VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Filip Kamenář

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

MONITORING PROVOZOVANÝCH SLUŽEB NA AKTIVNÍCH SÍŤOVÝCH PRVCÍCH MIKROTIK
MONITORING OF SERVICES WITHIN ACTIVE NETWORK ELEMENTS BY MIKROTIK

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Filip Kamenář**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. David Grenar**
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Telekomunikační a informační systémy**

Ústav telekomunikací

Student: Filip Kamenář ***ID:*** 195352

Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Monitoring provozovaných služeb na aktivních síťových prvcích Mikrotik

POKYNY PRO VYPRACOVÁNÍ:

Nejdříve budou popsány stávající nástroje pro monitorování sítě a detekci vybraných služeb. Následně pak budou použity v rámci realizace vhodné monitorovací nástroje, jež budou aplikovány na síťové prvky výrobce Mikrotik. Dále bude vytvořena konfigurace pro zachování maximální dostupnosti vybraných služeb. V neposlední řadě bude vypracován skript pro monitoring vybraných parametrů a vlastností v přístupové síti.

DOPORUČENÁ LITERATURA:

[1] HART, Tyler. Networking with MikroTik: MTCNA Study Guide. 2017. ISBN 9781973206354.

[2] DISCHER, Stephen, RouterOS by Example, 2nd Edition: B&W: B&W Version. ISBN 9780692777084.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Ing. David Grenar

prof. Ing. Jiří Mišurec, CSc.
předseda rady studijního programu

ABSTRAKT

Bakalářská práce se zaměřuje na monitorování služeb VPN na síťových prvcích Mikrotik. Teoretická část práce obsahuje popis systému RouterOS, možnosti jeho správy a síťová zařízení, která jsou v této práci použita. Rovněž práce obsahuje popis služby VPN a rozbor protokolů PPTP, SSTP, L2TP a OpenVPN, které jsou implementovány v rámci praktické části. Součástí teorie je také popis monitorovacích nástrojů, které obsahuje systém RouterOS. Pro srovnání jsou zde uvedeny i externí nástroje. Vybrané monitorovací nástroje jsou poté implementovány v praktické části této práce a vytvořeném monitorovacím skriptu.

Praktická část bakalářské práce je zaměřena na sestavení VPN tunelů a následné měření jejich parametrů. Klienti VPN se nachází v lokalitách Česko, Ukrajina a Egypt, čímž jsou vytvořeny reálné podmínky pro monitorování stavů v sítě. Poslední částí je vypracovaný skript, který automatizovaně monitoruje službu VPN v přístupové síti a nasbíraná data automaticky odesílá obsluze.

Cílem této práce je znázornit využití integrovaných monitorovacích nástrojů systému RouterOS v síti postavené na prvcích od společnosti Mikrotik. Vybranou službou, která je monitorována, je služba VPN, která je využívána pro vzdálený přístup k lokálním sítím z různých částí světa korporacemi i jednotlivci. Jednotlivé parametry, které byly monitorovány, jsou rovněž srovnány v závislosti na geografické poloze jednotlivých klientů.

KLÍČOVÁ SLOVA

MikroTik, Monitorování sítě, Přístupová síť, RouterOS, Síťové zařízení, Skript, VPN

ABSTRACT

This bachelor thesis deals with the monitoring of the VPN services on the networking elements Mikrotik. The theoretical part includes the description of RouterOS system, management options and networking devices used. The thesis consists of the description of the VPN services and analysis of PPTP, SSTP, L2TP and OpenVPN protocols, which are implemented in the practical part of this work. The theory also contains the description of monitoring devices included in the RouterOS system. In comparison, external tools are enlisted. Chosen monitoring tools are therefore implemented in the practical part of the thesis and in the monitoring script.

The practical part of the bachelor thesis is focused on the establishment of VPN tunnels and its parameter measurement. The VPN clients are to be found in the Czech Republic, Ukraine and Egypt, which establishes the real conditions for network monitoring status. The final part of the work deals with the script, which is created for the automatic-monitoring of VPN service in the accessible network and sends the gathered data to the operators.

The aim of the thesis is to illustrate the usage of integrated monitoring tools in the RouterOS system in the network built on the Mikrotik elements. The chosen monitoring service was the service VPN, which is being used for remote access to the local networks from distant part of the world by the corporations but also individuals. Individual monitored parameters are enlisted and compared depending on client geographic location.

KEYWORDS

Access network, MikroTik, Network monitoring, Networking hardware, RouterOS, Script, VPN

KAMENÁŘ, Filip. *Monitoring provozovaných služeb na aktivních síťových prvcích Mikrotik*. Brno, 2020, 89 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. David Grenar

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Monitoring provozovaných služeb na aktivních síťových prvcích Mikrotik“ jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autora

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce panu Ing. Davidovi Grenarovi za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Brno ....

podpis autora

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

Tato bakalářská práce se zabývá monitorováním služeb na aktivních síťových prvcích Mikrotik. Jako vybrané služby byly zvoleny protokoly, které se požívají při připojení vzdálených uživatelských stanic do privátních sítí přes veřejnou síť Internet. Tento proces připojení vzdálené uživatelské stanice je nazván jako VPN. Konkrétně byly zvoleny protokoly PPTP, SSTP, L2TP a OpenVPN. Důvodem zvolení těchto protokolů je podpora ze strany operačního systému RouterOS.

Přínosem této práce je také zaměření se na praktické řešení situací z praxe, se kterými se v současné době setkává nepřeberné množství společností. Já jsem se v této práci zaměřil na blíže nespecifikovanou technologickou společnost, která sídlí v Olomouckém kraji. Zaměřením této společnosti je zakázkový vývoj softwarových produktů. Důvodem pro implementaci monitorovacích nástrojů v síti této společnosti je ten, že v rámci České republiky působí kromě Olomouckého kraje také v kraji Jihomoravském, ale také vlastní vývojová centra na Ukrajině, ve městě Kyjev a v Egyptě, ve městě Mansoura. Tím je zajištěna možnost sledovat a vyhodnotit jaký vliv má na službu VPN geografická poloha v rámci tří států a dvou kontinentů.

V čase, kdy byla tato práce realizována, postihla prakticky celý svět infekční nemoc COVID-19, která je způsobena koronavirem typu SARS-CoV-2. Díky této nemoci byla napříč celým světem zavedena různá nařízení a doporučení, která omezila pohyb lidí.[1] Díky těmto událostem se stalo velmi aktuálním tématem, práce z domova, neboli home office.[2] Při práci z domova lidé často potřebují přístup k různým zařízením, která jsou dostupná pouze v lokální síti společností. Tento přístup je jim umožněn právě díky VPN a v této „koronavirové“ době se z VPN stává jedním z klíčových prvků infrastruktury společností, která musí zvládnout zvýšený počet uživatelů a monitoring této služby je čím dál důležitější.

V teoretické části práce jsem se věnoval popisu operačního systému RouterOS, který je využíván síťovými prvky Mikrotik. Také jsou zde popsány jednotlivé možnosti správy tohoto systému s konkrétním zaměřením na nástroje Winbox, Webfig, terminál a v neposlední řadě také na aplikační programovací rozhraní, které může být využito pro přístup aplikací třetích stran. Tato část rovněž obsahuje popis konkrétních síťových prvků, které jsem při této práci využil.
Následně jsem se věnoval podrobnému popisu jednotlivých protokolů služby VPN, které jsem rovněž využil při implementaci v praktické části práce. Pro ucelení představy čtenáře byly popsány i síťové modely OSI/ISO a TCP/IP, včetně jejich vrstev, na které se v textu odkazuji.

Součástí této práce je i popis vybraných monitorovacích nástrojů, které nabízí operační systém RouterOS. Tyto nástroje jsem popsal v kapitole 2.3.1. Vybrané

nástroje jsou popsány nejprve teoreticky a poté jsem provedl ukázku praktického nasazení těchto nástrojů. Zkušenosti z této implementace jsem poté použil v praktické části bakalářské práce.

V praktické části jsem se nejprve zabýval vytvořením serveru VPN pro všechny zvolené protokoly. Tento server se nachází v Olomouci. Poté jsem se věnoval vytvořením klientských směrovačů, které jsem později připojil k serveru v Olomouci a monitoroval vybrané parametry těchto spojení.

Poslední částí této práce je vytvoření skriptu za účelem monitorování služby VPN a jejich parametrů. Toto monitorování je prováděno automatizovaně a výsledky jsou poté odesílány pomocí emailu zvolenému příjemci.

1 Síťové prvky Mikrotik

Společnost Mikrotik byla založena v Litvě v roce 1997 a zabývá se produkcí síťových prvků, jako jsou směrovače, přepínače či bezdrátové systémy pro ISP. Tato společnost rovněž vyvíjí operační systém RouterOS, který využívá ve svých směrovačích. Mezi nejznámější produkty této společnosti patří hardwarová platforma RouterBOARD[1].[3]

Obr. 1.1: Logo společnosti Mikrotik.

1.1 Operační systém RouterOS

Operační systém RouterOS je postaven na jádru Linux a je předinstalovaný ve všech síťových prvcích společnosti Mikrotik, která jej také vyvinula. Tento systém je možné použít rovněž i na zařízeních třetích stran a může být i virtualizován.[4]

Dle mého názoru je největší výhodou tohoto operačního systému fakt, že RouterOS je stejný ve všech síťových zařízeních a množství funkcí tedy nezáleží na ceně daného zařízení. RouterOS nabízí 6 variant licencí, kdy jediný rozdíl mezi jednotlivými produkčními licencemi je maximální počet použitých funkcí jako jsou např. VPN tunely. Detailní popis licencí není pro tuto práci podstatný a je k nalezení na wiki společnosti Mikrotik.[2]

1.2 Možnosti správy síťových zařízení Mikrotik

1.2.1 Winbox

Winbox je samostatný softwarový nástroj, který je určen pro počítače s operačním systémem Windows, ale díky aplikačnímu rozhraní Wine může být spuštěn také na operačních systémech Linux či OSX. Výhodou tohoto nástroje oproti dalším variantám vzdálené správy zařízení Mikrotik, je rychlé, jednoduché GUI využívající okna

[1] Mikrotik také vyvíjí operační systém pro přepínače SwOS, viz <`https://wiki.mikrotik.com/wiki/SwOS`>.

[2] Odkaz na wiki Mikrotik s popisem jednotlivých variant licencí RouterOS, viz <`https://wiki.mikrotik.com/wiki/Manual:License`>.

a také zabečená komunikace mezi uživatelem a síťovým zařízením. Zabezpečení je dosaženo šifrovacím algoritmem AES128-CBC-SHA[3] a také tím, že obě strany (Winbox i síťové zařízení) vzájemně ověřují znalost hesla, které je využito při přihlášení, tím je zamezeno možnému kybernetickému útoku typu MITM.[5]

Největší benefitem Winboxu je možnost uložení síťového zařízení do spravovaných zařízení, kde je možné uložit IP, přihlašovací jméno a heslo. Tahle vlastnost je velmi užitečná při práci s větším počtem síťových zařízení od společnosti Mikrotik.

Rovněž je možné pro připojení k zařízení využít jeho unikátní MAC adresu namísto IP adresy.[5] Toto připojení ovšem není doporučeno pro produkční použití a to z důvodu nižší spolehlivosti, která je daná využitím protokolu UDP, jenž neobsahuje záruky doručení, protože se jedná o nespojový protokol.[6]

Winbox pro komunikaci se zařízením využívá port TCP 8291. V případě připojení s pomocí MAC adresy zařízení, probíhá komunikace na portu UDP 20561.[7]

Obr. 1.2: Náhled GUI software Winbox.

1.2.2 Webfig

Tento nástroj je webová alternativa software Winbox, kdy využívá stejného principu GUI s okny pro správu zařízení. Výhodou tohoto nástroje je jednoduchost spuštění, kdy je nutný pouze webový prohlížeč s podporou JS je multiplatformní

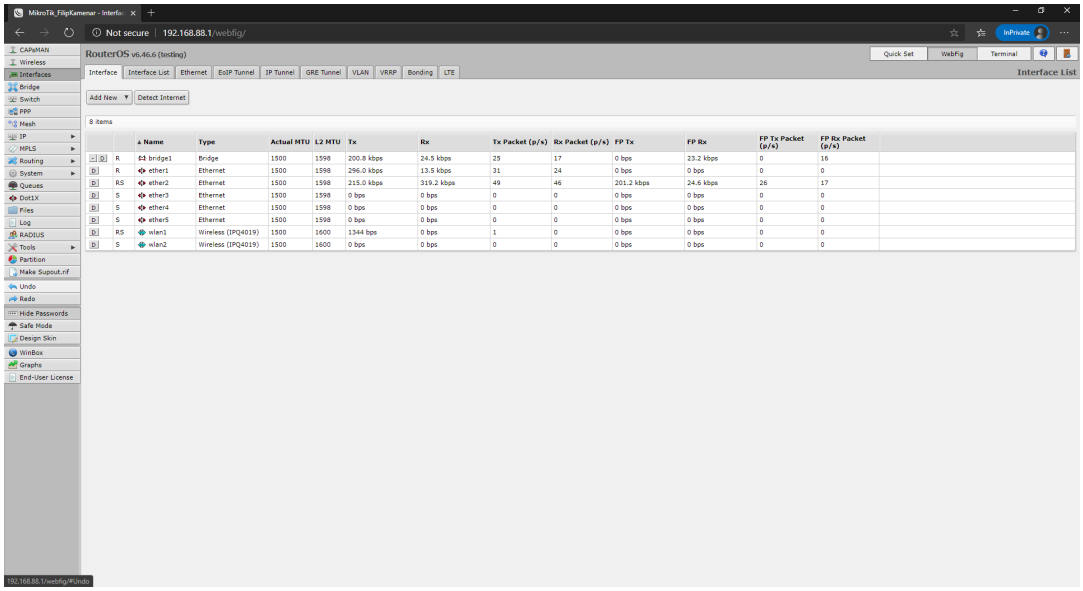
[3]Toto šifrování je využito od verze 3.14 nástroje Winbox

objektový programovací jazyk, používaný webovými stránkami, běžící na straně klienta. Tím je umožněno uživateli využít kromě počítačů také mobilní zařízení jako jsou chytré telefony, či tablety.[9]

Při nutnosti konfigurace síťových zařízení ve stížených podmínkách, je tato varianta vzdálené správy velmi užitečná. Příkladem může být síťový administrátor v odlehlých místech, kdy má k dispozici pouze chytrý telefon.

Komunikace s RouterOS může být nezabezpečená, protokol HTTP s TCP portem 80, či zabezpečená pomocí SSL s využitím protokolu HTTPs a TCP portem 443. [7]

Aby mohlo být vytvořeno šifrované spojení s využitím protokolu HTTPs, tak je nutné použít certifikát SSL[4]. Tento certifikát může být vydán důvěryhodnou certifikační autoritou a nebo je možné v rámci RouterOS vygenerovat certifikát vlastní, který je typu „self-signed“(podepsán sebou samým). [9]



Obr. 1.3: Náhled GUI webové aplikace Webfig.

1.2.3 Terminál

Pro terminálové ovládání, síťových zařízení Mikrotik, může být využito protokolů telnet, port TCP 23, či SSH, port TCP 22, případně sériový port, pokud jej dané zařízení nabízí. Terminál je také možné spustit v rámci grafických rozhraní Winbox a Webfig.[10]

[4]SSL certifikát obsahuje kryptografický klíč vázaný k detailům organizace, které jsou ověřeny certifikační autoritou

Při vzdáleném přístupu je z důvodů bezpečnosti vhodné využít protokol SSH namísto telnet. Nevýhodou telnetu je nešifrovaná komunikace, kdy jsou veškerá data odesílána jako prostý text, tudíž je celá komunikace vystavena většímu riziku úspěšného napadnutí útočníkem. SSH je díky šifrované komunikaci vhodnější volbou.[11]

Protože je operační systém RouterOS postaven na základech Linuxu, je ovládání příkazové řádky velmi podobné unixovým systémům.[12]

1.2.4 Aplikační programovací rozhraní

Toto rozhraní je využito při tvorbě externích softwarových řešení, které komunikují se systémem RouterOS např. za účelem sběru dat, úpravám konfigurace či řízení zařízení. Pro využití API je třeba použít RouterOS alespoň ve verzi 3.x či novějším.

Komunikace s API může být nezabezpečená či zabezpečená pomocí SSL. V případě nezabezpečené varianty probíhá komunikace na portu TCP 8728, zabezpečená varianta komunikuje na portu TCP 8729.[7]

1.3 Přehled využitých zařízení Mikrotik

Pro tuto práci byly využity 3 různé modely směrovačů od společnosti Mikrotik. Nejvýkonnějším použitým modelem je směrovač RB3011UiAS-RM, který je připraven pro umístění do serverového racku[5]. Následně byly využity směrovače hAP ac^2 a hAP lite TC, pro ukázku implementace jednotlivých monitorovacích nástrojů, které nabízí operační systém RouterOS.

Veškeré směrovače používají systém RouterOS ve verzi 6.45.6. Tato verze systému byla vydána dne 11. 9. 2019, v rámci programu „Stable release tree“.[8]
Srovnání využitých směrovačů dle vybraných parametrů je možné naleznout v tabulce 1.1.

1.3.1 RB3011UiAS-RM

Tento směrovač, jako první model od společnosti Mikrotik, využívá procesorovou architekturu ARM, čímž nabízí vysoký výpočetní výkon. Směrovač je vhodný pro systémovou montáž, protože podporuje standard 1U.[13] Tento model obsahuje také dotykový displej, který umožňuje obsluze rychlou kontrolu aktuálního stavu směrovače a také velmi jednoduchou konfiguraci. Tato funkce je výhodná při instalaci v

[5]Rack je standardizovaný systém pro montáž serverových komponent do organizované struktury. [14]

průmyslových datacentrech, kdy systémový administrátor nepotřebuje počítač, ale může získat informace o směrovači přímo v racku.[15]

Obr. 1.4: Směrovač Mikrotik RB3011UiAS-RM.

1.3.2 hAP ac²

Směrovač hAP ac² je určen do kanceláří a domácností, kdy nabízí podporu 1 Gbit/s portů ethernet a také pokrytí WiFi na frekvenci 2.4 GHz a 5 GHz. Směrovač umožňuje také instalaci na zeď.[16]

Obr. 1.5: Směrovač Mikrotik hAP ac².

1.3.3 hAP lite TC

Stejně jako model hAP ac² je i tento směrovač vhodný pro použití v kancelářích, či domácnostech. Nabízí možnost pokrytí signálem WiFi na frekvenci 2.4 Ghz. Bohužel zde chybí porty ethernet, ty podporují pouze přenosovou rychlost do výše 100 Mbit/s. Zajímavostí je přítomnost portu MicroUSB pro napájení.[17]

Obr. 1.6: Směrovač Mikrotik hAP lite TC.

1.3.4 Srovnání použitých směrovačů Mikrotik

Model	RB3011UiAS-RM	hAP ac^2	hAP lite TC
Architektura	ARM 32bit	ARM 32bit	SMIPS
Frekvence procesoru [GHz]	1.4	0.716	0.650
RAM [MB]	1024	128	32
Úložiště [MB]	128	16	16
Počet portů ethernet	10	5	4
Maximální rychlost portů ethernet [Mbit/s]	1000	1000	100
Úroveň licence RouterOS	5	4	4
Modul WiFi	Ne	Ano	Ano
Podporované WiFi standardy	-	802.11b/g/n/ac	802.11b/g/n
Displej	Ano	Ne	Ne
USB Port	Ano	Ano	Ne

Tab. 1.1: Tabulka srovnání použitých směrovačů

2 Problematika služeb a monitorování

V současné době a v následujících letech bude kladen důraz na stále vyšší dostupnost služeb. Tato bakalářská práce se proto bude konkrétně věnovat službám zabývajícím se zprostředkováním vzdáleného přístupu pomocí virtuálních privátních sítí a jejich následném monitoringu pomocí nástrojů, které jsou obsaženy v operačním systému RouterOS v síťových prvcích Mikrotik.

2.1 Vybraná služba

2.1.1 Virtuální privátní síť

VPN slouží ke vzdálenému přístupu uživatelů k privátním sítím, které nejsou, z důvodu bezpečnosti, volně dostupné ve veřejné síti internet. Ve zkratce je VPN technologie, která zajistí zabezpečené spojení mezi uživatelem a privátní sítí, ke které se chce uživatel připojit. Tím je umožněn bezpečný přístup k souborům, zdrojům a přenosu dat, které jsou dostupné pouze v privátní síti.[18]

Komunikace mezi uživatelem a privátní sítí přes VPN je šifrovaná pomocí různých typů klíčů.

