

Hálózatok építése és üzemeltetése

Hálózati funkciók a gyakorlatban gyakorlat...

A példa hálózatunk

BME Cloud - Füred



https://cloud.bme.hu

CIRCLE 

Welcome to BME Cloud!

Choose your datacenter!

**IIT/IK Cloud**
<https://ik.cloud.bme.hu>
ONLINE

VMs in last 8 days

**VIK Cloud**
<https://smallville.cloud.bme.hu>
ONLINE

VMs in last 8 days

**KIFÜ-NIIF Cloud**
<https://niif.cloud.bme.hu>
ONLINE

VMs in last 8 days

**Füred Cloud**
<https://fured.cloud.bme.hu>
ONLINE

VMs in last 8 days

Contact: help@cloud.bme.hu

© 2018 Copyright: **BME IK**

Smallville, VIK Cloud
("B terv")

Füred Cloud
(javasolt)

Címtáras
belépés

Special thanks to:
Szeberényi Imre (IIT) & CIRCLE Cloud team

CIRCLE  

CIRCLE   **mallville**

Login with SSO

[Forgot your password?](#)

VM-ek indítása (2023) - Füred



Gateway VM

Start 3 VMs

Create a VM

CentOS v4

HaEpUz 2022 - Ubuntu 20.04 + xfce4 v17

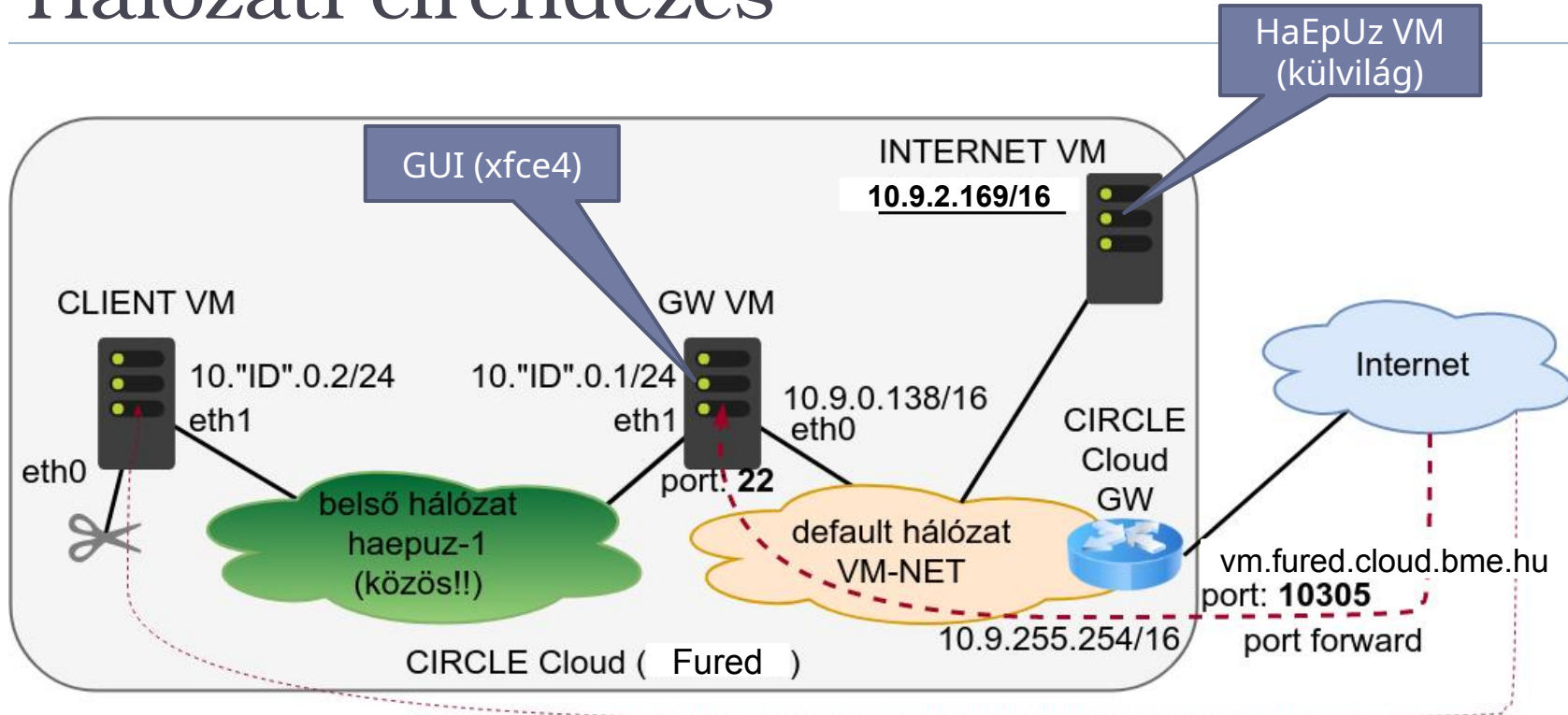
HaEpUz 2022 - Ubuntu 20.04 + xfce4 v19

Internet VM

Client VM

- ▶ HaEpUz 2022 v19 sablonból
 - ▶ GW VM
 - ▶ CLIENT VM
- ▶ HaEpUz 2022 v17 sablonból
 - ▶ Internet VM

Hálózati elrendezés



ID: Teams-ben! (General->Files->HaEpUz-2023-gyak3-IDs)

Belépés: ssh és rdp

Nevezzük át
a VM-eket!

