|  |  |
| --- | --- |
| **ŽILINSKÁ UNIVERZITA V ŽILINE**  **FAKULTA RIADENIA A INFORMATIKYNázov fakultyNázov vysokej školy** | |
| **Android aplikácia na sledovanie polohy mobilného zariadeniaIMPLEMENTÁCIA FIREMNEJ SIETE** | |
|  | |
|  | |
| **2016** | **Andrej Hucík**  **Miroslav Kozák**  **Andrej Šišila** |

|  |  |
| --- | --- |
| Žilinská univerzita v ŽilineŽILINSKÁ UNIVERZITA V ŽILINE  Fakulta riadenia a informatikyFAKULTA RIADENIA A INFORMATIKY | |
| **Android aplikácia na sledovanie polohy mobilného zariadeniaIMPLEMENTÁCIA FIREMNEJ SIETE**  SIEŤOVÉ OPERAČNÉ SYSTÉMY | |
| Bakalárska prácaSEMESTRÁLNA PRÁCA | |
| Študijný program: | Informatika - stará akreditáciaAplikované sieťové inžinierstvo |
| Katedra: | Katedra informatikyKatedra informačných sietí |
| Vedúci bakalárskej práce: | doc. Ing. Michal Varga PhD.Ing. Pavel Segeč, PhD. |
| Skupina: | SOS3 (Utorok) |
| ŽilinaŽilina20162016 | **Andrej Hucík**  **Miroslav Kozák**  **Andrej Šišila** |

Obsah

[Obsah 2](#_Toc474849990)

[Zoznam ilustrácií 4](#_Toc474849991)

[Úvod 5](#_Toc474849992)

[1. Ciele práce 6](#_Toc474849993)

[2. Topológia siete 7](#_Toc474849994)

[3. Inštalácia a konfigurácia zariadení 8](#_Toc474849995)

[3.1. Vytvorenie novej Debian VM a jej nastavenie. 9](#_Toc474849996)

[3.1.1. Inštalácia Linux OS - Debian. 10](#_Toc474849997)

[3.1.2. Základná konfiguráciu systému. 10](#_Toc474849998)

[3.1.3. Skript pre automatické pridanie záznamov do iptables. 10](#_Toc474849999)

[3.1.4. Automatické spúšťanie vlastných skriptov pri štarte systému. 16](#_Toc474850000)

[3.2. VLAN 17](#_Toc474850001)

[3.3. DNS 18](#_Toc474850002)

[3.4. DHCP 21](#_Toc474850004)

[3.5. NTP 22](#_Toc474850005)

[3.6. Web server 25](#_Toc474850006)

[3.6.1. Inštalácia joomla 26](#_Toc474850007)

[3.6.2. Inštalácia mediawiki 27](#_Toc474850008)

[3.7. Poštový server 27](#_Toc474850009)

[4. WIndows 28](#_Toc474850010)

[4.1. DHCP 28](#_Toc474850011)

[4.2. DNS 28](#_Toc474850012)

[4.3. NTP 29](#_Toc474850013)

[4.4. NAT 29](#_Toc474850014)

[4.5. ISS- Internet Information Server 30](#_Toc474850015)

[4.6. Poštový server 32](#_Toc474850016)

[5. Záver 32](#_Toc474850017)

Zoznam ilustrácií

[Obrázok 1 – Fyzická a logická topológia 6](#_Toc474845502)

[Obrázok 2 – db.sos3.local 18](#_Toc474845503)

[Obrázok 3 – db.sos3.external 19](#_Toc474845504)

[Obrázok 4 – named.conf.options 19](#_Toc474845505)

[Obrázok 5 – Pohľady (Views) 20](#_Toc474845506)

[Obrázok 6 – dhcpd.conf 21](#_Toc474845507)

[Obrázok 7 – ntp.conf 22](#_Toc474845508)

[Obrázok 8 – Overenie NTP 22](#_Toc474845509)

[Obrázok 9 – Ďalšie overenie NTP 23](#_Toc474845510)

[Obrázok 10 – Kontrola NTP cez tcpdump 23](#_Toc474845511)

[Obrázok 11 – Kontrola NTP serverov 24](#_Toc474845512)

[Obrázok 12 – Wiki web stránka (konfigurácia) 25](#_Toc474845513)

[Obrázok 13 – Zoznam súborov dostupných webstránok 25](#_Toc474845514)

[Obrázok 14 – Pridávanie Remote Access role 28](#_Toc474845515)

[Obrázok 15 – Pridávanie IIS na Windows Server 2016 29](#_Toc474845516)

[Obrázok 16 – Predvolená stránka IIS webservera 30](#_Toc474845517)

Úvod

Základom každej firmy, či už malej, strednej alebo veľkej, je stabilná a bezpečná sieťová infraštruktúra.

V našej práci sa budeme zaoberať implementáciou a konfiguráciou menšej firemnej siete, ktorá bude pozostávať z jedného smerovača, jedného prepínača, dvoch serverových systémov a dvoch pracovných staníc. Potom na potrebných uzloch nastavíme potrebné služby, ktoré umožnia firme poskytovať služby pre vnútornú, ale aj vonkajšiu sieť.

1. Ciele práce

Hlavným cieľom našej práce je vytvorenie jednoduchej sieťovej infraštruktúry, ktorú bude možné nasadiť do podnikového prostredia. Vytvorenie a konfigurácia takejto siete si vyžadovalo splnenie nasledovných čiastkových cieľov:

* Inštalácia operačného systému na serverové systémy, pracovné stanice a smerovač, a ich následná základná konfigurácia
* DNS: Master/Slave riešenie s replikáciou a overením
* Podpora viacerých virtuálnych web serverov a s inštaláciou niektorej z web aplikácii typu CMS or Wiki
* Firewall na smerovači cez netfilter s NAT
* Firewall na server systémoch
* NTP čas pre firmu
* SSH prístup
* DHCP s prideľovaním IP adries
* Email

Služby bolo potrebné sprevádzkovať najprv na linuxovej distribúcií Debian 8.6.0 x64 Stable a potom aj na Windows Server 2016, preto je aj táto práca rozdelená na dve hlavné časti.

1. Topológia siete

Naša topológia siete pozostáva z firewallu ku ktorému je na jednom rozhraní pripojený prepínač ku ktorému su napojené dva servery a dva počítače. Na druhom rozhraní je Internet. Na linuxoch aj na windowsoch bola rovnaká topológia s výnimkou, že pri pracovaní s linuxom sa nachádzali počítače a servery v rozdielnych VLAN: Servery vo VLAN-e 10 a desktopy vo VLAN-e 20.

Keďže si Windows Server nerozumel s VLAN-ami, topológia siete sa líši v tom, že všetky koncové uzly sú v defaultnej VLAN-e.

192.168.0.0 /25 VLAN 10

192.168.0.128 /25 VLAN 20 DHCP

eth0

eth1

158.193.139.74

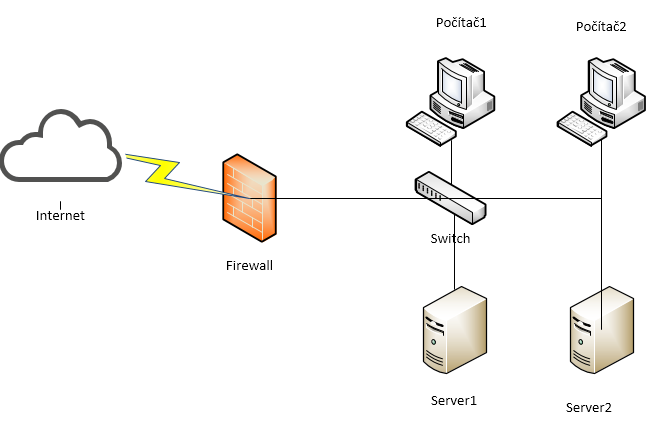
158.193.139.75

192.168.0.1

192.168.0.129

192.168.0.2

192.168.0.3



Obrázok – Fyzická a logická topológia

1. Inštalácia a konfigurácia zariadení

Vytvorenie virtuálnych strojov, inštalácia Debianu 8, konfigurácia firewallu, konfigurácia prepínača, konfigurácia serverov, konfigurácia desktopov

Nainštalovali sme funkčný Linux OS - Debian 8.6.0 stable, vykonali sme základnádnú konfigurácia nainštalovaného OS a nakonfigurovali sme funkčný firewall, ktorý spĺňa požiadavky zadania.

