VŠB - Technická univerzita Ostrava

Fakulta elektrotechniky a informatiky

Katedra informatiky

Systém pro správu a administraci síťových prvků heterogenní sítě

Heterogeneous Computer Network Administration and Management

2012 Jaromír Popovský

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání bakalářské práce

Student: **Jaromír Popovský**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R025 Informatika a výpočetní technika

Téma: Systém pro správu a administraci síťových prvků heterogenní sítě
Heterogeneous Computer Network Administration and Management

Zásady pro vypracování:

Cílem bakalářské práce je navrhnout a implementovat systém umožňující správu a administraci prvků heterogenní sítě (Linux, Windows) provozované na střední škole. Práce bude zahrnovat implementaci jednotného konfiguračního rozhraní umožňujícího monitorování a správu všech prvků.

1. Rešerše obdobných systémů a jejich srovnání.
2. Konfigurační rozhraní pro systémy Linux a Windows Server.
3. Monitorování sítě, síťového provozu a statistiky (SNMP, MRTG).
4. Konfigurace zabezpečení a filtrování provozu (DansGuardian, iptables)
5. Záznam událostí do jednotné databáze a její prohlížení.
6. Nasazení systému do reálného provozu a vyhodnocení jeho chování.

Seznam doporučené odborné literatury:

Andrew S. Tanenbaum, Computer Networks, Prentice Hall, 5 ed., 2010, ISBN 978-0132126953
Richard Froom, Implementing Cisco IP Switched Networks, Cisco Press, 2010, ISBN 978-1587058844
Tom Adelstein, Linux System Administration, O'Reilly Media, 2007, ISBN 978-0596009526

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Michal Krumnikl**

Datum zadání: 18.11.2011

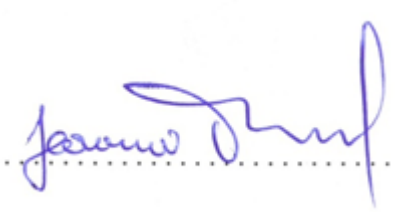
Datum odevzdání: 04.05.2012

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 4. 5. 2012



Na tomto místě bych rád poděkoval všem, kteří mi nepřímo s prací pomohli, především svému vedoucímu bakalářské práce Ing. Michalu Krumniklovi za pomoc při výběru tématu, sestavení obsahu, cenných rad, konzultací a připomínek, které mi byly vodítkem pro vypracování této práce.

Abstrakt

Bakalářská práce je zaměřena na návrh a implementaci systému umožňující správu a administraci prvků heterogenní sítě (Linux, Windows), provozované na střední škole. Práce obsahuje rozdělení na teoretickou část a praktickou část. V teoretické části jsou srovnávány obdobné systémy podle základního rozdělení systému do skupin a jejich vyhodnocení splnění zadaného rozsahu. V praktické části je popsán samotný navrhnutý systém a postupně jeho jednotlivé části. První část se zaměřuje na monitorování sítě, síťového provozu a jejich statistik. Další část obsahuje konfiguraci zabezpečení a filtrování provozu. Poslední praktická část se zabývá záznamem událostí a zobrazením jednotlivých statistik. Závěr je věnován vyhodnocení implementace systému a jeho přínosu. Veškeré zdrojové kódy použité pro navrhnutý systém jsou na přiloženém CD/DVD.

Klíčová slova

systém, administrace, monitorování sítě, síťový provoz, statistika, zabezpečení, filtrování provozu, události, Linux, Windows, SNMP, MRTG, iptables, DansGuardian

Abstract

The central focus of this thesis is a proposal and an implementation of a system used in high school that allows an administration of heterogeneous networks components (Linux, Windows). This thesis is divided into a theoretical and a practical part. In the theoretical part, similar systems are compared. The evaluated systems are divided into several groups based on their main functions, and evaluated on how well they satisfy the criteria. In the practical part, the proposed system and its parts are described. The focus of the first part is a monitoring of a network, its operation, and the statistics. Another part includes a configuration of the security and content filtering. The last practical part is dealing with an event logging and displaying of individual statistics. The end is devoted to an evaluation of the system implementation and its contribution. All resource codes used for the designed system are on the attached CD/DVD.

Keywords

system, administration, network monitoring, network traffic, statistics, security, traffic filtering, events, Linux, Windows, SNMP, MRTG, iptables, DansGuardian

Seznam použitých symbolů a zkratek

ACL	-	Access control list
BSD	-	Berkeley Software Distribution
CD	-	Compact Disc
CPU	-	procesor
DHCP	-	Dynamic Host Configuration Protocol
DNS	-	Domain Name Systém
DVD	-	Digital Versatile Disc
GPL	-	General Public License
HP	-	Hewlett-Packard
HTML	-	HyperText Markup Language
IP	-	Internet Protocol
MAC	-	Media Access Control
MIB	-	Management Information Base
MRTG	-	Multi Router Traffic Grapher
OID	-	Object Identifier
OS	-	operační systém
PC	-	Personal computer
PDO	-	PHP Data Objects
RADIUS	-	Remote Authentication Dial In User Service
RRD	-	Round-Robin Database
RX	-	Receive
SNMP	-	Simple Network Management Protocol
SSL	-	Secure Socket Layer
TX	-	Transmit
URL	-	Uniform resource locator
Wi-Fi	-	Wireless Fidelity
XML	-	Extensible Markup Language

Obsah

1 Úvod **5**

2 Rešerše systémů pro administraci sítí **6**

2.1 Monitorování sítě, síťového provozu a statistiky 6

2.1.1 Ganglia 6

2.1.2 Nagios 7

2.1.3 Ntop 7

2.2 Konfigurace zabezpečení a filtrace provozu 8

2.2.1 Webmin 8

2.2.2 Shorewall 9

2.2.3 SquidGuard 9

2.3 Záznam událostí do jednotné databáze 11

2.3.1 Nagios 11

2.4 Celkové zhodnocení rešerše systémů pro administraci sítí 12

2.4.1 Sysadminnet 12

2.4.2 Závěr srovnání a hodnocení 13

3 Konfigurační rozhraní navrhovaného systému **15**

3.1 Popis navrženého systému a jeho požadavky 15

4 Monitorování sítě, síťového provozu a statistiky **17**

4.1 Monitorování sítě (SNMP) 17

4.1.1 Správa uložených zařízení 18

4.1.2 Stav a konfigurace zařízení 20

4.1.3 Výpis přehledu událostí nedostupných zařízení 22

4.2 Síťový provoz (MRTG) 23

4.2.1 Popis grafu 23

4.2.2 Přehled rozhraní ve skupinách 24

5 Konfigurace zabezpečení a filtrování provozu **25**

5.1 Učebny internet (iptables) 25

5.1.1 Správa učeben a počítačů 26

5.1.2 Aktivace a deaktivace počítačů 27

5.2 Filtrování obsahu (DansGuardian) ... 28
5.2.1 Správa konfiguračních souborů ... 29
5.2.2 Blokování provozu ... 31
5.3 Připojení Wi-Fi ... 32
5.3.1 Správa MAC adres ... 32
6 Záznam událostí do jednotné databáze ... 34
6.1 Statistika událostí ... 34
6.1.1 Vyhledání událostí podle skupiny ... 36
6.1.2 Vyhledání událostí podle uživatele ... 36
7 Konfigurace systému ... 37
7.1 Systém - číselníky ... 37
8 Závěr ... 39
9 Literatura ... 40
Přílohy ... 42
A Obrázky uživatelského rozhraní ... 42

Seznam tabulek

Tabulka 2.1 - výsledné srovnání monitorování sítě, síťového provozu a statistiky 8
Tabulka 2.2 - výsledné srovnání konfigurace zabezpečení a filtrace provozu 10
Tabulka 2.3 - výsledné srovnání záznam událostí do jednotné databáze 11
Tabulka 2.4 - celkové zhodnocení rešerše systémů pro administraci sítí 14

Seznam obrázků

Obrázek 4.1 - sekvenční diagram SNMP dotazů na monitorovaná zařízení (snmp.pl) 17
Obrázek 4.2 - přehled uložených zařízení (SNMP) 18
Obrázek 4.3 - vložení nového zařízení (SNMP) 19
Obrázek 4.4 - přehled provozu zařízení v zadané skupině (SNMP) 20
Obrázek 4.5 - detailní přehled stavu vybraného zařízení (SNMP)..... 21
Obrázek 4.6 - konfigurace vybraného portu na zvoleném zařízení (SNMP) 22
Obrázek 4.7 - přehled a počty výskytu chyb na zařízeních online (SNMP) 22
Obrázek 4.8 - detailní výpis všech chybových stavů podle času v daném dni (SNMP) 23
Obrázek 4.9 - přehled výběru a ukázka síťového provozu (MRTG) 24
Obrázek 5.1 - sekvenční diagram skriptu pro blokování počítačů (internet.pl) 25
Obrázek 5.2 - konfigurace učeben a počítačů (iptables) 27
Obrázek 5.3 - přehled stavu počítačů v učebně, z pohledu všech uživatelů (iptables) 28
Obrázek 5.4 - výpis pravidel firewallu přesměrovaných počítačů (iptables)..... 28
Obrázek 5.5 - výběr konfiguračního souboru, restartování služby Dansguardian 29
Obrázek 5.6 - jeden z panelů (ipgroups) konfiguračních souborů (DansGuardian) 30
Obrázek 5.7 - výpis a konfigurace souboru ipgroups (DansGuardian)..... 30
Obrázek 5.8 - přehled blokování filtrování provozu DansGuardianu 31
Obrázek 5.9 - konfigurace připojení Wi-Fi, restartování služby FreeRadius 33
Obrázek 5.10 - výpis záznamů pro konfiguraci souboru users.mac (Wi-Fi) 33
Obrázek 6.1 - sekvenčví diagram uložení záznamů udalostí do databáze (dir_file_mysql.pl) ... 35
Obrázek 6.2 - panel pro vyhledání záznamů událostí 35
Obrázek 6.3 - ukázka výpisu vyhledání uživatele v záznamu události 36
Obrázek 7.1 - výběr konfigurace systému a číselníků 37
Obrázek 7.2 - přehled konfigurace systému..... 38
Obrázek A.1 - přihlášení do systému 42
Obrázek A.2 - úvod po přihlášení 42
Obrázek A.3 - modul učebny internet..... 43
Obrázek A.4 - modul filtrování provozu..... 43
Obrázek A.5 - modul připojení Wi-Fi..... 44
Obrázek A.6 - modul monitorování sítě..... 44
Obrázek A.7 - modul síťový provoz 45
Obrázek A.8 - modul statistika událostí..... 45
Obrázek A.9 - modul systém - číselníky..... 46

1 Úvod

Hlavní myšlenkou vytvoření systému bylo sjednocení správy několika základních skupin jako monitorování, zabezpečení, filtrování provozu a záznam základních událostí pro práci na počítači do jednoho systému. Cílem implementovaného rozhraní není doslovná základní konfigurace systému a služeb, ale možnost administrace vybraných částí jednotlivých služeb již nakonfigurovaného systému.

Při návrhu systému byla taky brána možnost rozdělení a využití některých modulů pro více skupin uživatelů, s různým oprávněním modifikace a prohlížení.

Do návrhu systému byly rovněž zakomponovány požadavky a specifikace různých kategorií, jako např. možnost vypínání počítačů k přístupu na internet. Jedna z hodně důležitých specifikací na střední škole je, že na škole studují žáci mladiství a plnoletí. Z tohoto důvodu je nutné filtrovat provoz přístupu na internet z hlediska žádoucího a nežádoucího obsahu.

Návrh základního rozdělení systému do kategorií (skupin)

- monitorování sítě, síťového provozu a statistiky
- konfigurace zabezpečení a filtrace provozu
- záznam událostí do jednotné databáze

Rozdělení používání systému podle práv uživatele

- admin - administrátor systému s právy konfigurace a prohlížení celého systému
- uživatel - učitel s právy blokování počítačů v učebnách pro přístup na internet a prohlížení monitorování sítě, síťového provozu, statistik a včetně prohlížení událostí

Při výběru programů do systému pro jednotlivé služby, byly zohledněny tyto aspekty

- možnost využití služeb dodávaných s operačním systémem (Linux, Windows)
- použitelnost již zakoupených programů
- vyhnout se placeným verzím
- použití pouze softwarového řešení, nikoliv hardwarového

Při celkovém konečném rozhodování výběru řešení nebylo zvoleno zakoupení administrativního systému, ale snaha vyřešit zadání ve stávajících podmínkách se stávajícími možnostmi. Vzhledem k tomu, že mezi nám známými systémy jsme nenašli žádný, který by vyhovoval našim zadaným podmínkám, rozhodli jsme se implementovat vlastní konfigurační rozhraní pro správu a administraci systému.

2 Rešerše systémů pro administraci sítí

V této kapitole si postupně popíšeme srovnání obdobných systémů a jejich vyhodnocení požadovaných vlastností v tabulce podle úvodního rozdělení do jednotlivých skupin. Dále u každého popisovaného systému uvedeme bodově klady a zápory hodnoceného systému. V závěru této kapitoly uděláme celkové zhodnocení rešerše obdobných systémů.

2.1 Monitorování sítě, síťového provozu a statistiky

V této skupině budeme představovat systémy, které mají za úkol monitorování sítí, síťového provozu a zaznamenávání statistik provozu s grafickým výstupem pro jednotlivá sledování.

2.1.1 Ganglia

Je to škálovatelný distribuovaný systém, sledovací nástroj pro vysoce výkonné výpočetní systémy, jako jsou clustery a sítě. Umožňuje uživateli na dálku sledovat online události, nebo statistiku historie, jako třeba události CPU, zátěž a využití sítě, nebo využití počítačů v síti, které jsou sledovány.

Ganglia je vydáván pod BSD licencí.

Hlavní možnosti systému:
Systém je rozdělen do dvou Démonů, PHP Web Front-end a dalších utilit.

1. **Ganglia Monitoring Daemon (gmond)**, běží na každém clusteru, který chceme sledovat.
   Hlavní démon systému má následující funkce:
   - sledování změn v hostitelském uzlu
   - oznamovat příslušné změny
   - poslouchat stavy všech ostatních uzlů přes unicast nebo multicast kanál
   - odpovídat na dotazy v popisu XML daného clusteru

2. **Ganglia Meta Daemon (gmetad)**
   Tento démon má za úkol vytváření federací (stromů XML). Toho je docíleno použitím stromu point-to-point, spojení mezi uzly clusteru do reprezentativního celkového stavu více clusterů. Na každém uzlu ve stromu, probíhá periodické dotazování zdroje dat, analýza a shromažďování XML.