GW - Ubuntu 20.04 + xfce4 v19 cloud-

17124.vm.fured.cloud.bme.hu ☆



▶ RUNNING

Connection details

Protocol SSH
Host **vm.fured.cloud.bme.hu:8470**
Host (IPv6) cloud-17124.vm.fured.cloud.bme.hu:22
Username cloud
Password *****-Y

[Generate new password!](#)

Command *****-Y

[Connect \(download client\)](#)

Home Resources Console Access **Network** Activity

Interfaces

VM-NET [remove](#)
IPv4 address: 10.9.1.72
IPv6 address: 2001:738:2010:1009:9:1:72:0
DNS name: cloud-17124.vm.fured.cloud.bme.hu
Groups: -

Port access

IPv4 IPv6
vm.fured.cloud.bme.hu:8470 → 22/tcp [x](#)
vm.fured.cloud.bme.hu:19280 → 3389/tcp [x](#)

ssh

rdp

+ → / tcp [Add](#)

Haepuz-1 (unmanaged) [remove](#)

Belépés: ssh

```
sonkoly@notty:~$ ssh -Y cloud@vm.smallville.cloud.bme.hu -p 10305 -i ~/.ssh/haepuz_id_rsa
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-33-generic x86_64)
```

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage
```

```
System information as of Tue Oct 9 22:49:48 CEST 2018
```

```
System load: 0.0      Processes:            77
Usage of /:  8.8% of 35.56GB   Users logged in:    0
Memory usage: 23%          IP address for eth0: 10.9.0.138
Swap usage:  0%
```

```
=> There is 1 zombie process.
```

```
8 packages can be updated.
8 updates are security updates.
```

Ezen a gépen tűzfal működik, ezért egy kívülről elérhető szolgáltatás megfelelő működéséhez szükséges lehet az adott port engedélyezése.

Ez webszerver esetén az alábbi módon tehető meg:

```
$ ufw allow 80/tcp
$ ufw allow 443/tcp
```

Bővebb információ:

```
http://sugo.ubuntu.hu/10.10/html/serverguide/hu/firewall.html
https://help.ubuntu.com/community/UFW
```

