FACULTEIT INGENIEURSWETENSCHAPPEN
EN ARCHITECTUUR

Beveiliging van netwerken en computers

Bert De Saffel

Master in de Industriële Wetenschappen: Informatica Academiejaar 2018–2019

UNIVERSITEIT
GENT

Inhoudsopgave

Hoofdstuk 1

Routing + DNS

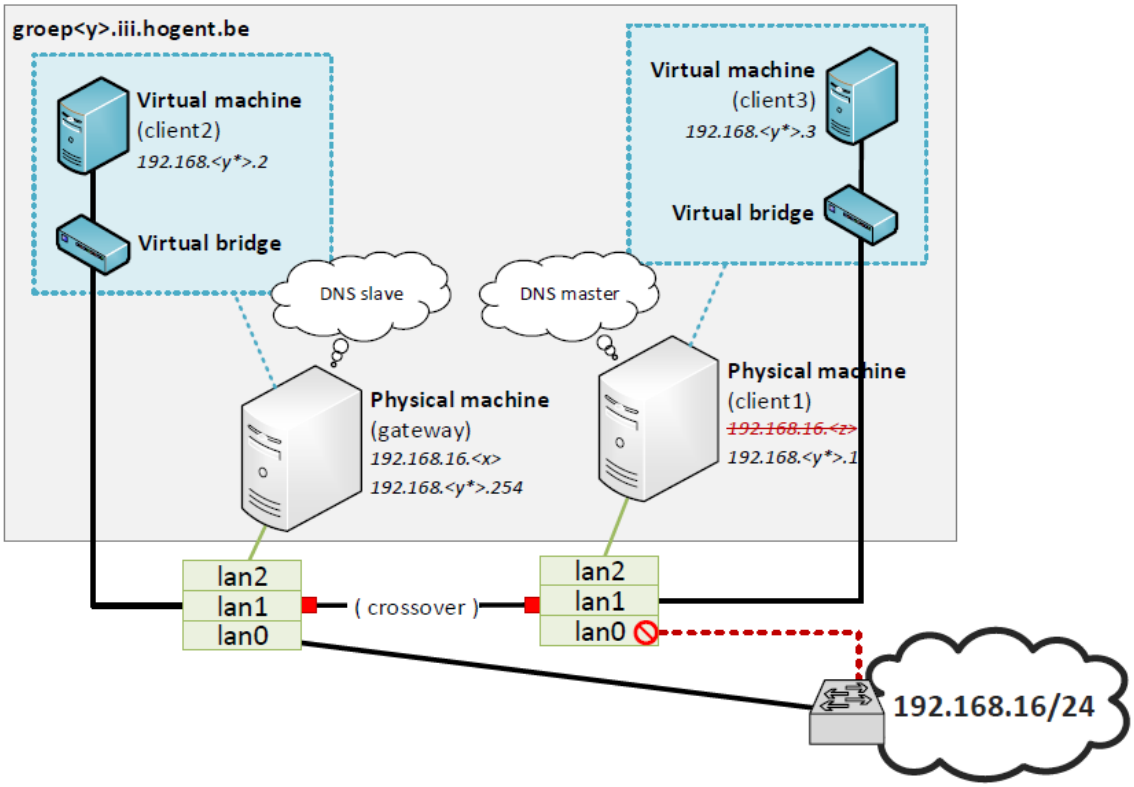
De bedoeling van dit labo is een netwerkconfiguratie op te stellen en een DNS-server op te zetten die je in latere labo's nog zal gebruiken. Zorg er dus voor dat je de configuratie waar mogelijk persistent maakt, en eventueel de nodige commando's in scripts opneemt zodat je tijdens volgende labo's de opstelling snel kan herstellen. Vooraleer aan de instellingen van de (fysieke) labotoestellen iets te veranderen maak je een volledige backup van de \etc directory (tar -cvjf \root \backup_etc.tar.bz2 \etc). Editeer geen enkel configuratiebestand zonder er eerst een kopie van te maken!

