné VPN brány jsou mezi sebou propojené směrovačem R2, který uskutečňuje překlad adres PAT. Z tohoto důvodu musí VPN brány podporovat technologii NAT traversal. Jednotlivé směrovače jsou mezi sebou rovněž propojeny rozbočovači, ke kterým jsou také připojeny stanice Eve a Marvina. Ti představují hrozbu, jelikož prostřednictvím aplikace Wireshark zachytávají potencionálně tajná data přenášená sítí, a proto hrozí riziko zneužití těchto dat. Alice s Bobem ovšem pro komunikaci skrz nedůvěryhodnou část sítě využívají technologie IPSec VPN, proto jsou jejich data chráněna a pro útočníky nečitelná.

Pro účely technologie NAT-T je vyžadováno použití agresivního režimu v první IKE fázi spolu s identifikací prostřednictvím jména namísto IP adresy. Vyžadováno je rovněž použití tunelovacího ESP módu. Tato kritéria jsou stanovena v dokumentaci společnosti Huawei [16].

6.1 Topologie

V této topologii představuje VPN bránu R1 i zařízení uskutečňující překlad adres R2 směrovač Cisco 2900 Series. Směrovač Huawei AR3200 pak reprezentuje VPN bránu R3. Detailní topologie je zobrazena na obrázku č. 6.1.



Obrázek 6.1: Topologie pro IPSec VPN

6.2 Konfigurace směrovače R1_VPNGW_C2900

V této topologii existuje pouze jediné rozhraní, kterým lze směrovat data na ostatní směrovače, proto je nastavena výchozí cesta přes toto rozhraní směrem na směrovač R2.

```
R1_VPNGW_C2900(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.2
```

Nyní je třeba vytvořit access-list, který je použit pro specifikaci datového provozu, který má být zabezpečen technologií IPSec VPN. V tomto případě je zabezpečena komunikace mezi sítěmi 10.0.0.0/24 a 2.2.2.0/24.

```
R1_VPNGW_C2900(config)#access-list 111 remark IPSec_ACL
R1_VPNGW_C2900(config)#access-list 111 permit ip 10.0.0.0 0.0.0.255
   2.2.2.0 0.0.0.255
```

Je také třeba vytvořit bezpečnostní IKE politiku a specifikovat algoritmy, které mají být použity. V rámci této topologie je nastaven šifrovací algoritmus AES-256, autentizační metoda využívající sdílené klíče, Diffie-Hellmanova skupina č. 5 (1536 bitů) a doba platnosti SA 3600 sekund. Hašovací algoritmus SHA-1 zde není definován, jelikož se jedná o výchozí hodnotu.

```
R1_VPNGW_C2900(config)#crypto isakmp policy 20
R1_VPNGW_C2900(config-isakmp)#encr aes 256
R1_VPNGW_C2900(config-isakmp)#authentication pre-share
R1_VPNGW_C2900(config-isakmp)#group 5
R1_VPNGW_C2900(config-isakmp)#lifetime 3600
```

Dále je třeba nastavit IKE identifikaci pomocí hostname namísto IP adres a změnit režim na agresivní za účelem dosažení interoperability se směrovačem Huawei pro komunikaci skrz zařízení uskutečňující překlad adres. Rovněž je třeba nastavit sdílený klíč a plně kvalifikované doménové jméno [16].

```
R1_VPNGW_C2900(config)#crypto isakmp identity hostname
R1_VPNGW_C2900(config)#crypto isakmp peer address 1.1.1.2
R1_VPNGW_C2900(config-isakmp-peer)#set aggressive-mode password
   letMeIn
R1_VPNGW_C2900(config-isakmp-peer)#set aggressive-mode client-
   endpoint fqdn R1_VPNGW_C2900
```

Následně je vytvořena bezpečnostní politika pro druhou fázi vyjednávaného tunelu. Pro zajištění bezpečnosti dat je nastaven protokol ESP, šifrování protokolem AES-256. Integritu a autentizaci poskytuje funkce HMAC (Keyed-Hash Message Authentication Code) využívající algoritmus SHA (Secure Hash Algorithm). Zapouzdření ESP je nastaveno na tunelovací mód.

```
R1_VPNGW_C2900(config)#crypto ipsec transform-set 20 esp-aes 256 esp-
   sha-hmac
R1_VPNGW_C2900(cfg-crypto-trans)#mode tunnel
```

Z dříve vytvořených komponent je sestavena kryptografická mapa, která tyto komponenty slučuje do jednoho prvku. V kryptografické mapě je specifikováno použití pro technologii ipsec-isakmp, dále je nastavena IP adresa VPN brány se kterou bude navázán tunel, transform-set vytvořený v předchozím kroku a access-list určující komunikaci, která má být zabezpečena.

```
R1_VPNGW_C2900(config)#crypto map CM 20 ipsec-isakmp
R1_VPNGW_C2900(config-crypto-map)#set peer 1.1.1.2
R1_VPNGW_C2900(config-crypto-map)#set transform-set 20
R1_VPNGW_C2900(config-crypto-map)#match address 111
```

Vytvořenou kryptografickou mapu je třeba aplikovat na rozhraní směrem do nedůvěryhodné části sítě.

```
R1_VPNGW_C2900(config)#interface GigabitEthernet0/1
R1_VPNGW_C2900(config-if)#crypto map CM
```

6.3 Konfigurace směrovače R2_PAT_C2900

Pokračujeme konfigurací směrovače R2. Aby byl směrovač schopen rozhodnout kudy zaslat pakety do cílových sítí, byly nakonfigurovány následující statické cesty.

```
R2_PAT_C2900(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
R2_PAT_C2900(config)#ip route 10.0.0.0 255.255.255.0 10.0.1.1
```

Hlavní funkcí tohoto směrovače je kromě směrování paketů také překlad adres. Proto je vytvořen access-list č. 1, který specifikuje adresy, které budou překládány. V tomto případně se jedná o IP adresy ze sítě 10.0.0.0/16.

```
R2_PAT_C2900(config)#access-list 1 remark NAT_ACL
R2_PAT_C2900(config)#access-list 1 permit 10.0.0.0 0.0.255.255
```

První příkaz v konfiguraci níže aktivuje dynamický překlad adres určených access-listem č. 1 na IP adresu rozhraní GigabitEthernet0/1. Dále jsou vytvořeny statické PAT záznamy zajišťující, aby komunikace z IP adresy 10.0.1.1 využívající UDP port 500 nebo 4500 byla překládána na adresu 1.1.1.1 se stejným UDP portem. Důvodem je využití UDP portu 500 protokolem ISAKMP a portu 4500 technologií NAT-T.

Statické PAT záznamy jsou potřeba pouze v případě, kdy sestavení IPSec VPN iniciuje VPN brána umístěná v části sítě s veřejnými IP adresami. Kdyby v tomto případě VPN brána R3 iniciovala spojení na veřejnou IP adresu 1.1.1.1, za kterou je adresa VPN brány R1 překládána, nebylo by možné bez statických záznamů sestavit spojení. Směrovač R2 uskutečňující překlad adres by totiž v daný okamžik neměl vytvořený žádný záznam v NAT tabulce pro odpovídající spojení a nemohl by tak rozhodnout, jak překlad adres uskutečnit, ani na jakou lokální adresu zprávy směrovat.

```
R2_PAT_C2900(config)#ip nat source list 1 interface GigabitEthernet
   0/1 overload
R2_PAT_C2900(config)#ip nat source static udp 10.0.1.1 500 1.1.1.1
   500 extendable
R2_PAT_C2900(config)#ip nat source static udp 10.0.1.1 4500 1.1.1.1
   4500 extendable
```

Poté již stačí aktivovat překlad adres na rozhraních.

```
R2_PAT_C2900(config)#interface GigabitEthernet0/0
R2_PAT_C2900(config-if)#ip nat enable

R2_PAT_C2900(config)#interface GigabitEthernet0/1
R2_PAT_C2900(config-if)#ip nat enable
```

6.4 Konfigurace směrovače R3_VPNGW_H3200

Konfigurace Huawei směrovače R3_VPNGW_H3200 je velmi podobná konfiguraci směrovače Cisco R1_VPNGW_C2900, přestože syntaxe příkazů i některé konstrukce pro nastavení IPSec VPN se mírně liší.

Jelikož existuje pouze jediná linka směřující na ostatní směrovače v síti, postačí za účelem směrování paketů nastavit výchozí cestu přes směrovač R2 s IP adresou rozhraní 1.1.1.1. Dynamické směrovací protokoly nejsou v této topologii potřeba.

```
[R3_VPNGW_H3200]ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

Následující část konfigurace je zaměřena na zabezpečení komunikace. Nejprve prostřednictvím access-listu 3000 určíme podsítě, mezi kterými má být komunikace zabezpečena. Podsítě specifikované v access-listu musí být symetrické vůči těm, které jsou použity v access-listu směrovače R1. Pouze dochází k záměně zdrojové podsítě za cílovou a obráceně.

```
[R3_VPNGW_H3200]acl number 3000
[R3_VPNGW_H3200-acl-adv-3000]description IPSec_ACL
[R3_VPNGW_H3200-acl-adv-3000]rule 10 permit ip source 2.2.2.0
   0.0.0.255 destination 10.0.0.0 0.0.0.255
```

Nastavíme lokální název a parametry pro vyjednávání první fáze IKE. Tyto parametry jsou totožné s těmi, které byly nakonfigurovány na směrovači R1. Opět není nutné definovat všechny algoritmy či autentizační metody jelikož např. *authentication-method pre-share* a *authentication-algorithm sha1* jsou pro tyto příkazy výchozími hodnotami.

```
[R3_VPNGW_H3200]ike local-name R3_VPNGW_H3200
[R3_VPNGW_H3200]ike proposal 10
[R3_VPNGW_H3200-ike-proposal-10]encryption-algorithm aes-cbc-256
[R3_VPNGW_H3200-ike-proposal-10]dh group5
[R3_VPNGW_H3200-ike-proposal-10]sa duration 3600
```

Druhým krokem je stanovení IKE vlastností, parametrů a funkcí, které budou použity pro komunikaci s druhou VPN bránou. Nejprve je nastaveno použití protokolu IKEv1. Poté je určeno použití agresivního režimu a sdíleného klíče letMeIn. Dále jsou přiřazeny parametry první fáze IKE, které byly nakonfigurovány v předchozím odstavci. Následně je nastaveno použití názvu jako ID namísto IP adresy a také je přidělen název vzdálené VPN brány. Na rozdíl od Cisco směrovačů, je třeba také aktivovat funkci NAT-T příkazem *nat traversal*. Posledním příkazem je specifikována IP adresa vzdálené VPN brány.

```
[R3_VPNGW_H3200]ike peer myIkePeer v1
[R3_VPNGW_H3200-ike-peer-myIkePeer]exchange-mode aggressive
[R3_VPNGW_H3200-ike-peer-myIkePeer]pre-shared-key simple letMeIn
[R3_VPNGW_H3200-ike-peer-myIkePeer]ike-proposal 10
[R3_VPNGW_H3200-ike-peer-myIkePeer]local-id-type name
[R3_VPNGW_H3200-ike-peer-myIkePeer]remote-name R1_VPNGW_C2900
[R3_VPNGW_H3200-ike-peer-myIkePeer]nat traversal
[R3_VPNGW_H3200-ike-peer-myIkePeer]remote-address 1.1.1.1
```

Po nastavení parametrů první IKE fáze je nutné nastavit druhou fázi. Pro účely HMAC funkce je použit algoritmus sha1. Šifrování je uskutečněno algoritmem AES-256. Ve výchozím nastavení je rovněž pro zabezpečení použit ESP tunelovací mód, proto ho není nutné nijak konfigurovat.

```
[R3_VPNGW_H3200]ipsec proposal myIPSecProposal
[R3_VPNGW_H3200-ipsec-proposal-myIPSecProposal]esp authentication-
   algorithm sha1
[R3_VPNGW_H3200-ipsec-proposal-myIPSecProposal]esp encryption-
   algorithm aes-256
```

Za účelem sjednocení všech konfigurací, týkajících se IPSec VPN, je vytvořena IPSec politika. Jedná se o podobnou strukturu jako je kryptografická mapa zmíněná v konfiguraci směrovače R1.

```
[R3_VPNGW_H3200]ipsec policy myIPSecPolicy 10 isakmp
[R3_VPNGW_H3200-ipsec-policy-isakmp-myIPSecPolicy-10]security acl
   3000
[R3_VPNGW_H3200-ipsec-policy-isakmp-myIPSecPolicy-10]ike-peer
   myIkePeer
[R3_VPNGW_H3200-ipsec-policy-isakmp-myIPSecPolicy-10]proposal
   myIPSecProposal
```

Vytvořenou IPSec politiku je poté nutné přiřadit na rozhraní.

```
[R3_VPNGW_H3200]interface GigabitEthernet0/0/1
[R3_VPNGW_H3200-GigabitEthernet0/0/1]ipsec policy myIPSecPolicy
```

6.5 Ověření funkčnosti

Funkčnost technologie IPSec VPN byla otestována použitím příkazu ping a tracepath z uživatelských stanic Boba a Alice tak, že Bob vždy testoval spojení s Alicí a naopak. Z výstupu lze vidět, že Alice spojení s Bobem otestovala úspěšně příkazem *tracepath 2.2.2.1*. Tracepath je aplikace podobná Traceroute, ale vyžaduje nižší systémová privilegia. Kromě cesty v síti zjišťuje také MTU na dané trase. Ke své funkci využívá protokol UDP namísto ICMP (Internet Control Message Protocol) [13].

Aby bylo zřejmé který uživatel spustil příkaz pro testování spojení, byly ve výstupech zaměněny skutečná jména uživatelů root a student za jména použitá ve schématu topologie. Tento princip bude aplikován i v ostatních testovaných topologiích a technologiích.

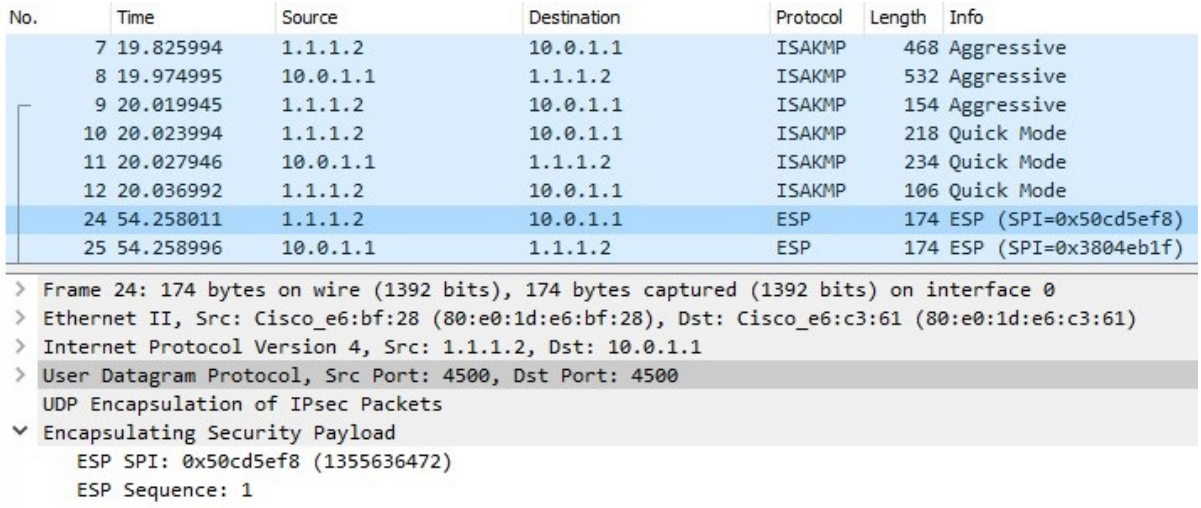
```
Alice@eb215-desktop:~$ tracepath 2.2.2.1
 1?: [LOCALHOST]                                      pmtu 1500
 1:  10.0.0.254                                         0.431ms
 1:  10.0.0.254                                         0.291ms
 2:  10.0.0.254                                         0.334ms pmtu 1422
 2:  1.1.1.2                                            4.297ms asymm 3
 3:  2.2.2.1                                            5.289ms reached
     Resume: pmtu 1422 hops 3 back 3
```

První sloupec výstupu příkazu tracepath zobrazuje TTL (Time To Live) odeslaného paketu. Druhý sloupec identifikuje zařízení, které na daný paket odpovědělo. Obvykle se jedná o adresu směrovače v síti. Zbytek řádku zobrazuje různé informace o cestě do příslušného síťového bodu. Zpravidla je zde obsažena informace o obousměrném zpoždění RTT (Round-Trip Time) a MTU v případě, že dojde k jeho změně. Také je zobrazena informace, pokud je cesta asymetrická. To je zjištěno odlišným počtem skoků mezi dopředným a zpětným směrem cesty. Tato informace ale není podle dokumentace spolehlivá [13].

Příkladem určení asymetrické cesty je pátý řádek výstupu. Pro odeslání testovacího paketu od Alice Bobovi je použit VPN tunel. Směrovač R3 však odešle ICMP zprávu „Time to live exceeded“ bez použití VPN tunelu, proto se cesta může jevit jako asymetrická. Poslední řádek výstupu zobrazuje souhrnné informace o použité cestě. Mezi tyto informace patří zjištěná velikost MTU a počet skoků do cíle a zpět.

Skutečnost, že byla data opravdu zabezpečena lze ověřit záznamy z aplikace Wireshark. Jak lze vidět na obr. č. 6.2 a 6.3, data byla zapouzdřena protokolem ESP, proto jejich obsah nebyl pro útočníky čitelný. Vzhledem k tomu že byl použit tunelovací mód ESP, není ze zachycených paketů známa ani skutečná identita komunikujících uživatelů. Veřejně viditelné jsou pouze IP adresy VPN brán. Z důvodů použití agresivního režimu při vyjednávání parametrů v první IKE fázi je ovšem možné zachytit kromě IP adres také identitu těchto VPN brán, jelikož je odesílána nešifrovaně. Ukázka zachycení identity VPN brány je zobrazena na obr. č. A.2 v příloze A. Vzhledem k tomu že komunikace byla uskutečněna skrz zařízení pro překlad adres, docházelo k zapouzdření dat protokolem UDP s portem 4500. Jak lze vidět na obrázku č. 6.2, UDP záhlaví je umístěno za vnější záhlaví protokolu IP. Z obrázku č. 6.2 a 6.3 lze také vypozorovat, že překlad adres fungoval správně a IP adresa 10.0.1.1 byla překládána na adresu 1.1.1.1.

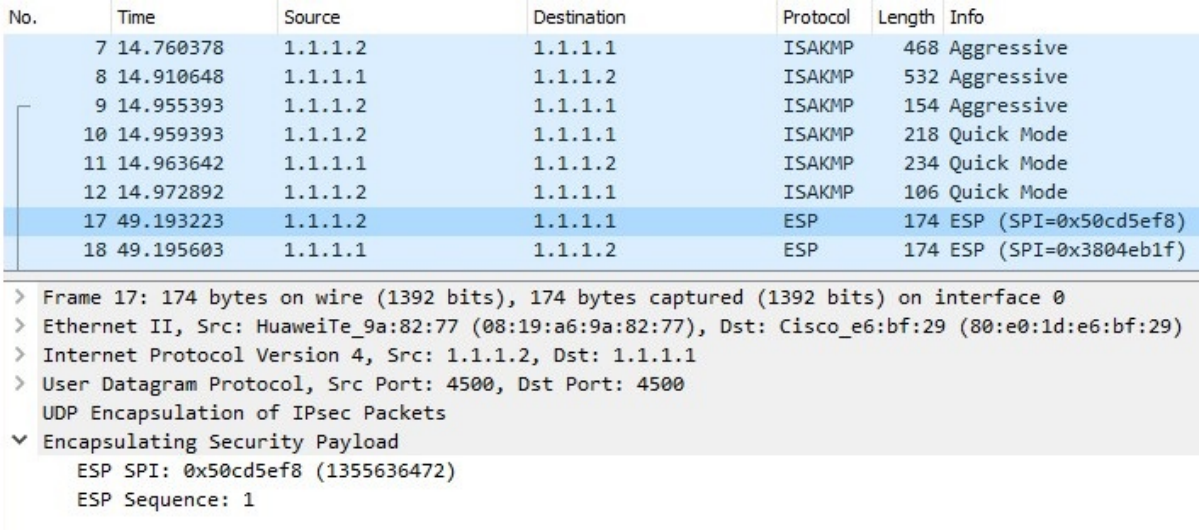
Jak již bylo zmíněno v topologii je uskutečňován překlad adres, proto je využit mechanismus NAT-T, který funguje následovně. Nejprve je třeba ověřit zda-li obě strany IPSec tunelu tuto technologii podporují. To je zjištěno výměnou řetězců výrobců (vendor strings) v prvních dvou zprávách IKE fáze č. 1 agresivního režimu. Zmíněný řetězec je viditelný na obrázku č. A.2 v příloze A – jedná se o pole typu Vendor ID. Řetězce pro konkrétní specifikaci NAT-T musí být odeslány, aby byla ověřena podpora této technologie. Jakmile je ověřena podpora na obou stranách, odešlou obě strany haš dat obsahující zjištěnou IP adresu a UDP port protistrany, ale také svou lokální IP adresu a port. Iniciátor spojení tyto informace odešle ve třetí zprávě agresivního režimu, odpovídající účastník již ve druhé zprávě, jak lze vidět na obr č. A.3 v příloze A. Po příjmutí zmíněných dat daná VPN brána vytvoří svůj vlastní haš z použitých IP adres a portů. Pokud se oba haše neshodují, tak je zřejmé, že se mezi VPN bránami nachází zařízení uskutečňující překlad adres. Aby byla umožněna komunikace při překladu adres, dojde k zapouzdření ESP paketu do UDP záhlaví [14, 15].



No.	Time	Source	Destination	Protocol	Length	Info
7	19.825994	1.1.1.2	10.0.1.1	ISAKMP	468	Aggressive
8	19.974995	10.0.1.1	1.1.1.2	ISAKMP	532	Aggressive
9	20.019945	1.1.1.2	10.0.1.1	ISAKMP	154	Aggressive
10	20.023994	1.1.1.2	10.0.1.1	ISAKMP	218	Quick Mode
11	20.027946	10.0.1.1	1.1.1.2	ISAKMP	234	Quick Mode
12	20.036992	1.1.1.2	10.0.1.1	ISAKMP	106	Quick Mode
24	54.258011	1.1.1.2	10.0.1.1	ESP	174	ESP (SPI=0x50cd5ef8)
25	54.258996	10.0.1.1	1.1.1.2	ESP	174	ESP (SPI=0x3804eb1f)

```
> Frame 24: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0
> Ethernet II, Src: Cisco_e6:bf:28 (80:e0:1d:e6:bf:28), Dst: Cisco_e6:c3:61 (80:e0:1d:e6:c3:61)
> Internet Protocol Version 4, Src: 1.1.1.2, Dst: 10.0.1.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
  UDP Encapsulation of IPsec Packets
v Encapsulating Security Payload
    ESP SPI: 0x50cd5ef8 (1355636472)
    ESP Sequence: 1
```

Obrázek 6.2: Data zachycená Marvinovou stanicí v IPSec VPN



No.	Time	Source	Destination	Protocol	Length	Info
7	14.760378	1.1.1.2	1.1.1.1	ISAKMP	468	Aggressive
8	14.910648	1.1.1.1	1.1.1.2	ISAKMP	532	Aggressive
9	14.955393	1.1.1.2	1.1.1.1	ISAKMP	154	Aggressive
10	14.959393	1.1.1.2	1.1.1.1	ISAKMP	218	Quick Mode
11	14.963642	1.1.1.1	1.1.1.2	ISAKMP	234	Quick Mode
12	14.972892	1.1.1.2	1.1.1.1	ISAKMP	106	Quick Mode
17	49.193223	1.1.1.2	1.1.1.1	ESP	174	ESP (SPI=0x50cd5ef8)
18	49.195603	1.1.1.1	1.1.1.2	ESP	174	ESP (SPI=0x3804eb1f)

```
> Frame 17: 174 bytes on wire (1392 bits), 174 bytes captured (1392 bits) on interface 0
> Ethernet II, Src: HuaweiTe_9a:82:77 (08:19:a6:9a:82:77), Dst: Cisco_e6:bf:29 (80:e0:1d:e6:bf:29)
> Internet Protocol Version 4, Src: 1.1.1.2, Dst: 1.1.1.1
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
  UDP Encapsulation of IPsec Packets
v Encapsulating Security Payload
    ESP SPI: 0x50cd5ef8 (1355636472)
    ESP Sequence: 1
```

Obrázek 6.3: Data zachycená stanicí Eve v IPSec VPN

Velmi užitečné příkazy pro verifikaci parametrů IPSec tunelu a jeho stavu jsou *show crypto ipsec sa* na směrovačích firmy Cisco a *display ipsec sa* na směrovaších značky Huawei. Jak lze vidět na výstupech níže, obsahují podstatné informace mezi které patří např. lokální a vzdálená IP adresa VPN brány, podsítě mezi kterými mají být data zabezpečena, počty zašifrovaných a dešifrovaných paketů, identifikátory SPI podle kterých VPN brány zjišťují, jaké parametry či algoritmy jsou pro danou bezpečnostní asociaci (Security Association) použity a v neposlední řadě také informaci o využití zapouzdření dat do UDP záhlaví pro účely NAT-T.