```
Last login: Tue Oct 9 19:22:53 2018 from 152.66.244.97
cloud@cloud-5349:~$
```

(GUI nélkül)

▶ célszerű Linux kliensről

▶ pl.: HaEpUz VM

▶ célszerű ssh kulcs feltöltése

▶ My profile

▶ SSH public keys

▶ kulcs pár (priv, pub)

☐ generálása (pl.: ssh-keygen)

☐ vagy meglévő feltöltése

▶ VM/Home

▶ Install SSH keys

opcionális

Belépés: ssh

(GUI nélkül)

- ▶ Hasonlóan a kliens gépre is
- ▶ DE itt a default hálózati kapcsolatot leállítjuk (majd)
- ▶ VIGYÁZZ!!
 - ▶ ki ne zárd magad a VM-ről!
 - ▶ mindig legyen legalább egy belépési lehetőség
 - ▶ pl. a GW gépről a belső hálózaton keresztül

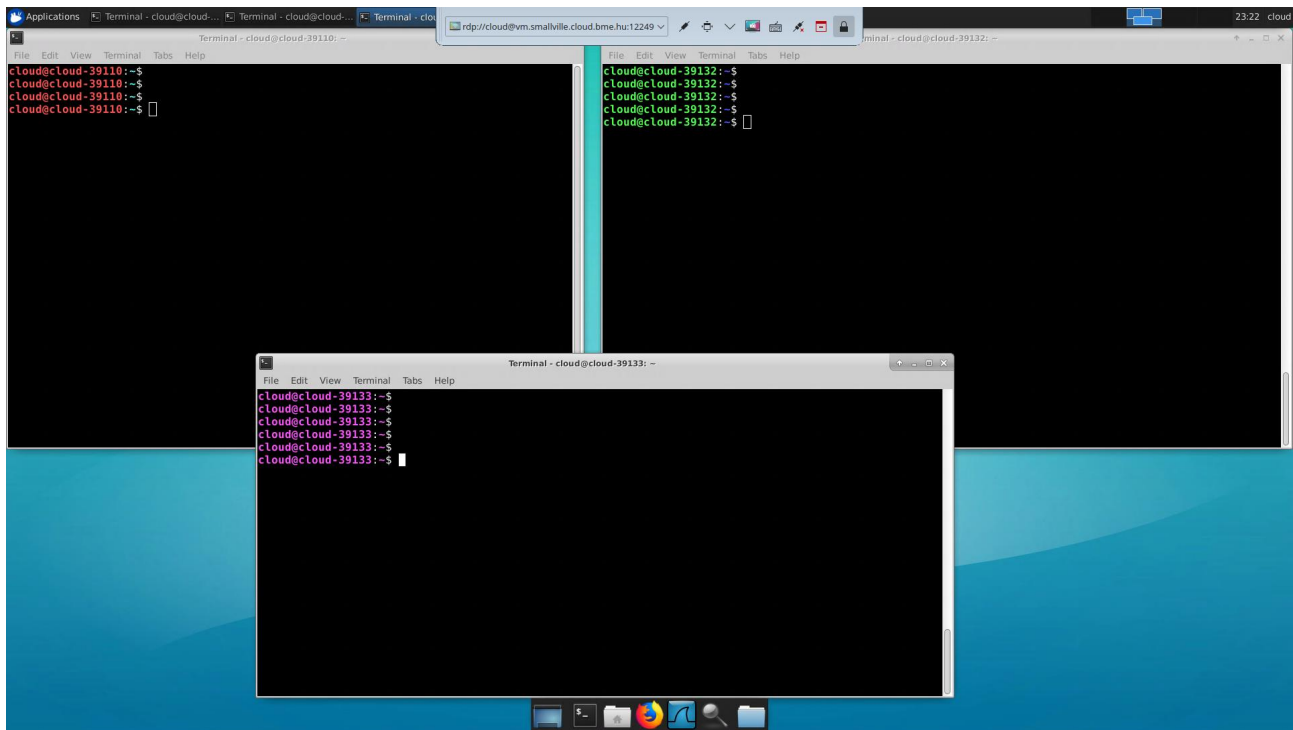
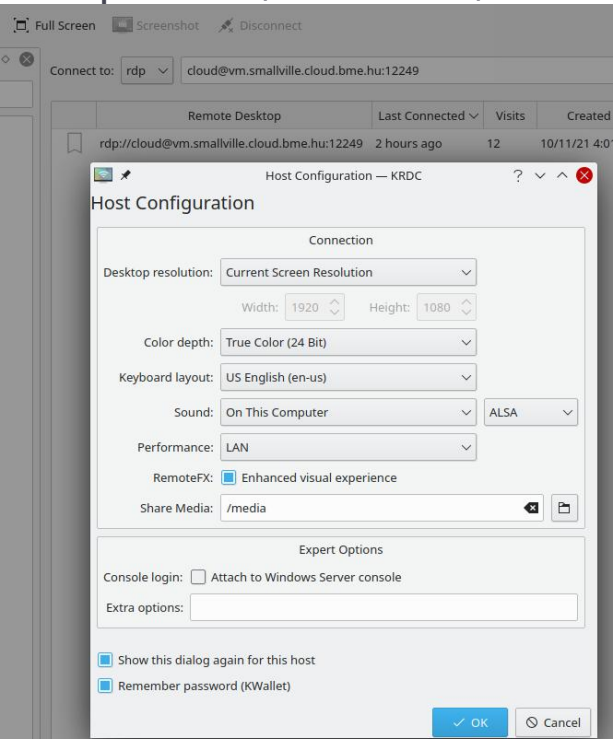
▶ Javaslat

opcionális (!)

- ▶ ssh kulcsot másoljuk fel mindkét gépre
- ▶ `scp -i ~/.ssh/haepuz_id_rsa -P 10305 ~/.ssh/haepuz_id_rsa cloud@vm.smallville.cloud.bme.hu:~/.ssh/id_rsa`

(xfce4 desktop)

- ▶ pl.: krdc, remmina, MS...



VM-ek konfigurálása: prompt színezés, hostname

▶ GW → piros (Smallville sablonban be van állítva)

```
GW:~$ cat .bashrc | sed -E 's/32m(.*)34m/31m\136m/' > .bashrc-gw;  
mv .bashrc-gw .bashrc
```

▶ utána: logout/login

▶ CLIENT → lila

