

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA CHEMICKÉJ A POTRAVINÁRSKEJ TECHNOLOGIE

VIRTUÁLNA PRIVÁTNÁ SIETĚ ÚSTAVU
DIPLOMOVÁ PRÁCA

Bc. Martin Struhár

FCHPT-5414-28136

2010

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA CHEMICKÉJ A POTRAVINÁRSKEJ TECHNOLOGIE
Ústav informatizácie, automatizácie a matematiky



VIRTUÁLNA PRIVÁTNÁ SIEŤ ÚSTAVU

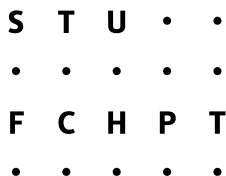
DIPLOMOVÁ PRÁCA

Bc. Martin Struhár

FCHPT-5414-28136

Študijný program:	Automatizácia a informatizácia v chémii a potravinárstve
Číslo a názov študijného odboru:	5.2.14 automatizácia
Školiace pracovisko:	Oddelenie informatizácie a riadenia procesov
Vedúci diplomovej práce:	prof. Ing. Miroslav Fikar, DrSc.

Bratislava 2010



ZADANIE DIPLOMOVEJ PRÁCE

Študent: **Bc. Martin Struhár**
ID študenta: 28136
Študijný program: automatizácia a informatizácia v chémii a potravinárstve
Študijný odbor: 5.2.14 automatizácia
Vedúci práce: prof. Dr. Ing. Miroslav Fikar
Miesto vypracovania: Bratislava

Názov práce: **Virtuálna privátna sieť ústavu**

Špecifikácia zadania:

Cieľom práce je štúdium a implementácia virtuálnej privátnej siete pre potreby Ústavu informatizácie, automatizácie a matematiky. Teoretická časť sa zaoberá otázkami bezpečnosti, firewallov, privátnych sietí. V praktickej časti sa získané poznatky využijú na návrh a konfiguráciu VPN pre firewall ústavu pomocou projektu pfSense.

Úlohy:

- problematika sietí vo všeobecnosti a virtuálnych sietí
- definovanie kritérií a návrh riešenia VPN pre UIAM
- implementácia a overovanie riešenia v testovacej sieti
- testy riešenia v prevádzke ústavu

Rozsah práce: 40

Zoznam odbornej literatúry:

1. SONNENREICH, W. – YATES, T. *Building Linux and OpenBSD Firewalls*. Toronto: John Wiley & Sons, 2000. 362 s. ISBN 0-471-35366-3.
2. KUSICK, M. K. – BOSTIC, K. – KARELS, M. – QUARTEMAN, J. S. *The design and implementation of the 4.4BSD operating system*. Reading: Addison-Wesley Publishing Company, 1996. 580 s. ISBN 0-201-54979-4.
3. GRAHAM, S. – SHAH, S. *Administrace systému LINUX : Podrobný průvodce začínajícího administrátora*. Praha: Grada, 2003. 550 s. ISBN 80-247-0641-5.
4. HATCH, B. – LEE, J. – KURTZ, G. *Linux Hackerské Útoky : Bezpečnost Linuxu – tajemství a řešení*. 2001: SoftPress, 2001. 576 s. ISBN 80-86497-17-8.

Riešenie zadania práce od: 15. 02. 2010

Dátum odovzdania práce: 21. 05. 2010

L. S.

Bc. Martin Struhár

študent

prof. Dr. Ing. Miroslav Fikar

vedúci pracoviska

prof. Ing. Miroslav Fikar, DrSc.

garant študijného programu

SÚHRN

Cieľom diplomovej práce je stručne oboznámiť čitateľa s teoretickými poznatkami o súčasných sieťach, konkrétne virtuálnych privátnych sieťach. Na vytvorenie a zabezpečenie testovacej siete, sme sa museli oboznámiť aj s problematikou zabezpečenia sietí pomocou firewallov. Praktická časť sa zaoberá tvorbou testovacej lokálnej siete. Táto sieť je zabezpečená firewallom pfSense. Ide o firewallové riešenie založené na platforme FreeBSD. V ďalšej časti sa využíva projekt OpenVPN, na tvorbu certifikátov a kľúčov pre server a jednotlivých klientov. Následne sa tento program inštaloval a konfiguroval na jednotlivých platformách. Použité platformy pre klientov boli Windows XP, Mandriva2010.0 a Ubuntu 9.10. Ako OpenVPN server nám slúžil už spomínaný pfSense firewall. Posledná časť je venovaná testovaniu konfigurácii servera a klientov na sieti ústavu UIAM.

Kľúčové slová: VPN, OpenVPN, pfSense.

ABSTRACT

The main goal of this master thesis is to become acquainted with theoretical findings of current networks, specifically virtual private networks. For creating and securing the testing network we had to become familiar with the problem of securing networks by firewalls. The practical part is dealing with the creating of the local network for testing purposes. This network is secured by firewall pfSense. It is a firewall solution based on the FreeBSD platform. In the next chapter the OpenVPN project is used for creating certificates and keys for server and particular clients. Subsequently, this program is installed and configured on various platforms as Windows XP, Mandriva 2010.0 Ubuntu 9.10. The above mentioned pfSense firewall served as an OpenVPN server. Last chapter is dedicated to the configurations of the server and clients for testing on the institute's network.

Keywords: VPN, OpenVPN, pfSense.

Pod'akovanie

Týmto by som sa chcel poďakovať vedúcemu diplomového projektu prof. Ing. Miroslavovi Fikarovi, DrSc. za cenné rady, pripomienky a vedenie, ktoré mi poskytol pri vypracovaní diplomovej práce.

Čestné prehlásenie

Čestne prehlasujem, že som diplomovú prácu vypracoval samostatne, podľa pokynov vedúceho práce a s použitím zdrojov uvedených v literatúre.

V Bratislave, 8. mája 2010

Bc. Martin Struhár

OBSAH

1	ÚVOD	10
2	TEORETICKÁ ČASŤ.....	11
2.1	STRUČNÝ PREHĽAD O SÚČASNÝCH SIEŤACH	11
2.2	OSI MODEL.....	12
2.3	VIRTUÁLNE SIETE	13
2.4	VPN.....	13
2.5	OPENVPN.....	14
2.6	KLÚČE A CERTIFIKÁTY.....	15
2.7	FIREWALL	16
3	PRAKTICKÁ ČASŤ.....	18
3.1	PFSENSE.....	18
3.1.1	Inštalácia.....	18
3.1.2	Konfigurácia	22
3.2	TVORBA CERTIFIKÁTOV.....	30
3.3	NASTAVENIE OPENVPN SERVERA PRE VZDIALENÝCH KLIENTOV	34
3.4	KONFIGURÁCIA OPENVPN KLIENTA PRE WINDOWS.....	38
3.5	KONFIGURÁCIA OPENVPN KLIENTA PRE UBUNTU 9.10.....	41
3.6	KONFIGURÁCIA OPENVPN KLIENTA PRE MANDRIVA 2010.0.....	44
3.7	ODSTRÁNENIE KLIENTA.....	46
3.8	TESTOVANIE NA ÚSTAVNEJ SIETI.....	48
4	ZÁVER	49
5	ZOZNAM POUŽITEJ LITERATÚRY	50

ZOZNAM OBRÁZKOV

<i>OBR.Č 1: VÝPOČET IP ADRESY PRE LAN ROZHRANIE</i>	<i>19</i>
<i>OBR.Č 2: SCHÉMA ZAPOJENIA INTERNET, FIREWALL A LAN.....</i>	<i>20</i>
<i>OBR.Č 3: HLAVNÉ MENU FIREWALLU</i>	<i>21</i>
<i>OBR.Č 4: NASTAVENIE IP ADRESY NA POČÍTAČI LOKÁLNEJ SIETE</i>	<i>22</i>
<i>OBR.Č 5: WEB-KONFIGURÁTOR PFSENSE</i>	<i>23</i>
<i>OBR.Č 6: NASTAVENIE WAN ROZHRANIA.....</i>	<i>24</i>
<i>OBR.Č 7: LAN ROZHRANIE</i>	<i>25</i>
<i>OBR.Č 8: POVOLENIE SSH</i>	<i>26</i>
<i>OBR.Č 9: PRAVIDLO SSH PRÍSTUPU Z WI-FI SIETE ÚSTAVU NA POČÍTAČ 147.175.79.162</i>	<i>27</i>
<i>OBR.Č 10: ZADEFINOVANIE ALIASU GARDA</i>	<i>28</i>
<i>OBR.Č 11: PRAVIDLO SSH PRÍSTUPU Z ALIASU GARDA NA POČÍTAČ 147.175.79.162</i>	<i>29</i>
<i>OBR.Č 12: PREHLAD ZADEFINOVANÝCH PRAVIDIEL</i>	<i>30</i>
<i>OBR.Č 13: HOSTNAME SERVERA.....</i>	<i>31</i>
<i>OBR.Č 14: NASTAVENIE OPENVPN SERVERA.....</i>	<i>34</i>
<i>OBR.Č 15: VKLADANIE CERTIFIKÁTOV PRE SERVER.....</i>	<i>35</i>
<i>OBR.Č 16 NASTAVENIE DNS SERVEROV A PRESMEROVANIA</i>	<i>36</i>
<i>OBR.Č 17: PRAVIDLO PRE OPENVPN SERVER</i>	<i>37</i>
<i>OBR.Č 18: NAT PRAVIDLÁ.....</i>	<i>37</i>
<i>OBR.Č 19: NOVÉ SIEŤOVÉ ZARIADENIE.....</i>	<i>38</i>
<i>OBR.Č 20: OBSAH KONFIGURAČNÉHO ADRESÁRA</i>	<i>39</i>
<i>OBR.Č 21: INFORMÁCIE O PRIPOJENÍ SIEŤOVÉHO ZARIADENIA OVPN</i>	<i>40</i>
<i>OBR.Č 22: TABUĽKA SIEŤOVÝCH ZARIADENÍ</i>	<i>45</i>
<i>OBR.Č 23: SYSTÉMOVÉ VÝPISY SERVERA</i>	<i>46</i>
<i>OBR.Č 24: VKLADANIE SÚBORU CRL.PEM</i>	<i>47</i>
<i>OBR.Č 25: MATLAB2009A NA KIRPHOME2</i>	<i>48</i>

1 ÚVOD

V teoretickej časti našej práce sa pokúsime stručne informovať o súčasných sieťach. Bližšie si vysvetlíme virtuálne privátne siete. Konkrétne sa budeme zaoberať projektom OpenVPN. Tento projekt sme si vybrali kvôli jeho širokej využiteľnosti a podpore rôznymi platformami. Ďalej sa budeme zaoberať tvorbou kľúčov a certifikátov, ktoré sú nevyhnutné pre náš typ konfigurácie (Road warrior konfigurácia – vzdialení klienti). Keďže budeme pracovať na testovacej sieti, ktorú potrebujeme zabezpečiť, musíme sa oboznámiť aj s problematikou zabezpečenia sietí pomocou firewallov.

V praktickej časti sa budeme najskôr zaoberať tvorbou lokálnej siete a následne inštaláciou a konfiguráciou firewallu pfSense, ktorý nám bude zároveň slúžiť ako OpenVPN server. Tento projekt je založený na platforme FreeBSD. Jednou z jeho hlavných výhod je pomerne jednoduchá konfigurácia pomocou web konfigurátora. Pomocou nástroja IP Calculátor sme si vypočítali rozsah našej lokálnej siete.

Ďalším krokom bude tvorba kľúčov a certifikátov pre server a klientov pomocou projektu OpenVPN. Následne si nakonfigurujeme OpenVPN server a jednotlivých klientov na rozličných platformách. Serverom je už spomínaný firewall pfSense. Klienti sú konfigurovaní pre platformy Windows, Mandriva 2010.0 a Ubuntu 9.10.

V poslednom kroku sa budeme zaoberať testovaním našej konfigurácie na sieti ústavu UIAM.

