Router Turris Omnia jako základ bezpečné počítačové sítě

Bc. Aleš Staněk

Diplomová práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2020/2021

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Aleš Staněk**
Osobní číslo:	**A18298**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Router Turris Omnia jako základ bezpečné počítačové sítě**
Téma práce anglicky:	**The Turris Omnia Router as the Basis of a Secure Computer Network**

Zásady pro vypracování

1. Proveďte literární rešerši na téma bezpečnosti routerů.
2. Analyzujte možnosti routeru Turris.
3. Vyhodnoťte možnosti připojení prvků domácí automatizace s důrazem na bezpečnost sítě.
4. Navrhněte konfiguraci routeru s ohledem na bezpečnost perimetru v souladu s doporučením NUKIB.
5. Realizujte zvolené řešení a toto otestujte.
6. Proveďte kritické zhodnocení navrženého řešení.

Forma zpracování diplomové práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. *ManagementMania: profesionální dynamická znalostní síť* [online]. Wilmington USA: MANAGEMENTMANIA.COM, © 2011-2020 [cit. 2020-11-20]. ISSN 2327-3658. Dostupné z: https://managementmania.com
2. *Raspberry Pi: Raspberry Pi for Education* [online]. England: Raspberry Pi Foundation, 2020 [cit. 2020-11-20]. Dostupné z: https://www.raspberrypi.org
3. Technická dokumentace: Turris. *CZ.NIC* [online]. Praha: CZ.NIC, správce domény CZ, 2020 [cit. 2020-12-04]. Dostupné z: https://docs.turris.cz/
4. *Turris: router* [online]. Praha: CZ.NIC, 2020 [cit. 2020-12-04]. Dostupné z: https://www.turris.cz/cs/
5. SOMMERVILLE, Ian. *Software engineering*. Tenth edition. Boston: Pearson, [2016]. ISBN isbn-978-0133943030.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. ledna 2021**
Termín odevzdání diplomové práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne v. r.

podpis studenta

ABSTRAKT

Cílem diplomové práce je seznámit čtenáře s unikátním zařízením Turris Omnia, jehož potenciál lze využít nejen jako výkonného routeru, ale také jako hardwarové platformy pro běh virtuálních serverů.

V úvodní části této práce je stručný popis historie vzniku routeru Turris, a dále teoretické možnosti jeho využití na příkladech testovaných technologií. Každá z testovaných technologií měla potenciál pro reálné nasazení. Provoz některých však byl náročný na systémové prostředky, nebo by nebyl přínosem pro reálné nasazení v navrženém systému.

Dále je návrh a implementace komplexního systému, routeru a domácí automatizace. Pro domácí automatizaci byla vybrána velmi levná zařízení, s prověřenou spolehlivostí. V těchto zařízeních byl přehrán původní ovládací software za software Tasmota, který je open source projektem s dobrou podporou a kontinuálním vývojem.

V závěru práce je zhodnocení z pohledu finančních nákladů, složitosti provedení a také z pohledu bezpečnosti.

Klíčová slova: router, OpenWRT, Linux, počítačová síť, kybernetická bezpečnost, Turris Omnia

ABSTRACT

The aim of this thesis is to introduce the reader to a unique device, Turris Omnia, whose potential can be used not only as a powerful router, but also as a hardware platform for running virtual servers.

The introductory part of this thesis provides a brief history of the Turris router, as well as the theoretical possibilities of using it in examples of tested technologies . Each of the technologies tested had the potential for real deployment. However, the operation of some was demanding on system resources or would not be beneficial for real deployment in the proposed system.

There is also the design and implementation of a complex system, router, and home automation system. Very cheap devices with proven reliability have been chosen for home automation. In these devices, the original control software has been replaced by Tasmota software, which is an open source project with good support and continuous development.

The conclusion of the work is an assessment from the perspective of financial costs, complexity of implementation and also in terms of security.

Keywords: router, OpenWRT, Linux, computer network, cybernetic security, Turris Omnia

Na prvním místě bych chtěl poděkovat svojí manželce Iloně, která po dobu mého studia plnila roli mámy/táty a bez její podpory bych studium jistě nezvládnul. Poděkování patří také mému vedoucímu práce panu prof. Mgr. Romanu Jaškovi, Ph.D, za podporu, vedení a motivaci v práci. V neposlední řadě bych chtěl poděkovat panu Mgr. Tomáši Kovaříkovi, který mě přivedl do „světa Linux“, IoT zařízení a také k routeru Turris Omnia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Router je zařízení, které pro připojení do internetu využívá téměř každá domácnost. V České republice je dle informací Českého statistického úřadu 81 % domácností připojených k internetu. [1] Většina domácích routerů je z pohledu běžných uživatelů „ta krabička“ nebo „naše wifina“ a naprosto bez povšimnutí leží někde na skříni nebo za stolem. Mnohdy se nikdo nestará o instalace aktualizací, v horším případě běží zařízení od první instalace v defaultním nastavení s původními hesly výrobce.

1.1 Motivace

Z pohledu bezpečnosti je neaktualizovaný nebo špatně konfigurovaný router potencionálně slabým místem pro všechna zařízení, která se přes něj připojují do internetu. Routery jsou většinu času nevytížené a jen spotřebovávají energii. Přitom právě router je zařízení, které je možné využívat mnohem komplexněji. Zejména pokud se jedná o výkonný hardware v podobě routeru Turris Omnia. V roce 2016 si autor práce přečetl článek Otakara Schöna, ve kterém uvedl: „*Turris Omnia zdaleka není nejlepší router na trhu. Nemá nejrychlejší Wi-Fi, není snadné ho využít naplno a chybí mu mobilní aplikace i jednoduché nastavení priorit provozu. A je drahý. Přesto je to nejspíše ideální volba, pokud chcete mít domácí síť v bezpečí a nechcete každý týden router restartovat, když vám začne zlobit bezdrátová síť*“ [2]. Co je na tom zařízení tak unikátní, když v porovnání parametrů propadá a přesto autor tvrdí, že je to nejlepší volba pro bezpečnou síť? To jistě stojí za kritické zhodnocení. V neposlední řadě by autor chtěl čtenáře inspirovat k provozování routeru Turris Omnia a tím přispět ke zvýšení úrovně kybernetické bezpečnosti.

1.2 Cíl práce

Cílem této práce je na základě analýzy navrhnout konfiguraci routeru Turris Omnia pro využití v domácnosti nebo malé firmě. Výkonný hardware routeru by měl zajišťovat systémové prostředky pro běh virtualizovaných serverů. Vzhledem k tomu, že router běží nepřetržitě 24/7, bude současně využit pro běh systému domácí automatizace, která musí také běžet nepřetržitě. Práce by měla sloužit jako inspirace, případně jako zásobník použitelných řešení pro návrh nové implementace routeru Turris Omnia. Čtenář by měl v práci najít funkční řešení integrace domácí automatizace a může ji také použít jako návod pro svoje vlastní řešení. Vypracováním této práce by autor rád přispěl ke zvýšení povědomí o možných bezpečnostních rizicích spojených s využíváním takzvaných chytrých zařízeních.

1.3 Struktura práce

Diplomová práce je rozdělena do dvou základních částí, a to na teoretickou a praktickou. Teoretická část se zabývá terminologií související s problematikou práce. Jsou vysvětleny funkce SW a HW, který pak dále autor použil pro realizaci. Postupně jsou popsány testované technologie, které je možné provozovat v routeru Turris Omnia. Při jejich výběru byly zohledněny zkušenosti autora a požadavky uživatelů SOHO sítí. V teoretické části jsou popsány všechny testované programy, třeba, že pak nejsou součástí finálního řešení. V době přípravy a testování však měly, dle názoru autora, zajímavé funkce, které by mohly zvýšit užitnou hodnotu celého řešení.

Praktická část popisuje nastavení routeru, instalaci a nastavení SW, a propojení jednotlivých komponent sítě a domácí automatizace. Obsahuje také postupy pro úpravy HW, které jsou nezbytné pro instalaci alternativního open source SW do inteligentních spínačů. Autor řadil jednotlivé kapitoly podle toho, jak by bylo potřeba postupovat, kdyby někdo použil tuto práci jako návod krok za krokem.

V poslední části je zhodnocení navrhnutého řešení, srovnání s řešeními dostupnými na trhu z pohledu funkcí a ceny. V závěru práce autor zhodnotil přínosy řešení, jeho výhody a nevýhody.

I. TEORETICKÁ ČÁST

2 ÚVOD DO PROBLEMATIKY

Protože je v zadání práce uveden konkrétní produkt, je třeba blíže vysvětlit motivaci tohoto výběru a blíže představit výrobce. Router Turris Omia patří do kategorie SOHO routerů, což znamená small office/home office. Router vytváří místní síť SOHO LAN, zpravidla se jedná o kancelář, která disponuje jedním až deseti pracovníky [3].

Turris Omnia je produktem výzkumného projektu sdružení CZ.NIC. *„Zájmové sdružení právnických osob CZ.NIC bylo založeno předními poskytovateli internetových služeb v roce 1998. Hlavními činnostmi sdružení jsou provozování registru jmen domén registrovaných pod doménou CZ, zabezpečování provozu domény nejvyšší úrovně .CZ a osvěta v oblasti jmen domén"* [4]. Pro připomenutí uvedu reklamní spoty ve vysílání České televize „Jak na internet", ve kterých herec Roman Zach vtipně provází diváky problematikou počítačů a připojení na internet. Dalším televizním projektem, za kterým stojí CZ.NIC je „Nebojte se internetu" s herci Danou Batulkovou a Václavem Koptou. CZ.NIC stojí také za projektem „mojeID", kampaní „Dobrá doména" nebo projektem na prosazování ochrany počítačů pomocí technologie „DNSSEC".

2.1 Projekt Turris

Počátky projektu sahají do roku 2013. Sdružení CZ.NIC potřebovalo k ochraně SOHO sítí nasbírat data. Pro tento účel bylo vyvinuto a vyrobeno zařízení router Turris 1.0 a později 1.1. Po reklamní kampani a dotazníkovém šetření byli ze zájemců zejména z řad technicky zdatnějších uživatelů vybráni uživatelé z různých lokalit s různou kvalitou připojení k internetu napříč Českou republikou. S uživateli byla sepsána smlouva na dobu tří let, kdy na straně uživatele nesmělo být zasahováno do sběru dat, a za to jim bylo umožněno po uplynutí smlouvy zařízení odkoupit za symbolickou 1 Kč. Náklady na výrobu jednoho routeru se v té době pohybovaly ve výši 12 tisíc Kč.

Sbírají se anonymizovaná data z rozhraní WAN. Pro sběr dat na routeru běží programy Nikola a Ucollect. Uncollect sleduje procházející packety a zaznamenává část jejich hlaviček. Pro sběr jsou relevantní zejména informace o typu protokolu, IP adresa vzdáleného zařízení, počet a velikost packetů. Důležitý je plugin „fwup", ten komunikuje s centrálou CZ.NIC a aktualizuje seznamy blokovaných IP adres. *„Plugin tak funguje jako přídavek k balíčku firewall, který obsahuje základní blacklisty a provádí samotné blokování. Takto mohou být IP adresy do blacklistu přidány i z něj odstraněny mnohem rychleji – v rámci minut spíše*

než hodin" [5]. Toto řešení umožňuje porovnat data z mnoha připojených routerů Turris a vyhodnotit nebezpečnost detekovaného provozu. Síť routerů se tak stává systémem sond, které reportují národnímu CERT týmu. To bylo základem pro budoucí systém adaptabilního firewallu.

2.2 Nástupci Turris 1.0, 1.1

Přes některé dílčí problémy si Turris oprávněně získal svoje zastánce a ti se postarali o rozšíření zájmu o router české provenience s relativně vysokým výkonem, ale hlavně s podporou výrobce a unikátními bezpečnostními funkcemi. Proto se ve druhé polovině roku 2015 na Turris fóru začaly objevovat informace o připravovaném zařízení Turris Lite. Původně mělo jít o odlehčenou produkční verzi původního routeru. Záměrem bylo vytvořit komerčně produkované zařízení. Vedení projektu se rozhodlo vyzkoušet životaschopnost projektu crowdfundingovou kampaní[1] na webu Indiegogo. Tato kampaň byla nad očekávání úspěšná, a nakonec vznikl router Turris Omnia, který se prodává na internetových obchodech nejen v ČR, ale i v zahraničí (např. Amazon). Dalším vývojovým stupněm byl Turris MOX. MOX byl opět financován úspěšným crowdfundingovým projektem. Smyslem tohoto produktu bylo nabídnout specializované moduly, které se dají jednoduše propojit do funkčního celku, přesně podle zadání uživatele.

Obr. 1. Takto konfigurace vznikla spojením 6 ks modulů E, jednoho modulu D a jednoho základního modulu [6]

[1] Jedná se o hromadné financování, kdy jednotlivci přispívají obnosem dle svých možností k cílové částce požadované pro realizaci předmětu financování.

Zákazník si vybere z různých kombinací modulů, sestaví si zařízení přesně podle svých potřeb a neplatí za nic, co nepotřebuje. Výsledkem takové sestavy může být futuristicky vyhlížející téměř půlmetrová housenka viz *Obr. 1*. Systém je navrhnut tak, aby pro sestavení nebylo potřeba použít nástroje, moduly se do sebe pouze zasunou a zacvakne se plastový kryt.

Posledním produktem je Turris Shield. Toto zařízení se asi nejvíce přiblížilo plánům na produkci levného zařízení pro masové nasazení. Jedná se o HW firevwall s funkcemi, které Shield podědil po předcích. Jak uvádí výrobce: *„Shield je jednoúčelové zařízení pro každého, kdo chce snadno zabezpečit celou svou domácnost nebo kancelář bez nutnosti měnit svůj modem a router. Žádné nadprůměrné IT dovednosti nejsou třeba!“* [7].

2.3 Turris Omnia HW

Jak již bylo zmíněno výše, za tímto produktem stojí CZ.NIC, což není typický výrobce routerů. To sebou přináší pozitiva, ale i negativa. Síla a unikátnost tohoto routeru je spojení výkonného hardwaru, odladěný software, data o provozu sítí, nepřetržitý vývoj a podpora výrobce. V následující tabulce jsou uvedeny základní HW parametry aktuálně prodávané varianty routeru Turris Omnia.

Tabulka 1. Parametry HW aktuálně prodávaného modelu

	Turris Omnia 2020
CPU	Marvel Armada 385, 2 jádra
Frekvence CPU	1,6 GHz
RAM	2 GB DDR3
Úložiště	8 GB flash
LAN	5 x Gbit port RJ-45
WAN	1 x Gbit port
SFP	1 x
USB	2 × USB 3.0
MiniPCI-e	2 x
mSATA/MiniPCI-e	1 x
WiFi moduly v MiniPCI-e slotech	3×3 MIMO 802.11ac, 2×2 MIMO 802.11b/g/n
WLAN (Wifi) standardy	802.11a, 802.11ac, 802.11b, 802.11g, 802.11n

Ve srovnání s komerčními produkty disponuje Omnia výkonnějším procesorem a minimálně 2 až 4násobkem operační paměti. Kapacita 8 GB flash paměti výrazně převyšuje obvyklých 128 – 250 MB. Osazení dvěma USB 3.0 porty v kategorii SOHO routerů také není obvyklé. Použití SFP pro připojení optického kabelu a Mini PCI-e mSATA konektorů, patří také spíše do kategorie průmyslových zařízení. Toho se dá využít například pro výměnu síťových karet, připojení disků, případně instalovat jiný modul. Může to být například Bluetooth, LTE modem, IEEE 802.11ac Wave2 a další karty MiniPCI-e. K parametrům z Tabulka 1 je třeba přidat další HW výbavu, jako slot pro SIM kartu, kryptočip, pin-headery s GPIO[2], I²C[3], SPI[4]. To už může být pádný argument pro uživatele, kteří mají dostatečné technické znalosti a zároveň mají pro tato rozhraní využití. Některé uživatele by mohlo oslovit, že Omnia je osazena 12 barevně svítícími LED diodami, které se dají plně konfigurovat. Dá se nastavit RGB barva, intenzita jasu, případně změna parametrů na základě události.

Z výše uvedeného se zdá, že Omnia je více počítač s funkcemi routeru, než jen obyčejný router. Toho bude v praktické části využito pro integraci domácí automatizace.

2.3.1 Shrnutí HW výbavy

Na trhu se dají pořídit routery s novějšími technologiemi (WiFi 6), někdy s dílčími lepšími HW parametry a zcela jistě za nižší cenu. Omnia však nabízí rozšiřitelnost a modulárnost, která je unikátní. Tímto se Turris Omnia přibližuje vlastnostem průmyslových síťových prvků. GPIO, I²C, SPI rozhraní umožní router modifikovat a ovládat přes tyto sběrnice nebo naopak pomocí nich ovládat routerem jiná zařízení. Redundantní zapojení síťových karet může být využito v případě poruchy jedné z nich při zachování alespoň částečné funkcionality. Napájení je realizováno za pomoci externího trafa, není nutné při poruše trafa na desce měnit celou základní desku nebo rovnou celé zařízení.

---

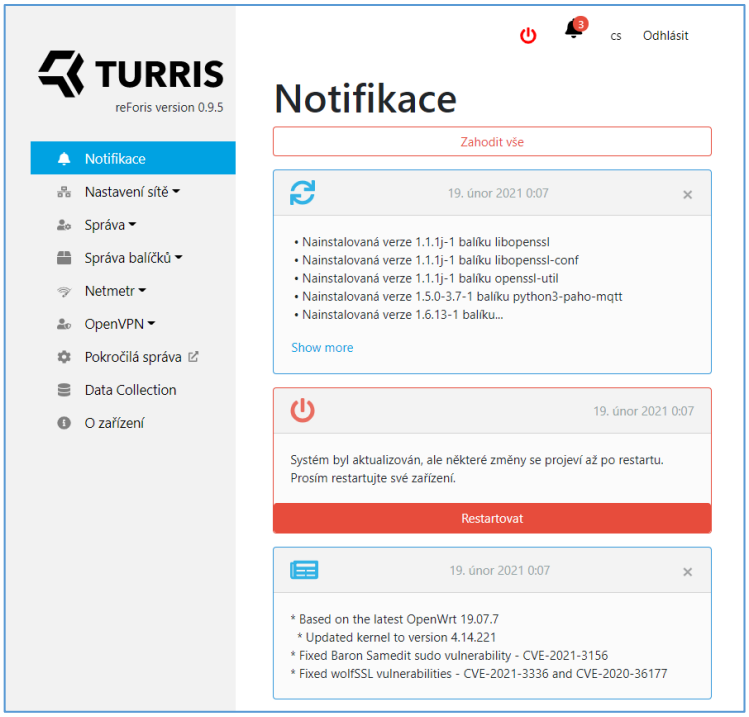
[2] GPIO je z anglického General Ppurpose Input/Output, což jsou vstupně/výstupní piny. Ty se využívají pro přímý přístup k elektrickému kontaktu buď integrovaného obvodu, nebo jednodeskového počítače. Programátor/uživatel má možnost tyto kontakty spínat/rozpínat příkazy z kódu.

[3] I²C sběrnice se používá v různých zařízeních včetně IBM PC kompatibilních počítačů pro čtení konfiguračních dat z paměťových modulů, pro správu PCI karet, ke změně hlasitosti reproduktorů, pro čtení údajů o zařízeních (teplota procesoru, rychlost ventilátorů) a dalším.

[4] SPI z anglického Serial Peripheral Interface je sériové periferní rozhraní. Používá se pro komunikaci mezi řídícími mikroprocesory a ostatními integrovanými obvody.

2.4 Turris Omnia SW

Základem softwarové výbavy routeru je operační systém Turris OS. Ten vychází z Linuxového systému OpenWrt. Systému OpenWrt vznikl díky uvolnění zdrojových kódů pro router Linksys WRT54G. Kolem tohoto systému se vytvořila velká komunita vývojářů a uživatelů. O síle komunitního vývoje a životaschopnosti projektu vypovídá podpora 1872 zařízení, 275 nejrůznějších výrobců, pro která je portován operační systém OpenWrt. Alternativní operační systém se tak dá nahrát do routerů od výrobců jako jsou například 3Com, AirLive, Aruba, ASRock, ASUS, Cisco, TP-Link, Western Digital, ZTE, ZyXEL a mnoho dalších. Údaj je aktualizován ke dni 5. 5. 2021 [8]. Vývojáři z CZ.NIC vycházeli z OpenWrt, ale operační systém dále modifikovali a rozšířili jeho funkcionality s důrazem na zvýšení bezpečnosti. Pro běžného uživatele je nejzásadnější změnou zavedení automatických aktualizací. Na *Obr. 2* je vidět oznámení o nainstalovaných aktualizacích, které se provedly bez zásahu uživatele. Pokud některé aktualizace vyžadují restart routeru, neprovedou se bez povolení uživatele. Nasazení aktualizací se dá v konfiguraci odložit o nastavený počet dní.