Voor dit labo werken we met groepjes van twee studenten. Iedere groep zal zich ontfermen over één DNS-domein dat vier hosts omvat (twee fysieke toestellen en twee virtuele machines). Ieder fysiek toestel zal dus als host fungeren voor één virtuele machine. Figuur 1.1 geeft een algemeen overzicht van de opstelling voor één groep. Voor de uitwerking van dit labo wordt de groep op figuur 1.2 gebruikt.

1.1 Routing

Voor elke groep bestaat de opstelling uit vier verschillende hosts:

- **gateway**: deze verbindt het interne netwerk van jouw groep met het HoGent netwerk via onze gateway 192.168.16.8. Dit toestel is via een crosskabel (lan1) verbonden met de tweede fysieke machine (client1).
- **client1**: deze is via een crosskabel (lan1) verbonden met de gateway. Merk op dat dit toestel niet rechtstreeks verbonden is met het HoGent netwerk!
- **client2**: dit is een virtuele machine die draait op de gateway. Deze virtuele machine is via een virtuele bridge verbonden met het interne netwerk (lan1) van de gateway.
- **client3**: dit is een virtuele machine die draait op client1. Deze virtuele machine is via een virtuele bridge verbonden met het interne netwerk (lan1) van client1.



Figuur 1.1: Opstelling

ivory	*hilbert*	*<gateway>*	*<client1>*
groep20		groepXX.iii.hogent.be	
192.168.70.254	*192.168.70.1*	*lan1*	*lan1*
192.168.16.168		*lan0*	

Figuur 1.2: Een groep

1.1.1 Configuratie IP-adressen

Voor de netwerkconfiguratie maak je overal gebruik van statische IP-adressen (ook voor lan0 op de gateway). Om te testen kan je eerst gebruikmaken van het *ip* commando, maar uiteindelijk is het eenvoudigst om een configuratiebestand te voorzien per interface. De configuratiebestanden vind je bij Fedora terug in de folder `/etc/sysconfig/network-scripts/`.

- **Gateway**:
  - `ifcfg-lan0`:

    ```
    DEVICE=lan0
    BOOTPROTO=none
    ONBOOT=yes
    NETMASK=255.255.255.0
    IPADDR=192.168.16.168
    GATEWAY=192.168.16.8
    ```

  - `ifcfg-lan1`:

    ```
    DEVICE=lan0
    BOOTPROTO=none
    ONBOOT=yes
    NETMASK=255.255.255.0
    IPADDR=192.168.70.254
    ```

- **Client1**:
  - `ifcfg-lan1`:

    ```
    DEVICE=lan1
    BOOTPROTO=none
    ONBOOT=yes
    NETMASK=255.255.255.0
    IPADDR=192.168.70.1
    GATEWAY=192.168.70.254
    ```

- **Client2**:
  - `ifcfg-enp0s3`:

    ```
    DEVICE=enp0s3
    BOOTPROTO=none
    ONBOOT=yes
    NETMASK=255.255.255.0
    IPADDR=192.168.70.2
    GATEWAY=192.168.70.254
    ```

- **Client3**:
  - `ifcfg-enp0s3`:

```
DEVICE=enp0s3
BOOTPROTO=none
ONBOOT=yes
NETMASK=255.255.255.0
IPADDR=192.168.70.3
GATEWAY=192.168.70.254
```

1.1.2 OSPF

Op de gateway gebruik je OSPF om de route naar jouw subnet te multicasten. Als router-software maak je gebruik van quagga en twee zelfgemaakte configuratiebestanden zebra.conf en ospfd.conf die je in de directory `/etc/quagga` plaatst. Aangezien iedere gateway rechtstreeks verbonden is met het 192.168.16.0/24 netwerk laten we dit overeenstemmen met area 0. Het is dus niet nodig om bijkomende areas in het leven te roepen! Ken aan je interfaces geen IP-adressen toe via quagga maar doe dit dus op de traditionele manier met het commando ip of via ifcfg-files. Vergeet niet om routing actief te zetten op de nodige hosts. Om te testen of je configuratie werkt, moet je zowel de zebra daemon als de ospfd daemon starten.

