examen LINUX advanced december 2016 -- Netwerkbeheerder -- Syntra-ab-mechelen

NAAM:

TOTAAL .. / **100**

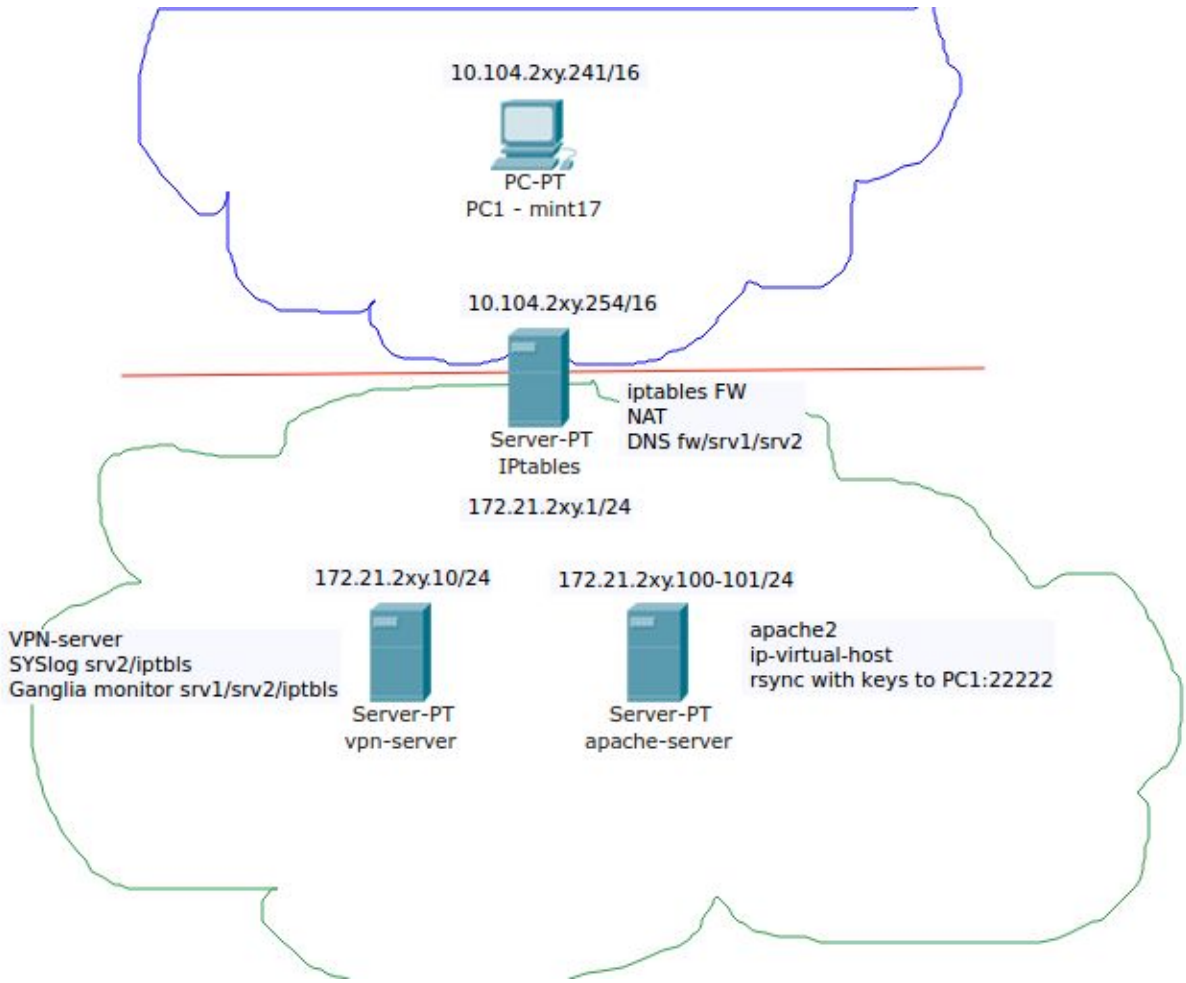
Definitieve Versie

Schrijf uw antwoorden duidelijk op,
begin met uw naam, afdeling en de datum.
Indien er niet genoeg plaats is voorzien voor een antwoord,
mag uw losse bladen toevoegen met uw naam erop.

LEES EERST AANDACHTIG DE VOLLEDIGE OPDRACHT ...