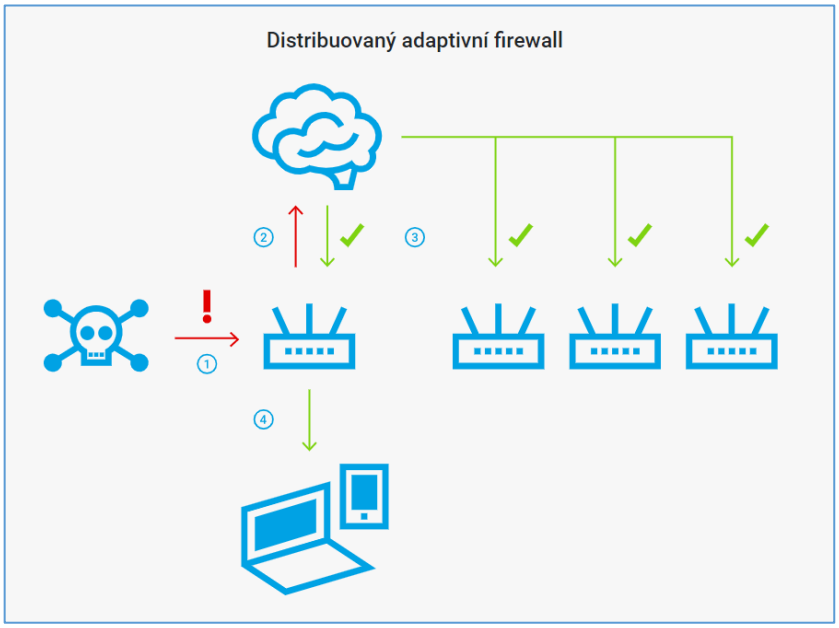


Obr. 2. Notifikace z prostředí Reforis o nainstalovaných aktualizacích [Zdroj: vlastní]

Podpora vyšší bezpečnosti ve výchozím nastavení neumožní přístup k administrátorskému rozhraní bez hesla. CZ.NIC je podporovatelem IPv6, proto je zajištěna podpora IPv6 i na firewallu, dále nabízí podporu DNSSEC v rekurzivním resolveru.

2.4.1 Adaptivní firewall

Součástí softwarového vybavení je distribuovaný adaptivní firewall. Jeho funkce jsou znázorněny na *Obr. 3*.



Obr. 3. Schéma distribuovaného adaptivního FW [9]

Do sítě se z internetu může pokusit proniknout škodlivý provoz s cílem šířit malware. Na obrázku označeno ①. Router Turris veškerý síťový provoz analyzuje. Při podezření na nežádoucí provoz pošle jeho otisk do centrály Turris, na obrázku označeno ②. V centrále jsou informace posouzeny, porovnány s daty z ostatních routerů Turris a, v případě odhalení útoku, je na všechna zařízení odeslána informace, že tento typ komunikace má být blokován, na obrázku označeno ③. Uživatelé si tak vzájemně pomáhají v ochraně sdílením informací o nových bezpečnostních hrozbách. Síť se zařízeními, často bez jakékoliv ochrany proti útokům zvenku, je tak chráněna, na obrázku označeno④ [9].

2.4.2 Blokování reklam a trackerů

Vývojáři k problematice blokování reklam přistoupili jinak, než například doplňky v prohlížečích, kde je přímo blokován obsah. To může mít na některých stránkách za následek, že se obsah stránky uživateli skryje. K obsahu se uživatel dostane až po zablokování adblock doplňku a zobrazení reklamních oznámení. Reklamy se blokují přímo na routeru, který všechny odkazy porovná s blacklistem a „závadné“ nahradí adresou 127.0.0.1 (localhost). To má za následek, že se reklama na stránce nezobrazí [10]. Blokování reklam není jen

o pohodlí, ale má také svoji bezpečnostní funkci. V nedávné minulosti byly zaznamenány problémy s nekalými praktikami některých inzerentů. Reklama zobrazená na mobilním telefonu nabádala k prověření bezpečnosti telefonu kliknutím na odkaz. To však způsobilo odeslání prémiové SMS v ceně 99 Kč. Současně bylo nastaveno opakované odesílání těchto zpráv. Někteří uživatelé takto přišli o stovky i tisíce korun.

2.4.3 LXC kontejnery

V dokumentaci k routeru Turris je popsán způsob instalace a provozování LXC kontejnerů. Jedná se o tzv. „light-weight“ virtualizaci, kdy na jednom fyzickém stroji lze provozovat více virtualizovaných linuxových kontejnerů. Této vlastnosti routeru Turris bude využito v praktické části práce. Každý kontejner v sobě má samostatný izolovaný souborový systém. *„Uvnitř kontejneru je možné provozovat různé GNU/Linux distribuce (např. Ubuntu nebo Debian)“* [11]. Virtuální stroje sdílí jádro operačního systému routeru. LXC technologie přiděluje každému kontejneru systémové prostředky, řídí přístupy k procesoru, operační paměti, diskovým jednotkám, síťovým rozhraním a podobně. Velkou výhodou tohoto řešení je, že kontejner není ovlivněn změnami v operačním systému routeru.

2.5 Testování LXC kontejnerů

Autor otestoval postupně 11 LXC kontejnerů, aby zjistil zatížení systému a použitelnost každého z kontejnerů pro naplnění zadání práce. Během několikaměsíčního testování bylo vydáno více aktualizací operačního systému. Všechny instalace proběhly bez negativního vlivu na fungování kontejnerů. Dokonce ani reset routeru do továrního nastavení neměl negativní vliv na fungování kontejnerů. Naopak smazání kontejneru se nijak neprojevilo na chod routeru. V následujících kapitolách budou popsány všechny testované kontejnery seřazené podle abecedy. Na závěr každé kapitoly bude uvedeno, jestli bude kontejner provozován v reálné instalaci a jaké k tomu měl autor důvody.

Tady je třeba zopakovat upozornění výrobce, že před zahájením instalace LXC kontejnerů je nezbytné připojit a nakonfigurovat externí úložiště. Bez externího úložiště by se využívala interní eMMC flash, která by byla nadměrným počtem zápisů velmi rychle zničena. O instalaci externího úložiště bude pojednáno v praktické části této práce.

2.5.1 Domoticz

Velice zajímavý OpenSource projekt, který umožňuje monitoring a řízení velkého množství nejrůznějších čidel, spínačů, měřicích zařízení a jiných zařízení bez ohledu na jejich architekturu. Ovládat lze světla (barva v RGB, intenzita svícení), spínače, dále je možné monitorovat různé senzory teploty, vlhkosti, množství srážek, rychlosti a směru větru, intenzity ultrafialového záření, spotřeby/výroby elektřiny, spotřeby plynu, spotřeby vody a mnoho dalšího. Je podporován také systém notifikací, kdy je možné oznámení zasílat na e-mail nebo formou SMS zpráv na mobilní telefon. Domoticz má svoji databázi, kde jsou uchovávány naměřené hodnoty a stavy komponent zapojených do systému. Funkce jednotlivých komponent umí Domoticz skládat do scénářů podle přání uživatele. Díky práci komunity je podporována obrovská šíře nejrůznějších elementů třetích stran, jsou to komerčně dodávané prvky systémů Z-Wave, P1 Smart Meter, YouLess Meter, Pulse Counters, 1-Wire, EnOcean, MySensors a mnoho dalších. Nízká náročnost systému Domoticz na systémové prostředky umožňuje jeho nasazení například na jednodeskové počítače Raspberry Pi. Otevřený systém umožňuje mimo jiné také tvorbu vlastních konektorů, díky nimž je možné například ovládat televizor, monitorovat stavy PC (teploty komponent, využití CPU nebo RAM), či cokoli jiného.

Potenciál systému Domotic ve spojení s routerem Turris byl využit ve výzkumném projektu společností JABLOTRON ALARMS a.s. a CZ.NIC, z. s. p. o. Projekt se jmenoval Turris Gadgets a cílem projektu bylo s pomocí routeru Turris vytvořit řešení chytré domácnosti s využitím 11 komponent Jablotron viz Tabulka 2

Tabulka 2. Obsah sady a popis periferií [12]

Označení	Popis	Počet	Příklad použití
AC-82	Přijímač 2x relé 230V	1 ks	Ovládání světel
AC-88	Dálkově ovládaná zásuvka	2 ks	Zapnutí přímotopu
JA-80L	Interní siréna	1 ks	Zvuková signalizace
JA-81M	Univerzální rozhraní	1 ks	Pro připojení externích detektorů
JA-82SH	Detektor otřesu nebo náklonu	1 ks	Detekce manipulace s předměty
JA-83M	Magnetický detektor mini	2 ks	Detekce otevření dveří
JA-83P	PIR detektor	2 ks	Detekce pohybu osob
JA-85ST	Detektor kouře a teploty	1 ks	Detekce požáru

RC-86K	Dálkový ovladač	2 ks	Aktivace/deaktivace systému
TP-82N	Termostat	1 ks	Regulace teploty

V rámci tohoto projektu byly v roce 2015 mezi 90 takzvaných „Turristů“ (uživatelů routerů Turris) rozdány sady komponent společnosti Jablotron. *„V pilotní etapě projektu byla vybraným účastníkům bezplatně zapůjčena sada periferií s úkolem navrhnout smysluplné i bláznivé příklady užití domácí automatizace“* [13]. Pro tento projekt existoval speciálně upravený firmware a server Domoticz byl jeho součástí. Pro komunikaci mezi routerem a periferiemi Jablotron byl použit USB dongle pro RF komunikaci na frekvenci 868,5 MHz.

Takto byla integrace popisována v dokumentaci k projektu.

„Domoticz je integrovaný software pro domácí automatizaci, který podporuje mnoho různých technologií jako je Z-Wave, 1-Wire, EnOcean, MySensors a další. Do této aplikace byla implementována i podpora pro sadu Turris Gadgets“ [14].

SRV_DOMOTICZ v LXC kontejneru funguje bez problémů. Pro plánované nasazení je jeho provoz nezbytný.

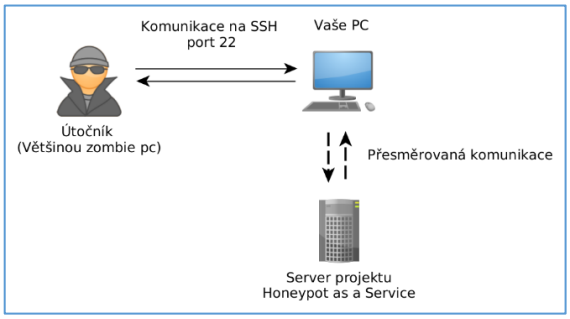
2.5.2 GitLab

GitLab je webový repozitář (úložiště) se systémem podporujícím řízení verzí. Podporuje sledování chyb a umožňuje ukládaný kód detailně dokumentovat ve vestavěné wiki. GitLab je podobný funkcemi projektu GitHub, ale navíc umožňuje, aby se dal použít na serverech třetích stran. Je dostupný jako balíček Omnibus. Nasazení je vhodné například pro vývojáře software. Git je centrálním bodem pro řízení workflow, spolupráci více vývojových týmů, ukládání rozpracovaných verzí, jejich testování a spojování. Gitlab server je velmi náročný na systémové prostředky.

SRV_GITLAB v LXC kontejneru při testování fungoval. Jeho nasazení je nezbytné zejména tam, kde se vyvíjí software. Pokud je pro provozovatele prioritou zajistit absolutní kontrolu nad tím, kde jsou data uložena, pak musí provozovat GitLab lokálně. Pro reálné používání je však vhodné využít jiný HW než router. V plánovaném nasazení nebude LXC kontejner použit.

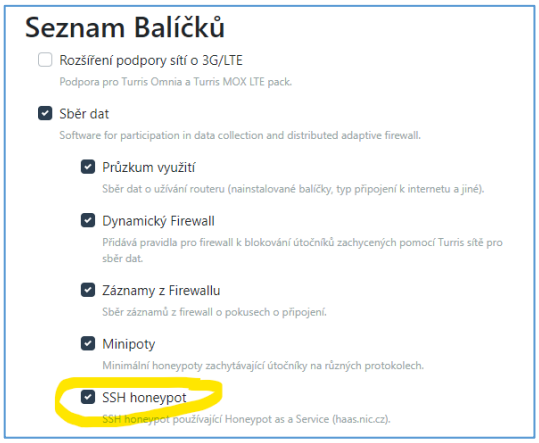
2.5.3 HAAS

Název tohoto kontejneru pochází ze zkratky Honeypot as a Service (HaaS). Provozování tohoto serveru simuluje běžící nezabezpečený operační systém. Útočník ho při prohledávání webu najde a pokusí se do něj přihlásit přes SSH nebo telnet. S tím se počítá a přes proxy je komunikace přesměrována na server projektu. Veškeré příkazy nebo pokusy o instalaci malware jsou zaznamenávány a vyhodnocovány v centrále Národního CSIRT týmu České republiky viz *Obr. 4*. Zapojit se může každý, kdo je ochoten svoje zařízení poskytnout pro analýzu chování útočníků.



Obr. 4 Schéma komunikace HaaS [15]

SRV_HAAS v LXC kontejneru funguje. Asi od poloviny roku 2020 je HaaS implementován přímo do operačního systému routeru. Pro jeho správný běh pak stačí pouze vybrat balíček ve webovém rozhraní routeru Turris viz obrázek *Obr. 5*.



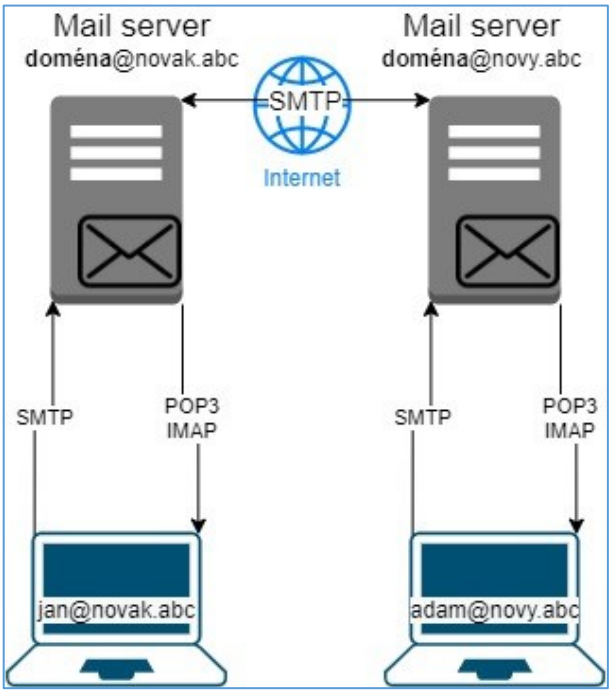
Obr. 5 Přidání balíčku SSH honeypot [Zdroj: vlastní]

Registrací na stránkách projektu https://haas.nic.cz dostane zájemce identifikační token, ten se pak vloží jako parametr při jednoduché konfiguraci honeypotu. Uživatel routeru Turris se tím zapojil do projektu. Přispívá tak ke zvyšování úrovně kybernetické bezpečnosti a připravenosti na kybernetické útoky ČR. Dalším benefitem je získání zajímavých informací

o útocích na zapojené zařízení. V plánovaném nasazení nebude LXC kontejner použit. Jeho funkce jsou implementovány do operačního systému routeru.

2.5.4 Mail server

Komunikace prostřednictvím e-mailových zpráv je notoricky známá, méně známé jsou prostředky, díky kterým je zasílání e-mailů umožněno. K provozování vlastního mail serveru mohou vést specifické požadavky provozovatele. Důvodem může být požadavek na absolutní kontrolu nad svými e-maily, snaha vymanit se ze závislosti na velkých poskytovatelích, potřeba specifických nastavení nebo jen chuť si hrát a rozšiřovat obzory. Simple Mail Transfer Protocol (SMTP) byl definován jako standard RFC 821 v roce 1982 jako protokol určený pro přenos zpráv elektronické pošty. [16] Standard definuje "účastníky" přenosu jako MTA – Mail Transfer Agent server. Pro přenos e-mailové zprávy MTA na straně odesílatele naváže spojení s MTA na straně příjemce a zajistí doručování zprávy přes internet. Na *Obr. 6* je znázorněna komunikace mezi dvěma mailservery.



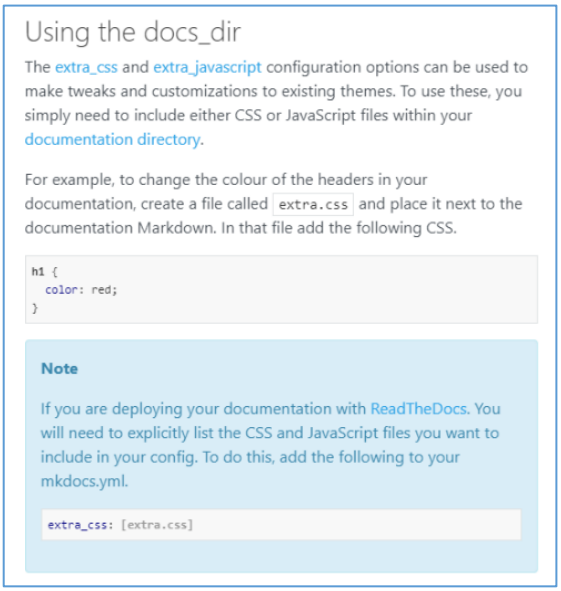
Obr. 6 Schéma komunikace dvou mail serverů [Zdroj: vlastní]

LVC kontejner SRV_MAIL byl úspěšně nakonfigurován a otestovány jeho funkce. Pro zajištění komfortního a bezpečného provozu je nutné v serveru spustit několik přidružených služeb. Aby byl mailserver použitelný pro osobní použití nebo pro menší firmy, musí se vybrat takové služby, aby byly zachovány požadavky na bezpečnost a rozumnou míru údržby. Cílem by měl být mail server s odpovídajícím zabezpečením a ochranou proti podvodným

e-mailům. Složitost a komplexnost problematiky a současně vysoké požadavky na systémové prostředky jsou důvodem, proč tento LXC kontejner nebude v plánovaném nasazení použit. Velcí poskytovatelé e-mailových služeb jako například Microsoft, Google, Yahoo, Protonmail, nebo největší poskytovatel v Česku Seznam, mají týmy profesionálů, kteří zajistí bezpečnost provozu mailserveru. Pokud nemá uživatel konkrétní specifické požadavky na provoz mail serveru, je bezpečnější využívat služeb například některé z výše uvedených firem.

2.5.5 MkDocs

MkDocs je open source „wiki software“ pro generování statických stránek. Jeho funkce ho předurčují pro využití na tvorbu dokumentace, blogu, wiki nebo jednoduchých poznámek na webu. K běhu nepotřebuje používat databázi. Syntax pro formátování textu je jednoduchá a umožňuje využít dostatečně atraktivní vzhled stránek. Na *Obr. 7* je ukázka možností formátování.



Obr. 7 Možnosti formátování v MkDocs [17]

Systém pro ukládání poznámek, případně psaní návodů může být velmi přínosný. Strukturované informace se dají publikovat do internetu a mohou být použity jako vždy přístupná znalostní báze. Systémové nároky na provozování tohoto kontejneru byly při testování příliš vysoké. LXC kontejner SRV_MKDOCS nebude v plánovaném nasazení použit. Jeho použití by nebylo přínosem pro požadované funkce a naplnění zadání práce. Autor je však přesvědčen o velkém potenciálu této technologie a bude hledat jiné možnosti pro jeho nasazení.