* 1. Vytvorenie novej Debian VM a jej nastavenie.

a. VM sme nazvali podľa zadania.

b. Študent prejde postupne jednotlivými nastaveniami, ktoré ponúka nástroj VB.

c. Pre jednotlivé VM sme správne nastavili sieťové adaptéry a virtualizačné parametre, napríklad PAE/NX a paravirtualizačné rozhranie v SYSTEM ACCELERATION.

d. Každej VM sme nastavili správny počet a funkčnosť sieťových adaptérov: 2 pre firewall, 1 pre servery a desktopy

e. Zdieľaný adresár sme na VM nepridávali.

* + 1. Inštalácia Linux OS - Debian.

a. Stiahli sme si obraz disku Debian 8 stable 64 bitovú verziu.

b. Obraz disku (iso súbor) sme pripojili k diskovej mechanike VM a spustili sme inštaláciu OS.

i. Hostname–každá VM má svoje meno odvodené od jej funkcie napr. všetky servery majú označenie „SX“ a desktopy „DX“, kde X je poradové číslo servera/desktopu.

ii.Domain – nastavili sme pridelenú doménu: sos3.local.

iii.Servery nemajú grafické rozhranie, iba textové. Desktopy majú nainštalované grafické rozhranie XFCE.

* + 1. Základná konfiguráciu systému.

Na virtuálne zariadenia sme si doinštalovali vim ako textový editor, ssh klienta aby sme mohli všetci pristupovať na všetky zariadenia, tcpdump na odchytávanie sieťovej prevádzky na riešenie problémov. Tiež sme nainštalovali bind9-host. Následne sme vyčistili cache. Doinštalovali sme si guestadditions pre uľahšenie práce s virtuálnymi zariadeniami. Pomocou fyzického prepínača sme prepojili klientov a serverry v stojane labáku. Na prepínači sme nastavili Rapid STP a VLAN pre servery a počítače. Vykonali sme základnú sieťovú konfiguráciu, kde sme nastavili statické IP adresy v súbore /etc/network/interfaces a povolili sme IP\_FORWARD. Po každom úspešnom kroku sme vytvorili SNAPSHOP, aby sme mali uchovaný stav funkčnej sieti.

* + 1. Skript pre automatické pridanie záznamov do iptables.

Náš firewall ktorý je pomenovaný ako fw je založený na kernelovom module netfilter.

Netfilter je framework obsiahnutý v jadre Linuxu od verzie 2.4.x, ktorý ponúka veľa možností pre filtrovanie paketov, preklad sieťových adries (NAT) alebo preklada sieťových portov (PAT). Netfilter nahrádza zastaraný modul ipchains v linuxovom jadre verzie 2.2. Iptables je user-space nástroj v Linuxe, ktory slúži na profesionálne nastavovanie pravidiel firewallov v jadre. Pravidlá firewallov ovplyvňovať prichádzajúce, odchádzajúce aj prechádzajúce pakety. Pravidlá sú v jadre spracovávaná niekoľkých netfilter modulmi.

Vytvorili sme skript s názvom firewall.sh ktorý slúži na automatické pridávanie záznamov do iptables. Nastavili sme premennú: **I=/sbin/iptables** . Nastavili sme práva tak , aby sme mohli daný skript spúšťať , prikazom **chmod 744 firewall.sh .** Následne sme mohli spúšťať skript manuálne a to : **./firewall.sh .**Vložené pravidlá cez iptables sa po reštarte systému stratia. Chceli sme, aby sa skript s pravidlami pre firewall spúšťal pri štarte operačného systému automaticky.Preto sme dopísali v **/etc/network/interfaces** pre daný interface riadok : **up /usr/sbin/firewall.sh.**

Hneď na začiatku skriptu sme vyčistili aktuálne tabuľky v iptables : **$I -F -t filter**a  
**$I -F -t nat**.

Pokračovali sme nastavením predvolenej politiky pre INPUT, FORWARD A OUTPUT .

**$I -P INPUT DROP-**input všetko zahadzuje **$I -P FORWARD DROP -** forward všetko zahadzuje

Pre output sme politiku nemenili , teda ostala defaultne accept (všetko povoľ). Ďalej sme povolili všetku prevádzku, ktorá prichádza na lo (loopback) rozhranie.

**$I -A INPUT -i lo -j ACCEPT**

Povolili sme všetky prichádzajúce ICMP správy a všetky prichádzajúce správy, ktoré sú súčasťou už existujúceho spojenia :

**$I -A INPUT -p icmp -j ACCEPT**🡪povoí pingy na FW

**$I -A FORWARD -i eth1 -o eth0 -p icmp -j ACCEPT🡪**povolipingy z vnútra siete von

**$I -A INPUT -i eth0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT** povolí pakety ktoré patria už existujúcemu spojeniu otvoreného z vnútornej siete.

Nastavili sme SSH prístup. Kam?

**$I -A INPUT -i eth1 -p tcp --sport 22 -j ACCEPT**

Doteraz sme využívali NAT maškarádu. Avšak je lepšie použiť SNAT/DNAT.

SNAT je nastavenie NAT prekladu z privátnej siete do vonkajšej/verejnej.

**$I -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 158.193.139.74**

Nakoniec sme vytvorili snapshot nášho plne funkčného firewallu uvedeného nižšie:

#!/bin/bash

I=/sbin/iptables

#vycisti povodne pravidla

$I -F -t filter

$I -F -t nat

#zakaz vsetko, co nie je vyslovene povolene

#$I -P INPUT DROP

#$I -P FORWARD DROP

$I -P INPUT ACCEPT

$I -P FORWARD ACCEPT

#povol loopback

$I -A INPUT -i lo -j ACCEPT

########## STAVOVY FIREWALL ##########

#FW CONNTRACK - nastav sledovanie aktivnych pripojeni inicializovanych z FW

#Co odide z firewallu, sa vrati na firewall

$I -A INPUT -i eth0 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

#VLAN CONNTRACK - aby sa nam vsetko z netu vratilo na VLANy

#Co odide z VLANiek, sa vrati do VLANiek

$I -A FORWARD -i eth0 -o eth1.10 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

$I -A FORWARD -i eth0 -o eth1.20 -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

########## SNAT ##########

$I -t nat -A POSTROUTING -o eth0 -j SNAT --to-source 158.193.139.74

#a co s druhou ipckou? treba na nu tiez prekladat? mozme pridat aj nat na druhu ip

########## VLAN ROUTING ############

#Povol routing medzi vlanami

$I -A FORWARD -i eth1.10 -o eth1.20 -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth1.10 -j ACCEPT

########## ICMP ############

#Povol pingy na fw

$I -A INPUT -p icmp -j ACCEPT

#Povol pingy z VLANiek von

$I -A FORWARD -i eth1.10 -o eth0 -p icmp -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth0 -p icmp -j ACCEPT