2 TEORETICKÁ ČASŤ

2.1 Stručný prehľad o súčasných sieťach

V súčasnosti najviac vyskytujúcimi sa sieťami sú TCP/IP siete. TCP/IP (Transmission Control Protocol / Internet Protocol) sú základné komunikačné protokoly Internetu. Pod pojmom internet sa rozumie celosvetová sieť. Táto je tvorená množstvom ďalej členených rôznych iných sietí a podsietí. Najspodnejšiu vrstvu hierarchie sietí tvoria malé lokálne siete LAN (Local Area Network). Tieto majú v rámci priestorového rozloženia rozsah maximálne jeden kilometer v rámci jedného celku. Pod týmto celkom sa rozumie napríklad UIAM FCHPT STU Bratislava. Tieto siete obsahujú rádovo desiatky až stovky počítačov. Takéto menšie siete sa ďalej spájajú a vytvárajú väčšie, rozsiahlejšie siete WAN (Wide Area Network). Sú charakteristické rozsahom viac ako jeden kilometer. Obsahujú rádovo stovky až tisíce počítačov. Čo sa technológie posielania paketov týka, dnešní správcovia sietí nahrádzajú zbernicové a kruhové topológie lokálnych sietí, ktoré boli často založené na technológií Ethernet IEEE 802.3. Túto technológiu nahrádza modernejšia sieťová architektúra Fast Ethernet IEEE 802.3u. Dosahované rýchlosti pripojenia sa pohybujú okolo 100Mb/s. V súčasnosti medzi najpopulárnejšie patria bezdrôtové siete. Rýchlosti dosahované pri týchto sieťach sa postupne približujú Fast Ethernetu. Technológia chrpticových sietí je pokročilejšia. Na smerovania dát z LAN sietí sa používa technológia Gigabit Ethernet IEEE 802.3z. Táto technológia dosahuje rýchlosti rádovo približne 1Gb/s. Hviezdicová topológia je preferovaná aj z hľadiska finančnej výhodnosti aktívnych prvkov siete. Takýmto prvkom je napríklad bridge. Bridge je zariadenie, ktoré na linkovej vrstve modelu OSI po prijatí paketu, prepošle tieto dáta do ďalšieho úseku siete. Funguje ako jednoduchý opakovač na danej vrstve. Najjednoduchším zariadením takéhoto typu je hub. Podstatou hubu je vysielanie paketov všetkými smermi. Toto je značne neefektívne ak chceme posilať pakety iba do rozhrania, kde sa nachádza príjemca, pretože hub obsahuje viacero rozhraní a pakety posila všetkým. Preto vznikli inteligentnejšie zariadenia slúžiace na smerovanie paketov. Takýmito zariadeniami sú switche. Switch je dokonalejšia forma hubu. Je schopný smerovať pakety iba do rozhrania, kde sa nachádza príjemca. Toto vykonáva na základe MAC adres, ktoré má uložené v bridgovacej tabuľke. Pre každé rozhranie má určenú individuálnu bridgovaciu tabuľku. Pod MAC adresou rozumieme fyzickú adresu konkrétneho zariadenia. Na základe vzniku switchov a rozvoja sietí založených na takomto smerovaní paketov dochádza k rozvoju technológie virtuálnych sietí. [1],[2]

2.2 OSI model

OSI model (Open Systems Interconnection reference model) je štandardný model sieťovej architektúry. Popisuje komunikáciu zaisťovanú počítačmi ako postupnosť siedmych vrstiev. Každá vrstva zaisťuje funkcie potrebné pre vrstvu vyššiu a využíva služby vrstvy nižšej. Medzi jednotlivými vrstvami sú definované rozhrania (medzivrstvové protokoly). Medzi prvkami rovnakej vrstvy sú definované pravidlá komunikácie (vrstvové protokoly).

Tabulka č. 1

7. úroveň	Aplikačná vrstva
6. úroveň	Prezentačná vrstva
5. úroveň	Relačná vrstva
4. úroveň	Transportná vrstva
3. úroveň	Sieťová vrstva
2. úroveň	Spojovacia (linková) vrstva
1. úroveň	Fyzická vrstva

Aplikačná vrstva - application layer – siedma vrstva v referenčnom modeli OSI. Táto vrstva predstavuje koncového užívateľa. Sprostredkúva a poskytuje služby aplikáciám. Každá aplikácia komunikuje pomocou určitého protokolu, pomocou ktorého môže prijímať alebo odosielať dáta.

Prezentačná vrstva – presentation layer – táto vrstva má hlavne transformačnú funkciu. Zabezpečuje vhodný výber syntaxe pre transformáciu informácií od aplikácií z aplikačnej vrstvy. Využíva služby spojovacej vrstvy a poskytuje služby aplikačnej vrstve.

Relačná vrstva – session layer – vrstva, ktorá nadväzuje, udržiava a ruší spojenie relácií a sprostredkúva výmenu dát medzi dvomi koncovými užívateľmi. Využíva informácie transportnej vrstvy a poskytuje informácie prezentačnej vrstve.

Transportná vrstva – transport layer – táto vrstva má za úlohu zabezpečiť bezchybný prenos dát medzi dvomi koncovými bodmi, ktoré sú pripojené k rôznym dátovým sieťam. Vyrovnáva rozdiely medzi týmito sieťami.

Sieťová vrstva – network layer – vrstva, ktorá zahŕňa celkovú komunikáciu v dátovej podsieti. Využíva služby spojovacej vrstvy a poskytuje služby transportnej vrstve. Má za úlohu smerovanie v sieti a prenos paketov medzi sieťovými uzlami.

Spojovacia (linková) vrstva – data link layer – má za úlohu riadiť dátovú komunikáciu medzi dátovými spojeniami dvoj i viacbodovými. Využíva služby fyzickej vrstvy a poskytuje služby sieťovej vrstve. Hľadá a opravuje chyby v dátovej komunikácii na fyzickej vrstve.

Fyzická vrstva – physical layer – vrstva zaoberajúca sa rozhraním medzi koncovým dátovým zariadeniami a konečným zariadením. Poskytuje služby spojovacej vrstve. Priamo dohliada na fyzické spojenie prenosového média. [3],[4]

2.3 Virtuálne siete

Virtuálna sieť je počítačová sieť založená na virtuálnych sieťových spojeniach medzi dvomi koncovými zariadeniami. Tento proces vytvárania virtuálnych sieťových spojení je založený na metódach sieťovej virtualizácie. Výsledkom tohto procesu je vhodné nakonfigurovanie sieťových prvkov tak, aby mohli medzi sebou komunikovať rôzne pracovné stanice nachádzajúce sa v rozdielnych fyzických sieťach. Komunikácia týchto zariadení prebieha pomocou virtuálnych sieťových rozhraní. Medzi takéto virtuálne siete patria VLAN, VPN a VPLS.

VLAN (Virtual LAN) sú virtuálne LAN siete založené na fyzických LAN sieťach. Vznikajú rozdelením fyzickej LAN siete na viacero virtuálnych LAN sietí.

VPN (Virtual Private Network) je virtuálna privátna sieť bližšie vysvetlená v nasledujúcej kapitole.

VPLS (Virtual Private LAN Service) je špeciálny typ takzvaných viacbodových VPN. [5]

2.4 VPN

VPN (Virtual Private Network) je privátna sieť, vybudovaná v rámci verejnej sieťovej infraštruktúry. VPN umožňujú prepájať cez verejnú sieť prostredníctvom VPN tunelov pobočky spoločností. Taktiež je ich pomocou možné jednoducho a bezpečne pripojiť počítač vzdialeného užívateľa k centrále. Táto technológia vytvára rovnaké podmienky a úroveň

bezpečnosti ako pri prenášaní vlastných fyzických liniek. Hlavnou výhodou je, že toto poskytuje za výrazne výhodnejších podmienok. [6],[8]

Tradičné systémy vzdialeného prístupu, ktoré sú chránené heslom, neposkytujú ani zďaleka takú vysokú bezpečnosť a ochranu ako šifrované spojenia založené na báze VPN. Takéto riešenie realizované pomocou VPN je teda efektívnejším, lacnejším, jednoduchším, a zároveň veľmi bezpečným spôsobom, ako možno zostať v kontakte so spoločnosťou alebo firmou aj mimo jej sídlo. [7]

Prostredníctvom virtuálnej privátnej siete sa dá uskutočniť napríklad pripojenie firemných notebookov kdekoľvek na internete do firemného intranetu (vnútornej firemnej siete). Na pripojenie prostredníctvom VPN je potrebné mať VPN server. Ten slúži buď len pre jedného klienta alebo ako hub prijíma spojenie od viacerých klientov. VPN klient, pripojený k serveru cez internet, sa potom pripojí do intranetu. VPN server potom slúži ako sieťová brána. Hlavný impulz rozšírenia VPN je rýchly rozvoj internetu a jeho cenovo prijateľný širokopásmový prístupom s možnosťou využívania množstva aplikácií. [9],[6]

2.5 OpenVPN

Pre našu prácu sme si zvolili prácu s projektom OpenVPN. Tento projekt patrí do skupiny open source VPN, ktoré používajú SSL/TLS (Secure Sockets Layer/ Transport Layer Security). Medzi jeho hlavné prednosti patrí:

- Podpora množstva platforiem - Linux, Solaris, OpenBSD, FreeBSD, NetBSD, Mac OS X a Windows 2000/XP
- Celý program beží v user mode
- Podpora režimov 1:1 (tunel) alebo N:1 (režim klient/server)
- Možnosť použitia zdieľaného kľúča alebo SSL certifikátov
- Jednoduchá konfigurácia
- Bezpečnosť
- Vysoká odolnosť pri použití na nekvalitných linkách
- Voliteľná kompresia
- Podpora HTTP a SOCKS proxy. To je výhodné predovšetkým pre RoadWarrior režim, klient sa tak môže pripojiť takmer odovšade. [7]

Čo sa bezpečnosti týka, vie toho OpenVPN skutočne veľa. Podporované sú režimy so zdieľaným kľúčom alebo použitie SSL/TLS certifikátov. Pre každý smer komunikácie je možné použiť iný kľúč. Takisto je možné nastaviť veľkosť replay-okna, ktoré znižuje možnosť prelomenia pomocou opätovného prehrania posielaných dát. Samozrejmosťou je použitie ľubovoľných šifrovacích algoritmov, ktoré podporuje použitá SSL knižnica.

OpenVPN štandardne používa protokol UDP (User Datagram Protocol), ale tiež sa dá použiť TCP (Transmission Control Protocol). Všetka komunikácia prebieha na jedinom porte a dá sa teda jednoducho nakonfigurovať firewall aby prepúšťal iba pakety na tomto porte.[4],[7]

Celý OpenVPN démon beží v užívateľskom režime a komunikuje prostredníctvom TAP alebo TUN rozhrania. Takto vytvorené rozhrania všetky prijaté dáta podávajú priamo užívateľskému procesu, ktorý tak môže vystupovať ako sieťová karta. Tým odpadá nutnosť znovu prekladať kernel (podpora TUN a TAP zariadení je vo väčšine distribúcií) a zároveň sa tak znižuje závislosť na niektorej platforme.

TUN a TAP sú virtuálne sieťové zariadenia. TUN predstavuje virtuálne zariadenie **sieťovej vrstvy**, teda tretej vrstvy OSI modelu a využíva sa na routing. TAP simuluje sieťové zariadenie pracujúce v druhej teda **spojovacej vrstve** OSI modelu a používa sa na vytváranie sieťových bridge-ov . [10],[11],[12]

2.6 Kľúče a certifikáty

Komunikácia medzi vpn serverom a klientmi prebieha pomocou takzvaného šifrovaného tunela. Týmto tunelom sú posielané pakety od vzdialeného klienta pre vpn server. Tieto pakety sú zašifrované a posielané internetom ako verejné pakety. Server ich prijme ako verejné pakety dešifruje ich a zistí, že sú to pakety určené pre privátne siete. Takýto tunel sa vytvorí pomocou šifrovania, ktoré zabezpečí že nebude možné odpočúvanie prenosov ani sa nebudú dať pozmeniť posielané údaje. Šifrovanie môžeme všeobecne rozdeliť do dvoch skupín: Symetrické šifrovanie a Asymetrické šifrovanie.

Symetrické šifrovanie je založené na šifrovaní dešifrovaní údajov pomocou hesla. Na jednej aj druhej strane komunikácie je potrebné rovnaké heslo. Teda zašifrované údaje heslom na jednej strane je možné dešifrovať na strane druhej iba tým istým heslom. Problémom tohto šifrovania teda zostáva len bezpečná výmena hesla medzi stranami.

Asymetrické šifrovanie využíva na rozdiel od symetrického šifrovania kľúčový pár. Ten pozostáva z verejnej a privátnej časti. Dáta, ktoré sú zašifrované verejným kľúčom sa dajú dešifrovať iba privátnym kľúčom a naopak. Verejná časť kľúčového páru tak môže byť posielaná aj nezabezpečeným kanálom.

Projekt OpenVPN pracuje s obidvomi typmi šifrovania. Pre symetrické šifrovanie je typická konfigurácia so statickým kľúčom. Asymetrické šifrovanie funguje zasa na základe certifikátov.

Medzi základné vlastnosti konfigurácie so statickým kľúčom patria:

- jednoduchá konfigurácia
- nie je potrebná certifikačná autorita
- kľúč musí byť uložený v textovej podobe na oboch systémoch teda aj na strane servera aj na strane klienta a tým je vystavený riziku odcudzenia
- možnosť pripojenia na server len jedného klienta

Základné vlastnosti konfigurácie s certifikátmi:

- zložitejšia konfigurácia
- nutná certifikačná autorita
- kľúč môže byť uložený na čipovej karte a chránený PIN kódom
- možnosť pripojenia viacerých klientov na server

Pre našu prácu sme zvolili konfiguráciu s certifikátmi pretože sme chceli aby bolo možné pripojenie viacerých klientov. [13]

2.7 Firewall

Súčasťou našej práce bolo vytvoriť a zabezpečiť lokálnu sieť. Toto sme urobili pomocou firewallu a preto si v nasledujúcej podkapitole lepšie priblížime, čo vlastne firewall je.

