Západočeská univerzita v Plzni

Fakulta aplikovaných věd

Katedra informatiky a výpočetní techniky

Bakalářská práce

Modernizace a rozšíření správy školní počítačové sítě

Plzeň, 2016 Albert Štefankovič

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů.

V Plzni dne 29. dubna 2016

Albert Štefankovič

Poděkování

Děkuji pánům Mgr. Robertu Válkovi a Ing. Ladislavovi Pešičkovi za odborné vedení a pomoc při vypracování této bakalářské práce. Dále děkuji vedení Gymnázia v Prachaticích za ochotu při spolupráci.

Abstract

This thesis is aimed to the modernization of school computer network at the Grammar School in Prachatice. The goals are to improve the computer network to the requirements of grammar school, preparation of network topology plan and the creation of applications to simplify management of firewall rules. All the goals were first thoroughly analyzed before they were implemented. The requirements set by the grammar school were satisfied. Network topology was created for all floors of grammar school that have IT equipment. To simplify management of firewall rules have been created three applications that facilitate the work of teachers and network administrator. The total solution provides advanced options when editing the topology of the network, increasing its safety, throughput, reduces the number of network outages and allows interaction with a security gate. Executed changes were tested with respect to functionality and safety.

Abstrakt

Tato práce řeší modernizaci školní počítačové sítě v budově Gymnázia v Prachaticích. Mezi cíle patří vylepšení počítačové sítě na základě požadavků gymnázia, vyhotovení topologie počítačové sítě budovy gymnázia a vytvoření aplikace pro jednodušší správu firewallových pravidel. Všechny cíle byly nejprve důkladně analyzovány, až poté byly prováděny. Požadavky nastavené gymnáziem byly splněny. Topologie sítě byla vytvořena pro všechna patra gymnázia, která mají IT vybavení. Pro jednodušší správu firewallových pravidel byly vytvořeny tři aplikace, které usnadňují práci učitelům a správci sítě. Celkové řešení poskytuje rozšířené možnosti při úpravách v topologii počítačové sítě, zvětšuje její bezpečnost, propustnost, snižuje počet síťových výpadků a umožňuje interakci s bezpečnostní branou. Provedené změny byly testovány s ohledem na funkcionalitu a bezpečnost.

Obsah

1 Úvod

Cílem této práce je modernizace a rozšíření správy školní počítačové sítě. Za úkol si klade především vyhovění požadavkům vedení Gymnázia v Prachaticích pro zlepšení jejich počítačové sítě a vytvoření aplikace pro pomoc se správou a konfigurací sítě s ohledem na jednoduché používání. Práce byla tvořena ve spolupráci s firmou Tribase, s. r. o., která je externím zadavatelem tématu této práce.

Gymnázium prochází postupnou změnou IT infrastruktury. Tato práce zastřešuje finální fázi, ve které jde o nasazení zařízení pro bezpečnost sítě (*firewall, unifikovaná bezpečnostní brána*) a dalších síťových zařízení, které by měli zvětšit propustnost sítě, zvýšit její bezpečnost a usnadnit její správu. V průběhu návrhu této fáze byla s vedením gymnázia diskutována možnost nasazení aplikace, která by byla schopna ovládat tok datového obsahu v počítačových učebnách. Spolu s ní bude vytvořena i aplikace pro administrátora sítě, jejíž hlavní funkcí bude zjednodušení práce s konfigurací a údržbou sítě.

Aplikace pro správu datového obsahu v počítačových učebnách bude určena především pro učitele, kteří budou moci jednoduše zablokovat různé druhy webových stránek, nebo veškerý síťový provoz učebny. Aplikace pro administrátora sítě bude plně oddělena od učitelské aplikace. Aplikace bude administrátorovi poskytovat základní informace o stavu unifikované bezpečnostní brány a bude plnit úkony zaměřené na ulehčení správy sítě.

Obě aplikace budou naprogramovány pro operační systém Microsoft Windows v programovacím jazyce C#, na platformě *Microsoft .NET*. Aplikace budou komunikovat s unifikovanými bezpečnostními branami ZyXEL a ovládání bude v českém jazyce. U každé aplikace bude kladen důraz na jednoduchost a přívětivost uživatelského rozhraní.

Závěr práce bude věnován zhodnocení realizovaných vylepšení, ověření funkcionality provedených změn a otestování vytvořených aplikací.

2 Vývoj počítačové sítě v budově gymnázia

V této kapitole se nachází popis vývoje počítačové sítě, který v budově gymnázia proběhl v průběhu posledních let. Díky účasti externího zadavatele této práce na předchozích fázích je možné popsat a definovat fáze, které předcházely a tak vytvořit představu o současném stavu. Za první fázi lze považovat rozvedení internetového připojení do celé budovy. Druhá fáze poté obsahuje nasazení bezdrátových přístupových bodů, které zajišťují bezdrátové připojení a ve třetí fázi jde o nasazení firewallu. Všechny fáze se v průběhu jejich plnění vzájemně prolínaly. Nejde tedy o přesné rozdělení toho, jak modernizace sítě probíhala, jde spíše o logické uspořádání pro přehlednost. Čtvrtou definovanou fázi zastřešuje tato práce. Jednotlivé fáze jsou různě finančně náročné a tak bylo zapotřebí je rozložit úměrně k požadavkům a kvalitě zpracování.

2.1 Fáze I. - budování drátové sítě

Před první fází síťových úprav bylo k Internetu připojeno jen několik málo zařízení, které se nacházeli nedaleko od sebe. Takový stav byl v gymnáziu nepřijatelný a bylo tedy potřeba vybudovat síť po celé budově, dle potřeb - drátovou, či bezdrátovou. Výhodou drátové sítě je vyšší přenosová rychlost, ovšem koncové zařízení (např. počítač) musí být umístěno na předem určeném místě. Bezdrátová síť obvykle nedosahuje takových přenosových rychlostí, ovšem neomezuje uživatele v pohybu s koncovým zařízením. Bezdrátovou sítí se dále eliminuje potřeba kabelu, který je u drátové sítě nezbytný. Studenti, či učitelé s sebou tedy nemusí nosit kabely pro svá bezdrátová zařízení a při problémech, které mohou v síti nastat, není nutné kontrolovat kabely, zda jsou v pořádku.

Budova Gymnázia v Prachaticích byla otevřena v roce 1897 a patří mezi významné domy postavené ve městě Prachatice. K tomuto faktu musí být přihlíženo, především při rozsáhlejších stavebních úpravách, které mohou při budování sítě nastat. Byla potřeba vhodně umístit racky (systém pro umístění síťových zařízení) a zásuvky pro připojení koncových zařízení. Umístění racku musí být na místě s omezeným přístupem pro běžné uživatele a rack by měl být uzamykatelný. Zásuvky by pak měly být vhodně umístěny podle počtu zařízení v dané části budovy. Před provedením těchto změn je také zapotřebí

brát v potaz maximální možnou délku ethernetového kabelu. Tato délka je dle standardu ANSI/TIA/EIA pro měděný kabel kategorie 5e rovna 100 metrům. [1] Všechny tyto činnosti byly v budově provedeny.

2.2 Fáze II. - budování bezdrátové sítě

Ve druhé fázi budování infrastruktury sítě v v budově gymnázia, bylo úkolem vytvořit bezdrátovou síť pro přenosná zařízení, zejména notebooky, tablety a chytré mobilní telefony. Tento úkol byl zajištěn pomocí bezdrátových přístupových bodů (*AP, access point*), u kterých byla významným kritériem výběru nízká pořizovací cena. Tyto levné přístupové body se obvykle nacházejí v domácnostech a jejich softwarová výbava není příliš připravena na konfiguraci v podnikovém prostředí, za které můžeme školu považovat. U všech přístupových bodů je zapotřebí provést ruční konfiguraci a řešení případných problémů v síti bývá komplikované.

Bezdrátovou sítí byla pokryta jen místa s největší předpokládanou koncentrací zařízení připojujících se k bezdrátové síti. Za takové kritické místo byla označena hlavní kancelář, kde se nachází ředitelna a sekretariát, vstupní hala a vybrané třídy. Přihlašování do sítě bylo zabezpečeno pomocí hesla, určeného zvlášť zaměstnancům a studentům. Pro učitele, sekretariát a ředitelnu byla vyhrazena unikátní síť. Počet bezdrátových přístupových bodů a zásuvek je uveden v kapitole 4.2.1.

2.3 Fáze III. - nasazení první bezpečnostní brány

Třetí fáze změn v síťové infrastruktuře primárně zajistila bezpečnost a ochranu síťového provozu. Jedná se o nasazení bezpečnostní brány, jejíž zařazení do síťové infrastruktury může být způsobem, jak zabezpečit spojení mezi internetem a interní sítí. Přítomnost bezpečnostní brány v počítačové síti může redukovat případy, kdy se vnější útočníci snaží nabourat do interní sítě.

V roce 1989 bylo oznámeno méně než 200 případů porušení bezpečnosti sítě v rámci

celého světa. V roce 1994 již bylo takových případů 2 241 a vzrůstající tendence samozřejmě pokračují dodnes. [2] Podle statistik vedených společností Kaspersky, je v dnešní době, jen v České republice, průměrně v jednom měsíci zjištěno 35 000 útoků do vnitřních sítí. [3] Bezpečnostní branou lze definovat pravidla, jak se uživatelé uvnitř sítě mohou a nesmějí chovat. Blíže o funkcích bezpečnostních bran pojednává kapitola 3.3.

Bezpečnostní brána, která byla v této třetí fázi vybrána, je od společnosti ZyXEL, konkrétně ZyXEL USG 50. Plní funkci firewallu, podporuje filtrování webového obsahu a je umožněn základní monitoring sítě. Pomocí tohoto zařízení lze například na škole zakázat stránky, ke kterým by studenti neměli mít přístup. Právě funkce filtrování byla hlavním důvodem nasazení bezpečnostní brány na Gymnáziu v Prachaticích. Tímto zařízením bylo také dosaženo duplikovaného připojení k internetu, díky více záložním portům. Duplikované připojení nefunguje jen jako záloha, kdy po odpojení jednoho připojení je dostupné druhé, ale USG 50 zvládá spojení obou připojení najednou a je schopné mezi dvěma poskytovateli rozkládat zátěž plynoucí z vnitřní sítě.

2.4 Fáze IV. - finální fáze

Čtvrtá fáze vývoje počítačové sítě tvoří téma této bakalářské práce. Jedná se především o zlepšení doposud vybudované infrastruktury a nasazení síťových zařízení, které jsou jednoduše nastavitelné pomocí webového rozhraní a ulehčují tak správu sítě a řešení problémů v síti. Po této fázi bude mít administrátor sítě větší možnosti kontroly bezpečnosti sítě a vedení školy se bude moci na svou počítačovou síť více spolehnout, jednotliví učitelé přitom budou mít možnost blokovat webové služby v rámci počítačových učeben. V rámci bakalářské práce bude řešeno:

- Výběr vhodné bezpečnostní brány
- Odstranění problémů v počítačové síti gymnázia
- Tvorba dokumentace topologie sítě
- Aplikace pro správu bezpečnostních politik vyučujícím a aplikace pro ulehčení správy bezpečnostní brány

3 Síťové prvky, technologie a řízení v síti

V této kapitole jsou definovány základní síťové prvky, technologie a v závěru kapitoly se nachází popis metody, která umožňuje řídit procesy v síti. Ze síťových prvků je věnována pozornost především unifikované bezpečnostní bráně, jejíž výměna je jedním z cílů této práce. V kapitole je kladen důraz na vysvětlení všech pojmů tak, aby čtenář porozuměl následujícím analýzám a jejich vyhodnocování.

3.1 Pasivní síťové prvky

Mezi pasivní síťové prvky řadíme kabely, konektory, rozvaděče, atd. Jsou to prvky, které s přijímaným signálem nedělají nic jiného, než že se postarají o jeho přenos. Tato část se dále věnuje základním rozdílům mezi metalickou a optickou kabeláží.

Kabely je vhodné v každém objektu, kde se provádí rozvod síťové infrastruktury, vést uspořádaně, v efektivních trasách a především je nutné každý kabel popsat pro jeho jednoznačnou identifikaci. Špatně označený, či dokonce neoznačený kabel, prodlužuje dobu výkonu práce. V racku je dobrým zvykem kabely uspořádat, udržovat ve svazcích, nekřížit je a nelámat.

Pro metalickou kabeláž se využívají kovové, především měděné vodiče. I přesto, že existuje několik typů metalických kabelů (rozdělení je dáno podle síly stínění), mají společné 4 páry barevně odlišených vodičů. Barvy musí být na koncích kabelů uspořádány do konektorů podle potřebné normy.

Díky standardizačním institucím, jsou definovány kategorie kabelů, které jsou rozdílné v přenosové rychlosti a v druhu kabeláže. Rozdíly mezi jednotlivými druhy kabelů se nachází v tabulce 3.1, tabulka 3.2 vyjadřuje rozdíly mezi klasifikacemi metalických kabelů. [4]

Pro metalické kabely se obvykle používá koncovka RJ45. Koncovkou RJ45 disponuje většina síťových prvků. Její fotografie se nachází na obrázku 3.1.

Každá technologie má své fyzikální vlastnosti, které se těžko překonávají. Optická

Typ	Popis
UTP	*Unshielded Twisted-pair* je tvořena čtyřmi páry izolovaných kroucených vodičů, Jedná se nejlevnější typ kabelu.
FTP	*Foil Twisted-pair* se skládá z ze čtyř párů kroucené dvoulinky obalené stínící fólií. Oproti UTP dražší, tlustší a těžší.
STP	*Shielded Twisted-pair* se skládá ze čtyř párů, kdy každý pár je obalen kovovou fólií. Oproti FTP dražší, hůře se instaluje.

Tabulka 3.1: Druhy kabeláže a jejich popis

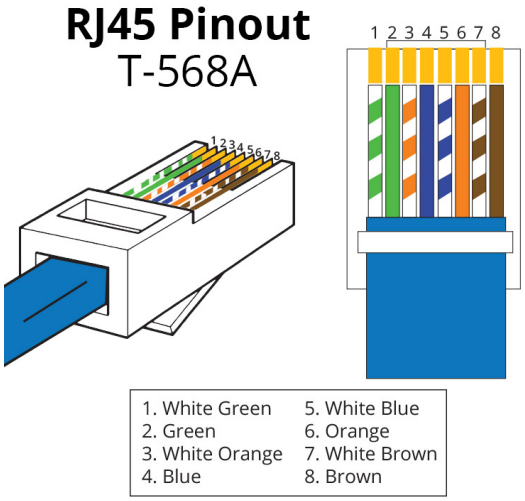
Kategorie	Rychlost přenosu	Používané typy kabelů
CAT 3	10 Mb/s	UTP
CAT 5e	1 Gb/s	UTP, FTP
CAT 6	10 Gb/s	UTP, FTP, STP
CAT 7	10gb/s	STP

Tabulka 3.2: Klasifikace metalických kabelů

kabeláž je technologickým pokrokem v oblasti kabelů, především kvůli lepší prostupnosti signálu. U optiky se využívají skleněná, nebo plastová vlákna, která pomocí světla přenášejí signál.

Výhodou optiky je její rychlost a možnost použití na delší vzdálenosti než metalické kabely. Optické kabely nejsou tvořeny z kovu a tak je možné vést trasu optických kabelů vedle kabelů vysokého napětí.

Šíření světla v optických kabelech může být dosaženo různými technologiemi. Dle průchodu světla vláknem dělíme optické kabely na jednovidové a multividové. Jednovidová optická vlákna mají velmi malý průřez jádra, to znamená, že světlo může procházet pouze pod jedním vstupním úhlem a jedním vláknem je tedy možné šířit pouze jeden vid. Oproti tomu multividová vlákna, mají velký průřez jádra a je tedy možné šířit pod různými úhly více vidů. Mutlividová vlákna jsou levnější a jejich výroba je jednodušší. Jednovidová vlákna jsou na výrobu složitější a jejich cena bývá vyšší, ovšem jejich perspektiva je v použití na delší vzdálenosti při vyšších rychlostech přenosu. Prosvícení vlákna může



Obrázek 3.1: Schéma zapojení konektoru RJ45, [5], 2015

být dosaženo technologií LED, nebo laserem.

3.2 Aktivní síťové prvky

Na rozdíl od pasivních prvků, aktivní mohou se signálem pracovat, např. jej mohou zesilovat, modifikovat či vyhodnocovat. Mezi aktivní síťové prvky můžeme zařadit např. router, switch, bezdrátový access point, nebo firewall. O všech těchto zařízeních následující část pojednává.

Switch je síťové zařízení, které má několik LAN portů a umožňuje v rámci sítě propojit zařízení, která jsou do LAN portů připojená. Pokud switch přijme zprávu (paket), přečte si cílovou adresu (fyzickou adresu zařízení) a hledá ji ve své tabulce. Pokud záznam najde, přepošle zprávu na daný port. Pokud záznam s cílovou fyzickou adresou chybí, přepošle zprávu na všechny své porty, kromě příchozího. Důležité je, že switch procházející data nijak nemění, pouze je čte.

Router, je na rozdíl od switche, schopen směrovat data mezi dvěma segmenty sítě - například mezi sítí počítačů v domácnosti a internetem. Pokud router přijme zprávu (rámec), obdobně jako switch nahlédne do své tabulky cílových adres (IP adres). Z tabulky

zjistí přes které rozhraní má zprávu odeslat a případně na kterou adresu. Poté router pozmění rámec přepsáním zdrojové adresy na svou vlastní. Pokud router nezná cestu k cíli, zprávu zahazuje.

Access point představuje zařízení, které umožňuje bezdrátové připojení k síti ostatním zařízením. Access pointy v mnoha případech využívají technologii PoE, popsanou v kapitole 3.4.1. Uživatel není díky access pointu omezen kabelem a může se volně pohybovat v oblasti, kde je access point schopný vysílat bezdrátový signál. Bezdrátové vysílání má z hlediska bezpečnosti nevýhodu - útočník může libovolně naslouchat komunikaci mezi uživatelem a access pointem. Z tohoto důvodu je při úvodní konfiguraci access pointu dbát na bezpečnost řešení.

Bezpečné komunikace lze dosáhnout několika úrovněmi zabezpečení. Nejnižší úroveň se skládá ze zablokování vysílání názvu wifi připojení (SSID - uživatel jej musí znát, aby se připojil) a z blokování fyzických adres zařízení (access point akceptuje pouze určitá zařízení). Tuto nejnižší úroveň ochrany však lze obejít a celé řešení se tedy nedá označit za bezpečné.

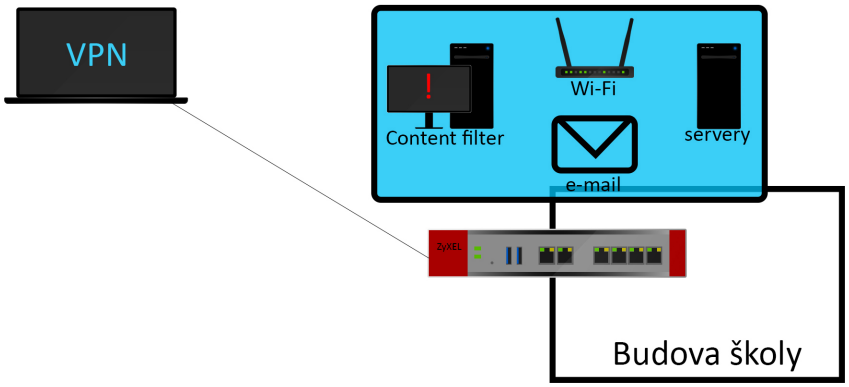
Na vyšší úrovni se nachází šifrování komunikace pomocí klíčů (přístupového hesla k wifi připojení). Mezi základní metody zabezpečení patří WEP, WPA a WPA2. Z nichž nejnovějším typem je WPA2. Pokud je ovšem pro připojení k síti určeno slabé heslo (číselné řady, datum narození, jména domácích mazlíčků) lze i takto šifrované připojení napadnout. [6]

Pro zvýšení zabezpečení sítě lze použít firewall. Jedná se o pomyslnou bezpečnostní bránu, která obdobně jako router odděluje dvě sítě. Firewall detekuje data, která mezi sebou propouští sítě a povoluje jen taková, která jsou předem definována správcem sítě.

