Univerzita Pardubice
Fakulta ekonomicko-správní

Zabezpečení počítačové sítě – e-learningový kurz

Michal Nykodým

Bakalářská práce

2011

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2010/2011**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michal NYKODÝM**
Osobní číslo:	**E07895**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Zabezpečení počítačové sítě - e-learningový kurz**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Práce bude mít následující strukturu:
Shromáždění poznatků z oblasti zabezpečení počítačové sítě
Vytyčení konkrétního postupu při analýze zabezpečení počítačové sítě
Návrh konkrétního postupu pro zabezpečení počítačové sítě
Vytvoření e-learningového kurzu

Rozsah grafických prací:

Rozsah pracovní zprávy: **30 - 40 stran**

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

Seznam odborné literatury:

1. BAREŠOVÁ, A. E-Learning ve vzdělávání dospělých. 1. vyd. Praha: VOX, 2003. 174 s. ISBN 80-86324-27-3.

2. PETERKA, J. EArchiv.cz [online]. [2010] [cit. 2010-06-15]. Dostupný z WWW: <http://www.earchiv.cz/>.

3. PUŽMANOVA, R. TCP/IP v kostce. 1. vyd. České Budějovice: Kopp, 2004. 607 s. ISBN 80-7232-236-2.

4. SCAMBRAY, J., MCCLURE, S. Hacking bez tajemství. 1. vyd. Praha: Computer Press, 2003. 461 s. ISBN 80-7226-781-7.

5. TANENBAUM, A., S. Computer networks. Upper Saddle River: Prentice Hal, 1996. 813 s. ISBN 0-13-394248-1.

Vedoucí bakalářské práce: **Ing. Pavel Jirava, Ph.D.**
Ústav systémového inženýrství a informatiky

Konzultant bakalářské práce: **doc. Ing. Jitka Komárková, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **5. října 2010**

Termín odevzdání bakalářské práce: **6. května 2011**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 5. října 2010

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Kolíně dne 28. 06. 2011

Michal Nykodým

Poděkování

Rád bych touto cestou poděkoval Ing. Pavlovi Jíravovi, Ph.D a doc. Ing. Jitce Komárkové, Ph.D. za cenné připomínky a rady k obsahu práce. Dále děkuji všem, kteří mi poskytli informace, podklady a materiály, bez nichž by má práce nemohla vzniknout.

ANOTACE

Práce je věnována zabezpečení počítačové sítě. Stěžejním úkolem této práce je vytvoření E-learningového kurzu, který má sloužit studentům Fakulty ekonomicko-spravní v Pardubicích jako studijní opora předmětu „Počítačové sítě I“. V první části kurzu jsou shromážděny poznatky z oblasti zabezpečení počítačových sítí. V druhé části kurzu je vytyčen konkrétní postup analýzy zabezpečení počítačové sítě. V poslední části kurzu je vytvořen konkrétní návrh postupu pro zabezpečení počítačové sítě.

KLÍČOVÁ SLOVA

Zabezpečení, počítačová síť, firewall, VPN, UPS, hardware, záloha.

TITLE

Computer network security – e-learning course

ANNOTATION

The work is devoted to computer network security. The main task of this work is to create e-learning courses to serve students of the Faculty of Economics and Administration in Pardubice as study support the course "Computer Networks". In the first part of the course are collected knowledge of the security of computer networks. In the second part of the course pursued by the specific analytical procedure, computer network security. In the last part of the course is designed for a specific proposal for the security of computer networks.

KEYWORDS

Security, computer network, firewall, VPN, UPS, hardware, advance.

Úvod

Nasazení informačních systémů a informačních technologií se v dnešní době stalo nutnou podmínkou úspěšnosti a v konečném důsledku i existence firem ve všech oblastech hospodářské činnosti. Informační technologie zaznamenaly v posledních desetiletích nebývalý rozmach a staly se jedním z rozhodujících faktorů rozvoje a konkurenceschopnosti hospodářských organizací. Jejich informační systémy dnes zajišťují chod jak výrobních podniků, státní správy, zdravotnictví, finančnictví a mnoha dalších odvětví. Práce s informacemi by se bez informačních technologií stala jednak neefektivní a také velmi zdlouhavou. Informační technologie znamenají pro lidstvo nezměrnou úsporu času i energie.

S prudkým rozvojem moderních technologií informačních systémů vzrůstá však i možnost jejich zneužití. Počítačová kriminalita, zneužívání údajů, elektronické krádeže a podvody se staly zcela běžnou realitou našeho života a zažívají stejně jako IT technologie obrovský boom.

S přibývajícím počtem počítačových sítí vzrůstá potřeba jejich kvalitního zabezpečení. Právě zabezpečení je jednou z nejdiskutovanějších oblastí IT. Při nejrůznějších útocích jsou v sázce citlivá data, služby, obchodní tajemství, tedy veškeré informace proudící tou kterou počítačovou sítí. Útoky se stávají stále propracovanější a méně odhalitelné, vynalézavost hackerů prakticky nezná mezí a tak neustále prověřuje kvalitu a stabilitu síťových zabezpečení. Slova jako „hacking“ nebo „smoofing“ se stala každodenním chlebem vlastníků sítí. Tyto a jiné různé způsoby útoků na počítačové sítě staví vlastníka a administrátora do nelehké obranné pozice. Je tedy zřejmé, že právě zabezpečení sítě proti útokům je oblast stejně tak důležitá jako bezporuchový chod sítě. Současný trend úroků naplňuje rčení.“Naším nepřítelem už není nevzdělanost, ale nepozornost.“

Cílem této bakalářské práce je vytyčení konkrétního postupu při analýze zabezpečení počítačové sítě a návrh konkrétního postupu zabezpečení počítačové sítě. Všechny tyto poznatky jsou přehledně zpracovány v e-learningovém kurzu, jež je koncipován tak, aby podal čtenáři kurzu co nejucelenější a věcné informace v přehledné a srozumitelné formě. V kurzu jsou dále nastíněny možnosti ochrany dat v komunikačních sítích a to z pohledu neoprávněného získávání, či záměrného poškozování informací. Kurz také vytyčuje konkrétní postup při analýze zabezpečení počítačové sítě a navrhuje konkrétní postup pro její zabezpečení.

V první části kurzu jsou shromážděny poznatky o počítačových sítích obecně. Druhá část se zabývá vytyčením postupu při analýze zabezpečení počítačové sítě. V poslední části kurzu je navržen konkrétní postup zabezpečení sítě.

Vytvořený e-learningový kurz bude sloužit jako studijní opora posluchačům předmětu: „Počítačové sítě I“ na Fakultě ekonomicko-správní při Univerzitě v Pardubicích.

1. Počítačová síť

Pro první desetiletí své existence, byly počítačové sítě zejména využívány akademickými pracovníky pro odesílání e-mailů a firemní zaměstnance pro sdílení tiskáren. Za těchto podmínek se nekladl důraz na jejich bezpečnost. Ale teď, když miliony obyčejných lidí prostřednictvím sítí využívá internetové bankovnictví, nakupování a jiné služby stává se udržení bezpečnosti sítí obrovským problémem. [8]

Počítačová síť je tvořena dvěma nebo více počítači, které jsou navzájem spojeny prostřednictvím média (tímto médiem může být např. kroucená dvojlinka, koaxiální kabel, optický kabel, elektromagnetické vlny atp). Takto spojené počítače mohou sdílet data a různá periferní zařízení jako jsou tiskárny, skenery, faxová zařízení a mnoho dalších. Podle způsobu komunikace v síti existují 2 typy spojení:

Client-server - kdy jeden z počítačů slouží jako server a ostatní počítače zapojené v síti pracují pouze jako stanice.

Peer-to-peer - kdy všechny do sítě zapojené počítače jsou si rovny v tom smyslu, že mohou pracovat současně jako pracovní stanice i jako server. V tomto případě mohou tedy všechny počítače nabízet svá zařízení (skenery, tiskárny atp.) všem ostatním počítačům zapojeným do sítě.

Sítě jsou hlavním komunikačním medium a páteř většiny firem. Bezpečnost sítě tak nelze brát na lehkou váhu, protože jakmile se útočník zmocní sítě, může si s daty, které jsou na síti, dělat cokoliv bude chtít.

Dnes se celý Internet skládá z desetitisíců různých sítí, které jsou vzájemně propojené bez hranic. V takovémto prostředí je již správné zabezpečení naprosto podstatné, protože se do sítě libovolné organizace dá dostat z kteréhokoli počítače na světě a síť je tím pádem potenciálně zranitelná vůči útokům ze strany jednotlivců, kteří k ní nemusí mít přímý fyzický přístup. [3]

1.2. *Topologie sítě*

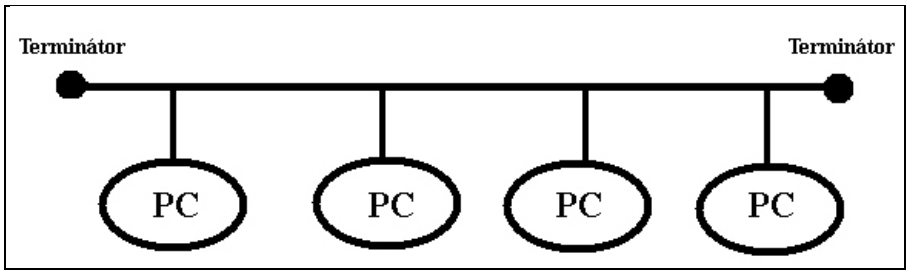
Termín "topologie" označuje způsob, jakým jsou počítače a další zařízení v síti propojeny kabely. Konkrétní typ kabelu, který se použije, stanovuje topologii sítě. Pro instalaci každého konkrétního typu kabelu je nutné použít správnou topologii.

Výběr správné topologie neovlivní až tak bezpečnost celé sítě, jako spíše spolehlivost provozu celé sítě. Topologií lze omezit škody, způsobené případnou poruchou některého

segmentu. Třemi hlavními topologiemi v sítích LAN jsou sběrnicová, hvězdicová a kruhová. [5]

1.2.1. Sběrnicová topologie

Počítače a jiná zařízení jsou propojeny v jedné linii a každý systém je kabelem spojen s dalším systémem. Tato konfigurace se často označuje jako uzavřený cyklus. Všechny signály přenášené systémy v síti procházejí podél sběrnice v obou směrech všemi systémy, než dosáhnou svého cíle. Sběrnicová topologie má vždy dva otevřené konce, jak ukazuje obrázek 1. Dva konce sběrnice musí být zakončeny elektrickými rezistory, takzvanými „terminátory“ tak, že se signály neodrážejí zpět do opačného směru, což by vedlo k interferenci s novějšími přenášenými signály. Chybějící zakončení u jednoho z konců může zabránit správné komunikaci počítačů připojených k dané sběrnici. [2]



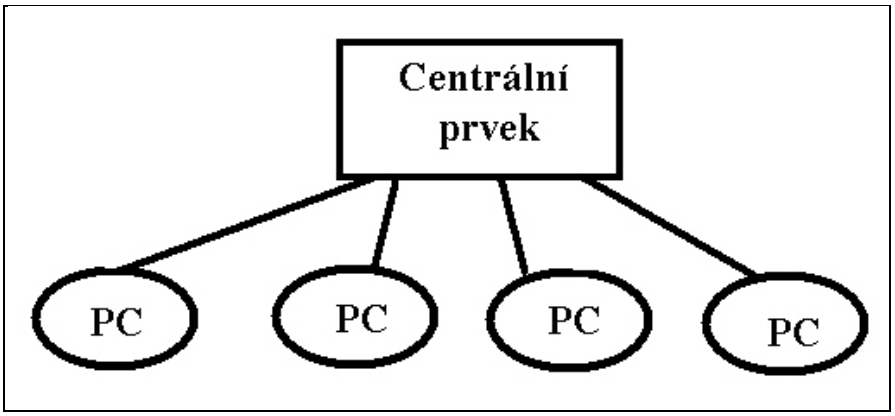
Obrázek 1 Sběrnicová topologie. Zdroj: autor

Kabeláž může mít ve sběrnicové topologii dvě podoby: tlustý a tenký Ethernet. Sítě tlustého Ethernetu používají jednu délku koaxiálního kabelu. Počítače v síti připojené k tomuto kabelu pomocí kratšího individuálně dlouhého kabelu daly název kabelům AUI (Attachment Unit Interface), které jsou také označovány jako vysílač (transceiver). Sítě tenkého Ethernetu používají užší typ koaxiálního kabelu rozděleného na jednotlivé části. Každá část kabelu připojuje jeden počítač k dalšímu. Každý počítač v síti má vysílač, který je odpovědný za odesílání i přijímání dat prostřednictvím síťového kabelu. Kromě sítě tlustého Ethernetu mají všechny standardy fyzické vrstvy své vysílače integrované do karty NIC. Tlustý Ethernet je jedinou formou sítě Ethernet, která používá rozhraní oddělené od karty NIC. Vysílač se připojuje ke koaxiálnímu kabelu prostřednictvím speciálního zařízení, kdy koaxiální kabel není přerušen, ale pouze "nabodnut" tak, aby se špička hrotu vodivě spojila se středovým vodičem koaxiálního kabelu a druhý kontakt v hrotu se spojil s vodivým pouzdrem koaxiálního kabelu. Hlavní nevýhodou sběrnicové topologie je to, že jakékoli poškození kabelu, vadná koncovka nebo špatný konektor ovlivňují funkčnost sítě. Síť je rozdělena na

dvě, což zabraňuje systémům na druhé straně v komunikaci. Pokud síť rozdělí chyba součásti, obě poloviny sítě nebudou ukončeny a výsledkem bude odrážení signálu, čímž se data promíchají. [2]

1.2.2. Hvězdicová topologie

Hvězdicová topologie používá centrální prvek nazývaný HUB nebo SWITCH. Každý počítač je připojen k tomuto centrálnímu prvku samostatným kabelem, jak ukazuje následující obrázek. Hvězdicová topologie používá kabely kroucené dvojlinky, jako je l0BaseT nebo l00BaseT. Hvězdicovou topologii používá většina sítí Ethernet LAN a mnoho sítí LAN používajících jiné protokoly.[2]

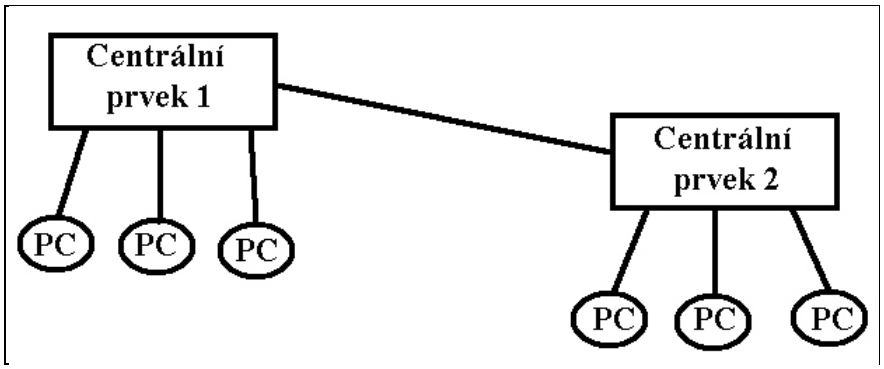


Obrázek 2 Hvězdicová topologie. Zdroj: autor

Je-li za centrální prvek zvolen HUB, síří se signál vysílaný z jedné stanice na všechny ostatní stanice připojené k tomuto HUBU. Jsou-li jednotlivé stanice připojeny ke SWITCHI šíří se signál pouze směrem k příjemci. Tento způsob připojení je odolnější vůči kolizím, které mohou nastat u všesměrového vysílání při připojení k HUBU. Protože má každý počítač vlastní vyhrazené připojení k centrálnímu prvku, je hvězdicová topologie odolnější vůči chybám než sběrnicová topologie, přičemž poškození jednoho z kabelů neovlivňuje zbývající část sítě. Ovlivněn je pouze konkrétní počítač, jehož kabel je poškozen. Nevýhoda použití hvězdicové topologie spočívá v tom, že pro její implementaci musí být použit další hardware – centrální prvek. Pokud tento prvek selže, ovlivňuje to celou síť.

1.2.3. Hierarchická hvězdicová topologie

V případě, že je potřeba rozšířit hvězdicovou síť z kapacity původního centrálního prvku, implementuje se hierarchicko-hvězdicová topologie (také známá jako stromová topologie), jak ukazuje následující obrázek.

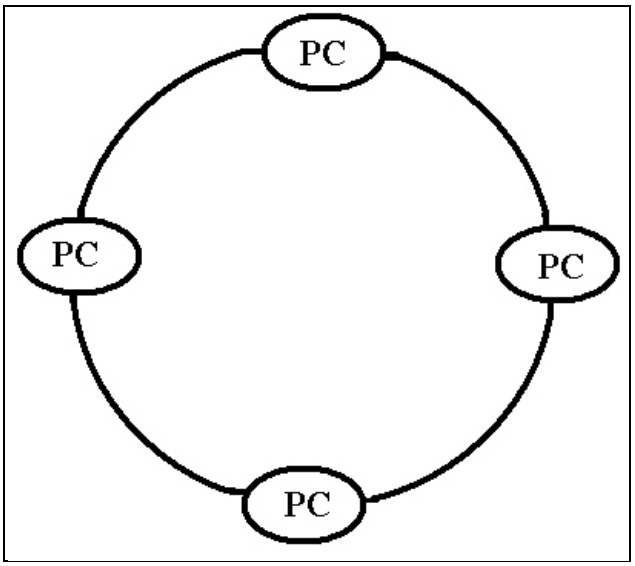


Obrázek 3 Hierarchická hvězdicová topologie. Zdroj: autor

Pro rozšíření hvězdicové topologie o další prvky se propojí původní centrální prvek s dalším centrálním prvek, ke kterému jsou připojena další zařízení sítě.

1.2.4. Kruhová topologie

Kruhová topologie se podobá sběrnicové topologii v tom, že každý počítač je propojený s dalším počítačem. Místo ukončení obou konců jsou však tyto spojeny dohromady ve formě kruhu, jak je vidět na následujícím obrázku.



Obrázek 4 Kruhová topologie. Zdroj: autor

Toto propojení způsobuje, že signály cestují cyklicky od jednoho počítače k dalšímu a nakonec se vrátí k počátečnímu bodu. Ve většině případů je kruhová topologie striktně logickou konstrukcí, a ne fyzickou, protože kabely se v kruhové topologii připojují k centrálnímu prvku a tvoří spíše hvězdici. [2]

1.3. *Síťový Hardware*

Síťový hardware může mít vliv na provoz počítačové sítě i na její bezpečnost. Provoz sítě může být ovlivněn nebo znemožněn výpadkem nebo poruchou některého z hardwaru. V neposlední řadě má hardware obrovský vliv na rychlost kvalitu a výkon celé sítě.