Jedná sa o sieťové zariadenie alebo softvér, ktorý je súčasťou informačného systému alebo siete. Má za úlohu blokovať nepovolený prístup a povoliť overenú komunikáciu. Toto zariadenie alebo súbor zariadení je nakonfigurovaný tak, aby povoľoval, blokoval, šifroval,

dešifroval alebo sprostredkoval každú dátovú komunikáciu medzi rozlične zabezpečenými doménami. Všeobecne povedané firewall často zabraňuje neoprávneným internetovým používateľom v prístupe do privátnych sietí pripojených na Internet, najmä intranety. Všetky správy prichádzajúce a odchádzajúce z intranetu prechádzajú cez firewall, ktorý každú preskúma a tie, ktoré nezodpovedajú bezpečnostným kritériám blokuje. [2],[3]

Toto všetko je definované súborom pravidiel, ktoré určujú podmienky a akcie. Tieto podmienky sú stanovené pre údaje pochádzajúce z toku dát. Jedná sa napríklad o informácie o zdrojovej, cieľovej adrese alebo o zdrojovom, cieľovom porte. Firewall má za úlohu vyhodnotiť podmienky a ak sú tieto splnené, tak sa vykoná akcia. Základnými podmienkami sú blokovanie toku dát a povolenie toku dát. Po vyhodnotení podmienky a následnom vykonaní akcie, firewall prestane ďalej spracovávať daný paket dát. Okrem základných akcií ako sú teda blokovanie a povolenie, existujú aj akcie, ktoré neurčujú čo sa s daným paketom stane, ale majú za úlohu napríklad logovanie hlavičky paketu alebo zmenu hlavičky paketu. [2],[3],[4]

3 PRAKTICKÁ ČASŤ

3.1 Pfsense

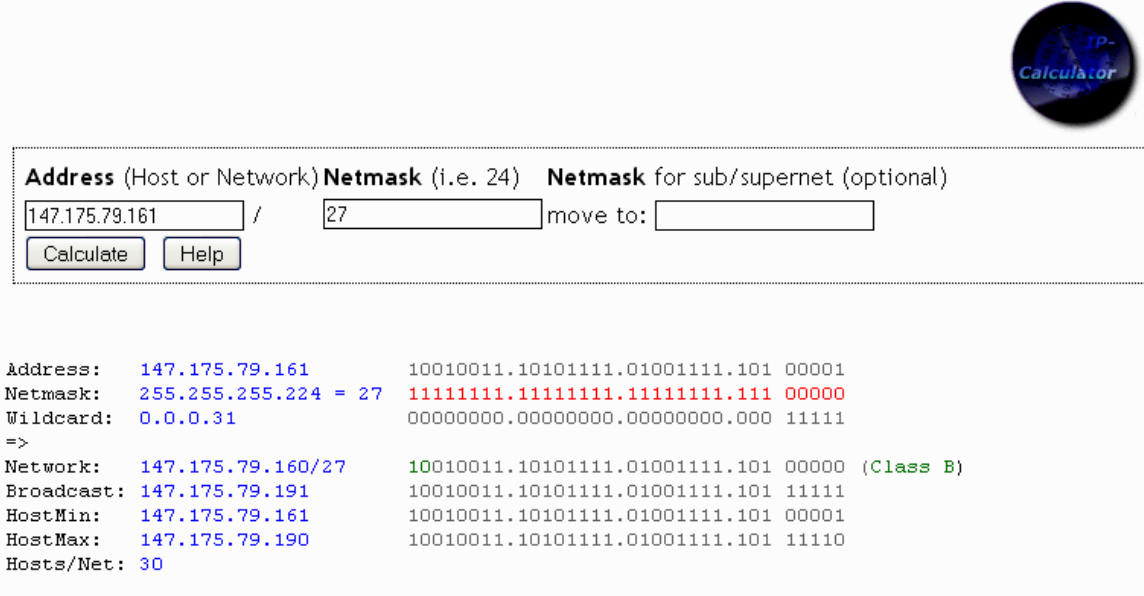
Pfsense je názov open source projektu založeného na platforme FreeBSD, ktorý má za úlohu slúžiť ako firewall a router. Vychádza z projektu m0n0wall. Ten je tiež firewallovým riešením založeným na FreeBSD. Jeho hlavnou výhodou je možnosť konfigurácie cez web rozhranie. Pfsense okrem toho, že je veľmi silný a flexibilný firewall a router, prichádza aj s množstvom ďalších funkcií a systémom balíčkov umožňujúcim rozšírenia. [14]

3.1.1 Inštalácia

Pred začatím našej práce s pfsense bolo potrebné si najskôr stiahnuť zo stránky projektu inštalačný súbor. Po jeho stiahnutí sme si vytvorili bootovateľné inštalačné CD, ktoré sme následne vložili do nášho stroja určeného na vytvorenie firewallu. Tento stroj má štyri sieťové karty, ale pre našu prácu sme zatiaľ využili len dve. Jednu sme zapojili do internetu ako zariadenie pre WAN rozhranie. Druhú sme zapojili ako zariadenie pre LAN rozhranie teda internú sieť.

Po spustení inštalácie sa nás inštalačný program spýtal na pripojenie jednotlivých sieťových zariadení. Ako prvé sa spýtal na pripojenie pre VLAN. Tie sme pre našu prácu nepotrebovali a tak sme zvolili možnosť nie. Ďalším rozhraním, ktoré bolo potrebné pripojiť k sieťovému zariadeniu bolo LAN rozhranie. V našom prípade to bolo zariadenie xl1. IP adresa našej lokálnej siete bola 147.175.79.161/27 . Pre dynamické pridelovanie IP adres DHCP serverom sme zvolili možnosť nie, pretože sme pracovali so statickými IP adresami. [6]

Na nasledujúcom obrázku si uvedieme výpočet IP adresy pre sieť LAN pomocou nástroja ip calc. [15]



Address (Host or Network) **Netmask** (i.e. 24) **Netmask** for sub/supernet (optional)

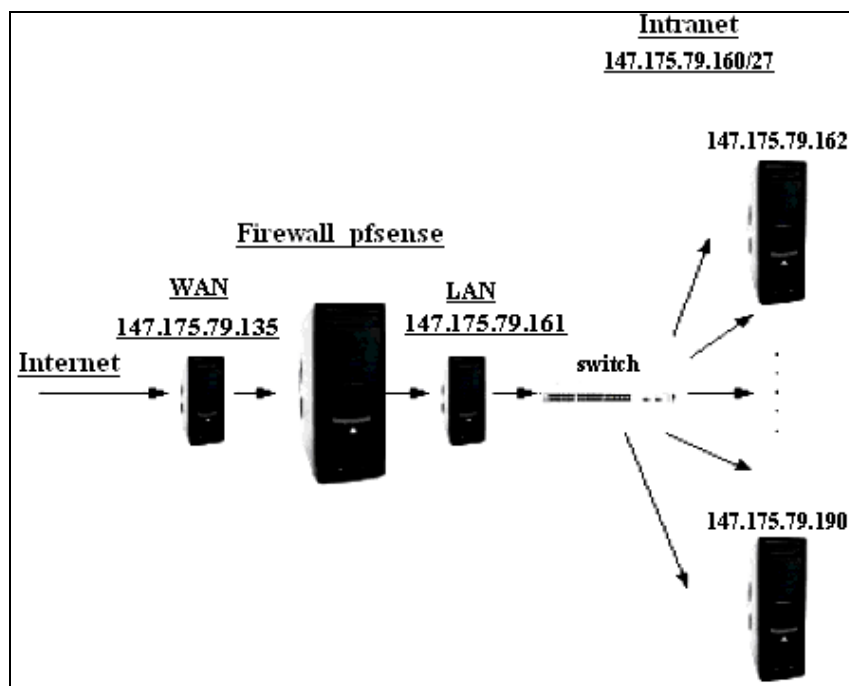
147.175.79.161 / 27 move to:

Address: 147.175.79.161 10010011.10101111.01001111.101 00001
Netmask: 255.255.255.224 = 27 11111111.11111111.11111111.111 00000
Wildcard: 0.0.0.31 00000000.00000000.00000000.000 11111
=>
Network: 147.175.79.160/27 10010011.10101111.01001111.101 00000 (Class B)
Broadcast: 147.175.79.191 10010011.10101111.01001111.101 11111
HostMin: 147.175.79.161 10010011.10101111.01001111.101 00001
HostMax: 147.175.79.190 10010011.10101111.01001111.101 11110
Hosts/Net: 30

Obr.č 1: Výpočet IP adresy pre LAN rozhranie

Pre našu lokálnu sieť sme mohli použiť IP adresy v rozpätí od 147.175.79.160 až po 147.175.79.191. Preto bolo potrebné vypočítať sieťovú masku tak, aby naše ip adresy spadali do tohto rozpätia. Pomocou nástroja ip calc sme si vyrátali sieťovú masku 255.255.255.224 čo predstavuje 27 bitov.

V ďalšom kroku inštalácie bolo potrebné priradiť sieťové zariadenie pre WAN rozhranie a to v našom prípade bolo zariadenie fxp0. IP adresa pre toto zariadenie je 147.175.79.135. Mohli sme v ďalších krokoch ešte pripojiť ostatné sieťové zariadenie, ale tie sme pre našu prácu nepotrebovali.



Obr.č 2: Schéma zapojenia Internet, Firewall a LAN

Na predchádzajúcom obrázku vidíme, znázornenú schému zapojenia našej lokálnej siete na firewall, ktorý je pripojený na globálnu sieť.

```

*** Welcome to pfSense 1.2.2-pfSense on pfsense ***

WAN*          ->  fxp0   ->    147.175.79.135
LAN*          ->  xl1    ->    147.175.79.161

pfSense console setup
*****
0) Logout (SSH only)
1) Assign Interfaces
2) Set LAN IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) PFtop
10) Filter Logs
11) Restart webConfigurator
12) pfSense PHP shell
13) Upgrade from console
14) Disable Secure Shell (sshd)
98) Move configuration file to removable device
99) Install pfsense to a hard drive/memory drive, etc.
Enter an option: █

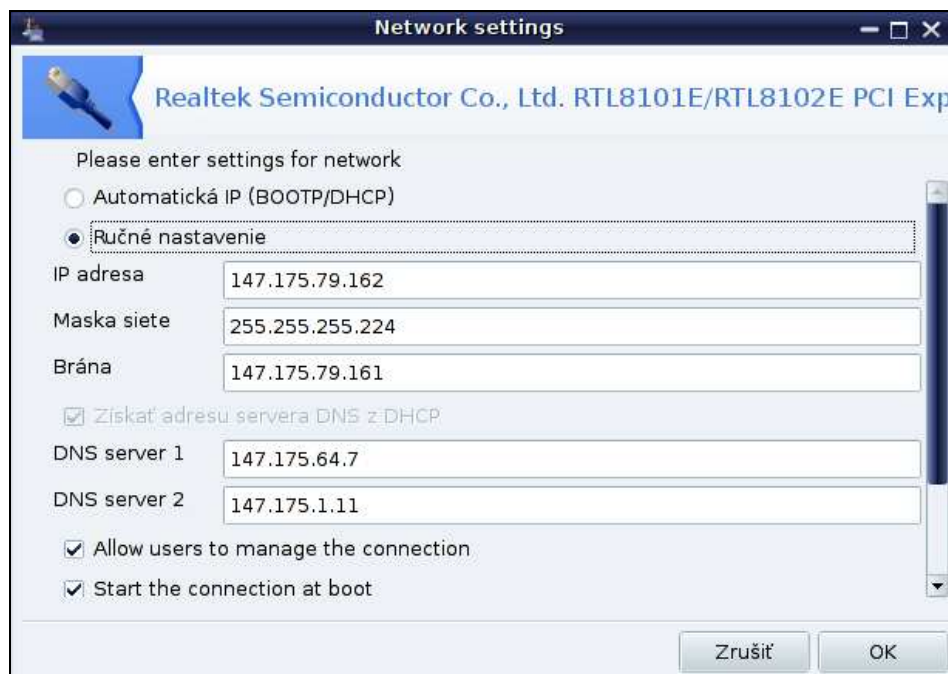
```

Obr.č 3: Hlavné menu firewallu

Po pripojení sieťových zariadení sa nám objavilo hlavné menu firewallu, kde sme zvolili možnosť 99 pre inštaláciu na pevný disk. Tu sme postupovali bod po bode podľa navigácie inštalačného menu. Toto je dôležité pre uloženie a zachovanie všetkých nastavení firewallu pre prípad, že by server padol napríklad dôsledkom výpadku elektrického prúdu.