3.3 Funkce unifikované bezpečnostní brány

Přesto, že každý výrobce má ve své unifikované bezpečnostní bráně specifické funkce, lze definovat obecné funkce, které se objevují napříč všemi zařízeními. Tyto funkce je nutné definovat pro efektivní a správnou analýzu. Obrázek 3.2 znázorňuje vybrané funkce

unifikované bezpečnostní brány, pojmy, které se na obrázku vyskytují, jsou uvedeny následujících podkapitolách.



Obrázek 3.2: Funkce unifikované bezpečnostní brány. Zdroj: vlastní zpracování, 2015

3.3.1 Unifikovaná bezpečnostní brána

Původní myšlenka firewallu představovala definici pravidel mezi sítěmi, které od sebe firewall odděloval. [7] Vzhledem k tomu, že technologický vývoj a s ním stále rostoucí význam internetu, neustále postupují vpřed, společnosti vyvíjející firewally cítí potřebu umístit do svých zařízení co nejvíce funkcí.

Výhodou více funkcí v jednom zařízení je především jednodušší správa, přehlednější analýza a snadná prvotní konfigurace, která probíhá v unifikovaném prostředí. Není tedy nutné znát mnoho různých nastavení pro každého výrobce a s tím souvisejících aktualizací jejich výrobků. Na druhou stranu více funkcí může mít vliv na menší propustnost sítě a taková skutečnost může některým zákazníkům vadit. [8]

Marketingové označení unifikované bezpečnostní brány - firewall nové generace, představuje komplexní zařízení zaměřené na bezpečnost sítě. Jejich výrobci obvykle nevkládají do svého produktu všechny funkce, ale zákazníkům nabízí možnosti předplatného

(např. na jeden rok) s výběrem jednotlivých funkcí. Níže uvedené funkce, především *anti-virus, anti-spam, VPN a IDP* jsou právě těmi funkcemi, které jsou vkládány do nových typů bezpečnostních bran a v porovnání s předchozí generací jsou tyto funkce mnohem robustnější a disponují větší propustností.

3.3.2 Content filter

Content filtering představuje soubor pravidel, které definují, zda konkrétní stroj (případně množina strojů) má umožněn přístup ke konkrétní webové stránce či jinému obsahu dostupnému ve vnitřní síti, nebo v internetu. Domácnosti mohou tato pravidla využívat pro nastavení domácí počítačové sítě, podle kterého budou mít jejich děti přístup jen ke vhodnému obsahu. V korporátní sféře lze pro content filtery najít využití především k omezení přístupu zaměstnanců k sociálním sítím a dalším stránkám bránícím v produktivitě pracovníka.

Nové typy bezpečnostních bran umožňují rozšířené možnosti filtrování obsahu. Je možné nastavit blokaci specifické oblasti internetu. Například sociální sítě, online hry, zprávy, finance apod.

3.3.3 Anti-virus a Anti-spam

Cílem obou funkcí je ochrana sítě před průnikem škodlivých souborů. Anti-virus, nebo anti-spam kontroluje soubory, které v síti procházejí přes bezpečnostní bránu, například stahované soubory, e-maily a jejich přílohy.

Výrobci obvykle zabezpečují tyto funkce pomocí aplikací třetích stran. Využívají renomované společnosti v oblasti virů a jejich vyhledávání. Administrátor vše konfiguruje v rámci prostředí unifikované bezpečnostní brány.

3.3.4 IDP

IDP z anglického *Intrusion detection protection* (odhalení průniku) je obranný systém, který monitoruje síť a snaží se odhalit podezřelé aktivity, například pokud se útočník snaží v síti prokazovat jako legitimní uživatel. [9] Tyto aktivity určuje na základě databáze známých průniků a ohrožení. Na trhu se objevují různá řešení IDP. Od speciálně upravených linuxových distribucí až právě po funkce v unifikovaných bezpečnostních branách.

3.3.5 VPN

Virtuální privátní síť (VPN) je propojení mezi dvěma uzly sítě realizovaná přes privátní nebo veřejnou síť, jako je například internet, přičemž přenášená data jsou z důvodu bezpečnosti šifrována. [10] VPN umožňuje uživatelům připojit se do podnikové sítě a využívat ji z domova tak, jako v kanceláři. VPN se dnes často používá například při práci z domova (*Home Office*). [11]

3.3.6 Upozornění na problém v síti

Pokud v síti nastane nějaký problém, je vhodné, aby se o tom administrátor dozvěděl. V ideálním případě ještě před tím, než ho o nějakém problému informuje uživatel. Pokud administrátor provozuje v síti unifikovanou bezpečnostní bránu s velikým množstvím aktivních funkcí, má veliký rozsah dat o síťové aktivitě, které aktivní funkce vyhodnocují. Informace o nebezpečí v síti pak může bezpečnostní brána zapisovat do logového souboru, který lze kdykoliv prostudovat. Některé unifikované bezpečnostní brány umožňují vymezit situace za kterých je administrátorovi odeslán e-mail. Správce sítě má tedy přehled o aktuálním stavu sítě a zjištěné problémy může hned začít řešit.

3.3.7 SSH

Protokol SSH (*Secure Shell*) zajišťuje bezpečnou (šifrovanou) komunikaci mezi dvěma počítači. SSH použijeme, chceme-li například ovládat počítač (k němuž máme při-

hlašovací údaje) na dálku, nebo přenášet soubory pomocí jiných protokolů (*SFTP, SCP*). [12] SSH server standardně naslouchá na portu TCP/22. U bezpečnostních bran se SSH používá pro vzdálenou konfiguraci. Pomocí příkazů určených výrobcem, je možné v příkazové řádce, definovat pravidla firewallu.

Protokol SSH verze 1 je dnes již zastaralý a nedoporučuje se, jej používat. První verze je nahrazována historicky o dva roky mladší verzí 2. Při sestavování komunikace SSH v2 si obě strany nejprve vymění informace o verzi protokolu a další parametry. Poté dojde k jednoznačné autentizaci uživatele, která může být uskutečněna pomocí hesla, nebo mechanismu veřejného a privátního klíče.

3.4 Další technologie

Síťových technologií existuje mnoho, pro tuto práci jsou důležité technologie Power over Ethernet, Virtual LAN a NAT, jejichž popis se v této části nachází.

3.4.1 Power over Ethernet

Některé síťové prvky využívají technologii *Power Over Ethernet (PoE)*, která umožňuje napájení pomocí ethernetového kabelu. Takové řešení má výhodu především v ušetření potřebné kabeláže k provozu zařízení. PoE je definováno standardy IEEE 802.11af a 802.11at. Pro integraci PoE je nutné umístit do sítě switche, které touto technologií disponují. [13] Mezi zařízení, pro která je technologie PoE typická patří například access pointy, nebo IP telefony.

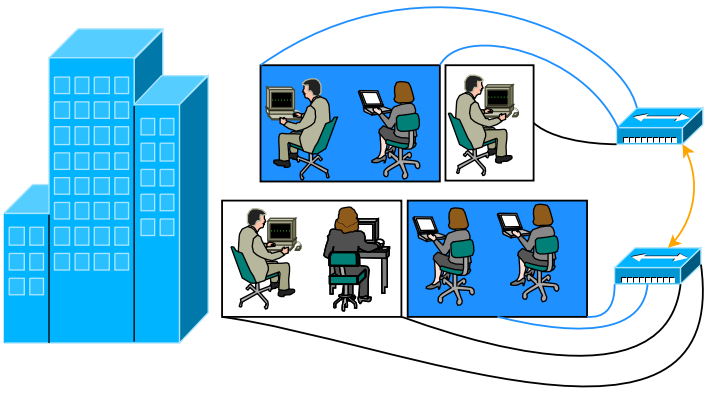
3.4.2 Virtual LAN

Hlavní myšlenkou VLAN je rozdělení sítě do logických skupin, nezávisle na fyzickém umístění. Typickým příkladem je budova podniku se dvěma patry. V přízemí se nachází oddělení A, v patře jsou oddělení A a B. Cílem je propojení oddělení do dvou skupin. Bez VLAN by bylo nutné všechny počítače z každého oddělení propojit do jednoho switche,

což může být v rámci patrové budovy problém. Jak je vidět na obrázku 3.3, VLAN v tomto směru usnadňují práci. Na obrázku je modře vyznačené oddělení A, bíle oddělení B.

Při komunikaci je zapotřebí řešit příslušnost posílané zprávy k určité VLAN. V rámci jednoho switche je komunikace jednoduchá. Switch má svou operační paměť, ve které udržuje informace, do které VLAN patří daná komunikace (port). S těmito informacemi je možné povolit pouze správné směrování.

Složitější situace nastává, pokud komunikace prochází více než jedním switchem. Jde o stav kdy je cílem využívat stejné VLAN v celé síti, nezávisle na tom, ke kterému switchi jsou zařízení připojena. Komunikaci pomocí VLAN v celé síti umožňuje protokol IEEE 802.1q, neboli *trunking protocol*. Jedná se o standardizovanou metodu, kterou podporují všechny moderní switche s podporou VLAN. Funguje na principu tzv. tagování. Originální zpráva je rozšířena o informaci pro kterou VLAN je určena. [14]



Obrázek 3.3: Příklad řešení propojení sítě pomocí VLAN. Zdroj: vlastní zpracování, 2016

3.4.3 Překlad síťových adres

Překlad síťových adres *Network Address Translation, NAT* se používá k úspoře IP adres v současném internetu. Většinou je realizován například na routeru, nebo firewallu připojujícím lokální síť k síti poskytovatele internetového připojení. V lokální síti pak mohou být použity libovolné adresy (nejčastěji se jedná o adresy z neveřejného rozsahu).

Pokud počítač z lokální sítě odesílá paket do vnější sítě (např. internetu), odešle jej se svou zdrojovou IP adresou a portem. Při průchodu zařízením obsluhujícím NAT jsou

však zdrojové IP adresy v paketech přepsány na veřejnou IP adresu. Také je přepsáno číslo zdrojového portu na port, který NAT odesílajícímu počítači přidělil. NAT si zároveň uloží toto přidělení do své převodní tabulky (v které jsou uloženy veškeré informace o vzájemném mapování jednotlivých adres). NAT je poté schopen pomocí převodní tabulky přiřadit odpověď vzdáleného počítače, správnému zařízení uvnitř sítě. [15]

3.5 Procesy a řízení v síti

V této části jsou popsány základní pravidla bezpečnostních politik a trend Bring Your Own Device, který do jisté míry vystihuje zasahování osobních počítačů do lidského života.

3.5.1 Bezpečnostní politika sítě

Každou sítí (domácí i podnikovou) mohou protékat důležitá data např. hesla, vnitřní podnikové dokumenty atd. Ve většině domácnostech nemá bezpečnost uvnitř sítě vysokou prioritu, nicméně zabezpečení proti průniku do vnitřní sítě je zajisté na místě.

Podnikové prostředí obsahuje veliké množství faktorů, které mohou narušit bezpečnost síťového provozu a tím může být ohrožena existence společnosti. Mohou uniknout data tvořící konkurenční výhodu a tak je na společnostech, aby si svá data chránily a přistupovaly k nim obezřetně. Z hlediska bezpečnostní politiky se doporučuje vytvořit dokument, který sjednotí všechna bezpečnostní doporučení a postupy. Dokument s bezpečnostní politikou minimalizuje případná nedorozumění. Ovšem ať společnost vlastní bezpečnostní dokument, nebo ne, je patřičné aby bezpečnostní politika existovala a všichni zaměstnanci firmy ji respektovali.

Bezpečnostní politika by měla respektovat procesy a postupy ve společnosti. Definice pravidel přihlašování a práv podle uživatelů, nebo jejich skupin, ošetření krajních možností (např. pokud uživatel zapojí cizí zařízení do sítě) to vše je součástí bezpečnostní politiky.

3.5.2 Bring your own device

V podnikovém prostředí je trendem *Bring Your Own Device (BYOD)*, kdy mají zaměstnanci možnost pracovat na vlastních zařízeních, která znají a nemusí se učit s novými systémy, rozložením pracovní plochy apod. Zaměstnavatel však musí důkladně zabezpečit podnikovou síť, aby předešel vynášení důvěrných dat, či možnosti průniku do podnikové sítě přes osobní zařízení zaměstnanců[16]. Nicméně 20% zaměstnanců [17] své vlastní zařízení v podniku používá bez vědomí zaměstnavatele a BYOD je tak nástrojem pro udržení bezpečnosti v podniku. [18]

3.6 Kryptografie a hashovací funkce

Kryptografie je věda zabývající se návrhem šifer. Vstupem do šifry je otevřený text, který je transformován šifrovací funkcí. Výstupem je zašifrovaný text. Šifrovací funkce se dělí na symetrické a asymetrické.

Symetrické šifry šifrují text po blocích a využívají substituce a permutace těchto bloků. Symetrické šifry využívají různý počet iterací, kdy při každé iteraci dojde k substituci, permutaci, či k součtu s klíčem. Klíč je u symetrických šifer identický pro šifrování i dešifrování. Mezi symetrické šifry řadíme například DES, AES, nebo Blowfish. [19][20]

Asymetrické šifrování používá k šifrování veřejný klíč, k dešifrování soukromý klíč. Oba klíče jsou přitom propojeny matematickými výpočty. Asymetrická šifrovací funkce je například RSA.

Hash, neboli otisk je jednocestná funkce, která z libovolně dlouhého textu vytvoří řetězec konstantní délky. Existují různé hashovací funkce, například MD5, nebo SHA1. U hashovacích funkcí platí jednoduchá rovnost, malá změna textu, znamená velikou změnu výsledného hashe. [21]

4 Topologie sítě

Kapitola topologie sítě pojednává o tom, jaká síťová zařízení jsou ve škole umístěna, kolik se jich v budově nachází a jejich přibližné umístění a propojení. V přílohách je přiloženo schéma topologie sítě, které vytvoří představu o rozmístění prvků a bude sloužit správcům sítě na gymnáziu. Mapa topologie sítě je tvořena na základě dat dodaných externím zadavatelem, které byla ověřována osobní prohlídkou.

4.1 Úvod do topologie v budově gymnázia

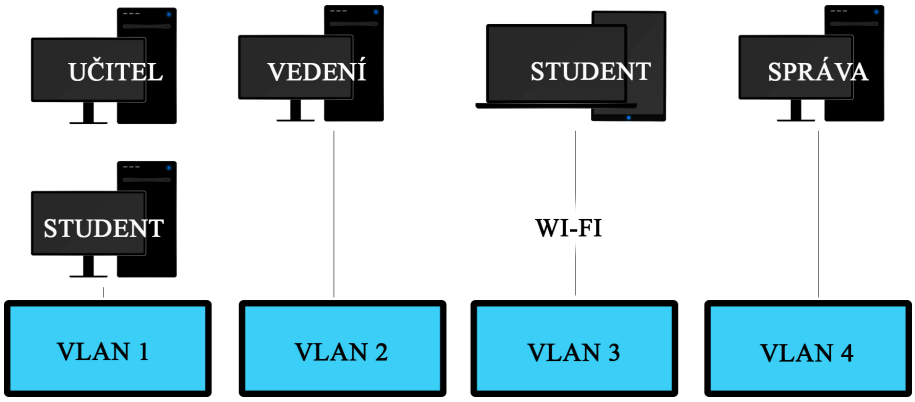
Na Gymnáziu v Prachaticích v současné době studuje 289 studentů a je zde zaměstnáno 35 zaměstnanců školy [1]. Pro takové množství lidí je potřeba správně nadimenzovaná síť, splňující především školní potřeby - použití výpočetní techniky ve výuce a udržování databáze studijních výsledků studentů. Vedlejším cílem školní počítačové sítě může být umožnění přístupu k internetu studentům a učitelům na jejich osobních zařízeních. Tento cíl může být podpořen politikou BYOD (viz kapitola 3.5.2).

Z hlediska citlivých dat se ve škole nachází systém pro zapisování známek a docházky, webové a e-mailové služby, kamerový a bezpečnostní systém. Tyto systémy je nutné uchovat v bezpečné zóně a nedovolit neoprávněným uživatelům do těchto systémů proniknout.

Lidé pohybující se v budově školy, mohou být rozděleni na několik kategorií podle jejich zájmu a chování v síti - studenti, učitelé, vedení školy a správce sítě. Tomuto dělení odpovídá i dělení sítě na tzv. *virtuální sítě LAN (VLAN)*.

Z obrázku 4.1 lze pozorovat jak jsou pracovní skupiny v síti gymnázia odděleny. Každá z výše definovaných pracovních skupin má svou VLAN. Učitelské a studentské školní počítače mají přiřazenou VLAN 1. Vedení školy má svou oddělenou VLAN 2, VLAN 3 slouží pro bezdrátové připojení osobních počítačů studentů k internetu a VLAN 4 je určená pro správu sítě. Ve všech VLAN je možný přístup k internetu, po připojení k doméně je umožněn přístup do vnitřní sítě, například ke sdíleným diskům.

[1] Čísla vycházejí z výroční zprávy gymnázia, poskytnuté sekretariátem školy

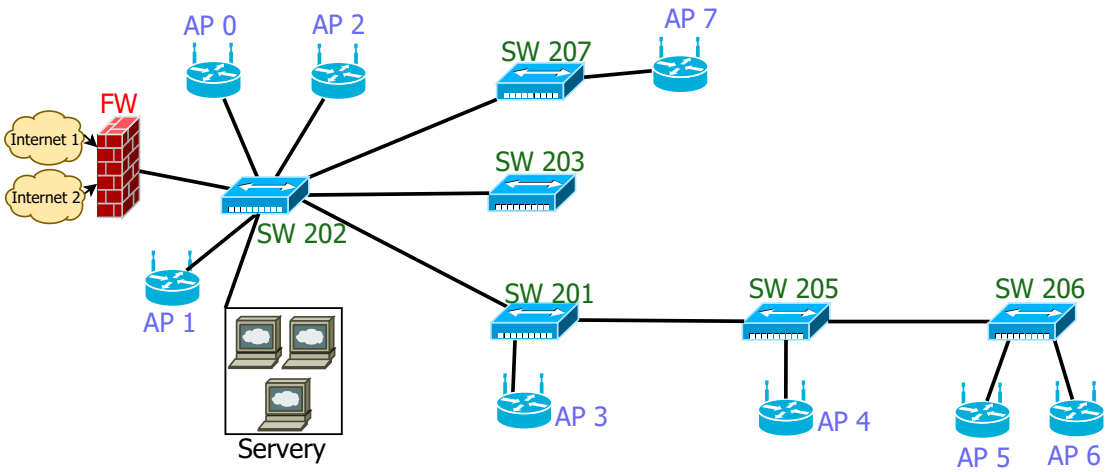


Obrázek 4.1: Znázornění rozdělení VLAN. Zdroj: vlastní zpracování, 2016

4.2 Vytvoření topologického schématu

Tato podkapitola se věnuje vytvoření schématu sítě od prvotního získávání informací, po celkovou kompletaci. Schéma sítě se nachází v přílohách A1-A6 znázorňujících jednotlivá patra a části budovy a v příloze A5 znázorňující umístění a spojení rackových skříní.

