



Friends of Oracle and Java

# Security in de praktijk

De security consultant aan het woord

Bram van Pelt, 9-2-2016

## Wie ben ik

- Bram van Pelt
- Senior Security Consultant
- Identity and access management
- Penetration testing
- Intrusion detection and prevention
- Enterprise private key infrastructure
- Network Security
- Security architecture
- Stage begeleider / bedrijfscoach
- <https://nl.linkedin.com/in/bram-van-pelt-77a15021>



# Klanten



Inspectie Veiligheid en Justitie  
Ministerie van Veiligheid en Justitie



Sociale Verzekeringsbank



Hogeschool van Amsterdam



## Amis

AMIS is dé Oracle technologie partner in Nederland. Consultants van AMIS zijn betrokken bij alle grote Oracle projecten in Nederland en diverse spraakmakende projecten wereldwijd. Wij helpen onze opdrachtgevers maximaal rendement uit hun investeringen in moderne Oracle technologie te halen.

- 2015 - Oracle Nederland Middleware Partner of the Year
- 2014 - Oracle EMEA Middleware Partner of the Year
- 2014 - Oracle Nederland Middleware Partner of the Year
- 2014 - Oracle EMEA SOA Partner Community Award
- 2013 - Oracle Nederland Middleware Partner of the Year
- 2011 - Oracle Nederland Middleware Partner of the Year
- 2010 - EMEA SOA Partner Community Award
- 2007 - Oracle PL/SQL Innovation and Community award
- 2004 - XML Holland Award

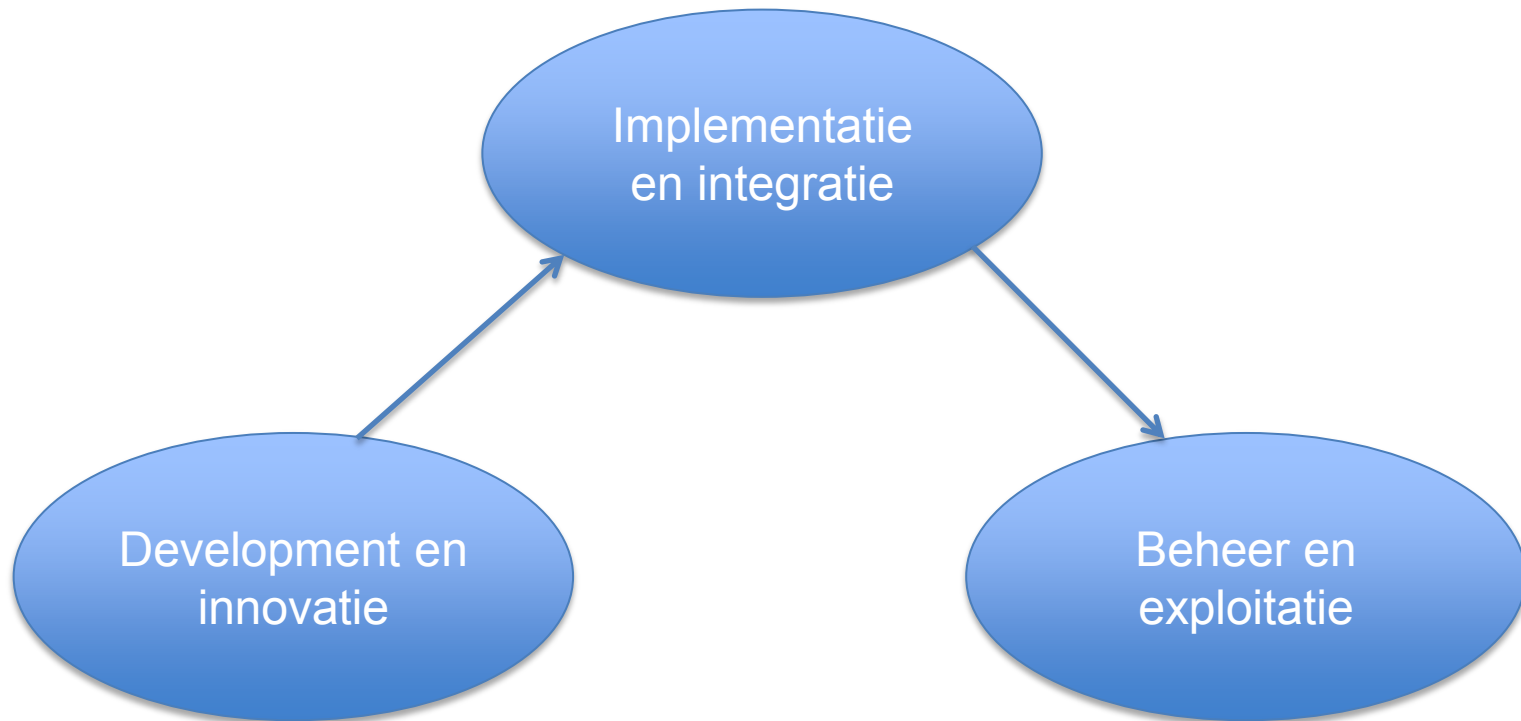
*De beste door XML aangedreven website van Nederland: <http://studiegids.uva.nl>*