> „Virtuální privátní síť (VPN) je síť, která je vytvořena s využitím veřejné sítě – běžně skrze internet – pro připojení vzdálených uživatelů nebo regionálních kanceláří k soukromé interní síti společnosti.“[19]

Správně navržená síť VPN může být pro společnost velmi výhodná, například:

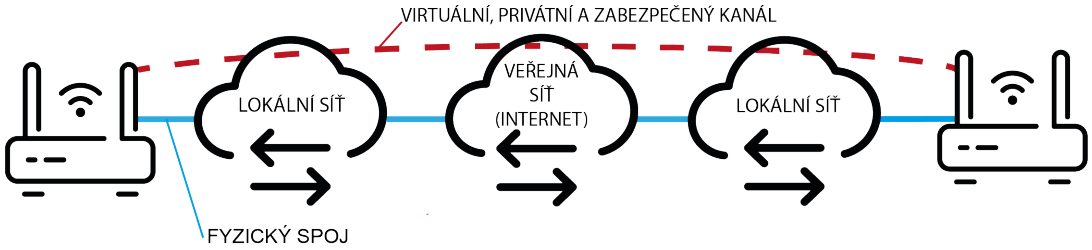
- rozšiřuje dostupnost připojení k síti
- snižuje provozní náklady v porovnání s klasickou sítí WAN
- snižuje přenosovou rychlost a náklady pro externí uživatele
- zvyšuje produktivitu (např. zaměstnanců, kdy dojde ke zjednodušení přístupu ke zdrojům sítě)
- zjednodušuje síťovou topologii
- umožňuje realizaci globální sítě
- nabízí telekomunikační podporu
- návratnost investice je rychlejší v porovnání s WAN sítí

2.1.2 Typy VPN

VPN se nejčastěji dělí na 2 hlavní druhy: Site-to-site a vzdálený přístup.[20] Oba typy jsou detailněji popsány níže.

Site-to-Site

Tento typ VPN je nejčastěji využíván velkými korporacemi, které mají za cíl spojit dvě nebo více privátních sítí do jedné virtuální sítě, aby bylo umožněno sdílet své zdroje, k tomuto spojení je využita veřejná síť, třeba internet. K takovému propojení dochází mezi dvěmi a více lokálními sítěmi (např. různé pobočky společnosti), které jsou často v různých zemích, tudíž dochází k vytvoření nadnárodní sítě. Tento typ VPN může být dále rozdělen na intranet a extranet. Intranet může být výše zmíněné spojení dvou či více lokálních sítí poboček kanceláří v rámci jedné korporace. Extranet slouží také pro spojení více lokálních sítí, ale na rozdíl od intranetu, tyto sítě nejsou vlastněny jednou korporací, ale je to spojení se sítí zákazníka či partnera.[20]



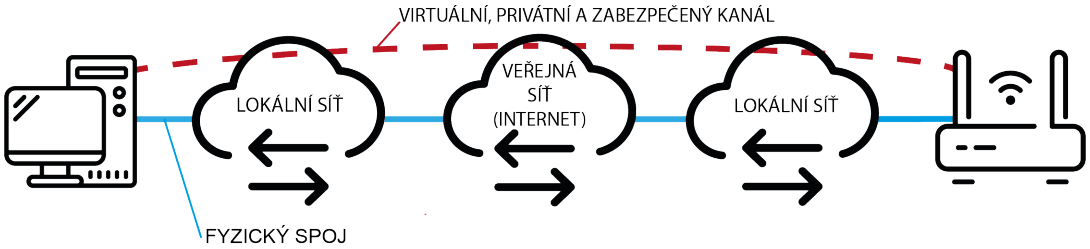
Obr. 2.1: Schéma Site-to-Site VPN.

Vzdálený přístup

Tento typ VPN může být také nazýván jako vytáčená virtuální privátní síť (Virtual Private Dial-up Network - VPDN). Uživatel se zde přes VPN tunelovací protokoly připojuje do privátní sítě např. zaměstnanec připojující se do privátní sítě zaměstnavatele. Často je tohle řešení využíváno uživateli, kteří se potřebují opakovaně připojovat do privátní sítě z různých lokalit, kde působí. Může se jednat o práci z domova, služební cestu nebo jinou situaci, kdy je nutné mít přístup k lokálním zdrojům sítě. V konkrétním případě, olomoucké společnosti, se jedná o zprostředkování spojení mezi privátní sítí a vývojáři, kteří potřebují přístup k databázovým serverům, vývojovému prostředí, či potřebují vystupovat v síti internet pod veřejnou IP olomoucké kanceláře, která má vytvořené přístupy do dalších systémů zákazníků.

2.1.3 Protokoly VPN

Pro použití VPN je možný výběr z několika typů protokolů. Tato práce je zaměřena na zařízení z rodiny Mikrotik, proto byly zvoleny protokoly, které jsou podporované systémem RouterOS. Jedná se o protokoly PPTP, SSTP, OpenVPN a L2TP. Způsob připojení, který bude v této práci využíván je vzdálený přístup.



Obr. 2.2: Schéma vzdáleného přístupu VPN.

Při implementaci VPN např. do podnikové sítě je nutné myslet na koncové uživatele, kteří budou VPN využívat a k jakému účelu bude VPN využívána. V praxi to znamená, vytvořit nejprve přehled uživatelských zařízení, které jsou v dané organizaci a podle toho pak zvolit protokol. Důvodem je ten, že každý protokol má omezený počet platforem, které podporuje, proto je třeba zvážit jaký typ OS využívají pracovní stanice v dané organizaci, zda se jedná o OS Windows, Linux nebo OSX. Rovněž je třeba brát v úvahu jestli bude nutné připojit k VPN také mobilní zařízení a pokud ano, s jakým mobilním OS tato zařízení pracují. A v neposlední řadě je třeba brát v potaz také úroveň zabezpečení, kterou organizace vyžaduje. Srovnání všech protokolů, které jsou v této práci použity, je přehledně zobrazen v tabulce 2.1

PPTP

Tento protokol patří mezi nejstarší protokoly, které se pro VPN používají. Jeho původ sahá do devadesátých let 20. století. Původní verze tohoto protokolu nenabízela žádnou možnost šifrování. Popularita tohoto protokolu přišla s operačním systémem Windows od Microsoftu, kdy byly implementovány i šifrovací mechanismy. Protokol je podporovaný kromě Windows také operačními systémy macOS[1], iOS[2], Android a Linux.

Výhodou tohoto protokolu je především rychlost a jednoduchost implementace, což je stále jeden z důvodů, proč je tento protokol využívaný i na vzdory nízkému zabezpečení. Rychlost protokolu je dána absencí pokročilého šifrování komunikace.

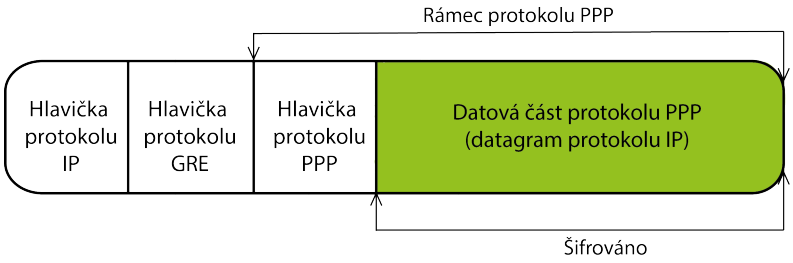
Největší nevýhodou tohoto protokolu je již zmíněná nízká úroveň zabezpečení a také fakt, že šifrování pap, chap, mschap1 i mschap2, které tento protokol využívá, byly již prolomeny. Je třeba podotknout, že zneužití dat jedincem je sice nepravděpodobné, ale při dostatku zdrojů útočníka je únik dat pro organizaci výraznou

[1]U macOS Apple ukončil podporu PPTP v nativním VPN klientu od verze OSX 10.11 a vyšších (El Capitan).[21]

[2]U iOS skončila podpora PPTP od verze iOS 10 a vyšších.[22]

hrozbou. Z pohledu datové bezpečnosti je protokol PPTP považován jako nešifrovaný z důvodu prolomení šifrovacích mechanismů, které využívá. Před použitím tohoto protokolu je důležité určit, k jakému účelu bude využíván a jaká data budou tímto tunelem protékat.[24]

Struktura paketu PPTP, který obsahuje uživatelská data, je zobrazena na obr. 2.3. Pro vytvoření tunelu je použito spojení pomocí protokolu TCP. Protokol GRE je pak využit k zapouzdření PPP rámce. Data uvnitř rámce pak mohou být šifrovaná.[24]



Obr. 2.3: Struktura paketu protokolu PPTP.

SSTP

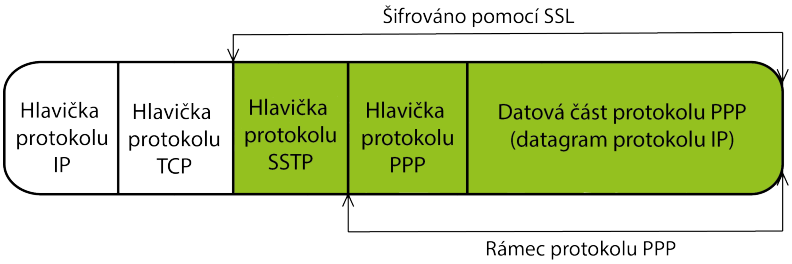
Protokol SSTP je proprietárním protokolem společnosti Microsoft, která jej vytvořila a vyvíjí. Nejčastěji je spojován s operačními systémy z dílny této společnosti. Šifrování komunikace je zajištěno pomocí SSL 3.0[3]. Protokol využívá pro komunikaci protokol TCP s portem 443. To znamená velkou výhodu pro použití v oblastech, kde jsou používány technologie pro blokování VPN. Tato výhoda je zajištěna zmíněnou šifrovanou komunikací na portu 443, kterou je velmi obtížné zablokovat.[24]

Protokol SSTP nejprve zapouzdří PPP hlavičku a část s původními daty do PPP rámce. K tomuto rámci je pak přiložena hlavička SSTP a tyto části jsou poté zašifrovány protokolem SSTP. Poté jsou přiloženy hlavičky TCP a IP.[25] Celá struktura paketu je popsaná na obr. 2.4.

L2TP/IPSec

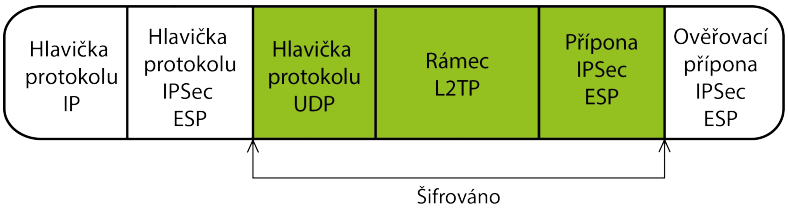
Protokol L2TP je využíván pro vytvoření „tunelu“ mezi jednotlivými zařízeními. Komunikace probíhá pomocí protokolu UDP na portu 1701. L2TP sám o sobě nenabízí žádný druh šifrování. Z toho důvodu je využíván ve spojení s protokolem IPSec, které se stará o zabezpečení protékaných dat.[26]

[3]V roce 2014 bylo vydáno oficiální upozornění od Microsoftu o potenciální zranitelnosti tohoto protokolu.[23]



Obr. 2.4: Struktura paketu protokolu SSTP.

K rámci L2TP, který obsahuje data, je přidána hlavička UPD a přípona IPSec ESP. Tato celá část je poté zašifrována. K zašifrovaným datům je poté přiložena hlavička a ověřovací přípona protokolu IPSec, které zajišťují autentizaci a integritu dat. Celá struktura paketu je poté dostupná na obr. 2.5.

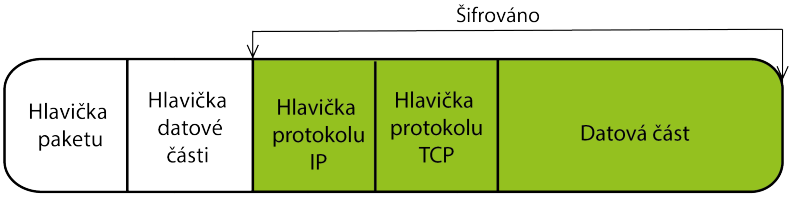


Obr. 2.5: Struktura paketu protokolu L2TP zabezpečeného pomocí IPSec.

OpenVPN

Protokol OpenVPN je vydán jako open source a využívá protokoly SSLv3 a TLSv1 pro zabezpečení. Nativně probíhá jeho provoz na protokolu UDP s portem 1194, ale může být také konfigurován pro protokol TCP. Nevýhodou je nutnost použití software třetích stran na většině operačních systémů.

Struktura paketu protokolu OpenVPN je znázorněna na obr. 2.6, kdy kdy k datové části paketu jsou přidány hlavičky protokolů IP a TCP, které jsou poté zašifrovány pomocí SSL. K zašifrované části paketu je poté přiložena hlavička datové části a hlavička paketu.



Obr. 2.6: Struktura paketu protokolu OpenVPN.

Srovnání použitých VPN protokolů

Protokol	PPTP	SSTP	L2TP	OpenVPN
Tvůrce	Microsoft	Microsoft	Microsoft & Cisco	Opensource (GNU GPL)
Šifrování	Max. 128-bit	Max. 256-bit	Max. 256-bit	Max. 256-bit
Standardní port	1723	443	1701	1194
Protokol transportní vrstvy	TCP	TCP	UDP	UDP
Podporované platformy	Windows, Android, Linux, RouterOS	Windows, Linux, RouterOS	Windows, MacOS, Android, iOS, Linux, RouterOS	Windows, MacOS, Android, iOS, Linux, RouterOS
Výhody	Rychlost, jednoduchost	Průchodnost skrz firewall	Zabezpečení	Certifikace, bezpečnost
Nevýhody	Zabezpečení, chybějící podpora nových OS	Rychlost, teoretická zranitelnost SSL	Náročnost na výkon CPU	Komplikovanost instalace, nutné použití SW třetích stran pro implementaci

Tab. 2.1: Srovnání použitých VPN protokolů

2.2 Síťové modely

Protože komunikace v datových sítích probíhá v různých fázích, bylo nutné definovat způsoby komunikace. Samotná komunikace byla rozdělena do několika vrstev, kdy každá vrstva má svůj vlastní způsob jak řešit dané úkoly. Samotná realizace komunikace je řešena pomocí komunikačních protokolů. Každá vrstva má své vlastní protokoly, se kterými pracuje.

2.2.1 Referenční model OSI/ISO

V počátcích datové komunikace si každá společnost řešila způsob komunikace v síti vlastním způsobem, to vedlo k velké nesourodosti, protože byly většinou vzájemně nekompatibilní a často ani nebylo možné je v vzájemně propojit. Proto byl zaveden OSI model, který byl vytvořen v ISO (International Organization for Standardization). Tento model popisuje veškeré potřebné součásti, aby mohla zařízení mezi sebou korektně komunikovat. Postupně se stal výchozím modelem pro počítačově řízenou komunikaci. Model se skládá celkem ze sedmi vrstev, které se číslují od nejnižší vrstvy vzestupně. Příklad komunikace mezi jednotlivými vrstvami lze vidět na obr. 2.7. Postupně si rozebereme všechny vrstvy tohoto modelu.

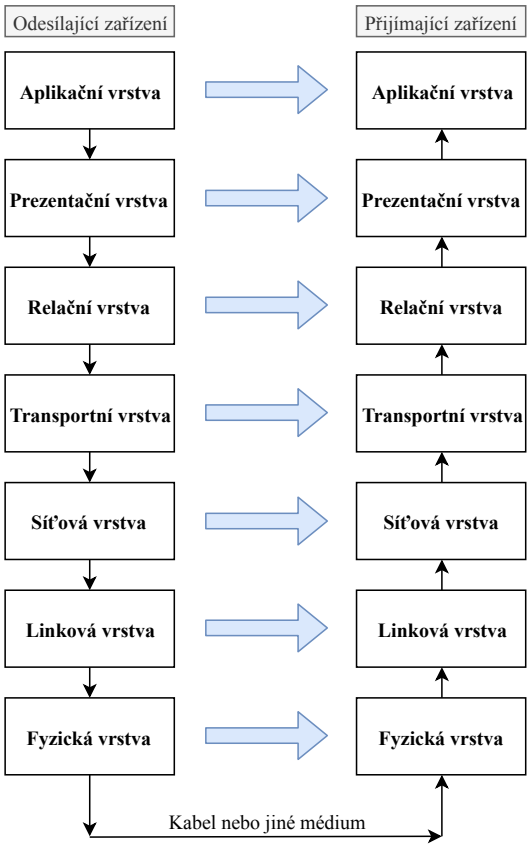
Přehled jednotlivých vrstev:
1. Fyzická vrstva
2. Spojová vrstva
3. Síťová vrstva
4. Transportní vrstva
5. Relační vrstva
6. Prezentační vrstva
7. Aplikační vrstva

Fyzická vrstva (Physical Layer)

Jedná se o nejnižší vrstvu síťového modelu OSI/ISO. Tato vrstva se stará o přenos dat ve formě „nul a jedniček“. Jejím úkolem je mimo jiné sestavení spojení mezi jednotlivými zařízeními, efektivní rozložení zdrojů napříč všemi uživateli a zařízeními. Součástí této vrstvy jsou také převodníky(A/D, D/A), které slouží ke konverzi dat. Na této vrstvě pracují také různá, zejména jednodušší, zařízení a to třeba rozbočovače, opakovače, síťové karty a modemy. [27]

Spojová vrstva (Data Link Layer)

Často označovaná jako linková vrstva je druhou nejnižší vrstvou modelu OSI/ISO.



Obr. 2.7: Komunikace jednotlivých vrstev v OSI/ISO modelu.

Základní funkcí je přeměna bitového datového toku, se kterým pracuje fyzická vrstva, na datové bloky neboli rámce. Jak už vyplývá z jejího názvu, tak spojová vrstva vytváří spojení, ty vznikají z pravidla dynamicky a dynamicky také zanikají. To znamená, že spojení vznikají podle potřeby a nedochází tak ke zbytečnému plýtvání šířky pásma. Zařízení na této vrstvě jsou mosty a přepínače.[27]

Tato vrstva se dále dělí na dvě podvrstvy a to:

- MAC (Media Access Control)
- LLC (Logical Link Control)

Síťová vrstva (Network Layer)

Síťová vrstva je třetí nejnižší vrstvou referenčního OSI/ISO modelu. Jejím hlavním úkolem je směrování, adresování a přenos datagramů. Určitě nejznámější protokol, který na této vrstvě pracuje je protokol IP. Rovněž se tato vrstva stará o definici priorit protékaného datového toku (princip QoS - Quality of Service). Hlavním zařízením, které pracuje na této vrstvě je směrovač (router).[27]

Transportní vrstva (Transport Layer)

Tato vrstva zajišťuje adresování přímo ke konkrétním aplikacím. To zajišťuje pomocí portů. O samotné spojení se tato vrstva již nestará, protože tím se zabývají nižší vrstvy. Veškeré protokoly, pracující na této vrstvě, jsou koncové, neboli end-to-end. Nejčastěji používanými protokoly jsou TCP a UDP. Hlavním rozdílem mezi těmito protokoly je, že protokol TCP je „se spojením“, zatímco protokol UDP je „bez spojení“, tzn. TCP protokol nejprve vytvoří spojení a až poté, co se ujistí, že je spojení úspěšné, začne vysílat samotná data. Naopak protokol UDP se o bezpečné spojení nestará a místo toho rovnou vysílá pakety příjemci. Z toho nám vyplývá, že protokol UDP má sice nižší zpoždění, ale chybovost je mnohem větší.[27]

Relační vrstva (Session Layer)

Relační vrstva se stará o synchronizaci a organizaci komunikačního dialogu. Obsahuje mechanizmy pro otevírání, zavírání a řízení tohoto dialogu. Vhodným příkladem popisu její funkce je například videohovor. U videohovoru potřebujeme sesynchronizovat obrazovou a zvukovou složku tak, aby pohyby úst odpovídaly vydávanému zvuku.[27]

Prezentační vrstva (Presentation Layer)

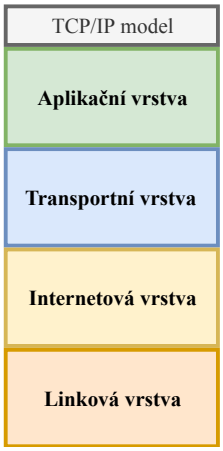
Šestou nejvyšší vrstvou je vrstva Prezentační, která je často označována jako „překladač“ dat, které jsou pak dále zpracována nebo přímo zobrazována. Má na starosti také šifrování, dešifrování a kompresi přenášených dat. Je také jedinou vrstvou, která může přímo zasáhnout do těchto dat. Pracuje zde také velké množství různých bran, které slouží jako propojovací body mezi různými sítěmi. Jedná se na příklad o emailovou bránu.[27]

Aplikační vrstva (Application Layer)

Nejvyšší, tedy sedmou vrstvou, je aplikační vrstva. Jak již z názvu vyplývá, tak zprostředkovává aplikacím přístup ke komunikačnímu systému. Většina protokolů, které se podílejí na funkčnosti internetu, tak jak jej dnes známe, pracuje na této vrstvě. Jedná se třeba o protokoly DNS, HTTP, HTTPS a další. Poskytuje a stará se také o další služby jako jsou například elektronická pošta, přenos souborů, vzdálený přístup k počítačům, ať již konzolový nebo s grafickým rozhraním a také, v poslední době velmi důležitému: streamování videa.[27]

2.2.2 Síťový model TCP/IP

Na rozdíl od modelu OSI/ISO, který má sedm vrstev, má TCP/IP model pouze čtyři vrstvy. Došlo zde tedy ke zjednodušení a sloučení vrstev. Hlavní odlišností tohoto modelu je větší kladený důraz na samotné koncové stanice, kdy se předpokládá již určitá inteligence těchto stanic, tudíž je možné jim přenechat některé funkce, zatímco model OSI/ISO předpokládá méně inteligentní koncová zařízení, tudíž se snaží komunikaci co nejvíce rozložit a rozvětvit.