```
R1_VPNGW_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/1
    Crypto map tag: CM, local addr 10.0.1.1

   local ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
   current_peer 1.1.1.2 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7

     inbound esp sas:
      spi: 0x50CD5EF8(1355636472)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1707967/3316)

     outbound esp sas:
      spi: 0x3804EB1F(939846431)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1707964/3316)
```

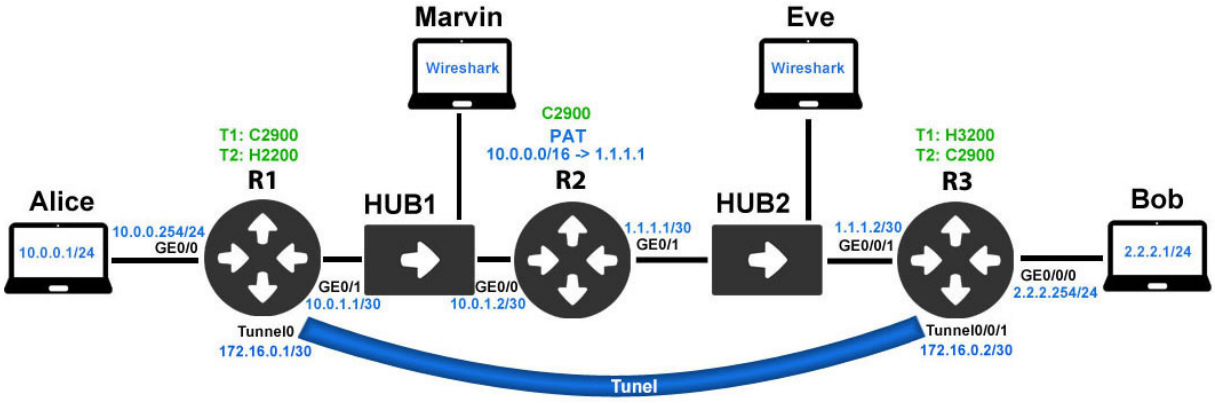
```
 [R3_VPNGW_H3200]display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: GigabitEthernet0/0/1
===============================

  -----------------------------
  IPSec policy name: "myIPSecPolicy"
  Sequence number : 10
  -----------------------------
    Encapsulation mode: Tunnel
    Tunnel local     : 1.1.1.2
    Tunnel remote    : 1.1.1.1
    Flow source      : 2.2.2.0/255.255.255.0 0/0
    Flow destination : 10.0.0.0/255.255.255.0 0/0

    [Outbound ESP SAs]
      SPI: 1355636472 (0x50cd5ef8)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887426720/3387
      UDP encapsulation used for NAT traversal: Y

    [Inbound ESP SAs]
      SPI: 939846431 (0x3804eb1f)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887433452/3387
      UDP encapsulation used for NAT traversal: Y
```

7 Konfigurace GRE over IPSec VPN

V této kapitole je popsána konfigurace technolgie GRE over IPSec VPN. Pro její ověření mezi směrovači Huawei a Cisco je využita identická topologie, která byla použita v konfiguraci IPSec VPN, její popis lze proto v případě potřeby nalézt v kapitole č. 6. Vzhledem ke skutečnosti, že je velká část konfigurace shodná, není tato část konfigurace uvedena. Popsány jsou pouze její změny. Konfigurace směrovače R2_PAT_C2900, uskutečňujícího překlad adres, nebyla nijak pozměněna, proto není uvedena vůbec. V případě potřeby jsou veškeré konfigurace uvedeny v příloze H.

7.1 Topologie

Topologie vytvořená pro technologii GRE over IPSec VPN je vybudována na základech první topologie pro IPSec VPN. Liší se pouze využitím tunelového rozhraní, které je použito z důvodu implementace technologie GRE. Topologie je znázorněna na obr. č. 7.1.



Obrázek 7.1: Topologie pro GRE over IPSec VPN

7.2 Konfigurace směrovače R1_VPNGW_C2900

Po základní konfiguraci všech fyzických rozhraní je třeba vytvořit logické rozhraní tunelu GRE. Tomu je přiřazena IP adresa a následně změněno MTU, aby bylo zamezeno zbytečné fragmentaci z důvodu využití dodatečných záhlaví pro činnost technologií GRE a IPSec. Dále je třeba nastavit zdrojovou a cílovou IP adresu tunelu. Možné je také explicitně nastavit režim GRE tunelu příkazem *tunnel mode gre ip*, jedná se však o výchozí nastavení použité platformy.

```
R1_VPNGW_C2900(config)#interface Tunnel0
R1_VPNGW_C2900(config-if)#ip address 172.16.0.1 255.255.255.252
R1_VPNGW_C2900(config-if)#ip mtu 1400
R1_VPNGW_C2900(config-if)#tunnel source GigabitEthernet0/1
R1_VPNGW_C2900(config-if)#tunnel destination 1.1.1.2
```

Výchozí cesta směrovače je nastavena přes směrovač R2 s IP adresou 10.0.1.2 na svém rozhraní GigabitEthernet0/0. Dalším příkazem je specifikována síť, pro jejíž dosažení má být využito tunelové rozhraní. Data směřující na toto rozhraní jsou zapouzdřena protolem GRE a následně šifrována technologií IPSec.

```
R1_VPNGW_C2900(config)#ip route 0.0.0.0 0.0.0.0 10.0.1.2
R1_VPNGW_C2900(config)#ip route 2.2.2.0 255.255.255.0 Tunnel0
```

Drobná úprava je také nutná pro access-list 111. IPSec VPN zabezpečovala IP pakety, ty jsou nyní zapouzdřeny protokolem GRE. Nově vzniklé vnější IP záhlaví rovněž neobsahuje původní IP adresy, nýbrž IP adresy použité pro počátek a konec GRE tunelu. Zbylá konfigurace technologie IPSec pro zabezpečení přenášených dat je shodná s kapitolou č. 6.

```
R1_VPNGW_C2900(config)#access-list 111 remark IPSec_ACL
R1_VPNGW_C2900(config)#access-list 111 permit gre host 10.0.1.1 host
   1.1.1.2
```

7.3 Konfigurace směrovače R3_VPNGW_H3200

Změny potřebné k provedení na směrovači R3_VPNGW_H3200 jsou obdobné.

```
[R3_VPNGW_H3200]interface Tunnel0/0/1
[R3_VPNGW_H3200-Tunnel0/0/1]ip address 172.16.0.2 255.255.255.252
[R3_VPNGW_H3200-Tunnel0/0/1]mtu 1400
[R3_VPNGW_H3200-Tunnel0/0/1]tunnel-protocol gre
[R3_VPNGW_H3200-Tunnel0/0/1]source 1.1.1.2
[R3_VPNGW_H3200-Tunnel0/0/1]destination 10.0.1.1

[R3_VPNGW_H3200]ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
[R3_VPNGW_H3200]ip route-static 10.0.0.0 255.255.255.0 Tunnel0/0/1

[R3_VPNGW_H3200]acl number 3000
[R3_VPNGW_H3200-acl-adv-3000]description IPSec ACL
[R3_VPNGW_H3200-acl-adv-3000]rule 10 permit gre source 1.1.1.2 0
   destination 10.0.1.1 0
```

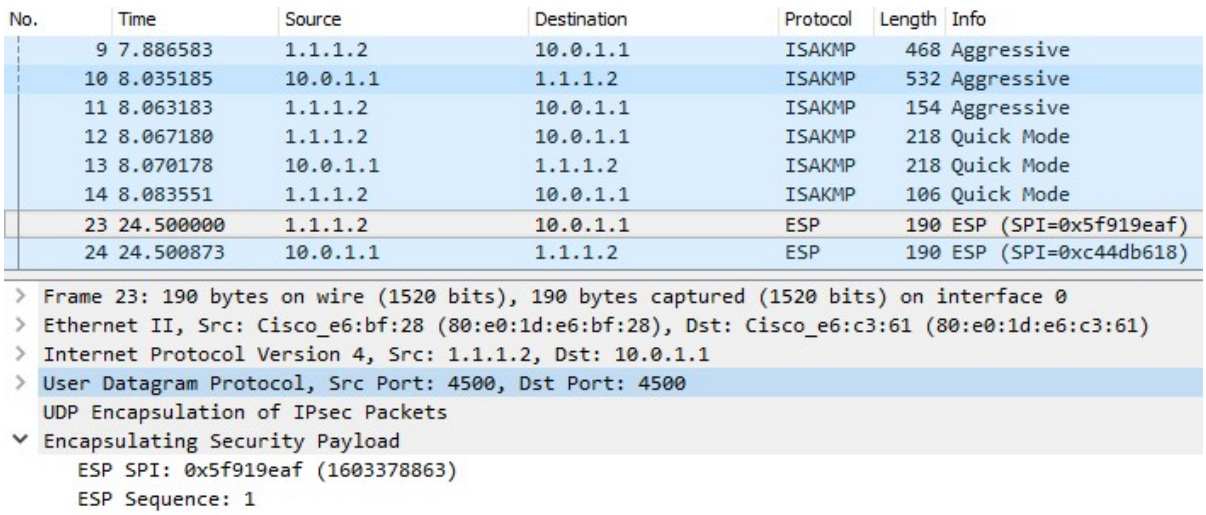
7.4 Ověření funkčnosti

Spojení bylo testováno programy Ping a Tracepath z uživatelských stanic. Z výstupu programu Tracepath lze vidět jednotlivé skoky v síti. Nejprve byl paket odeslán na VPN bránu R1 s IP adresou 10.0.0.254, poté je dalším skokem v síti identifikována IP adresa 172.16.0.2. Jedná se o adresu tunelového rozhraní VPN brány R3. Poslední skok s IP adresou 2.2.2.1 je již Bobova

koncová stanice. Důvodem vynechání směrovače R2 mezi těmito skoky je skutečnost, že tato zpráva byla zapouzdřena a byl zde vytvořen tunel mezi oběma VPN bránami. Obsah zprávy nebyl z pohledu směrovače R2 viditelný a pole TTL na tomto směrovači bylo kontrolováno a snižováno pouze ve vnějším IP záhlaví, které pro něj bylo dostupné.

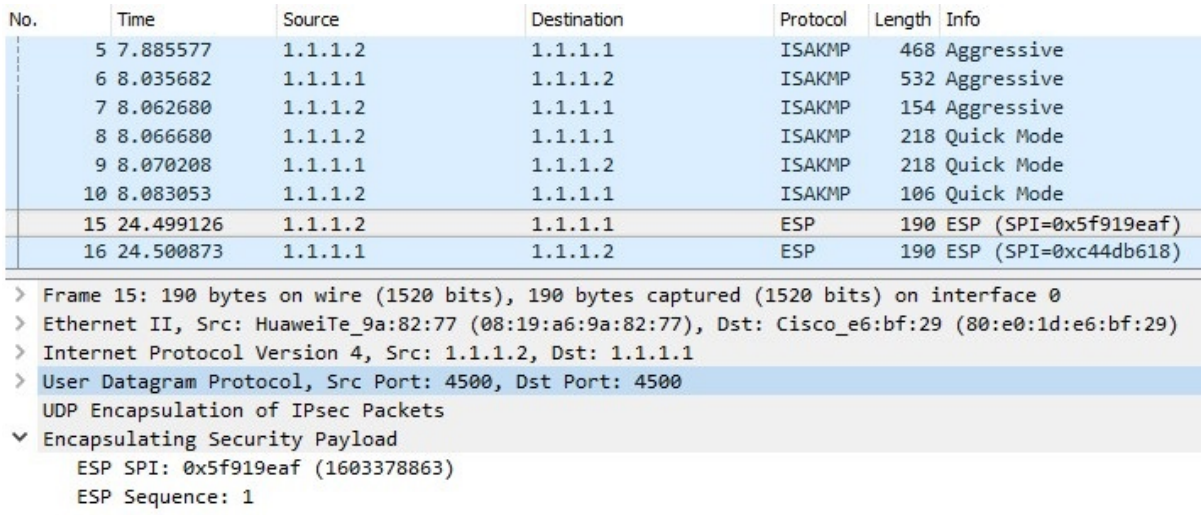
```
Alice@eb215-desktop:/home/student# tracepath 2.2.2.1
 1?: [LOCALHOST]                                      pmtu 1500
 1:  10.0.0.254                                         0.559ms
 1:  10.0.0.254                                         0.443ms
 2:  10.0.0.254                                         0.460ms pmtu 1400
 2:  172.16.0.2                                         6.087ms
 3:  2.2.2.1                                            4.832ms reached
     Resume: pmtu 1400 hops 3 back 3
```

Komunikace vzniklým tunelem byla zachycena softwarem Wireshark. Jak lze ověřit na obrázcích č. 7.2 a 7.3, byl úspěšně vytvořen IPSec tunel, který zabezpečoval původně vytvořený GRE tunel. Data byla také zapouzdřena protokolem UDP využívajícím port 4500. To značí, že se úspěšně vyjednal mechanismus NAT-T z důvodu využití překladu adres. Na zmíněných obrázcích lze vidět i úspěšný překlad IP adresy 10.0.1.1 na IP adresu 1.1.1.1.



Obrázek 7.2: Data zachycená Marvinovou stanicí v GRE over IPSec VPN

Jak již bylo zmíněno v kapitole pojednávající o IPSec VPN, dobrým zdrojem informací o vytvořené VPN síti jsou také následující příkazy *show crypto ipsec sa* a *display ipsec sa*.



Obrázek 7.3: Data zachycená stanicí Eve v GRE over IPSec VPN

```
R1_VPNGW_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/1
    Crypto map tag: CM, local addr 10.0.1.1

   local ident (addr/mask/prot/port): (10.0.1.1/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (1.1.1.2/255.255.255.255/47/0)
   current_peer 1.1.1.2 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 24, #pkts encrypt: 24, #pkts digest: 24
    #pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 24

     inbound esp sas:
      spi: 0x5F919EAF(1603378863)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1691249/3470)

     outbound esp sas:
      spi: 0xC44DB618(3293427224)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1691249/3470)
```

```
<R3_VPNGW_H3200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: GigabitEthernet0/0/1
===============================

  -----------------------------
  IPSec policy name: "myIPSecPolicy"
  Sequence number : 10
  -----------------------------


    Encapsulation mode: Tunnel
    Tunnel local     : 1.1.1.2
    Tunnel remote    : 1.1.1.1
    Flow source      : 1.1.1.2/255.255.255.255 47/0
    Flow destination : 10.0.1.1/255.255.255.255 47/0

    [Outbound ESP SAs]
      SPI: 1603378863 (0x5f919eaf)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      UDP encapsulation used for NAT traversal: Y
      SA remaining key duration (bytes/sec): 1887436152/3318

    [Inbound ESP SAs]
      SPI: 3293427224 (0xc44db618)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      UDP encapsulation used for NAT traversal: Y
      SA remaining key duration (bytes/sec): 1887436152/3318
```

8 Konfigurace DMVPN s IPSec zabezpečením

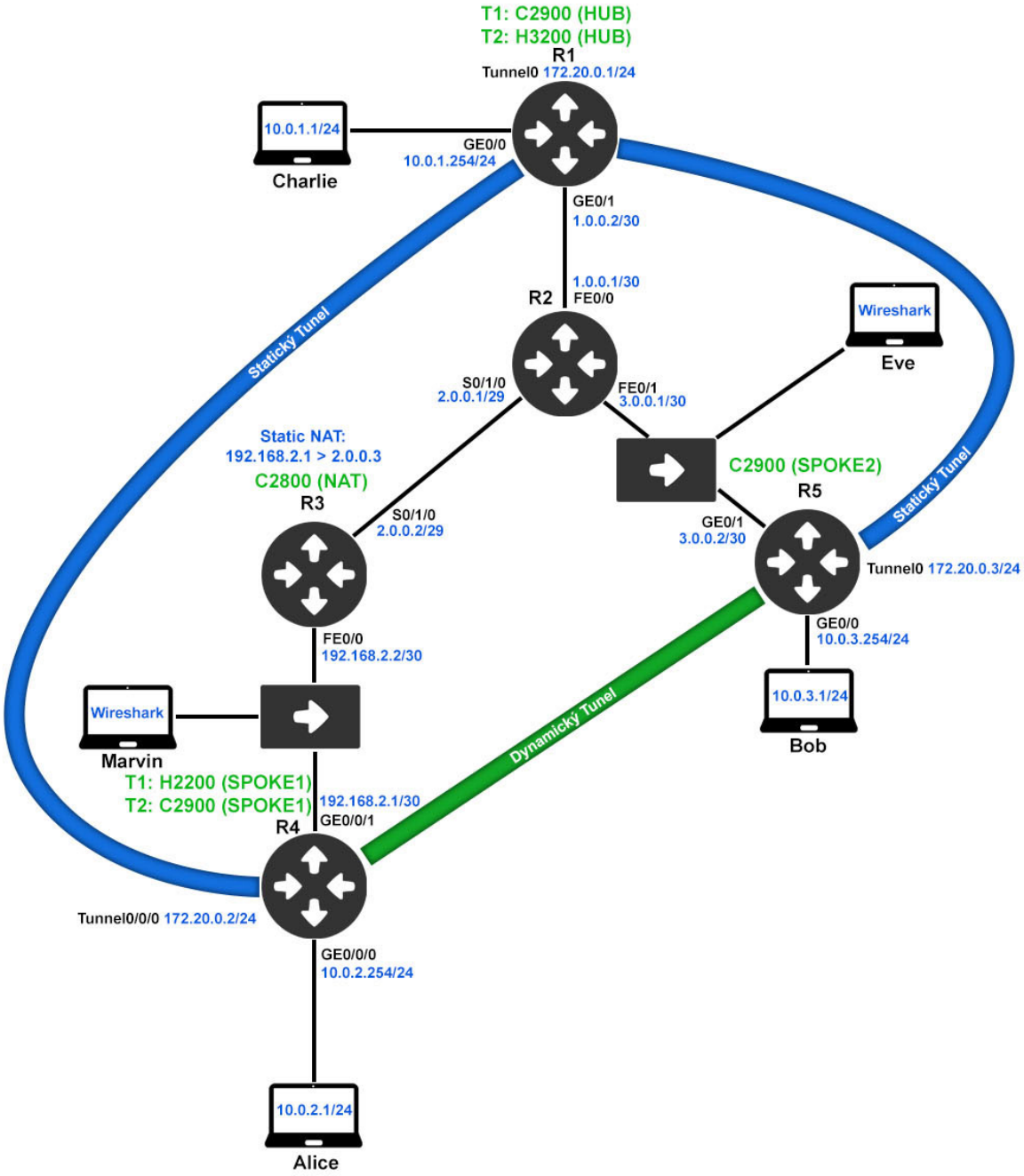
Za účelem ověření správné funkce NAT-T mezi Huawei a Cisco zařízeními v rámci technologie DMVPN jsou vytvořeny dvě topologie s pěti směrovači. Pro ověření interoperability je v jednotlivých topologiích zaměněn centrální směrovač R1 a pobočkový směrovač R4 tak, aby se zde vždy nacházel směrovač odlišného výrobce. Dva směrovače v topologii představují funkci pobočkové VPN brány. Jedná se o směrovač R4 a R5. Směrovač R1 je použit jako tzv. centrála (hub). V případě potřeby komunikace mezi pobočkou 10.0.2.0/24 a pobočkou 10.0.3.0/24 je nejprve komunikace směrována přes statický tunel na centrálu R1, která vykonává funkci prostředníka. Jakmile pobočkové VPN brány prostřednictvím protokolu NHRP zjistí asociaci mezi IP adresou tunelu a skutečnou IP adresou na fyzickém rozhraní, navážou mezi sebou dynamický tunel, který již nevede přes centrálu. Naopak vede přes nejkratší cestu naučenou ze směrovacího protokolu OSPF (Open Shortest Path First). Aby bylo možné ověřit technologii NAT-T, je na směrovači R3 uskutečněn statický překlad adres, kdy je IP adresa 192.168.2.1 použitá jako zdrojová adresa tunelu překládána na adresu 2.0.0.3. Za účelem odchycení komunikace jsou mezi směrovače také připojeny dva rozbočovače s připojenými stanicemi, na kterých byla spuštěna aplikace Wireshark.

8.1 Topologie

V první topologii je jako centrální směrovač R1 a pobočková VPN brána R5 zvolena platforma Cisco 2900 Series. Pobočkovou VPN bránu R4 představuje směrovač Huawei AR2200. Pro zbytek směrovačů v topologii je použita platforma Cisco 2800 Series viz obr. č. 8.1. Konfigurace směrovačů R2 a R3 neobsahuje nastavení, týkající se VPN technologií a zároveň je zde provedena pouze základní konfigurace, která již byla popsána v dřívějších kapitolách. Proto je tato konfigurace uvedena pouze v příloze I.

8.2 Konfigurace směrovače R1_HUB_C2900

Nejprve je vytvořeno logické tunelové rozhraní, kterému je přiřazena IP adresa a sníženo MTU, aby nedocházelo k fragmentaci paketů. Příkazem *ip nhrp map multicast dynamic* je zajištěno, že při NRHP unicastové registraci poboček na NHRP server dojde také k vytvoření NHRP asociace všesměrového a vícesměrového vysílání pro danou pobočku. Centrální směrovač (hub) pak replikuje pakety na všechny pobočky zaregistrované přes NHRP a není proto třeba vytvářet asociace všech poboček manuálně. Tato vlastnost je velmi důležitá např. pro použití dynamických směrovach protokolů [10]. Následně je použit příkaz *ip nhrp network-id 1*, kterým je umožněna identifikace logické NHRP sítě. Dalšími dvěma příkazy je ovlivněn směrovací protokol OSPF. Je změněn výchozí typ spojení bod-bod na všesměrové spojení, aby bylo umožněno automatické sestavení vícenásobných vztahů na jednom rozhraní. Také je změněna priorita na hodnotu 255



Obrázek 8.1: Topologie pro DMVPN/DSVPN

tak, aby byl centrální směrovač zvolen za OSPF DR (Designated Router). Dále je nastavena zdrojová adresa tunelu a režim tunelu na vícebodový.

```
R1_HUB_C2900(config)#interface Tunnel0
R1_HUB_C2900(config-if)#ip address 172.20.0.1 255.255.255.0
R1_HUB_C2900(config-if)#ip mtu 1400
R1_HUB_C2900(config-if)#ip nhrp map multicast dynamic
R1_HUB_C2900(config-if)#ip nhrp network-id 1
R1_HUB_C2900(config-if)#ip ospf network broadcast
R1_HUB_C2900(config-if)#ip ospf priority 255
R1_HUB_C2900(config-if)#tunnel source 1.0.0.2
R1_HUB_C2900(config-if)#tunnel mode gre multipoint
```

Navazující část příkazů je určena konfiguraci směrování. Vytvořeny jsou dvě OSPF instance. První pro distribuci směrovacích informací skrz VPN tunel, druhá pro tranzitní síť propojující všechny směrovače v topologii. Aby nedocházelo ke zbytečnému přenosu nadbytečných informací mezi OSPF oblastmi, jsou tyto oblasti nastaveny jako stub. Distribuce směrovacích dat je omezena na rozhraních, za kterými není umístěn směrovač příkazem *passive-interface*. Také je nastavena výchozí cesta přes směrovač R2.

```
R1_HUB_C2900(config)#router ospf 1
R1_HUB_C2900(config-router)#area 1 stub
R1_HUB_C2900(config-router)#passive-interface GigabitEthernet0/0
R1_HUB_C2900(config-router)#network 10.0.1.0 0.0.0.255 area 0
R1_HUB_C2900(config-router)#network 172.20.0.0 0.0.0.255 area 1

R1_HUB_C2900(config)#router ospf 2
R1_HUB_C2900(config-router)#network 1.0.0.0 0.0.0.3 area 0

R1_HUB_C2900(config)#ip route 0.0.0.0 0.0.0.0 1.0.0.1
```

Poslední částí konfigurace je její zabezpečení technologií IPSec. Nejprve jsou nastaveny klíče použité v průběhu IKE autentizace. Příkazem *pre-shared-key address 0.0.0.0 0.0.0.0 key letMeIn* je sice nastaven klíč letMeIn pro komunikaci s VPN bránami se všemi možnými IP adresami, ovšem z důvodů použití identifikátorů ve formě jmen, nikoli IP adres, je potřeba také specifikovat klíč pro obě pobočky s využitím jmen uzlů.

```
R1_HUB_C2900(config)#crypto keyring MyKeyring
R1_HUB_C2900(conf-keyring)#pre-shared-key address 0.0.0.0 0.0.0.0 key
    letMeIn
R1_HUB_C2900(conf-keyring)#pre-shared-key hostname R5_SPOKE2_C2900
   key letMeIn
R1_HUB_C2900(conf-keyring)#pre-shared-key hostname R4_SPOKE1_H2200
   key letMeIn
```

Bezpečnostní IKE politika a její algoritmy je zvolena stejně jako v kapitole zabývající se konfigurací IPSec VPN.

```
R1_HUB_C2900(config)#crypto isakmp policy 20
R1_HUB_C2900(config-isakmp)#encr aes 256
R1_HUB_C2900(config-isakmp)#authentication pre-share
R1_HUB_C2900(config-isakmp)#group 5
R1_HUB_C2900(config-isakmp)#lifetime 3600
```

Následně je vytvořen isakmp profil s názvem MyISAKMPprofile v němž je specifikována sada nakonfigurovaných sdílených klíčů, identifikace prostřednictvím plně specifikovaného doménového jména a identita ostatních VPN brán. Posledním příkazem je nastaven režim vyjednávání první IKE fáze na agresivní.

```
R1_HUB_C2900(config)#crypto isakmp profile MyISAKMPprofile
R1_HUB_C2900(conf-isa-prof)#keyring MyKeyring
R1_HUB_C2900(conf-isa-prof)#self-identity fqdn
R1_HUB_C2900(conf-isa-prof)#match identity host R4_SPOKE1_H2200
R1_HUB_C2900(conf-isa-prof)#match identity host R5_SPOKE2_C2900
R1_HUB_C2900(conf-isa-prof)#match identity address 0.0.0.0
R1_HUB_C2900(conf-isa-prof)#initiate mode aggressive
```

Dále je vytvořena bezpečnostní politika pro druhou IKE fázi.

```
R1_HUB_C2900(config)#crypto ipsec transform-set 20 esp-aes 256 esp-
   sha-hmac
R1_HUB_C2900(cfg-crypto-trans)#mode tunnel
```

V předchozích krocích vytvořený transform-set a isakmp profil je nyní svázán do IPSec profilu MyIPSecProfile.

```
R1_HUB_C2900(config)#crypto ipsec profile MyIPSecProfile
R1_HUB_C2900(ipsec-profile)#set transform-set 20
R1_HUB_C2900(ipsec-profile)#set isakmp-profile MyISAKMPprofile
```

Posledním nutným krokem je nastavení vytvořeného IPSec profilu na tunelové rozhraní.

```
R1_HUB_C2900(config)#interface Tunnel0
R1_HUB_C2900(config-if)#tunnel protection ipsec profile
   MyIPSecProfile
```

8.3 Konfigurace směrovače R4_SPOKE1_H2200

Aby bylo možné použít technologii DSVPN na směrovačích Huawei, je nejprve potřeba přijmout a aktivovat konkrétní licenci.

```
<R4_SPOKE1_H2200>license active accept agreement
<R4_SPOKE1_H2200>license function dsvpn
```

Na tunelovém rozhraní je opět třeba snížit hodnotu MTU, aby nedocházelo ke fragmentaci a následně je nastavena logická IP adresa tunelu. Dále je nastaven typ GRE tunelu na vícebodový a jeho zdrojová IP adresa na 192.168.2.1. Dalším příkazem je změněn typ OSPF spojení na všesměrové, aby bylo umožněno automatické sestavení vícenásobných vztahů na jednom rozhraní a změněna priorita na hodnotu 0 tak, aby nebyl pobočkový směrovač zvolen za DR / BDR (Backup Designated Router). Funkci DR v této topologii vykonává centrální směrovač. Příkazem *nhrp network-id 1* byl nastaven identifikátor NHRP sítě. Posledním příkazem je vytvořen statický záznam pro centrální směrovač a je na něj umožněna NHRP registrace pobočky.