## Agenda

- Ik doe een presentatie over security in de praktijk
- Mijn stijl is van de hak op de tak, sorry

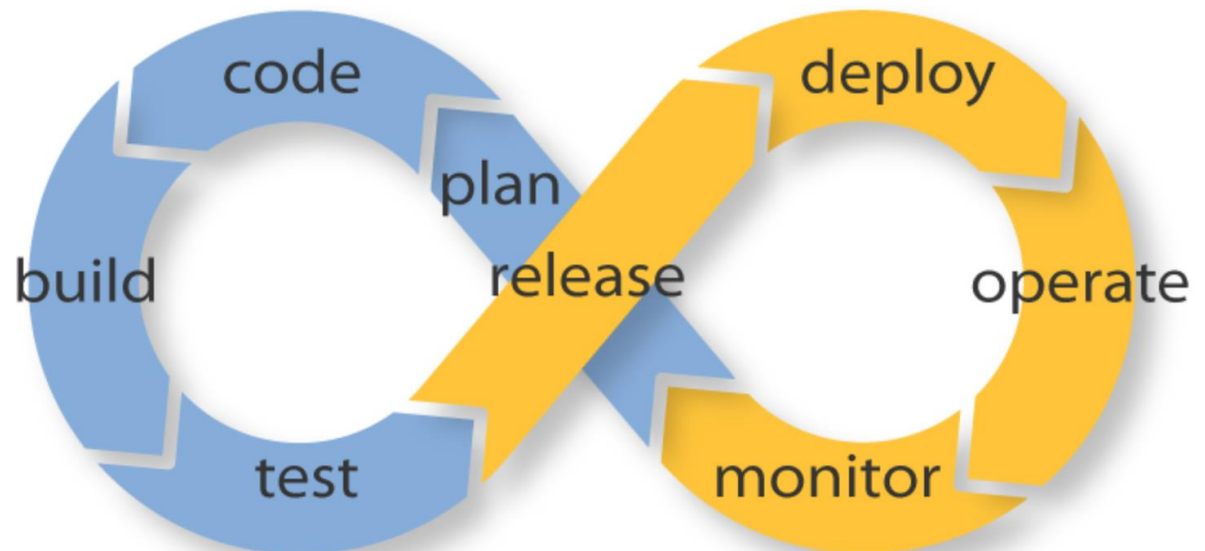


## De context



## Development en innovatie

- Programmeurs / testers / devopsers
- Product coördinatoren
- 80% custom software / 20 % general software
- Licentie betalingsmodel
- Je bent afhankelijk van de kwaliteit van je ideeën, daarna pas de kwaliteit van je software