- **zebra.conf**:

```
hostname ivory
password pass
enable password pass
log stdout
!
interface lan0
!
interface lan1
!
```

- **ospfd.conf**:

```
hostname ivory
password pass
enable password pass
log stdout
!
interface lan0
!
interface lan1
!
router ospf
        redistribute connected
        network 192.168.16.0/24 area 0.0.0.0
!
```

Voeg `net.ipv4.ip_forward = 1` toe aan het bestand `/etc/sysctl.conf`. Voer nu het commando `systemctl status/restart/enable zebra/ospfd` uit. *Restart* zal de daemon herstarten en *enable* geeft aan dat de daemon bij de bootprocedure moet opgestart worden. Met *status* kan nagegaan worden of dat de configuratie correct verlopen is.

1.2 DNS

Binnen de opstelling configureer je ook twee DNS-servers die verantwoordelijk zijn voor het subdomein van de groep (groep20.iii.hogent.be). **client1** doet dienst als primaire (master) DNS-server, de **gateway** als secundaire (slave) DNS-server. Binnen je domein voorzie je zowel een forward als een reverse DNS lookup zone. Alle aanvragen die niet voor jouw domein bedoeld zijn stuur je via een **forwarder** door naar 192.168.16.8.

1.2.1 Configuratie named

Wij hebben reeds voor jou een DNS-root-server geconfigureerd. Bijgevolg kunnen alle DNS-aanvragen die geen betrekking hebben op jouw domein doorgestuurd worden naar 192.168.16.8. Dit is ook de default-gateway van de router en moet als dusdanig worden ingesteld. Jouw DNS-server voorziet in de naamgeving voor de vier hosts in het domein. Om voldoende redundantie te hebben, configureer je op de gateway een secundaire nameserver.

Voor DNS maken we gebruik van de BIND/named service die reeds op de fysieke toestellen geïnstalleerd is. De configuratie moet je zelf nog aanpassen of aanmaken. Maak hiervoor gebruik van volgende directories en bestanden:

- `/etc/named.conf`: algemene configuratie BIND/named.
- `/var/named/`: zonebestanden voor jouw domein

Om te testen of het configuratiebestand en de zonebestanden correct zijn, kan je respectievelijk gebruikmaken van de `named-checkconf` en `named-checkzone` commando's. Eenmaal de configuratie correct is, kan je de named service (her)starten via het systemctl commando. Voor de virtuele machines gebruik je als hostname de naam van je toestel, gevolgd door 'VM'. De virtuele machine op computer Kronecker zal bv. de naam KroneckerVM hebben. Voorzie zowel een forward als een reverse DNS lookup zone die de vier hosts bevat en test grondig uit! Aangezien veel services die we tijdens de labo's gebruiken steunen op reverse DNS, is het belangrijk dat deze correct geconfigureerd is.

- **/etc/named.conf**:
  - client1:

```
options {
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
```

```
        memstatistics-file "var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes,
        empty-zones-enable no;
        forwarders { 192.168.16.8; };
};

logging {
        channel default_debug {
                syslog daemon;
                severity dynamic;
        }
};

zone "groep20.iii.hogent.be" IN {
        type master;
        file "groep20.iii.hogent.be";
        allow-transfer { 192.168.70.254; };
};

zone "70.168.192.in-addr.arpa" {
        type master;
        file "70.168.192.in-addr.arpa";
        allow-transfer { 192.168.70.254; };
};
```

- gateway:

```
options {
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes,
        empty-zones-enable no;
        forwarders { 192.168.16.8; };
};

logging {
        channel default_debug {
                syslog daemon;
                severity dynamic;
        }
};

zone "groep20.iii.hogent.be" IN {
        type slave;
        file "groep20.iii.hogent.be";
```

```
        masters { 192.168.70.254; };
};

zone "70.168.192.in-addr.arpa" {
        type slave;
        file "70.168.192.in-addr.arpa";
        masters { 192.168.70.254; };
};
```