2.5.6 MQTT

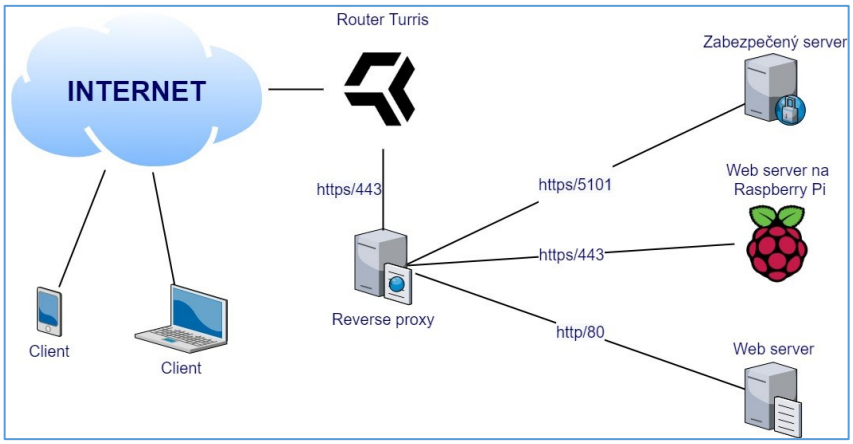
Pro zajištění komunikace mezi prvky domácí automatizace se s výhodou používá MQTT protokol. Definován byl firmou IBM v roce 1999 jako jednoduchý a nenáročný protokol pro předávání zpráv mezi klienty prostřednictvím centrálního bodu – brokeru. Nenáročnost jej předurčila pro implementaci do zařízení s jednoduchými procesory, které se používají v zařízeních pro IoT. Přenos probíhá pomocí TCP spojení. Jeden centrální bod, MQTT broker zajišťuje vzájemnou komunikaci všech zařízení v síti. Pro plánované nasazení je LXC kontejner SRV_MQTT nezbytný. V kontejneru byl otestován open source MQTT broker Mosquitto, ten může běžet jak pod operačním systémem Windows, tak i pod Linux. Testována byla pochopitelně verze pod Linux.

2.5.7 Nginx

Nginx je softwarový webový server s otevřeným zdrojovým kódem. Pracuje s protokoly HTTP, SMTP, POP3, IMAP a SSL. Podle dokumentace je jeho výhodou nízká náročnost, zejména nízké nároky na paměť a vysoký výkon [18]. LXC kontejner SRV_ NGINX byl úspěšně zprovozněn a otestován. NGINX je podmínkou pro fungování Vouch proxy viz kapitola 2.5.11. Důvodem pro jeho implementaci je deklarovaná schopnost rychlé distribuce statického obsahu webových stránek pro větší počet připojených klientů. Tento kontejner je nezbytný pro plánované nasazení.

2.5.8 Proxy

Proxy server je často nasazován do firemní infrastruktury pro funkcionality jako je filtrování komunikace, statistika provozu, cashování načítaných webových stránek nebo jako náhrada NAT. Možnosti využití proxy jsou velice široké a nemělo by smysl je všechny popisovat. V principu proxy plní roli prostředníka mezi klientem a cílovým serverem. Klient, tím může být webový prohlížeč, pošle požadavek na zobrazení určité webové stránky, proxy server požadavek přebere, vytvoří záznam, zkontroluje, jestli není požadavek v rozporu s pravidly a pak klientovi předá/nepředá požadovanou informaci. Pokud je využíváno cashování stránek, každý další požadavek ze sítě na stejnou webovou stránku může být vyřízen rychleji z casch paměti proxy. Chování proxy z pohledu komunikace se tady dá rozdělit na dva případy, kdy se chová jako server při komunikaci s klientem a jako klient při komunikaci se serverem. Pro názornost je na *Obr. 8* je zobrazeno zapojení proxy v popisované realizaci.



Obr. 8 Schéma použití reverzní proxy pro rozdělení komunikace [Zdroj: vlastní]

LXC kontejner SRV_ PROXY byl úspěšně zprovozněn a otestován. Jeho využití v plánovaném nasazení bude popsáno v praktické části. Využita bude pouze funkcionalita rozdělení požadavků od klientů na různé servery uvnitř sítě.

2.5.9 SSLH

Funkcionalitou tohoto serveru je přepínání příchozího spojení na jednom portu (443, protokol HTTPS) mezi servery SSH a SSL. To umožní přístup do sítě přes port 443 a spravovat servery přes SSH. Nejčastěji bude tato funkcionalita využívána z nějaké podnikové sítě, kde je povolena komunikace pouze přes porty 80 a 443. Odchozí komunikace ze sítě s restrikcemi je povolena pouze na portech 80 a 443. Požadavky jsou odesílány šifrovaně přes port 443, což je standardní port pro prohlížení webových stránek zabezpečených šifrováním. SSHL na straně příjemce rozdělí tato příchozí připojení k příslušnému serveru. To vyžaduje pouze spuštění serveru HTTPS na nestandardním portu (ne 443) [19]. Takto bývají zabezpečeny podnikové sítě ale mnohde i sítě v hotelích a podobně. *„Určitě se vám už nejednou stalo, že jste přišli do sítě, ve které příliš horlivý správce zakázal všechny porty kromě 80 a 443. Typicky se to stává třeba v hotelích. Běžnému uživateli „internet funguje“, takže nemá důvod se zlobit. Pokud ale chcete použít třeba SSH, Jabber nebo OpenVPN, jste nahraní. Na příslušný port se prostě nedostanete“* [20] . Bez funkčního serveru SSHL by pak nebylo v těchto specifických případech přistupovat k domácí síti. LXC kontejner SRV_SSLH byl úspěšně otestován, jeho provoz měl zanedbatelný vliv na zvýšení zátěže systému, pro naplnění požadavků je nezbytný, proto bude použit v plánovaném nasazení.

2.5.10 Synbak

Synbak je Linux aplikace navržená k zálohování. Poskytuje velmi jednoduché rozhraní pro konfigurační soubory a systém hlášení, který se dá detailně nastavit. Provádění každé jednotlivé zálohy se dá detailně nastavit. O výsledku je vytvořena podrobná a konfigurovatelná zpráva o výsledku zálohování.

Synbak podporované způsoby zálohování:

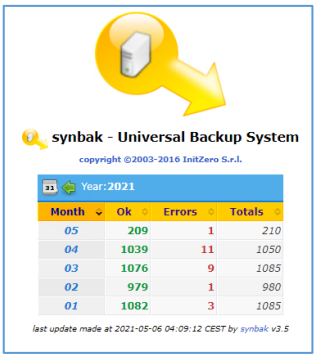
- RSync přes protokoly ssh, rsync, smb a cifs (pomocí interních funkcí automatického připojení)
- Tar archivy (tar, tar.gz a tar.bz2)
- Pásková zařízení (s podporou uložení na více pásek)
- LDAP databáze
- MySQL databáze
- Databáze Oracle
- PostgreSQL databáze
- CD-RW / DVD-RW
- Wget pro zrcadlení serverů HTTP / FTP

Modulární povaha synbaku umožní psát nové metody zálohování, zpráv a překladů. Jedná se o opesource projekt, takže se znalostí programování se dá jakkoli přizpůsobit konkrétním potřebám.

Synbak podporované způsoby vytváření zpráv

- E-mailem
- Vytvoření stránky HTML
- Vytvoření RSS zdroje

Na *Obr. 9* je výpis provedených záloh za rok 2021. Při detailnějším pohledu je možné jednoduše dohledat a odstranit problémy se zálohováním.

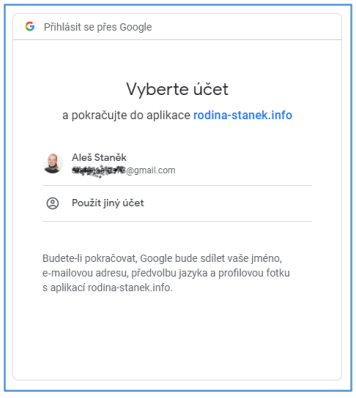


Obr. 9. HTML stránka generovaná Symbak [Zdroj: vlastní]

Informace čerpány z dokumentace přístupné na GitHub projektu [21]. Pro zamýšlené nasazení je zavedení systému zálohování velice důležité. LXC kontejner SRV_SYNBAK byl otestován a bude použit v plánovaném nasazení.

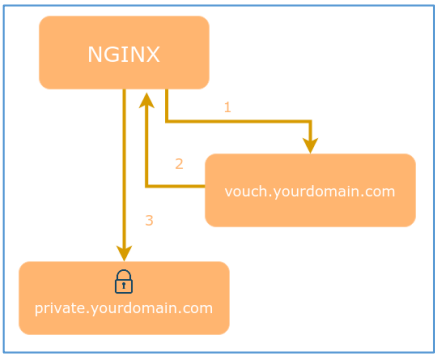
2.5.11 Vouch proxy

Vouch proxy je zajímavým řešením pro zabezpečený přístup k webovým stránkám. Využívá se tu modul auth_request, který vyhodnocuje požadavky na připojení na základě subpožadavku. Princip spočívá v tom, že se ověří identita u identity providera (často se požívá zkratka IdP nebo IDP). Mezi podporovanými autoritami jsou například: Google, GitHub, GitHub Enterprise, IndieAuth, Okta, ADFS, Azure AD, Alibaba / Aliyun iDaas, AWS Cognito, Gitea, Keycloak, OAuth2 Server Library for PHP, HomeAssistant, OpenStax, Nextcloud a mnoho dalších [22]. Přístup k webovým stránkám tak majitel může povolit pouze vybranému uživateli nebo skupině uživatelů, kteří svoji totožnost ověřili u extení autority. Vouch Proxy před přístupem k zabezpečené stránce nutí návštěvníka, aby se přihlásili a ověřili pomocí IdP, než mu umožní přístup na web. Ukázka ověřovacího okna před umožněním přístupu na zabezpečenou stránku je na *Obr. 10*.



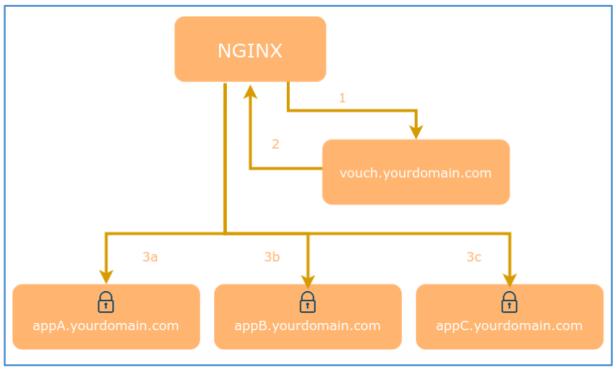
Obr. 10 Požadavek na přihlášení u Google [Zdroj: vlastní]

Pro větší názornost je na *Obr. 11* schematicky znázorněno předávání požadavku na ověření a zapojení SRV_NGINX.



Obr. 11 Zabezpečení jedné domény [23]

Vouch proxy lze také použít jako řešení jednotného přihlášení (SSO) k ochraně všech webových aplikací ve stejné doméně viz *Obr. 12*.



Obr. 12 Zabezpečení více domén [23]

Po přihlášení návštěvníka umožňuje Vouch Proxy přístup na chráněné webové stránky na několik hodin. Každý nový požadavek zkontroluje, aby se ujistil, že je platný [23].

SRV_VOUCH lze použít k úplnému nahrazení správy uživatelů aplikace. Při zachování poměrně vysoké míry zabezpečení je ověření identity velmi efektivní při současném zachování velké míry pohodlí pro uživatele. Pro plánované nasazení bylo otestováno ověření přes Google. Tento kontejner bude použit pro plánované nasazení.

2.6 Domácí automatizace

Pojem Home Automation s překladem do češtiny domácí automatizace je mnohdy spojován s pojmem smart home neboli chytrá domácnost. Do této kategorie bývají zařazovány

nejrůznější výrobky, které se mohou ovládat přes mobilní telefon. Mohou mít možnost vzdáleného ovládání přes webový prohlížeč v místní síti, častěji však přes cloud výrobce. Pak je možné se odkudkoli podívat na stavové hodnoty takového zařízení nebo měnit jeho funkční nastavení. To ale ještě není automatizace. Aby byl naplněn význam slova automatizace, je potřeba, aby systém něco dělal automaticky na základě vyhodnocení vstupních/výstupních hodnot. Některá zařízení, která jsou prodávána jako „chytrá" nakonec nejsou ani chytrá, ani nepomáhají jejich uživatelům ke snadnějšímu a pohodlnějšímu ovládání zařízení. Pokud je jedinou „chytrou" funkcionalitou možnost zapnout zařízení přes mobilní telefon, pak je takové zařízení pro provoz v běžné domácnosti spíše přítěží. Je mnohem rychlejší a pohodlnější zapnout lampu tradičním vypínačem než hledat pro zapnutí mobilní telefon, ten odemknout, najít a spustit ovládací aplikaci, a teprve potom zapnout lampu. Dalším problémem může být bezpečnost takových zařízení s ohledem na to, jak výrobce přistupuje k bezpečnosti a ochraně soukromí uživatele. Jedním z takových zařízení je například „E.ON Chytrá zásuvka". Více v kapitole 2.6.1 Chytrá zásuvka Revogy.

Požadavky autora na výběr komponent pro vybudování modelového řešení domácí automatizace byly zejména důraz na bezpečnost, přiměřené finanční náklady a spolehlivost řešení. Dalším požadavkem bylo také smysluplné vyřešení konkrétních případů používání. Nasazování „chytrých" technologií musí v první řadě zpříjemnit život uživatelům. Společnost Loxone na svých stránkách přímo uvádí: *„Pod pojmem chytrý dům si dnes můžeme představit ledasco. Většinou všemožná udělátka, která nás okrádají o čas a komplikují nám život. Podle Loxone musí inteligentní dům splňovat přesný opak. Vědět vždy sám, co má dělat a šetřit obyvatelům tisíce akcí"* [24]. Účelem této práce není návrh komplexního řešení chytré domácnosti. V praktické části bude zprovozněn systém s velkým potenciálem pro další rozvoj. Bude však založen pouze na základních komponentách s důrazem na to, aby se řešení nestalo rizikem pro domácí počítačovou síť. Domácí automatizační prvky byly voleny takové, které mají jednoduchou funkcionalitou a umožní ověření funkčnosti celého systému. Další charakteristické znaky jsou použití open source a nízká cena. Zvolená konfigurace je zaměřena zejména na praktické využití. Některé automatizační systémy bývají komplikované na použití, případně bez promyšlené ergonomie. Systémy mohou ušetřit mnoho času sestavením scénářů, kdy po příchodu domů se zapne osvětlení na chodbě, to se po nastavené době automaticky vypne, v obýváku se mezitím rozsvítí tlumené osvětlení a spustí se centrum multimediální zábavy. Podobný scénář může být navržen například pro pohony žaluzií a venkovní markýzy, kdy při překročení nastavené rychlosti větru se markýza složí do bezpečné polohy

a žaluzie jsou natáčeny tak, aby se odpoledním sluncem zbytečně neprohříval interiér budovy. Naproti tomu ovládat světla v pokoji aplikací v mobilu je velmi nepraktické. Musíte najít telefon, odemknout ho, spustit potřebnou aplikaci, najít správný pokoj a v něm ovládací prvek pro osvětlení, a teprve pak zapnout světlo, zatímco osvědčeným postupem najdete vypínač a vše je jednodušší a praktičtější.

A právě na jednoduchost, praktičnost, a zároveň také modulárnost a rozšiřitelnost je zaměřena praktická část této práce.

2.6.1 Chytrá zásuvka Revogy

Tato kapitola byla zařazena zejména proto, že autor narazil na bezpečnostní riziko konkrétního produktu. Po analýze bude v praktické části navržen způsob, jak minimalizovat rizika takového zařízení, aniž by došlo k ohrožení LAN sítě uživatele.

Společnost E.ON Česká republika před časem svým zákazníkům při splnění určitých podmínek rozdávala „E.ON Chytrou zásuvku“. Jednalo se o re branding zařízení čínské firmy Revogi. Chytrá zásuvka Revogi se v té době prodávala v mnoha e-shopech v Česku za cenu cca 1.100 Kč viz *Obr. 13*.

Obr. 13 Zásuvka Revogi [25]

V rámci re brandingu byla vytvořena aplikace pro OS Android v barvách e.on. viz *Obr.* 14. Tato aplikace však nebyla dobře odladěna a zprovoznit ovládání přes mobilní telefon končilo chybou. Aplikace byla v kombinaci s použitým mobilním telefonem, jeho verzí operačního systému a Chytrou zásuvkou nefunkční. V hodnocení uživatelů byla aplikace na velmi nízké úrovni, stejně tak slovní komentáře uživatelů byly velmi kritické.

Obr. 14. *Nefunkční aplikace E.ON* [26]

Pro otestování produktu bylo nutné použít původní aplikaci od Revogi. Při testování však byly odhaleny poměrně závažné bezpečnostní problémy. V praktické části této práce bude popsán způsob, jak lze výrazně snížit rizika a s určitými omezeními zařízení připojit do domácí sítě a používat jej.

Obr. 15. Funkční aplikace Revogi Home [27]

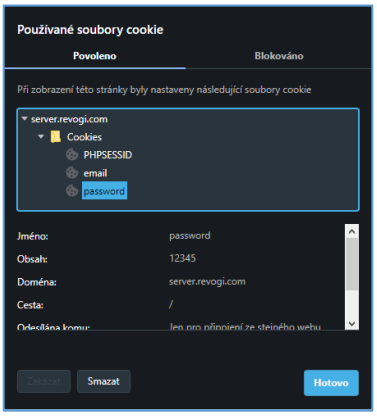
Podle přiloženého návodu k použití je nejdříve nutné se zaregistrovat na webu výrobce s adresou http://server.revogi.com. Existuje také verze přihlašovací stránky, která komunikaci šifruje https://server.revogi.com, ale preferovanou stránkou je verze s protokolem http viz *Obr. 16*.

```
305         <script type="text/javascript">
306             if ("ontouchend" in document) document.write("<script src='rassets/js/jquery.mobile.custom.min.js'>" + "<" + "/script>");
307             var mainDomain='server.revogi.com';
308 var ssl='HTTP';     </script>
309
```

Obr. 16 Kód stránek s nastavením preferované verze stránek [Zdroj: vlastní]

Problém je v tom, že komunikace je vedena protokolem http (tedy bez šifrování). Login a heslo se přenáší internetem v plain textu. Obě webové stránky jak http, tak i https, jsou během procesu registrace přesměrovány na adresu http://eu.revogi.net (opět stránka bez

šifrování). Tato stránka už nemá ekvivalent s použitým šifrování. Dalším problémem je, že stránka si ukládá do souboru cookies jak login, tak i heslo, a to bez možnosti heslo neukládat. Heslo se tak uloží vždy viz *Obr. 17*.

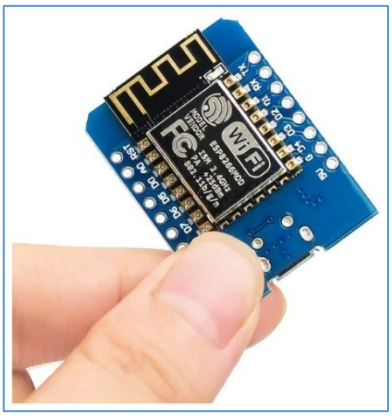


Obr. 17 Analýza cookies, heslo v plaintextu [Zdroj: vlastní]

Pro uživatele je to možná pohodlné, z pohledu bezpečnosti to přináší velká rizika. Společně s přihlašovacími údaji do cloudu společnosti Revogi uživatel také odešle SSID svojí WiFi sítě a samozřejmě i heslo k této síti. Založit domácí automatizaci na podobných zařízeních by znamenalo velké bezpečnostní riziko a zcela jistě by byl také naplněn výše zmiňovaný problém s „udělátky“, která uživatele okrádají o čas.

2.6.2 Sonoff

Čínská firma ITEAD Inteligent System Co. Ltd. produkuje velké množství jednoduchých elektronických zařízení. Před rozdělením produktového portfolia v roce 2018 uváděla produktová wiki počet nabízených produktů 222, z toho 17 zařízení Sonoff [28]. Z počátku byly produkty Sonoff postaveny na čipu ESP8266, produktová řada je aktuálně rozšiřována o radiofrekvenční (RF) verze, komunikující v pásmu 433MHz a nejnovější s implementovanou technologií ZigBee. Charakteristickým znakem pro IoT komponenty komunikující přes síť WiFi je právě čip ESP8266 viz *Obr. 18*.