Obr. 2.8: Posloupnost vrstev TCP/IP modelu.

Vrstva síťového rozhraní (Network Interface Layer)

Tato vrstva bývá někdy nazývána také linkovou vrstvou (link layer). Pracuje přímo na konkrétních síťových zařízeních. Důkazem vysoké flexibility modelu je, že na této vrstvě nejsou přímo specifikované protokoly a používá tak jakékoli dostupné síťové rozhraní.[28]

Internetová vrstva (Internetwork Layer)

Internetová vrstva již není přímo závislá na konkrétních přenosových technologiích. Hlavním protokolem, který na této vrstvě pracuje, je IP protokol. Tento protokol je bez spojení, čili není tak spolehlivý jako komunikace na nižších vrstvách. Internetový protokol nám neposkytuje kontrolu datového toku ani zotavení z chyb. Tyto funkce jsou obsaženy ve vyšších vrstvách.

Jednotkou internetového protokolu jsou datagramy. Ty jsou vysílány do koncové destinace, ale již se neřeší potvrzení o jejich doručení příjemci. Jedná se o nespolehlivý přenos dat.

Další známé protokoly, které pracují na této vrstvě jsou ICMP, IGMP a nebo ARP.[28]

Transportní vrstva (Transport Layer)

Často bývá označována i jako TCP vrstva a to díky TCP protokolu, který nejčastěji zprostředkovává přenos dat. Na rozdíl od internetového protokolu se stará o spolehlivý přenos dat se spojením. Můžeme zde také řídit datový tok a vytvořit z ne spojového přenosu přenos se spojením.

I když je TCP nejvíce používaným protokolem, tak je možné využívat služeb dalších protokolů. Dalším hojně používaným protokolem je protokol UDP. Hlavní odlišností od TCP je vynechání zajištění spolehlivosti přenosu dat. To využíváme u aplikací, které komunikují v reálném čase. Jedná se třeba třeba o video-hovory, on-line hry a další. Ve zkratce jsou to aplikace, které potřebují rychlý přenos dat a jsou schopné tolerovat ztrátu určité části přenášených dat.[28]

Aplikační vrstva (Application Layer)

Na této vrstvě operuje největší množství protokolů. Patří mezi ně například protokol HTTP, FTP, DHCP a další. Tato vrstva komunikuje přímo s vrstvou transportní. Rozhraní mezi transportní a aplikační vrstvou jsou definována pomocí portů.[28]

2.3 Monitorování přístupových sítí

Jedná se o systém, který konstantně nebo v určitých intervalech sleduje stav počítačové sítě. Podle požadavků, které si stanoví ať už zákazník nebo správce sítě, můžeme sledovat různé parametry sítě. Daný systém bude pak obsluhu různými varovat před krizovými situacemi. Může se jednat o výpadky, zpomalení datového provozu, ztrátu spojení, ztrátu napájení, prolomení zabezpečení sítě a nebo prosté sledování toku dat a informací o síti. Notifikace může probíhat různými způsoby a to jak již při krizových situacích, tak při pravidelných informačních zprávách.

Ikdyž je práce primárně zaměřena na monitorování provozovaných služeb na prvcích Mikrotik, tak tyto nástroje, obsažené v systému RouterOS, nejsou jediné, které jsou na trhu dostupné. Z tohoto důvodu jsou v kapitole 2.3.2 popsány také externí monitorovací nástroje, které je možné využít pro monitoring přístupové sítě.

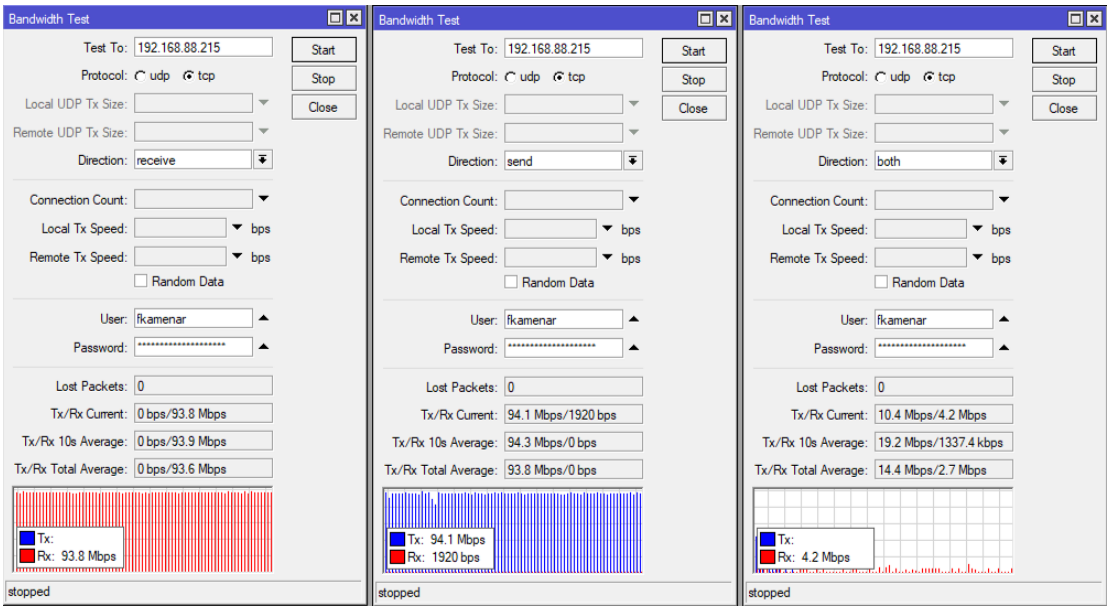
2.3.1 Integrované monitorovací nástroje v systému RouterOS

Bandwidth Test

Bandwidth test je nástroj sloužící k měření šířky pásma mezi dvěma směrovači Mikrotik. Měření šířky pásma mezi jednotlivými směrovači je využívání k objevení kritických míst sítě. Měření může probíhat s využitím protokolu TCP nebo UDP.[29]

Pro měření sítě s pomocí nástroje Bandwidth Test, byla vytvořena lokální síť, která se skládala ze směrovačů hAP ac^2 a hAP lite TC. Tyto směrovače jsou přímo spojeny ethernetovým kabelem typu cat 6 o délce 5 metrů. Podle srovnávací tabulky jednotlivých směrovačů 1.1 bylo zjištěno, že směrovač hAP ac^2 má ethernetové porty o rychlosti 1000 Mbit/s a směrovač hAP lite TC má porty o rychlosti 100 Mbit/s. To znamená, že maximální teoretická rychlost komunikace mezi směrovači může být 100 Mbit/s.

Na obrázku 2.9 jsou uvedeny výsledky měření. Měření bylo provedeno na směrovači hAP ac^2 s využitím protokolu TCP pro odeslání dat, příjem dat a kombinovaného spojení. Dle celkového průměru (Total Average) byla rychlost pro odesílání dat 93,6 Mbit/s, pro příjem dat 93,8 Mb/s a pro kombinované spojení byla celková průměrná rychlost odesílání 14,4 Mbit/s a přijímání 2,7 Mbit/s.

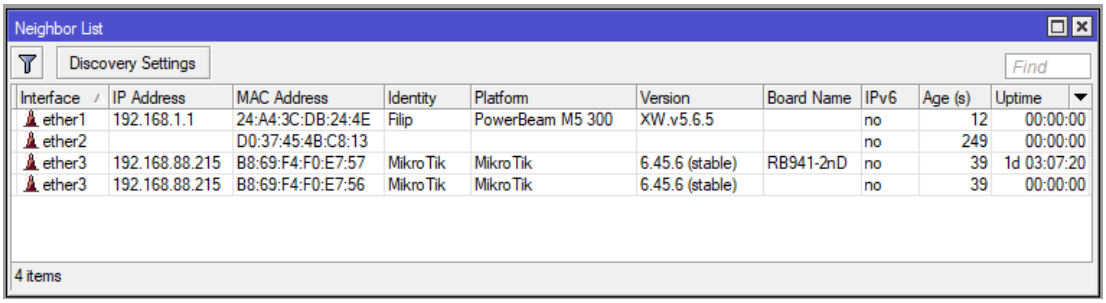


Obr. 2.9: Měření šířky pásma s využitím nástroje Bandwidth Test.

Neighbors

Nástroj Neighbor slouží k vyhledání okolních zařízení skrze protokoly MNDP, CDP a LLDP. Rozhraní směrovače, na kterých bude vyhledávání prováděno, je možné upravit v nastavení tohoto nástroje.[30]

Ukázka výstupních dat tohoto nástroje je pak na obrázku 2.10. Zde je možné vidět, že v této testovací lokální síti jsou dostupnými zařízeními směrovače PowerBeam M5 300 a RB941-2nD. Rovněž je u obou směrovačů možné vidět nasazenou verzi software a u směrovače RB941-2nD je možné také vidět aktuální dobu spuštění. U každého záznamu je možné zobrazit i detail s podrobným popisem o daném zařízení. Ukázka detailu zařízení je na obrázku 2.11.



Obr. 2.10: Nástroj Neighbors.

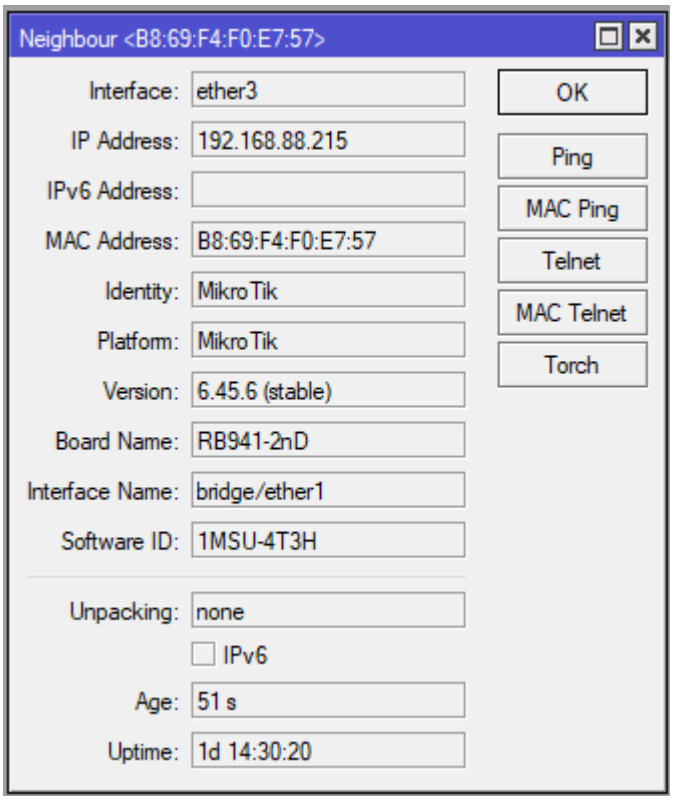
Traffic Monitor

Tento nástroj slouží pro monitorování datového provozu, který směrovačem protéká.

Při nastavení nového pravidla v Traffic Monitoru je nutné upřesnit následující položky:

- název pravidla,
- rozhraní, které bude monitorováno,
- typ datového provozu - přijaté pakety/odeslané pakety,
- spouštěč,
- limit,
- událost (skript).

Nástroj Traffic Monitor je vhodný pro sledování jednotlivých rozhraní směrovače. Je možné vytvořit pro každé rozhraní vlastní pravidlo se specifickými parametry a podmínkami. Po sepnutí pravidla je vyvolána událost, která je definována libovolným skriptem, který je naprogramován obsluhou.



Obr. 2.11: Detail zařízení v nástroji Neighbors.

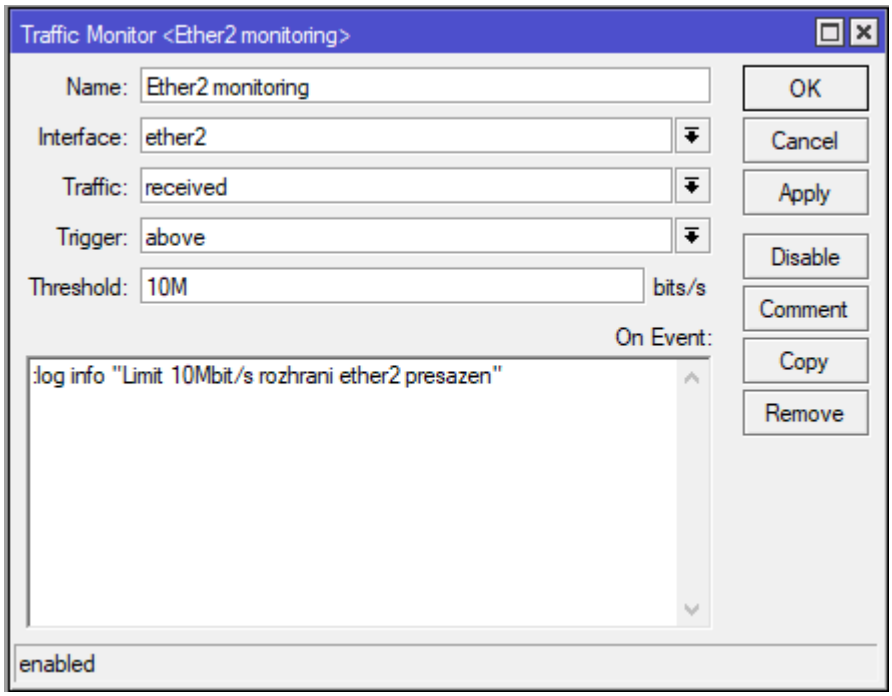
V příkladu na obrázku 2.12 je popsáno pravidlo, které monitoruje množství stažených dat na rozhraní „ether2“. Při překročení limitu 10 Mbit/s bude do logu směrovače vypsaná událost typu „info“ ve znění „Limit 10 Mbit/s rozhrani ether2 presazen“.

Traffic Flow

Traffic flow je nástroj, který poskytuje statistické informace o paketech, které prochází směrovačem. Díky tomu mohou systémoví administrátoři, kteří danou síť spravují, identifikovat různé problémy, které se ve sledované síti objeví. Rovněž mohou i analyzovat stav sítě a díky získaným datům také optimalizovat síť pro vyšší výkonnost.[31]

Příklad nástroje Traffic Flow na obrázku 2.13 je nastaven na odesílání dat ze směrovače Mikrotik na cílovou IP „192.168.88.240“ s portem 2055. V tomto příkladu jsou data, která odesílá Traffic Flow, sbírány nástrojem nProbe[4] a vizualizovány pomocí webové aplikace ntopng[5]. Příklad vizualizace sesbíraných dat je na obrázku

[4] <https://www.ntop.org/products/netflow/nprobe/>.
[5] <https://www.ntop.org/products/traffic-analysis/ntop/>.



Obr. 2.12: Ukázkové pravidlo nástroje Traffic Monitor.

2.14.

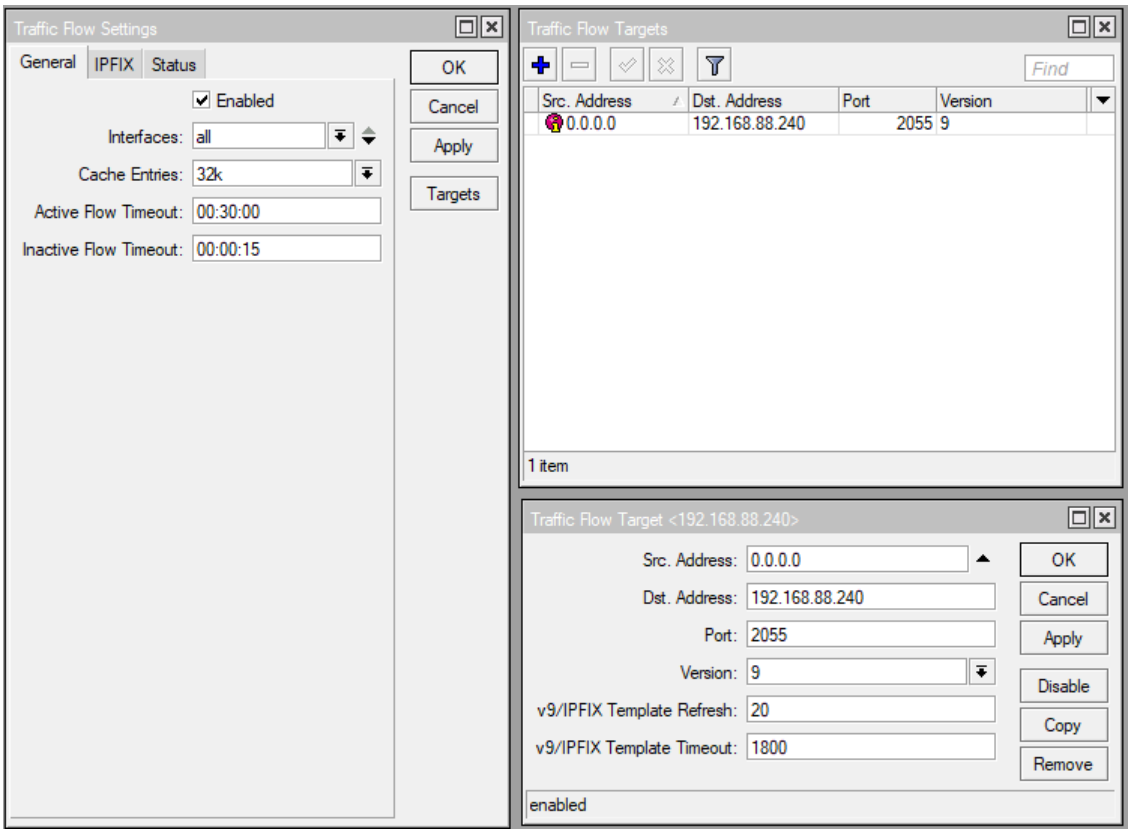
Ping

Ping využívá protokol ICMP, který pracuje na internetové vrstvě síťového modelu TCP/IP. Při pingu odesílá host diagnostické zprávy ICMP „echo request“ (ICMP zpráva typu 8) na vzdálený server (IP adresa). Po vyslání zprávy „Echo request“ čeká host na odpověď typu „echo reply“ (ICMP zpráva typu 0) od vzdáleného serveru. Čas mezi jednotlivými požadavky se nazývá latencí neboli prodleva. Pokud je odezva delší než nastavený časový limit (timeout), tak je předpokládáno, že čas vypršel a není možné se v daném časovém limitu spojit se vzdáleným serverem.[32]

> „Ping označuje latenci neboli délku prodlevy mezi dvěma síťovými rozhraními.“[33]

Při použití nástroje ping je možné v RouterOS nastavit tyto základní parametry[34]:

- IP adresa vzdáleného serveru na který bude odeslán požadavek (Ping To),
- rozhraní, odkud bude odeslán požadavek (Interface),
- celkové množství odeslaných paketů (Packet count),
- časový limit, po jehož uplynutí je paket označen jako ztracený (Timeout),
- velikost odeslaných paketů (Packet Size),



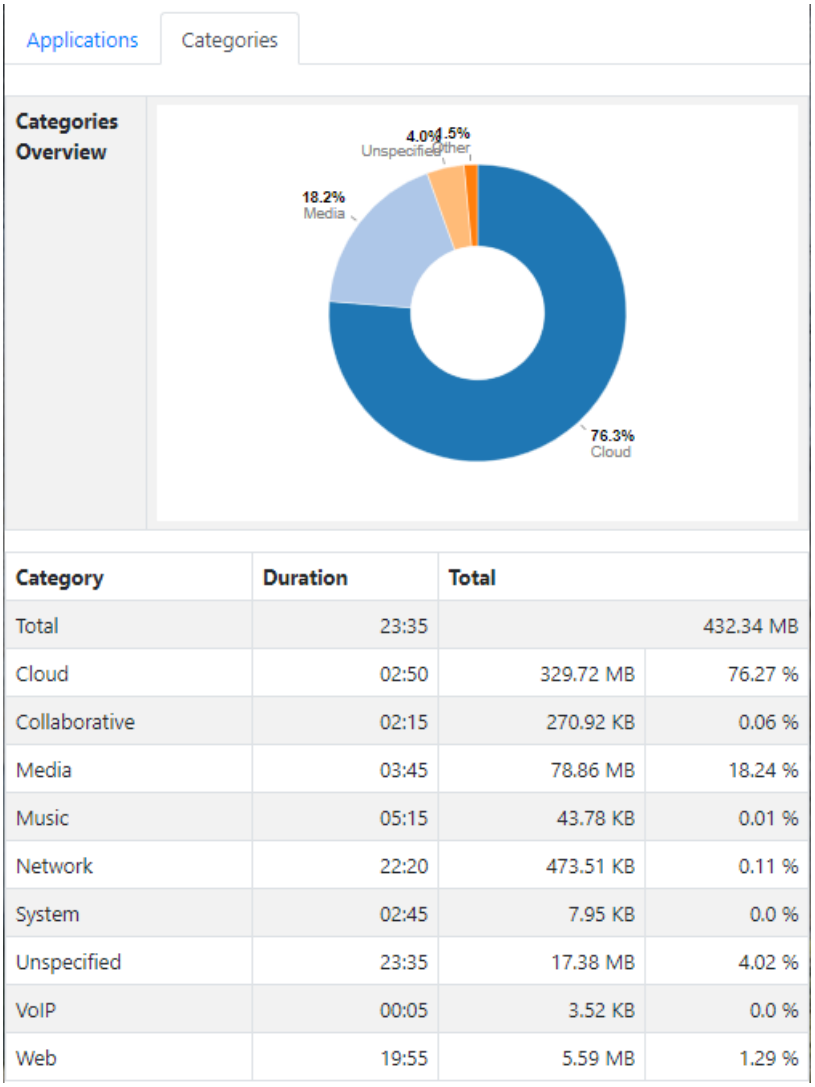
Obr. 2.13: Nástavení nástroje Traffic Flow.