```
CLIENT:~$ cat .bashrc | sed -E 's/32m(.*)34m/35m\135m/' > .bashrc-client;  
mv .bashrc-client .bashrc
```

▶ INTERNET/HaEpUz → zöld

▶ további lehetőség: sudo hostnamectl set-hostname CLIENT; sudo reboot

▶ célszerű /etc/hosts frissítése is (pl: 127.0.1.1 cloud-17124 CLIENT)

▶ ha kell: apt install sshpass

▶ ~/.bashrc: force_color_prompt=yes

▶ PS1=... 32m... 34m... vs. PS1=... 31m... 36m...

s üzemeltetése, H... ízs, BME-TMIT

VM-ek konfigurálása

▶ IPv6 kipucolása

- ▶ `sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1`
- ▶ `sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1`
- ▶ `sudo sysctl -w net.ipv6.conf.lo.disable_ipv6=1`

▶ vagy /etc/sysctl.conf fájlhoz hozzáadni

- ▶ `net.ipv6.conf.all.disable_ipv6=1`
- ▶ `net.ipv6.conf.default.disable_ipv6=1`
- ▶ `net.ipv6.conf.lo.disable_ipv6=1`

▶ utána: `sudo sysctl -p`

▶ resolvconf vs. systemd-resolved

- ▶ ~~`sudo dpkg-reconfigure resolvconf`~~ (Yes, OK) (csak Ubuntu 18.04-nél kell)

▶ ~~`sudo apt update; sudo apt install apache2`~~

2021-es VM-től
benne van



VM-ek konfigurálása

▶ Gateway (GW)

- ▶ `sudo systemctl stop bind9`
- ▶ `sudo ifconfig eth1 up`
- ▶ (vagy: `sudo ip link set dev eth1 up`)
- ▶ `sudo ifconfig eth1 10."ID".0.1/24`
- ▶ (vagy: `sudo ip addr add 10."ID".0.1/24 dev eth1`)

▶ Kliens (CLIENT)

- ▶ `sudo ifconfig eth1 up`
- ▶ `sudo ifconfig eth1 10."ID".0.2/24`

▶ ellenőrzés:

- ▶ `ifconfig` (vagy `ip addr`)
- ▶ `route -n` (vagy: `ip route`)
- ▶ `cat /etc/resolv.conf` és `resolvectl status`

+ Internet VM (külvilág)
Nézzük meg, milyen IP-t kapott!

VM-ek konfigurálása

- ▶ belépés: GW -> CLIENT
 - ▶ GW:~\$ ssh -Y 10."ID".0.2
- ▶ működik??
 - ▶ Igen: kliens "levágása" a default hálózatról
 - ▶ CLIENT:~\$ sudo ip link set dev eth0 down
 - ▶ Nem: további tesztelés

Összeköttetés tesztelése

- ▶ CLIENT <-> GW
 - ▶ GW <-> külvilág (INTERNET VM)
 - ▶ CLIENT <-> külvilág (INTERNET VM)
-
- ▶ mi működik, mi nem?

Hogyan tovább?

- ▶ Belső hálózatról (CLIENT) szeretnénk “netezni”
 - ▶ NAT
- ▶ Azért minden forgalmat nem szeretnénk engedélyezni
 - ▶ Firewall
- ▶ Manuális konfiguráció???
 - ▶ DHCP, DNS

NAT

iptables

SNAT konfigurálása (GW)

- ▶ Első lépés: forwarding engedélyezése
 - ▶ alapból nem tudjuk routerként használni a gépünket
 - ▶ `cat /proc/sys/net/ipv4/ip_forward`
 - ▶ engedélyezés
 - ▶ `sudo sysctl -w net.ipv4.ip_forward=1`
- ▶ címfordítás beállítása

SNAT konfigurálása (GW)

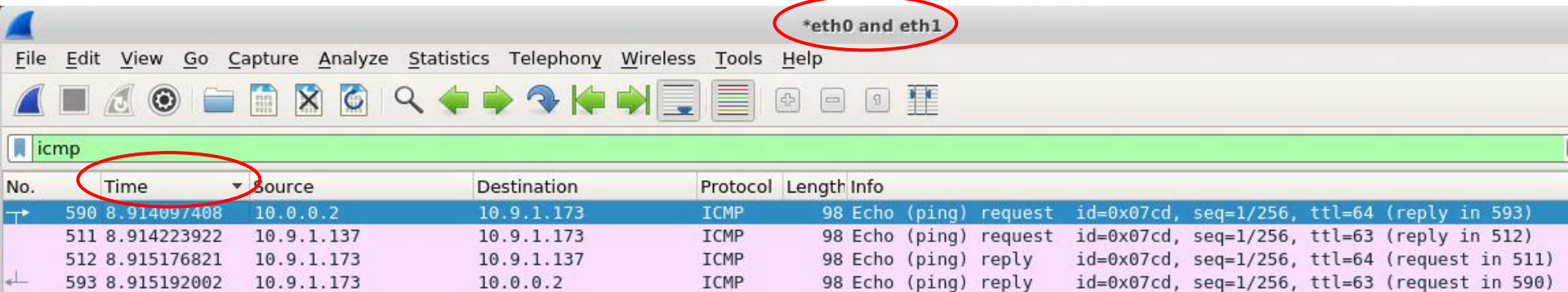
- ▶ Első lépés: forwarding engedélyezése
 - ▶ alapból nem tudjuk routerként használni a gépünket
 - ▶ `cat /proc/sys/net/ipv4/ip_forward`
 - ▶ engedélyezés
 - ▶ `sudo sysctl -w net.ipv4.ip_forward=1`
- ▶ címfordítás beállítása
 - ▶ `iptables -t nat`
 - ▶ `-A POSTROUTING` (append, új szabály hozzáfűzése a POSTROUTING láncához)
 - ▶ `-s 10."ID".0.0/24` (ha ez a source IP)
 - ▶ `-o eth0` (ha ez az output interfész)
 - ▶ `-j MASQUERADE` (akkor source IP fordítása dinamikusan)
 - ▶ (output interfésztől függően)

SNAT konfigurálása (CLIENT)

- ▶ default gateway beállítása
 - ▶ `sudo route add default gw 10."ID".0.1 [dev eth1]`
