Sessão 2: Firewall

1) Configuração inicial do firewall

Criar DMZ host-only faixa 10.0.42.0/24, ip host físico 10.0.42.254. Criar Intranet host-only faixa 192.168.42.0/24, ip host físico 192.168.42.254.

Clonar debian-template para `fw` com 2 interfaces de rede, 1 bridge dhcp, 2 host-only estático 10.0.42.1/24, 3 host-only estático 192.168.42.1/24.

Renomear vm.

```
# bash ~/changehost.sh fw
```

Configurar rede.

```
# cat /etc/network/interfaces
source /etc/network/interfaces.d/*

auto lo enp0s3 enp0s8 enp0s9

iface lo inet loopback

iface enp0s3 inet dhcp

iface enp0s8 inet static
address 10.0.42.1/24

iface enp0s9 inet static
address 192.168.42.1/24
```

Habilitar repasse.

```
# sed -i '/net.ipv4.ip_forward/s/^#//' /etc/sysctl.conf
```

```
# sysctl -p
net.ipv4.ip_forward = 1
```

Habilitar nat.

```
# iptables -t nat -A POSTROUTING -s 10.0.42.0/24    -o enp0s3 -j MASQUERADE
```

```
# iptables -t nat -A POSTROUTING -s 192.168.42.0/24 -o enp0s3 -j MASQUERADE
```

Instalar iptables-persistent, salvar regras.

```
# apt-get install iptables-persistent -y
```

2) Configuração do servidor DNS

Instale os pacotes.

```
# apt-get install nsd unbound dnsutils
```

Configure as chaves TLS de controle.

```
# nsd-control-setup
```

Gerar chave TSIG aleatória para transferência de zona.

```
# dd if=/dev/random of=/dev/stdout count=1 bs=32 | base64
1+0 registros de entrada
1+0 registros de saída
twjSFcE/A1sBoNfNgdv+Gy3z9GLV9yC8SgobK5hyaVg=
32 bytes copiados, 0,000523239 s, 61,2 kB/s
```

Crie o arquivo `/etc/nsd/nsd.conf`. Obs.: não configuraremos DNS secundário por razões de tempo).

```
server:
  ip-address: 127.0.0.1
  ip-address: 10.0.42.1
  ip-address: 192.168.42.1
  do-ip4: yes
  port: 8053
  username: nsd
  zonesdir: "/etc/nsd"

  logfile: "/var/log/nsd.log"
  pidfile: "/run/nsd/nsd.pid"
  hide-version: yes
  version: "intnet DNS"
  identity: "unidentified server"

remote-control:
  control-enable: yes
  control-interface: 127.0.0.1
  control-port: 8952
  server-key-file: "/etc/nsd/nsd_server.key"
  server-cert-file: "/etc/nsd/nsd_server.pem"
  control-key-file: "/etc/nsd/nsd_control.key"
  control-cert-file: "/etc/nsd/nsd_control.pem"

key:
  name: "inkey"
  algorithm: sha512
  secret: "mIl6XgI2u3NN8a8oldMqTalaTh/dgON0Txg4VqTC4bc="

pattern:
  name: "inslave"
  notify: 10.0.42.11 inkey
  provide-xfr: 10.0.42.11 inkey

zone:
  name: "intnet"
  include-pattern: "inslave"
  zonefile: "intnet.zone"

zone:
  name: "42.0.10.in-addr.arpa"
  zonefile: "10.0.42.zone"
  include-pattern: "inslave"
```

Crie o arquivo de zona direta `/etc/nsd/intnet.zone`.

```
$TTL 86400 ; (1 day)
$ORIGIN intnet.

@       IN   SOA   fw.intnet.   admin.intnet. (
                   2018110300   ;serial (YYYYMMDDnn)
                   14400        ;refresh (4 hours)
                   1800         ;retry (30 minutes)
                   1209600      ;expire (2 weeks)
                   3600         ;negative cache TTL (1 hour)
                   )

@       IN   NS                 fw.intnet.
@       IN   NS                 ns2.intnet.

@       IN   MX    10           mx1.intnet.
@       IN   MX    20           mx2.intnet.

fw      IN    A                 10.0.42.1
ldap    IN    A                 10.0.42.2
nfs     IN    A                 10.0.42.3

ns2     IN    A                 10.0.42.11
mx1     IN    A                 10.0.42.12
mx2     IN    A                 10.0.42.13

files   IN    CNAME             nfs
pop     IN    CNAME             mx1
imap    IN    CNAME             mx1
```