- dobu platnosti (TTL).

Na obrázku 2.15 je pak možné vidět průběh nástroje ping v systému RouterOS. Nástroj ve spodní části okna zobrazí ztrátovost, nejnižší a nejvyšší dobu odezvy a také spočítá průměrnou dobu odezvy.

V testovacím měření byly odesílány pakety na vzdálený server s IP adresou 8.8.8.8, což je veřejný DNS server společnosti Google.[35] Celkově se vrátilo 999 paketů z 1000 odeslaných, po zaokrouhlení ztrátovost činila 0 %. Velikost paketů byla 50 bytů. Nejnižší doba latence byla 6 ms a nejvyšší 48 ms, průměrná doba latence pak byla 6 ms.

Tato průměrná hodnota latence je velmi dobrá a pokud by tato hodnota nabývala stejné velikosti i pro spojení s VoIP serverem, tak by dostačovala pro plynulý hovor, protože dle společnosti Cisco, by při VoIP hovoru neměla latence překročit hranici 150 ms.[36]



Category	Duration	Total	
Total	23:35		432.34 MB
Cloud	02:50	329.72 MB	76.27 %
Collaborative	02:15	270.92 KB	0.06 %
Media	03:45	78.86 MB	18.24 %
Music	05:15	43.78 KB	0.01 %
Network	22:20	473.51 KB	0.11 %
System	02:45	7.95 KB	0.0 %
Unspecified	23:35	17.38 MB	4.02 %
VoIP	00:05	3.52 KB	0.0 %
Web	19:55	5.59 MB	1.29 %

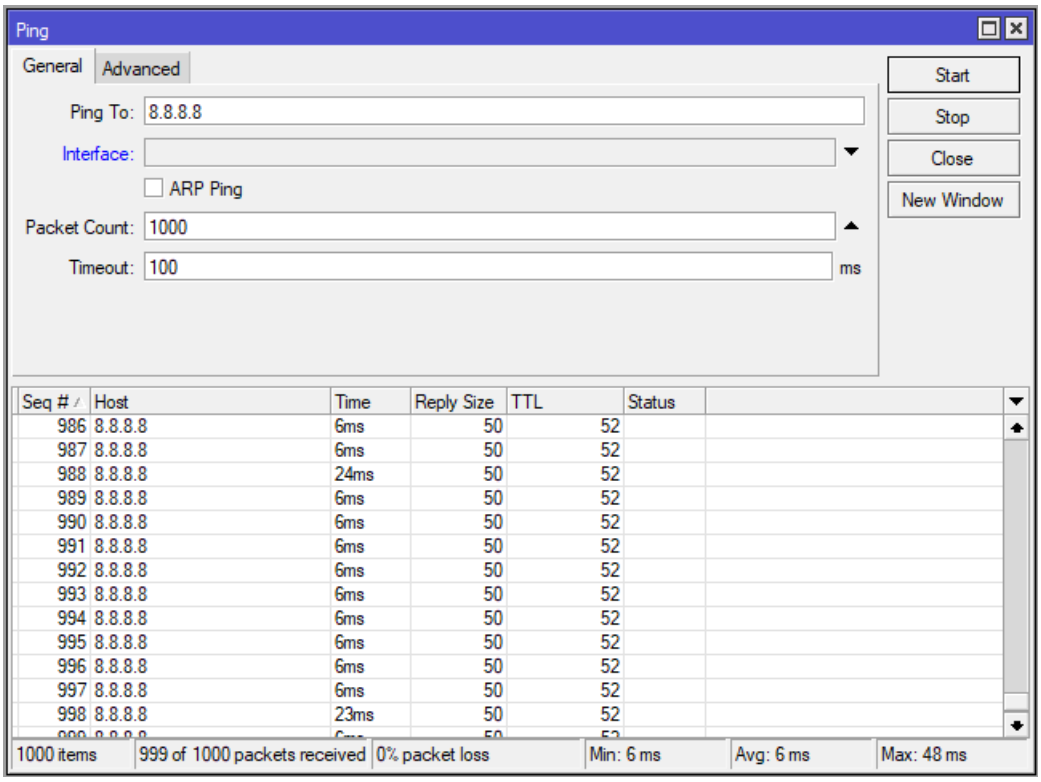
Obr. 2.14: Ukázka vizualizace dat v nástroji ntopng.

Flood Ping

Nástroj Flood Ping je velmi podobný nástroji Ping, který je rovněž popsaný v kapitole 2.3.1. Jak už z názvu vypovídá[6], tento typ nástroje slouží k odeslání většího počtu ICMP Echo požadavků na zvolené zařízení v síti. V ideálním případě pak bude doručeno stejné množství požadavků, jako bylo odesláno. Pokud by byla ztrátovost požadavků vysoká, nebo by byl čas RTT[7] příliš vysoký, tak by to mohlo indikovat na případné kritické místo v síti.[38]

[6]Flood může být přeloženo z anglického jazyka jako záplava. Doslovný překlad by tedy mohl být „záplava pingu“.

[7]Hodnota RTT znamená rozdíl času od odeslání prvního bitu příjemci po doručení posledního bitu příslušného TCP Acknowledgment.[39]



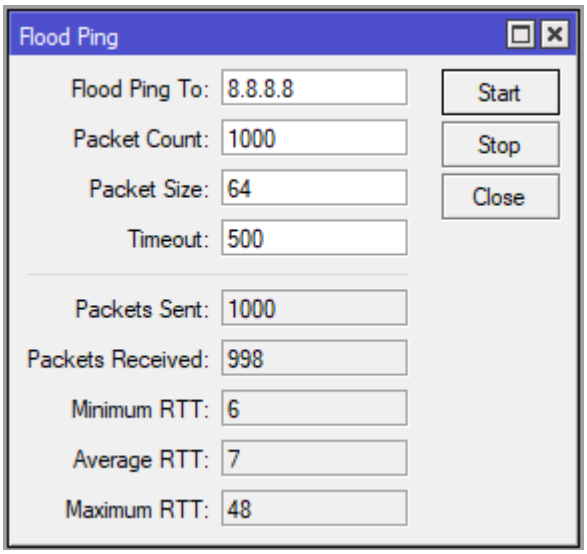
Obr. 2.15: Nástroj Ping.

Hlavní odlišnost Flood Pingu od běžného Pingu je ve výpisu dat uživateli. Ping zobrazí uživateli jednotlivě vypsané echo požadavky v řádcích, zatímco Flood Ping odesílá požadavky na pozadí a uživateli zobrazí pouze výsledek měření. Příklad použití nástroje Flood Ping je na obrázku 2.16.

Popis jednotlivých parametrů nástroje Flood Ping, obrázek 2.16:

- Flood Ping To,
  - IP adresa vzdáleného serveru na který bude odeslán požadavek.
- Packet Count,
  - Celkové množství odeslaných paketů.
- Packet size,
  - Velikost odeslaných paketů.
- Timeout,
  - Časový limit, po jehož uplynutí je paket označen jako ztracený.
- Packets Sent,
  - Celkové množství odeslaných paketů ICMP „echo request“.
- Packets Received,
  - Celkové množství přijatých paketů ICMP „echo reply“.

- Minimum, Average, Maximum RTT.
  - Minimální, průměrná a maximální hodnota obousměrného zpoždění.



Obr. 2.16: Nástroj Flood Ping.

Ping Speed

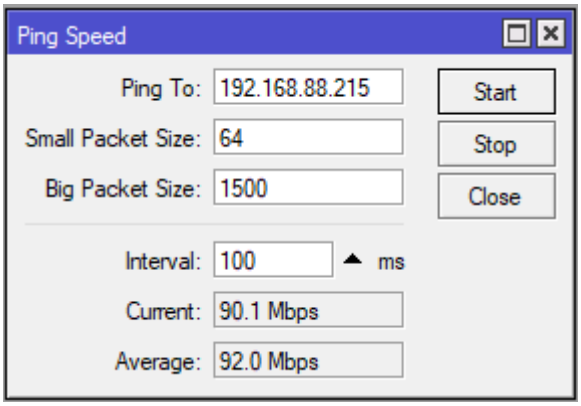
Tento nástroj slouží k určení přibližné propustnosti linky pomocí ICMP zpráv „echo request“ a „echo reply“. Při měření jsou použity dvě různé velikosti paketů. Jedná se o malé a velké pakety, jejich velikost je možné ručně nastavit dle daných potřeb. V průběhu měření jsou tyto dva druhy paketů střídavě odesílány.[40]

Naměřené hodnoty šířky pásma nástrojem Ping Speed není možné srovnávat s hodnotami, které jsou naměřeny nástrojem Bandwidth Test. Důvodem je, že Ping Speed využívá protokol ICMP, který pracuje na internetové vrstvě síťového modelu TCP/IP, zatímco Bandwidth Test využívá protokoly UDP nebo TCP, které pracují na transportní vrstvě síťového modelu TCP/IP.

Popis jednotlivých parametrů nástroje Ping Speed, obrázek 2.17:

- Ping To,
  - IP adresa vzdáleného serveru na který budou odeslány požadavky.
- Small Packet Size,
  - Velikost malých ICMP paketů v bytech.
- Big Packet Size,
  - Velikost velkých ICMP paketů v bytech.
- Interval,

  - Prodleva mezi jednotlivými pakety.
- Current, Average.
  - Aktuální a průměrná velikost naměřené šířky pásma.



Obr. 2.17: Nástroj Ping Speed.

Traceroute

Nástroj traceroute[8] zobrazuje seznam směrovačů, přes které paket musí projít, než je doručen do cílové destinace. Traceroute využívá, obdobně jako ping, protokol ICMP.[37]

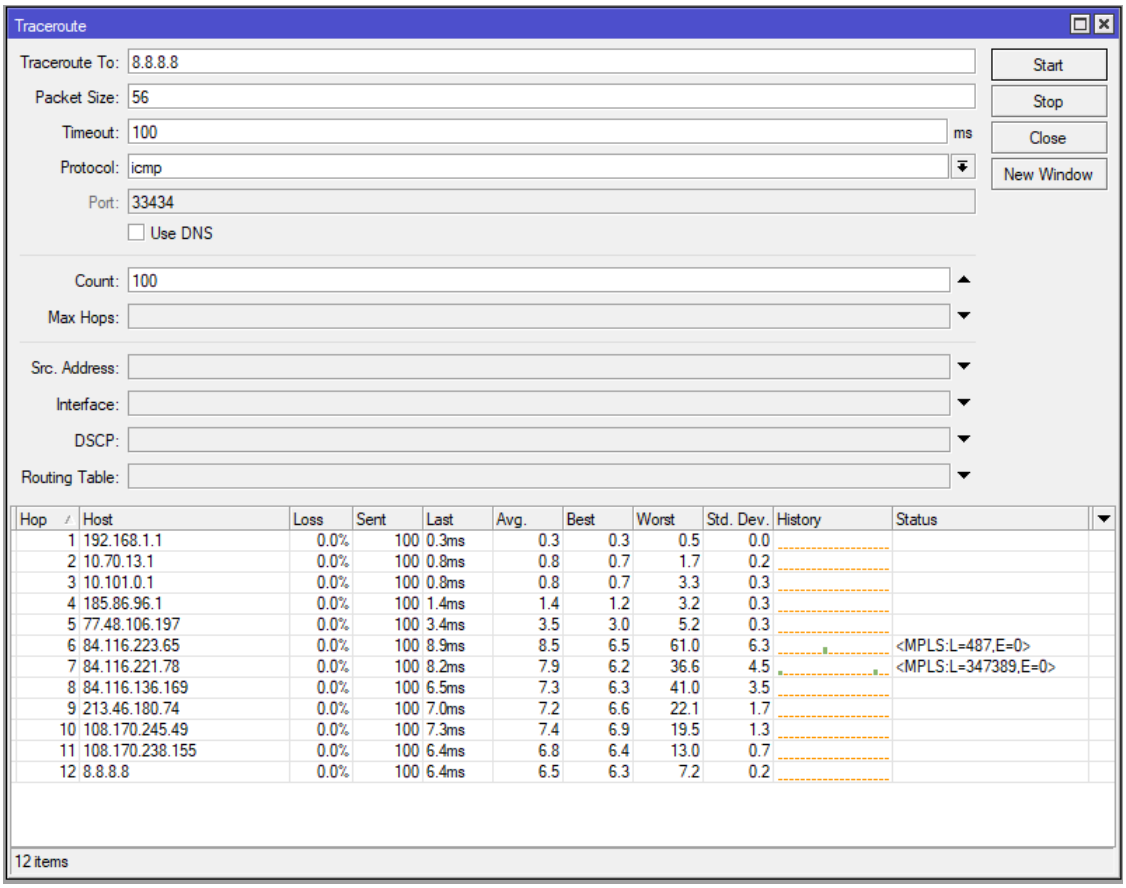
Tento nástroj je často využíván systémovými administrátory pro diagnostikování chyb, či zpoždění při spojení mezi hostem a vzdáleným serverem. Při výpisu jednotlivých skoků je možné vidět odezvu u každého směrovače, kterým musí paket po své cestě projít. Pokud není paket doručen až do cílové destinace, uvidí administrátor poslední směrovač, kterým paket prošel, čímž bude odkázán na možný zdroj chyby.

Jako koncový bod testovacího měření byl zvolen DNS server od společnosti Google s IP adresou 8.8.8.8. Velikost paketu byla 56 bytů, časový limit 100 ms a počet odeslání požadavku byl sto. Při měření bylo zjištěno, že paket, odeslaný ze směrovače v lokální síti, musí po cestě k DNS serveru 8.8.8.8 udělat 12 přeskoků.

Torch

Torch slouží k monitorování datového provozu v reálném čase, které zařízením protéká. Množství dat, které mají být monitorována, je možné detailně specifikovat

[8] V operačním systému Windows je možné tento nástroj naleznout pod názvem „tracert“.



Obr. 2.18: Nástroj Traceroute.

úpravou jednotlivých parametrů.[41]

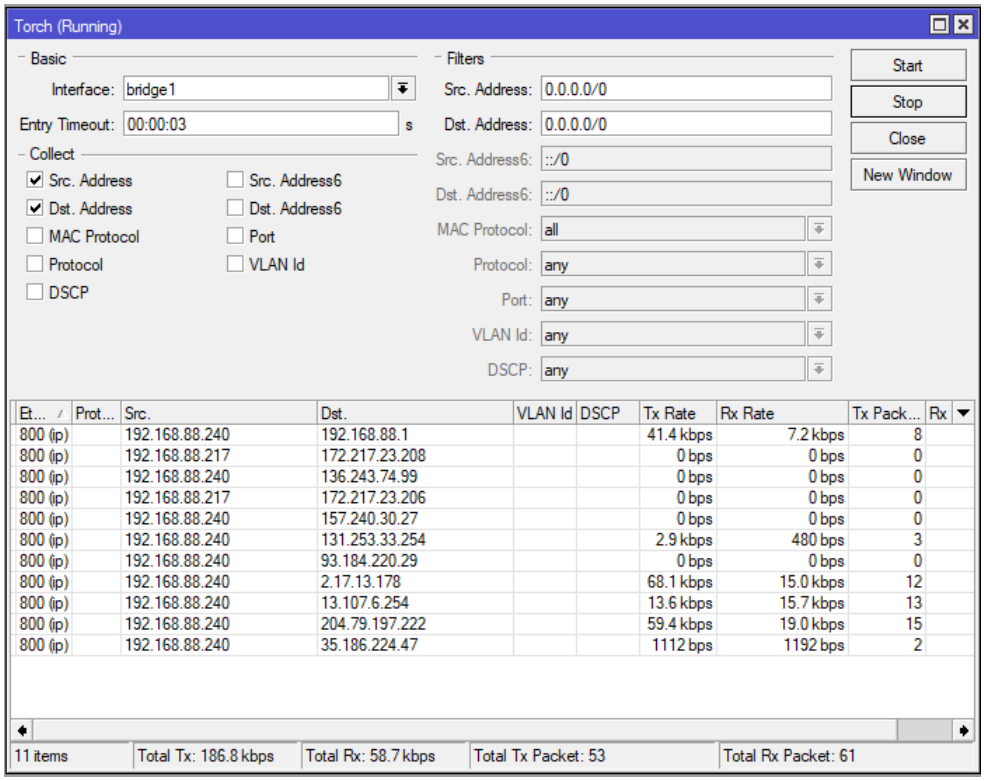
Přehled parametrů, které je možné specifikovat:

- rozhraní (Interface),
- časový limit (Timeout),
- výchozí adresa (IPv4 i IPv6),
- cílová adresa (IPv4 i IPv6),
- MAC protokol,
- protokol,
- DSCP,
- port,
- VLAN Id.

Data, která jsou sbírána, je pak možné dále třídit dle následujících filtrů:

- konkrétní výchozí adresa (IPv4 i IPv6),
- konkrétní cílová adresa (IPv4 i IPv6),
- typ MAC protokolu,
- typ protokolu,

- číslo portu,
- VLAN Id.
- hodnota DSCP.



Obr. 2.19: Nástroj Torch.

Watchdog

Funkce watchdog slouží k nastavení automatického restartu zařízení Mikrotik při chybovém stavu. Obsluha může být může o výpadcích informována odesláním emailové notifikace. Detekce výpadku nástroje watchdog může být dvojího typu:[42]

- Softwarový watchdog časovač, který je nejčastěji spuštěn hardwarovou chybou zařízení. V tomto případě, pokud bude zařízení více než šedesát sekund nedostupné, tak RouterOS zahájí restart systému (parametr watchdog-timer).
- Ping watchdog, kdy zařízení automaticky odesílá požadavky na vzdálené zařízení a v případě, že po určité době nepřijde od zařízení odpověď, tak RouterOS zahájí restart systému (parametr watch-address).

Popis jednotlivých parametrů funkce watchdog, obrázek 2.20:

- Watchdog Timer,
  - Hlídání chybových stavů zařízení, v případě nedostupnosti zahájen automatický restart zařízení.