Mezi síťový hardware se řadí: [2, 5]

- Rozbočovače.
- Opakovače.
- Mosty
- Směrovače.
- Brány.
- Síťové karty.
- Kabely(propojovací medium).

1.3.1. Rozbočovače

Jednoduše řečeno rozbočovač je centrálním spojovacím zařízením, které propojuje počítače v hvězdicové topografii. Rozbočovače jsou v moderních sítích standardním zařízením a dělí se na pasivní nebo aktivní. Pasivní rozbočovač vůbec nezpracovává data - jde jen o propojovací panel. Naproti tomu aktivní rozbočovače (někdy nazývané opakovače) zpracovávají data, aby udržely příslušnou sílu signálu. Některé rozbočovače mají také schopnost zpracovávat další úkoly, jako je přemostění, směrování a přepínání. Systémy založené na rozbočovačích jsou všestranné a nabízejí oproti systémům bez využití rozbočovačů několik výhod. Narušení kabelu v obyčejné sběrnicové topologii například způsobí vypnutí sítě. Při použití rozbočovačů však narušení jakéhokoli kabelu připojeného k rozbočovači ovlivní pouze omezenou část sítě nebo samotný počítač. [2]

Většina rozbočovačů je aktivních - to znamená, že obnovují a znovu odesílají signály. Aktivní rozbočovače neustále vyžadují přívod elektrické energie. Některé rozbočovače jsou pasivní (patří sem například zapojovací desky). Fungují pouze jako propojovací body

a nezesilují ani neobnovují signál. Signál rozbočovačem pouze prochází. Pasivní rozbočovače nevyžadují přívod elektrické energie. Přicházející generace rozbočovačů bude vyhovovat několika různým typům kabelů. Nazývají se hybridní rozbočovače.

1.3.2. Opakovače

Jak se elektrický signál šíří kabely, je degradován a zkreslen. Tento efekt se nazývá útlum. Se zvětšující se délkou kabelu se zvětšuje útlum. Je-li kabel příliš dlouhý, útlum nakonec znemožní rozpoznatelnost signálu a vzniknou tak datové chyby v síti. Instalace opakovačů umožňuje, aby signály cestovaly dále pomocí obnovení signálů sítě a jejich novým odesláním na další úsek kabelů. Opakovač vezme slabý signál z jednoho kabelu, obnoví jej a pošle do dalšího kabelu.

Opakovače jsou v podstatě opakovače signálu (či obnovovače signálu). Nepřekládají ani nefiltrují síťové signály z jednoho kabelu na druhý. Aby opakovač mohl správně fungovat, musí oba k němu připojené kabely používat stejné rámce, logické protokoly a přístupové metody.

1.3.3. Mosty

Mosty nabízí zatížené síti více funkcí. Most může fungovat jako opakovač k prodloužení efektivní délky síťového kabelu. Most však má větší "inteligenci" a může rozdělit síť pro izolování nadměrného provozu nebo problematických dat. Pokud například svazek z jednoho či dvou počítačů (nebo jednoho oddělení) zaplavuje síť daty a zpomaluje tak její činnost, může most tyto počítače (nebo oddělení) izolovat umístěním do jejich vlastní části kabelu. Místo rozlišování mezi protokoly mohou mosty jednoduše odesílat všechny protokoly po síti. Protože všechny protokoly procházejí mosty, je na jednotlivých počítačích, aby stanovily, které protokoly mohou být rozpoznány. Mosty mohou propojovat také různá fyzická média, jako je kabel s kroucenou dvojlinkou a optický kabel.

1.3.4. Směrovače

Když se pracuje ve složitějších síťových prostředích, která používají různé segmenty sítě - každý s jinými protokoly a architekturami - most je často pro rychlou a efektivní komunikaci mezi jednotlivými segmenty nedostatečný. Taková složitá síť vyžaduje propracovaná zařízení, která znají adresy každého segmentu, stanovují nejlepší cestu pro odesílání dat a filtrují data vysílaná na místní segmenty. Tento typ zařízení se nazývá směrovač. Stejně jako most mohou směrovače filtrovat a izolovat data posílaná sítí a mohou

také připojovat segmenty sítě. Směrovače mohou navíc přepínat a směrovat pakety přes více sítí. Činí tak vyměňováním informací o určitém protokolu mezi samostatnými sítěmi. Směrovače mají přístup k více informacím o paketech než most a používají tyto informace ke zdokonalení přenosu paketů. Směrovače se používají ve složitých sítích, protože poskytují lepší správu přenosu dat. Směrovače mohou například sdílet informace o stavu a směrování a používat tyto informace k překlenutí pomalých nebo špatně fungujících připojení. [2]

Existují dva základní směrovací protokoly: statické a dynamické. "Statický směrovač" se někdy nazývá také "ruční směrovač", protože všechny směrovače musí být nakonfigurovány ručně správcem sítě. Směrovací tabulky jsou pevně dané, takže statický směrovač vždy používá stejnou trasu (i když se změní aktivita sítě). To znamená, že není záruka, že statický směrovač používá nekratší trasy. Naproti tomu "dynamické směrovače" musí být nejprve nakonfigurovány, avšak přizpůsobí se automaticky měnícím se podmínkám sítě - za použití nižších nákladů nebo méně zatížených tras podle potřeby.

1.3.5. Brány

Brána funguje jako výkonný překladač určený pro připojení radikálně odlišných sítí. Ačkoli je pomalejší než most nebo směrovač, může brána provádět složitější funkce, jako je překlad mezi sítěmi, které hovoří různými jazyky (za pomoci technik, jako je převod protokolu a šířky pásma). Brána může například převádět aplikace, jako je cc:Mail na SMTP (a obráceně). Brány umožňují komunikaci mezi zcela odlišnými architekturami a prostředími. Efektivně přetvářejí pakety a převádějí data pocházející z jednoho typu sítě do jiného tak, že každý z nich rozumí datům toho druhého. Brána přetváří informace, aby vyhovovaly požadavkům cílového systému, a změní formát zprávy tak, aby se přizpůsobil aplikaci přijímající přenášená data. Ve většině případů jsou brány úkolově specifické, což znamená, že jsou vyhrazeny určitému typu přenosu. Často se označují podle svého úkolu.

1.3.6. Síťové karty

Síťová karta (NIC - network interface card, také známá jako adaptér LAN) funguje jako rozhraní mezi samostatným počítačem (serverem nebo klientem) a síťovými kabely. Uvnitř musí karta NIC identifikovat počítač v síti a načíst do vyrovnávací paměti data mezi počítačem a kabelem. Při odesílání dat musí karta NIC převést data z paralelních bajtů na sériové bity (poté znovu zpět během přijímání). Na straně sítě musí karta NIC vygenerovat elektrické signály, které cestují prostřednictvím sítě, řídit přístup k síti a vytvořit fyzické připojení ke kabelu. Každý počítač v síti musí mít alespoň jeden nainstalovaný port NIC.

1.3.7. Kabely

Sítě všech velikostí a konfigurací jsou založeny na fyzické kabeláži, která spojuje všechny počítače a další hardware dohromady. Kabeláž (také označovaná jako síťové médium) přichází v mnoha různých konfiguracích, avšak mezi běžné typy kabelů používaných pro běžné sítě patří nestíněná kroucená dvojlinka (UTP), koaxiální kabel, stíněná kroucená dvojlinka (STP) a optický kabel (FO).

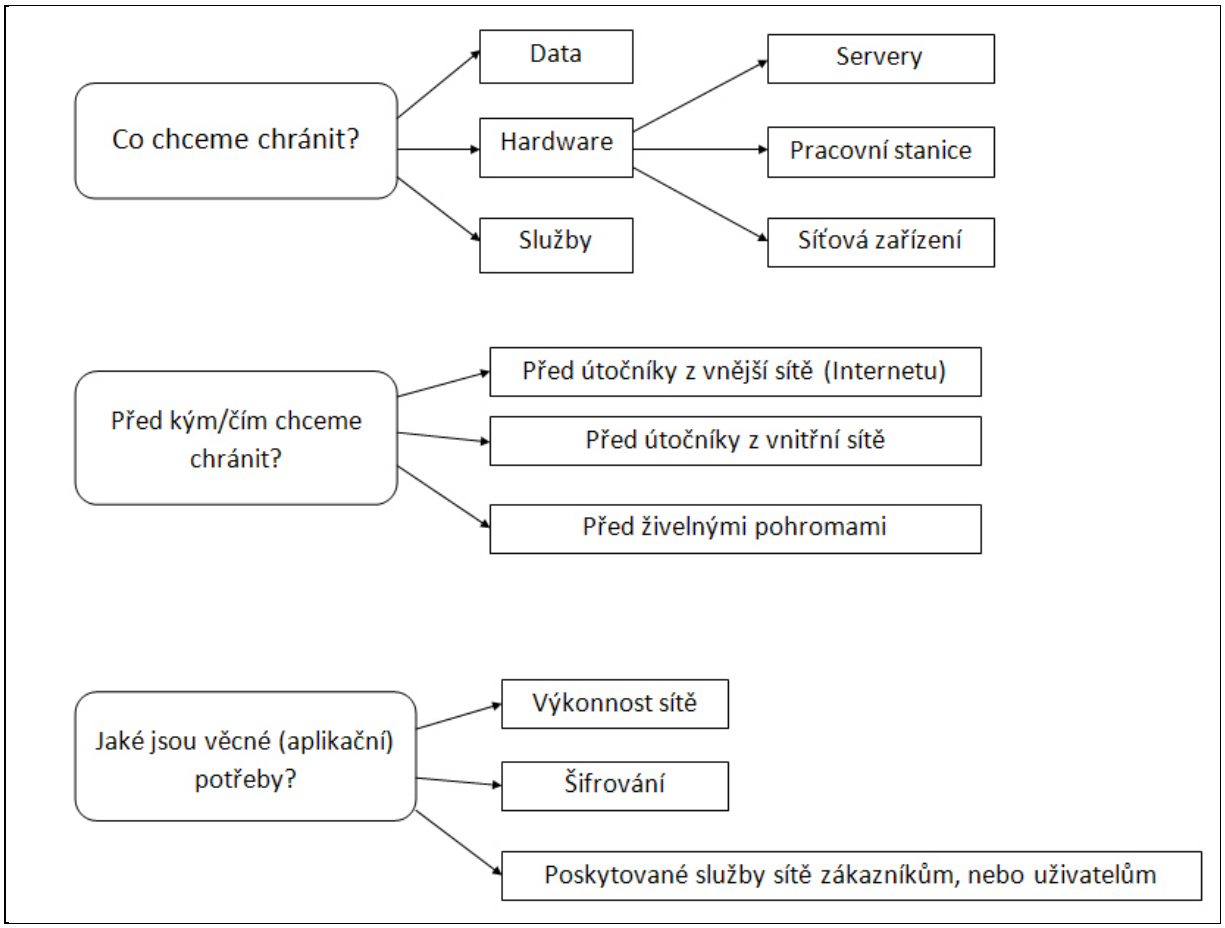
Je důležité znát tři hlavní aspekty kabeláže [2]:

- Odolnost vůči přeslechu (elektřina probíhá mezi páry drátů ve stejném kabelu).
- Odolnost vůči narušení z vnějšku elektrického pole (šum vytvářený elektrickými motory, převaděči a vysílači).
- Snadnost instalace.

Toto jsou důležité aspekty, protože kabely odolné vůči přeslechu a narušení mohou běžet déle a podporovat vyšší hodnoty přenosu dat. Například koaxiální kabely a kabely STP mají ve vnější vrstvě tenkou kovovou fólii, která nabízí dobrou odolnost vůči elektrickému šumu, avšak fólie navíc vytváří větší, tlustší kabel, který lze hůře protáhnout instalačními trubkami a zdmi během instalace. Kabel UTP je tenčí a jeho instalace je snazší, nabízí však menší odolnost vůči elektrickému šumu. Oproti tomu nese optický kabel místo elektrických impulsů světelné signály. To optickému kabelu umožňuje přenášet signály rychleji a dále, než je tomu u jakéhokoli jiného kabelu. Optický kabel je bohužel mnohem dražší než jiné typy kabelů a správná instalace vyžaduje specializované nástroje a zkušenosti.

2. Vytyčení konkrétního postupu při analýze zabezpečení počítačové sítě

Zabezpečení sítě je nepřetržitý a nikdy nekončící proces, protože i pokrok ve vývoji počítačových technologií a jejich rozšiřování pokračuje neustále. Jestliže bude porozuměno potenciálním hrozbám síťové bezpečnosti, je možno tak předejít nečekaným událostem, které by pro firmu či instituci mohly mít fatální následky ať už z důvodu ztráty dat nebo úniku citlivých informací. Pro lepší objasnění, na co si dát při zabezpečení počítačových sítí pozor a před čím je potřeba síť chránit, bylo vytvořeno následující schéma, které bude podrobněji popsáno v následující části této práce.



Obrázek 5 Analýza zabezpečení. Zdroj: autor

2.1. *Co je potřeba chránit*

Při zabezpečování sítí si nejdříve musíme uvědomit, co je v naší síti potřeba chránit. Každá síť je jiná, každá organizace má svá jasná pravidla, které věci je potřeba chránit před okolím. Pro jednu organizaci to mohou být data nacházející se na síti, pro jinou zase služby, které firemní síť poskytuje svým zaměstnancům, zákazníkům či obchodním partnerům. V neposlední řadě by se nemělo zapomínat i na samotný hardware počítačové sítě.
V následující části tohoto průvodce si popíšeme možnosti ochrany hardwaru sítě, ochrany dat a síťových služeb.

2.1.1. Hardware

Hardware sítě určuje některé významné parametry sítě jako celku. Jsou to především přenosová rychlost, metoda přístupu k přenosovému médiu, topologie sítě a maximální rozsah sítě.

Hardware je nezastupitelným komponentem každé počítačové sítě. Porucha byť jen jednoho prvku sítě může mít nedozírné následky na provoz, stabilitu a rychlost celé sítě. V následující části tohoto elektronického materiálu si popíšeme jak zabezpečit servery, pracovní stanice a síťová zařízení.

a) Servery

V dnešních počítačových sítích se informace obvykle soustřeďují na serverech. Je to velice rozumné, protože centrálně uložená data jsou mnohem lépe pod kontrolu. Na druhou stranu je to i dosti nebezpečné, protože pokud se potenciální útočník zmocní nějakého serveru, má v tu chvíli přístup k datům a službám jím poskytovaným. V počítačových sítích by se tak měl klást největší důraz na zabezpečení dat a služeb poskytovaných servery.

Při analýze sítě je nesmírně důležité přesně vědět, jaké servery jsou v síti instalovány, kde jsou rozmístěny, jaké jsou jejich síťové parametry a jaké na nich běží operační systémy, aplikace a záplaty (opravy). Kromě technických specifikací každého serveru a jeho softwaru musíme pečlivě zaznamenat a dokumentovat také kontaktní údaje o osobách zodpovědných za konkrétní věcný úkol zajišťovaný daným serverem. S tímto člověkem se budeme muset spojit v případě zjištěného incidentu.

b) Pracovní stanice

Pracovní stanice jednotlivých koncových uživatelů jsou jakýmsi rozhraním mezi technickou infrastrukturou výpočetního prostředí a lidmi, kteří pomocí nich skutečně zajišťují chod firmy. Bez ohledu na to, jak přísné zabezpečení síť má musí se vždy propustit alespoň nějaký provoz, aby tito lidé mohli využívat internetových prostředků a aby tak fakticky v této webově orientované době vůbec mohli pracovat.

Je dobré posoudit, nakolik budou systémoví administrátoři schopni pravidelně záplatovat pracovní stanice, a podle výsledku rozhodnout, jestli segmentovat prostředí vnitřní sítě pomocí firewallů. V organizacích, které mají zavedenou dálkovou distribuci aktualizovaných oprav operačního systému aplikací na systémy jednotlivých uživatelů, zdaleka tolik nehrozí, že by se útočník zmocnil některé pracovní stanice a odtud dále pokračoval do ostatních vnitřních systémů. Tato centralizovaná správa ale současně znamená, že případné napadení ústředního řídícího kanálu zasáhne velkou část sítě.

Při kontrole pracovních stanic je třeba se podívat, jaké aplikace a operační systémy na nich běží a nakolik jsou aktualizované pomocí oprav (záplat). Dále je potřeba se ptát: "Jsou data uložena jen na serverech, nebo mají uživatelé také nějaké soubory u sebe". Kromě toho musíme vzít v úvahu zvláštní opatření pro uživatele na cestách a domácí pracovníky, kteří jsou rozmístěny vně základní firemní sítě a fakticky tak nic netušící výrazně rozšiřují počítačovou síť organizace.

c) Síťová zařízení

Pojmem síťová zařízení se označují veškerá zařízení, která jsou připojena do počítačové sítě a která buď vysílají, nebo přijímají data.

Všechny tyto prvky jsme si popsali v předešlé kapitole "Síťový hardware", nemá tedy smysl je popisovat znova.

Důležité je však podotknout, že výpadek jakéhokoli z těchto prvků, může mít fatální následky na provoz a celé sítě. Výpadkem jednoho z nich může být v danou chvíli např. naše síť.

Všechna tato zařízení by měla být i pečlivě uschována před případnými útočníky. Připojení kabelu do nechráněného prvku zvládne i naprostý laik. V danou chvíli mohou být všechna naše opatření k ničemu, neboť útočník je již v naší síti připojen.

2.1.2. Data

Na každé počítačové síti se nacházejí data, která by neměla být prozrazena osobám neoprávněnými s těmito daty nakládat. Proto je nesmírně důležité tato data před těmito osobami ochránit. Pod těmito daty je možno si představit údaje o zákaznících, klientech, ale i stavech bankovních účtů nebo interních informacích firmy.

2.1.3. Síťové služby

Pod pojmem síťové služby se rozumí služby poskytované serverem klientům v počítačové síti. Příkladem to může být sdílení disků, tiskáren, schopnost ověřovat uživatele na základě jména a hesla.

Dobře fungující síťová infrastruktura je základem veškeré komunikace. Ať už se jedná o sdílení síťových disků, tiskáren nebo VoIP telefonii.

2.2. *Před kým / čím je nutné síť chránit*

Počítačovou síť je nutné chránit před třemi základními typy ohrožení. Prvním z nich je ochrana před útočníky z vnější sítě, tedy internetu. Následuje ochrana počítačové sítě před vlastními uživateli sítě a v neposlední řadě je důležité ochránit síť před zásahem vyšší moci, tedy například před živelnými pohromami a jinými nepředvídatelnými událostmi. Tyto 3 typy ohrožení budou popsány v následujících podkapitolách tohoto průvodce.

2.2.1. Zabezpečení sítě proti útoku „zevnitř“

Při zabezpečení počítačové sítě je potřeba se chránit i před útoky ze vnitř samotné sítě. Útoky z vnitřní sítě jsou buď úmyslné například od nespokojeného zaměstnance, nebo neúmyslné od nezkušeného uživatele, který například svým nedopatřením smaže důležitá data.

