Router na bázi linuxové distribuce

Linux based internet router

Roman Váňa

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Roman VÁŇA**
Osobní číslo:	**A09831**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Router na bázi linuxové distribuce**

Zásady pro vypracování:

1. **Sestavte literární rešerši na téma funkce routeru v síti, využití Linux v rámci sítí.**
2. **Formulujte požadavky na takový router pro využití v rámci LAN sítě HP TRONIC Zlín na jednotlivých pobočkách – routing, podpora VLAN, funkce firewallu, proxy, VPN a další.**
3. **Vyberte 3–5 specializovaných distribucí Linuxu pro plnění požadovaných rolí.**
4. **V praktické části popište jednotlivé distribuce. Srovnejte jejich vlastnosti, přívětivost konfigurace, podporu. Proveďte také srovnání se specializovaným HW zařízením (Fortigate).**
5. **Zhodnoťte jednotlivá řešení a vyberte nejvhodnější řešení s ohledem na celkové náklady, spojené s provozem v průběhu 5 let.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SCHRODER, Carla. Linux: kuchařka administrátora sítě. Vyd. 1. Brno: Computer Press, 2009, 596 s. ISBN 978-802-5124-079.**
2. **HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce: kuchařka administrátora sítě. 5., aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-802-5131-763.**
3. **SOSINSKY, Barrie. Mistrovství - počítačové sítě. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-802-5133-637.**
4. **SPURNÁ, Ivona. Počítačové sítě: praktická příručka správce sítě. Vyd. 1. Kralice na Hané: Computer Media, c2010, 180 s. ISBN 978-807-4020-360.**
5. **NEMETH, Evi, Garth SNYDER a Trent R HEIN. Linux: kompletní příručka administrátora: 2. aktulizované vydání. Vyd. 1. Brno: Computer Press, 2008, 984 s. ISBN 978-802-5124-109.**
6. **Root.cz: Informace nejen ze světa Linuxu [online]. 1998-2012 [cit. 2012-01-31]. Dostupné z: http://www.root.cz/**
7. **FORTINET, Inc. [online]. 2011 [cit. 2012-01-31]. Dostupné z: http://www.fortinet.com/**
8. **List of router or firewall distributions. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation [cit. 2012-01-31]. Dostupné z: http://en.wikipedia.org/wiki/List_of_router_or_firewall_distributions**

Vedoucí bakalářské práce: **Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **8. června 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Vladimír Vašek, CSc.
v z. *ředitel ústavu*

ABSTRAKT

Tato bakalářská práce se zabývá srovnáním několika specializovaných linuxových distribucí, které vytvoří z klasického PC plnohodnotný router při minimálních nákladech. Jejich vlastnosti a funkce jsou srovnávány také s profesionálním podnikovým routerem Fortigate 60C. Úkolem je najít optimální řešení, které by ušetřilo náklady na provoz routeru na pobočce nebo prodejně firmy HP Tronic po dobu 5 let. Výsledkem je celkové srovnání a doporučení řešení na základě reálných testů a jednoduché finanční analýzy.

Klíčová slova: počítačové sítě, router, Linux, směrování, Internet, ochrana sítě, správa sítě

ABSTRACT

This bachelor thesis deals with the comparison of several specialized Linux distributions, which creates the high-quality router from classic PC for minimum cost. Their features and functions are also compared with a professional business router Fortigate 60C. The challenge is to find an optimal solution that would save the cost of running the router at a branch store of HP Tronic company for 5 years. The result is an overall comparison of recommendations and solutions based on real tests and simple financial analysis.

Keywords: computer network, router, Linux, routing, Internet, network protection, network administration

Tímto děkuji vedoucímu své práce, Ing. Jiřímu Vojtěškovi, Ph.D., za poskytnutí konzultací, rychlou komunikaci a za vedení při zpracování práce. Dále chci poděkovat mé rodině a přítelkyni za podporu a trpělivost a v nemalé míře také firmě HP Tronic za poskytnutí prostředků, které umožnili vytvoření této práce.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 POČÍTAČOVÉ SÍTĚ **11**
1.1 HISTORIE 11
1.2 DĚLENÍ SÍTÍ 12
1.2.1 Sítě podle velikosti 12
1.2.2 Sítě podle hierarchie 12
1.3 SÍŤOVÝ HARDWARE 14
2 SMĚROVÁNÍ V SÍTI **16**
2.1 SÍŤOVÉ PROTOKOLY 16
2.1.1 Protokol IP 16
2.1.2 Protokol ARP 18
2.1.3 Protokol DHCP 19
2.1.4 Protokol IPX/SPX 19
2.2 ROUTER 20
2.2.1 Proces směrování 20
2.2.2 Směrovací protokoly 21
2.2.3 Možnosti routeru 23
3 LINUX JAKO ROUTER **26**
3.1 SMĚROVÁNÍ V LINUXU 26
3.2 LINUXOVÉ DISTRIBUCE 26
3.2.1 Router/Firewall distribuce 27
II PRAKTICKÁ ČÁST **28**
4 POŽADAVKY NA ROUTER V HP TRONIC **29**
4.1 PŘEDSTAVENÍ FIRMY HP TRONIC 29
4.2 POŽADAVKY NA ROUTER 29
4.2.1 Routovací funkce 29
4.2.2 Nízké náklady 30
4.2.3 Intuitivnost správy 30
4.2.4 Spolehlivost 30
5 VOLBA HARDWARE A DISTRIBUCÍ **31**
5.1 HARDWARE PRO TESTY 31
5.1.1 PC sestava 31
5.1.2 Router Fortigate 60C 32
5.2 VÝBĚR DISTRIBUCE 33
5.3 TESTOVACÍ KRITÉRIA 34
5.3.1 Instalace, konfigurace, vzhled 34
5.3.2 Funkce routeru 34
5.3.3 Záloha, obnova, údržba 34

6 SROVNÁNÍ 35
6.1 ASTARO SECURITY GATEWAY 35
6.1.1 Instalace, konfigurace, vzhled 35
6.1.2 Funkce routeru 37
6.1.3 Záloha, obnova, údržba 38
6.2 PSSENSE 40
6.2.1 Instalace, konfigurace, vzhled 40
6.2.2 Funkce routeru 42
6.2.3 Záloha, obnova, údržba 43
6.3 CLEAROS 44
6.3.1 Instalace, konfigurace, vzhled 44
6.3.2 Funkce routeru 46
6.3.3 Záloha, obnova, údržba 48
6.4 ROUTER FORTIGATE 60C 49
6.4.1 Instalace, konfigurace, vzhled 50
6.4.2 Funkce routeru 51
6.4.3 Záloha, obnova, údržba 54
7 ZHODNOCENÍ ŘEŠENÍ 55
7.1 UŽIVATELSKÉ ZHODNOCENÍ 55
7.2 FINANČNÍ ZHODNOCENÍ 55
7.3 CELKOVÉ ZHODNOCENÍ 57
ZÁVĚR 58
ZÁVĚR V ANGLIČTINĚ 59
SEZNAM POUŽITÉ LITERATURY 60
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 62
SEZNAM OBRÁZKŮ 64
SEZNAM TABULEK 66
SEZNAM PŘÍLOH 67

ÚVOD

V dnešním otevřeném světě Internetu je důležité bezpečně oddělit osobní a firemní citlivá data od přístupu nezvaných hostů a úniků. Existuje spousta nástrojů jak toho docílit. Běžnému uživateli jde hlavně o zabezpečení koncových stanic (počítačů, notebooků, ale i mobilních telefonů a tabletů). Toho lze většinou dosáhnout softwarovým firewallem i antivirovým programem přímo v počítači, či jinému domácímu zařízení.

Podnikové prostředí se však skládá z velké síťové infrastruktury, obsahující stovky i tisíce počítačů a síťových zařízení, kterou je potřeba nejenom chránit, ale také efektivně řídit a spravovat. K těmto účelům se používá router, což je aktivní síťové zařízení obsahující logiku pro řízení a směrování mezi sítěmi. Zároveň také funguje jako ochrana dat a přístupů na různých úrovních síťových vrstev.

Potřebu směrovat data a chránit síť má v dnešní době již téměř každá domácnost, kdy je napojena přes místního ISP k Internetu a po domě má vytvořenou bezdrátovou síť. K těmto účelům postačí jednoduché cenově dostupné routery. Pro podnikovou sféru jsou však zapotřebí mnohem výkonnější a logicky mnohem dražší routery, které řídí celé komplexy sítí.

Existují však vysoce specializované distribuce, postavené na Linuxu, které lze nainstalovat na běžný počítač obsahující více síťových rozhraní a plnohodnotně tak router v síti zastoupit. Největší výhoda je jejich cena, protože v základu bývají především zdarma.

Tato bakalářská práce se bude těmito distribucemi zabývat a srovnávat vybrané zástupce jak mezi sebou, tak s podnikovým routerem Fortigate 60C, který mi byl zapůjčen firmou HP Tronic. V práci budu dbát na to, aby distribuce splňovaly požadavky firmy HP Tronic pro směrování a řízení provozu v menších pobočkách a prodejnách této firmy.

Výstupem této práce bude pak celkové srovnání a zhodnocení distribucí oproti podnikovému řešení.

I. TEORETICKÁ ČÁST

1 POČÍTAČOVÉ SÍTĚ

Počítačová síť se skládá z technického a programového vybavení, které umožňuje vzájemné propojení počítačů za účelem vzájemné komunikace uživatelů a sdílení prostředků sítě. U samostatných počítačů by bylo nutné aplikace a prostředky (např. tiskárny nebo skenery) mezi počítači duplikovat, což by bylo velmi neefektivní a nákladné řešení.

Protože v síti může pracovat několik počítačů, je možné řídit celou síť z centrálního místa. Centralizovaná správa umožňuje také zabezpečení a sledování systému z jednoho místa. Všechny počítače v síti musí být samozřejmě fyzicky propojeny pomocí síťových adaptérů a příslušných kabelů nebo pomocí optického kabelu či bezdrátovým připojením. [1]

1.1 Historie

Historie vývoje počítačových sítí sahá až na konec 60. let 19. století, kdy bylo potřeba čím dál více rozšířené počítače propojit pro vzájemnou komunikaci. Start tomu udalo ministerstvo obrany Spojených států, které zadalo požadavek firmě RAND na vybudování nové komunikační sítě, která by v případě krize umožnila rychlou komunikaci a výměnu dat. RAND přišlo s návrhem sítě, která nemá žádné centrální uzly a byla schopná funkce i při masivním poškození. Byla složena z nezávislých a rovnocenných uzlů, které si předávaly malé fragmenty = pakety. Pakety byly předávány postupně od odesílatele k cíli, samotná cesta paketů nebyla důležitá.

Původní návrh byl v roce 1969 uveden do praxe a tím vznikl základ sítě ARPANET. Na počátku propojovala 4 významné vědecké instituce. Původně byla určena pro vojenské účely, ale čím dál častěji sloužila k zasílání soukromých zpráv a elektronické pošty.

Zásadní zlom ve vývoji sítí a Internetu přinesl rok 1982, kdy byl definován komunikační protokol TCP/IP. Tento protokol umožnil propojit ohromné množství heterogenních sítí a umožnit tak vzniku podobě Internetu, jak ho známe dnes. V roce 1983 se vojenská část oddělila a masovému rozšíření ARPANETU již nic nebránilo. [2]

1.2 Dělení sítí

Počítačové sítě dělíme podle několika kritérií.

1.2.1 Sítě podle velikosti

Počítačové sítě spadají podle své velikosti a funkce do jedné z několika skupin:

- **PAN** (Personal Area Network) je síť s nejmenší rozlehlostí a je používána pro propojení osobních elektronických zařízení (mobil, tablet, notebook). Kladou si za cíl odolnost proti rušení, nízkou spotřebu a také snadnou konfiguraci.
- **LAN** (Local Area Network) je *místní síť* a je základní klasifikací každé počítačové sítě. Architektura může být jednoduchá (dva až tři počítače propojené kabelem) až složitá (několik stovek počítačů a periferních zařízení v celé obchodní společnosti). Rozlišující vlastností sítě LAN je její geografická oblast, která pokrývá jednu budovu nebo menší areál budov (do 5 km).
- **CAN** (Campus Area Network) je to síť spojující několik málo LAN sítí a počítačů. Do této kategorie spadají sítě v různých areálech v jednom místě působení. Například univerzita, průmyslový areál, vládní budovy, kdy jsou vzájemně propojeny budovy sídlící u sebe.
- **MAN** (Metropolitan Area Network) je síť propojující např. několik budov ve velkém městě a rozšiřující tak působnost LAN sítě jejich prodloužením a zvýšením rychlosti a počtu připojených stanic.
- **WAN** (Wide Area Network) je rozlehlá síť, která nemá žádné geografické omezení. Je tvořena z většího počtu propojených LAN sítí. Jako příklad nejzákladnější WAN sítě můžeme nazvat Internet. Z dalších rozlehlých sítí můžu uvést třeba WiMAX. [3]

1.2.2 Sítě podle hierarchie

Počítačové sítě můžeme dále dělit podle hierarchie, podle tzv. role uzlu:

- **PEER-TO-PEER** síť lze přeložit jako *rovný s rovným*. Nejsou zde žádné vyhrazené servery, každý počítač slouží jako server i klient zároveň. Uživatel každého počítače stanovuje, která data a prostředky budou sdíleny v síti. Schopnost připojit se do sítě peer-to-peer v dnešní době umožňuje každý operační systém od

Windows (XP, Vista, 7) přes Linuxové distribuce až po MAC OS X od Applu a není potřeba žádný síťový operační systém navíc. Nevýhodou je, že se hodí spíše pro malý počet uživatelů, neexistují žádné servery pro sdílení a správu provozu sítě.

- **KLIENT-SERVER** je typem sítě, ve které je jeden nebo několik počítačů (serverů) nadřazen jinému nebo dalším počítačům (klientům). Servery jsou optimalizovány pro rychlé zpracování požadavků od velkého počtu klientů. Mezi příklady různých typů serverů patří např. tyto: [1]
  - **Souborové a tiskové servery:** spravují celkový přístup uživatele a používání souborů a prostředků pro tisk.
  - **Databázové servery:** server přistoupí k uložené databázi, zpracuje daný požadavek a vrátí odpověď klientovi
  - **Aplikační servery:** klientskému počítači se zasílají opět jen výsledky požadavku. Jsou vhodné pro správu obrovských množství dat a efektivní poskytování dat klientům.
  - **Poštovní servery:** zpracovávají tok elektronické pošty a zpráv mezi uživateli sítě. Ve většině případů se podobají aplikačním serverům, protože e-mail na serveru většinou zůstává. Ukládání e-mailů v centrálním umístění umožňuje lepší správu a zabezpečení pošty (Microsoft Exchange Server nebo Sendmail)
  - **FTP servery:** umožňují pohyb jednoho či více souborů mezi počítači s ovládacími prvky zabezpečení a integrity dat vhodnými pro síť Internet. Server FTP provádí hlavní část práce při zabezpečení souborů, jejich uspořádání a řízení přenosu. Klient (FTP klient, prohlížeč) přijímá soubory a ukládá je na pevný disk.
  - **Firewall a server proxy:** Firewall slouží k zabránění v neoprávněném přístupu k nebo z privátní sítě a obvykle slouží jako první obranná linie při ochraně soukromých informací. Firewally mohou být implementovány hardwarově i softwarově (často jejich kombinace). Všechny zprávy vstupující do nebo opouštějící intranet prochází firewallem, který zablokuje tu, která nevyhovuje požadovaným kritériím zabezpečení. Server proxy je nejoblíbenější z firewallů. Je umístěn mezi klientem (webový prohlížeč) a externím serverem (webový server). Server proxy efektivně skrývá skutečné síťové adresy a filtruje

požadavky odesílané na externí servery nebo přicházející z Internetu. Firewall lze v dnešní době aktivovat přímo na routeru, pro menší společnosti a firmy není potřeba zvláštní server pro firewall.