3. **Ganglia PHP Web Front-end**, nabízí pohled na získané informace v reálném čase prostřednictvím dynamických webových stránek. Ganglia web front-end je napsán v PHP skriptovacím jazyce a používá grafy vytvářené démonem gmetad. Zobrazuje podrobné grafy využití paměti, CPU, disky, síťové statistiky, běžící procesy a všechna ostatní sledování.[1]

Celkové hodnocení

+ systém zdarma
+ možnosti monitorování a statistik
– neobsahuje všechny skupiny požadované v systému

2.1.2 Nagios

Nagios je open source systém pro automatizované sledování stavu počítačových sítí a jimi poskytovaných služeb. Systém nabízí kompletní monitorování a upozorňování pro servery, switche, aplikace, služby a při vyskytnutí se nějakého problému možnost informovat zadanou kontaktní osobu. Monitorování koncových uzlů a služeb je prováděno periodicky pomocí externích modulů, které předávají získané hodnoty do modulu hlavního systému Nagiosu.

Nagios je vydáván pod GPL licencí.

Hlavní možnosti systému:

- monitorování nezávislé na OS
- monitorování různých typů služeb
- monitorování síťových služeb
- monitorování systémových prostředků (CPU, disk)

Nagios rovněž, jako spousta obdobných systémů, nabízí pohled na získané informace v reálném čase prostřednictvím dynamických webových stránek. Navíc ještě nabízí možnost prohlížení aktuálních hodnot a statistik historie na mobilním telefonu.[2]

Hodnocení

+ systém zdarma
+ možnosti monitorování a statistik
– vysoké nároky na hardware
– neobsahuje všechny skupiny požadované v systému

2.1.3 Ntop

Ntop slouží k monitorování síťového provozu, vyhodnocení využití sítě. Je založen na použití knihovny pro filtrování paketů libpcap, díky čemuž je možné provádět sledování síťového provozu na platformách Unix a taky Win32.

Ntop je vydáván pod GPL licencí.

Hlavní možnosti systému:

- řazení síťového provozu podle protokolů
- třídění síťového provozu podle kritérií
- zobrazení statistik provozu

- možnost ukládání získaných hodnot v RRD formátu
- analýza IP provozu a setřídění podle zdroje a cíle, nebo podle typu protokolu

Ntop rovněž, jako spousta obdobných systémů nabízí pohled na získané informace v reálném čase prostřednictvím webového rozhraní, které zrovna slouží jako server.[3]

Hodnocení

+ systém zdarma
+ možnosti monitorování a statistik
– využití CPU a paměti (závislost na velikosti sítě)
– omezená konfigurace a správa přes webové rozhraní
– neobsahuje všechny skupiny požadované v systému

Program (systém)	Monitorování sítě	Statistika síťového provozu	Konfigurace síťových prvků	Konfigurace zabezpečení přístupu na internet	Filtrování provozu přístupu na internet	Záznam událostí počítačů v Active Directory
Ganglia	x	x	-			
Nagios	x	x	-			
Ntop	x	x	-			
Sysadminnet	**x**	**x**	**x**	**x**	**x**	**x**

Tabulka 2.1 - výsledné srovnání monitorování sítě, síťového provozu a statistiky

2.2 Konfigurace zabezpečení a filtrace provozu

Další skupina systémů má podle zadání za úkol zabezpečení a filtrování provozu sítě.

2.2.1 Webmin

Webmin je webové rozhranní pro administraci linuxového systému. Jako takový se skládá z jednoduchého webového serveru a ze spousty modulů, které zajišťují dané konkrétní činnosti. V libovolném internetovém prohlížeči můžete nastavovat např. firewall, Apache, DNS, sdílení souborů a mnoho dalších služeb. Díky Webminu není nutné provádět editaci konfiguračních souborů manuálně, ale umožňuje spravovat systém vzdáleně, nebo z terminálu.[4]

Webmin je vydáván pod BSD licencí.

Hlavní možnosti systému:

- monitorování propustnosti sítě
- firewall Linuxu

moduly třetích stran

- filtrování provozu (DansGuardian 0.7.1)
- statistika síťového provozu (MRTG 0.2p3)
- monitorování sítě, síťového provozu a statistiky (Nagios Configuration 2.0)

Hodnocení

+ systém zdarma
+ možnosti použití různých modulů
– neobsahuje všechny skupiny požadované v systému

2.2.2 Shorewall

Shorewall je nástroj sloužící k zabezpečení sítě konfigurací netfilteru. Pomocí iptables, iptables-restore a utilit, Shorewall nakonfiguruje netfilter a linuxový síťový subsystém, aby odpovídal požadavkům. Je možné jej použít jako vyhrazený firewall systému, multifunkční bránu, router, server, nebo na samostatném systému linux. Shorewall není démon, po nakonfigurování síťového subsystému se ukončí.[5]

Shorewall je vydáván pod GPL licencí.

Hlavní možnosti systému:

- vytvoření a administrace IPv4 firewallu
- vytvoření a administrace IPv6 firewallu

Možnost konfigurace je provádět editaci konfiguračních souborů jenom manuálně, nebo v grafickém rozhraní při využití předešlého systému Webmin za pomocí modulu třetích stran (Shorewall Firewall 1.580).

Hodnocení

+ systém zdarma
+ možnosti použití (iptables)
– neobsahuje všechny skupiny požadované v systému

2.2.3 SquidGuard

Slouží k filtrování a přesměrování URL provozu na základě černé listiny na proxy serveru Squid. Při nalezení shody v pravidlech pro blokování se uživateli zobrazí hlášení o zablokování

požadované stránky URL. Jako zdroje pro filtrování má možnost používání několika různých svobodných i komerčních černých listin, nebo využití možnosti vytvoření vlastní listiny.[6]

SquidGuard je vydáván pod GPL licencí.

Hlavní možnosti systému:

- blokování podle cílových ACL
- blokování podle zdrojových ACL
- blokování proti DNS černých listin
- blokování na základě regulérních výrazů
- pravidla založená na zdrojové IP adrese
- pravidla bílé listiny

Možnost konfigurace je provádět editaci konfiguračních souborů pouze manuálně, nebo využití systému Webmin za pomocí modulu třetích stran (Squid Guard 1.0).

Hodnocení

+ systém zdarma
+ možnosti použití pravidel
– neobsahuje všechny skupiny požadované v systému

Program (systém)	Monitorování sítě	Statistika síťového provozu	Konfigurace síťových prvků	Konfigurace zabezpečení přístupu na internet	Filtrování provozu přístupu na internet	Záznam událostí počítačů v Active Directory
Ganglia	x	x	-			
Nagios	x	x	-			
Ntop	x	x	-			
Webmin				x	x	
Shorewall				x	-	
SquidGuard				-	x	
Sysadminnet	**x**	**x**	**x**	**x**	**x**	**x**

Tabulka 2.2 - výsledné srovnání konfigurace zabezpečení a filtrace provozu

2.3 Záznam událostí do jednotné databáze

Poslední představená skupina má za úkol zpracovávat záznamy událostí do jednotné databáze.

2.3.1 Nagios

Nagios je open source systém pro automatizované sledování stavu počítačových sítí a jimi poskytovaných služeb. Systém nabízí kompletní monitorování systémů. Monitorování koncových uzlů a služeb je prováděno periodicky pomocí externích modulů, které předávají získané hodnoty do modulu hlavního systému Nagiosu.

Nagios je vydáván pod GPL licencí.

Hlavní možnosti systému[1]:

- monitorování operačního systému Microsoft Windows s pluginem NRPE_NT.
- monitorování systémových prostředků (logování systému)

Nagios nabízí pohled na získané informace prostřednictvím dynamických webových stránek.[2]

Hodnocení

\+ systém zdarma
\+ možnosti monitorování a statistik
– vysoké nároky na hardware
– neobsahuje všechny skupiny požadované v systému

Program (systém)	Monitorování sítě	Statistika síťového provozu	Konfigurace síťových prvků	Konfigurace zabezpečení přístupu na internet	Filtrování provozu přístupu na internet	Záznam událostí počítačů v Active Directory
Ganglia	x	x	-			
Nagios	x	x	-			
Ntop	x	x	-			
Webmin				x	x	
Shorewall				x	-	
SquidGuard				-	x	
Nagios						x
Sysadminnet	**x**	**x**	**x**	**x**	**x**	**x**

Tabulka 2.3 - výsledné srovnání záznam událostí do jednotné databáze

[1] Výpis možností daného systému jenom pro záznam událostí.

2.4 Celkové zhodnocení rešerše systémů pro administraci sítí

V této oblasti si popíšeme srovnání představených systémů v předešlých podkapitolách s námi vytvořeným administrativním systémem. Prvně si rovněž v krátkosti představíme zastoupení našeho navrženého systému v jednotlivých skupinách.

2.4.1 Sysadminnet

Sysadminnet je zkratka našeho vytvořeného systému.

Monitorování sítě, síťového provozu a statistiky

- SNMP - součástí instalace distribuce CentOS (BSD licence). Široce používaný protokol pro sledování zařízení sítě (např. směrovačů), serverů, počítačových čidel, tiskáren, přístupových bodů. NET-SNMP projekt obsahuje nástroje pro předkládání žádostí a informací ze SNMP agentů, které používají k provedení dotazy verze SNMP v1, SNMP v2c a SNMP v3 pomocí protokolu IPv4, ale i IPv6.[7]
- MRTG - součástí instalace distribuce CentOS (GPL licence). Sleduje na základě SNMP síťová zařízení a generuje grafy, které ukazují, jak velký provoz prošel každým rozhraním. MRTG je napsán v Perlu a pracuje na Unix/Linux systémech, stejně jako ve Windows a dokonce i na systémech NetWare.[8]

Konfigurace zabezpečení a filtrace provozu

- Iptables - paketový firewall součástí instalace distribuce CentOS (GPL licence). Nástroj iptables slouží k ovládání filtrování paketů v jádře Linuxu.[9]
- Dansguardian - nástroj pro filtrování nežádoucího webového obsahu (Open Source). Filtrování obsahu není založeno pouze na seznamu nevhodných URL, ale využívá např. filtrování obrázků a porovnávání frází. DansGuardian lze zcela přizpůsobit. Umožňuje plnou kontrolu nad tím, co má být filtrováno.[10]
- FreeRadius - součástí instalace distribuce CentOS (GPLv2+ and LGPLv2+). RADIUS umožňuje autentizaci a autorizaci pro sítě, centralizovat a minimalizovat množství re-konfiguraci, které se provádí při přidávání nebo odstraňování uživatelů.[11]

Záznam událostí do jednotné databáze

- kombinace služeb a utilit systémů Windows a Linux. Správa zásad skupiny W2008 R2, VBScript, Perl

2.4.2 Závěr srovnání a hodnocení

Pokud se podíváme na tabulku 2.4 je vidět, že pro porovnání systémů jsme vybrali šest hodnocených bodů. Postupně tedy všechny vyhodnotíme.

1. **Monitorování sítě**
   U tohoto kritéria byly srovnávány tři systémy Ganglia, Nagios, Ntop. Všechny vyhověly naším požadavkům z hlediska konkrétního zadání, ale bohužel v celkovém hodnocení nesplňují všechny požadavky.
2. **Statistika síťového provozu**
   V tomto zadání byly rovněž srovnávány tři předchozí systémy Ganglia, Nagios, Ntop. Rovněž jako v předchozím hodnocení vyhověly našim požadavkům konkrétního zadání, ale jako v předešlém celkovém hodnocení nesplňují všechny požadavky.
3. **Konfigurace síťových prvků**
   U tohoto zadání nebyl hodnocen žádný systém, problém byl v tom, že většina softwaru podporuje systém Windows, který je v tomto případě pro nás nepoužitelný, nebo je software placený, což bylo hned v úvodu jedním z kriterií vyřazeno.
4. **Konfigurace zabezpečení přístupu na internet**
   V tomto dalším zadání byly srovnávány dva systémy Webmin a Shorewall. Oba vyhověly našemu požadavku tohoto zadání. Ovšem z hlediska hodnocení celku opět nesplňují všechna kritéria.
5. **Filtrování provozu přístupu na internet**
   Tady byly rovněž srovnávány dva systémy, Webmin z předchozího srovnání a nově SquidGuard. Oba systémy opět vyhověly konkrétnímu zadání, ale opakovaně nesplňují podmínky celkového zadání.
6. **Záznam událostí počítačů v Active Directory**
   U tohoto kritéria byl hodnocen pouze jeden systém Nagios. Vyhověl zadanému kritériu, ale rovněž nesplňuje podmínky celkového hodnocení.

Závěr

Celkově jsme srovnávali sedm obdobných systémů, bohužel žádný systém nesplnil naši myšlenku sjednocení požadovaných kritérií do jednotného administrativního rozhraní. Nejblíže našemu požadavku je systém Webmin, i když podle celkového hodnocení tabulka 2.4 to tak nevypadá. Tuto pozici si zasloužil svou rozšiřitelností, kdy za podpory modulů třetích stran je schopen ovládat i některé zde uvedené systémy (Nagios) a námi zvolené projekty Dansguardian a MRTG, čímž by celkově splnil čtyři kriteria. Druhý v pořadí, stojí za zmínku právě výše uvedený systém Nagios, který v celkovém hodnocení vyhověl jako jediný třem požadavkům.

Program (systém)	Monitorování sítě	Statistika síťového provozu	Konfigurace síťových prvků	Konfigurace zabezpečení přístupu na internet	Filtrování provozu přístupu na internet	Záznam událostí počítačů v Active Directory
Ganglia	x	x	-	-	-	-
Nagios	x	x	-	-	-	-
Ntop	x	x	-	-	-	-
Webmin	-	-	-	x	x	-
Shorewall	-	-	-	x	-	-
SquidGuard	-	-	-	-	x	-
Nagios	o	o	-	-	-	x
Sysadminnet	**x**	**x**	**x**	**x**	**x**	**x**

legenda: (x) vyhověl, (-) nevyhověl, (o) opakovaně vyhověl

Tabulka 2.4 - celkové zhodnocení rešerše systémů pro administraci sítí

3 Konfigurační rozhraní navrhovaného systému

V této kapitole je popsáno navržené konfigurační rozhraní pro správu a administraci systému.

Navrhovaný systém sjednocuje správu několika základních skupin, jako je monitorování, zabezpečení, filtrování provozu a záznam událostí do jednoho konfiguračního rozhraní. Zde popsané skupiny a jejich zastoupení nalezneme v těchto kapitolách:

- **Monitorování sítě, síťového provozu a statistiky**
  - Monitorování sítě (SNMP)
  - Síťový provoz (MRTG)
- **Konfigurace zabezpečení a filtrování provozu**
  - Učebny internet (iptables)
  - Filtrování obsahu (DansGuardian)
  - Připojení WIFI
- **Záznam událostí do jednotné databáze**
  - Statistika událostí

3.1 Popis navrženého systému a jeho požadavky

Konfigurace serveru, na kterém je navržený systém implementován:

HW: HP ProLiant ML350G6 - 2x Intel Xeon 2,4GHz , 12GB (DDR3), 3x300GB SAS RAID5
OS: Linux CentOS 5.6 (x86_64)[16]

Samotný navržený systém je vytvořen ve skriptovacím jazyce PHP za využití objektového programování, kaskádových stylů a validace dat pomocí javascriptu. Ukládání dat je realizováno v databázi MySQL za využití transakcí a vázaných proměnných pomocí knihovny PDO[13], která je součásti PHP[12]. Komunikace se systémem je možná jedině pomocí zabezpečeného spojení SSL na portu 443, jakýmkoliv moderním internetovým prohlížečem. Při přihlašování do systému se využívá autentizace vůči Active Directory Windows serveru 2008. Pro každé sezení se vytváří relace (session) pro jednoznačnou identifikaci a možnost využívání session proměnných. Uživatelské rozhraní je zobrazeno v příloze A.