- **/var/named/groep20.iii.hogent.be**

```
$TTL 60
@ IN SOA groep20.iii.hogent.be. bert.desaffel.ugent.be (1 60 1H 60 3H)
  IN NS  hilbert
  IN NS  ivory
hilbert         IN      A       192.168.70.1
hilbertVM       IN      A       192.168.70.3
ivory           IN      A       192.168.70.254
ivoryVM         IN      A       192.168.70.4
```

- **/var/named/70.168.192.in-addr.arpa**

```
$TTL 60
@   IN SOA 70.168.192 bert.desaffel.ugent.be (1 60 1H 60 3H)
    IN NS hilbert.groep20.iii.hogent.be.
1   IN PTR hilbert.groep20.iii.hogent.be.
3   IN PTR hilbertVM.groep20.iii.hogent.be.
2   IN PTR ivoryVM.groep20.iii.hogent.be.
254 IN PTR ivory.groep20.iii.hogent.be.
```

1.2.2 Clientconfiguratie

Alle hosts moeten gebruikmaken van de eigen DNS-servers, hiervoor pas je `/etc/resolv.conf` aan. Voeg aan dit bestand ook een optie toe om de verschillende DNS-aanvragen over beide nameservers te verdelen. Zorg er voor dat DHCP uitgeschakeld is (BOOTPROTO=none in de ifcfg-files) voor elke netwerkinterface van de host! Indien dit niet het geval is, zal de dhcp-client bij elke herstart de inhoud van het /etc/resolv.conf bestand overschrijven.

Bovendien stel je ook op elk van de 4 clients de juiste hostname in, maak hierbij gebruik van de Fully Qualified Domain Name (FQDN). Om de hostname in te stellen kan je gebruikmaken van onderstaande commando's.

```
hostnamectl set-hostname --static <name>.groep20.iii.hogent.be
hostnamectl set-hostname --transient <name>.groep20.iii.hogent.be
hostnamectl set-hostname --pretty <name>.groep20.iii.hogent.be
```

Op alle vier de toestellen in `/etc/resolv.conf`:

```
domain groep20.iii.hogent.be
nameserver 192.168.70.1
nameserver 192.168.70.254
options rotate
```

1.3 Uittesten

Vooraleer de opstelling af te breken test je deze grondig uit! Eventueel kan je ook alle machines eens herstarten, om na te gaan of de configuratie volledig persistent is.

Uiteindelijk moet je vanaf elke host alle toestellen binnen het eigen netwerk kunnen bereiken. Dit kan je eenvoudig testen via het ping commando. Bovendien moet je vanaf elke host ook onze gateway (192.168.16.8) kunnen bereiken, alsook alle toestellen van de andere groepen binnen het lokaal. Een ping pakket sturen naar buiten (bv. ping google.be) heeft weinig zin, aangezien de firewall van de HoGent alle ICMP-pakketten blokkeert.

Om je DNS-server te testen kan je gebruikmaken van het dig commando. Test je DNS-servers kritisch uit, en probeer ook of je het domein van je buren kan bereiken.

Hoofdstuk 2

SSH

Voor dit deel maak je gebruik van de virtuele machines die je in het vorige labo hebt aangemaakt. Maak vooraf een zip van de virtuele harde schijf die je na afloop van het labo terugplaatst. Wijzig in geen geval de configuratiebestanden van de fysieke toestellen.

Het aanpassen van de configuratie en het herstarten van de server doe je als root-gebruiker. Het configureren en uitvoeren van de de client-commando's doe je meestal als een gewone gebruiker (tiwi1, ...), soms als root indien nodig. Maak daarom bij het begin van dit labo 3 extra gebruikers aan op je virtuele machine: tiwi1, tiwi2 en tiwi3 (zelfde wachtwoord als root).

```
(in de command shell)
adduser tiwi1
passwd tiwi1
root
adduser tiwi2
passwd tiwi2
root
adduser tiwi3
passwd tiwi3
root
```

Om in te loggen met een gebruiker: `su - tiwi1`

2.1 Host Based Authentication

SSH laat toe om host-based authentication te doen, zodat een specifieke gebruiker op een specifieke host kan inloggen zonder wachtwoord. Om Host-Based Authenticatie te gebruiken moet je zowel de **/etc/ssh/sshd_config** (server) als de **/etc/ssh/ssh_config** (client) moeten aanpassen, en zal je eveneens de nodige informatie moeten toevoegen aan **/.ssh/known_hosts** en **/.shosts**.