Crie o arquivo de zona reversa `/etc/nsd/10.0.42.zone`.

```
$TTL 86400 ; (1 day)
$ORIGIN 42.0.10.in-addr.arpa.

@       IN   SOA   fw.intnet.   admin.intnet. (
                   2018110300   ;serial (YYYYMMDDnn)
                   14400        ;refresh (4 hours)
                   1800         ;retry (30 minutes)
                   1209600      ;expire (2 weeks)
                   3600         ;negative cache TTL (1 hour)
                   )

@       IN   NS                 fw.intnet.
@       IN   NS                 ns2.intnet.

@       IN   MX    10           mx1.intnet.
@       IN   MX    20           mx2.intnet.

1       IN   PTR                fw.intnet.
2       IN   PTR                ldap.intnet.
3       IN   PTR                nfs.intnet.

11      IN   PTR                ns2.intnet.
12      IN   PTR                mx1.intnet.
13      IN   PTR                mx2.intnet.
```

Cheque a configuração, inicie o serviço e verifique se está rodando.

```
# nsd-checkconf /etc/nsd/nsd.conf
```

```
# systemctl restart nsd
```

```
# tail /var/log/nsd.log
[2018-11-03 12:12:25.905] nsd[1820]: notice: nsd starting (NSD 4.1.14)
[2018-11-03 12:12:25.923] nsd[1821]: notice: nsd started (NSD 4.1.14), pid 1820
```

```
# ss -tunlp | grep 8053
udp    UNCONN     0      0      192.168.42.1:8053                  *:*
users:(("nsd",pid=2821,fd=6),("nsd",pid=2820,fd=6),("nsd",pid=2819,fd=6))
udp    UNCONN     0      0      10.0.42.1:8053                  *:*
users:(("nsd",pid=2821,fd=5),("nsd",pid=2820,fd=5),("nsd",pid=2819,fd=5))
udp    UNCONN     0      0      127.0.0.1:8053                  *:*
users:(("nsd",pid=2821,fd=4),("nsd",pid=2820,fd=4),("nsd",pid=2819,fd=4))
tcp    LISTEN     0      128    192.168.42.1:8053                  *:*
users:(("nsd",pid=2821,fd=9),("nsd",pid=2820,fd=9),("nsd",pid=2819,fd=9))
tcp    LISTEN     0      128    10.0.42.1:8053                  *:*
users:(("nsd",pid=2821,fd=8),("nsd",pid=2820,fd=8),("nsd",pid=2819,fd=8))
tcp    LISTEN     0      128    127.0.0.1:8053                  *:*
users:(("nsd",pid=2821,fd=7),("nsd",pid=2820,fd=7),("nsd",pid=2819,fd=7))
```

Teste a resolução direta e reversa.

```
# dig @127.0.0.1 -p 8053 ldap.intnet +noadditional

; <<>> DiG 9.10.3-P4-Debian <<>> @127.0.0.1 -p 8053 ldap.intnet +noadditional
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49827
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;ldap.intnet.                   IN      A

;; ANSWER SECTION:
ldap.intnet.            86400   IN      A       10.0.42.2

;; AUTHORITY SECTION:
intnet.                 86400   IN      NS      fw.intnet.
intnet.                 86400   IN      NS      ns2.intnet.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#8053(127.0.0.1)
;; WHEN: Sat Nov 03 13:05:06 -03 2018
;; MSG SIZE  rcvd: 123
```

```
# dig @127.0.0.1 -p 8053 -x 10.0.42.3 +noadditional

; <<>> DiG 9.10.3-P4-Debian <<>> @127.0.0.1 -p 8053 -x 10.0.42.3 +noadditional
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23418
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;3.42.0.10.in-addr.arpa.                IN      PTR

;; ANSWER SECTION:
3.42.0.10.in-addr.arpa. 86400   IN      PTR     nfs.intnet.

;; AUTHORITY SECTION:
42.0.10.in-addr.arpa.   86400   IN      NS      fw.intnet.
42.0.10.in-addr.arpa.   86400   IN      NS      ns2.intnet.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#8053(127.0.0.1)
;; WHEN: Sat Nov 03 13:05:51 -03 2018
;; MSG SIZE  rcvd: 110
```