Topologické schéma sítě před vytvářením této práce neexistovalo, byly dostupné jen přibližné počty zařízení a o jejich poloze vědělo jen pár lidí (správce sítě a sekretářky z kanceláře vedení školy). Logické schéma sítě se nachází na obrázku 4.2.



Obrázek 4.2: Logické schéma sítě. Zdroj: vlastní zpracování, 2016

4.2.1 Získání dat

Při vytváření schématu bylo vycházeno z prvotních dat od externího zadavatele (přibližné počty zařízení a jejich pozice). Na základě těchto dat bylo nutné školu osobně projít a zkontrolovat umístění jednotlivých prvků. Takto zjištěná data byla zakreslena do předem připravených plánků školy, které přibližně korespondují s reálným plánem.

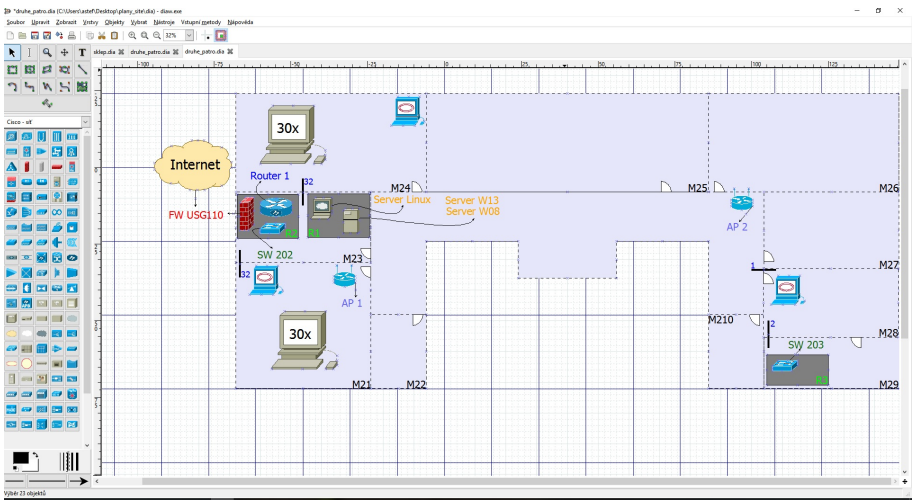
Pro vytvoření představy o velikosti sítě slouží tabulka 4.1, která zachycuje množství jednotlivých síťových prvků.

Typ	Počet (ks)
Racky	7
Počítače	111
Notebooky	20
Tablety	15
Serverová PC	2
Switche	6
Routery	1
Bezdrátová AP	8
Unifikované bezpečnostní brány	1

Tabulka 4.1: Počet jednotlivých síťových prvků v budově

4.2.2 Výběr aplikace

Zakreslené pozice síťových prvků bylo zapotřebí převést do formátu, který by odpovídal dokumentaci a byl použitelný v reálném nasazení. Pro návrh schémat se na trhu nachází několik aplikací. V rámci této práce byly vyzkoušeny aplikace Cisco PacketTracer a Dia. Po vyzkoušení jednoduchých schémat byla vybrána kombinace aplikace Dia spolu s piktogramy od společnosti Cisco. Piktogramy jsou dodávány v jednom balíku s instalací z oficiálních stránek aplikace Dia. Ukázka pracovního prostředí se nachází na obrázku 4.3.



Obrázek 4.3: Ukázka pracovního prostředí aplikace Dia. Zdroj: vlastní zpracování, 2016

4.3 Popis topologie

Všechna schémata se nachází v části příloh A1-A5. Schémata jsou do jisté míry zjednodušená, především pro zachování bezpečností politiky gymnázia a také pro udržení přehlednosti celého schématu. Schéma je dokumentací stavu sítě po veškerých úpravách v rámci této bakalářské práce.

Celková koncepce topologie vychází z postupné obměny a modernizace sítě v průběhu let, popsané v kapitole 2. Je nutné brát v potaz, že síť nebyla budována najednou s jedním komplexním plánem, ale byla vytvářena postupně dle požadavků gymnázia.

4.3.1 Klíčové prostory

Na základě příloh A1-A6 můžeme definovat klíčové prostory, které se v budově nachází a z hlediska topologie mají podstatný význam. Mezi takové místnosti patří počítačové učebny - M21, M24, M05 a M09. Tyto učebny jsou určené pro výuku pomocí výpočetní techniky. V těchto učebnách bude nasazena aplikace pro správu unifikované bezpečnostní brány. Popis aplikace se nachází kapitole 7.

Nejdůležitější místností z hlediska počítačové sítě je místnost M23. Zde se nachází Main Distribution Frame (nebo také Main Distribution Facility, MDF) se kterým jsou spojeny (přímo i nepřímo) Intermediate Distribution Frames (IDF) z celé budovy. Pod pojmem MDF se skrývá hlavní rozvodna spojující vnitřní a venkovní (připojení k internetu od poskytovatele) síť, v topologických schématech označena jako R2 - rack 2. V MDF se nachází tzv. Point of Presence (PoP), neboli přístupový bod poskytovatele internetových služeb (v budově gymnázia metalický kabel). PoP je důležitý především při výběru poskytovatele internetových služeb - je nutné ověřit zda se v dané lokalitě nachází dostupnost poskytovatele, v požadované kvalitě a poskytovatel je tak schopen poskytnout PoP. V MDF jsou umístěna zařízení, umožňují distribuci internetového připojení do celé budovy a jedná se tak o centrální místo a kritický bod celé topologie [22]. MDF se nachází v zamykaném kabinetu, do kterého má přístup jen omezený počet zaměstnanců školy.

IDF je pojem označují vedlejší rozvodny, v topologických schématech jednotlivých pater jsou to racky odlišné od R2. Jejich hlavním úkolem je distribuce síťového připojení k uživateli a usnadňují fyzickou výstavbu sítě (není potřeba vést mnoho kabelů přes celou budovu).

4.3.2 Servery

V gymnáziu se nachází tři fyzické servery. Server s OS Linux určený pro řízení webových a e-mailových služeb a dva servery s OS MS Windows Server 2003 a 2012. Servery s OS Windows mají roli správce síťové domény, slouží jako síťový souborový systém a je na nich spuštěna MySQL databáze pro potřeby vedení školy.

4.3.3 Síťové prvky

Umístění síťových prvků odpovídá požadavkům v jednotlivých fázích vývoje počítačové sítě. Změna se obvykle plánuje tak, aby každá další případná změna s sebou nesla co nejmenší úpravy. Pro názornost může být uvedena změna při natažení kabelu od racku do učebny. I když je potřebný jen jeden kabel, je vhodné jich protáhnout více a v cíli například vytvořit vhodně umístěnou zásuvku pro jednoduchou manipulaci. Dalším příkladem

může být výběr síťových zařízení s dostatečným počtem portů.

4.3.4 Pozice a propojení racků

Tuto kapitolu doplňuje příloha A6, kde se nachází přibližný plánek rozmístění racků napříč celou budovou školy. Racky mají přiřazené číslo podle toho, jak byly v průběhu let instalovány. Všechny racky se spojují v MDF (R2).

Optické spojení mezi budovu školy a přístavbu bylo zvoleno zejména kvůli vzdálenosti přesahující 100 metrů (optické kabely je možné vést na delší vzdálenosti[23]). Dalším důležitým faktorem pro výběr optického kabelu byla tehdejší omezená rychlost kabelů metalických. Datový přenos po optice dosahoval 1Gb, zatímco u metalických kabelů byla taková rychlost teprve plánována. Typicky oranžové optické kabely v hlavní budově školy jsou vyfoceny na obrázku 4.4.

Obrázek 4.4: Optické kabely spojující hlavní budovu s přístavbou. Zdroj: vlastní zpracování, 2016

5 Analýza požadavků

Kapitola obsahuje analytickou část této práce. Požadavky klienta můžeme rozdělit na dvě části. Požadavky na změnu síťové infrastruktury a požadavek na funkcionalitu aplikace, která bude měnit konfiguraci unifikované bezpečnostní brány. Kromě požadavků klienta je nutné přihlížet i k požadavkům správce sítě, tedy na správnou konfiguraci nových zařízení a aplikaci, která mu umožní jednodušší diagnostiku bezpečnostní brány.

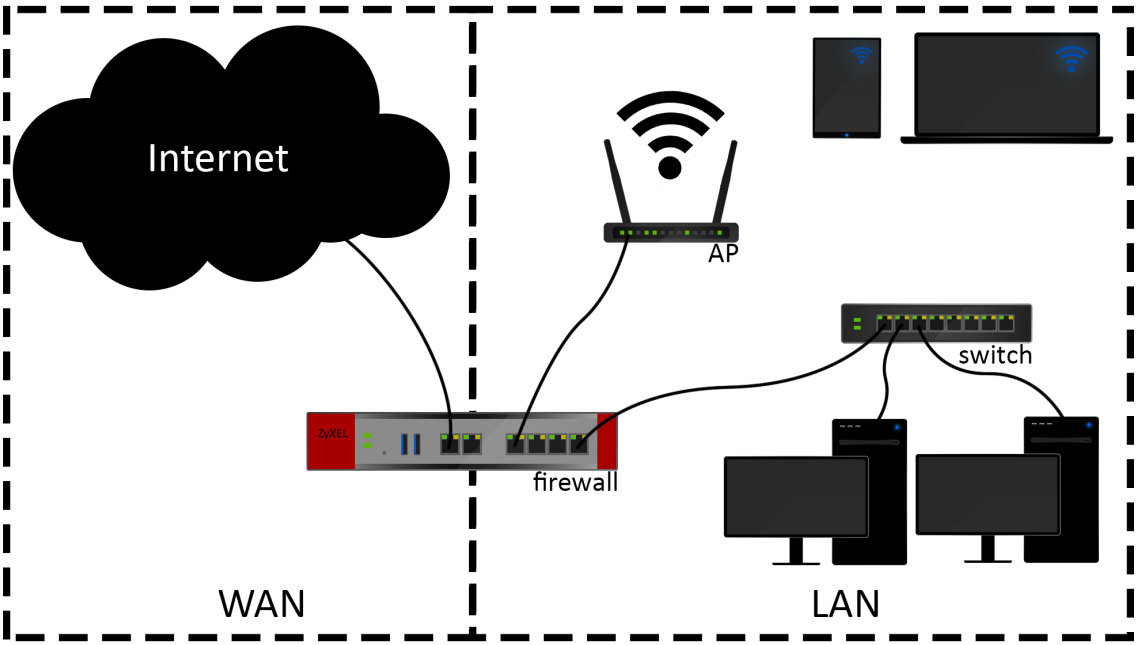
5.1 Vlastnosti stávající unifikované bezpečnostní brány

Základní funkcionalitu unifikované bezpečnostní brány můžeme vymezit hardwarovou a softwarovou výbavou. Z hardwarové stránky by měla bezpečnostní brána disponovat minimálně jedním portem pro připojení vnitřní sítě a minimálně jedním portem, určeným pro připojení do vnější sítě. Vnitřní sítí se označuje soubor síťových zařízení, propojených pomocí přepínačů, které jsou v rámci sítě vzájemně dosažitelné (např. počítače v učebnách). Vnitřní síť také označujeme jako LAN (*Local Area Network*). Vnější sítí se rozumí síť přivedená poskytovatelem, neboli síť internetu, označována také jako WAN (*Wide Area Network*). Obrázek 5.1 zachycuje rozdíl mezi těmito pojmy na topologicky jednoduché síti. Internetové připojení od poskytovatele je zapojeno do portu WAN a uvnitř bezpečnostní brány poté distribuováno do vnitřní sítě. Vnitřní síť na obrázku 5.1, tvoří koncová zařízení, bezdrátový access point a síťový přepínač, anglicky *switch*.

Softwarové vybavení unifikované bezpečnostní brány by mělo obsahovat nástroje pro konfiguraci zabezpečení sítě. Základní přehled takových nástrojů je uveden v předchozí části 3.3.

5.1.1 Hardwarová specifikace současné bezpečnostní brány

Z hlediska hardwarové výbavy má USG 50 čtyři porty LAN. Do těchto portů se obvykle zapojují síťové prvky (např. access pointy, switche) nebo koncová zařízení (např. počítače). Propojením těchto prvků v místní počítačové síti, zajistíme jejich vzájemnou



Obrázek 5.1: Znázornění rozdílu mezi vnitřní a vnější sítí. Zdroj: vlastní zpracování, 2015

dostupnost. Zařízení od výrobce ZyXEL dále disponuje 2 porty WAN zabezpečující připojení místní počítačové sítě do internetu. Dvojice portů poté umožňuje mít více poskytovatelů a minimalizovat tak výpadky připojení k internetu. Porty na USG 50 dosahují maximální přenosové rychlosti 1 Gb/s.

Tato bezpečnostní brána má ještě 2 USB porty, ke kterým máme možnost připojit *USB flashdisk*, či externí pevný disk a umožnit uživatelům přístup k souborům na těchto zařízeních uložených.

5.1.2 Softwarová specifikace současné bezpečnostní brány

Samotný hardware ovšem nezajistí takové funkce, které specifikují unifikovanou bezpečnostní bránu. Společnost ZyXEL má na svých zařízeních nainstalovaný svůj vlastní operační systém a záleží na prodejní politice, které funkce budou v daném zařízení dostupné. USG 50 patří z hlediska prodeje k první generaci unifikovaných bezpečnostních bran této společnosti, přehled jeho funkcí se nachází v tabulce níže.

Název zařízení	USG 50
LAN porty	4x Gb
WAN porty	2x
USB	2x
Firewall	ANO
Anti-virus	ANO
Anti-spam	ANO
Content filter	ANO
IDP	ANO
Upozornění na výjimečné události	ANO
Propustnost (Mb/s)	
Firewall	225
VPN	90
UTM[1]	30

Tabulka 5.1: Funkce ZyXEL USG50

5.2 Požadavky kladené na novou unifikovanou bezpečnostní bránu

Hlavním přáním klienta bylo vyměnit stávající bezpečnostní bránu popsanou v části 5.1. K tomuto kroku vedl fakt, že stávající ZyXEL USG 50, který byl pořízen ve III. fázi úprav, nemá podporu nových a vylepšených bezpečnostních funkcí, popsaných v kapitole 3.3.1, a také nemá potřebnou propustnost. Rychlost připojení od poskytovatele činí 120 Mb/s[2], USG 50 má však se zapnutými bezpečnostními funkcemi propustnost jen 30 Mb/s. [24] Výměna tohoto síťového zařízení znamená porovnat podobné, na trhu dostupné produkty s parametry, které budou nejlépe odpovídat požadavkům, kladeným na počítačovou síť. Nově vybranou unifikovanou bezpečnostní bránu je poté potřeba nakonfigurovat a otestovat nové nastavení.

[1] UTM označuje zapnuté funkce pro analýzu síťového provozu

[2] Tento údaj vychází ze specifikace připojení od poskytovatele internetu

Funkce, které jsou od nové bezpečnostní brány vyžadované jsou filtr obsahu a podpora VPN. VPN je vyžadována především pro umožnění vzdáleného přístupu vedení školy, které tak bude mít možnost připojit se do školy z domova a například se podívat na živé přenosy z bezpečnostních kamer. Vzhledem k tomu, že se jedná o gymnázium, je vhodné v tomto zařízení provádět filtraci síťového obsahu a nedovolit studentům přístup k nevhodnému obsahu, případně studentům omezit přístup ke stránkám, které mohou odvádět jejich pozornost.

5.3 Ostatní požadavky na změnu počítačové sítě

Gymnázium žádalo o vyřešení častých výpadků sítě v jedné z učeben. Tento problém může být důsledkem mnoha poruch, které mohou v počítačové síti nastat. Jelikož se jedná o učebnu připojenou pomocí bezdrátového access pointu může být důvodem slabý signál wifi, poškozený kabel, poškozená síťová karta počítače, může být vadný access point, nebo jeho konfigurace.

Externí zadavatel uvedl v průběhu vypracovávání této práce poruchy výpadků specifikovaných switchů a úkolem tedy bylo zjistit, proč jsou dané síťové prvky nedostupné, především ve večerních hodinách a o víkendech.

Řešení obou problémů je blíže popsáno v kapitole 6.1.

5.4 Analýza aplikací komunikujících s bezpečnostní branou

Během úvahy jak bude aplikace vznikat, je zapotřebí zamyslet se nad funkcionalitou a několika důležitými parametry.

Aplikace bude ovládat datový tok v počítačové učebně. Toho bude možné dosáhnout komunikací aplikace s bezpečnostní branou. Bezpečnostní brána bude mít administrátorem definovaná pravidla, která bude aplikace zapínat.

Při vytváření aplikace pro učitele bude zároveň vyvíjena aplikace pro administrátora sítě. Tato aplikace bude vytvářet konfigurační soubory pro učitelskou aplikaci a bude mít další funkce, které podpoří práci správce sítě. Mezi takové funkce bude patřit zobrazení názvu a stavu zařízení, ke kterému se administrátor přihlásí, nebo nastavení opakovaného restartování zařízení. Tyto funkcionality jsou požadovány externím zadavatelem a budou naprogramovány dle jeho zadání.

Dále je potřeba definovat rozhraní aplikace, programovací jazyk a formát konfiguračních souborů.

5.4.1 Aplikační rozhraní

Je nutné vybrat rozhraní, přes které bude aplikace pomocí SSH posílat bezpečnostní bráně příkazy. Obecně lze tato rozhraní vymezit webovou, nebo desktopovou aplikací. Webové aplikace jsou v dnešní době velmi rozšířené a mají několik výhod před desktopovými. Aplikace běží v okně webového prohlížeče, který ji načte z webového serveru. Je tedy umístěna centralizovaně a její aktualizace nepřináší problémy. Lze ji spustit na mobilních i desktopových zařízeních. Desktopová aplikace je umístěna na konkrétním stroji, její aktualizace se musí provést na všech zařízeních kde je nainstalována.

Aplikace bude užívána v několika gymnaziálních třídách a bude spravovat nastavení unifikované bezpečnostní brány pro množinu studentských počítačů umístěných ve třídě. Aby byla snížena pravděpodobnost chybného chování uživatele, bude vybrána desktopová aplikace, která bude uložena na učitelských počítačích (aktuálně 3 PC), pod zabezpečeným účtem v zabezpečené třídě. Oproti webové verzi bude aplikace více skryta před studenty, kteří budou mít minimální možnost, zkoušet různými technikami prolomit zabezpečení aplikace.

5.4.2 Programovací jazyk

Zvoleným řešením s ohledem na výše uvedené skutečnosti je tedy desktopová aplikace. Vzhledem k tomu, že operačním systémem na všech školních počítačích je Micro-

soft Windows, zvolený programovací jazyk je C# .NET s frameworkem WPF.

Jazyk C# je jednoduchý moderní vysokoúrovňový objektově orientovaný programovací jazyk vyvinutý společností Microsoft. [25] Přesto že je určen pro operační systém MS Windows, je možné *.exe* soubory spouštět i na ostatních platformách. [26]

WPF (Windows Presentation Foundation) je framework pro komplexní tvorbu formulářových aplikací, který je součástí .NET frameworku od verze 3.0. Disponuje širokou paletou formulářových prvků a také umožňuje bohaté stylování vzhledu aplikace.

