Coyote Linux floppy gataway/firewall – vytvoření systémové živé diskety

Tato distribuce nám nabízí jednoduché vytvoření živé diskety (není nutné instalace) a to jak v prostředí Linuxu tak i Windows.

Informace

- jádro 2.x
- firewall iptables ver 1.x
- DHCP server
- SSH server (SSH ver 2.x)
- webové rozhraní pro správu (na portu 8180)

Kroky ve Windows:

- Naformátujeme disketu v příkazové řádce s parametrem „format a: /u“
- Spustíme *wizard/coyote.exe* a program se představí.
- Nastavení rozsahu IP adres, masky podsítě jaké používá vnitřní síť.
- Nastavení hesla uživatele *root*
- SysLog server, na který bude Coyote ukládat logy.
  (Coyote bude (v omezené míře) logovat stejně,pokud se nevyplní)
- Výběr způsobu připojení k Internetu, Use Static IP configuration, vyplňme IP, masku, bránu (gateway) a případně DNS servery, podle naší karty připojení. Volby *PPPoE* a *PPP* jsou určeny pro připojení modemem nebo linkou s nutností přihlášení. V položkách *Hostname* a *Domain* je možné změnit jména dle libosti, např. místo přednastaveného "coyote" vyplnit "router" a místo "*localdomain*" zadat "*mojesit.cz".* Takto se posléze můžeme k routeru přihlásit pro konfiguraci pomocí webového rozhraní a jako adresu můžete zadat namísto *http://192.168.1.254:8180* přímo název routeru *http://router.mojesit.cz:8180.*
- Zapnutí Coyota jako DHCP serveru pro vnitřní síť. Pokud jej povolíme, může router dynamicky přidělovat IP adresy v naší vnitřní síti a nám odpadne nutnost konfigurace lokálních strojů. Povolíme a nastavíme třeba 64 adres pro DHCP. Můžeme pak libovolně kombinovat pevné a dynamicky přidělované adresy.
- Nyní si vybereme typ síťové karty, jejíž ovladač se má přidat na disketu pro vnitřní a vnější rozhraní. Coyote má v sobě zahrnutu podporu pro mnoho síťových karet, od nejstarších *non-plug and play ISA (NE2000...)* až po nejvíce používané *PCI (Realtek 8139...).* Můžeme, pokud známe typ driveru, zvolit přímo pro nejpoužívanější *Edimaxy* či vůbec síťovky založené na *RTL8139x* je to driver *8139too*, nebo je možné pomocí tlačítka Select zvolit karu podle typu

či podle chipsetu. Pro *PCI* karty a pro *3Com* není nutno zadávat *IRQ* a adresu, pro staré *NE2000* je nutno zadat alespoň adresu, která bývá obvykle *0x300*. Pokud si nejsme jisti adresou, na které se karta hlásí, budeme muset použít její konfigurační program, obvykle se nachází na dodané disketě s ovládači nebo je možné jej stáhnout ze stránek výrobce karty.

- Zadáme jazyk ve kterém bude prostředí – angličtina
- Teď vložíme FD disk do mechaniky a klikneme na vytvořit.

Počítač z této diskety nabootuje a za chvilku se můžeme nalogovat.

Pracujeme-li přímo se serverem a nebo se připojíme přes SSH, pro opuštění menu se zvolí *Q*. Návrat do menu je pomocí příkazu *menu*.

Nápověda Alt+H a dozvíme se například, že ukončení editoru je Ctrl+Q.

Webové rozhraní pro správu můžeme navštívit na *http://server:8180*. Přihlásíme se jako root svým heslem. Toto rozhraní není zabezpečené.

Vysvětlení pojmů ve webovém prostředí.

Show configuration nám řekne, jak na tom je náš server teď. Která síťová rozhraní (ne)jsou nahozená a jaké jsou jim přiděleny adresy. Je zde rovněž informace o tom, jak dlouho již náš firewall plane (nebo spíš hasí).

LAN configuration umožní nastavit adresy pro jednotlivá síťová rozhraní.