 - ▶ vagy: `sudo ip route add default via 10."ID".0.1`
- ▶ tesztelés
 - ▶ `ping 8.8.8.8`
 - ▶ `ping telex.hu ???`

SNAT vizsgálata

- ▶ Wireshark GW-en
- ▶ közben forgalom generálása CLIENT-ről INTERNET felé
- ▶ eth1-en bejövő/kimenő csomagok és
- ▶ eth0-án bejövő/kimenő csomagok
- ▶ Sorrend!
- ▶ iptables counterek figyelése (`watch -d "sudo iptables -t nat -nvL"`)



The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. The packet list pane on the left shows a list of captured packets, with the first packet (No. 590) selected. The packet details pane on the right shows the selected packet's details, including the ICMP Echo (ping) request. The packet bytes pane at the bottom shows the raw data of the selected packet. The interface is titled '*eth0 and eth1'.

No.	Time	Source	Destination	Protocol	Length	Info
590	8.914097408	10.0.0.2	10.9.1.173	ICMP	98	Echo (ping) request id=0x07cd, seq=1/256, ttl=64 (reply in 593)
511	8.914223922	10.9.1.137	10.9.1.173	ICMP	98	Echo (ping) request id=0x07cd, seq=1/256, ttl=63 (reply in 512)
512	8.915176821	10.9.1.173	10.9.1.137	ICMP	98	Echo (ping) reply id=0x07cd, seq=1/256, ttl=64 (request in 511)
593	8.915192002	10.9.1.173	10.0.0.2	ICMP	98	Echo (ping) reply id=0x07cd, seq=1/256, ttl=63 (request in 590)

DNAT konfigurálása (GW)

- ▶ Adott porton tegyük elérhetővé kívülről a belső gép
 - ▶ web szerverét (8080)
 - ▶ de előtte installáljuk! (apache2)
- ▶ címfordítás beállítása

DNAT konfigurálása (GW)

- ▶ Adott porton tegyük elérhetővé kívülről a belső gép
 - ▶ web szerverét (8080)
 - ▶ de előtte installáljuk! (apache2):
 - ▶ `sudo apt install apache2; sudo systemctl start apache2`
- ▶ címfordítás beállítása
 - ▶ `iptables -t nat`
 - ▶ `-A PREROUTING` (append, új szabály hozzáfűzése PREROUTING-hoz)
 - ▶ `-d 10.9.0.138` (ha ez a destination IP)
 - ▶ `-p tcp` (ha TCP protokoll)
 - ▶ `--dport 8080` (és 8080-as TCP destination port)
 - ▶ `-j DNAT` (akkor destination IP:port fordítása)
 - ▶ `--to-destination 10."ID".0.2:80` (a belső web szerverre)

DNAT tesztelése

- ▶ INTERNET VM gépről
 - ▶ web browser: lynx :)
 - ▶ `http://10.9.0.X`
 - ▶ `http://10.9.0.X:8080`
 - ▶ vagy nc (ha szükséges, apache2 leállítása)
 - ▶ GW, CLIENT: `nc -k -l 80`
 - ▶ INTERNET VM: `nc 10.9.0.X 80`
 - ▶ INTERNET VM: `nc 10.9.0.X 8080`
- ▶ Közben Wireshark és iptables counterek figyelése

Firewall

iptables

Firewall konfigurálása (GW)

▶ Jó tanácsok:

- ▶ default policy legyen DROP (vagy REJECT)
- ▶ a kívánt forgalmakat külön-külön, explicit módon engedélyezzük (ACCEPT)
- ▶ amelyik csomag végigmegy minden láncon és nincs illeszkedés, eldobásra kerül
- ▶ a végére betehetünk egy loggoló szabályt, ami az eldobás előtt egy log bejegyzést készít

Firewall konfigurálása (GW)

► Feladat

- az előadáson látott példa alapján konfiguráljuk fel a GW FORWARD láncát hasonló funkcionalitásra
- de most az ssh-val nem kell foglalkozni, csak a web forgalommal
- szerkesztéshez pl. nano
- ne lepődjünk meg az ufw üres láncaitól...
 - Uncomplicated Firewall
 - le van tiltva (`sudo systemctl disable ufw.service`)

Firewall konfigurálása (GW)