WPF framework umožňuje definici vzhledu aplikace pomocí XAML jazyka. Kromě lepšího oddělení prezentační a aplikační vrstvy aplikace umožňuje XAML lepší napojení objektů na formulářové prvky. [27]

Vývojovým prostředím pro vývoj aplikací bude MS Visual Studio Ultimate 2013. Verze Ultimate je plnou verzí softwaru a obsahuje všechny dostupné funkce.

5.4.3 Formát konfiguračních souborů

Pro uložení dat, která uživatel změní v průběhu používání aplikace je nutné vytvářet soubory, které umožní změněná data uložit a načíst při opětovném spuštění aplikace.

Uložení konfiguračních souborů je možné provádět v několika možných formátech. Nejčastějším formátem konfiguračních souborů jsou soubory *.xml* a *.txt*. Oba z vyjmenovaných mají své výhody a nevýhody.

Soubory *.xml* jsou čitelnější běžným uživatelům a umožňují strukturovaný zápis dat, ovšem jejich vytváření je složitější. Naproti tomu *.txt* soubory zabírají méně místa na disku a jejich vytvoření je jednoduché.

Vzhledem k jednoduchosti byly vybrány soubory *.txt*, s přesně definovanou strukturou zápisu dat, blíže v kapitole 7.2.

6 Úprava síťové infrastruktury

V této kapitole je uveden postup při řešení všech úkolů určených v předchozích částech. Jedná se o postup při výměně unifikované bezpečnostní brány a opravách síťového připojení.

6.1 Výpadky sítě

Přáním klienta bylo zjistit a opravit časté výpadky síťové konektivity v jedné z učeben. Po výpadku nejsou učitelé schopni připojit se ke svému síťovému úložišti a studentům zobrazit daný materiál, případně test. Z toho důvodu, že v této době zatím nebyly v budově instalovány síťové prvky, které by byly schopny sledovat potřebná síťová připojení, bylo zapotřebí vynaložit více úsilí pro identifikaci tohoto jevu.

Počítač je ve třídě umístěný v zamčené skříni a k síti byl připojený pomocí bezdrátového připojení. Access point, který konektivitu zajišťoval, byl ovšem v pořádku a nevykazoval žádné známky poruchy. Počítač sám o sobě také neprojevil žádné vady a tak přišla na řadu fáze důkladnější analýzy problému. Po výpadku sítě bylo zapotřebí v co nejkratší době problém nahlásit. To se ze strany učitelů podařilo a tak mohl být problém nalezen. Příčinou poruch, byla činnost studentů, kteří z access pointu vytahovali napájecí kabel zajišťující přívod elektrické sítě. Access point byl totiž kvůli síle signálu umístěn na skříni a studenti k němu měli volný přístup. Tuto závadu nebyli učitelé schopni identifikovat a bylo potřeba tento jev minimalizovat.

Vzhledem tomu, že na každém patře je umístěný rack s propojovacími síťovými prvky, řešení nebylo složité. Bylo nutné k inkriminovanému místu dovést síťový kabel. To obnášelo pár stavebních zásahů, především při průchodu místnostmi od racku až k dané třídě. Vzhledem k nutným průrazům byly vytvořeny kanály, které jsou v budoucnu znovupoužitelné a pokud vznikne potřeba natažení dalšího kabelu, nebude tato činnost náročná. Počítač byl poté připojen pomocí kabelu a možnost přerušení spojení se tak minimalizovala.

Předcházením těmto nechtěným zásahům do sítě by se podobné problémy mohly iden-

tifikovat mnohem rychleji a mnohem efektivněji by mohly být odstraněny. V tomto případě byla v síti síťová zařízení, která takové problémy nedokáží řešit, a vedení gymnázia tedy byl předložen návrh na zlepšení sítě použitím novějších síťových prvků s větší možností jejich správy. Nasazení nové bezpečnostní brány spolu s možností řízení aktivních prvků v síti se vzájemně doplňuje a gymnázium tento návrh nakonec uvítalo.

6.2 Fyzické zabezpečení síťových prvků

Předchozí, zdánlivě jednoduchý, problém v důsledku vyvolal mnoho dalších změn a úprav, které byly vykonány v rámci této práce. Jelikož od předchozích fází úprav síťové infrastruktury neuplynula příliš dlouhá doba, umístění některých síťových prvků nebylo ještě dovedeno k dokonalosti.

Po zkušenosti s vypojeným kabelem v jedné třídě přišla na řadu kontrola podobných slabých míst v celé budově. Bylo nalezeno několik volně přístupných access pointů, které byly posléze uschovány do uzavíratelných krabic.

Dalším takto nalezeným problémem bylo umístění některých switchů v kabinetech učitelů. Switche se do kabinetů umisťovali s důvěrou, že nedojde k přerušení dodávky elektrického proudu a odpojení ethernetových kabelů. Někteří učitelé ovšem při odchodu z práce vypojovali veškerá elektrická zařízení, a pokud chtěl administrátor sítě během noci zkontrolovat pomocí vzdálené správy síť, nebo konkrétní počítač, neměl k potřebným objektům přístup. Řešení tohoto problému bylo spojeno s probíhajícími pracemi na zabezpečovacím systému pro školu. Tyto práce vykonávala také společnost Tribase. Pro switche z kabinetů a nové bezpečností prvky byl v prostorách školy umístěn nový rack. Umístění toho racku bylo navrhnuto tak, aby propojení prvků v něm umístěných nevyžadovalo veliké úpravy a zároveň aby byl umístěn na bezpečném místě.

6.3 Výměna současné unifikované bezpečnostní brány

Pro výběr nové unifikované bezpečnostní brány je důležité prozkoumat nabídku trhu a vybrat zařízení, které bude nejvíce odpovídat požadované funkčnosti. Průzkum trhu byl uskutečněn vyhledáváním v nabídkách českých i zahraničních e-shopů. Bylo zjištěno, že na tomto trhu se pohybuje menší množství výrobců, kteří nabízejí podobná zařízení s obdobnou specifikací. Od každého výrobce byl posléze vybrán jeden produkt, nejlépe odpovídající daným specifikacím. Mezi vybrané výrobce patří ZyXEL, Kerio, Ubiquity, Netgear a Cisco. Nově vybrané zařízení je po instalaci nutné nakonfigurovat a vrátit síť do funkčního stavu.

6.3.1 Výběr vhodného zařízení

Pro porovnání vybraných zařízení byly určeny sledované parametry - propustnost unifikované bezpečnostní brány, propustnost po aktivování dalších funkcí, počet portů, VPN, IPS, možnost antivirové ochrany, content filtering, možnosti upozornění na vzniklý problém a v neposlední řadě cena. Tyto parametry patří mezi základní vlastnosti a zároveň odpovídají požadavkům klienta a současné konfiguraci sítě. Sledovaným parametrům nejlépe odpovídají produkty v tabulce 6.1.

Označení výrobku	Název výrobku
A	ZyXEL USG 110
B	Kerio control box 3130
C	Ubiquity EdgeRouter PRO
D	Netgear FVS336G-300
E	Cisco ASA 5585-X with SSP-10

Tabulka 6.1: Vybrané produkty ke srovnání, 2016

Někteří výrobci neuvádějí všechny parametry. Jedná se především o propustnost unifikované bezpečnostní brány po zapnutí filtrovacích funkcí, kdy může propustnost dostát významného poklesu. Tato informace je velmi podstatná a na jejím základě lze jednotlivá zařízení porovnávat. Někteří výrobci také uvádějí přítomnost content filteru, ovšem

po hlubší analýze bylo zjištěno, že se úroveň jednotlivých content filterů liší a je důležité tento fakt brát v úvahu při rozhodování. Různé funkce content filterů se odvíjí od faktu, zdali je zařízení unifikovanou bezpečnostní branou, popsanou v části 3.3.1.

V tabulce 6.2 se nachází porovnání vybraných produktů. Veškeré informace, které jsou v tabulce uvedené, pochází z oficiálních katalogů výrobců. Ceny jsou získány z volně dostupných internetových ceníků oficiálních prodejců zkoumaných značek. Znakem „-“ je označen stav, kdy není možné z technických specifikací produktů danou informaci zjistit. Výrobky Ubiquity a Netgear patří k levnějším variantám, ovšem na základě zkušeností zadavatele této práce také k těm méně vybaveným. Tyto bezpečnostní brány by stávající USG 50 předčily jen v několika málo funkcích a jejich nákup by nepředstavoval získání větších výhod, které ostatní výrobci nabízejí a zákazník by je využil.

Výrobek	A	B	C	D	E
LAN porty	4x Gb	8x Gb	6x Gb	4x Gb	8x Gb
WAN porty	2x Gb	2x Gb	2x Gb	2x Gb	2x 10Gb
USB	2x	2x	0	0	0
Firewall	ANO	ANO	ANO	ANO	ANO
Anti-virus	ANO	ANO	NE	NE	NE
Anti-spam	ANO	ANO	NE	NE	NE
Content filter	ANO	ANO	ANO	ANO	ANO
IDP	ANO	ANO	NE	NE	ANO
Upozornění	ANO	ANO	NE	ANO	ANO
Propustnost	(Mb/s)				
Firewall	1 600	1 000	1 000	350	4 000
VPN	400	-	-	78	1 000
UTM[1]	250	190	-	-	-
Ceny (Kč)					
Ceny HW[2]	19 990	35 300	10 174	5 766	420 069
Ceny SW[3]	19 360	7 135	-	-	-

Tabulka 6.2: Srovnání dostupných produktů. Zdroj: oficiální katalogy výrobců, 2015

[1] UTM označuje zapnuté funkce pro analýzu síťového provozu

Produkt od společnosti Cisco se vymyká především cenově. Tuto cenu si zákazník nemůže dovolit, ovšem i přesto je v tabulce uveden, především z důvodu mapování celého trhu.

Ze zjištěných informací je patrné, že mezi nejlépe vybavená zařízení s ohledem na cenovou dostupnost a funkce, které jsou klientem požadovány, patří bezpečnostní brány od výrobců ZyXEL a Kerio. Tyto dva produkty mají také velmi podobné funkce i uživatelské rozhraní. Obě zařízení se také dají zařadit mezi unifikované bezpečnostní brány, které by bylo s nahlédnutím do budoucna vhodné do školy pořídit. Nižší pořizovací cena a zkušenost se zařízeními ZyXEL jsou rozhodující faktory, které určily výběr unifikované bezpečnostní brány ZyXEL USG 110. Tento výběr byl konzultován s externím vedoucím práce a poté s vedením gymnázia, které tento návrh odsouhlasilo. Fotografie nového USG 110 umístěného v racku se nachází na obrázku 6.1. Při instalaci byly využity oba WAN porty, kterými zařízení disponuje a jeden LAN port pro řídící switch.

Obrázek 6.1: USG 110 umístěné v rackové skříni. Zdroj: vlastní zpracování, 2016

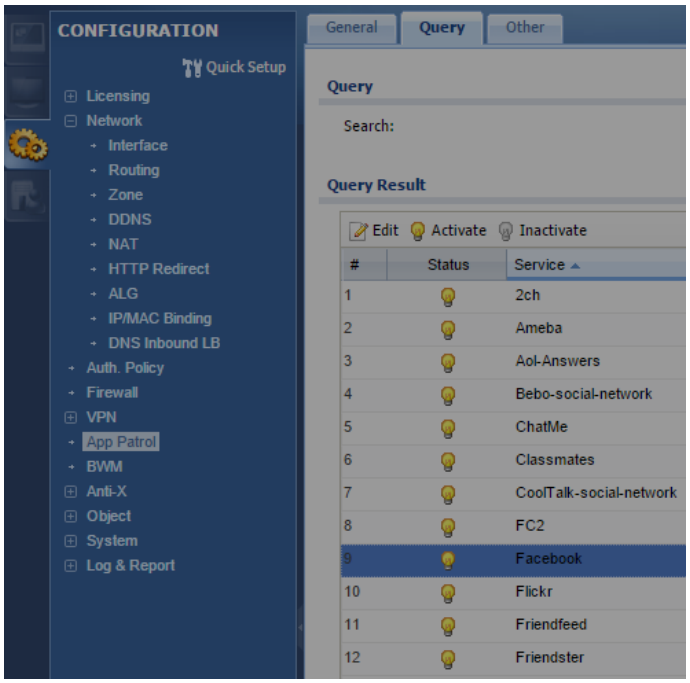
[2]Uvedené ceny zařízení vycházejí z ceníků oficiálních prodejců umístěných na internetu

[3]SW se rozumí SW balíčky obsahující všechny dostupné funkce

6.3.2 Konfigurace

Vzhledem k tomu, že nově vybranou bezpečnostní branou se stalo zařízení od stejného výrobce, jako předchozí bezpečnostní brána, průběh konfigurace byl téměř identický jako na původní bezpečnostní bráně. Společnost ZyXEL dokonce umožňuje automatickou transformaci konfigurace mezi zařízeními, bohužel jen v rámci stejné třídy. Původní USG 50 je však třídou nejnižší a nové USG 110 se řadí do vyšší třídy. Bylo tedy nutné stávající nastavení USG 50 ručně transformovat do nového zařízení. Díky stejnému grafickému uživatelskému prostředí, které je vidět na obrázku 6.2, nebyl tento krok nikterak náročný.

Konfiguraci lze provést i pomocí SSH konzole a příkazů příkazové řádky. Soubor těchto příkazů vystavuje výrobce na svých webových stránkách. U tohoto výrobce umožňují SSH příkazy širší možnosti, než grafické uživatelské rozhraní. Těchto rozšířených možností bude využito v aplikacích, které jsou popsány v kapitole 7.



Obrázek 6.2: Grafické uživatelské prostředí USG 110. Zdroj: vlastní zpracování, 2016

6.4 Výměna bezdrátových access pointů

Jak bylo zmíněno v kapitole 6.1, ve škole se nacházela jen bezdrátová AP, která není možné spravovat z jednoho místa a mít o nich alespoň základní informace. Při koupi nové unifikované bezpečnostní brány byla prodejcem nabídnuta snížená prodejní cena na bezdrátová AP ZyXEL (konkrétně NWA 3560 viz obrázek 6.3).

V tomto případě není výhodná jen cena, ale nově pořízená unifikovaná bezpečnostní brána dokáže bezdrátová AP ZyXEL v síti identifikovat a administrátorovi sítě umožní jejich správu na jednom centrálním místě. Správce sítě má možnost nahlédnout na stav AP, jeho vytížení, aktualizace firmwaru a má možnost konfigurovat jej. Urychluje tak řešení případných problémů. USG 110 dokáže takto spravovat až 34 zařízení.

Technické specifikace modelu uvedené v tabulce 6.3 uvádějí čím NWA 3560 disponuje. Výrobce tento model řadí do podnikových řešení, právě kvůli možné centralizované správě. U tohoto modelu lze využít technologii *Power Over Ethernet (PoE)*, více o této technologii viz kapitola 3.4.1.

Obrázek 6.3: NWA 3560. Zdroj: http://www.zyxel.com, 2016

Po konzultaci s vedením školy byly zatím zakoupeny 2 kusy NWA 3560, s vizí do budoucna, aby všechna AP byla řízena centrálně. Nová AP nahradila stávající - v příloze A3 jsou označena jako AP 4 a AP 6. Jedná se o pokrytí prostoru u vchodu do budovy, kde se nachází stravovací zařízení a zdržuje se zde nejvíce lidí. Jedno staré AP (příloha A4 - AP 5) bylo použito ve sklepě, kde mají školník a uklízečky své prostory, druhé bylo umístěno do přístavby (příloha A6 - AP 7), kde mají studenti prostor k sezení a mohou

NWA 3560	
Přenosová rychlost wifi	1Gb
Podporovaná pásma	2,4 a 5GHz
Podpora VLAN	Ano
Počet antén	4
IEEE	802.11a/b/g/n
PoE	Ano

Tabulka 6.3: Technická specifikace NWA 3560, Zdroj: [13], 2016

zde využívat wifi připojení.

7 Návrh aplikací pro usnadnění správy bezpečnostní brány

V této kapitole je popsána návrhová část tvorby aplikací pro správu nové bezpečnostní brány. Jsou zde popsány problémy, které bylo potřeba při návrhu eliminovat pro správnou a bezpečnou funkcionalitu vytvářených aplikací.

Správná funkcionalita aplikací úzce souvisí s možnými příkazy, které lze bezpečnostní bráně zadat. Vybrané příkazy bylo nutné vyhledat a vyzkoušet, zda opravdu fungují. Dalším parametrem, který má vliv na správnost aplikace je zajisté její uživatelské prostředí. To musí být přehledné a jednoduché tak, aby se v něm cílový uživatel vyznal za každých okolností.

Vzhledem k tomu, že vytvářené aplikace ovlivňují datový tok uvnitř školní sítě, je při návrhu velmi důležité věnovat pozornost bezpečnosti celého řešení. Aplikace musí být důkladně zabezpečené, nesmí být narušena integrita jejich konfiguračních souborů.

7.1 Funkcionalita aplikací

V průběhu analýzy, která je popsána v části 5.4, vyplynula ze strany vedení školy potřeba kontroly dostupného webového obsahu během vyučovacích hodin. Hlavním požadavkem je zajistit tuto funkci v počítačových učebnách a případně tuto funkci zapnout v celé budově. Během vyučovací hodiny někteří studenti využívají sociálních sítí a dalších stránek, které mohou odvádět jejich pozornost od výuky a snižovat jejich produktivitu. Vypnutím celého připojení by však učitelé přišli o možnost nechat studenty využívat internetu pro vyhledávání potřebných informací.

Funkcionalitu webového filtru lze konfigurovat z webového rozhraní unifikované bezpečnostní brány. V tomto administrátorském rozhraní se ovšem nachází i mnoho jiných nastavení, jejichž změna může mít fatální následky na stav sítě. Z tohoto důvodu není vhodné umožnit přístup zaměstnancům školy k tomuto konfiguračnímu rozhraní. Nastavení filtru pro určité časové intervaly (např. 8-12 hodin) webové prostředí ZyXEL nepod-

poruje. Můžeme využít možnost připojení pomocí SSH a pomocí příručky definovaných příkazů provádět rozsáhlejší a detailnější nastavení. Ovládání zařízení přes SSH terminál a definované příkazy by bylo obtížné a jako správné řešení se tedy nabízí vytvoření jednoduché, funkční aplikace.