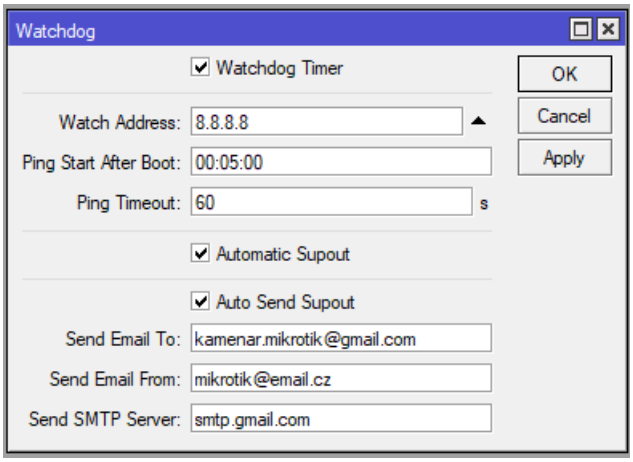
- Watch Address,
  - Sledované vzdálené zařízení definované IP adresou.
- Ping Start After Boot,
  - Doba od restartu zařízení, kdy má být opět zahájen ping na vzdálené zařízení.
- Ping Timeout,
  - Specifikace časového intervalu, ve kterém bude šest krát odeslána zpráva typu „Echo request“. Podrobnější popis funkce ping je uveden v kapitole 2.3.1.
- Automatic Supout,
  - Pokud nastane chyba SW, tak bude vytvořen soubor „autosupout.rif“, kde bude uveden detailní popis chyby. Pokud již tento soubor existuje, tak bude přejmenován na „autosupout.old.rif“.
- Auto Send Supout,
  - Vygenerovaný chybový soubor „autosupout.rif“, může být odeslán obsluze emailovou zprávou.
- Send Email To,
  - Emailová adresa příjemce notifikace.
- Send Email From,
  - Emailová adresa odesílatele notifikace.
- Send SMTP Server.
  - Adresa SMTP serveru, kterým bude emailová notifikace odeslána.

V příkladu, uvedeném na obrázku 2.20, je nastavena funkce „softwarový watchdog“ i „ping watchdog“. Ping watchdog sleduje IP adresu 8.8.8.8, s opětovným spuštěním pingu po pěti minutách od restartu a časovým intervalem 60 sekund pro ping. V případě výpadku je zapnuta funkce „Auto Send Supout“, která odešle obsluze notifikaci z emailové adresy „mikrotik@email.cz“ na emailovou adresu „kamenar.mikrotik@gmail.com“ skrz SMTP server „smtp.gmail.com“.

Packet Sniffer

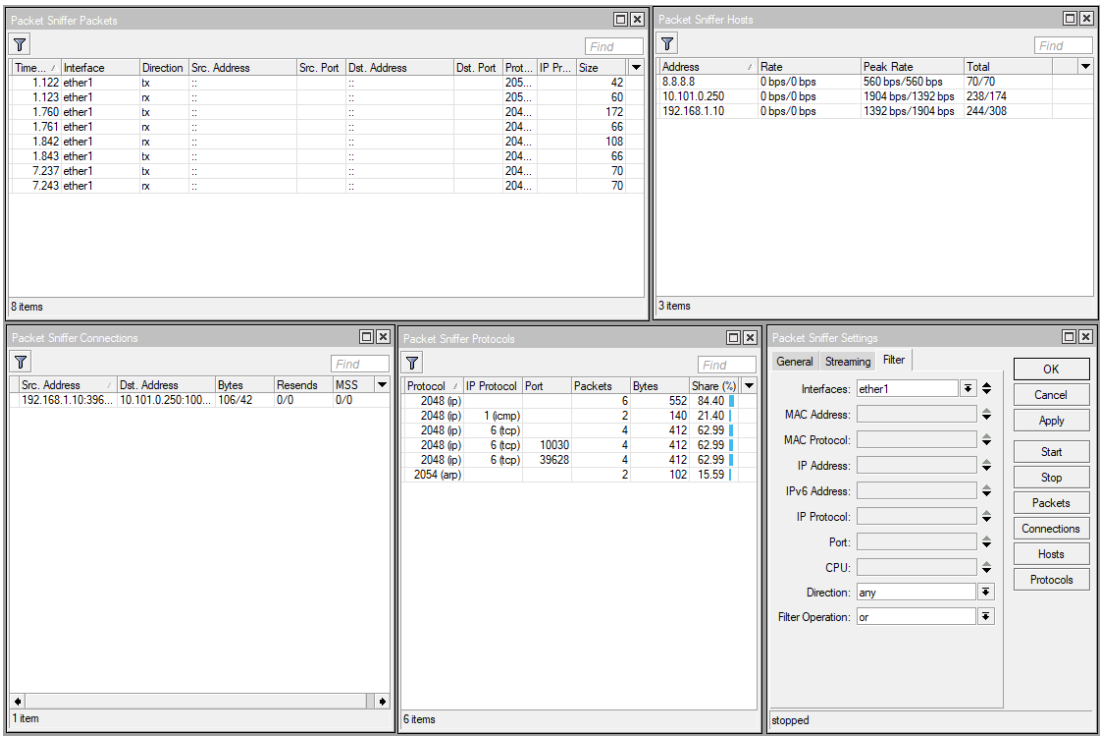
Packet Sniffer je nástroj, který umožňuje zachytit a analyzovat jednotlivé pakety, které daným zařízením prochází. Činnost packet sniffing je velmi užitečná při diagnostice sítě nebo ochraně proti případnému napadnutí sítě.[43]

Tento nástroj umožňuje obsluze zachytávat pakety, spojení, protokoly a velikost datového toku s jednotlivými hosty. Zachytávaná data je také možné filtrovat dle jednotlivých parametrů. Průběh zachytávání dat je možné zobrazit na obrázku 2.21. Data, která jsou sbírána, je možné také odesílat v reálném čase na vzdálený server.



Obr. 2.20: Nástroj Watchdog.

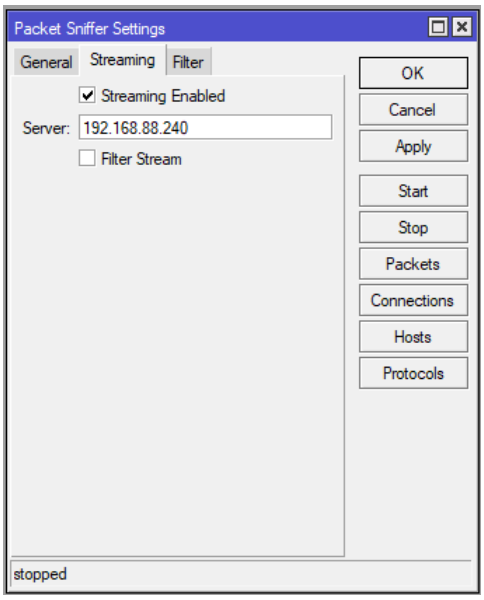
Detail specifikace serveru je uveden na obrázku 2.22.



Obr. 2.21: Nástroj Packet Sniffer.

Netwatch

Netwatch je svou funkčností velmi podobný nástroji „Ping Watchdog“, který je popsaný v kapitole 2.3.1. Netwatch, obdobně jako ping watchdog, sleduje stav



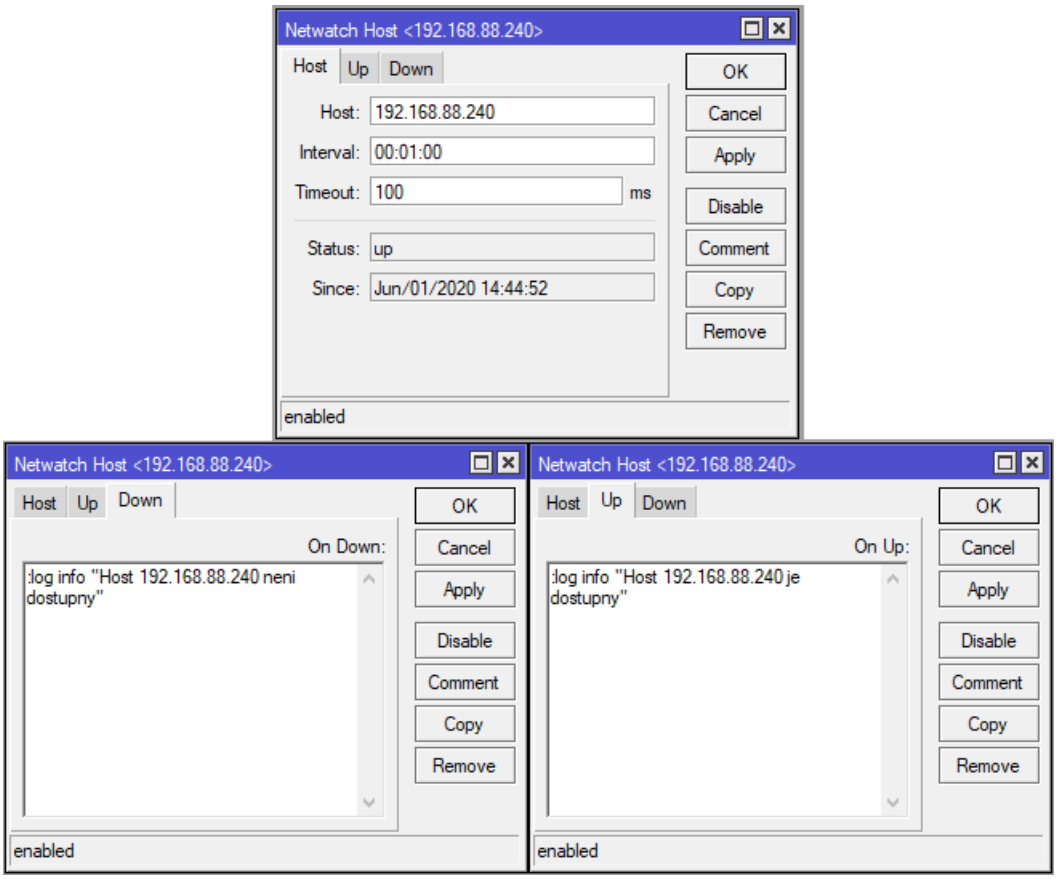
Obr. 2.22: Odesílání sbíraných dat z nástroje packet sniffer na vzdálený server.

vzdáleného zařízení pomocí odesílání ICMP požadavků. Rozdílem je, že zatímco watchdog nabízí již předem připravené scénáře, které nastanou při výpadku, tak netwatch umožňuje ruční konfiguraci následných činností, pomocí skriptu při dostupnosti nebo nedostupnosti sledovaného zařízení.[44]

Parametry nástroje netwatch:

- Host,
  - IP adresa sledovaného zařízení.
- Interval,
  - Časový interval mezi odeslanými ICMP požadavky na sledované zařízení.
- Timeout,
  - Časový interval po jehož uplynutí je předpokládáno, že je sledované zařízení nedostupné.
- On Up,
  - Skript, který je proveden, pokud je sledované zařízení dostupné.
- On down.
  - Skript, který je proveden, pokud je sledované zařízení nedostupné.

Na obrázku 2.23 je možná varianta nastavení nástroje netwatch. V tomto ukázkovém případě probíhá ověření dostupnosti zařízení s IP adresou „192.168.88.240“. Četnost odesílání požadavku je jedna minuta s časovým intervalem 100ms. Pokud je zařízení dostupné, tak je do logu zařízení vypsána hláška typu info s textem „Host 192.168.88.240 je dostupny“. V případě, že zařízení dostupné není, je vypsána do logu informační hláška „Host 192.168.88.240 neni dostupny“.



Obr. 2.23: Nástroj Netwatch.

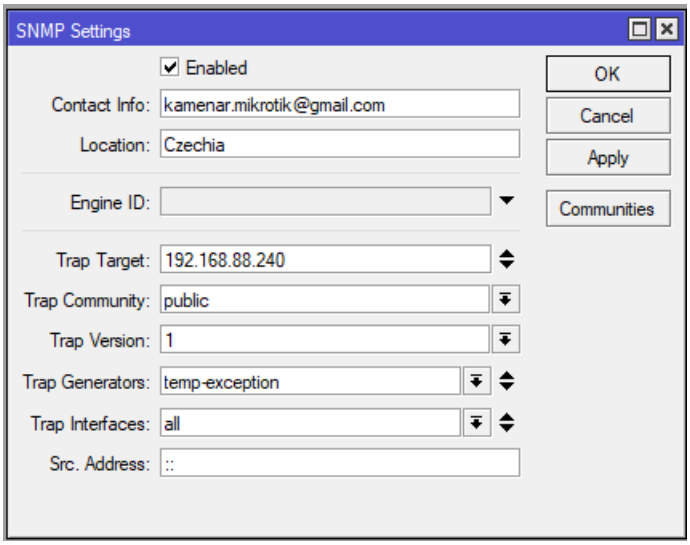
SNMP

Protokol SNMP není vlastním nástrojem systému RouterOS, ale jedná se o standardní protokol pro správu zařízení v IP sítích. Data posílané protokolem SNMP mohou sbírat různé externí monitorovací nástroje jako jsou např. Cacti nebo The Dude. Tyto nástroje jsou popsány v kapitole 2.3.2.[45]

2.3.2 Externí monitorovací nástroje

Kromě nástrojů pro monitorování sítě, které jsou obsaženy v systému RouterOS od Mikrotiku, je možné také použít různé externí nástroje. Tyto nástroje jsou vhodné do situací, kdy monitorovaná síť není postavena na prvcích Mikrotik a nebo zadavatel požaduje větší množství monitorovacích funkcí, či chce na danou síť aplikovat pokročilejší analýzu nasbíraných dat.

Tyto nástroje mohou být rozděleny do dvou hlavních kategorií.



Obr. 2.24: Konfigurace SNMP.

První kategorií jsou nástroje softwarové. Tyto nástroje jsou instalovány na již existující servery v síti a sbírají data, které jim posílají jednotlivé síťové prvky v síti. V případě, že již daný server, na který bude softwarový nástroj instalován, v síti existuje, tak není nutné do sítě vkládat jakýkoliv nový síťový prvek. Příkladem těchto nástrojů jsou např. NetFlow Analyzer, The Dude, či Cacti.

Druhou kategorií jsou monitorovací nástroje založené vlastních hardwarových prvcích. To znamená, že v případě využití tohoto typu nástrojů, je nutné vložit do sledované sítě další síťový prvek. Tyto nástroje poskytují velké množství analytických nástrojů pro monitorování sítě, ale i pro analýzu chování jednotlivých uživatelů, kteří se v síti nachází. Nevýhodou pak může být náročnější instalace prvku do sítě a také určitá forma nedůvěry z pohledu bezpečnosti, protože je nutné do sítě umístit externí prvek, který zachytává veškerý provoz na síti. Příkladem těchto nástrojů mohou být Flowmon Collector a Mendel.

Tato kapitola slouží pro ucelení čtenářovy představy o možnostech a dostupnosti externích nástrojů pro sledování sítě.

Flowmon Collector

Řešení od společnosti Flowmon spočívá v zapojení monitorovacího centra přímo do stávající sítě. Toto centrum bude následně měřit, zachytávat a kontrolovat datový tok v dané síti. Následně přikládaný software dokáže vykreslit naměřené hodnoty do grafů a zpracovat statistiky o různých stavech sítě.

Nevýhodou tohoto řešení je nutnost zapojení dalšího prvku do sítě, což může odradit spoustu zákazníků, kteří nebudou mít důvěru a ochotu si nechat připojit

do sítě „cizí“ zařízení. [46]

Obr. 2.25: Ukázka prostředí FLOWMON MONITORING CENTER.

Mendel

Toto řešení je vyvíjeno společností GREYCORTEX. Jeho hlavní doménou je zabezpečení sítě a ochrana před vnějšími hrozbami. Kromě aplikace na tradiční počítačové sítě je možné jej nasadit i na sítě SCADA/ICS.

Opět je zde nutné připojit externí zařízení do monitorované sítě. Výhodou tohoto systému je automatické naučení sítě do které se zařízení připojí. [47]

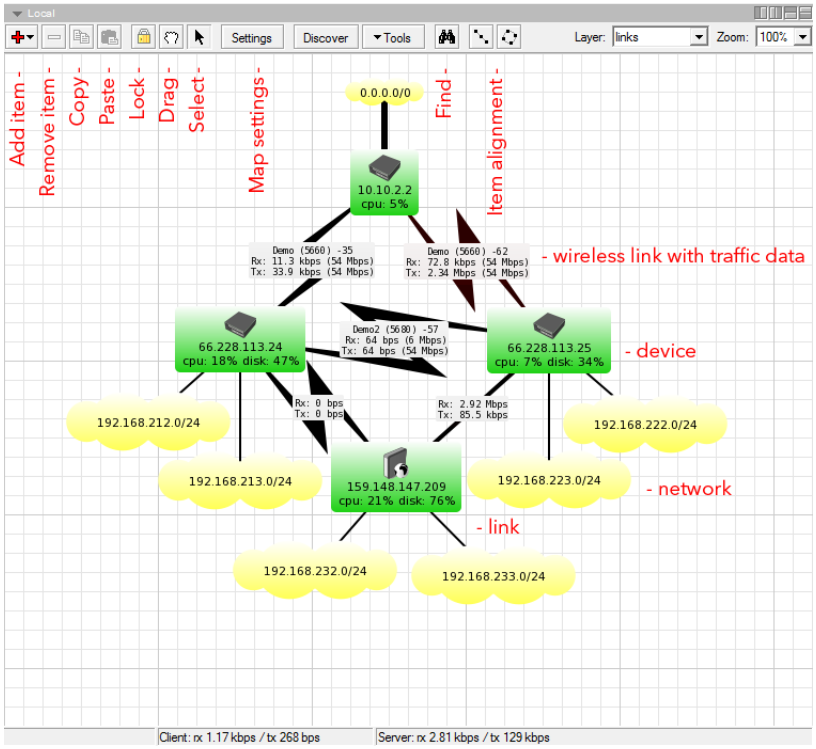
NetFlow Analyzer

Software NetFlow Analyzer je vyvíjen společností ManageEngine. Pro zavedení tohoto řešení není nutné instalovat hardwarové zařízení. V tom spočívá velká výhoda oproti systémům Mendel a Flowmon Collector. Software stačí pouze nainstalovat, ovšem je nutné ověřit, aby software podporoval síťová zařízení používaná v síti. Tento systém se zaměřuje z velké části na sítě, které jsou založeny na síťových prvcích od společnosti Cisco. [48]

Obr. 2.26: Ukázka prostředí GREYCORTEX MENDEL.

The Dude

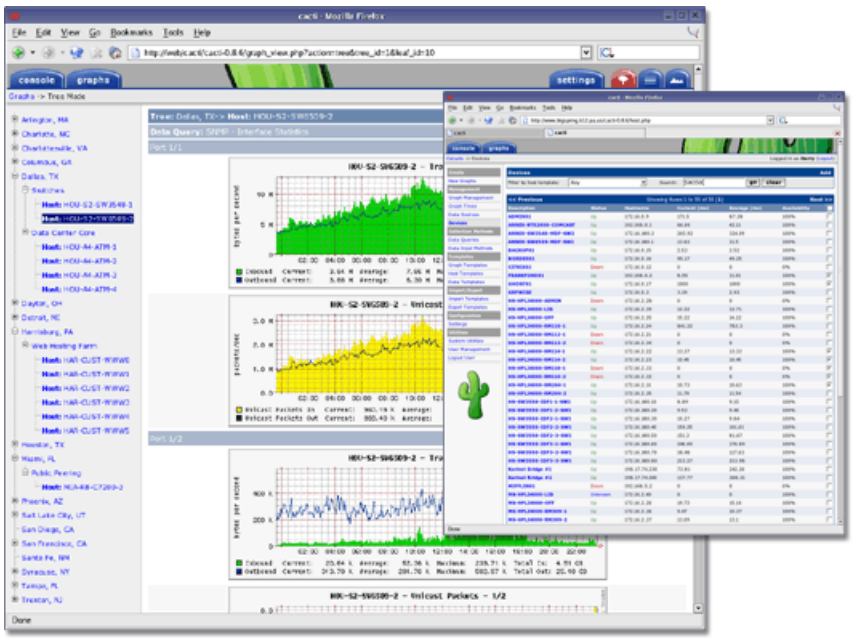
The Dude monitor je služba vyvíjena společností MikroTik. Toto řešení je omezeno pouze na síťová zařízení od tohoto výrobce. Oproti předchozím systémům je značně jednodušší a méně intuitivní. Tento software se doinstaluje jako volitelný balíček, přímo na síťové prvky. Slouží především pro vykreslení sítě a sledování vytížení jednotlivých linek. [49]



Obr. 2.27: Ukázka vykreslení sítě softwarem The Dude.

Cacti

Cacti je open-source systém pro monitorování sítě. Pro jeho správnou funkci je nutné získávat data pomocí skriptů. Tento program dokáže z nasbíraných dat tvořit statistiky a grafy. Z námi popisovaných nástrojů se jedná o nejjednodušší a nejméně uživatelsky přívětivý nástroj pro monitorování sítě. [50]



Obr. 2.28: Ukázka prostředí nástroje Cacti.