PRAKTIJK EXAMEN

U moet een klein netwerk opzetten met 4 machines:

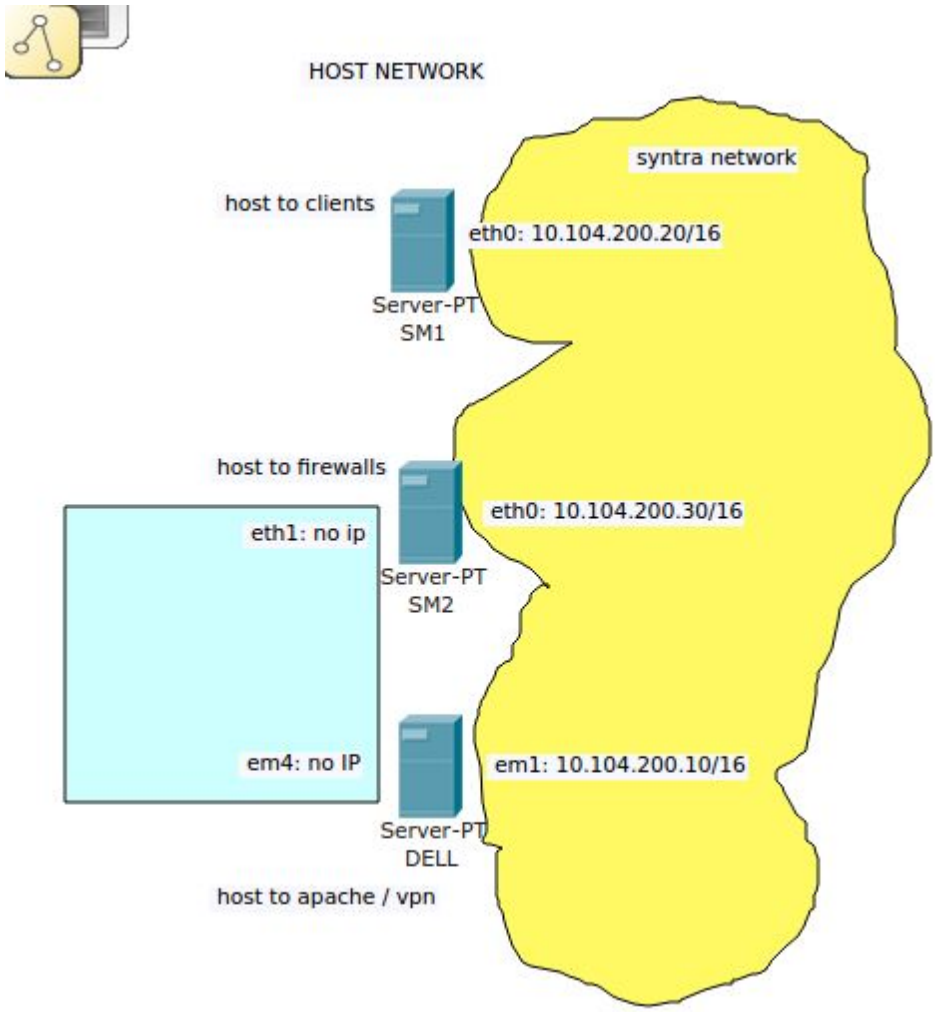


Enerzijds heeft u het standaardnetwerk van lokaal 104: 10.104/16, met daarin een client en een firewall;
Anderzijds heeft u een private LAN: 172.21.2xy/24, met daarin het andere eind van de firewall, een vpn-server en een apache server.

U maakt een virtuele firewall in **10.104.2xy.254**/16 met NAT naar 172.21.2XY.**1**/24
U zet een APACHE2-server op 172.21.2XY.**100**/24 en 172.21.2XY.**101**/24 (2 ip-adressen)
U zet een VPN-server op 172.21.2XY.**10**/24
Bovenstaande **3 servers** maakt u op een **virtualbox in hosts DELL en SM2**

U maakt gebruik van een **virtuele linux-mint17 10.104.2xy.241** onder **virtualbox op uw eigen laptop** voor de **client.**

Om dit te realiseren krijgt u via SSH toegang tot 3 servers:



Server ~~SM1~~ komt te vervallen en wordt vervangen door uw laptop.

Op server SM2 is er plaats je je firewall naar jouw intern netwerk.
Op server DELL is er plaats je 2 servers: vpn-server en apache-server

Dit is de basis, maar er zijn nog andere functionaliteiten nodig … (dns, ganglia, syslog, rsync-backup, ...)

