FACULTEIT INGENIEURSWETENSCHAPPEN
EN ARCHITECTUUR

Beveiliging van netwerken en computers

Bert De Saffel

Master in de Industriële Wetenschappen: Informatica Academiejaar 2018–2019

Gecompileerd op 18 december 2018

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 **??** geeft een algemeen overzicht van de opstelling voor één groep. Voor de uitwerking van dit labo wordt de groep op figuur **??** 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

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 x y 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.**

Hoofdstuk 5

PGP

Dit labo voer je elk afzonderlijk uit op je eigen **virtuele machine**, dus niet in groep. Maak op je VM drie gewone gebruikers aan: *pgp1, pgp2* en *pgp3*. Alle vollgende opdrachten voer je uit als één van deze gebruikers.

5.1 Sleutelbeheer

Figuur 5.1: Keyrings

5.1.1 Aanmaken sleutels

Maak voor gebruiker *pgp1* drie sleutelparen aan (RSA and RSA, DSA en RSA). Voor gebruikers *pgp2* en *pgp3* maak je telkens twee sleutelparen aan; een RSA and RSA sleutelpaar en een DSA-sleutelpaar. Zorg er voor dat elke sleutel een verschillend ID heeft die de naam van de gebruiker bevat alsook de encryptiemethode. Kies een verschillende geldigheidsperiode voor de sleutels.

Indien gpg nog niet geïnstalleerd is :

```
yum install gpg
```

Het kan zijn dat hij de mirrors niet kan resolven, clear de cache dan:

```
yum clean all
```

Installeer ook de rng-tools om entropy te genereren:

```
yum install rng-tools
```

In de virtual machine kan je nieuwe terminals openen via CTRL + | F1 | F2 | F3 | ... | F7. Log in op deze verschillende terminals als de drie gebruiker accounts. Behou ook nog een terminal voor de root gebruiker (CTRL + F1 voor root bijvoorbeeld). Run het commando rng-tools in de voorgrond, zodat het random activiteit zal blijven genereren, dit is nodig bij het genereren van sleutels:

```
/usr/sbin/rngd -f -r /dev/urandom
```

Een sleutel genereren kan met

```
gpg --gen-key
```

Als *pgp1* doe je dit drie keer, telkens met een verschillend algoritme. Als *pgp2* en *pgp3* twee keer: eens met DSA en dan met RSA.

- **Waarvoor dient de passphrase?** De passphrase dient om de private sleutel te beschermen. Sommige acties op sleutels vereisen ook deze passphrase.
- **Waarom wordt er bij het aanmaken van een sleutel soms naar extra toetsaanslagen gevraagd en soms ook niet?** GPG maakt gebruik van activiteiten zoals toestaanslagen en muisbewegingen (systeemactiviteiten) om entropy te genereren. Gelukkig kan dit vermeden worden door *rngd* te gebruiken.
- **Wat is het verschil tussen "RSA and RSAën "DSA and Elgamal"?**

5.1.2 Exporteren en uitwisselen sleutels

Exporteer al je publieke sleutels naar meerdere bestanden die je aan andere gebruikers kan aanbieden. Exporteer deze in 2 verschillende formaten, waarvan er één geschikt is voor transport via e-mail of publicatie op een webserver.

Gebruik het volgende commando om één enkele sleutel te exporteren. De variabele `UNIEKE_NAAM` bevat een identificatie van de sleutel (bv op basis van Real Name en Comment, of gewoon het ID van de sleutel).

```
gpg --export UNIEKE_NAAM --output ~/outputnaam
```

Voor leesbare exports gebruik je de `--armor` optie:

```
gpg --armor --export UNIEKE_NAAM --output ~/outputnaam
```

Het is ook mogelijk om alle sleutels direct te exporten, door geen argument mee te geven aan `--export`:

```
gpg --export --output ~/outputnaam
```

Wat is het formaat van deze bestanden? Zonder de `--armor` optie hebben de exportbestanden een binair formaat. Deze bestanden uitprinten op een terminal heeft dan ook geen nut. Met de `--armor` optie ziet het er bijvoorbeeld als volgt uit (ingekort):

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.2.1 (GNU/Linux)
Comment: For info see http://www.gnupg.org

mQGiBDkHP3URBACkWGsYh43pkXU9wj/X1G67K8/DSrl85r7dNtHNfLL/ewil10k2
q8saWJn26QZPsDVqdUJMOdHfJ6kQTAt9NzQbgcVrxLYNfgeBsvkHF/POtnYcZRgL
=BMEc
-----END PGP PUBLIC KEY BLOCK-----
```

Wissel deze bestanden uit met de andere gebruikers (bv. door ze in een gedeelde directory te plaatsen). We gaan er op dit ogenblik van uit dat sleutels die op deze manier zijn verkregen, volledig te vertrouwen zijn.

De eenvoudigste manier is om als root gebruiker de bestanden te kopieëren naar de root folder van elke gebruiker (gebruik hiervoor de terminal die voor de root gebruiker beschikbaar is).