Obr. 18 Čip ESP 8266 na jednoduché destičce pro prototypování [29]

Jedná se o velmi levný čínský čip, který se dostal nejdříve do hledáčku hackerů díky své funkcionalitě a nízké ceně. Tento malý modul umožňuje mikrokontrolérům připojení k síti WiFi a vytváření jednoduchých připojení TCP/IP. Díky zabudované flash paměti umožňuje budování jednočipových zařízení schopných připojení k WiFi.

V říjnu 2014 společnost Espressif Systems vydala“ (SDK) pro přímé programování čipu ESP 8266, která odstranila potřebu samostatného mikrokontroléru [30]. Alternativou k oficiální sadě Espressif je více, než 20 open-source SDK. Mezi nejznámější asi patří Arduino, založené na C++, ESP Easy, ESPHome, MicroPython s implementací Pythonu a v neposlední řadě Tasmota - open-source firmware, velmi oblíbený u nadšenců domácí automatizace. Právě toto SDK bude použito pro úpravu HW spínačů viz kapitola 2.6.3.

Všechny produkty Sonoff mají certifikaci CE, jsou tedy schváleny k prodeji a užití v EU. Další certifikací je RoHS, což je norma omezující používání některých nebezpečných látek v elektrických a elektronických zařízeních. Zařízení Sonoff jsou velice levná. Dají se objednat na zahraničních e-shopech za několik dolarů. České e-shopy je mají v nabídkách také, většinou asi o 50 % dražší, ale některé nabízí možnost objednat spínače už s nahraným firmware Tasmota.

K zajištění požadovaných funkcionalit byly zvoleny následující produkty:

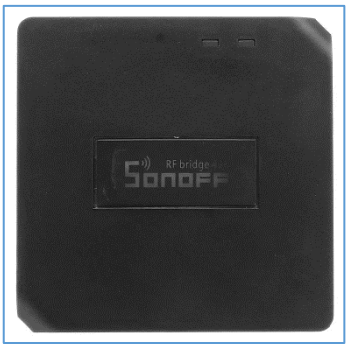
- **Sonoff Basic** – nejjednodušší vypínač viz *Obr. 19*, který je vhodný tam, kde se nepoužívá zemnící vodič, typicky lampička. Vnější rozměry krabičky z ABS plastu jsou 88 x 38 x 25 mm. Vstupní napětí se může pohybovat v rozmezí 90 - 250 V střídavého napětí. Dokáže spínat maximálně 10 A. Pro bezdrátovou komunikaci používá standardy IEEE 802.11 b/g/n. Výrobcem uváděná spotřeba v režimu stand-by je menší než 0,5 W.

Obr. 19 Jednoduchý spínač Sonoff Basic [31]

- **Sonoff POW** – tento vypínač viz *Obr. 20* je konstrukčně určen pro vyšší zátěž než předchozí Basic, zvládne spínat obvod do maximálního proudu 16 A. Hodnota vstupního napětí i standardy pro bezdrátovou komunikaci jsou stejné jako u Basic. Vnější rozměry jsou větší 114 x 52 x 32 mm. V zapojení se už počítá se zemnícím vodičem, tento vypínač je vhodný pro spínání spotřebičů jako je rychlovarná konvice, automatický kávovar, pračka a jiné. Přidanou funkcionalitou je měření aktuálních elektrických veličin napětí a proudu, a z nich počítaný příkon a spotřeba připojeného spotřebiče. Hodnoty ukládá v interní paměti, zobrazit se dají v historii po dnech a měsících.

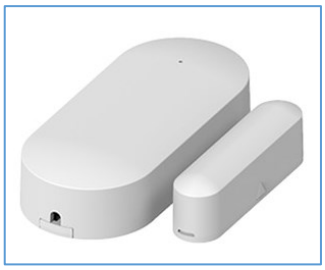
Obr. 20 Sonoff POW umí navíc měřit hodnoty proudu, napětí a spotřeby [31]

- **Sonoff RF bridge** – už z názvu se dá vytušit, že toto zařízení viz *Obr. 21* zajistí spojení dvou „břehů“. Spojí WiFi síť s téměř jakýmkoliv RF zařízením s pracovní frekvencí 433MHz. Důležitou podmínkou je shodné RF kódování. Sonoff RF bridge má implementováno dle dokumentace 17 různých kódování, ale existuje jich více. Bohužel se často nedá dohledat specifikace RF kódování neznačkových zařízení. Správný výběr se dá ověřit na uživatelských fórech nebo vlastním otestováním. Sonoff RF bridge podporuje spárování až se 16 zařízeními. Vnější rozměry krabičky jsou 62 x 62 x 20 mm. Bridge potřebuje externí napájení, které se připojí do konektoru mikro USB 5V.



Obr. 21 Sonoff RF bridge [31]

- **Magnetické RF čidlo PB-68** – pro výběr vhodného čidla je důležitá pracovní frekvence a kódování. U tohoto modelu je použito kódování EV1527, které podporuje také RF bridge. Dalším důležitým parametrem je počet stavů, které čidlo rozeznává. Čidlo z produktové řady Sonoff je velmi jednoduché a dokáže rozeznat pouze stav „otevřeno“. Pro zamýšlené nasazení je to nevhodné, neboť se nedá detekovat opětovné zavření okna. To byl důvod pro výběr čidla jiného výrobce, čínské firmy HIVA *Obr. 22*. Toto čidlo rozezná tři stavy a odešle o nich informaci (otevřeno, zavřeno, sabotáž). Principiálně je čidlo tvořeno dvěma částmi, jedna je pasivní a druhá je napájena baterií. Otevření detekuje odloučením jedné části od druhé a následně pošle tuto informaci přes RF signál do RF bridge a ten ji pak dál pošle přes WiFi do sítě LAN.



Obr. 22 Magnetické čidlo PB-68 [32]

2.6.3 Tasmota

Za vývojem tohoto software stojí Theo Arends, dnes CIO ve společnosti Tasmota. Od počátku byl vyvíjen jako alternativní firmware pro zařízení postavená na čipu ESP8266. Vývoj stále pokračuje a v IoT implementacích je velmi oblíbený. Používá licenci GNU General Public License v3.0. Podmínkou pro využití této licence je zveřejnění úplného zdrojového kódu licencovaných děl a úprav. Přístup k takto licencovanému SW je volný a pro komerční

i nekomerční využití je zdarma. Důvodem, proč měnit původní firmware za Tasmota, je při zachování všech funkcí, zamezení připojování do cloudu výrobce. Uživatel tak má absolutní kontrolu nad tím, kdo bude mít přístup ke stavovým hodnotám jeho prvků domácí automatizace.

Vše začalo v roce 2016, kdy Theo Arendst hacknul spínač firmy ITEAD Sonoff Basic. Vytvořil vlastní firmware a umožnil nahrávání nových verzí firmware metodou OTA „Over the Air“. Vše pečlivě dokumentoval a zveřejňoval podle zásad licence open source GPL-3.0. Vzniklo tak jednoho z prvních levných a přístupných zařízení pro inteligentní domácnosti na trhu. Během krátké doby tak vyrostl plnohodnotný ekosystém pro prakticky jakékoli zařízení založené na čipu ESP8266, informace čerpány z [33]. Na internetové adrese

http://ota.tasmota.com/tasmota/release/

je aktuálně 27 jazykových mutací včetně české. Pro zařízení Sonoff autor použil k flashování soubor „tasmota-CZ.bin“.

2.7 Shrnutí

V předchozích kapitolách jsem se věnoval popisu zdánlivě nesouvisejících témat. V následující praktické části budou výše popsaná témata spojena v jeden funkční celek. Základem bude výjimečný router Turris Omnia. Ten díky svým vlastnostem bude plnit roli síťového zařízení na perimetru sítě a zároveň zajistí HW platformu pro běh několika virtuálních serverů. Servery plní samostatné úkoly ve dvou oblastech, a to v oblasti bezpečnosti a správy počítačové sítě, a druhou oblastí je domácí automatizace.

II. PRAKTICKÁ ČÁST

3 DOMÁCÍ SÍŤ

Jaké mají být požadavky na počítačovou síť? Z pohledu laika by odpověď mohla znít asi takto: „Je mi jedno, jak se to udělá, jen ať to funguje“. Horák a Keršláger ve své knize definují důvod k tvorbě počítačové sítě takto: „Počítačové sítě se vytvářejí nebo vznikají za účelem výměny dat. Jedná se o jedno či více spojení mezi dvěma a více počítači za účelem výměny dat“ [34]. Důvodů by se dalo najít nespočet, stejně tak každé zadání může mít mnoho různých řešení, pro naplnění požadavků různými způsoby. V následující části této práce bude popsána konkrétní implementace. Autor se snažil každé rozhodnutí pro konkrétní řešení zhodnotit z těchto tří pohledů:

- Vliv na bezpečnost,
- ergonomie a snadné používání,
- přiměřená cena.

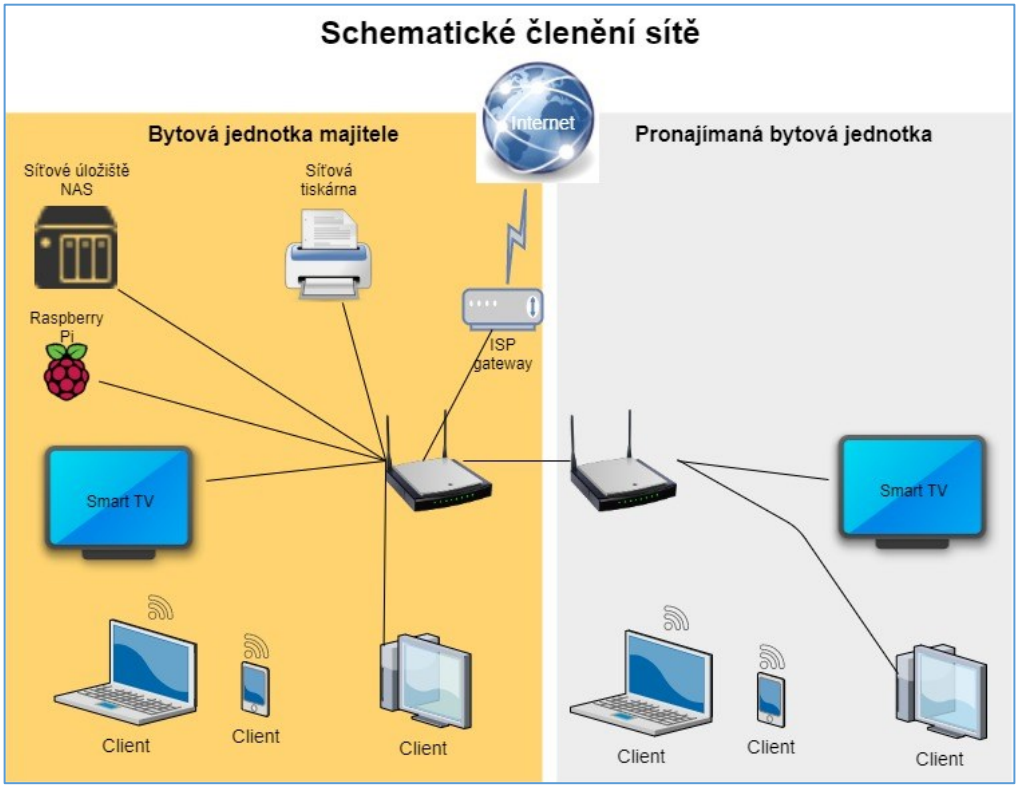
Z pohledu uživatelů měly být splněny zejména tyto funkční požadavky:

- Zajištění přístupu koncových zařízení do internetu, těmi zařízeními jsou počítače, notebooky a mobilní zařízení s operačním systémem Android,
- zajištění sdíleného datového úložiště s definovatelnými právy pro ukládání dat, zálohování, sdílení multimediálního obsahu, prostoru pro vytváření záloh,
- přístup k centrálnímu multifunkčnímu zařízení pro skenování a tisk dokumentů,
- nasdílení připojení do internetu pro návštěvy, bez možnosti přistupovat do domácí sítě,
- nasdílení připojení do internetu pro pronajímanou bytovou jednotku,
- vyřešení požadavků na automatické procesy v domácnosti s možností pohodlného „ručního“ zásahu,
- zajištění vzdáleného bezpečného přístupu z internetu pro administraci,
- zpřístupnění informací z některých zařízení v domácí síti pro definovanou skupinu uživatelů z internetu po ověření jejich identity.

3.1 Konfigurace domácí sítě

Jako referenční objekt byl vybrán rodinný dům se dvěma bytovými jednotkami. V domě je rozvedena strukturovaná kabeláž pro počítačovou síť. V době realizace stavby byla v dané lokalitě jediná možnost připojením k internetu přes venkovní WiFi anténu. Pro zajištění kvalitního signálu byla anténa umístěna na střeše domu. V roce 2017 byla k domu přivedena

internetová přípojka pomocí optického kabelu a majitel přešel k jinému poskytovateli připojení k internetu. Veškerá strukturovaná kabeláž pro budoucí domácí LAN byla svedena do jedné místnosti do samostatné rozváděcí skříně. Toto řešení je vhodné pro zajištění fyzické bezpečnosti počítačové sítě. Na *Obr. 23* je schematicky znázorněn aktuální stav sítě.



Obr. 23. Schematické členění počítačové sítě objektu [Zdroj: vlastní]

3.2 Konfigurace routeru Turris Omnia

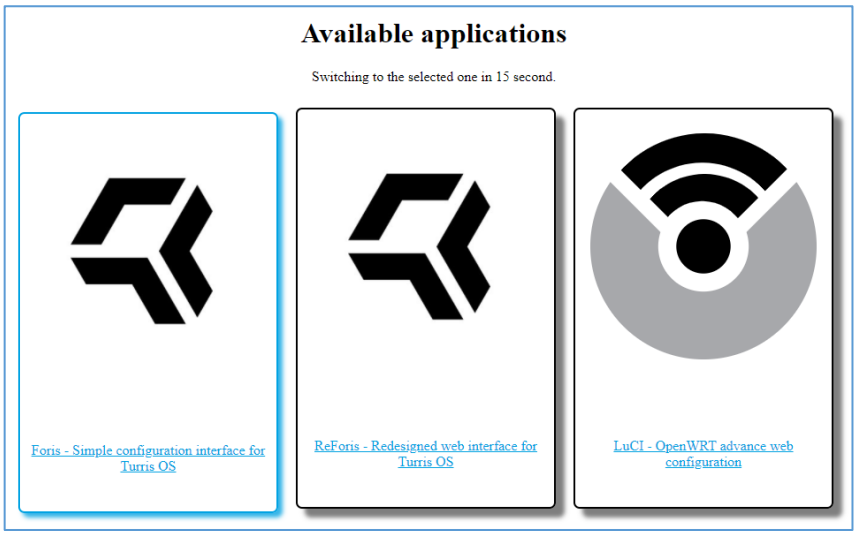
V této kapitole bude popsán postup pro nastavení routeru Turris Omnia pro tento konkrétní případ. Nebudou popisovány všechny možnosti nastavení, pouze ty, které jsou zásadní pro dosažení cílů práce.

Pro nastavení routeru je nutné se k němu připojit pomocí síťového kabelu. Předpokladem pro přístup do konfiguračního prostředí je, že jak router, tak i počítač, ze kterého se provádí konfigurace, jsou v jedné síti. První nastavení není možné provést přes WiFi. Toto nastavení zvyšuje bezpečnost procesu nastavení routeru. WiFi síť je defaultně vypnuta a její zapnutí lze provést v konfiguračním prostředí. Nemůže tak dojít k situaci, že se během prvotní konfigurace útočník připojí k WiFi s defaultním heslem. Je tím také eliminován nežádoucí stav, kdy se administrátor věnuje nastavení routeru, zatímco WiFi běží v default nastavení. Pro vstup do konfiguračního prostředí lze použít běžný webový prohlížeč, kde pak stačí

do adresního řádku napsat http://192.168.1.1/. Při prvním spuštění se zobrazí uvítací obrazovka viz *Obr. 24*.

Obr. 24. Úvodní konfigurační stránka [Zdroj: vlastní]

Průvodce je detailně komentován a to jak v češtině, tak i v angličtině. Detailní popis instalace přes průvodce by byl nadbytečný. Zásadní nastavení je nastavení dostatečně silného hesla. Autor doporučuje pro hesla používat SW správce hesel například KeePass, který nejen že dokáže generovat náhodná hesla s dostatečnou složitostí a definovanou délkou, ale také tato hesla spravuje a udržuje v šifrované databázi. Router Turris Omnia používá dvě, respektive tři různá grafická administrační prostředí. viz *Obr. 25*.

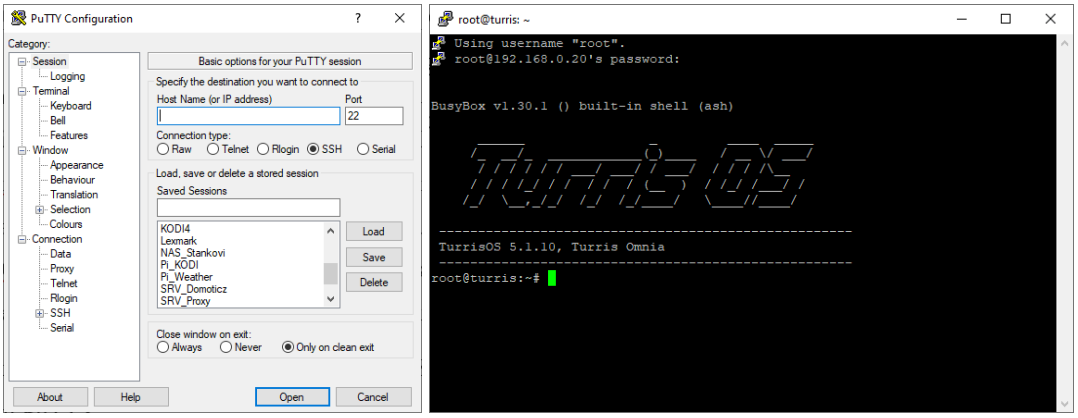


Obr. 25. Možnosti konfigurace routeru přes webové rozhraní [Zdroj: vlastní]

Pro zvýšení bezpečnosti je vhodné pro každé z těchto prostředí zvolit rozdílná hesla. Přístup k pokročilému konfiguračnímu rozhraní LuCI využívá stejné heslo také pro přístup do SSH terminálu uživatele root. SSH je další možností konfigurace routeru, zejména pro zkušené

uživatele. Konfigurace přes SSH nabízí nejširší možnosti nastavení oproti grafickým rozhraním (Foris, Reforis a LuCI). Funkce, které nelze v grafickém prostředí nastavit se, dají konfigurovat buď příkazy nebo editací konfiguračních souborů v příkazovém řádku.

Autor používal ke konfiguraci PC s operačním systémem MS Windows 10, na který nainstaloval aplikaci typu PuTTY viz *Obr. 26*.



Obr. 26. Program Putty a přihlášení do administrace Turris [Zdroj: vlastní]

Poslední nezbytné nastavení v průvodci se provede na kartě WAN. Pro připojení k vnější síti, v tomto případě do internetu, se nastaví WAN port podle specifikací ISP (většinou je to volba „DHCP automatické nastavení“). Po stažení aktualizací, jejich instalaci a následném restartu zařízení, je možné provést kontrolu nastavení a přístupu ke konfiguraci. Pokud vše funguje, je možné router zapojit jako centrální přístupový bodu domácí sítě.

3.2.1 Nastavení ze zjednodušeného konfiguračního prostředí Foris/Reforis

Prostředí Reforis má anglickou a českou lokalizaci. V české lokalizaci jsou však některé pasáže pouze v angličtině.