Internet configuration - v této kategorii nastavíme parametry nutné pro připojení k Internetu

DHCP configuration - při vytváření diskety jsme měli možnost nastavit pouze počet IP adres, které budou přidělovány. Tady již můžeme nastavit rozsah adres, ze kterého se bude přidělovat a hlavně další údaje, které budou klientům předány (je zde i WINS server, který umožňuje připojení starším Windows klientům podle jména).

Administrative configs - zde jsou některá klíčová nastavení týkající se administrace. Můžeme zakázat ping nebo ssh připojení zvnějšku. Je rovněž možné zakázat webové administrační rozhraní nebo změnit port, na kterém běží (už jen změna portu může útočníka začátečníka zmást) a rovněž změna portu na kterém naslouchá sshd není od věci.

Optional configs - zde je opět možnost nastavení vzdáleného log serveru a time serveru.

QoS configuration - můžeme zvolit, v jakém režimu poběží zabezpečení dostupnosti služeb serveru.

Configuration file - tady zavzpomínáme na textové rozhraní. Nenastavujme proměnné, pokud si nejsme jisti tím, co děláme, protože všechny změny je možné provádět na jiných místech tohoto rozhraní.

Read the system log - to je slíbené logování

Backup configuration - své nastavení zálohujeme na disketu (na tu stejnou, ze které se startuje systém).

Reboot system - Pokud by jsme chtěli počítač restartovat, připojme se přes SSH (dobrý program je *PuTTY*), vyskočme z menu a zadejme příkaz ... třeba *halt*.

Coyote Linux floppy gataway/firewall – vytvoření bootovací diskety MS-DOS 6,2x uložení Linuxu na HDD a provoz webu

Stáhneme disketový obraz pro MS-DOS 6.22. Připravíme si volnou disketu naformátovanou bez vadných sektorů a vložíme do mechaniky. Spustíme program *boot622.exe*, který nám vytvoří bootovací disketu pro MS-DOS 6.22.

Po vytvoření diskety editujeme *config.sys*, ve kterém necháme jen řádky a následně uložíme:

device=himem.sys /testmem:off
files=30
buffers=20

Editujeme *autoexec.bat* a necháme jen řádek a uložíme:

@echo off

Nyní z diskety smažeme všechny soubory kromě:

autoexec.bat
command.com
config.sys
fdisk.exe
format.com
himem.sys
io.sys
msdos.sys

Dále stáhneme *Volkov commander* a rozbalíme archív, na disketu zkopírujeme soubory *VC.COM* a *VC.INI.* Disketu si odložíme.

Zkopírování Coyote Linux na HDD

Potřebujeme k tomu již udělanou disketu s nakonfigurovaným Coyote Linuxem, systémovou disketu DOS 6.22 a několik souborů k tomu, aby se z MS-DOS Disku stal Linux Disk.

První si stáhneme *syslinux*, s jehož pomocí připravíme zaváděcí záznam disku tak, aby zaváděl Linux. Dále budeme potřebovat *linuxové jádro* s podporou harddisku, pro vypínání harddisku a *scp*, aby jsme byli schopní kopírovat na harddisk nové soubory za běhu routeru. A ještě si stáhneme *WinSCP klienta*, který nám ve Windows zajistí možnost připojení se a kopírování souborů.

Soubory *linux.zip* a *syslinux.zip* rozbalíme a soubory *scp.tgz* a *hdparm.tgz* nakopírujeme na DOS 6.22 disketu tak jak jsou. Připravíme si HDD maximální velikosti do 1GB, nebo Linux nebude fungovat. Pro zaváděcí part Linuxu bude stačit oddíl o velikosti 10 MB jako primární partition.

PC nabootuje z DOS 6.22 diskety a až se dostaneme do promptu, spustíme *fdisk.exe*. Odstraníme všechny partitions na disku, vytvoříme primární partition o velikosti 10MB, uděláme ji aktivní a vytvoříme extended partition o velikosti zbytku disku. V ní vytvořime logický disk D o velikosti celé extended partition. Ukončíme fdisk a restartujeme PC.
Provedeme formát disku příkazem *format c: /u/c*, po proběhnutí formátu ještě *format d: /u/c*. Zadáme příkaz *syslinux c:* a spustíme si *vc.com*. Z diskety překopírujeme na disk C: soubory:

linux
syslinux.cfg
hdparm.tgz
scp.tgz

Vyměníme v mechanice disketu za Coyote Linux disketu, obnovíme *(CTRL+R)* obsah okna a zkopírujeme na disk C: vše, co je na disketě, *kromě souborů:*

linux
syslinux.cfg
ldlinux.sys

Tyto soubory nepřepisujeme. Vložíme zpět DOS 6.22 disketu, obnovíme obsah okna a na disku D: vytvoříme adresář "*WEB*".