```
cp /home/pgp1/exportbestand /home/pgp2/exportbestand_pgp1
```

5.1.3 Toevoegen sleutels

Voeg voor elke gebruiker de verkregen publieke sleutels toe aan zijn publieke sleutelhanger. Verifieer of ze wel zijn opgenomen.

Een sleutel importeren kan met

```
gpg --import bestandsnaam
```

Dit commando zal ook specificeren hoeveel publieke sleutels er zijn toegevoegd. Om een lijst van alle sleutels op te vragen gebruik je

```
gpg --list-key
```

Verwijder één van de sleutels uit de sleutelhanger. Controleer en voeg de sleutel nadien weer toe.

Een sleutel verwijderen kan met

```
gpg --delete-key sleutelID
```

5.1.4 Wijzigen sleutels

Wijzig één van de sleutels: verander de passeerzin. Een sleutel wijzigen kan met

```
gpg --edit-key sleutelID
```

Na het uitvoeren van dit commando zit je in een menu. Met *help* kan je alle mogelijke opties ophalen. Een passphrase veranderen kan met *passwd*.

5.1.5 Vertrouwen sleutels

- **Controleer de sleutels en de handtekeningen die er bij horen.**
- **Verifieer de fingerprint van de sleutels bij de verschillende gebruikers.**

  Gebruik `gpg --verify sleutelID`
- **Zorg er voor dat al de sleutels in de sleutelhangers volledig vertrouwd worden, indien dit nog niet het geval zou zijn.**

  Een sleutel vertrouwen kan terug met `gpg --edit-key sleutelID`. In het menu gebruik je nu `trust`, en geef je ultimate trust aan elke sleutel. Hiervoor moet dus elke keer het gpg commando met de `--edit-key` optie uitgevoerd worden voor elke sleutel.
- **Teken voor elke gebruiker de eigen sleutels en die van de andere gebruikers van wie de sleutel vertrouwd wordt.**

  Gebruik hiervoor de `sign` optie in de `--edit-key` menu.

5.2 Encrypteren en decrypteren van bestanden

Figuur 5.2: Encryptie.

5.2.1 Lokaal encrypteren en decrypteren

Maak als gebruiker *pgp1* vijf korte tekstbestanden aan om ze nadien aan de andere gebruikers over te maken. Encrypteer deze bestanden als volgt:

1. **het eerste bestand encrypteer je door middel van conventionele encryptie op twee manieren: de eerste keer met het default algoritme, de tweede keer geef je zelf het algoritme op (bv. AES256).** Het default algoritme is CAST5. Het volgende commando zal een bestand encrypteren met dit algoritme:

   ```
   gpg --encrypt bestand1
   ```

   Er zal een prompt komen voor User IDs, laat dit voorlopig leeg. Het uitvoerbestand zal `bestand1.gpg` zijn. Dit zullen ook de bestanden zijn die moeten verzonden worden over een netwerk naar de begunstigde.

   Zelf aan algoritme meegeven kan met de `--cipher-algo` optie:

   ```
   gpg --encrypt --cipher-algo AES256 bestand1
   ```

2. **het tweede bestand encrypteer je zodat alleen gebruiker pgp2 het bestand kan decrypteren.**

   Hier wordt ervan uitgegaan dat de naam van de sleutels van de gebruiker pgp2, zelf ook de string "pgp2"bevatten.

   ```
   gpg --encrypt --recipient pgp2 bestand2
   ```

3. **het derde bestand encrypteer je zodat dit door gebruikers pgp2 en pgp3 kan ontcijferd en gelezen worden. Zorg dat de encryptie met een ander dan het default algoritme gebeurt.**

   ```
   gpg --encrypt --cipher-algo AES256 bestand3
   ```

   Vul nu in de prompt twee User IDs in, namelijk die van pgpp2 en pgp3 (op aparte lijnen).

4. **het vierde bestand encrypteer je zodat gebruiker pgp2 hem niet zonder meer kan opslaan op zijn vaste schijf.**

   ???

5. **het vijfde bestand encrypteer je conventioneel maar het resultaat is in radix64.**

Veeg de originele plaintextbestanden uit. Probeer nu de plaintext te herstellen uitgaande van de ciphertext van elk bestand. Controleer wat er al dan niet nog kan gebeuren

5.2.2 Remote decrypteren

Wissel al de geëncrypteerde bestanden uit met de gebruikers pgp2 en pgp3. Decrypteer alle ontvangen bestanden. Beschrijf in elk van de gevallen wat er gebeurt. Een bestand decrypteren kan met:

```
gpg --decrypt bestandsnaam
```

Indien dit bestand bedoeld was voor de huidige gebruiker, dan zal hij deze kunnen decrypteren, en zal de inhoud van het bestand naar de console geschreven worden. Is dit niet zo zal er een foutmelding komen dat de juiste sleutel niet beschikbaar is.

5.3 Sleutelbeheer

Hoofdstuk 6

Sendmail

Dit labo bestaat uit 2 delen: in het eerste deel maken we een basisconfiguratie aan voor sendmail, die we in het tweede deel gebruiken om de mogelijkheden van S/MIME even uit te testen. Binnen elke groep zal één virtuele machine dienst doen als sendmail-server. Deze server zal verantwoordelijk zijn voor jouw domein. Vooraleer echt aan de slag te gaan, doe je best het volgende:

- Voor dit labo start je best met een 'cleane' VM. Zet indien nodig de backup van je virtuele machine terug. Controleer zeker volgende instellingen:
  - De virtuele netwerkinterface is in bridge modus verbonden met de fysieke netwerkadapter en heeft een IP-adres binnen jouw netwerkrange (192.168.x.2 of 192.168.x.3).
  - De default gateway is ingesteld naar jouw gateway (192.168.x.254).
  - Je eigen DNS-servers staan ingesteld in /etc/resolv.conf.
  - `firewalld` is **niet** geïnstalleerd (yum remove firewalld + reboot).
  - Om problemen te voorkomen schakel je ook best SELinux uit.
- Maak eventueel een extra backup van je VM die je indien nog snel kan terugplaatsen.
- Maak een kopie van het configuratiebestand sendmail en plaats dit in de homedirectory van de root-gebruiker (`cp /etc/mail/sendmail.mc  /sendmail.mc.bak`).
- Zorg dat je over twee gebruikers beschikt: *tiwi1* en *tiwi2* met hetzelfde wachtwoord als *root*

Aangezien er twee DNS-domeinen per tafel zijn voorzien, kan je voor het uittesten van sendmail gebruikmaken van het naburige domein. E-mailverkeer treedt dan ook voornamelijk op tussen deze twee domeinen, maar is ook mogelijk met andere domeinen.

6.1 Configuratie sendmail

6.1.1 Basisconfiguratie

Voor de basisconfiguratie van sendmail kan je starten van dit (wordt gegeven) **configuratiebestand. Let op: hier en daar moet je nog iets aanpassen! Ga na of je nu met deze basisconfiguratie via jouw mailserver een mail kan versturen naar een lokale gebruiker. Controleer ook of je een mail kan versturen naar een lokale gebruiker van het andere domein. Een e-mail versturen kan je m.b.v. het commando mail -v (of -vv om nog**

meer informatie te verkrijgen). Zorg er tenslotte voor dat post die bestemd is voor lokale gebruikers niet meer wordt rondgestuurd naar eventuele andere mailservers.

Wij gebruiken de gateway als mailserver. Dus alle configuratie gebeurd dan ook op dat toestel. Installeer eerst de software:

```
yum install sendmail sendmail-cf mailx m4
```

Het sendmail.mc bestand dat we gekregen hebben is grotendeels goed, enkel twee lijnen moeten aangepast worden:

```
MASQUERADE_AS(groep20.iii.hogent.be)dnl
GENERICS_DOMAIN('groep20.iii.hogent.be')dnl
```

Voeg bij de primaire DNS (NIET de gateway) het volgende **MX** (mail exchange) record toe in het zonebestand (`/var/named/groep20.iii.hogent.be`) en herstart hierna de **named** service:

```
ivoryVM IN MX 10 192.168.70.2

service named restart
```

Terug op de gateway in het bestand `/etc/mail/local-host-names`:

```
ivoryVM.groep20.iii.hogent.be
groep20.iii.hogent.be
FEATURE('use_cw_file')
```

Verstuur een email met:

```
[root@ivoryVM]: mail -s "Onderwerp" tiwi1@hilbertVM < /dev/null
```

en bekijk deze met:

`root@hilbertVM` : $cat/var/mail/tiwi1$

6.1.2 Aliases

Zorg er voor dat tiwi1 een alias is voor jouwvoornaam.jouwnaam@jouwdomein.iii.hogent.be. Doe hetzelfde voor jouw collega, maar dan met gebruiker tiwi2. Welke bestanden heb je aangepast en welke informatie heb je aan die bestanden toegevoegd? Test deze instellingen eerst uit vanuit je lokale domein, en nadien vanuit een ander domein.

In het bestand `/etc/aliases`:

```
xandro.vermeulen@groep20.iii.hogent.be: tiwi1@ivoryVM
bert.desaffel@groep20.iii.hogent.be: tiwi2@hilbertVM
```

Hierna moet het commando `newaliases` uitgevoerd worden, zodat sendmail op de hoogte is van deze aliases. Vanaf dan kunnen de aliases gebruikt worden.

Wat moet je aanpassen als je ook mails wenst te versturen vanaf jouwvoornaam.jouwnaam@jouwdomein.iii.hogent.be?

6.1.3 IMAP en/of POP3

Om via IMAP en/of POP3 je mails te kunnen ophalen kan je gebruikmaken van dovecot. Installeer indien nodig dovecot op je VM (via yum).

Voor een correcte werking van dovecot overschrijf je het configuratiebestand (/etc/dovecot/dovecot.conf) door dit bestand. De bestanden /etc/dovecot/conf.d/10-auth.conf en /etc/dovecot/conf.d/10-ssl.conf vervang je respectievelijk door dit en dit bestand.

Lees de man-pagina van het commando mail en gebruik dit commando met bijhorende opties om op een ander toestel jouw persoonlijke berichten via POP3 van de mailserver af te halen. Beantwoord een ontvangen bericht en ga na of alles correct werkt.

Gewoon de bestanden kopieren, daarna:

```
yum install dovecot
service dovecot start
```

6.2 S/MIME

6.2.1 Configuratie e-mail client

Om S/MIME te kunnen gebruiken en uittesten is het noodzakelijk een e-mail-client te gebruiken die dit aankan. In dit labo maken we hiervoor gebruik van Mozilla Thunderbird.

Configureer op beide fysieke toestellen (gateway en client1) Thunderbird voor de gebruikers tiwi1 en tiwi2. Kies bijvoorbeeld tiwi1 op de gateway en tiwi2 op de primaire DNS-server.

Probeer je berichten op te halen via IMAP of POP3. Merk op dat dovecot hiervoor correct geconfigureerd moet zijn! Stuur een mail naar de andere gebruiker en controleer of alles werkt.

6.2.2 Certificaat

Om een digitale handtekening toe te voegen aan e-mails, of e-mails te kunnen encrypteren hebben we opnieuw een certificaat nodig. Vraag via onze CA (link) een certificaat aan en voeg dit certificaat toe in Thunderbird. Voor deze vraag moet je geen CSR genereren, maar mag je het online formulier gebruiken.

6.2.3 Authenticatie en/of encryptie

Verzend naar je collega een bericht dat je probeert te encrypteren. Waarom lukt dat niet? Waarom lukt dit wel als je naar jezelf een e-mail stuurt?

Verzend nu naar elkaar een ondertekend bericht. Bij ontvangst wordt het gebruikte certificaat automatisch geïnstalleerd. Controleer dit en verifieer ook de vingerafdruk.

Probeer nu opnieuw een bericht te encrypteren en naar je collega te versturen. Voeg eventueel ook een handtekening toe aan je bericht.

6.2.4 Opslag mails op server

Alle mails worden op de sendmail-server opgeslagen in de directory /var/spool/mail/. Bekijk de inhoud van deze bestanden. Wat is het formaat van een mail met authenticatie en/of encryptie?

Hoofdstuk 7

PAM

Dit labo voer je elk afzonderlijk uit op je eigen **virtuele machine**, dus niet in groep. Om dit labo te kunnen uitvoeren moeten de globale configuratieinstellingen in `/etc/pam.d` worden aangepast. Neem daarom bij het begin van het labo een backup van je virtuele harde schijf. Aan het einde van dit labo plaats je deze kopie terug!

Opgelet: het aanpassen van de configuratie doe je als root-gebruiker en **TREEDT ONMIDDELLIJK IN WERKING**. **Blijf dus op elk moment op minstens 1 console als root-gebruiker ingelogd** voor het geval er iets verkeerd zou gaan!

Maake 2 extra lokale gebruikers aan met volgende eigenschappen:

- pam1: UID $>$ 1000 en GID $>$ 1000
- pam2: UID $<$ 1000 en GID $<$ 1000
- beide gebruikers hebben een wachtwoord.

Voordat je een gebruiker aanmaakt, controleer je best of het UID dat je wil instellen nog niet door een andere gebruiker ingenomen is.

```
cat /etc/passwd | cut -d ':' -f3 // om reeds gebruikte UIDs te zien
cat /etc/groups | cut -d ':' -f3 // om reeds gebruikte GIDs te zien

adduser pam1 -u 1500
groupmod -g 1600 pam1
passwd pam1

adduser pam2 -u 500
groupmod -g 600 pam2
passwd pam2
```

7.1 Pamtester

Pamtester is een tool die werd ontwikkeld voor het testen van de PAM-configuratie. Meer informatie over Pamtester en over het gebruik ervan kun je vinden in de bijgevoegde man-pages. De installatie gebeurt als volgt:

```
yum install pamtester
```

Na deze stappen kun je de tester gewoon gebruiken. Probeer hem ook eens uit, zodat je weet hoe hij werkt.

7.2 Opdrachten

1. **Configureer PAM zodat de meeste modules debug-informatie wegschrijven.**

   Het bestand `/etc/pam.d/system-auth` aanpassen, zodat elke lijn eindigt met 'debug'.

   ```
   auth       required    pam_env.so debug
   auth       sufficient  pam_unix.so nullok try_first_pass debug
   auth       requisite   pam_succeed_if.so uid >= 500 debug
   auth       required    pam_deny.so debug

   account    required    pam_unix.so debug
   account    sufficient  pam_succeed_if.so uid < 500 debug
   account    required    pam_permit.so debug

   password   requisite   pam_pwquality.so try_first_pass retry=3 debug
   password   sufficient  pam_unix.so md5 ... use_authtok debug
   password   required    pam_deny.so debug