########## SSH ##########

#Povol SSH na firewall zvonku aj zvnutra

$I -A INPUT -p tcp --dport 22 -j ACCEPT

########## SSH ##########

#Povol SSH na firewall zvonku aj zvnutra

$I -A INPUT -p tcp --dport 22 -j ACCEPT

#Navrat SSH na FW

$I -A INPUT -i eth1.10 -p tcp --sport 22 -j ACCEPT

$I -A INPUT -i eth1.20 -p tcp --sport 22 -j ACCEPT

#Povol spatne SSH z vnutornej siete na FW

$I -A INPUT -i eth1.10 -p tcp --sport 22 -j ACCEPT

$I -A INPUT -i eth1.20 -p tcp --sport 22 -j ACCEPT

#S1 SSH zvonku dnu

$I -t nat -A PREROUTING -d 158.193.139.74 -p tcp --dport 3002 -j DNAT --to-destination 192.168.0.2:22

$I -A FORWARD -p tcp -d 192.168.0.2 --dport 22 -j ACCEPT

$I -A FORWARD -p tcp -s 192.168.0.2 --sport 22 -j ACCEPT

#S2 SSH zvonku dnu

$I -t nat -A PREROUTING -d 158.193.139.74 -p tcp --dport 3003 -j DNAT --to-destination 192.168.0.3:22

$I -A FORWARD -p tcp -d 192.168.0.3 --dport 22 -j ACCEPT

$I -A FORWARD -p tcp -s 192.168.0.3 --sport 22 -j ACCEPT

#S1 zvnutra von

$I -A FORWARD -d 192.168.0.2 -p tcp --dport 22 -j ACCEPT

$I -A FORWARD -s 192.168.0.2 -p tcp --sport 22 -j ACCEPT

#S2 zvnutra von

$I -A FORWARD -d 192.168.0.3 -p tcp --dport 22 -j ACCEPT

$I -A FORWARD -s 192.168.0.3 -p tcp --sport 22 -j ACCEPT

########## DNS ############

#Povol DNS na FW

$I -A INPUT -p udp --sport 53 -j ACCEPT

$I -A INPUT -p udp --dport 53 -j ACCEPT

#Povol DNS zvnutra von

$I -A FORWARD -i eth1.10 -o eth0 -p tcp --dport 53 -j ACCEPT

$I -A FORWARD -i eth1.10 -o eth0 -p udp --dport 53 -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth0 -p tcp --dport 53 -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth0 -p udp --dport 53 -j ACCEPT

#MASTER DNS (S1) lokalne

$I -A FORWARD -d 192.168.0.2 -p tcp --dport 53 -j ACCEPT

$I -A FORWARD -s 192.168.0.2 -p tcp --sport 53 -j ACCEPT

$I -A FORWARD -d 192.168.0.2 -p udp --dport 53 -j ACCEPT

$I -A FORWARD -s 192.168.0.2 -p udp --sport 53 -j ACCEPT

#SLAVE DNS (S2) lokalne

$I -A FORWARD -d 192.168.0.3 -p tcp --dport 53 -j ACCEPT

$I -A FORWARD -s 192.168.0.3 -p tcp --sport 53 -j ACCEPT

$I -A FORWARD -d 192.168.0.3 -p udp --dport 53 -j ACCEPT

#S1 DNS zvonku dnu

$I -t nat -A PREROUTING -d 158.193.139.74 -p tcp --dport 53 -j DNAT --to-destination 192.168.0.2

$I -t nat -A PREROUTING -d 158.193.139.74 -p udp --dport 53 -j DNAT --to-destination 192.168.0.2

#S2 DNS zvonku dnu

$I -t nat -A PREROUTING -d 158.193.139.75 -p tcp --dport 53 -j DNAT --to-destination 192.168.0.3

$I -t nat -A PREROUTING -d 158.193.139.75 -p udp --dport 53 -j DNAT --to-destination 192.168.0.3

#Povovl DNS zvoknu dnu

$I -A FORWARD -i eth0 -o eth1.10 -d 192.168.0.2 -p udp --dport 53 -j ACCEPT

$I -A FORWARD -i eth0 -o eth1.10 -d 192.168.0.3 -p udp --dport 53 -j ACCEPT

########## NTP ##########

#Povol NTP na FW

$I -A INPUT -p udp --sport 123 -j ACCEPT

#Povol pripojenia na NTP server

$I -A FORWARD -d 192.168.0.3 -i eth1.10 -p udp --sport 123 -j ACCEPT

#Povol NTP vnutri

$I -A FORWARD -d 192.168.0.3 -p udp --dport 123 -j ACCEPT

$I -A FORWARD -s 192.168.0.3 -p udp --sport 123 -j ACCEPT

#NTP DNAT - Povol NTP zvonku dnu

$I -t nat -A PREROUTING -d 158.193.139.74 -p udp --dport 123 -j DNAT --to-destination 192.168.0.3:123

$I -t nat -A PREROUTING -d 158.193.139.75 -p udp --dport 123 -j DNAT --to-destination 192.168.0.3:123

########## HTTP ##########

#Povol HTTP von

$I -A FORWARD -i eth1.10 -o eth0 -p tcp --dport 80 -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth0 -p tcp --dport 80 -j ACCEPT

#HTTP lokalne

$I -A FORWARD -d 192.168.0.2 -p tcp --dport 80 -j ACCEPT

$I -A FORWARD -s 192.168.0.2 -p tcp --sport 80 -j ACCEPT

#HTTP zvonku dnu

$I -t nat -A PREROUTING -d 158.193.139.74 -p tcp --dport 80 -j DNAT --to-destination 192.168.0.2

########## HTTPS ##########

#Povol HTTPS von

$I -A FORWARD -i eth1.10 -o eth0 -p tcp --dport 443 -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth0 -p tcp --dport 443 -j ACCEPT

#HTTPS lokalne

$I -A FORWARD -d 192.168.0.2 -p tcp --dport 443 -j ACCEPT

$I -A FORWARD -s 192.168.0.2 -p tcp --sport 443 -j ACCEPT

#HTTP zvonku dnu

$I -t nat -A PREROUTING -d 158.193.139.74 -p tcp --dport 443 -j DNAT --to-destination 192.168.0.2

########## FTP ##########

#Povol FTP von

$I -A FORWARD -i eth1.10 -o eth0 -p tcp --dport 20 -j ACCEPT

$I -A FORWARD -i eth1.10 -o eth0 -p tcp --dport 21 -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth0 -p tcp --dport 20 -j ACCEPT

$I -A FORWARD -i eth1.20 -o eth0 -p tcp --dport 21 -j ACCEPT

########## DHCP ##########

#Povol DHCP

#$I -I FORWARD -i eth1.10 -p udp --dport 67:68 --sport 67:68 -j ACCEPT

#$I -I FORWARD -i eth1.20 -p udp --dport 67:68 --sport 67:68 -j ACCEPT

########## SMTP ##########

$I -t nat -A PREROUTING -p tcp --dport 25 -j DNAT --to-destination 192.168.0.3:25

$I -A FORWARD -p tcp -d 192.168.0.3 --dport 25 -j ACCEPT

$I -A FORWARD -p tcp -s 192.168.0.3 --sport 25 -j ACCEPT

########## IMAP ##########

$I -A FORWARD -p tcp -d 192.168.0.3 --dport 143 -j ACCEPT

$I -A FORWARD -p tcp -s 192.168.0.3 --sport 143 -j ACCEPT

# Pridaj logovanie do /var/messages/kern.log kvoli debuggingu

$I -A INPUT -j LOG

$I -A FORWARD -j LOG

# Zapni Forwarding pre iptables (aby fungovali "FORWARD" prikazy)

echo 1 > /proc/sys/net/ipv4/ip\_forward

* + 1. Automatické spúšťanie vlastných skriptov pri štarte systému.

Chceme, aby sa skript s pravidlami pre firewall spúšťal pri štarte operačného systému s „root“ oprávneniami. Docielili sme to tým, že sme do súboru „/etc/network/interfaces“ pridali up absolútnu\_cestu\_bash\_skriptu. Skripty sa nachádzajú v adresári „/etc/skripty“.

Po otestovaní funkčnosti firewallu sme urobili snapshoty všetkých VM.