```
[R4_SPOKE1_H2200]interface Tunnel0/0/0
[R4_SPOKE1_H2200-Tunnel0/0/0]mtu 1400
[R4_SPOKE1_H2200-Tunnel0/0/0]ip address 172.20.0.2 255.255.255.0
[R4_SPOKE1_H2200-Tunnel0/0/0]tunnel-protocol gre p2mp
[R4_SPOKE1_H2200-Tunnel0/0/0]source 192.168.2.1
[R4_SPOKE1_H2200-Tunnel0/0/0]ospf network-type broadcast
[R4_SPOKE1_H2200-Tunnel0/0/0]ospf dr-priority 0
[R4_SPOKE1_H2200-Tunnel0/0/0]nhrp network-id 1
[R4_SPOKE1_H2200-Tunnel0/0/0]nhrp entry 172.20.0.1 1.0.0.2 register
```

Stejně jako u centrálního směrovače jsou vytvořeny dva OSPF procesy, aby došlo k odlišení směrovacích informací přenášených přes síť VPN a tranzitní síť. Příkaz *silent-interface* má stejný význam jako *passive-interface* na operačním systému IOS. Slouží tedy k omezení distribuce směrovacích informací. Také je nastavena výchozí cesta přes směrovač R3.

```
[R4_SPOKE1_H2200]ospf 1
[R4_SPOKE1_H2200-ospf-1]silent-interface GigabitEthernet0/0/0
[R4_SPOKE1_H2200-ospf-1]area 0.0.0.1
[R4_SPOKE1_H2200-ospf-1-area-0.0.0.1]network 10.0.2.0 0.0.0.255
[R4_SPOKE1_H2200-ospf-1-area-0.0.0.1]network 172.20.0.0 0.0.0.255
[R4_SPOKE1_H2200-ospf-1-area-0.0.0.1]stub

[R4_SPOKE1_H2200]ospf 2
[R4_SPOKE1_H2200-ospf-2]area 0.0.0.0
[R4_SPOKE1_H2200-ospf-2-area-0.0.0.0]network 192.168.2.0 0.0.0.3
```

```
[R4_SPOKE1_H2200]ip route-static 0.0.0.0 0.0.0.0 192.168.2.2
```

Následující část konfigurace je zaměřena na zabezpečení přenášených dat. Nejprve je nastaven lokální název a parametry pro vyjednávání první IKE fáze.

```
[R4_SPOKE1_H2200]ike local-name R4_SPOKE1_H2200
[R4_SPOKE1_H2200]ike proposal 10
[R4_SPOKE1_H2200-ike-proposal-10]encryption-algorithm aes-cbc-256
[R4_SPOKE1_H2200-ike-proposal-10]dh group5
[R4_SPOKE1_H2200-ike-proposal-10]sa duration 3600
```

Poté jsou nastaveny další vlastnosti pro sestavení zabezpečeného spojení s ostatními VPN bránami. Rozdílem oproti konfiguraci standardní IPSec VPN je skutečnost, že není nutné specifikovat adresy či doménové jména uzlů, se kterými bude vyjednáváno zabezpečené spojení.

```
[R4_SPOKE1_H2200]ike peer myIkePeer v1
[R4_SPOKE1_H2200-ike-peer-myIkePeer]exchange-mode aggressive
[R4_SPOKE1_H2200-ike-peer-myIkePeer]pre-shared-key simple letMeIn
[R4_SPOKE1_H2200-ike-peer-myIkePeer]ike-proposal 10
[R4_SPOKE1_H2200-ike-peer-myIkePeer]local-id-type name
[R4_SPOKE1_H2200-ike-peer-myIkePeer]nat traversal
```

Také je nutné provést konfiguraci parametrů druhé IKE fáze.

```
[R4_SPOKE1_H2200]ipsec proposal myIPSecProposal
[R4_SPOKE1_H2200-ipsec-proposal-myIPSecProposal]esp authentication-
   algorithm sha1
[R4_SPOKE1_H2200-ipsec-proposal-myIPSecProposal]esp encryption-
   algorithm aes-256
```

Dříve vytvořené struktury jsou nyní sjednoceny do IPSec profilu a ten přiřazen k tunelovému rozhraní.

```
[R4_SPOKE1_H2200]ipsec profile MyProfile
[R4_SPOKE1_H2200-ipsec-profile-MyProfile]ike-peer myIkePeer
[R4_SPOKE1_H2200-ipsec-profile-MyProfile]proposal myIPSecProposal
```

IPSec profil je již pouze třeba přiřadit k tunelovému rozhraní.

```
[R4_SPOKE1_H2200]interface Tunnel0/0/0
[R4_SPOKE1_H2200-Tunnel0/0/0]ipsec profile MyProfile
```

8.4 Konfigurace směrovače R5_SPOKE2_C2900

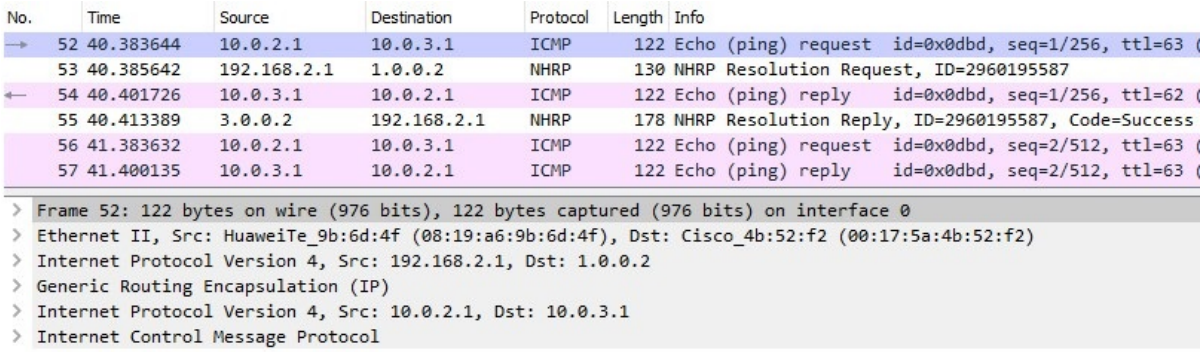
Princip konfigurace směrovače R5_SPOKE2_C2900 je stejný jako u směrovače R1_HUB_-C2900 a R4_SPOKE1_H2200, kde již byl vysvětlen. Proto již není konfigurace popisována. V případě potřeby ji lze nalézt v příloze I.

8.5 Ověření funkčnosti

Síťové spojení mezi koncovými stanicemi Alice a Boba bylo nejprve otestováno příkazy ping a následně také příkazem tracepath z uživatelké stanice Alice, aby byla ověřena cesta sítí. Napřed byla topologie ověřena bez použití technologie IPSec. Ta byla aktivována až po ověření správné funkce DMVPN. Příklad zjištěné cesty v síti lze vidět na následujícím výstupu příkazu tracepath.

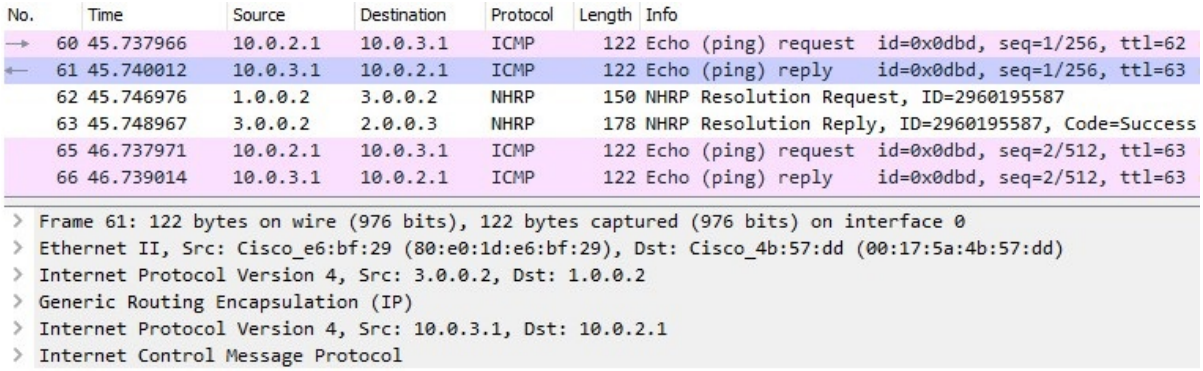
```
Alice@eb215-desktop:/home/student# tracepath 10.0.3.1
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.0.2.254                                            1.337ms
 1:  10.0.2.254                                            1.220ms
 2:  172.20.0.3                                          106.468ms
 3:  10.0.3.1                                            140.412ms reached
     Resume: pmtu 1500 hops 3 back 3
```

Z dat zachycených aplikací wireshark lze rovněž vidět, že první ICMP Echo Request zpráva odeslaná od Alice Bobovi byla směrována na IP adresu 1.0.0.2. Jedná se o IP adresu hub směrovače, který jednal v počáteční fázi jako prostředník pro komunikaci mezi pobočkami. Také je viditelné fungující zapouzdření protokolem GRE. Situace je zobrazena na obr. č. 8.2. Na následujícím obrázku č. 8.3 lze vidět, že i odpověď byla směrována přes centrální směrovač a využívala GRE zapouzdření.



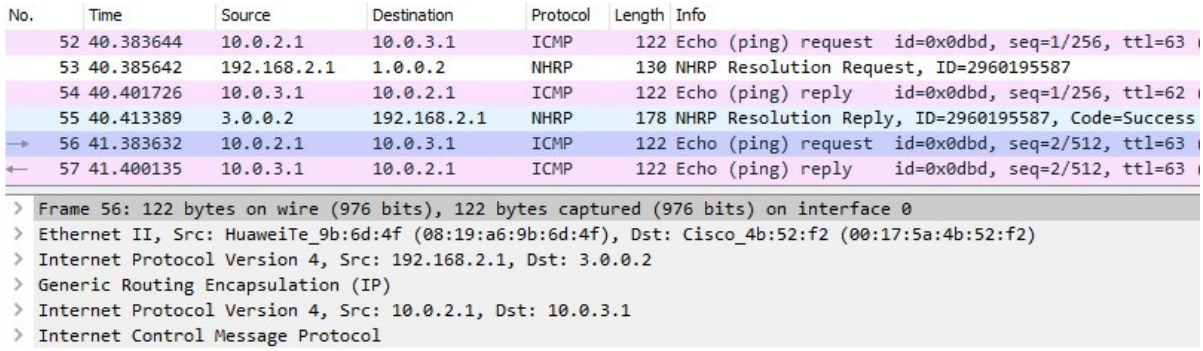
Obrázek 8.2: Data zachycená Marvinovou stanicí v DMVPN

Po odeslání první zprávy mezi pobočkami byl vygenerován NHRP požadavek pro zjištění IP adresy druhé pobočkové VPN brány. Jak lze vidět na obr. č. A.4 v příloze A, tato zpráva obsahuje NBMA (Non-Broadcast Multiple-Access) adresu odesílatele, adresu odesílatele použitou pro tunelové rozhraní a také IP adresu tunelového rozhraní druhé VPN brány, ke které je třeba zjistit NBMA adresu. V sekci Cisco NAT Address Extension lze také vidět obsah rozšíření protokolu NHRP pro interoparabilitu s technologí NAT. Pomocí tohoto pole je druhá VPN brána schopna zjistit, že je nutné NHRP odpověď zaslat na IP adresu 2.0.0.3, nikoli na 192.168.2.1, jelikož tato adresa byla přeložena.

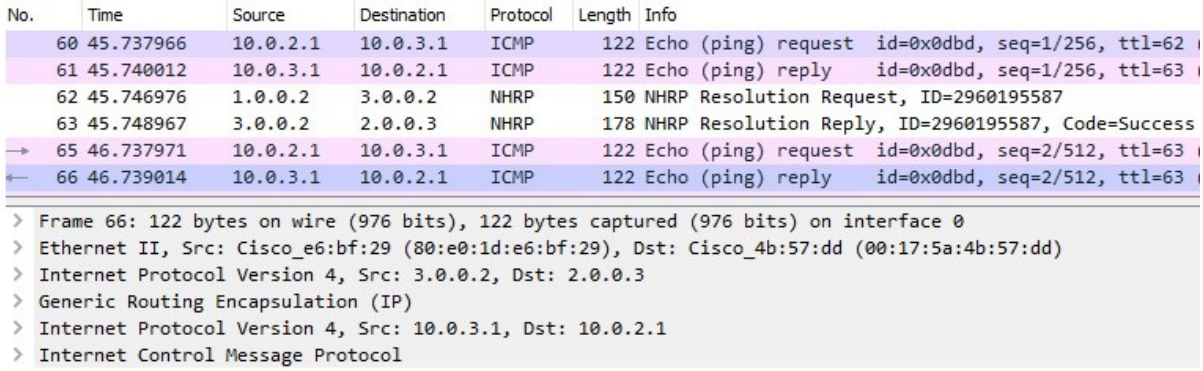


Obrázek 8.3: Zpráva ICMP Echo Reply zachycená stanicí Eve

Poté, co byla prostřednictvím NHRP vytvořena asociace mezi NBMA adresami a adresami tunelu je možné navázat komunikaci přímo mezi pobočkovými bránami bez využití centrály jako prostředníka. Skutečnost, že jednotlivé VPN brány komunikovaly přímo mezi sebou lze vidět na obrázku číslo 8.4 a 8.5. První z nich reprezentuje data zachycená stanicí Marvina, druhý záznam je ze stanice Eve.



Obrázek 8.4: Zpráva Echo Request směrovaná skrz dynamicky vytvořený tunel



Obrázek 8.5: Zpráva Echo Reply směrovaná skrz dnyamicky vytvořený tunel

Zda-li byla správně vytvořena NHRP asociace lze ověřit např. následujícími příkazy.

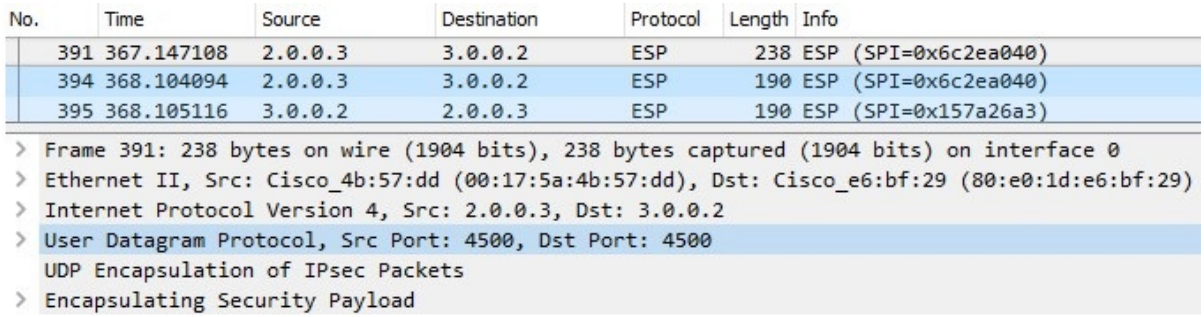
```
<R4_SPOKE1_H2200>display nhrp peer all
!Pro zachování stručnosti byl výstup částečně zkrácen!

------------------------------------------------------------------------

Protocol-addr Mask NBMA-addr NextHop-addr Type    Flag
------------------------------------------------------------------------

172.20.0.1    32   1.0.0.2    172.20.0.1   static   hub
172.20.0.3    32   3.0.0.2    172.20.0.3   dynamic  route tunnel
------------------------------------------------------------------------


R1_HUB_C2900#show dmvpn
!Pro zachování stručnosti byl výstup částečně zkrácen!

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
# Ent  Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- -------------- -------------- ----- -------- ----
     1 2.0.0.3         172.20.0.2     UP    00:14:51  DN
     1 3.0.0.2         172.20.0.3     UP    00:16:29   D




R5_SPOKE2_C2900#show dmvpn
!Pro zachování stručnosti byl výstup částečně zkrácen!

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
# Ent  Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- -------------- --------------- ----- --------- ---
     1 1.0.0.2         172.20.0.1     UP     00:17:37    S
     1 2.0.0.3         172.20.0.2     UP     00:14:32   DN
```

Ověřit, jestli směrovače skutečně znají jednotlivé pobočkové sítě z protokolu OSPF a opravdu využívají tunelových rozhraní pro dosažení těchto sítí lze zjistit příkazem *show ip route*.

```
R5_SPOKE2_C2900#show ip route
!Pro zachování stručnosti byl výstup částečně zkrácen!

Codes: L - local, C - connected, O - OSPF, , IA - OSPF inter area
O IA    10.0.1.0/24 [110/1001] via 172.20.0.1, 00:17:43, Tunnel0
O       10.0.2.0/24 [110/1001] via 172.20.0.2, 00:16:02, Tunnel0
C       172.20.0.0/24 is directly connected, Tunnel0
L       172.20.0.3/32 is directly connected, Tunnel0
```

Po ujištění, že veškerá komunikace fungovala v pořádku došlo k umístění IPSec profilu na rozhraní a spojení bylo opět testováno příkazem ping. Spojení fungovalo v pořádku a bylo zabezpečeno, což lze vidět na obr. č. 8.6. Také mechanismus NAT-T fungoval a dodatečné zapouzdření do UDP záhlaví je viditelné.

```
Bob@eb215-desktop:/home/student# ping 10.0.2.1
PING 10.0.2.1 (10.0.2.1) 56(84) bytes of data.
64 bytes from 10.0.2.1: icmp_seq=1 ttl=62 time=26.2 ms
64 bytes from 10.0.2.1: icmp_seq=2 ttl=62 time=26.1 ms
64 bytes from 10.0.2.1: icmp_seq=3 ttl=62 time=26.0 ms
^C
--- 10.0.2.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 26.037/26.132/26.258/0.092 ms
```



Obrázek 8.6: Ukázka UDP zapouzdření v síti DMVPN

Příklad vyjednaných parametrů a vlastnosti IPSec sa lze vidět z výstupu příkazu *display ipsec sa* na směrovači R4_SPOKE1_H2200.

```
<R4_SPOKE1_H2200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!
===============================
Interface: Tunnel0/0/0
  ------------------------------
  IPSec profile name: "MyProfile"
  ------------------------------
    Encapsulation mode: Tunnel
    Tunnel local     : 192.168.2.1
    Tunnel remote    : 1.0.0.2

    [Outbound ESP SAs]
      SPI: 1854868267 (0x6e8f0b2b)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887410976/1561
      UDP encapsulation used for NAT traversal: Y
    [Inbound ESP SAs]
      SPI: 4061154915 (0xf2104e63)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887411444/1561
      UDP encapsulation used for NAT traversal: Y
  ------------------------------
  IPSec profile name: "MyProfile"
  ------------------------------
    Encapsulation mode: Tunnel
    Tunnel local     : 192.168.2.1
    Tunnel remote    : 3.0.0.2

    [Outbound ESP SAs]
      SPI: 1814995008 (0x6c2ea040)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887429648/1842
      UDP encapsulation used for NAT traversal: Y
    [Inbound ESP SAs]
      SPI: 360326819 (0x157a26a3)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887435624/1842
      UDP encapsulation used for NAT traversal: Y
```

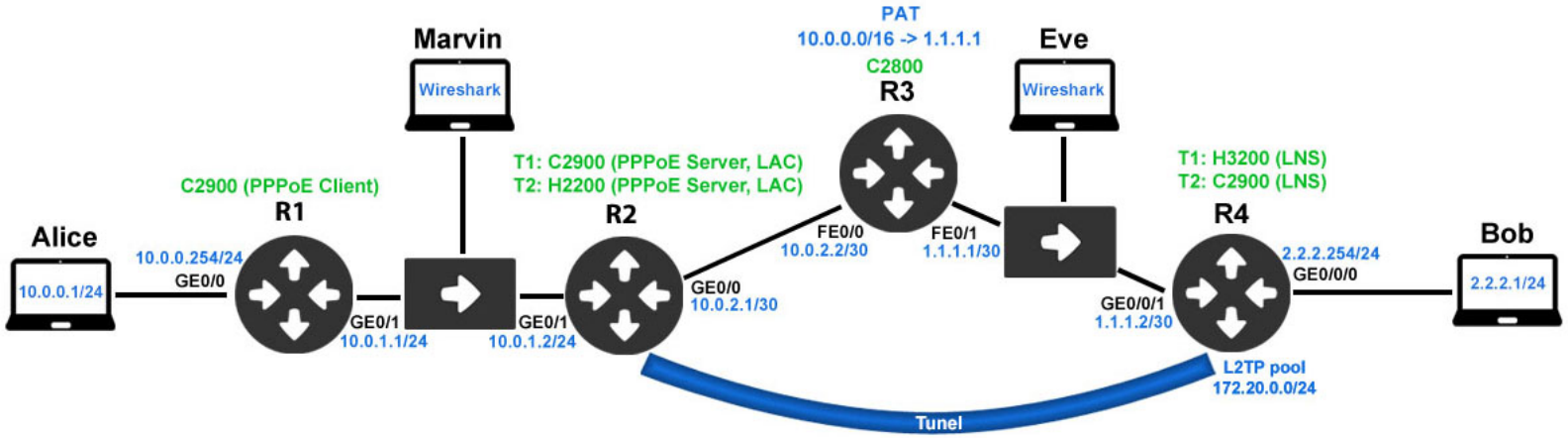
9 Konfigurace L2TP over IPSec VPN

Kapitola pojednává o konfiguraci L2TP VPN mezi směrovači Cisco a Huawei. Vytvořený L2TP tunel je také zabezpečen technologií IPSec, protože samotný protokol L2TP nezajišťuje důvěrnost, ani silnou autentizaci či jiné účinné možnosti zabezpečení. Testovací topologie jsou tvořeny čtyřmi směrovači. Dva z nich vykonávají funkci L2TP přístupového koncentrátoru (LAC) a L2TP síťového serveru (LNS). Mezi těmito směrovači je tedy vytvořen L2TP tunel, který je následně zabezpečen technologií IPSec. Zmíněný tunel prochází napříč směrovačem uskutečňujícím překlad adres typu PAT. Poslední směrovač v topologii představuje klienta technologie PPPoE (Point-to-Point Protocol over Ethernet). Ten se připojuje na PPPoE server, jehož funkci zastává LAC. Mezi směrovači jsou také umístěny rozbočovače, aby bylo možné zachytávat procházející pakety na stanicích Marvina a Eve, kde je spuštěn software Wireshark.

9.1 Topologie

Funkce LAC je v této topologii zajištěna směrovačem R2. K tomuto zařízení se připojují klienti využívající protokol PPP. Směrovač R2 je v síti použit také v roli PPPoE serveru a využívá platformu Cisco 2900 Series stejně jako směrovač R1, jenž vykonává funkci PPPoE klienta. S využitím zmíněných směrovačů ve funkci PPPoE klienta a serveru je možné přenášet PPP rámce zapouzdřené v rámcích protokolu Ethernet.

Směrovač R4 operuje ve funkci LNS a je zde tedy ukončen L2TP i IPSec VPN tunel. Zároveň představuje logické zakončení PPP relací uživatelů, jejichž spojení je tunelováno z LAC na LNS. Pro toto zařízení je použita platforma Huawei AR3200. Směrovač R3 uskutečňující překlad adres využívá platformu Cisco 2800 Series. Na tomto směrovači je třeba provést pouze základní konfiguraci fyzických rozhraní a překladu adres. Postup zmíněné konfigurace již byl popsán v dřívějších kapitolách, proto je uveden v příloze J a není zde popisován.



Obrázek 9.1: Topologie pro L2TP over IPSec VPN

9.2 Konfigurace směrovače R1_PPPoEclient_C2900

V úvodu konfigurace je na rozhraní GigabitEthernet0/1 nejprve nastaven textový popis. Dále si lze višmnout, že rozhraní nemá přiďelenou žádnou statickou IP adresu. Důvodem je přidělení IP adresy logickému rozhraní Dialer1. Dalšími dvěma příkazy je aktivována PPPoE relace a fyzické rozhraní je svázáno k tomu logickému.

```
R1_PPPOECLIENT_C2900(config)#interface GigabitEthernet0/1
R1_PPPOECLIENT_C2900(config-if)#description TO_R2_LAC_C2900
R1_PPPOECLIENT_C2900(config-if)#no ip address
R1_PPPOECLIENT_C2900(config-if)#pppoe enable group global
R1_PPPOECLIENT_C2900(config-if)#pppoe-client dial-pool-number 1
R1_PPPOECLIENT_C2900(config-if)#no shutdown
```

Rozhraní Dialer1 bylo sníženo MTU, aby nedocházelo ke fragmentaci paketů. Adresa IP protokolu je vyjednávána prostřednictvím protokolů PPP/IPCP (Internet Protocol Control Protocol). Také bylo nastaveno zapouzdřování dat do PPP rámců. Poslední příkazy jsou věnovány svázání logického rozhraní k fyzickému a nastavení autentizace.

```
R1_PPPOECLIENT_C2900(config)#interface Dialer1
R1_PPPOECLIENT_C2900(config-if)#mtu 1492
R1_PPPOECLIENT_C2900(config-if)#ip address negotiated
R1_PPPOECLIENT_C2900(config-if)#encapsulation ppp
R1_PPPOECLIENT_C2900(config-if)#dialer pool 1
R1_PPPOECLIENT_C2900(config-if)#ppp chap hostname user1@lab.local
R1_PPPOECLIENT_C2900(config-if)#ppp chap password 0 letMeIn
```

Vytvořené rozhraní je použito pro výchozí cestu ze směrovače.

```
R1_PPPOECLIENT_C2900(config)#ip route 0.0.0.0 0.0.0.0 Dialer1
```

Vzhledem k tomu že IP adresu vyjednanou pro rozhraní Dialer1 budou využívat všechny zařízení ze sítě 10.0.0.0/24 pro komunikaci s ostaními sítěmi, je zde použit překlad adres. Proto je nejprve vytvořen access-list 1, kterým je určeno které sítě budou překládány a následně je vytvořen samotný překlad. Ten je také aktivován na jednotlivých rozhraních.