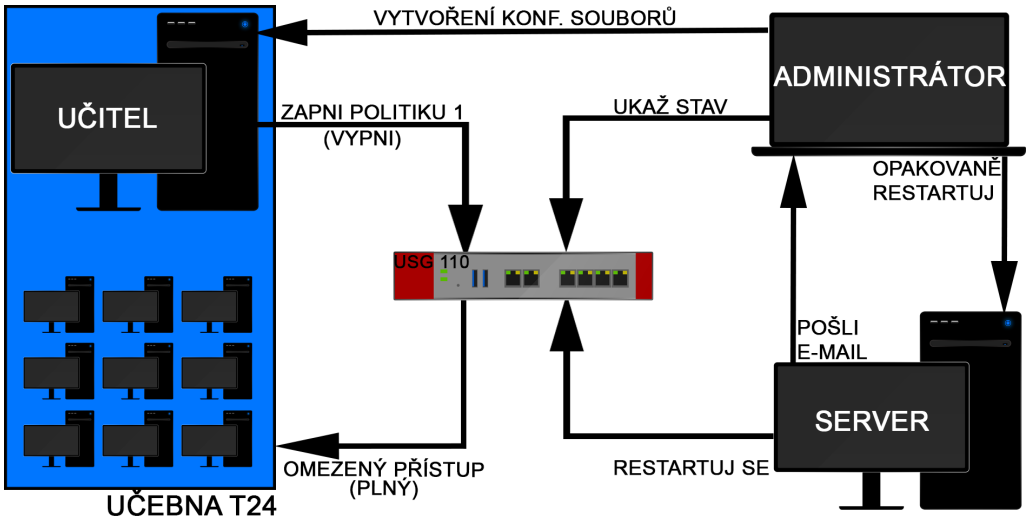
Konzultací s vedením školy i s externím vedoucím této práce bylo zjištěno, že by oběma stranám omezení webového obsahu v celé budově vadilo a tak dále není tato funkce brána v potaz. Důvodem je nutnost vedení databáze, kde by byly zapsány přístroje všech studentů. To by představovalo mnoho administrativní práce, která by byla neefektivní. Nutnost vedení takové databáze spočívá v tom, že škola má v úmyslu omezit připojení studentům, nikoliv učitelům. Bez databáze by administrátor sítě nebyl schopný detekovat, které zařízení může a které naopak nesmí omezit. Aplikace tedy bude mít vliv na omezení obsahu jen v počítačových učebnách.

Pro bezpečnost aplikace určené pro učitele je nutné zavést taková ošetření konfiguračních souborů, aby byly neoprávněné změny detekovány. Zároveň je nutné ponechat možnost změny konfiguračních souborů. Pro usnadnění práce s aplikací určené učitelům je tedy vhodné vytvořit druhou aplikaci, určenou pro správce sítě. Vzhledem k tomu, že správce sítě má zájem na jednoduché aplikaci umožňující získat základní informace o bezpečnostní bráně a umožnit automatický restart bezpečnostní brány, bude do aplikace jemu určené, přidána funkcionalita podle jeho požadavků.

Zachycení komunikace a funkcí aplikací vzhledem k uživatelům zachycuje diagram na obrázku 7.1, na kterém jsou znázorněny uživatelé a pokyny, které pomocí aplikací předávají bezpečnostní bráně. Například správce sítě pomocí aplikace vytvoří konfigurační soubory pro všechny aplikace, dotáže se brány na její stav (verze firmwaru a vytížení paměti) a nastaví opakované restartování bezpečnostní brány.

7.2 Struktura aplikací

Všechny vytvořené aplikace využívají stejný mechanismus zabezpečení a stejné knihovny třetích stran. V této kapitole jsou společné soubory popsány a je zde definována jejich struktura.



Obrázek 7.1: Diagram použití aplikací vzhledem k uživatelům. Zdroj: vlastní zpracování, 2016

7.2.1 Knihovny

Knihovny třetích stran, které jsou důležité pro správný chod aplikace, zajišťují připojení k SSH serveru a umožňují definovat úlohy v plánovači úloh operačního sytému MS Windows. Všechny knihovny se musí nacházet ve složce s aplikací, aby bylo možné je načíst.

SSH připojení zajišťuje knihovna *SharpSSH*, která se po vyzkoušení několika ostatních knihoven osvědčila a jeví se jako plně funkční. [28] Tato knihovna umožňuje šifrované připojení k SSH serveru a jako jediná z ostatních testovaných knihoven, umožňuje získat text vrácený SSH serverem po zadání příkazu. Navázání spojení se serverem pomocí knihovny *SharpSSH* viz níže.

```
SshConnectionInfo input = Util.GetInput(host, user, pswd);
SshShell ssh = new SshShell(input.Host, input.User);

ssh.Connect();
```

Knihovna *SharpSSH* využívá další knihovny *DiffieHellman* a *Org.Mentalis.Security*, které umožňují zabezpečené připojení. *SharpSSH* je poskytována po licencí BSD, je tedy možné ji s uvedením autora volně užívat.

Knihovna, která umožňuje přístup do plánovače úloh operačního systému MS Windows se nazývá *Microsoft.Win32.TaskScheduler*. [29] Pomocí objektu *TaskDefinition* umožňuje vytvořit opakovaně spouštěnou úlohu.

7.2.2 Konfigurační soubory

Všechny potřebné konfigurační soubory jsou uloženy ve složce *config*. Soubory musí být dostupné při spuštění aplikace, jinak je vypsána hláška o neexistenci konfiguračních souborů.

Soubor s připojovacími údaji

Soubor *connection.txt* obsahuje IP adresu bezpečnostní brány, přihlašovací údaje pro navázání SSH spojení, unikátní název, kterým lze odlišit stanici v předmětu e-mailu, e-mailovou adresu správce sítě, název učebny a heslo, které je požadováno při vstupu do aplikace. E-mailová adresa správce sítě bude sloužit pro odeslání informačního e-mailu po restartu bezpečnostní brány. Název učebny uvedený v souboru musí korespondovat s názvem politiky v bezpečnostní bráně.

Vzhledem k citlivé povaze dat uložených v tomto souboru, je soubor šifrován, aby nemohlo dojít ke kompromitaci dat. Změna souboru *connection.txt* je umožněna aplikací pro administrátora sítě.

Soubor s ověřovanými IP adresami

V souboru *ipaddress.txt* se nachází IP adresy určené pro ověření správné funkcionality sítě po restartu bezpečnostní brány. Soubor není šifrován, je možné jej upravovat pomocí textového editoru.

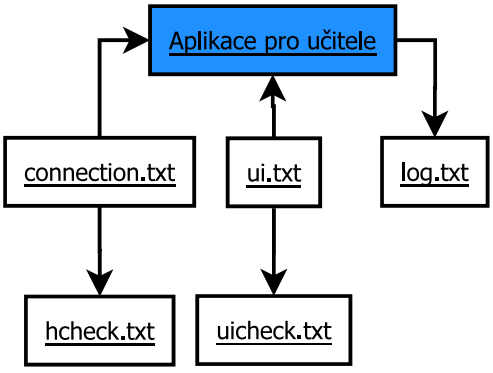
Soubor s definicí uživatelského prostředí

Definice dynamického prostředí aplikace určené pro učitele se nachází v souboru *ui.txt*. Vzhledem k citlivé povaze dat uložených v tomto souboru, je soubor šifrován, aby nemohlo dojít ke kompromitaci dat. Změna souboru *ui.txt* je umožněna aplikací pro administrátora sítě. Struktura tohoto souboru definuje jednotlivá zaškrtávací pole. Definice jednoho zaškrtávací pole viz níže.

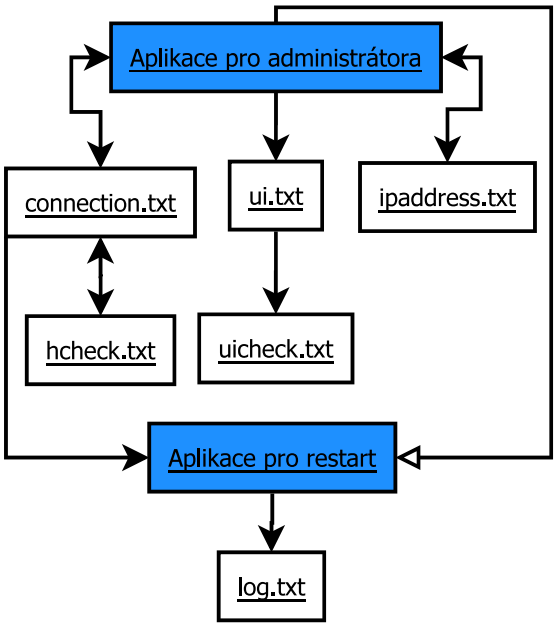
```
#Popis zaškrtávacího pole
@Tooltip nápověda po najetí myší na otazník za zaškrtávacím
   polem
&Fčísla bezpečnostních politik oddělená "-"
```

Soubor s historií událostí

V adresáři *config* se dále nachází soubor *log.txt*, obsahující záznamy o akcích prováděných s aplikacemi. Správce systému má tedy možnost kontrolovat co se za poslední dobu odehrálo a je možné identifikovat případné problémy. Diagramy použitých konfiguračních souborů a jejich vzájemný vliv na aplikace se nachází na obrázcích 7.2 a 7.3.



Obrázek 7.2: Diagram použití konfiguračních souborů u aplikace pro správce sítě



Obrázek 7.3: Diagram použití konfiguračních souborů u aplikace pro správu obsahu

7.2.3 Kontrolní soubory

Aby nemohlo dojít k přepsání konfiguračních souborů, jsou při každém vytvoření konfiguračního souboru generovány otisky těchto souborů pro kontrolu správnosti dat.

Soubor *hcheck.txt* obsahuje hash vztahující se ke konfiguračnímu souboru *connection.txt*. Otisk souboru *ui.txt* se poté nachází v *uicheck.txt*.

7.3 Podpora dalších výrobců

Různí výrobci používají u svých zařízení odlišné příkazy, které bezpečnostní brána akceptuje a vyhodnocuje. Stejný příkaz může vést k odlišným návratovým hodnotám. Kompletní univerzálnost aplikace by tedy znamenala hloubkovou analýzu definovaných příkazů od různých výrobců.

Vzhledem k náročnosti tohoto úkolu je aplikace schopna komunikovat pouze se zařízeními od výrobce ZyXEL, ovšem struktura aplikace umožňuje jednoduché přepsání používaných příkazů. Příručka ZyXEL s příkazy pro příkazovou řádku se nachází na při-

loženém CD, viz příloha C.

7.4 Zajištění bezpečnosti aplikací

Aplikace podporující grafické rozhraní jsou chráněny přístupovým heslem. Konfigurační soubory, obsahující citlivá data, jsou šifrované. Z každého šifrovaného souboru je vytvořen otisk, který ověřuje, zda nebylo do konfiguračních souborů zasaženo.

Veškerá, výše uvedená opatření, jsou druhým stupněm zabezpečení. Všechny aplikace budou uloženy pod zabezpečenými účty na školních počítačích. Přístupové údaje k těmto účtům by měl znát pouze vlastník účtu. Ovšem v případě, že dojde k prozrazení hesla, jsou aplikace dostatečně zabezpečené proti jejich zneužití.

7.5 Požadavky pro běh aplikací

Shrnutí požadavků pro korektní běh aplikací obsahuje tabulka 7.1.

Operační systém	MS Windows od verze 7
Verze .NET	4.5
Místo na pevném disku	10 Mb

Tabulka 7.1: Doporučené požadavky pro správný běh aplikací

8 Aplikace určená pro učitele

Aplikací pro učitele bude dosaženo možnosti základní, jednoduché správy bezpečnostní brány. Učitel bude schopen v počítačové učebně zablokovat studentům zvolenou část datového toku, pomocí spojení aplikace přes SSH protokol s bezpečnostní branou. Aplikace musí být zabezpečena před zcizením a je nutné použít ochranné prvky, které zabrání úmyslným útokům v případě jejího zcizení.

8.1 Popis implementace

V této části je popsána programátorská dokumentace aplikace, určené pro učitele. Nachází se zde popis všech použitých tříd a vybraných funkcí. Na obrázku 8.1 se nachází diagram popisující události při spuštění aplikace.

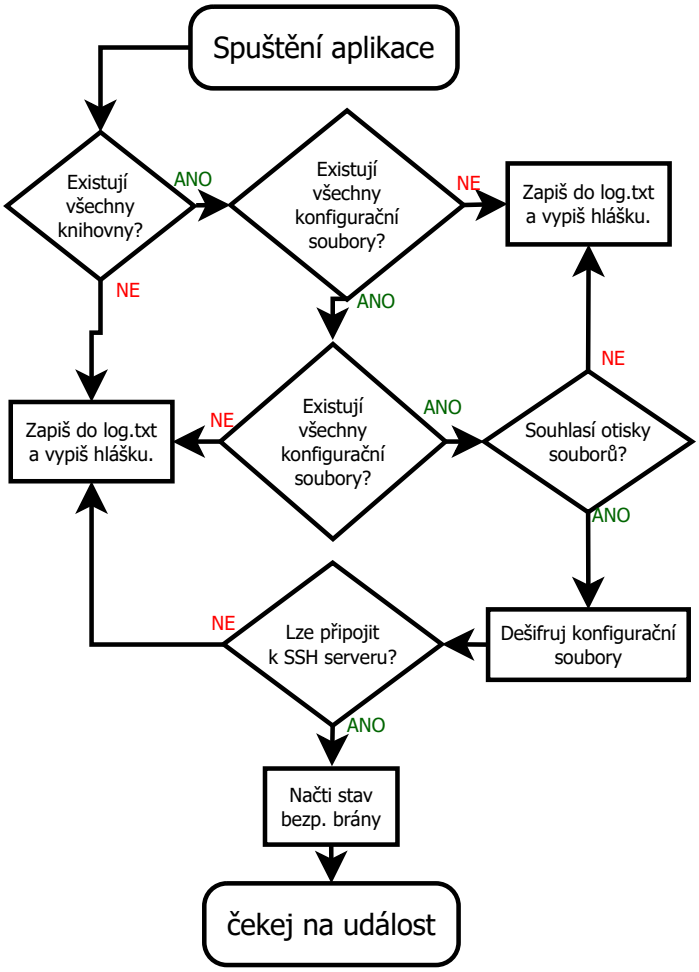
8.1.1 Třída Cipher

Ve třídě *Cipher* se nacházejí funkce určené pro šifrování a dešifrování dat. Všechny funkce v této třídě využívají standardní knihovny pro jazyk C#. Ve třídě se nachází globálně veřejné proměnné *myRijndaelKey* a *myRijndaelIV*, které představují vstupní hodnoty do šifrovacích funkcí.

Vytvoření hashe z celého souboru zajišťuje funkce *HashSHA1*. Funkce vytvoří SHA1 hash, u kterého je možné dále definovat výstupní formát. Vypočtený hash může mít podobu hexadecimálních čísel, oddělených například po trojicích, specifickým znakem.

Další funkcí této třídy je šifrovací funkce *EncryptStr*, která v parametru převezme řetězec a pomocí šifrovacího klíče a inicializačního vektoru řetězec zašifruje. Pro správné uložení šifrovaného textu je nutné jej převést do kódování Base64, které zaručí korektní uložení.

Dešifrovací funkce se nazývá *DecryptStr* a je inverzní k funkcí k *EncryptStr*.



Obrázek 8.1: Diagram procesů při startu aplikace pro správu obsahu

8.1.2 Třída Commands

Třída *Commands* obsahuje funkce, které zajišťují správnou syntaxi příkazů posílaných bezpečnostní bráně. Globální proměnná *desc* vyjadřuje obecný popis politiky pro třídu, které je příkaz určen.

Funkcí *setFirewall* je dosaženo nastavení politik, která jsou uvedena v parametru funkce. Parametr s čísly jednotlivých politik je pole řetězců *numbers*.

Funkce *checkFirewall* zajišťuje inicializační zjištění, které politiky jsou již zapnuté. Tato inicializace probíhá při startu aplikace. Vyhledání stavu politik pro třídu, které je

daný spuštěný program určen, využívá výše zmíněnou proměnnou *desc*.

8.1.3 Třída FormControl

Třída *FormControl* obsluhuje pomocí funkcí ovládání formuláře v aplikaci. Jediný prvek, který má v aplikaci rozhodující funkci je zaškrtávací políčko. Zaškrtávacích políček, může mít formulář několik a první vždy označuje zaškrtnutí všech ostatních.

Funkce *setCheckBoxAction* umožňuje aplikaci chovat se přirozeně a reagovat na různé stavy zaškrtnutých políček.

Voláním funkce *countkCheckboxChecked* lze získat celkový počet zaškrtnutých políček. Tělo funkce viz níže.

```
public static int countCheckboxChecked(CheckBox[] checkBoxes)
{
    int ret = 0;
    for (int i = 0; i < checkBoxes.Length; i++)
        {
            if(checkBoxes[i].IsChecked == true)
            {
                ret += 1;
            }
        }
    return ret;
}
```

Důležitou funkcí třídy *FormControl* je funkce *justDoIt*, která zajišťuje zpracování formuláře, volá potřebné funkce pro připojení k bezpečnostní bráně a pro definici nových politik. V této funkce je zajištěno ošetření stavu, kdy je bezpečnostní brána nedostupná.

8.1.4 Třída GetText

Třída *GetText* obsahuje funkce určené pro parsování textu. Parsování je důležité při získávání zpětné vazby od bezpečnostní brány. Při odeslání požadavku, je u některých příkazů možné získat text definovaný v dokumentaci od výrobce a tím ověřit správnost provedení příkazu.

Mezi vybrané funkce v této třídě patří získání textu mezi dvěma řetězci, získání textu před nebo za určitým řetězcem či získání prvního znaku z určitého řetězce.

8.1.5 Třída CheckBoxAndCommand

V této třídě se nachází pouze objekt *CheckboxAndCommand*, který udržuje informace, které se týkají určitého zaškrtávacího políčka. Jde především o přiřazení, která čísla politik políčko ovlivňuje.

8.1.6 Třída MainWindow

MainWindow definuje akce, které nastanou po nastavené interakci s uživatelem (např. Stiskne-li uživatel tlačítko) v prostředí přihlašovacího okna. K této třídě se pojí třída *MainWindow.xaml*, která definuje uživatelské prostředí přihlašovacího okna.

Vstup do aplikace je implementován porovnáním zadaného hesla s posledním řetězcem v konfiguračním souboru *connection.txt*.

8.1.7 Třída StatusCheck

Funkce ve třídě *StatusCheck* ověřují stav bezpečnostní brány pomocí funkce *checkFirewall* ze třídy *Commands*.

8.1.8 Třída Ui

Třída Ui zajišťuje dynamické chování aplikace, ve smyslu možných změn uživatelského prostředí na základě konfiguračních souborů.

Funkce *prepareCheckBoxes* nejprve načte konfigurační soubor, poté jej parsuje dle definovaných pravidel a pokud dojde k načtení znaků, které aplikace rozezná jako řídící jsou postupně vytvářena zaškrtávací políčka s parametry načtenými z konfiguračního souboru.

8.1.9 Třída Util

Ve třídě Util se nachází funkce použité z dostupné knihovny Tamir.SharpSsh, obsluhující připojení k SSH serveru, v tomto případě SSH připojení k bezpečnostní bráně.

Samotné SSH připojení zajišťuje funkce *SshConnect*. Funkce se na základě přihlašovacích údajů pokusí připojit k SSH serveru. Všechny výjimky jsou ošetřeny tak, aby nedošlo k pádu aplikace. Ověření zda je možné připojit se k určitému zařízení v síti viz tělo funkce *IsAvaible* níže.

```
public static bool IsAvaible(string host)
{
    Ping ping = new Ping();
    PingReply reply;
    string ip = host;
    reply = ping.Send(ip);

    if (reply.Status == IPStatus.Success)
        return true;
    else
        return false;
}
```

Funkcí *doCommand* jsou posílány jednotlivé příkazy bezpečnostní bráně. Na základě

parametrů je složen výsledný příkaz, který je bezpečnostní bráně odeslán a pokud je to žádané, funkce uloží zpětnou vazbu bezpečnostní brány.