* 1. VLAN

Servery sú vo VLAN 10, desktopy vo VLAN 20. Smerovanie medzi VLANami je vykonávané na FW. Preto sme na FW museli nainštalovať balíčky „isc-dhcp-server“ a „vlan“ t.j. „apt-get installisc-dhcp-server vlan“. Potom sme editovali súbor „/etc/network/interfaces“ tak, že sme odstránili adresné informácie z vnútorného interfacu eth1, ale nechali sme „auto eth1“, aby sa port zapol (UP). Následne sme pridali subinterface eth1.10 pre VLAN 10 (servery) a eth1.20 pre VLAN 20 (desktopy). Adresný rozsah pre jednotlivé VLAN bola sieť 192.168.0.0/24 rozdelená na dve /25 siete: 192.168.0.0 - 192.168.0.127 pre VLAN 10 a 192.168.0.128 - 192.168.0.255 pre VLAN 20.

FW je DHCP relay server. Všetky DHCP požiadavky prepošle FW DHCP serveru, ktorý pridelí klientovi IP adresu a ďalšie nakonfigurované informácie. Týmto spôsobom je FW zodpovedný iba za filtrovanie premávky a server za služby poskytované na sieti.

IP adresa DHCP servera sa do konfiguračného súboru „/etc/default/isc-dhcp-relay“ DHCP relay agenta musí zadať BEZ úvodzoviek a musíme počúvať na obidvoch subinterfacocht.j. eth1.10 aj eth1.20.

* 1. DNS

Systém názvov domén alebo systém mien domén, alebo systém doménových mien (Domain Name System), skr. DNS, je systém, ktorý ukladá prístup k informácii o názve stroja (hostname) a názve domény v istej distribuovanej databáze v počítačových sieťach ako internet. Najdôležitejšie je, že poskytuje mechanizmus získania IP adresy pre každé meno stroja (lookup) a naopak (reverse), a uvádza poštové servery (MX záznam) akceptujúce poštu pre danú doménu.

DNS poskytuje na internete všeobecne dôležitú službu, pretože kým počítače a sieťový hardvér pracujú s IP adresami, ľudia si vo všeobecnosti ľahšie pamätajú mená strojov a domén pri použití napr. v URL a e-mailovej adrese (obzvlášť nepríjemné by to bolo pri IPv6 adrese). DNS tak tvorí prostredníka medzi potrebami človeka a softvéru.

V rámci našej doménovej zóny „sos3.local“ sme si museli nastaviť dva DNS servery: Master (S1) a Slave (S2). Slave zrkadlí hlavný DNS server a v prípade poruchy ho zastúpi. Keďže si Slave DNS server všetko stiahne z Master DNS servera, netreba ho primárne konfigurovať, ale stačí mu nastaviť „allow-transfer“ na privátnu IP Master DNS.

Na obidva servery sme nainštalovali DNS server a nástroje na overenie jeho funkčnosti príkazom „apt-get install bind9 bind9utils dnsutils“.

Master DNS serveru sme upravovali súbory „/etc/resolv.conf“ (konfigurácia adries DNS serverov), „/etc/bind/master/db.sos3.local“ (view-lokálny), „/etc/bind/master/db.sos3.external“ (view-verejný), „/etc/bind/named.conf.local“ (definovanie lokálnych a verejných DNS View). Obsah súboru „/etc/resolv.conf“ je uvedený nižšie.

domain sos3.local

nameserver 192.168.0.2

nameserver 192.168.0.3

V adresári „/etc/bind“ na S1 sme vytvorili adresár „master“, do ktorého sme ukladali zónové súbory pre DNS.

Viewy sme nastavovali na Master DNS serveri súbormi „/etc/bind/named.conf.local“, „/etc/bind/master/db.sos3.local“, „/etc/bind/master/db.sos3.external“. Pri dotazovaní na doménové meno nášho DNS zvnútra sa použijú privátne adersy DNS serverov zo súboru „/etc/bind/master/db.sos3.local“. Pri dotazovaní na doménové meno nášho DNS zvonku sa použijú verejné adersy DNS serverov zo súboru „/etc/bind/master/db.sos3.external“. O tom, aký súbor sa použije, rozhoduje súbor „/etc/bind/named.conf.local“

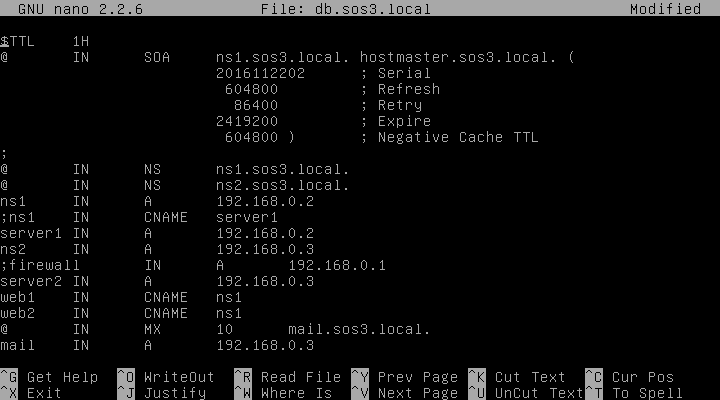
Počítače v lokálnej sieti sa dokážu navzájompingať pomocou svojich hostname. Preklad hostname názvov na IP adresy je definovaný v súbore „/etc/bind/master/db.sos3.local“

Firewall bol nakonfigurovaný tak, aby prepúšťal DNS požiadavky na lokálnej sieti, a tiež aby prepúšťal požiadavky z internetu na obidva DNS servery t.j. aby boli obidva DNS servery viditeľné zvonku (PREROUTING). Záznamy pre DNS sú pre obidve verejné IP adresy pre udp aj tcp port 53 (zdrojový aj cieľový).

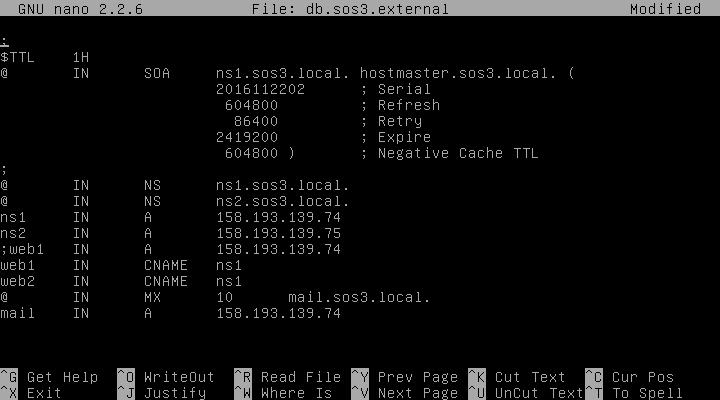
V prípade, že sa vyskytli problémy, skúšali sme vypnúť firewall, kontrolovali sme konfiguračné súbory Master DNS servera príkazmi „named-checkconf“ a „named-checkzone“ a príkazom „tcpdump“ sme monitorovali prenášané správy. Pri každej zmene konfiguračných súborov bolo treba reštartovať bind9 / isc-dhcp-server / interface.