Pro plnou funkčnost vyžaduje systém administrace na serveru tyto služby:

- webový server Apache (SSL, mod rewrite)
- PHP min verze 5.2
- MySQL (transakce, vázané proměnné)
- FreeRadius (autentizace uživatele, autorizace MAC adresy)
- Perl (pomocné skripty)
- iptables (paketový firewall, přístup na internet vytvoření řetězce UCEBNYX)
- SNMP (dotazy na agenty)

- DansGuardian (filtrování provozu internetu)
- MRTG (statistika síťového provozu)
- crontab (časové spouštění skriptu)
- sudo (omezené spouštění skriptů pod uživatelem root)
- sendmail (poštovní server)

Adresářová struktura navrženého systému:

- /class - třídy systému
- /css - kaskádové styly
- /functions - jednotlivé moduly funkcí
- /images - obrázky, generované grafy síťového provozu
- /js - javascript
- /logpc - adresáře a soubory záznamů událostí
- /savefile - generované soubory pro konfiguraci systému
- /scripts - skripty pro jednotlivé moduly

Navržená struktura systému je rozdělena do jednotlivých modulů. Každý modul obsahuje funkce, které pomocí vytvořených objektů pracují s metodami daných tříd.

Přístupné moduly v systému na základě práva uživatele:

Skupina Administrátor

- Učebny internet
- Filtrování obsahu
- Připojení WIFI
- Monitorování sítě
- Síťový provoz
- Statistika událostí
- Systém - číselníky

Skupina Uživatel

- Učebny internet
- Monitorování sítě
- Síťový provoz
- Statistika událostí

Tato skupina nemá práva žádného přidávání záznamů ani jejich modifikaci. Tato oblast je jim skryta, nebo daný prvek není aktivní.

Oproti základnímu rozdělení systému v úvodu do tří kategorií nám tady u skupiny administrátor přibývá další kategorie a tou je konfigurace systému (Systém - číselníky).

4 Monitorování sítě, síťového provozu a statistiky

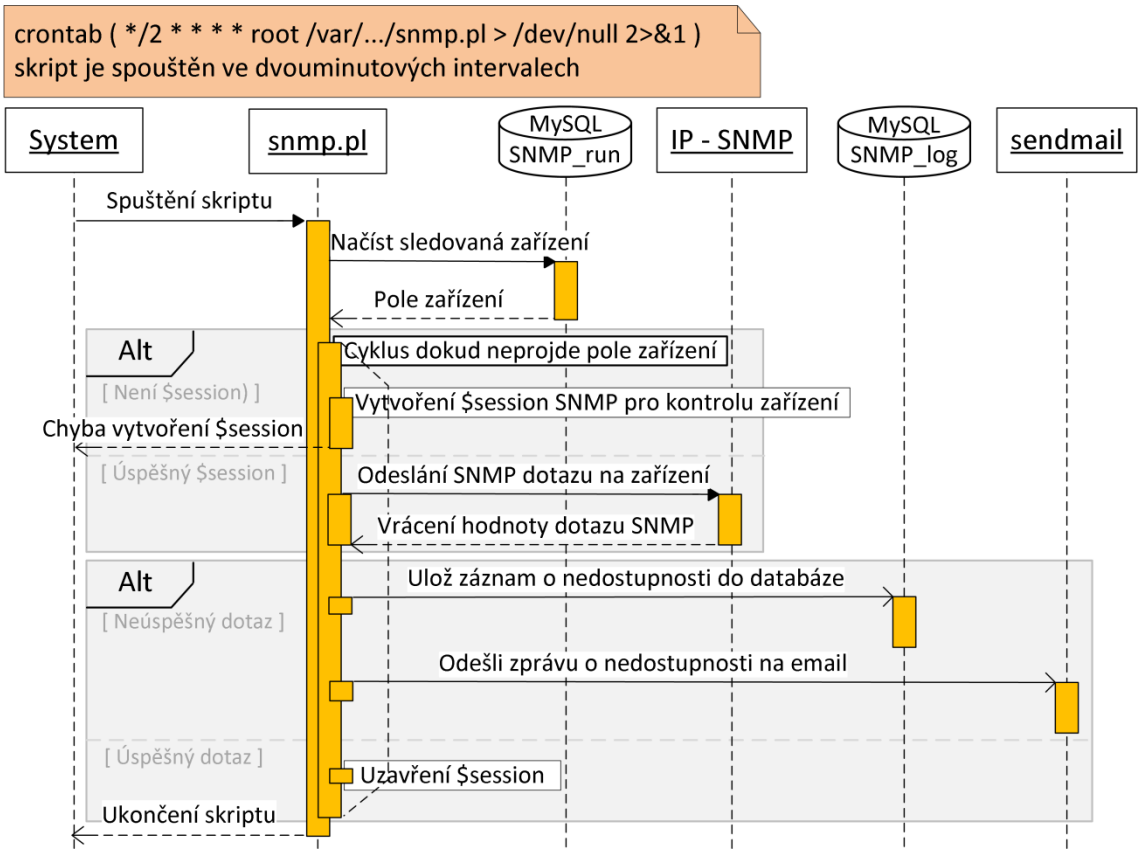
Tato kapitola popisuje dva moduly „monitorování sítě (SNMP)“ a „síťový provoz (MRTG)“.

4.1 Monitorování sítě (SNMP)

Tento modul má za úkol pravidelné monitorování evidovaných zařízení označených online provozem v časovém intervalu. Zaznamenávání logů při výpadcích zařízení do databáze a odesílání upozornění na email správce. S tím souvisí evidence monitorovaných zařízení a jejich modifikace, kontrola stavu zařízení, konfigurace zařízení a modifikace zařízení.

Princip funkce modulu

Monitorování online zařízení je prováděno pravidelným spouštěním perlového skriptu načasovaného v intervalu dvou minut pomocí systémové služby crontab obrázek 4.1. Perlový skript „snmp.pl“[15] načte z databáze záznamy a zasíláním SNMP dotazu[14] zjišťuje dostupnost zařízení. Pokud není zařízení dostupné, uloží informaci do databáze a odešle na kontaktní email uložený u zařízení varovnou zprávu.



Obrázek 4.1 - sekvenční diagram SNMP dotazů na monitorovaná zařízení (snmp.pl)

Popis uživatelského rozhraní modulu

Modul monitorování sítě Obrázek A.6 je rozdělen do tří základních oblastí. První popisovanou oblastí bude „správa uložených zařízení“, i když při spuštění se zobrazuje oblast „přehled a konfigurace zařízení“ a s touto oblastí v základu spojená poslední „výpis přehledu událostí nedostupných zařízení“.

4.1.1 Správa uložených zařízení

V této oblasti modulu je zajištěna správa nových záznamů zařízení pro sledování stavu, konfigurování a jejich případnou modifikaci. V úvodu spuštění se nám zobrazí tabulka s uloženými záznamy pro jednotlivá zařízení obrázek 4.2. V tabulce se zobrazují jen základní údaje k upřesnění identifikace zařízení. Tato oblast je přístupná pouze uživateli s právy administrátora.

Popis hlavičky tabulky:

- **Mon** - A (modrá barva), zařízení je monitorováno v pravidelných intervalech. N (bílá barva), není monitorováno, může být vypnuto například učebna.
- **Název, lokalita -** název zařízení, nebo upřesněná lokalita
- **IP adresa** - IP adresa zařízení, na kterou se odesílá dotaz SNMP
- **Kategorie -** Určení vybraných zařízení do skupin s možností zobrazení stavu všech, které jsou ve stejné kategorii obrázek 4.4
- **Email -** emailová adresa správce, kterému se odesílá zpráva o nedostupnosti zařízení, které má být v provozu a není.
- **Edit -** modifikace vybraného zařízení
- **Del -** Smazání vybraného zařízení

Zvolte pro záznam nového zařízení - Nový záznam

<< < Počet řádků k zobrazení 20 Zadat Záznamy 1 - 20 (34) > >>

Mon	Název, lokalita	IP adresa	Kategorie	Email	Edit	Del
A	Server switch no. 250	192.168.0.250	Server rack	popovsky@spsbv.cz	Edit	Del
A	Server switch no. 251	192.168.0.251	Server rack	popovsky@spsbv.cz	Edit	Del
N	Server switch no. 252	192.168.0.252	Server rack	zavodny@spsbv.cz	Edit	Del
A	Server 2008(Server)	192.168.0.2	Server windows	popovsky@spsbv.cz	Edit	Del
A	Server 2008(ProgServer)	192.168.0.3	Server windows	popovsky@spsbv.cz	Edit	Del

Obrázek 4.2 - přehled uložených zařízení (SNMP)[2]

Záznamy v tabulce můžeme procházet podle zadaných počtu řádků k zobrazení šipkami vlevo a vpravo. Pro upřesnění vidíme, které záznamy máme zobrazeny a celkový počet záznamů.

[2] Tabulka na obrázku nezobrazuje skutečný stav, ale přehled možností nastavení zařízení.

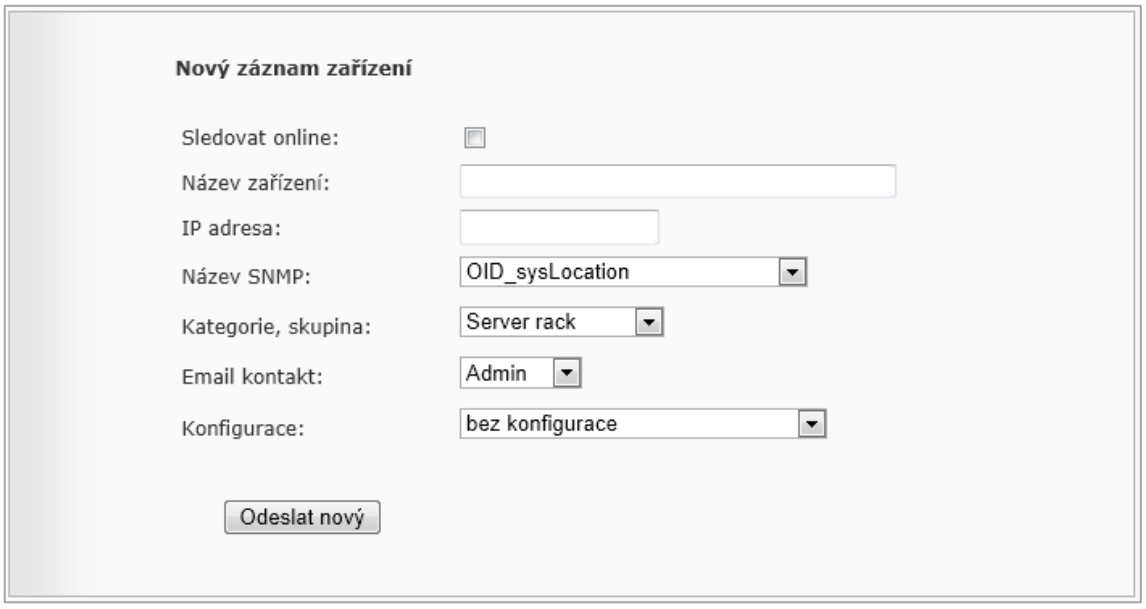
Poslední objekt zobrazený v této oblasti, ale nejdůležitější je tlačítko zvolení vytvoření záznamu nového zařízení. Po výběru tlačítka „Nový záznam“ se nám zobrazí formulář obrázek 4.3 pro zadání hodnot pro nové zařízení.

Popis zadávaných hodnot nového zařízení:

- **Sledovat online** - zvolení výběru pro nepřetržitý provoz zařízení, monitorování stavu v pravidelných intervalech
- **Název zařízení -** název upřesňující funkci zařízení, nebo lokalitu
- **IP adresa -** IP adresa zařízení, na kterou se odesílá dotaz vybraný níže „Název SNMP“

Zbývající část hodnot je vybírána na základě naplněných číselníků

- **Název SNMP -** výběr SNMP dotazu, který se odesílá na zařízení, prezentované ve výběru názvem z MIB databáze
- **Kategorie, skupina** - výběr kategorie podle společných vlastností zařízení, do které bude zařazeno a v které bude zobrazen stav všech zařízení ve stejné kategorii
- **Email kontakt -** výběr komu se má odeslat zpráva o nedostupnosti zařízení
- **Konfigurace** - zvolení výběru, jestli je zařízení konfigurovatelné (bez konfigurace, konfigurace bez MAC, konfigurace s MAC - HP ProCurve)



Obrázek 4.3 - vložení nového zařízení (SNMP)

Průběh modifikace je stejný jako nový záznam. Rozdíl je pouze v tom že pro výběr modifikace zvolíme tlačítko „Edit“ obrázek 4.2 u záznamu, který chceme modifikovat. Pokud chceme konkrétní záznam odstranit, zvolíme výběr tlačítka „Del“ a po potvrzení dotazu o smazání dojde k odstranění vybraného záznamu.

4.1.2 Stav a konfigurace zařízení

V této oblasti modulu můžeme sledovat stav jednotlivých zařízení podle výběru kategorie. Po zvolení kategorie se zobrazí tabulka zařízení a stav, ve kterém se nachází obrázek 4.4. Při zjišťování stavu každého zařízení jsou pro dotazování použity IP adresa a OID (Název SNMP) načtené z databáze. Po zpracování všech zařízení ve skupině se výsledky zobrazí do tabulky.