Zorg er voor dat je toegang kunt krijgen/geven voor een gebruiker op een andere machine via Host-Based Authentication. Test dit uitgebreid uit! Dit effect kan ook verkregen worden door een globale

serverinstelling en niet door gebruik te maken van een .shosts-file voor de gebruiker. Configureer dit en test uit voor zowel root als voor een gewone gebruiker.

- *Vm van hilbert (client)*
  - Volgende lijn aanpassen in **ssh_config**:

    ```
    HostBasedAuthentication yes
    EnableSSHKeysign yes
    ```

  - Genereer een sleutelpaar met

    ```
    ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key -N '' ''
    ```

- *VM van ivory (server)*
  - Volgende lijnen aanpassen in **sshd_config**:

    ```
    HostBasedAuthentication yes
    IgnoreRhosts no
    IgnoreUserKnownHosts no
    RHostsRSAAuthentication yes
    ```

  - Genereer een **known_hosts** bestand door

    ```
    ssh root@hilbert.groep20.iii.hogent.be
    ```

    in te geven. Er zal een waarschuwing komen dat hij een entry zal toevoegen. Het is belangrijk dat de sshclient dit bestand zelf genereerd zodat de rechten onmiddelijk goed zijn. Na het genereren moet de publieke sleutel van de client toegevoegd worden aan dit bestand. Gebruik hiervoor volgend commando:

    ```
    ssh-keyscan -t rsa hilbert.groep20.iii.hogent.be >> .ssh/known_hosts
    ```

  - De Fully Qualified Domain Name (FQDN) van de client moet toegevoegd worden in het **.shosts** bestand. Dit kan eenvoudig door

    ```
    echo hilbert.groep20.iii.hogent.be >>  /.shosts
    ```

    uit te voeren. De rechten van dit bestand worden best aangepast zodat enkel de eigenaar schrijfrechten heeft.

    ```
    chmod og-w  /.shosts
    ```

2.2 Public Host Keys

??

2.3 Toegangscontrole

??

2.4 Public Key Authentication

??

2.5 Port Forwarding

SSH kan ook gebruikt worden om aan port forwarding te doen. Log in op de gateway-computer van jouw opstelling en zorg dat alle aanvragen op poort 8888 doorgestuurd worden naar poort 22 van een welbepaalde client-computer van een ander privaat netwerk.

```
ssh -L 8888:192.168.70.3:22 root@192.168.70.1
```

In welke praktische situatie is deze configuratie nuttig? Is dit local of remote port forwarding? Een connectie maken die een firewal kan omzeilen.

Veronderstel nu dat de computers binnen jouw privaat netwerk van buitenuit niet bereikbaar zijn! Hoe kan je er voor zorgen dat de SSH-poort (poort 22) van je interne client beschikbaar wordt op poort 8888 van de gateway-computer? Test grondig uit of een toestel buiten jouw privaat netwerk een connectie kan maken met poort 8888 van jouw gateway en dat er op deze manier veilig kan worden ingelogd op de interne client.

```
ssh -R 8888:192.168.70.254:22 root@192.168.70.3
```

In welke praktische situatie is deze configuratie nuttig? Is dit local of remote port forwarding?

2.6 Bestandsbeheer

In het ssh-pakket zit ook een utility om op een beveiligde manier aan ftp te doen. Dit laat toe om bijvoorbeeld via een ssh-windows-implementering bestandsbeheer op de server mogelijk te maken. Test dit uit. Een beperkter commando dat alleen toelaat om bestanden te kopiëren is ook aanwezig (scp). Test uit.

```
scp bestand root@192.168.70.254:/home
```

Hoofdstuk 3

Certificaten

Tijdens dit labo configureren we de Apache-webserver zodat die kan werken met SSL. Meer informatie over de configuratie van Apache kan je hier vinden.