# Development en innovatie

- Pluspunten
  - Software schrijven
  - Theoretisch oplossingen bedenken
  - Focus op je eigen product
- Minpunten
  - Je bent geen Indiër
  - Hoge concurrentie druk

```
@staticmethod
def format_bytes(bytes):
    if bytes is None:
        return "N/A"
    suffixes = ['B', 'KiB', 'MiB', 'GiB', 'TiB', 'PiB', 'EiB', 'ZiB', 'YiB']
    exponent = 0
    while bytes > 1024:
        bytes = bytes / 1024
        exponent += 1
    suffix = suffixes[exponent]
    converted = float(bytes) / float(1024 ** exponent)
    return '%.1f%s' % (converted, suffix)
```

"Always code as if the guy who ends up  
maintaining your code will be a violent  
psychopath who knows where you live."

~ John Woods

```
@staticmethod
def calc_percent(byte_counter, data_len):
    if data_len is None:
        return "----%"
    return '%s' % ('%.1f%%' % (float(byte_counter) / float(data_len) * 100.0))
```



# Implementatie en integratie

- Consultants / engineers / architecten
- Probleem -> oplossing
- Grote consultancy bedrijven
- Uurtje factuurtje
- Moeilijkste puzzels
- Het belangrijkste is niet welke oplossing je maakt, maar hoe je jouw oplossing aan de klant kan uitleggen.



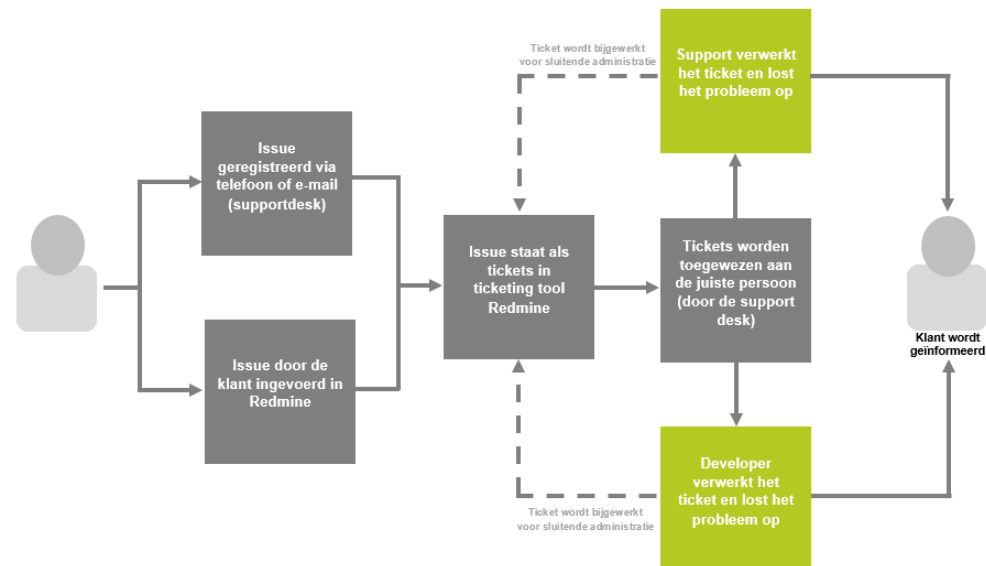
# Implementatie en integratie

- Pluspunten
  - Afwisselende projecten
  - Praktische oplossingen bedenken
  - Ingehuurd om jouw kennis
- Minpunten
  - Afhankelijk van development
  - Klantsturing moet je leren



# Beheer en exploitatie

- Functioneel / technisch Beheerder, product eigenaar, technisch specialist
- Onderdeel van een bedrijf
- Lijn organisatie
- Optimalisatie van de implementatie
- Changes doorvoeren
- De klant heeft altijd gelijk, jij hebt altijd minder gelijk