- **Webové servery:** umožňují poskytovat obsah prostřednictvím sítě Internet pomocí jazyka HTML. Webový server (např. Apache) přijímá požadavky od prohlížečů (Internet Explorer, Firefox, Google Chrome…) a poté vrátí příslušný dokument HTML danému počítači. Pro zvýšení výkonu může být použito spoustu serverových technologií (skripty CGI, zabezpečení SSL, stránky ASP) [1]

1.3 Síťový hardware

Síťový hardware má obrovský vliv na rychlost, kvalitu a výkon celé sítě. Za základní prvky sítě můžeme považovat rozbočovače (hub), přepínače (switch), mosty (bridge), směrovače (routery - v této práci budu jednotně používat slovo *router*, protože je v praxi běžně používané), síťové karty, kabely a další spojovací prvky (optické vlákna, převaděče signálu). Dnes se řada síťových prvků již moc nevyužívá (například rozbočovač, brána, opakovač), nahradila je komplexnější zařízení, které jejich bývalou funkcionalitu obsahují v sobě a dále ji rozšiřují. [1]

- **Rozbočovač (hub)** je centrálním spojovacím zařízením, které propojuje počítače v hvězdicové topologii. Přijme data a rozešle je na všechny ostatní porty bez ohledu na to, kterému portu data náleží. U větších sítí tak dochází k přetěžování segmentů, kterým data nepatří. Dnes se již nepoužívají, nahradili je jiné prvky sítě. [1]
- **Most (bridge)** naproti tomu rozděluje na základě MAC adresy rámců jednotlivé segmenty sítě. Kontrolují rámce z hlediska chyb a specificky řídí jejich tok. Most je v síti neviditelný pro koncové stanice. Pracuje pomaleji než přepínač, protože vnitřní rozhodování se odehrává softwarově, nikoliv hardwarově jako to je u přepínačů, které mosty nahradily. Nepodporuje virtuální lokální sítě (VLAN). [1]
- **Přepínač (switch)** je aktivní prvek sítě propojující navzájem jednotlivé zařízení nebo části sítě. Pracuje na druhé vrstvě OSI modelu = řídí se podle MAC adresy rámců. U přicházejících rámců tak čte MAC adresy a zapisuje je do tabulky MAC adres a portů označované jako CAM (Content Addressable Memory) tabulka. Pokud nemá záznam pro cílovou MAC adresu, pošle rámec na všechny ostatní

porty, pokud má, tak rámec pošle na cílový port. Jsou rychlé, mají desítky portů (běžně 50 portů). Přepínače umožňují výběr režimu práce – *store-and-forward* režim nejprve uloží celý rámec a na základě MAC adresy se rozhoduje o přepnutí mezi porty. Další režim *cut-through* je rychlejší, kdy přepínání na výstupní porty probíhá již v průběhu přijímání rámce na vstupní port. Dále podporují ***VLAN***, což jsou virtuální logické podsítě, díky kterým lze flexibilně měnit strukturu sítě bez změny v hardwaru sítě. [7]

- **Směrovač (router)** je zařízení, které má schopnost směrovat data mezi dvěma a více odlišnými sítěmi. Jelikož je toto zařízení hlavním tématem této práce, je mu věnována vlastní kapitola. [1]

2 SMĚROVÁNÍ V SÍTI

Pro směrování v lokálních jsme si vystačili s přepínači a mosty, kdy tato zařízení pracují na druhé vrstvě (linková) modelu OSI a přepínají tak provoz mezi jednotlivými zařízeními nebo segmenty v rámci jedné sítě.

Směrování mezi odlišnými dílčími sítěmi, kterými mohou být například jednotlivé lokální sítě (Ethernet, Token Ring apod.), probíhá na třetí vrstvě modelu OSI, a to na vrstvě síťové. Důvodem je minimalizace objemu směrovacích tabulek, protože v nestrukturované síti je směrování založeno na adresách (dílčích) sítí a nikoliv na adresách jednotlivých hostitelských počítačů v rámci těchto sítí. K těmto účelům se používá router.

V síťové vrstvě se oproti rámcům směrovaných na MAC adresy zasílají na jednotlivé zařízení či počítače v sítí IP datagramy. Každé síťové zařízení komunikuje s ostatními pomocí IP adres, které jsou v IP datagramu obsaženy. Ke správnému směrování a adresování byla vytvořena sada protokolů. [5]

2.1 Síťové protokoly

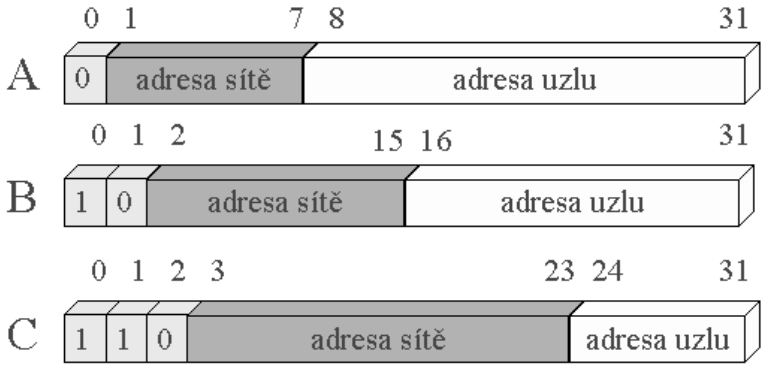
Jsou to sady pravidel, kterými se řídí každé zúčastněné zařízení v síti. Pro konfiguraci, správu a údržbu je nutné znát, jak každý z protokolů funguje a jak spolu navzájem spolupracují.

2.1.1 Protokol IP

Internet Protocol je základní síťový protokol zodpovědný za směrování IP datagramů ze zdrojového počítače do cílového hostitele přes jednu nebo více sítí. Hostiteli mohou být routery, pracovní stanice, servery či každé zařízení s IP adresou. Datagramy putují v síti nezávisle na sobě a pořadí jejich doručení nemusí odpovídat pořadí ve zprávě. Doručení není zaručeno, o to se stará protokol z vyšší vrstvy TCP, proto se nepoužívá samotný IP protokol ale kombinace TCP/IP. IP protokol se také stará o segmentaci a zpětné sestavení do a z rámců pro protokoly z nižší vrstvy. V současnosti se používají dvě verze protokolu IP a to IPv4 a IPv6. V této práci bude používán pouze protokol IPv4. IPv6 se postupně nasazuje i z důvodu vyčerpání volných adres IPv4. [5]

IP adresa je číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti. Má velikost 32 bitů a je vyjádřena jako 4 desítková čísla oddělená tečkami. Skládá se z adresy hostitele a síťovou adresu tohoto hostitele. O tom, která část je adresa sítě a která adresa

hostitele, dříve rozhodovalo, jaké *třídě* sítí daná adresa náleží. Tyto hranice určuje maska sítě. Základní třídy IP adres máme tři a označují se jako třída A, B nebo C.



Obrázek 1 - Třídy IP adres [6]

IP adresy třídy A jsou určeny pro velmi velké sítě. Pro adresu uzlu je vyhrazeno zbývajících 24 bitů a pro adresu sítě 8 bitů, z nichž je ale první bit využit k identifikaci, že se jedná o adresu třídy A. Takže pro adresu sítě zbývá 7 bitů, takže sítí s adresou třídy A může být jen 2^7 neboli 128. Maska této třídy je 255.0.0.0.

IP adresa třídy B má pro adresu sítě vyhrazeno 16 bitů, ale pro identifikaci třídy jsou využity první dva bity, čili třída B může mít maximálně 2^14 adres sítí. Maska této sítě je 255.255.0.0.

IP adresy třídy C používají prvních 24 bitů pro adresu sítě, z nichž první bity určují typ třídy C. Pro adresy uzlů zbývá tedy jenom 8 bitů, čili v takovéto síti může být pouze 2^8 neboli 256-2=254 koncových uzlů (jedna je adresa sítě a druhá broadcast). Maska této sítě je 255.255.255.0.

Existují ještě další dvě třídy. Třída D, která v prvním bajtu adresuje oblast 224-239, slouží pro *multicasting* (více směrové vysílání), který slouží k adresování skupin specifických hostů. Třída E (oblast 240-247) je vyhrazena jako rezerva. Zbytek rozsahu (do 255) je také rezervován, není však zařazován již do třídy E.

Kvůli neustále vzrůstající síti Internet, začaly postupně docházet volné IP adresy. Aby se tento jev alespoň zpomalil, vzniklo nové adresní schéma a mechanismus přidělování adres.

CIDR (Classless Inter-Domain Routing) odstranil původní dělení do tříd A, B a C s pevně danou délkou adresy sítě a nahradil ji libovolnou délkou adresy. Taková adresa se pak zapisuje ve formě prefix/délka, kdy délka určuje, kolik bitů adresy patří adrese sítě.

Příklad: `192.168.128.0/21`

Což znamená, že adresa sítě je určena prvními 21 bity a zbylých 11 určuje adresu uzlu. Rozsah IP adres a maska sítě by v tomto případě byla:

IP adresa:

Decimálně `192.` `168.` `128.` `0`

Binárně `11000000.10101000.10000|000.00000000` (prvních 21 bitů)

Maska:

Binárně: `11111111.11111111.11111|000.00000000` (prvních 21 bitů)

Decimálně: `255.` `255.` `248.` `0`

Rozsah IP adres by byl tedy: `192.168.128.0 – 192.168.135.255`

Tímto procesem se zpomalil úbytek volných IP adres, kdy ISP dostane určitý prefix, jehož části (delší prefixy začínající tímto společným prefixem) pak přiděluje svým zákazníkům.

I tak se ale postupně vyčerpávají volné IP adresy *IPv4* protokolu a postupně se nasazuje nový *IPv6* protokol, který má rozsah 128 bitů oproti 32 bitům verze IPv4, takže k vyčerpání volných adres v nejbližší době nejspíše nedojde a každé zařízení může mít svou vlastní IPv6 adresu (jedinečných IPv6 adres může být až 2^128, což je v přirovnání milionkrát více IP adres pro jednu hvězdu ve vesmíru, než umožňoval IPv4 protokol pro naši jednu planetu). [6]

2.1.2 Protokol ARP

Datová vrstva řídí pohyby paketu v sítí pomocí MAC adres komunikujících zařízení. Když je paket předán z třetí, síťové, vrstvy do druhé, datové, vidí datová vrstva informaci o IP adrese jen jako data, která pro ni nejsou potřebná. K tomu aby se mohl paket dál šířit k cíli je potřeba převést IP adresu na MAC adresu cílového počítače. Právě k tomu slouží protokol ARP.

Vysílající vyšle ARP dotaz obsahující hledanou IP adresu a údaje o sobě (IP adresu a MAC adresu) všem účastníkům sítě (MAC adresa FF:FF:FF:FF:FF:FF). Po přijetí tohoto dotazu odpoví vlastník dané IP adresy svou MAC adresou, ostatní hostitelé dotaz ignorují.

Informace o MAC adresách odpovídajících jednotlivým IP adresám se ukládají do ARP cash, kde záznam zůstává po nějakou dobu, než zanikne nebo se znovu obnoví. Tím se tak snižuje zatížení sítě, kdy odesílatel zkontroluje nejprve ARP cash a pokud nenajde cílovou adresu, tak odešle ARP dotaz.

RARP (Reverzní ARP) poskytuje opačnou funkci. Slouží ke zjištění IP adresy podle známé MAC adresy. Používá se například u bez diskových stanic k získání IP adresy ze serveru RARP. [1]

2.1.3 Protokol DHCP

DHCP je protokol používaný k dynamickému přiřazování IP adres pracovním stanicím v rámci sítě a pro automatickou konfiguraci. DHCP server přiřazuje počítačům zejména IP adresu, masku sítě, bránu a adresu DNS serveru. Klient, který má nastaveno získávání IP adresy pomocí DHCP protokolu požádá o přidělení adresy server DHCP. Používá přitom broadcasting, který umožňuje rozesílat pakety všem zařízením v síti. Tyto pakety mají nastavenou adresu 255.255.255.255. Na ty reaguje DHCP server a odešle odpověď klientovi, ten si vybere nejvhodnější adresu a pošle potvrzení DHCP serveru a ten přidělí adresu z definovaného rozsahu. Tento proces se nazývá *dynamická alokace*.

IP adresa může být přidělena DHCP serverem také na základě *statické alokace*. V tomto případě má DHCP server seznam MAC adres a k nim přiřazeny nastavené IP adresy. V momentě kdy se do sítě připojí zařízení s MAC adresou v tomto seznamu, dostane pokaždé stejnou, předem definovanou IP adresu. [2]

2.1.4 Protokol IPX/SPX

Tento protokol byl vyvinut firmou Novell NetWare. IPX je protokol používaný pro směrování paketů v síti. Stejně jako IP protokol pracuje ve třetí síťové vrstvě a vyžaduje použití schématu adres, které rozlišuje mezi adresou sítě a uzlu. IPX adresa je napsána v hexadecimálním tvaru. Síťová část adresy má 32 bitů a druhá část podobající se části hostitele u adresy IP má 48 bitů. Adresa uzlu je však MAC adresa síťové karty. Není tedy nutné používat ARP protokol pro překlad adres. Pro svou koncepci se protokol IPX/SPX hodí spíše do LAN sítí. Pro rozsáhlé sítě WAN je téměř nepoužitelný. V dnešní době se používá hlavně protokol TCP/IP, který IPX/SPX protokol již téměř vytlačil. [1]

2.2 Router

Router je aktivní síťové zařízení se schopností směrovat data mezi dvěma a více různými sítěmi. Pracuje na třetí, síťové, vrstvě modelu OSI a hlavním úkolem je přeposílání IP datagramů z jednoho síťového rozhraní na další. Aby mohly routery odesílat a přijímat data mezi různými sítěmi, musí být router připojen ke každé ze sítí a mít adresu IP ve všech logických sítích, ve kterých bude směrovat data.

2.2.1 Proces směrování

Proces směrování probíhá následovně:

1. Po přijetí dat router oddělí informaci o rámci a zkontroluje, jestli datagram neobsahuje chyby a ty případně opraví a odešle datagram do zásobníku.
2. Síťová vrstva vyčte z hlavičky cílovou adresu a identifikuje část adresy pro vyhledání ve směrové tabulce.
3. Při hledání cílové sítě ve směrové tabulce se router snaží nalézt co nejpřesnější dostupnou adresu (například trasu pro 192.168.128.0 místo 192.168.0.0). Pokud adresu nenalezne, odpoví ICMP zprávou „Network Unreachable“.
4. Router upraví pole datagramu TTL (Time-To-Live), které pomáhá při detekci časových smyček datagramu. Dosáhne-li čítač TTL nulové hodnoty, datagram se vynechá a odešle se ICMP zpráva „TTL Expired“.
5. Podle směrovací tabulky probíhá příprava pro odeslání datagramu. Dle potřeby se provádí ověření MTU (Maximum Transmit Unit, což je maximum bajtů pro rámec) sítě dalšího směrování a fragmentování datagramu.
6. Poté se odešle připravený paket do fronty výstupního rozhraní a přeposlání paketu k dalšímu směrování. Pokud je fronta plná nebo dojde k poškození trasy, je paket vynechán a na tuto skutečnost je upozorněno.

Router musí vědět, jakou trasou má paket odeslat. Potřebné informace o trasách jsou mezi routery sdíleny za pomocí jednoho či více směrovacích protokolů. [1]

2.2.2 Směrovací protokoly

Z obecného hlediska existují tři typy tras – připojované, statické a dynamické.

Připojované trasy jsou vytvářeny, když se router přímo připojí k dané síti. Tento proces je popsán v předchozí podkapitole.

Statické trasy se liší tím, že musí být zadávány manuálně a jednoduše uvádějí další směrování pro danou cílovou síť. Údaje nejsou za běhu nijak měněny a přepisovány. Statické směrování je typické pro koncové stanice nebo routery v malé počítačové síti (LAN). Trasy definují také metriku trasy, kterou router použije ke stanovení použité trasy. Čím nižší metrika trasy je, tím výhodnější je trasa. Výchozí trasa routeru říká, kam má data odeslat, pokud nenalezne v tabulce směrování žádnou trasu pro cílovou síť. Obecná konfigurace výchozí trasy Cisco routeru vypadá následovně:

```
ip route (destination network) (destination mask) next-hop metric
```

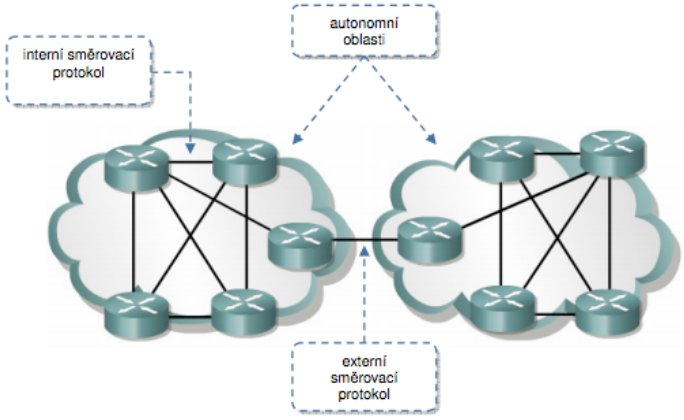
Příklad:

```
ip route 0.0.0.0 0.0.0.0 192.168.128.1 0
```

Cílová síť v tomto případě definuje jakoukoliv síť. Pokud tedy router nenalezne v tabulce přesnější položku, použije tuto trasu a odešle data na další směrování na adresu 192.168.128.1.