   session    required    pam_limits.so debug
   session    required    pam_unix.so debug
   ```

   In welk(e) bestand(en) komt deze informatie terecht? Je kan logbestanden opvragen met

   ```
   journalctl -f -l SYSTEM_FACILITY=10
   ```

2. **Pas de configuratie aan zodat een gebruiker 5 kansen krijgt om een aanvaardbaar nieuw wachtwoord in te geven bij het wijzigen van zijn wachtwoord.**

   Verander lijn 8 van het bestand `/etc/pam.d/system-auth` zodat retry op 5 staat i.p.v. 3.

   ```
   password   requisite   pam_pwquality.so try_first_pass retry=5 debug
   ```

3. **Pas het systeem aan zodat gebruikers met UID > 1000 (bv. pam1) niet kunnen inloggen en die met een UID < 1000 (bv. pam2) wel. Test uit met de nieuw aangemaakte gebruikers.**

   Voeg deze twee lijnen toe in de bestanden `/etc/pam.d/su` en `/etc/pam.d/login` in hun respectievelijke stack. Waar dat deze lijnen komen maakt niet zoveel uit, als het maar zeker niet onder de pam module `pam_deny.so` staat:

   ```
   auth     requisite pam_succeed_if.so uid < 1000
   account  requisite pam_succeed_if.so uid < 1000
   ```

4. **Bij systeemonderhoud is het wenselijk dat niet-root-gebruikers zich voor een bepaalde tijd niet kunnen aanmelden; pas dit toe voor ssh en voor login. Zorg er bovendien voor dat gebruikers die toch proberen in te loggen een passende boodschap te zien krijgen.**

   In de bestanden `/etc/pam.d/sshd` en `/etc/pam.d/login` staat al de nodige lijn om deze module in te schakelen, namelijk:

   ```
   auth required pam_nologin.so
   ```

Deze module wordt echter pas uitgevoerd indien er een bestand `/etc/nologin` bestaat. In dit bestand staat ook de boodschap die getoond zal worden indien een niet-root gebruiker zal proberen inloggen.

5. **Configureer PAM zodat gebruiker pam1 enkel kan inloggen vanop de computer van je collega.**

   Voeg de volgende lijn toe in het bestand `/etc/pam.d/system-auth`:

   ```
   auth requisite pam_access.so debug
   ```

   Deze module kijkt in het bestand `/etc/security/access.conf`. Vul de inhoud aan met (vanuit perspectief van hilbertVM):

   ```
   + : pam1 : 192.168.70.2
   - : pam1 : 192.168.70.3
   ```

6. **Configureer PAM zodanig dat root uitsluitend nog kan inloggen vanop tty4. Vergeet niet om root nog steeds ingelogd te houden op 1 andere console!**

   Ook hier staat de nodige pam module (`pam_securetty`) al ingesteld in de nodige bestanden. Enkel het bestand `/etc/securetty` moet aangepast worden zodat deze enkel tty4 bevat. Maak eerst een backup met

   ```
   cp /etc/securetty /etc/securetty.bak
   ```

   en verwijder daarna alles behalve tty4 uit `/etc/securetty`.

7. **Zorg ervoor dat lokaal inloggen en inloggen via ssh enkel mogelijk is op maandagen van 10 tot 12. Uiteraard pas je deze tijden aan om te kunnen testen.**

   Voeg volgende lijn toe in `/etc/pam.d/sshd` en `/etc/pam.d/login`:

   ```
   auth required pam_time.so
   ```

   Pas dan volgende instelling toe in het bestand `/etc/security/time.conf`:

   ```
   login;*;*;Th1000-1200
   sshd;*;*;Th1000-1200
   ```

8. **Zorg ervoor dat lokaal inloggen en inloggen via ssh enkel mogelijk is op maandagen en vrijdagen voor pam1 en pam2. Uiteraard pas je deze dagen aan om te kunnen testen.**

   Terug het bestand `/etc/security/time.conf` aanpassen:

   ```
   login ; * ; pam1 | pam2 ; MoFr0000-2400
   sshd ; * ; pam1 | pam2 ; MoFr0000-2400
   ```

9. **Wat gebeurt er indien iemand zich aanmeldt via een service die niet voorkomt in de directory `/etc/pam.d`?**

Hoofdstuk 8

iptables

Tijdens dit labo werk je alleen aan een toestel. Dit labo voer je volledig uit op je **virtuele machine**, voer dus geen commando's uit op de gateway of op client1. Plaats eventueel bij het begin van dit labo een backup van je virtuele disk terug. Vergeet niet om firewalld te verwijderen mocht dit nog geïnstalleerd zijn (`yum remove firewalld`).

Zorg er voor dat je **NIET** bent ingelogd als gewone gebruiker maar als *root* (dus ook geen `su -` !!).

8.1 Vooraf

Implementeer volgende firewallregels met behulp van het `iptables`-commando. Informatie over de poorten kan je vinden in `/etc/services`. Test uit op je eigen machine en ook via je buren. Vergeet niet dat je telkens de instellingen kan nakijken met de list-vlag van het `iptables`-commando.

Hou ook rekening met volgende opmerkingen:

- Het is zeer handig en **tijdbesparend** als je alle regels opslaat in een script!! Dit laat ook toe om voor bepaalde dns-namen of ip-adressen een variabele (inderdaad: een shell-variabele!) te gebruiken die je in het begin van het script initialiseert.
- Je kan in de opgestelde regels zowel ip-adressen als dns-namen gebruiken. Het gebruik van ip-adressen geniet de voorkeur, omdat op die manier je firewall blijft functioneren los van het feit of de nameserver werkt/bereikbaar is of niet.

Om na te gaan welke poorten er op een toestel open staan, kan je gebruikmaken van de nmap-tool. Meer informatie over het gebruik van het commando `nmap` kan je vinden in de man-pages.

Via iptables kan je zowel stateless als stateful regels toevoegen. Voor dit labo mag je **alle regels stateless** toevoegen, tijdens het labo firewalls (inhaalweek) zullen we ook met stateful regels werken.

Belangrijk: Indien je om **10u45** nog niet aan vraag 8 bent gekomen, begin je op dat moment zeker bij 8 (Opgave deel 2). Ben je klaar met de tweede reeks voor het einde van het labo, dan werk je de eerste reeks opgaven verder af.

8.2 DEEL1 - Default policy ACCEPT

Bij de volgende 9 opgaven is het de bedoeling dat je de standaard ingestelde **policy (ACCEPT)** niet verandert.

Zorg er ook voor dat bij het toevoegen van een nieuwe regel alle tevoren ingestelde regels blijven gelden !!

1. Zorg er voor dat je een ftp-connectie kan leggen met je machine. Installeer indien nodig een ftp server op je virtuele machine (`yum install pure-ftpd`). De service starten kan via `systemctl start pure-ftpd`. Merk op dat je op de ftp-server enkel kan inloggen als niet-root gebruiker. Stel regels op die er voor zorgen dat geen enkele computer een ftp-verbinding kan maken met jouw virtuele machine.