```
(mininet) 192.168.56.102 — Konsole
File Edit View Bookmarks Settings Help
File Edit Options Buffers Tools Sh-Script Help
#!/bin/bash

# delete chains
iptables -F FORWARD
iptables -X # delete all user-specified chains
iptables -Z # reset counters
# set default policies
iptables -P FORWARD DROP

# allow icmp traffic
iptables -A FORWARD -p icmp -j ACCEPT
# enable outgoing traffic
iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT
# enable backward direction if it was initiated from the internal domain
iptables -A FORWARD -d 10.0.0.0/24 -p tcp \
-m state --state ESTABLISHED,RELATED -j ACCEPT
# enable DNAT ports from the external net
iptables -A FORWARD ! -s 10.0.0.0/24 -p tcp --dport 80 \
-m state --state NEW -j ACCEPT
iptables -A FORWARD ! -s 10.0.0.0/24 -p tcp --dport 22 \
-m state --state NEW -j ACCEPT
# enable DNS
iptables -A FORWARD -p udp --sport 53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -j ACCEPT
# log dropped packets
iptables -A FORWARD -m limit --limit-burst 5 --limit 2/s \
-j LOG --log-prefix 'FIREWALL: ' --log-level 7
```

Átmenő forgalom szűrése
(FORWARD lánc)
előadáson bemutatott
példa

Firewall konfigurálása (GW)

```
#!/bin/bash

# delete chains
iptables -F FORWARD
iptables -X # delete all user-specified chains
iptables -Z # reset counters
# set default policies
iptables -P FORWARD DROP

# allow icmp traffic
iptables -A FORWARD -p icmp -j ACCEPT
# enable outgoing traffic
iptables -A FORWARD -s 10.0.0.0/24 -j ACCEPT
# enable backward direction if it was initiated from the internal domain
iptables -A FORWARD -d 10.0.0.0/24 -p tcp \
    -m state --state ESTABLISHED,RELATED -j ACCEPT
# enable DNAT ports from the external net
iptables -A FORWARD ! -s 10.0.0.0/24 -p tcp --dport 80 \
    -m state --state NEW -j ACCEPT
iptables -A FORWARD ! -s 10.0.0.0/24 -p tcp --dport 22 \
    -m state --state NEW -j ACCEPT
# enable DNS
iptables -A FORWARD -p udp --sport 53 -j ACCEPT
iptables -A FORWARD -p udp --dport 53 -j ACCEPT
# log dropped packets
iptables -A FORWARD -m limit --limit-burst 5 --limit 2/s \
    -j LOG --log-prefix 'FIREWALL: ' --log-level 7
```

Átmenő forgalom szűrése
(FORWARD lánc)
előadáson bemutatott
példa

Tesztelés

- ▶ ping, web, közben logok, counterek figyelése
 - ▶ CLIENT -> INTERNET

- ▶ INTERNET -> CLIENT

- ▶ Töröljük az icmp szabályt! Mi történik?
 - ▶ `tail -f /var/log/syslog`

DHCP

Installáljunk dhcp szerveret!

- ▶ GW VM-en telepítve van
 - ▶ `sudo apt-get install isc-dhcp-server`
 - ▶ (Ubuntu-t vagy Debian-t feltételezünk)
 - ▶ Internet Software Consortium implementációja
 - ▶ alapból nem indul
- ▶ tesztelés (újabb systemd)
 - ▶ `sudo systemctl status isc-dhcp-server`
- ▶ tesztelés (régebbi SysV init)
 - ▶ `sudo service isc-dhcp-server status`

Konfiguráljunk dhcp szervert!

▶ 1. lépés

- ▶ állítsuk be az interfészeket, ahol DHCP kéréseket kezelünk
- ▶ `/etc/default/isc-dhcp-server`

▶ 2. lépés

- ▶ konfiguráljuk a szervert
- ▶ `/etc/dhcp/dhcpd.conf`
- ▶ **csak a saját kliensünket szolgálja ki!**
 - ▶ **mástól jön kérés, ignoráljuk**
 - ▶ **saját kliens mindig ugyanazt az IP címet kapja**

▶ 3. lépés

- ▶ `isc-dhcp-server` service indítása:
 - ▶ `sudo systemctl start isc-dhcp-server`
 - ▶ `sudo systemctl status isc-dhcp-server`
 - ▶ `journalctl -b -u isc-dhcp-server -f`

Konfiguráljunk dhcp szerveret!

- ▶ 1. lépés
 - ▶ állítsuk be az interfészeket, ahol DHCP kéréseket kezelünk
 - ▶ /etc/default/isc-dhcp-server
 - ▶ INTERFACESv4="eth1"
- ▶ 2. lépés
 - ▶ konfiguráljuk a szerveret
 - ▶ /etc/dhcp/dhcpd.conf
 - ▶ **csak a saját kliensünket szolgálja ki!**
 - ▶ mástól jön kérés, ignoráljuk
 - ▶ saját kliens mindig ugyanazt az IP címet kapja
- ▶ 3. lépés
 - ▶ isc-dhcp-server service indítása:
 - ▶ sudo systemctl start isc-dhcp-server
 - ▶ sudo systemctl status isc-dhcp-server
 - ▶ journalctl -b -u isc-dhcp-server -f