8.1.10 Třída WindowContent

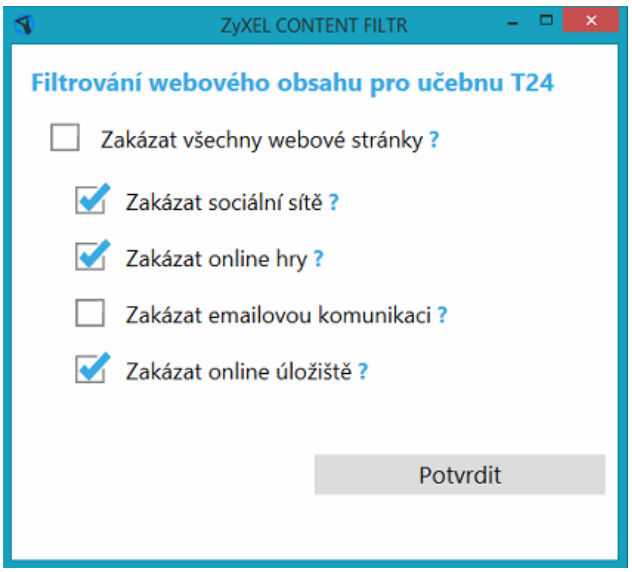
WindowContent definuje akce, které nastanou po nastavené interakci s uživatelem (např. klikne-li uživatel do textového pole) v prostředí hlavního okna. K této třídě se pojí třída *WindowContent.xaml*, která definuje uživatelské prostředí hlavního okna.

Po načtení hlavního okna aplikace je zkontrolována integrita konfiguračních souborů a pro možnost další funkcionality aplikace je ověřováno, zda je možné připojit se k bezpečnostní bráně.

8.2 Popis uživatelského prostředí

Aplikace vytvořená pro potřeby řízení datového toku v počítačových učebnách dbá především na jednoduchost uživatelského prostředí. Všechny krizové stavy jsou ošetřeny chybovými hláškami a uživatel je schopen za pomoci správce sítě diagnostikovat problém. Uživatelské prostředí aplikace je zobrazeno na obrázku 8.2.

Označením zaškrtávacích tlačítek a kliknutím na tlačítko potvrdit se odešle informace bezpečnostní bráně. Pro změnu pravidel je nutné nejprve povolit předchozí nastavení a až poté je možné vybrat nové. Instalační a uživatelská příručka se nachází v příloze B.



Obrázek 8.2: Uživatelské prostředí aplikace pro správu obsahu. Zdroj: vlastní zpracování, 2015

9 Aplikace určená pro administrátora sítě

Aplikace určená pro administrátora sítě si klade za cíl pomoci se základní diagnostikou a správou bezpečnostní brány. Její funkce mohou být různorodé, založené především na potřebách správce sítě. I když se jedná o aplikaci určenou pro znalého a poučeného správce, je stále nutné myslet na bezpečnost jejího řešení. Aplikace bude mimo jiné administrátorovi sloužit pro konfiguraci programu určeného pro učitele.

9.1 Popis implementace

V této části je popsána programátorská dokumentace aplikace, která má zjednodušit správu bezpečnostní brány správci sítě. Nachází se zde popis všech použitých tříd a vybraných funkcí.

9.1.1 Třída Cipher

Ve třídě *Cipher* se nacházejí funkce určené pro šifrování a dešifrování dat. Třída je blíže popsána v části 8.1.1.

9.1.2 Třída GetText

Třída *GetText* obsahuje funkce určené pro parsování textu. Třída je blíže popsána v části 8.1.4.

9.1.3 Třída MainWindow

Ve třídě *MainWindow* jsou funkce, které obsluhují události po interakci uživatele v přihlašovacím okně aplikace. K této třídě se pojí třída *MainWindow.xaml*, která definuje uživatelské prostředí přihlašovacího okna. Vstup do aplikace je implementován porovnáním zadaného hesla s posledním řetězcem v konfiguračním souboru *connection.txt*.

Funkce *passwd_KeyDown* reaguje na stisk tlačítka enter v textovém poli pro zadání hesla. Pokud je tlačítko enter stisknuto, funkce zavolá evaluaci, zda je heslo správné, či ne. Tělo funkce viz níže.

```
private void passwd_KeyDown(object sender, KeyEventArgs e)
{
    if (e.Key == Key.Return)
    {
                Authorization(passwd);
    }
}
```

9.1.4 Třída SetIPWindow

Tato třída obsluhuje události vykonané uživatelem v okně pro zadání IP adres. Pokud uživatel zadané IP adresy uloží, vznikne textový soubor, který je načítán aplikací pro restart bezpečnostní brány a použit pro ping uložených IP adres po restartu.

9.1.5 Třída StatusWindow

Pokud správce sítě vyvolá akci pro zobrazení informací o bezpečnostní bráně, je zobrazeno okno *StatusWindow*. Třída *StatusWindow* definuje události, které obsluhují funkce uvnitř třídy.

9.1.6 Třída Util

Ve třídě *Util* se nachází funkce použité z dostupné knihovny Tamir.SharpSsh, obsluhující připojení k SSH serveru, v tomto případě SSH připojení k bezpečnostní bráně. Třída *Util* je blíže popsána v části 8.1.9.

9.1.7 Třída WindowContent

Třída *WindowContent* obsluhuje události v hlavním okně aplikace. Jsou zde funkce umožňující ovládání aplikace a funkce umožňující splnit funkcionalitu události. K této třídě se pojí třída *WindowContent.xaml*, která definuje uživatelské prostředí hlavního okna.

Po načtení hlavního okna aplikace je zkontrolována integrita konfiguračních souborů, pokud jsou soubory v pořádku aplikace je spuštěna.

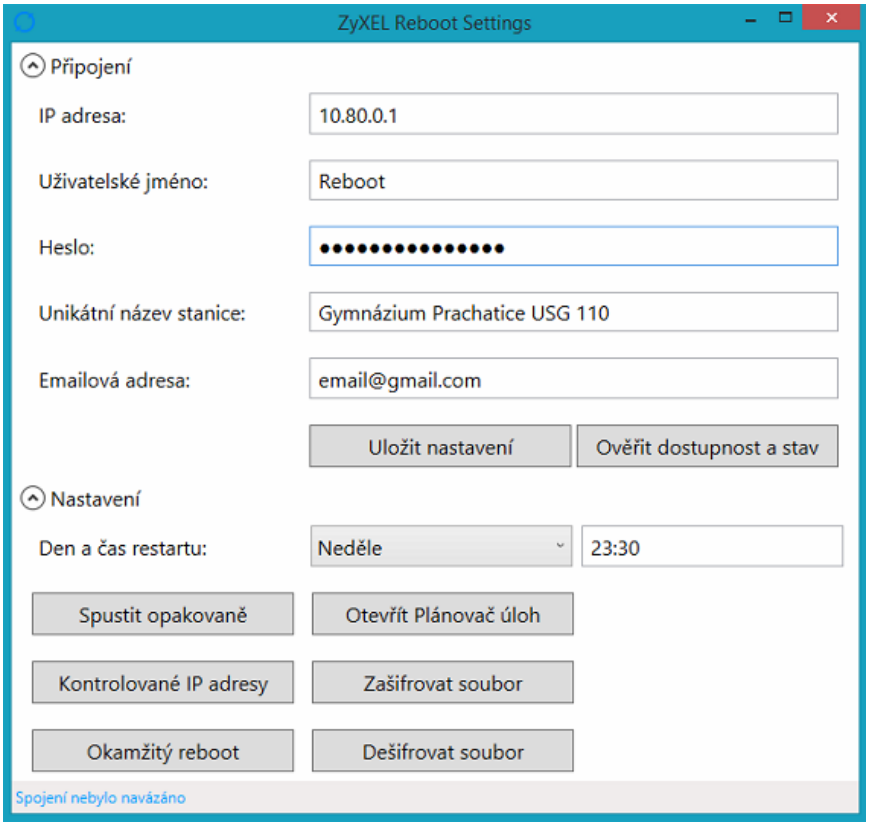
Funkce *update_Statement* se spojí s bezpečnostní branou a získá informace o firmwaru, sériové číslo zařízení, barvu LED kontrolky (signalizace stavu) a vytížení paměti bezpečnostní brány. Volání funkce ze třídy Util, pro odeslání příkazu zařízení viz níže.

```
Util.doCommand(ssh, true, false, "show version", false);
```

Funkce obsluhující stisknutí tlačítka pro nastavení opakovaného restartu bezpečnostní brány *paramReset_Button_Click* ukládá záznam do plánovače úloh operačního systému MS Windows.

9.2 Popis uživatelského prostředí

Vzhledem k tomu, že cílovým uživatelem této aplikace je správce sítě, rozložení uživatelského prostředí odpovídá jeho požadavkům. Všechny krizové stavy jsou ošetřeny chybovými hláškami a správce je schopen diagnostikovat daný problém. Uživatelské prostředí aplikace je zobrazeno na obrázku 9.1. Instalační a uživatelská příručka se nachází na přiloženém CD, viz příloha C.



Obrázek 9.1: Uživatelské prostředí aplikace pro správce sítě. Zdroj: vlastní zpracování, 2015

10 Aplikace pro restart bezpečnostní brány

Aplikací restartování bezpečnostní brány je dosaženo splnění požadavku správce sítě na tuto funkcionalitu. Opakovaný restart bude umožněn definicí v plánovači úloh na zabezpečeném školním serveru. Na rozdíl od předchozích dvou aplikací, je tato aplikace pouze konzolová.

10.1 Popis implementace

V této části je popsána programátorská dokumentace aplikace, vykonávající restart bezpečnostní brány. Nachází se zde popis všech použitých tříd a vybraných funkcí.

10.1.1 Třída Cipher

Ve třídě *Cipher* se nacházejí funkce určené pro šifrování a dešifrování dat. Třída je blíže popsána v části 8.1.1.

10.1.2 Třída Email

Ve třídě *Email* se nachází jediná funkce *sendEmail*, která odesílá e-mail po proběhnutí restartu. E-mail je odeslán pod e-mailovým účtem založeným pouze pro tyto účely. Příjemce e-mailu je definován v konfiguračních souborech aplikace. Odeslaný e-mail slouží jako informační zpráva, předmět odeslaného e-mailu tvoří název zařízení (definovaný správcem sítě v konfiguračních souborech) a tělo e-mailu obsahuje text o stavu sítě po restartu bezpečnostní brány. Funkce *sendEmail* využívá příkazy ze standardní knihovny *System.Net.Mail*.

10.1.3 Třída GetText

Třída *GetText* obsahuje funkce určené pro parsování textu. Třída je blíže popsána v části 8.1.4.

10.1.4 Třída Program

Hlavní funkce *Main* obsluhuje celou rutinu restartu bezpečnostní brány. Při spuštění načte konfigurační soubory, odešle příkaz „reboot“ a počká 10 minut. Poté se pokouší o ping IP adres definovaných správcem sítě a vyhodnocení ukládá do logovacího souboru a odesílá e-mailem.

10.1.5 Třída Util

Ve třídě *Util* se nachází funkce použité z dostupné knihovny Tamir.SharpSsh, obsluhující připojení k SSH serveru, v tomto případě SSH připojení k bezpečnostní bráně. Třída *Util* je blíže popsána v části 8.1.9.

10.2 Popis uživatelského prostředí

Aplikace vykonávající restart bude automaticky pouštěna plánovačem úloh operačního systému na školním serveru. Z důvodu nízké potřeby interakce uživatele s aplikací, je rozhraní aplikace pouze konzolové. Instalační a uživatelská příručka se nachází na přiloženém CD, viz příloha C.

11 Testování

Kapitola je věnována testování provedených změn a vytvořených aplikací. Testy jsou vztažené k bezpečnosti a k výhodám získaným touto prací.

V průběhu vývoje aplikací byla aplikace testována nejprve v testovacím prostředí na dvou různých zařízeních (ZyXEL USG 50 a USG 40W). Po odladění všech chyb byly aplikace nainstalovány v reálném provozu na gymnáziu.

11.1 Testování sítě vzhledem k provedeným změnám

V rámci testování změn v síťové topologii byl proveden test zabezpečení wifi a byla změřena propustnost sítě.

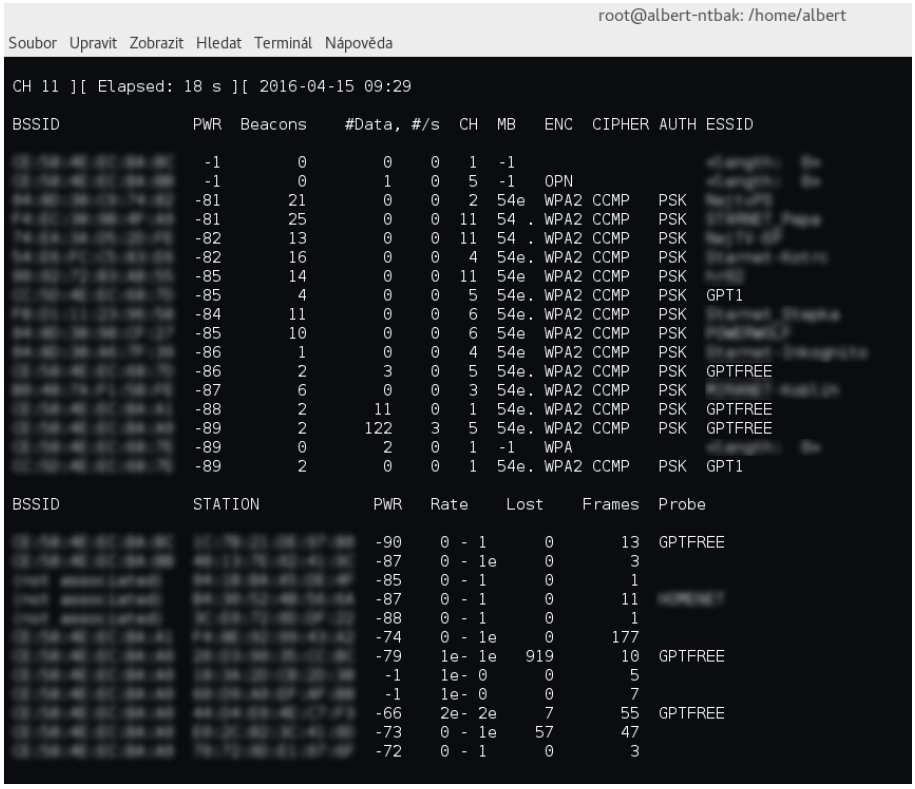
11.1.1 Test 1 - ověření zabezpečení wifi

K ověření správného zabezpečení wifi sítě byla vybrána metodika bezpečnostního testu. Byla využita volně dostupná Linuxová distribuce Kali Linux s předinstalovanými aplikacemi pro penetrační testování sítí.

V tomto případě byl konkrétně použit program airmon-ng, který zapne wifi kartu počítače do monitorovacího módu (karta naslouchá i signál určený někomu jinému) a tím pádem odposlouchává okolní bezdrátové přenosy dat. Sledování takto odkrytého síťového provozu je zobrazeno na obrázku 11.1, na kterém jsou rozmazány názvy ostatních sítí.

Aplikace airmon-ng poté odchytává a ukládá pakety při kterých dojde k výměně bezpečnostních dat mezi uživatelem a bezdrátovým access pointem. Z uložených paketů je potom možné, pomocí slovníkového útoku, získat přístupové údaje k bezdrátovému připojení.

Celý proces penetračního testu, za pomoci aplikace airmon-ng [30], byl proveden a nepodařilo se prolomit wifi zabezpečení. Neúspěch je dán šifrováním WPA2 v kombinaci se



Obrázek 11.1: Sledování veškerého bezdrátového provozu v dosahu síťové karty

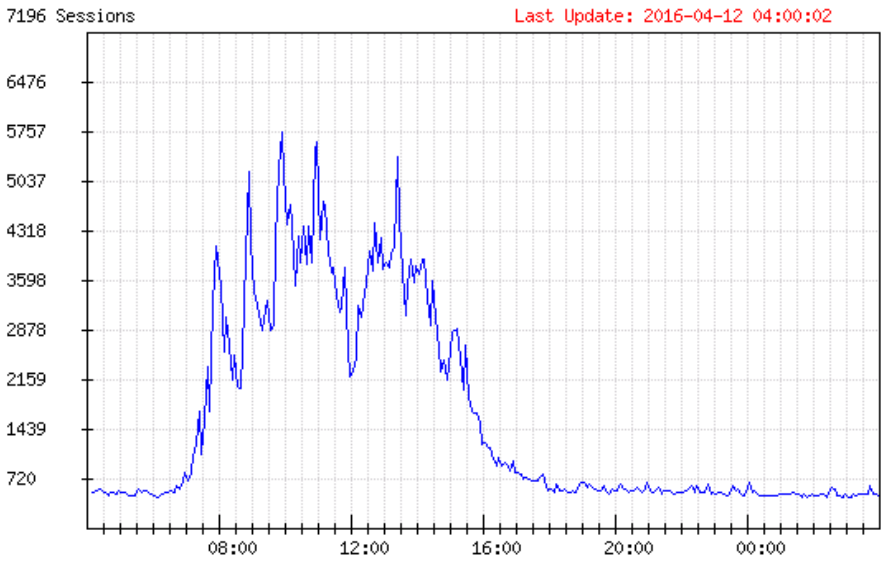
silným heslem, které se nenachází v žádném ze slovníků, učených pro slovníkové testy.

11.1.2 Test 2 - Propustnost sítě

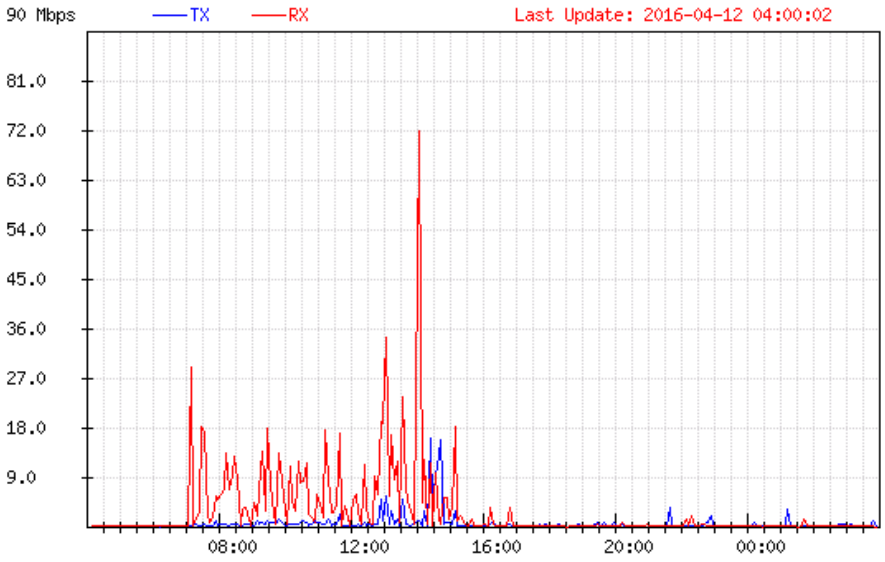
Test byl uskutečněn při plném provozu, aby nedošlo ke zkreslení hodnot. Graf na obrázku 11.2 zobrazuje vytížení sítě, graf na obrázku 11.3 vystihuje přenosové rychlosti na WAN portu. Z grafů je možné pozorovat vyšší přenosové rychlosti než jsou maximální možné hodnoty původní bezpečnostní brány.

11.2 Testování aplikací

Testování aplikací je důležitý proces, kterým je možné odhalit neošetřené stavy. Byly zvoleny tři testy, které ověřily, že aplikace je dobře ošetřená vůči krizovým stavům.