```
iptables -A INPUT -p tcp --dport 20 -j DROP
iptables -A INPUT -p udp --dport 20 -j DROP
iptables -A INPUT -p tcp --dport 21 -j DROP
iptables -A INPUT -p udp --dport 21 -j DROP
```

2. Laat nadien selectief alleen ftp vanaf je eigen vm naar jezelf toe. Test zeer kritisch: gebruik zowel localhost, de naam, het ip-adres als de loopback van je machine.

```
iptables -I INPUT -p tcp -s 127.0.0.1 --dport 20 -j ACCEPT
iptables -I INPUT -p udp -s 127.0.0.1 --dport 20 -j ACCEPT
iptables -I INPUT -p tcp -s 127.0.0.1 --dport 21 -j ACCEPT
iptables -I INPUT -p udp -s 127.0.0.1 --dport 21 -j ACCEPT
```

3. Zorg er nu voor dat je een telnet-connectie kan leggen met je virtuele machine. Installeer hiervoor xinetd (`yum install xinetd`) en telnet-server (`yum install telnet-server`). Maak bovendien een configuratiefile `telnet` aan in `/etc/xinetd.d`. De inhoud van dit bestand vind je hier.

   Zorg ook dat er op jouw virtuele machine een webserver draait.

   Stel nadien dezelfde twee regels in (cfr. 1 en 2) voor de protocols www en telnet.

```
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p udp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 23 -j DROP
iptables -A INPUT -p udp --dport 23 -j DROP
iptables -I INPUT -p tcp -s 127.0.0.1 --dport 80 -j ACCEPT
iptables -I INPUT -p udp -s 127.0.0.1 --dport 80 -j ACCEPT
iptables -I INPUT -p tcp -s 127.0.0.1 --dport 23 -j ACCEPT
iptables -I INPUT -p udp -s 127.0.0.1 --dport 23 -j ACCEPT
```

4. Maak nu gebruik van de optie `multiport` om al de vorige regels te groeperen. Meer informatie over deze optie vind je in de man-pages van `iptables-extensions`.

```
iptables -I INPUT -p tcp -s 127.0.0.1
         -m multiport --dports 20, 21, 23, 80 -j ACCEPT
iptables -I INPUT -p udp -s 127.0.0.1
         -m multiport --dports 20, 21, 23, 80 -j ACCEPT
iptables -I INPUT -p tcp
         -m multiport --dports 20, 21, 23, 80 -j DROP
iptables -I INPUT -p udp
         -m multiport --dports 20, 21, 23, 80 -j DROP
```

5. Ga voor het telnet-protocol na wat de effectverschillen zijn tussen de opties `DROP` en `REJECT` bij het instellen van de regels. Bij REJECT kan je ook zelf kiezen uit een aantal `icmp-type 3` foutboodschappen. Test uit.

```
iptables -I INPUT -p tcp --dport 23 -j REJECT
         --reject-with icmp-port-unreachable
```

6. Zorg ervoor dat er op geen enkele poort boven 1024 informatie kan verstuurd worden naar moore.iii.hogent.be. Test bijvoorbeeld dat http wel werkt, maar dat de tomcat-server op poort 8080 niet te bereiken is.

```
iptables -I OUTPUT -d 192.168.134.8 -p tcp
         -m multiport --dports 1025:65535 -j REJECT
iptables -I OUTPUT -d 192.168.134.8 -p udp
         -m multiport --dports 1025:65535 -j REJECT
```

7. Maak dat je eigen machine niet kan ge*ping*d worden. Dit kan je verwezenlijken op verschillende manieren: langs ingangszijde geen aanvragen toelaten, langs uitgangszijde geen antwoord sturen. Probeer beide mogelijkheden uit.

```
# Geen aanvragen toelaten
iptables -I INPUT -p icmp --icmp-type echo-request -j REJECT
# Geen antwoorden sturen
iptables -I OUTPUT -p icmp  --icmp-type echo-reply -j REJECT
```

8.3 DEEL2 - Default policy DROP

Aan dit gedeelte start je ten laatste om 10u45. Het oplossen van deze reeks opgaven is belangrijk als voorbereiding voor de volgende sessies van het labo firewalls.

Bij de volgende opgaven is het de bedoeling dat je de standaard ingestelde policy verandert in DROP.

```
iptables -p INPUT DROP
iptables -p FORWARD DROP
iptables -p OUTPUT DROP
```

Controleer op meerdere manieren of dit het gewenste effect heeft !!

8. Zorg er in eerste instantie voor dat je eigen machine in staat is om DNS-namen op te vragen. Controleer met dig (vb. dig a www.google.be).

```
iptables -I OUTPUT -p udp --dport 53 -j ACCEPT
iptables -I INPUT  -p udp --dport 53 -j ACCEPT
iptables -I OUTPUT -p udp --sport 53 -j ACCEPT
iptables -I INPUT  -p udp --sport 53 -j ACCEPT
```

9. Natuurlijk moet je van op je eigen machine ook nog de webpagina's van http(s)://www.ugent.be kunnen opvragen. Pas je firewall aan en test eventueel uit met behulp van het commando curl of wget.

```
iptables -I OUTPUT -p tcp -d 157.193.43.50 --dport 80 -j ACCEPT
iptables -I INPUT  -p tcp -d 157.193.43.50 --dport 80 -j ACCEPT
iptables -I OUTPUT -p tcp -d 157.193.43.50 --dport 80 -j ACCEPT
iptables -I INPUT  -p tcp -d 157.193.43.50 --dport 80 -j ACCEPT
```

10. Stel nu een regel op die het mogelijk maakt om je eigen machine als webserver te gebruiken. Laat dit controleren door een van je buren.