Iedereen heeft een account op de HOST-servers van de figuur hierboven.
Met deze account kun je, via ssh, virtualbox gebruiken op deze servers, en er je 3 virtuele servers op aanmaken.
De HOST servers zijn al correct bekabeld. Maar je zal je virtuals wel moeten connecteren op de juiste netwerkpoort van de HOSTs.
Er zijn al clean-to-clone machines aanwezig op de servers zodat je niet meer moet installeren.

SSH TESTEN

1. Voor je iets anders doet verbindt je jezelf eerst met de drie servers op **10.104.200.10 en 10.104.200.30** via standaard SSH en **je voornaam als user**. Wijzig onmiddellijk je paswoord. Log-uit en log opnieuw in om te testen of het gelukt is.

   Als je niet kan inloggen vraag de docent om hulp.

2. **Probeer vervolgens je grafische toegang … (zie hieronder)**

TOEGANG TOT VIRTUALBOX OP HOST-servers -> Dit doe je via een virtuele linuxmint17 op je eigen laptop.

1. **SSH op linux-GUI**

   Gebruik bij voorkeur deze methode …
   vanaf je lokale virtuele linux mint client op je eigen laptop
   my-machine **$ ssh -Y <host-address>**
   my-hostsrv **$ virtualbox**
   Meer info:
   http://new.linux800.be/inleiding/info-pagina-s/ssh-client of
   http://linux800.be/lx-svs-info-sshclient.php

2. **CLI**

   Het is mogelijk virtuals te configureren via de CLI commandset van vboxmanage, en dat direct op de 3 HOST servers … Als je dit nog nooit gedaan hebt, is dit af te raden. Een virtual starten/stoppen is wel eenvoudig, die commando's vind je wat verder …

   Klonen is makkelijk,
   https://www.virtualbox.org/manual/ch08.html#vboxmanage-clonevm

   Netwerkinstellingen aanpassen is *een beetje* ingewikkelder:
   https://www.virtualbox.org/manual/ch08.html#vboxmanage-modifyvm
   vervolgens **8.8.2. Networking settings**

3. ~~**PUTTY onder windows**~~

   ~~Onder windows kun je xming downloaden op https://sourceforge.net/projects/xming/~~
   ~~En daarna laten samenwerken met Putty als onder~~
   ~~https://docs.math.osu.edu/windows/how-tos/ssh-from-windows-graphical-linux-programs-x11-forwarding/~~
   ~~Ik heb dit echter niet meer getest sedert 2011.~~

ip-ADRESSEN:

Je virtuals moet je straks voorzien van een correcte netwerkconfiguratie.
Die vind je in de figuur hieronder …

	SYNTRA-104: 10.104/16		LOCAL: 172.21.2xy/24		
gebruiker	Mint client	Firewall		vpn-server	apache-server
bert	10.104.201.241	10.104.201.254	172.21.201.1	172.21.201.10	172.21.201.100
aristote	10.104.202.241	10.104.202.254	172.21.202.1	172.21.202.10	172.21.202.100
arno	10.104.203.241	10.104.203.254	172.21.203.1	172.21.203.10	172.21.203.100
ayoub	10.104.204.241	10.104.204.254	172.21.204.1	172.21.204.10	172.21.204.100
bramdv	10.104.2xy.241	10.104.205.254	172.21.205.1	172.21.205.10	172.21.205.100
bramvh	10.104.2xy.241	10.104.206.254	172.21.206.1	172.21.206.10	172.21.206.100
dario	10.104.2xy.241	10.104.207.254	172.21.207.1	172.21.207.10	172.21.207.100
dylan	10.104.2xy.241	10.104.208.254	172.21.208.1	172.21.208.10	172.21.208.100
nick	10.104.2xy.241	10.104.209.254	172.21.209.1	172.21.209.10	172.21.209.100
nicolas	10.104.2xy.241	10.104.210.254	172.21.210.1	172.21.210.10	172.21.210.100
sander	10.104.2xy.241	10.104.211.254	172.21.211.1	172.21.211.10	172.21.211.100
senne	10.104.2xy.241	10.104.212.254	172.21.212.1	172.21.212.10	172.21.212.100
sergei	10.104.2xy.241	10.104.213.254	172.21.213.1	172.21.213.10	172.21.213.100
steffen	10.104.2xy.241	10.104.214.254	172.21.214.1	172.21.214.10	172.21.214.100
steve	10.104.2xy.241	10.104.215.254	172.21.215.1	172.21.215.10	172.21.215.100
stijn	10.104.2xy.241	10.104.216.254	172.21.216.1	172.21.216.10	172.21.216.100
sven	10.104.2xy.241	10.104.217.254	172.21.217.1	172.21.217.10	172.21.217.100