Dynamické trasy lze získat za použití jednoho z mnoha dynamických směrovacích protokolů. Označují se „dynamické“ proto, neboť mohou být dynamicky změněny podle toho, tak se mění daná síť. Router musí být nakonfigurován tak, aby naslouchal nebo se účastnil v příslušném dynamickém směrovacím protokolu u stanovených routerů.

Dynamické směrovací protokoly se dělí na dvě hlavní skupiny podle využití protokolu v síti. Tyto skupiny jsou označeny jako „interní“ a „externí“ směrovací protokoly. [1]



Obrázek 2 - Skupiny dynamických protokolů [11]

Interní směrovací protokoly zajišťují vyměňování informací o směrování v dané skupině interních sítí či autonomním systému.

Autonomní systém je skupinou sítí v organizaci nebo se správou prováděnou centrální organizací. ISP (Internet Service Provider) obvykle spravuje vlastní autonomní systém. Mezi nejběžnější interní směrovací protokoly patří protokoly RIP a OSPF.

- **RIP (Routing Information Protocol)** využívá metodu vektorování vzdálenosti směrování, která své rozhodnutí o směrování zakládá na vzdálenosti nebo počtu směrování a vektoru (směru) k cíli paketu. Poté co protokol RIP informace shromáždí, provede analýzu za použití Bellman-Ford algoritmu (počítá nejkratší cestu na základě hodnocení hran, kladné i záporné), který stanoví nejlepší trasu. V dnešních sítích se již RIP nepoužívá i z důvodu omezeného počtu hopů (pouze 15), čímž je ve velkých sítích nepoužitelný.
- **OSPF (Open Shortest Path First Protocol)** využívá oproti tomu metodu zjišťování stavu linky, při které shromažďuje informace o směrování na topografické úrovni sítě. Informace poté analyzuje pomocí algoritmu Dijkstra (funguje nad hranově kladně hodnoceným grafem a je konečný), který vypočítá aktuální tabulku pro odeslání datových paketů. Je výhodný pro použití v rozsáhlých sítích, ve kterých efektivní aktualizace tras velmi přispívají ke stabilitě sítí při změnách směrování. Pokud router potřebuje aktualizovat dostupné trasy pro ostatní routery, vydá zprávu *LSA (Link-State Advertisment)* o stavu linky, která je předána všem přilehlým routerům. Tato zpráva LSA je poté zpracována a zanesena do tabulky sousedních routerů, které tuto zprávu předají zase dalším routerům atd. Oproti RIP protokolu k tomuto procesu dochází, pouze pokud dojde ke změně

tabulce daného routeru, kdežto RIP odesílá aktualizace bez ohledu na změny v trasách. OSPF také používá oblasti v hierarchii směrování. Rozsáhlá síť tak může být rozdělena do menších oblastí směrování OSPF. Pro integraci oblastí existuje princip páteřní oblasti či oblasti 0, do které všechny ostatní oblasti OSPF předávají informace o stavu linky pro shromáždění tras mezi oblastmi.

Zatímco interní směrovací protokoly poskytují dynamické směrování v rámci autonomního systému, externí směrovací protokoly zajišťují směrování mezi autonomními systémy. Jeden z nejčastěji používaných externích směrovacích protokolů je protokol BGP.

- **BGP (Border Gateway Protocol)** je používán na jednom či více hraničních routerech, které poskytují bránu z jednoho autonomního systému do jiného. Tento protokol je velmi často využíván poskytovateli Internetu (ISP), kteří ho používají k výměně informací o směrování. BGP má poskytovat směrování mezi rozsáhlými sítěmi. Je schopen zpracovat přes 100 000 tras, které každý hraniční router poskytovatele používá k efektivnímu předávání dat v síti Internet. [1]

2.2.3 Možnosti routeru

V dnešní době má již téměř každá malá firma nebo domácnost více než jeden počítač, notebook nebo mobilní zařízení v podobě tabletu nebo chytrého telefonu s WiFi. Je proto potřeba routeru, který se postará o řízení provozu v těchto sítích a zajistí komunikaci s vnějším světem. Je to jak kvůli neustále narůstajícímu počtu zařízení, co potřebují přístup do Internetu (televize, chladničky…), tak i kvůli cenové dostupnosti.

Router již dávno neslouží pouze ke směrování dat mezi jednotlivými sítěmi a zařízeními. Je do něj integrováno spousta dalších funkcí a služeb, kterými nahradí mnohé k různým účelům používané zařízení (proxy server, firewall…).

Mezi nejčastější rozšíření, funkce a další vlastnosti routeru patří:

- **Firewall** – slouží k zabezpečení a řízení síťového provozu. Filtruje provoz podle nastavených pravidel. Prochází jím veškerá komunikace, povoluje pouze data, která jsou ověřená, a je odolný vůči napadení. Téměř všechna rozhodnutí zakládá firewall na informacích o portech obsažených uvnitř hlaviček paketů. Filtry paketů se rozhodují podle zdrojové a cílové IP adresy, použitém síťovém protokolu (TCP, UDP nebo ICMP), zdrojovém a cílovém TCP/UDP portu, případně typu zprávy ICMP. Dále může filtrovat pakety dle rozhraní, v jakém je paket přijímán. [1]

- **Proxy server** – funguje jako prostředník mezi počítačem a cílovým serverem. Překládá klientské požadavky a vůči cílovému počítači nebo serveru vystupuje sám jako klient. To znamená, že když se z vnitřní sítě LAN připojíte přes proxy server, nevidí koncový počítač nebo server vaši IP adresu, nýbrž adresu routeru. Proxy server analyzuje obsah komunikace a může ji případně pozměnit (např. pro blokování určitého obsahu). Požadavky si může ukládat do vyrovnávací paměti pro pozdější rychlejší použití. [6]
- **IDS/IPS (Intrusion Detection/Protection System)** – oproti firewallu, který blokuje porty, které nejsou používány, se snaží systém IDS hledat pokusy o útok na konkrétní aplikace, kdy útočník může využít chyby v aplikaci. IPS nejen detekuje jednotlivé útoky, ale snaží se jim aktivně zabránit. Lze tak vytvořit druhou obrannou linii za firewally u aplikací komunikující vně chráněné sítě. [8]
- **VPN (Virtual Private Network)** – je šifrované síťové spojení, které využívá mezi dvěma koncovými body bezpečný komunikační tunel, vedený po Internetu či jiné WAN síti. V routerech se používá pro site-to-site spojení pro propojení budov nebo vzdálených pracovišť firmy. Vzdálení zaměstnanci tak můžou využívat stejné síťové služby jako pracovníci v ústředí. Standardem pro vytvoření VPN se stal protokol *IPSec (IP Security),* který nabízí standardní prostředky pro navázání autentizačních a šifrovacích služeb mezi komunikujícími stranami. Protokol **IPSec** zajišťuje důvěrnost dat, integritu dat (kontrola, zda nebyly data při přenosu změněna), autentizaci původu dat a ochranu proti opakování relace (detekce opakovaných paketů). [8]
- **Antivirus/Antispyware** – integrovaná ochrana proti virům, spyware (odesílá data z PC bez vědomí uživatele) a červům obsažena přímo v routeru. Router tak může detekovat a přerušit škodlivý software ukrytý v povolených datových aplikačních paketech dříve, než se dostane do infrastruktury sítě nebo ke koncovým stanicím a způsobit tak škodu. [9]
- **Web Filtering** – chrání koncové stanice, sítě a citlivé informace před webovými hrozbami pomocí bránění přístupu uživatelům na známé phishingové (podvodná technika k získávání citlivých údajů – hesla, čísla kreditních karet) weby a zdroje malware (program k poškození PC). [9]

- **VLAN (Virtual LAN)** – Virtuální lokální síť LAN lze definovat jako doménu všesměrového vysílání. Je to tedy logicky organizovaná síť nezávislá na fyzické vrstvě. Je-li v síti více VLAN, tak se bude všesměrové vysílání z jednoho zařízení zasílat jen zařízením v rámci stejné VLAN. Do jiných VLAN se již nevysílá. Nejvhodnější je definovat VLAN podle podsítí IP – zařízení umístěna v jedné VLAN náleží také do stejné podsítě IP. Router s touto funkcí tedy umožňuje směrovat data nejen mezi podsítěmi, ale také mezi virtuálními sítěmi, kdy může být v jedné VLAN umístěno i několik podsítí. [10]

3 LINUX JAKO ROUTER

3.1 Směrování v Linuxu

Pokud je potřeba zařízení, které by mělo fungovat jako router v malé nebo střední síti, nabízí se několik možností. Jedním z bezproblémových řešení může být hardwarové řešení postavené na Linuxu (unixový operační systém). Jedná se v podstatě o počítač, který je vybaven jednou a více síťovými kartami a na kterém běží některá z desítek až stovek linuxových distribucí. Ne všechny jsou pro to vhodné, ale prakticky každá distribuce dokáže fungovat jako router.

Komerčně prodávané routery pro sektor malých a středních firem mají v sobě hardware odpovídající standardnímu vybavení počítače. Hlavní rozdíl dostupných zařízení je ve firmwaru a vzhledu zařízení. Routery, které používají realtimový operační systém např. od Cisco – IOS, vykazují při vysokém zatížení lepší výsledky než routery postavené na Linuxu. Routery, na něž jsou kladeny vysoké požadavky, používají speciální hardware od výkonných datových sběrnic, několika procesorů až po paměti typu TCAM (Ternary Content Addressable Memory). Paměti TCAM jsou v porovnání s moduly RAM několikanásobně rychlejší, ale také jsou několikanásobně dražší. V lacinějších zařízeních je proto nenajdete, neboť ani neexistuje žádný program, který by dokázal manipulovat s pakety tak jako právě TCAM.

Proto je pro menší firmy vynikající alternativou zařízení s operačním systémem Linux, než cenově nákladný komerční router, neboť v menší firmě není potřeba manipulovat se směrovacími tabulkami obsahující stovky až tisíce záznamů. Nabízí se tedy řešení, které v jednom zařízení umožňuje poskytovat prakticky všechny potřebné služby. [8]

3.2 Linuxové distribuce

Kromě běžných linuxových distribucí, které jsou běžné pro použití na architektuře x86/x64, sloužící jako plnohodnotný operační systém pro používání počítače, existují také specializované distribuce upravené pro konkrétní použití.

Jedná se o router/firewall distribuce, které jsou speciální v tom, že dokáží běžet na běžném počítači a zastoupit tak drahý komerční router a ušetřit tak mnoho nákladů. Drtivá většina těchto distribucí je zdarma, takže se platí pouze za použitý hardware, nikoliv za systém.

3.2.1 Router/Firewall distribuce

Jsou to distribuce primárně sloužící jako router s firewallem. Existuje jich několik typů.

- **Diskové distribuce** – nainstalovány na pevném disku počítače. Instalace těchto distribucí se provádí z CD nebo z USB flash disku a nastavení a systém je uložen na pevném disku a zůstává tak i po restartu počítače, na kterém systém běží. Mezi nejznámější takovéto distribuce patří: IPCop, MonoWall, PfSense, ClearOS, Astaro Gateway Security.
- **CD distribuce** – nejsou instalovány na pevný disk počítače, ale jsou spouštěny z bootovatelného CD. Distribuce tak běží pouze v operační paměti počítače a operační systém počítače tak není nijak ovlivněn nebo pozměněn. Po restartu počítače se musí opět „nabootovat“ z CD. Tady lze řadit distribuci Devil-Linux nebo redWall.
- **Disketové distribuce** – ačkoliv je to dnes již téměř nepoužívané médium, stále existují distribuce, které jsou pravidelně aktualizovány a vylepšovány, co se vlezou na jednu disketu o velikosti 1.44 MB. Mezi zástupce patří Coyote, který se již nevyvíjí od r. 2009 a Freesco, které má velkou podporu a časté aktualizace a vylepšení. Na provoz takové distribuce postačí i386 procesor a 16MB RAM paměti.

Tyto distribuce jsou založeny na Linuxu a upravených distribucích nebo na FreeBSD operačním systému. Jako nejvíc použitelné a stabilní jsou distribuce diskové, kde hrozí menší riziko poškození média. Tyto distribuce budou testovány a srovnávány jak mezi sebou, tak i s komerčním routerem od Fortinetu.

Nastavení a ovládání těchto distribucí probíhá výhradně pomocí webového rozhraní, které je uzpůsobeno k zobrazení v jakémkoliv webovém prohlížeči na počítači, který je k tomuto routeru přímo nebo nepřímo připojen. Některé speciální distribuce ovšem neobsahují webové rozhraní a lze se na ně připojit jenom pomocí konzole přes telnet nebo SSH.

Při instalaci diskové router/firewall distribuce se nastaví IP adresa routeru, administrátorský účet a další možnosti, které daná instalace nabízí. Toto nastavení lze samozřejmě později změnit a nakonfigurovat router podle potřeby.

Jsou to hotové kompletní řešení bez potřeby instalace dalších balíčků a klasické konfigurace. Všechno lze nastavit přes webové rozhraní.

II. PRAKTICKÁ ČÁST

4 POŽADAVKY NA ROUTER V HP TRONIC

Pro nasazení linuxové distribuce jako routeru ve společnosti HP TRONIC, je potřeba, aby tato distribuce splnila určitá kritéria.

4.1 Představení firmy HP TRONIC

Firma HP Tronic patří k lídrům na trhu domácích spotřebičů a spotřební elektroniky. Provozuje přes 40 maloobchodních prodejen Euronics po celé České Republice, vlastní obchodní značku Proton, nově také značku ETA a exklusivně zastupuje elektrospotřebiče GoGen, Huyndai, Goddes a Gallet. Od roku 1997 provozuje také 3 horské hotely v Beskydech – Lanterna, Horal a Galík.

Pro řízení a správu sítě takto velké společnosti, která spravuje přes 1000 pracovních stanic, je zapotřebí spoustu serverů, aktivních síťových zařízení a centrální správu jednotlivých segmentů sítě. Právě na menších segmentech sítě lze ušetřit spoustu nákladů použitím routerů na základě linuxové distribuce, místo drahých komerčních routerů (konkrétně Fortigate 60C od Fortinetu).

4.2 Požadavky na router

Mezi hlavní požadavky firmy HP TRONIC patří především:

4.2.1 Routovací funkce

Takový router musí splňovat běžné i pokročilejší funkce:

- **Routing** – neboli směrování mezi sítěmi i v rámci nich, což je základní vlastností každého routeru.
- **DHCP server** – je nutné, aby byl schopen přidělovat adresy na základě DHCP protokolu ve vymezeném rozsahu adres, který lze libovolně konfigurovat v rámci sítě. Pro konkrétní zařízení je vhodná i možnost IP reservation (přidělení konkrétní IP adresu na základě MAC adresy síťového rozhraní).
- **Accesslist** – neboli firewall je seznam instrukcí, které definují routeru, jaké pakety má přijmout nebo odmítnout. Filtruje jednotlivé IP adresy i rozsahy adres. Standartní accesslist umí povolit nebo zamítnout jen zdrojovou IP adresu.

Rozšířený accesslist filtruje provoz na základě zdrojové i cílové IP adresy, protokolu a čísla portu. [6]

4.2.2 Nízké náklady

Hlavním požadavkem a důvodem nasazení linuxové distribuce jsou co nejnižší náklady. Náklady se počítají jak pořizovací, tak provozní. Počítejme dobu provozu na ***3 roky***, kde se bude brát ohled na náklady spojené s časem stráveným údržbou a spotřebu elektrické energie.

V tomto ohledu je pořizovací cena závislá pouze na pořízeném hardware, neboť všechny testované distribuce jsou zdarma. Je vhodné zvolit kompromis mezi výkonem a cenou. Na jednu stranu aby nebyla zbytečně velká spotřeba při nepřetržitém provozu, na druhou stranu aby sestava měla dostatečný výkon pro fungování v síti.

4.2.3 Intuitivnost správy

Je nutné dbát na zastupitelnost obsluhy takové distribuce. Je potřeba, aby nebylo nutné školit více lidí pro správu takového routeru, aby stačila víceméně jedna osoba, která by v krátkosti seznámila další osoby s používáním a obsluhou.