```
iptables -I INPUT  -p tcp -d 192.168.70.3 --dport 80 -j ACCEPT
iptables -I OUTPUT -p tcp -s 192.168.70.3 --dport 80 -j ACCEPT
```

11. Stel nu regels op die het mogelijk maken om je eigen machine als FTP-server te kunnen laten gebruiken: je machine moet door een ftp-client bij je buur kunnen gebruikt worden om er bestanden van op te halen en er op te plaatsen; gebruik hiervoor een van de gewone tiwi-gebruikers. In welke mode moet het ftp-commando een connectie leggen opdat de firewall-linstellingen effect zouden hebben? Waarom?

    Opmerking: Om FTP in active mode te gebruiken geef je de optie -A mee: ftp -A hostname.

    Ga na of je effectief ook bestanden kan uitwisselen.

12. Tracht alle (normaal 6) regels die je hebt ingesteld in de twee vorige punten 10 en 11 te combineren tot twee regels.

13. Vanuit je machine moet je in staat zijn om naar andere toestellen te pingen. Zorg er bovendien voor dat je eigen machine niet reageert op ping-aanvragen van andere machines.

Hoofdstuk 9

Firewall

De bedoeling van dit labo is een firewall op te zetten met een gedemilitariseerde zone (DMZ) en een intern netwerk. Deze opdracht wordt uitgevoerd in groepen van 4, de indeling van de groepen vind je hier.

Elke groep maakt een opstelling met 4 PC's: een externe router (RE), een interne router (RI), een bastion host (BH) en een client in het interne netwerk (CL). Deze figuur toont de volledige opstelling voor één groep. Let in elk geval ook op de manier waarop de toestellen met elkaar zijn verbonden.

Welk toestel binnen jouw groep zal fungeren als RE, BH, RI en CL kan je hier vinden per lokaal: 2.031 en 2.035. Een overzicht van alle IP-adressen voor jouw groep vind je op figuur

9.1 Routing

Zorg er in eerste instantie voor dat de routing correct werkt:

Sluit de nodige netwerkkabels aan, en maak overal gebruik van statische IP-adressen, bij voorkeur via ifcfg-bestanden. Om de route naar de DMZ te verspreiden, zal de externe router (RE) gebruikmaken van een RIPv2-router (via Quagga). De bastion host (BH) fungeert als bridge, zodat hij in de DMZ verbonden is met zowel de interne als externe router. De interne router (RI) maakt gebruik van NAT om het interne netwerk te maskeren.

	Client Intern	Router Intern		Bastion Host	Router Extern	
	lan1	lan1	lan0		lan1	lan0
Groep1	10.0.0.1	10.0.0.254	192.168.51.250	192.168.51.1	192.168.51.254	huidig IP adres
Groep3	10.0.0.1	10.0.0.254	192.168.53.250	192.168.53.1	192.168.53.254	huidig IP adres
Groep5	10.0.0.1	10.0.0.254	192.168.55.250	192.168.55.1	192.168.55.254	huidig IP adres
Groep7	10.0.0.1	10.0.0.254	192.168.57.250	192.168.57.1	192.168.57.254	huidig IP adres
Groep9	10.0.0.1	10.0.0.254	192.168.59.250	192.168.59.1	192.168.59.254	huidig IP adres
Groep11	10.0.0.1	10.0.0.254	192.168.61.250	192.168.61.1	192.168.61.254	huidig IP adres
Groep12	10.0.0.1	10.0.0.254	192.168.62.250	192.168.62.1	192.168.62.254	huidig IP adres
Groep15	10.0.0.1	10.0.0.254	192.168.65.250	192.168.65.1	192.168.65.254	huidig IP adres
Groep17	10.0.0.1	10.0.0.254	192.168.67.250	192.168.67.1	192.168.67.254	huidig IP adres
Groep20	10.0.0.1	10.0.0.254	192.168.70.250	192.168.70.1	192.168.70.254	huidig IP adres
Groep21	10.0.0.1	10.0.0.254	192.168.71.250	192.168.71.1	192.168.71.254	huidig IP adres
Groep22	10.0.0.1	10.0.0.254	192.168.72.250	192.168.72.1	192.168.72.254	huidig IP adres
Groep23	10.0.0.1	10.0.0.254	192.168.73.250	192.168.73.1	192.168.73.254	huidig IP adres
Groep24	10.0.0.1	10.0.0.254	192.168.74.250	192.168.74.1	192.168.74.254	huidig IP adres

De externe router is verbonden met een extern netwerk dat zal fungeren als het internet. Dit is het netwerk waar alle computers zijn op aangesloten die niet in de testopstelling zijn betrokken, zo ook intranet.iii.hogent.be en moore.iii.hogent.be (192.168.16.8). Het internet op de externe router moet je aansluiten op lan0, dus op de interface waarmee de machine in de normale toestand met het net is verbonden. Om de route naar de DMZ te verspreiden naar alle andere externe routers, alsook naar moore.iii.hogent.be, zal de externe router gebruikmaken van een RIPv2-router (via Quagga). Belangrijk: voor een correcte werking is het noodzakelijk dat je elk toestel gebruikt voor de functie zoals aangegeven in de figuur voor 2.031 of 2.035.

De bastion host bevindt zich in de DMZ. De bastion host fungeert als bridge, zodat hij in de DMZ ook verbonden is met zowel de interne als met de externe router. Hij zal ook dienst doen als nameserver, als webserver, en als proxyserver voor HTTP en HTTPS (zie verder).

De interne router verbindt het interne netwerk met de DMZ. Op het interne netwerk is één pc aangesloten die dienst doet als testclient (CL).