Zdroje:

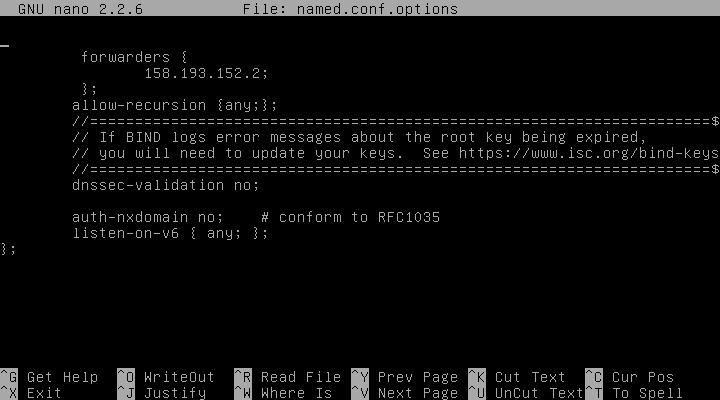
<https://www.howtoforge.com/two_in_one_dns_bind9_views>



Obrázok – db.sos3.local



Obrázok – db.sos3.external



Obrázok – named.conf.options



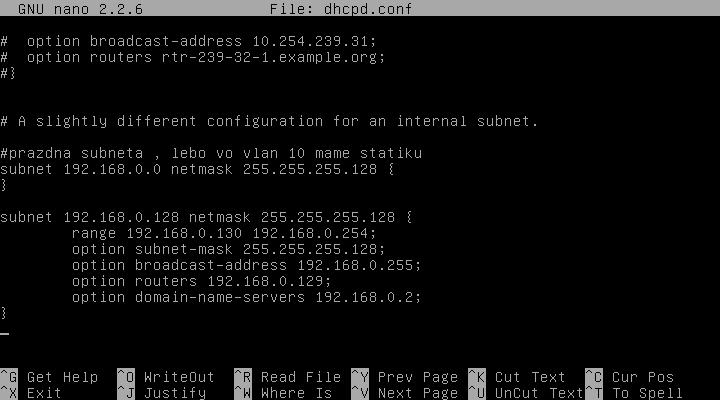
Obrázok – Pohľady (Views)

Doreobit dns popis, nie je dobry

* 1. DHCP

DHCP server (S2) sme museli upraviť tak, aby prideľoval aj DNS adresy serverov. Súbor „/etc/dhcp/dhcpd.conf“ na S1 sme upravili tak, že sme doň pridali privátne IP adresy DNS serverov (option domain-name-servers). Do časti pre podsieť sme definovali názvy týchto serverov. Voľbu „optionhost-name“ sme zmenili z pôvodného „example.org“ na „sos3.local“. Tým, že sme nastavili DNS server, nemusíme meniť na jednotlivých hostoch súbor „/etc/resolv.conf“

Dynamic Host Configuration Protocol (DHCP) je súbor zásad, ktoré využívajú komunikačné zariadenia (počítač, router alebo sieťový adaptér), umožňujúci zariadeniu vyžiadať si a získať IP adresu od servera, ktorý má zoznam adries voľných na použitie.DHCP Server (Dynamic Host Configuration Protocol) vykonáva automatické pridelenie IP adries svojim klientom. Môžu to byť akékoľvek systémy, podporujúce DHCP. DHCP je štandardný protokol, môžu ho využívať aj systémy mimo Microsoft. Z Microsoft operačných systémov podporujú funkciu DHCP klienta všetky až na veľmi exotický LAN Manager pre OS / 2.V rámci siete potom máme DHCP Server - prideľujúca adresy a počítače - ktoré je od neho preberajú (DHCP Clients). V sieti môžu byť aj počítače, ktoré majú tieto adresy nastavené manuálne.

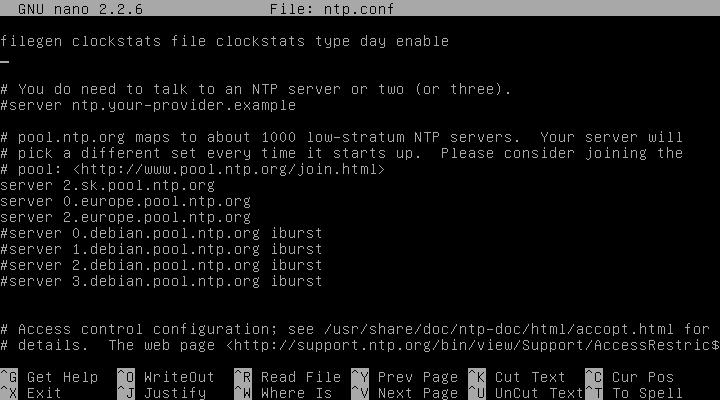


Obrázok – dhcpd.conf

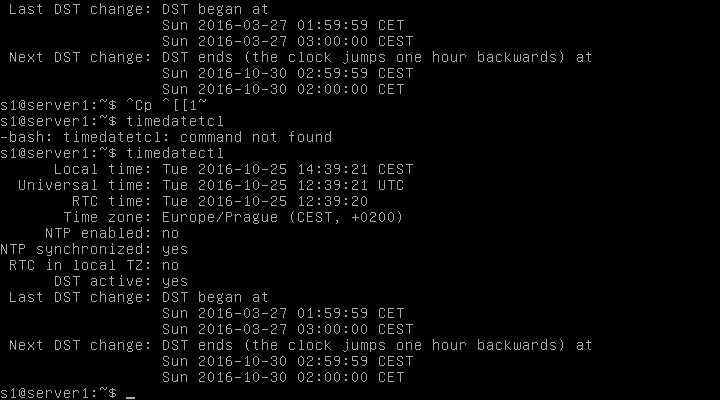
Konifg nie je vobec popisany---dorobit prerobit

* 1. NTP

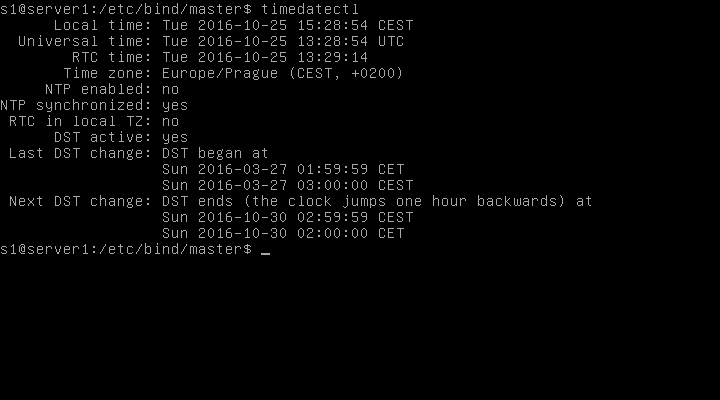
NTP(Network Time Protocol) je protokol na sychronizáciu všetkých počítačov pripojených do vnutornej siete. Tento protokol zaisťuje, aby všetky počítače v sietei mali rovnaký a presný čas. Bol nvrhnutý aby odolával následkom premenlivého zdržania pri doručovaní paketov. NTP používa UDP na porte 123. NTP server sme zvolili server2, ktorý má ip adresu 192.168.0.3. Nainštalovali sme NTP príkazom **apt-get install ntp.** Na klientoch sme nainštalovali NTP pomocou príkazu apt-get installntpntpdate. V súbore na serveri s2 /etc/ntp.conf sme pridali slovenské servery zo stránky [www.pool.ntp.org/zone/sk](http://www.pool.ntp.org/zone/sk). a ostatné servery sme zakomentovali. Klienti si z master serveru aktualizujú čas.