Před útoky zevnitř sítě je třeba soustředit se zejména na:

- Uživatele.
- Správné nastavení systému.
- Dodržování pravidel bezpečnosti.

Zabezpečení uživatelského přístupu

Každý uživatel sítě je pro útočníka otevřenými dveřmi do domu. Dojde-li k nějaké bezpečnostní chybě, zejména vyzrazení uživatelských údajů do systému, mohou být všechna

ostatní opatření naprosto zbytečná. Určitě záleží na tom, jak velkými pravomocemi daný uživatel disponuje, tedy jaká má nastavená přístupová práva do systému. Z tohoto hlediska je určitě nejnebezpečnějším uživatelem správce sítě administrátor nebo též nazývaný root.

Základní podmínkou pro dodržování bezpečnostních pravidel všemi uživateli sítě, je jejich jasné stanovení. Každého uživatele je nutné zřetelně a jasně s danými pravidly seznámit a vysvětlit mu případná rizika spojená s porušením těchto pravidel. Neinformovaný a nezkušený uživatel je jedním z největších nebezpečí sítě.

Další nutnou podmínkou správného fungování celé sítě, je i dostatečná počítačová odbornost a odbornost v rozsahu jeho vlastní pracovní náplně. Každému uživateli by se měly nastavit jen taková prává, jaká jsou pro jeho práci nezbytně nutná. Každý uživatel by měl znát hardware a software, který ke své práci používá. Všechny povinnosti a znalosti uživatelů, je nutné pravidelně kontrolovat.

Konfigurace přístupu k síti

Nastavení přístupu k síti, musí být od správce počítačové sítě, co nejdůkladnější, aby riziko napadení bylo minimalizováno.

Každý uživatel, který se přihlašuje do sítě svým uživatelským jménem, by měl mít i spolehlivé heslo.

Za spolehlivé heslo se považuje takové heslo, které splňuje následující podmínky [6]:

- Obsahuje alespoň 8 znaků.
- Obsahuje malá a velká písmena.
- Obsahuje minimálně jednu číslici.
- Obsahuje minimálně jeden ne-alfanumerický znak.

Všem heslům je dobré nastavit určitou omezenou životnost. Systém, pak například každé 2 měsíce upozorní uživatele na změnu hesla. Doba, po které by se mělo heslo změnit, si stanovuje každá organizace podle svého. Jedná-li se o přístup k aplikacím, je dobré zaslat uživateli notifikační e-mail, pro potvrzení změn. Pokročilejší metody některých aplikací dokážou účet zamknout, například pokud útočník zkouší uhodnout heslo a po určitém počtu pokusů se mu to nepodaří, pak systém účet zamkne a vyrozumí správce.

Hesla není vhodné ukládat v čisté podobě, ale upravená některou z hashovacích funkcí, například SHA nebo MD5. Takto hashovaná hesla nebudou pro případného útočníka,

který se dostane k databázi vůbec čitelná. Jedinou možností jak odhalit z hashovaného hesla pravé heslo je útok takzvanou hrubou silou. [2]

Dalším pravidlem, na které by měl dávat správce systému pozor je blokování neaktivních uživatelských účtů, například od bývalých zaměstnanců. Stejně tak je důležité změnit při odchodu zaměstnance všechna hesla, která mohl znát.

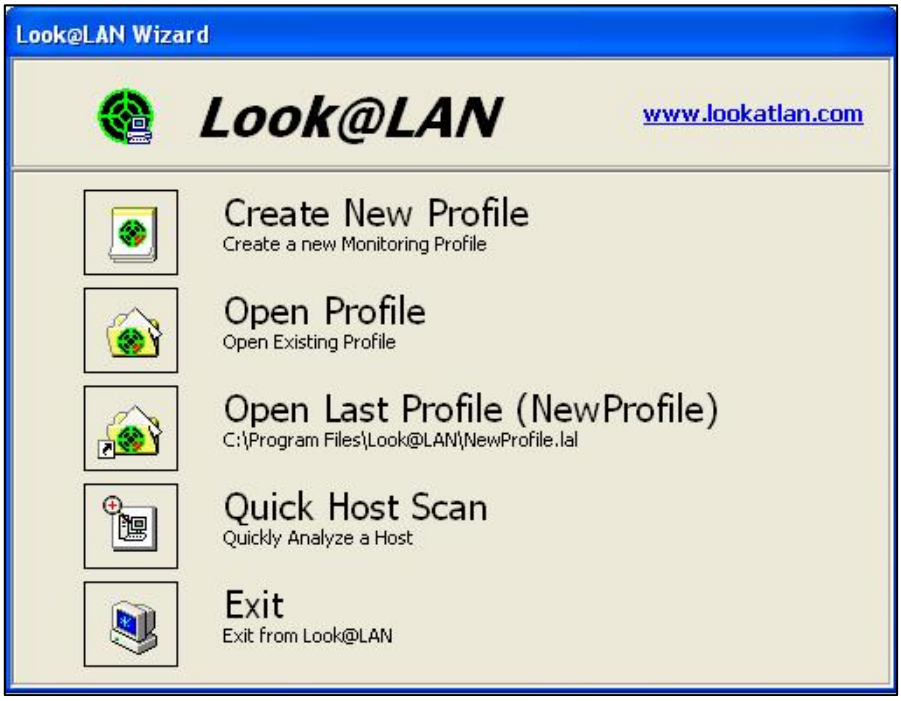
Dodržování pravidel bezpečnosti

Kromě výše uvedených pravidel, je nutné dodržovat i další pravidla bezpečnosti příkladem mohou být tato doporučení[5]:

- Minimalizace používání účtu administrátora nebo root.
- Odhlašování uživatelů.
- Uzamykání PC při odchodu uživatele ze svého pracoviště.

Kontrola zabezpečení z vnitřní sítě:

Nastavení otevřenosti portů jednotlivých systémů v síti je dobré zkontrolovat a nechat otevřené jen ty nezbytně nutné. V následující části práce je popsán postup této kontroly pomocí programu Look@LAN, který je šířen pod licencí freeware a je možné si ho stáhnout ze stránek výrobce na adrese http://www.lookatlan.com. Po nainstalování a spuštění programu se nám zobrazí okno, které je zobrazeno na následujícím obrázku.



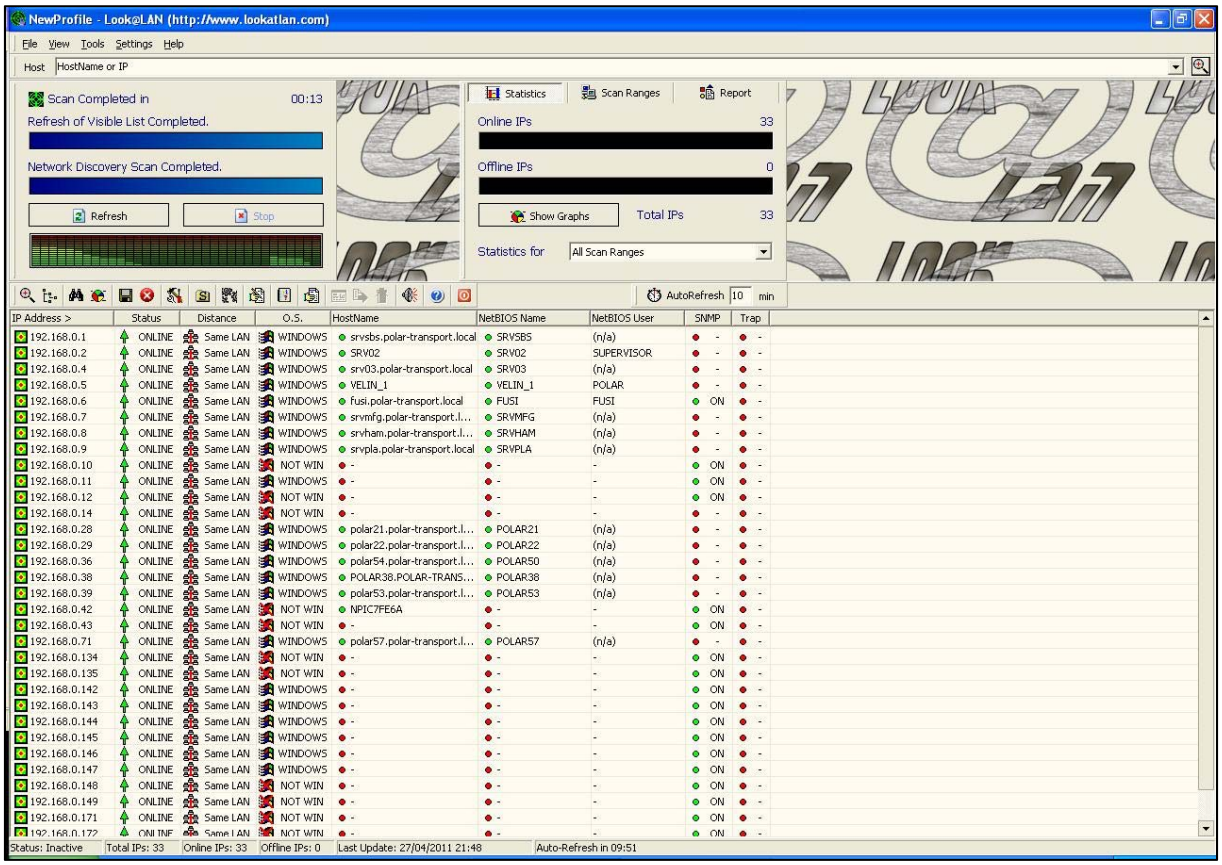
Obrázek 6 Spuštění programu Look@LAN. Zdroj: autor

Při prvním spuštění programu se klikne na ikonu „Create New profile“ po stisku tohoto tlačítka se vyvolá akce, která otevře nové okno, kde je potřeba zadat IP rozsah, na kterém se budou skenovat porty, tak jak je znázorněno na následujícím obrázku.

Obrázek 7 Nastavení IP rozsahu pro skenování portů. Zdroj: autor

V této modelové situaci konkrétního případu je zvolen IP rozsah od adresy 192.168.0.1 do adresy 192.168.0.255. Z daného obrázku je vidět, že celý proces skenování je prováděn z IP adresy 192.168.0.38.

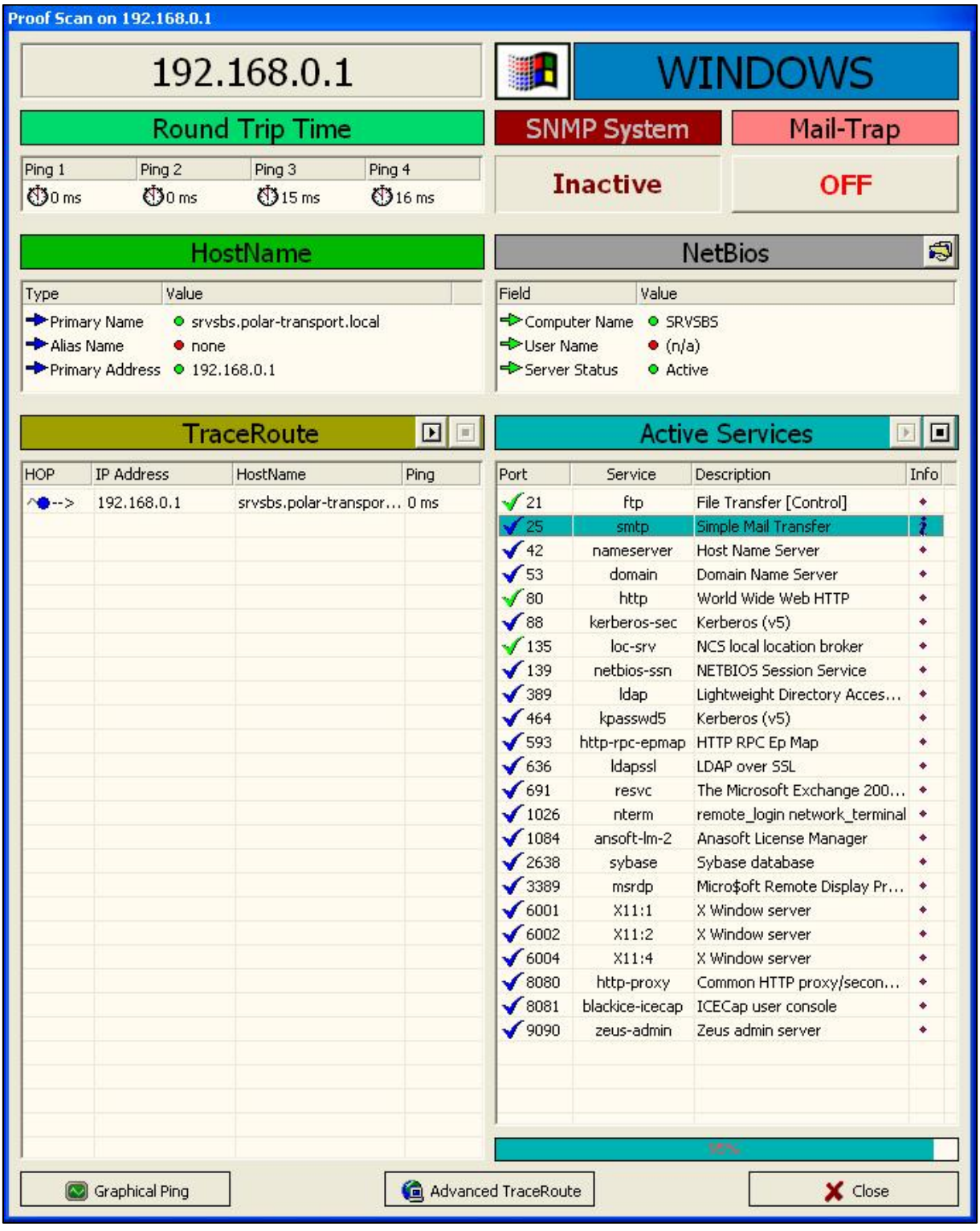
Po stisknutí tlačítka „Next“ se spustí proces skenování portů. Výsledek skenování sítě je znázorněn na následujícím obrázku.



Obrázek 8 Výsledek skenování porů. Zdroj: autor

Tímto způsobem jsou otestována veškerá připojená zařízení do počítačové sítě. Z následujícího obrázku lze vyčíst IP adresy jednotlivých prvků připojených do sítě a operační systém, který je na nich nainstalován.

Po kliknutí na kterou-li IP adresu se otevře okno s popisem otevřených portů na daném zařízení, tak jak znázorňuje obrázek číslo 9.



Obrázek 9 Ukázka otevřenosti portů. Zdroj: autor

Programem Look@LAN byla prověřena všechna připojená zařízení, podle skenování jednotlivých portů se lze rozhodnout, které je nutné nechat otevřené pro správný běh systému v dané síti a které je třeba v zájmu zabezpečení nechat zavřené.

2.2.2. Ochrana před útočníky z vnější sítě

Neoprávněný vzdálený přístup je velmi nežádaný jev pro správnou funkci sítě nebo samotného počítače. Jelikož se v počítačích a na síti uchovávají různé citlivé údaje a data, je potřeba zamezit případnému odposlechu datové komunikace v síti, který by hrozil formou vzdáleného přístupu. Nejlepším prostředkem jak se bránit proti neoprávněnému vzdálenému přístupu je izolovat síť od veškerých externích sítí. Síť pak bude postavena pouze lokálně a případný útočník není schopen se vzdáleně do sítě připojit. V mnoha případech však tato možnost není a síť je připojena na další externí sítě, nejčastěji internet. V této variantě je velké riziko, že se do sítě vzdáleně někdo připojí. Možnost jak se proti takovému útoku bránit je použití firewallu.

Firewall

Firewall je zařízení ležící na obvodu sítě. Pomocí množiny pravidel definuje jaký přístup ze sítě nebo do sítě bude povolovat nebo naopak zamítat.

Firewallů je více druhů [5]:

- Paketové filtry.
- Proxy filtry.
- Stavové filtry.

Paketové filtry

Filtrování paketů je jednou z nejstarších a nejrozšířenějších metod řízení přístupu k sítím. Základní myšlenka je velice jednoduchá: Podle určitých identifikačních údajů v hlavičce paketu se stanový jestli smí paket vstoupit, případně vystoupit ze sítě. Technologie filtrování paketů je součástí mnoha různých operačních systémů, softwarových i hardwarových firewallu a patří také mezi bezpečnostní funkce většiny směrovačů. [5]

Firewall, který spadá do kategorie paketových filtrů TCP/IP, zpravidla analyzuje síťový provoz na transportní vrstvě, případně síťové (internetové) vrstvě sady protokolů TCI/IP; to znamená, že může v konkrétní síti filtrovat libovolná přenášená data, odpovídající standardní sadě protokolů TCP/IP (případně jiné standardní rodině protokolů). Jednotlivá pole každého datového paketu jsou dobře známá (příkladem je pole zdrojové IP adresy, cílové IP adresy, zdrojového portu a cílového portu); paketový filtr v nich tedy analyzuje statické informace z hlavičky paketu. [3]

Brána firewall zkoumá každou hlavičku všech paketů a použije uvedené informace

k učinění rozhodnutí, zda paket přijmout a směrovat jej k cíli, zda paket odstranit bez oznámení či jej odmítnout (to znamená paket odstranit a upozornit odesílatele na to, že paket byl zahozen). [2]

Paketové filtry se rozhodují podle následujících informací v hlavičkách [2]:

- Zdrojová adresa IP.
- Cílová adresa IP.
- Používaný síťový protokol (TCP, UDP nebo ICMP).
- Zdrojový port TCP nebo UDP.
- Cílový port TCP nebo UDP.
- Jedná-li se o protokol ICMP, typ zprávy ICMP.

Proxy filtry

Proxy server, označovaný někdy také jako aplikační brána či proxy filtr, je specializovaná aplikace, která zajišťuje komunikaci internetových protokolů mezi vnitřní chráněnou sítí a vnějším světem (Internetem). Proxy servery pracují obvykle nad programy postavenými na TCP/IP a zpravidla v nich běží několik programových proxy („prostředníků“), které je možné zabezpečit a důvěřovat jim. Tyto programy slouží vždy pro konkrétní aplikaci a každý jednotlivý podporovaný protokol musí mít samostatnou proxy službu nebo jej musí obsluhovat obecný (univerzální) proxy. Jako proxy server může pracovat také transparentní program, který předává pakety na libovolném daném portu přes hranice sítě.