```
R1_PPPOECLIENT_C2900(config)#access-list 1 remark NAT_ACL
R1_PPPOECLIENT_C2900(config)#access-list 1 permit 10.0.0.0 0.0.0.255
R1_PPPOECLIENT_C2900(config)#ip nat source list 1 interface Dialer1
   overload
```

```
R1_PPPOECLIENT_C2900(config)#interface GigabitEthernet0/0
R1_PPPOECLIENT_C2900(config-if)#ip nat enable

R1_PPPOECLIENT_C2900(config)#interface Dialer1
R1_PPPOECLIENT_C2900(config-if)#ip nat enable
```

9.3 Konfigurace směrovače R2_LAC_C2900

Napřed aktivujeme podporu VPDN sítí a autorizaci založenou na použití doménového jména. Poté je vytvořena VPDN skupina, ve které je specifikován požadavek na sestavení L2TP tunelu na LNS. V rámci tohoto požadavku je nastaven protokol L2TP, doména lab.local a IP adresa LNS, na kterou je tunel iniciován. Předposlední příkaz zajišťuje nastavení lokálního názvu, který bude použit jako identifikátor. Posledním příkazem je nastaveno heslo pro autentizaci.

```
R2_LAC_C2900(config)#vpdn enable
R2_LAC_C2900(config)#vpdn search-order domain
R2_LAC_C2900(config)#vpdn-group MyVpdnGroup
R2_LAC_C2900(config-vpdn)#request-dialin
R2_LAC_C2900(config-vpdn-req-in)#protocol l2tp
R2_LAC_C2900(config-vpdn-req-in)#domain lab.local
R2_LAC_C2900(config-vpdn-req-in)#initiate-to ip 1.1.1.2
R2_LAC_C2900(config-vpdn)#local name LAC
R2_LAC_C2900(config-vpdn)#l2tp tunnel password 0 letMeIn
```

Dále je třeba vytvořit skupinu BBA, která bude použita pro sestavení PPPoE relací a také určit šablonu virtuálních rozhraní pro klonování virtuálních přístupových rozhraní.

```
R2_LAC_C2900(config)#bba-group pppoe MyGroup
R2_LAC_C2900(config-bba-group)#virtual-template 1
```

Fyzickému rozhraní GigabitEthernet0/1 není třeba přidělovat IP adresu. Ta je totiž nastavena v konfiguraci rozhraní Virtual-Template1, ke kterému je fyzické rozhraní svázáno příkazem *pppoe enable group MyGroup*. Tímto příkazem je rovněž aktivována prodpora PPPoE na daném rozhraní.

```
R2_LAC_C2900(config)#interface GigabitEthernet0/1
R2_LAC_C2900(config-if)#description TO_R1_PPPoEclient_C2900
R2_LAC_C2900(config-if)#no ip address
R2_LAC_C2900(config-if)#pppoe enable group MyGroup
R2_LAC_C2900(config-if)#no shutdown
```

Nyní je vytvořen adresní prostor MyPool. Z něj jsou přidělovány adresy PPPoE klientům. V této topologii je pouze jeden PPPoE klient, kterému je přiřazována jediná IP adrea z adresního prostoru.

```
R2_LAC_C2900(config)#ip local pool MyPool 10.0.1.1
```

Následně je vytvořeno rozhraní Virtual-Template1, které umožňuje dynamické vytváření virtuálních přístupových rozhraní. Opět je snížena hodnota MTU, aby nedocházelo ke fragmentaci paketů, a také nastavena IP adresa rozhraní. Dalším příkazem je zajištěno použití dříve vytvořeného prostoru adres MyPool, ze kterého je klientům přiřazována IP adresa. Posledním příkazem je nastavena autentizace prostřednictvím metody CHAP.

```
R2_LAC_C2900(config)#interface Virtual-Template1
R2_LAC_C2900(config-if)#mtu 1492
R2_LAC_C2900(config-if)#ip address 10.0.1.2 255.255.255.0
R2_LAC_C2900(config-if)#peer default ip address pool MyPool
R2_LAC_C2900(config-if)#ppp authentication chap callin
```

Příkazem *ip route* je nastavena výchozí cesta přes rozhraní GigabitEthernet0/0 a také cesta do sítě 10.0.0.0/24 přes rozhraní GigabitEthernet0/1.

```
R2_LAC_C2900(config)#ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
R2_LAC_C2900(config)#ip route 10.0.0.0 255.255.255.0 GigabitEthernet
   0/1
```

Další část konfigurace je věnována zabezpečení L2TP VPN technologií IPSec. Jelikož L2TP využívá UDP port 1701 je vytvořen access-list specifikující, že se má zabezpečit právě tato komunikace. Zbytek konfigurace je totožný s konfigurací IPSec VPN v ostatních kapitolách jako je kapitola č. 6, proto již není uveden. V případě potřeby lze konfiguraci nalézt v příloze J.

```
R2_LAC_C2900(config)#access-list 111 remark IPSec_ACL
R2_LAC_C2900(config)#access-list 111 permit udp host 10.0.2.1 eq 1701
    host 1.1.1.2 eq 1701
```

9.4 Konfigurace směrovače R4_LNS_H3200

Na směrovači R4 je nejprve aktivována podpora protokolu L2TP a následně vytvořen prostor adres, z nějž budou přiřazovány IP adresy klientům. Příkazem *gateway-list 172.20.0.1* je jim také nastavena IP adresa výchozí brány.

```
[R4_LNS_H3200]l2tp enable
[R4_LNS_H3200]ip pool MyL2TPpool
[R4_LNS_H3200-ip-pool-MyL2TPpool]gateway-list 172.20.0.1
[R4_LNS_H3200-ip-pool-MyL2TPpool]network 172.20.0.0 mask
   255.255.255.0
```

V sekci AAA je vytvořen uživatelský účet s heslem letMeIn a typ služby zvolen ppp, aby mohlo dojít k úspěšné autentizaci.

```
[R4_LNS_H3200]aaa
[R4_LNS_H3200-aaa]local-user user1@lab.local password cipher letMeIn
[R4_LNS_H3200-aaa]local-user user1@lab.local service-type ppp
```

Obdobně jako u směrovače R2 ve funkci LAC je i zde vytvořeno rozhraní Virtual-Template1. Tomu je nastavena metoda autentizace CHAP, prostor adres MyL2TPpool, ze kterého jsou IP adresy přiřazovány klientům, a také je na toto rozhaní přiřazena IP adresa.

```
[R4_LNS_H3200]interface Virtual-Template1
[R4_LNS_H3200-Virtual-Template1]ppp authentication-mode chap
[R4_LNS_H3200-Virtual-Template1]remote address pool MyL2TPpool
[R4_LNS_H3200-Virtual-Template1]ip address 172.20.0.1 255.255.255.0
```

Následně je vytvořena L2TP skupina č. 1, ve které je umožněno sestavení tunelu ze vzdáleného zařízení s identifikátorem LAC. Dále je nastaveno heslo tunelu a lokální strana tunelu je identifikována názvem LNS.

```
[R4_LNS_H3200]l2tp-group 1
[R4_LNS_H3200-l2tp1]allow l2tp virtual-template 1 remote LAC
[R4_LNS_H3200-l2tp1]tunnel password simple letMeIn
[R4_LNS_H3200-l2tp1]tunnel name LNS
```

Výchozí cesta je nastavena přes směrovač R3 s IP adresou 1.1.1.1.

```
[R4_LNS_H3200]ip route-static 0.0.0.0 0.0.0.0 1.1.1.1
```

Zbylá část konfigurace je určena technologii IPSec, kterou je tato L2TP VPN zabezpečena. Jelikož již byla IPSec technologie popsána, není zde její konfigurace uvedena. Lze ji nalézt v příloze J.

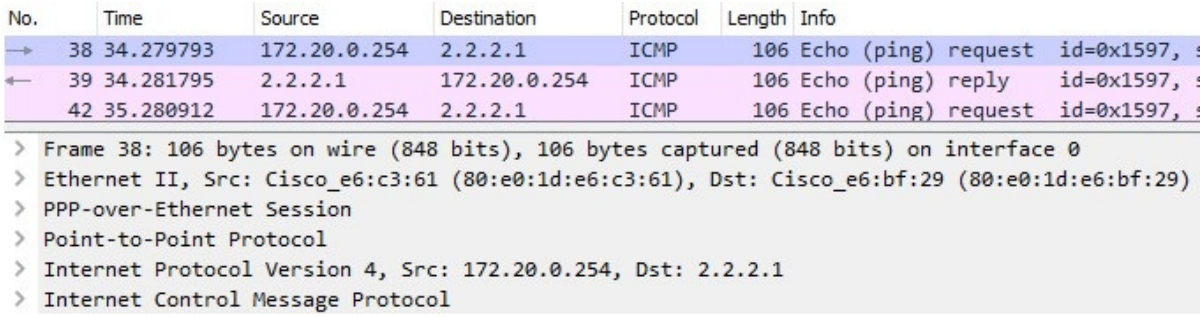
9.5 Ověření funkčnosti

K účelu ověření funkčnosti této technologie byl nejprve proveden příkaz *ping 2.2.2.1* a *tracepath 2.2.2.1* z koncové stanice Alice. Z výstupu příkazu tracepath lze vidět, že nejsou uvedeny všechny skoky mezi směrovači, kterými paket musel projít. Je tedy zřejmé, že byl paket zapouzdřen za pomocí VPN technologií a proto nedocházelo ke snižování hodnoty pole TTL mezi směrovači, přes které byl sestaven tunel.

```
Alice@eb215-desktop:/home/student# tracepath 2.2.2.1
 1?: [LOCALHOST]                                      pmtu 1500
 1:  10.0.0.254                                         0.728ms
 1:  10.0.0.254                                         0.476ms
 2:  172.20.0.1                                        15.794ms
 3:  2.2.2.1                                            6.175ms reached
     Resume: pmtu 1492 hops 3 back 3
```

Jak lze vidět na obr. č. 9.2, klient komunikoval s cílovou stanicí za použití IP adresy 172.20.0.254 z vytvořeného prostoru adres pro L2TP. Adresa tedy byla úspěšně vyjednána. To lze také vidět na výstupu příkazu *show ip int brief*.

```
R1_PPPoEclient_C2900#show ip int brief
!Pro zachování stručnosti byl výstup částečně zkrácen!

Interface                  IP-Address      OK? Method Status Protocol
GigabitEthernet0/0         10.0.0.254      YES manual up     up
GigabitEthernet0/1         unassigned      YES unset up      up
Dialer1                    172.20.0.254    YES IPCP  up      up
NVI0                       10.0.0.254      YES unset up      up
```

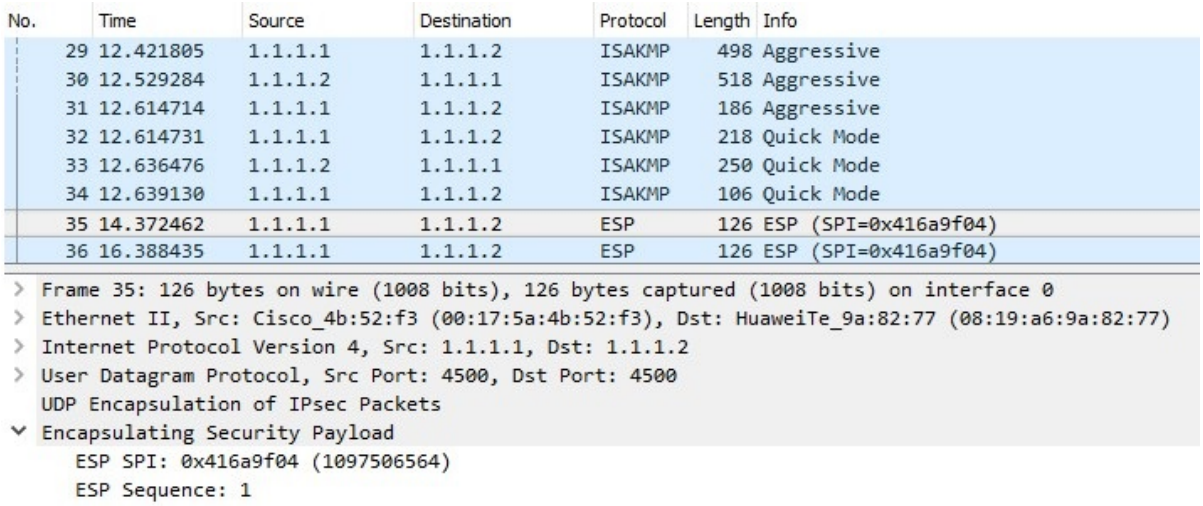


Obrázek 9.2: Komunikace zachycená Marvinovou stanicí v L2TP over IPSec VPN

Skutečnost, že byla data mezi LAC a LNS opravdu posílána přes tunel lze ověřit na obrázku číslo 9.3. Došlo zde k úspěšnému sestavení IPSec VPN překrývající L2TP tunel. Z obrázku je také zřejmé, že docházelo k zapouzdření dat do UDP záhlaví s portem 4500, technologie NAT-T tedy byla aplikována.

Existenci překrytého L2TP tunelu lze ověřit náledujícími příkazy:

```
R2_LAC_C2900#show vpdn tunnel l2tp
L2TP Tunnel Information Total tunnels 1 sessions 1
LocTunID RemTunID Remote Name State Remote Address Sessn L2TP Class/
                                                    Count VPDN Group
45037     1        LNS         est    1.1.1.2        1     MyVpdnGroup


<R4_LNS_H3200>display l2tp tunnel
 Total tunnel = 1
 LocalTID RemoteTID RemoteAddress Port  Sessions RemoteName
 1         45037    10.0.2.1      1701  1        LAC
```



Obrázek 9.3: Sestavení IKE/IPSec SA a zapouzdření paketů v L2TP over IPSec VPN

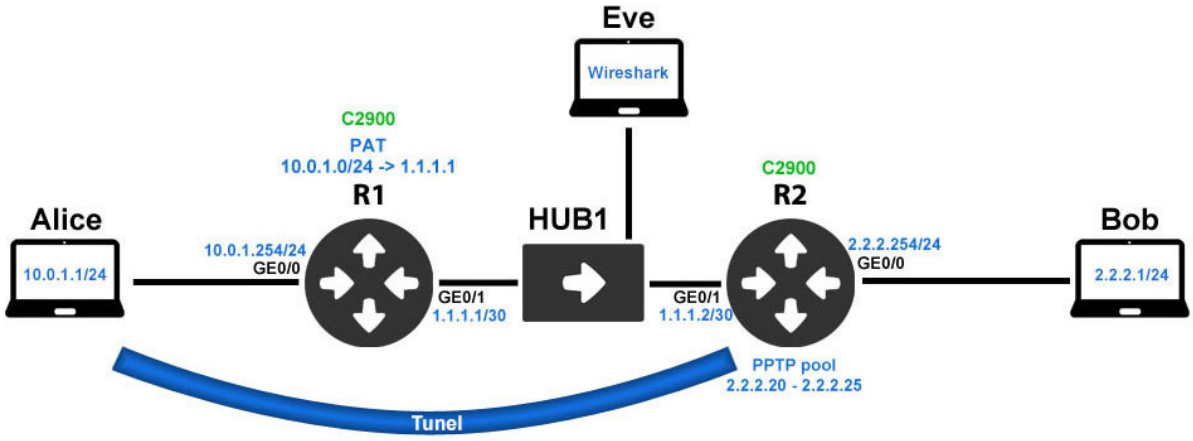
Pro ověření informací o sestavené IPSec VPN síti byly stejně jako v předchozích kapitolách použity příkazy *show crypto ipsec sa* a *display ipsec sa*.

```
R2_LAC_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/0
    Crypto map tag: CM, local addr 10.0.2.1

   local  ident (addr/mask/prot/port):
      (10.0.2.1/255.255.255.255/17/1701)
   remote ident (addr/mask/prot/port):
      (1.1.1.2/255.255.255.255/17/1701)
   current_peer 1.1.1.2 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 157, #pkts encrypt: 157, #pkts digest: 157
    #pkts decaps: 56, #pkts decrypt: 56, #pkts verify: 56


     inbound esp sas:
      spi: 0xCDC6BA3E(3452353086)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1667776/3381)


      spi: 0x416A9F04(1097506564)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1667763/3381)
```

```
<R4_LNS_H3200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: GigabitEthernet0/0/1
===============================

  IPSec policy name: "myIPSecPolicy"
  Sequence number : 10
  ----------------------------
    Encapsulation mode: Tunnel
    Tunnel local     : 1.1.1.2
    Tunnel remote    : 1.1.1.1
    Flow source      : 1.1.1.2/255.255.255.255 17/1701
    Flow destination : 10.0.2.1/255.255.255.255 17/1701

    [Outbound ESP SAs]
      SPI: 3452353086 (0xcdc6ba3e)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887431360/3185
      UDP encapsulation used for NAT traversal: Y

    [Inbound ESP SAs]
      SPI: 1097506564 (0x416a9f04)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887420708/3185
      UDP encapsulation used for NAT traversal: Y
```

10 Konfigurace PPTP VPN

Pro ověření interoperability PPTP VPN v součinnosti s překladem adres je vytvořena pouze jedna topologie, jelikož dostupné směrovače značky Huawei tuto technologii nepodporují. Topologie je tvořena ze dvou směrovačů Cisco 2900 Series, jednoho rozbočovače a tří uživatelských stanic. Účelem směrovače R1 je kromě směrování paketů především překlad adres. Konkrétně dochází k překladu adres typu PAT ze sítě 10.0.1.0/24 na adresu rozhraní GigabitEthernet0/1 s IP adresou 1.1.1.1. Směrovač R2 pak provádí zejména činnost VPN brány pro technologii PPTP VPN. Rozbočovač v síti umožňuje zachytávání přenášených dat mezi směrovač R1 a R2 stanicí Eve, která k zachytávání dat využívá aplikaci Wireshark. Alice a Bob představují uživatele, mezi kterými dochází k testované komunikaci. Schéma zmíněné topologie je zobrazeno na obrázku č. 10.1.



Obrázek 10.1: Topologie pro PPTP VPN

10.1 Konfigurace směrovače R1_PAT_C2900

Po počáteční konfiguraci fyzických rozhraní je nastavena výchozí cesta přes směrovač R2.

```
R1_PAT_C2900(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.2
```

Pro činnost překladu adres je vytvořen access-list 111, kterým je specifikována síť 10.0.1.0/24, která bude překládána.

```
R1_PAT_C2900(config)#access-list 111 remark NAT_ACL
R1_PAT_C2900(config)#access-list 111 permit ip 10.0.1.0 0.0.0.255 any
```

Následně je zmíněný access-list použit v příkazu, kterým je specifikován překlad adres určených access-listem 111 na IP adresu rozhraní GigabitEthernet0/1. Klíčovým slovem *overload* je nastaven překlad adres typu PAT.

```
R1_PAT_C2900(config)#ip nat inside source list 111 interface
   GigabitEthernet0/1 overload
```

Překlad adres je nutné aktivovat také na daných rozhraních.

```
R1_PAT_C2900(config)#interface GigabitEthernet0/0
R1_PAT_C2900(config-if)#ip nat inside

R1_PAT_C2900(config)#interface GigabitEthernet0/1
R1_PAT_C2900(config-if)#ip nat outside
```

10.2 Konfigurace směrovače R2_VPNGW_C2900

Na VPN bráně je nejprve nutné aktivovat podporu VPDN sítí příkazem vpdn enable. Poté je vytvořen prostor adres myPool, z nějž budou přidělovány IP adresy klientům.

```
R2_VPNGW_C2900(config)#vpdn enable
R2_VPNGW_C2900(config)#ip local pool myPool 2.2.2.20 2.2.2.25
```

Dalším krokem je vytvoření rozhraní Virtual-Template1 umožňující dynamické vytváření přístupových rozhraní. Funkce IP protokolu je aktivována bez potřeby přidělení konkrétní IP adresy v tomto kroku. Také je přidělen prostor adres myPool pro přidělování IP adres klientům a vypnuta funkce keepalive, aby nedocházelo k deaktivaci rozhraní pokud nejsou přenášena žádná data. Poslední dva příkazy umožňují nastavení šifrování a autentizaci.

Je vhodné poznamenat, že příkaz *ppp encrypt mppe 128* sice umožňuje použití šifrování 128-bitovým klíčem, ale šifrování není nijak vynucováno. Pro případy vynuceného použití šifrování dat je nutné na konec příkazu zadat klíčové slovo *required*.

```
R2_VPNGW_C2900(config)#interface Virtual-Template1
R2_VPNGW_C2900(config-if)#ip unnumbered GigabitEthernet0/0
R2_VPNGW_C2900(config-if)#peer default ip address pool myPool
R2_VPNGW_C2900(config-if)#no keepalive
R2_VPNGW_C2900(config-if)#ppp encrypt mppe 128
R2_VPNGW_C2900(config-if)#ppp authentication ms-chap ms-chap-v2
```

Vytvořená skupina vpdn-group 1 povoluje požadavky na sestavení PPTP spojení s využitím rozhraní virtual-template 1.

```
R2_VPNGW_C2900(config)#vpdn-group 1
R2_VPNGW_C2900(config-vpdn)#accept-dialin
R2_VPNGW_C2900(config-vpdn-acc-in)#protocol pptp
R2_VPNGW_C2900(config-vpdn-acc-in)#virtual-template 1
```

Pro účely autentizace je vytvořen uživatelský účet user1.

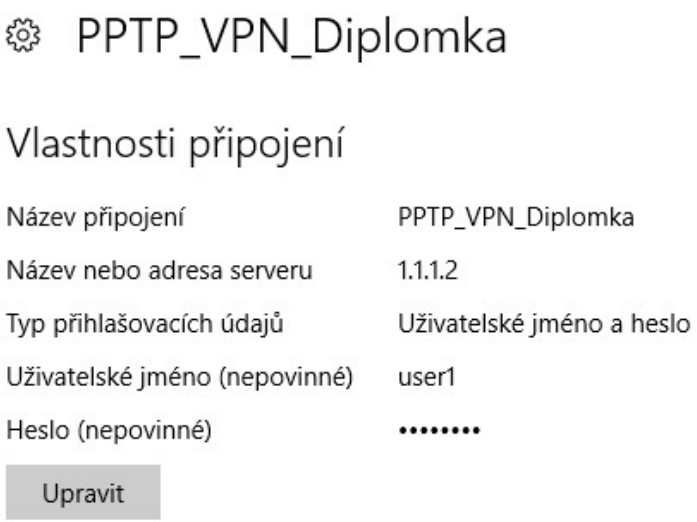
```
R2_VPNGW_C2900(config)#username user1 password 0 letMeIn
```

Poslední příkaz zajišťuje nastavení výchozí cesty přes směrovač R1 s IP adresou 1.1.1.1.

```
R2_VPNGW_C2900(config)#ip route 0.0.0.0 0.0.0.0 1.1.1.1
```

10.3 Ověření funkčnosti

Pro ověření funkčnosti bylo nejprve třeba nastavit síť VPN v operačním systému Windows klienta Alice. Nastavení VPN je možné nálezt v menu Windows > Nastavení > Síť a internet > VPN. Síť VPN byla nastevana podle obrázku 10.2.

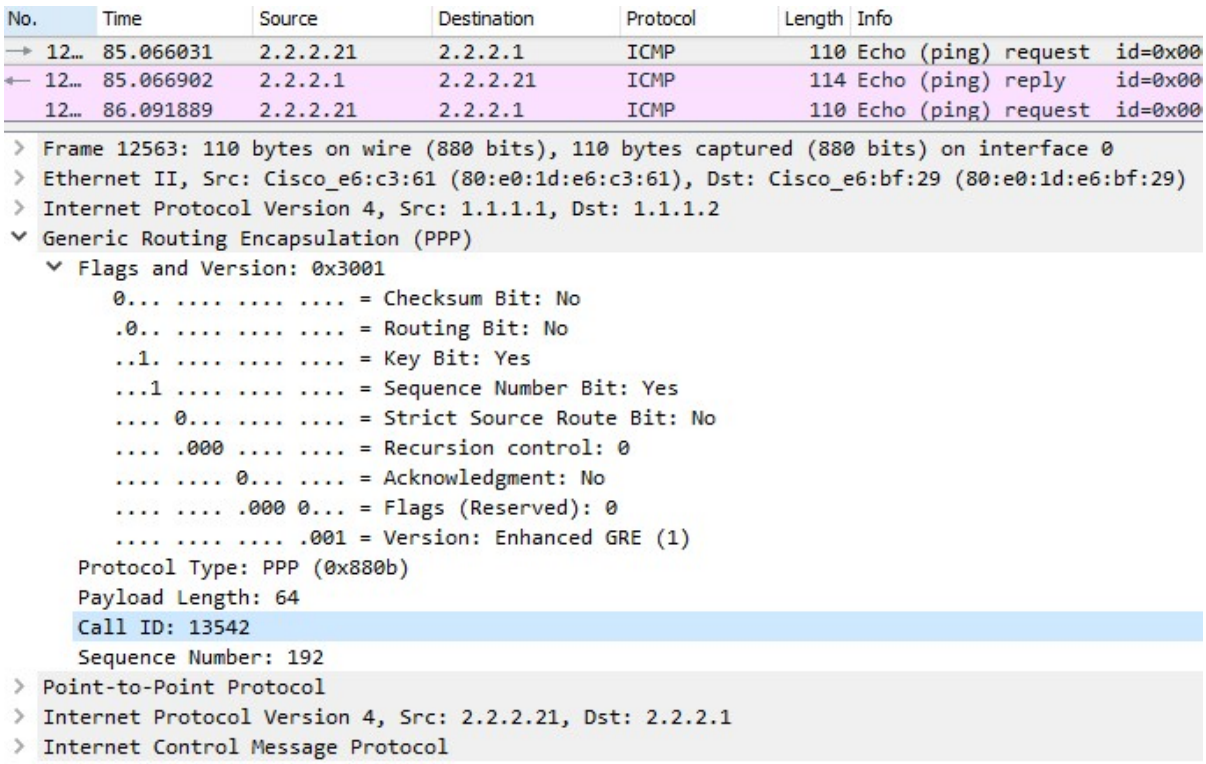


Obrázek 10.2: Ukázka konfigurace PPTP VPN klienta

Funkčnost technologie byla nejprve tradičně ověřena příkazem ping a také tracert namísto tracepath, jelikož v tomto případě byla využita stanice s OS Windows 10. Z výstupu příkazu tracert je viditelná úspěšná komunikace prostřednictvím protokolu ICMP a je zjevná i existence VPN tunelu.