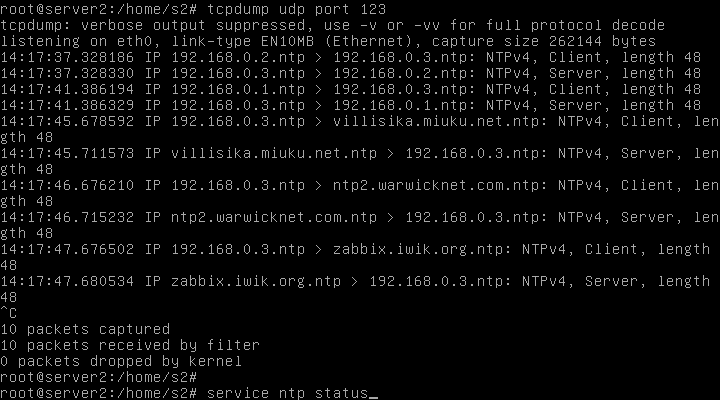
Obrázok – ntp.conf



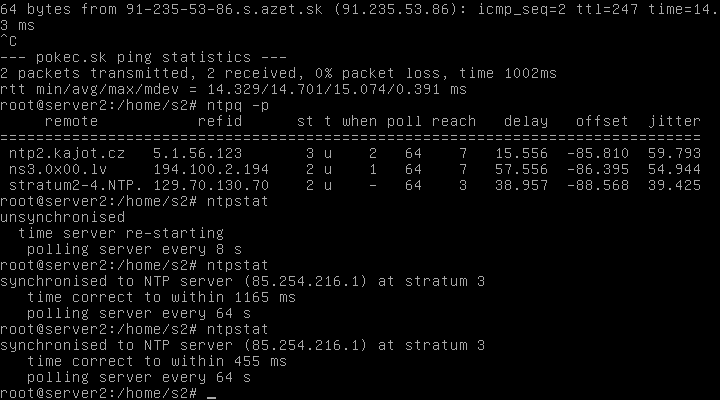
Obrázok – Overenie NTP



Obrázok – Ďalšie overenie NTP



Obrázok – Kontrola NTP cez tcpdump



Obrázok – Kontrola NTP serverov

Vynikky fo fw boli ake aby slo ntp? Konfig ntp klienta bol aky? Kto je ntp masdter pre firmu s2?

* 1. Web server

Apache HTTP Server je softwarový webový server s Opensource licenciou pre Linux, BSD, Microsoft Windows a iné platformy.

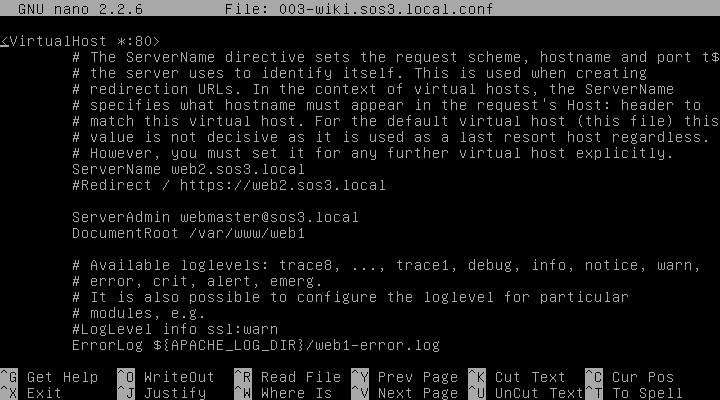
PHP (PHP: Hypertext Preprocessor) je populárny opensource skriptovací jazyk, ktorý sa používa najmä na programovanie klient-server aplikácií (na strane servera) a pre vývoj dynamických webových stránok.

MySQL je slobodný a otvorený viacvláknový, viacužívateľský SQL relačný databázový server. MySQL je podporovaný na viacerých platformách (ako Linux, Windows či Solaris) a je implementovaný vo viacerých programovacích jazykoch ako PHP, C++ či Perl. Databázový systém je relačný, typu DBMS (database management system). Každá databáza je v MySQL tvorená z jednej alebo z viacerých tabuliek, ktoré majú riadky a stĺpce. V riadkoch sa rozoznávajú jednotlivé záznamy, stĺpce udávajú dátový typ jednotlivých záznamov, pracuje sa s nimi ako s poľami. Práca s MySQL databázou je vykonávaná pomocou takzvaných dotazov, ktoré vychádzajú z programovacieho jazyka SQL (StructuredQueryLanguage).

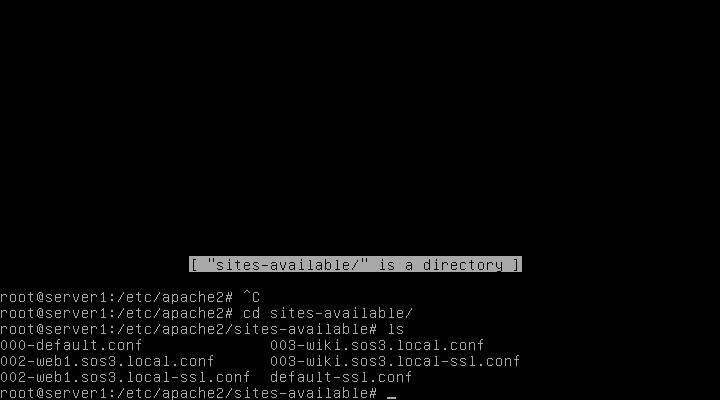
Na webový server sme použili apache. Apache HTTP Server je [softwarový](https://sk.wikipedia.org/wiki/Software) [webový server](https://sk.wikipedia.org/wiki/Server) s [Opensource licenciou](https://sk.wikipedia.org/wiki/Open_source" \o "Open source) pre [Linux](https://sk.wikipedia.org/wiki/Linux), [BSD](https://sk.wikipedia.org/wiki/BSD), [Microsoft Windows](https://sk.wikipedia.org/wiki/Microsoft_Windows) a iné platformy. V dnešnej dobe je najrozšírenejším na celom svete. Pre plnú fukncionalitu webového servera sme museli nainštalovať nainštalovaťapache, mysql, php pomocou príkazov.

apt-get install apache2 mysql php5

V adresári /var/www/ sme vytvorili priečinky s názvami web1 a web2. Kde web1 a web2 predstavovali dva virutálne webové servery. Následne sme v etc/apache2/sites-available 003-wiki.sos3.local.conf sme pridali cestu ku web stránke /var/www/web1 a ServerName web2.sos3.local. Pre joomlu v súbore 002-joomla.sos3.local.conf sme pridlai cestu k adresaru ked uz DocumentRoot /var/www/web1 a ServerName web1.sos3.local



Obrázok – Wiki web stránka (konfigurácia)



Obrázok – Zoznam súborov dostupných webstránok

Následne do DNS záznamov sme museli pridať

db.sos1.local :

web1 IN A 192.168.0.4

web2 IN A 192.168.0.4

db.sos1.public :

web1 IN A 158.193.139.74

web2 IN A 158.193.139.74

* + 1. Inštalácia joomla

V priečinku /var/www/web2 sme stiahli joomlu verziu 3.6 pomocou príkazu

wget [https://github.com/.../Joomla\_3.6.0-Stable-Full\_Package.zip](https://l.facebook.com/l.php?u=https%3A%2F%2Fgithub.com%2Fjoomla%2Fjoomla-cms%2Freleases%2Fdownload%2F3.6.0%2FJoomla_3.6.0-Stable-Full_Package.zip&h=ATOsGJv6INrx86zCq7bl4VW_wTJcot8V6c7ngRwLWvIZSUZM8uhFkuM47H9d7c8Fp0Tony-dLpgQoRhDj0nvH5-d_3mJ-EUFyp1IuNboTsLbI16y5ctN8jie83vrQyhpr4oI_NOpSg)

V ďalšom kroku sme odzipovali tento súbor príkazom

unzip Joomla\_3.6.0-Stable-Full\_Package.zip

Následne sme v prehliadači otvorili web1.sos3.local a podľa príslušných krokov sme nainštalovali joomlu. Ake su tam prava? Root:root nefunguje

* + 1. Inštalácia mediawiki

V priečinku var/www/web1 sme stiahli Wikimedia pomocou príkazuWget<https://www.mediawiki.org/wiki/Download/mediawiki-1.2.8.zip>Následne sme odzipovali tento súbor príkazomUnzip mediawiki-1.2.8.zip A v poslednom kroku sme v prehliadači web2.sos3.local nainštalovali mediawiki.

* 1. Poštový server

Na poštový server sme použili postfix.**Postfix** je počítačový program pre unixové systémy pro prepravu elektronickej pošty (MTA).