1. **Configureer Apache op de gateway-VM zodat je deze in het hele lokaal kan bereiken via http://groepXX.iii.hogent.be (zonder www!). Voorzie een gepaste index-pagina en test voldoende uit.**

   Eerst `yum install httpd` uitvoeren op de gateway-VM. Eens dit klaar is moet er een nieuw configuratiebestand `vhost.conf` (willekeurige naam) aangemaakt worden in de `etc/httpd/conf.d/` directory. De inhoud van dit bestand wordt:

   ```
   <VirtualHost 192.168.70.2>
           DocumentRoot /var/www/html/default
           ServerName groep20.iii.hogent.be
           <Directory "/var/www/html/default">
                   Order allow,deny
                   allow from all
           </Directory>
   </VirtualHost>
   ```

   Nadien met de service gestart worden met `service httpd restart`. Voeg een `index.html` (met willekeurige inhoud) bestand toe in `/var/www/html/default/`. Verder moet ook de inhoud van het zonebestand `groep20.iii.hogent.be` van de primaire DNS aangepast worden:

   ```
   $TTL 60
   @ IN SOA groep20.iii.hogent.be. bert.desaffel.ugent.be (1 60 1H 60 3H)
                IN  NS   hilbert
                IN  NS   ivory
                IN  A    192.168.70.2  <!----
   test         IN  A    192.168.70.2  <!---- (voor volgende stap)
   hilbert      IN  A    192.168.70.1
   hilbertVM    IN  A    192.168.70.3
   ```

```
ivory       IN  A   192.168.70.254
ivoryVM     IN  A   192.168.70.4
```

2. **In Apache is het mogelijk om meerdere subdomeinen te configureren. Configureer http://test.groepXX.iii.hogent.be en voorzie een aparte index-pagina.**

Het is enkel vereist om het betand `vhost.conf` uit te breiden met volgende (gelijkaardige) syntax.

```
<VirtualHost 192.168.70.2>
        DocumentRoot /var/www/html/test
        ServerName test.groep20.iii.hogent.be
        <Directory "/var/www/html/test">
        Order allow,deny
        allow from all
</Directory>
```

De httpd daemon moet wel herstart worden met `service httpd restart`.

3. **Om SSL te gebruiken binnen Apache hebben we een certificaat nodig. Genereer een self-signed certificaat voor test.groepXX.iii.hogent.be en zorg er voor dat deze website enkel nog via HTTPS bereikbaar is.**

Op de gateway-VM:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout key.out -out test.out
```

Er zullen een aantal prompts tevoorschijnkomen. Het enige belangrijke is de `Common Name` prompt die de volgende waarde `test.groep20.iii.hogent.be` krijgt. Installeer `mod_ssl` met `yum install mod_ssl`. Plaats `test.out` en `key.out` respectievelijk in de `/etc/pki/tls/certs/` en `/etc/pki/tls/private/` directory.

4. **In de praktijk maak je meestal geen gebruik van self-signed certificaten, maar ga je certificaten aanvragen via een Certificate Authority (CA). Voor dit labo hebben wij een CA opgezet die bereikbaar is via https://godfather.iii.hogent.be/CertSrv.**

   Installeer het root certificaat van deze server in firefox.

5. **Genereer op jouw toestel een Certificate Signing Request (CSR) voor groepXX.iii.hogent.be, en vraag het certificaat aan bij de CA. Een correct aangevraagd certificaat wordt door onze CA automatisch uitgegeven.**

   Download het certificaat in base64 codering.

Op de gateway-VM:

```
openssl req -new -newkey rsa:2048 -nodes -keyout default.key -out default.csr
```

Het bestand `default.csr` moet gegeven worden aan de CA, die een certificaat zal teruggeven.

6. **Zorg er nu voor dat de website geconfigureerd in het eerste puntje (http://groepXX.iii.hogent.be) enkel nog via HTTPS bereikbaar is en gebruikmaakt van dit certificaat.**

7. **Zorg er nu voor dat alle aanvragen naar http://groepXX.iii.hogent.be doorgestuurd worden naar https://groepXX.iii.hogent.be. Analoog voor http://test.iii.hogent.be. Test dit grondig uit!**

Hoofdstuk 4

VPN

Voor dit labo beschik je over een host en een gateway en is het de bedoeling een verbinding te maken met de gateway en/of host van de groep op dezelfde tafel.

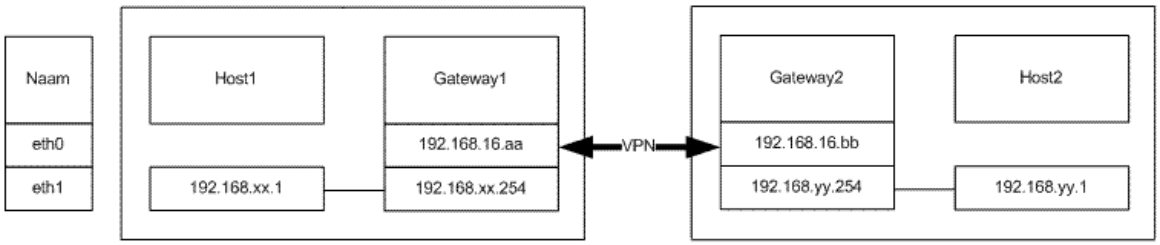
4.1 Opstelling

Tijdens dit labo maak je een aantal VPN-configuraties met behulp van IPSec. Je kan de SAD en de SPD instellen en configureren met het commando setkey. Neem aandachtig de man-page van dit commando door om alle mogelijkheden te leren kennen.

De optie -f laat toe dat alle instellingen uit een bestand gelezen worden. Zorg ervoor dat de eerste lijnen in dat bestand als volgt zijn, zodat steeds de SAD en SPD in de kernel leeg gemaakt worden.

```
spdflush;
flush;
```

Voor alle opdrachten maak je gebruik van de volgende opstelling:



Figuur 4.1: IPSec configuratie.

In deze opstelling blijven enkel de twee gateways verbonden met het bestaande netwerk via de lan0 interface, en zijn de IP-adressen 192.168.16.(aa bb) de originele IP-adressen van je toestel. De VPN-verbinding op de figuur loopt dus over het bestaande 192.168.16/24 netwerk.

Maak op de gateways gebruik van wireshark om alle inkomende en/of uitgaande IP-pakketten te bekijken. Ga steeds na of de IP-pakketten over de juiste headers beschikken (ESP en/of AH) en of de payload al dan niet werd geëncrypteerd.

4.2 Opgave

1. **Voorzie een veilige IPSec-verbinding tussen de twee clientcomputers. Test eerst uit met ESP zonder AH, daarna met AH zonder ESP. Voor deze vraag maak je nog geen gebruik van een combinatie van beide of van tunneling.**

Verkorte notatie: x = 192.168.70.1 en y = 192.168.76.1

Voer het commando `setkey -f bestandsnaam` uit, met **bestandsnaam** de naam van het configuratiebestand waarin volgende instellingen komen.

- **ESP configuratie.**
  - hilbert

```
spdflush; -> zit in elk bestand
flush; -> zit in elk bestand
add y x esp 0x01 -m transport -E des-cbc "01234567";
add x y esp 0x02 -m transport -E des-cbc "01234567";
spdadd y x any -P out ipsec esp/transport//require;
spdadd x y any -P in ipsec esp/transport//require;
```

  - fermat

```
add y x esp 0x01 -m transport -E des-cbc "01234567";
add x y esp 0x02 -m transport -E des-cbc "01234567";
spdadd x y any -P out ipsec esp/transport//require;
spdadd y x any -P in ipsec esp/transport//require;
```

- **AH configuratie.**
  - hilbert