Proxy server přistupuje jménem klienta či uživatel k určité síťové službě a fakticky tím zakrývá přímé spojení mezi oběma partnery. Klient naváže potřebná spojení s proxy serverem (včetně úplné navázání třícestné komunikace) a proxy se poté spojí s cílovým serverem. Dále již proxy odesílá cílovému serveru veškerá data přijatá od klienta a zpětné předává klientu data doručená od cílového serveru. Formálně vzato je proxy server současně klientem i serverem. Vůči svému klientovi vystupuje jako server a vůči cílovému serveru vystupuje jako klient. [5]

Stavové filtry

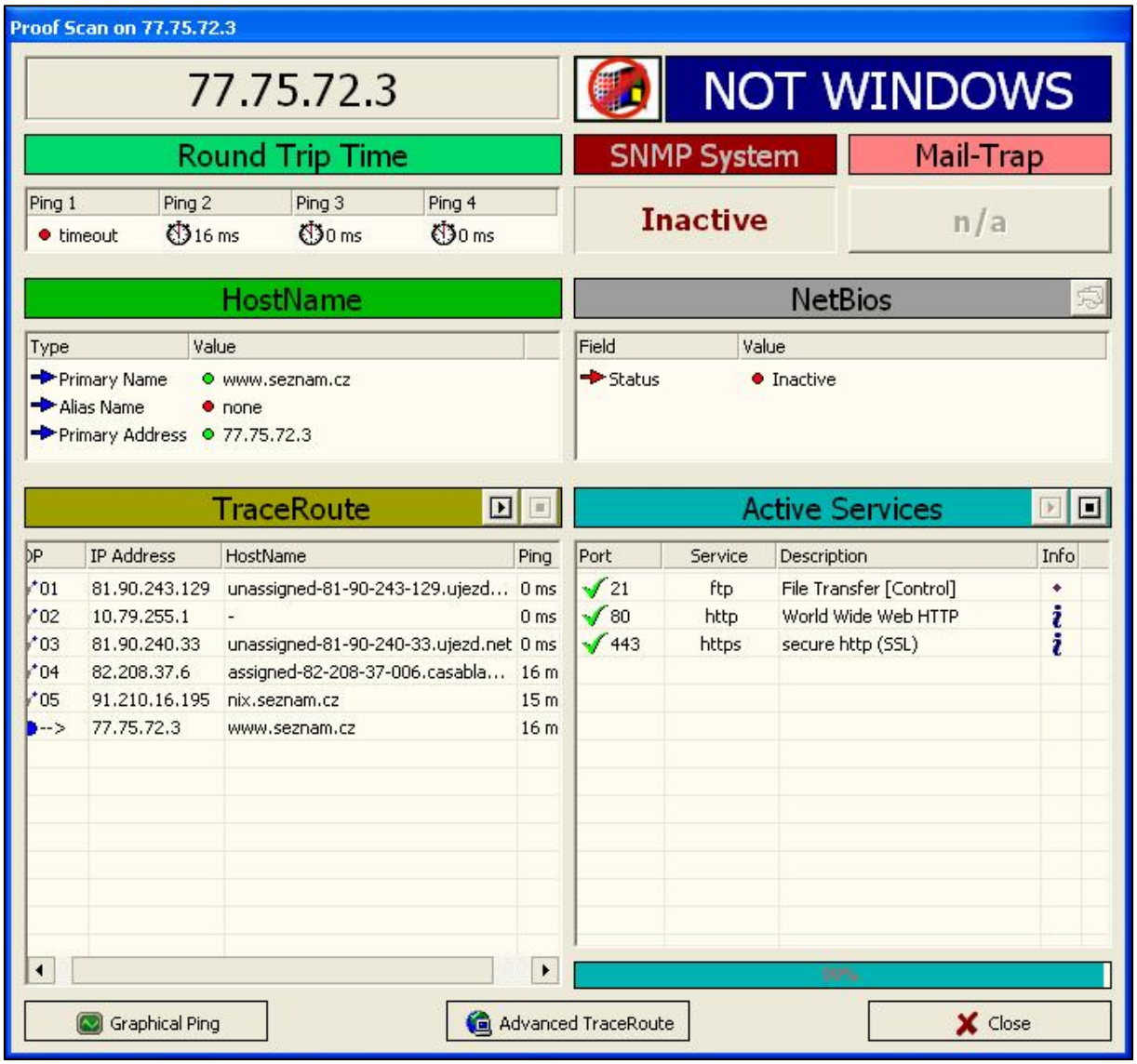
Třetí typ firewallů v sobě spojuje ty nejlepší vlastnosti z technologií paketových filtrů

a proxy filtrování. Stavový paketový filtr si pro každou relaci, vedenou přes firewall, pamatuje kompletní stavové informace. Při každém navázání nového spojení IP, ať už v příchozím nebo odchozím směru, se do stavové tabulky relačních toků zaznamenávají příslušné údaje. Stavová tabulka relačních toků obsahuje ke každému spojení TCP/UDP, sdruženému s příslušnou komunikační relací, informace o zdrojové a cílové adrese, čísla portů, údaje o pořadových číslech TCP, a případné doplňující příznaky. S navázáním relace přes firewall se vytvoří objekt spojení, veškeré příchozí i odchozí pakety se následně porovnávají s relačním tokem, zaznamenaným ve stavové tabulce relačních toků, a průchod dat firewallem se povolí jen v případě, že k nim existuje příslušné spojení. Tato metoda je při filtrování velice účinná, protože pracuje nad jednotlivými pakety a každý z nich porovnává vůči navázaným komunikačním spojením. Běží rychleji než filtrování paketů či proxy filtr. Ke každé spojované i nespojované transakci zaznamenává určité údaje do tabulky, ke které se firewall může později vracet a může stanovit, jestli přijatý paket náleží k některému stávajícímu spojení, nebo jestli pochází z neoprávněného zdroje. [5]

Kontrola zabezpečení sítě proti vniknutí z vnější sítě:

Kontrola zabezpečení bude opět popsána pomocí programu Look@LAN.Toto prověření je možné provést zadáním veřejné IP adresy hraničního směrovače do kolonky „Host“ v obrázku číslo 8 a poté kliknutí na ikonku lupy.

Jelikož je v práci popisována konkrétní modelová situace a není tedy dána IP adresa hraničního směrovače, byla pro následující výstup použita tato IP adresa: 77.75.72.3, jedná se o IP adresu serveru seznam.cz. Výstup tohoto skenování je znázorněn na obrázku číslo 10.



Obrázek 10 Výstup skenování veřejné IP adresy. Zdroj: autor

Z výstupu znázorněném na obrázku číslo 10 lze vyčíst, že na tomto serveru jsou otevřeny porty číslo: 21, 80 a 443. Přes tyto porty je tedy možné proniknout do vnitřní sítě. Program Look@LAN využívá pro výše uvedené výsledky protokol ICMP[1].

ICMP je jeden z nejdůležitějších protokolů ze sady protokolů internetu. Používají ho operační systémy počítačů v síti pro odesílání chybových zpráv, například pro oznámení, že požadovaná služba není dostupná nebo že potřebný počítač nebo router není dosažitelný. Program pracuje tak, že postupně posílá na jednotlivé adresy dotazy ping, pokud program obdrží odpověď, prozkoumá jednotlivé porty na dané IP adrese.

[1] **ICMP** (anglicky *Internet Control Message Protocol*)

2.2.3. Živelné a jiné pohromy

Zabezpečení hardwaru sítě

V počítačových sítích není potřeba jen chránit cenná data, která se na síti nacházejí před potenciálními útočníky ať už z naší sítě nebo z vnější sítě. Důležitým a mnohdy opomíjeným prvkem zabezpečení dat, která jsou na sítí je zabezpečení samotného hardwaru, na kterém jsou cenná data uložena. Hardware je zejména důležité chránit nejen před proudovými a napěťovými špičkami v elektrické síti, ale i před výpadky elektrické energie. K tomuto účelu ochrany se používají záložní zdroje UPS.

Ne všechny prvky ochrany jsou stoprocentní, a proto se nesmí zapomínat ani na zálohu důležitých dat.

Záložní napájení – UPS

Sítě se spoléhají na stálou činnost serverů, pracovních stanic a dalších zařízení. V mnoha případech je zařízení spuštěno nepřetržitě. Funkce závisí na příslušném zdroji elektrické energie. Dodávka elektrické energie však není dokonalá a může dojít k jejímu náhlému přerušení. Přerušení elektrického napájení může způsobit nesprávnou funkci serveru nebo restartování. V extrémnějších případech může dojít k poškození dat či dokonce k poškození síťového zařízení. UPS (Uninterruptible Power Supply) neboli nepřerušitelný zdroj napájení je zařízení, které zajišťuje napájení v případě, že dojde k přerušení dodávky elektrické energie. Zdroj UPS je vložen mezi zásuvku a zařízení počítače, které je potřeba chránit před výpadkem. Dojde-li k problému, UPS se přepne na zdroj napájení z baterie a zařízení zůstane spuštěno dostatečně dlouho na to, aby se dala uložit data a provedlo se správné vypnutí. Ve většině případů obsahuje zdroj UPS také ochranný okruh, který zabraňuje průchodu náhodných elektrických výbojů do zařízení počítače. [2]

Úkolem zdrojů nepřerušitelného napájení (zdrojů UPS) je pouze to, aby při výpadku napájecí sítě umožnily provést akce potřebné k řádnému ukončení (shutdownu) práce počítače[9].

Existují následující tři základní typy zdrojů UPS [2, 9]:

- Online UPS.
- Offline UPS.
- Interaktivní UPS

Online UPS

Online zdroj UPS je systém, ve kterém je invertor (okruh měnící stejnosměrný proud na střídavý proud) neustále funkční a napájí zařízení počítače. Ve skutečnosti je počítač nepřetržitě napájen z baterie, i když je střídavý proud již k dispozici a baterie zdroje UPS jsou nabité. Střídavý proud přicházející ze zásuvky je převáděn na stejnosměrný proud, který nabíjí baterie.

Díky tomu dokáže on-line zdroj zajistit téměř ideální průběh výstupního napětí a odfiltrovat nejrůznější poruchy, včetně přepětí [9].

Napětí baterií je poté převáděno zpět na střídavý proud pro napájení zařízení počítače. Napětí i frekvence mohou být velmi dobře regulovány. Druhý typ online zdroje UPS se rozšířil v roce 1990. V tomto typu zdroje UPS je procesem převodu střídavého proudu na stejnosměrný a zpět na střídavý proud zpracovávána pouze část elektrické energie. [2]

Offline UPS

Po technické stránce mohou být zdroje nepřerušitelného napájení řešeny jako off-line zdroje, které za normálního stavu sítě pouze "propouštějí" napájecí napětí ze sítě přímo k připojeným spotřebičům, a teprve v okamžiku výpadku sítě se automaticky přepnou na napájení z baterie [9].

V případě potřeby je zapojen invertor UPS, který zajišťuje chod zařízení počítače napájením z baterie. Projektování a správa tohoto typu zdroje UPS je o něco jednodušší, zatížení baterií je však vyšší, protože se při podpoře připojených zařízení počítače dosti vybijí. V normálních aplikacích se záložní zdroj UPS používá k ochraně méně důležitých zařízení na krátkou dobu (např. pracovní stanice). [2]

Interaktivní UPS

Interaktivní systémy UPS jsou dramatickým zdokonalením záložních systémů, protože jsou schopné opravit mírné podpětí nebo přepětí, aniž by vyprazdňovaly baterie. Při použití funkce zesílení pro podpoření zvýšení napětí nebo funkce pro snížení příchozího napětí odkládá interaktivní zdroj UPS použití baterie, pokud není napětí podstatně mimo rozsah. interaktivní zdroj UPS má obvykle displej zobrazující procenta zatížení, procenta zbývající kapacity baterie a další informace o stavu. Jsou výbornou volbou téměř pro všechna důležitá zařízení. [2]

Systémy UPS jsou téměř vždy založeny na baterii. Některé pokročilejší systémy UPS však mohou používat generátory s benzínovým nebo naftovým pohonem, které doplňují energii a prodlužují dobu napájení.

2.2.4. Zálohování dat

Potíže obvykle přicházejí bez varování a důležitá data v síti jsou obvykle ztracena. Zatímco poškozené součásti nebo kabely jednoduše nahradíte, ztracená data prakticky není možné znovu vytvořit - musí být nahrazena.

Mezi příčiny selhání, při kterých může dojít ke ztrátě dat, patří následující [2]:

- Selhání součásti (tj. chyba síťového adaptéru).
- Počítačové viry (způsobené přenosy souborů nebo napadením aplikací).
- Odstranění a poškození dat (například špatně naladěným zaměstnancem).
- Požár způsobený žhářstvím nebo elektrickým zkratem.
- Živelné pohromy (tj. blesk, záplavy, tornáda či zemětřesení).
- Výpadek dodávky elektřiny.
- Krádež a vandalismus.

Zálohy na externí média:

Úkoly vytváření, ověřování a obnovování záloh jsou základní součástí údržby sítě. Nejjednodušší a nejlevnější možností, jak předejít takové katastrofální ztrátě dat, je implementace pravidelných zálohování (nejlépe za použití externího úložiště). Pásková zařízení poskytují jednoduchý a ekonomický způsob zajištění bezpečnosti a použitelnosti důležitých dat v síti. Spolehlivá strategie zálohování minimalizuje riziko ztráty dat uchováváním aktuální zálohy - kopií existujících souborů - takže operační systémy, aplikace a datové soubory mohou být obnoveny, pokud dojde ke ztrátě nebo poškození původních dat. [2]

Důležitá data by se měla zálohovat denně, týdně nebo měsíčně - záleží na úrovni důležitosti dat a četnosti jejich aktualizací. Zálohovací operace by se měly naplánovat na dobu nízkého využití systému (tj. na večerní nebo víkendové hodiny). Uživatelé by měli být upozorněni na to, kdy bude zálohování prováděno, protože během této doby nebudou moci server používat. To, zda se budou zálohovat celé disky, vybrané adresáře nebo jednotlivé soubory, závisí na tom, jak rychle je potřeba obnovit funkčnost po ztrátě důležitých dat.

Úplné zálohování velmi usnadňuje obnovení konfigurací disků, protože jsou všechny soubory obnoveny najednou. Musí se však použít větší počet pásek (zvláště v případě velkého množství dat). Zálohování jednotlivých souborů a adresářů je rychlejší a vyžaduje menší počet pásek, může však být potřeba ručně obnovit konfiguraci disku. Pásková jednotka by měla mít v nejlepším případě dostatečnou kapacitu pro zálohování největšího serveru v síti. Měla by také poskytovat detekci a opravování chyb během operací zálohování a obnovování. [2]

Metody zálohování

Při zálohování se může zvolit jedna z mnoha metod, přičemž v praxi se používá kombinace těchto metod: [2, 5]

- **Úplné zálohování** - Tento typ zálohování se používá k ukládání a označení vybraných souborů bez ohledu na to, zda se od posledního zálohování změnily, nebo ne. Úplné zálohování poskytuje největší ochranu dat, jeho implementace je však nejdelší.
- **Kopírování** - Kopírováním zálohujete všechny vybrané soubory, aniž by se označily jako zálohované.
- **Přírůstkové zálohování** - Při tomto procesu jsou uloženy a označeny vybrané soubory pouze v případě, že se od posledního zálohování změnily.
- **Denní kopírování** - Ukládány jsou pouze ty soubory, které byly ve stejný den změněny, aniž by byly označeny jako zálohované.
- **Rozdílové zálohování** - Vybrané soubory jsou uloženy pouze v případě, že se od posledního zálohování změnily, aniž by byly označeny jako zálohované.

Přírůstkové vs. Rozdílové zálohování

Úplné zálohování trvá nejdéle, může však obnovit server ve stejné podobě, v jaké byl při vytvoření zálohy. Přírůstkové a rozdílové zálohování uloží pouze soubory, které se od posledního zálohování změnily. Při přírůstkovém zálohování budou označeny soubory, které se změnily, zatímco u rozdílového zálohování ne. To znamená, že rozdílová zálohování se budou postupně zvětšovat, protože pravidelně zahrnují soubory, které se změnily od úplného zálohování. Přírůstkové a rozdílové zálohování zahrnuje méně souborů a obvykle je rychlejší, neobsahuje však celý systém.

Ve skutečnosti se většinou začne úplným zálohováním systému a poté se bude pravidelně provádět přírůstkové zálohování, jak se systém a jeho data mění. Nejprve by se systém obnovil úplnou zálohou a poté by se systematicky přidávali každé přírůstkové zálohy, dokud systém nedosáhne svého původního stavu. Obnovování velkého množství přírůstkových záloh však může trvat velmi dlouho.

Pokud se upřednostňuje rozdílové zálohování, obnovil by se systém úplnou zálohou a poté nejnovější rozdílovou zálohu - protože poslední rozdílová záloha bude obsahovat všechny soubory změněné od úplného zálohování, toto může být efektivnější než přírůstkové zálohování, pokud je zahrnut poměrně malý počet souborů. [2]

2.3. *Věcné (aplikační) potřeby*

Při návrhu infrastruktury zabezpečení počítačové sítě je nutné mít na paměti, že cílem řešení informační bezpečnosti je nakonec vždy trvalé udržení firmy v chodu. Bezpečnost je tedy prostředkem, nikoli cílem, a proto se musí při návrhu zvážit různé faktory, jako jsou očekávaná výkonnost sítě, metody šifrování dat a v neposlední řadě okruh poskytovaných služeb sítě uživatelům a zákazníkům.[5]

2.3.1. Výkonnost sítě

Při analýze věcných požadavků firemní sítě se musí zjistit, jaká výkonnost bude od sítě očekávána po zavedení bezpečnostní infrastruktury. Každá nová obranná vrstva znamená větší zpoždění paketů, které musí procházet dalšími filtrovacími zařízeními, pojistnými kontrolami a šifrovacími mechanismy. Pokud je výkonnost či rychlost zpracování pro dané prostředí velmi důležitá, může být zcela oprávněný požadavek na další investice do posílení a upgrade zařízení, která kompenzují vlivy bezpečnostních kontrol. Druhou možností je jasně si říci, že na tak výkonný bezpečnostní hardware a software nemáme dostatek finančních prostředků a dát rychlé odezvě sítě přednost před zabezpečením. Potom ale na sebe musíme vzít veškerá rizika s tím spojená.