- Nastavení sítě
  - WiFi

    Zde byly nastaveny parametry WiFi sítě. Pro připojení „chytré zásuvky“ Revogi je třeba nakonfigurovat WiFi pro hosty. Zařízením připojeným k této síti je umožněn přístup do Internetu, nemají však přístup k ostatním zařízením v síti a nemají přístup k rozhraní Reforis. Síť pro hosty je oddělená od místní sítě (LAN).
  - WAN

    Protože ISP v lokalitě nepodporuje Protokol IPv6, je tato volba vypnuta

- DNS

  Zde je třeba zapnout volbu DNSSEC. „*Ve vzácných případech poskytovatelé připojení nemají správně nastavenou síť, což ovlivňuje DNSSEC ověřování. Pokud narážíte na problémy s DNS, můžete dočasně vypnout DNSSEC ověřování, abyste zjistili zdroj problému. Nicméně, mějte na paměti, že bez DNSSEC ověřování jste zranitelní k útokům podvržením DNS! Proto doporučujeme ponechat DNSSEC zapnuté a řešit situaci s vaším poskytovatelem připojení, protože se jedná o závažný nedostatek na jejich straně.“* [35]
- Rozhraní
- Síť pro hosty

3.2.2 Přidané balíčky do Turris OS

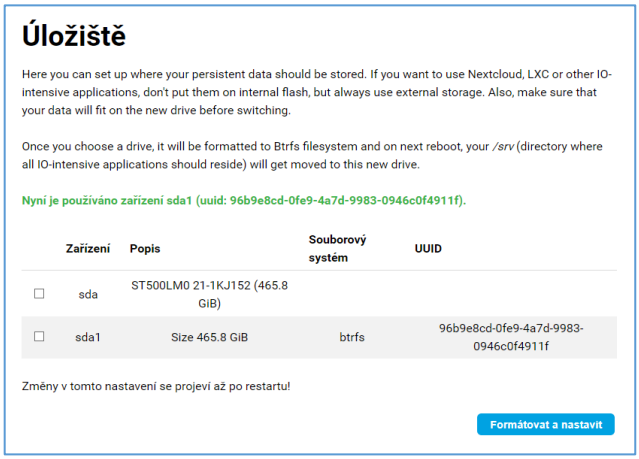
V nabídce Správa balíčků je možné zvolit sady dodatečného softwaru, pro dodatečnou instalaci do router. Výhodou toho je, že se potřebné balíčky jednoduše vyberou, po uložení se automaticky stáhnou, nainstalují a pak jsou součástí Turris OS. To znamená, že budou spravovány automatickými aktualizacemi. To se však netýká balíčků, které uživatel nainstaluje ručně nebo pomocí opkg.

Balíčky vybrané pro realizaci ze Správy balíčků:

- Sběr dat - Software pro účast na sběru dat a distribuovaný adaptivní firewall.
- Průzkum využití - Sběr dat o užívání routeru, odesílají se informace o nainstalovaných balíčcích, typ připojení k internetu a jiné.
- Dynamický Firewall - Přidává pravidla pro firewall k blokování útočníků zachycených pomocí Turris sítě pro sběr dat.
- Záznamy z Firewallu - Sběr záznamů z firewall o pokusech o připojení.
- Minipoty - Minimální honeypoty zachytávající útočníky na různých protokolech.
- SSH honeypot - SSH honeypot používající Honeypot as a Service (haas.nic.cz).
- Rozšíření do LuCI – Přidá několik dalších karet a ovládacích prvků pro pokročilé rozhraní LuCI.
- AdBlock – Umožní efektivně blokovat reklamy z webových stránek na úrovni routeru.
- Statistiky - Sběr a vykreslení diagramů pro systémové statistiky pomocí collectd.
- Nástroje pro LXC - Sada nástrojů pro správu linuxových kontejnerů (odlehčená virtualizační technologie).

- NAS - Služby umožňující připojit k routeru jednotku datového úložiště a používat ji jako síťovou.
- Samba - Implementace SMB síťového protokolu.
- Dohled nad sítí a rodičovská kontrola - Nástroje pro dohled nad sítí a jejích uživatelů.
- Měření rychlosti připojení k Internetu - Provádí aktivní měření rychlosti připojení k internetu pomocí služby netmetr.cz.
- Detekce nových zařízení – Upozorní na zařízení, která se poprvé objeví v síti.
- OpenVPN - OpenVPN server přístupný pro snadnou konfiguraci z uživatelského rozhraní Foris.

Po nainstalování všech výše uvedených balíčků je možné postoupit k připojení pevného disku. Postup připojení externího disku je jednoduchý. Provádí se v konfiguračním prostředí Foris, kde se provede připojení disku do systému tlačítkem Formátovat a nastavit. Na *Obr. 27* je vidět úspěšně připojený pevný disk.



Obr. 27 Úspěšně připojený disk [Zdroj: vlastní]

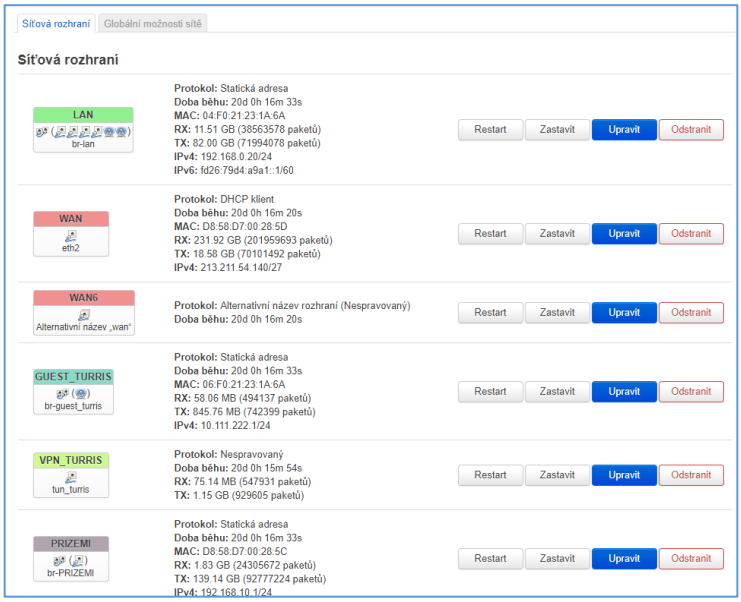
Pro toto nasazení je vhodné použít 2,5“ plotnový HDD s rozhraním USB 3.0. Rychlost disku při zápisu/čtení není limitující a díky použitému rozhraní je napájen výhradně z USB portu routeru. Dalšími výhodami plotnového disku je vysoká životnost při častém přepisování a nízká cena.

Pro zabezpečenou komunikaci z internetu je nutné konfigurovat VPN server v nabídce OpenVPN. V podnabídce Server Settings povolit běh serveru a nastaví se jeho parametry. V další podnabídce Client Registration se pomocí tlačítka Add přidávají oprávnění uživatelé. Každému přidanému uživateli se vygeneruje konfigurační soubor s certifikáty a klíči, který je potřeba oprávněným uživatelům bezpečně distribuovat, aby si mohli nastavit OpenVPN

klienta. Tlačítkem Revoke je možné odvolat platnost povolení pro kteréhokoli ze založených uživatelů.

3.2.1 Nastavení z pokročilého konfiguračního prostředí LuCI

Pro některá nastavení je nutné se přihlásit do pokročilé správy LuCI. Toto prostředí je velice podobné původnímu prostředí OpenWrt. Jedním z požadavků na implementaci bylo, že má být router Turris Omnia centrálním bodem pro přístup k internetu pro dvě domácnosti. Síť pro nájemníky však nemá mít přístup do sítě majitele nemovitosti. Toho lze dosáhnout konfigurací síťových rozhraní. Konfigurace je přístupná z nabídky Síť → Síťová rozhraní. Aby se dosáhlo oddělení sítí, je nutné vybrat jeden port RJ45, k tomu připojit oddělenou síť pro nájemníky a provést jeho konfiguraci. Na Obr. 28 se jedná o síťové rozhraní s názvem PRIZEMI.



Obr. 28 Nastavení síťového rozhraní „PRIZEMI“ *[Zdroj: vlastní]*

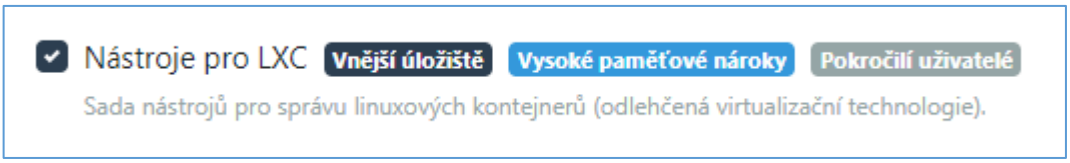
Detailně se nastaví, kam tato síť „vidí“, kdo k ní může přistupovat a kam mohou přistupovat zařízení z této sítě. Tuto nabídku lze také využít k hrubému přehledu o tom, které síťové rozhraní je nejvíce využíváno. U každého aktivního síťového rozhraní se zobrazují údaje o přenesených paketech, objemu přenesených dat a době běhu.

3.3 Instalace LXC serverů

Před zahájením instalace a provozování LXC kontejnerů musí být k routeru připojen externí disk a nakonfigurován jako úložiště. *„Běžné GNU/Linux distribuce nepočítají s provozem na zařízení jako je router a provádí velké množství zápisů na disk. Nepřiměřenými zápisy*

na interní eMMC flash disk dochází k jeho opotřebení a může tak dojít i k nenávratnému poškození zařízení" [11]. Připojení externího disku je popsáno v předešlé kapitole.

Pro spuštění všech LXC kontejnerů je zpočátku stejný postup, ten bude popsán jen jednou, specifická nastavení pro každý kontejner bude popsán v samostatné kapitole. Nejdříve je nutné v konfiguračním prostředí Reforis přidat balíček „Nástroje pro LXC" viz *Obr. 29*.

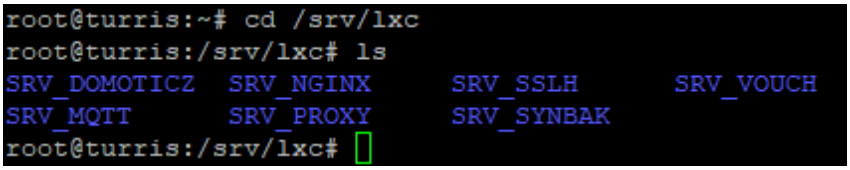


Obr. 29 Přidání balíčku v prostředí Reforis [Zdroj: vlastní]

Po instalaci balíčku je možné LXC kontejnery spravovat dvěma způsoby:

- Pokročilé administrační rozhraní LuCI - správa LXC kontejnerů je umístěna v nabídce LuCI → Nástroje → LXC Containers
- Příkazový řádek (CLI) – pro uživatele bez zkušeností s LINUX je používání příkazového řádku méně pohodlná. Přináší však oproti správě přes grafické prostředí výhodu sledování průběhu vytváření kontejnerů a detailní debugging v případě, že vytvoření selhalo.

Přihlášením přes SSH do administrace routeru se provedou následující kroky. Po nainstalování je nutné kontejnerům konfigurovat síťové rozhraní. Konfigurační soubory kontejnerů jsou uloženy v adresáři `/srv/lxc` viz *Obr. 30*.



Obr. 30 Umístění konfiguračních souborů LXC kontejnerů [Zdroj: vlastní]

V jednotlivých adresářích je vždy uložen soubor config, do kterého je třeba doplnit síťovou konfiguraci. Parametr `lxc.net.0.hwaddr =` je MAC adresa automaticky přidělená kontejneru při jeho vytváření, pod tento parametr je nutné přidat další dva parametry a doplnit hodnoty *Obr. 31*.

- `lxc.net.0.ipv4.address =` IP adresa ve formátu IPv4
- `lxc.net.0.ipv4.gateway=` IP adresa gateway

```
# Network configuration
lxc.net.0.type = veth
lxc.net.0.link = br-lan
lxc.net.0.flags = up
lxc.net.0.name = eth0
lxc.net.0.hwaddr = f2:48:ca:fd:1a:4a
lxc.net.0.ipv4.address = 192.168.0.75/24
lxc.net.0.ipv4.gateway = 192.168.0.20
```

Obr. 31 Síťová konfigurace LXC kontejneru [Zdroj: vlastní]

Takto vytvořený kontejner by se však nespustil po restartu routeru. Automatické spouštění kontejnerů při startu routeru se nastaví editací souboru `/etc/config/lxc-auto` *Obr. 32*.

```
config container
        option name SRV_MQTT
        option timeout 300
config container
        option name SRV_DOMOTICZ
        option timeout 400
config container
        option name SRV_SSLH
        option timeout 500
```

Obr. 32 Ukázka nastavení v souboru `lxc-auto` [Zdroj: vlastní]

Nastavení hodnoty timeout se osvědčilo využít pro první kontejner default hodnotu 300 a pro každý další kontejner hodnotu o 100 zvýšit. Tato hodnota je čas v sekundách, po který router při vypínání počká na korektní ukončení běžícího kontejneru.

Všechny testované kontejnery byly vytvořeny pro operační systém Ubuntu Focal, což byla v době testování nejaktuálnější verze Ubuntu distribuce ve verzi 20.04.1. Při využití jiných operačních systémů by se mohly příkazy lišit, proto je nutné nejdříve nastudovat dokumentaci pro každý operační systém. Další konfigurace se provádí přímo v kontejnerech, připojení ke kontejneru zajistí příkaz `lxc-attach -n nazev_kontejneru`. Pak se již pracuje v odděleném prostředí kontejneru. Prvním úkonem v nově vytvořeném kontejneru je nastavení dostatečně silného hesla spuštěním příkazu `passwd`. Dalším krokem je nastavení unikátní hodnoty hostname pro každý kontejner. Hostname slouží k identifikaci kontejneru v síti. Nastavení se provede editací původní hodnoty v souboru `/etc/hostname`.

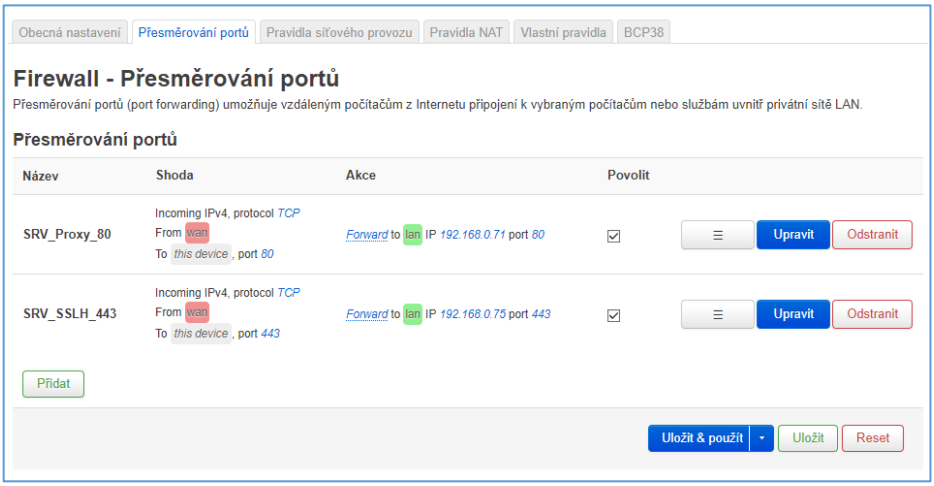
Je možné vytvořit `.ssh/authorized keys` potom se k serveru připojovat pomocí SSH klíče. Když je nastaveno, že má být vyžadován jak klíč, tak i heslo, zvyšuje se tím zabezpečení serverů. Nikdo se bez private klíče a znalosti hesla k serveru nepřihlásí. Tento postup

je třeba zopakovat pro každý kontejner, následuje popis nejdůležitějších nastavení jednotlivých LXC kontejnerů.

3.3.1 Kontejner Proxy

Provozování proxy serveru má mnoho využití a konfigurovat se musí podle toho, jaké jsou požadavky na funkce, které má plnit. Kromě zkušeností se změnami konfiguračních souborů v Linux, bude nutné editovat DNS záznamy v prostředí správce domény. Nastavení sice není složité, ale každý parametr má svoji syntax a chyba může znamenat nefunkční překlad adresy. Před změnou doménových záznamů je vhodné nastudovat, co který doménový záznam znamená. Celý postup je funkční pro tento konkrétní modelový případ.

Nejdříve je potřeba povolit přesměrování portů (port forwarding) v konfiguraci routeru. Tato volba je přístupná pouze v rozšířené administraci LuCI. Na *Obr. 33* jsou dva záznamy, které umožní komunikaci z internetu přímo na servery umístěné uvnitř lokální sítě.



Obr. 33 Port forwarding [Zdroj: vlastní]

Dalším krokem je nastavení DNS záznamů u správce domény. První podmínkou je, že od poskytovatele připojení k internetu máme v rámci zakoupené služby, přidělenou veřejnou IP adresu. Druhou podmínkou je registrace vlastní domény u některého správce domén. V tomto případě byly nastaveny „A“ záznamy na domény, které chceme směřovat na náš server. Veřejná IP adresa je 213.211.54.140 a zakoupená doména rodina-stanek.info. Na *Obr. 34* jsou dva A DNS záznamy.

Hostname	TTL	Typ	Hodnota	
rodina-stanek.info	1800	A	213.211.54.140	[Upravit | Smazat]
*.rodina-stanek.info	1800	A	213.211.54.140	[Upravit | Smazat]

Obr. 34 DNS záznamy [Zdroj: vlastní]

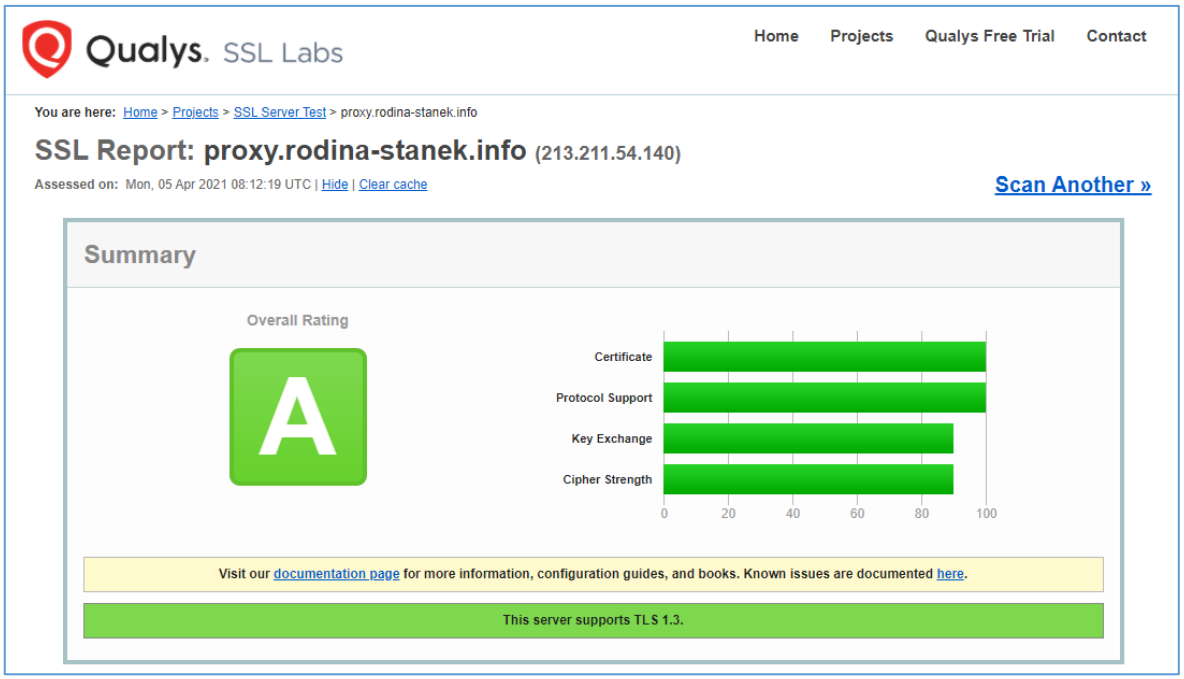
První přesměruje požadavky klientů na veřejnou IP adresu po zadání adresy

rodina-stanek.info, druhý záznam slouží pro zajištění přesměrování tzv. subdomén, v tomto případě např proxy.rodina-stanek.info

Pokud vše proběhlo správně, po zadání naší domény do adresního řádku webového prohlížeče, jsme přesměrováni na default stránku apache2 serveru. Než je možné spustit nějakou službu, která bude přenášet data od klientů a zpět, je nezbytné zajistit šifrovanou komunikaci pomocí certifikátu. Autor zvolil službu certifikační autority Let's Encrypt. Tato služba je poskytována zdarma s cílem odstranění poměrně složitého procesu manuální tvorby, ověřování, podepisování a instalace certifikátu. Snahou společnosti je celý proces zjednodušit, tím masově rozšířit šifrovanou komunikaci na internetu, což by mělo vést ke zvýšení úrovně kybernetické bezpečnosti. Zdarma jsou poskytovány doménově ověřené certifikáty typu X.509 pro šifrování protokolu TLS. Celý postup je velice detailně popsán zde:

https://www.digitalocean.com/community/tutorials/how-to-secure-apache-with-let-s-encrypt-on-ubuntu-18-04

Nemělo by tedy význam postup přepisovat do této práce. Kontrolu, zda vše proběhlo korektně a náš server je správně nakonfigurován, lze provést on-line nástrojem dostupným na adrese https://www.ssllabs.com/ssltest/



Obr. 35 Kontrola online nástrojem Qualys [Zdroj: vlastní]

Na *Obr. 35* je výstup analýzy domény **proxy.rodina-stanek.info**, která používá certifikát vydaný certifikační autoritou Let's Encrypt. Hodnocení A nedosahují na svých webech mnohé instituce z oblasti státní správy, bank nebo výrobních podniků.