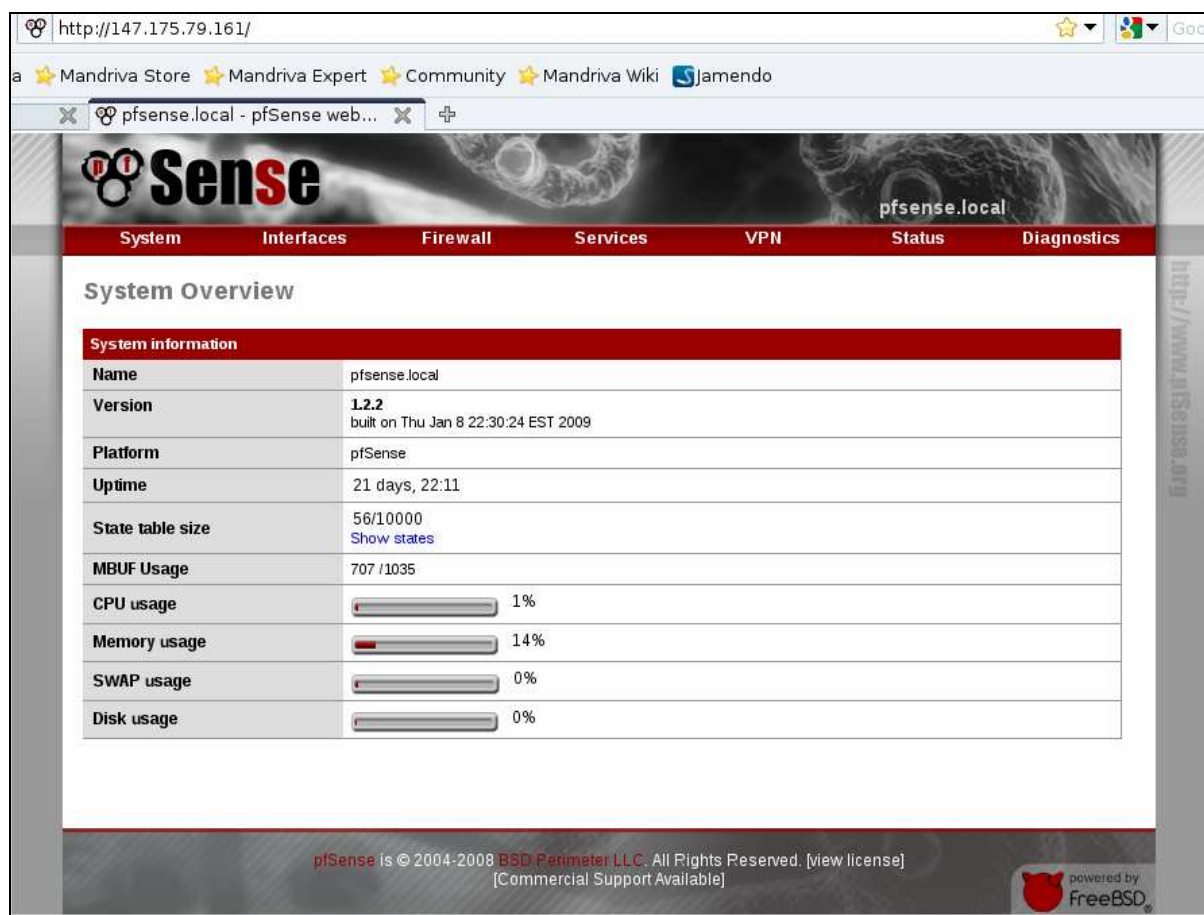
3.1.2 Konfigurácia

Po úspešnej inštalácii sme nastavili počítaču v našej lokálnej sieti IP adresu z vypočítaného rozpätia 147.175.79.162.



Obr.č 4: Nastavenie IP adresy na počítači lokálnej siete

V nasledujúcom kroku sme si v prehliadači na lokálnom počítači zavolali adresu našej lokálnej siete 147.175.79.161. Objavilo sa nám web rozhranie pfsense pre konfiguráciu firewallu.



Obr.č 5: Web-konfigurátor pfSense

Pomocou tohto web-konfigurátora sa dajú pomerne jednoducho a prehľadne nastavovať rôzne funkcie. Takýmto spôsobom si môžeme nakonfigurovať aj jednotlivé sieťové zariadenia. V menu „**Interfaces**“ si vyberieme rozhranie ktoré chceme konfigurovať. Pre konfiguráciu sieťového zariadenia pre WAN rozhranie zvolíme danú možnosť.

Interfaces: WAN

General configuration

Type: Static

MAC address: [Copy my MAC address](#)
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

Static IP configuration

IP address: / 26

Gateway:

DHCP client configuration

Hostname:
The value in this field is sent as the DHCP client identifier and hostname when requesting a DHCP lease. Some ISPs may require this (for client identification).

PPPoE configuration

Username:

Password:

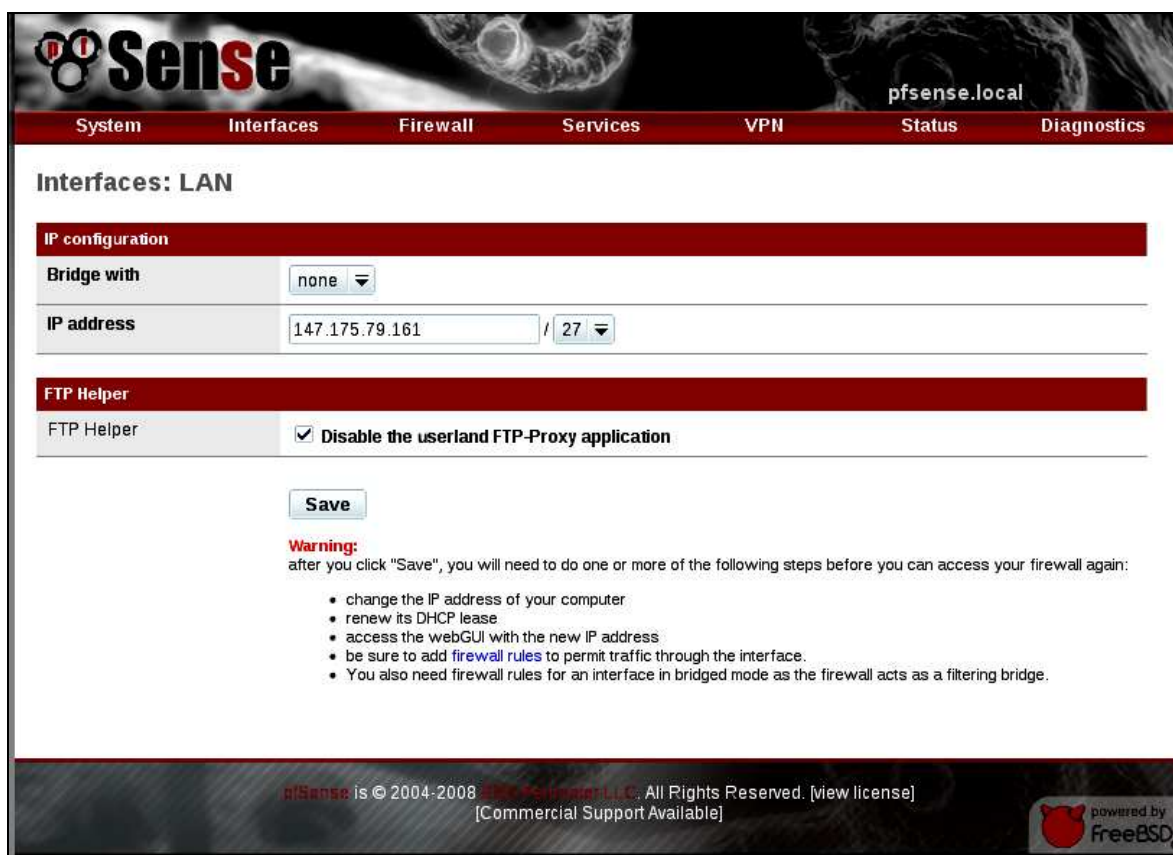
Service name:
Hint: this field can usually be left empty

Dial on demand: ☐ **Enable Dial-On-Demand mode**
This option causes the interface to operate in dial-on-demand mode, allowing you to have a *virtual full time* connection. The interface is configured, but the actual connection of the link is delayed until qualifying outgoing traffic is detected.

Idle timeout: seconds
If no qualifying outgoing packets are transmitted for the specified number of seconds, the connection is

Obr.č 6: Nastavenie WAN rozhrania

Keďže máme na WAN rozhraní pevnú IP adresu zvolíme pre typ možnosť „**Static**“. Ďalej by sme mohli nastaviť MAC adresu stroja, na ktorom je nainštalovaný pfSense. Toto však pre konfiguráciu nášho firewallu a siete nepotrebujeme. Je to nevyhnutné len pre určitý druh sieťového zapojenia. Čo potrebujeme nastaviť je IP adresa WAN rozhrania a predvolená brána (viď obrázok 6).



Obr.č 7: LAN rozhranie

Rovnakým spôsobom môžeme nastaviť LAN rozhranie. V menu „**Interfaces**“ zvolíme príslušnú možnosť a otvorí sa nám konfiguračné okno pre LAN rozhranie. Tu nastavíme IP adresu našej lokálnej siete 147.175.79.161/27.

Potom ako máme konfiguráciu rozhraní ukončenú je potrebné nastaviť pravidlá pre tieto rozhrania. Určiť čo je dovolené a čo nie je. Štandardne platí pravidlo čo nie je dovolené je zakázané. Teda ak na začiatku nemáme definované žiadne pravidlá znamená to, že je všetko prednostne zakázané. Pre LAN bolo predvolené pravidlo „**from LAN to any**“. To znamená, že zo siete LAN je možné ísť na akúkoľvek adresu a na hociktorý port. Späťne to samozrejme neplatí. Toto pravidlo ako jediné pravidlo pre LAN je postačujúce.

V prípade pfSense sú všetky pravidlá definované ako pravidlá „**in**“. To znamená, že sa týkajú všetkej komunikácie, ktorá prichádza na dané rozhranie. Teda pre LAN rozhranie všetky pakety prichádzajú z vnútornej siete na toto rozhranie a na základe vyššie uvedeného pravidla sú púšťané ďalej do globálnej siete teda internetu.

Na rozhranie WAN prichádzajú všetky pakety z internetu. Musíme definovať pravidlá určujúce, ktoré pakety môžu prejsť ďalej do lokálnej siete a ktoré nie.

Ak chceme spravovať náš firewall prostredníctvom vzdialeného prístupu cez SSH, musíme v menu „**System**“ najskôr vybrať možnosť „**Advanced**“ a tu povoliť SSH.

Sense pfsense.local

System Interfaces Firewall Services VPN Status Diagnostics

System: Advanced functions

Note: the options on this page are intended for use by advanced users only.

Enable Serial Console

☐ This will enable the first serial port with 9600/8N/1
Note: This will disable the internal video card/keyboard

Save

Secure Shell

☒ Enable Secure Shell

☐ Disable Password login for Secure Shell (KEY only)

SSH port: 22
Note: Leave this blank for the default of 22

Obr.č 8: Povolenie SSH

Následne musíme v menu „**Firewall**“ zvoliť možnosť „**Rules**“ a tu nastaviť príslušné pravidlo pre rozhranie WAN.

Pre pripojenie sa prostredníctvom vzdialeného prístupu do lokálnej siete na počítač 147.175.79.162 sme definovali viacero pravidiel.

System	Interfaces	Firewall	Services	VPN	Status	Diagnostics
Firewall: Rules: Edit						
Action	Pass <input type="button" value="v"/> Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.					
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.					
Interface	WAN <input type="button" value="v"/> Choose on which interface packets must come in to match this rule.					
Protocol	TCP/UDP <input type="button" value="v"/> Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.					
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: Network <input type="button" value="v"/> Address: 147.175.79.192 / 26 <input type="button" value="v"/> <input type="button" value="Advanced"/> - Show source port range					
Source OS	OS Type: any <input type="button" value="v"/> Note: this only works for TCP rules					
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: Single host or alias <input type="button" value="v"/> Address: 147.175.79.162 / 31 <input type="button" value="v"/>					
Destination port range	from: SSH <input type="button" value="v"/> <input type="button" value="v"/> to: SSH <input type="button" value="v"/> <input type="button" value="v"/> Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port					
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).					
Advanced Options	<input type="button" value="Advanced"/> - Show advanced options					

Obr.č 9: Pravidlo ssh prístupu z wi-fi siete ústavu na počítač 147.175.79.162

Toto pravidlo dovoľuje prejsť všetkým paketom komunikujúcim prostredníctvom protokolu TCP a UDP, prichádzajúcim z IP adresy 147.175.79.192/26 smerujúcim na port 22. IP adresa 147.175.79.192/26 predstavuje wi-fi sieť na ústave Informatizácie, automatizácie a riadenia procesov. Teda všetky pakety prichádzajúce z tejto siete zodpovedajúce príslušnému pravidlu môžu prejsť.

Ďalej sme chceli aby bolo možné sa prostredníctvom ssh pripojiť na náš lokálny počítač zo siete študentského domova Mladá garda. Do tejto siete však spadá viacero podsietí preto bolo potrebné zadať si alias.

Firewall: Aliases: Edit

Name garda
NOTE: This alias is in use so the name may not be modified!

Description pristup mladej gardy
You may enter a description here for your reference (not parsed):

Type Network(s)

Network(s)

Networks can be expressed like 10.0.0.0 format. Select the CIDR (network mask) that pertains to each entry.

Network	CIDR	Description
147.175.216.0	24	Entry added Thu, 26 Nov 2009 09:12:32 +0100
147.175.217.0	24	Entry added Thu, 26 Nov 2009 09:12:32 +0100
147.175.218.0	24	Entry added Thu, 26 Nov 2009 09:12:32 +0100
147.175.219.0	24	Entry added Thu, 26 Nov 2009 09:12:32 +0100
147.175.220.0	24	Entry added Thu, 26 Nov 2009 09:12:32 +0100
147.175.221.0	24	Entry added Thu, 26 Nov 2009 09:12:32 +0100

Save **Cancel**

pfSense is © 2004-2008 BSD Router LLC. All Rights Reserved. [view license]
[Commercial Support Available]

powered by FreeBSD

Obr.č 10: Zadeňovanie aliasu garda

Tento alias sme si pomenovali „garda“. Každá z uvedených sietí môže mať 256 IP adries pričom prvá z rozsahu je vždy predvolená brána danej siete a posledná je broadcast. Napríklad 147.175.216.0/24 je sieť, 147.175.216.1 je predvolená brána a 147.175.216.255 je broadcast.