Najprv bolo ptorebné nainštalovať postfix príkazom apt-get installpostfix prešli sme inštaláciou kde sme nastavili hostname sos3.local. Následne sme museli reštartovať postfixservicepostfixrestart. V súbore /etc/postfix/main.cf je potrebné upraviť myhostname = sos3.local, odkomentovaťmyorigin = $myhostname, taktiež odkomentovaťinet\_interfaces = all a inet\_protocols = all a tiež bolo potrebné pridať mynetworks = 192.168.1.0/24 192.168.0.0/24. Mail\_spool\_directory = /var/spool/mailje cesta ku mailu. Následne nám po restarte servera vypísalo startedpostix: ok.

Toto nieje uplne ani zdaleka

1. WIndows
   1. DHCP

Inštaláciu sme vykonali vo Windows service manager - *Add Roles and Features*, vybrali si možnosť *DHCP* server .

Pre konfiguráciu sme klikli na *TOOLS* a následne *DHCP.*

Zobrazilo sa nám okno s ponukou , my sme vybrali náš server, IPv4 a možnosť *new scope*. Spustil sa New ScopeWizard. V prvom kroku sme napisali názov pravidla na prideľovanie IP adries. Ďalej sme zvolili rozsah IP adries a masku.

Rozsah IP adries od 192.168.0.1 po 192.168.0.254

Maska 255.255.255.0

Následne sme využili možnosti pridať výnimku z predtým zadaného rozsahu, teda adresy ktoré sa nebudu prideľovať napriek tomu, že sú zo nami zadaného rozsahu v predchádzajúcom kroku. Ide o adresy serverov 192.168.0.2 a 192.168.0.3 .

Potom sme zvolili aký dlhý čas si server bude pamätať IP adresy ktoré niekomu pridelil. Stačilo nám 5 hodín (dĺžka cvičenia aj s rezervou).

Nakoniec sme nastavili bránu na „192.168.1.1”, pridali sme IP adresy našich DNS serverov, teda „192.168.1.2“ a „192.168.1.3”. , a dokončili inštaláciu kliknutím na *Finish.*

* 1. DNS

V prvom rade sme si zvolili Master a Slave. Master je server1 (192.168.0.2) a Slave server2 (192.168.0.1)

DNS master nainštalujeme pomocouWindows Server Manager.Klikneme na *Manage* , vyberieme možnosť *Addroles and features*daľej*Role-based or feature-basedinstallation*, zobrazí sa zoznam serverov, my vyberieme náš server a zvolímezo zoznamu roles*DNS Server* a dokončíme inštaláciu.

Po inštalácií DNS balíka sme sa dostali cez Tools → DNS → Configure a DNS server →Create a forward lookupzone k vytvoreniuprimárnej forward lookupzóny *sos1.local* , nastavili sme aj nech záznamy preposiela na Slave 192.168.0.3.

Prešli sme k inštalácii DNS Slave.Postup ako pri DNS Master avšak DNS server bolo potrebné nastaviť na slavemode. Vybrali sme T*ools → Forward lookupzones → New zone.*Hneď v prvom kroku sme vybrali možnosť nie Primaryzone ale *Secondaryzone* a taktiež meno zóny .V ďalšom kroku určíme DNS Masterserver,v našom riešení ma IP 192.168.0.2 .Dokončíme vytváranie zóny pomocou *Next a Finish*. Onedlho si Slave stiahne záznamy z DNS Master servera.

* 1. NTP

Na spustenie NTP na Windows servery sme museli vykonať zmeny v registroch. Spustíme okno RUN (WIN+R) , kde napíšeme *regedit*. Následne sa dostaneme cestou *HKEY\_LOCAL\_MACHINE | SYSTEM | CurrentControlSet | Services | W32Time | TimeProviders | NtpServer* až k hodnote *Enabled ,* ktorá bola nastavená na *0* , a my ju zmeníme na *1*.Využijeme opäť win+R , zadáme *w32tm /config /update*,čím vlastne spustíme NTP server na danom zariadení .

Na aplikáciu zmien sme reštartovali Windows Timeservice príkazom zadaným do commandline*: net stop w32time && net start w32tim.*

* 1. NAT

Nainštalovanie sme vykonali vo Windows Server Manageri, kde cez Add Roles and Features pridali sme



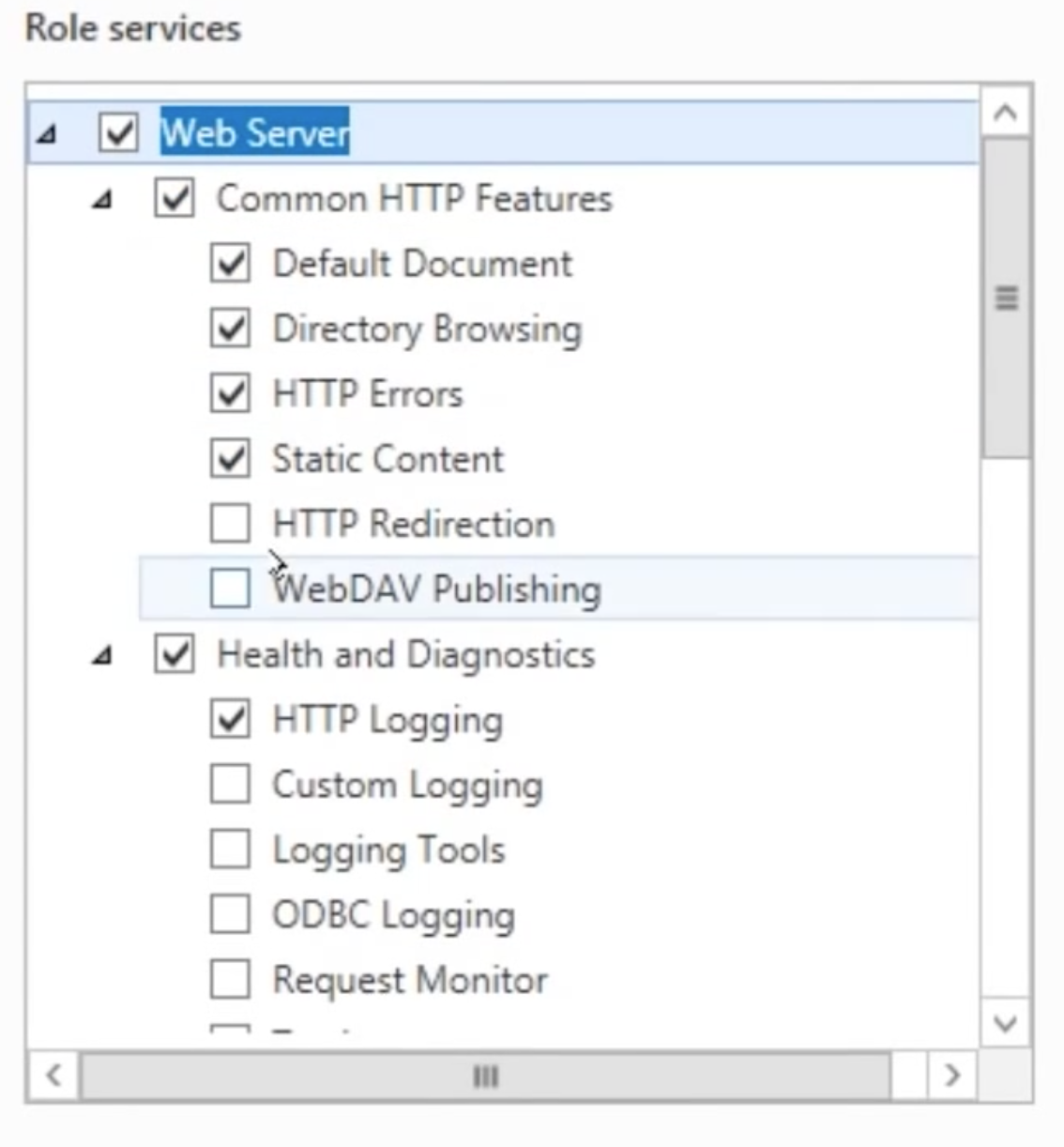
Obrázok – Pridávanie Remote Access role

,

potvrdili sme službuRoutinga následne sme ju nainštalovali . Pri inštalácii zvolíme sieťovýadapter eth0, ktorý je pripojený k internetu.Po inštalácii je NAT plne funkčné, ale je potrebné pridať NAT záznamy na porte 53. Ďalej sme ho potrebovali nakonfigurovať v control panel=>Administrativetools =>routing and remoteaccess. Po kliknutí na NAT, vyberieme záložku s adaptérom, ktorý je pripojený k internet. V addresspool je potrebné nastaviť from, čo znamená našu počiatočnú public adresu 158.193.139.74 a to, čo je naša koncová adresa 158.193.139.75 a netmask 255.255.255.0. V záložke services and ports je potrebné pridať 4 nové záznamy NAT pre DNS(Master-Slave, TCP-UDP).