3.3.1 Kontejner SSHL

Po vytvoření kontejneru SRV_SSHL je třeba se připojit k serveru přes terminál pomocí příkazu

```
lxc-attach SRV_SSLH
```

Pro instalaci stačí postupně zadat následující příkazy:

```
apt update
```

```
apt install sslh
```

Konfigurace sslh se provádí editací konfiguračního souboru umístěného v adresáři

```
/etc/default/sslh
```

V soboru se nastaví následující parametry:

```
RUN=yes
```

```
DAEMON=/usr/sbin/sslh
```

```
DAEMON_OPTS="--user sslh --listen 0.0.0.0:443 --ssh
192.168.x.x:22 --ssl 192.168.x.x:443 --http 192.168.x.x:80 --
openvpn 192.168.x.x:443 --anyprot 192.168.x.x:443 --pidfile
/var/run/sslh/sslh.pid"
```

Výše uvedené parametry je třeba blíže vysvětlit, aby si případný čtenář byl schopen konfiguraci přizpůsobit pro vlastní nastavení. Server SSLH má za úkol poslouchat příchozí komunikaci z internetu a tu pak správně přesměruje na servery uvnitř LAN sítě.

`--listen 0.0.0.0:443` - SSLH server poslouchá na portu 443

`--ssh 192.168.x.x:22` - SSH, které přijde na 443 je přesměrováno na ip:port

`--ssl 192.168.x.x:443` - SSL, které přijde na 443 je přesměrováno na ip:port

`--http 192.168.x.x:80` - HTTP, které přijde na 443 je přesměrováno na ip:port

`--openvpn 192.168.x.x:443` openVPN, které přijde na 443 je přesměrováno na ip:port

`--anyprot 192.168.x.x:443` libovolný jiný protokol, který přijde na 443 je přesměrován na ip:port

Server SSLH musí běžet nepřetržitě, proto je po konfiguraci nutné povolit spouštění service.

Následující příkazy spustí SSLH, povolí service a ověří, zda service běží:

```
systemctl start sslh
```

```
systemctl enable sslh
```

```
systemctl status sslh
```

Aby kontejner startoval i po restartu routeru, musí se nastavit automatické spuštění LXC containeru SRV_SSLH. To se provádí v terminálu na Omnie, kde se upraví následující soubor `/etc/config/lxc-auto`

Vysvětlení parametrů konfiguračního souboru bylo již vysvětleno v kapitole 3.3. Konfiguraci serveru SSHL autor doporučuje dát na první místo, aby se spouštěl jako první.

Posledním krokem je nastavení port forwardingu v konfiguraci Omnie. Toto nastavení bylo popsáno v kapitole 3.3.1, pro SSHL nastavíme libovolný hostitel 443 TCP na WAN přesměrovat na IP_SRV_SSLH:443.

3.3.1 Kontejner Vouch

Po vytvoření kontejneru SRV_VOUCH se připojíme k serveru přes terminál pomocí příkazu

```
lxc-attach SRV_VOUCH
```

Prvním krokem bude stažení zdrojových kódů VOUCH proxy příkazem:

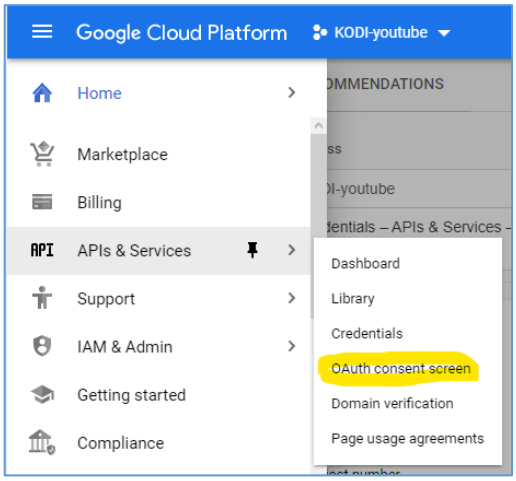
```
wget --output-document=vouch.zip
https://github.com/vouch/vouch-proxy/archive/master.zip
```

Instalační soubory se nejdříve musí rozbalit a pak provést samotnou instalaci. Postup je popsán na stránkách GitHub projektu [22].

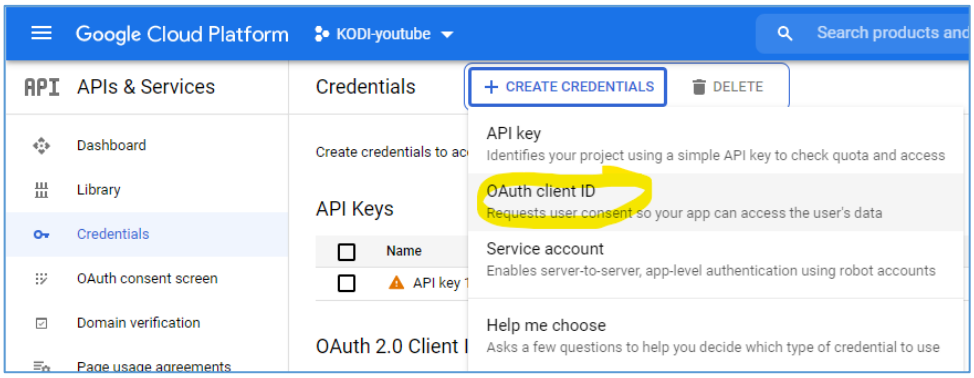
Další poměrně rozsáhlou částí konfigurace bude nastavení API pro ověřování identity. Autor se rozhodl využít ověřovací autoritu Google. Pro úspěšné ověření musí mít oprávnění uživatelé účet u Google. Správa „Google Cloud Platform“ je přístupná na adrese:

https://console.cloud.google.com/apis/credentials

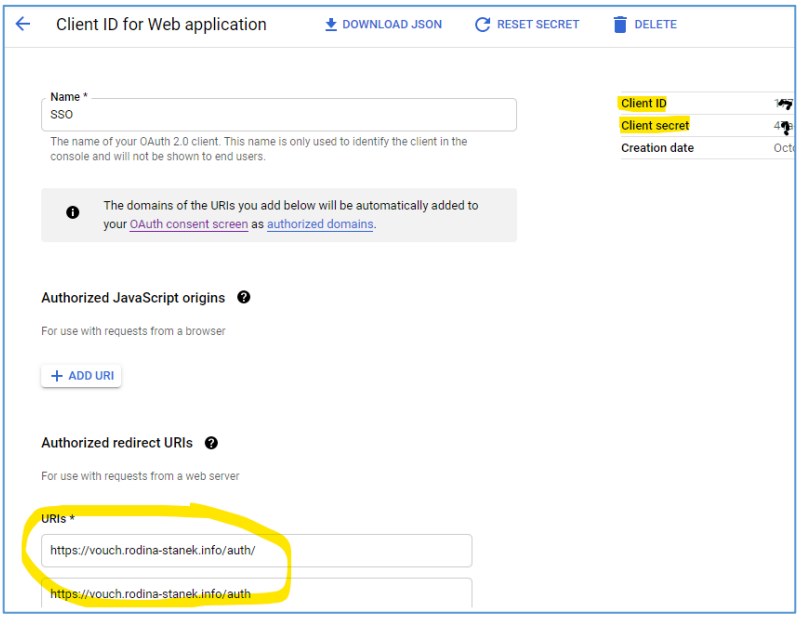
Z nabídky vybereme APIs & Services → 0Auth constent screen viz *Obr. 36*.



Obr. 36 Nabídka Google Cloud Platform [Zdroj: vlastní]



Obr. 37 Vytvoření nového 0Auth client ID [Zdroj: vlastní]



Obr. 38 Konfigurace pověření pro jednotné přihlašování [Zdroj: vlastní]

Vytvoření nového pověření (Credencial) pro Vouch server je na *Obr. 37*. Na *Obr. 38* jsou označeny pole pro vyplnění URL adresy Vouch serveru dvou zásadních hodnot Client ID, Client secret. Tyto dva kódy jsou unikátní pro každé pověření a jsou citlivým údajem, který nesmí být zveřejněn, aby je někdo nemohl zneužít.

V této fázi konfigurace je třeba se vrátit ke konfiguraci Vouch serveru. Přes terminál je třeba editovat konfigurační soubor config.yml uložený v adresáři /opt/vouch-proxy/config/config.yml.

Konfigurační soubor je formou komentářů velice podrobně vysvětlen, proto zde budou uvedeny jen parametry, které byly použity pro popisované nastavení a bez nich by nebylo

ověřování identity funkční. Řádky, které začínají znakem # jsou komentáře, ty nejsou při běhu programů zpracovávány.

```
testing: false
listen: 0.0.0.0
port: 9090
domains:
     - gmail.com
     - rodina-stanek.info

whiteList:
     - adresa1@gmail.com
     - adresa2@gmail.com
```

`secret:` kód vygenerovaný v Google API

```
issuer: Vouch
test_url: https://vouch.rodina-stanek.info
oauth:
provider: google
```

`client_id:` kód vygenerovaný v Google API

client_secret: kód vygenerovaný v Google API

```
callback_urls:
- https://vouch.rodina-stanek.info/auth
preferredDomain: gmail.com
```

Předpoklad pro plnou funkčnost SSO je instalace SRV_NGINX, který bude přesměrovávat na Vouch proxy.

3.3.2 Kontejner MQTT

Instalace broukeru je velice jednoduchá, po vytvoření kontejneru SRV_MQTT se aktualizují instalační balíčky příkazem:

```
apt update
```

Poté se spustí instalace příkazem:

```
apt install mosquitto
```

Po dokončení instalace lze ověřit, zda běží MQTT broker příkazem:

```
netstat -antup|grep mosquitto
```

Na *Obr. 39* je výpis příkazu, program mosquitto, ten poslouchá na portu 1883 a komunikovat s ním může jakákoli IP adresa.

```
root@turris:~# lxc-attach SRV_MQTT
root@MQTT:~# netstat -antup|grep mosquitto
tcp        0      0 0.0.0.0:1883            0.0.0.0:*               LISTEN      63/mosquitto
```

Obr. 39. Program mosquitto poslouchá na portu 1883 [Zdroj: vlastní]

Dalším krokem je zabezpečení MQTT brokeru heslem. K tomu je třeba uložit konfigurační soubor default.conf do adresáře:

```
/etc/mosquitto/conf.d/default.conf
```

Do konfiguračního souboru je třeba uložit následující parametry:

```
allow_anonymous false
```

```
password_file /etc/mosquitto/passwd
```

Posledním krokem je tvorba klientských účtů pro MQTT. Každý klient by měl mít svůj vlastní účet. Klienty jsou všechna zařízení, které mají s brokerem komunikovat, například zásuvka Sonnoff, Domoticz server, nebo homebridge server. Pro prvního uživatele zadáme následující příkaz.

```
mosquitto_passwd -c /etc/mosquitto/passwd username
```

Pro každého následujícího uživatele je třeba změnit parametr -c za -d. Následně jsme vyzváni k zadání hesla uživatele username. Hesla je vhodné ukládat do správce hesel. Posledním krokem konfigurace je povolení service a restart brokeru, to zajistí následující příkazy:

```
systemctl enable mosquitto
```

```
systemctl restart mosquitto
```

Pro provoz brokeru je to vše, další nastavení se provádí v serveru Domoticz a přímo v zařízení Sonoff. Pouze v případě, že by bylo potřeba doplnit další zařízení, bylo by nutné znovu konfigurovat broker.

3.3.1 Kontejner Domoticz

Instalace tohoto kontejneru je popsána v kapitole 4.2 včetně popisu a postupu konfigurace s vazbou na domácí automatizaci.

4 ZÁKLAD DOMÁCÍ AUTOMATIZACE

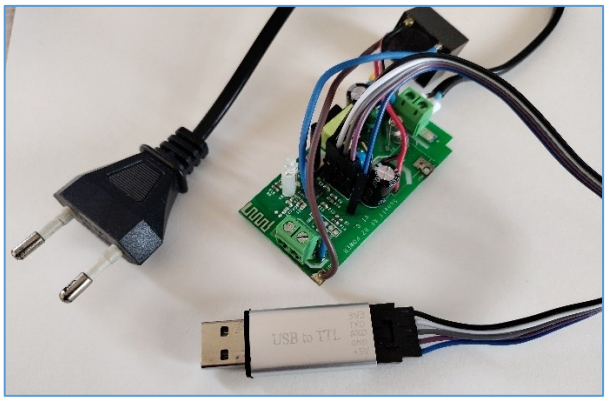
V této kapitole budou popsány požadavky na automatizaci a konkrétní způsob, jak byly vyřešeny. Účelem nebylo vytvářet nepotřebné scénáře pro demonstraci všech možností, ale vyřešit požadavky obyvatel domu tak, aby byly činnosti automatizované a spolehlivě fungovaly. Na těchto 3 jednoduchých příkladech se však dá demonstrovat potenciál zvolené technologie.

- Požadavek číslo 1 – řízení nočního vypínání ohřevu vody a záznam spotřeby elektrické energie.
- Požadavek číslo 2 – řízení vytápění a osvětlení terária.
- Požadavek číslo 3 – rozpojení obvodu termostatu v případě, že je otevřeno okno.

4.1 Příprava HW spínačů

Spínače Sonoff jsou dodávány s firmware výrobce, který umožňuje jejich ovládání pomocí mobilní aplikace eWeLink, ta je dostupná zdarma v Google Play pro Android nebo v Apple Store pro iOS. Z důvodu zvýšení bezpečnosti se autor práce rozhodl nahradit původní firmware alternativou Tasmota. Bezpečnostním přínosem je plná kontrola nad tím, kam spínače komunikují. Komunikace je vedena pouze v interní síti. Přínosem je větší svoboda v možnostech ovládání, ale hlavně nezávislost na cloudu. Po změně firmware není možné ovládat spínače z původní aplikace eWeLink. Pro níže popsané činnosti jsou nutnými předpoklady znalost práce s elektrickými zařízeními a dovednost pájení elektrických obvodů. Postup bude popsán pouze na spínači Sonoff Basic, protože pro další dvě zařízení se v postupu nic nemění, jen rozmístění součástek na destičce plošného spoje je rozdílné.

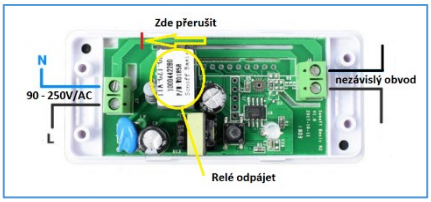
Prvním krokem je demontáž krytu spínače, který se musí provádět **zásadně bez připojeného napájení!** Na plošném spoji jsou neosazené 4 otvory s označením 3V3, RX, TX a GND. Otvory mají standardizovanou rozteč pro PIN header. Na *Obr. 40* je již připájený header k destičce Basic, zatímco na *Obr. 41* je destička RF Bridge s vyznačením místa pro připájení headeru.



Obr. 40 Úprava Sonof Basic – připájený header, na něj připojené UART a výměna spínacího relé pro spínání odděleného obvodu [Zdroj: vlastní]

Obr. 41 Sonoff RF Bridge před pájením headeru [Zdroj: vlastní]

Jeden ze spínačů Sonoff Basic byl hardwarově upraven tak, aby mohl být napájen ze sítě AC 230V, ale na výstupu mohl spínat/rozpínat obvod termostatu. Úprava spočívala v přepájení relé a v přerušení obvodu spínače viz *Obr. 42*. Zásah je to minimální, jen je třeba zajistit izolaci živých částí obvodů. Toho bylo dosaženo přetažením smršťovací izolace na pájené kontakty a následné vlepení relé do krabičky s vymezením proti pohybu nevodivou pěnovkou.



Obr. 42 Úprava modulu basic pro spínání nezávislého obvodu [Zdroj: vlastní]

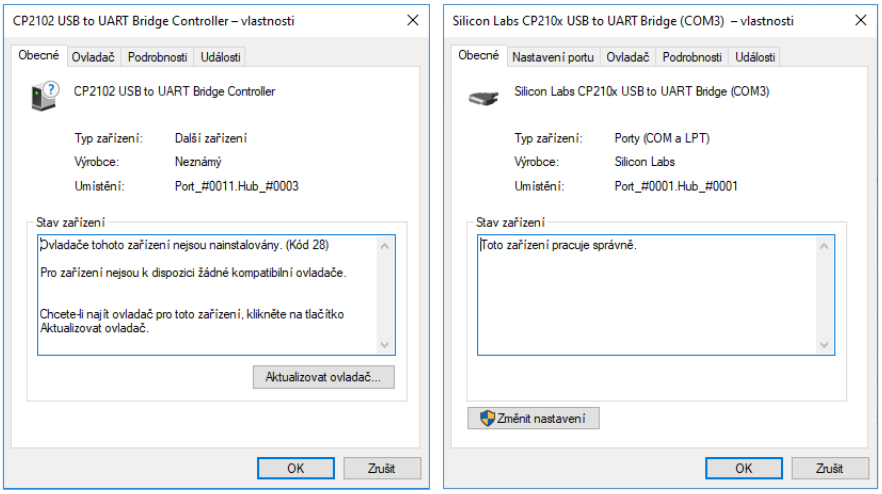
Po připájení headeru je možné připojit UART bridge. Jedná se o převodník, zprostředkovávající komunikaci mezi PC (USB) a čipem ESP8266 (UART). Ke komunikaci se využijí konektory RXD, TXD, GND a 3V3. Komunikace probíhá podle specifikace sériového

přenosu dat, standardu RS-232. Při propojení počítače a destičky basic jde o propojení dvou počítačů, kdy se používá tzv. křížený kabel. Je tedy nutné prohodit vodiče vstupů a výstupů (Rx a Tx).

Tabulka 3. Propojení UART a Sonoff Basic

UART CP 2102	**Sonoff basic**
GND (zem)	GND
RXD (Receive Data)	TX
TXD (Transmit Data)	RX
3V3 (napájení 3,3 V)	3V3

Změna firmware byla prováděna pomocí počítače s OS Windows 10, kde bylo potřeba doinstalovat ovladače pro UART. Po připojení UART do USB portu PC se ve Správě počítače → Správce zařízení objevila mezi porty položka s chybějícími ovladači viz *Obr. 43*.



Obr. 43. Zobrazení vlastností před a po instalaci ovladače [Zdroj: vlastní]

Ovladač je nutné nejdříve stáhnout, nejlépe z webových stránek výrobce čipu firmy Silikon Labs https://www.silabs.com. Po korektní instalaci ovladače se objeví v poli Stav zařízení oznámení „Toto zařízení pracuje správně“. Důležitá je také informace, jaký sériový port počítač pro UART přidělil. V tomto případě to je COM3.

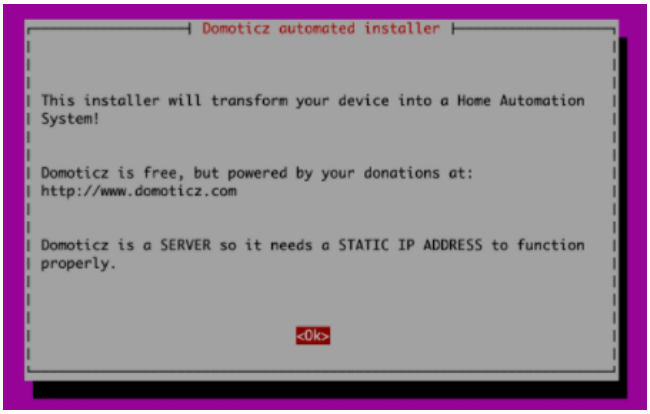
Nejdříve z GitHub repozitáře stáhneme a uložíme aktuální verzi SW Tasmota, https://github.com/arendst/Tasmota. Výběr software pro upload firmware a komunikaci se zařízeními Sonoff je poměrně široký, autor zvolil Python 3.7. Kompletní postup

flashování spínačů by byl nadbytečný, postupy jsou popsány například v GitHub repozitáři Tasmota. Pro méně zkušené uživatele se nabízí další možnost, tou je využití nákupu spínačů s již nainstalovaným software Tasmota. Takto upravené spínače nabízí například e-shop https://www.chytrevypinace.cz.