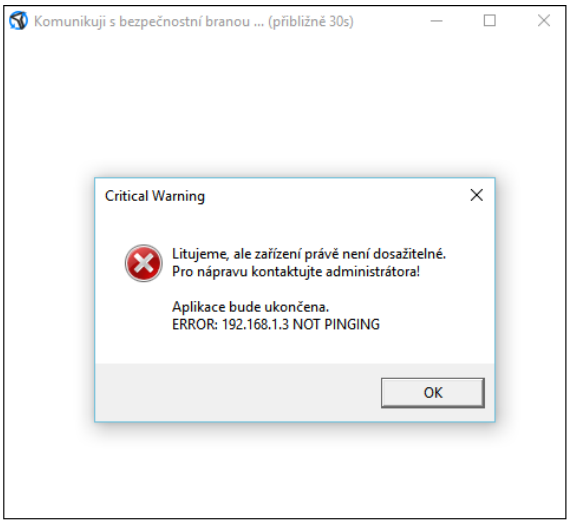
Obrázek 11.2: Vytížení bezpečnostní brány v čase



Obrázek 11.3: Přenosová rychlost na WAN portu bezpečnostní brány

11.2.1 Test 1 - nedostupnost bezpečnostní brány

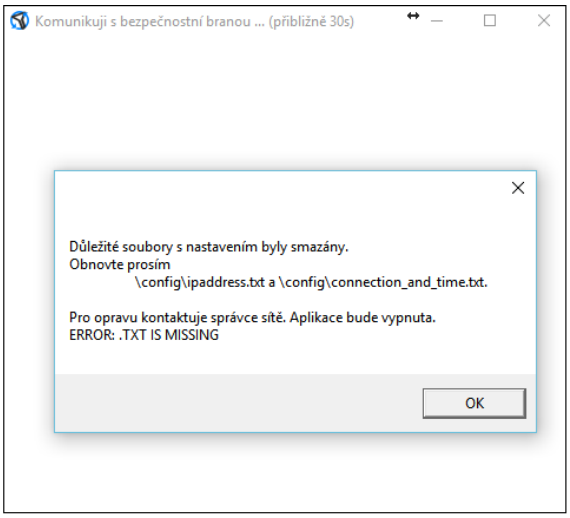
Test byl proveden odpojením bezpečnostní brány od počítačové sítě a následným zapnutím aplikace. bylo ověřeno, že aplikace se chová standardně tato výjimka je ošetřena. Viz obrázek 11.4.



Obrázek 11.4: Test nedostupnosti bezpečnostní brány - stav po zapnutí aplikace ZyCONTENT

11.2.2 Test 2 - chybějící konfigurační soubory

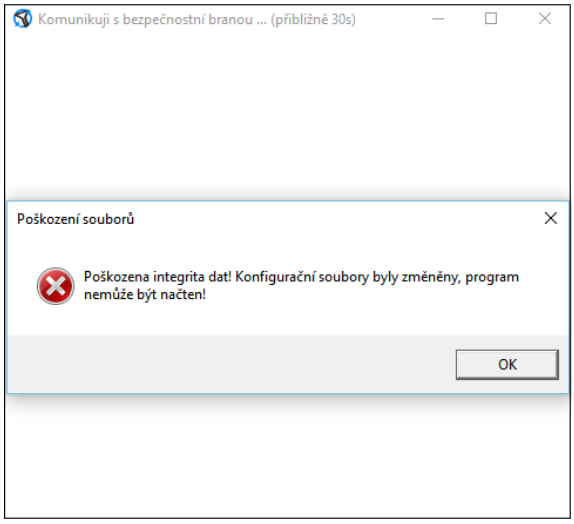
Test byl proveden smazáním souboru connection.txt, který je načítán při startu aplikace. Bylo ověřeno, že aplikace se chová standardně tato výjimka je ošetřena. Viz obrázek 11.5.



Obrázek 11.5: Test chybějících konfiguračních souborů - stav po zapnutí aplikace ZyCONTENT

11.2.3 Test 3 - pokus o přepsání konfiguračního souboru

Test byl proveden změnou řádků v souboru connection.txt a následným spuštěním aplikace. Bylo ověřeno, že aplikace se chová standardně tato výjimka je ošetřena. Viz obrázek 11.6.

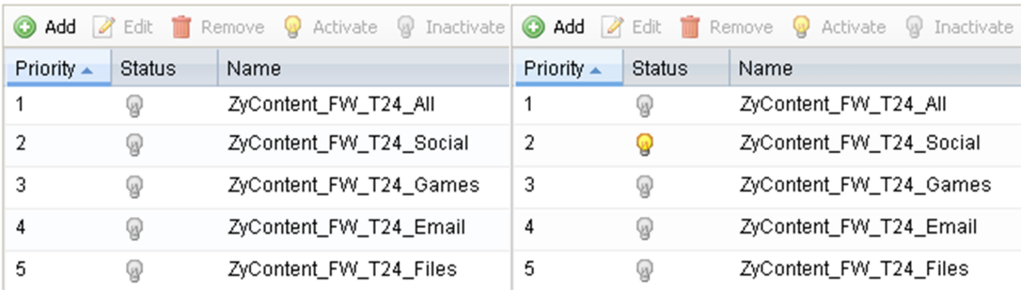


Obrázek 11.6: Test přepsání konfiguračních souborů - stav po zapnutí aplikace ZyCONTENT

11.2.4 Test 4 - pokus o zablokování konkrétní stránky v konkrétní třídě

Test byl proveden použitím aplikace pro správu obsahu, určené pro učitele. Ve třídě T24 byly z učitelského počítače zakázány sociální sítě (facebook.com, twitter.com, apod.). Následně byla ověřena konektivita známých sociálních sítí u učitelského a u studentského počítače.

Výsledek potvrdil správné fungování aplikace - na učitelské PC neměla změna vliv, studentský počítač měl přístup na známé sociální sítě zablokovaný. Obrázek 11.7 znázorňuje stav bezpečnostní brány před potvrzením nastavení v aplikaci (pravidlo je vypnuté) a po potvrzení (pravidlo je zapnuté).



Obrázek 11.7: Test zablokování sociálních sítí - vypnuté / zapnuté pravidlo bezpečnostní brány

11.3 Vyhodnocení testů

Testování změn, provedených v rámci síťové topologie, ukázalo bezpečnost aplikovaného řešení v oblasti bezdrátového připojení k síti a také potvrdilo vhodný výběr bezpečnostní brány. Nová bezpečnostní brána prokazuje vyšší propustnost, než byla maximální propustnost jejího předchůdce.

Testy aplikací prokázaly, že aplikace je odolná vůči smazání konfiguračních souborů i proti úmyslnému přepsání jejich obsahu. Dále byla ověřena správná funkcionalita aplikací. Aplikace svojí funkčnost prokázaly, lze je tedy považovat za bezpečné a stabilní.

12 Zhodnocení přínosu realizovaných vylepšení

Kapitola se věnuje přínosu vylepšení, které tato práce přinesla. Přínos lze definovat jako splnění zadání od vedení gymnázia a od externího vedoucího.

12.1 Přínos změn v topologii sítě

Požadavky a jejich splnění jsou přehledně popsány v tabulce 12.1. Všechny požadavky byly splněny a byly průběžně konzultovány s vedením gymnázia i s externím vedoucím této práce. Díky tomu mohlo dojít k oboustranné spokojenosti a k dotažení celého projektu.

Po implementaci všech úprav došlo, dle vedení gymnázia, ke snížení stížností na funkcionalitu sítě. Tento fakt potvrzuje menší frekvence hlášení závad v síti gymnázia externímu vedoucímu práce.

Funkcionalita	Původně	Po úpravách
Zvýšení propustnosti sítě	220Mb	1 500Mb
Zabezpečení konkrétních síťových prvků	Možnost prvky odpojit od sítě	Všechny síťové prvky přiměřeně zabezpečeny vůči odpojování potřebných kabelů.
Vytvoření aplikace pro správu síťového obsahu	Nemožnost jednoduché správy.	Funkční aplikace umožňující jednoduchou správu.
Vytvoření topologického schématu	Topologii znalo jen několik lidí, nebyla sepsána.	Topologické schéma je zakresleno a je možné z něj vycházet.

Tabulka 12.1: Zhodnocení dodržení požadavků, Zdroj: Vlastní zpracování

12.2 Přínos aplikací

S ohledem na fakt, že původně nebyla ve škole téměř žádná možnost správy obsahu, je aplikace pro školu velikým přínosem. V aplikaci je implementováno ověřování provedených akcí a uživatel tak má neustálý přehled o tom zda je vše v pořádku.

Aplikace pro administrátora sítě umožňuje bezproblémové nastavení aplikace pro správu obsahu a jsou v ní implementovány další podpůrné funkce. Rychlé zobrazení stavu bezpečnostní brány, či automatický restart bezpečnostní brány jsou funkce, který není výrobcem jednoduše implementován.

12.3 Možná rozšíření

Dalších možností v úpravách síťové topologie je mnoho. Mezi doporučené kroky do budoucna patří vedení databáze osobních počítačů a chytrých telefonů studentů a širší pokrytí školy wifi signálem. Databáze studentských strojů by umožnila větší bezpečnost a transparentnost síťového provozu. Širší pokrytí wifi signálem by bylo, vzhledem k počtu lidí, příznivou změnou, avšak je důležité dbát na ekonomické faktory.

Vytvořené aplikace by mohly načítat konfigurační soubory ze sdíleného diskového prostoru na serveru. Aplikacím by byla přidána funkce na rozpoznání síťového jména počítače a všechny aplikace by pak mohly načítat stejné konfigurační soubory.

Administrátorská aplikace by mohla být rozšířena o větší množství diagnostických funkcí a mohla by být upravena do vzhledu tzv. kokpitu. Kokpit by zobrazoval důležitá upozornění, formou grafů a barev by informoval správce sítě o stavu sítě.

Pokud by byla vedena databáze studentských osobních počítačů, bylo by možné aplikaci rozšířit tak, že by bylo možné omezovat jejich datový tok, aplikací pro správu bezpečnostní brány. Aplikaci by tak byly umožněny širší možnosti.

13 Závěr

Tato bakalářská práce se zabývala modernizací školní počítačové sítě budovy Gymnázia v Prachaticích. Činnosti provedené v rámci modernizace můžeme rozdělit do tří celků a sice vytvoření topologického schématu sítě, úpravy v síťové topologii vztažené k požadavkům gymnázia a vytvoření aplikace pro správu bezpečnostní brány.

Topologické schéma bylo vytvořeno na základě osobní prohlídky budovy a zakreslení pozice síťových prvků. Schéma zjednodušuje orientaci při dalších síťových úpravách v budově školy. Schéma bylo poskytnuto gymnáziu v elektronické podobě a je tedy možné jej aktualizovat.

Úpravy síťové topologie se týkaly výběru výkonnějšího modelu bezpečnostní brány, dále byl rozšířen bezdrátový signál pomocí nových bezdrátových access pointů, které lze centrálně spravovat a byla identifikována všechna potencionálně nezabezpečená místa v síti, která byla posléze zabezpečena. Požadavky gymnázia na funkce nové bezpečnostní brány byly splněny, signál byl rozšířen a síťové prvky jsou nyní bezpečně uloženy.

Vzhledem k požadavkům učitelů, mít kontrolu nad tím, jaké internetové stránky studenti prohlížejí, byla vytvořena aplikace pro správu datového toku. Pro správce sítě byla vytvořena aplikace usnadňující základní diagnostiku bezpečnostní brány. Aplikace komunikují s nově nasazenou bezpečnostní branou a je možné ji modifikovat pro různé výrobce bezpečnostních bran. Vytvořené aplikace splňují požadavek jednoduché správy bezpečnostní brány a dbají na jednoduché uživatelské prostředí. Pro aplikace byl vytvořen uživatelský manuál.

Provedené změny a vytvořené aplikace byly otestovány přímo v gymnáziu. Při testování bylo dbáno především na funkčnost a bezpečnost celého řešení.

Všechny cíle práce byly naplněny. Myslím si, že celkový výstup této práce přinesl gymnáziu mnohé výhody a rozšířil možnosti správy síťové infrastruktury. Tento názor je potvrzen vedením gymnázia školy, které zaznamenalo menší množství síťových výpadků. Učitelé i správce sítě již využívají vytvořené aplikace a jsou spokojeni s jejich funkcionalitou.

Seznam zkratek

AP Access point, bezdrátový přístupový bod

BYOD Bring your own device

IDF Intermediate Distribution Frames

IDP Intrusion Detection and Prevention systems

IP Internet Protocol

IT Informační technologie

MDF Main Distribution Frame

MS Microsoft

NAT Network Address Translation

OS Operační systém

PoE Power over Ethernet

RJ45 Koncovka pro ethernetový kabel

SCP Secure Copy Protocol

SFTP SSH File Transfer Protocol

SSH Secure Shell

SSID Service Set Identifier - identifikátor bezdrátové sítě wifi

TCP Transmission Control Protocol

UTM Unified threat management

VPN Virtual private network

WEP Wired Equivalent Privacy

WPA Wifi Protected Access

Literatura

[1] Petr Odvárka. Ethernet, 2015. [online][cit. 2015-11-21] Dostupné z http://www.svetsiti.cz/clanek.asp?cid=Ethernet-1992000.

[2] D. B. Chapman and E. D. Zwicky. *Principy budování a udržování - Firewally*. Computer Press, 1998, ISBN 80-7226-051-0.

[3] Kaspersky. Cyberthreat real-time map, 2015. [online][cit. 2015-10-06] Dostupné z https://cybermap.kaspersky.com/stats/.

[4] Ladinn. Základy strukturované kabeláže, 2015. [online][cit. 2016-01-12] Dostupné z http://www.ladinn.cz/ostatni/technika/SKS.html.

[5] Showme cables. Rj45, 2015. [online][cit. 2016-01-12] Dostupné z http://blog.showmecables.com/rj45-pinout/.

[6] IT Biz. Letmý ponor do historie wifi sítí., 2013. [online][cit. 2016-03-06] Dostupné z http://www.itbiz.cz/clanky/letmy-ponor-do-historie-wi-fi-siti.

[7] Jiří Peterka. Firewall, 1995. [online][cit. 2015-10-11] Dostupné z http://www.earchiv.cz/a95/a505k130.php3.

[8] Computerworld. Kam směřují firewally, 2015. [online][cit. 2015-10-11] Dostupné z http://computerworld.cz/securityworld/kam-smeruji-firewally-51925.

[9] Samuraj. Začínáme s monitoringem sítě, 2009. [online][cit. 2015-10-11] Dostupné z http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/.

[10] Microsoft. Co je vpn?, 2015. [online][cit. 2015-10-06] Dostupné z https://technet.microsoft.com/cs-cz/library/cc731954(v=ws.10).aspx.

[11] Busines dictionary. Home office, 2015. [online][cit. 2015-10-06] Dostupné z http://www.businessdictionary.com/definition/home-office.html.

[12] DSL.cz. Jak na ssh, 2015. [online][cit. 2015-09-10] Dostupné z ttp://www.dsl.cz/jak-na-to/jak-na-ssh.

[13] Zyxel. Zyxel nwa3560, 2014. [online][cit. 2015-12-14] Dostupné z http://shop.zyxel.cz/1428-karta-zyxel-nwa3560-n.html.

[14] Samuraj. Co je to vlan, 2007. [online][cit. 2016-02-13] Dostupné z http://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/.

[15] ABC Linuxu. Nat, 2006. [online][cit. 2016-03-04] Dostupné z http://www.abclinuxu.cz/slovnik/nat.

[16] Clever and smart. Byod: bezpečnostní politika, 2012. [online][cit. 2015-11-22] Dostupné z http://www.cleverandsmart.cz/byod-bezpecnostni-politika/.

[17] Anect. Do byodu, 2016. [online][cit. 2015-11-22] Dostupné z http://www.anect.com/cz/5-kroku-k-byod/.

[18] Bob Hayes and Kathleen Kotwica. *Bring Your Own Device (BYOD) to Work*. Elsevier, 2013, ISBN 978-0-12-411592-7.

[19] Christof Paar and Jan Pelzl. *Understanding Cryptography*. Springer, 2010, ISBN 978-3-642-04100-6.

[20] Jan Staudek Petr Hanáček. *Bezpečnost informačních systémů*. Úřad pro státní informační systém, 2000, ISBN 80-238-5400-3.

[21] Svět sítí. Základní slovníček z kryptografie, 2002. [online][cit. 2016-03-04] Dostupné z http://www.svetsiti.cz/clanek.asp?cid=Zakladni-slovnicek-z-kryptografie-1-2942002.

[22] Jiří Peterka. Pop, 1996. [online] Dostupné z http://www.earchiv.cz/a96/a634k130.php3.

[23] Svět sítí. Optický kabel pro páteřní (vertikální) rozvody, 2001. [online][cit. 2016-02-13] Dostupné z http://www.svetsiti.cz/clanek.asp?cid=Opticky-kabel-pro-paterni-vertikalni-rozvody-1052001.

[24] Zyxel. Usg 200/100-plus/100/50/20w/20, 2015. [online][cit. 2015-08-10] Dostupné z http://www.zyxel.com/cz/cs/products_services/usg_200_100_plus_100_50_20w_20.shtml?t=p.

[25] Tutorials Point. C# overview, 2015. [online][cit. 2015-09-01] Dostupné z http://www.tutorialspoint.com/csharp/csharp_overview.htm.

[26] Null byte. Multiplatformní aplikace v c#, 2015. [online][cit. 2015-09-02] Dostupné z http://www.itnetwork.cz/csharp/pokrocile/c-sharp-mono-aplikace-na-linuxu/.

[27] IT network. Úvod do wpf, 2015. [online][cit. 2015-09-01] Dostupné z http://www.itnetwork.cz/csharp/wpf/c-sharp-tutorial-wpf-uvod-a-prvni-formularova-aplikace/.

[28] Tamir Gal. Sharpssh - a secure shell (ssh) library for .net, 2008. [online][cit. 2015-09-01] Dostupné z http://www.tamirgal.com/blog/page/sharpssh.aspx.

[29] Code Plex. Task scheduler managed wrapper, 2015. [online][cit. 2015-09-01] Dostupné z https://taskscheduler.codeplex.com/.

[30] Null byte. How to hack wi-fi, 2015. [online][cit. 2016-04-05] Dostupné z http://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/.