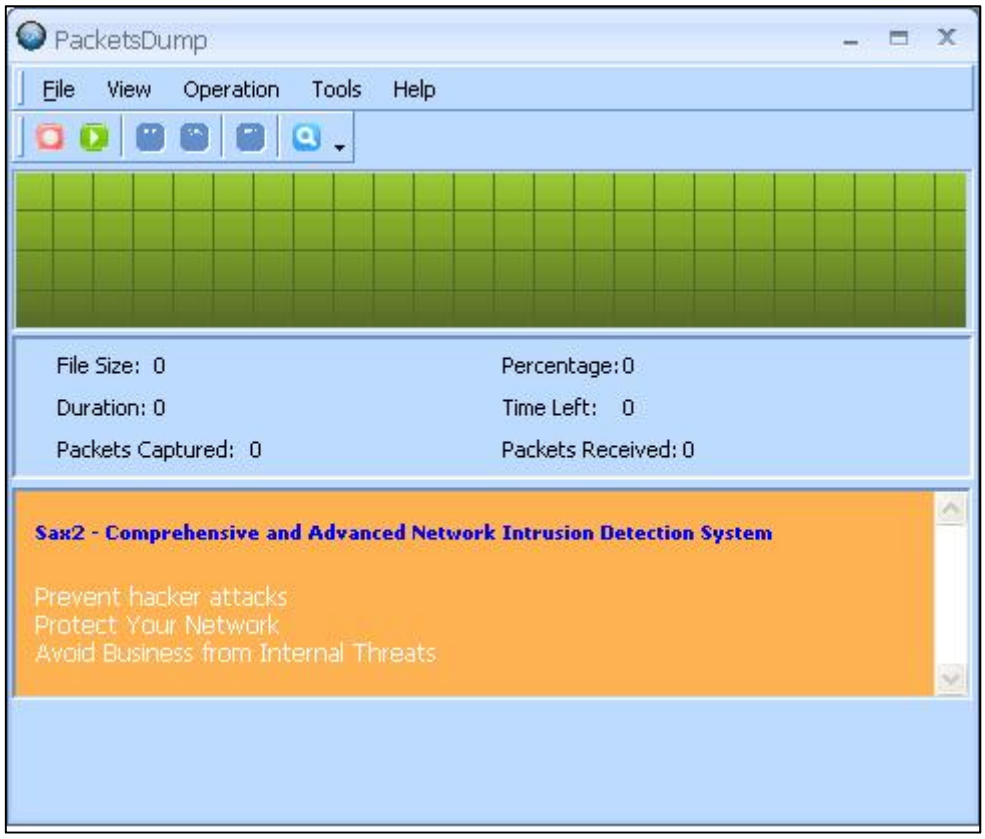
Jasně vymezit představy uživatelů o cílové výkonnosti sítě již během návrhu (před vlastním implementací) je sice obtížné, ale velice důležité. Často se skutečně nedá přesně odhadnout, kolik zátěže bude pro směrovač znamenat šifrovací tunel IPSec nebo o kolik milisekund se prodlouží reakční doba, pokud namísto stavového firewallu použijeme proxy server. Pokud ale v návrhu sítě výkonové požadavky odpovídajících výpočetních zařízení přeceníme, nezbudou nám například finance na vlastní provoz systému. Na druhou stranu,

pokud do systému neinvestujeme prostředky hned na začátku, mohou nás zanedlouho čekat nepříjemně drahé upgrade. [5]

Ověření výkonnosti sítě:

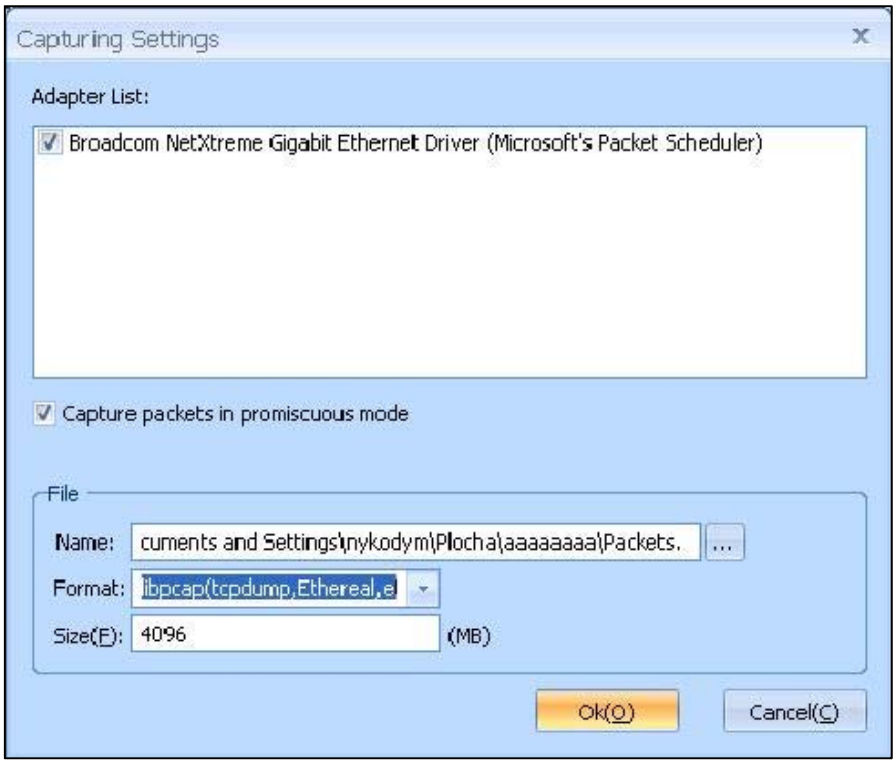
Pro ověření výkonnosti počítačové sítě bude použit program „PacketsDump“, jedná se program, který je šířen pod licencí Freeware. Použití programu je velice jednouché a přehledné. Program umožňuje zaznamenávat provoz počítačové sítě do log souborů, které se nechají kdykoli spustit a analyzovat správcem sítě.

Po nainstalování a spuštění programu se objeví následující okno.



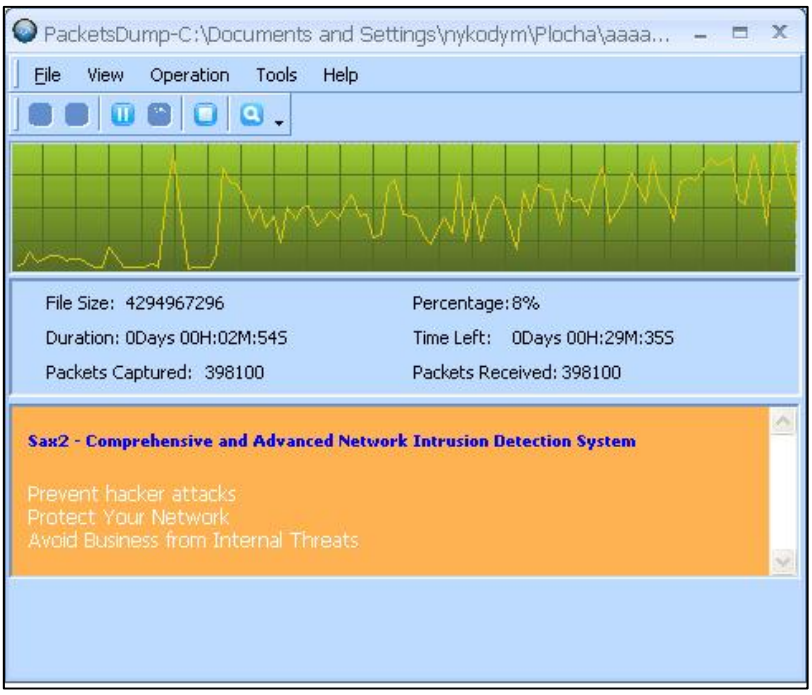
Obrázek 11 Spuštění programu PacketsDump. Zdroj: autor

Pro nahrávání log souborů zatíženosti sítě je potřeba kliknout na červené tlačítko, tím se vyvolá okno, které bude vybízet k odkazu, kam uložit soubor se záznamem provozu sítě, tak jak ukazuje obrázek číslo 12.



Obrázek 12 Uložení záznamu provozu sítě. Zdroj: autor

Po stisknutí tlačítka ok se začne nahrávat provoz na síti do log souboru. Vytíženost provozu sítě je možné vyčíst hned z hlavního okna programu v grafu, tak jak je zaznamenáno na obrázku číslo 13.



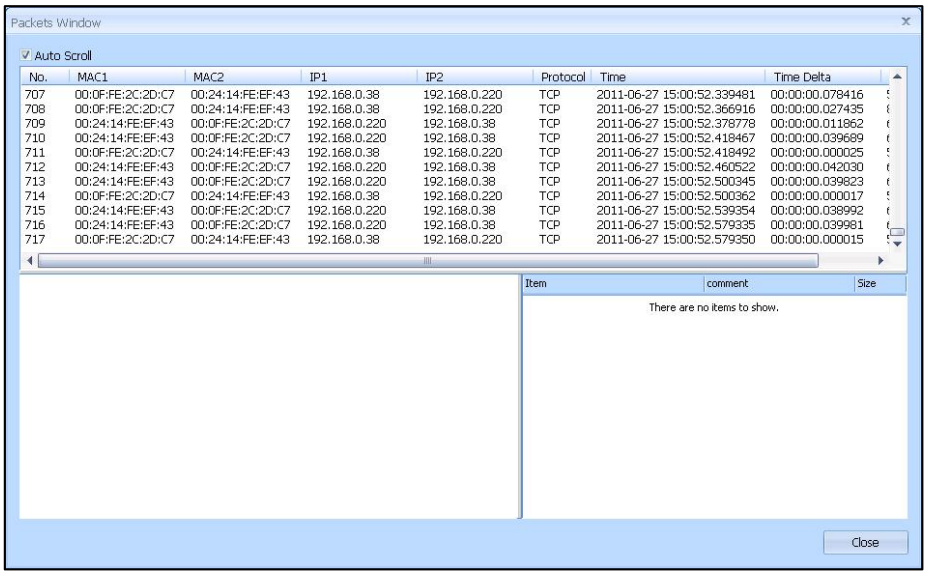
Obrázek 13 Záznam vytíženosti sítě v grafu. Zdroj: autor.

Program také umožňuje zobrazení zatíženosti sítě i v jiném formátu než grafickém. Zatížení sítě v jednotkách rychlosti přenosu dat je zobrazeno na obrázku číslo 14. Toto zobrazení se zapíná v menu kliknutím na View a dále na Statistic WIndow.

Protocol	Packets	Packets(%)	Packets/s	Avg. Packets/s	Bytes	Bytes(%)	Bytes/s	Avg. Bytes/s
Total	105977	(100%)	3340 /s	963 /s	84.846 MB	(100%)	2.996 MB/s	789.842 KB/s
IP	105716	(99%)	3338 /s	961 /s	84.830 MB	(99%)	2.996 MB/s	789.688 KB/s
TCP	105711	(99%)	3338 /s	961 /s	84.829 MB	(99%)	2.996 MB/s	789.677 KB/s
HTTP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
HTTPS	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
SSL	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
SMTP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
MIME	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
IMAP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
POP3	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
FTP_CTRL	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
NTP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
DHCP	1	(0%)	0 /s	0 /s	342 B	(0%)	0 B/s	3 B/s
SNMP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
LDAP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
ICMP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
ARP	95	(0%)	0 /s	0 /s	5.566 KB	(0%)	0 B/s	51 B/s
RARP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
BOOTP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s
PPTP	0	(0%)	0 /s	0 /s	0 B	(0%)	0 B/s	0 B/s

Obrázek 14 Číselné zobrazení zatíženosti sítě. Zdroj: autor.

Další možností zobrazení je Packet Window, v tomto přehledu je vidět jak probíhá datový přenos z jedné IP adresy na druhou IP adresu. Kromě IP adres jsou v tom přehledu zobrazeny i zdrojové a cílové MAC adresy účatníků komunikace a celková velikost přenesených dat mezi nimi, přesně jak ukazuje následující obrázek.



No.	MAC1	MAC2	IP1	IP2	Protocol	Time	Time Delta
707	00:0F:FE:2C:2D:C7	00:24:14:FE:EF:43	192.168.0.38	192.168.0.220	TCP	2011-06-27 15:00:52.339481	00:00:00.078416
708	00:0F:FE:2C:2D:C7	00:24:14:FE:EF:43	192.168.0.38	192.168.0.220	TCP	2011-06-27 15:00:52.366916	00:00:00.027435
709	00:24:14:FE:EF:43	00:0F:FE:2C:2D:C7	192.168.0.220	192.168.0.38	TCP	2011-06-27 15:00:52.378778	00:00:00.011862
710	00:24:14:FE:EF:43	00:0F:FE:2C:2D:C7	192.168.0.220	192.168.0.38	TCP	2011-06-27 15:00:52.418467	00:00:00.039689
711	00:0F:FE:2C:2D:C7	00:24:14:FE:EF:43	192.168.0.38	192.168.0.220	TCP	2011-06-27 15:00:52.418492	00:00:00.000025
712	00:24:14:FE:EF:43	00:0F:FE:2C:2D:C7	192.168.0.220	192.168.0.38	TCP	2011-06-27 15:00:52.460522	00:00:00.042030
713	00:24:14:FE:EF:43	00:0F:FE:2C:2D:C7	192.168.0.220	192.168.0.38	TCP	2011-06-27 15:00:52.500345	00:00:00.039823
714	00:0F:FE:2C:2D:C7	00:24:14:FE:EF:43	192.168.0.38	192.168.0.220	TCP	2011-06-27 15:00:52.500362	00:00:00.000017
715	00:24:14:FE:EF:43	00:0F:FE:2C:2D:C7	192.168.0.220	192.168.0.38	TCP	2011-06-27 15:00:52.539354	00:00:00.038992
716	00:24:14:FE:EF:43	00:0F:FE:2C:2D:C7	192.168.0.220	192.168.0.38	TCP	2011-06-27 15:00:52.579335	00:00:00.039981
717	00:0F:FE:2C:2D:C7	00:24:14:FE:EF:43	192.168.0.38	192.168.0.220	TCP	2011-06-27 15:00:52.579350	00:00:00.000015

Obrázek 15 Zdroj a cíl vysílání paketů. Zdroj: autor.

2.3.2. Šifrování

V počítačových sítích je možno zachytávat cizí přenášená data a při využití vhodných nástrojů je lze i pozměňovat. Toto riziko je třeba brát v úvahu, pokud přenosová cesta mezi klientem a serverem není celá pod spolehlivou kontrolou, zvláště pak v případě připojení po internetu. Ochranu dat přenášených mezi klientem a serverem před vyzrazením a pozměněním zajišťuje šifrování síťové komunikace.

Moderní kryptografie využívá stejné základní myšlenky jako tradiční kryptografii (transpozice a substituce), ale její důraz je jiný. Tradiční, kryptografové používali jednoduché algoritmy. V současné době je tomu naopak. Cílem je, aby šifrovací algoritmus byl komplexní tak, že i když útočník získá velký objem zašifrovaného textu nebude moci tento text bez příslušného klíče rozluštit. [8]

Pro ochranu dat se běžně používají různé šifrovací algoritmy. Většina z nich se může charakterizovat jako algoritmy se symetrickým nebo asymetrickým klíčem, obojí představují velmi rozdílné metody šifrování. [4]

Symetrické šifrování - sdílený klíč

Sdílený klíč neboli symetrický klíč představuje metodu šifrování, u které se kódování i dekódování zprávy provádí pomocí stejné hodnoty klíče. Předpokládáme u ní, že si všechny strany předem vyměnily tajný klíč, a to tak, aby se jej nikdo jiný nedozvěděl. Symetrický klíč znamená rychlý výpočet, protože potřebné matematické vztahy nejsou tak složité jako u asymetrických šifer. Tím pádem nejsou potřebné tak vysoké finanční prostředky na šifrovací mechanismy. Dnes se používá celá řada symetrických šifrovacích algoritmů, například DES (Data Encryption Standard), 3DES, Rijndael, Blowfish nebo IDEA (International Data Ecryption Algorithm). Nejčastěji se přitom v současných VPN sítích setkáváme s algoritmy DES a s vylepšenou verzí 3DES. [4, 5]

Symetrické algoritmy jsou pro sítě VPN velice důležité, protože zajišťují její důvěrnost. Velmi dobře dokážou ochránit datavou zátěž sítě VPN, protože jejich rychlost v poměru k šifrovací síle vychází oproti jiným typům šifrovacích algoritmů velmi výhodně. [5]

Asymetrické šifrování - Veřejný a privátní klíč

Algoritmy a asymetrickým klíčem pracují podle jiné metody šifrování. Vystupují zde dva klíče: veřejný klíč slouží k šifrování prostého textu a privátní klíč k jeho dešifrování.

Zajímavý je zde především vztah mezi těmito dvěma klíči. Z veřejného klíče se žádným způsobem nedá zjistit privátní klíč. Šifrovaný text může proto za pomoci veřejného klíče vytvořit kdokoli, ale dešifrovat a přečíst si jej může jen právoplatný příjemce. Matematický základ asymetrických algoritmů je proto také podstatně složitější než u symetrických šifer. Algoritmy jsou tím pádem pomalejší a náročnější na čas procesoru. Dvěma nejčastěji používanými asymetrickými algoritmy jsou Diffie-Hellman a algoritmus veřejného klíče od RSA. [5]

Asymetrické algoritmy jsou příliš pomalé a nejsou tedy prakticky použitelné pro šifrování hlavního datového toku přes síť VPN, jsou však efektivním prostředkem pro výměnu informací o klíčích v počáteční dohadovací fázi a při výměně klíčů během inicializace spojení VPN [5]

2.3.3. Poskytované služby sítě

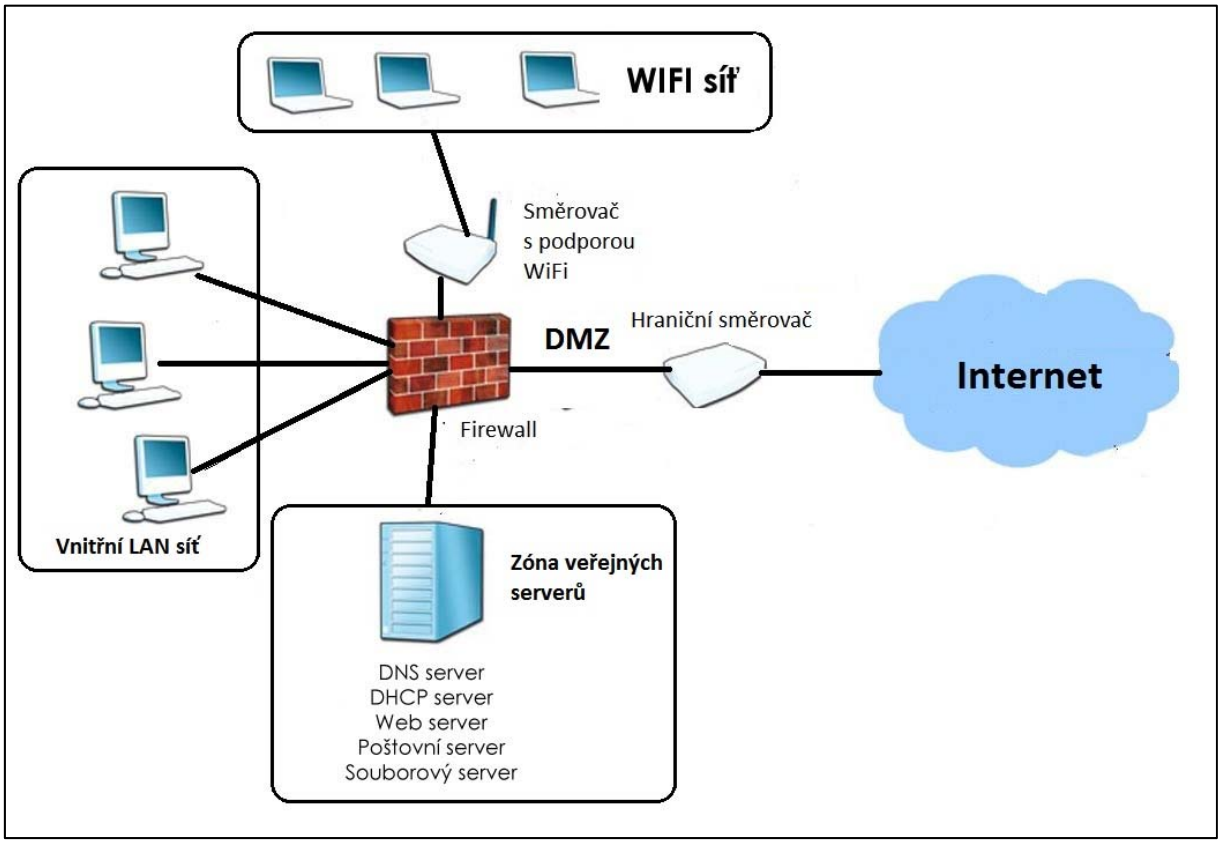
Při výstavbě sítě musíme samozřejmě vědět, jaké služby má síť poskytovat uživatelům a zákazníkům. V typickém firemním prostředí je vhodné všechny nepotřebné služby hned na hranicích sítě zablokovat. V univerzitním prostředí se naopak setkáváme s tím, že neomezený přístup je pro uživatele jednou z poskytovaných služeb. Potom ale nemůže být neznámý provoz implicitně blokován, ale naopak se musí filtrovat jen takový provoz, který zřejmě může síťové prostředí ohrožovat. [5]

Ochránit síťové prostředky proti hrozbám přicházejícím přes kanál, který musí být z důvodu zajištění činnosti firmy otevřený, není nijak snadné. Pokud například bude rozhodnuto povolit v síti z ladících důvodů provoz ICMP, ale zároveň se bojuje proti útokům se záplavou paketů ICMP, může být vhodným řešením zablokování provozu ICMP ve směrovači u poskytovatele, protože takto se část šířky komunikačního pásma uvolní pro služby, které rozhodně musí být přístupné. Jestliže ale naopak přicházejí záplavy paketů SYN, zaměřené na TCP port 80, přičemž jsou poskytovány webové služby třeba v rámci elektronické komerce, pak se tento provoz u poskytovatele zablokovat nemůže. Je možné se pokusit o zablokování provozu z konkrétních zdrojů, ale při distribuovaném útoku s odepřením služeb DoS je hodně těžké sestavit vůbec úplný seznam útočících adres. [5]

Před útoky, které mohou přicházet přes právoplatně otevřené kanály, může ochránit pouze dobře postavená architektura hloubkové obrany.