Zoek uw naam in deze tabel, en u vindt uw 5 vaste ip-adressen terug …
Kies zelf voor alle 4 virtuele machines een correcte default gateway en dns

Nuttige TIPS:

- **Begin in elk geval met een PLAN van aanpak.**

- Zorg zo snel mogelijk voor SSH toegang vanaf netwerk 10.104/16 naar alle machines (dat werkt makkelijker en sneller) zie **HOWTO**

- Het vorige punt impliceert dat je na het klonen van je drie servers met de firewall begint, **niet alles**, maar op zijn minst **NAT naar het binnen netwerk** en **SSH open van 10.104 naar APACHE-server en naar VPN-server.**

- **Telkens als je een service op een server configureert die naar buiten moet, voeg je die ook toe aan iptables. Zo wordt de firewall niet onoverkomelijk ingewikkeld, maar een stap voor stap oplossing.**

- Doe eerst **wat je het makkelijkst kan**, en waar je het minste tijd aan besteedt.

- **Je kan het ook anders aanpakken -- er zijn vele manieren om deze opdracht tot een goed einde te brengen. Begin in elk geval met een PLAN.**
  JE PLAN tonen kan een voordeel opleveren bij een slecht examen.

- **De VPN-service plan je best tegen het eind ... de andere diensten op de VPN-server zijn makkelijker en doe je beter halfweg ...**

OPDRACHT + puntenverdeling:

VPN-server (25)

- 00 ***(a)*** SSH op poort 22 (translate gebeurt op FW)
- **10** ***(b)*** **Ganglia Website** (3 machines (fw - vpn - apa) zichtbaar dus 3 ganglia clients)
- **05** ***(c)*** **SYSLOG-service** (2 machines (fw - apa) syslog client)
- **10** ***(d)*** **VPN-service** key size 1024 (don't waste time and cpu)

APAche-server (35)

- 00 ***(a)*** SSH op standaard poort 22 (translate gebeurt op FW)
- **03** ***(b)*** **GANGLIA-client apache in ganglia vpn-server (wacht er niet op)**
- **02** ***(c)*** **SYSLOG-client apache in syslog vpn-server (wacht er niet op)**

- **05** ***(e)*** **APAche-service**
- **05** ***(f)*** 2nd-IP + 2nd Website

- **05** ***(g)*** **SFTP-service** ***writeable*** naar 2 websites (zelfde account)

- **05** ***(h)*** **KEYS** op mint-client
- **10** ***(i)*** **correct RSYNC** command **(5)** in werkende CRON-job hourly bash-script **(5)**

Firewall (45)

- **05** ***(j)*** **SSH-service naar FW** SSH port 22 vanaf 172.21 en port 30022 van 10.104
- **03** ***(c)*** **GANGLIA-client FW in ganglia vpn-server (wacht er niet op)**
- **02** ***(d)*** **SYSLOG-client FW in syslog vpn-server (wacht er niet op)**

- **iptables**:

- **05** ***(k)*** **binnen naar buiten** NAT 172.21->10.104 (van 172.21 naar 10.104)

- **03** ***(l)*** **buiten naar naar APA-srv** SSH forwarding FW-addr:10022 port 22
- **02** ***(l)*** **buiten naar naar VPN-srv** SSH forwarding FW-addr:1022 port 22

- **03** ***(m)*** **van buiten naar FW** SSH op 30022
- **02** ***(m)*** **van binnen naar FW** SSH op 22

- **03** ***(n)*** **van buiten naar APA HTTP:80** website 1 van apache-server
- **02** ***(n)*** **van buiten naar APA HTTP:81** website 2 van apache-server

- **03** ***(o)*** **van buiten naar VPN HTTP:8080** ganglia website vpn
- **02** ***(o)*** **van buiten naar VPN TCP:1194** vpn service

- **03** ***(p)*** **van binnen naar DNS 10.28.100.10 en 10.28.100.20**
- **02** ***(p)*** **van binnen naar alle HTTP (apt-get etc)**
- **02** ***(p)*** **van binnen naar alle SSH op poort 22**
- **03** ***(p)*** **van binnen (APA-srv) naar Mint-CLT SSH op 22222**

- **--** ***(q)*** ALL ELSE CLOSED - ***if not subtract***

Mint-client (25)