De DMZ is rechtstreeks bereikbaar van overal op het ïnternet"maar maskeert het interne netwerk. Dat betekent dat geen enkele computer op het interne netwerk (o.a. de testclient CL) bereikbaar is van buiten, ook niet vanaf de DMZ. Het private netwerk 10.0.0.0/8 moet dus gemaskeerd worden met behulp van NAT. Voor de configuratie van NAT maak je gebruik van iptables.

Opgelet: Op moore.iii.hogent.be (192.168.16.8) worden de routes naar alle gedemilitariseerde zones door Quagga verzameld. Je zal 192.168.16.8 dus moeten instellen als default gateway!

Indien nodig kan je voor de toestellen binnen je netwerk tijdelijk 192.168.16.8 instellen als DNS-server. Wanneer je opstelling volledig geconfigureerd is, zou je dan vanaf elk toestel (dus ook de interne client) moeten kunnen surfen op het Internet. Begin niet aan een volgende onderdeel zolang de routing nog niet volledig werkt!

9.2 DNS, web- en proxyserver

Configureer de bastion host zodat hij dienst doet als nameserver, webserver en proxyserver voor HTTP/HTTPS:

De nameserver is de primaire (en enige) nameserver voor je eigen zone. Hij moet zowel kunnen antwoorden op forward als op reverse DNS query's. Voor de toestellen binnen jouw zone maak je gebruik van de oorspronkelijke computernamen (bv. archimedes.groep19.iii.hogent.be). Vragen die de nameserver zelf niet kan beantwoorden stuurt hij door (via een forwarder) naar 192.168.16.8. Voor de configuratie van de webserver maak je gebruik van apache (httpd). De website is vanaf het interne netwerk bereikbaar op poort 80. Het is niet nodig om HTTPS te configureren. Voor de proxyserver maak je eveneens gebruik van apache (httpd). De proxy-server zal alle HTTP en HTTPS requests op poort 8080 doorsturen naar de remote proxyserver op 192.168.16.8:8080.

Eenmaal je DNS-configuratie in orde is, is het de bedoeling dat elk toestel binnen jouw groep je eigen DNS-server gebruikt (en dus niet 192.168.16.8). Bovendien configureer je de browser van de interne client zodat deze de proxyserver van jouw BH gebruikt voor alle HTTP/HTTPS aanvragen, behalve deze naar je eigen website. Als je configuratie correct is zou je vanaf de interne client nog steeds moeten kunnen surfen op het Internet (maar dus nu via de proxyserver). Test je opstelling grondig vooraleer je begint met de configuratie van de firewallregels!

9.3 Firewall

Nu is het de bedoeling dat je de nodige firewallregels toevoegt op zowel de externe router als de interne router. In tegenstelling tot het vorige labo (iptables) gebruik je tijdens dit labo statefull firewallregels waar mogelijk. Schrijf bovendien de firewall regels zo strikt mogelijk.

Zorg ook voor de nodige firewallregels zodat:

De interne router HTTP, DNS, SSH en proxyverkeer doorlaat van het private netwerk naar de bastion host, en speciaal voor dit labo de client ook toelaat om te pingen naar alle computers binnen de DMZ maar niet verder. De externe router DNS, SSH en proxyverkeer doorlaat van de bastion host naar het publieke netwerk (het internet). Bovendien moet de DNS-informatie op de bastion host van buiten je DMZ (internet) bereikbaar zijn. De website op de bastion host mag echter enkel intern bereikbaar zijn. Zorg er bovendien voor dat je van een extern toestel naar de bastion host (enkel dit toestel!) kunt pingen. De externe router draait RIP via Quagga, alle inkomende en uitgaande berichten die te maken hebben met RIPv2 moeten dus ook worden toegelaten.

Vooraleer je de opstelling weer mag afbreken, moet ze geëvalueerd worden door één van de docenten. Alvorens een docent te vragen om je opstelling na te kijken, kan je zelf controleren of alles correct werkt via deze checklist. Algemene richtlijnen:

Om deze opstelling te verwezenlijken moet de bestaande netwerkbekabeling worden aangepast. Bedenk dat op het einde van de labosessie de oorspronkelijke toestand moet hersteld worden in een werkende staat. Bij groepen die dit verzuimen zal de quotering worden aangepast! Noteer dus alles goed vooraleer je iets verandert en test of de teruggeplaatste instellingen functioneren.

Bovendien moet je er rekening mee houden dat van elk paar UTP-netwerkcontactdozen op de tafel er steeds maar één connector is verbonden; onthoud dus de welke. Ook is het van belang om van de twee (of meer) netwerkinterfaces in de pc's opnieuw de juiste te verbinden!

Bedenk ook dat eens het netwerk is onderbroken, het publieke internet en dus ook Minerva (tijdelijk) niet meer van op elke machine bereikbaar zijn. Enkel de externe router blijft aangesloten op het ïnternet"met zijn origineel IP-adres.