Popis hodnot v tabulce:

- **Stav** - zelená barva znamená, že zařízení je v provozu, červená - zařízení je mimo provoz
- **Název, lokalita** - název zařízení, nebo lokality, údaj je načten z uložené hodnoty v databázi
- **Detail -** zobrazení detailu je závislé od zadané položky „Konfigurace“ u záznamu zařízení v databázi

Vysvětlení detailu podle zadání konfigurace:

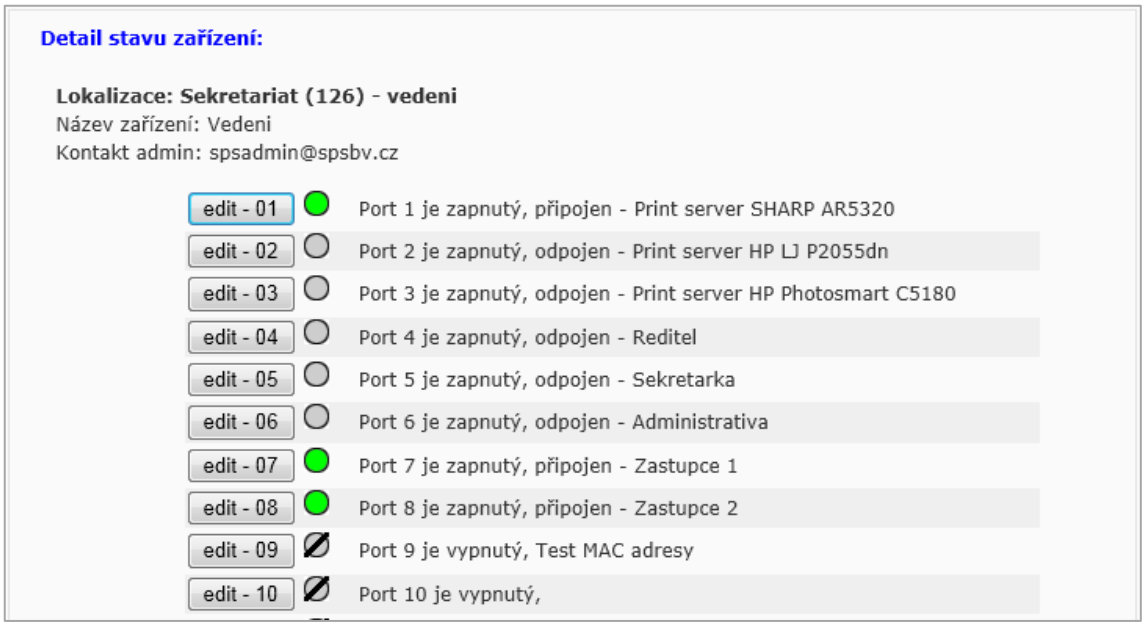
a) **bez konfigurace** – není k dispozici
b) **konfigurace bez MAC, konfigurace s MAC - HP ProCurve** - tlačítko detail-config

Pokud není zařízení dostupné a má zadanou variantu jakékoliv konfigurace, zobrazí se tlačítko detail-config neaktivní a nelze zvolit jeho výběr.

Obrázek 4.4 - přehled provozu zařízení v zadané skupině (SNMP)[3]

Pokud se jedná o zařízení konfigurovatelné, v našem případě to jsou aktivní síťové prvky (switch), máme možnost po zvolení tlačítka detail-config zobrazení informací systému a u každého portu vidět stav, jestli je zapnutý nebo vypnutý. Pokud je zapnutý a připojené zařízení k portu je aktivní, zobrazuje stav připojení „připojen“, nebo v opačném případě „odpojen“. Volitelnou hodnotou, pokud je zadána, zobrazuje v detailu název aliasu zadaného portu. Alias se zadává pro bližší určení připojeného zařízení na daný port obrázek 4.5. Všechny tyto informace získáme přímo dotazem SNMP z konkrétního zařízení předáním jeho IP adresy a jednotlivých MIB dotazů na základě zadaných OID řetězců.

[3] Tabulka na obrázku nezobrazuje skutečný stav, ale simuluje stav možností.



Obrázek 4.5 - detailní přehled stavu vybraného zařízení (SNMP)

Pokud potřebujeme změnit konfiguraci vybraného portu, klikneme na tlačítko Edit - vybrané číslo portu. Po zvolení výběru se zobrazí formulář, ve kterém můžeme změnit informační hodnoty systému zařízení a v druhé části konfiguraci zvoleného portu obrázek 4.6.

Popis informací systému:

- **Název zařízení** – jakýkoliv smysluplný název určující konkrétní zařízení
- **Lokalizace** – fyzické umístění např. místnost
- **Kontakt admin** – většinou kontaktní email na správce sítě

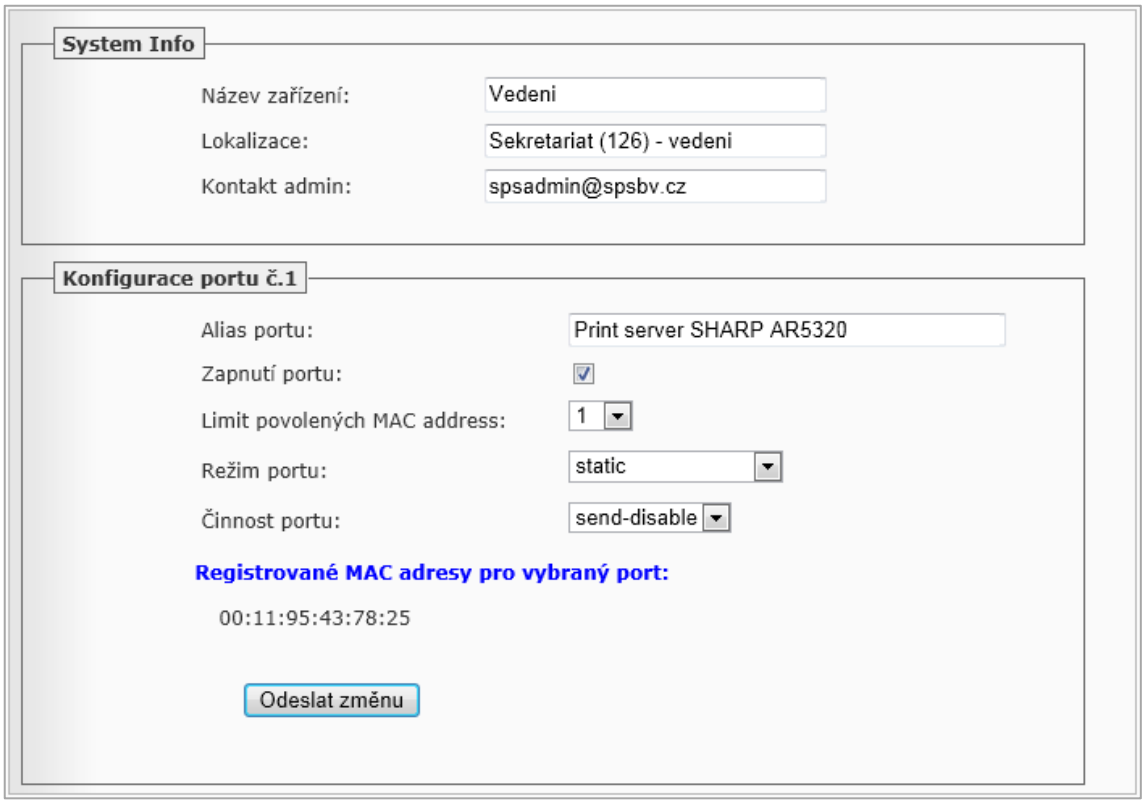
Popis konfigurace portu:

- **Alias portu** – zadává se název zařízení, které je připojené k danému portu
- **Zapnutí portu** – výběr fyzického zapnutí, nebo vypnutí portu

Další část je aktivní jen při nastavené konfiguraci zařízení na „konfigurace s MAC - HP ProCurve“. Tento typ konfigurace nám umožňuje zapnout kontrolu na portu připojeného zařízení na základě MAC adresy.

- **Limit povolených MAC adres** - určuje maximální počet zaregistrovaných MAC adres na daném portu; max. limit je 38, my máme zadaných 10
- **Režim portu –** nepřetržitý; statický; nakonfigurovaný; naučit přístup na port; naučit omezením nepřetržitého
- **Činnost portu –** žádná, odeslat zprávu; odeslat zprávu a zakázat

Poslední položka zobrazuje MAC adresy zaregistrované na daném portu.



Obrázek 4.6 - konfigurace vybraného portu na zvoleném zařízení (SNMP)

4.1.3 Výpis přehledu událostí nedostupných zařízení

Poslední oblastí je zobrazování statistiky výskytu nedostupnosti zařízení pravidelným monitorováním, popsaným v úvodu v odstavci „Princip funkce modulu“.

Přehled výskytu událostí je načítán a zobrazován z databáze vždy v rozmezí jednoho týdne od aktuálního data zpět. Výpis v tabulce zobrazuje celkový počet výpadků v daném dni konkrétního zařízení se zobrazením data a času posledního výpadku obrázek 4.7. Mimo těchto údajů zobrazuje IP adresu k danému zařízení, jeho zařazení do kategorie a tlačítko „Výpis“.

Obrázek 4.7 - přehled a počty výskytu chyb na zařízeních online (SNMP)

Pro zobrazení všech výpadků zvoleného zařízení v daném dni stiskněte výše zmiňované tlačítko výpisu. Zobrazí se přehled obrázek 4.8, kde máme kompletní výpis všech výpadků seřazených, podle času a ve sloupci „Výpis“ zadáno číselné pořadí výpadku.

Přehled a počty výskytu chyb za období : 09.04.2012 - 15.04.2012

<< < Počet řádků k zobrazení 20 Zadat Záznamy 1 - 20 (42) > >>

suma error	Název, lokalita	IP adresa	Kategorie	Poslední výskyt chyby	Výpis
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 11:00:05	1
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 11:02:05	2
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 11:04:05	3
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 11:06:06	4
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 11:08:05	5
	Kabinety strojní lab.			15.04.2012 - 11:10:05	6
	Kabinety strojní lab.	192.168.171.242	Kabinety		39
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 12:18:06	40
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 12:20:05	41
	Kabinety strojní lab.	192.168.171.242	Kabinety	15.04.2012 - 12:22:06	42

Obrázek 4.8 - detailní výpis všech chybových stavů podle času v daném dni (SNMP)

4.2 Síťový provoz (MRTG)

Modul síťového provozu má na starosti získávat hodnoty o provozu ze síťových rozhraní a z nasbíraných dat generovat stránky HTML s grafy.

Princip funkce modulu

Pro funkčnost modelu je zapotřebí mít nainstalovaný program MRTG v systému a vytvořené konfigurační soubory pro jednotlivá síťová rozhraní. Konfigurační soubory jsou pak využity k periodickému dotazování monitorovaných síťových prvků v časovém intervalu pěti minut pomocí systémové služby crontab.

Popis uživatelského rozhraní modulu

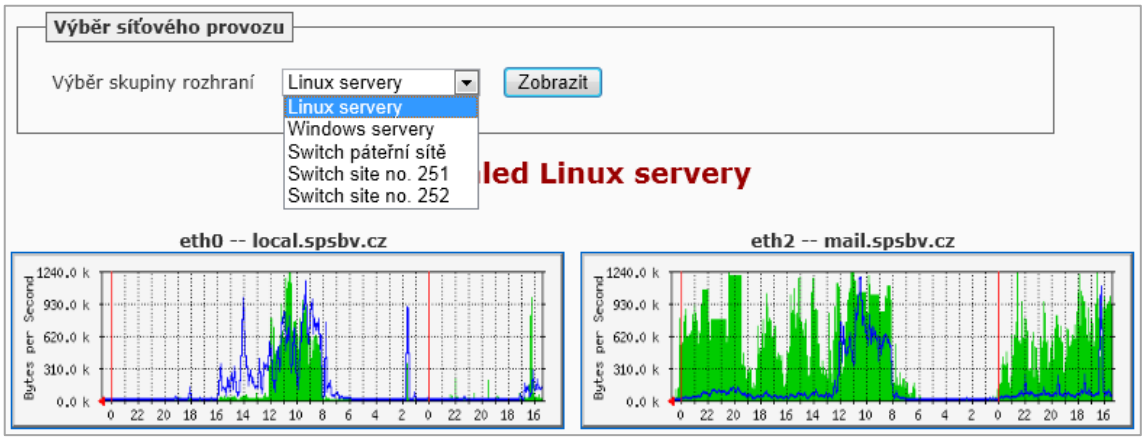
Modul síťového provozu Obrázek A.7 má na výběr zobrazení dvou skupin serveru a tří síťových prvků obrázek 4.9, tvořící základní strukturu sítě školy.

4.2.1 Popis grafu

Základní zobrazení grafu se skládá s osy x, kde je časový údaj a osy y, kde je přenos v bajtech za sekundu na aktuálním rozhraní. Podle času a hodnoty přenosu (průměr pěti minut) na ose x v daném čase vykreslí výšku grafu buď po celé délce zelenou barvou, nebo jen vrcholy hodnot modře. Modrý graf zobrazuje hodnoty odeslaných dat na rozhraní směrem ven (TX) a zelený graf zobrazuje hodnoty přijatých dat směrem dovnitř (RX).

Jaké grafy se nám generují:

- denní (5 minutový průměr)
- týdenní (30 minutový průměr)
- měsíční (2 denní průměr)
- roční (1 denní průměr)



Obrázek 4.9 - přehled výběru a ukázka síťového provozu (MRTG)

Zobrazení požadovaného síťového provozu, zvolíme z nabídky výběru skupin rozhraní. Pro zobrazení všech generovaných grafů klikneme na zobrazený výběr konkrétního rozhraní a tím se nám zobrazí přehled všech již dříve zmiňovaných grafů. V přehledu všech grafů se nám navíc zobrazují kromě systémových údajů rozhraní hodnoty maximálního, průměrného a aktuálního přenosu dat na vstupu i výstupu s datem a časem poslední aktualizace.

4.2.2 Přehled rozhraní ve skupinách

Výběr skupiny rozhraní může v generovaných grafech obsahovat zastoupení rozhraní několika serverů. Například vytvoření skupin podle operačního systému.