3. Návrh konkrétního postupu pro zabezpečení počítačové sítě

Před samotným návrhem zabezpečení počítačové sítě, je nejprve potřeba si uvědomit, co od zabezpečení očekáváme a co nám přinese. V žádném případě neexistuje jediný návrh, který by se dal použít na všechny možné sítě, neboť každá organizace má jiné požadavky na svoji síť. Z tohoto důvodu si ukážeme jeden konkrétní případ návrhu postupu pro zabezpečení počítačové sítě. Konkrétní návrh sítě je zakreslen do následujícího obrázku.



Obrázek 16 Konkrétní návrh sítě. Zdroj: autor

Tento návrh zabezpečení počítačové sítě popisuje modelovou situaci firmy, která má 20 zaměstnanců, z toho někteří zaměstnanci pracují vzdáleně z domova. Firma provozuje svůj internetový obchod, který běží na serveru umístěném přímo v počítačové síti firmy. V sídle firmy je pro zákazníky a obchodní partnery umožněno WIFI připojení, které umožňuje připojení k internetu.

Pro daný případ se budou používat následující IP adresy:

- IP adresa hraničního směrovače: 192.168.0.254
- IP adresa serveru: 192.168.0.1
- IP adresa klientských stanic 192.168.0.100 – 192.168.0.150
- IP adresa WIFI routeru 192.168.0.200
- Maska sítě: 255.255.255.0
- IP adresa DNS serveru 192.168.0.1
- IP adresa DHCP serveru 192.168.0.1
- IP rozsah připojených bezdrátových klientů k WIFI routeru 192.168.10.100 – 192.168.10.130.

V následující části práce je sepsán postup, jak takovouto počítačovou síť vhodně zabezpečit před možnými riziky.

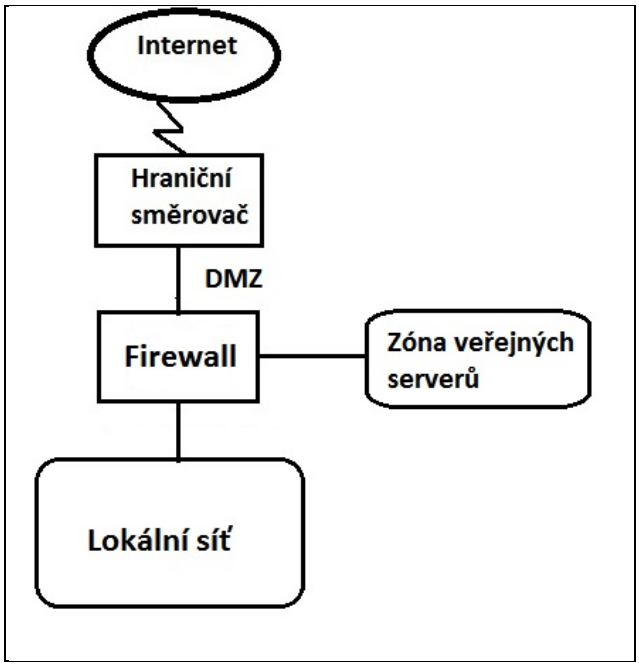
Předešlé poznatky o síti se dají přepsat do následujících bodů:

a) Síť je připojena k internetu, bude tedy potřeba vyřešit problém s neoprávněným vzdáleným přístupem, s infiltracemi, které hrozí při prohlížení webových stránek.
b) Zaměstnanci se připojují vzdáleně, je tedy potřeba vyřešit vzdálený přístup a jeho zabezpečení proti odposlechu.
c) Připojení zákazníků s notebookem po firmě bude jednoduší s bezdrátovým připojením do sítě. Hrozí zde však riziko nepovoleného přístupu do sítě.
d) V síti se nacházejí cenná data, která je potřeba vhodným způsobem zálohovat.
e) Je potřeba vyřešit ochranu serveru proti nečekaným proudovým a napěťovým špičkám v elektrické síti.

Všechny výše uvedené body budou dále popsány v následujících podkapitolách.

3.1. *Připojení sítě k Internetu*

Při připojení sítě k internetu je potřeba vyřešit neoprávněné vniknutí útočníka do interní sítě firmy. Na následujícím obrázku je znázorněno, jak je možné tuto interní síť chránit pomocí hraničního směrovače a hraničního firewallu.



Obrázek 17 Připojení firemní sítě k internetu. Zdroj: autor

Obrázek 17 ukazuje jedno z nejběžnějších uspořádání sítě se směrovačem a firewallem dohromady. Do firemní sítě spadají všechny pracovní stanice, servery, síťové tiskárny a ostatní používaný hardware. V této fázi návrhu doporučuji zakázat všechny porty na příchozí komunikaci z internetu, kromě portu 80, na kterém ve firemní síti běží internetový obchod.

V této konfiguraci je směrovač zodpovědný za funkce směrování, pro které je ostatně stavěný, připojuje tedy firemní síť k Internetu. Často má ale smysl využít ve směrovači filtrování paketů a z provozu odfiltrovat část nežádoucího „šumu“, který je zbytečné zaznamenávat do systémových protokolů firewallu, nebo který chceme „odstřihnout“ hned na vstupní hraně sítě.

Hlavní odpovědnost za řízení přístupu má v tomto návrhu firewall. Na něm je nezbytné implementovat zásadu implicitního blokování veškerého provozu a explicitního povolení jen těch protokolů, které jsou opravdu nezbytné pro provoz firemních procesů a aplikací.

Jestliže se nacházíme v této fázi návrhu sítě, měli bychom již dobře znát aplikační potřeby, pak již nebude tak složité implementovat množinu firewallových pravidel.

Pro navrhovanou síť je vybrán tento router: „CISCO RV082-EU“, jedná se o spolehlivý a vysoce výkonný router společnosti Cisco Systems zobrazen na obrázku 18. Vyznačuje se vysokou úrovní zabezpečení, 4portovým fastethernetovým switchem s automatickým rozpoznáním připojeného typu kabelu a dvěma WAN porty, které buď zvýší výkon

stávajícího internetového připojení, nebo umožní připojení k internetu od dalšího poskytovatele současně. Tento model routeru v sobě zahrnuje jak směrovač tak i firewall.

Obrázek 18 CISCO RV082-EU [11].

3.2. *Vzdálený přístup do sítě*

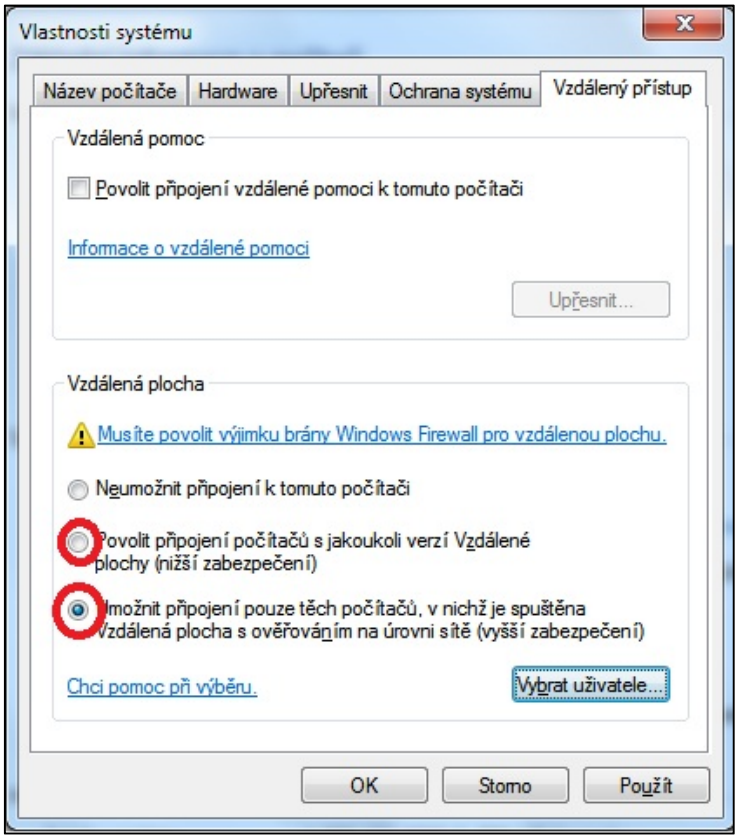
V návrhu sítě je uvedeno, že někteří zaměstnanci firmy se připojují vzdáleně z domova. Tato problematika je však poměrně složitá na řešení, hlavně co se týče správné konfigurace hardwaru a softwaru. Pokud zabezpečujeme síť proti neoprávněnému přístupu, použijeme nejčastěji firewall. Jak již bylo řečeno, firewall může být jak hardwarového, tak i softwarového typu. Softwarové typy jsou již obsaženy v operačních systémech. Hardwarové typy jsou obsaženy například v routerech. Zde nastává již zmíněný problém s konfigurací. Hardwarové firewally bývají obtížné pro nastavení. Nastavit absolutní zákaz nevyžádaného přístupu není až tak složité nastavení, ale nastává problém v případě, že udělujeme výjimku určitému softwaru či uživateli.

Vzdálené přístupy budou řešeny dvěma způsoby:

1. Vzdálenou plochou
2. VNC

3.2.1. Vzdálený přístup pomocí vzdálené plochy

Tuto metodu můžeme využívat při vzdáleném přístupu. Jedná se celkem o bezpečnou metodu z důvodu šifrovaného přenosu. Pro správnou funkci musí být správně nakonfigurovaný router.



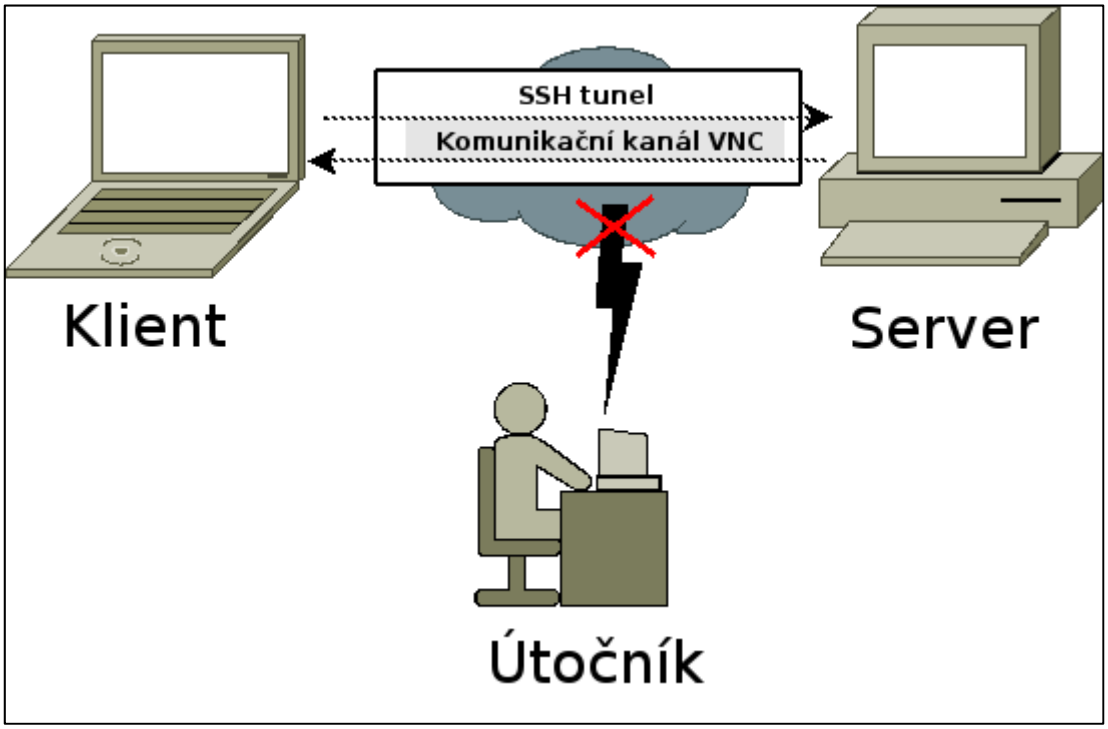
Obrázek 19 Nastavení povolení vzdálené plochy. Zdroj: autor

Pro to, abychom se mohli vzdáleně připojit k pc ve firemní sítě, je potřeba na počítači, ke kterému se chceme vzdáleně připojovat povolit připojení vzdálenou plochou k tomu pc, tak jak ukazuje obrázek 19. Nastavení se provádí ve vlastnostech systému v položce vzdálený přístup.

3.2.2. Vzdálený přístup pomocí VNC

Metoda pracuje na podobném principu jako předchozí. Mění se zde čísla portů a bezpečnost přenosu. Metoda vzdáleného připojení pomocí programu VNC není příliš bezpečná, jelikož přenos dat není nijak šifrován. Pro zvýšení bezpečnosti se používají VPN tunely, jak ukazuje obrázek 20. Volba metody a správné nastavení VPN tunelu je na správci sítě, který ji bude konfigurovat. Pro tunelování můžeme použít dvě metody a to připojení na 2 hardwarové zařízení nebo 2 softwarová zařízení. V našem případě můžeme využít obou

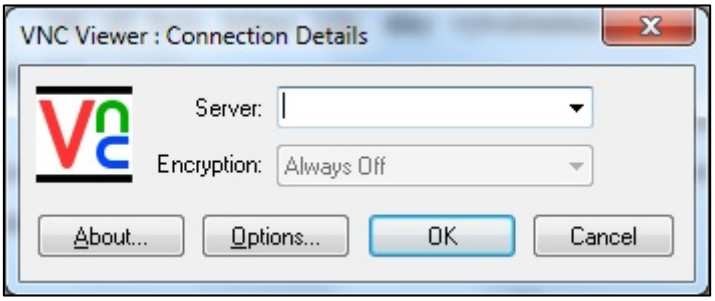
těchto metod, jelikož jsme použili router s podporou VPN. Abychom tedy správně tunelovali, museli bychom přistupovat vzdáleně ze zařízení, které podporuje VPN.



Obrázek 20 Tunel a VNC. [13]

Jak již bylo řečeno výše, díky vytvořenému tunelu, je používání programu VNC bezpečné a znemožní tak útočníkovy odposlouchávat komunikaci.

Pro to abychom mohli používat program VNC je potřeba mít na pc, ke kterému se chceme připojovat nainstalovaný VNC server a na pc, ze kterého se chceme připojovat zase nainstalovaný VNC klienta (VNC Viewer) jak ukazuje obrázek 21.



Obrázek 21 VNCC Viewer. Zdroj: autor

Do kolonky Server se zadává IP adresa pc, ke kterému se chceme připojit. Po připojení ke vzdálenému pc se nám v programu VNC Viewer zobrazí pracovní plocha připojovaného pc

3.3. *Bezdrátová síť ve firmě*

Základem pro vybudování bezdrátové sítě je přístupový bod (AP, Access Point). Jedná se vlastně o bezdrátový hub, prostřednictvím kterého probíhá veškerá komunikace vzduchem (WM, Wireless Medium). Bezdrátové stanice spolu nikdy nekomunikují přímo, ale vždy prostřednictvím AP. Výjimku tvoří pouze tzv. ad-hoc bezdrátové sítě, kde přístupový bod není nutný. V tomto návrhu se ale sítí ad-hoc zabývat nebudeme.