Díky tomuto kritériu je tedy vhodné zvolit přehlednou, intuitivní distribuci se snadnou konfigurací a údržbou.

4.2.4 Spolehlivost

Dalším požadavkem je spolehlivost a rychlost zálohy nebo obnovy konfigurace. To jest možnosti ihned reagovat na případnou poruchu nebo havárii zařízení.

Existují dva hlavní přístupy:

- Mít připraveno k dispozici druhé identické zařízení, na které se jednoduše a rychle přehraje záloha konfigurace poškozeného zařízení a uvede se místo něj do provozu.
- *HA (High Availability)* backup/restore - Jedná se o obnovu v reálném čase, kdy jsou dva stejné systémy postaveny vůči sobě a automaticky se nahrávají změny z jednoho na druhý. V případě velmi kritických závad prvního systému se automaticky začne používat druhý, který běžel souběžně.

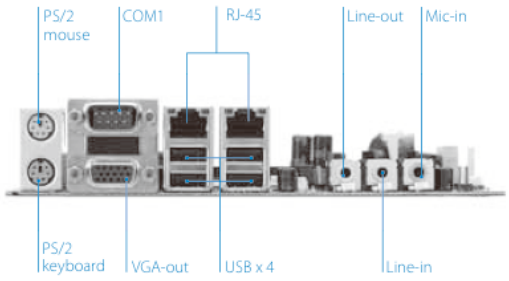
5 VOLBA HARDWARE A DISTRIBUCÍ

Pro otestování a srovnání různých distribucí mezi sebou a také s komerčním výkonově, nikoliv však cenově, odpovídajícím routerem bylo potřeba zvolit vhodné distribuce, kterých je dostupných velká spousta, vhodné testovací kritéria a také PC sestavu, na které se instalace a konfigurace všech vybraných distribucí provádělo.

5.1 Hardware pro testy

5.1.1 PC sestava

Na provoz firewall/router distribuce stačí obyčejné PC na architektuře x86 a aby mělo alespoň dvě síťové karty. K těmto účelům je však vhodné zvolit architekturu Mini-ITX pro kompaktní rozměry. Testovací sestava je tvořena z tohoto hardware:



Obrázek 3 - Porty na desce [12]

- Základní deska - VIA EPIA LT10000EAG Mini-ITX s 2 ethernet porty
- Procesor - 1 GHz VIA C7 s pasivním chlazením
- Pevný disk - 160GB SATA HDD, 5400 otáček
- Optická mechanika - DVD SATA mechanika
- Operační paměť - 512MB DDR2 RAM
- Zdroj - Micro-atx FSP220-60PLA 220W

Tato sestava je vhodná pro nepřetržitý provoz, kvůli tichému provozu, neaktivním chlazení, které by se mohlo časem poškodit, zanést prachem a s dostatečným výkonem 1GHz procesoru. Síťové karty disponují rychlostí 10/100 Mbps.

Spotřeba osazené základní desky při běžném výkonu se pohybuje kolem ***58W*** bez zapnutého LCD. Výpočet je proveden na základě kalkulátoru pro EPIA desky. [12]

Cena této sestavy je podle aktuálních internetových cen (26. 5. 2012):

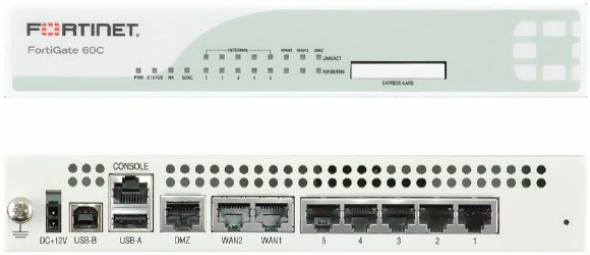
Tabulka 1 - Cena sestavy (včetně DPH)

Komponenta	Typ	Cena
Základní deska	VIA EPIA LT10000EAG, 1GHz	4935 Kč
Operační paměť	512MB DDR2 RAM	205 Kč
Pevný disk	WD 160GB SATA HDD	690 Kč
Skříň	Mini ITX case	450 Kč
Zdroj	FSP220-60PLA 220W	480 Kč
CD/DVD	Samsung SH-S222	320 Kč
Celková cena sestavy		**7 080 Kč**

Pro ušetření nákladů a částečně spotřeby by se mohl zvolit méně výkonný zdroj, který by disponoval výkonem 120W. Pevný disk by dostačoval o velikosti 20 GB pro další snížení ceny.

5.1.2 Router Fortigate 60C

Firma HP TRONIC mi k účelům testování a srovnání zapůjčila router od společnosti Fortinet. Nabízí gigabitovou propustnost firewallu, 5 nezávislých gigabitových portů možných spojit do switche, DMZ port (Demilitarised Zone – samotný síťový segment, mezistupeň mezi chráněnou privátní sítí a Internetem) a dva gigabitové WAN porty. USB porty jsou pro konfiguraci zařízení při prvním spuštění a pro připojení externího zařízení (například USB flash nebo 3G modem). Dále je tu prostor pro externí WiFi kartu.



Obrázek 4 - Fortigate 60C

Router běží na operačním systému FortiOS, tvořený na míru zařízením od Fortinetu. Hardware se liší od PC architektury, jsou použity rychlejší paměti, obsahuje 8GB flash paměť pro ukládání potřebných dat a pro systém. Vše je optimalizováno účelu tomuto zařízení. Router je napájen 12V adaptérem s průměrnou spotřebou ***16W***.

Cena Fortigate 60C s 1 letou podporou a FortiGuard službami se dle aktuálních Internetových cen pohybuje kolem ***27 750 Kč***. Cena je uvedena k datu 26. 5. 2012 a to včetně DPH.

5.2 Výběr distribuce

Existují desítky distribucí vhodných pro fungování jako firewall/router. Většina těchto distribucí je vydáváno pod GPL (General Public License) licencí nebo jako open-source projekt. Znamená to, že jsou dostupné zdarma a volně šiřitelné. Platí se tedy jen za použitý hardware, nikoliv za vývoj a operační systém jako u Fortinetu. Jsou ale i distribuce s placenou licencí, které však nabízí velkou podporu a funckionalitu, která v open-source nebývá dostupná nebo jen částečně.

Vybíráno bylo podle mnoha srovnávacích i odborných testů. Vybrané distribuce tedy jsou:

Astaro Security Gateway

Je to asi nejlepší distribuce z výběru. Obsahuje všechno, co byste od routeru čekali. Kromě základních běžných funkcí routeru (routing, zkoumání paketů, IDS/IPS) disponuje také podporou VLAN nebo funkcí High availability backup/restore. Prostředí pro správu vypadá přehledně a profesionálně.

PfSense

PfSense je založen na FreeBSD a je to open-source projekt. Oproti ASG nenabízí tolik možností, konfigurace a uzpůsobení pro potřeby uživatele. Je to hlavně firewall s pár službami navíc jako je třeba VPN.

ClearOS

Tato distribuce si zakládá na přehlednosti a jednoduchosti jak vzhledu, tak správy jednotlivých služeb a konfigurace. Nabízí základní i pokročilé volby nastavení a funkcí, které byste od routeru čekali. Umožňuje také domácí sdílení přes SAMBU nebo FTP, na které se jde připojit i z vnější sítě.

5.3 Testovací kritéria

Pro testovací kritéria bylo vycházeno především z požadavků firmy HP TRONIC. Pro lepší přehled budou důležitá data uspořádána do tabulky.

5.3.1 Instalace, konfigurace, vzhled

Je hodnocena přívětivost, logičnost instalace. Výhodou je také přehledné nastavení a konfigurace jednotlivých služeb a celková srozumitelná správa. Kladně hodnocena je i česká lokalizace umožňující rychlejší zaškolení náhradní obsluhy.

5.3.2 Funkce routeru

Testováno je jak výčet funkcí a služeb, tak jejich aktivace, nastavení a funkčnost. Mezi hlavními funkcemi nesmí chybět statické, případně dynamické routování, firewall/accesslist, DHCP server, DNS, web filtering. Hodnocena je také podpora VLAN a VPN připojení.

5.3.3 Záloha, obnova, údržba

Nejdůležitější vlastností je spolehlivost bezpečnost a na tu se váže snadná záloha a obnova konfigurace a provozu při kritických haváriích. Proto je důležitá funkce High Availability, případně snadná záloha (manuální i automatická) konfigurace a její obnovení.

6 SROVNÁNÍ

Jednotlivé distribuce jsou zhodnoceny a otestovány dle zvolených kritérií. Jsou srovnávány nejen vzájemně, ale hlavně s routerem Fortigate 60C. Výstupem pak bude tabulka a celkové zhodnocení výhod a nevýhod oproti komerčnímu dražšímu řešení.

6.1 Astaro Security Gateway

Obrázek 5 - Logo distribuce Astaro

Na stránkách německého výrobce bezpečnostní i serverové techniky Sophos je volně ke stažení aktuální ISO obraz tohoto produktu pro vypálení na CD instalaci do PC. K volnému použití je verze Astaro Security Gateway Home Edition ve verzi 8.3. Tento OS výrobce používá i pro své hardwarové řešení, kde se platí za licenci nabídky služeb. Ceny licencí platí i pro tuto distribuci, kterou si uživatel nainstaluje na svém hardware. Plná nabídka služeb je zdarma na 30 dní, vyžaduje pouze registraci u společnosti Sophos. Po uplynutí této doby zůstanou aktivní jen základní služby jako: firewall, NAT, DHCP, DNS, NTP služby. Pro dokoupení funkcionality si lze vybrat verze podle požadavků:

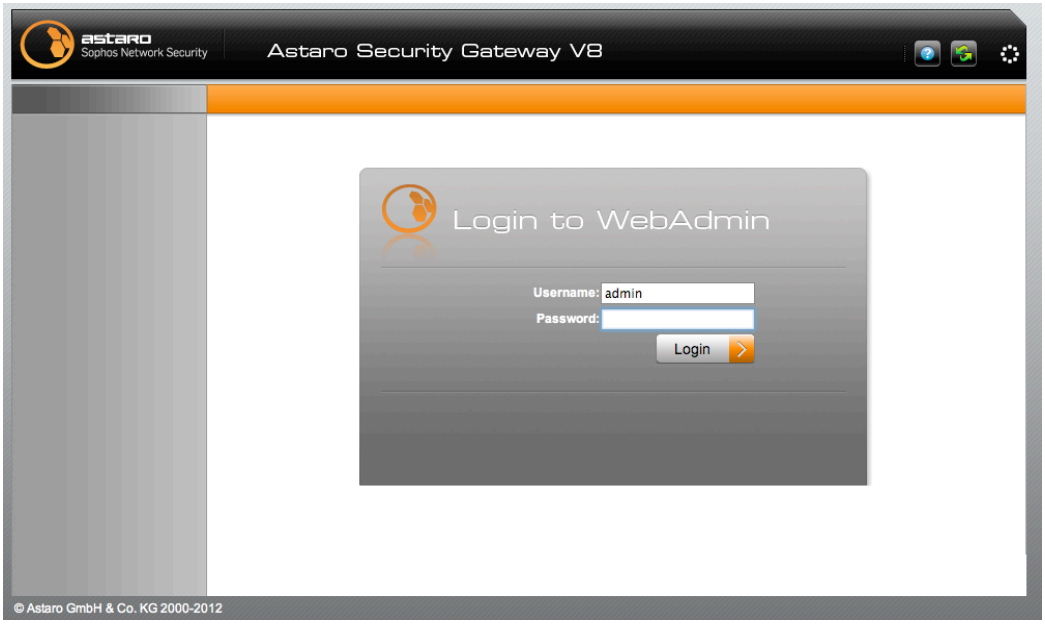
Tabulka 2 - Ceny licencí k 26. 5. 2012 na internetu vč. DPH

Verze	Cena na 1 rok	Počet licencí	Cena za 5 let
Network Protection	5 548 Kč	1-10	27 740 Kč
Email Protection	7 544 Kč	1-10	37 720 Kč
Web Protection	9 536 Kč	1-10	47 680 Kč
Full Protection	19 252 Kč	1-10	96 260Kč

Full Protection by na 5 let provozu tedy vyšla na ***96 260 Kč***.

6.1.1 Instalace, konfigurace, vzhled

Pro instalaci na naši sestavu je nutné „nabootovat“ z optické mechaniky. Poté se spustí instalace, při které se nastavuje postupně prvotní IP adresa routeru, administrátorský účet a funkce, které mají být od začátku spuštěny. Toto lze později změnit v nastavení. Hardware sestavy byl rozpoznán bez chyby.



Obrázek 6 - Přihlašovací obrazovka

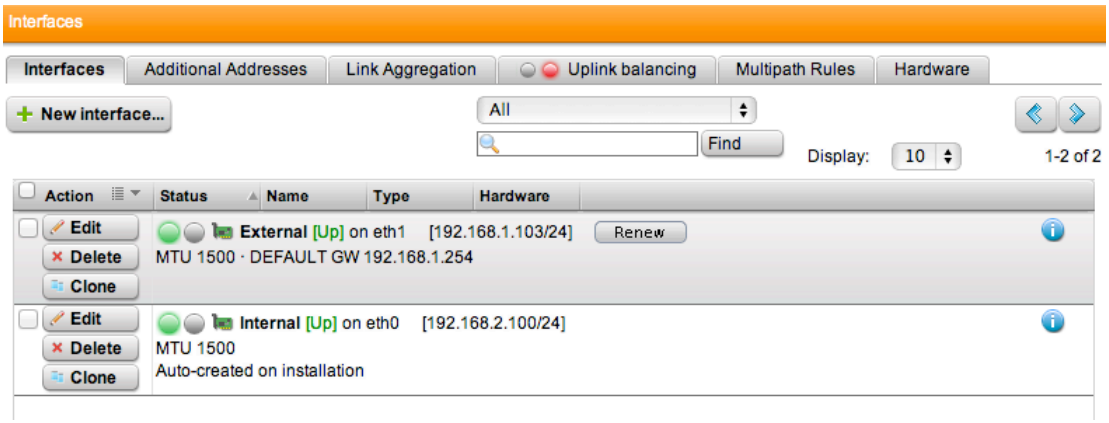
Poté je potřeba zapojit notebook nebo jiné PC k naší sestavě do portu ***eth0*** (čili první síťová karta v sestavě) pro připojení k této distribuci na dané IP adrese pomocí libovolného webového prohlížeče. V našem případě je do prohlížeče nutné zadat adresu a port:

```
https://192.168.2.100:4444
```

Spojení je šifrováno protokolem HTTPS a port si lze později v konfiguraci změnit.

Obrázek 7 - Základní obrazovka Astaro distribuce

Základní obrazovka je velmi přehledná a informuje nás o hlavní funkcionalitě, jako je: vytížení procesu, operační paměti a využití místa na disku. Dále je tam aktivní rozhraní (interface) a běžící služby, v levé nabídce pak lze konfigurovat jednotlivé služby.



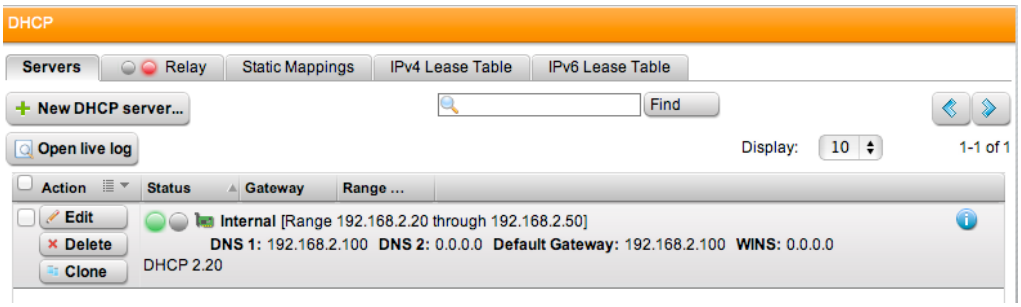
Obrázek 8 – Záložka Interface u Astaro

Důležité je správně nakonfigurovat jednotlivá rozhraní. Internal interface (eth0) je síťové rozhraní sloužící k připojení zařízení ve vnitřní síti. External interface (eth1) slouží k připojení do Internetu nebo jiné externí sítě. Interní rozhraní je nakonfigurováno jako DHCP server a externí jako DHCP klient, kterému zařízení od ISP přiřadí automaticky IP adresu, masku, bránu a DNS pro přístup do Internetu.