Příklad zastoupení OS Linux:

1. **server mail**
   1.1. eth0 -- local.spsbv.cz
   1.2. eth1 -- internat.spsbv.cz
   1.3. eth2 -- mail.spsbv.cz
   1.4. eth3 -- wifi.spsbv.cz
   1.5. tun0 -- vpn.spsbv.cz
   1.6. tap0 -- vpn-tunel.spsbv.cz
2. **server intranet**
   2.1. eth0 -- intra.spsbv.cz
   2.2. eth1 -- ftp.spsbv.cz
3. **server moodle**
   3.1. eth0 -- zaskolou.spsbv.cz
4. **server isas**
   4.1. eth0 -- sas.spsbv.cz

5 Konfigurace zabezpečení a filtrování provozu

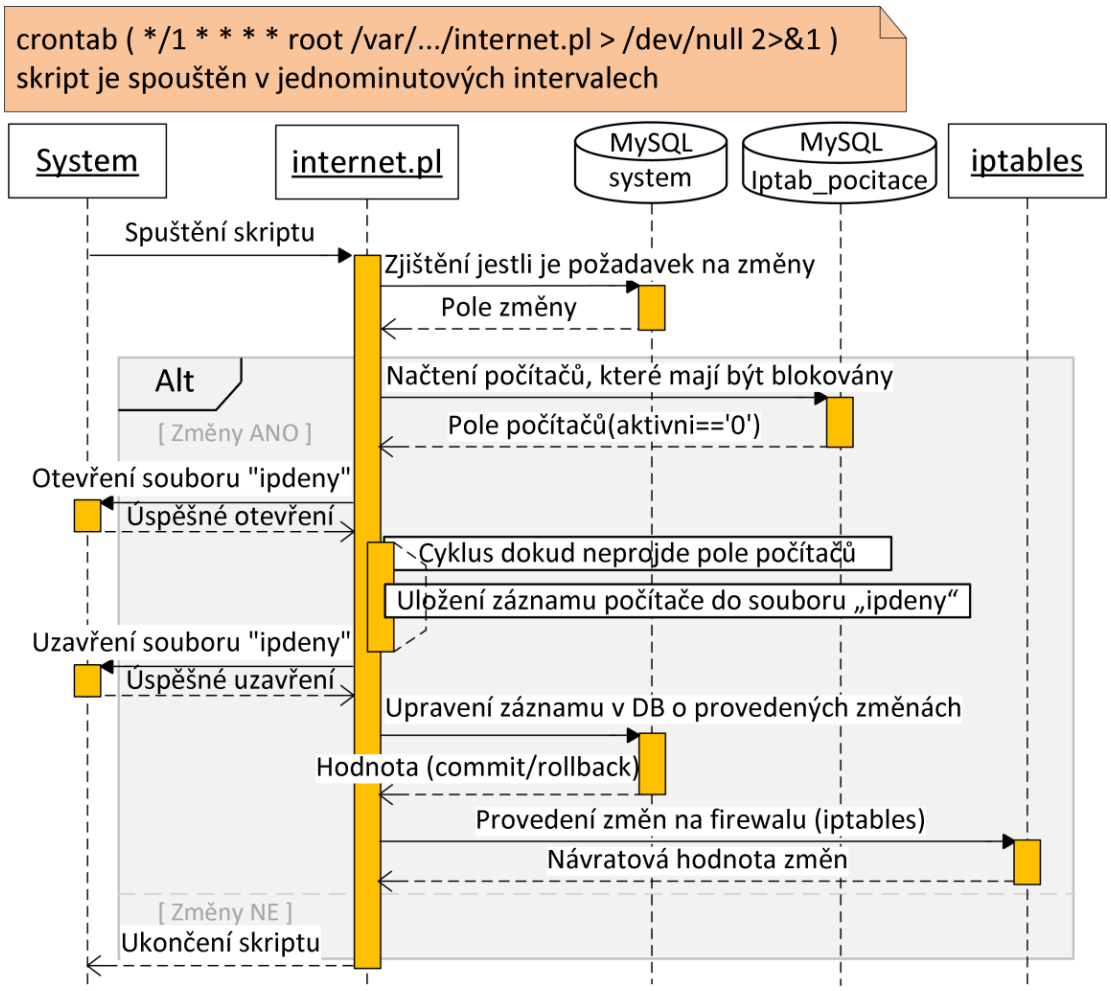
V další kapitole popisujeme moduly „učebny internet (iptables)“, „filtrování obsahu (DansGuardian)“ a „připojení Wi-Fi“.

5.1 Učebny internet (iptables)

Modul učebny internet má za úkol povolení nebo zakázaní přístupu počítačů v učebnách na internet. Zajišťuje správu učeben, počítačů a modifikaci záznamů. Možnosti nastavení stavu na aktivní a neaktivní pro jednotlivé počítače, nebo celou učebnu.

Princip funkce modulu

Aktivace a deaktivace provedených změn stavu počítačů je kontrolována periodickým spouštěním perlového skriptu „internet.pl“[15] v jednominutových intervalech pomocí systémové služby crontab obrázek 5.1.



Obrázek 5.1 - sekvenční diagram skriptu pro blokování počítačů (internet.pl)

Pokud skript zjistí v databázi, tabulce system změnu pro atribut iptables na hodnotu jedna obrázek 7.2, projde postupně všechny záznamy počítačů. U blokovaných načte jejich IP adresu a uloží pro každý počítač záznam do souboru ipdeny podle příkladu 5.1, kde $IP = IP adresa.

Příklad 5.1

*"iptables -t nat -A UCEBNYX -i eth0 -p tcp -m tcp -s **$IP** -j DNAT --to-destination 192.168.0.1:81"*

Po uložení všech blokovaných počítačů do souboru provede skript vyprázdnění všech pravidel z řetězce UCEBNYX a poté spustí uložený soubor ipdeny pro nové naplnění pravidel do řetězce UCEBNYX. Počítače jsou tak přesměrovány na server, ze kterého se jím v prohlížeči zobrazí stránka informující o zablokování přístupu na internet.

Popis uživatelského rozhraní modulu

Společná část Obrázek A.3 je zobrazení výběru učebny a aktivace a deaktivace celé učebny. Dále je modul rozdělen na dvě části. První část slouží ke správě učeben a počítačů, tato oblast je přístupná pouze uživateli v roli administrátora. Druhá oblast je uživatelská, která slouží k aktivaci a deaktivaci přístupu jednotlivých počítačů na internet.

5.1.1 Správa učeben a počítačů

Tuto část máme rozdělenou na oblast zadávání, modifikaci záznamů učeben a počítačů a druhá oblast je přehled uložených učeben. Tabulka učebny obrázek 5.2 slouží jako číselník výběru, kam bude evidovaný počítač zařazen. V tabulce jsou mimo zadávaných hodnot učebny tlačítka Edit a Del, které slouží k modifikaci uložených záznamů a odstranění zvolené učebny.

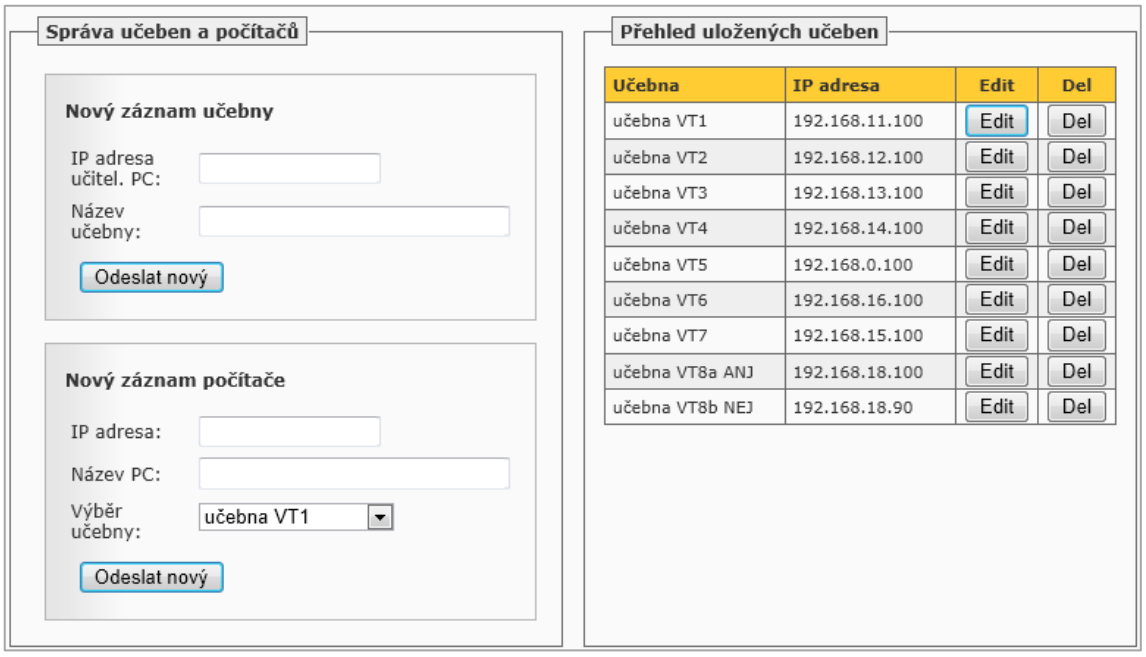
Popis zadávaných hodnot nové učebny:

- **IP adresa učitel PC** – zadání IP adresy učitelského počítače.
- **Název učebny** – zadání názvu, pod kterým budou zadané počítače identifikovány jako učebna

Popis zadávaných hodnot nového počítače:

- **IP adresa** – zadání IP adresy, kterou dostal počítač přidělenou od DHCP serveru na základě registrace jeho MAC adresy
- **Název PC** – zadání názvu počítače, aby byl naprosto jednoznačně identifikovatelný, nejlépe zadat název počítače v síti
- **Výběr učebny** – zařazení počítače do předdefinovaných učeben, které nám slouží k vytvoření skupiny zadaných počítačů

Průběh modifikace učebny nebo počítače je stejný jako nový záznam. Rozdíl je v tom, že pro výběr modifikace zvolíme tlačítko „Edit“ v příslušné tabulce zobrazení u záznamu, který chceme modifikovat. Pokud chceme konkrétní záznam odstranit, zvolíme výběr tlačítka „Del“ opět v příslušné tabulce a po potvrzení dotazu o smazání se záznam odstraní.



Obrázek 5.2 - konfigurace učeben a počítačů (iptables)

5.1.2 Aktivace a deaktivace počítačů

Oblast pro aktivaci a deaktivaci přístupu počítače do internetu je přístupná uživatelům všech rolí, pouze s tím rozdílem, že běžný uživatel nemá přístupná tlačítka pro modifikaci a mazání záznamů obrázek 5.3.

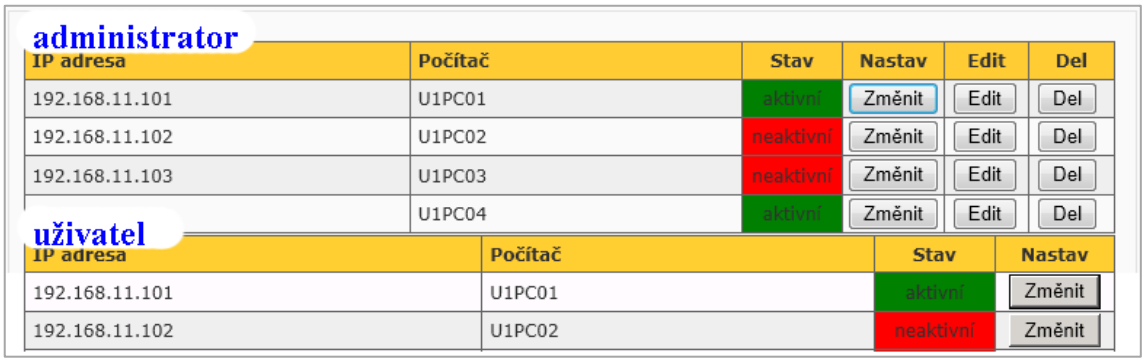
Popis hlavičky tabulky:

- **IP adresa** – IP adresa, kterou má počítač přidělenou DHCP serverem a která slouží k vytvoření blokovacího pravidla pro firewall
- **Počítač** – název počítače slouží k jednoduššímu rozpoznání konkrétního počítače
- **Stav** – určuje a barevně zobrazuje, jestli je počítač aktivní (zelená) v přístupu na internet, nebo neaktivní (červená)
- **Nastav** – tlačítko pro změnu stavu konkrétního počítače

Objekty přístupné pouze s právy administrátora

- **Edit** – modifikace zvoleného záznamu pro vybraný počítač
- **Del** – smazání konkrétního počítače

Aktivaci nebo deaktivaci přístupu na internet lze provádět buď změnou stavu konkrétního počítače, nebo zapnutím, vypnutím celé učebny. Požadované změny se projeví na základě pravidelného spouštění perlového skriptu, jehož princip je popsaný na začátku v odstavci „Princip funkce modulu“.



Obrázek 5.3 - přehled stavu počítačů v učebně, z pohledu všech uživatelů (iptables)

Možnost ověření že se požadované změny provedly, můžeme udělat zadáním příkazu výpisu pravidel pro řetězec UCEBNYX z firewallu v terminálu systému Linux obrázek 5.4.

```
[root@mail servis]# iptables -t nat -L UCEBNYX
Chain UCEBNYX (1 references)
target     prot opt source               destination
DNAT       tcp  --  192.168.11.102       anywhere            tcp to:192.168.0.1:81
DNAT       tcp  --  192.168.11.103       anywhere            tcp to:192.168.0.1:81
[root@mail servis]#
```

Obrázek 5.4 - výpis pravidel firewallu přesměrovaných počítačů (iptables)

5.2 Filtrování obsahu (DansGuardian)

Modul filtrování obsahu slouží pro konfiguraci vybraných částí nainstalovaného programu Dansguardian, který má za úkol filtrovat přístup na internet podle seznamu domén, URL, nebo podle frází obsažených v požadované stránce. Pro tento účel je možnost ukládání záznamů do jednotlivých tabulek v databázi a jejich modifikace. Tento modul je přístupný pouze uživateli s právy administrátora.

Princip funkce modulu

Aktivaci změn v tomto modulu provedeme restartováním služby „DansGuardian“ v systému.

Poznámka 5.1 Pro zajištění restartování služby musíme mít správně nakonfigurovanou aplikaci „sudo“, která nám umožňuje omezený přístup k dané službě, jako „root“ pro uživatele spouštějícího službu webového serveru. V našem případě se jedna o uživatele „apache“.

Po provedení všech zamýšlených úprav v daném modulu, vždy provedeme restartování služby. Během tohoto procesu dojde k uložení záznamů podle příslušných tabulek v databázi do určených konfiguračních souborů. Zadaná cesta k těmto souborům je součástí konfigurace programu DansGuardian. Pokud nedojde k chybě při ukládání dat do souborů, v dalším kroku se restartuje služba dansguardianu, jinak k restartu služby nedojde. Systém vrátí informaci o průběhu restartování služby a tento výpis je zobrazen v daném modulu obrázek 5.5.

Obrázek 5.5 - výběr konfiguračního souboru, restartování služby Dansguardian

Popis uživatelského rozhraní modulu

Modul filtrování obsahu Obrázek A.4 se skládá z konfigurace pěti vybraných položek, u kterých dochází nejčastěji k modifikaci.

5.2.1 Správa konfiguračních souborů

Námi vybraných pět položek pro konfiguraci, můžeme dále rozdělit do tří kategorií.

a) **základ konfigurace, rozdělení sítí, nebo počítačů do skupin**
   - **ipgroups** - přidělení IP adresy počítače, nebo rozsahu sítě do skupiny obrázek 5.7 (každá skupina má nastavené různé filtrování provozu)

b) **povolení provozu, bílá listina**
   - **exceptioniplist** - zadaná IP adresa počítače, nebo rozsah sítě je vyřazen z filtrování obsahu a má plný přístup do internetu
   - **exceptionsitelist** - zadaná doména v seznamu je zařazena na bílou listinu

c) **zakázaný provoz, černá listina**
   - **black-domains** - zadaná doména v seznamu je zařazena na černou listinu
   - **black-urls** – zadaná cesta URL v seznamu je zařazena na černou listinu

Každý konfigurační soubor má v databázi svou vlastní tabulku, kde má uložené potřebné záznamy pro zajištění správné role, kterou zastává v modulu filtrování provozu. Podle výše popsaného rozdělení kategorií můžeme udělat ještě sloučení do dvou skupin pro snazší popis hodnot ukládaných do jednotlivých tabulek v databázi. Konfigurační soubory sloučené v těchto dvou skupinách mají stejnou, nebo v základu podobnou strukturu navržené tabulky.