System	Interfaces	Firewall	Services	VPN	Status	Diagnostics
Firewall: Rules: Edit						
Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>					
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.					
Interface	<div>WAN</div> <p>Choose on which interface packets must come in to match this rule.</p>					
Protocol	<div>TCP/UDP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>					
Source	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>Single host or alias</div> Address: <div>garda</div> / <div>31</div> <div>Advanced</div> - Show source port range					
Source OS	OS Type: <div>any</div> Note: this only works for TCP rules					
Destination	<input type="checkbox"/> not Use this option to invert the sense of the match. Type: <div>Single host or alias</div> Address: <div>147.175.79.162</div> / <div>31</div>					
Destination port range	from: <div>SSH</div> <div></div> to: <div>SSH</div> <div></div> Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port					
Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).					
Advanced Options	<div>Advanced</div> - Show advanced options					

Obr.č 11: Pravidlo ssh prístupu z aliasu garda na počítač 147.175.79.162

Po zadefinovaní aliasu sme vytvorili pravidlo, ktoré umožňuje paketom prichádzajúcim z príslušných IP adries na WAN rozhranie, smerujúcim na port 22, prejsť. Rovnakým spôsobom sme si vytvorili pravidlá pre pakety smerujúce na porty pre protokoly HTTP a HTTPS.

Ako posledné pravidlo, si vytvoríme pravidlo pre našu virtuálnu sieť, ktorú budeme v nasledujúcich krokoch vytvárať. Náš firewall bude zároveň serverom pre virtuálnu privátnu sieť. Povedali sme si, že klienti sa budú môcť pripájať odovšadiaľ a server ich bude počúvať na jedinom porte a to 1194. Toto pravidlo sme pridali do pravidiel pre WAN rozhranie. Prehľad jednotlivých pravidiel vidíme na nasledujúcom obrázku.

Firewall: Rules

The settings have been applied. The firewall rules are now reloading in the background. You can also monitor the reload progress.

LAN WAN

	Proto	Source	Port	Destination	Port	Gateway	Schedule	Description
<input type="checkbox"/>	TCP/UDP	147.175.79.192/26	*	147.175.79.162	22 (SSH)	*		from 147.175.79.192/26 ssh to 147.175.79.162
<input type="checkbox"/>	TCP/UDP	garda	*	147.175.79.162	22 (SSH)	*		from networks garda ssh to 147.175.79.162
<input type="checkbox"/>	TCP/UDP	garda	*	147.175.79.162	80 (HTTP)	*		from networks garda ssh to 147.175.79.162
<input type="checkbox"/>	TCP/UDP	garda	*	147.175.79.162	443 (HTTPS)	*		from networks garda ssh to 147.175.79.162
<input type="checkbox"/>	TCP/UDP	*	*	147.175.79.135	22 (SSH)	*		
<input type="checkbox"/>	TCP/UDP	*	*	*	1194 (OpenVPN)	*		OpenVPN

☒ pass
☐ pass (disabled)
 ☒ block
☐ block (disabled)
 ☒ reject
☐ reject (disabled)
 ☒ log
☐ log (disabled)

Hint:
 Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

pfSense is © 2004-2008 BSD Perimeter LLC. All Rights Reserved. [view license]
 (Commercial Support Available)

Obr.č 12: Prehľad zadefinovaných pravidiel

3.2 Tvorba certifikátov

Pri tvorbe certifikátov sme pracovali na Linuxe Mandriva verzia 2010.0. Zo stránky projektu OpenVPN sme si stiahli zdrojový kód inštalačného balíka. V našom prípade išlo o balík `openvpn-2.1.1.tar.gz`. Vytvoríme sme si adresár, v ktorom budeme pracovať a vytvárať všetky potrebné kľúče a certifikáty. Sem rozbalíme náš zdrojový kód pomocou príkazu „`tar -xvzf openvpn-2.1.1.tar.gz`“. [16]

Po rozbalení sa nastavíme do adresára „`openvpn-2.1.1/easy-rsa/2.0/`“ a v ľubovoľnom editore, napríklad `vi`, si otvoríme súbor „`vars`“. Na konci tohto súboru nastavíme hodnoty parametrov. Tieto budú používané ako predvolené aj pre iné skripty a nie je ich potrebné zadávať znovu.


```
export KEY_COUNTRY="SR"
export KEY_PROVINCE="BA"
export KEY_CITY="Bratislava"
export KEY_ORG="STUBA"
export KEY_EMAIL="nase.meno@domena.com"
```

Po tomto kroku je potrebné spustiť nasledovné skripty:

```
source ./vars
./clean-all
./build-ca
```

Spustením posledného príkazu vytvoríme certifikačnú autoritu a je potrebné zadať niektoré parametre, konkrétne „**Common Name**“, kde použijeme hostname nášho servera. Toto je nastavené na našom serveri v menu „**General Setup**“

```
Country Name (2 letter code) [SR]:
State or Province Name (full name) [BA]:
Locality Name (eg, city) [Bratislava]:
Organization Name (eg, company) [STUBA]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) [STUBA
CA]:pfsense.local
Name []:
Email Address [nase.meno@domena.com]:
```

System: General Setup	
Hostname	<input type="text" value="pfsense"/> <small>name of the firewall host, without domain part e.g. firewall</small>
Domain	<input type="text" value="local"/> <small>e.g. mycorp.com</small>

Obr.č 13: Hostname servera

Ďalším krokom je vytvorenie certifikátu pre server. Spustíme nasledovný skript kde za meno servera dáme už predtým použitý „**Hostname**“ servera:

```
./build-key-server pfsense.local
```

Na všetky výzvy odpovieme kladne a pri extra atribútoch zadáme heslo a voliteľný názov spoločnosti. Tieto atribúty majú byť zasielané spolu s certifikačnou požiadavkou.

```
Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
```

```
A challenge password []:HESLO
```

```
An optional company name []:NAZOV_SPOLOCNOSTI
```

```
Using configuration from /home/martin/vpn2/openvpn-2.1.1/easy-rsa/2.0/openssl.cnf
```

```
Check that the request matches the signature
```

```
Signature ok
```

```
The Subject's Distinguished Name is as follows
```

```
countryName          :PRINTABLE:'SR'
```

```
stateOrProvinceName  :PRINTABLE:'BA'
```

```
localityName         :PRINTABLE:'Bratislava'
```

```
organizationName     :PRINTABLE:'STUBA'
```

```
commonName           :PRINTABLE:'pfsense.local'
```

```
emailAddress         :IA5STRING:'nase.meno@domena.com'
```

```
Certificate is to be certified until Apr  3 08:37:07 2020 GMT (3650 days)
```

```
Sign the certificate? [y/n]:y
```

```
1 out of 1 certificate requests certified, commit? [y/n]y
```

```
Write out database with 1 new entries
```

```
Data Base Updated
```

V ďalšom kroku vytvoríme takzvaný „**Diffie Helman**“ parameter.

```
./build-dh
```

Výstup:

```
Generating DH parameters, 1024 bit long safe prime, generator 2
```

```
This is going to take a long time
```

Dostávame sa k tvorbe certifikátov pre klientov. Vytvoríme ich spustením nasledovných skriptov:

```
./build-key client1
```

```
./build-key client2
```

```
./build-key client3
```

Opäť odpovieme na všetky výzvy kladne a zadáme potrebné parametre.

Takto môžeme vytvoriť toľko klientov koľko potrebujeme. K tvorbe klientov sa môžeme opätovne vrátiť kedykoľvek budeme potrebovať vytvoriť ďalšieho klienta. Stačí spustiť príkaz „./build-key client_meno“. Musíme mať však na pamäti, že všetky certifikáty a kľúče, ktoré sme predtým vytvárali, musia byť v spoločnom adresári, aby všetko fungovalo ako má. Preto si vždy zálohujeme adresár so všetkými certifikátmi a kľúčmi, aby sme ich potom nemuseli vytvárať všetky odznova.

Teraz máme všetky certifikáty a kľúče v novovytvorenom podadresári „**keys/**“. Pre lepšie pochopenie jednotlivých certifikátov si uvedieme nasledovnú tabuľku:

Tabuľka č. 2

Názov súboru	Potrebný pre	Účel	Tajný
ca.crt	server + všetci klienti	Root CA certifikát	Nie
ca.key	len server	Root CA kľúč	Áno
dh{n}.pem	len server	Diffie Hellman parametre	Nie
server.crt	len server	Server certifikát	Nie
server.key	len server	Server kľúč	Áno
client1.crt	len klient1	Klient1 certifikát	Nie
client1.key	len klient1	Klient1 kľúč	Áno
client2.crt	len klient2	Klient2 certifikát	Nie
client2.key	len klient2	Klient2 kľúč	Áno
client3.crt	len klient3	Klient3 certifikát	Nie
client3.key	len klient3	Klient3 kľúč	Áno

3.3 Nastavenie OpenVPN servera pre vzdialených klientov

Náš server sme nastavili pre takzvaný „**Road Warrior**“ mód, čo v prenesenom význame predstavuje vzdialených klientov. Na serveri sme si v hlavnom menu zvolili VPN a odtiaľ možnosť OpenVPN. Pre server sme pridali nové pravidlo.

System	Interfaces	Firewall	Services	VPN	Status	Diagnostics
OpenVPN: Server: Edit						
Server Client Client-specific configuration						
Disable this tunnel		<input type="checkbox"/> This allows you to disable this tunnel without removing it from the list.				
Protocol		TCP The protocol to be used for the VPN.				
Dynamic IP		<input checked="" type="checkbox"/> Assume dynamic IPs, so that DHCP clients can connect.				
Local port		1194 The port OpenVPN will listen on. You generally want 1194 here.				
Address pool		10.10.1.0/24 This is the address pool to be assigned to the clients. Expressed as a CIDR range (eg. 10.0.8.0/24). If the 'Use static IPs' field isn't set, clients will be assigned addresses from this pool. Otherwise, this will be used to set the local interface's IP.				
Use static IPs		<input type="checkbox"/> If this option is set, IPs won't be assigned to clients. Instead, the server will use static IPs on its side, and the clients are expected to use this same value in the 'Address pool' field.				
Local network		147.175.79.160/27 This is the network that will be accessible from the remote endpoint. Expressed as a CIDR range. You may leave this blank if you don't want to add a route to the local network through this tunnel on the remote machine. This is generally set to your LAN network.				
Remote network		 This is a network that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a CIDR range. If this is a site-to-site VPN, enter here the remote LAN here. You may leave this blank if you don't want a site-to-site VPN.				
Client-to-client VPN		<input checked="" type="checkbox"/> If this option is set, clients will be able to talk to each other. Otherwise, they will only be able to talk to the server.				
Cryptography		BF-CBC (128-bit) Here you can choose the cryptography algorithm to be used.				
Authentication method		PKI (Public Key Infrastructure) The authentication method to be used.				

Obr.č 14: Nastavenie OpenVPN servera

Protokol sme nastavili na TCP, pretože hoci je UDP rýchlejší je známe, že pre niektoré routre dochádza pri ňom k zlému filtrovaniu dát. TCP protokol je pomalší, ale pre nás bezpečnejší. Ďalej sme zvolili možnosť „**Dynamic IP**“. Klienti sa tak budú môcť priamo pripájať na náš server, ktorý im bude dynamicky pridelovať IP adresy. Táto možnosť je typická pre „**Road Warrior**“ konfiguráciu. „**Address pool**“ je rozsah adries, ktoré budú dynamicky pridelované prihlasujúcim sa klientom. Tento rozsah musí byť nezávislá podsieť, ktorú sme nepoužili

nikde inde. V našom prípade sme pre klientov použili privátne IP adresy a rozsah podsiete bol 10.10.1.0/24. Pre túto podsieť s netmaskou 255.255.255.0 bolo dostupných 255 IP adries, kde prvá z rozsahu bola brána pre túto podsieť a posledná broadcast. Do okna „**Local network**“ sme vložili rozsah pre našu lokálnu sieť, pretože sme chceli aby sa OpenVPN klienti mohli dostať na systémy v lokálnej sieti. Autentifikačnú metódu sme zvolili PKI.