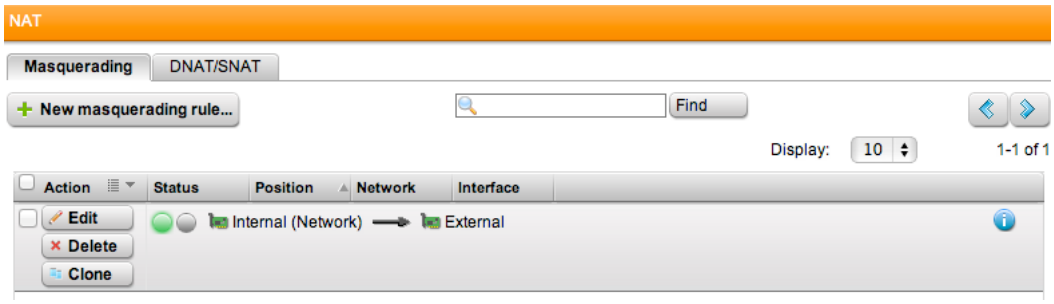
6.1.2 Funkce routeru

Astaro Security Gateway v plné verzi nechybí téměř nic:

- firewall pracující na síťové (kontrola IP adres a portů) i aplikační vrstvě (kontrola obsahu paketu)
- běžné síťové služby (DHCP, DNS, DynDNS, NAT, SIP)

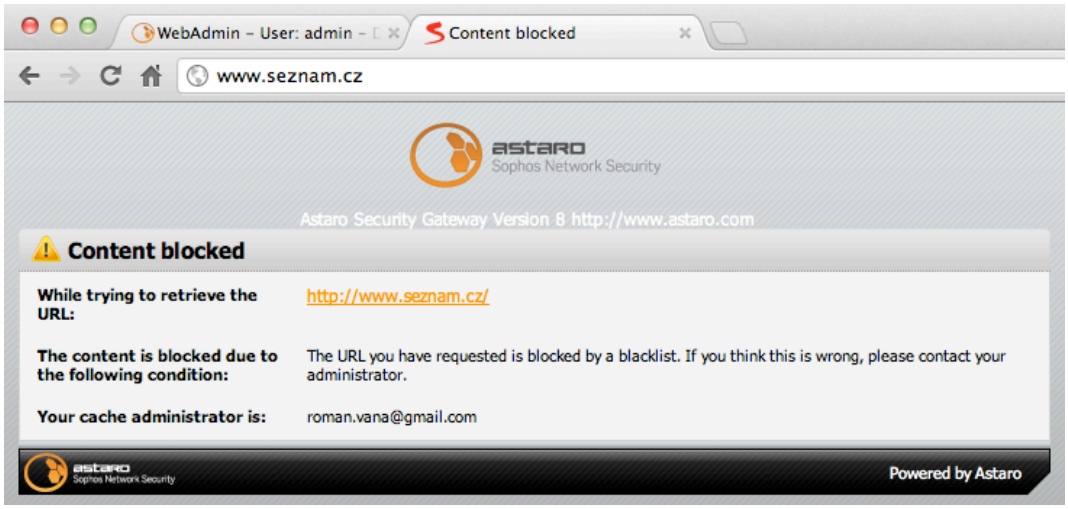


Obrázek 9 - DHCP server u Astaro



Obrázek 10 - NAT (překlad adres)

- SSL a IPSec VPN (připojení k privátním sítím pro zařízení ve vnitřní síti)
- webové služby (web/FTP proxy, antivirus ochrana, URL filtrace)

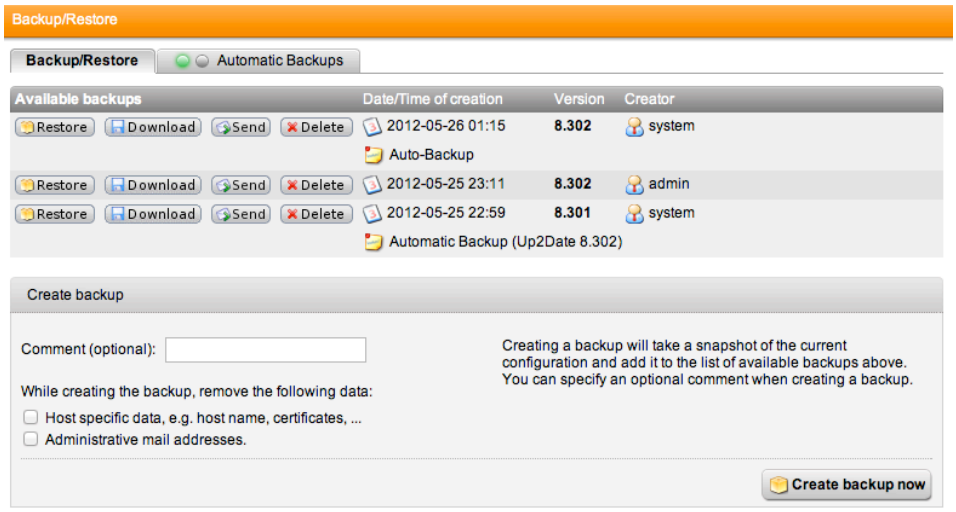


Obrázek 11 - Pokus o přístup na blokovanou stránku

- mailové služby (SMTP/POP3 proxy, antivirus, anti-phishing)
- tvorba VLAN (virtuálních sítí)
- IDS/IPS – detekce a bránění útokům z Internetu
- mnoho dalšího (VoIP služby, IM a P2P kontrola…)

6.1.3 Záloha, obnova, údržba

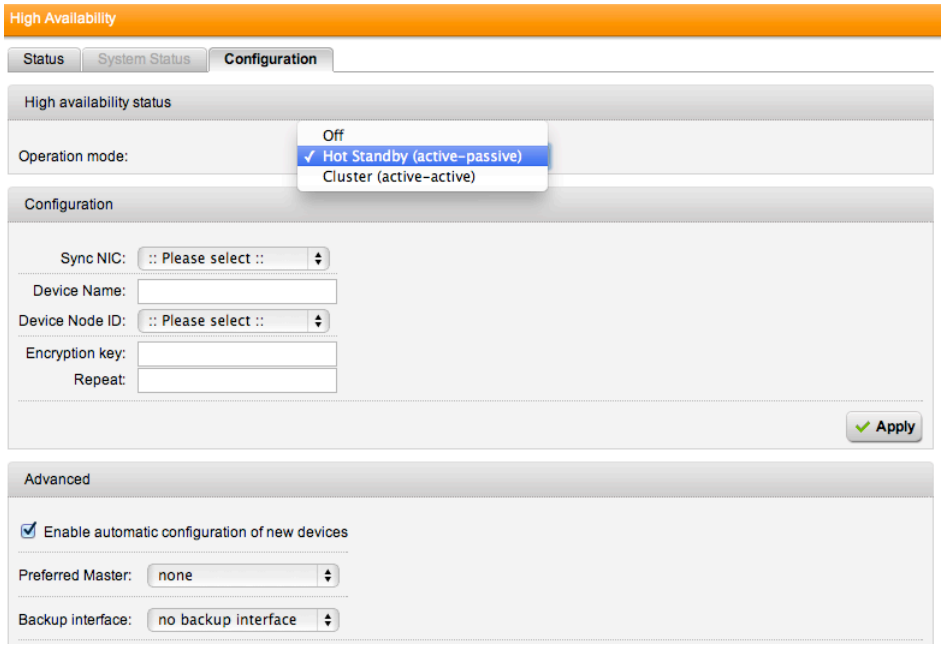
U Astaro Security gateway se nabízí obě požadované možnosti zálohy a obnovy konfigurace. Je zde možnost si ručně nebo automaticky zálohovat konfiguraci. Lze nastavit časový interval zálohy i na jaký e-mail se mají zálohy posílat (jedná se o malou velikost souboru). E-mail s konfigurací lze i zašifrovat. Obnovu lze nahrát manuálně taktéž.



Obrázek 12 - Záloha nebo obnova konfigurace

Další možností je HA, kdy lze nastavit druhé shodné zařízení v síti, které běží souběžně a na které se odesílá konfigurace a změny prováděné na našem routeru, tak aby bylo automaticky použito v případě poruchy. Lze nastavit do dvou režimů:

- **Hot Standby**: aktivní – pasivní, kdy střídavě běží jedno nebo druhé zařízení
- **Cluster**: aktivní – aktivní, kdy běží obě zařízení najednou a neustále se předávají informace mezi sebou - clustery. Výhoda oproti Hot Standby , že pokud zhavaruje aplikace na jednom zařízení, plynule se tato aplikace rozjede na druhém zařízení.



Obrázek 13 - High Availability u Astaro

Aktualizace systému jsou hlášeny na úvodní obrazovce nebo ve správě systému. Jdou provést buď manuálně nahráním aktualizačního balíku, nebo automaticky. Vše probíhá opět přes webové rozhraní, není proto potřeba nic instalovat pomocí konzole na samotné sestavě.

Obrázek 14 - Update systému Astaro

6.2 PsSense

Obrázek 15 - Logo distribuce PfSense

PfSense lze doporučit pro jeho jednoduchost a účelnost. Lze ho bezproblémů spustit i na starých PC sestavách. Distribuce PfSense oproti linuxové distribuci filtruje komunikaci pomocí ***pf*** (odtud název) programu (místo ***iptables*** u linuxových distribucí), který umí to samé jako iptables, ale funguje trochu jinak. Je zdarma, ale lze dokoupit telefonická podpora pro komerční sféru 10 hodin ročně za $1000 čili za ***20 580 Kč*** za rok s aktuálním kurzem (26. 5. 2012).

6.2.1 Instalace, konfigurace, vzhled

Po stažení IMG obrazu ze stránek projektu jej lze instalovat z CD nebo jako v mém případě z USB Flash. Základní instalace proběhne svižně, systém se nainstaluje na pevný disk a poté naběhne hlavní nabídka v konzoli na naší sestavě.

Prvotní nastavení rozhraní a síťových adres probíhá oproti Astaro již přes konzolovou nabídku a nikoliv až přes webové rozhraní. V konzolové nabídce je několik možností:

- Nastavení IP adres rozhraní
- Reset webového rozhraní, celého systému, tovární nastavení

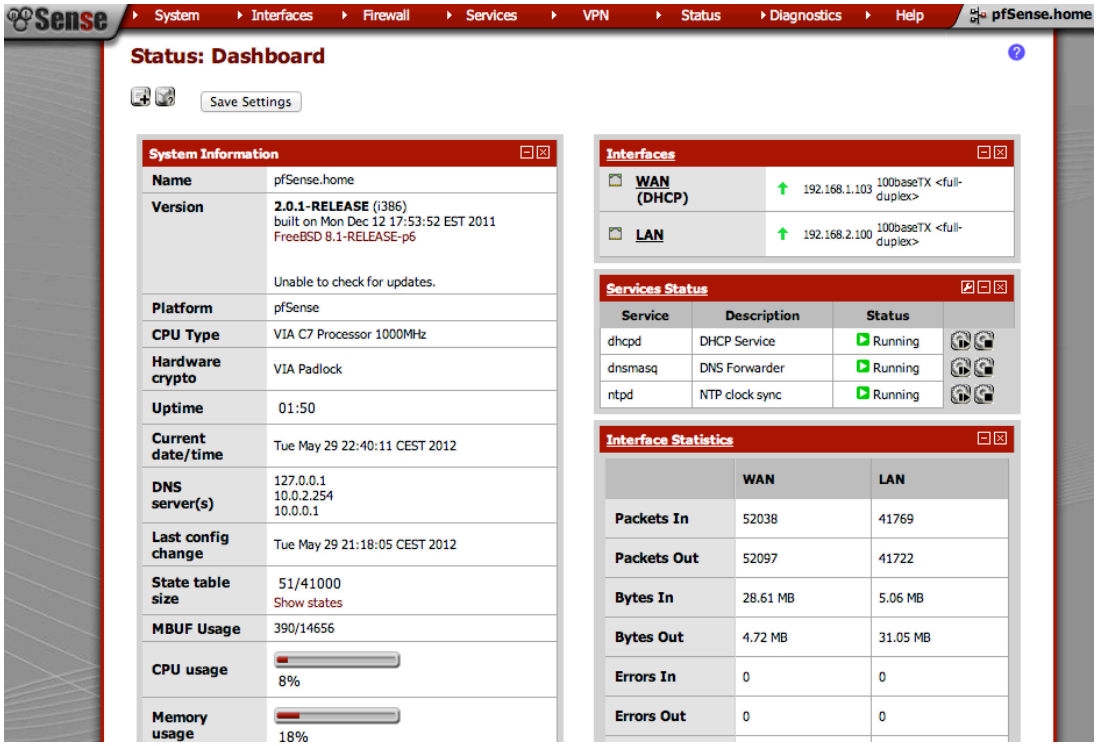
- Příkaz PING, přepnutí do Shellu

Obrázek 16 - Přihlášení do PfSense

Po základním nastavení již známe adresu webového rozhraní. V našem případě je to:

```
https://192.168.2.100
```

Port se nezadává žádný. Na PC připojeném k naší sestavě do vnitřní sítě na rozhraní LAN (***vr0***) tedy tuto adresu zadáme do libovolného prohlížeče a můžeme konfigurovat.



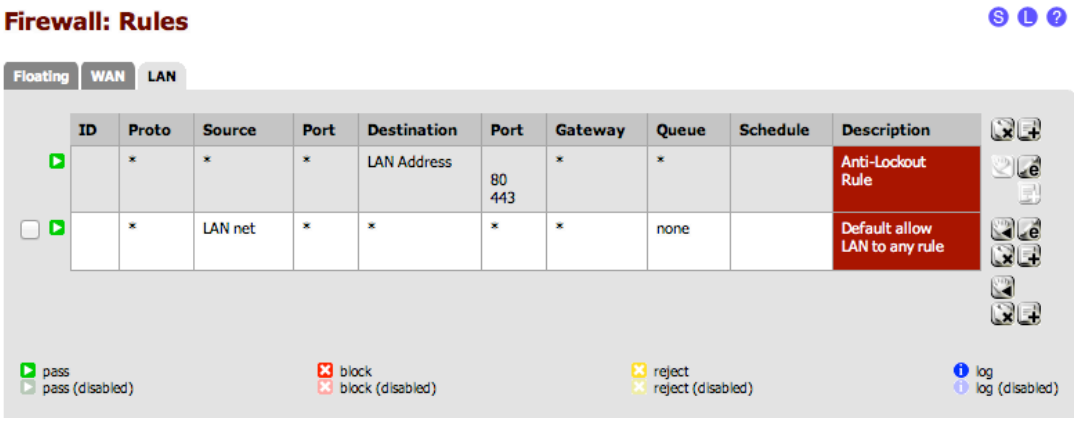
Obrázek 17 - Základní obrazovka PfSense

Uspořádání prvků je jednoduché a zobrazuje potřebné minimum o stavu systému. Jednotlivé moduly lze libovolně uspořádat, přidávat a odebírat. Grafické rozhraní je dost strohé a rozhodně nenabízí takové možnosti jako u Astara.

6.2.2 Funkce routeru

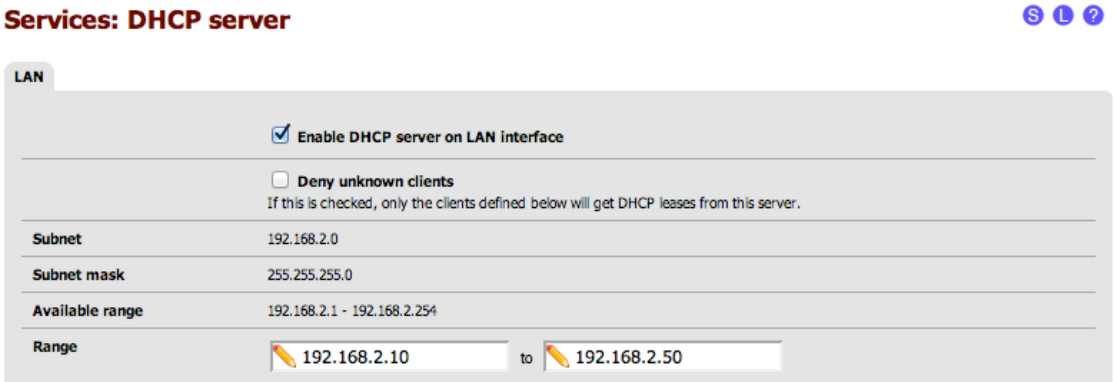
Konfigurace u PfSense není tak jednoduchá a optimalizovaná pro webové rozhraní. Vyžaduje u pár funkcí manuální konfiguraci a znalosti shell příkazů. Co se týká funkcí, tak PfSense v základu obsahuje jen potřebné minimum pro routování a firewall:

- Firewall – lze detailně nastavit pravidla pro jaké rozhraní, zdrojovou nebo cílovou IP adresu, porty, protokoly nebo třeba operační systém počítače, má být přístup povolen nebo zakázán. Nastavit můžeme také omezení rychlostí pro jednotlivá rozhraní (i virtuální).