I. **Konfigurační soubory založené na základě IP adres, nebo rozsahu sítí obrázek 5.6**
   - **ipgroups** – Dansg_ipgroups (id,ip, poznamka, *id_filter*)
   - **exceptioniplist** – Dansg_exceptioniplist (id,ip, poznamka)

   Popis zadávaných hodnot:

   - IP – rozsah sítě, nebo IP adresa počítače
   - Poznámka – upřesnění sítě, nebo počítače k jednoduššímu určení
   - Výběr skupiny – pouze konfigurační soubor ipgroups, určuje, do jaké skupiny bude rozsah sítě nebo počítač zařazen

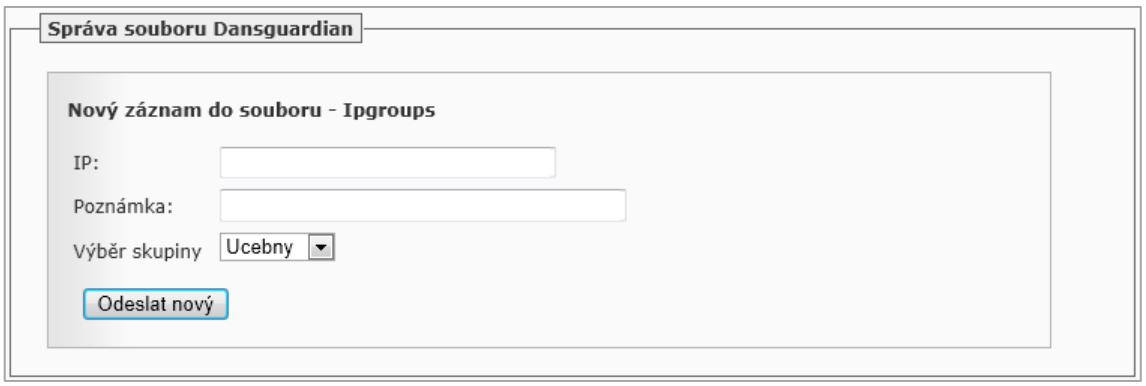
II. **Konfigurační soubory založené na názvu domény, nebo URL**

- **exceptionsitelist** – Dansg_exceptionsitelist (id,domain, poznamka)
- **black-domains** – Dansg_blackdomains (id,domain, poznamka)
- **black-urls** – Dansg_blackurls (id,url, poznamka)

Popis zadávaných hodnot:

- Domain / URL – zadání řetězce domény, nebo URL adresy
- Poznámka – možnost zadání, pokud potřebujeme upřesnit Domain / URL

Před zamýšlenou operací je potřeba zvolit, se kterým konfiguračním souborem obrázek 5.5, chceme pracovat a pak již jenom vykonat zamyšlenou operaci. Pro nový záznam i modifikaci je popis konfiguračních souborů totožný. Obrázek 5.6 je ukázka formuláře pro konfigurační soubor ipgroups. Pro ostatní konfigurační soubory vypadá formulář podobně s tím, že obsahuje popisované hodnoty v přehledu konfiguračních souborů.



Obrázek 5.6 - jeden z panelů (ipgroups) konfiguračních souborů (DansGuardian)

Při zvolení konfiguračního souboru obrázek 5.5 se nám současně zobrazí tabulka uložených záznamů pro vybraný konfigurační soubor.

Obrázek 5.7 - výpis a konfigurace souboru ipgroups (DansGuardian)

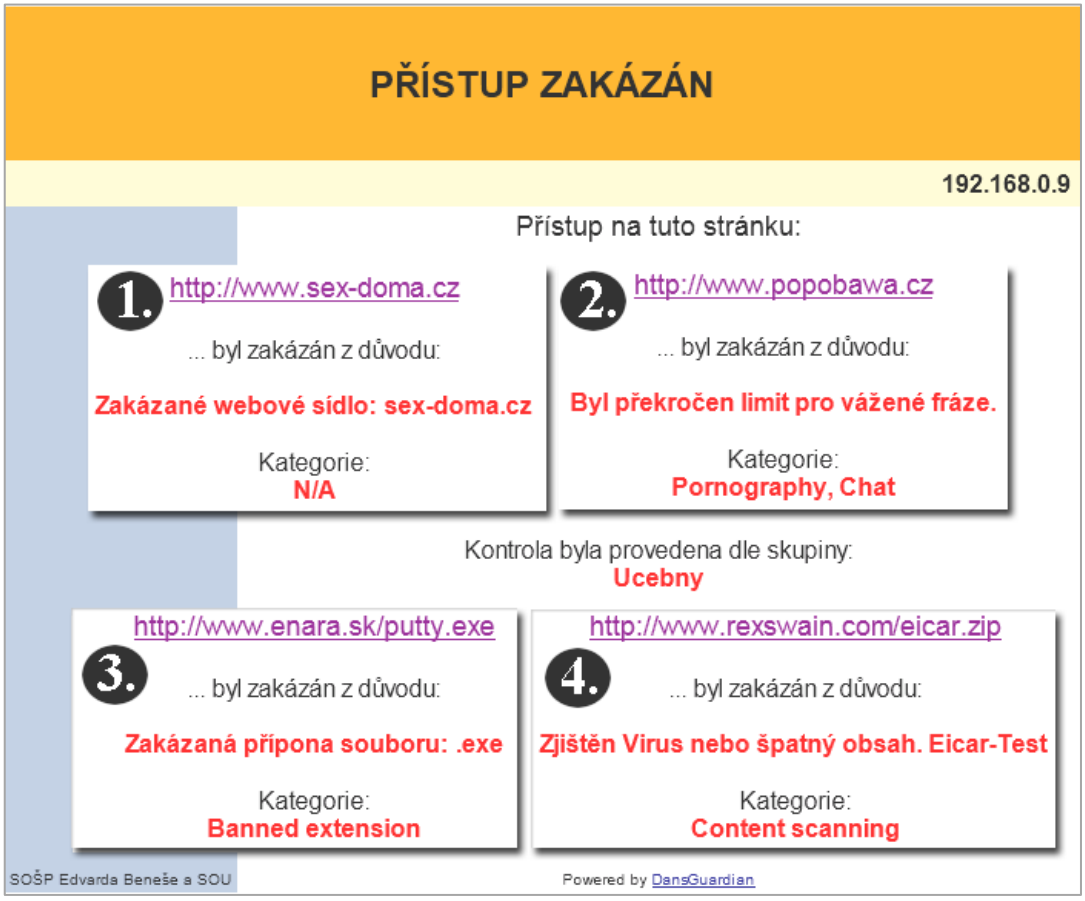
Hodnoty zobrazené v tabulce jsou srovnatelné s popisem jednotlivých konfiguračních souborů pro ukládání, nebo modifikaci záznamu. Tabulka rovněž obsahuje ke každému záznamu tlačítko pro modifikaci a mazání zvoleného záznamu.

5.2.2 Blokování provozu

Blokování filtrovaného provozu je realizováno nejen na základě našich konfiguračních souborů. Obrázek 5.8 ukazuje možnosti blokování a zobrazení se stránky v prohlížeči uživatele, kterému byl přístup na stránku zakázán.

Popis jednotlivých blokování:

1. Tato varianta blokování je přímo ovlivněna naší konfigurací (bílých a černých listin).
2. Zablokování na základě nalezených frází v dokumentu, postupně sčítá body za každou frázi a po překročení zvoleného maxima stránku zablokuje. Každá skupina má jiné maximum. Nastavení není potřeba často modifikovat.
3. Filtrování na základě přípony souboru, každá skupina má povolené jiné možnosti stahování souborů. Nastavení není potřeba často modifikovat.
4. Kontrola obsahu stánek antivirovým programem ClamAV.



Obrázek 5.8 - přehled blokování filtrování provozu DansGuardianu

5.3 Připojení Wi-Fi

Modul připojení Wi-Fi (jiný rozsah sítě) zajišťuje povolení přístupu do interní sítě školy na základě autorizace MAC adresy pře RADIUS server. Z hlediska zabezpečení, samotné povolení přístupu do sítě neumožňuje přístup na servery a ke sdíleným složkám. Rovněž zajišťuje pro daný modul evidenci a modifikaci záznamů v jednotné databázi. Tento modul je přístupný pouze uživateli s právy administrátora.

Princip funkce modulu

Aktivaci nového záznamu MAC adresy, nebo deaktivaci provedeme restartováním služby FreeRadius serveru v systému.

Pro úspěšné restartování služby musí být splněny stejné podmínky jako u modulu „Filtrování obsahu“ poznámka 5.1.

Po uložení nebo modifikaci záznamu musíme vždy restartovat službu FreeRadius serveru. Během restartování uvedené služby se načtou jednotlivé záznamy z databáze a uloží pro každou MAC adresu záznam do souboru users.mac podle příkladu 5.2.

Příklad 5.2

„ ***$MACAdresa*** *Auth-Type := Accept, User-Password == "xxx-xxxxxxxx" “*

Uložený soubor je pomocí příkazu „$INCLUDE users.mac“ přidán do konfiguračního souboru users. Pokud nedojde k chybě při ukládání dat do souboru, restartuje se služba a systém vrátí zprávu o jejím průběhu obrázek 5.9, v opačném případě vypíše chybu uložení dat do souboru a k restartování služby nedojde.

Popis uživatelského rozhraní modulu

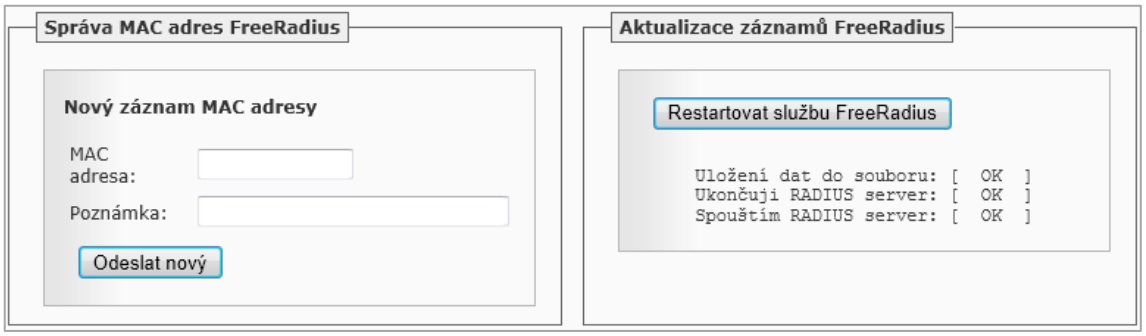
Modul připojení Wi-Fi Obrázek A.5 je nejjednodušší model v našem navrženém systému. Při spuštění se zobrazí formulář pro přidávání a modifikaci záznamu MAC adres. Vedle něj možnost restartování služby FreeRadius a ve spodní části tabulka vypisující uložené záznamy.

5.3.1 Správa MAC adres

V této části je zajištěno ukládání MAC adres, jejich modifikace a restartování služby FreeRadius obrázek 5.9.

Popis zadávaných hodnot:

- MAC adresa – zadání MAC adresy počítače, nebo zařízení, které není schopno pro vstup do sítě použít ověření přihlašovacím jménem a heslem například kopírka
- Poznámka – upřesnění evidovaného zařízení pro identifikaci majitele, lokalizace



Obrázek 5.9 - konfigurace připojení Wi-Fi, restartování služby FreeRadius

Modifikace a mazání záznamů je vybíráno pro konkrétní záznam pomocí tlačítek Edit a Del v tabulce zobrazení evidovaných MAC adres obrázek 5.10. Pro modifikaci záznamu je popis zadávaných hodnot stejný jako u nového záznamu. Před smazáním záznamu se musí zadat potvrzení souhlasu.

Výpis hodnot záznamů v tabulce evidovaných MAC adres rovněž odpovídá popisu zadávaných hodnot u nového záznamu.

Obrázek 5.10 - výpis záznamů pro konfiguraci souboru users.mac (Wi-Fi)

6 Záznam událostí do jednotné databáze

Předposlední kapitola popisuje modul „statistika událostí“ počítačů registrovaných v Active Directory u nás minimálně používaného systému Microsoft Windows XP SP3 a vyšší.

6.1 Statistika událostí

Modul statistika událostí umožňuje prohlížení a vyhledávání jednotlivých záznamů uložených v tabulkách jednotné databáze. Má za úkol získané záznamy pouze ukládat do tabulek, nemůže je modifikovat. Tento modul je přístupný všem uživatelům.

Princip funkce modulu

Před samotným zpracováním a uložením dat v tomto modulu je zapotřebí zajistit několik dalších kroků k úspěšnému cíli.

a) Získání námi požadovaných záznamů událostí na jednotlivých počítačích zařazených v Active Directory školy spuštěním VBScriptů na jednotlivých počítačích pomocí distribuce systémové politiky na jednotlivé počítače v nastavení správy zásad skupin Windows serveru 2008 R2.

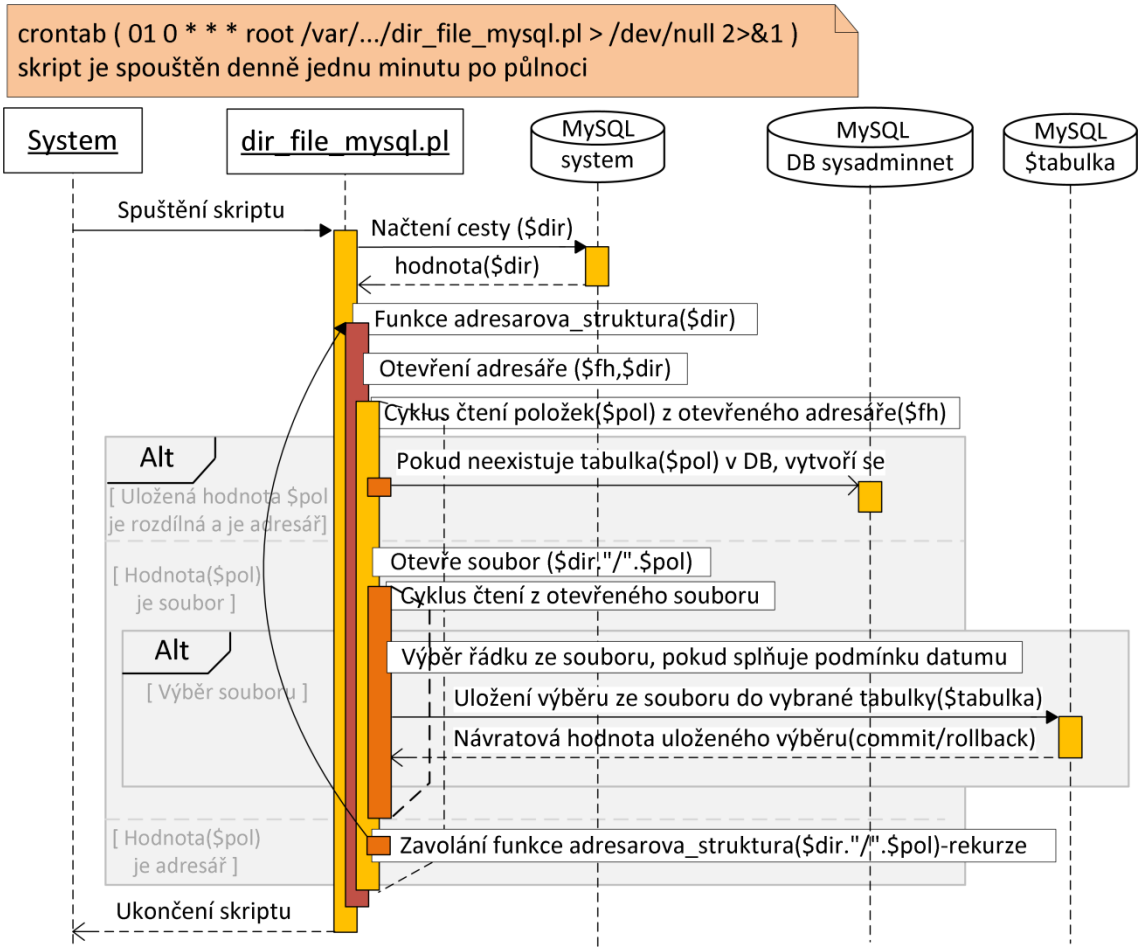
   Rozdělení VBScriptů[4]:
   - start počítače
   - přihlášení uživatele
   - odhlášení uživatele
   - vypnutí počítače

b) Zajištění sdílení adresářů a vygenerovaných souborů pro jednotlivé počítače s naším systémem k načtení dat do jednotlivých tabulek databáze.