Pro navrhovanou síť bych doporučil tento přístupový bod „CC&C WA-6206-V4“, zobrazen na obrázku 22. Jde o přístupový bod, který je vybaven dvojicí odnímatelných antén pracující v nelicenčním pásmu 2,4 GHz za podpory WiFi standardu 802.11g, který v turbo módu dovolí přenos dat rychlostí až 300 Mbit/s. Zařízení díky technologii WDS[2] dokáže pracovat i jako bridge a repeater, čímž zajistí bezdrátové propojení dvou samostatných síťových segmentů a rozšíří bezdrátový přístup do klientských stanic

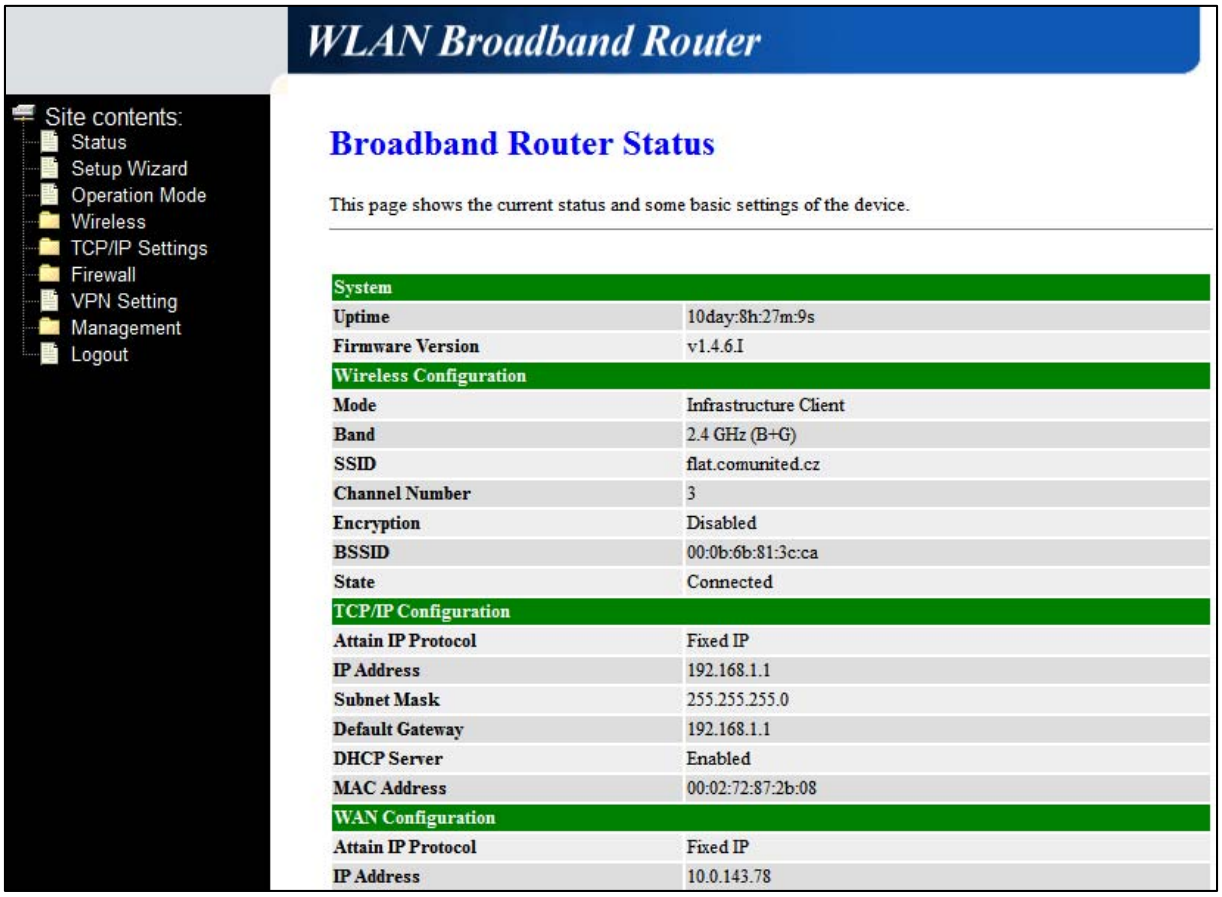
Obrázek 22 CC&C WA-6206-V4. [12]

[2] (WDS)Wireless Distribution System - systém umožňující bezdrátové propojení přístupových bodů v IEEE 802.11.

O zabezpečení sítě proti neoprávněnému přístupu se postará WPA2 šifrování, blokování SSID, filtr MAC adres. Přístupový bod se velice snadno vzdáleně konfiguruje přes webový prohlížeč.

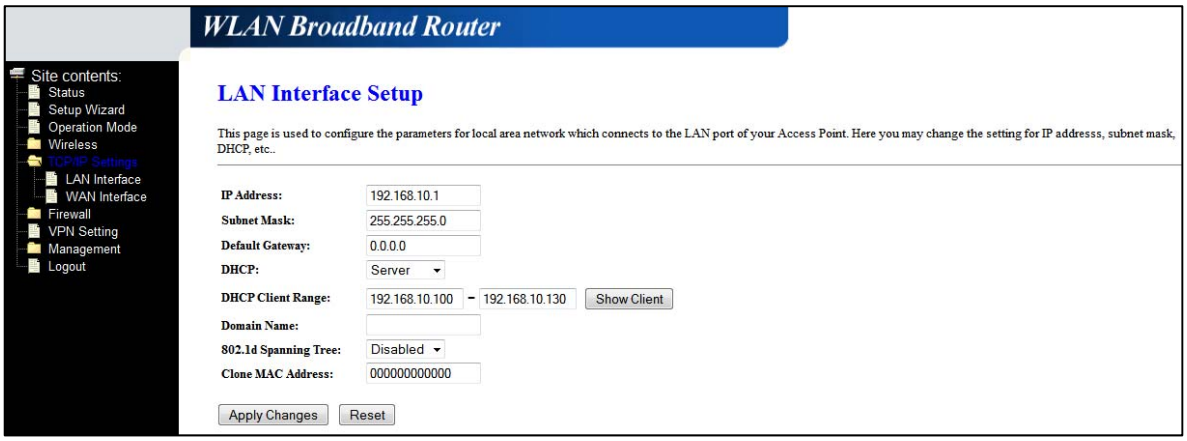
Postup nastavení zařízení

Pro nastavení tohoto zařízení se využije webové rozhraní, zadáním výchozí adresy zařízení, která je z výroby nastavena na 192.168.1.254 se zobrazí následující stránka s menu v levé části, tak jak na obrázku číslo 23.



Obrázek 23 Úvodní stránka CC&C WA-6206-V4. Zdroj: autor

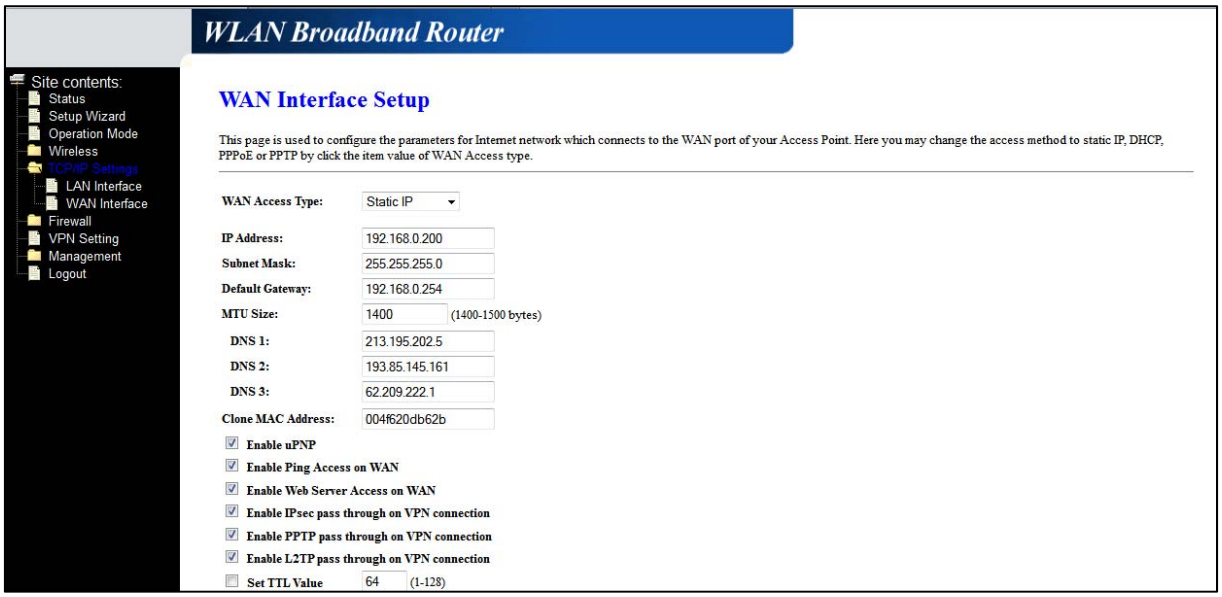
V prvních krocích nastavení je potřeba nejprve nastavit IP adresy. V první řadě se nastaví. IP adresy pro LAN interface, v tomto případě pro WI-FI. Nastavení IP adres pro LAN interface bude vypadat následovně, jak ukazuje obrázek číslo 24.



Obrázek 24 Nastavení IP adresy na LAN inerfacu. Zdroj: autor

Z nastavení je vidět, že IP adresa tohoto routeru je 192.168.10.1, výchozí brána není nastavena, protože toto zařízení v sobě zahrnuje funkce routeru a všechnu komunikaci přes LAN interface (WIFI) předává dál na WAN interface (tedy do naši lokální sítě, kterou chceme chránit). V dalším nastavení je nastaveno, že se tento prvek bude chovat jako DHCP server pro svoje klienty připojené přes WIFI. Tím, že bylo zvoleno, že se prvek bude chovat jako DHCP server, je nutné nastavit rozsah adres, které bude poskytovat připojeným WIFI klientům. Pro WIFI klientů bylo použito adres 192.168.10.100 – 192.168.10.130. Důležitým nastavením je zde, že se jedná o jiný IP rozsah, než je IP rozsah klientských stanic v síti. Jiný rozsah IP adres byl zvolen záměrně, při tomto nastavení nebudou moci klienti připojeni přes WIFI procházet vnitřní počítačovou síť, která se zabezpečuje. Toto je možnost, jak zabezpečit tuto lokální síť od nežádoucího přístupu přes WIFI.

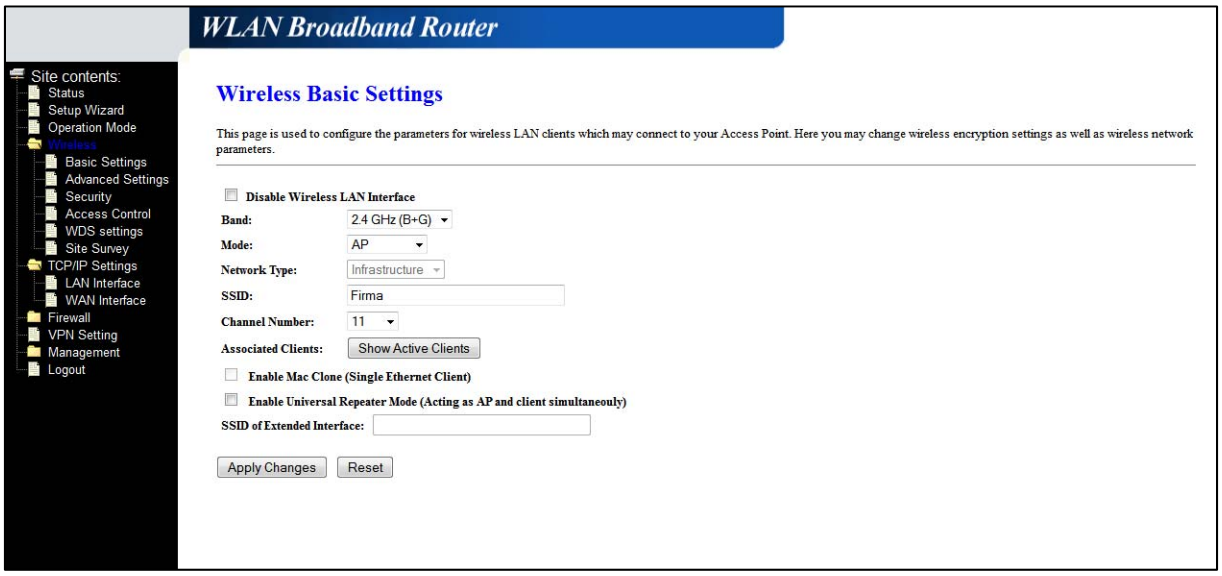
Pro další správné fungování tohoto zařízení je potřeba nastavit WAN interface, tedy tu část, která bude komunikovat s naší lokální sítí. Nastavení IP adres bude vypadat tak, jak ukazuje obrázek 25.



Obrázek 25 Nastavení IP adresy na WAN inerfacu. Zdroj: autor

Z obrázku lze vyčíst, že adresa tohoto prvku je 192.168.0.200, výchozí bránu mu tvoří hraniční směrovač s IP adresou 192.168.0.254. Aby byl umožněn připojeným klientům přes WIFI rozraní přístup k internetu jsou vyplněny i adresy DNS serverů.

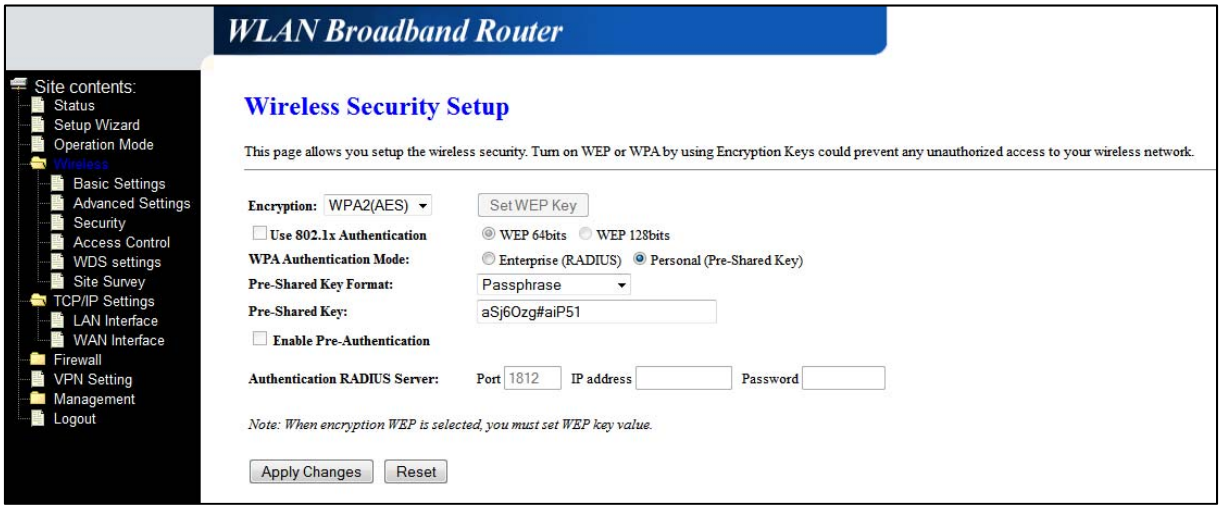
Po nastavení obou interfaců, je potřeba přejít k nastavení WIFI části. Do WIFI nastavení se dostaneme v menu přes položku Wireless. V natavení Wireless nás nejprve bude zajímat záložka Basic Settings, přesne tak, jak je na obrázku 26.



Obrázek 26 Nastavení Basic settings. Zdroj: autor

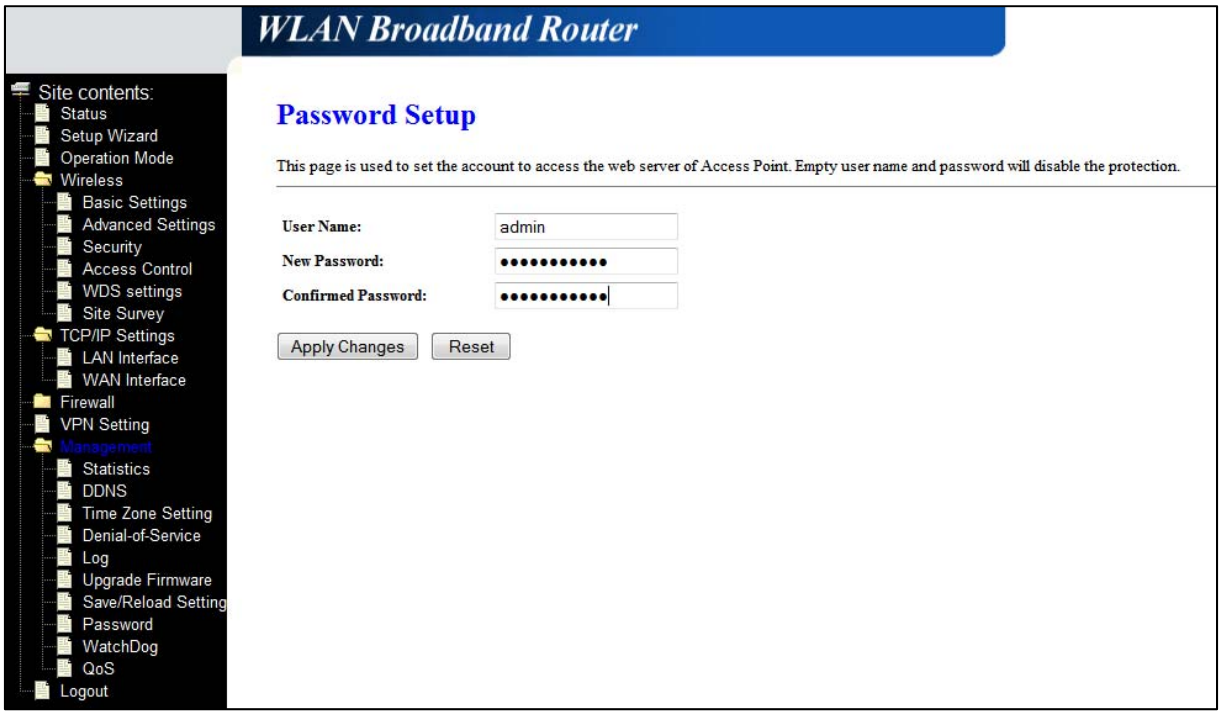
V tomto nastavení se provede výběr B+G normy, módu AP a SSID:Firma. Výběrem normy B+G zajistíme, že se do naší sítě budou moci připojovat klienti se starším typem WIFI hardwaru, který podporuje pouze normu 2,4GHz B a zároveň i ti, kteří využívají hardware podporující normu 2,4GHz G. Rozdíl mezi normami je následující. Norma B umožňuje teoretickou rychlost připojení 11Mb/s a norma G 54Mb/s.
Zvolením módu AP zajistíme, že se zařízení bude chovat jako Access Point neboli přístupový bod. SSID:FIRMA znamená, že se WIFI síť bude jmenovat Firma.

V tuto chvíli je nastavena WIFI část, do které se může připojit kdokoli, kdo zachytí vysílaný signál. Aby se zamezilo neoprávněnému připojení k síti, je potřeba zařízení zabezpečit, Nastavení zabezpečení bezdrátové části se provádí v menu výběrem Security.



Obrázek 27 Nastavení zabezpečení bezdrátové části. Zdroj: autor

Na obrázku 27 je vidět, že pro zabezpečení bezdrátové sítě bylo požito technologie WPA2, jako heslo bylo zvoleno tzv. silné heslo, tedy heslo, které obsahuje nejméně 8 znaků, obsahuje malá a velká písmena, číslice a ne-alfanumerický znak. V tuto chvíli je nastavena WIFI síť, nezbývá už nic jiného, než zaheslovat zařízení, aby nikdo nemohl ať už úmyslně nebo neúmyslně změnit nastavení zařízení. Nastavení přihlašovacího jména a hesla se provádí v menu výběrem položky Management a následně výběrem Password, přesně tak, jak ukazuje obrázek 28.