4.2 Konfigurace serveru Domoticz

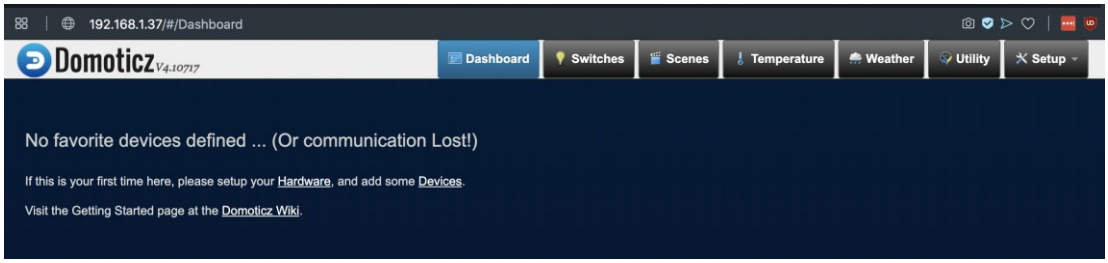
Řízení automatizace zajišťuje server Domoticz (SRV_DOMOTICZ), pro ovládání spínačů a sběr stavových hodnot je nezbytný centrální bod – broker server MQTT (SRV_MQTT). Po instalaci kontejneru SRV_DOMOTICZ se instalace serveru provede pomocí příkazu `curl -sSL install.domoticz.com | sudo bash`.

Po stažení instalačního balíčku se spustí průvodce instalací viz *Obr. 44*.



Obr. 44 Instalační průvodce Domoticz [Zdroj: vlastní]

Instalace je dobře komentována a není s ní žádný problém. Po úspěšném ukončení instalace je třeba server Domoticz nakonfigurovat. Přes webový prohlížeč je přístupná konfigurace po zadání IP adresy serveru viz *Obr. 45*.



Obr. 45 Úvodní konfigurační stránka nově nainstalovaného serveru Domoticz [Zdroj: vlastní]

Detailní popis všech nastavení by byl nadbytečný, na stránkách https://www.domoticz.com/wiki/Main_Page je velmi detailní dokumentace, navíc velmi dobře funguje

podpora komunity. Stačí prohledat dotazy ostatních uživatelů, na které někdo odpověděl, případně položit vlastní dotaz. Velmi rozsáhlá nabídka nastavení je přístupná přes volbu

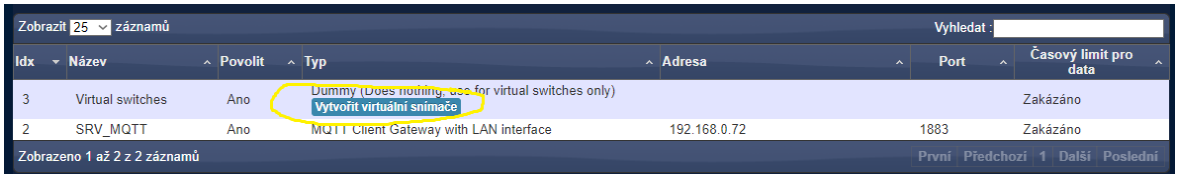
Nastanení → Nastavení. Tady by se hodilo ještě zapracovat na logice ovládání a popisu. Na druhou stranu je to o zvyku. V nastavení se zobrazí následující karty, kde každá z nich umožní velmi detailní nastavení daných oblastí.

- Systém – nastavení jazyka, přístup k webovému rozhraní, místní sítě,..
- Historie protokolu – délka historie protokolů
- Oznámení – možnost konfigurace jak má Domotic posílat oznámení (např SMS)
- E-mail – konfigurace e-mailových oznámení
- Měřidla/Počítadla – výběr jednotek pro měřidla, nastavení ceny energií,..
- Půdorysy – konfigurace, jak má Domoticz zobrazovat půdorysy
- Ostatní – různá nastavení časových limitů, parametrů Raspberry Pi kamer,…
- Zálohovat/Obnovit – umožní provést zálohu a obnovu databáze

Všechna tato nastavení jsou detailně dokumentována. Jedná se o přizpůsobení systému dle preferencí každého uživatele. Na funkčnost systému jako takového nemají vliv, proto zde nebudou popsány detaily těchto nastavení. Zásadní konfigurace se nachází pod nabídkou viz *Obr. 46* Nastavení → Hardware označeno ① a Nastavení → Zařízení označeno ②

Obr. 46 Nabídka nastavení [Zdroj: vlastní]

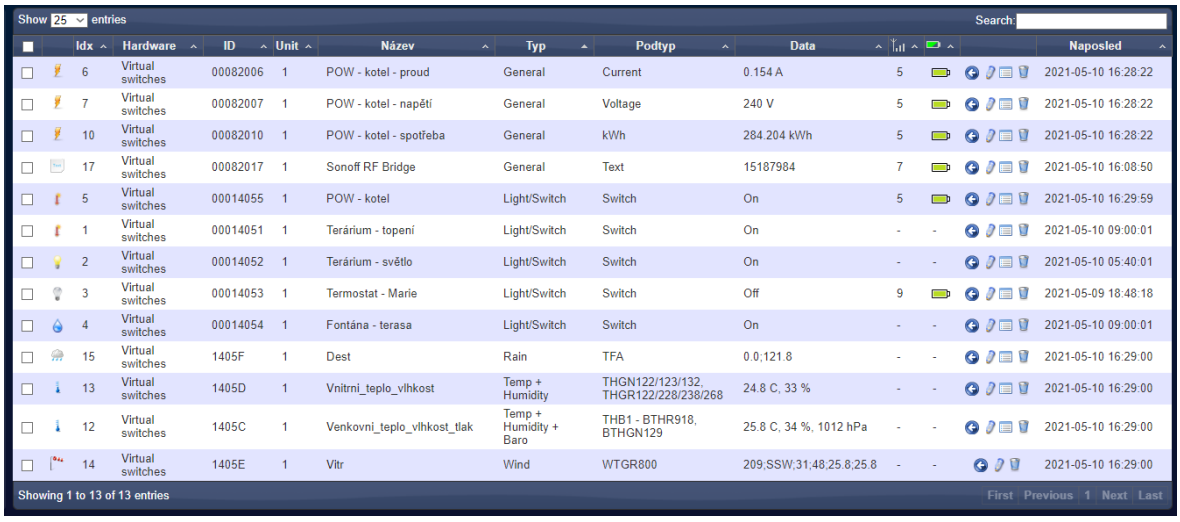
Nastavení → Hardware → Přidat se musí přidat dvě zařízení. Prvním je MQTT server, který byl vytvořen v kapitole **Chyba! Nenalezen zdroj odkazů.**. Stačí pak zadat IP adresu MQTT b rokeru a port, na kterém komunikuje. Druhým zařízením jsou Virtuální switche. Do políčka Typ se vybere „Dummy (Does nothing, use for virtual switches only)“. Pomocí tlačítka „Vytvořit virtuální spínače“, tlačítko je zvýrazněno na *Obr. 47*



Obr. 47 Seznam HW zařízení v serveru Domoticz a tlačítko pro vytváření virtuálních spínačů [Zdroj: vlastní]

Postupně se přidají všechna zařízení, která chceme ze serveru Domotic ovládat, nebo vyčítat jejich stavové hodnoty. Logika je taková, že například Sonoff POW má čtyři samostatná zařízení: spínač, měření proudu, napětí a spotřeby. Každé z těchto zařízení pak předává hodnoty zvlášť. Trochu zvláštní je v tomto Sonoff RF Bridge, který se připojuje jako zařízení typu General, podtyp TEXT. Toto bude dále podrobněji popsáno.

Přehled všech nainstalovaných virtuálních spínačů lze zobrazit v nabídce Nastavení → Zařízení na *Obr. 46* označeno ②. Na následujícím *Obr. 48* je výpis všech nainstalovaných virtuálních spínačů.



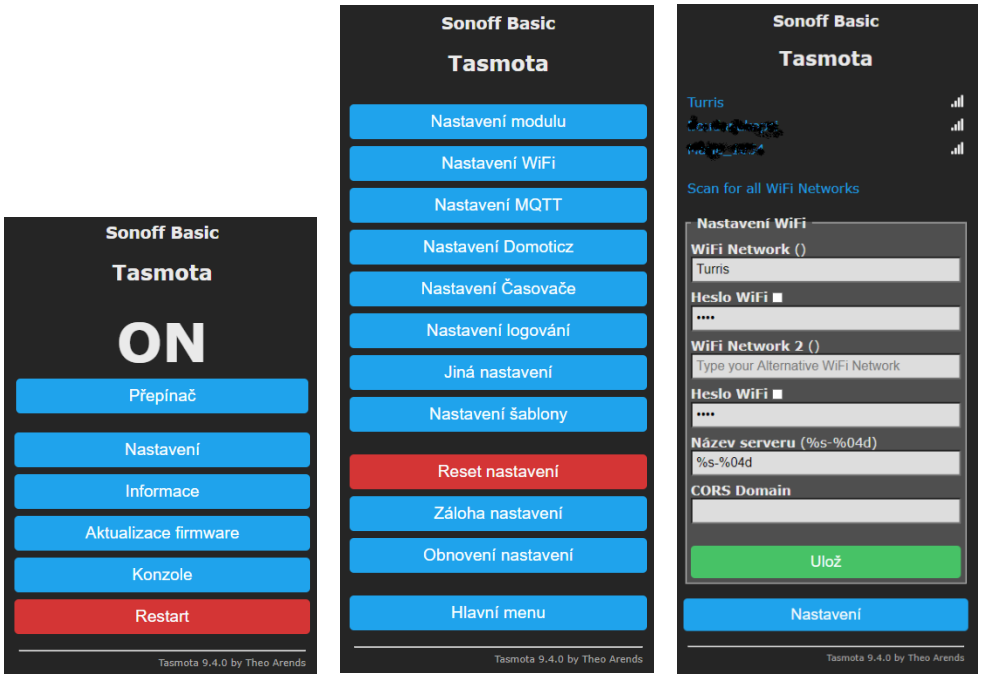
Obr. 48 Seznam virtuálních spínačů [Zdroj: vlastní]

Pro další konfiguraci je důležitá hodnota Idx, jejíž hodnoty jsou zobrazeny ve třetím sloupci *Obr. 48*. Hodnota Idx je identifikátorem pro komunikaci se spínači a čidly.

4.3 Napojení modulů Sonnof

Předpokladem je mít v modulu Sonnof flashnutý firmware Tasmota, zprovozněný broker a server Domoticz. Při prvním spuštění se modul zapne s aktivním WiFi Managerem, který vysílá WiFi síť s názvem sonoff-1560.

Připojíme se tedy nejprve na WiFi Sonoffu a ve webovém prohlížeči načteme konfiguraci modulu viz *Obr. 49*, kde v nabídce Nastavení → Nastavení WiFi vybereme WiFi síť, do které má být modul připojen. Po uložení nastavení dojde k restartu modulu, ten již nevysílá svoji WiFi síť, ale je připojen k routeru Turris. V nastavení routeru je nutné přejít do LuCI a nastavit statickou zápůjčku pro přiřazení fixních IP adres a symbolických jmen DHCP klientů. Nastavení je dostupné v nabídce Síť → DHCP a DNS → Statické zápůjčky. Použitím tlačítka Přidat se přidá nová zápůjčka. MAC adresa identifikuje zařízení, IPv4 adresa určuje, jaká pevná adresa bude použita z rozsahu sítě. Hostname je přiřazeno jako symbolické jméno. Volitelná doba výpůjčky (lease time) lze použít k nastavení nestandardní doby zapůjčení specifické pro hostitele, například 12h, 3d nebo infinite (nekonečná). Při restartu zařízení nebo routeru bude mít spínač vždy stejnou IP adresu. Bez tohoto nastavení by bylo nutné jednotlivé spínače v síti hledat.



Obr. 49 Konfigurace ve webovém rozhraní [Zdroj: vlastní]

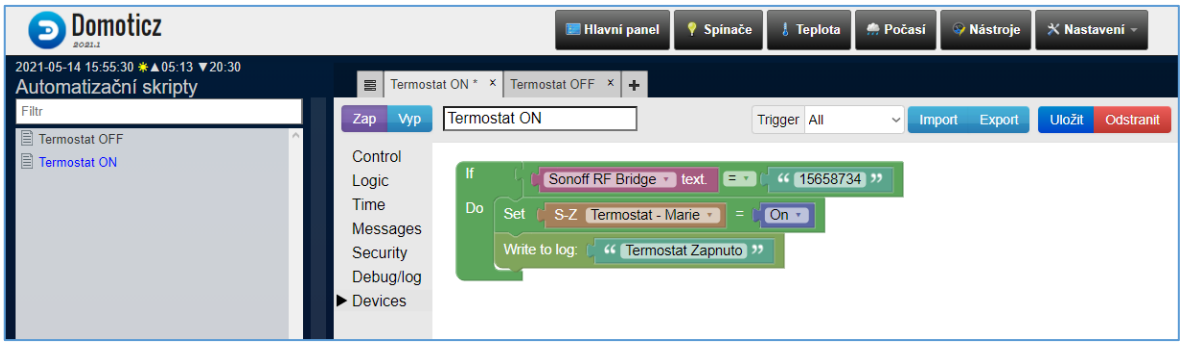
Nastavení → Nastavení MQTT vyplníme Server (adresa MQTT), Port (1883), Uživatel a Heslo. Obdobně se musí vyplnit údaje v nabídce Nastavení → Domoticz, kde se vyplňují hodnoty Idx z konfigurace virtuálních serverů viz kapitola 4.2.

Po napojení modulů Sonoff je možné programovat jejich spínání. Spínání se dá programovat třemi různými způsoby.

1) Časovač přímo v modulu Sonof. K nabídce časovače se dostaneme z webového rozhraní Sonof viz *Obr. 49*, nabídka Nastavení → Nastavení Časovače. V nabídce je 16 hodnot zapnutí/vypnutí podle nastaveného času nebo podle času svítání a soumraku. Změnu je možné provést jednou nebo opakovaně, a také pouze ve vybraných dnech v týdnu.
2) Druhou volbou je nastavit časovače z prostředí Domoticz. Výhodou tohoto nastavení je neomezený počet nastavení, dny je možné vybrat z kategorií „Každý den“, „Pracovní dny“, „Víkendy“ a „Vybrané dny“. Toto nastavení je přístupné z prostředí Domoticz z nabídky Spínače → Časovače. Tímto způsobem byly nakonfigurovány dva moduly Basic pro spínání osvětlení terária a spínání topení do terária. Modul POW byl konfigurován s rozdílným nastavením spínání ve všední dny a o víkendu.
3) Poslední volbou je nastavení závislého ovládání pomocí událostí. Toto nastavení je přístupné z prostředí Domoticz z nabídky Nastavení → Další možnosti → Události. Zde jsou další možnosti, jak konfigurovat události. Pro zjednodušení bude popsán pouze způsob, který zvolil autor. Tou volbou je systém grafického programování Blockly.

4.3.1 Programování událostí v Blockly

Úkolem pro tento algoritmus je ovládat upravený spínač Sonoff, který je vložen do okruhu termostatu. Pokud teplota okolí klesne pod hodnotu nastavenou v termostatu, termostat sepne a tím pošle signál kotli, aby začal topit. Díky chybně zvolenému umístění termostatu v blízkosti okna je ovlivňován prouděním chladného vzduchu otevřeným oknem. To mělo za následek přetápění a zbytečnému plýtvání energií. Logika algoritmu musí zajistit, že se signál od termostatu dostane ke kotli pouze tehdy, když je okno zavřené. Pro detekci otevřeného okna na něj byl nainstalován magnetický RF detektor PB-68. Zvláštností RF čidel je, že se serverem Domoticz komunikují přes FR Bridge pomocí textových kódů. Po spárování každého RF čidla je nutné „odchytat“ textové zprávy, které čidlo odešle do RF Bridge. Zprávy jsou ve tvaru číselného kódu a jsou pro každé čidlo i stav unikátní. To umožní vytvoření algoritmu viz *Obr. 50*.



Obr. 50 Automatizační skripty programované pomocí grafického prostředí Blockly

Prostředí Blockly je po troše praxe velmi jednoduše použitelné i pro uživatele bez znalostí programování. Stačí vybrat z nabídky správné bloky a ty poskládat do požadované funkce. Tvary bloků do sebe zapadají jako dílky puzzle, což pomůže při správném skládání bloků. Pokud do sebe dílky „nezapadnou“ znamená to, že je potřeba použít jiné bloky (příkazy). Pro požadovanou funkcionalitu byly naprogramovány dva skripty, jeden pro vypnutí a druhý pro zapnutí.

4.4 Naplnění požadovaných funkcí automatizace

V úvodu kapitoly 4 byly definovány tři požadavky, které má systém plnit.

- Požadavek číslo 1 – řízení nočního vypínání ohřevu vody a záznam spotřeby elektrické energie. Tento požadavek byl naplněn pomocí modulu Sonoff POW a naprogramovaného časovače. Kotel se v nastavenou dobu vypne a opět zapne. Efektem je úspora energie na dotápění TUV v době, kdy ji nikdo nepotřebuje.

- Požadavek číslo 2 – řízení vytápění a osvětlení terária. Tento požadavek byl naplněn pomocí dvou modulů Sonof Basic. Aby bylo prostředí v teráriu pro plaza, pokud možno co nejpřirozenější, měly by se střídat během dne teploty (den/noc). K ohřevu je používán topný kámen a k osvětlení LED žárovka. Spínače byly naprogramovány rozdílně, spínač pro osvětlení zapíná s rozbřeskem a se soumrakem se vypíná. Druhý spínač byl nejdříve naprogramován na konkrétní čas zapnutí/vypnutí. To by v letním období mohlo způsobovat přehřívání, proto byl vytvořen algoritmus, který přidává podmínku pro sepnutí v závislosti na teplotě v pokoji. Teplota je snímána meteostanicí a hodnoty předávány do serveru Domoticz.

- Požadavek číslo 3 – rozpojení obvodu termostatu v případě, že je otevřeno okno. Naplnění tohoto požadavku bylo nejsložitější, protože bylo potřeba nejdříve upravit HW spínače, pak spínané kontakty relé zapojit do okruhu termostatu a nakonec do Domoticz

dostat informaci o tom, jestli je okno zavřené nebo otevřené. Pro domácnost mělo vyřešení tohoto požadavku asi největší přínos. Nedochází už k přetápění a šetří se energie.

4.5 Shrnutí

Celý proces trval velice dlouho, některé pokusy končily ve slepých uličkách, jiné byly naopak snadné. Autor čerpal z nejrůznějších diskusních fór z komunit vývojářů a nadšenců kolem IoT, Linux a samozřejmě také kolem Turris. Takový postup rozhodně není pro každého. Předpokladem je především schopnost čerpat ze zdrojů psaných v angličtině, důležité jsou znalosti z prostředí Linux systémů a v neposlední řadě znalosti z oblasti počítačových sítí a IoT. Testování nových možností a funkcionalit několikrát způsobilo nefunkčnost jiných dílčích funkcionalit. Následné hledání chyb a hlavně jejich odstraňování však bylo zdrojem poznání. Autora to velmi silně motivovalo k dalšímu studiu a prohlubování znalostí.

