# Integratie Oefening ANT (2011)

**Versie: 14/02/2011 (initiële versie)**

In dit labo wordt een groot stuk van je reeds verworven kennis op de proef gesteld om een nieuwe, complexe probleemsituatie op te lossen. Concreet zal je een volledig netwerk moeten opbouwen waarin verschillende functionaliteiten voorzien moeten worden zoals ze in een echte bedrijfssituatie zouden kunnen voorkomen. Hier zal heel wat opzoekingswerk en planning aan vooraf gaan. Ook tijdens het configureren zal je wellicht verschillende struikelblokken tegenkomen. Laat je hierdoor echter niet ontmoedigen!! Het eindresultaat zal een mooi stukje concrete en realistische ervaring opleveren.

## Timing en evaluatie

Voor de opdracht krijg je het hele semester de tijd, waarbij er ook een halve dag werd ingeroosterd. Tijdens de laatste 2 weken (lesweek 12 en 13 volgens academische kalender) volgt dan de evaluatie (mondeling)

## Opdracht

Concreet verwachten we van jullie als team de volgende functionaliteiten:

- Een netwerk beheerd door een Active Directory (Single Domain)
- Volledige DNS configuratie voor alle servers, clients en diensten aanwezig in het netwerk.
- Een professionele best-practice setup met Exchange 2010 die een mailomgeving voorziet voor interne en externe (mobiele) gebruikers.
    - Voorzie hiervoor zeker een aparte server voor alle client protocollen (voor connecties van de clients via bv: pop, imap, exchange proto, activesysnc, webmail)
    - Voorzie een aparte server voor alle binnenkomende mail vanop het internet. (SMTP)
    - Andere rollen mogen gerust op 1 overblijvende server geplaatst worden.
    - Respecteer best-practices van msft zoals bijvoorbeeld de locatie in het netwerk en de gevraagde beveiliging (DMZ, firewall toegang,…)
    - Uiteraard moeten de klassieke diensten (protocollen) via de gangbare DNS-benamingen bereikbaar zijn (pop.domein.be; smtp.domain.be; webmail.domein.be,…)
    - Mobiele devices (gebruikers) moeten ook in staat zijn om op basis van hun mailadres een autoconfiguratie voor Exchange Activesyc  toe te passen.
- Voorzie een MSSQL server die verschillende databanken intern kan aanbieden maar ook aan webservers die in de DMZ staan. (opnieuw locatie bepalen en nodige beveiliging voorzien)

- Voorzie één webserver waarop minstens 2 websites staan (met SSL), volledige onafhankelijk van elkaar (2 compleet aparte URL's: vb => www.mijndomein.be en www.eenanderdomein.be) . Een van de websites moet een databank raadplegen van de MSSQL server.

- Voor de beveiliging (Firewall) en scheiding van de verschillende netwerken gebruik je Microsoft Forefront Threat Management Gateway.

- Uiteraard probeer je dit alles zo goed mogelijk volgens de best practices van de fabrikant(en) uit te voeren.

## Vorm

Tijdens deze opgave zal je zelf heel veel opzoekwerk en configuratiewerk moeten doen. Om dit alles wat overzichtelijk te houden vragen we je minimaal volgende zaken:

- Allereerst vooraleer aan de slag te gaan maak je een planning op.
    - Zowel een planning inhoudelijk, bv. welke functionaliteiten je waar zal installeren en welke vereisten er zijn. (dus eigenlijk een design planning)
    - Alsook een planning in de tijd: Welke zaken moeten eerst opgezet worden, welke deadlines hanteer je daar zelf voor? Hoe spreek je onderling af (verdeling, timing).

- Heel belangrijk voor jezelf en voor je docenten zal een degelijk en uitgebreid VISIO schema zijn waarop alle servers, netwerken en andere nuttige info staan.