```
subnet 10.0.0.0 netmask 255.255.255.0 {  
    range 10.0.0.102 10.0.0.150;  
    option domain-name-servers 8.8.8.8;  
    option domain-name "haepuz.hu";  
    option subnet-mask 255.255.255.0;  
    option routers 10.0.0.1;  
    option broadcast-address 10.0.0.255;  
    default-lease-time 600;  
    max-lease-time 7200;  
    host client1 {  
        hardware ethernet 02:00:01:4e:40:64;  
        fixed-address 10.0.0.101;  
    }  
    host client2 {  
        hardware ethernet 02:00:01:4d:20:64;  
    }  
    deny unknown-clients;  
}
```

Teszteljük a kliens gépről!

- ▶ Közben GW-en: wireshark capture
 - ▶ `/etc/ssh/sshd_config`: `X11Forwarding` `yes` és `X11UseLocalhost` `no`
 - ▶ `sudo systemctl restart sshd...` utána működik az X forwarding (`ssh -Y`)
- ▶ CLIENT
 - ▶ trükkösen csináljuk egy lépésben!
 - ▶ manuálisan konfigurált cím törlése
 - ▶ cím kérése dhcp-vel
 - ▶ `nohup sh -c 'sudo ip addr del 10.ID.0.2/24 dev eth1; sudo dhclient eth1'`
 - ▶ belépés GW-ről az új (dhcp) címen
 - ▶ routing tábla ellenőrzése
 - ▶ névfeloldás (`resolv.conf` fájl vagy `resolvectl status`) ellenőrzése
 - ▶ teszt: `ping telex.hu`

Kliens gép konfigurálása

- ▶ Ha nem akarjuk kézzel kérni a címet
 - ▶ eth1 interfész konfigurálása az /etc/network/interfaces fájlban:
 - ▶ auto eth1
 - ▶ iface eth1 inet dhcp
 - ▶ ezután használhatók a következő parancsok
 - ▶ sudo ifup eth1
 - ▶ sudo ifdown eth1
 - ▶ “auto” esetén indulásnál felkonfigurálódik

DNS

bind9

Házi feladat



bind9

- ▶ GW VM-en telepítve van
- ▶ `sudo apt-get install bind9`
- ▶ `sudo netstat -atn | grep -i listen`
- ▶ konfigurációs fájlok
 - ▶ `/etc/bind` könyvtár alatt
 - ▶ `named.conf.default-zones`
 - zone entry-k megadása
 - zone db hivatkozás (pl. `db.local`)
 - ▶ nézzünk meg pár példát!

```
;
; BIND data file for local loopback interface
$TTL      604800
@         IN      SOA      localhost. root.localhost. (
                        2      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200  ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       localhost.
@         IN      A        127.0.0.1
@         IN      AAAA     ::1
```

```
(mininet) 192.168.56.102 — Konsole
File Edit View Bookmarks Settings Help
File Edit Options Buffers Tools Conf Help
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

bind9 (db.root)

A példa alapján
konfiguráljuk be
a saját GW-t!