CA certificate	<pre>-----BEGIN CERTIFICATE----- MIIDaTCCAtKgAwIBAgIJANZDZLAGJi43MA0GCSqG SIb3DQEBBQUAMIGAMQswCQYD VQQGEwJlUjELMAkGA1UECBMkExEzARBgNVBAcT CkYyYXRpc2xhdmExDDAKBgNV BAoTA1NUVTEwMBQGA1UEAxMNcGZzZW5zSS5sb2Nh bDEpMCcGCsQGSib3DQEQJARYa c3RydWhhcnR5YXJ0aW44NUBnbWVpC5jb20wHhcN MTAwMzAxMTAzMTAzWhcNMjAw </pre> <p>Paste your CA certificate in X.509 format here.</p>
Server certificate	<pre>-----BEGIN CERTIFICATE----- MIIDyzCCAzSgAwIBAgIBATANBgkqhkiG9w0BAQUF ADCBgDELMAkGA1UEBhMCUlx CzAJBgNVBAGTAkJBMRMEQYDVQQHEwpmF0aXNs YXZhMmQwCgYDVQQKEwNTVFUx FjAUBgNVBAMTDXBmc2Vuc2UubG9jYXVwKTAnBgkq hkiG9w0BCQEWGnN0cnVoYXJ0aW44NUBnbWVpC5jb20wHhcN bWVpC5jb20wHhcN MzQOMVoXDTIwMDIyNzEwMzQ0 </pre> <p>Paste your server certificate in X.509 format here.</p>
Server key	<pre>-----BEGIN RSA PRIVATE KEY----- MIICXgIBAAKBgQCcjicsxjcv16HBjjfsL0laQZqG fg/BIOAz9dyoh+1H3r3tKs9J O3MgDPZTm4pwhA703t08xhuuQDAFbQxt9ZgVs jZK eLNASsiu+VMH6V3KI f77CRqp 9k+U1MJOP5wFwn t pL2Z3vixQtgHcqMLoAVzrttzk /F+59eeiLFmG6B lqvQIDAQAB AoGATmGto3EqKz lmt y2pOgsEw2eNIkEDSk0H5Xv3 GjnTxuPyW0fPuG6XWTikK3/4 </pre> <p>Paste your server key in RSA format here.</p>
DH parameters	<pre>-----BEGIN DH PARAMETERS----- MIGHAoGBALVY05Cl53g8G2ECwSn/vyExj5QDAIxxi EJq9/i7KYB9cFexGBR0iX2 V0lkIIjg0Jn7v/4B4xsiZ9Y07T+fF8lm7KAR0QqYwI Q9MRCHGe4+XWEY/n9qf+n aE2TIfmkG+Uo jKaD6TRTpRUMXEnuGeSLtWSmyED5qF OTpl7ie+PLAgEC -----END DH PARAMETERS----- </pre> <p>Paste your Diffie Hellman parameters in PEM format here.</p>

Obr.č 15: Vkládanie certifikátov pre server

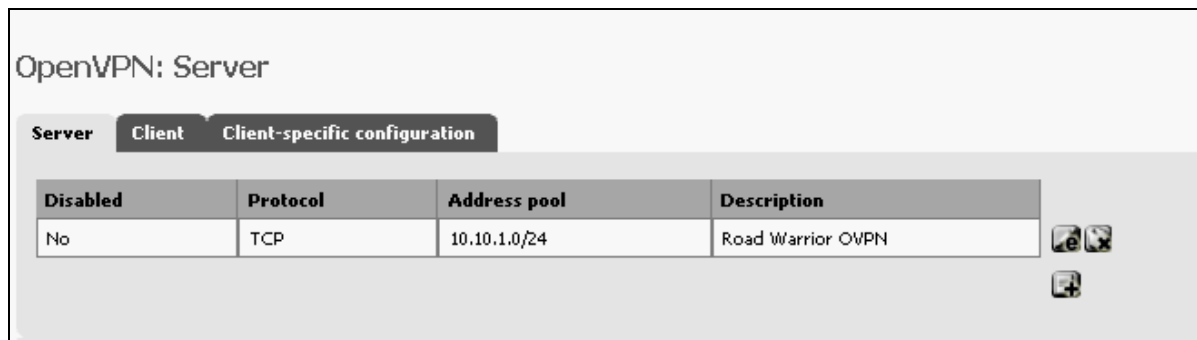
V ďalšom kroku nasleduje vkladanie jednotlivých certifikátov pre server ako to vidíme na Obr.č: 15. Tieto certifikáty si otvoríme v niektorom zo známych editorov a obsah týchto súborov skopírujeme do určených okien vo web konfiguratore nášho servera. Pre možnosť DHCP pridelenia DNS serverov vložíme naše DNS servery 147.175.64.7 a 147.175.1.11. Ďalej aktivujeme LZO kompresiu a do okna pre „**Custom options**“ vložíme direktívu

„push "redirect-gateway def1" “. Táto direktíva znamená, že smerovanie bude priamo posielané na našu defaultnú bránu do internetu a to je v našom prípade IP adresa nášho firewallu, 147.175.79.135. Pod touto IP adresou budú aj navonok vystupovať OpenVPN klienti pripojení k serveru.

DHCP-Opt.: DNS-Server	<input type="text" value="147.175.64.7;147.175.1"/> Set domain name server addresses, separated by semi-colons (;).
DHCP-Opt.: WINS-Server	<input type="text"/> Set WINS server addresses (NetBIOS over TCP/IP Name Server), separated by semi-colons (;).
DHCP-Opt.: NBDD-Server	<input type="text"/> Set NBDD server addresses (NetBIOS over TCP/IP Datagram Distribution Server), separated by semi-colons (;).
DHCP-Opt.: NTP-Server	<input type="text"/> Set NTP server addresses (Network Time Protocol), separated by semi-colons (;).
DHCP-Opt.: NetBIOS node type	<input type="button" value="none"/> Set NetBIOS over TCP/IP Node type. Possible options: b-node (broadcasts), p-node (point-to-point name queries to a WINS server), m-node (broadcast then query name server), and h-node (query name server, then broadcast).
DHCP-Opt.: NetBIOS Scope	<input type="text"/> Set NetBIOS over TCP/IP Scope. A NetBIOS Scope ID provides an extended naming service for NetBIOS over TCP/IP. The NetBIOS scope ID isolates NetBIOS traffic on a single network to only those nodes with the same NetBIOS scope ID.
DHCP-Opt.: Disable NetBIOS	<input type="checkbox"/> If this option is set, Netbios-over-TCP/IP will be disabled.
LZO compression	<input checked="" type="checkbox"/> Checking this will compress the packets using the LZO algorithm before sending them.
Custom options	<div><pre>push "redirect-gateway def1"</pre></div> You can put your own custom options here, separated by semi-colons (;). They'll be added to the server configuration.
Description	<input type="text" value="Road Warrior OVPN"/> You may enter a description here. This is optional and is not parsed.

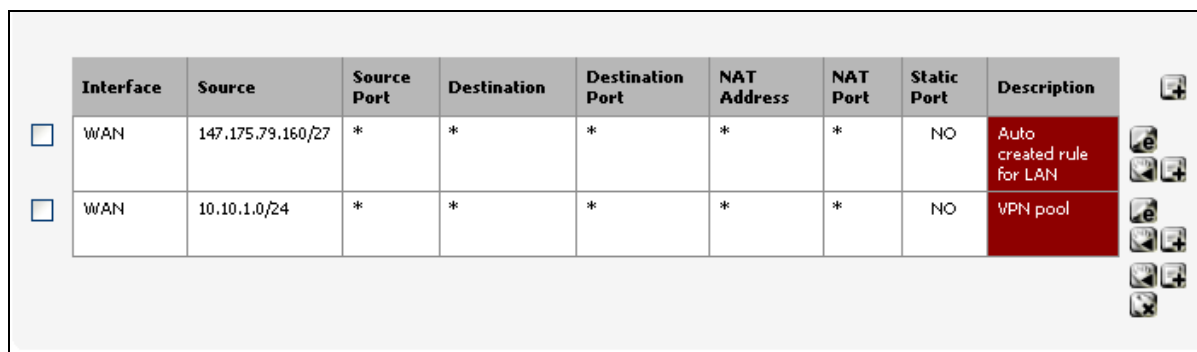
Obr.č 16 Nastavenie DNS serverov a presmerovania

Ako posledné , vložíme popis pre toto nastavenie a uložíme. Naše OpenVPN nastavenie servera potom vyzerá nasledovne.



Obr.č 17: Pravidlo pre OpenVPN server

Je ešte potrebné pridať pár pravidiel pre NAT smerovanie. V menu pre firewall zvolíme možnosť NAT. Tu vyberieme možnosť „**Outbound**“ a manuálne generovanie NAT pravidiel. Po uložení vidíme automaticky vytvorené pravidlo pre LAN a zvolíme možnosť pridať ďalšie pravidlo.



Obr.č 18: NAT pravidlá

V daný pravidlách zmeníme len možnosť „**Source**“, kde pre prvé pravidlo je zdrojom naša lokálna sieť a pre druhé zasa podsieť určená pre OpenVPN klientov.

3.4 Konfigurácia OpenVPN klienta pre Windows

Zo stránky projektu si stiahneme inštalačný balík klienta OpenVPN pre Windows. Spustíme inštaláciu a postupujeme podľa navigácie inštalačného menu. Po inštalácii klienta sa nám nainštalovalo nové sieťové zariadenie. Toto zariadenie má dlhý názov a je potrebné ho premenovať na kratšie a hlavne bez medzier. V našom prípade sme si ho nazvali „**ovpn**“.



Obr.č 19: Nové sieťové zariadenie

V ďalšom kroku potrebujeme vytvoriť konfiguračný súbor klienta. Najskôr sa nastavíme do adresára, v ktorom máme nainštalovaného OpenVPN klienta v našom prípade „**C:\Program Files\OpenVPN**“ a následne do adresára „**config**“. Tu vytvoríme textový súbor a nazveme si ho ľubovoľne podľa toho, ako chceme popísať náš vytváraný tunel. Musíme mu však dať koncovku „**.ovpn**“.

Otvoríme tento súbor a vložíme do neho nasledovné parametre:

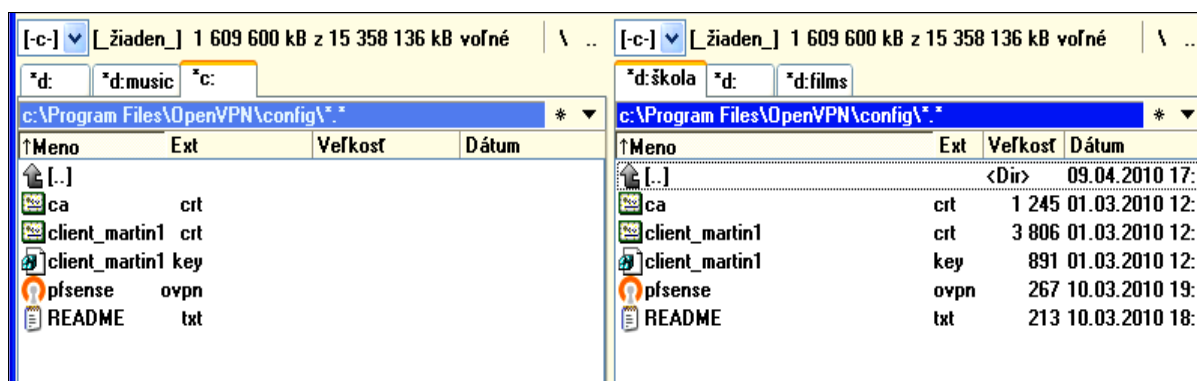
```
tls-client
float
port 1194
dev tun
dev-node ovpn
proto tcp-client
remote 147.175.79.135 1194
resolv-retry infinite
nobind
ping 10
persist-tun
persist-key
ca ca.crt
cert client_martin1.crt
```

```

key client_martin1.key
ns-cert-type server
cipher BF-CBC
keysize 128
comp-lzo # to enable LZO remove the #
pull
verb 4

```

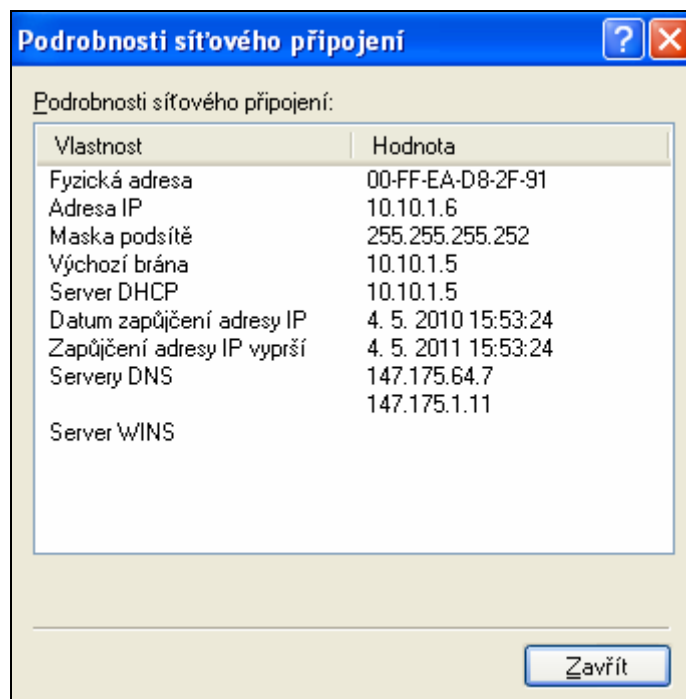
Dané parametre popisujú dôležité údaje, ako na aký port sa daný klient bude prihlasovať alebo o aké virtuálne sieťové zariadenie ide. Parameter „**dev-node**“ popisuje názov nášho sieťového zariadenia, ktoré sme si predtým premenovali. Ďalší parameter popisuje o aký komunikačný protokol ide a parameter „**remote**“ predstavuje IP adresu nášho servera a port na akom počúva. Do parametrov „**ca**“, „**cert**“, „**key**“ vložíme názvy našich vytvorených certifikátov. Parameter „**ns-cert-type server**“ má bezpečnostnú funkciu. Má zaistiť klientom, že sa prihlasujú k správne serveru. „**cipher BF-CBC**“ je parameter, ktorý hovorí o kryptovacej metóde. Rovnaký parameter musí byť nastavený na strane servera i klienta. Pre povolenie LZO kompresie sme odstránili poznámku pre daný riadok, aby sme mali rovnaké nastavenie ako máme na serveri. Po vložení parametrov uložíme náš konfiguračný súbor. Teraz potrebujeme bezpečnou cestou skopírovať do rovnakého adresára všetky potrebné certifikáty.



Obr.č 20: Obsah konfiguračného adresára

Teraz nám zostáva už len otestovať funkčnosť nášho vytváraného tunela. Súčasťou inštaláčného balíka je aj OpenVPN GUI . Po inštalácii ho spustíme a na paneli nástrojov sa nám zobrazí ikona OpenVPN GUI, ktorá je červenej farby, čo signalizuje, že spojenie nie je nadviazané . Pravým tlačítkom naň klikneme a zvolíme možnosť pripojiť. Ak sme všetko

urobili správne tak nám náš server prideli IP adresu z určeného rozsahu. Spojenie je nadviazané a ikona na paneli nástrojov zmení farbu na zelenú.