Obrázek 18 - Přehled pravidel firewallu u PfSense

- Běžné služby (DHCP, DNS, DynDNS, NAT, VLAN)



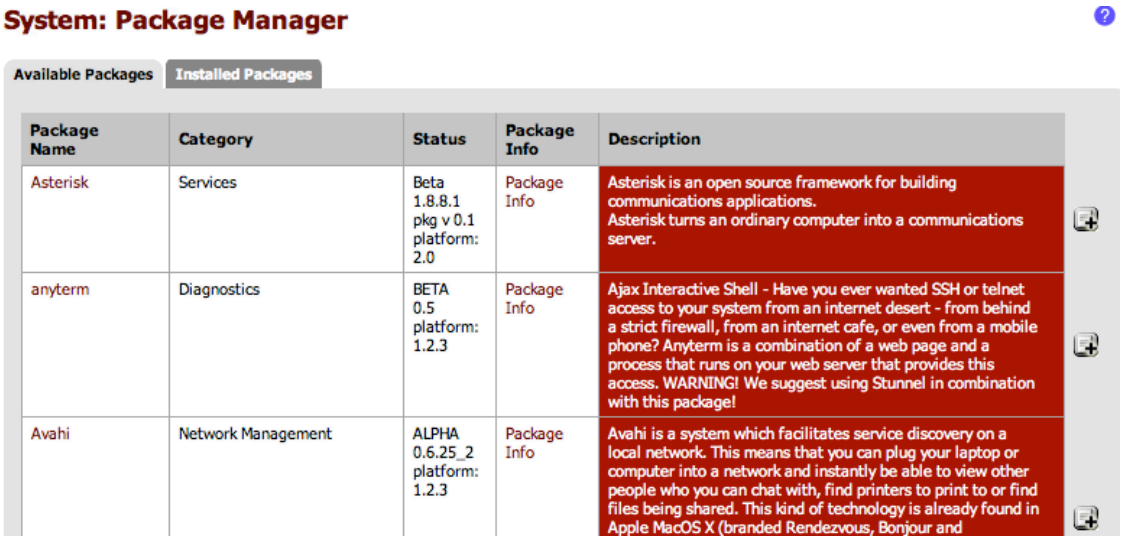
Obrázek 19 - DHCP server u PfSense

- Podporuje také VPN sítě a to protokoly L2TP, IPSec, PPTP i OpenVPN.
- Z pokročilejších zvládá CARP (pro rozložení zátěže v síti), RADIUS autentifikaci

Hlavní výhodou je ovšem volná instalace balíčků a rozšíření pro tuto distribuci. Jelikož je to open-source, tak je k dispozici velká spousta balíčků dostupných zdarma přímo přes webové rozhraní PfSense.

Lze tedy doinstalovat i pokročilé služby jako je:

- IDS/IPS, HTTP Proxy
- HTTP antivirus proxy, Mail scanner
- Dynamické routovací protokoly: BGP, OSPF
- Další různé služby: PHP, TFTP, IM inspector



Obrázek 20 - Správce balíčků u PfSense

6.2.3 Záloha, obnova, údržba

PfSense zvládá klasickou zálohu a obnovu konfigurace (i šifrovaně). Pomocí CARP protokolu si poradí s rozložením zátěže mezi ostatní aktivní prvky sítě, kdy sdílí sadu IP adres, aby nedošlo k přetížení routeru. Využívá při tom i možnosti virtuálních IP adres.

High Availibility backup/restore tato distribuce nenabízí.

Update distribuce probíhá buď automaticky anebo lze zvolit manuálně aktualizační balík. Doinstalované balíčky navíc se musí bohužel updatovat jednotlivě každý zvlášť.

6.3 ClearOS

Obrázek 21 – Logo distribuce ClearOS

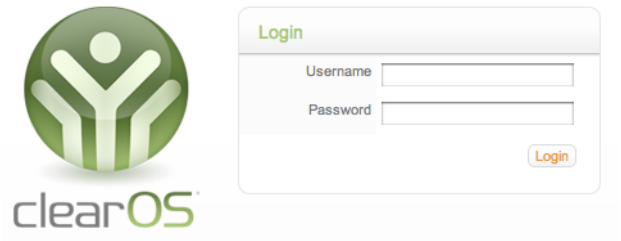
Poslední distribucí v této práci je linuxová distribuce ClearOS. Je ke stažení ve dvou verzích. Jedna je verze ClearOS Community, která je kompletně zdarma a která je použita i do této práce. Druhá verze je ClearOS Proffesional, která je s placenou podporou začínající na ceně ***$280/rok*** pro nekomerční použití a ***$1674/3roky*** pro komerční nebo vzdělávací účely. Na ***5 let*** v plné konfiguraci by tedy byla cena ***55 800 Kč*** s aktuálním kurzem (26. 5. 2012) Verze Proffesional má 30 denní zkušební plnou verzi, podobně jako Astaro.

6.3.1 Instalace, konfigurace, vzhled

Instalace ClearOS je celkem zdlouhavá, ale jako u jediné distribuce z výběru si lze zvolit český jazyk instalace pro snadnější konfiguraci. Po nastavení root účtu systém „nabootuje“ nikoliv do konzolového prostředí jako u dvou předchozích distribucí, ale přivítá nás HTML prostředí přímo na LCD připojeném k sestavě, které umožnuje přihlášení a základní konfiguraci rozhraní pro nastavení IP adres. Do konzole se jde samozřejmě také přepnout.

Přihlášení přes webové rozhraní na připojeném notebooku lze provést na adrese sestavy:

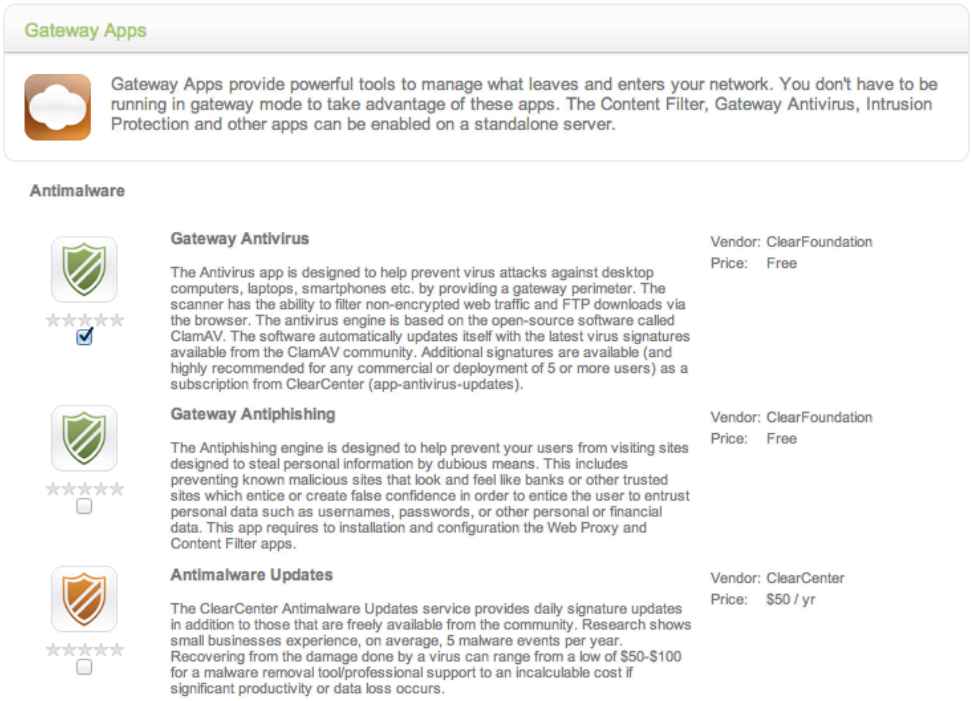
```
https://192.168.2.100:81
```



Obrázek 22 – Přihlášení do ClearOS

Po přihlášení je k dispozici podrobný konfigurační průvodce, který nás provede podrobnějším nastavením služeb rozhraní jako je DHCP, DNS, firewall nebo nastavení domény. V průvodci lze také zvolit jaké aplikace (balíčky) se mají nainstalovat.

ClearOS totiž disponuje přehledným ***Marketplace***, což je místo, kde lze vybrat a nainstalovat různorodé aplikace rozšiřující možnosti a funkce routeru. K dispozici jsou jak aplikace zdarma, tak placené (po nastavení platebních informací). Verze Proffesional má ovšem navíc některé aplikace třetích stran, které nelze zakoupit v ClearOS Community.



Obrázek 23 - Výběr aplikací při prvotní konfiguraci ClearOS

Po delší instalaci aplikací nás přivítá velmi přehledná základní obrazovka ***Dashboard***.

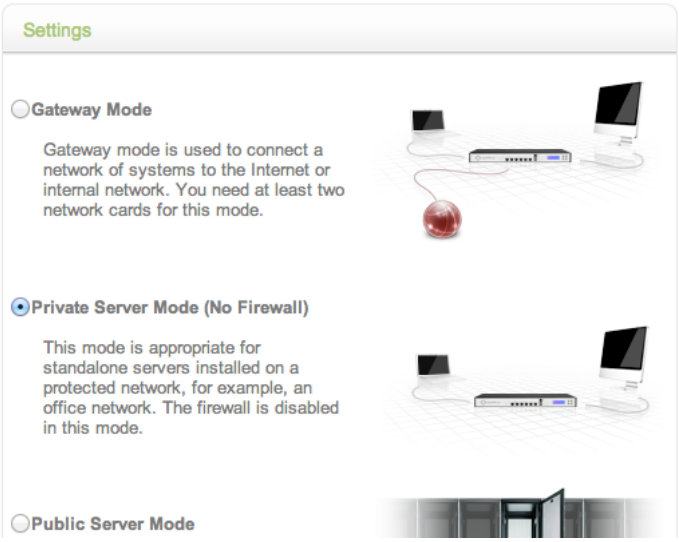
Obrázek 24 - Základní obrazovka u ClearOS

Prostředí je velmi intuitivní a logicky uspořádané, na základní obrazovce máme přehled o vytížení operační paměti. Bohužel nejde základní obrazovku nijak modifikovat či rozšířit o další informace o systému, jako např. u PfSense.

6.3.2 Funkce routeru

ClearOS Community patří k těm vybavenějším distribucím. Lze nastavit do třech módů:

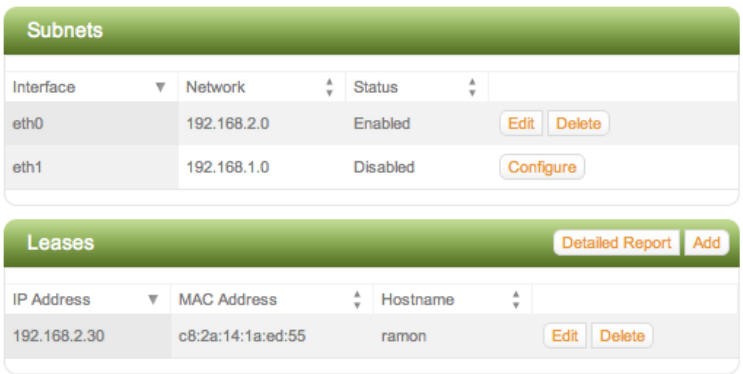
- brána (firewall/router) připojená k Internetu
- privátní server (bez firewallu, v lokální síti)
- veřejný server



Obrázek 25 - Režimy distribuce

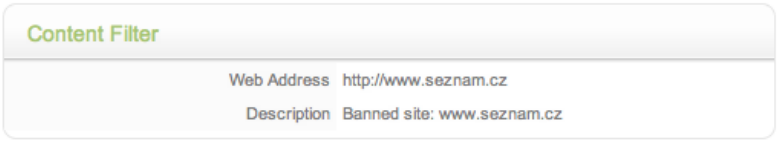
Pro naše účely je nastavena jako router s připojením k Internetu. ClearOS nabízí:

- klasické routovací funkce (DHCP, DNS a SSH server)

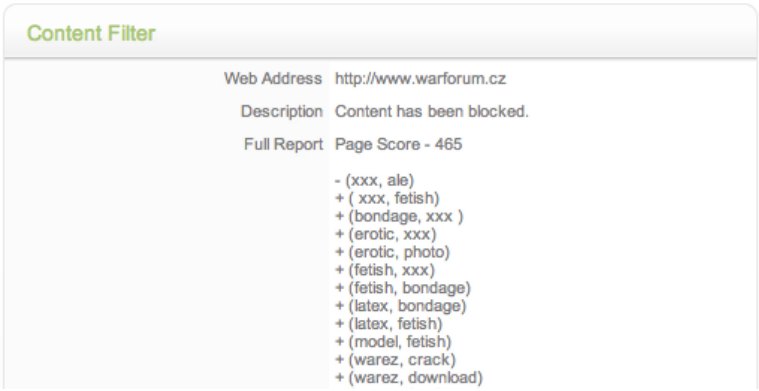


Obrázek 26 - DHCP server u ClearOS

- firewall (jak na úrovni portů a adres, tak na úrovni služeb), port forwarding
- web proxy, web access control (nastavení nejen časového přístupu na web pro skupiny počítačů podle IP nebo MAC adres)
- web filtering (blokování stránek na základě zjištěného obsahu dle kategorií, manuálního zadání URL konkrétní stránky nebo přípon souborů)



Obrázek 27 - Blokování webu na základě URL u ClearOS

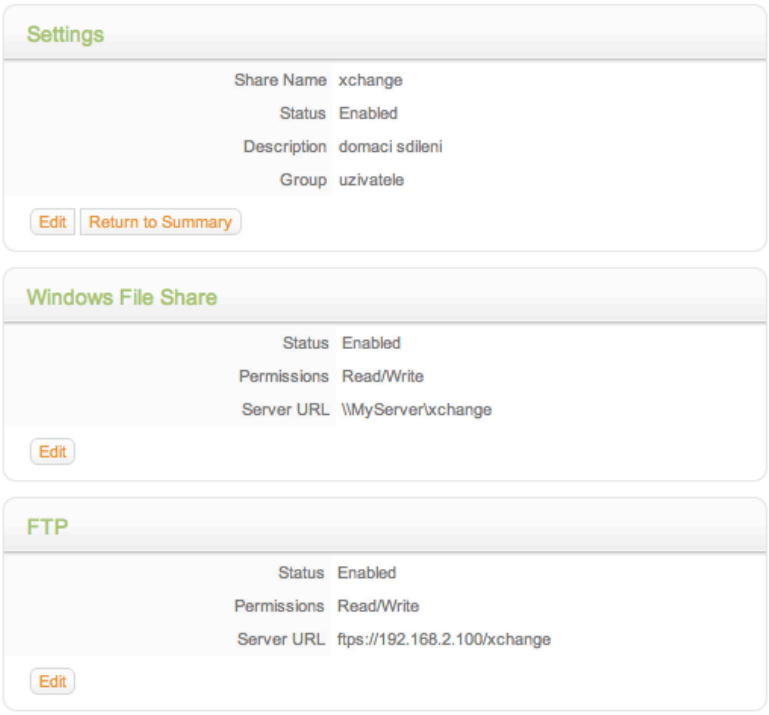


Obrázek 28 - Blokování webu na základě obsahu u ClearOS

- antivirus a antiphishing, QoS
- VPN služby (IPSec, OpenVPN a PPTP)
- IDS/IPS v podobě aplikací v Marketplace
- ***nenabízí*** podporu VLAN ani High Availability backup/restore

Velkou výhodou je již zmiňovaný Marketplace, kdy si v případě chybějící služby jednoduše aplikaci stáhnete a nainstalujete. Takto lze rozšířit ClearOS například o ***domácí sdílení souborů*** nebo webový server. Sdílení souborů lze jak přes FTP, tak přes SAMBU systém na Windows platformě. Stejně tak lze z ClearOS udělat doménový server pro správu uživatelů Active Directory, nebo MySQL server.

Možnosti jsou velké a vše lze nastavit a zprovoznit jednoduše přes webové rozhraní bez nějakých extra konfigurací v konzole.



Obrázek 29 - Sdílení souborů v síti u ClearOS

Každému uživateli nebo skupině uživatelů lze přiřadit přistup na FTP s tím, že každý má svůj prostor na disku FTP serveru (routeru) a vidí tak jen své soubory (lze jim nastavit práva čtení/zápis). Pro domácí sdílení nastaven speciální port pro FTP.