Nyní můžeme vypnou PC a případně odpojit FD a znovu zapnout a v *BIOS*u nastavit aby bootoval PC rovnou z HDD.

Teď by mělo vše naběhnou z HDD a pak se můžeme přihlásit jako *„root*“ vypneme menu klávesou „*q*“ a jestli budeme chtít provozovat na routeru WWW server upravíme pár parametrů pro *hdparm*, ten vypíná disk po 1 minutě, což je málo – pořád by se vypínal při brouzdání po webu.

Vytvoření Web Coyote Linux

Napíšeme příkaz *cd /etc/rc.d/pkgs* a následně *edit rc.hdparm*, zobrazí se nám toto:

```
#!/bin/sh
#
# Coyote local command init script
#
# rc.hdpram - Sets harddisk sleeping, 1 minute timeout
#

echo "Setting disk sleeping timeout ..."

/sbin/hdparm -u 1 /dev/hda
/sbin/hdparm -S 12 /dev/hda
```

V posledním řádku opravíme číslici 12 na 120, čímž nebude prodleva pro vypnutí disku jedna minuta, ale deset minut. Soubor uložíme *CTRL+S* a opustíme editor *CTRL+Q*. Napíšeme příkaz *cd ..* a následně *edit rc.local*, zobrazí se nám:

```
#!/bin/sh
#
# Coyote local command init script
```

Soubor doplníme následovně:

```
mkdir /www
sync
mount -t vfat /dev/hda5 /www
sync
chmod -R ugo-x /www/web
sync
LOCAL_IPADDR=`getifaddr eth0`
/usr/sbin/thttpd -u root -T cp1250 -d /www/web -h $LOCAL_IPADDR -p 80
IPADDR=`getifaddr eth1`
```

Opět uložíme *CTRL+S* a vyskočíme z editoru *CTRL+Q*. Teď bude důležité tyto změny zapsat, aby se po restartu neztratily. Spustíme tedy příkazem *menu* hlavní menu routeru a zvolíme položku "*w) Write configuration to disk*". Vyčkáme až proběhne záloha konfigurace, vrátíme se zpět do menu a restartujeme router volbou "*r) Reboot system*".

Tyto kroky jsou potřebné při každém restartu opakovat, neboť file systém Coyote Linuxu se po každém startu vytváří znovu. Proto jsme upravovali skript *rc.local*, je to něco jako autoexec.bat v DOSu, provede to za nás zcela automaticky.
Od této chvíle nám tedy na coyote běží i webserver a stačí jen napsat stránky a nakopírovat je do adresáře "WEB" na disku D:.Web server je přístupný prozatím pouze z lokální sítě na adrese routeru např. *http://192.168.1.254* nebo *http://coyote.localdomain***,** nebo jak jsme pojmenovali router a lokální doménu.

WEB na Coyote Linux

Je několik možností, jak webové stránky dostat na server, nakopírovat je na disketu a překopírovat je přes disketovou mechaniku do adresáře */www/web*. Pokud je již FD mechanika odpojená, je tady připravena druhá možnost a to je *SCP*. Na začátku jsme si na disketu kopírovali soubor *scp.tgz*. Tento samo-instalační balíček nám na routeru umožní, abychom se k němu mohli připojit *WinSCP* klientem z Windows přes LAN. *WinSCP* klient komunikuje s routerem přes zabezpečený kanál a umožňuje mimo jiné kopírovat soubory z routeru a na router. Nyní ho nainstalujeme a dáme se na překopírování.
Naprosto běžným způsobem, na jaký jsme zvyklí třeba z Volkova či Windows Commanderu, překopírujem z našeho lokálního PC soubory WWW stránek. Umístíme je do adresáře */www/web*. WWW server, použitý v Coyote Linuxu vyžaduje, aby soubory, které jsou použity pro běh WWW, měly zrušený atribut "*execute*". Můžeme toho dosáhnout změnou atributů souborů přímo pomocí *WinSCP*, ale možná bude jednodušší prostě restartovat tlačítkem RESET celý router. Nabíhá velice rychle (cca 1 minutu) a o potřebné změny se postará sám při startu.