Práce s komponentami Sonoff byla příjemná, ve spojení se serverem Domoticz je možné modulárně připojovat další zařízení. Autor plánuje další rozšíření systému o snímače teploty a vlhkosti. Výsledkem bude kompletní přepracování řízení vytápění v celém domě. Produktová řada Sonoff obsahuje také dotykové vypínače, vypínače pro instalaci na DIN lišty v rozváděčích nebo miniaturní vypínače, které se instalují pod stávající vypínače světel. Systém lze doplnit například o pohybová PIR čidla a automaticky spínat světla nebo třeba odsávání na WC. O takřka neomezené modulárnosti svědčí také možnost spojení z dalšími platformami. Takovým zařízením je například meteostanice, která je napojena na jednodeskový počítač Raspberry Pi s nainstalovaným OS Raspbian a spuštěnou aplikací weewx. Hodnoty z meteostanice jsou posílány do serveru Domoticz, kde je možné je sledovat včetně historie, ale také je použít jako „spouštěč“ pro automatizační prvky.

Při psaní závěru autor narazil na titulek článku: „Na každý router Turris míří denně více než devět tisíc útoků“ [36]. Pod článkem se „strhla“ diskuse o tom, jestli to jsou reálná čísla nebo jestli jde pouze o marketingové strašení na podporu prodeje drahých Turrisů. Co si představit pod pojmem útok na router Turris? Jakékoli zařízení, které má přidělenou veřejnou IP adresu a je viditelné ze sítě internet, se stává terčem pro automatizované skeny internetových botů. Bez jejich práce by nebylo vyhledávání na internetu tak efektivní, protože sbírají informace o publikovaných stránkách, ty se pak indexují a zefektivňují vyhledávací dotazy. Jiné typy botů mají rozdílné zadání, jejich úkolem je vyhledávání zařízení. Do této skupiny patří automatizované skeny projektu Shodan https://www.shodan.io, který neúnavně prohledává internet a snaží se najít nezabezpečená zařízení. Zjistí otevřené TCP porty, pokusí se navázat

spojení, odpověď otaguje, a všechno uloží do databáze. V databázi projektu jsou servery, routery, kamery, IoT zařízení. Dokonce byla objevena nezabezpečená rozhraní pro ovládání solárních elektráren. To, co dělá Shodan s čistými úmysly, může dělat kdokoli jiný. Pokud je autorem bota jedinec nebo skupina lidí, která se snaží na špatně zabezpečených zařízeních získat finanční prospěch, mohou být důsledky skenování fatální. Trend počtu kybernetických útoků a jejich následky mají vzrůstající tendenci. Větší důraz na zabezpečení počítačových systémů by proto měl být prioritou nejen v organizacích, ale také v domácnostech.

4.6 Finanční náklady

Pro rozhodnutí, zda vybrat výše popsané řešení, je třeba zohlednit také finanční stránku. Náklady na pořízení jednotlivých komponent dosáhly výše 9 tisíc korun. Soupis všech komponent s uvedenými cenami viz Tabulka 4.

Tabulka 4. Náklady na pořízení použitých komponent

Název komponenty	**Počet ks**	**Cena za Kus**
Router Turris Omnia 2GB	1	7.000,-
UART	1	45,-
Sonoff Basic	3	150,-
Sonoff POW	1	300,-
Sonoff RF bridge	1	150,-
Magnetické čidlo PB-68	1	60,-
Externí box	1	200,-
HDD 2,5“ 500GB	1	1.100,-
Cena celkem		**9.005,-**

Nejdražší položkou rozpočtu je router Turris Omnia. Router se stejnými vlastnostmi na trhu neexistuje, na druhou stranu je možné pořídit SOHO router s možností instalace OpenWRT v ceně kolem 2 tisíc korun. Pro běh serverů by se dal využít jednodeskový počítač Raspberry Pi, ten však včetně napájení a krabičky v konfiguraci se 4 GB RAM stojí 3 tis. Kč. To už se cenový rozdíl nezdá tak velký.

Pokud by se někdo rozhodnul jít cestou specializovaného HW pro domácí automatizaci, pak je jednou z možností řešení od firmy Loxone. Tady je však nutné počítat s podstatně vyšší cenou. Miniserver - centrální jednotka pro řízení inteligentní elektroinstalace v domácnostech, firmách či pro speciální projekty automatizace stojí 13,5 tis. korun. K tomu je zapotřebí připočíst další náklady na moduly a nejspíš také na odbornou montáž. Cena instalace podobného systému, který je popisován v této práci by mohla dosáhnout cca 50 tis. korun.

ZÁVĚR

Cílem diplomové práce bylo navrhnout konfiguraci routeru Turris Omnia pro využití v domácnosti nebo malé firmě. Po analýze možností výkonného hardware routeru byly vybrány vhodné programy pro doplnění funkcí routeru. Prioritou byla bezpečnost sítě a všech zařízení připojených v této síti. Router je zařízení, které je provozováno v nepřetržitém režimu 24/7. Tohoto provozního režimu bylo využito pro kombinaci funkcí routeru a systémů nezbytných pro provoz domácí automatizace.

V úvodu teoretické části práce byly popsány možnosti routeru Turris Omnia. Unikátní přístup výrobce k neustálému vývoji, rychlé distribuci aktualizací a funkcím, jako například adaptivní firewal, honey pot a blokování reklam, posouvají tento SOHO router spíše do vyšší kategorie. Dále byly popsány testované programy. Jejich výběr měl doplnit funkce od výrobce o další, které ještě zvýší použitelnost celého systému. Využití tzv. „light-weight“ virtualizace potvrdilo vhodnost této technologie pro provozování virtuálního serveru domácí automatizace.

V praktické části jsou popsány nejdůležitější kroky pro prvotní instalaci routeru, dále pak detailní postupy pro zprovoznění SW a HW domácí automatizace. Systém byl nasazen v reálné domácnosti, kde vyřešil tři jednoduché požadavky na automatizaci. Efektem bylo nejen větší pohodlí obyvatel, ale také úspora energií.

Díky principům popsaným v této práci je možné postavit jakoukoli vlastní realizaci a tu přizpůsobit podle požadavků a představ realizátora. Díky rozsahu testovaných řešení může být tato práce jakýmsi zásobníkem nápadů.

Spojení routeru Turris Omnia a serveru Domoticz se osvědčilo. Realizace ukázala velký potenciál pro další rozšiřování systému. Asi největší slabinou projektu je šíře záběru. Pro realizaci jsou nezbytnou podmínkou znalosti z více oblastí IT a IoT. Nelze tedy předpokládat, že by se o podobnou realizaci mohl pokusit běžný uživatel.

SEZNAM POUŽITÉ LITERATURY

[1.] Informační společnost v číslech - 2020. *Český statistický úřad.* [Online] 24. 03 2020. [Citace: 17. 02 2021.] https://www.czso.cz/csu/czso/informacni-spolecnost-v-cislech-2020.

[2.] Schön, Otakar. *Hospodářské noviny iHNed.cz* . [Online] [Citace: 09. 11 2016.] https://tech.ihned.cz/testy/c1-65513350-test-turris-omnia-je-fantasticky-router-ktery-ztraci-na-konkurenci-v-rychlosti-i-pohodli.

[3.] Gála, Libor, Pour, Jan a Šedivá, Zuzana. *Podniková informatika: Počítačové aplikace v podnikové a mezipodnikové praxi.* Praha : Grada Publishing a.s., 2015. ISBN 978-80-247-9918-6.

[4.] O sdružení. *CZ.NIC.* [Online] CZ.NIC, z. s. p. o. [Citace: 22. 12 2020.] https://www.nic.cz/page/351/.

[5.] O sběru dat. *Wikipedie projektu Tutrris.* [Online] CZ.NIC, z. s. p. o. [Citace: 20. 12 2020.] https://wiki.turris.cz/doc/cs/howto/collect.

[6.] MOX. *Turris.* [Online] CZ.NIC, o.p.s. [Citace: 12. 04 2021.] https://www.turris.cz/cs/mox/predstaveni/.

[7.] Shield. *Turris.* [Online] CZ.NIC, o.p.s. [Citace: 08. 09 2020.] https://www.turris.cz/cs/shield/predstaveni/.

[8.] Supported devices. *OpenWrt.* [Online] [Citace: 05. 05 2021.] https://openwrt.org/supported_devices.

[9.] Představení. *Turris Omnia.* [Online] CZ.NIC, . [Citace: 20. 12 2020.] https://www.turris.cz/cs/omnia/predstaveni/.

[10.] Wiki Turris. *Blokování reklam a trackerů.* [Online] CZ.NIC, z. s. p. o. [Citace: 14. 03 2021.] https://wiki.turris.cz/doc/cs/public/blokace-reklam.

[11.] CZ.NIC, z. s. p. o. Linuxové kontejnery. *Oficiální dokumentace Turris.* [Online] [Citace: 3. 01 2021.] https://doc.turris.cz/doc/cs/howto/lxc.

[12.] Turris Gadgets. *Wiki Turris.* [Online] [Citace: 14. 03 2021.] https://wiki.turris.cz/gadgets/start.

[13.] Turris Gadgets. *Wiki Turris.* [Online] CZ.NIC, z. s. p. o. [Citace: 14. 03 2021.] https://wiki.turris.cz/gadgets/start.

[14.] Turris Gadgets. *Wiki Turris.* [Online] CZ.NIC, z. s. p. o. [Citace: 14. 03 2021.] https://wiki.turris.cz/gadgets/domoticz.

[15.] Úvod do projektu HaaS - honeypot jako služba. *HaaS.* [Online] CZ.NIC, z. s. p. o. [Citace: 11. 03 2021.] https://haas.nic.cz.

[16.] RFC 821 - Simple Mail Transfer Protocol. *RFC Editor.* [Online] [Citace: 12. 2 2021.] https://www.rfc-editor.org/info/rfc821.

[17.] Styling your docs. *MkDocs.* [Online] [Citace: 12. 1 2021.] https://www.mkdocs.org/user-guide/styling-your-docs/.

[18.] Dokumentace NGINX. *https://www.nginx.com.* [Online] NGINX. [Citace: 22. 01 2021.] https://docs.nginx.com/nginx/admin-guide/installing-nginx/installing-nginx-open-source/.

[19.] Bruhat, Philippe. Net-Proxy-0.13. *Philippe Bruhat (BooK).* [Online] [Citace: 02. 01 2021.] https://metacpan.org/pod/distribution/Net-Proxy/script/sslh.

[20.] SSLH: SSH, SSL, VPN a další služby na jednom portu. *Root.cz.* [Online] [Citace: 25. 12 2020.] https://www.root.cz/clanky/sslh-ssh-ssl-vpn-a-dalsi-sluzby-na-jednom-portu/.

[21.] Vouch Proxy. *GitHub.* [Online] GitHub, Inc. [Citace: 04. 04 2021.] https://github.com/vouch/vouch-proxy.

[22.] Vouch Proxy. *github.com.* [Online] [Citace: 10. 12 2020.] https://github.com/vouch/vouch-proxy.

[23.] Co je to Real Smart Home? *Loxone.* [Online] [Citace: 04. 04 2021.] https://www.loxone.com/cscz/chytry-dum/.

[24.] Revogi Smart Power Plug. *E-shop Mironet.* [Online] [Citace: 11. 03 2021.] https://www.mironet.cz/revogi-smart-power-plug-chytra-zasuvka-wifi+dp277663/.

[25.] Google Play. *E.ON Chytrá zásuvka.* [Online] LIVE SMART. [Citace: 13. 03 2021.] https://play.google.com/store/apps/details?id=com.eon.home&hl=cs.

[26.] RevogiHome. *Google Play.* [Online] [Citace: 13. 03 2021.] https://play.google.com/store/apps/details?id=com.revogi.home.

[27.] ITEAD Wiki. *Products.* [Online] ITEAD Inteligent System Co., Ltd. [Citace: 14. 12 2020.] https://www.itead.cc/wiki/Product.

[28.] ESP8266 vývojová deska. *E-shop Wish.* [Online] [Citace: 15. 03 2021.] https://canary.contestimg.wish.com/api/webimage/5f96878927f0d90040469f6a-4-large.jpg.

[29.] Benchoff, Brian. An SDK for the ESP8266 WiFi Chip. [Online] [Citace: 04. 12 2020.] https://hackaday.com/2014/10/25/an-sdk-for-the-esp8266-wifi-chip/.

[30.] Sonoff produkts. *Sonoff technical support.* [Online] [Citace: 28. 01 2021.] https://sonoff.tech/products/.

[31.] Wireless Magnetic Door & Window Sensor EV1527 Coding Mode RF 433MHz. *Aliexpress.* [Online] [Citace: 14. 01 2021.] https://ae04.alicdn.com/kf/H9b19a7fb3a594f36bd5b23690ae2f91d4.jpg.

[32.] About. *Tasmota Github.* [Online] [Citace: 15. 01 2020.] https://tasmota.github.io/docs/About/.

[33.] HORÁK, Jaroslav a KERŠLÁGER, Milan. *Počítačové sítě pro začínající správce.* místo neznámé : Computer Press, 2013. ISBN 9788025131763.

[34.] CZ.NIC, z. s. p. o. *Nápověda k routeru Turris Omnia.*

[35.] Články. *Root.cz.* [Online] [Citace: 06. 05 2021.] https://www.root.cz/zpravicky/na-kazdy-router-turris-miri-denne-vice-nez-devet-tisic-utoku.

[36.] Google Play. *Revogi Home.* [Online] Revogi Innovation Co., Ltd. [Citace: 13. 03 2021.] https://play.google.com/store/apps/details?id=com.revogi.home&hl=cs.

[37.] Symbak. *Githab.* [Online] [Citace: 05. 01 2021.] https://github.com/ugoviti/synbak.

[38.] O sběru dat. *Oficiální dokumentace projektu Turris.* [Online] CZ.NIC, z. s. p. o. [Citace: 25. 12 2020.] https://doc.turris.cz/doc/cs/howto/collect.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CERT	Z angl. Computer Emergency Response Team – tým odborníků pro nápravu škod po napadení počítačových systémů.
CIO	Z angl. Chief Information Officer - používá se místo pojmu ředitel IT.
CPU	Centrální procesorová jednotka.
CSIRT	Z angl. Computer Security Incident Response Team – tým, který má zajistit reakci na incident nebo událost v IT.
DNS	Z angl. Domain Name System – systém, jehož hlavním úkolem je převod doménových jmen a IP adres.
DNSSEC	Z angl. Domain Name System Security Extensions – rozšíření původního systému DNS s ochranou proti manipulacím díky elektronickému podpisu.
eMMC	Flash paměť pro ukládání dat je robustnější než například výměnné SD karty.
FW	Z angl. Firewall - je zařízení nebo program pro zabezpečení síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti. Dle definovaných pravidel komunikaci buď povolí nebo odmítne.
GB	Násobek 10^9 byte, byte je základní jednotka kapacity počítačové paměti.
GND	Z angl. GrouND – uzemnění.
GNU	Projekt zaměřený na vývoj svobodného software.
GPIO	Z angl. General Ppurpose Input/Output – jsou to vstupně/výstupní piny.
HTTP	Z angl. Hyper Text Transfer Protocol - protokol používaný k přenosu souborů mezi serverem a klientem.
HTTPS	Z angl. Hyper Text Transfer Protocol Secure - je šifrovanou variantou protokolu HTTP. Veškerou přenášenou komunikaci šifruje algoritmem SSL nebo TSL.
HW	Z angl. Hardware - technické vybavení počítače (fyzické komponenty).
I²C	Sběrnice se používá v různých zařízeních pro čtení konfiguračních dat z paměťových modulů.

IDP	Z angl. Identity Provider – jedná se o techniku, kdy se identita uživatele ověří u externího poskytovatele.
IEEE 802.1	Z angl. The Institute of Electrical and Electronics Engineers Standards Association – jedná se o normu.
IMAP	Z angl. Internet Message Access Protocol - je protokol pro vzdálený přístup k e-mailové schránce prostřednictvím e-mailového klienta.
IoT	Z angl. Internet of Things - síť zařízení, která jsou vybavena, softwarem, senzory, a síťovou konektivitou, která umožňuje těmto zařízením se propojit a vyměňovat si vzájemně data.
IP	Z angl. Internet Protocol – protokol vyvinutý pro komunikaci zařízení v internetu.
IPv4	Jsou to 32bitová čísla, která jsou zapisována dekadicky po jednotlivých oktetech, například 192.168.0.1.
IPv6	Jsou to 128bitová čísla zapsaná hexadecimálně, například fd26:79d4:a9a1::309.
LAN	Z angl. Local Area Network – lokální počítačová síť.
LDAP	Z angl. Lightweight Directory Access Protocol- protokol pro přístup k datům na adresářovém serveru.
LED	Z angl. Light Emitting Diode – je to elektronická součástka, dioda, která emituje světlo.
LTE	Z angl. Long Term Evolution - v telekomunikacích se takto označují sítě pro vysokorychlostní přenos dat v mobilních sítích.
MB	Násobek 10^6 byte, byte je základní jednotka kapacity počítačové paměti.
MTA	Z angl. Mail Transfer Agent – označení pro účastníka přenosu zpráv elektronické pošty dle protokolu SMTP.
MySQL	Otevřený systém pro řízení báze dat, který uplatňuje relační databázový model.
NAS	Z angl. Network Attached Storage - datové úložiště pro ukládání nebo sdílení dat počítačů v jedné síti.

NAT	Z angl. Network Address Translation – díky technice překladu síťových adres umožní překládat adresy z vnitřního adresního rozsahu do veřejného a naopak a tím zajistí vzájemnou komunikaci.
OPKG	Z angl. Open Package Management - odlehčený systém pro správu softwarových balíčků systémů LINUX.
OS	Operační systém
OTA	Z angl. Over the Air – technika, která umožňuje nahrávání nových verzí firmware přes bezdrátovou síť.
PC	Osobní počítač
PIR	Pasivní infračervené čidlo, které měří infračervené záření vyzařující z objektů v jeho zorném poli.
POP3	Z angl. Post Office Protocol - protokol pro stahování emailové pošty přes e-mailového klienta.
RAM	Z angl. Random Access Memory – v elektronických zařízeních operační paměť.
RF	Z angl. Radio Frequency – vysokofrekvenční signál pro přenos informací.
RGB	Barevný model založený na třech barvách červená-zelená-modrá.
RSS	Z angl. Rich Site Summary – technologie, která na internetu umožní příjem novinek z webových stránek.
SDK	Z angl. Software Development Kit jedná se o sadu pro vývoj softwaru.
SFP	Konektor pro optické připojení o rychlosti až 2,5 Gb/s.
SIM	Z angl. Subscriber Identity Module je účastnická identifikační karta pro mobilní telefony
SMB	Z angl. Server Message Block - je síťový komunikační protokol, který slouží ke sdílenému přístupu k souborům, tiskárnám, a dalším zařízením v síti.
SMS	Z angl. Short Message Service - je služba pro posílání krátkých textových zpráv v sítích mobilních telefonů.

SMTP	Z angl. Simple Mail Transfer Protocol - protokol určený pro přenos zpráv elektronické pošty.
SOHO	Z angl. Small Office/Home Office – zařízení pro domácnost nebo malou firmu.
SOHO LAN	Domácí nebo firemní síť s přibližně 10 účastníky.
SPI	Z angl. Serial Peripheral Interface - sériové periferní rozhraní pro komunikaci mezi řídícími mikroprocesory a ostatními integrovanými obvody.
SSH	Z angl. Secure Shell - program a zároveň také zabezpečený komunikační protokol. Umožňuje vzdálenou zabezpečenou komunikaci.
SSL	Z angl. Secure Sockets Layer - vrstva bezpečných socketů, vrstva vložená mezi vrstvu transportní pro zabezpečení komunikace šifrováním a autentizací.
SSO	Z angl. Single Sign-On - jedením jménem a heslem se dá přistoupit k více službám.
SW	Z angl. Software - programové vybavení.
TCP	Z angl. Transmission Control Protocol - protokol na transportní vrstvě pro vytvoření spojení mezi aplikacemi.
TLS	Z angl. Transport Layer Security - kryptografické protokoly pro zabezpečenou komunikaci na internetu.
UART	Z angl. Universal Asynchronous Receiver-Transmitter - univerzální asynchronní přijímač-vysílač pro komunikaci PC a čipů.
USB	Z angl. Universal Serial Bus – průmyslové sériové rozhraní pro připojení zařízení
VPN	Z angl. Virtual Private Network - zabezpečené šifrované připojení mezi dvěma sítěmi
WAN	Z angl. Wide Area Network - česky rozlehlá síť v informatice síť, která pokrývá rozlehlé geografické území
WiFi	Technologie pro bezdrátový přenos dat v lokální síti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK