

Firewall pod Linuxem

InstallFest 2005

Martin Pohl

Úvodem

- Personální FW – Firestarter
- Shorewall jako personální FW
- Shorewall jako domácí FW
- Integrace shorewallu
 - ulog
 - Port knocking
 - fwlogwatch

Personální firewall - Firestarter

- Firestarter
 - <http://www.fs-security.com/>



Firestarter brimstone.sby.abo.fi

Firewall Edit Events Policy Help

Preferences Lock Firewall Stop Firewall

Status Events Policy

Firewall

Status	Events	
	Total	
	Serious	
Inbound	17	7
Outbound	9	0

Active

Network

Device	Type	Received	Sent	Activity
eth0	Internet	0.7 MB	0.0 MB	2.2 KB/s
eth1	Local	0.0 MB	0.1 MB	0.0 KB/s
sit0	IPv6 Tunnel	0.0 MB	0.0 MB	0.0 KB/s

Active connections

Source	Destination	Port	Service	Program
130.232.120.53	66.102.9.99	80	HTTP	firefox-bin
130.232.120.53	204.225.124.69	6667	ircd	xchat
130.232.120.53	216.239.51.104	80	HTTP	firefox-bin

Firestarter brimstone.sby.abo.fi

Firewall Edit Events Policy Help

Save List Clear Reload

Status Events Policy

Blocked Connections

Time	Direction	Port	Source	Protocol	Service
Nov 20 01:48:35	Inbound	113	130.232.213.6	TCP	Unknown
Nov 20 01:48:49	Inbound	22	130.232.213.6	TCP	SSH
Nov 20 01:49:01	Inbound	48393	130.232.213.6	TCP	Unknown
Nov 20 01:49:13	Inbound	21	130.232.213.6	TCP	FTP

Firestarter brimstone.sby.abo.fi

Firewall Edit Events Policy Help

Add Rule Remove Rule Edit Rule Apply Policy

Status Events Policy

Editing Inbound traffic policy

Allow connections from host

www.example.com

Allow service	Port	For
NTP	123	193.166.5.177

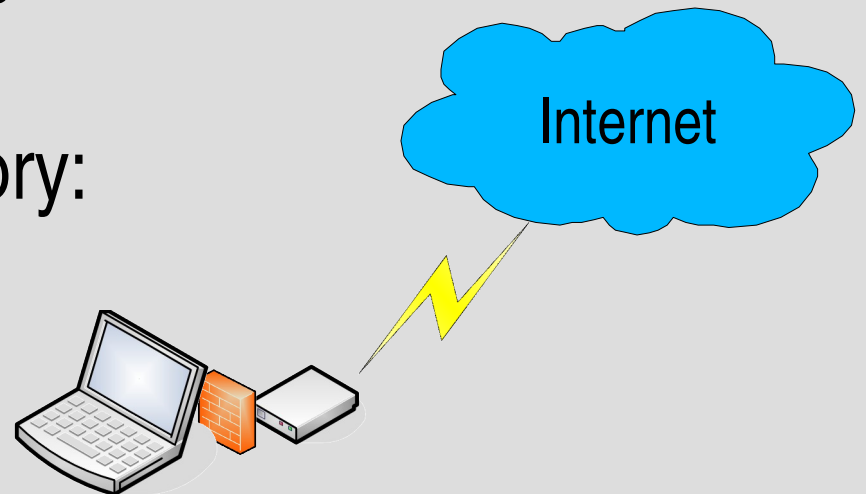
Forward service	Firewall Port	To	Port
BitTorrent	6881-6889	192.168.0.1	6881-6889

Shorewall – úvod

- <http://www.shorewall.net/>
 - Bohatá dokumentace
 - Několikaletý vývoj
 - Snadná konfigurace
 - Mnoho fcí jednoduše použitelných

Shorewall – Personální FW (1)

- Konfigurace je uložena v `/etc/shorewall`
- Vzorová pak obvykle v `/usr/share/doc/shorewall/default-config`
- Základny ovládání:
 - `shorewall start|restart|clear|stop`
 - `shorewall check|ipcalc`
- Minimální konfigurace – soubory:
 - `zones`
 - `interfaces`
 - `policy`



Shorewall – Personální FW (2)

- Příklad konfigurace

```
/etc/shorewall/zones
```

```
#ZONE      DISPLAY      COMMENTS
ppp        Net          Internet
```

```
/etc/shorewall/interfaces
```

```
#ZONE      INTERFACE    BROADCAST  OPTIONS
ppp        ppp+         -          dhcp,blacklist,tcpflags
```

```
/etc/shorewall/policy
```

```
#SOURCE    DEST         POLICY     LOG          LIMIT:BURST
ppp        all         REJECT    INFO
fw         all         ACCEPT
all        all         REJECT    INFO
```

Shorewall – Personální FW (3)

- Výsledek?
 - Odchozí spojení povoleny
 - Příchozí zakázány
 - Co více:
 - Ping povolen
 - Logy nejsou zahlcovány smetím (DHCP, SAMBA, apod)
 - Invalidní pakety zahozeny

```
/var/log/syslog
```

```
Sep 26 20:31:09 fwstroj Shorewall:ppp2all:REJECT:  
IN=ppp0 OUT= MAC= SRC=125.36.132.8 DST=85.36.132.8  
LEN=60 TOS=00 PREC=0x00 TTL=64 ID=46886 CE DF PROTO=TCP  
SPT=39928 DPT=80 SEQ=2046421234 ACK=0 WINDOW=5840 SYN  
URGP=0
```

Shorewall – Personální FW (4)

- Pokračujeme... soubor rules
 - Povolení přístupu na ssh

```
/etc/shorewall/rules
```

```
#ACTION    SOURCE      DEST        PROTO      DEST        .....
#          PORT        .....
ACCEPT     ppp         fw          tcp        80
```

- Povolení přístupu na sambu či ftp

```
/etc/shorewall/rules
```

```
#ACTION    SOURCE      DEST        PROTO      DEST        .....
#          PORT        .....
AllowSMB   ppp:$LOC           fw
AllowFTP   ppp           fw
```


Shorewall – Personální FW (5)

- Zástupná pravidla

```
/usr/share/shorewall/action.AllowSMB
```

```
ACCEPT      -      -      udp      135,445
ACCEPT      -      -      udp      137:139
ACCEPT      -      -      udp      1024:    137
ACCEPT      -      -      tcp      135,139,445
```

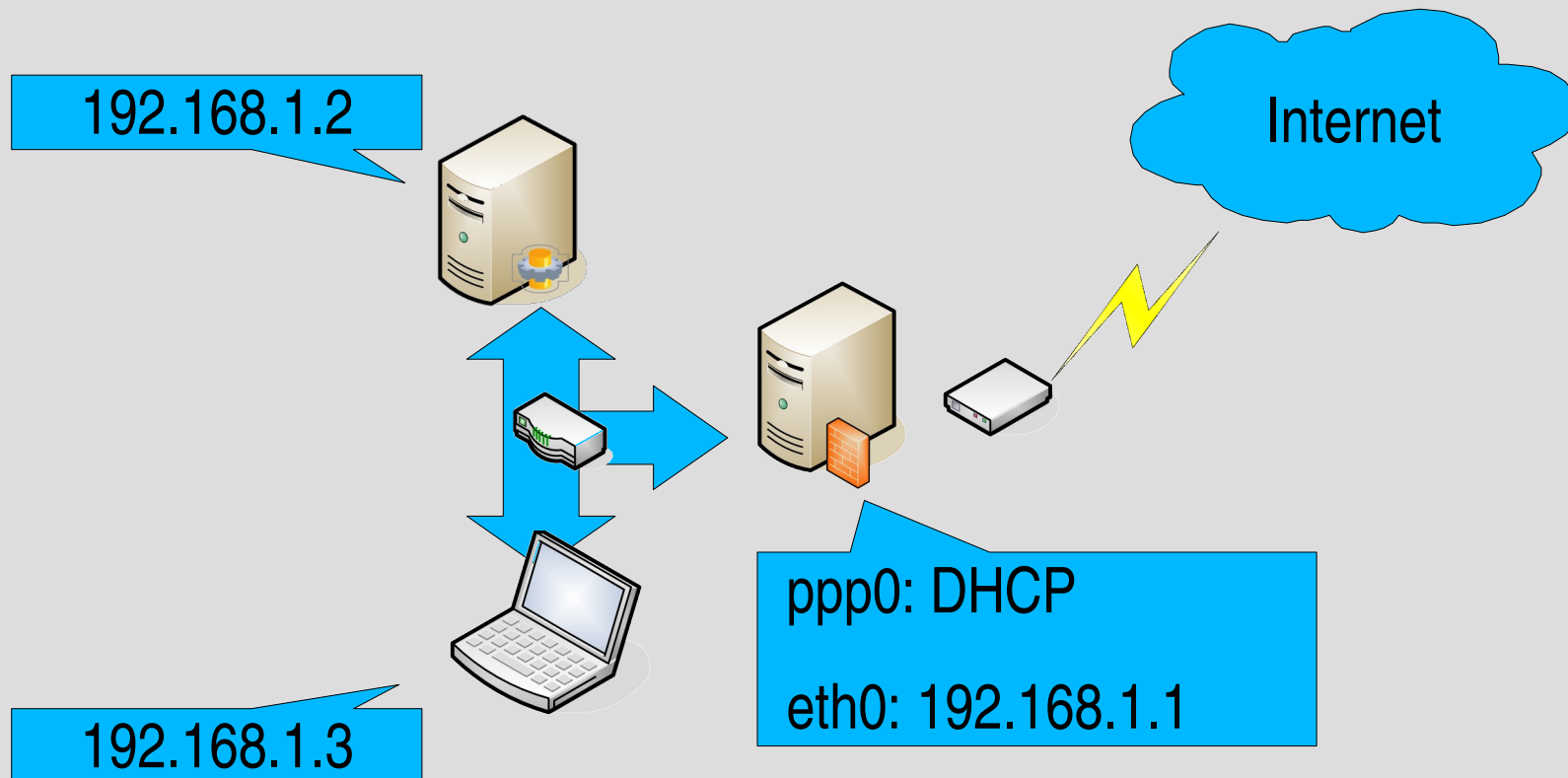
- Proměnné v konfiguraci

```
/etc/shorewall/params
```

```
LOC="192.168.1.0"
```

Shorewall – Domácí FW (1)

- Maškaráda /masq + ipforward/
- DNAT



Shorewall – Domácí FW (2)

- Jak na „maškarádu“ - rozšíříme předchozí konfiguraci
 - zones – další zóna (loc)
 - Interfaces – další síťové rozhraní (eth0)
 - Policy – pouze pro úplnost
 - masq – konfigurace vlastní „maškarády“
 - shorewall.conf – povolení forwardu paketů

Shorewall – Domácí FW (3)

- Konkrétně

```
/etc/shorewall/zones
```

```
ppp      Net      Internet
loc      Loc      Local network
```

```
/etc/shorewall/interfaces
```

```
ppp      ppp+      -      dhcp,blacklist,tcpflags
loc      eth0      detect  blacklist,tcpflags
```

```
/etc/shorewall/policy
```

```
loc      ppp      ACCEPT
all      all      REJECT      INFO
```

```
/etc/shorewall/masq
```

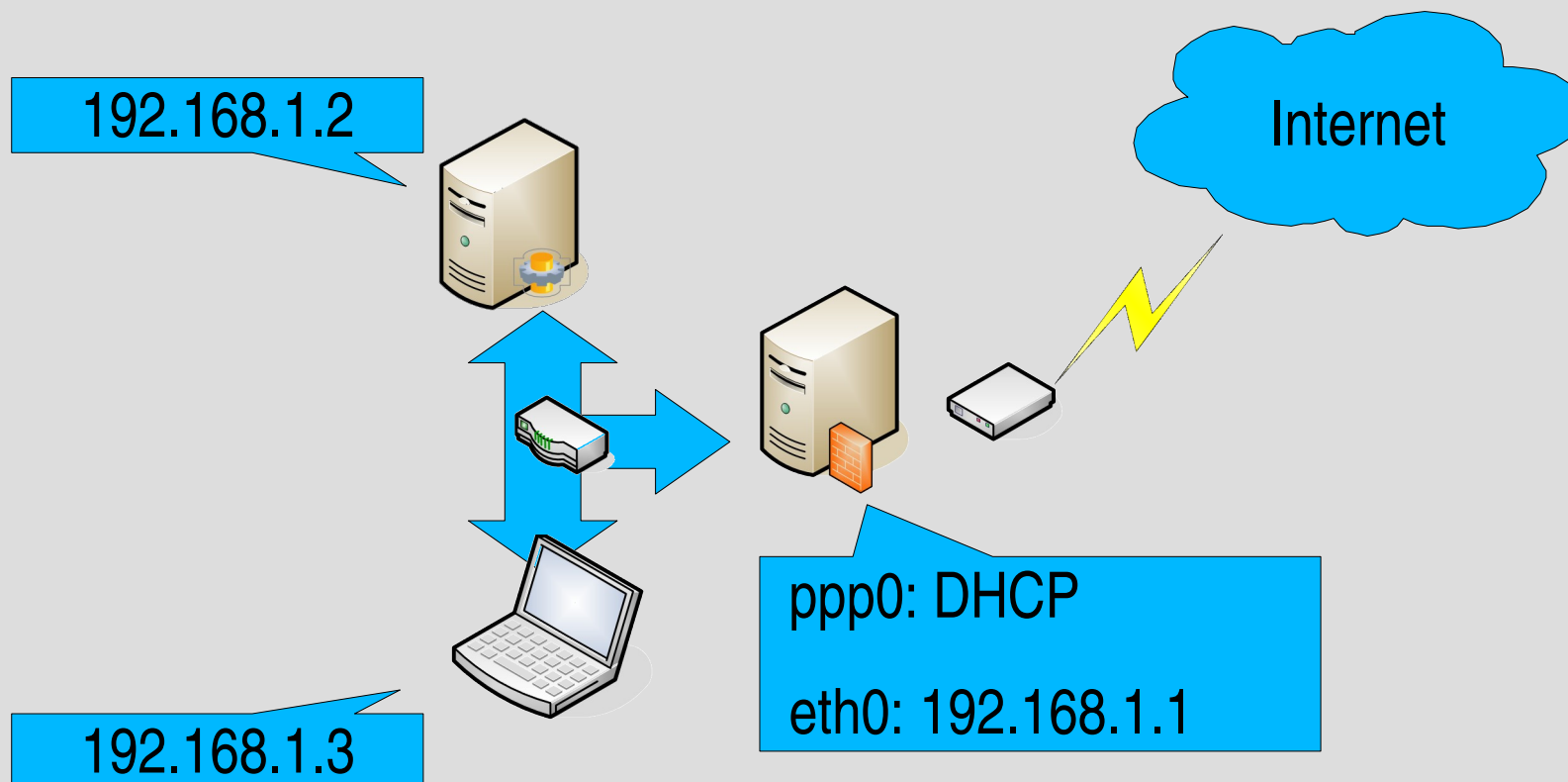
```
ppp0      eth0      # INETERFACE -> SUBNET
```

```
/etc/shorewall/shorewall.conf
```

```
IP_FORWARDING=On
```

Shorewall – Domácí FW (4)

- DNAT pro přístup na www
- Nouzový přístup na fw



Shorewall – Domáci FW (5)

```
/etc/shorewall/rules
```

```
DNAT ppp      loc:192.168.1.2    tcp    80
```

```
/etc/shorewall/shorewall.conf
```

```
DETECT_DNAT_IPADDRS=Yes
```

```
/etc/shorewall/rules
```

```
AllowSSH  loc:192.168.1.3    fw
```

```
/etc/shorewall/routestopped
```

```
eth0  192.168.1.3
```

Shorewall – Integrace (1)

- Ulog – logy firewallu v userspace OS

- <http://gnumonks.org/projects/ulogd>

```
/etc/shorewall/policy
```

#SOURCE	DEST	POLICY	LOG	LIMIT: BURST
ppp	all	REJECT	ULOG	
fw	all	ACCEPT		
all	all	REJECT	ULOG	