Obr.č 21: Informácie o pripojení sieťového zariadenia ovpn

Náš server by mal v systémových záznamoch pre OpenVPN vypísať nasledovné riadky:

```
Apr 10 12:20:31 openvpn[24093]:Initialization Sequence Completed
Apr 10 12:20:31 openvpn[24093]:TCP connection established with xxx.xxx.xxx.xxx:1177
Apr 10 12:20:31 openvpn[24093]: TCPv4_SERVER link local:[undef]
Apr 10 12:20:31 openvpn[24093]: TCPv4_SERVER link remote: xxx.xxx.xxx.xxx:1177
Apr 10 12:20:31 openvpn[24093]: [client_martin1]Peer Connection Initiated with
xxx.xxx.xxx.xxx:1177
```

Kde „xxx” predstavuje IP adresu nášho klienta, z ktorej sa prihlasuje.

Teraz už máme vytvorený bezpečný tunel medzi našim serverom a klientom. Ako sme mali možnosť vidieť, klient rovnako ako aj server využíva pre svoje sieťové zariadenie vždy dve IP adresy z daného rozsahu. Jedna IP adresa je priamo pridelená konkrétnemu virtuálnemu sieťovému zariadeniu a druhá je využívaná „**Point-to-Point**“ protokolom. Tento protokol je komunikačný protokol sieťovej vrstvy a používa sa pre priame spojenie dvoch sieťových uzlov. Umožňuje autentifikáciu, šifrovanie a kompresiu. Ďalej tiež dynamické nastavovanie klienta alebo zabezpečenie pomocou hesla.

3.5 Konfigurácia OpenVPN klienta pre Ubuntu 9.10

Pomocou správcu balíčkov nainštalujeme potrebný OpenVPN balíček. Pri práci v termináli pre Ubuntu ako správca balíčkov slúži program „**apt-get**“. Inštaláciu vykonáme nasledovným príkazom:

```
$ sudo apt-get install openvpn
```

Tento inštalačný program vykoná potrebné operácie pre nainštalovanie aktuálnej verzie OpenVPN. Teraz potrebujeme vytvoriť konfiguračný súbor na základe ktorého sa bude nadväzovať spojenie medzi klientom a serverom. Tento súbor vytvoríme v adresári „**/etc/openvpn**“ a dáme mu koncovku „**conf**“.

Náš súbor sme si nazvali „**openvpn.conf**“. Do tohto súboru vložíme nasledovné parametre:

```
dev tun
tls-client
float
port 1194
proto tcp-client
remote 147.175.79.135 1194
resolv-retry infinite
nobind
ping 10
user nobody
group nogroup
persist-key
persist-tun
ca ca.crt
cert client_martin2.crt
key client_martin2.key
ns-cert-type server
cipher BF-CBC
keysize 128
comp-lzo
pull
verb 4
```

Kde prvý parameter popisuje, že sa jedná o virtuálne sieťové zariadenie „**tun**“, ďalší hovorí o tom, že sa jedná o klienta. Parameter „**remote**“ nesie rovnaké informácie ako pri konfigurácii klienta pre Windows.

Potom ako máme vytvorený náš konfiguračný súbor, potrebujeme do rovnakého adresára vložiť potrebné certifikáty a to „ca.crt“, „client_martin2.crt“ a „client_martin2.key“.

Chceli sme aby sa náš klient pripájal automaticky po štarte systému respektíve po pripojení k sieti. V adresári „/etc/default“ sme v súbore openvpn zapoznámkovali všetky riadky a na koniec súboru sme jeden pridali nasledovne:

```
# This is the configuration file for /etc/init.d/openvpn
#
# Start only these VPNs automatically via init script.
# Allowed values are "all", "none" or space separated list of
# names of the VPNs. If empty, "all" is assumed.
#
#AUTOSTART="all"
#AUTOSTART="none"
#AUTOSTART="home office"
#
# Refresh interval (in seconds) of default status files
# located in /var/run/openvpn.$NAME.status
# Defaults to 10, 0 disables status file generation
#
#STATUSREFRESH=10
#STATUSREFRESH=0
# Optional arguments to openvpn's command line
#OPTARGS=" "
AUTOSTART="openvpn"
```

Tento príkaz hovorí, ktorý konfiguračný súbor bude použitý pri štarte. Teraz nám stačí nášho klienta spustiť príkazom:

```
$ sudo service openvpn start
```

Výstup:

```
* Starting virtual private network daemon(s)...
* Autostarting VPN 'openvpn' [ OK ]
```

Po spustení nášho klienta si overíme či bolo nadviazané spojenie a či náš klient funguje správne. Konfiguráciu sieťových rozhraní zobrazíme nasledovným príkazom:

```
$ ifconfig
```

Výstup:

```
eth0      Link encap:Ethernet  HWaddr 00:1b:38:3d:83:e0
          inet addr:147.175.220.49  Bcast:147.175.220.255
Mask:255.255.255.0
          inet6 addr: fe80::21b:38ff:fe3d:83e0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5939 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3172 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2453626 (2.4 MB)  TX bytes:474020 (474.0 KB)
          Interrupt:27 Base address:0xc000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:20 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1584 (1.5 KB)  TX bytes:1584 (1.5 KB)

tun0      Link encap:UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
Mask:255.255.255.255
          inet addr:10.10.1.6 P-t-P:10.10.1.5
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Vidíme že máme vytvorené virtuálne sieťové zariadenie „**tun0**“. Náš server mu pridelil IP adresu 10.10.1.6 . Ďalšia IP adresa 10.10.1.5 je využívaná už spomínaným „**Point-to-Point**“ protokolom.

3.6 Konfigurácia OpenVPN klienta pre Mandriva 2010.0

Ako prvé si nainštalujeme OpenVPN klienta pomocou správcu balíčkov. V tomto prípade to za nás pri práci v termináli vykoná program „urpmi“. Inštaláciu vykonáme príkazom :

```
# urpmi openvpn
```

Tento program zabezpečí, aby sa nainštalovala aktuálna verzia programu OpenVPN a ak sú potrebné knižnice a zásuvné moduly pre správnu funkčnosť tohto programu, tak ich za nás doinštaluje.

Ak máme inštaláciu úspešne vykonanú, nastavíme sa do adresára /etc/openvpn/. Sem skopírujeme naše certifikáty pre tretieho klienta „ca.crt“, „client3.crt“, „client3.key“. Do toho istého adresára skopírujeme prednastavený konfiguračný súbor, ktorý priamo obsahuje inštalovaná verzia OpenVPN.

```
# cp /usr/share/openvpn/sample-config-files/client.conf /etc/openvpn/
```

Keď máme tento súbor skopírovaný do nášho adresára, otvoríme si ho v ľubovoľnom editore a zmeníme v ňom niektoré parametre.

```
;dev tap  
dev tun
```

Virtuálne sieťové zariadenie tap bodkočiarkou zapoznámkujeme a tun zasa naopak odpoznamkujeme. Takto zmeníme aj ďalšie parametre, ktoré potrebujeme.

```
proto tcp  
;proto udp
```

Do parametra remote vložíme IP adresu nášho servera a zmeníme port, na ktorom počúva prihlasovaných klientov.

```
remote 147.175.79.135 1194
```

Ďalej odpoznamkujeme nasledovné parametre:

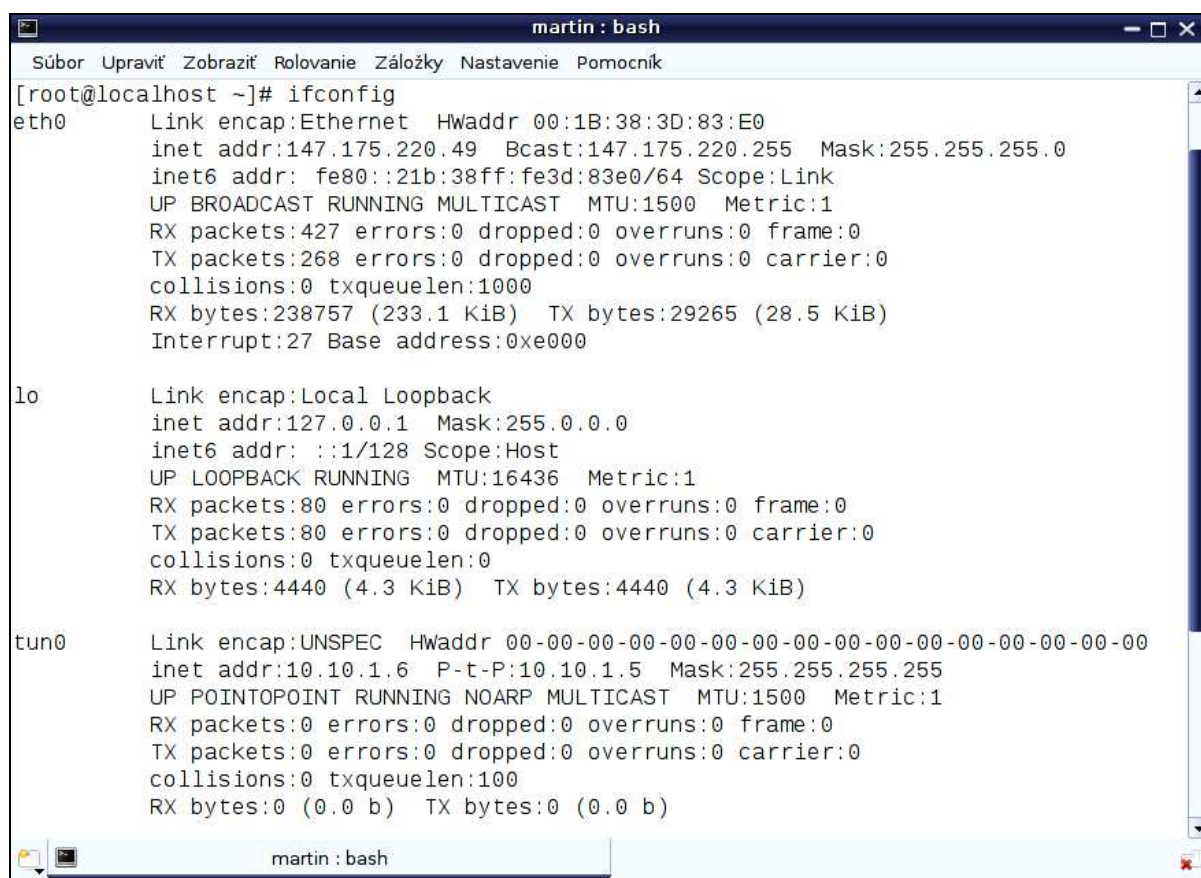
```
user nobody  
group nogroup
```

Do parametrov „ca.crt“, „client.crt“ a „client.key“ vložíme názvy našich certifikátov. Ostatné parametre sú prednastavené štandardne a nič v nich nemeníme.

Teraz nám stačí nasledovným príkazom spustiť OpenVPN a ak je všetko správne nakonfigurované mal by sa vytvoriť tunel medzi klientom a serverom.

```
# service openvpn start
```

Ak sa klient úspešne spustil, zavoláme príkaz „ifconfig“ a zobrazí sa nám tabuľka sieťových rozhraní.



```
martin : bash
[root@localhost ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:1B:38:3D:83:E0
          inet addr:147.175.220.49  Bcast:147.175.220.255  Mask:255.255.255.0
          inet6 addr: fe80::21b:38ff:fe3d:83e0/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:427 errors:0 dropped:0 overruns:0 frame:0
          TX packets:268 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:238757 (233.1 KiB)  TX bytes:29265 (28.5 KiB)
          Interrupt:27 Base address:0xe000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:80 errors:0 dropped:0 overruns:0 frame:0
          TX packets:80 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:4440 (4.3 KiB)  TX bytes:4440 (4.3 KiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.10.1.6  P-t-P:10.10.1.5  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```

Obr.č 22: Tabuľka sieťových zariadení

Na obrázku č. 20 vidíme novovytvorené virtuálne zariadenie „tun0“, ktorému náš server priradil IP adresu 10.10.1.6. IP adresa 10.10.1.5 slúži pre „point-to-point“ protokol.

Náš server nám v systémových výpisoch pre OpenVPN zaznamenal, pripájanie sa klienta.

Apr 15 10:40:41	openvpn[63627]: Re-using SSL/TLS context
Apr 15 10:40:41	openvpn[63627]: LZO compression initialized
Apr 15 10:40:41	openvpn[63627]: TCP connection established with 147.175.79.162:44893
Apr 15 10:40:41	openvpn[63627]: TCPv4_SERVER link local: [undef]
Apr 15 10:40:41	openvpn[63627]: TCPv4_SERVER link remote: 147.175.79.162:44893
Apr 15 10:40:42	openvpn[63627]: 147.175.79.162:44893 [client2] Peer Connection Initiated with 147.175.79.162:44893

Clear log

Obr.č 23: Systémové výpisy servera

Z predchádzajúceho obrázka vidíme, že spojenie bolo nadviazané a server komunikuje s daným klientom.