3 Konfigurace služby VPN

3.1 Serverová část

Jako hlavní server, který bude sloužit pro hostování všech jednotlivých VPN serverů bude využit směrovač RB3011UiAS-RM, který je popsaný v kapitole 1.3.1. Tento směrovač se nachází v Olomouckém kraji. Jednotlivé VPN servery budou nastaveny v rámci operačního systému RouterOS, který je popsaný v kapitole 1.1.

3.1.1 Společná konfigurace jednotlivých serverů

Pro všechny typy VPN byly použity stejné hodnoty MTU a MRU, pro obě tato hodnota činí 1500. Hodnota MTU stanoví maximální velikost paketu, který může být odeslán bez paketové fragmentace. Obdobně MRU slouží pro stanovení maximální velikosti přijatého paketu bez použití paketové fragmentace. Rovněž hodnota Keepalive Timeoutu je stejná na všech serverech, konkrétně 120 vteřin. Keepalive Timeout stanoví dobu času výpadku, po kterou se bude server snažit o opětovné navázání spojení s klientem.

IP Pool

Pro všechny vytvořené VPN servery byl zvolen rozsah IP adres 172.16.22.10–172.16.22.50. K tomuto účelu je vhodné vytvořit IP Pool (rozsah), který tyto adresy bude obsahovat. Příkaz pro nastavení poolu je možné najít ve výpisu 3.1.

```
ip pool add name="VPN_Pool" ranges
   =172.16.22.10-172.16.22.50
```

Výpis 3.1: Příkaz pro vytvoření IP Poolu.

PPP Profile

Následně je nutné vytvořit PPP Profile, který definuje výchozí vlastnosti serveru a uživatelů, kteří jej použijí. Konzolový příkaz pro vytvoření profilu je uveden ve výpisu 3.2.

```
ppp profile add name="VPN_Profile" local-address
   =172.16.22.1 remote-address=VPN_Pool
```

Výpis 3.2: Příkaz pro vytvoření PPP Profilu.

PPP Secrets

Zde jsou vytvořeny účty jednotlivých uživatelů, kteří mohou využívat VPN. V tomto případě byl vytvořen pro každou lokalitu, která bude měřena, jeden uživatelský účet. Účtům bylo přiřazeno přihlašovací jméno, heslo, PPP profile a Service (VPN služba). U všech účtů byl zvolen PPP Profile „VPN_Profile“ a typ služby byl ponechaný jako „any“[1]. Důvodem je, že pro měření vlastností jednotlivých protokolů bude u dané lokality použit jeden uživatelský účet pro všechny použité typy VPN protokolů. Další parametry není nutné vyplnit.

Vytvořené účty:

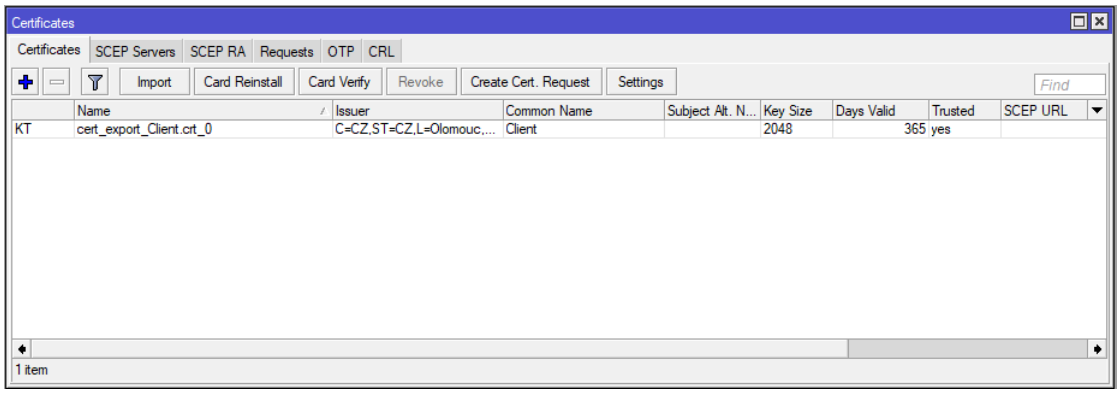
- client.brno
- client.egypt
- client.ukraine
- client.homeoffice

Certificates

Protokoly SSTP a OVPN používají certifikáty pro zabezpečení komunikace. Tyto certifikáty je možné vygenerovat ověřenou certifikační autoritou a nebo je možné certifikát vytvořit přímo v systému RouterOS. V této práci jsou použity certifikáty vygenerované v RouterOS.

Nejprve je nutné vytvořit certifikát „CA“, který bude sloužit pro podepsání následujících certifikátů.

Poté je třeba vytvořit certifikát pro server a také certifikát pro klienta. Klientský certifikát je poté třeba vyexportovat ze směrovače ve tvaru PEM a poté nahrát na jednotlivé klienty. Při exportování certifikátu bude vyexportován také klíč (KEY), obě části je nutné importovat na klientské zařízení.



Obr. 3.1: Správa certifikátů v RouterOS, nástroj Certificates.

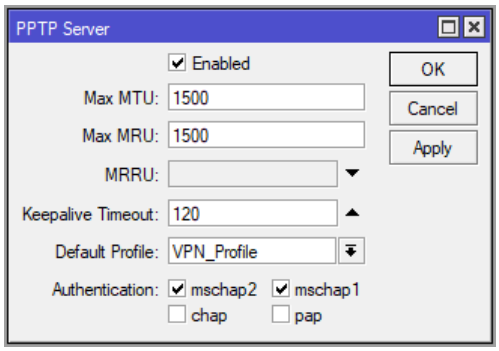
[1] „any“ znamená v překladu „jakákoliv.“

3.1.2 Server PPTP

Konfigurace serveru

PPTP server je, i díky méně komplexnímu zabezpečení, nejméně komplikovaným protokolem k nasazení na server. Výchozím profilem serveru je „VPN_Profile“. Detail konfigurace PPTP serveru je možné zobrazit na obrázku 3.2.

Pole „authentication“ pak nabízí metody, které je možné použít pro autentizaci. V tomto případě byly zvoleny metody „mschap1“ a „mschap2“. Tyto metody byly zvoleny z důvody vyšší bezpečnosti než u metody „pap“, verze „ms“ pak byla zvolena z důvodu podpory operačních systémů od společnosti Microsoft.[51]



Obr. 3.2: Nastavení PPTP serveru.

Firewall pravidlo

Aby mohl být klient připojen, je třeba vytvořit ve firewallu pravidlo, které připojení umožní.

PPTP využívá protokol TCP, který pracuje na portu 1723. Pravidlo tedy musí být s řetězcem typu „vstup“(input) s akcí „povolit“. Přesné znění příkazu pro zavedení tohoto pravidla je možné naleznout ve výpisu 3.3.

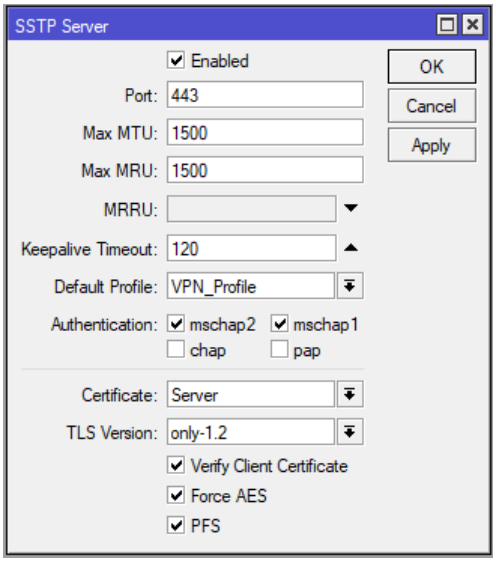
```
chain=input protocol=tcp dst-port=1723 action=accept
   comment="Allow PPTP"
```

Výpis 3.3: Firewall pravidlo - PPTP.

3.1.3 Server SSTP

Konfigurace serveru

Nastavení SSTP serveru je velmi podobné jako u PPTP, ovšem s rozdílem, že u SSTP je využit také certifikát, který je popsán v kapitole 3.1.1. Náhled konfigurace serveru je pak na obrázku 3.3.



Obr. 3.3: Nastavení SSTP serveru.

Firewall pravidlo

Firewallové pravidlo je obdobné jako u PPTP. SSTP pro svou funkci využívá protokol TCP s portem 443.

```
chain=input protocol=tcp dst-port=443 action=accept
   comment="Allow SSTP"
```

Výpis 3.4: Firewall pravidlo - SSTP.

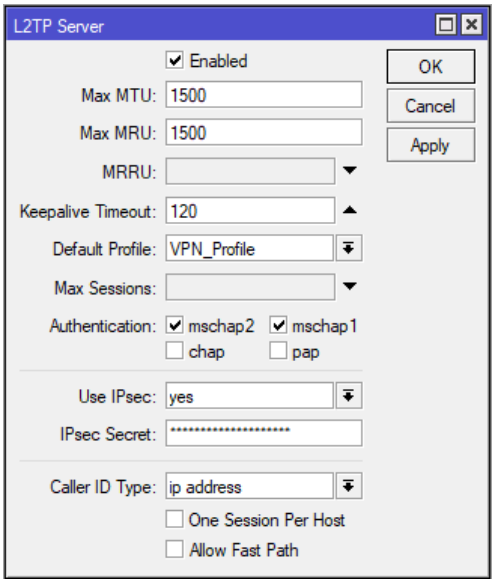
3.1.4 Server L2TP

Konfigurace serveru

Při konfiguraci serveru bylo využito autentizačních metod mschap1 a mschap2. V rámci zvýšeného zabezpečení bylo využito také protokolu IPsec, kdy je nutné vytvořit privátní klíč (IPsec Secret). Tento klíč je pak nutné nastavit také na straně klienta. Při použití protokolu IPsec je nutné nastavit další parametry tohoto protokolu. Nastavení jednotlivých parametrů je možné zobrazit ve výpisu 3.5.

```
/ip ipsec profile
set [ find default=yes ] dh-group=modp1024 enc-algorithm=
   aes-256,aes-128,3des
/ip ipsec proposal
set [ find default=yes ] enc-algorithms=aes-256-cbc,aes
   -128-cbc,3des
```

Výpis 3.5: Nastavení protokolu IPsec.



Obr. 3.4: Nastavení L2TP serveru.

Firewall pravidlo

VPN L2TP využívá kromě protokolu L2TP také IPsec, IKE a NAT-T. Pro správnou funkci je tedy nutné tyto protokoly rovněž povolit ve firewallu.

```
chain=input protocol=ipsec-esp action=accept comment="
   IPSec-ESP"
chain=input protocol=ipsec-ah action=accept comment="
   IPSec-AH"
chain=input protocol=udp dst-port=1701 action=accept
   comment="Allow L2TP"
chain=input protocol=udp dst-port=500 action=accept
   comment="Allow IKE"
```

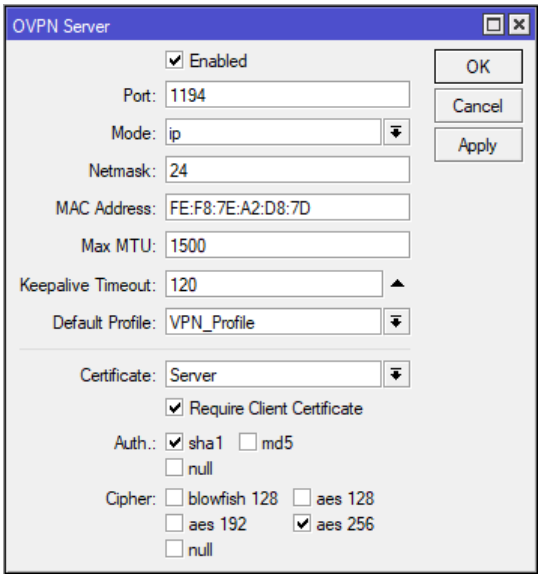
```
chain=input protocol=udp dst-port=4500 action=accept
   comment="Allow NAT-T"
```

Výpis 3.6: Firewall pravidlo - L2TP.

3.1.5 Server OpenVPN

Konfigurace serveru

Pro OpenVPN server byl využit jeho standardní port 1194, pracovní mód IP a certifikát. Jako autentizační metoda bylo zvoleno sha1, šifrování je aes256. Rovněž byla také vynucena kontrola klientského certifikátu, viz náhled konfigurace na obrázku 3.5.



Obr. 3.5: Nastavení OpenVPN serveru.

Konfigurace serveru

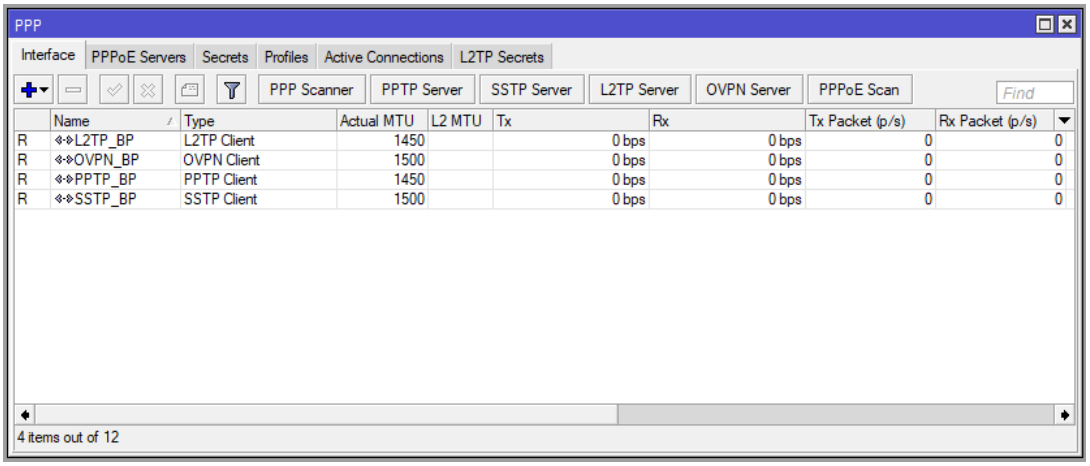
Firewall pravidlo

```
chain=input protocol=tcp dst-port=1194 action=accept
   comment="Allow OVPN"
```

Výpis 3.7: Firewall pravidla - OpenVPN.

3.2 Klientská část

Jako klientská zařízení, která budou demonstrovat připojení na VPN servery, byly v této práci využity směrovače Mikrotik. Nastavení je stejné pro všechny směrovače, ve všech lokalitách. Pro připojení k serveru bylo využito integrovaných klientů v RouterOS. Ve všech klientech je pak nutné specifikovat veřejnou IP adresu serveru a účet klienta vytvořený na VPN serveru, viz 3.1.1.



Obr. 3.6: Přehled jednotlivých klientů na klientském směrovači.

Účelem klienta je také přístup k interním zdrojům podnikové sítě, proto je tedy nutné vytvořit statickou směrovací cestu, která tento přístup zajistí. Interní síť hlavního serveru je 10.244.205.0/24, ta je specifikována v cílové adrese a jako brána slouží vytvořené VPN tunely. Náhled cesty je na obrázku 3.7.

3.2.1 Klient PPTP

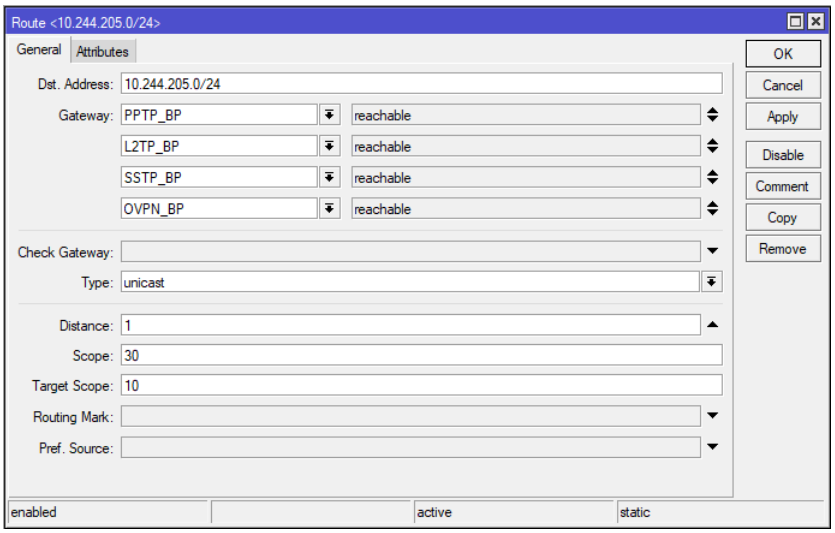
Konfigurace klienta

Konfigurace klienta kopíruje nastavení serveru, které je popsáno v kapitole 3.1.2.

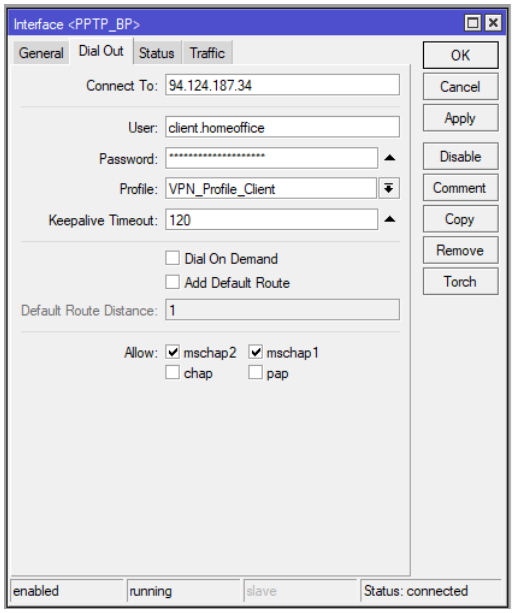
3.2.2 Klient SSTP

Konfigurace klienta

Nastavení opět vychází ze serveru s tím rozdílem, že pro klienta je využito klientského certifikátu.



Obr. 3.7: Nastavení statické cesty.

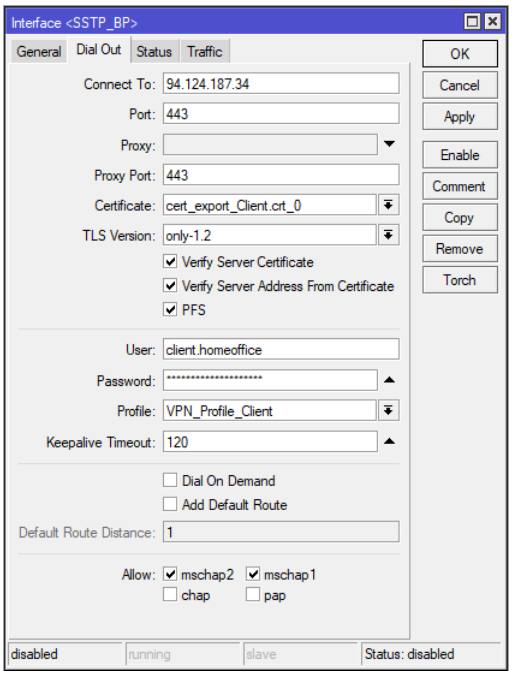


Obr. 3.8: Nastavení VPN klienta, protokol PPTP.

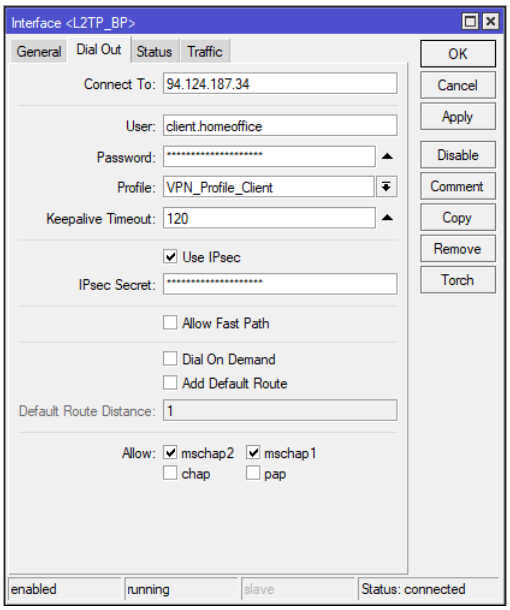
3.2.3 Klient L2TP

Konfigurace klienta

Jako u ostatních, i L2TP klient vychází z nastavení serveru. Je nutné označit položku „Use IPsec“ a následně vyplnit stejný klíč, který je vyplněn na straně serveru. Ukázka konfigurace klienta je na obrázku 3.10.



Obr. 3.9: Nastavení VPN klienta, protokol SSTP.