Pokud jsme splnili podmínky předešlých kroků, máme nyní připraveny adresáře a soubory se záznamy událostí evidovaných v Active Directory školy.

Přenesení záznamů událostí do databáze je realizováno periodickým spouštěním perlového skriptu[15] načasovaného denně minutu po půlnoci pomocí systémové služby crontab obrázek 6.1. Po spuštění skript otevře adresář, jehož cestu si načetl ze systému a postupně rekurzí prochází všechny adresáře a soubory. Pokud narazí na adresář, který nemá v databázi tabulku, vytvoří pro něj tabulku se stejným jménem jako adresář. Otevře každý soubor uložený v adresáři a načte z něj záznamy, které odpovídají datu zápisu z předešlého dne a uloží je do jednotlivých tabulek s názvy podle zrovna procházeného adresáře. Po projití všech adresářů a zpracování souborů se skript ukončí.

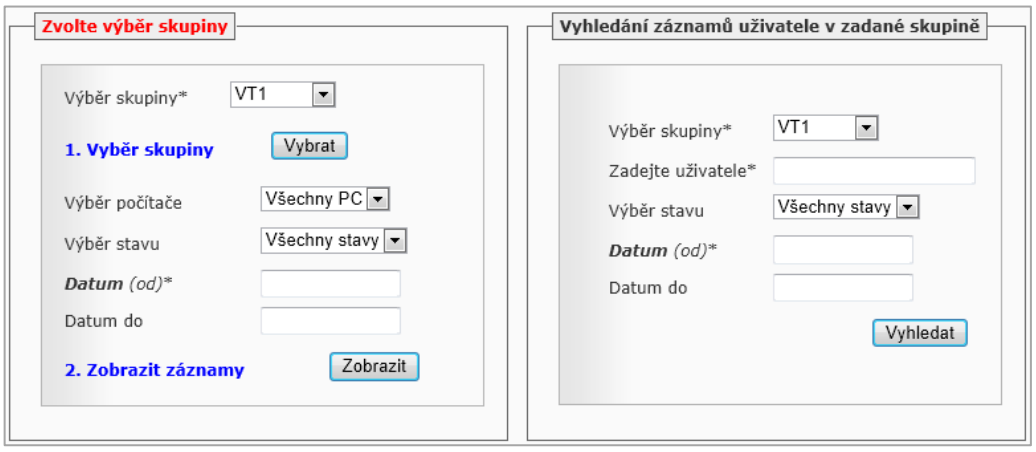
[4] Uvedené skripty jsou součástí přiloženého CD/DVD v adresáři Windows.



Obrázek 6.1 - sekvenční diagram uložení záznamů udalostí do databáze (dir_file_mysql.pl)

Popis uživatelského rozhraní modulu

Modul prohlížeče událostí Obrázek A.8 je rozdělen do dvou oblastí vyhledávání, kde v každé oblasti máme možnost specifikace záznamů podle zadání určitých hodnot a kritérií obrázek 6.2.



Obrázek 6.2 - panel pro vyhledání záznamů událostí

6.1.1 Vyhledání událostí podle skupiny

První varianta je v podstatě vyhledání záznamů ve zvolené skupině všech počítačů dle zadaného data. Při zvolení tohoto výběru je nutné prvně vybrat skupinu, ve které budeme vyhledávat zaznamenané události a potvrdit její výběr. V této variantě je dále možnost specifikace konkrétního počítače a výběru stavu události pro uživatele, nebo počítač. Dále můžeme výběr specifikovat o zadání rozmezí hledaných záznamů o datum začátku výskytu a konce.

Doplňující informace záznamu události první varianta

- **Výběr skupiny** - zvolení výběru skupiny, učebny, do které je počítač v doméně zařazen
- **Výběr počítače** - možnost výběru konkrétního počítače v zadané skupině
- **Výběr stavu** - zvolení události, start počítače, přihlášení uživatele, odhlášení uživatele, vypnutí počítače
- **Datum** (od) - možnost zadat datum vyhledání záznamu jednoho dne, nebo rozsahu více dnů
- **Datum do** - zadání konce hledaného data, pokud chceme vyhledat záznamy v určitém rozsahu

6.1.2 Vyhledání událostí podle uživatele

Ve druhé variantě můžeme uskutečnit vyhledání záznamů pro konkrétního uživatele podle uživatelova přihlašovacího jména. Zadání hodnot pro vyhledávání je totožné s první variantou. Rozdíl je pouze v tom, že tady není možnost výběru konkrétního počítače, ale zadáváme pro vyhledání jméno uživatele. Vyhledání je prováděno metodou „%LIKE%“, obsažení zadané hodnoty v hledaném řetězci, tudíž můžeme u neznalosti celého jména začít s vyhledáním známé zkratky. Rovněž nezáleží na velikosti písma při zadávání hodnoty pro vyhledání. Co není poleno při vyhledávání je použití diakritiky.

Doplňující informace záznamu události druhá varianta (uvedeme jen rozdíl s první variantou)

- **Zadejte uživatele** – zadání uživatelova přihlašovacího jména do sítě. Nezáleží na zadané velikosti písma, vyhledání záznamu v databázi se provádí metodou %LIKE%

Na uvedeném výpisu obrázek 6.3 vidíme přiklad vyhledání událostí podle uživatele.

Uživatel	Počítač	Stav	Datum-čas
ZAVODNY	ICT	LogOn	10.04.2012-07:35:45
ZAV	SBOROVNA	LogOn	10.04.2012-10:58:46
ZAV	U1UCITEL	LogOn	10.04.2012-08:10:09
ZAV	U1UCITEL	LogOn	10.04.2012-10:33:53

Obrázek 6.3 - ukázka výpisu vyhledání uživatele v záznamu události

7 Konfigurace systému

Poslední kapitola popisuje modul „systém - číselníky“.

7.1 Systém - číselníky

V tomto modulu je řešena základní konfigurace systému a číselníků pro ostatní moduly, které číselníky používají pro svoji činnost.

Princip funkce modulu

Modul nemá žádnou specifickou funkci. Má za úkol jenom ukládání a modifikaci dat pro určené tabulky v databázi.

Popis uživatelského rozhraní modulu

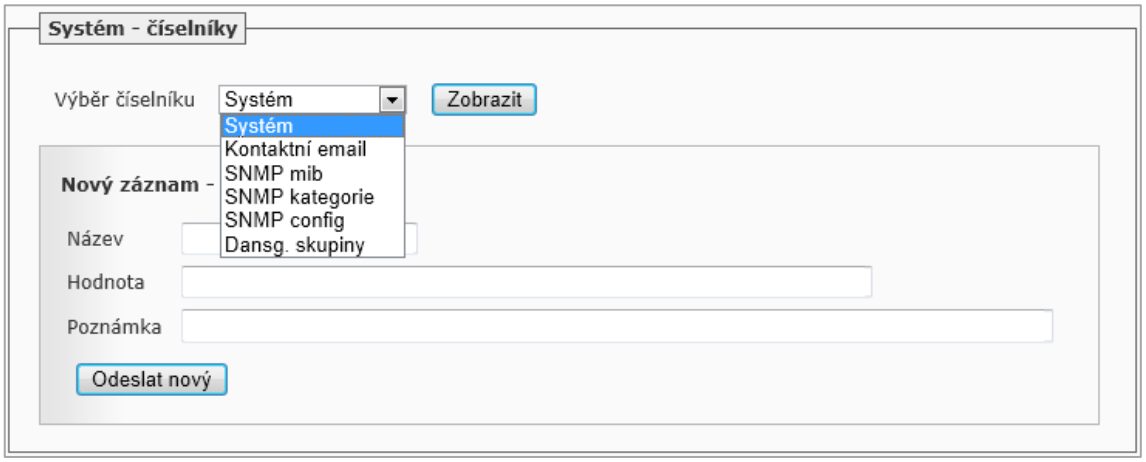
Správa systému a číselníků Obrázek A.9 je řešena principem výběru tabulky, do které chceme přidávat, nebo modifikovat již uložené záznamy. S výběrem se upraví prvky ve formuláři pro hodnoty požadované v tabulce.

Konfigurace systému a číselníku, jejich rozdělení a popis ukládaných hodnot:

- **Systém** – základní konfigurace systému, má přednastaveny čtyři záznamy, které se dají jenom modifikovat, nelze je smazat obrázek 7.1

  #### Popis ukládaných hodnot do konfigurace systému:

  - **Název** – jednoznačný, unikátní název, na základě kterého získáváme uloženou hodnotu
  - **Hodnota** – jakákoliv smysluplná hodnota předávaná ve spojení s názvem
  - **Poznámka** – konkrétnější popis uloženého záznamu, použití, typ zápisu



Obrázek 7.1 - výběr konfigurace systému a číselníků

- **Číselníky k modulu** - „Monitorování sítě (SNMP)“ - číselníky pro hlavní tabulku

  Popis Kontaktní email, může být požít i v jiném modulu:

  - **Jméno** – identifikace správce, může být i uživatel
  - **Email** – emailová adresa

  Popis SNMP mib:

  - **Název** – název SNMP dotazu, nejlépe název MIB databáze
  - **OID** – číselný identifikátor pro získání hodnoty ze zařízení

  Popis SNMP kategorie:

  - **Kategorie** – název kategorie, rozdělení zařízení

  Popis SNMP config:

  - **Konfigurace** – typ konfigurace pro evidovaná zařízení

- **Dansg. skupiny** – číselník pro modul „Filtrování obsahu (DansGuardian)“

  Popis ukládaných hodnot:

  - **Filter** – zadání hodnoty skupiny konfiguračního souboru ipgroups (filter3)
  - **Poznámka** – popis upřesnění názvu skupiny (filter3 = Server)

Poslední ukázka tabulky obrázek 7.2 na základě zadané poznámky plně vystihuje význam atributů Název, Hodnota a jejich spojení.

Název	Hodnota	Poznámka	Edit	Del
dir_log_pc	/var/www/html/ssl/sysadminnet/logpc	Plná cesta k log souborům, Windows server 2008	Edit	Del
admin	pop0015:krumnikl:zavodny	pole administrace oddelovač dvojtečka (jmeno:jmeno)	Edit	Del
iptables	0	Kontrola blokování učeben pro script PERL	Edit	Del
pc_users	VT1:VT2:VT3:VT4:VT5:VT6:VT7:VTANJ:VTNEJ:Knihovna:Ostatni	Pole učeben, logování přístupů (název:název). Název musí souhlasit s názvem tabulky v DB.	Edit	Del

Obrázek 7.2 - přehled konfigurace systému

8 Závěr

Námi vytvořené konfigurační rozhraní, „Systém pro správu a administraci síťových prvků heterogenní sítě“ byl nasazen do reálného provozu 30. ledna 2012 ve verzi 0.09 pro testovací účely s přístupem pouze pro administrátora. Na této verzi byla testována hlavně bezchybnost konfigurace síťových prvků, převážně ProCurve Switch 2510B-24 (J9019B) ve skupinách kabinety a vedení.

Další verze 1.00.00 byla nasazena 16. února 2012 s povoleným přístupem všech uživatelů. Postupně byly testovány všechny moduly a opravovány zjištěné spíše kosmetické závady a překlepy do verze 1.00.02.

Poslední aktuálně nasazená verze 1.01.02 dne 3. dubna 2012 byla rozšířena o zaznamenávání vlastních událostí například veškeré stavy přihlášení do systému. Všechny moduly pracující s databází byly rozšířeny o doplněk funkce pro ukládání veškerých transakcí rovněž do záznamu událostí.

Bylo nasazení jednotného konfiguračního rozhraní přínosem?

Jednoznačně se dá odpovědět, že ano. Hlavně v zjednodušení konfigurace vybraných služeb, programů a jejich využití na serveru. Dále pokud budeme pokračovat ve výčtu kladných hodnot, tak bezesporu velkým přínosem je modul obsahující monitorování sítě a konfiguraci síťových prvků. Informovanost o výpadcích monitorovaných zařízení a filtrování provozu. V podstatě se dá říci, že s každým modulem zakomponovaným do systému jsme něco získali. Námi vybudované rozhraní určitě oceníme v budoucnosti, kdy nás čeká sloučení naší školy s obchodní akademií. Tím nám přibude další odloučené pracoviště, které budeme moci monitorovat námi vytvořeným administrativním rozhraním.

Určitě bezespornou výhodou našeho konfiguračního rozhraní je možnost použití jakéhokoliv moderního webového prohlížeče s přístupem pro administrátora odkudkoliv zvenčí. Menší nevýhodou je, že systém je hodně specifický, vyžaduje instalaci a konfiguraci určitých služeb, programů a základní konfiguraci síťových prvků a aktivních zařízení. Tím se do určité míry snižuje jeho použitelnost pro jiné správce.

9 Literatura

[1] Ganglia Monitoring System. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://ganglia.sourceforge.net/.

[2] Nagios – The Industry Standard in IT Infrastructure Monitoring. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z:http://www.nagios.org/.

[3] ntop - Traffic analysis with NetFlow™ and sFlow™ support. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://www.ntop.org/products/ntop/.

[4] Webmin - home page. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://www.webmin.com/index.html.

[5] Shorewall – Shoreline firewall. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://shorewall.net/.

[6] SquidGuard. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://www.squidguard.org/.

[7] Net-SNMP. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://net-snmp.sourceforge.net/.

[8] MRTG - Tobi Oetiker's MRTG - The Multi Router Traffic Grapher. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://oss.oetiker.ch/mrtg/.

[9] netfilter/iptables project homepage - The netfilter.og project. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://www.netfilter.org/.

[10] DansGuardian – True Web Content Filtering for All. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://dansguardian.org/.

[11] FreeRADIUS The world's most popular RADIUS Server. [Online] 1. duben 2012. [Citace: 1. duben 2012.]. Dostupné z: http://www.freeradius.org/.