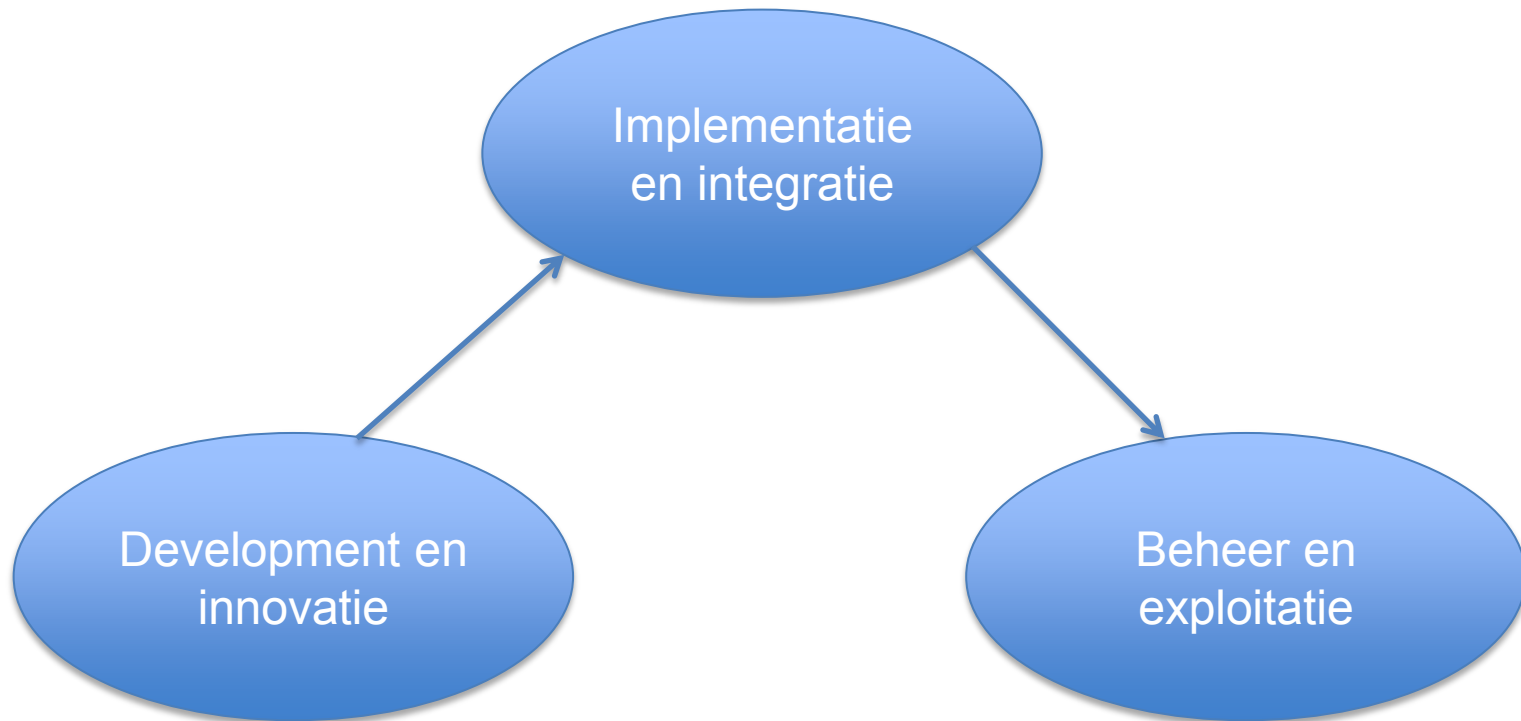
## Beheer en exploitatie

- Pluspunten
  - Paycheck
  - Eigenaarschap
  - Baanzekerheid
- Minpunten
  - Gebruikerscontact
  - Regulatiedruk



# NETWORK ADMIN

We may be strange, but we know what you surf for during lunch.



## Security, how does it work?

- Security consultant:
- Think – plan – act
- Think: What are my securables?
- Plan: How do I secure these?
- Act: How do I keep securing these?