* 1. ISS- Internet Information Server

Webserver ISS sme pridali cez windows server manager tlačidlom Addroles and features, kde sme vyhľadali Web Server ISS a pokračujeme ďalej. Pri ponuke Role Services

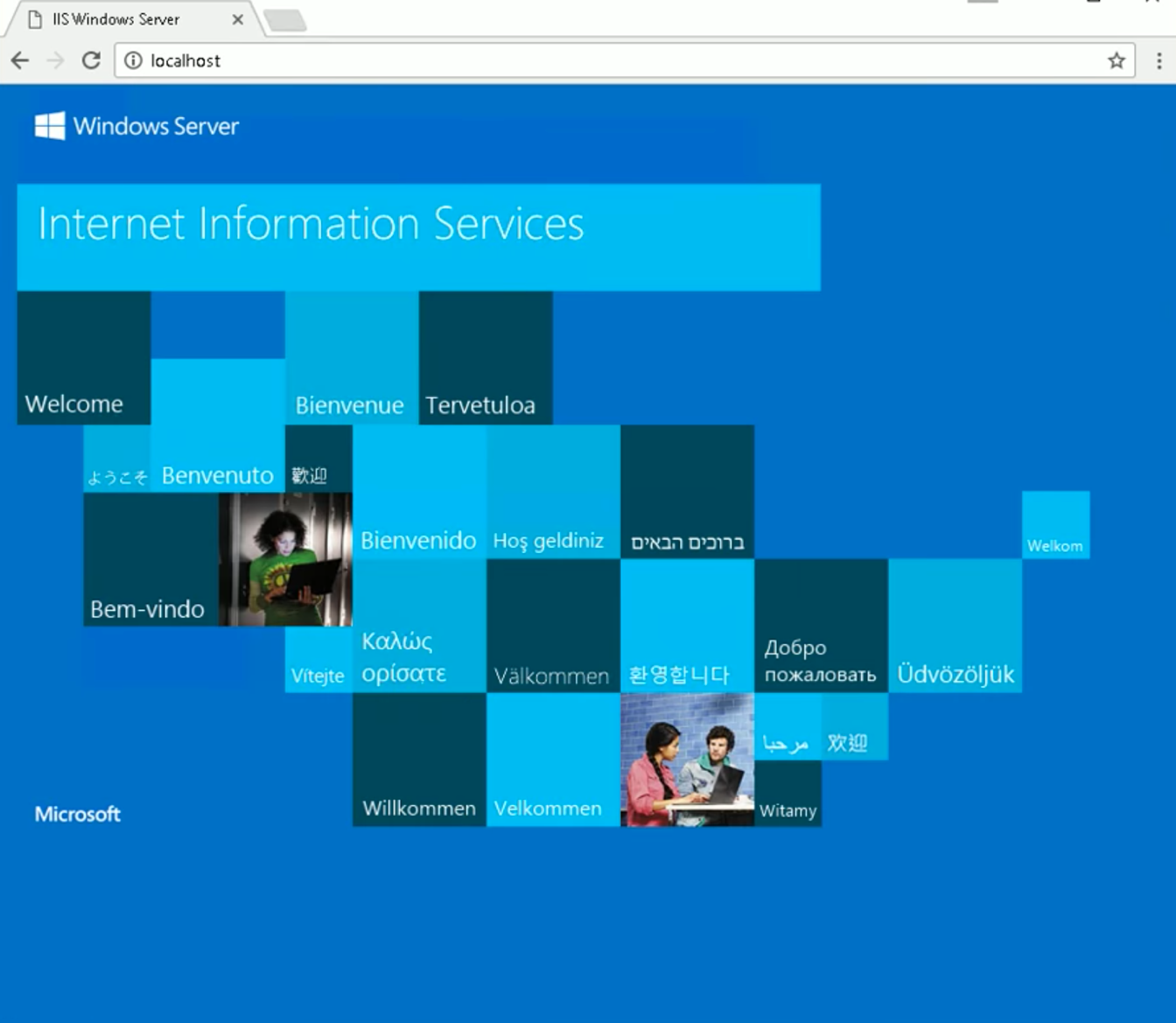


Obrázok – Pridávanie IIS na Windows Server 2016

Následne nainštalujeme služby na server.

Po úspešnej inštalácii sa IIS objaví na ľavom paneli v server manager-i. Klikneme na ikonu IIS a v zozname dostupných serverov sa zjaví jeden - ten, na ktorom uskutočňujeme konfiguráciu. Klikneme naň pravým tlačidlom myši a z ponuky zvolíme možnosť Internet InformationServices (IIS) Manager. Otvorí sa nové okno, v ktorého ľavom paneli sa nachádza náš server. Rozbalíme jeho ponuku a klikneme na Sites. Pravý klik na Default Web Site nám ponúkne viacero možností vrátane nastavenia webstránky a pridania novej.

Po inštalácii sa nachádza ISS v ľavom paneli vo windows sever manageri. Po kliknutí na tools v pravom hornom rohu klikneme Internet informationservices (ISS) manager. A po rozkliknutí na ľavom rohu je už vytvorená default sites. Otvoriť ju je možné zadaním do browseru “localhost”.



Obrázok – Predvolená stránka IIS webservera

* 1. Poštový server

V server manageri klikneme na tools a v záložne DNS, nasmerujume sa ku DNS severu a vytvoríme nové záznamy pre mail server. Cname záznam mail 158.193.139.74, dva MX(Mail exchanger) záznamy 0 mail sos3.local a 10 mail sos3.local.

Zo stránky mailenable.com stiahneme standart edition. Začneme inštaláciou stiahnutého balíčka, zaklikneme web mail service(server). V nasledujúcich krokoch napíšeme do Domain Name: sos3.local a DNS host: 192.168.0.2 a smtp port: 25. Počas inštalácie nám vybehne tabuľká, kde odklikneme aby sa mailserver inštaloval ako webserver ISS. V server manageri po kliknutí servers => localhost => system=>diagnose si skontrolujeme či všetky políčka sú pass, čo nám značí že mail enable funguje. V ďalšom kroku servers => localhost =>services and connectors a na SMTP klikneme pravým tlačidlom a klikneme na properties. V záložne general nastavíme default mail domain name čo je v našom prípade mail.sos3.local. Ďalej v záložke smart host nastavíme IP/DOMAIN 158.193.139.74. Po reštarte serveru vidíme že, všetky service sú running 

1. Záver

Vytvorili sme dve verzie funkčnej základnej firemnej siete – linuxovú a windowsovú. Linuxová verzia bola postavená na operačnom systéme Debian 8.6.0 x64 Stable, windowsová na Windows Server 2016.

V linuxovej verzií sme sprevádzkovali firewall, VLAN smerovanie, DNS, DHCP, NTP, web server, poštový server.

Vo windowsovej verzií sme sprevádzkovali NAT, DHCP, DNS, NTP, web server IIS.