[12] Vrána, Jakub. *1001 tipů a triků pro PHP.* Brno: Computer Press, a.s., 2010. ISBN 978-80-251-2940-1.

[13] PHP: PDO – Manual. [Online] 1 prosinec 2011. Dostupné z: http://www.php.net/manual/en/book.pdo.php.

[14] PHP: SNMP – Manual. [Online] 14 prosinec 2011. Dostupné z: http://cz.php.net/manual/en/book.snmp.php.

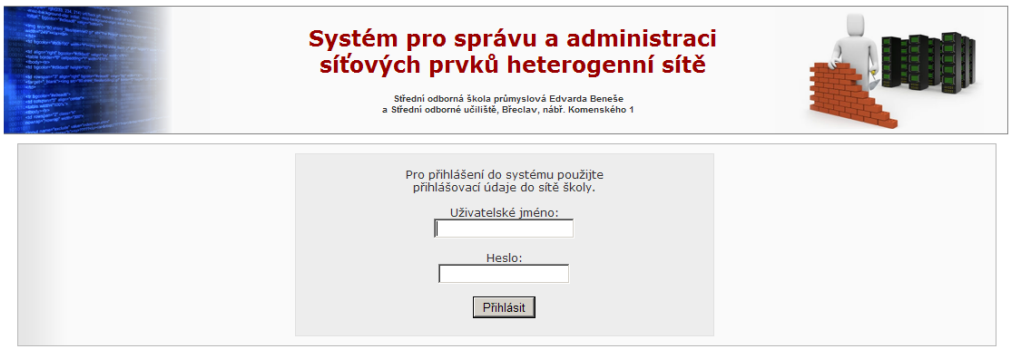
[15] Lemay, Laura. *Naučte se Perl za 21 dní*. Praha: Computer Press, 2002. ISBN 80-7226-616-0.

[16] Nemeth, Evi, Snyder, Garth a Hein, Trent R. *Linux Kompletní příručka administrátora*. Brno: Computer Press, 2004. ISBN 80-722-6919-4.

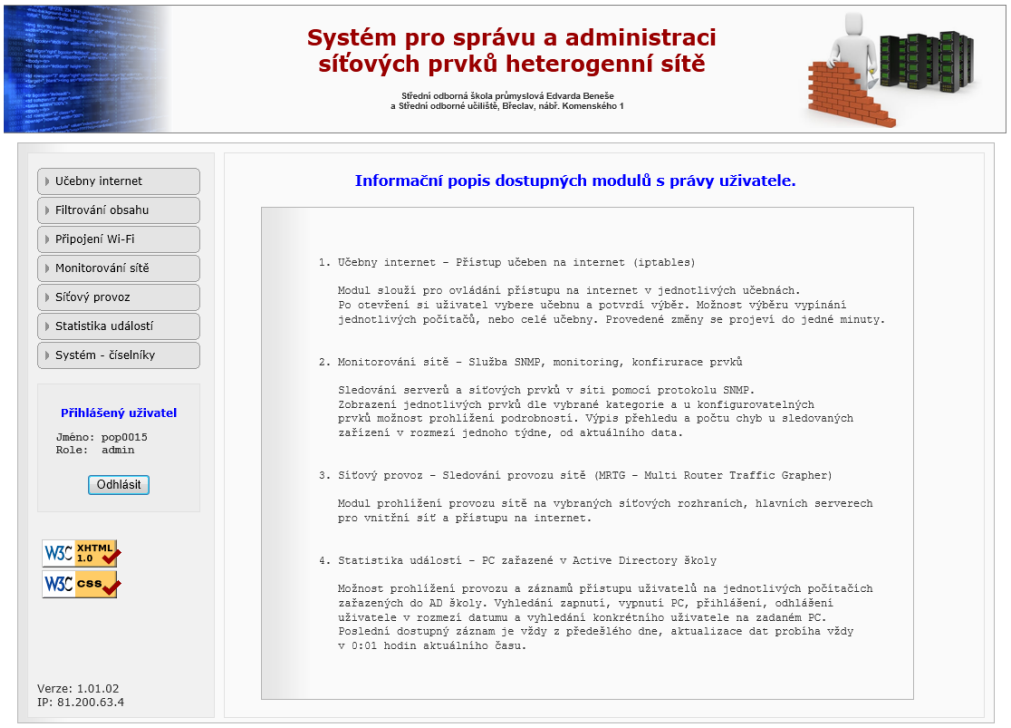
Přílohy

A Obrázky uživatelského rozhraní

V této příloze najdeme základní náhledy všech modulů, které náš administrativní systém obsahuje.

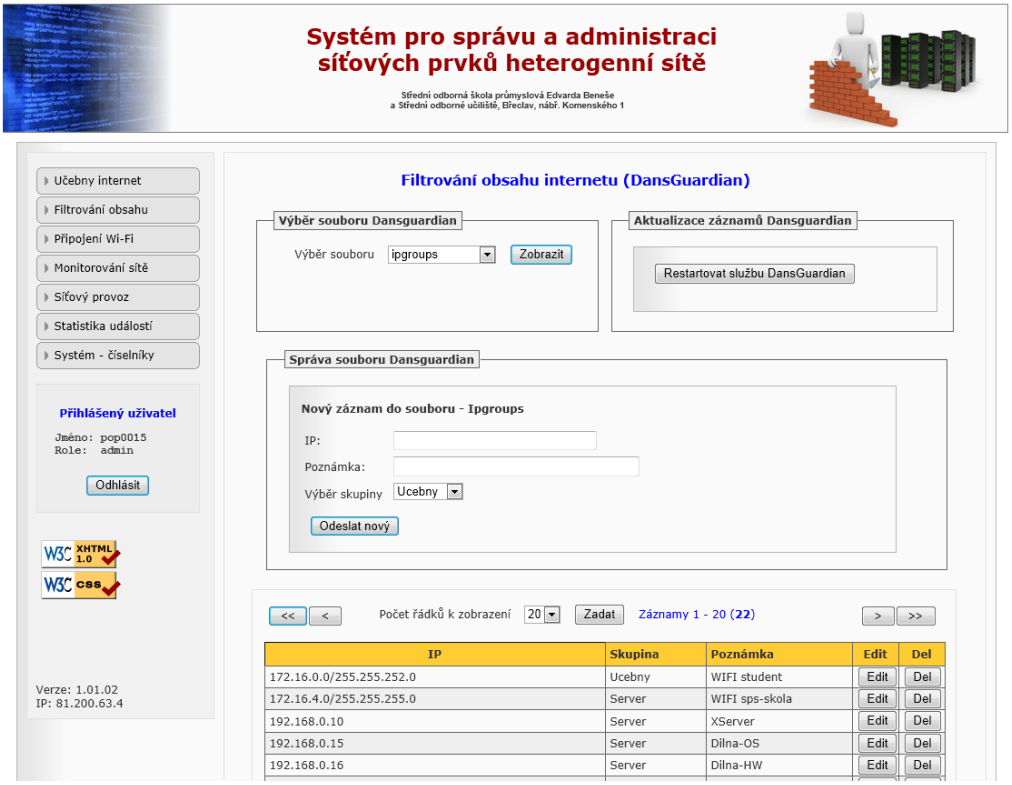


Obrázek A.1 - přihlášení do systému



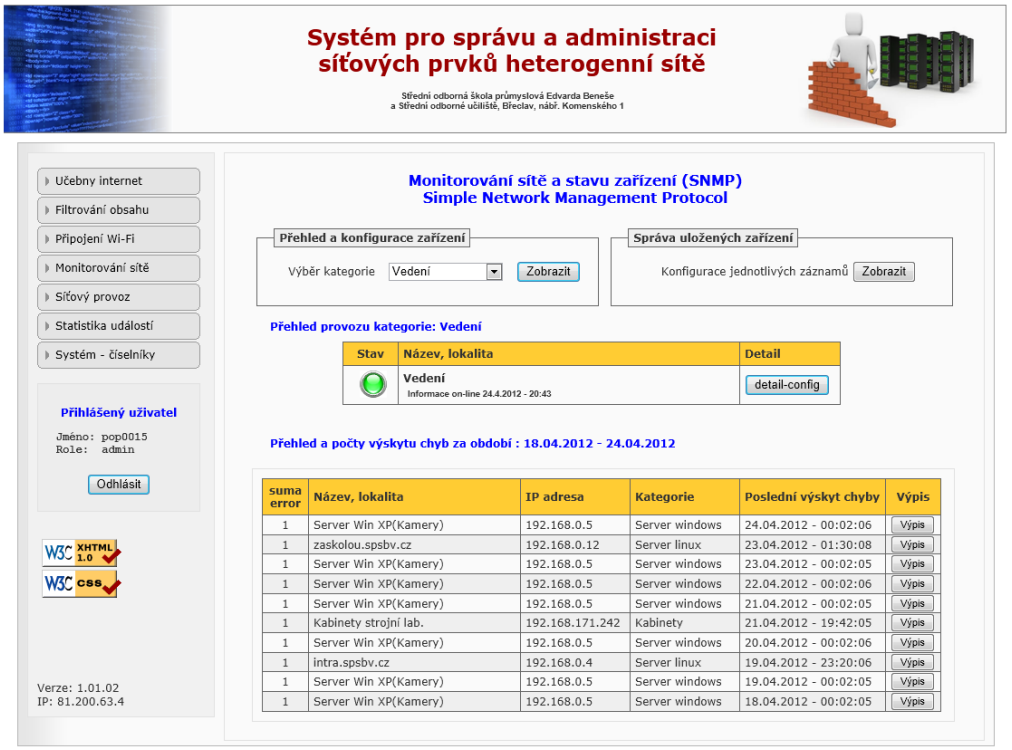
Obrázek A.2 - úvod po přihlášení

Obrázek A.3 - modul učebny internet

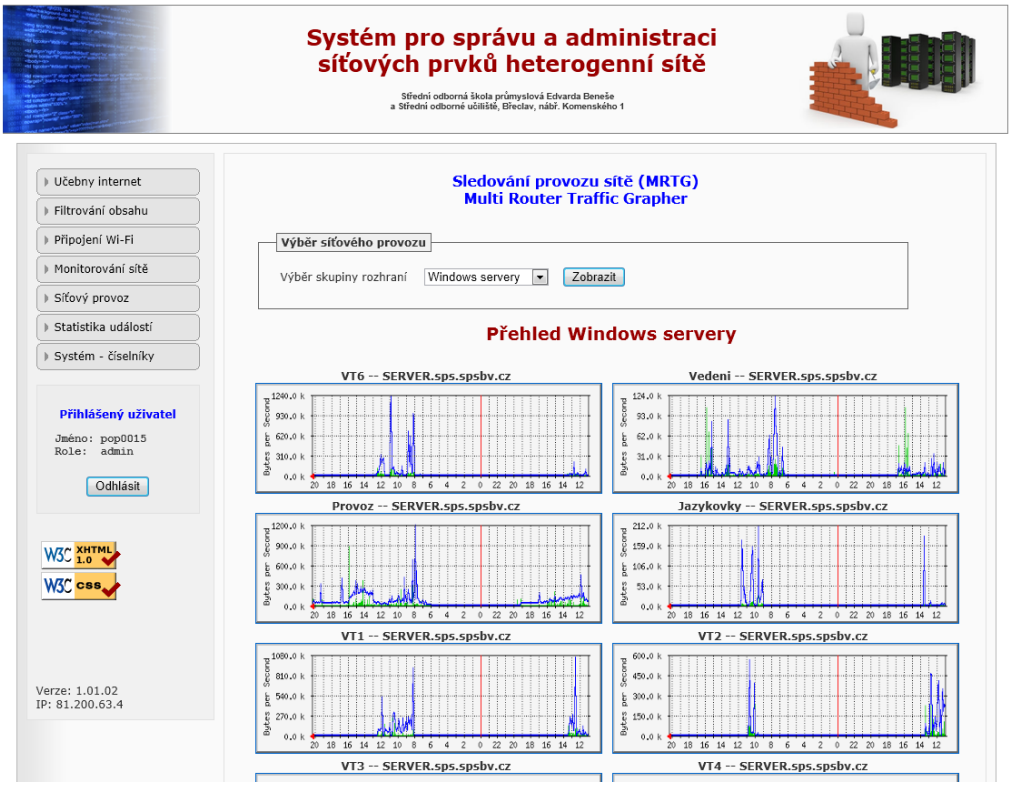


Obrázek A.4 - modul filtrování provozu

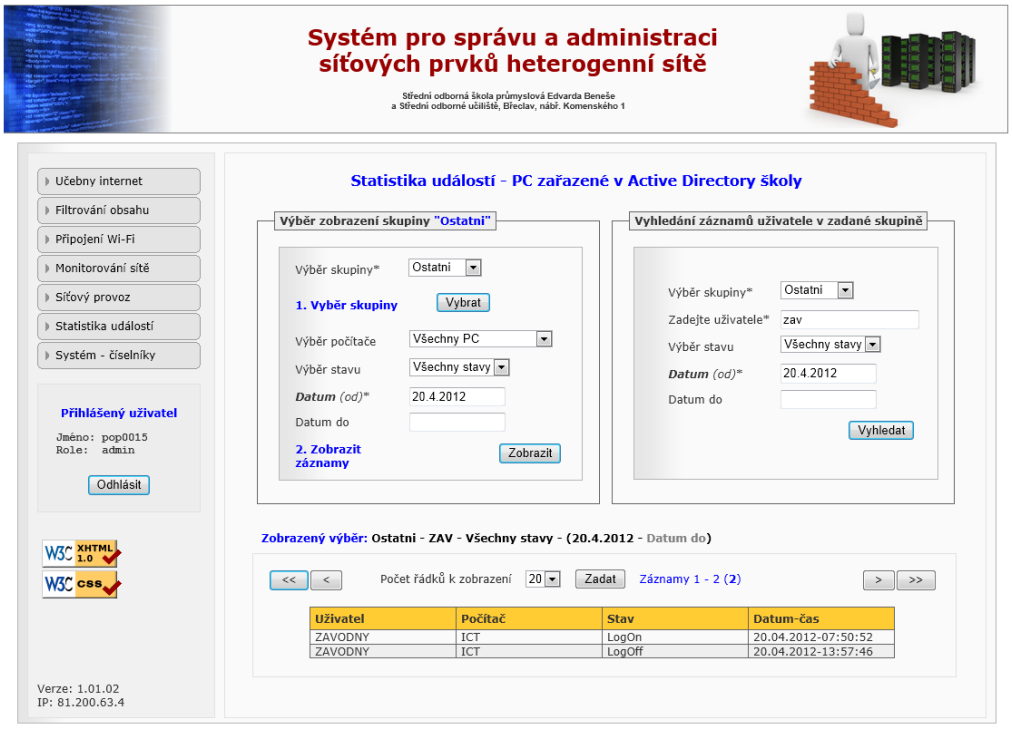
Obrázek A.5 - modul připojení Wi-Fi



Obrázek A.6 - modul monitorování sítě



Obrázek A.7 - modul síťový provoz



Obrázek A.8 - modul statistika událostí

Obrázek A.9 - modul systém - číselníky