```
C:\Users\Alice>tracert 2.2.2.1
Tracing route to 2.2.2.1 over a maximum of 30 hops
  1     2 ms     1 ms     1 ms  2.2.2.254
  2     2 ms     2 ms     2 ms  2.2.2.1
Trace complete.
```

Ve výstupu příkazu *ipconfig* lze taktéž vidět, že byla uživateli úspěně přidělena IP adresa z prostoru adres myPool. V tomto případě uživatel obdržel adresu 2.2.2.21. Skutečnost, že uživatel tuto adresu opravdu využívá je zobrazena na zachycené komunikaci na obrázku č. 10.3. Na něm je také viditelné zapouzdření vnitřního IP paketu do PPP a GRE záhlaví. Zdrojová IP adresa vnějšího paketu byla 1.1.1.1, proto je tedy zřejmé že i překlad adresy z 10.0.1.1 na 1.1.1.1 proběhl v pořádku.



Obrázek 10.3: Zachycená komunikace mezi Alicí a Bobem v PPTP topologii

Na obrázku je také možné vidět upravený format GRE pro PPTP účely. Za pomocí pole Call ID byla zařízení uskutečňujícímu překlad adres typu PAT umožněna jeho funkce. Pro identifikaci jednotlivých relací bylo využito místo portů pole Call ID. To lze vidět i na zkráceném vypisu NAT tabulky.

```
R1_PAT_C2900#show ip nat translations
!Pro zachování stručnosti byl výstup částečně zkrácen!
Pro Inside global    Inside local     Outside local    Outside global
gre 1.1.1.1:13542    10.0.1.1:13542   1.1.1.2:13542    1.1.1.2:13542
```

```
C:\Users\Alice>ipconfig
Ethernet adapter Ethernet:
   Connection-specific DNS Suffix . :
   Link-local IPv6 Address . . . . . : fe80::5de4:5346:2c2c:46ba%2
   IPv4 Address. . . . . . . . . . . : 10.0.1.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.1.254
PPP adapter PPTP_VPN_Diplomka:
   Connection-specific DNS Suffix . :
   IPv4 Address. . . . . . . . . . . : 2.2.2.21
   Subnet Mask . . . . . . . . . . . : 255.255.255.255
   Default Gateway . . . . . . . . . : 0.0.0.0
```

Zda-li je vytvořena PPTP relace, bylo ověřeno příkazem *show vpdn session pptp*. Z výstupu lze vidět aktivní relaci od uživatele identifikovaného názvem user1.

```
R2_VPNGW_C2900#show vpdn session pptp
PPTP Session Information Total tunnels 1 sessions 1
LocID RemID TunID Intf  Username     State  Last Chg Uniq ID
13542 52858 43252 Vi3   user1        estabd 00:06:44 8
```

11 Konfigurace IPSec IKEv2 VPN

Přestože je IKEv1 stále hojně využívaným protokolem pro sestavení IPSec SA, existuje i novější verze IKEv2. Proto je v této kapitole představena ukázka konfigurace druhé verze tohoto protokolu. Jelikož se v ukázce vychází z původních topologií a konfigurací IPSec VPN popsaných v kapitole č. 6, nebude již princip funkce ani konfigurace tak detailně vysvětlena. Z konfigurace jsou vynechány části, jejichž nastavení zůstalo beze změny. Proto je tato kapitola věnována zejména konfiguraci technologie IPSec nikoli směrování, nastavení IP adres na rozhraní apod. Kompletní konfigurace je uvedena v příloze L.

11.1 Topologie

Stejně jako v případě IPSec VPN s využitím protokolu IKEv1 je i zde zařízení R1 představující VPN bránu i směrovač R2 uskutečňující překlad adres tvořen platformou Cisco 2900 Series. Platformou Huawei AR3200 je reprezentována VPN brána R3. Schéma topologie je shodné se schématem v kapitole č. 6.

11.2 Konfigurace směrovače R1_VPNGW_C2900

Pro specifikaci datového provozu, který má být zabezpečen technologií IPSec VPN je vytvořen access-list 111. Komunikace bude zabezpečena mezi sítí 10.0.0.0/24 a 2.2.2.0/24.

```
R1_VPNGW_C2900(config)#access-list 111 remark IPSec_ACL
R1_VPNGW_C2900(config)#access-list 111 permit ip 10.0.0.0 0.0.0.255
   2.2.2.0 0.0.0.255
```

Také jsou nastaveny parametry a algoritmy pro použití v rámci první IKE fáze při vyjednávání tunelu.

```
R1_VPNGW_C2900(config)#crypto ikev2 proposal myIKE2proposal
R1_VPNGW_C2900(config-ikev2-proposal)#encryption aes-cbc-256
R1_VPNGW_C2900(config-ikev2-proposal)#integrity sha1
R1_VPNGW_C2900(config-ikev2-proposal)#group 5
```

Následně je vytvořena IKEv2 politika, ve které je specifikováno využití v předchozím kroku vytvořených parametrů a algoritmů.

```
R1_VPNGW_C2900(config)#crypto ikev2 policy myIKE2policy
R1_VPNGW_C2900(config-ikev2-policy)#proposal myIKE2proposal
```

Také je nutné definovat sdílené klíče a IP adresu pro sestavení tunelu s VPN branou R3.

```
R1_VPNGW_C2900(config)#crypto ikev2 keyring myIKE2keyring
R1_VPNGW_C2900(config-ikev2-keyring)#peer R3
R1_VPNGW_C2900(config-ikev2-keyring-peer)#address 1.1.1.2
R1_VPNGW_C2900(config-ikev2-keyring-peer)#pre-shared-key local
   letMeIn
R1_VPNGW_C2900(config-ikev2-keyring-peer)#pre-shared-key remote
   letMeIn
```

V kryptografickém profilu nastavíme lokální a vzdálenou formu identifikace a autentizační metodu spolu se sdílenými klíči, které byly definovány v předchozím kroku.

```
R1_VPNGW_C2900(config)#crypto ikev2 profile myIKE2profile
R1_VPNGW_C2900(config-ikev2-profile)#match identity remote fqdn R3
R1_VPNGW_C2900(config-ikev2-profile)#identity local fqdn R1
R1_VPNGW_C2900(config-ikev2-profile)#authentication remote pre-share
R1_VPNGW_C2900(config-ikev2-profile)#authentication local pre-share
R1_VPNGW_C2900(config-ikev2-profile)#keyring local myIKE2keyring
```

Příkazem *crypto ipsec transform-set 20 esp-aes 256 esp-sha-hmac* nastavíme za účelem zabezpečení dat využití protokolu ESP, šifrování protokolem AES-256 a integritu s autentizací prostřednictvím funkce HMAC využívající algoritmus SHA. Pro zapouzdření dat je následně zvolen ESP tunelovací mód.

```
R1_VPNGW_C2900(config)#crypto ipsec transform-set 20 esp-aes 256 esp-
   sha-hmac
R1_VPNGW_C2900(cfg-crypto-trans)#mode tunnel
```

Poté jsou jednotlivé, dříve vytvořené struktury, sjednoceny do formy kryptografické mapy CM 20, která je následně aplikována na rozhraní GigabitEthernet0/1.

```
R1_VPNGW_C2900(config)#crypto map CM 20 ipsec-isakmp
R1_VPNGW_C2900(config-crypto-map)#set peer 1.1.1.2
R1_VPNGW_C2900(config-crypto-map)#set transform-set 20
R1_VPNGW_C2900(config-crypto-map)#set ikev2-profile myIKE2profile
R1_VPNGW_C2900(config-crypto-map)#match address 111

R1_VPNGW_C2900(config)#interface GigabitEthernet0/1
R1_VPNGW_C2900(config-if)#crypto map CM
```

11.3 Konfigurace směrovače R3_VPNGW_H3200

U zažízení Huawei je nutná pouze minimální změna konfigurace. Ta spočívá ve specifikaci IKE verze 2 při konfiguraci IKE vlastností pro komunikaci s druhou VPN bránou. Další změnou je nepoužití příkazu *exchange-mode aggressive*, jelikož v druhé verzi IKE již tento režim není používán.

```
[R3_VPNGW_H3200]ike peer myIkePeer v2
[R3_VPNGW_H3200-ike-peer-myIkePeer]pre-shared-key simple letMeIn
[R3_VPNGW_H3200-ike-peer-myIkePeer]ike-proposal 10
[R3_VPNGW_H3200-ike-peer-myIkePeer]local-id-type name
[R3_VPNGW_H3200-ike-peer-myIkePeer]remote-name R1
[R3_VPNGW_H3200-ike-peer-myIkePeer]nat traversal
[R3_VPNGW_H3200-ike-peer-myIkePeer]remote-address 1.1.1.1
```

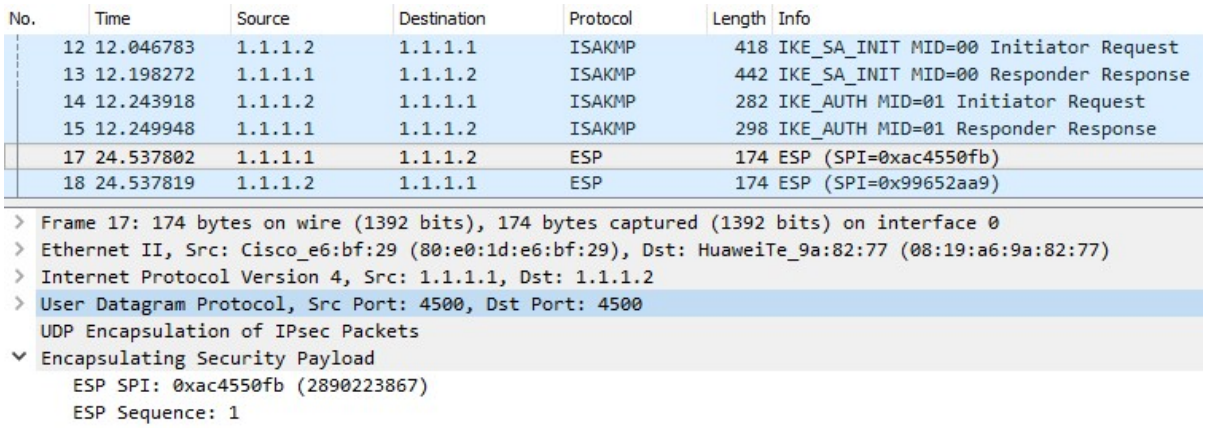
11.4 Ověření funkčnosti

Funkčnost IPSec VPN s využitím protokolu IKEv2 byla nejprve ověřena příkazy ping a tracepath z uživatelských stanic. Na základně těcho příkazů bylo úspěšně ověřeno spojení mezi stanicí Boba a Alice. Výstup příkazu tracepath lze vidět níže.

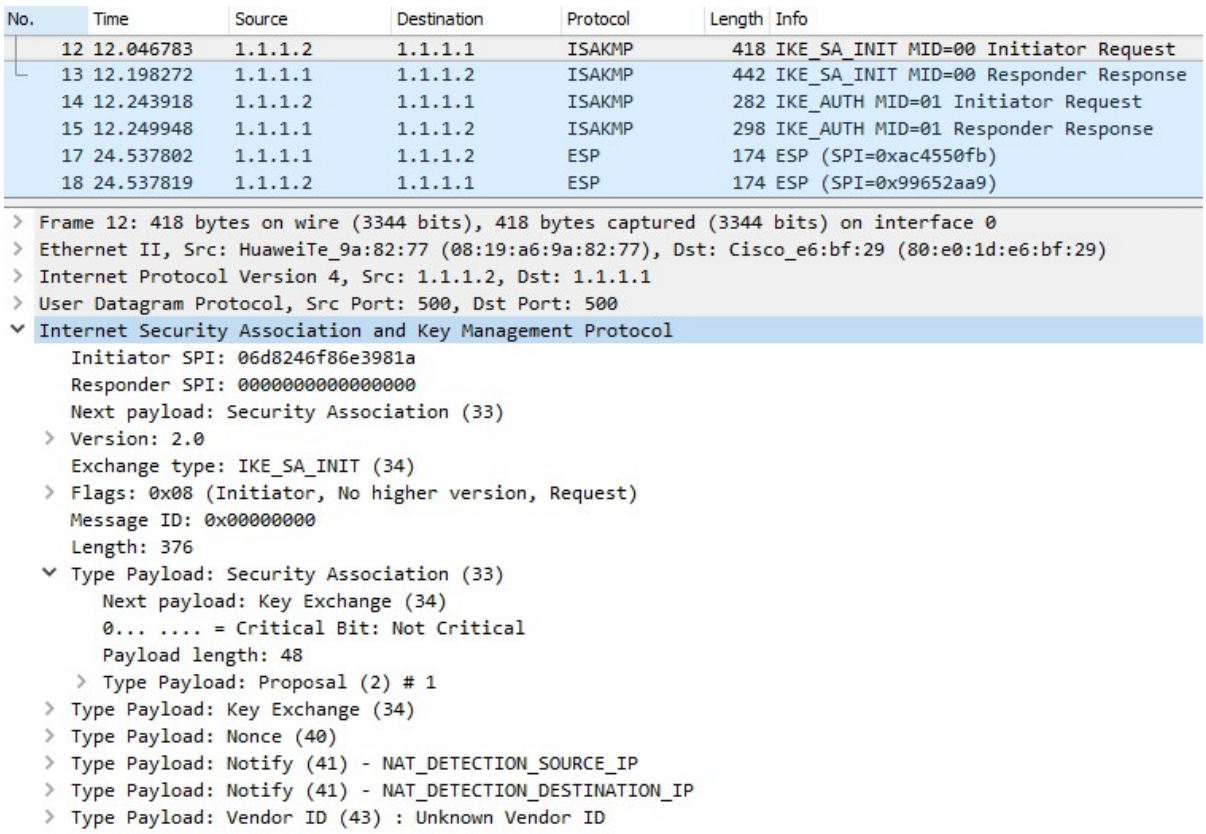
```
Alice@eb215-desktop:/home/student# tracepath 2.2.2.1
 1?: [LOCALHOST]                                      pmtu 1500
 1:  10.0.0.254                                         0.551ms
 1:  10.0.0.254                                         0.405ms
 2:  10.0.0.254                                         0.469ms pmtu 1422
 2:  1.1.1.2                                            4.302ms asymm 3
 3:  2.2.2.1                                            5.243ms reached
     Resume: pmtu 1422 hops 3 back 3
```

Z komunikace, která byla zachycena stanicí Eve je viditelné, že IP adresa 10.0.1.1 VPN brány R1 byla skutečně překládána na IP adresu 1.1.1.1 a před ESP záhlaví bylo umístěno dodatečné UDP záhlaví pro funkci NAT-T. Situace je zobrazena na obrázku č. 11.1.

Na následujícím obrázku č. 11.2 lze také vidět informace přenášené ve zprávě Initiator Request první IKEv2 fáze IKE_SA_INIT. Z pohledu technologie NAT-T jsou důležitá data přenášená v polích NAT_DETECTION_*_IP, která jsou obsažena právě ve zprávě Initiator Request a Responder Response. V sekci NAT_DETECTION_*_IP je přenášen haš, který je tvořen IP adresami a porty, které jsou použity pro sestavení VPN. Pokud příjemce porovná tento haš s tím, který sám vygeneruje a zjistí, že hodnoty nejsou shodné, je zřejmé že mezi VPN bránami dochází k překladu adres, případně také portů. Proto je nutné aktivovat NAT-T využívající zapouzdření ESP paketů do UDP.



Obrázek 11.1: Sestavení SA a zapouzdření paketů v IPSec IKEv2 topologii



Obrázek 11.2: Obsah zprávy Initiator Request

Informace o sestavených IPSec SA byly vypsány následujícími příkazy.

```
<R3_VPNGW_H3200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: GigabitEthernet0/0/1
===============================
  -----------------------------
  IPSec policy name: "myIPSecPolicy"
  Sequence number : 10
  -----------------------------
    Encapsulation mode: Tunnel
    Tunnel local     : 1.1.1.2
    Tunnel remote    : 1.1.1.1
    Flow source      : 2.2.2.0/255.255.255.0 0/0
    Flow destination : 10.0.0.0/255.255.255.0 0/0

    [Outbound ESP SAs]
      SPI: 2573544105 (0x99652aa9)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887435720/3491
      UDP encapsulation used for NAT traversal: Y

    [Inbound ESP SAs]
      SPI: 2890223867 (0xac4550fb)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887433452/3491
      UDP encapsulation used for NAT traversal: Y
```

```
R1_VPNGW_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/1
    Crypto map tag: CM, local addr 10.0.1.1

   local ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
   current_peer 1.1.1.2 port 4500
     PERMIT, flags={origin_is_acl,}

    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7

     inbound esp sas:
      spi: 0x99652AA9(2573544105)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (4341540/3401)