(named.conf.options)

```
; formerly NS.INTERNIC.NET
;
A.ROOT-SERVERS.NET. 3600000 IN NS A.A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET. 3600000 A 198.41.0.4
A.ROOT-SERVERS.NET. 3600000 AAAA 2001:503:BA3E::2:30
;
; FORMERLY NS1.ISI.EDU
;
B.ROOT-SERVERS.NET. 3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET. 3600000 A 192.228.79.201
;
; FORMERLY C.PSI.NET
;
C.ROOT-SERVERS.NET. 3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET. 3600000 A 192.33.4.12
;
; FORMERLY TERP.UMD.EDU
;
D.ROOT-SERVERS.NET. 3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET. 3600000 A 199.7.91.13
D.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2D::D
;
; FORMERLY NS.NASA.GOV
;
E.ROOT-SERVERS.NET. 3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET. 3600000 A 192.203.230.10
;
; FORMERLY NS.ISC.ORG
;
F.ROOT-SERVERS.NET. 3600000 NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET. 3600000 A 192.5.5.241
F.ROOT-SERVERS.NET. 3600000 AAAA 2001:500:2F::F
```

```
(mininet) 192.168.
File Edit View Bookmarks Settings Help
File Edit Options Buffers Tools Conf Help
# HeEpUz
acl goodclients {
    10.0.0.0/24;
    localhost;
};

options {
    directory "/var/cache/bind";

    # HaEpUz
    recursion yes;
    allow-query { goodclients; };
    forwarders {
        8.8.8.8;
    };
    forward only;

    dnssec-validation auto;

    auth-nxdomain no; # conform to RFC1035
    listen-on-v6 { any; };
};
```

GW konfigurálása, tesztelés

- ▶ bind9 indítása (vagy újraindítása)
 - ▶ `sudo systemctl enable named` (`sudo service named enable`)
 - ▶ `sudo systemctl start bind9` (`sudo service bind9 start`)
 - ▶ `sudo systemctl status bind9` (`sudo service bind9 status`)
 - ▶ milyen portokon figyel? milyen protokollt használ?

- ▶ DHCP átkonfigurálása
 - ▶ saját DNS szerver (8.8.8.8 helyett)
 - ▶ DHCP szerver újraindítás!
- ▶ forgalom rögzítése GW-en
 - ▶ wireshark vagy
 - ▶ `sudo tcpdump -i any -ne port 53 [-vvv]`

GW konfigurálása, tesztelés

- ▶ bind9 indítása (vagy újraindítása)
 - ▶ `sudo systemctl enable bind9` (`sudo service bind9 enable`)
 - ▶ `sudo systemctl start bind9` (`sudo service bind9 start`)
 - ▶ `sudo systemctl status bind9` (`sudo service bind9 status`)
 - ▶ milyen portokon figyel? milyen protokollt használ?
 - ▶ `sudo netstat -aputne | grep named`
 - ▶ udp és tcp!
 - ▶ 53, 953
- ▶ DHCP átkonfigurálása
 - ▶ saját DNS szerver (8.8.8.8 helyett)
 - ▶ DHCP szerver újraindítás!
- ▶ forgalom rögzítése GW-en
 - ▶ wireshark vagy
 - ▶ `sudo tcpdump -i any -ne port 53 [-vvv]`

CLIENT konfigurálása

- ▶ `sudo dhclient -v eth1`
- ▶ `cat /etc/resolv.conf`
 - ▶ `nameserver 10."ID".0.1`
- ▶ `sudo systemd-resolve --status`
- ▶ (systemd-resolved vs. resolvconf)
- ▶ tesztelés
 - ▶ `ping telex.hu`

CLIENT: “DNS teszt”

- ▶ tesztelés a kliens gépről (közben GW-en capture)
 - ▶ `dig stanford.edu +norecurse +short`
 - ▶ `dig stanford.edu +short`
 - ▶ `dig stanford.edu +norecurse +short`
 - ▶ `dig @10.0.0.1 stanford.edu +norecurse +short`
 - ▶ `dig -t A @10.0.0.1 stanford.edu +trace`

CLIENT: “DNS teszt”

- ▶ tesztelés a kliens gépről (közben GW-en capture)
 - ▶ `dig stanford.edu +norecurse +short`
 - ▶ nincs találat, referral jön vissza (root DNS szerverek listája)
 - ▶ `dig stanford.edu +short`
 - ▶ van találat, rekurzív lekérdezések (->10.0.0.1->8.8.8.8)
 - ▶ `dig stanford.edu +norecurse +short`
 - ▶ nincs találat a local stub-tól (systemd-resolved)
 - ▶ `dig @10.0.0.1 stanford.edu +norecurse +short`
 - ▶ van találat, cache-ből (10.0.0.1 server)
 - ▶ `dig -t A @10.0.0.1 stanford.edu +trace`
 - ▶ iteratív lekérdezés nyomkövetése

Összefoglalás

- ▶ Egyszerű teszhálózat kialakítása
 - ▶ Smallville CIRCLE Cloud
 - ▶ GW, CLIENT, belső hálózat
- ▶ Hálózati funkciók vizsgálata, konfigurálása
- ▶ NAT
 - ▶ SNAT, DNAT
 - ▶ iptables
- ▶ Firewall
 - ▶ iptables
- ▶ DHCP
 - ▶ isc-dhcp-server
- ▶ DNS
 - ▶ bind9