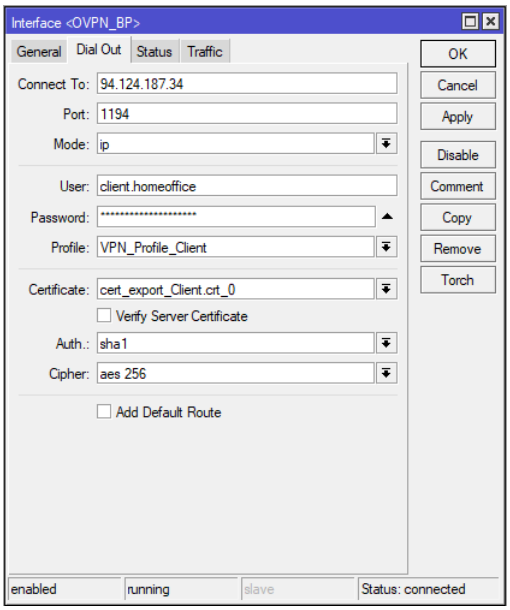


Obr. 3.10: Nastavení VPN klienta, protokol L2TP.

3.2.4 Klient OpenVPN

Konfigurace klienta

Konfigurace OpenVPN vychází z konfigurace serveru, je nutné pouze zvolit klientský certifikát.



Obr. 3.11: Nastavení VPN klienta, protokol OpenVPN.

4 Měření parametrů služby VPN

4.1 Popis měřené sítě

Při měření bylo využito prostředků podnikové sítě, jejíž hlavní část se nachází v Olomouci. Do této sítě přistupují přes VPN uživatelé z kanceláři v Brně, Kyjevě a Mansouře. Proto demonstraci těchto přístupů byly využity směrovače, které se v těchto lokalitách nachází. Rovněž je potřeba brát v úvahu uživatele, kteří přistupují ze soukromých sítí, tuto část demonstruje přístup z lokality Fryšták. Práce je zaměřena na zařízení od společnosti Mikrotik, proto byly ve všech lokalitách použity směrovače Mikrotik.

Olomoucká síť pracuje s adresním prostorem 10.244.205.0/24. V této síti se nachází serverový směrovač Mikrotik RB3011UiAS-RM. Tato síť je připojena na páteřní lince metropolitní sítě Olomouc.

Pro měření parametrů sítě byl zvolen aplikační server s adresou 10.244.205.74. Aplikační server byl zvolen pro měření z důvodu demonstrace konkrétní situace z praxe, kdy se vývojář připojí přes VPN do podnikové sítě za účelem přístupu k tomuto serveru, který je využíván pro hostování vývojového prostředí webových aplikací. Tento server má síťovou kartu s podporou Gigabit Ethernet[1] a je připojen ke směrovači ethernetovým kabelem typu cat 6.

V lokalitě Brno je použit klientský směrovač Mikrotik hAP ac^2, který je součástí místní lokální sítě, kancelářského komplexu. Tato síť je připojena metalickým spojením do brněnské metropolitní sítě. Přenosová rychlost linky je omezena na rychlost datového přenosu 100 Mbps pro příjem a 20 Mbps pro odesílání.

Lokalita Fryšták slouží pro demonstraci připojení z domácí sítě, pří práci z domova. Pro připojení k VPN je využit směrovač Mikrotik hAP ac^2. Tato síť je připojena do globální sítě internet pomocí místního poskytovatele internetového přípojení (ISP). Toto připojení je realizováno pomocí bezdrátové sítě WiFi.

Pro připojení k VPN z Kyjeva je opět využit směrovač Mikrotik hAP ac^2. Tento směrovač je součástí lokální sítě v rámci kancelářské budovy. Budova je připojena metalickým spojením do metropolitní sítě města Kyjev.

V Mansouře je pro připojení k VPN používán směrovač Mikrotik RB3011UiAS-RM, který se nachází v lokální síti kancelářské budovy. Připojení do globální sítě internet je realizováno pomocí linky ADSL.

[1] Gigabit Ethernet podporuje šířku pásma o velikosti 1000 Mbit/s.[52]

4.2 Měřené parametry

Pro měření parametrů sítě bylo využito nástrojů, které jsou přímo součástí operačního systému RouterOS. Jednotlivé nástroje jsou podrobněji popsány v kapitole 2.3.1. Měřenými veličinami jsou šířka pásma, ztrátovost, obousměrné zpoždění, rychlost spojení a jitter.

4.2.1 Šířka pásma

Pro měření šířky pásma je využit nástroj Bandwidth Test. Pro realizaci měření s tímto nástrojem musí být na obou stranách spojení zařízení se systémem RouterOS. Z toho důvodu probíhalo měření šířky pásma s využitím směrovače (IP adresa 10.244.205.1) namísto aplikačního serveru.

Měření bylo prováděno pomocí protokolů TCP a UDP, ve směrech odesílání a příjem paketů.

4.2.2 Ztrátovost

Ztrátovost je parametr, popisující pakety, které nedosáhnou své koncové stanice. Běžně je udáváno v procentech.

Pro měření ztrátovosti spojení byl využit nástroj Ping. Tímto nástrojem bylo odesláno na aplikační server 500 paketů o velikosti 50 bytů s časovým limitem 500 ms. Toto měření bylo opakováno 5 krát v průběhu běžného pracovního dne.

4.2.3 Obousměrné zpoždění

Obousměrné zpoždění je časový rozdíl mezi odesláním prvního bitu a příjmem bitu posledního. Zde je zastoupeno hodnotou RTT, která je udávána v milisekundách.

Měření obousměrného zpoždění probíhalo s využitím nástroje Flood Ping, viz kapitola 2.3.1. Pakety byly odesílány na aplikační server. Celkové množství paketů bylo 1000, což je zároveň také maximální počet odeslaných paketů. Velikost paketů byla 1500 bytů a maximální timeout byl 500 ms.

4.2.4 Rychlost spojení

Rychlost spojení byla měřena pomocí nástroje Ping Speed, který komunikoval s aplikačním serverem. Tento nástroj využívá pro měření rychlosti protokol ICMP

s využitím malých paketů o velikosti 32 bytů a velkých paketů o velikosti 1500 bytů. Pakety byly odesílány s intervalem 100 ms.

4.2.5 Jitter

Pro měření hodnoty Jitter byl využit nástroj systému RouterOS, Speed Test. Jedno měření trvalo 55 vteřin a bylo opakováno 10 krát v průběhu běžného pracovního dne, aby bylo docíleno vyšší přesnosti. Pro měření byl využit aplikační server.

4.3 Výsledky měření parametrů jednotlivých protokolů

4.3.1 Česká republika, Brno

Protokol	PPTP	SSTP	L2TP	OVPN
Šířka pásma - TCP				
Odesílání [Mbps]	18,5	9,2	17,6	13,8
Příjem [Mbps]	91,2	9,6	59,1	14,2
Šířka pásma - UDP				
Odesílání [Mbps]	19,4	17,8	18,3	15,4
Příjem [Mbps]	94,7	33,8	44,2	34,3
Ztrátovost				
Odeslané pakety	500	500	500	500
Přijaté pakety	500	500	500	500
Ztrátovost [%]	0	0	0	0
Obousměrné zpoždění				
Minimální RTT [ms]	13	14	13	14
Průměrné RTT [ms]	14	17	14	14
Maximální RTT [ms]	43	303	54	35
Rychlost spojení				
Průměrná rychlost [Mbps]	57,2	32,8	44,4	24,1
Jitter				
Minimální [μs]	4	0	0	2
Průměrný [ms]	2,16	2,31	1,33	2,12
Maximální [ms]	28,1	23,4	13,6	19,5

Tab. 4.1: Tabulka výsledků měření VPN parametrů - Česká republika, Brno

4.3.2 Česká republika, Fryšták

Protokol	PPTP	SSTP	L2TP	OVPN
Šířka pásma - TCP				
Odesílání [Mbps]	4,2	3,6	4,1	4,2
Příjem [Mbps]	11,8	10,2	17,1	15,2
Šířka pásma - UDP				
Odesílání [Mbps]	4,3	3,8	0,6747	4,4
Příjem [Mbps]	13,6	13,2	16,2	17,4
Ztrátovost				
Odeslané pakety	500	500	500	500
Přijaté pakety	494	494	497	495
Ztrátovost [%]	1,21	1,21	0,6	1,01
Obousměrné zpoždění				
Minimální RTT	12	11	11	11
Průměrné RTT	22	15	14	14
Maximální RTT	69	280	45	283
Rychlost spojení				
Průměrná rychlost [Mbps]	11,5	7,5	12,3	11,4
Jitter				
Minimální [μs]	7	23	5	1
Průměrný [ms]	4,76	5,09	3,78	2,68
Maximální [ms]	22,1	231	98,7	18,3

Tab. 4.2: Tabulka výsledků měření VPN parametrů - Česká republika, Fryšták

4.3.3 Ukrajina, Kyjev

Protokol	PPTP	SSTP	L2TP	OVPN
Šířka pásma - TCP				
Odesílání [Mbps]	51,7	3,2	50,7	6,7
Příjem [Mbps]	52,2	3,3	51,1	8,3
Šířka pásma - UDP				
Odesílání [Mbps]	53,6	9,9	51,4	17,1
Příjem [Mbps]	53,2	32,1	51,5	29,3
Ztrátovost				
Odeslané pakety	500	500	500	500
Přijaté pakety	496	500	496	500
Ztrátovost [%]	0,81	0	0,81	0
Obousměrné zpoždění				
Minimální RTT	36	37	37	37
Průměrné RTT	40	44	38	39
Maximální RTT	72	366	72	348
Rychlost spojení				
Průměrná rychlost [Mbps]	42,6	11,1	23,5	15,1
Jitter				
Minimální [μs]	3	2	1	3
Průměrný [ms]	3,81	2,55	2,74	3,4
Maximální [ms]	32,2	31,9	20,7	40,1

Tab. 4.3: Tabulka výsledků měření VPN parametrů - Ukrajina, Kyjev

4.3.4 Egypt, Mansoura

Protokol	**SSTP**
Šířka pásma - TCP	
Odesílání [Mbps]	1,9
Příjem [Mbps]	2,3
Šířka pásma - UDP	
Odesílání [Mbps]	2,6
Příjem [Mbps]	22,7
Ztrátovost	
Odeslané pakety	1000
Přijaté pakety	1000
Ztrátovost [%]	0
Obousměrné zpoždění	
Minimální RTT	98
Průměrné RTT	101
Maximální RTT	192
Rychlost spojení	
Průměrná rychlost [Mbps]	3,4
Jitter	
Minimální [ms]	37,3
Průměrný [ms]	48,1
Maximální [ms]	84,8

Tab. 4.4: Tabulka výsledků měření VPN parametrů - Egypt, Mansoura

4.3.5 Vyhodnocení měření

Měření bylo prováděno za účelem porovnání parametrů protokolů PPTP, SSTP, L2TP a OpenVPN vybrané služby VPN, která je monitorována v síti s využitím síťových zařízení Mikrotik. Rovněž bylo cílem zjistit, jaký vliv má na jednotlivé protokoly lokalita, odkud je připojení realizováno.

V první řadě bylo zjištěno, že v Egyptě není možné, pro vytvoření VPN tunelu, využívat určité protokoly. Důvodem je blokování těchto protokolů ze strany egyptské vlády za účelem cenzury a omezením přístupu k zakázaným webovým serverům. Nejprve byly blokovány egyptskou vládou pouze protokoly PPTP a L2TP, později

pak přibyl také protokol OpenVPN. K blokování těchto protokolů je využívána technika hluboké inspekce paketů.[53]

Z tohoto důvodu je v tabulce výsledků 4.4 uveden pouze protokol SSTP. Protokol SSTP není blokován egyptskou vládou nejspíš z důvodu použití portu 443 a kryptografického protokolu TLS.

Kromě protokolu SSTP by bylo teoreticky možné použít také protokol OpenVPN, pokud by došlo k úpravě jeho konfigurace. Konkrétně by musela být komunikace přesunuta na port 443 a muselo by být implementováno šifrování pomocí TLS. Toto jednání by ovšem bylo nejspíš na hraně se zákonem a mohlo by být považováno ze strany egyptské vlády jako jeho porušení, proto bylo od této varianty odstoupeno.

Při srovnání hodnot šířky pásma a rychlosti spojení jednotlivých protokolů bylo zjištěno, že největší šířku pásma a rychlost spojení poskytuje protokol PPTP. To je nejspíš dáno absencí pokročilých metod zabezpečení, které nabízí ostatní protokoly a tím dochází ke zpoždění rychlosti spojení. Rychlost tohoto protokolu vyniká zejména pokud je mezi klientem a serverem malá vzdálenost a kvalitní spojení. Příkladem je měření z Brna, kdy protokol PPTP dokáže využít prakticky maximální velikost šířky pásma linky. Při využití protokolu UDP byla hodnota šířky pásma u odesílání 19,4 Mbps z maximálních 20 Mbps a při přijímání 94,7 Mbps z možných 100 Mbps.

Průměrné hodnoty ztrátovosti i obousměrného zpoždění byly prakticky stejné pro všechny typy protokolů, pouze protokoly SSTP a OpenVPN měly vyšší hodnoty maximálního obousměrného zpoždění, což mohlo být zapříčiněno SSL certifikátem, který je použit pro zabezpečení komunikace mezi klientem a serverem. Hodnoty jitteru jsou rovněž mezi jednotlivými protokoly velmi podobné.

V závislosti na lokalitě byla potvrzena očekávaná přímá úměra, kdy s rostoucí vzdáleností od serveru klesá velikost šířky pásma a rychlost spojení, naopak se zvyšuje obousměrné zpoždění a jitter.

Pokud bychom srovnali hodnoty obousměrného zpoždění mezi lokalitami Brno a Mansoura, tak zjistíme, že tato hodnota je, při připojení z Mansoury, takřka desetinásobná. Při srovnání obousměrného zpoždění mezi Brnem a Kyjevem je zjištěno, že průměrné zpoždění přibližně třikrát vyšší z Kyjeva. U jitteru je pak tento rozdíl ještě vyšší. Jitter při spojení z Brna nabývá průměrných hodnot 2,31 ms pro protokol SSTP, zatímco při spojení z Mansoury je průměrná hodnota jitteru 48,1 ms.

Při měření šířky pásma z Mansoury, což je geograficky nejvzdálenější bod od

serveru, byl naměřen velký rozdíl mezi protokoly TCP a UDP. Protokol UDP poskytuje výrazně vyšší šířku pásma, protože se, na rozdíl od TCP, jedná o nespojový protokol, který vyžaduje minimální režii.[54]

Za všimnutí stojí také srovnání mezi metalickým a bezdrátovým připojením k síti internet. Ikdyž je geografická vzdálenost z Brna do Olomouce podobná jako z Fryštáku do Olomouce, tak hodnota jitteru je dvojnásobně větší u připojení z Fryštáku.

Připojení z Fryštáku, jako jediná lokalita, vykazuje soustavnou ztrátovost, ta je ovšem pouze v nízkých jednotkách procent. Tato ztrátovost je pravděpodobně způsobená bezdrátovým připojením, které může být za zhoršených podmínek méně stabilní, např. při dešti, či sněžení.

5 Skript pro monitorování přístupové sítě

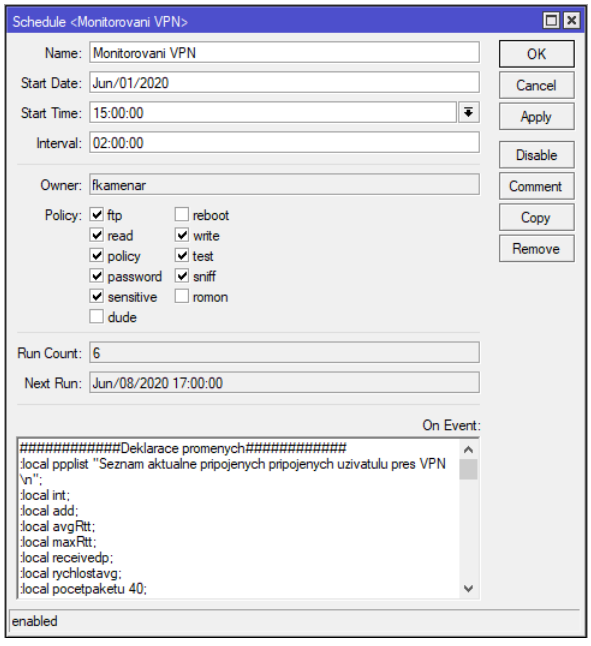
5.1 Monitorované parametry a vlastnosti řešení

Vybranými parametry pro monitorování sítě pomocí skriptu byly parametry a vlastnosti VPN tunelu. Monitorovanými parametry jsou typ protokolu, vlastnosti klienta, obousměrné zpoždění, jitter, ztrátovost paketů a rychlost spojení. Tyto parametry byly zvoleny z důvodu sledování kvality připojení.

Pro automatizaci celé činnosti monitorování byl použit nástroj „Scheduler“, který je součástí systému RouterOS. Scheduler umožňuje nastavit četnost spouštění vytvořeného skriptu, práva a datum i čas zahájení činnosti.

Skript také obsahuje funkci pro odesílání dat emailem obsluze. Naměřená data jsou uložena do textového souboru, který obsahuje v názvu souboru aktuální datum i čas, aby bylo možné procházet jednotlivé záznamy. Tento soubor je poté pomocí nástroje „E-mail“ přidán do přílohy a odeslán obsluze. Obsluha tedy může kontrolovat stav sítě vzdáleně bez nutnosti ručního připojení k serveru.

Pro větší přehlednost byly v jednotlivých výpisech odebrány značky pro formátování textu. Zdrojový kód skriptu je uložen v příloze v textovém souboru s názvem „monitorovaci-skript.txt“.



Obr. 5.1: Nástroj Scheduler.

5.2 Popis vytvořeného skriptu

Skript je rozdělen pomocí komentářů do několika částí, aby byla orientace v kódu snazší.[1]

První částí skriptu je deklarace proměnných, které jsou v rámci skriptu použity. Lokální proměnná je vytvořena příkazem „:local“, globální proměnná poté obdobně příkazem „:global“.

5.2.1 Funkce pro výpočet podílu

Další částí skriptu je funkce pro podíl dvou hodnot. Bohužel základní operace pro podíl, která je obsažena v systému RouterOS, neukládá zbytek a vrací pouze celá čísla. To by způsobovalo velkou nepřesnost při převodu jednotek, které je použito u měření rychlosti spojení, kde jsou převáděny bity za sekundu na megabity za sekundu. Funkce nese název „deleniFunkce“ a přijímá dva vstupní parametry - „delenec“ a „delitel“. Volání funkce je uvedeno ve výpisu 5.1. Do lokální proměnné „rychlostavgmbps“ je uložena návratová hodnota funkce „deleniFunkce“, která má jako dva vstupní parametry proměnnou „rychlostavg“, ta obsahuje průměrnou rychlost spojení v bitech za sekundu, a číslo „1000000“. Výsledkem je tedy převod čísla na megabity za sekundu.

```
:local rychlostavgmbps [$deleniFunkce $rychlostavg
   1000000];
```

Výpis 5.1: Zdrojový kód volání funkce „deleniFunkce“.

5.2.2 Vytvoření souboru

Poté následuje vytvoření souboru, který ponese v názvu aktuální datum a čas. Tvar souboru je „Monitoring-RRRR-MM-DD–HH-MM.txt“. Jednotlivé údaje pro datum a čas jsou uloženy do proměnných. Měsíc je převeden z písmen na čísla. Po uložení všech potřebných časových údajů je uložen celý název souboru do proměnné „soubor“ a následně je soubor vytvořen příkazem „/file print“. Pak následuje příkaz „delay“, který slouží k pozastavení činnosti skriptu, pro zajištění dostatku času na vytvoření souboru. Celý průběh vytvoření souboru je uveden ve výpisu 5.2.

```
:local soubor;
:local datum [/system clock get date];
:local cas [/system clock get time];
```

[1]Pro zobrazení skriptu je vhodné použít editor zdrojového kódu, např. Notepad++, který je volně dostupný na adrese <https://notepad-plus-plus.org>.

```
:local mesicpole ("jan","feb","mar","apr","may","jun","
   jul","aug","sep","oct","nov","dec");
:local hodina [:pick $cas 0 2];
:local minuta [:pick $cas 3 5];
:local mesic [:pick $datum 0 3];
:local den [:pick $datum 4 6];
:local rok [:pick $datum 7 11];
:set mesic ([ :find $mesicpole $mesic -1 ] + 1);
:if ($mesic < 10) do={ :set mesic ("0" . $mesic); }
:set soubor ("Monitoring-" .$rok."-".$mesic."-".$den."--"
   .$hodina."-".$minuta.".txt");
/file print file=$soubor;
:delay 3;
```

Výpis 5.2: Zdrojový kód vytvoření souboru s aktuálním datem.