     outbound esp sas:
      spi: 0xAC4550FB(2890223867)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (4341538/3401)
```

12 Závěr

Cílem této diplomové práce bylo popsat využití technologie NAT-T se zaměřením na její použití ve virtuálních privátních sítích a ověření kompatibility mezi směrovači společnosti Huawei a Cisco. Pro jednotlivé VPN technologie byla navržena vhodná topologie obsahující zařízení uskutečňující NAT, nebo PAT. Zapojení daných topologií se uskutečnilo v laboratorních podmínkách, kde následně došlo k jejich konfiguraci a testování. K tomuto účelu byly v topologiích použity směrovače společnosti Huawei a Cisco, aby se ověřila jejich vzájemná kompatibilita. Konkrétně byly použity modely Huawei AR2200, Huawei AR3200, Cisco 2800 Series a Cisco 2900 Series.

V rámci práce byly implementovány následující VPN technologie: IPSec VPN, GRE over IPSec VPN, DMVPN/DSVPN s IPSec zabezpečením, L2TP over IPSec VPN, PPTP VPN a IPSec IKEv2 VPN. Jedná se tedy převážně o kombinace různých VPN technologií s technologií IPSec pro zajištění jejich bezpečnosti. Tato kombinace se použila také proto, že IPSec VPN je v současnosti převládající VPN technologie, jež je negativně ovlivněna překladem adres. Proto nejprve došlo k implementaci IPSec VPN a jejímu popisu. Kompatibilita mezi zařízeními společnosti Huawei a Cisco sice byla úspěšně otestována, ale docházelo zde k jistému problému. Pro účely technologie NAT-T bylo vyžadováno použití agresivního režimu v první IKE fázi spolu s identifikací prostřednictvím jména namísto IP adresy. Také bylo vyžadováno použití tunelovacího ESP módu. Tato kritéria jsou stanovena v dokumentaci společnosti Huawei. V případě splnění daných podmínek se již nevyskytovaly žádné jiné potíže a VPN byla úspěšně sestavena.

Konfigurace GRE over IPSec VPN vyžadovala pouze drobné změny oproti IPSec VPN a její funkce nejevila žádné potíže. Pochopitelně bylo nutné dodržet dříve zmíněné podmínky pro IPSec NAT-T. Ty bylo nutné dodržovat ve všech dalších technologiích využívajících IPSec. Za určitou evoluci této technologie lze považovat koncept DMVPN/DSVPN, který umožňuje dynamické vytváření tunelů mezi uzly typu spoke v hub-and-spoke topologii. Při konfiguraci technologie DSVPN je třeba upozornit na potřebu aktivace specifické licence pro danou technologii na směrovačích společnosti Huawei. Směrovač sice i bez aktivace umožní použití potřebných příkazů, ty však nebudou mít žádný efekt. U Cisco směrovačů není aktivace dodatečné licence nutná. Funkčnost této technologie byla otestována úspěšně. Nevýhodou ale byla nutnost použití ESP tunelovacího módu pro účely IPSec NAT-T. Pro DMVPN je standardně doporučováno použití transportního módu, jelikož tunelovací mód představuje nadbytečnou režii při již existujícím GRE zapouzdření.

V případě L2TP over IPSec VPN nebyly zaznamenány žádné potíže s kompatibilitou či funkčností a VPN tunel mezi LAC a LNS zařízením byl sestaven úspěšně. Autentizace metodou CHAP a technologie PPPoE také fungovala správně. Technologie PPTP VPN byla testována pouze na směrovačích Cisco. Použité směrovače společnosti Huawei tuto technologii nepodporují. Nebyla tedy ověřena kompatibila. Funkčnost na Cisco směrovačích byla otestována úspěšně. Také kompatibilita a funkčnost IPSec IKEv2 VPN byla ověřena úspěšně. Pochopitelně zde neplatí podmínka pro použití IKE agresivního režimu, jelikož ten již v IKEv2 neexistuje.

Závěrem lze tedy prohlásit, že při splnění definovaných podmínek jsou mezi sebou směrovače Cisco a Huawei kompatibilní v rámci všech testovaných VPN a NAT-T technologií, které jsou podporovány na zařízeních obou výrobců. Směrovače obou značek lze tedy společně využít v praxi za účelem zabezpečení komunikace a sestavení tunelů v síti. Tato práce proto může být prospěšná osobám, které se rozhodnou zařízení obou výrobců využít v praxi, nebo se zajímají o danou tématiku.

Budoucí vývoj mé práce lze zaměřit na testování technologie NAT-T u dalších platforem a zařízení jiných výrobců, případně také na analýzu technologie NAT-T mimo rámec VPN technologií.

Literatura

[1] LAMMLE, Todd. CCNA: výukový průvodce přípravou na zkoušku 640-802. Vyd. 1. Brno: Computer Press, 2010, 928 s. ISBN 978-802-5123-591.

[2] PAQUET, Catherine. Implementing Cisco IOS: network security (IINS). Vyd. 1. Indianapolis: Cisco Press, 2009, xix, 600 s. ISBN 978-1-58705-815-8.

[3] Cisco VPN: How Virtual Private Networks Work. [online]. [cit. 2016-6-3]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html#req

[4] Virtual Private Networks: Practical IPSec Operation. [online]. [cit. 2016-12-3]. Dostupné z: http://wh.cs.vsb.cz/sps/images/6/6b/VPN.pdf

[5] Think Like A Computer: PPTP Passthrough and How It Works. [online]. [cit. 2017-1-12]. Dostupné z: http://think-like-a-computer.com/2011/07/28/pptp-passthrough/

[6] MS TechNet: Address and Port Mapping for VPN Traffic. [online]. [cit. 2017-1-12]. Dostupné z: https://technet.microsoft.com/en-us/library/cc958044.aspx

[7] MS TechNet: VPN Tunneling Protocols. [online]. [cit. 2017-1-12]. Dostupné z: https://technet.microsoft.com/en-us/library/cc771298(v=ws.10).aspx

[8] HOOPER, Howard. CCNP security VPN 642-648 offical cert guide. Indianapolis, IN: Cisco Press, c2012. ISBN 1-58720-447-9.

[9] G. Dommety. RFC 2890: Key and Sequence Number Extensions to GRE. [online]. [cit. 2017-1-14]. Dostupné z: https://tools.ietf.org/html/rfc2890

[10] DMVPN: Using Multipoint GRE/NHRP to Scale IPsec VPNs. [online]. [cit. 2017-1-14]. Dostupné z: http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/41940-dmvpn.html

[11] DMVPN: Configuration Guide. [online]. [cit. 2017-1-18]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/12-4t/sec-conn-dmvpn-12-4t-book/sec-conn-dmvpn-dt-spokes-b-nat.html

[12] IP Diagnosis Guide. Traversing a NAT. [online]. [cit. 2017-2-3]. Dostupné z: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.hald001/travnat.htm

[13] Příkazy správy systému: tracepath. [online]. [cit. 2017-4-2]. Dostupné z: https://www.root.cz/man/8/tracepath/

[14] M. Stenberg, S. Paavolainen, T. Ylonen, T. Kivinen. RFC IPsec NAT-Traversal: draft-stenberg-ipsec-nat-traversal-02. [online]. [cit. 2017-4-2]. Dostupné z: https://tools.ietf.org/html/draft-stenberg-ipsec-nat-traversal-02

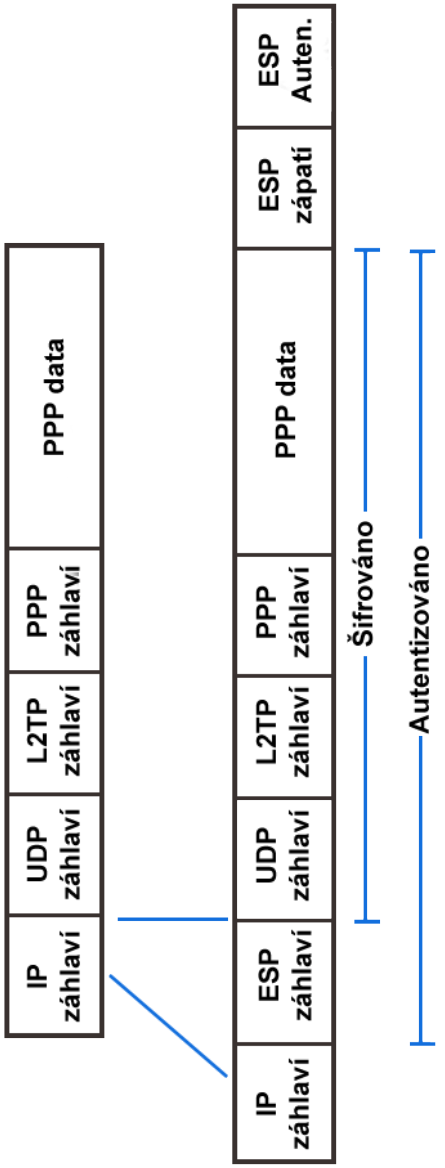
[15] Cisco Support Community: How Does NAT-T work with IPSec?. [online]. [cit. 2017-4-2]. Dostupné z: https://supportforums.cisco.com/document/64281/how-does-nat-t-work-ipsec

[16] Configuration Guide - VPN: IPSec Configuration. [online]. [cit. 2017-4-5]. Dostupné z: http://support.huawei.com/enterprise/docinforeader.action?contentId=DOC1000019452&partNo=100102

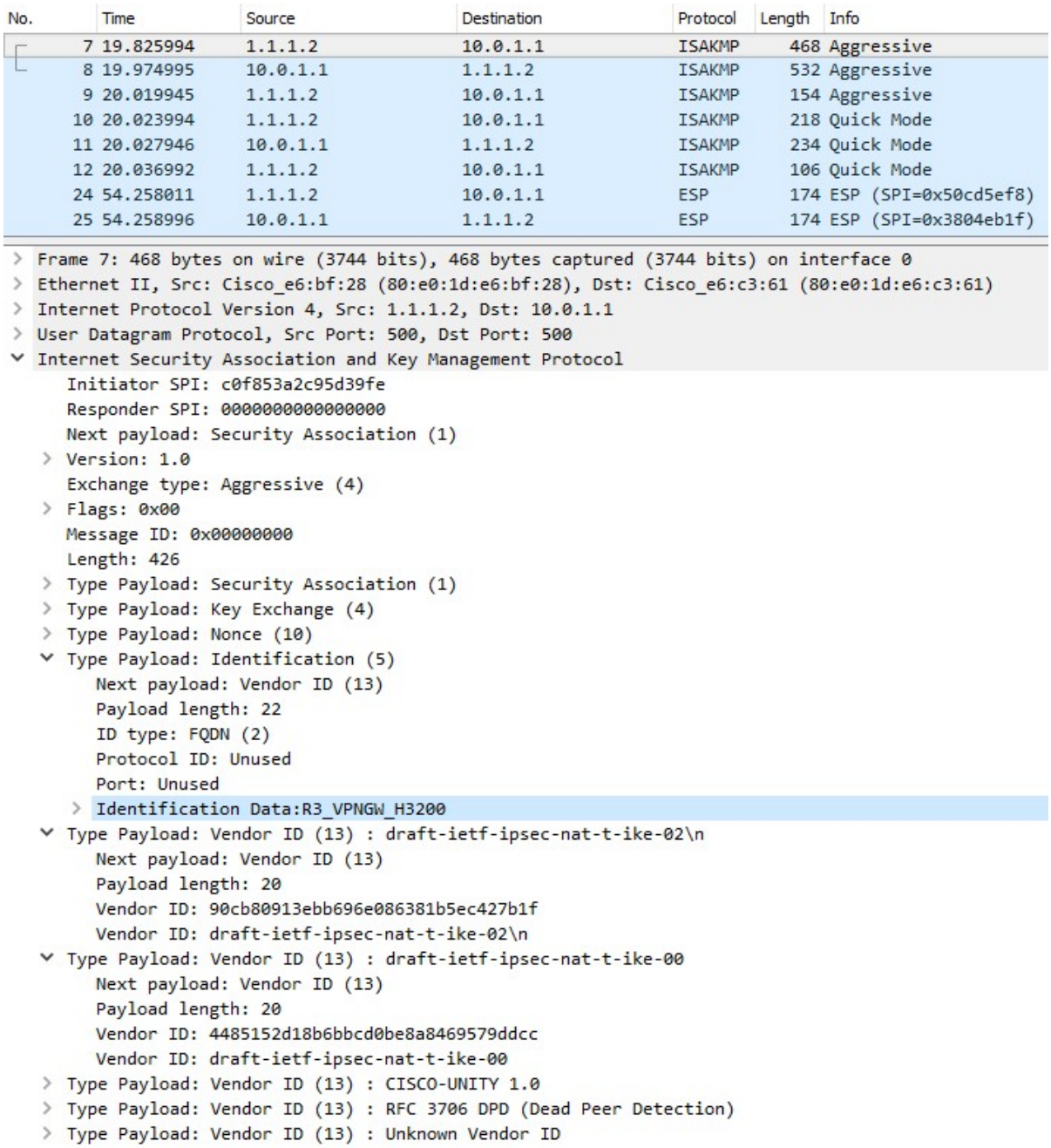
[17] Virtual Private Networks: Layer 2 Tunneling Protocol. [online]. [cit. 2017-4-9]. Dostupné z: http://docwiki.cisco.com/wiki/Virtual_Private_Networks

Seznam příloh

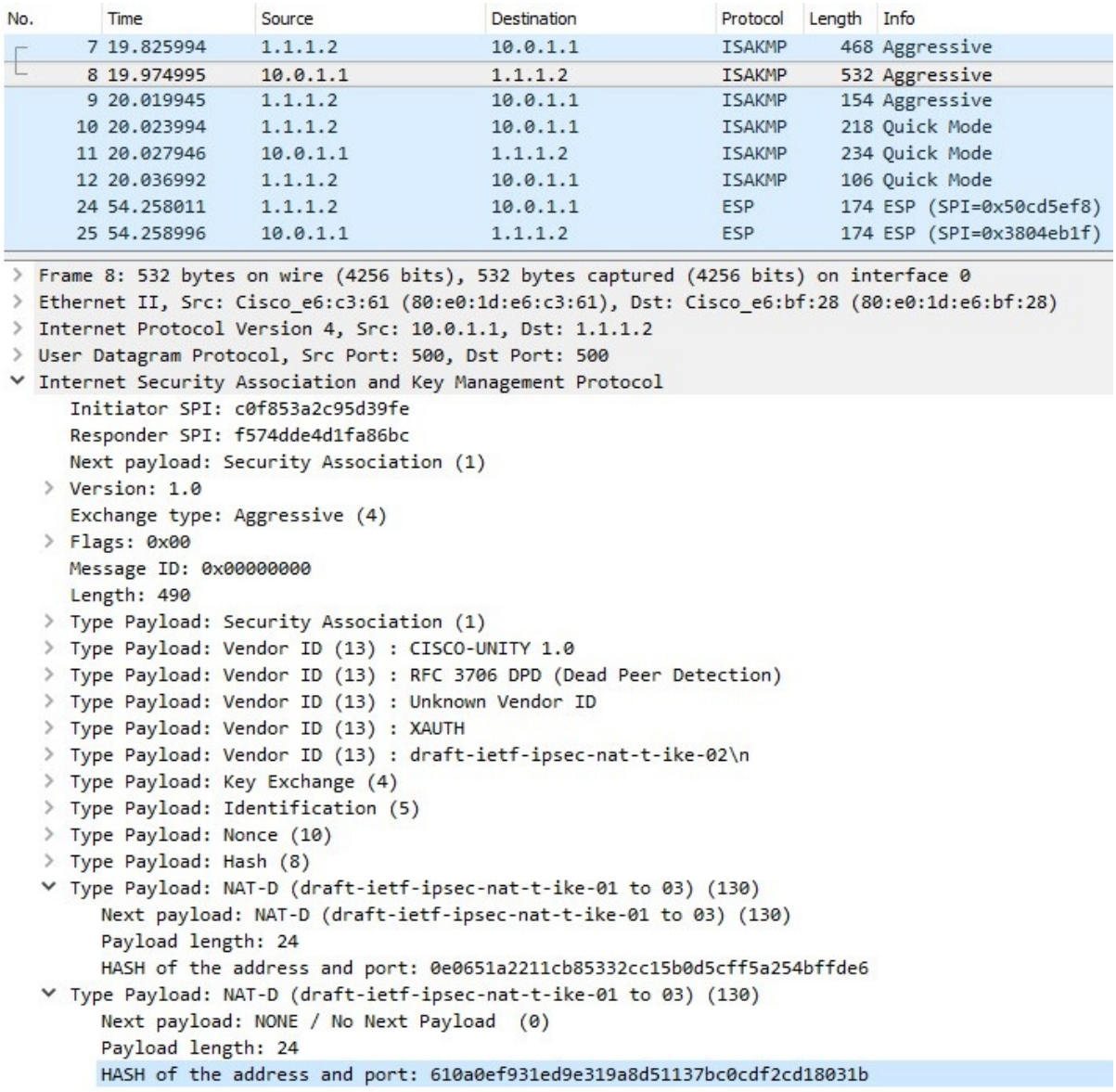
A Obrázky



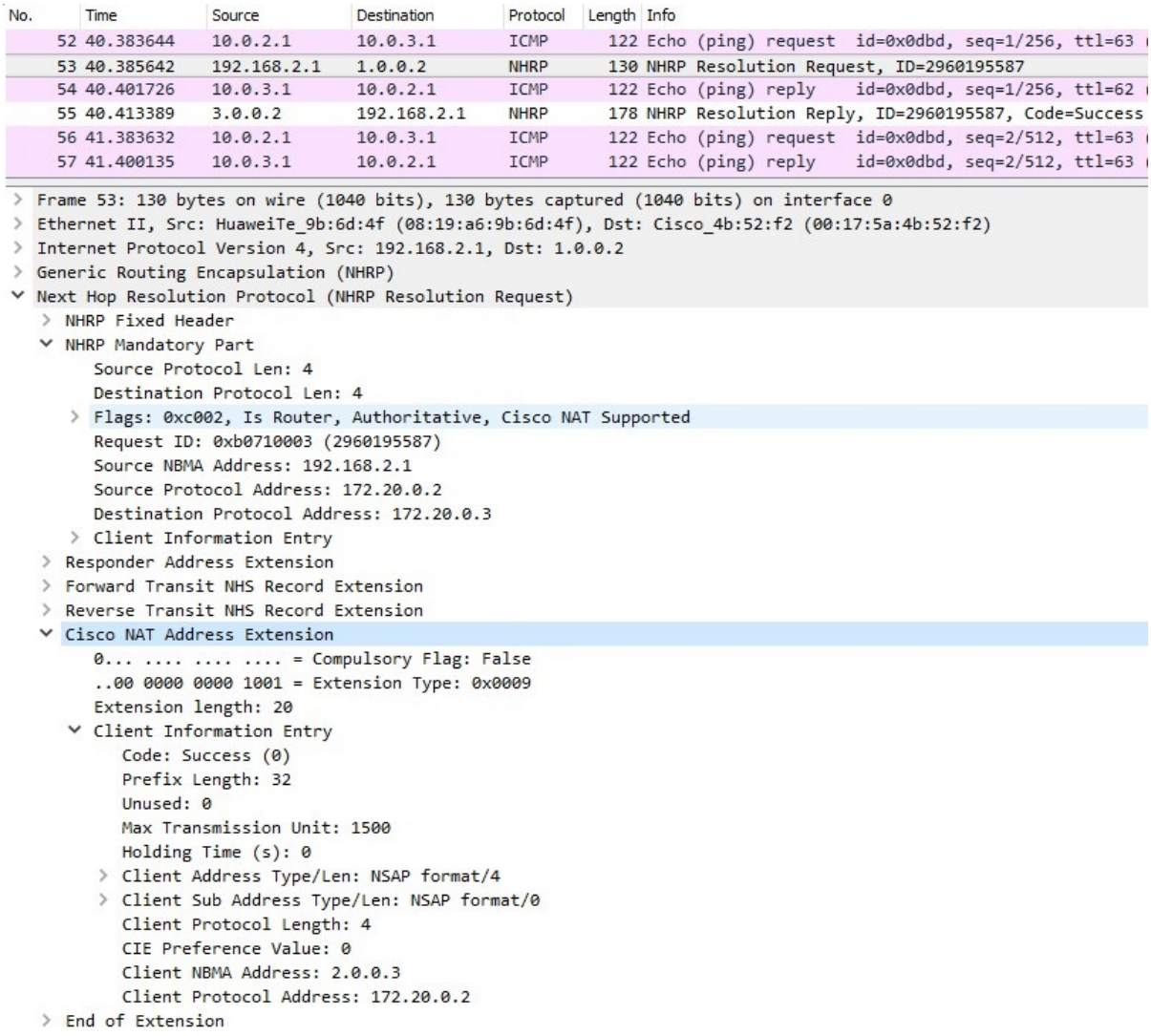
Obrázek A.1: Struktura zapouzdření dat v L2TP over IPSec VPN



Obrázek A.2: Odhalená identita VPN brány R3



Obrázek A.3: Haš IP adresy a portu pro účely technologie NAT-T



Obrázek A.4: Zpráva NRHP Resolution Request zachycená Marvinovou stanicí

B Konfigurace IPSec VPN topologie č. 2

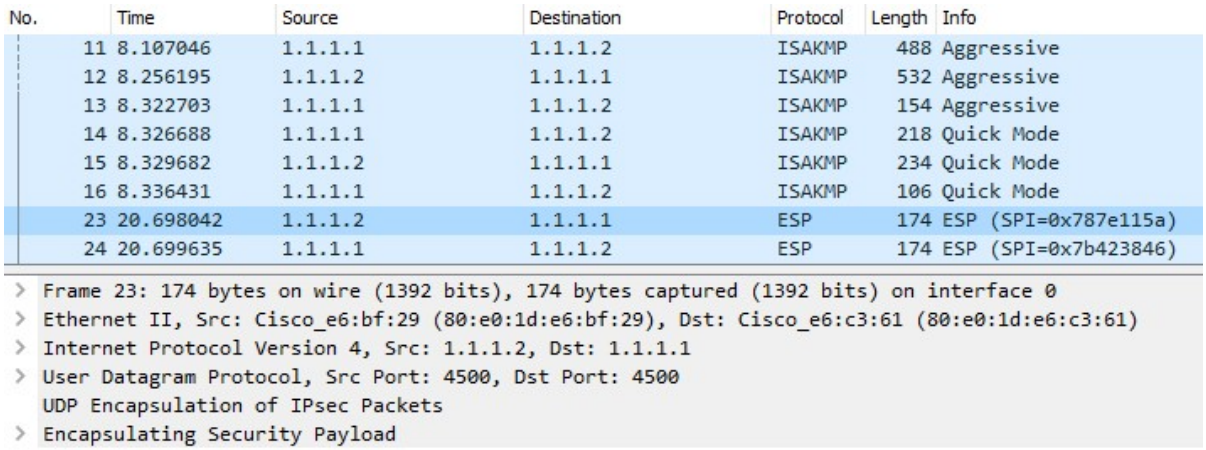
Tato topologie navazuje na původní IPSec VPN topologii. Došlo zde k záměně pozic mezi VPN branou R1 a R3. Také je směrovač Huawei AR3200 nahrazen modelem AR2200, aby byla otestována interoperabilita s větším počtem zařízení společnosti Huawei. Vzhledem k tomu, že konfigurace druhé topologie je obdobná té první, tak je v následující části uvedeno pouze ověření funkčnosti. Konfiguraci lze v případě potřeby nalézt v příloze G.

B.1 Ověření funkčnosti

Ověření funkčnosti IPSec VPN v topologii č. 2 je uskutečněno stejně jako v první topologii. Proto již nejsou následující výstupy detailně komentovány a jsou stručnější. Nejprve je zobrazen úspěšný test spojení prostřednictvím příkazu ping a poté výstup příkazu *show ip nat nvi translations*, který zobrazuje informace o překládaných adresách na směrovači R2_PAT_C2900. Z něj lze vyčíst, že docházelo k překladu IP adresy 10.0.1.1 na adresu 1.1.1.1. Rovněž jsou zde zobrazeny statické NAT záznamy pro UDP port 500 a 4500.

```
Bob@eb215-desktop:/home/student# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=62 time=2.31 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=62 time=1.98 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=62 time=2.09 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.987/2.131/2.317/0.147 ms

R2_PAT_C2900#show ip nat nvi translations
Pro Source global    Source local     Destin local     Destin global
udp 1.1.1.1:500      10.0.1.1:500     1.1.1.2:500      1.1.1.2:500
udp 1.1.1.1:500      10.0.1.1:500     ---              ---
udp 1.1.1.1:4500     10.0.1.1:4500    1.1.1.2:4500     1.1.1.2:4500
udp 1.1.1.1:4500     10.0.1.1:4500    ---              ---
```

Níže na obrázku č. B.1 lze vidět zprávy zachycené aplikací Wireshark. Přenášená data byla zabezpečena protokolem ESP a zapouzdřena protokolem UDP umožňujícím NAT traversal. Následně je vyobrazen výstup příkazů *show crypto ipsec sa* a *display ipsec sa* pro kontrolu vlastností tunelu.



Obrázek B.1: Ukázka sestavení IKE/IPSec SA a zapouzdření paketů

```
R3_VPNGW_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/1
    Crypto map tag: CM, local addr 1.1.1.2

   local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   current_peer 1.1.1.1 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 35, #pkts encrypt: 35, #pkts digest: 35
    #pkts decaps: 35, #pkts decrypt: 35, #pkts verify: 35

     inbound esp sas:
      spi: 0x7B423846(2067937350)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1735564/3475)

     outbound esp sas:
      spi: 0x787E115A(2021527898)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1735564/3475)
```

```
<R1_VPNGW_H2200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: GigabitEthernet0/0/1
===============================

  -----------------------------
  IPSec policy name: "myIPSecPolicy"
  Sequence number : 10
    Encapsulation mode: Tunnel
    Tunnel local     : 10.0.1.1
    Tunnel remote    : 1.1.1.2
    Flow source      : 10.0.0.0/255.255.255.0 0/0
    Flow destination : 2.2.2.0/255.255.255.0 0/0

    [Outbound ESP SAs]
      SPI: 2067937350 (0x7b423846)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436296/3396
      UDP encapsulation used for NAT traversal: Y

    [Inbound ESP SAs]
      SPI: 2021527898 (0x787e115a)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436296/3396
      UDP encapsulation used for NAT traversal: Y
```

C Konfigurace GRE over IPSec VPN topologie č. 2

V druhé topologii byla pouze uskutečněna záměna pozic mezi VPN branou R1 a R3. Rovněž je směrovač Huawei AR3200 nahrazen modelem AR2200. Princip konfigurace druhé topologie se neliší od té první, proto nevyžaduje komentář a veškeré konfigurace jsou uvedeny v příloze H.

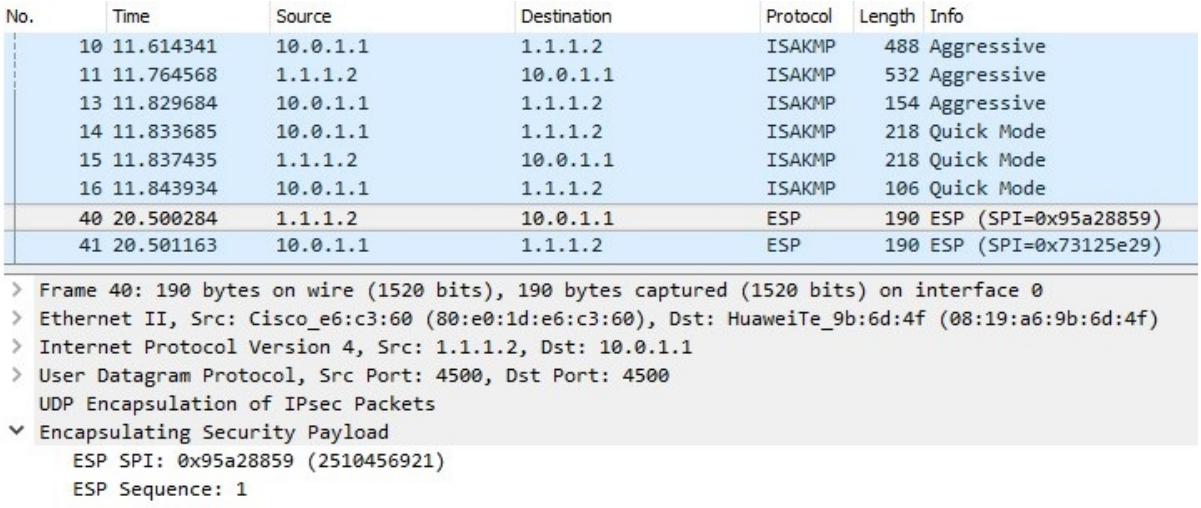
C.1 Ověření funkčnosti

V této topologii byl nejprve vygenerován datový provoz příkazem ping. Následně byla příkazem *show ip nat nvi translations* ověřena správně nakonfigurovaná tabulka překladu adres a na obr. č. C.1 je zobrazena zabezpečená komunikace spolu s využitím technologie NAT traversal. Vlastnosti tunelu jsou vypsány ve výstupech příkazů *show crypto ipsec sa* a *display ipsec sa*.

```
Bob@eb215-desktop:/home/student# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=62 time=2.51 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=62 time=2.19 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=62 time=1.97 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.970/2.228/2.518/0.224 ms

R2_PAT_C2900#show ip nat nvi translations
Pro Source global    Source local     Destin local     Destin global
udp 1.1.1.1:500      10.0.1.1:500     1.1.1.2:500      1.1.1.2:500
udp 1.1.1.1:500      10.0.1.1:500     ---              ---
udp 1.1.1.1:4500     10.0.1.1:4500    1.1.1.2:4500     1.1.1.2:4500
udp 1.1.1.1:4500     10.0.1.1:4500    ---              ---

R3_VPNGW_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/1
    Crypto map tag: CM, local addr 1.1.1.2

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (1.1.1.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port):
      (10.0.1.1/255.255.255.255/47/0)
```

```
  current_peer 1.1.1.1 port 4500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 11, #pkts encrypt: 11, #pkts digest: 11
   #pkts decaps: 11, #pkts decrypt: 11, #pkts verify: 11

    inbound esp sas:
     spi: 0x73125E29(1930583593)
       transform: esp-256-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       sa timing: remaining key lifetime (k/sec): (1687075/3504)

    outbound esp sas:
     spi: 0x95A28859(2510456921)
       transform: esp-256-aes esp-sha-hmac ,
       in use settings ={Tunnel UDP-Encaps, }
       sa timing: remaining key lifetime (k/sec): (1687075/3504)


<R1_VPNGW_H2200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: GigabitEthernet0/0/1
===============================
  IPSec policy name: "myIPSecPolicy"
  Sequence number : 10

    Encapsulation mode: Tunnel
    Tunnel local    : 10.0.1.1
    Tunnel remote   : 1.1.1.2
    Flow source     : 10.0.1.1/255.255.255.255 47/0
    Flow destination : 1.1.1.2/255.255.255.255 47/0

    [Outbound ESP SAs]
      SPI: 1930583593 (0x73125e29)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887436152/3439
      UDP encapsulation used for NAT traversal: Y
```

```
[Inbound ESP SAs]
  SPI: 2510456921 (0x95a28859)
  Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
  SA remaining key duration (bytes/sec): 1887436152/3439
  UDP encapsulation used for NAT traversal: Y
```



Obrázek C.1: Data zachycená Marvinovou stanicí

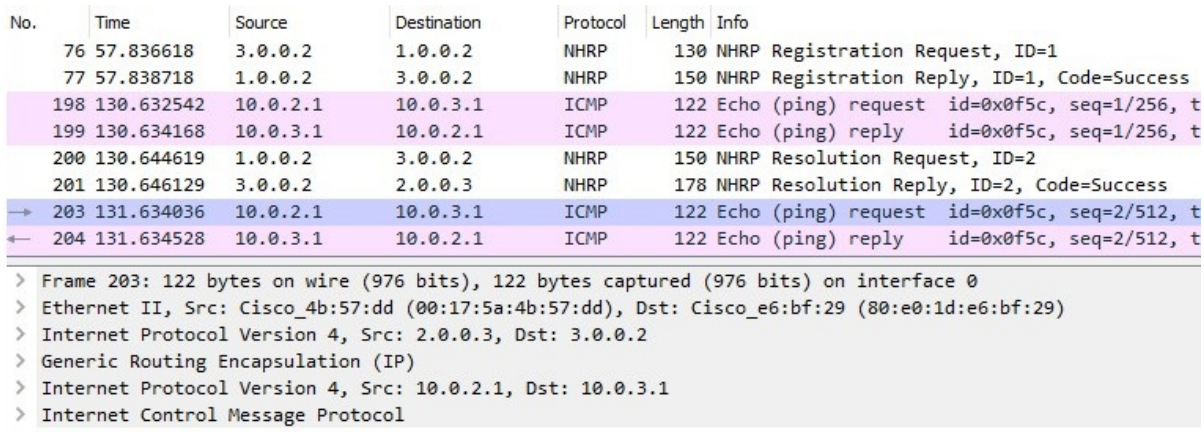
D Konfigurace DMVPN VPN topologie č. 2

V topologii došlo k nahrazení směrovače Huawei AR2200 směrovačem Huawei AR3200 a výměně pozic mezi směrovačem R1 a R4. Platforma Huawei AR3200 je proto nyní v pozici centrály a naopak směrovač Cisco 2900 Series představuje pobočkovoou VPN bránu. Konfigurace směrovače R2_INTER_C2800 a R3_NAT_C2800 je nepozměněna vůči původní topologii. Také konfigurace VPN brán zůstala z pohledu principu funkce shodná, pouze došlo k záměně platforem, proto jsou zde mírné syntaktické rozdíly v konfiguraci. Konfigurace lze nalézt v příloze I.

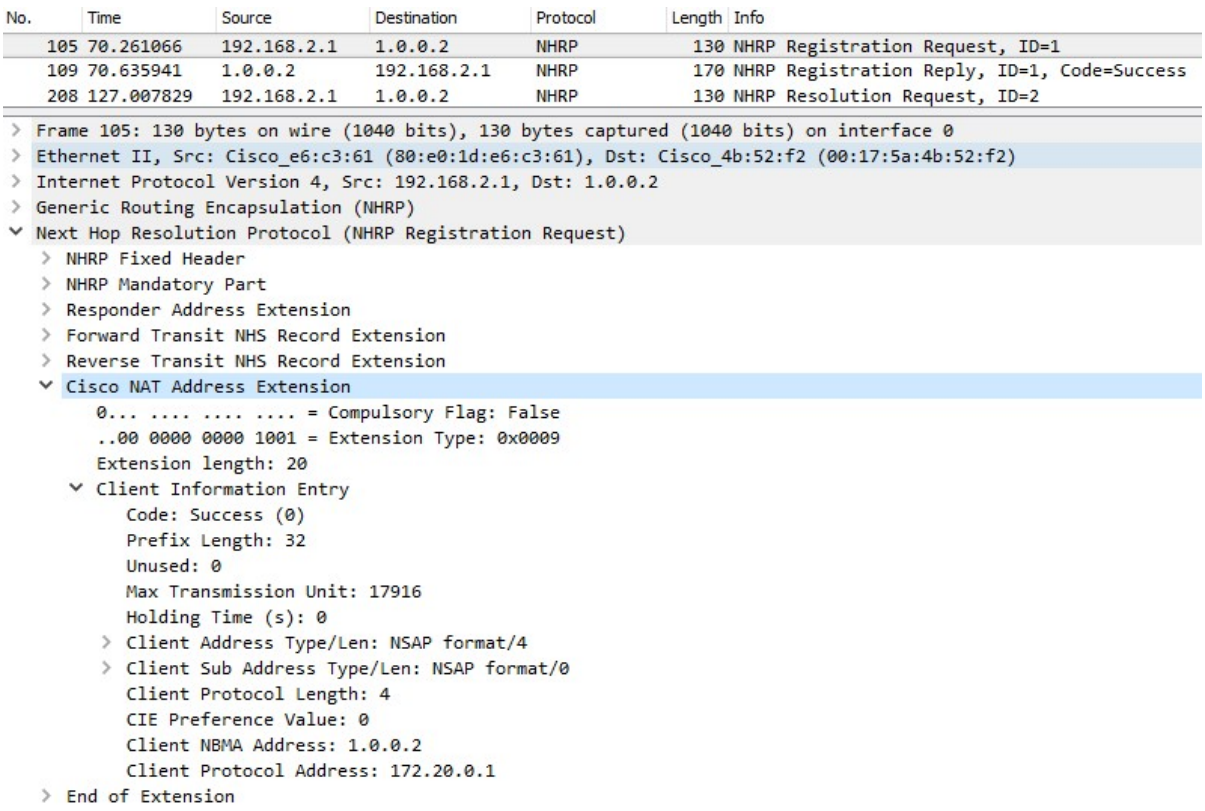
D.1 Ověření funkčnosti

Předně došlo ke spuštění příkazů ping a tracepath pro vygenerování datového provozu. Poté byla ověřena data zachycená aplikací Wireshark. Jak lze vypozorovat z obrázku č. D.1, docházelo zde nejprve k registraci pobočky na ústřednu prostřednictvím protokolu NHRP. Poté byla odeslána zpráva ICMP Echo Requst, která nejprve procházela skrz centrální směrovač, který vykonával službu prostředníka. Následně byl odeslán NHRP požadavek z jehož odpovědi se směrovač dozvěděl informace potřebné k asociaci mezi NBMA adresou a adresou použitou pro tunelové rozhraní. Dále již byly zprávy směrovány bez prostředníka, jak lze vidět na zmíněném obrázku. Na obrázku č. D.2 lze také vidět NHRP zprávu Registration Request obsahující rozšíření pro NAT. Součástí této zprávy je informace o logické IP adrese tunelu centrálního směrovače, ale také je zde obsažena jeho skutečná NBMA adresa, pod kterou je znám směrovači R4.