- Fwlogwatch – sledování logů

- <http://fwlogwatch.inside-security.de/>

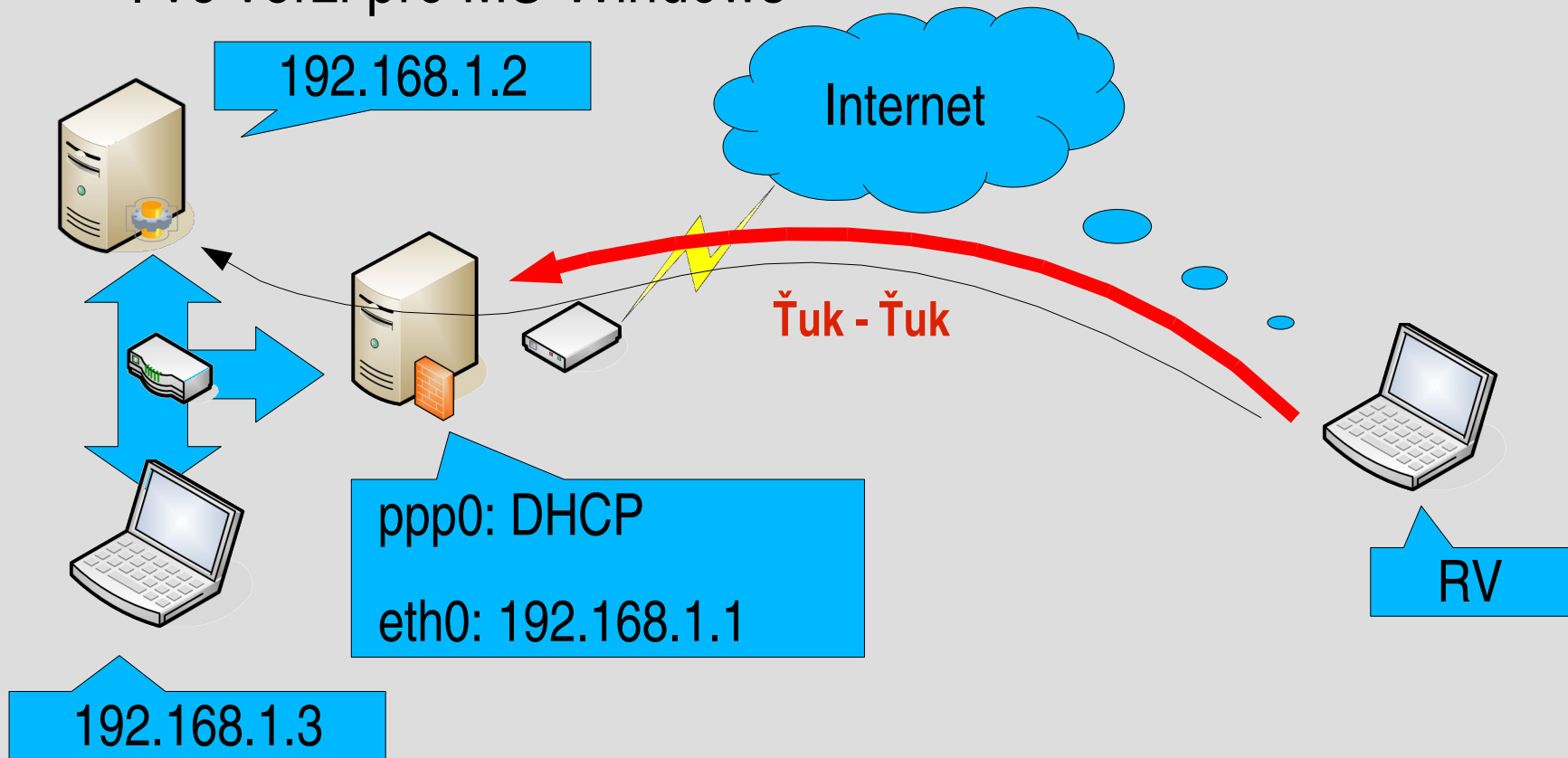
- Možnost real-time kontroly

- Pravidelné denní reporty

- Zpracuje i další logy (Snort, Cisco IOS, atd...)

Shorewall – Integrace (2)

- Port – knocking
 - <http://www.zeroflux.org/cgi-bin/cvstrac/knock/wiki>
 - I ve verzi pro MS-Windows



Shorewall – Integrate (3)

- Konfigurace knockd

```
/etc/knockd.conf (fragment)
```

```
[openSSH]
sequence      = 7000,8000,9000
seq_timeout  = 10
tcpflags     = syn
command      = /usr/local/bin/KnockdAllowSSH %IP%
```

- Integrate do shorewallu

```
/usr/local/bin/KnockAllowSSH
```

```
/sbin/iptables -t nat -A net_dnat -s $1 -d $FWIP -p tcp -m
tcp --dport 22 -j DNAT --to-destination 192.168.1.2
/sbin/iptables -I ppp2loc 4 -s "$1" -d 192.168.1.2 -p tcp -m
tcp --dport 22 -m conntrack --ctorigdst $IPFW -j ACCEPT
```

Klepeme

- knock \$FWIP 7000 8000 9000

Závěrem...

Další možnosti shorewallu:
QOS, IPSec, ProxyARP

Otázky?

(martin.pohl@etnetera.cz)