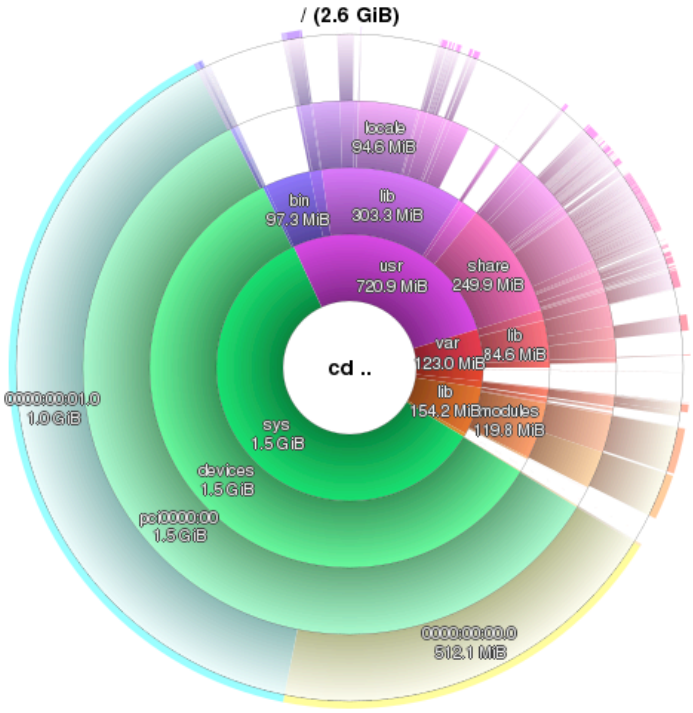
Windows sdílení je pro uživatele ve stejné doméně nebo s doménovým účtem, kdy se každý může dostat ke stejným sdíleným datům.

6.3.3 Záloha, obnova, údržba

V tomto směru ClearOS distribuce trochu pokulhává. Nabízí pouze standartní zálohu a obnovu konfigurace na lokální disk, která nejde zautomatizovat nebo zasílat na e-mail.

High Availability nepodporuje ani placená verze Proffesional. Výhodou je správa SSL certifikátů.

Aktualizace systému jsou automatické a systém Vás na ně upozorní. Užitečný je i přehled a rozložení dat na pevném disku.



Obrázek 30 - Využití místa na HDD u ClearOS

6.4 Router Fortigate 60C

Obrázek 31 - Logo společnosti Fortinet

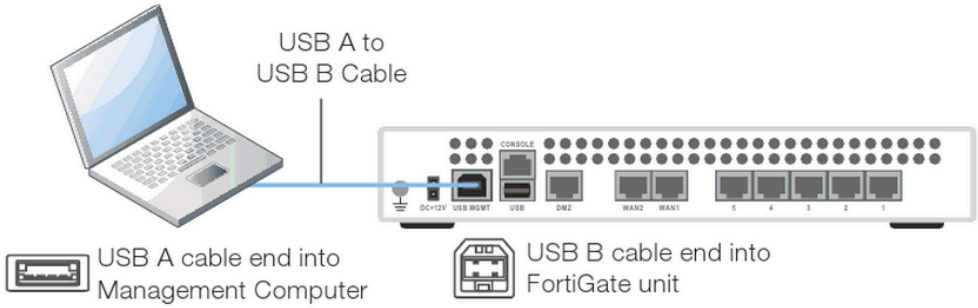
Pro srovnání s linuxovými distribucemi, které nám z běžného PC vytvoří plnohodnotný router a firewall, mně byl firmou HP Tronic doporučen a zapůjčen router Fortigate 60C od společnosti Fortinet.

Je to profesionální hardwarový router vhodný nejen pro podnikovou vzdělávací sféru a využití. Hardwarové vlastnosti jsou popsány v kapitole 5.1.2.

Router pohání vestavěný firmware (operační systém) FortiOS 4.0, který je uzpůsoben pro velkou rychlost dnešních sítí a jejich maximální zabezpečení.

6.4.1 Instalace, konfigurace, vzhled

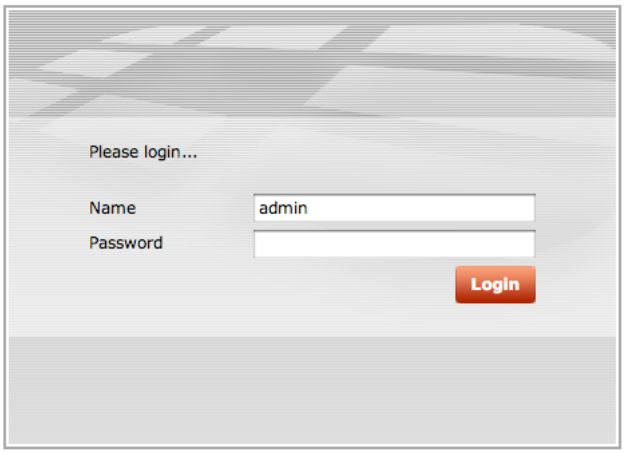
Fortigate 60 přichází s již předinstalovaným systémem FortiOS. Pro prvotní zapojení a nastavení je ale potřeba připojit router k PC pomocí přibaleného USB kabelu a z CD, které taktéž najdeme v balení, spustit program FortiExplorer. Ten nás provede nastavení administrátorského hesla a základní konfigurací portů, abychom byli schopni se na router poté přes síť připojit.



Obrázek 32 - Prvotní konfigurace routeru [9]

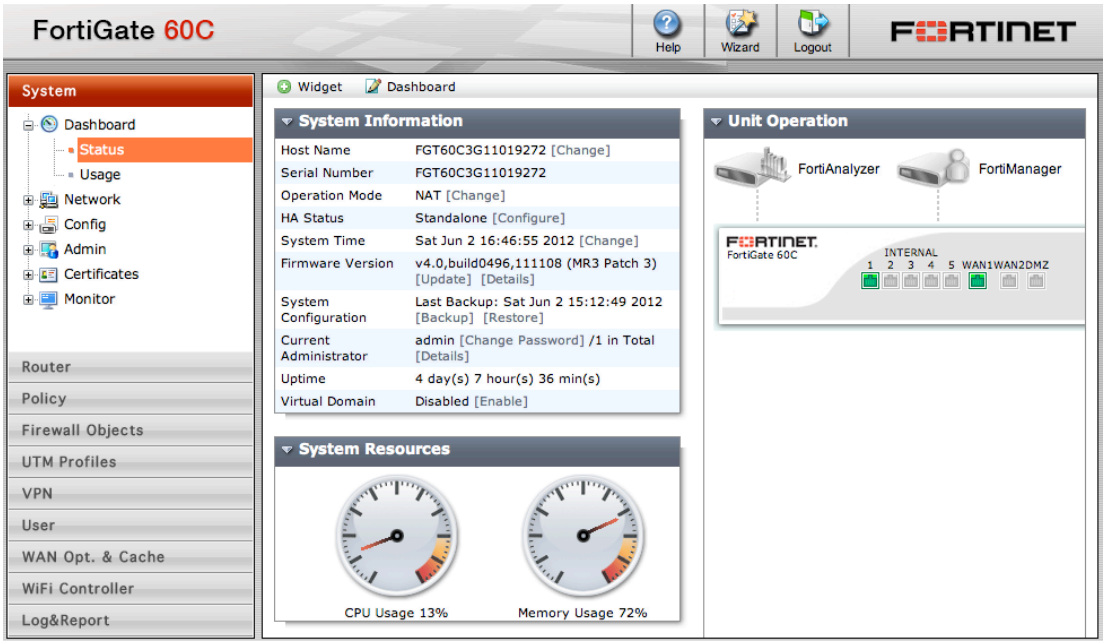
Nyní se dá na router připojit po síti přes webové rozhraní. V našem případě na adresu:

`https://192.168.2.1`



Obrázek 33 - Přihlášení na router Fortigate

Po zabezpečeném připojení po síti se můžeme pustit do konfigurace buď manuálně, nebo pomocí rychlého průvodce, který nás potřebný nastavením provede.



Obrázek 34 - Základní obrazovka Fortigate

Základní obrazovka je přehledná s možností uspořádat si jednotlivé moduly podle sebe nebo vytvořit zcela nový „dashboard“ a i ten si upravit podle sebe. Z modulů lze zvolit:

- Systémové informace s přehledem o systému, jeho firmware či zálohách nastavení
- Vytížení procesoru a operační paměti
- Přehled o aktivních a neaktivních portech a připojení
- Správa licencí (licence pro technickou podporu, pro FortiGuard služby – antivirus, IPS, Web filtering a jiné)
- Přehledy o vytížení sítě, historie připojení jednotlivých PC v síti apod.

6.4.2 Funkce routeru

Fortigate 60C nabízí komplexní ochranu vaší sítě. Ačkoliv je pořizovací cena celkem vysoká, tak přesto je potřeba pro používání všech možných služeb mít tyto služby předplaceny, nazývají se FortiGuard. To samé platí i o technické podpoře – FortiCare.

Fortinet nabízí tzv. Bundle balíčky, které obsahují jak technickou podporu FortiCare, tak veškeré FortiGuard služby (Antivir a Antispyware, Intrusion Prevention System (IPS), Web Content Filtering, Antispam pro e-maily). Předplatné je možné volit až na 5 let.

Tabulka 3 - Ceny dokoupení podpory

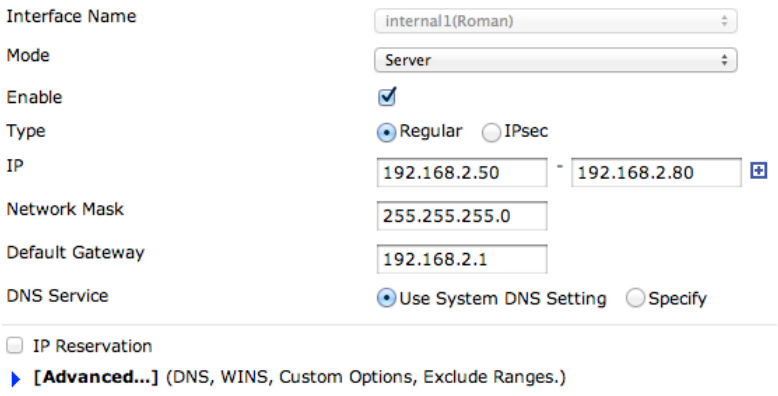
Režim podpory	**Cena/5let**
8 x 5 email a web podpora, aktualizace software a firmware,	**10 325 Kč**
zaslání nového boxu do 3 dnů od obdržení vadného	
24 x 7 telefonická a web podpora, aktualizace software a firmware,	**17 075 Kč**
zaslání nového boxu 1 den po nahlášení závady, vadný box se	
odešle až po obdržení nového, dopravu platí výrobce	

Tabulka 4 - Ceny včetně FortiGuard služeb

Režim Bundle	**Cena/5let**
8 x 5 email a web podpora, aktualizace software a firmware,	**29 450 Kč**
zaslání nového boxu do 3 dnů od obdržení vadného	
včetně všech služeb FortiGuard	
24 x 7 telefonická a web podpora, aktualizace software a firmware,	**38 275 Kč**
zaslání nového boxu 1 den po nahlášení závady, vadný box se	
odešle až po obdržení nového, dopravu platí výrobce	
včetně všech služeb FortiGuard	

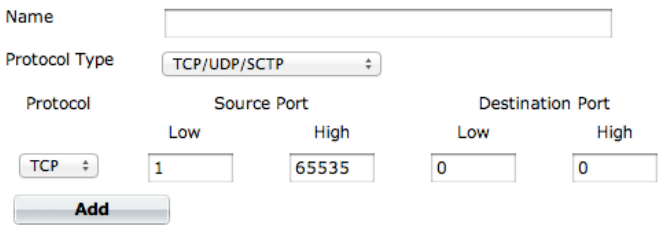
Bohužel nebylo možné tyto funkce reálně otestovat, neboť je firma HP Tronic nemá momentálně předplaceny. Po dokoupení všech služeb tak router podporuje:

- routovací funkce (statické i dynamické – BGP, OSPF, RIP) mezi rozhraním i VLAN sítěmi, IPv6 podpora, DHCP server, DNS server, proxy



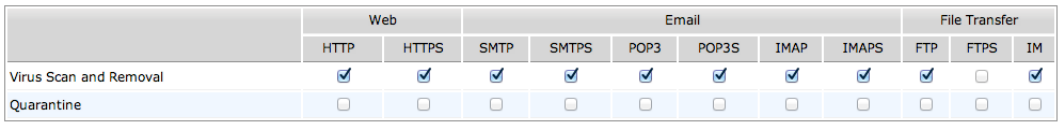
Obrázek 35 - DHCP server u Fortigate

- kompletní firewall splňující nejvyšší certifikaci ICSA Labs



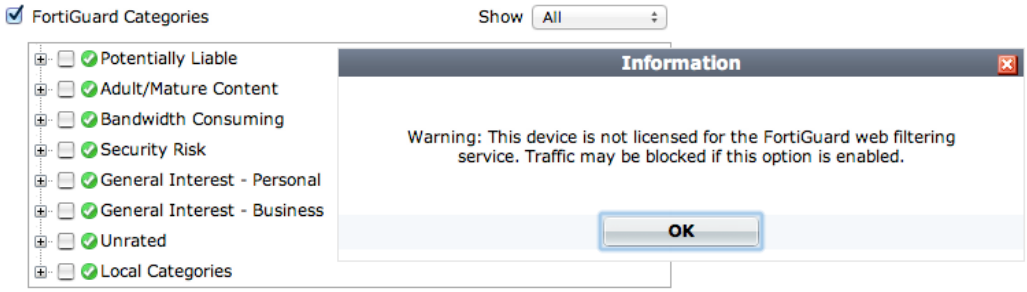
Obrázek 36 - Vytvoření pravidla firewallu

- antivirus a antispyware, také s ICSA Labs certifikací, kontrola protokolů HTTP/S, SMTP/S, IMAP/S, POP3/S, FTP, IM protokoly



Obrázek 37 - Antivirus u Fortigate

- VPN – s ICSA Labs certifikací, podpora IPSec, PPTP, L2TP, SSL
- Antispam – kontrola mailů, protokoly SMTP/S, POP3/S, IMAP/S, real-time blacklist, filtrování frází, slovních spojení
- Web filtering - 76 kategorií, přes 2 biliony stránek v evidenci, URL blokování



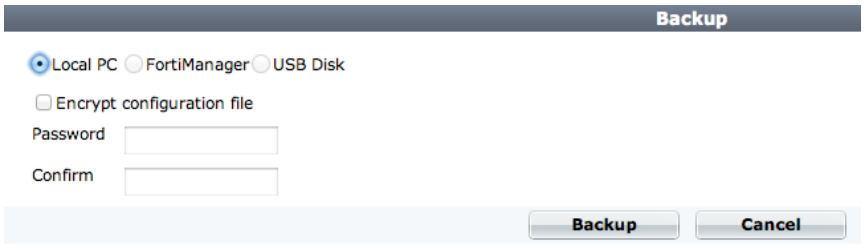
Obrázek 38 - Blokování obsahu webu – chybí licence

- Kontrola aplikací a internetových služeb, IDS/IPS, Data Loss Prevention
- High availability – aktivní-aktivní, aktivní-pasivní, samostatně, detekce selhání

Oproti distribucím nelze u Fortigate dokoupit nebo přidat další jiné funkce a služby, pouze výše zmíněné. Na druhou stranu je zase výkonější a obsahuje více portů.

6.4.3 Záloha, obnova, údržba

V této oblasti Fortigate obsahuje všechny dostupné funkce, jaké by měl podnikový router mít. Zálohu konfigurace lze provádět manuálně nebo využít funkci High Availability, která při poškození nebo výpadku routeru zařídí plynulý přechod na druhý router k tomuto účelu určený.



Obrázek 39 - Možnosti zálohy konfigurace Fortigate

Fortigate dále umožňuje správu certifikátů, pokročilé monitorování sítě, možnost úpravy systémových zpráv (např. při blokování obsahu webu) a samozřejmě správu uživatelů a skupin. Umí také správu a řízení WiFi sítí v infrastruktuře.