Komunikace s routerem přes *Win SCP* je popsána v „*Doplňky ke Coyote Linux*“

Po restartu routeru se můžeme podívat browserem na naše stránky adresa je naše IP.

Web server Coyote Linux na internetu

Předně musíme zapnout webserver pro internetovou adresu routeru. Známým postupem se dostaneme do linuxového promptu.(K routeru se můžete připojit i po síti za pomocí SSH protokolu. K tomu je dobrý *PuTTY*, nastavíme IP adresu routeru, přihlásíme se a už jsme v promptu, nyní můžeme nastavovat vše přes síť.)

Editujeme *rc.local* a na konec dopíšeme *"/usr/sbin/thttpd -u root -T cp1250 -d /www/web -h $IPADDR -p 80"*, tím zajistíme spuštění webserveru i na internetové adrese routeru. Internetové stránky nemusí být shodné s těmi intranetovými (vnitřními), nic nám nebrání v tom, aby jsme si někam jinam uložili jinou sadu stránek. Cesta k nim se nastavuje právě parametrem *"-d /www/web*". Takže pokud si vytvoříme (příkazem *mkdir /www/inet"* adresář "inet", můžeme směrovat externí stránky do něj... jen nesmíme zapomenout patřičně upravit *rc.local* co se týče *chmod* - vložme ještě před příkaz pro spuštění webserveru řádek *"chmod -R ugo-x /www/inet".* Náš *rc.local* pak může vypadat asi takto:

```
#!/bin/sh
#
# Coyote local command init script
mkdir /www
sync
mount -t vfat /dev/hda5 /www
sync
chmod -R ugo-x /www/web
sync
chmod -R ugo-x /www/inet
sync
LOCAL_IPADDR=`getifaddr eth0`
/usr/sbin/thttpd -u root -T cp1250 -d /www/web -h $LOCAL_IPADDR -p 80
```

```
IPADDR=`getifaddr eth1`
/usr/sbin/thttpd -u root -T cp1250 -d /www/inet -h $IPADDR -p 80
```

Třeba je ještě zajistit, aby firewall "*iptables*" směroval požadavky na www stránky tam kam je potřeba. Před tím, než uložíme konfiguraci, editujeme skript "*rc.firewall*", který najdeme v */etc/rc.d*. Tam najdeme řádek, který začíná příkazem "*iptables*":

```
....
IPADDR=`getifaddr $IF_INET`

# Block traffic that is not part of an existing connection
# or part of a permitted ACL list
iptables -D INPUT -i $IF_INET -m state --state NEW -j DROP 2>/dev/null
iptables -A INPUT -i $IF_INET -m state --state NEW -j DROP
....
```

Mezi *"# or part..."* a "*iptables -D..."* vložíme další řádek: *"iptables -A INPUT -i $IF_INET -p TCP --dport 80 -j ACCEPT"*. Tento příkaz řekne firewallu, aby vstupní požadavky na internetovém rozhraní, které přicházejí po portu 80 protokolem TCP, nezahazoval a neforwardoval, ale tyto požadavky akceptoval. Takže část našeho *rc.firewall* bude vypadat takto:

```
.........
IPADDR=`getifaddr $IF_INET`

# Block traffic that is not part of an existing connection
# or part of a permitted ACL list
iptables -A INPUT -i $IF_INET -p TCP --dport 80 -j ACCEPT
iptables -D INPUT -i $IF_INET -m state --state NEW -j DROP 2>/dev/null
iptables -A INPUT -i $IF_INET -m state --state NEW -j DROP
.....
```

Soubor uložíme a ukončíme editaci, nastartujeme menu zapíšeme konfiguraci na HDD a restartujeme. Náš web server je hotov.