Crie o arquivo `/etc/unbound/unbound.conf`.

```
server:
  interface: 127.0.0.1
  interface: 10.0.42.1
  interface: 192.168.42.1
  port: 53

  access-control: 127.0.0.0/8 allow
  access-control: 10.0.42.0/24 allow
  access-control: 192.168.42.0/24 allow

  cache-min-ttl: 300
  cache-max-ttl: 14400

  local-zone: "intnet" nodefault
  domain-insecure: "intnet"

  local-zone: "10.in-addr.arpa." nodefault
  domain-insecure: "10.in-addr.arpa."

  verbosity: 1
  prefetch: yes
  hide-version: yes
  hide-identity: yes
  use-caps-for-id: yes
  rrset-roundrobin: yes
  minimal-responses: yes
  qname-minimisation: yes
  do-not-query-localhost: no

stub-zone:
  name: "intnet"
  stub-addr: 127.0.0.1@8053

stub-zone:
  name: "42.0.10.in-addr.arpa."
  stub-addr: 127.0.0.1@8053

forward-zone:
  name: "."
  forward-addr: 8.8.8.8
  forward-addr: 8.8.4.4

include: "/etc/unbound/unbound.conf.d/*.conf"
```

Reinicie o unbound.

```
# systemctl restart unbound
```

Reconfigure o DNS *system-wide*.

```
# cat /etc/resolv.conf
domain intnet.
search intnet.
nameserver 127.0.0.1
```

Teste a resolução de domínios internos e externos usando o unbound.

```
# dig fw.intnet

; <<>> DiG 9.10.3-P4-Debian <<>> fw.intnet
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14190
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;fw.intnet.                     IN      A

;; ANSWER SECTION:
fw.intnet.              86400   IN      A       10.0.42.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 03 13:09:15 -03 2018
;; MSG SIZE  rcvd: 54
```

```
# dig openbsd.org

; <<>> DiG 9.10.3-P4-Debian <<>> openbsd.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20180
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;openbsd.org.                   IN      A

;; ANSWER SECTION:
openbsd.org.            21599   IN      A       129.128.5.194

;; Query time: 482 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 03 13:09:21 -03 2018
;; MSG SIZE  rcvd: 56
```

3) Configuração da VM template

Ligue a VM `debian-template` e reconfigure o DNS padrão.

```
# hostname ; whoami
debian-template
root
```

```
# cat /etc/resolv.conf
domain intnet.
search intnet.
nameserver 10.0.42.1
```

4) Configuração do DNSSEC

Instale as ferramentas de suporte.

```
# apt-get install ldnsutils haveged
```

Crie as chaves de assinatura de zona (ZSK) e chave (KSK).

```
# cd /etc/nsd/

# export ZSK=`ldns-keygen -a RSASHA1-NSEC3-SHA1 -b 2048 intnet`

# export KSK=`ldns-keygen -k -a RSASHA1-NSEC3-SHA1 -b 2048 intnet`

# ls Kintnet.+007+* -1
Kintnet.+007+50114.key
Kintnet.+007+50114.private
Kintnet.+007+64113.ds
Kintnet.+007+64113.key
Kintnet.+007+64113.private

# rm Kintnet.+007+*.ds
```

Assine a zona `intnet.zone`.

```
# ldns-signzone -n -p -s $(head -n 1000 /dev/random | sha1sum | cut -b 1-16)
intnet.zone $ZSK $KSK

# ls intnet.zone* -1
intnet.zone
intnet.zone.signed
```

Configure o `nsd` para usar a zona assinada.

```
# cat /etc/nsd/nsd.conf | grep intnet.zone.signed -B3
zone:
  name: "intnet"
  include-pattern: "inslave"
  zonefile: "intnet.zone.signed"

# nsd-control reconfig
reconfig start, read /etc/nsd/nsd.conf
ok

# nsd-control reload intnet
ok
```