Obrázek 28 Nastavení přihlašovacích údajů. Zdroj: autor

3.4. *Záloha dat*

Sítě se prostřednictvím odolnosti proti chybám pokoušejí předcházet potenciálním problémům dříve, než nastanou. Jednou z nejčastěji používaných metod je RAID (Redundant Array Of Independent Disks). RAID umožňuje používat více fyzických jednotek tvořících různé logické svazky, které zrcadlí jednotky nebo sdílená data, čímž zvyšují výkon. [2]

Pro zálohu dat, je navržena metoda RAID 1, jde o metodu, kde se 1 disk zrcadlí na druhý. Při selhání jednoho disku, tak zůstávají cenná data na druhém. Jedním důvodem, proč volit tuto metodu, je její lehké nastavení, které je již dnes dostupné na většině serverových deskách a náklady na provoz se rovnají koupi disku o stejné kapacitě jako je disk, který chceme zálohovat.

Při zrcadlení jsou data zapsána na jednu diskovou jednotku a souběžně i na další jednotku. Selže-li jedna z jednotek, může systém použít obsah druhé jednotky (a obnovit jednotku, která selhala). Hlavní výhodou zrcadlení disků je to, že poskytuje stoprocentní redundanci dat. Protože je obsah jednotky zcela zapsán i na druhou jednotku, nevznikne problém, když jedna jednotka selže. Obě jednotky obsahují neustále stejná data a každá z nich může pracovat jako funkční jednotka. Tato metoda je však nákladná, protože každá jednotka v systému musí být duplikována. Aby se mohlo provést zrcadlení jednotky o velikost 500 GB, je potřeba mít k dispozici druhou jednotku s velikostí 500 GB. [2]

3.5. *Ochrana serveru před přepětím*

Jako ochranou serveru před přepětím byl zvolen záložní zdroj: „APC Power Saving Back-UPS Pro 1500“ zobrazen na obrázku 29. Jedná se o zdroj, který v sobě kombinuje jak funkce záložního zdroje, tak i přepěťové ochrany, navíc má v sobě i přepěťovou ochranu konektoru RJ-11 pro telefonní linku a konektoru RJ-45 pro síťové rozhraní ethernet.

Při dlouhodobém výpadku elektrického proudu a tím pádem i vybití akumulátorů tohoto záložního zdroje umí tento záložní zdroj uspat počítač. Tato funkce je velice důležitá, při výpadku proudu, tak se předejde ztrátě cenných data uložená na serveru.

Obrázek 29 UPS - APC Power Saving Back-UPS Pro 1500.[13]

Parametry:

- Ochrana telefonní linky
- Technologie: Line-interaktivní
- Komunikační rozhraní: USB
- Barva: černá
- Kapacita [VA]: 1500
- Výkon [W]: 865
- Počet baterií: 1
- Nominální vstupní napětí [V]: 230
- Doba dobíjení akumulátorů: 8 hodin
- Možnost rozšířit o další akumulátory

4. E-learningový kurz

E-learning je označení pro vzdělávací proces, jež využívá a komunikační a IT k tvorbě kurzů, také k distribuci studijního obsahu, nebo i komunikaci mezi studenty a pedagogy a v neposlední řadě i k řízení studia.

Spolehlivý e-learningový systém nutně vyžaduje zpětnou vazbu. Důvodem je fakt, že je stejně důležité informace uživatelům zpřístupnit, ale zároveň i umožnit procvičování získané znalosti pomocí pravidelných testů a úkolů. Neméně důležité je i sledovat chování uživatelů v tom kterém systému. Vyhodnocení získaných uživatelských trendů je pak nápomocné k odhalení silných i slabých míst v e-learningových kurzech a pomůže také získat jasnou představu o tom, jak se uživatele při studiu chovají.[1]

Nutnost neustálého celoživotního vzdělávání si dnes již naštěstí uvědomuje skoro každý, jedinci, firmy i vládní představitelé. Otázkou tedy není, jak o této nutnosti někoho přesvědčit, nýbrž jakým způsobem je možné vzdělávání poskytovat tak, aby bylo pro každého, kdykoliv a kdekoliv. [9]

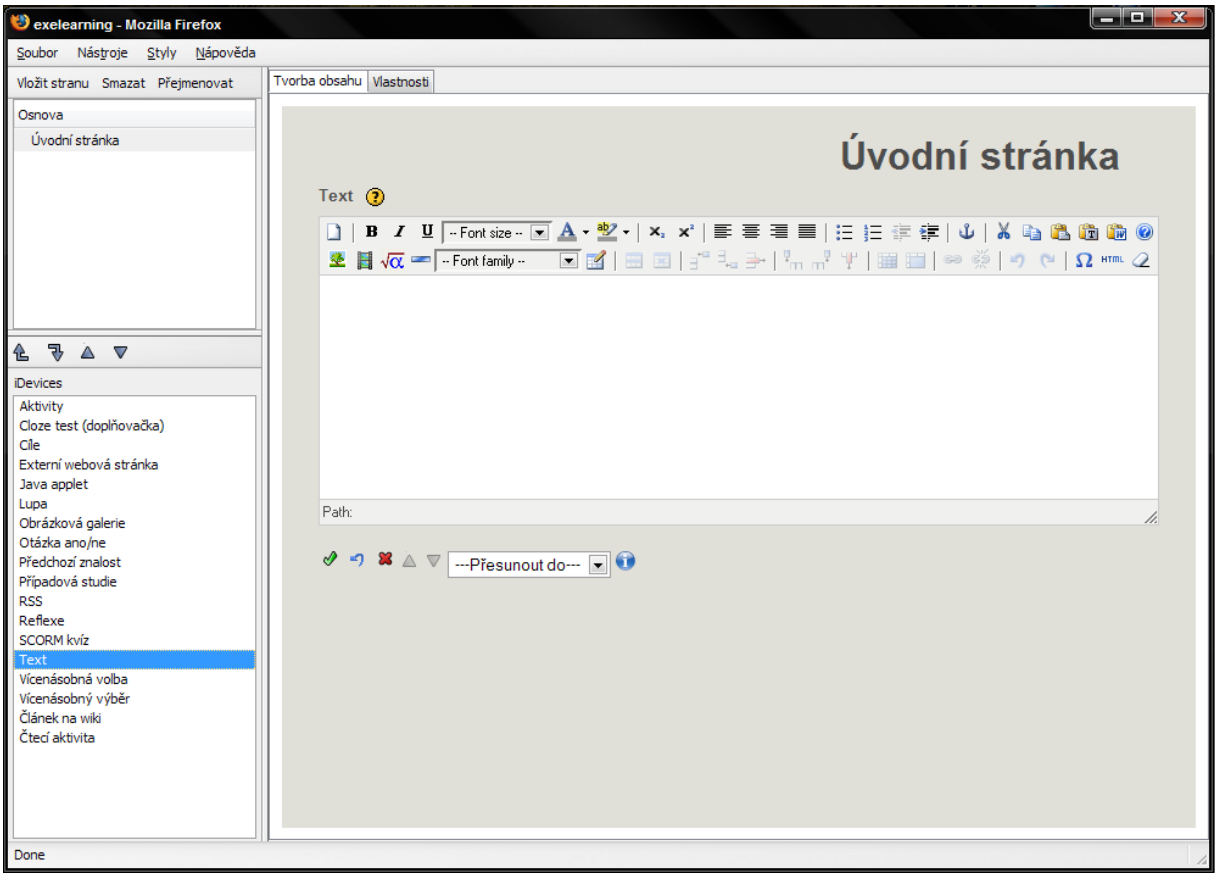
Jedna z vlastností e-learningu je, že je schopen podat požadované informace kdykoli a kdekoliv, toto bylo důvodem k jeho vytvoření. „E-learning je vzdělávací proces, využívající informační a komunikační technologie“[1].

Pro samotnou tvorbu e-learningového kurzu byl zvolen editor eXe. Zkratka eXe je: „e-learning XHTML editor“. Jedná se o program, který je poskytován zcela zdarma v české lokalizaci. Jde o editor, který je velice podobný Wordu nebo konkurenčnímu Writeru z distribuce OpenOffice.org. V editoru se jednoduše vloží text, obrázek případně audio nebo video soubory. Pracovní prostředí editoru eXe je znázorněno na obrázku 30.

Program eXe podporuje [10]:

- Vložení textových článků, úryvků.
- Vložení MP3 audio souborů.
- Vložení video souborů a ukázek.
- Načtení RSS kanálů.
- Vytvoření jednoduchých testů a kvízů.
- Vložní obrázkové galerie.
- Provázání jednotlivých částí i podstran hypertextovými odkazy.

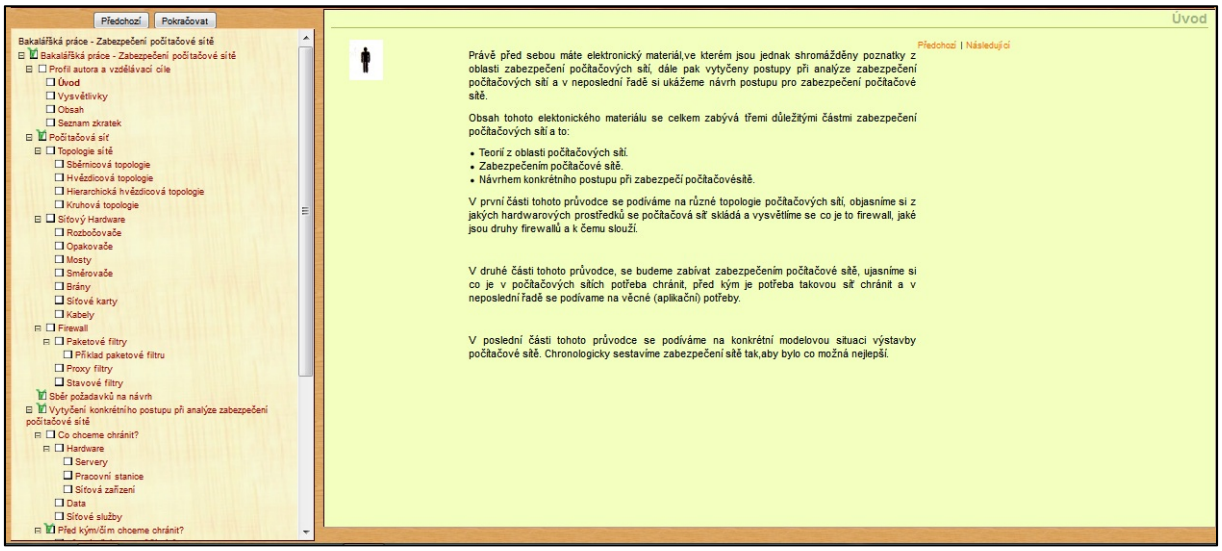
- Podporuje export vzdělávacích materiálů ve formátu IMS nebo SCORM.
- Podporuje vlastní formát souborů - ty lze následně i vkládat jeden do druhého.
- Dokáže vytvoření vzdělávací kurz vyexportovat jako běžnou webovou stránku.



Obrázek 30: Pracovní prostředí editoru eXe. Zdroj: autor

Vytvořený kurz

Jak je již uvedeno v úvodu, stěžejním úkolem této práce je vytvoření e-learningového kurzu, který má sloužit studentům Fakulty ekonomicko-správní v Pardubicích, jako studijní opora předmětu „Počítačové sítě I“. Na obrázku 31 je zobrazena struktura vytvořeného kurzu, který je nahrán do prostředí Moodlu.



Obrázek 31 Vytvořený kurz v MOODLU. Zdroj:autor

Při spuštění kurzu se posluchači zobrazí v levé části obrazovky obsah kurzu. Pro zobrazení jednotlivých kapitol a podkapitol kuru je potřeba vybrat v menu příslušný odkaz. Po zvolení odkazu se otevře daná kapitola nebo podkapitola v hlavním okně. V textu jsou požívány 2 piktogramy. Na obrázku 32 je zobrazen piktogram postavy, který vždy uvádí jednotlivé kapitoly.

Obrázek 32 Piktogram postava. Zdroj: autor

Piktogram prstu zobrazen na obrázku 33 vyzdvihuje důležité pojmy nebo myšlenky k zapamatování.

Obrázek 33 Piktogram prst. Zdroj: autor

5.Závěr

Tato bakalářská práce se zabývá zabezpečením počítačových sítí. Práce na počítačích spojených v počítačových sítích se stala každodenní rutinou snad v každém odvětví. Spojení sítí vytváří podmínky k rychlejšímu a efektivnímu proudění dat. Zmíněné spojení počítačových jednotek do sítě umožňuje jednak sdílet prostředky s jinými uživateli, dále pak odpadá nutnost nakupovat pro každého uživatele vlastní prostředky, jakými jsou například tiskárny, scanery a další. Velmi podstatnou výhodou je také možnost sdílení dat v síti. Veškeré sdílení dat a prostředků nutně provází potřebu chránit tyto data před zneužitím zabezpečení a ochranu samotného hardwaru sítě, který je nosnou infrastrukturou každé sítě.

Na začátku této práce jsou shromážděny poznatky ze zabezpečení počítačových sítí, následuje popis jednotlivých součástí obvodu sítě a jednotlivé typy síťových útoků. V druhé části této bakalářské práce je obsaženo vytyčením konkrétního postupu při zabezpečování počítačové sítě. V této kapitole je vysvětlena jak nutnost potřeby ochrany dat. Dále je přesně definováno, co je potřeba v počítačových sítích chránit a před kým nebo čím je tyto věci nutné udržovat bezpečí. V neposlední řadě se v této kapitole práce zabývá i věcnými (aplikačními) potřebami sítě.

Třetí část této práce obsahuje konkrétní návrh počítačové sítě. V této kapitole se práce zabývá jednotlivými, chronologicky uspořádanými postupy, které mají za cíl tu kterou počítačovou síť zabezpečit. Je zde popsána konfigurace hardwaru sítě i postup pomocí vybraných programů, jak dané nastavení a celkové zabezpečení dané počítačové sítě zkontrolovat. Výstupem celé práce je e-learningový kurz, který bude sloužit studentům předmětu: "Počítačové sítě I" na Fakultě Ekonomicko-Správní při Univerzitě Pardubice. V kurzu jsou stejně jako v této práci shromážděny poznatky z počítačových sítích, je sestavena analýza zabezpečení počítačové sítě a navržen konkrétní postup zabezpečení počítačové sítě. Věřím, že vytvořený kurz bude sloužit těm účelům, pro něž byl vytvořen a umožní tak získat posluchačům kurzu věcný a ucelený přehled o dané problematice.

Seznam literatury

Monografie

[1] BAREŠOVÁ, Andrea. *E-Learning ve vzdělávání dospělých*. 1. vyd. Praha : VOX, 2003. 174 s. ISBN 80-86324-27-3.

[2] BIGELOW, Stephen J. *Mistrostvím v počítačových sítích : Správa, konfigurace, diagnostika a řešení problémů*. Vyd 1. Brno : Computer Press, 2004. 990 s. ISBN 80-251-0178-9.

[3] CHAPMAN, Dawid W.; FOX, Andy. *Zabezpečení sítí pomoci CiscoPIX Firewall : Autorizovaný výukový průvodce*. Vyd 1. Brno : Computer Press, 2004. 343 s. ISBN 80-722-6963-1.

[4] DOSTÁLEK, Libor; KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémém DNS*. 5. aktualizované vydání. Brno : Computer Press, 2008. 488 s. ISBN 978-80-251-2236-5.

[5] NORTHCUTT, Stephen, et al. *Bezpečnost počítačových sítí : Kompletní průvodce návrhem, implementací a údržbou zabezpečení sítě*. Vyd 1. Brno : CP Books, 2005. 589 s. ISBN 80-251-0697-7.

[6] SCAMBRAY, Joel, MCCLURE, Stuart. *Hacking bez tajemství* 1. vyd. Praha : Computer Press, 2003. 461 s. ISBN 80-7226-781-7.

[7] STREBE, Matthew; PERKINS, Charles. *Firewally a proxy servery : Praktický průvodce*. Vyd 1. Brno : Computer Press, 2003. 450 s. ISBN 80-7226-983-6.

[8] TANENBAUM, Andrew S. *Computer networks.* Upper Saddle River : Prentice Hal, 1996. 813 s. ISBN 0-13-394248-1.

Webové stránky

[9] PETERKA, Jiří. *E-archiv Jiřího Peterky* [online]. 2000 [cit. 2010-03-23]. E-archiv. Dostupné z WWW: <http://www.earchiv.cz/>.

[10] *Zdarma.org* [online]. c2005-2010 [cit. 2010-03-23]. EXe - e-Learning XHTML Editor - autorský prostředek, tvorba e-learningu a online kurzů. Dostupné z WWW: <http://www.zdarma.org/1306-exe-e-learning-xhtml-editor-autorsky-prostredek-tvorba-e-learningu-online-kurzu/>.

[11] *Alza.cz* [online]. 2011 [cit. 2011-05-05]. ALZA.cz. Dostupné z WWW: <http://www.alza.cz/cisco-rv082-eu-d217103.htm#popis>.

[12] *Xcomputer.cz* [online]. 2011 [cit. 2011-05-05]. Xcomputer.cz. Dostupné z WWW: <http://www.xcomputer.cz/netgear-wg302-prosafe-d176244.htm>.

[13] *Abclinuxu.cz* [online]. 2011 [cit. 2011-05-05]. Abclinuxu.cz. Dostupné z WWW: <http://www.abclinuxu.cz/clanky/site/vnc-pouzivame-vzdaleny-desktop>.

Seznam zkratek

AUI - Attachment Unit Interface

DNS - Domain Name System

FTP - File Transfer Protocol

HTTP - Hyper Text Transport Protocol

HTTPS - HTTP Secure

ICMP - Internet Control Message Protocol.

IDS - Intrusion Detection System

IMAP - Internet Mail Access Protocol

L2TP - Layer 2 Tunneling Protocol

LAN - Local Area Network

MD5 - Message Digest algorithm

NAT - Network Address Translation

NetBios - Network Basic Input/Output Systém

NFS - Network File System

NIC - Network Interface Card.

PPP - Point to Point Protocol

RAID - Redundant Array of Inexpensive Disks

SHA - Secure Hash Algorithm

SMTP - Simple Mail Transfer Protocol

SNMP - Simple Network Management Protocol

SSH - Secure Shell

SSL - Secure Sockets Layer

TCP - Transmission Control Protocol

UDP - User Datagram Protocol

UPS - Uninterruptible Power Supply

UTP - Unshielded twisted pair

VPN - Virtual Private Network

WAN - Wide Area Network

Seznam obrázků