7 ZHODNOCENÍ ŘEŠENÍ

V celkovém hodnocení bude brán ohled především na požadavky firmy HP Tronic. U jednotlivých distribucí bylo těžké srovnat a sjednotit ceny za služby, neboť to má každý výrobce uváděné jinak. U Astara jsou uváděny ceny licencí pro minimální počet 10 zařízení v síti, přičemž vycházím z použití maximálně 20-ti zařízení v síti. Pro sjednocení budu počítat se stejným počtem zařízení i u ostatních distribucí i routeru Fortigate. U ClearOS se u free Community verze dají přikoupit jednotlivé služby bez technické podpory, ale u Professional s technickou podporou lze zakoupit licenci pouze se všemi službami. Proto jsou propočty pouze orientační, abych mohl sjednotit odpovídající výbavu distribucí s routerem Fortigate. V hodnocení jsou také zahrnuty poplatky spojené s provozem za 5 let užívání.

7.1 Uživatelské zhodnocení

Z uživatelského hlediska je brán důraz hlavně na snadnou a přehlednou správu systému. Hodnoceno je intuitivní ovládání, konfigurace a logičnost celého systému. Dále také snadná možnost zálohování. Subjektivní plusy a minusy jsou zde:

Tabulka 5 - Plusy a minusy řešení

ASG	PfSense	ClearOS	Fortigate 60C
+ profesionální vzhled + nabídka funkcí + High Availability	+ rychlost instalace + instalace balíčků + cena (zdarma)	+ přehlednost + jednoduchost + Marketplace (aplikace) + rozšiřitelnost (FTP)	+ odezva systému + jednoduchost + technická podpora + spotřeba
- neuspořádanost - pomalejší odezva - cena	- nelogičnost menu - nefunkčnost některých balíčků a funkcí - vzhled	- slabé zálohovací možnosti - chybí podpora VLAN	- pořizovací cena - uzavřenost systému

7.2 Finanční zhodnocení

Výběr vhodného řešení spočívá hlavně v účelu jeho používání, v jak velké síti bude router fungovat a jak bude potřeba zabezpečit síť a data v ní. V HP Tronicu by se jednalo o menší pobočky a prodejny. K tomuto účelu nám router v podobě distribuce bude stačit. Jednotlivá řešení jsou různě a nesourodě ceněny.

Pokusím se do tabulky cenově srovnat jejich náklady v rozmezí ***5 let*** nepřetržitého provozu včetně jejich spotřeby elektrické energie. Spotřeba u všech tří distribucí bude stejná, jelikož jsou testovány na stejné počítačové sestavě.

Ceny služeb jak u distribucí tak u Fortigate routeru zahrnují (pokud to umožňují):

- Telefonickou nebo webovou podporu
- Odpověď nebo dodání nového zařízení (Fortigate) do 1 dne
- Plnou nabídku uváděných služeb (Antivir, Antispam, pokročilou ochranu sítě, atd.)

Průměrná cena energie je brána k datu 26. 5. 2012 ve výši ***5 Kč/kWh***.

Tabulka 6 - Výsledné cenové srovnání

	ASG	**PfSense**	**ClearOS**	**Fortigate**
30 denní verze zdarma	ANO	NE	ANO	NE
Zapůjčení zařízení na test	NE	NE	NE	ANO
Placená podpora	ANO	ANO	ANO	ANO
Placené plné využití služeb	ANO	NE	ANO	ANO
Spotřeba energie	58W	58W	58W	16W
Cena hardware + systém	7 080 Kč	7 080 Kč	7 080 Kč	27 750 Kč
Cena služeb a podpory (5 let)	96 260 Kč	20 580 Kč	55 800 Kč	38 275 Kč
Spotřeba elektřiny (5 let)	12 702 Kč	12 702 Kč	12 702 Kč	3 504 Kč
Celková cena (5 let)	116 042 Kč	40 362 Kč	75 582 Kč	69 529 Kč

V plné výbavě a s podporou se cenově nejvýhodnější nabídkou stala PC sestava s nainstalovanou distribucí PfSense na hodnotě 40 362 Kč za 5 let. Za to nejdražší se jeví řešení Astaro Security Gateway, kdy nás cena za 5 let vyjde přes 115 tisíc korun. Router Fortigate a distribuce ClearOS zůstaly cenově uprostřed.

Co se týká funkcí a profesionálních služeb se však například PfSense, které je víceméně open-source projekt nemůže rovnat kvalitě a stabilitě ostatním distribucím (hlavně ASG, které je na tom funkčně nejlépe) i routeru v testu, takže je potřeba *zvážit náklady na servis a údržby systému*, které se za 5 let můžou vyšplhat na vysokou částku.

Dále nastává otázka, zda se využije veškerých služeb, co systémy nabízí. Pokud bychom vynechali například u ClearOS plnou nabídku služeb a podpory (55 800 Kč) a zůstali

pouze na free verzích případně dokoupili jednotlivě potřebné řešení v Marketplace, dostaneme se na částku ***nepřevyšující 25 tisíc Kč***, což je velmi přijatelná cena v poměru výkonu a kvality zpracování distribuce ClearOS, kde mírně PfSense zaostává.

Při vynechání předplacených služeb a podpory u ASG nám zůstane pouze firewall se základními funkcemi. Lze dokoupit jednotlivé moduly, ale tím se pak dostaneme vysoko nad cenu ClearOS nebo PfSense, které toto splňují bez navýšení základní ceny (cena sestavy + spotřeba).

V poměru cena/kvalita vyšel dobře, i přes vysokou pořizovací cenu, router Fortigate 60C. Za plnou funkčnost a profesionální podporu zaplatíme za 5 let necelých 70 tisíc Kč. Při vynechání podpory a služeb navíc se dostaneme na částku kolem ***30 tisíc***, což je ale pořád více než nabízí distribuce ClearOS.

7.3 Celkové zhodnocení

Celkově se ze srovnávaných distribucí jeví jako nejlepší řešení, v poměru ceny a výkonu, PC sestava a na ní nainstalována distribuce ***ClearOS***. Hned za ní je ale samotný router ***Fortigate 60C***. V porovnání s ním má ClearOS v základní nabídce, která je zdarma, více funkcí a služeb než má Fortigate a dále je lze rozšiřovat. Má nejpřehlednější a intuitivní prostředí ze všech hodnocených řešení.

Oproti tomu ClearOS nenabízí ani po rozšíření podporu pro VLAN sítě ani High Availability backup/restore.

Distribuce PfSense sice vyšla jako nejlevnější řešení ovšem s podporou, která se nemůže rovnat například s podporou od Fortinetu. Je tu brán zřetel hlavně na nabídku funkcí, než na jejich kvalitu a zpracování, což není nejvhodnější řešení pro podnikovou síť.

Astaro za to disponuje funkcemi, kvalitou a množstvím služeb, ovšem za vysokou cenu. Při omezení hlavních bezpečnostních služeb na nutné minimum je i tak provozní cena vysoká oproti srovnatelné distribuci ClearOS.

ZÁVĚR

Hlavním cílem této bakalářské práce bylo vybrat vhodné řešení, které by dokázalo v plné míře nahradit nákladnější routery a uspořit tak firmě HP Tronic nemalé finance, vzhledem k počtu poboček a prodejen. Řešení spočívá v linuxové distribuci nainstalované na běžně dostupném počítači, kdy koncový uživatel nebo firma platí jenom náklady na hardware a provoz sestavy.

Tento předpoklad by se naplnil, pokud bychom vybírali z řad open-source projektů bez technické podpory. Ovšem fungování v podnikové sféře vyžaduje určitou kvalitu a dostupnost služeb. Proto byly zvoleny do srovnání v této práci distribuce s možností dokoupení podpory a dalších služeb.

Po výsledném vyhodnocení z uživatelského (subjektivního) a finančního pohledu a po zvážení všech výhod, nevýhod a praktických zkušeností vyšla z distribucí nejvýhodněji distribuce ClearOS.

Nabízí srovnatelný komfort v ovládání, kvalitu a možnosti jako router Fortigate 60C. S plnou podporou a službami je řešení v podobě ClearOS finančně víceméně srovnatelné s cenovou politikou Fortigate 60C a nabízí oproti tomu další služby navíc (FTP, SAMBA).

Při omezení podpory pouze na webovou komunitu a vynechání placených služeb, které ne vždy využijeme, vychází mnohem výhodněji distribuce ClearOS. Navíc velké množství placených služeb nabízí ClearOS v omezené verzi zdarma.

Vezmeme-li však v potaz požadavky v podobě VLAN a High Availability, které se používají převážně u větších a podnikových sítí, tak nám dle celkového zhodnocení vyjde jako nejlepší a nejlevnější varianta router Fortigate 60C. Tyto požadavky zároveň totiž nesplňuje mnoho distribucí, a pokud ano, tak jsou finančně nákladné (viz. Astaro). V konečném výsledku tedy záleží na zhodnocení vlastních potřeb s ohledem na velikost sítě a potřebného zabezpečení.

ClearOS je vyhovující pro malé firemní i nefiremní sítě a domácnosti, které spojují 20 až 30 počítačů a síťových zařízení se základním zabezpečením.

Pro podnikové sítě čítající stovky propojených zařízení se jako nejlepší varianta jeví router Fortigate 60C, který nabízí pokročilé funkce a zabezpečení, rozsáhlou a rychlou podporou a je v cenově rozumné hladině.

ZÁVĚR V ANGLIČTINĚ

The main objective of this work was to select a solution that could fully replace expensive routers and save the HP Tronic considerable finances, given the number of branches and stores. The solution lies in a Linux distribution installed on commonly available computers, where the end user or company pays only the cost of hardware and operating reports.

This assumption would be filled if we chose from among the open-source projects without technical support. However, the functioning of the corporate sector requires a certain quality and availability of services. In this work are just distributions with option of support and other services.

After the final evaluation from the user (subjective) and financial point of view and considering all the advantages, disadvantages and practical experience is the best choice ClearOS distribution.

It offers comparable control, quality and options such as Fortigate router 60C. With the full support and services is ClearOS comparable with pricing of Fortigate 60C and also offer other additional services (FTP, SAMBA).

When restrictions on aid to the Web community and the omission of paid services, distribution ClearOS is much more favorable. In addition, a large number of paid services ClearOS offers in a limited free version.

If you need features such as VLAN and High Availability, which are mainly used for larger and enterprise networks, the Fortigate router 60C is the best and cheapest option. These requirements also does not have many distributions, and if so, are expensive (see Astaro). The final outcome depends on the assessment of our needs with regard to the size of the network and the necessary security.

ClearOS is suitable for small business and non-business and home networks that connect the 20 to 30 computers and network devices with basic security.

For business networks comprising hundreds of interconnected devices to be the best option seems to Fortigate router 60C, which offers advanced features and security, extensive and rapid support and is priced at a reasonable level.

SEZNAM POUŽITÉ LITERATURY

[1] BIGELOW, Stephen J. *Mistrovství v počítačových sítích*: *správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Překlad Petr Matějů. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[2] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*: *kuchařka administrátora sítě*. 5., aktualiz. vyd. Brno: Computer Press, 2011, 303 s. ISBN 978-802-5131-763.

[3] SOSINSKY, Barrie. *Mistrovství – počítačové sítě*. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-802-5133-637.

[4] SCHRODER, Carla. *Linux*: *kuchařka administrátora sítě*. Vyd. 1. Brno: Computer Press, 2009, 596 s. ISBN 978-802-5124-079.

[5] NEMETH, Evi, Garth SNYDER a Trent R HEIN. *Linux*: *kompletní příručka administrátora: 2. aktulizované vydání*. Vyd. 1. Brno: Computer Press, 2008, 984 s. ISBN 978-802-5124-109.

[6] PETERKA, Jiří. *Jiří Peterka*: *Archiv článků a přednášek* [online]. 2006 [cit. 2012-05-20]. Dostupné z: http://www.earchiv.cz/

[7] *Automa*: *Časopis pro automatizační techniku* [online]. 2005 [cit. 2012-05-12]. Dostupné z: http://www.odbornecasopisy.cz/

[8] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

[9] FORTINET, Inc. [online]. ©2011 [cit. 2012-01-31]. Dostupné z: http://www.fortinet.com/

[10] ODOM, Wendell, Rus HEALY a Naren MEHTA. *Směrování a přepínání sítí*: *autorizovaný výukový průvodce*. Vyd. 1. Brno: Computer Press, 2009, 55 - 60. ISBN 9788025125205.

[11] LOMNICKÝ, Marek a Vladimír VESELÝ. *Směrování a směrovací protokoly* [online]. Brno, 2007 [cit. 2012-05-15]. Dostupné z: http://netacad.fit.vutbr.cz/texty/ccna-moduly/ccna2-6.pdf. Seminární práce. FIT VUT Brno.

[12] *Mini-box Power Calculator* [online]. 2006 [cit. 2012-05-26]. Dostupné z: http://www.mini-box.com/site/mb/Power_MB.htm

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARP	Adress Resolution Protocol
ASP	Active Server Pages
BGP	Border Gateway Protocol
CAM	Content Addresable Memory
CAN	Campus Area Network
CGI	Common Gateway Interface
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarised Zone
DNS	Domain Name System
FTP	File Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IM	Instant Messaging
IP	Internet Protocol
IPS	Intrusion Protection System
IPSec	Internet Protocol Security
ISO	International Organization for Standartization
ISP	Internet Service Provider
LAN	Local Area Network
LSA	Link-State Advertisment
MAC	Media Access Control
MAN	Metropolitan Area Network
NAT	Network Address Translation

OSI	Open System Interconnection
OSPF	Open Shortest Path First Protocol
PAN	Personal Area Network
POP3	Post Office Protocol
QoS	Quality of Service
RAM	Random Access Memory
RIP	Routing Information Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCAM	Ternary Content Addressable Memory
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VLAN	Virtual Local Area Network
VoIP	Voice Over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access

SEZNAM OBRÁZKŮ

Obrázek 1 - Třídy IP adres [6] 17
Obrázek 2 - Skupiny dynamických protokolů [11] 22
Obrázek 3 - Porty na desce [12] 31
Obrázek 4 - Fortigate 60C 32
Obrázek 5 - Logo distribuce Astaro 35
Obrázek 6 - Přihlašovací obrazovka 36
Obrázek 7 - Základní obrazovka Astaro distribuce 36
Obrázek 8 – Záložka Interface u Astaro 37
Obrázek 9 - DHCP server u Astaro 37
Obrázek 10 - NAT (překlad adres) 38
Obrázek 11 - Pokus o přístup na blokovanou stránku 38
Obrázek 12 - Záloha nebo obnova konfigurace 39
Obrázek 13 - High Availability u Astaro 39
Obrázek 14 - Update systému Astaro 40
Obrázek 15 - Logo distribuce PfSense 40
Obrázek 16 - Přihlášení do PfSense 41
Obrázek 17 - Základní obrazovka PfSense 41
Obrázek 18 - Přehled pravidel firewallu u PfSense 42
Obrázek 19 - DHCP server u PfSense 42
Obrázek 20 - Správce balíčků u PfSense 43
Obrázek 21 – Logo distribuce ClearOS 44
Obrázek 22 – Přihlášení do ClearOS 44
Obrázek 23 - Výběr aplikací při prvotní konfiguraci ClearOS 45
Obrázek 24 - Základní obrazovka u ClearOS 45
Obrázek 25 - Režimy distribuce 46
Obrázek 26 - DHCP server u ClearOS 46
Obrázek 27 - Blokování webu na základě URL u ClearOS 47
Obrázek 28 - Blokování webu na základě obsahu u ClearOS 47
Obrázek 29 - Sdílení souborů v síti u ClearOS 48
Obrázek 30 - Využití místa na HDD u ClearOS 49
Obrázek 31 - Logo společnosti Fortinet 49
Obrázek 32 - Prvotní konfigurace routeru [9] 50

Obrázek 33 - Přihlášení na router Fortigate 50
Obrázek 34 - Základní obrazovka Fortigate 51
Obrázek 35 - DHCP server u Fortigate 52
Obrázek 36 - Vytvoření pravidla firewallu 53
Obrázek 37 - Antivirus u Fortigate 53
Obrázek 38 - Blokování obsahu webu – chybí licence 53
Obrázek 39 - Možnosti zálohy konfigurace Fortigate 54

SEZNAM TABULEK

Tabulka 1 - Cena sestavy (včetně DPH) 32
Tabulka 2 - Ceny licencí k 26. 5. 2012 na internetu vč. DPH 35
Tabulka 3 - Ceny dokoupení podpory 52
Tabulka 4 - Ceny včetně FortiGuard služeb 52
Tabulka 5 - Plusy a minusy řešení 55
Tabulka 6 - Výsledné cenové srovnání 56

SEZNAM PŘÍLOH

P I DVD s elektronickou verzí bakalářské práce a obrazy pro instalace distribucí Astaro Security Gateway, PfSense a ClearOS