Pesquise os registros DNSKEY do domínio no `nsd`, verificando as chaves ZSK e KSK.

```
# dig DNSKEY intnet. @localhost +multiline +norec -p 8053

; <<>> DiG 9.10.3-P4-Debian <<>> DNSKEY intnet. @localhost +multiline +norec -p 8053
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37343
;; flags: qr aa; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;intnet.                        IN DNSKEY

;; ANSWER SECTION:
intnet.                 86400 IN DNSKEY 256 3 7 (
                              AwEAAc2pUUOTiK7+pW0bz6ovwIPFcbbNkwhltxaIVCuX
                              OpS2uGufu9m15AW6hKb8JHLNlRMNbkeDcwRW996cpRqz
                              QWt/Ya1e4xfbyUkdoE6+YolAt6SBgkH1Nsi7MGtiz0w3
                              C8GORqJSF6WvreEJyEAdcxP8A+6a8zqZ69Y44udafpiu
                              nSh773i1txNgNER0gLzQbdvQujXRmork/HCtjeDCNWzg
                              1xqhXqnD4IVeIjGeB05uxcTpFZ6SLN25cfoECesqk/zs
                              VafUJdCPxqaGd3szaDvTVhZ37eGfY1pZNXNL826NRNVF
                              UdNCfeWGVL13gGAyFvxUxfR/Bwtpkr8Y1Ts/4Pc=
                              ) ; ZSK; alg = NSEC3RSASHA1; key id = 25253
intnet.                 86400 IN DNSKEY 257 3 7 (
                              AwEAAcLaf9zFlDEL5dWhB4HzWx6iptWnj42WOUIZmT6f
                              7GEOwgBBUuT88Q3dZQwWSvydveH16TNUtt7/7JJJPk4H
                              JjUS79lmLbahUvDEgTwnyphiKEFGWmcVo449o6oqB5mo
                              1kiWkMepq51QYFATHEjG2kRib47LDejZQ6VrnjeHEq0w
                              jnRQbp1rrp217LuvayFgKBVJgpswQBNI8yaqmZO4oPjd
                              i21oH2CyjnFW2x/FWoWlv373l/r426QxQL8OfOqa4EC+
                              a1tBOoIsZanlqViOOzHdhYhaxumZhou0Q7/AsPZveFfu
                              BSCAyFX4tJIClxI51uES6hB6obNaOT5OoOMzOss=
                              ) ; KSK; alg = NSEC3RSASHA1; key id = 48774

;; Query time: 0 msec
;; SERVER: 127.0.0.1#8053(127.0.0.1)
;; WHEN: Sat Nov 03 16:13:34 -03 2018
;; MSG SIZE  rcvd: 587
```

Teste uma resolução de nome direta, via unbound, usando DNSSEC.

```
# dig nfs.intnet +dnssec +multiline

; <<>> DiG 9.10.3-P4-Debian <<>> nfs.intnet +dnssec +multiline
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30386
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;nfs.intnet.            IN A

;; ANSWER SECTION:
nfs.intnet.             86385 IN A 10.0.42.3
nfs.intnet.             86385 IN RRSIG A 7 2 86400 (
                               20181201191314 20181103191314 25253 intnet.
                               SldCjrjnb8iQ+ozjJBIOh8t+BNX7iqRffJ6qSQtj32W9
                               2FCmxW/TCkrMZ4RM1ViqzMVnsY3yCmqD+8jHVvVH3Bp6
                               Jon1iEYAfhUPq4NcXH4mjsZU8Ite8lnox3krpeF9DhRr
                               mvNibmJyq6clwNu6MIoOySY2odHrwmW7rg0vYmdtQTLs
                               vuBdaZ+bOs959Cf0lGoUItHPVKGBirWoTf9i0qC5QdSK
                               miMNUgBdCWxRRe+zCPLdV8p1adW3yFKA+LQoy6IV5w7y
                               0srO/dNzpmBGYIpWXbygYFaJ26zBlIViO9GI09TDcvoc
                               4t2t+FvSwKmSa3tP7Q9ZSoMMSQXy89uauQ== )

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Nov 03 16:18:02 -03 2018
;; MSG SIZE  rcvd: 349
```

Caso fosse desejável exportar a configuração DNS para um *registrar* hierarquicamente superior (fechando a cadeia de verificação DNS), pode-se gerar os registros DS — *delegation of signing* — das chaves com o comando abaixo.

```
# ldns-key2ds -n -1 intnet.zone.signed && ldns-key2ds -n -2 intnet.zone.signed
intnet. 86400   IN      DS      48774 7 1 571d6a2b7822eb6c6989b8ede2e9c38d395ab5e9
intnet. 86400   IN      DS      48774 7 2
57e574424987489e222ce4b3ad1abef58d6638c977193257f8202fc141944615
```