Pre overenie či náš virtuálny tunel naozaj funguje sme sa pokúsili najskôr pingnúť IP adresu stroja v lokálnej sieti, čo bolo úspešné. Následne sme na firewall vypli pravidlá povoľujúce ssh prístup na lokálny stroj. Potom sme sa pokúsili prostredníctvom nášho klienta dostať cez ssh na počítač v lokálnej sieti. Toto sa nám úspešne podarilo.

3.7 Odstránenie klienta

Občas sa môžu vyskytnúť situácie, keď budeme chcieť niektorému z klientov zamedziť prístup do našej siete. Takouto situáciou je napríklad ak niektorý študent ukončí štúdium a chceme, aby sa viac nemohol pomocou svojich certifikátov prihlasovať na náš server, keďže prestáva byť študentom. Toto uskutočníme pomocou pár nasledovných príkazov.

Na stroji, na ktorom sme vytvárali certifikáty, sa nastavíme do príslušného adresára „**openvpn-2.1.1/easy-rsa/2.0/**“ a tu spustíme nasledovné skripty:

```
source ./vars
./revoke-full client2
```

Výstup:

```
Using configuration from /etc/openvpn/2.0/openssl.cnf
Adding Entry with serial number 03 to DB for
/C=SR/ST=BA/L=Bratislava/O=STU/CN=client2/emailAddress=struhar.martin85@gmail.com
Revoking Certificate 03.
```

```
Data Base Updated
Using configuration from /etc/openvpn/2.0/openssl.cnf
client2.crt:
/C=SR/ST=BA/L=Bratislava/O=STU/CN=client2/emailAddress=struhar.martin85@gmail.com
error 23 at 0 depth lookup:certificate revoked
```

Kde „**client2**“ predstavuje klienta, ktorému chceme zamedziť prístup. Hlásenie „error 23“ poukazuje na to, že zrušenie certifikátov bolo úspešné. Po vykonaní týchto príkazov sa nám vytvoril v adresári s kľúčmi a certifikátmi „**keys/**“ nový súbor „**crl.pem**“. Daný súbor si otvoríme v editore a skopírujeme jeho obsah do okna „**CRL**“ určeného pre tento súbor vo web konfiguratore nášho servera. Toto okno sa nachádza v menu OpenVPN vo vytvorenom pravidle pre server.

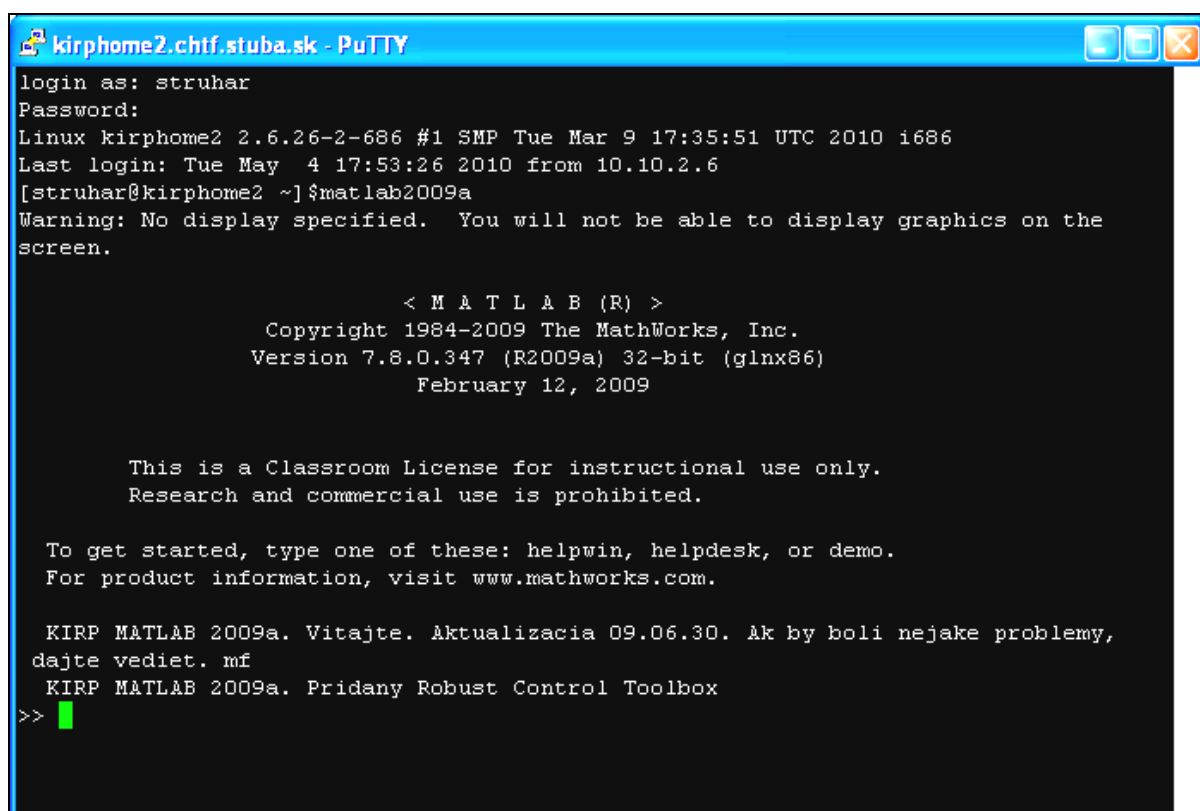
DH parameters	<pre>-----BEGIN DH PARAMETERS----- MIghAoGBALVY05Cl53g8G2ECWwSn/vyExj5QDAIxxi EJq9/i7KYB9cFexGBR0iX2 V0lkIIjg0Jn7v/4B4xsiZ9Y07T+fF8lm7KAR0QqYwI Q9MRCHGe4+XWEY/n9qf+nC aE2TIfmkG+Uo jKaD6TRTpRumXEnuGeSLtWSmyED5qF OTpl7ie+PLAgEC -----END DH PARAMETERS-----</pre> <p>Paste your Diffie Hellman parameters in PEM format here.</p>
CRL	<pre>-----BEGIN X509 CRL----- MIIBXDCBxjANBgqhkiG9w0BAQFADCBgDELMakG A1UEBhMCU1IxCzAJBgNVBAGT AkJBMRMwEQYDQHQHEwCcmF0aXNsYXZhMQwwCgYD VQKKEwNTVFUxYjAUBgNVBAMT DXBmc2Vuc2UubG9jYXVwKTANBgqhkiG9w0BCQEW GnN0cnVoYXludWFydGluODVA Z21haWwvY29tFw0xMDA1MDkwOTM4NDZaFw0xMDA2 MDgwOTM4NDZaMBQwEgIBAxN</pre> <p>Paste your certificate revocation list (CRL) in PEM format here (optional).</p>
DHCP-Opt.: DNS-Domainname	<input type="text"/> <p>Set connection-specific DNS Suffix.</p>
DHCP-Opt.: DNS-Server	<input type="text" value="147.175.64.7;147.175.1.11"/> <p>Set domain name server addresses, separated by semi-colons (;).</p>

Obr.č 24: Vkladanie súboru *crl.pem*

Tento súbor obsahuje zoznam všetkých zamietnutých certifikátov. Po vložení tohto súboru je potrebné náš server reštartovať. Týmto sa zamietnutý klient nebude môcť viac prihlásiť na náš server.

3.8 Testovanie na ústavnej sieti

Na základe spracovaného návodu sme vytvorili certifikáty pre ústavný server a pre klientov. Keďže firewall na ústavnej sieti je rovnako ako v našej testovacej sieti pfSense, vykonali sme rovnaké nastavenia. Pripojenie klienta na server bolo úspešné. Bolo možné sa prostredníctvom ssh prístupu prihlásiť na server kirphome2, ktorý je prístupný len z ústavnej siete. Na kirphome2 sme si spustili licencovaný Matlab 2009a a mohli sme na ňom pracovať vzdialene bez toho, aby sme boli priamo na počítači v ústavnej sieti.



```
kirphome2.chtf.stuba.sk - PuTTY
login as: struhar
Password:
Linux kirphome2 2.6.26-2-686 #1 SMP Tue Mar 9 17:35:51 UTC 2010 i686
Last login: Tue May  4 17:53:26 2010 from 10.10.2.6
[struhar@kirphome2 ~]$matlab2009a
Warning: No display specified.  You will not be able to display graphics on the
screen.

      < M A T L A B (R) >
      Copyright 1984-2009 The MathWorks, Inc.
      Version 7.8.0.347 (R2009a) 32-bit (glnx86)
      February 12, 2009

      This is a Classroom License for instructional use only.
      Research and commercial use is prohibited.

      To get started, type one of these: helpwin, helpdesk, or demo.
      For product information, visit www.mathworks.com.

      KIRP MATLAB 2009a. Vitajte. Aktualizacia 09.06.30. Ak by boli nejaké problémy,
      dajte vedieť. mf
      KIRP MATLAB 2009a. Pridaný Robust Control Toolbox
      >>
```

Obr.č 25: Matlab2009a na kirphome2

4 ZÁVER

V teoretickej časti bolo úlohou našej práce oboznámiť čitateľa so súčasnými sieťami. Konkrétnejšie sme sa zaoberali problematikou virtuálnych privátnych sietí. Pre našu prácu sme si vybrali projekt OpenVPN. Ide o open source projekt, ktorý je všestranný svojím využitím pre rôzne platformy. Zaoberali sme sa princípom tvorby certifikátov a kľúčov pomocou tohto projektu. Kľúče a certifikáty sú nevyhnutné pre typ konfigurácie vzdialených klientov (Road warrior konfigurácia). Keďže sme pracovali na testovacej sieti, ktorú sme potrebovali zabezpečiť, museli sme sa oboznámiť s teóriou zabezpečenia sietí pomocou firewallov.

V praktickej časti práce sme v prvom kroku vytvárali našu testovaciu sieť. Mali sme povolené používať IP adresy od 147.175.79.144 až 147.175.79.191. Pomocou nástroja IP Calculator sme si vypočítali rozsah našej lokálnej siete 147.175.79.160/27. IP adresa WAN rozhrania nášho firewallu a zároveň servera bola 147.175.79.135. Konfigurácie nášho servera sme uskutočňovali pomocou web konfigurátora. IP adresa LAN rozhrania bola 147.175.79.161, ktorá bola zároveň bránou do našej lokálnej siete. Túto adresu sme volali v prehliadači pre prácu s web konfigurátorom.

Potom ako sme nakonfigurovali firewall, sme začali vytvárať certifikáty a kľúče pre server a jednotlivých klientov. OpenVPN serverom bol v tomto prípade firewall pfSense. Klienti boli nakonfigurovaní pre rôzne platformy a to Windows, Mandriva 2010.0 a Ubuntu 9.10.

Po úspešnom nakonfigurovaní a nadviazaní spojenia klientov so serverom sme v poslednom kroku testovali naše konfigurácie na ústavnej sieti. Toto testovanie bolo úspešné a podarilo sa nám prostredníctvom VPN siete dostať na server kirphome2 a pracovať na licencovanom Matlabe 2009a.

5 ZOZNAM POUŽITEJ LITERATÚRY

- [1] *LMSC, LAN/MAN Standards Committee (Project 802)*, [on line], 8.5.2010. Dostupné z: < www.ieee802.org >
- [2] *Computer network*, [on line], 8.5.2010. Dostupné z: < http://en.wikipedia.org/wiki/Computer_network >
- [3] *OSI model*, [on line], 8.5.2010. Dostupné z: < www.topbits.com/osi-model.html >
- [4] *OSI model*, [on line], 8.5.2010. Dostupné z: < http://en.wikipedia.org/wiki/OSI_model >
- [5] *Virtual network*, [on line], 8.5.2010. Dostupné z: < http://en.wikipedia.org/wiki/Virtual_network >
- [6] *Virtuální privátní síť*, [on line], 8.5.2010. Dostupné z: < <http://owebu.blogger.cz/PC-site/Virtualni-privatni-sit-uvod-1-dil> >
- [7] *Virtuálne privátne siete*, [on line], 8.5.2010. Dostupné z: <<http://www.swan.sk/swan/?id=46>>
- [8] *HowStuffWorks*, [on line], 8.5.2010. Dostupné z: < <http://computer.howstuffworks.com/vpn.htm> >
- [9] *StavímeVPN*, [on line], 8.5.2010. Dostupné z: < <http://www.root.cz/clanky/stavime-vpn-cipe/> >
- [10] *OpenVPN – VPN jednoduše*, [on line], 8.5.2010. Dostupné z: < www.root.cz/clanky/openvpn-vpn-jednoduse/ >
- [11] *OpenVPN – VPN jednoduše 2*, [on line], 8.5.2010. Dostupné z: < www.root.cz/clanky/openvpn-vpn-jednoduse-2/ >
- [12] *TUN/TAP*, [on line], 8.5.2010. Dostupné z: < <http://en.wikipedia.org/wiki/TUN/TAP> >
- [13] *VPN siete s OpenVPN (2)*, [on line], 8.5.2010. Dostupné z: < <http://www.jariq.sk/2008/10/20/vpn-siete-s-openvpn-2/> >
- [14] *Installing pfSense – PFSense Docs*, [on line], 8.5.2010. Dostupné z: < http://doc.pfsense.org/index.php/Installing_pfSense >
- [15] *IP Calculator / IP Subnetting*, [on line], 8.5.2010. Dostupné z: < <http://jodies.de/ipcalc> >
- [16] Gino Thomas.: *Pfsense and OpenVPN for new users. Edition 28.09.2006.*