```
Alice@eb215-desktop:/home/student# tracepath 10.0.3.1
 1?: [LOCALHOST]                                      pmtu 1500
 1:  10.0.2.254                                         0.362ms
 1:  10.0.2.254                                         0.286ms
 2:  10.0.2.254                                         0.279ms pmtu 1476
 2:  172.20.0.3                                       106.750ms
 3:  10.0.3.1                                         141.226ms reached
     Resume: pmtu 1476 hops 3 back 3
```



Obrázek D.1: Data zachycená stanicí Eve v DMVPN topologii č. 2



Obrázek D.2: Zpráva Registration Request zachycená Marvinovou stanicí

Správně vytvořené NHRP asociace byly ověřeny následujícími příkazy.

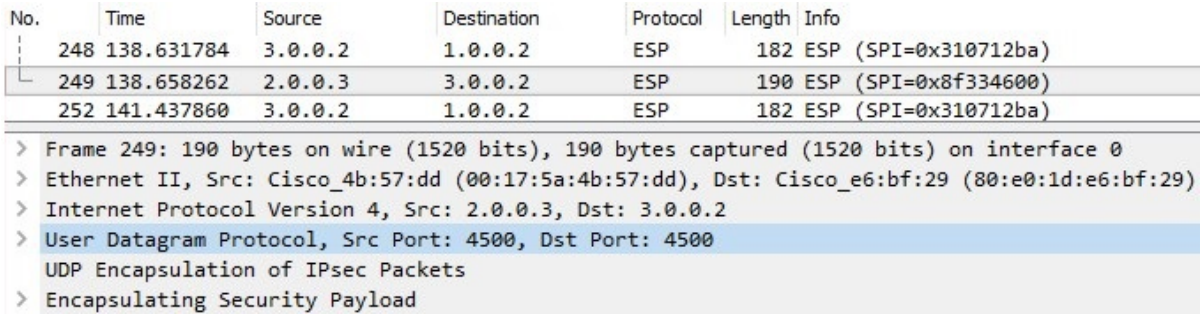
```
R4_SPOKE1_C2900#show dmvpn
!Pro zachování stručnosti byl výstup částečně zkrácen!

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
# Ent  Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- -------------- --------------- ---- -------- ----
     1 1.0.0.2          172.20.0.1    UP   00:06:39    S
     1 3.0.0.2          172.20.0.3    UP   00:05:43    D


R5_SPOKE2_C2900#show dmvpn
!Pro zachování stručnosti byl výstup částečně zkrácen!

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
       N - NATed, L - Local, X - No Socket
 # Ent  Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- -------------- --------------- ---- -------- ----
     1 1.0.0.2          172.20.0.1    UP   00:07:46    S
     1 2.0.0.3          172.20.0.2    UP   00:06:33   DN
```

Také byla ověřena správná funkce OSPF protokolu a skutečnost, že pobočkové sítě jsou dosažitelné přes tunelové rozhraní.

```
R5_SPOKE2_C2900#show ip route
!Pro zachování stručnosti byl výstup částečně zkrácen!

Codes: L - local, C - connected, O - OSPF, IA - OSPF inter area
O IA    10.0.1.0/24 [110/1001] via 172.20.0.1, 00:07:24, Tunnel0
O       10.0.2.0/24 [110/1001] via 172.20.0.2, 00:07:24, Tunnel0
C       172.20.0.0/24 is directly connected, Tunnel0
L       172.20.0.3/32 is directly connected, Tunnel0
```

Posledním krokem bylo aplikování IPSec profilu na rozhraní, čímž bylo zajištěno zabezpečení dat přenášných VPN tunelem. Po aplikaci IPSec profilu na rozhraní bylo spojení otestováno příkazem ping mezi Alicí a Bobem. Ná obrázku č. D.3 lze vidět, že data byla šifrována a úspěšně zapouzdřena do UDP protokolu využívajícího port 4500 pro NAT-T.

Vlastnosti nakonfigurovaného IPSec SA lze ověřit např. příkazem *display ipsec sa* na centrále R1_HUB_H3200.



Obrázek D.3: Zabezpečená data technologií IPSec zachycená stanicí Eve

```
<R1_HUB_H3200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: Tunnel0/0/0
===============================

  -------------------------------
  IPSec profile name: "MyProfile"
  Mode              : PROF-Template
  -------------------------------
    Connection ID    : 6
    Encapsulation mode: Tunnel
    Tunnel local     : 1.0.0.2
    Tunnel remote    : 3.0.0.2

    [Outbound ESP SAs]
      SPI: 3812335967 (0xe33ba15f)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887428380/2904
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
      SPI: 822547130 (0x310712ba)
      Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
      SA remaining key duration (bytes/sec): 1887426360/2904
      UDP encapsulation used for NAT traversal: N
```

```
------------------------------
IPSec profile name: "MyProfile"
Mode            : PROF-Template
------------------------------
  Connection ID   : 5
  Encapsulation mode: Tunnel
  Tunnel local    : 1.0.0.2
  Tunnel remote   : 2.0.0.3

  [Outbound ESP SAs]
    SPI: 2921127375 (0xae1cddcf)
    Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
    SA remaining key duration (bytes/sec): 1887426400/2896
    UDP encapsulation used for NAT traversal: Y

  [Inbound ESP SAs]
    SPI: 4177025026 (0xf8f85802)
    Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
    SA remaining key duration (bytes/sec): 1887426028/2896
    UDP encapsulation used for NAT traversal: Y
```

E Konfigurace L2TP over IPSec VPN topologie č. 2

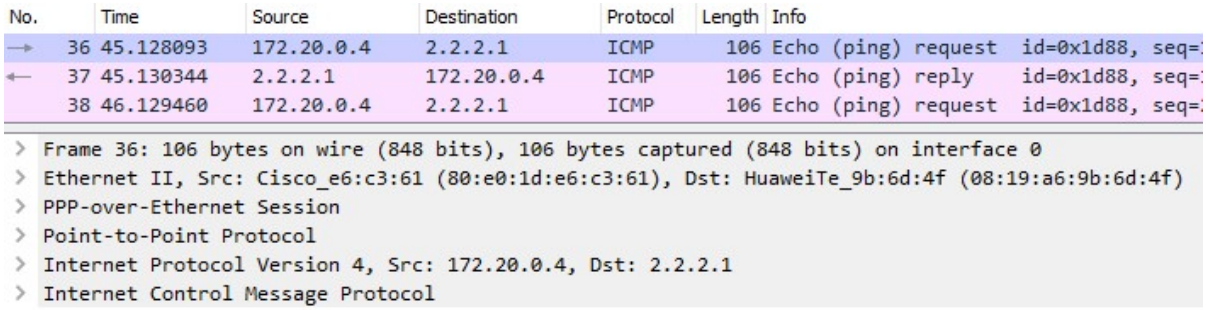
Druhá topologie byla změněna výměnou směrovače R2 za směrovač R4 a obráceně. Také byla zaměněna platforma Huawei AR3200 za AR2200. Konfigurace byla upravena pouze na směrovačích R2 a R4. Na směrovačích R1 a R2 dochází pouze ke změně popisu rozhraní. V případě potřeby je konfigurace uvedena v příloze J.

E.1 Ověření funkčnosti

Nejprve došlo k vytvoření datového provozu příkazy ping a tracepath z koncové stanice uživatele Alice. Zde vypadá opět vše v pořádku.

```
Alice@eb215-desktop:/home/student# tracepath 2.2.2.1
 1?: [LOCALHOST]                                         pmtu 1500
 1:  10.0.0.254                                            0.640ms
 1:  10.0.0.254                                            0.503ms
 2:  2.2.2.1                                               3.008ms pmtu 1492
 2:  2.2.2.1                                             113.570ms reached
     Resume: pmtu 1492 hops 2 back 3
```

Z obrázku č. E.1. je viditelné, že klient správně obdržel IP adresu z adresního prostoru MyPool, který je definován rozsahem IP adres 172.20.0.2 - 172.20.0.254.



Obrázek E.1: Komunikace zachycená Marvinovou stanicí v L2TP over IPSec topologii č. 2

Úspěšné vytvoření IPSec VPN spolu se zapouzdřením technologií NAT-T je pak možné spatřit na obrázku č. E.2. Vzhledem k tomu, že byla L2TP VPN překrytá technologí IPSec VPN, tak je také ověřeno sestavené L2TP spojení příkazy *display l2tp tunnel* a *show vpdn tunnel l2tp*.

```
<R2_LAC_H2200>display l2tp tunnel
Total tunnel : 1
LocalTID RemoteTID RemoteAddress Port  Sessions RemoteName
1         9944     1.1.1.2       1701  1        R4_LNS_C2900


R4_LNS_C2900#show vpdn tunnel l2tp
L2TP Tunnel Information Total tunnels 1 sessions 1
LocTunID RemTunID Remote Name State Remote Address Sessn L2TP Class/
                                                    Count VPDN Group
9944     1         LAC         est    10.0.2.1       1     MyVpdnGroup
```

No.	Time	Source	Destination	Protocol	Length	Info
17	11.690146	1.1.1.1	1.1.1.2	ISAKMP	486	Aggressive
18	11.836720	1.1.1.2	1.1.1.1	ISAKMP	530	Aggressive
19	11.883327	1.1.1.1	1.1.1.2	ISAKMP	154	Aggressive
20	11.887301	1.1.1.1	1.1.1.2	ISAKMP	218	Quick Mode
21	11.890130	1.1.1.2	1.1.1.1	ISAKMP	218	Quick Mode
22	11.894644	1.1.1.1	1.1.1.2	ISAKMP	106	Quick Mode
30	33.558332	1.1.1.1	1.1.1.2	ESP	206	ESP (SPI=0x22f7a591)
31	33.560729	1.1.1.2	1.1.1.1	ESP	270	ESP (SPI=0x416b0e93)

```
> Frame 30: 206 bytes on wire (1648 bits), 206 bytes captured (1648 bits) on interface 0
> Ethernet II, Src: Cisco_4b:52:f3 (00:17:5a:4b:52:f3), Dst: Cisco_e6:bf:29 (80:e0:1d:e6:bf:29)
> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 1.1.1.2
> User Datagram Protocol, Src Port: 4500, Dst Port: 4500
  UDP Encapsulation of IPsec Packets
v Encapsulating Security Payload
    ESP SPI: 0x22f7a591 (586655121)
    ESP Sequence: 1
```

Obrázek E.2: Sestavení IKE/IPSec SA a zapouzdření paketů v L2TP over IPSec topologii č. 2

K účelu ověření detailních informací o sestavené IPSec VPN síti lze opět využít výstup příkazu *show crypto ipsec sa*, případně pro zobrazení souhrnných informací je možné použít výstup příkazu *display ipsec sa brief*.

```
R4_LNS_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/1
    Crypto map tag: CM, local addr 1.1.1.2

   local  ident (addr/mask/prot/port):
      (1.1.1.2/255.255.255.255/17/1701)
   remote ident (addr/mask/prot/port):
      (10.0.2.1/255.255.255.255/17/1701)
   current_peer 1.1.1.1 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 91, #pkts encrypt: 91, #pkts digest: 91
    #pkts decaps: 91, #pkts decrypt: 91, #pkts verify: 91

     inbound esp sas:
      spi: 0x22F7A591(586655121)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1736041/3218)

     outbound esp sas:
      spi: 0x416B0E93(1097535123)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (1736043/3218)

<R2_LAC_H2200>display ipsec sa brief
Number of SAs:2
    Src address Dst address  SPI    VPN  Protocol Algorithm
-------------------------------------------------------------------
      1.1.1.2 10.0.2.1 1097535123    0   ESP  E:AES-256 A:SHA1-96
     10.0.2.1  1.1.1.2  586655121    0   ESP  E:AES-256 A:SHA1-96
```

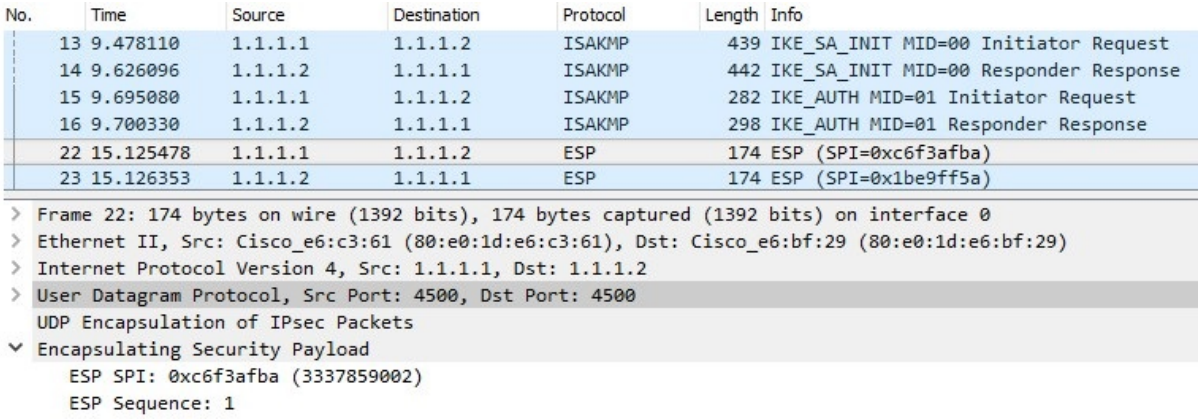
F Konfigurace IPSec IKEv2 VPN topologie č. 2

V druhé topologii došlo k záměně pozic mezi směrovačem R1 a R3. Rovněž je platorma Huawei AR3200 nahrazena modelem AR2200. Konfigurace jsou uvedeny v příloze L.

F.1 Ověření funkčnosti

Pro ověření funkčnosti druhé topologie byl nejprve taktéž využit příkaz ping. Z obrázku č. F.1 je zřejmé, že IP adresa VPN brány R1 byla úspěšně překládána na adresu 1.1.1.1 a komunikace byla správně zabezpečena protokolem ESP a zapouzdřena do UDP záhlaví pro funkci NAT-T.

```
Bob@eb215-desktop:/home/student# ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=62 time=2.19 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=62 time=2.01 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=62 time=1.98 ms
^C
--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 1.986/2.066/2.195/0.099 ms
```



Obrázek F.1: Zachycená komunikace v IPSec IKEv2 VPN síti

Pro účely ověření vlastností vytvořené IPSec bezpečností asociace byly použity příkazy *show crypto ipsec sa* a *display ipsec sa*. Z výstupu lze vidět, že docházelo k zabezpečení komunikace mezi sítěmi 2.2.2.0/24 a 10.0.0.0/24. Pro komunikaci byl použit UDP port 4500. Byla tedy využita funkce NAT-T. To dokazuje také fráze "in use settings =Tunnel UDP-Encaps". Dále lze z výstupu zjistit použití protokolu ESP, šifrování protokolem AES-256 a integritu s autentizací poskytovala funkce HMAC využívající algoritmus SHA. Také lze např. vidět index SPI prostřednictvím kterého VPN brány identifikují, kterou bezpečnostní asociaci použít pro danou komunikaci.

```
R3_VPNGW_C2900#show crypto ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

interface: GigabitEthernet0/1
    Crypto map tag: CM, local addr 1.1.1.2

   local ident (addr/mask/prot/port): (2.2.2.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   current_peer 1.1.1.1 port 4500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 3, #pkts decrypt: 3, #pkts verify: 3

     inbound esp sas:
      spi: 0xC6F3AFBA(3337859002)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (4332366/3537)

     outbound esp sas:
      spi: 0x1BE9FF5A(468320090)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        sa timing: remaining key lifetime (k/sec): (4332366/3537)


<R1_VPNGW_H2200>display ipsec sa
!Pro zachování stručnosti byl výstup částečně zkrácen!

===============================
Interface: GigabitEthernet0/0/1
===============================
  -----------------------------
  IPSec policy name: "myIPSecPolicy"
  Sequence number : 10
  -----------------------------
    Encapsulation mode: Tunnel
    Tunnel local    : 10.0.1.1
    Tunnel remote   : 1.1.1.2
```

```
Flow source      : 10.0.0.0/255.255.255.0 0/0
Flow destination : 2.2.2.0/255.255.255.0 0/0

[Outbound ESP SAs]
  SPI: 3337859002 (0xc6f3afba)
  Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
  SA remaining key duration (bytes/sec): 1887436548/3450
  UDP encapsulation used for NAT traversal: Y

[Inbound ESP SAs]
  SPI: 468320090 (0x1be9ff5a)
  Proposal: ESP-ENCRYPT-AES-256 ESP-AUTH-SHA1
  SA remaining key duration (bytes/sec): 1887436548/3450
  UDP encapsulation used for NAT traversal: Y
```

G Zkrácená konfigurace IPSec VPN

G.1 Konfigurace směrovače R1_VPNGW_C2900

```
hostname R1_VPNGW_C2900
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp identity hostname
!
crypto isakmp peer address
   1.1.1.2
 set aggressive-mode password
    letMeIn
 set aggressive-mode client-
    endpoint fqdn R1_VPNGW_C2900
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.2
 set transform-set 20
 match address 111
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R2_PAT_C2900
 ip address 10.0.1.1
    255.255.255.252
 crypto map CM
!
ip route 0.0.0.0 0.0.0.0 10.0.1.2
!
access-list 111 remark IPSec_ACL
access-list 111 permit ip
   10.0.0.0 0.0.0.255 2.2.2.0
   0.0.0.255
```

G.2 Konfigurace směrovače R2_PAT_C2900

```
hostname R2_PAT_C2900
!
interface GigabitEthernet0/0
 description TO_R1_VPNGW_C2900
 ip address 10.0.1.2
    255.255.255.252
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R3_VPNGW_H3200
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip nat source list 1 interface
   GigabitEthernet0/1 overload
ip nat source static udp 10.0.1.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.1.1
    4500 1.1.1.1 4500 extendable
ip route 0.0.0.0 0.0.0.0 1.1.1.2
ip route 10.0.0.0 255.255.255.0
   10.0.1.1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

G.3 Konfigurace směrovače R3_VPNGW_H3200

```
 sysname R3_VPNGW_H3200
#
 ike local-name R3_VPNGW_H3200
#
acl number 3000
 description IPSec_ACL
 rule 10 permit ip source 2.2.2.0
     0.0.0.255 destination
    10.0.0.0 0.0.0.255
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R1_VPNGW_C2900
 nat traversal
 remote-address 1.1.1.1
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description TO_R2_PAT_C2900
 ip address 1.1.1.2
    255.255.255.252
 ipsec policy myIPSecPolicy
#
ip route-static 0.0.0.0 0.0.0.0
   1.1.1.1
```

G.4 Topologie č. 2: Konfigurace směrovače R1_VPNGW_H2200

```
 sysname R1_VPNGW_H2200
#
 ike local-name R1_VPNGW_H2200
#
 acl number 3000
 description IPSec ACL
 rule 10 permit ip source
    10.0.0.0 0.0.0.255
    destination 2.2.2.0 0.0.0.255
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R3_VPNGW_C2900
 nat traversal
 remote-address 1.1.1.2
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description TO_R2_PAT_C2900
 ip address 10.0.1.1
    255.255.255.252
 ipsec policy myIPSecPolicy
#
ip route-static 0.0.0.0 0.0.0.0
   10.0.1.2
```

G.5 Topologie č. 2: Konfigurace směrovače R2_PAT_C2900

```
hostname R2_PAT_C2900
!
interface GigabitEthernet0/0
 description TO_R1_VPNGW_H2200
 ip address 10.0.1.2
    255.255.255.252
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R3_VPNGW_C2900
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip nat source list 1 interface
   GigabitEthernet0/1 overload
ip nat source static udp 10.0.1.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.1.1
    4500 1.1.1.1 4500 extendable
ip route 0.0.0.0 0.0.0.0 1.1.1.2
ip route 10.0.0.0 255.255.255.0
   10.0.1.1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

G.6 Topologie č. 2: Konfigurace směrovače R3_VPNGW_C2900

```
hostname R3_VPNGW_C2900
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp identity hostname
!
crypto isakmp peer address
   1.1.1.1
 set aggressive-mode password
    letMeIn
 set aggressive-mode client-
    endpoint fqdn R3_VPNGW_C2900
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set 20
 match address 111
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R2_PAT_C2900
 ip address 1.1.1.2
    255.255.255.252
 crypto map CM
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
!
access-list 111 remark IPSec_ACL
access-list 111 permit ip 2.2.2.0
    0.0.0.255 10.0.0.0 0.0.0.255
```

H Zkrácená konfigurace GRE over IPSec VPN

H.1 Konfigurace směrovače R1_VPNGW_C2900

```
hostname R1_VPNGW_C2900
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp identity hostname
!
crypto isakmp peer address
   1.1.1.2
 set aggressive-mode password
    letMeIn
 set aggressive-mode client-
    endpoint fqdn R1_VPNGW_C2900
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.2
 set transform-set 20
 match address 111
!
interface Tunnel0
 ip address 172.16.0.1
    255.255.255.252
 ip mtu 1400
 tunnel source GigabitEthernet0/1
 tunnel destination 1.1.1.2
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R2_PAT_C2900
 ip address 10.0.1.1
    255.255.255.252
 crypto map CM
!
ip route 0.0.0.0 0.0.0.0 10.0.1.2
ip route 2.2.2.0 255.255.255.0
   Tunnel0
!
access-list 111 remark IPSec_ACL
access-list 111 permit gre host
   10.0.1.1 host 1.1.1.2
```

H.2 Konfigurace směrovače R2_PAT_C2900

```
hostname R2_PAT_C2900
!
interface GigabitEthernet0/0
 description TO_R1_VPNGW_C2900
 ip address 10.0.1.2
    255.255.255.252
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R3_VPNGW_H3200
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip nat source list 1 interface
   GigabitEthernet0/1 overload
ip nat source static udp 10.0.1.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.1.1
    4500 1.1.1.1 4500 extendable
ip route 0.0.0.0 0.0.0.0 1.1.1.2
ip route 10.0.0.0 255.255.255.0
   10.0.1.1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

H.3 Konfigurace směrovače R3_VPNGW_H3200

```
 sysname R3_VPNGW_H3200
#
 ike local-name R3_VPNGW_H3200
#
acl number 3000
 description IPSec ACL
 rule 10 permit gre source
    1.1.1.2 0 destination
    10.0.1.1 0
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R1_VPNGW_C2900
 nat traversal
 remote-address 1.1.1.1
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description TO_R2_PAT_C2900
 ip address 1.1.1.2
    255.255.255.252
 ipsec policy myIPSecPolicy
#
interface Tunnel0/0/1
 ip address 172.16.0.2
    255.255.255.252
 mtu 1400
 tunnel-protocol gre
 source 1.1.1.2
 destination 10.0.1.1
#
ip route-static 0.0.0.0 0.0.0.0
   1.1.1.1
ip route-static 10.0.0.0
   255.255.255.0 Tunnel0/0/1
```

H.4 Topologie č. 2: Konfigurace směrovače R1_VPNGW_H2200

```
 sysname R1_VPNGW_H2200
#
 ike local-name R1_VPNGW_H2200
#
 acl number 3000
 description IPSec ACL
 rule 10 permit gre source
    10.0.1.1 0 destination
    1.1.1.2 0
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R3_VPNGW_C2900
 nat traversal
 remote-address 1.1.1.2
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description TO_R2_PAT_C2900
 ip address 10.0.1.1
    255.255.255.252
 ipsec policy myIPSecPolicy
#
 interface Tunnel0/0/1
 mtu 1400
 ip address 172.16.0.1
    255.255.255.252
 tunnel-protocol gre
 source 10.0.1.1
 destination 1.1.1.2
#
ip route-static 0.0.0.0 0.0.0.0
   10.0.1.2
ip route-static 2.2.2.0
   255.255.255.0 Tunnel0/0/1
```

H.5 Topologie č. 2: Konfigurace směrovače R2_PAT_C2900

```
hostname R2_PAT_C2900
!
interface GigabitEthernet0/0
 description TO_R1_VPNGW_H2200
 ip address 10.0.1.2
    255.255.255.252
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R3_VPNGW_C2900
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip nat source list 1 interface
   GigabitEthernet0/1 overload
ip nat source static udp 10.0.1.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.1.1
    4500 1.1.1.1 4500 extendable
ip route 0.0.0.0 0.0.0.0 1.1.1.2
ip route 10.0.0.0 255.255.255.0
   10.0.1.1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

H.6 Topologie č. 2: Konfigurace směrovače R3_VPNGW_C2900

```
hostname R3_VPNGW_C2900
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp identity hostname
!
crypto isakmp peer address
   1.1.1.1
 set aggressive-mode password
    letMeIn
 set aggressive-mode client-
    endpoint fqdn R3_VPNGW_C2900
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set 20
 match address 111
!
interface Tunnel0
 ip address 172.16.0.2
    255.255.255.252
 ip mtu 1400
 tunnel source GigabitEthernet0/1
 tunnel destination 10.0.1.1
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R2_PAT_C2900
 ip address 1.1.1.2
    255.255.255.252
crypto map CM
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
ip route 10.0.0.0 255.255.255.0
   Tunnel0
!
access-list 111 remark IPSec_ACL
access-list 111 permit gre host
   1.1.1.2 host 10.0.1.1
```

I Zkrácená konfigurace DMVPN s IPSec zabezpečením

I.1 Konfigurace směrovače R1_HUB_C2900