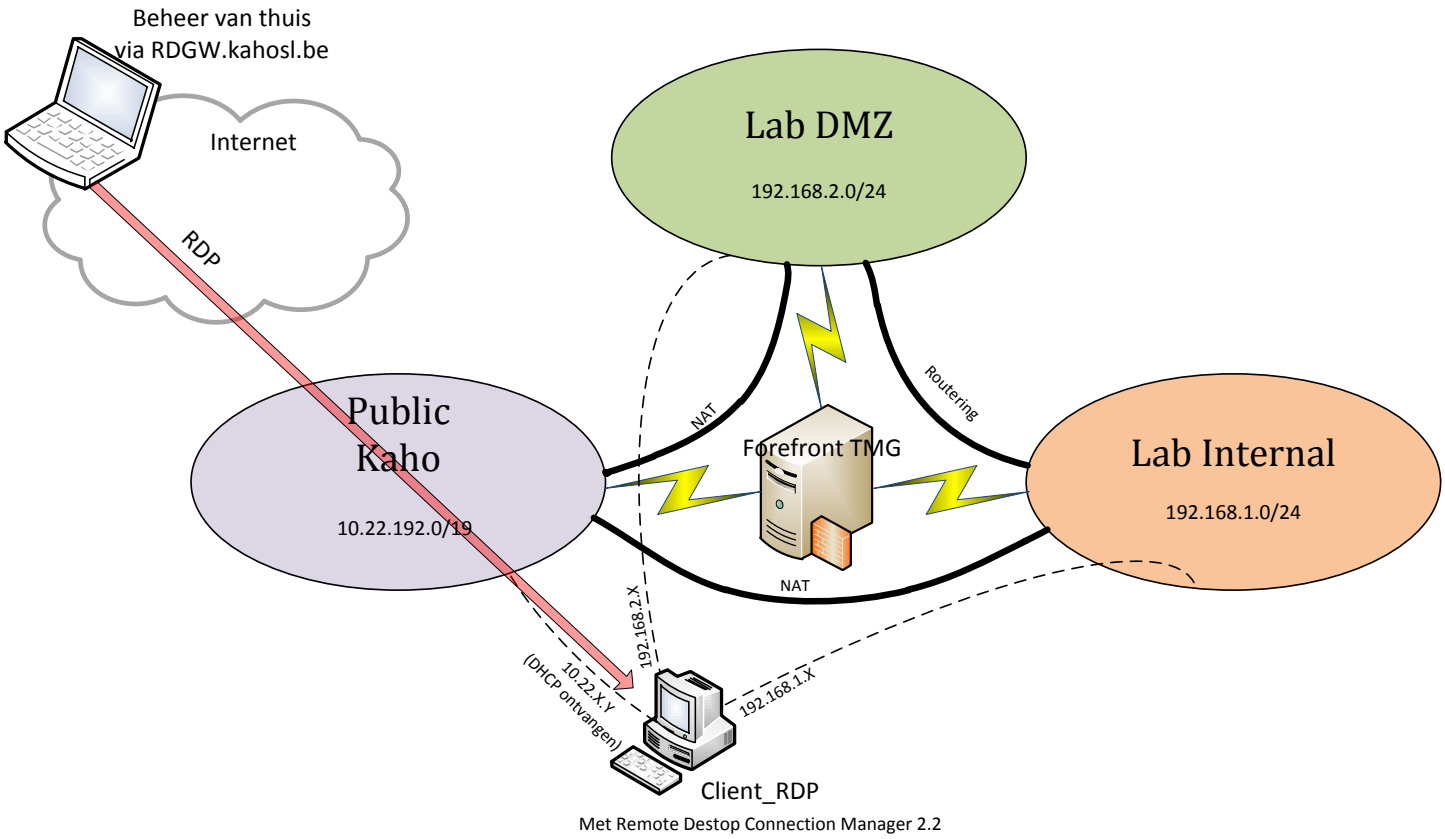
- Als gebruikers voorzie je zeker een "administrator" account met als wachtwoord Ant12345 zodat de docenten op alle servers en clients kunnen inloggen met deze account.

- De volledige opstelling wordt geïmplementeerd in de virtualisatieomgeving.

- Je voorziet voor elke service die je configureert (eventueel opgesplitst in kleinere entiteiten) een neerslag van de installatiestappen die je uitvoerde. Gebruik daarvoor Google Docs. Je mailt hiervoor ook een publieke link (die je best verder niet doorgeeft…) naar één van je docenten. Zo zijn we in staat jullie status te volgen… Je zal dit sowieso nodig hebben om je teamgenoot op de hoogte te houden van de stappen die elk ondernomen hebt.

# Start van de opgave

Om je goed op weg te zetten krijg je hieronder enkele praktische tips mee:




## *Netwerken*

- Het netwerk zal opgesplitst moeten worden in drie zones (Publiek, DMZ en intern)
  Op bovenstaand schema zie je de gebruikte netwerken hiervoor.
- Het connecteren van deze verschillende zones zal gebeuren door een software router/firewall genaamd Forefront Threat Management Gateway.
- Deze hierboven genoemde server zal dus drie netwerkkaarten moeten bevatten die in de verschillende netwerken gekoppeld worden
- In labmanager zal je zelf de nodige netwerkkaarten moeten toevoegen aan de server die in het juiste netwerk zitten. Je zal dan ook in Lab Manager volgende netwerken kunnen selecteren:
    - Lab Internal
    - Lab DMZ
    - Virtuele Machines (gewoon) => Public Kaho

- Zoals je uit het schema kan afleiden, wordt de communicatie tussen het Interne netwerk en het publieke door een NAT functie gescheiden. Dat is ook zo voor de communicatie tussen de DMZ en het publieke netwerk

- De communicatie tussen het interne netwerk en de DMZ is gewoon gerouteerd.

- Uiteraard laat je enkel tussen de verschillende zones het juist noodzakelijke verkeer door de firewall.

### *Beheren*

- Om je verschillende servers en clients makkelijk via RDP (van thuis) te beheren moet er een speciale setup voorzien worden die ook schematisch in bovenstaande figuur weergegeven is. Dit is een situatie die eigenlijk geen deel uitmaakt van het "echte" netwerk dat je opbouwt aangezien dit een security issue veroorzaakt.

- We voorzien een gewone client (Client_RDP) die (net zoals de Forefront server) drie netwerkaarten krijgt in de verschillende zones

- Op die client installeer je de Remote Desktop Connection Manager 2.2 waarin je al je servers en clients in de verschillende zones toevoegt.

- Op die manier ben je in staat om alle servers en clients via RDP te configureren vanuit deze client. Deze client kan je ook rechtstreeks van thuis bereiken via de RDGW.kahosl.be gateway server (meer info op Wiki ICT van Toledo)

### *Naamgeving*

- Draag zorg voor je naamgeving. Geef je servers en cleints heel duidelijke namen die vertellen wat hun functie is en waar ze zich bevinden (bv: DC1_intern is een domeincontroller in het interne netwerk)

- Geef ook de netwerken in je servers en clients ook een naamgeving die verwijst naar het netwerk waarin ze zitten. Dat zal je redelijk wat problemen besparen (bv: NIC_intern, NIC_DMZ,…)