Doplňky ke Coyote Linux

K tomuto Linuxu se najde na internetu mnoho balíčků.
IPTraf, Printer Sparing, *LP, TinyProxi, mail..*atd .

IPTraf

Slouží k měření traffic na síťovích kartách – můžeme zde sledovat, která stanice právě „sosá“ a jakou rychlostí. Ovládání je velice jednoduché, po instalaci přibude položka "*i: IPTraf*"...
Název balíčku: *iptraf.tgz*

Pointer Sparing a LP

Tyto moduly slouží, aby přidaly do Coyote Linux sdílení tisku – klasický *IP Printing*. Tiskárna která je připojená k routeru se bude chovat jako by měla síťovou kartu a bude přístupná pro všechny PC v lokální síti.
Název balíčku: *lp.tgz* a *p910nd.tgz*

Funkčnost tiskového serveru pro Windows
Abychom se mohly připojit z operačního systému Windows musíme mít nainstalovanou podporu *TCP/IP*, nainstalujeme proto *AXIS Print Port*. Tiskárnu přidáme ve Windows pomocí dialogu *„Přidat tiskárnu“* zadáme jako místní tiskárnu a port do nějž se tiskne „*AXIS Port*“. V konfiguraci portu zadáme IP routeru a port 9100. Na tomto chodí snad všechny tiskárny, jež mají podporu připojení přes LPT port.
Název souboru pro Windows: *axipprt.zip*

TinyProxy Server

Transparent Proxy server usnadňuje přístup k internetu tím, že do paměťového prostoru, který je pro něj vyhrazen nahrává (*cachuje*) obsahy navštívených internetových stránek a při další návštěvě pak klientovy tento obsah nahraje do prohlížeče, čímž se ušetří čas pro opětovné načítání celého obsahu stránek. Konfigurace je možná přes web rozhraní, velice jednoduše konfigurovatelný přes *Webadmin*. Pracuje hned po restartu *CoyoteLinux* a brání uživatelům v přístupu na definované "nebezpečné" stránky. Tyto stránky lze průběžně zadávat do konfiguračního souboru "*filter*", přístupného na webovém rozhraní. Nesmíme zapomenout na souborový systém *VFAT*, *TinyProxy* má dlouhý název a pokud by jsme kopírovali ve *MS-DOS* filesystému, nakopíroval by se s krátkým jménem a následně by *TinyProxy* nepracoval.
Zde použitá *proxy* má jednu nevýhodu a tou je, že je povolena pro všechny uživatele. Proto byl napsán doplněk jež umožňuje pro určité IP adresy přístup bez omezení a ostatní ignoruje. Tento doplněk se jmenuje *Bypass IP´s*, instalace je popsána níže. Po restartu počítače se ve *Webadmin*u objeví nová položka, pomocí které se nastaví adresy a podsítě, z níž chceme mít neomezený přístup. Nastavení si uložíme a restartujeme PC.
A nyní je Proxy hotová..
Název balíčku: *tinyproxy.tgz* a *bypass.tgz*

Instalace všech těchto balíčků probíhá jednoduše, nakopírují se do systémové složky *„mmt*“.
Můžeme tedy použít *Win SCP* a připojit se k routeru a nakopírovat, nebo potřebné soubory dát na bootovací disketu a následně přenést do routeru..
Při použití *Win SCP* je nutno před přihlášením v programu změnit v nabídce stromečku (úvodní stránka) *Prostředí* složku *SCP,* kde najdeme *Shell* a přepneme na *Zadejte* zde vypíšeme */bin/sh* a následovně vyplníme *Hostitele* což je IP routeru, *Uživatelské jméno* jako root a naposled naše *heslo*
Po přihlášení stiskneme *CTRL+T* nebo si najdeme na horní liště „Terminál“, jako příkaz zadáme *"mount /dev/boot /mnt"* a potvrdíme. Po chvíli by měl jít otevřít adresář */mnt* ve struktuře, pokud je prázdný zkusíme obnovit *CTRL+R* . Jestliže je všechno v pořádku měl by se zobrazit obsah boot sekce routeru. Následovně nakopírujeme všechny stažené soubory s příponou *.tgz* a nyní jsou balíčky nainstalovány. Tímto způsobem se kopírují do serveru i ostatní balíčky.