5.2.3 Informace o klientech VPN

Další částí je zjištění všech aktuálně připojených klientů. Ke každému klientovi je vypsáno jméno, služba, lokální IP, veřejná IP a délka doby připojení. Lokální IP adresa je uložena do proměnné „add“, která je pak využita pro monitorování jednotlivých parametrů v následujících částech.

```
:foreach int in=[/ppp active find] do={
  :set ppplist "$ppplist Klient $[/ppp active get $int
     name]"
  :set ppplist "$ppplist Sluzba: $[/ppp active get $int
     service]"
  :set ppplist "$ppplist Status klienta "
  :set ppplist "$ppplist Lokalni IP: $[/ppp active get $
     int address] Verejna IP: $[/ppp active get $int
     caller-id] Doba pripojeni: $[/ppp active get $int
     uptime]";
 /ppp active;
     :set add [get $int address];
     :log info "$add";
```

Výpis 5.3: Zdrojový kód zíkání informací o klientech VPN.

5.2.4 Obousměrné zpoždění

Lokální IP adresa klienta, která je uložena v proměnné „add“ je vložena jako cílová adresa pro nástroj flood-ping. V proměnné „pocetpaketu“ je uložen celkový počet paketů, které budou odeslány v rámci měření. Získaná data jsou pak uložena do proměnných a vypsána k aktuálnímu uživateli. Náhled zdrojového kódu je ve výpisu 5.4.

```
/tool flood-ping $add count=$pocetpaketu interval=2 do={
          :set maxRtt $"max-rtt"
          :set receivedp $"received"
          :set avgRtt $"avg-rtt"
       }
    :set ppplist "$ppplist Prumer: $avgRtt [ms] Maximum:
       $maxRtt [ms] Odeslane pakety: $pocetpaketu Prijate
        pakety: $receivedp";
```

Výpis 5.4: Zdrojový kód měření obousměrného zpoždění.

5.2.5 Jitter a ztrátovost

Měření jitteru a ztrátovosti probíhá pomocí nástroje speed-test. Jako cílová adresa pro měření je opět použita lokální IP uživatele, která je uložena v proměnné „add“. Náhled části skriptu je ve výpisu 5.5.

```
/tool speed-test duration=10 address=$add do={
          :set jitter $"jitter-min-avg-max"
          :set ztratovost $"loss"
       }
:set ppplist "$ppplist  Jitter Min/Avg/Max: $jitter";
:set ppplist "$ppplist  Ztratovost(pocet): $ztratovost";
```

Výpis 5.5: Zdrojový kód měření jitteru a ztrátovosti.

5.2.6 Rychlost spojení

Pro měření rychlosti spojení je využito funkce ping-speed. Jako cílová adresa měření je použita lokální IP daného uživatele v proměnné „add“. Naměřená rychlost spojení je v bitech za sekundu, převedení na megabity za sekundu je pomocí funkce „deleniFunkce“.

```
/tool ping-speed $add duration=20 do={
```

```
            :set rychlostavg $"average";
        }
:set ppplist "$ppplist Prumerna ryhclost: $rychlostavg  [
    bps]";
:local rychlostavgmbps [$deleniFunkce $rychlostavg
    1000000]
:set ppplist "$ppplist Prumerna rychlost: $
    rychlostavgmbps [Mbps]";
```

Výpis 5.6: Zdrojový kód měření rychlosti spojení.

6 Závěr

Tato bakalářská práce se zabývá monitorováním služby VPN na aktivních síťových prvcích od společnosti Mikrotik. Součástí této práce bylo vytvoření VPN serveru v Olomouci a konfigurace VPN klientů s využitím směrovačů Mikrotik v lokalitách Brno, Fryšták, Kyjev a Mansoura. Veškerá práce a monitorování probíhalo na skutečné síti, což přibližuje naměřená data více ke skutečnosti a praktickému využití.

Prvním zásadním zjištěním při sestavování tunelů VPN bylo, že stát Egypt blokuje protokoly PPTP, L2TP a OpenVPN, což znamená, že tyto protokoly nebylo možné v Egyptě použít. Při hlubším průzkumu jsem zjistil, že blokace těchto protokolů je realizována pomocí techniky hluboké inspekce jednotlivých paketů.
V Egyptě je tedy možné použít pouze protokol SSTP, který pracuje na portu 443 a používá kryptografický protokol TLS, čímž zabraňuje případnému blokování.

Při srovnání protokolů v rámci jednotlivých zemí bylo zjištěno, že nejnižší režii VPN tunelu poskytuje protokol PPTP. To je pravděpodobně způsobeno především absencí pokročilého šifrování. Bohužel jednotlivé metody šifrování, které tento protokol využívá jsou již v současné době prolomeny a tak i přes jeho rychlost nemůže být z důvodu bezpečnosti tento protokol doporučen.
Velmi dobrých výsledků dosahoval protokol SSTP, který principielně vychází z protokolu PPTP, ale přidává zabezpečení pomocí TLS. Bohužel tento protokol není podporován operačními systémy od společnosti Apple, což brání jeho nasazení do prostředí, kde jsou tyto systémy využívány.
Dle mého názoru je protokol L2TP nejlepší variantou pro implementaci, protože nabízí širokou podporu operačních systémů, bezpečnost a rychlost.

Při implementaci jednotlivých monitorovacích nástrojů, které obsahuje systém RouterOS mne překvapil samotný rozsah a způsob využití těchto nástrojů. Myslím si, že základní úroveň monitorování jsou tyto nástroje plně dostačující a pokud je monitorovaná síť postavena na síťových prvcích Mikrotik, tak není třeba implementovat externí nástroje, které by sice v některých ohledech umožnily větší rozsah nastavení, ale také by vnesly do sítě případné bezpečnostní riziko, což v některých případech může být kritickým faktorem.

Vytvořený monitorovací skript sbírá informace o aktuálních uživatelích služby VPN. Tyto informace, jako např. IP adresa jsou poté využity pro automatizovaný monitoring s využitím nástrojů flood-ping, ping-speed a speed-test. Naměřená data jsou poté uložena do textového souboru (náhled souboru je v příloze, „vystup-dat-skriptu.txt“) a odeslána pomocí emailu zvoleným uživatelům. Tím je umožněn obsluze monitoring i v případech, kdy nemají přímý přístup k monitorované síti.

Literatura

6.1 Citované v textu

[1] WORLD HEALTH ORGANIZATION. Q&A on coronaviruses (COVID-19) [online]. 2020, 17. 4. 2020 [cit. 2020-05-23]. Dostupné z URL: <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/question-and-answers-hub/q-a-detail/q-a-coronaviruses>

[2] BERÁNKOVÁ, Anna. Prevence proti koronaviru? Dejte svým zaměstnancům home office. *Forbes* [online]. 2020, 3. 3. 2020 [cit. 2020-05-23]. Dostupné z URL: <https://www.forbes.cz/prevence-proti-koronaviru-dejte\-svym-zamestnancum-home-office-jako-v-nestle>

[3] MIKROTIK. Routers and Wireless [online]. Latvia [cit. 2020-05-20]. Dostupné z URL: <https://mikrotik.com/aboutus>

[4] MIKROTIK. Router OS [online]. In: . [cit. 2020-05-15]. Dostupné z URL: <https://help.mikrotik.com/docs/display/ROS/>

[5] MIKROTIK. Manual:Winbox. *MikroTik: Documentation* [online]. [cit. 2020-05-17]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:Winbox>

[6] Co je UDP? *Sprava Sítě: Slovník pojmů* [online]. Praha, 2016 [cit. 2020-05-15]. Dostupné z URL: <https://www.sprava-site.eu/udp/>

[7] MIKROTIK. Manual:IP/Services. *MikroTik: Documentation* [online]. [cit. 2020-05-17]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:IP/Services>

[8] MIKROTIK. Routers and Wireless *Stable release tree* [online]. 14. 5. 2020 [cit. 2020-06-02]. Dostupné z URL: <https://mikrotik.com/download/changelogs/stable-release-tree>

[9] MIKROTIK. Manual:Webfig. *MikroTik: Documentation* [online]. [cit. 2020-05-22]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:Webfig>

[10] MIKROTIK. Manual:Console. *MikroTik: Documentation* [online]. [cit. 2020-05-17]. Dostupné z URL:
<https://wiki.mikrotik.com/wiki/Manual:Console>

[11] THE EDITORS OF ENCYCLOPAEDIA BRITANNICA. Telnet: Networking Protocol. *Encyclopaedia Britannica* [online]. 17. 10. 2008 [cit. 2020-05-19]. Dostupné z URL:
<https://www.britannica.com/technology/Telnet>

[12] MIKROTIK. Manual:RouterOS. *MikroTik: Documentation* [online]. [cit. 2020-05-17]. Dostupné z URL:
<https://wiki.mikrotik.com/wiki/Manual:RouterOS>

[13] Rack Shelves & Drawers. *Cable Organizer* [online]. [cit. 2020-05-30]. Dostupné z URL:
<https://www.cableorganizer.com/computer-cabinets/rack-mount-shelves.htm>

[14] Co je Rack? *Sprava Sítě: Slovník pojmů* [online]. Praha, 2016 [cit. 2020-05-15]. Dostupné z URL:
<https://www.sprava-site.eu/rack/>

[15] MIKROTIK. *Products: RB3011UiAS-RM* [online]. [cit. 2020-05-30]. Dostupné z URL:
<https://mikrotik.com/product/RB3011UiAS-RM>

[16] MIKROTIK. *Products: hAP ac²* [online]. [cit. 2020-05-30]. Dostupné z URL:
<https://mikrotik.com/product/hap_ac2>

[17] MIKROTIK. *Products: RB941-2nD-TC* [online]. [cit. 2020-05-30]. Dostupné z URL:
<https://mikrotik.com/product/RB941-2nD-TC>

[18] Overview of VPN: Evolution of Private Networks. *UK essays* [online]. 1. 2. 2018 [cit. 2020-05-14]. Dostupné z URL:
<https://www.ukessays.com/essays/information-systems/vpn.php#citethis>

[19] BEAL, Vangie. VPN: Virtual Private Network. *Webopedia* [online]. [cit. 2020-05-26]. Dostupné z URL:
<https://www.webopedia.com/TERM/V/VPN.html>

[20] How Virtual Private Networks Work. *Cisco* [online]. 13. 10. 2008 [cit. 2020-05-14]. Dostupné z URL:
<https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html>

[21] VLADTALKS. How to set up PPTP VPN on Mac. *VladTalks: Tech from Transylvania* [online]. Romania, 2020, 4. 6. 2020 [cit. 2020-06-05]. Dostupné z URL:
<https://vladtalks.tech/vpn/setup-pptp-vpn-on-mac>

[22] How to setup PPTP VPN on iOS. *Secure VPN* [online]. [cit. 2020-05-30]. Dostupné z URL:
<https://www.securevpn.pro/eng/setup/ios-pptp-vpn>

[23] MACKIE, Kurt. Microsoft Issues Advice on SSL 3.0 Security Vulnerability. *Redmondmag: The independent voice of the Microsoft IT community* [online]. 21. 10. 2017 [cit. 2020-06-07]. Dostupné z URL:
<https://redmondmag.com/articles/2014/10/21/ssl-3-security-vulnerability.aspx?m=2>

[24] BOZOVIC, Novak. Which VPN Protocol Should You Use?: Five Common VPN Protocols Explained & Compared! *TechNadu* [online]. 14. 2. 2020 [cit. 2020-05-14]. Dostupné z URL:
<https://www.technadu.com/vpn-protocols/8436/>

[25] Windows Server 2008 R2: Server-to-Client Remote Access and DirectAccess - VPN Protocols [online]. 20. 3. 2011 [cit. 2020-06-07]. Dostupné z URL:
<http://tutorial.wmlcloud.com/>

[26] MIKROTIK. Manual:Interface/L2TP. *MikroTik: Documentation* [online]. [cit. 2020-06-07]. Dostupné z URL:
<https://wiki.mikrotik.com/wiki/Manual:Interface/L2TP>

[27] SHINDER, Debra Littlejohn. *Počítačové sítě: nepostradatelná príručka k pochopení sítové teorie, implementace a vnitrních funkcí [sic]*. 1. Praha: SoftPress, c2003. Cisco systems. ISBN 80-864-9755-0.

[28] PARZIALE, Lydia. *TCP/IP tutorial and technical overview* [online]. 8th ed. United States: IBM International Technical Support Organization, c2006 [cit. 2018-11-12]. ISBN 07-384-9468-2.

[29] MIKROTIK. Manual:Tools/Bandwidth_Test. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL:
<https://wiki.mikrotik.com/wiki/Manual:Tools/Bandwidth_Test>

[30] MIKROTIK. Manual:IP/Neighbor_discovery. *MikroTik: Documentation* [online]. [cit. 2020-06-03]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:IP/Neighbor_discovery>

[31] MIKROTIK. Manual:IP/Traffic_Flow. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:IP/Traffic_Flow>

[32] ICMP. *Mendelova univerzita v Brně* [online]. [cit. 2020-05-30]. Dostupné z URL: <https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=597>

[33] Slovník pojmů: Ping. *Vodafone* [online]. [cit. 2020-05-31]. Dostupné z URL: <https://www.vodafone.cz/uzitecne-odkazy/slovnik-pojmu/ping/>

[34] MIKROTIK. Manual:Tools/Ping. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:Tools/Ping>

[35] Public DNS. *Google: Developers* [online]. [cit. 2020-06-01]. Dostupné z URL: <https://developers.google.com/speed/public-dns>

[36] GRECH, Matt. Acceptable Jitter & Latency for VoIP: Everything You Need to Know. *GetVoIP: Cloud Communication Advisor* [online]. 20. 12. 2019 [cit. 2020-06-02]. Dostupné z URL: <https://getvoip.com/blog/2018/12/20/acceptable-jitter-latency/>

[37] MIKROTIK. Manual:Troubleshooting_tools. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL: <https://wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools>

[38] RICKFREY1000. Flood Ping Tool. *Rick Frey Consulting* [online]. Texas, 17. 4. 2017 [cit. 2020-06-02]. Dostupné z URL: <https://rickfreyconsulting.com/flood-ping-tool/>

[39] Měření datových parametrů sítí pomocí TCP protokolu [online]. Praha: Český telekominukační úřad, 2014 [cit. 2020-06-02]. Dostupné z URL: <https://www.ctu.cz/sites/default/files/obsah/stranky/937/soubory/merenidatovychparametrusitipomocitcpprotokolu.pdf>

[40] RICKFREY1000. Ping Speed. *Rick Frey Consulting* [online]. Texas, 5. 4. 2017 [cit. 2020-06-03]. Dostupné z URL: <http://https://rickfreyconsulting.com/ping-speed/>

[41] MIKROTIK. Manual:Troubleshooting_tools_torch. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL: <http://\wiki.mikrotik.com/wiki/Manual:Troubleshooting_tools>

[42] MIKROTIK. Manual:System/Watchdog. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL: <http://https://wiki.mikrotik.com/wiki/Manual:System/Watchdog>

[43] Router OS: Packet Sniffer. *MikroTik: Help* [online]. [cit. 2020-05-27]. Dostupné z URL: <http://https://help.mikrotik.com/docs/display/ROS/Packet+Sniffer>

[44] MIKROTIK. Manual:Tools/Netwatch. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL: <http://https://wiki.mikrotik.com/wiki/Manual:Tools/Netwatch>

[45] MIKROTIK. Manual:SNMP. *MikroTik: Documentation* [online]. [cit. 2020-05-20]. Dostupné z URL: <http://https://wiki.mikrotik.com/wiki/Manual:SNMP>

[46] FLOWMON NETWORKS A.S.[online]. Brno: FLOWMON, 2018 [cit. 2018-11-13]. Dostupné z URL: <http://www.flowmon.com>

[47] GREYCORTEX [online]. Brno: GREYCORTEX, 2018 [cit. 2018-11-13]. Dostupné z URL: <http://www.greycortex.com>

[48] ManageEngine [online]. Kalifornie: ManageEngine, 2018 [cit. 2018-11-13]. Dostupné z URL: <http://www.manageengine.com>

[49] MIKROTIK [online]. Litva: MikroTik, 2018 [cit. 2018-11-13]. Dostupné z URL: <http://mikrotik.com>

[50] CACTI [online]. open-source: Cacti, 2018 [cit. 2018-11-13]. Dostupné z URL: <http://www.cacti.net>

[51] Uživatelská příručka k nástroji pro připojení Intel PROSet/Wireless WiFi: Přehled zabezpečení [online]. [cit. 2020-06-05]. Dostupné z URL: <http://support.elmark.com.pl/rgd/drivery/u12c/wlan/win7/Docs/CSY/overview.htm#chap>

[52] Gigabit Ethernet (GbE). *Techopedia: The IT Education Site* [online]. 21. říjen 2012 [cit. 2020-06-06]. Dostupné z URL: <https://www.techopedia.com/definition/7407/gigabit-ethernet-gbe>

[53] RAZA, Ali. Best VPN For Egypt: How To Bypass The Egypt Block On OpenVPN *Anonymster* [online]. 5. 5. 2020 [cit. 2020-06-06]. Dostupné z URL: <https://anonymster.com/best-egypt-vpn-block-openvpn/>

[54] Definice protokolu UDP. *Mendelova univerzita v Brně* [online]. [cit. 2020-06-07]. Dostupné z URL: <https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=602>

6.2 Všeobecný zdroj

[55] *Information technology - Open Systems Interconnection - Basic Reference Model: The basic model*. 07/94. Švýcarsko: ITU-T, 1994.

[56] JANSEN, Horst a Heinrich RÖTTER. *Informační a telekomunikační technika*. Praha: Europa - Sobotáles, 2004. ISBN 80-867-0608-7.

[57] GIAMBENE, Giovanni. *Queuing theory and telecommunications: networks and applications*. New York: Springer, c2005. ISBN 03-872-4065-9.

[58] ALHAMEDI, Adel H., Vaclav SNASEL, Hamoud M. ALDOSARI a Ajith ABRAHAM. Internet of things communication reference model. In: *2014 6th International Conference on Computational Aspects of Social Networks* [online]. IEEE, 2014, 2014, s. 61-66 [cit. 2018-11-27]. DOI: 10.1109/CASoN.2014.6920423. ISBN 978-1-4799-5940-2. Dostupné z URL: <http://ieeexplore.ieee.org/document/6920423/>

6.3 Citace obrázků

[59] MIKROTIK: Routers and Wireless [foto]. Latvia [cit. 2020-05-20]. Dostupné z URL: <https://mikrotik.com/>

[60] MIKROTIK *Products:RB3011UiAS-RM* [foto]. [cit. 2020-05-30]. Dostupné z URL: <https://mikrotik.com/product/RB3011UiAS-RM>

[61] MIKROTIK *Products:hAP ac²* [online]. [cit. 2020-05-30]. Dostupné z URL: <https://mikrotik.com/product/hap_ac2>

[62] MIKROTIK *Products:RB941-2nD-TC* [online]. [cit. 2020-05-30]. Dostupné z URL: <https://mikrotik.com/product/RB941-2nD-TC>

Seznam symbolů, veličin a zkratek

ADSL	Asymmetric Digital Subscriber Line
API	Application Programming Interface - Aplikační programovací rozhraní
ARM	Acorn RISC Machine
ARP	Address Resolution Protocol
CA	Certification Authority - Certifikační autorita
CDP	Cisco Discovery Protocol
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface - Grafické uživatelské rozhraní
GRE	Generic Routing Encapsulation
HTTP	HyperText Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
CHAP	Challenge Handshake Authentication Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protokol
Internet	International Network - Mezinárodní síť
IP	Internet Protocol
ISO	International Organization for Standardization
ISP	Internet service provider - Poskytovatel internetového připojení
JS	JavaScript
L2TP	Layer 2 Tunneling Protocol
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MITM	Man in the middle - člověk uprostřed
MNDP	MikroTik Neighbor Discovery Protocol
MRU	Maximum Receive Unit - Maximální přijatá jednotka
MTU	Maximum Transmission Unit - Maximální odeslaná jednotka
OS	Operační systém
OSI model	Open Systems Interconnection model
OSX	Macintosh Operating System X
pap	Password Authentication Protocol
Ping	Packet InterNet Groper
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol

QoS	Quality of Service
RTT	Round Trip Time - Obousměrné zpoždění
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
SSTP	Secure Socket Tunneling Protocol
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TTL	Time-to-live - Doba platnosti
UDP	User Datagram Protocol
VPDN	Virtual Private Dial-up Network
VPN	Virtual Private Network - Virtuální privátní síť

Seznam příloh

.1 Operační systém MikroTik RouterOS

- routeros-arm-6.45.6.npk
- routeros-smips-6.45.6.npk

.2 Monitorování pomocí skriptu

- monitorovaci-skript.txt
- vystup-dat-skriptu.txt