```
add y x esp 0x01 -m transport -A hmac-md5 "0123456789ABCDEF";
add x y esp 0x02 -m transport -A hmac-md5 "0123456789ABCDEF";
spdadd y x any -P out ipsec ah/transport//require;
spdadd x y any -P in ipsec ah/transport//require;
```

  - fermat

```
add y x esp 0x01 -m transport -A hmac-md5 "0123456789ABCDEF";
add x y esp 0x02 -m transport -A hmac-md5 "0123456789ABCDEF";
spdadd y x any -P out ipsec ah/transport//require;
spdadd y x any -P in ipsec ah/transport//require;
```

2. **Voortbouwend op de vorige vraag test je nu uit of je het verkeer tussen de clients kan encrypteren en bovendien ook kunt voorzien van de nodige authenticatie. Opnieuw wordt er geen tunneling gebruikt. Om dit te realiseren zijn er twee mogelijkheden, eerst encrypteren en dan authenticeren of omgekeerd. Test beide mogelijkheden uit en ga telkens na of er tussen de clients nog communicatie mogelijk is. Wanneer dit niet het geval is, maak je een schets om aan te tonen dat de uitgeteste configuratie niet kan werken.**

De combinatie waarbij AH eerst gebruikt wordt is onmogelijk. AH zal eerst het bericht authenticeren op basis van de IP header. ESP zal deze IP header overschrijven, waardoor het onmogelijk is om de authenticatie te bevestigen. Eerst ESP, gevolgd door AH zal werken.

- hilbert

```
add y x esp 0x01 -m transport -E des-cbc "01234567";
add y x esp 0x02 -m transport -A hmac-md5 "0123456789ABCDEF";.
spdadd y x any -P out ipsec esp/transport//require ah/transport//require;
spdadd x y any -P in ipsec esp/transport//require ah/transport//require;
```

- fermat

```
add y x esp 0x01 -m transport -E des-cbc "01234567";
add y x esp 0x012 -m transport -A hmac-md5 "0123456789ABCDEF";.
spdadd x y any -P out ipsec esp/transport//require ah/transport//require;
spdadd y x any -P in ipsec esp/transport//require ah/transport//require;
```

3. **Op de clientcomputers behoud je het authenticatiegedeelte in transportmode. Het is dus niet nodig om het verkeer tussen beide clients te encrypteren. Tussen de gateways voorzie je nu bovendien een IPSec-tunnel. Test eerst uit met een AH-tunnel, daarna met een ESP-tunnel. Maak bij iedere opstelling een schets die aantoont of de gevraagde configuratie mogelijk is.**

Extra notatie: a = 192.168.70.254 en b = 192.168.76.254

4. **Net zoals bij de vorige vraag zet je tussen de beide gateways een ESP-tunnel op. Aanvullend zorg je ervoor dat er tussen beide gateways authenticatie gebeurt in transportmode. Beide clients maken nog steeds gebruik van AH in transportmode. Test grondig uit en maak opnieuw de nodige schetsen.**

5. **Herneem de vorige vraag maar gebruik nu de racoon-daemon voor het aanmaken van de SA's op de clients en op de gateways. Om niet vanaf nul te moeten vertrekken kan je gebruikmaken van dit configuratiebestand. Vergeet niet om het bestand /etc/racoon/psk.txt aan te vullen zodat beide eindpunten over dezelfde sleutel beschikken. Ter info: wanneer er geen verkeer optreedt tussen de eindpunten, worden er door racoon geen nieuwe SA's aangemaakt! Je doet er dus goed aan om steeds een console open te houden waar je een ping stuurt naar het andere eindpunt.**

6. **Tot slot kan je eens nagaan wat er gebeurt als je tussen de gateways een dubbele tunnel opzet (ESP en AH in tunnelmode). Test uit in welke mate de volgorde een rol speelt en maak opnieuw een schets om na te gaan of het gevraagde enerzijds mogelijk is en anderzijds zinvol is.**