## The security toy chest!

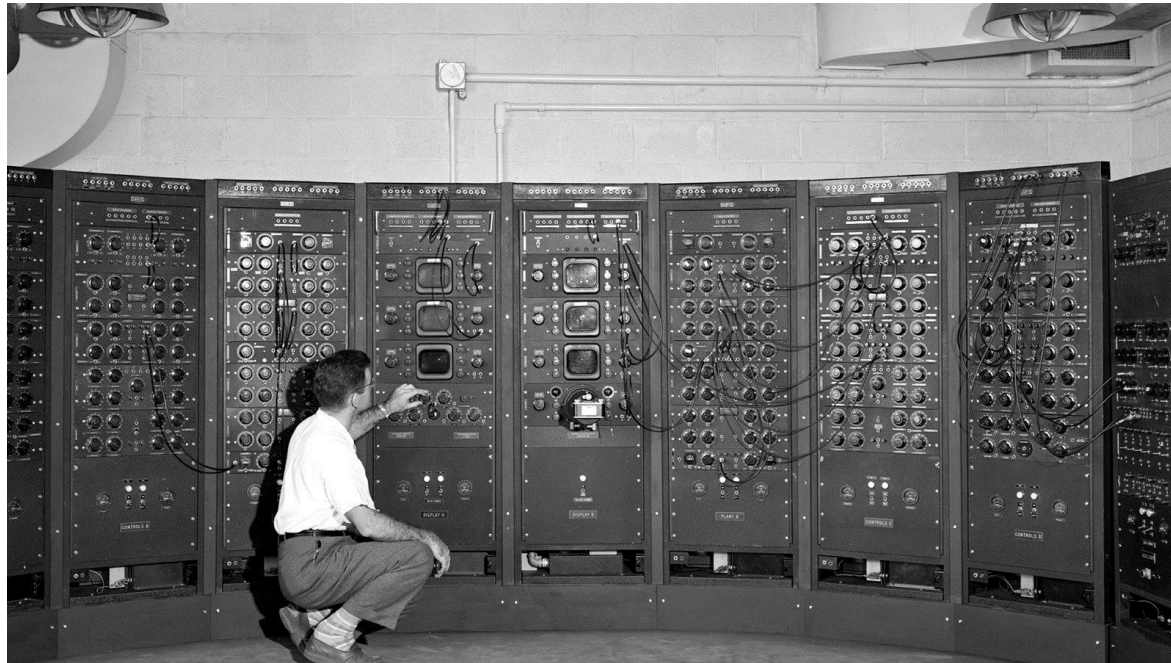
- Network security
- Endpoint security
- Application security
- Data security
- Entity Security





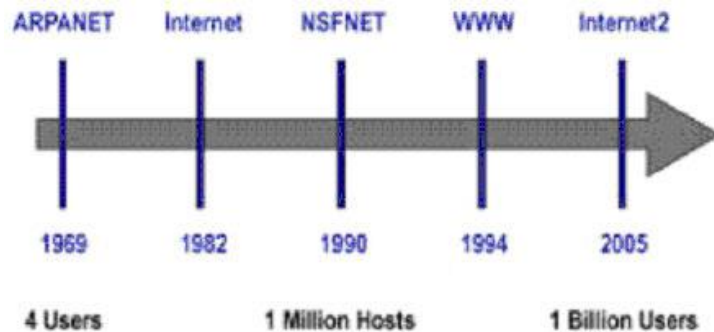
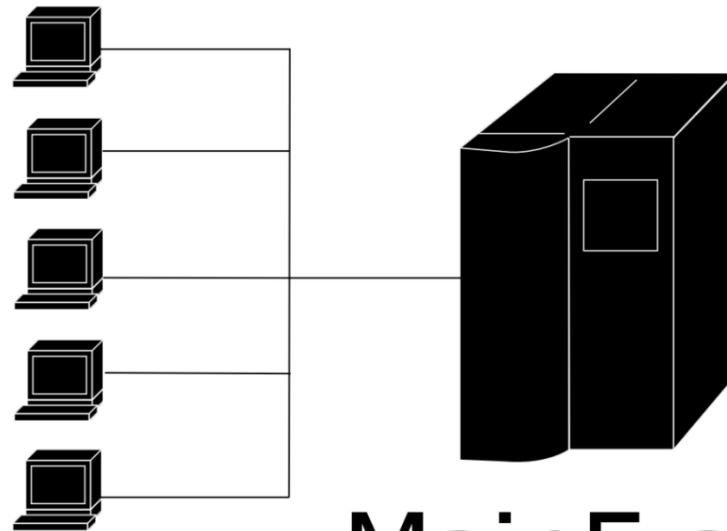
# Network security