- 00 ***(r)*** SSH-target, KEY-target, Rsync-target werkt vanuit APache-server
- **05** ***(s)*** **SSH-service** geconfigureerd als "root without password" op port 22222
- **10** ***(t)*** VPN-client-werkt volledig:
  (ssh 172.21.2xy.10 of 172.21.2xy.100 werkt **zodra VPN AAN** staat)
- **05** ***(u)*** Ganglia-website zichtbaar op firefox 172.21.2xy.10 in client **als VPN AAN** staat
- **05** ***(v)*** SFTP werkt naar APA-server **met en zonder VPN** -- sftp via CLI is OK

HOWTO …

Begin met de DELL-HOST op 10.104.200.10 voor je apache-server en je vpn-server:

- ssh -Y <user>@10.104.200.10
- start virtualbox
- voeg machine toe /home/extras/ubu14srv-c2c
- kloon deze machine twee keer (vpn en apa server) en pas MAC aan
- start een machine (niet allebei tegelijk)
- maak een sudo useraccount voor jezelf aan (standaard login staat in 'description') (test)
- Kijk op welk netwerk je kaart zit -> als die een dhcp adres krijgt zit die verkeerd en moet je in virtualbox kiezen voor de andere (em1 of em4)
- configureer /etc/hostname /etc/hosts /etc/network/interfaces met statisch en correct address / gateway / dns
  (herstart en test)

Vervolgens de SM2-HOST op 10.104.200.30 voor je firewall:

- Idem als hierboven, maar slechts één machine en wel twee netwerkkaarten (kiezen tussen eth0 of eth1 in virtualbox)
- Test SSH vanaf 10.104 naar je FW
- Stel iptables in zodat je google kan pingen vanaf apache-server en vpn-server
- Stel iptables in zodat je ssh vanaf 10.104 naar apache-server (poort 10022) en vpn-server (poort 1022) kan doen.

Herstart nu je 3 machines **HEADLESS** en werk vanaf je terminal met SSH

Configureer nu alles zoals in **<u>je PLAN</u>** volgens de lijst OPDRACHT hierboven …
<u>Een plan wordt ook regelmatig aangepast aan de situatie en onvoorziene problemen …</u>

Doe de **iptables stap voor stap** … je kan er zonodig nog steeds in via virtualbox-GUI

- **Je mag de APACHE server en de GANGLIA server testen vanaf je eigen laptop**

- **Ganglia en syslog test je best na een tijdje …**

- **SFTP naar apache vanaf je eigen linux mint virtual op je laptop: Je moet een index.html op de tweede site (port 81) kunnen aanpassen. Werk bvb. met symbolic links in de home directory van je default user op je apache-server. Pas ownership aan in /var/www ….**

- **Ganglia client op FW: vermits de firewall twee netwerkkaarten heeft moeten we specificeren op welke netwerkkaart (die met 172.21) de multicast gebeurt:**

```
>>> /etc/ganglia/gmond.conf
/* Feel free to specify as many udp_send_channels as you like.  Gmond
   used to only support having a single channel */
udp_send_channel {
  mcast_join = 239.2.11.71
  mcast_if = eth1
  port = 8649
  ttl = 1 }
```

- SSH naar de MINT-client: eerst ssh testen naar de client als gewone user, Root-Keys overzetten naar de client, SSH configureren op poort 22222, testen + Firewall-rule: testen, Controlleer de setting root without password
  Vervolgens een RSYNC testen, tenslotte in de CRON plaatsen.

- **DOE de VPN-server/client als voorlaatst**

- **De allerlaatste stap is het dichtmaken van de Firewall (maak eerst een snapshot van je FW) -- de regels zijn dan al allemaal toegevoegd, maar er is nog niets verboden met DROP - dat is de allerlaatste actie**

Nuttige VBOX CLI commands (als gewone user) **op de HOSTS** (10.104.200.10-20-30)**:**

Start een machine headless

```
$ vboxmanage startvm <machine-naam> -type=headless
```

Shutdown een machine

```
$ vboxmanage controlvm <machine-naam> acpipowerbutton
```

Pauzeer en Ga weer verder:

```
$ vboxmanage controlvm <machine-naam> pause
$ vboxmanage controlvm apa-ub14-srv resume
```

Oplijsten:

```
$ vboxmanage list runningvms
"ubu14srv-apa" {cb6f64b3-8a9c-4aa9-9523-19d1827a1947}
"ubu14srv-vpn" {8a9f09db-9fe6-4895-859b-f4d9df54b1f9}

$ vboxmanage list vms
>> Alle virtuals
```