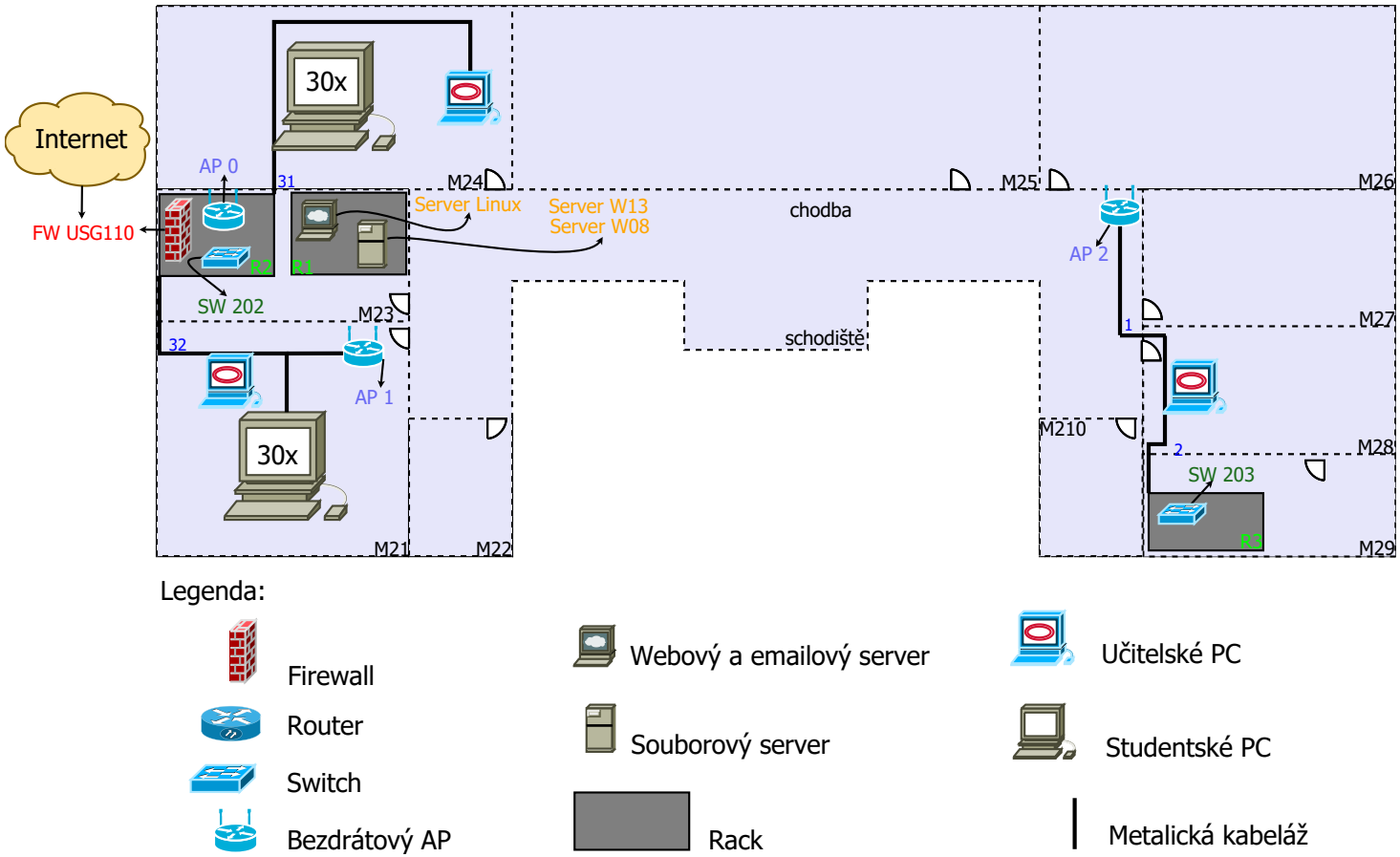
Seznam obrázků

Seznam tabulek

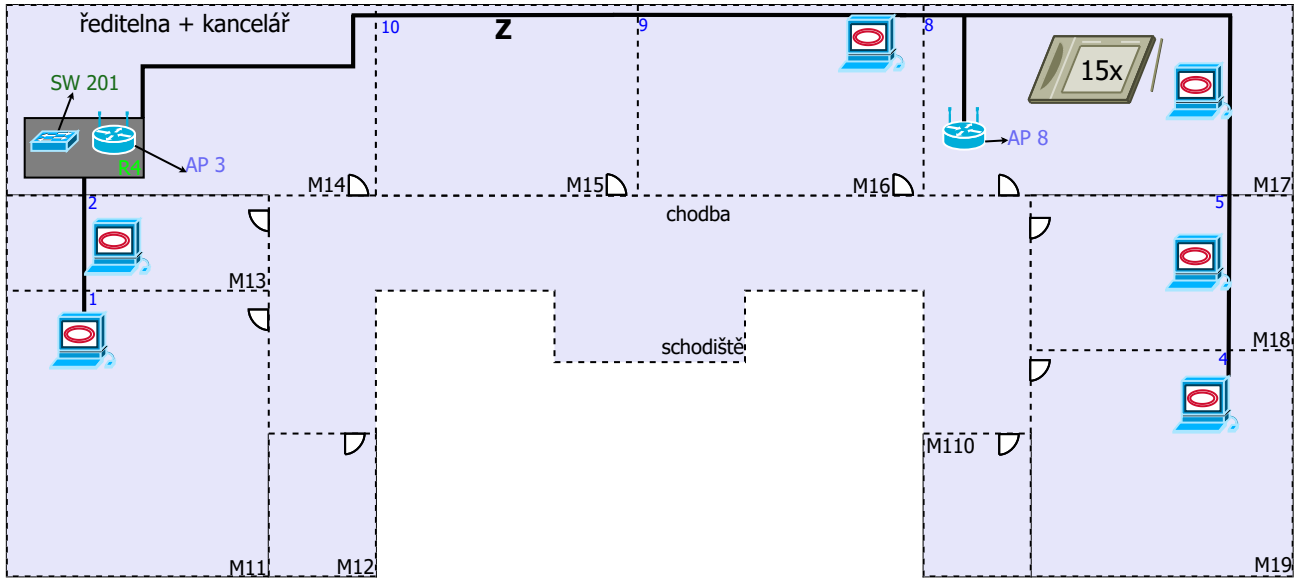
Seznam příloh

A Schéma sítě

A.1 Schéma sítě ve druhém patře.



A.2 Schéma sítě v prvním patře.



Legenda:

Switch

Učitelské PC

Z Zakončení kabelu

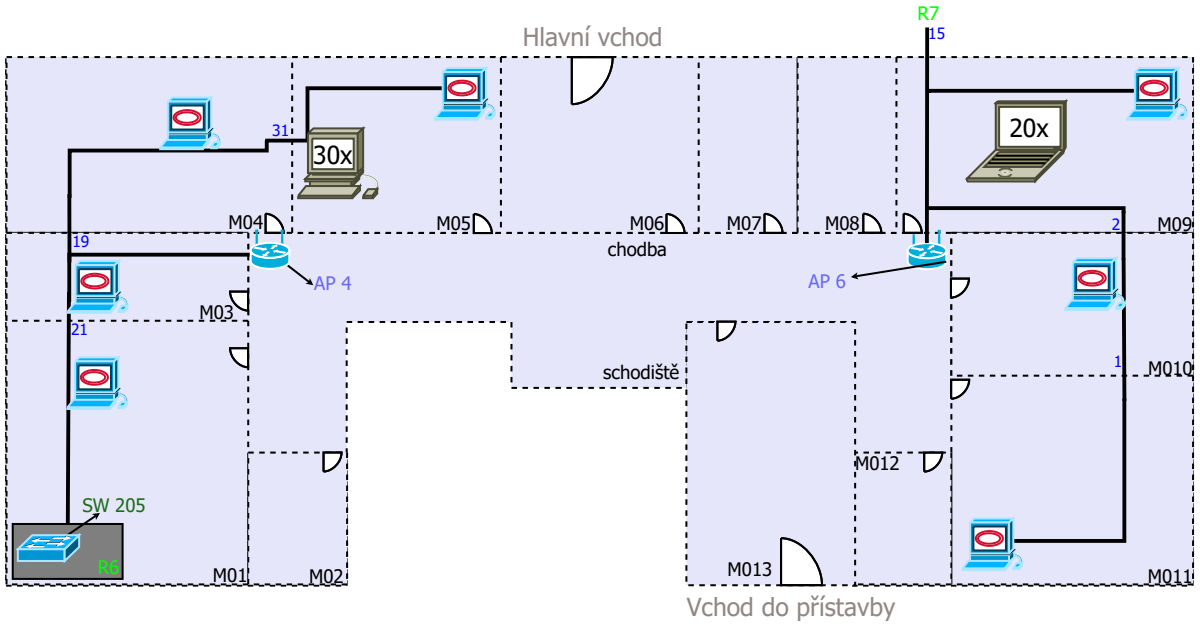
Bezdrátový AP

Tablet

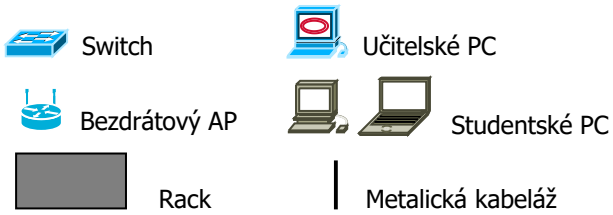
Rack

Metalická kabeláž

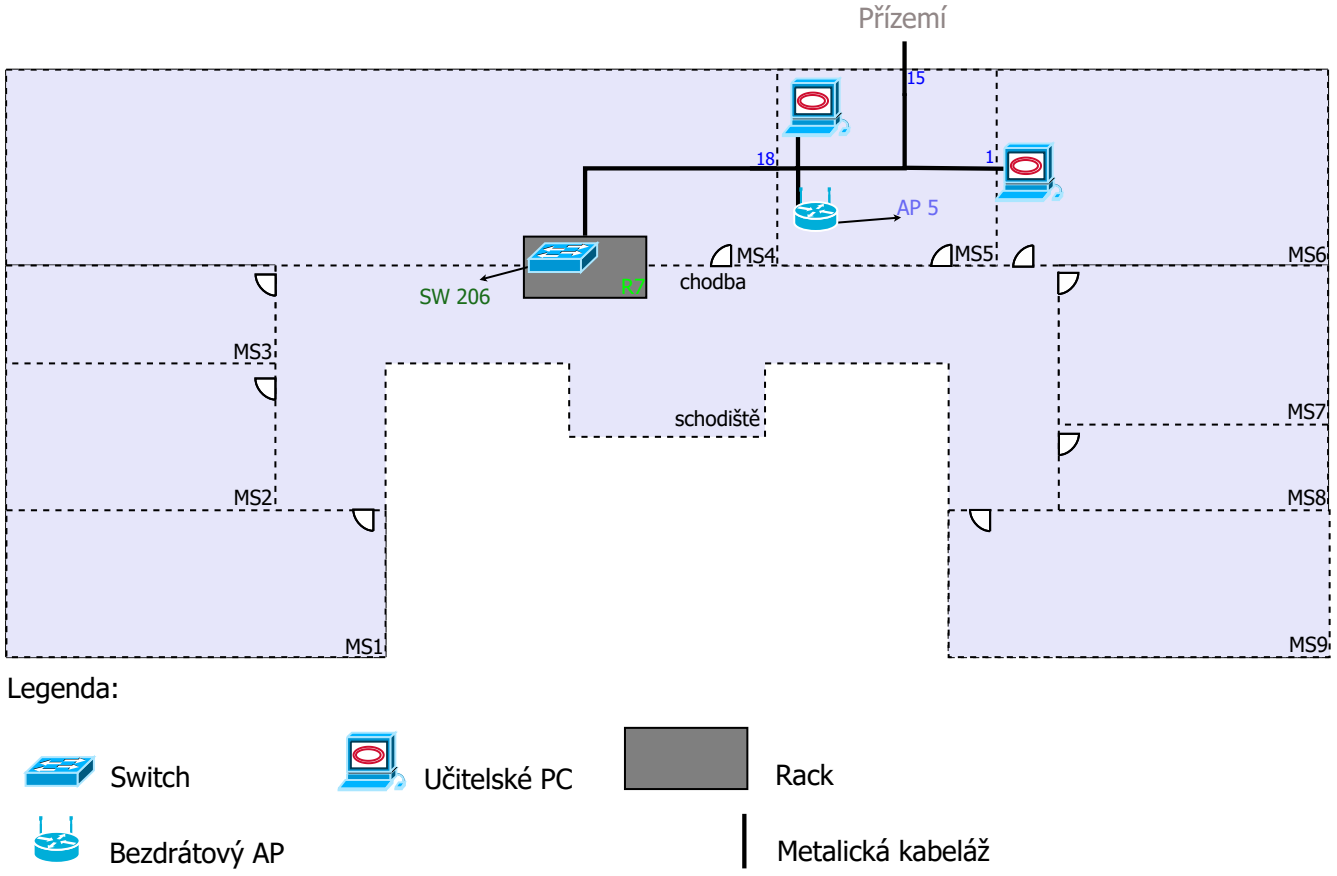
A.3 Schéma sítě v přízemí.



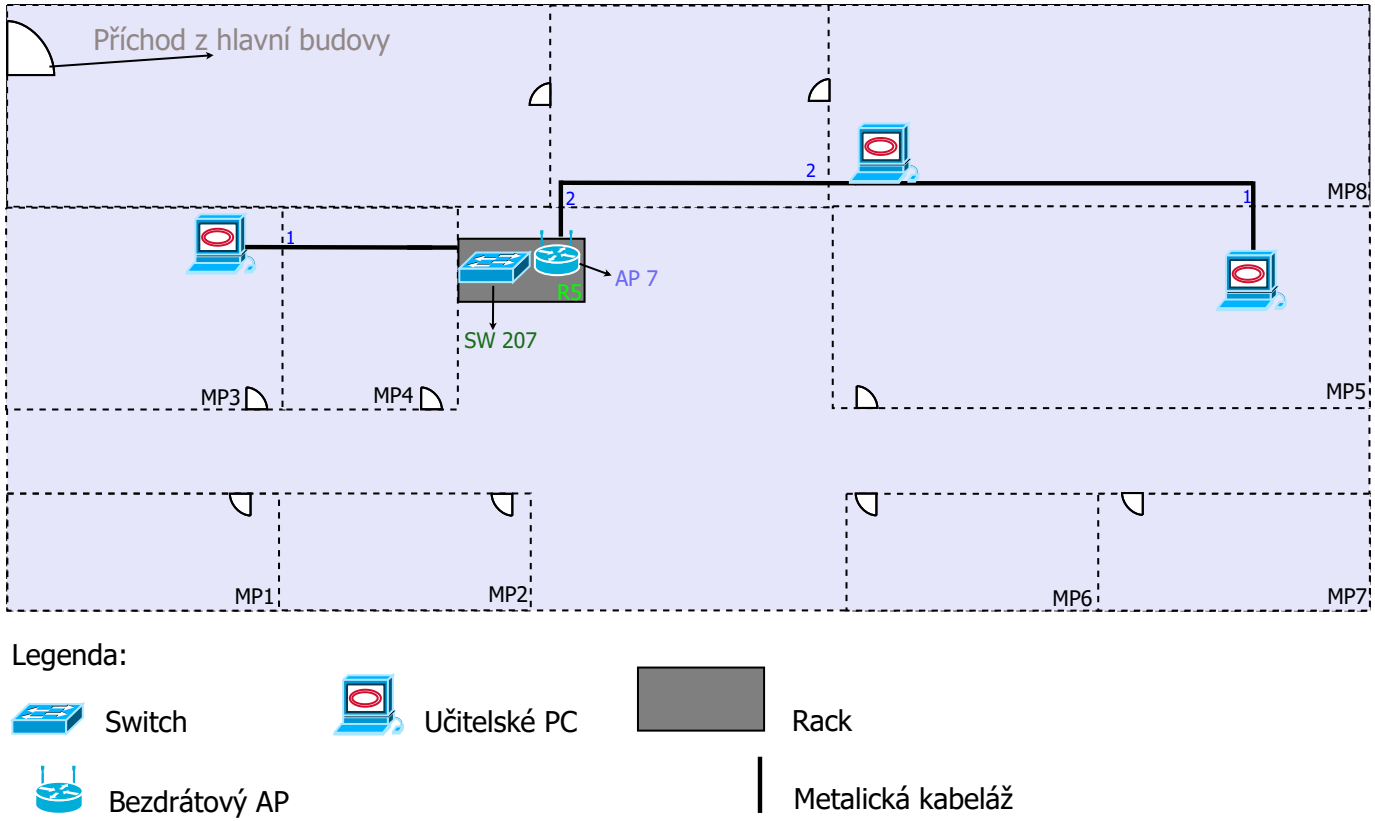
Legenda:



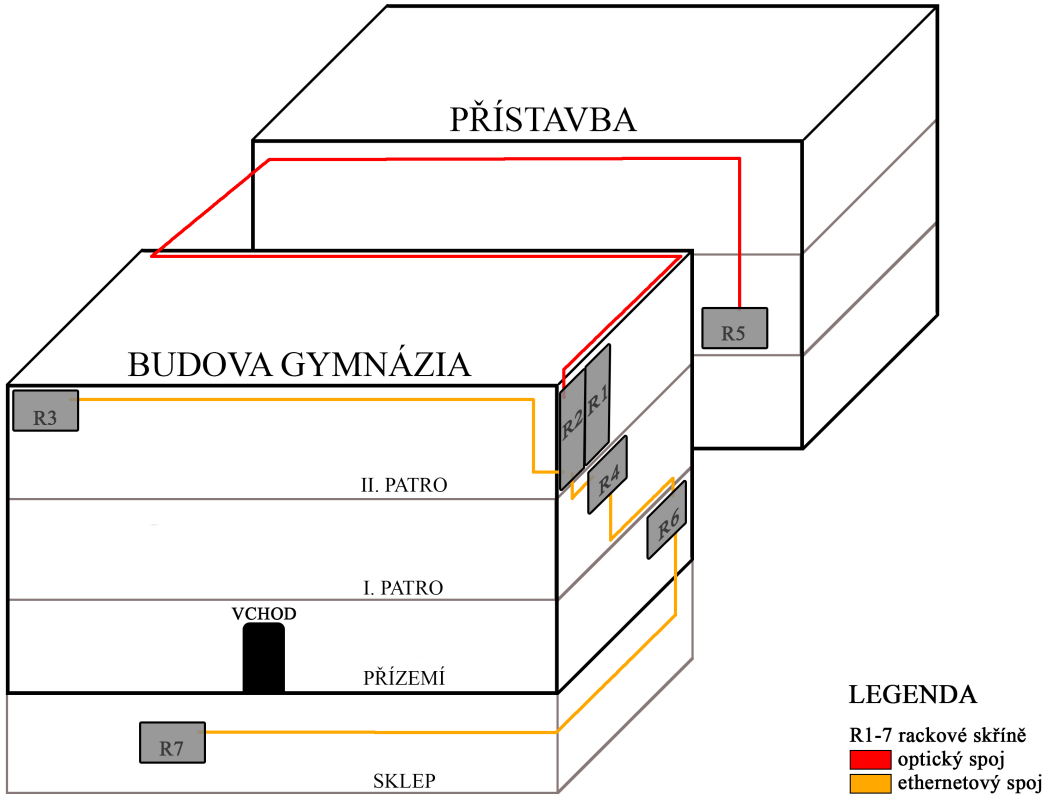
A.4 Schéma sítě v podzemních prostorech.



A.5 Schéma sítě v přístavbě.



A.6 Schéma rozmístění rackových skříní.



B Instalační a uživatelská dokumentace aplikace pro správu obsahu

C Obsah přiloženého CD

Na přiloženém CD se nachází všechny soubory potřebné pro spuštění aplikací a jejich používání. Dále jsou na CD přiložené plány topologie sítě v budově Gymnázia v Prachaticích a další soubory související s touto bakalářskou prací. Obsah CD viz níže.

```
\Bakalářská práce
    bakalarska_prace_Albert_Stefankovic.pdf
\Aplikace
    ZyCONFIG.zip
    ZyREBOOT.zip
    ZyCONTENT.zip
    \uživatelské_manuály
    readme.txt
\Topologie sítě
    \dia_zdroj
    \pdf
\Ostatní
    ZyXEL_USG110_CLI.pdf
    ZyXEL_USG110_UserManual.pdf
readme.txt
```