```
hostname R1_HUB_C2900
!
crypto keyring MyKeyring
  pre-shared-key address 0.0.0.0
     0.0.0.0 key letMeIn
  pre-shared-key hostname R5_SPOKE
     2_C2900 key letMeIn
  pre-shared-key hostname R4_SPOKE
     1_H2200 key letMeIn
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp profile
   MyISAKMPprofile
   keyring MyKeyring
   self-identity fqdn
   match identity host R4_SPOKE1_H
      2200
   match identity host R5_SPOKE2_C
      2900
   match identity address 0.0.0.0
   initiate mode aggressive
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile
   MyIPSecProfile
 set transform-set 20
 set isakmp-profile
    MyISAKMPprofile
!
interface Tunnel0
 ip address 172.20.0.1
    255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp network-id 1
 ip ospf network broadcast
 ip ospf priority 255
 tunnel source 1.0.0.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile
    MyIPSecProfile
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.1.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description R2_INTER_C2800
 ip address 1.0.0.2
    255.255.255.252
!
router ospf 1
 area 1 stub
 passive-interface
    GigabitEthernet0/0
 network 10.0.1.0 0.0.0.255 area
    0
 network 172.20.0.0 0.0.0.255
    area 1
!
router ospf 2
 network 1.0.0.0 0.0.0.3 area 0
!
ip route 0.0.0.0 0.0.0.0 1.0.0.1
```

I.2 Konfigurace směrovače R2_INTER_C2800

```
hostname R2_INTER_C2800
!
interface FastEthernet0/0
 description R1_HUB_C2900
 ip address 1.0.0.1
    255.255.255.252
!
interface FastEthernet0/1
 description R5_SPOKE2_H2200
 ip address 3.0.0.1
    255.255.255.252
!
interface Serial0/1/0
 description R3_NAT_C2800
 ip address 2.0.0.1
    255.255.255.248
 clock rate 128000
!
router ospf 2
 log-adjacency-changes
 network 1.0.0.0 0.0.0.3 area 0
 network 2.0.0.0 0.0.0.7 area 0
 network 3.0.0.0 0.0.0.3 area 0
```

I.3 Konfigurace směrovače R3_NAT_C2800

```
hostname R3_NAT_C2800
!
interface FastEthernet0/0
 description R4_SPOKE1_C2900
 ip address 192.168.2.2
    255.255.255.252
 ip nat enable
!
interface Serial0/1/0
 description R2_INTER_C2800
 ip address 2.0.0.2
    255.255.255.248
 ip nat enable
!
router ospf 2
 log-adjacency-changes
 network 2.0.0.0 0.0.0.7 area 0
 network 192.168.2.0 0.0.0.3 area
     0
!
ip route 0.0.0.0 0.0.0.0 2.0.0.1
!
ip nat source static 192.168.2.1
   2.0.0.3
```

I.4 Konfigurace směrovače R4_SPOKE1_H2200

```
 sysname R4_SPOKE1_H2200
#
 ike local-name R4_SPOKE1_H2200
#
 license active accept agreement
 license function dsvpn
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 nat traversal
#
ipsec profile MyProfile
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 10.0.2.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description R3_NAT_C2800
 ip address 192.168.2.1
    255.255.255.252
#
interface Tunnel0/0/0
 mtu 1400
 ip address 172.20.0.2
    255.255.255.0
 tunnel-protocol gre p2mp
 source 192.168.2.1
 ospf network-type broadcast
 ospf dr-priority 0
 ipsec profile MyProfile
 nhrp network-id 1
 nhrp entry 172.20.0.1 1.0.0.2
    register
#
ospf 1
 silent-interface GigabitEthernet
    0/0/0
 area 0.0.0.1
  network 10.0.2.0 0.0.0.255
  network 172.20.0.0 0.0.0.255
  stub
#
ospf 2
 area 0.0.0.0
  network 192.168.2.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0
   192.168.2.2
```

I.5 Konfigurace směrovače R5_SPOKE2_C2900

```
hostname R5_SPOKE2_C2900
!
crypto keyring MyKeyring
  pre-shared-key address 0.0.0.0
     0.0.0.0 key letMeIn
  pre-shared-key hostname R1_HUB_C
     2900 key letMeIn
  pre-shared-key hostname R4_SPOKE
     1_H2200 key letMeIn
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp profile
   MyISAKMPprofile
   keyring MyKeyring
   self-identity fqdn
   match identity host R4_SPOKE1_H
      2200
   match identity host R1_HUB_C
      2900
   match identity address 0.0.0.0
   initiate mode aggressive
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile
   MyIPSecProfile
 set transform-set 20
 set isakmp-profile
    MyISAKMPprofile
!
interface Tunnel0
 ip address 172.20.0.3
    255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 172.20.0.1 1.0.0.2
 ip nhrp map multicast 1.0.0.2
 ip nhrp network-id 1
 ip nhrp nhs 172.20.0.1
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source 3.0.0.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile
    MyIPSecProfile
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.3.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description R2_INTER_C2800
 ip address 3.0.0.2
    255.255.255.252
!
router ospf 1
 area 1 stub
 passive-interface
    GigabitEthernet0/0
 network 10.0.3.0 0.0.0.255 area
    1
 network 172.20.0.0 0.0.0.255
    area 1
!
router ospf 2
 network 3.0.0.0 0.0.0.3 area 0
!
ip route 0.0.0.0 0.0.0.0 3.0.0.1
```

I.6 Topologie č. 2: Konfigurace směrovače R1_HUB_H3200

```
 sysname R1_HUB_H3200
#
 ike local-name R1_HUB_H3200
#
 license active accept agreement
 license function dsvpn
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 nat traversal
#
ipsec profile MyProfile
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 10.0.1.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description R2_INTER_C2800
 ip address 1.0.0.2
    255.255.255.252
#
interface Tunnel0/0/0
 mtu 1400
 ip address 172.20.0.1
    255.255.255.0
 tunnel-protocol gre p2mp
 source 1.0.0.2
 ospf network-type broadcast
 ospf dr-priority 255
 ipsec profile MyProfile
 nhrp entry multicast dynamic
 nhrp network-id 1
#
ospf 1
 silent-interface GigabitEthernet
    0/0/0
 area 0.0.0.0
  network 10.0.1.0 0.0.0.255
 area 0.0.0.1
  network 172.20.0.0 0.0.0.255
  stub
#
ospf 2
 area 0.0.0.0
  network 1.0.0.0 0.0.0.3
#
ip route-static 0.0.0.0 0.0.0.0
   1.0.0.1
```

I.7 Topologie č. 2: Konfigurace směrovače R2_INTER_C2800

```
hostname R2_INTER_C2800
!
interface FastEthernet0/0
 description R1_HUB_H3200
 ip address 1.0.0.1
    255.255.255.252
!
interface FastEthernet0/1
 description R5_SPOKE2_C2900
 ip address 3.0.0.1
    255.255.255.252
!
interface Serial0/1/0
 description R3_NAT_C2800
 ip address 2.0.0.1
    255.255.255.248
 clock rate 125000
!
router ospf 2
 log-adjacency-changes
 network 1.0.0.0 0.0.0.3 area 0
 network 2.0.0.0 0.0.0.7 area 0
 network 3.0.0.0 0.0.0.3 area 0
```

I.8 Topologie č. 2: Konfigurace směrovače R3_NAT_C2800

```
hostname R3_NAT_C2800
!
interface FastEthernet0/0
 description R4_SPOKE1_C2900
 ip address 192.168.2.2
    255.255.255.252
 ip nat enable
!
interface Serial0/1/0
 description R2_INTER_C2800
 ip address 2.0.0.2
    255.255.255.248
 ip nat enable
!
router ospf 2
 log-adjacency-changes
 network 2.0.0.0 0.0.0.7 area 0
 network 192.168.2.0 0.0.0.3 area
     0
!
ip route 0.0.0.0 0.0.0.0 2.0.0.1
!
ip nat source static 192.168.2.1
   2.0.0.3
```

I.9 Topologie č. 2: Konfigurace směrovače R4_SPOKE1_C2900

```
hostname R4_SPOKE1_C2900
!
crypto keyring MyKeyring
  pre-shared-key address 0.0.0.0
     0.0.0.0 key letMeIn
  pre-shared-key hostname R1_HUB_H
     3200 key letMeIn
  pre-shared-key hostname R5_SPOKE
     2_C2900 key letMeIn
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp profile
   MyISAKMPprofile
   keyring MyKeyring
   self-identity fqdn
   match identity host R5_SPOKE2_C
      2900
   match identity host R1_HUB_H
      3200
   match identity address 0.0.0.0
   initiate mode aggressive
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile
   MyIPSecProfile
 set transform-set 20
 set isakmp-profile
    MyISAKMPprofile
!
interface Tunnel0
 ip address 172.20.0.2
    255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 172.20.0.1 1.0.0.2
 ip nhrp map multicast 1.0.0.2
 ip nhrp network-id 1
 ip nhrp nhs 172.20.0.1
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source 192.168.2.1
 tunnel mode gre multipoint
 tunnel protection ipsec profile
    MyIPSecProfile
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.2.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description R3_NAT_C2800
 ip address 192.168.2.1
    255.255.255.252
!
router ospf 1
 area 1 stub
 passive-interface
    GigabitEthernet0/0
 network 10.0.2.0 0.0.0.255 area
    1
 network 172.20.0.0 0.0.0.255
    area 1
!
router ospf 2
 network 192.168.2.0 0.0.0.3 area
     0
!
ip route 0.0.0.0 0.0.0.0
   192.168.2.2
```

I.10 Topologie č. 2: Konfigurace směrovače R5_SPOKE2_C2900

```
hostname R5_SPOKE2_C2900
!
crypto keyring MyKeyring
  pre-shared-key address 0.0.0.0
     0.0.0.0 key letMeIn
  pre-shared-key hostname R1_HUB_H
     3200 key letMeIn
  pre-shared-key hostname R4_SPOKE
     1_C2900 key letMeIn
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp profile
   MyISAKMPprofile
   keyring MyKeyring
   self-identity fqdn
   match identity host R4_SPOKE1_C
      2900
   match identity host R1_HUB_H
      3200
   match identity address 0.0.0.0
   initiate mode aggressive
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto ipsec profile
   MyIPSecProfile
 set transform-set 20
 set isakmp-profile
    MyISAKMPprofile
!
interface Tunnel0
 ip address 172.20.0.3
    255.255.255.0
 no ip redirects
 ip mtu 1400
 ip nhrp map 172.20.0.1 1.0.0.2
 ip nhrp map multicast 1.0.0.2
 ip nhrp network-id 1
 ip nhrp nhs 172.20.0.1
 ip ospf network broadcast
 ip ospf priority 0
 tunnel source 3.0.0.2
 tunnel mode gre multipoint
 tunnel protection ipsec profile
    MyIPSecProfile
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.3.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description R2_INTER_C2800
 ip address 3.0.0.2
    255.255.255.252
!
router ospf 1
 area 1 stub
 passive-interface
    GigabitEthernet0/0
 network 10.0.3.0 0.0.0.255 area
    1
 network 172.20.0.0 0.0.0.255
    area 1
!
router ospf 2
 network 3.0.0.0 0.0.0.3 area 0
!
ip route 0.0.0.0 0.0.0.0 3.0.0.1
```

J Zkrácená konfigurace L2TP over IPSec VPN

J.1 Konfigurace směrovače R1_PPPoEclient_C2900

```
hostname R1_PPPoEclient_C2900
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R2_LAC_C2900
 no ip address
 pppoe enable group global
 pppoe-client dial-pool-number 1
!
interface Dialer1
 mtu 1492
 ip address negotiated
 ip nat enable
 encapsulation ppp
 dialer pool 1
 ppp chap hostname user1@lab.
    local
 ppp chap password 0 letMeIn
!
ip nat source list 1 interface
   Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.0.255
```

J.2 Konfigurace směrovače R2_LAC_C2900

```
hostname R2_LAC_C2900
!
vpdn enable
vpdn search-order domain
!
vpdn-group MyVpdnGroup
 request-dialin
  protocol l2tp
  domain lab.local
 initiate-to ip 1.1.1.2
 local name LAC
 l2tp tunnel password 0 letMeIn
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp identity hostname
!
crypto isakmp peer address
   1.1.1.2
 set aggressive-mode password
    letMeIn
 set aggressive-mode client-
    endpoint fqdn R2_LAC_C2900
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.2
 set transform-set 20
 match address 111
!
bba-group pppoe MyGroup
 virtual-template 1
!
interface GigabitEthernet0/0
 description TO_R3_PAT_C2800
 ip address 10.0.2.1
    255.255.255.252
 crypto map CM
!
interface GigabitEthernet0/1
 description TO_R1_PPPoEclient_C
    2900
 no ip address
 pppoe enable group MyGroup
!
interface Virtual-Template1
 mtu 1492
 ip address 10.0.1.2
    255.255.255.0
 peer default ip address pool
    MyPool
 ppp authentication chap callin
!
ip local pool MyPool 10.0.1.1
!
ip route 0.0.0.0 0.0.0.0
   GigabitEthernet0/0
ip route 10.0.0.0 255.255.255.0
   GigabitEthernet0/1
!
access-list 111 remark IPSec_ACL
access-list 111 permit udp host
   10.0.2.1 eq 1701 host 1.1.1.2
   eq 1701
```

J.3 Konfigurace směrovače R3_PAT_C2800

```
hostname R3_PAT_C2800
!
interface FastEthernet0/0
 description TO_R2_LAC_C2900
 ip address 10.0.2.2
    255.255.255.252
 ip nat enable
!
interface FastEthernet0/1
 description TO_R4_LNS_H3200
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip route 0.0.0.0 0.0.0.0
   FastEthernet0/0
ip route 2.2.2.0 255.255.255.0
   FastEthernet0/1
!
ip nat source list 1 interface
   FastEthernet0/1 overload
ip nat source static udp 10.0.2.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.2.1
    4500 1.1.1.1 4500 extendable
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

J.4 Konfigurace směrovače R4_LNS_H3200

```
 sysname R4_LNS_H3200
#
 l2tp enable
#
 ike local-name R4_LNS_H3200
#
acl number 3000
 description IPSec_ACL
 rule 5 permit udp source 1.1.1.2
     0 source-port eq 1701
    destination 10.0.2.1 0
    destination-port eq 1701
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R2_LAC_C2900
 nat traversal
 remote-address 1.1.1.1
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
ip pool MyL2TPpool
 gateway-list 172.20.0.1
 network 172.20.0.0 mask
    255.255.255.0
#
aaa
local-user user1@lab.local
   password cipher %$%$8S*]K
   $'<|(>_'PX{@A*8&<45%$%$
 local-user user1@lab.local
    service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
 remote address pool MyL2TPpool
 ip address 172.20.0.1
    255.255.255.0
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description TO_R3_PAT_C2800
 ip address 1.1.1.2 255.255.255.0
 ipsec policy myIPSecPolicy
#
l2tp-group 1
 allow l2tp virtual-template 1
    remote LAC
 tunnel password simple letMeIn
 tunnel name LNS
#
ip route-static 0.0.0.0 0.0.0.0
   1.1.1.1
```

J.5 Topologie č. 2: Konfigurace směrovače R1_PPPoEclient_C2900

```
hostname R1_PPPoEclient_C2900
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R2_LAC_H2200
 no ip address
 pppoe enable group global
 pppoe-client dial-pool-number 1
!
interface Dialer1
 mtu 1492
 ip address negotiated
 ip nat enable
 encapsulation ppp
 dialer pool 1
 ppp chap hostname user1@lab.
    local
 ppp chap password 0
    letMeInLetMeIn
!
ip nat source list 1 interface
   Dialer1 overload
ip route 0.0.0.0 0.0.0.0 Dialer1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.0.255
```

J.6 Topologie č. 2: Konfigurace směrovače R2_LAC_H2200

```
sysname R2_LAC_H2200
#
 l2tp enable
#
 ike local-name R2_LAC_H2200
#
acl number 3000
 description IPSec_ACL
 rule 5 permit udp source
    10.0.2.1 0 source-port eq
    1701 destination 1.1.1.2 0
    destination-port eq 1701
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v1
 exchange-mode aggressive
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R4_LNS_C2900
 nat traversal
 remote-address 1.1.1.2
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
ip pool MyPPoEPool
 gateway-list 10.0.1.2
 network 10.0.1.0 mask
    255.255.255.0
 excluded-ip-address 10.0.1.3
    10.0.1.254
#
aaa
domain lab.local
local-user user1@lab.local
   password cipher %@%@~a<@(
   cyvJAKssY#^Yv=,%VTA%@%@
 local-user user1@lab.local
    service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode chap
    call-in domain lab.local
 remote address pool MyPPoEPool
 mtu 1492
 timer hold 20
 ip address 10.0.1.2
    255.255.255.0
```

J.7 Topologie č. 2: Konfigurace R2_LAC_H2200 - pokračování

```
interface GigabitEthernet0/0/0
 description TO_R3_PAT_C2800
 ip address 10.0.2.1
    255.255.255.252
 ipsec policy myIPSecPolicy
#
interface GigabitEthernet0/0/1
 pppoe-server bind Virtual-
    Template 1
 description TO_R1_PPPoEclient_C
    2900
#
l2tp-group 1
 tunnel password simple letMeIn
 tunnel name LAC
 start l2tp ip 1.1.1.2
    fullusername user1@lab.local
#
ip route-static 0.0.0.0 0.0.0.0
   10.0.2.2
ip route-static 10.0.0.0
   255.255.255.0 10.0.1.1
```

J.8 Topologie č. 2: Konfigurace směrovače R3_PAT_C2800

```
hostname R3_PAT_C2800
!
interface FastEthernet0/0
 description TO_R2_LAC_H2200
 ip address 10.0.2.2
    255.255.255.252
 ip nat enable
!
interface FastEthernet0/1
 description TO_R4_LNS_C2900
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip route 0.0.0.0 0.0.0.0
   FastEthernet0/0
ip route 2.2.2.0 255.255.255.0
   FastEthernet0/1
!
ip nat source list 1 interface
   FastEthernet0/1 overload
ip nat source static udp 10.0.2.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.2.1
    4500 1.1.1.1 4500 extendable
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

J.9 Topologie č. 2: Konfigurace směrovače R4_LNS_C2900

```
hostname R4_LNS_C2900
!
vpdn enable
!
vpdn-group MyVpdnGroup
 accept-dialin
  protocol l2tp
  virtual-template 1
 terminate-from hostname LAC
 l2tp tunnel password 0 letMeIn
!
username user1@lab.local password
    0 letMeInLetMeIn
!
crypto isakmp policy 20
 encr aes 256
 authentication pre-share
 group 5
 lifetime 3600
crypto isakmp identity hostname
!
crypto isakmp peer address
   1.1.1.1
 set aggressive-mode password
    letMeIn
 set aggressive-mode client-
    endpoint fqdn R4_LNS_C2900
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set 20
 match address 111
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R3_PAT_C2800
 ip address 1.1.1.2
    255.255.255.252
 crypto map CM
!
interface Virtual-Template1
 mtu 1492
 ip address 172.20.0.1
    255.255.255.0
 peer default ip address pool
    MyPool
 ppp authentication chap
!
ip local pool MyPool 172.20.0.2
   172.20.0.254
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
!
access-list 111 remark IPSec_ACL
access-list 111 permit udp host
   1.1.1.2 eq 1701 host 10.0.2.1
   eq 1701
```

K Zkrácená konfigurace PPTP VPN

K.1 Konfigurace směrovače R1_PAT_C2900

```
hostname R1_PAT_C2900
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.1.254
    255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface GigabitEthernet0/1
 description TO_R2_VPNGW_C2900
 ip address 1.1.1.1
    255.255.255.252
 ip nat outside
 ip virtual-reassembly in
!
ip nat inside source list 111
   interface GigabitEthernet0/1
   overload
ip route 0.0.0.0 0.0.0.0 1.1.1.2
!
access-list 111 remark NAT_ACL
access-list 111 permit ip
   10.0.1.0 0.0.0.255 any
```

K.2 Konfigurace směrovače R2_VPNGW_C2900

```
hostname R2_VPNGW_C2900
!
vpdn enable
!
vpdn-group 1
 ! Default PPTP VPDN group
 accept-dialin
  protocol pptp
  virtual-template 1
!
username user1 password 0 letMeIn
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R1_PAT_C2900
 ip address 1.1.1.2
    255.255.255.252
!
interface Virtual-Template1
 ip unnumbered GigabitEthernet0/0
 peer default ip address pool
    myPool
 no keepalive
 ppp encrypt mppe 128
 ppp authentication ms-chap ms-
    chap-v2
!
ip local pool myPool 2.2.2.20
   2.2.2.25
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
```

L Zkrácená konfigurace IPSec IKEv2 VPN

L.1 Konfigurace směrovače R1_VPNGW_C2900

```
hostname R1_VPNGW_C2900
!
crypto ikev2 proposal myIKE2
   proposal
 encryption aes-cbc-256
 integrity sha1
 group 5
!
crypto ikev2 policy myIKE2policy
 proposal myIKE2proposal
!
crypto ikev2 keyring myIKE2
   keyring
 peer R3
  address 1.1.1.2
  pre-shared-key local letMeIn
  pre-shared-key remote letMeIn
 !
!
crypto ikev2 profile myIKE2
   profile
 match identity remote fqdn R3
 identity local fqdn R1
 authentication remote pre-share
 authentication local pre-share
 keyring local myIKE2keyring
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.2
 set transform-set 20
 set ikev2-profile myIKE2profile
 match address 111
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R2_PAT_C2900
 ip address 10.0.1.1
    255.255.255.252
 crypto map CM
!
ip route 0.0.0.0 0.0.0.0 10.0.1.2
!
access-list 111 remark IPSec_ACL
access-list 111 permit ip
   10.0.0.0 0.0.0.255 2.2.2.0
   0.0.0.255
```

L.2 Konfigurace směrovače R2_PAT_C2900

```
hostname R2_PAT_C2900
!
interface GigabitEthernet0/0
 description TO_R1_VPNGW_C2900
 ip address 10.0.1.2
    255.255.255.252
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R3_VPNGW_H3200
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip nat source list 1 interface
   GigabitEthernet0/1 overload
ip nat source static udp 10.0.1.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.1.1
    4500 1.1.1.1 4500 extendable
ip route 0.0.0.0 0.0.0.0 1.1.1.2
ip route 10.0.0.0 255.255.255.0
   10.0.1.1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

L.3 Konfigurace směrovače R3_VPNGW_H3200

```
 sysname R3_VPNGW_H3200
#
 ike local-name R3
#
acl number 3000
 description IPSec_ACL
 rule 10 permit ip source 2.2.2.0
     0.0.0.255 destination
    10.0.0.0 0.0.0.255
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v2
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R1
 nat traversal
 remote-address 1.1.1.1
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description TO_R2_PAT_C2900
 ip address 1.1.1.2
    255.255.255.252
 ipsec policy myIPSecPolicy
#
ip route-static 0.0.0.0 0.0.0.0
   1.1.1.1
```

L.4 Topologie č. 2: Konfigurace směrovače R1_VPNGW_H2200

```
 sysname R1_VPNGW_H2200
#
 ike local-name R1
#
 acl number 3000
 description IPSec ACL
 rule 10 permit ip source
    10.0.0.0 0.0.0.255
    destination 2.2.2.0 0.0.0.255
#
ipsec proposal myIPSecProposal
 esp authentication-algorithm sha
    1
 esp encryption-algorithm aes-256
#
ike proposal 10
 encryption-algorithm aes-cbc-256
 dh group5
 sa duration 3600
#
ike peer myIkePeer v2
 pre-shared-key simple letMeIn
 ike-proposal 10
 local-id-type name
 remote-name R3
 nat traversal
 remote-address 1.1.1.2
#
ipsec policy myIPSecPolicy 10
   isakmp
 security acl 3000
 ike-peer myIkePeer
 proposal myIPSecProposal
#
interface GigabitEthernet0/0/0
 description LAN_SEGMENT
 ip address 10.0.0.254
    255.255.255.0
#
interface GigabitEthernet0/0/1
 description TO_R2_PAT_C2900
 ip address 10.0.1.1
    255.255.255.252
 ipsec policy myIPSecPolicy
#
ip route-static 0.0.0.0 0.0.0.0
   10.0.1.2
```

L.5 Topologie č. 2: Konfigurace směrovače R2_PAT_C2900

```
hostname R2_PAT_C2900
!
interface GigabitEthernet0/0
 description TO_R1_VPNGW_H2200
 ip address 10.0.1.2
    255.255.255.252
 ip nat enable
!
interface GigabitEthernet0/1
 description TO_R3_VPNGW_C2900
 ip address 1.1.1.1
    255.255.255.252
 ip nat enable
!
ip nat source list 1 interface
   GigabitEthernet0/1 overload
ip nat source static udp 10.0.1.1
    500 1.1.1.1 500 extendable
ip nat source static udp 10.0.1.1
    4500 1.1.1.1 4500 extendable
ip route 0.0.0.0 0.0.0.0 1.1.1.2
ip route 10.0.0.0 255.255.255.0
   10.0.1.1
!
access-list 1 remark NAT_ACL
access-list 1 permit 10.0.0.0
   0.0.255.255
```

L.6 Topologie č. 2: Konfigurace směrovače R3_VPNGW_C2900

```
hostname R3_VPNGW_C2900
!
crypto ikev2 proposal myIKE2
   proposal
 encryption aes-cbc-256
 integrity sha1
 group 5
!
crypto ikev2 policy myIKE2policy
 proposal myIKE2proposal
!
crypto ikev2 keyring myIKE2
   keyring
 peer R1
  address 1.1.1.1
  pre-shared-key local letMeIn
  pre-shared-key remote letMeIn
 !
!
crypto ikev2 profile myIKE2
   profile
 match identity remote fqdn R1
 identity local fqdn R3
 authentication remote pre-share
 authentication local pre-share
 keyring local myIKE2keyring
!
crypto ipsec transform-set 20 esp
   -aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CM 20 ipsec-isakmp
 set peer 1.1.1.1
 set transform-set 20
 set ikev2-profile myIKE2profile
 match address 111
!
interface GigabitEthernet0/0
 description LAN_SEGMENT
 ip address 2.2.2.254
    255.255.255.0
!
interface GigabitEthernet0/1
 description TO_R2_PAT_C2900
 ip address 1.1.1.2
    255.255.255.252
 crypto map CM
!
ip route 0.0.0.0 0.0.0.0 1.1.1.1
!
access-list 111 remark IPSec_ACL
access-list 111 permit ip 2.2.2.0
    0.0.0.255 10.0.0.0 0.0.0.255
```