- Lang, lang geleden...



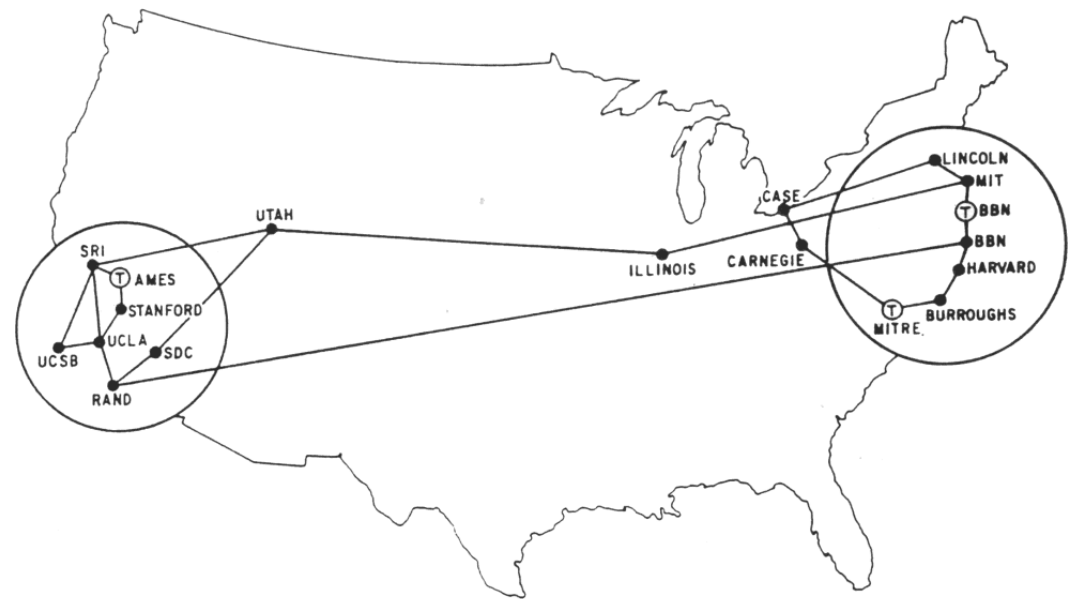
## Network security

- Uitvinding van het wachtwoord

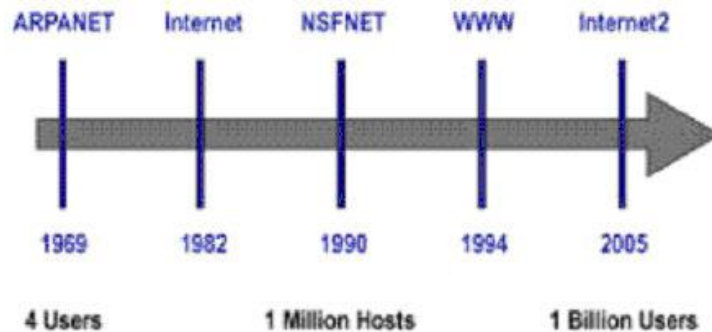


# Network security

- Birth of an “interconnected net”
- Aanvallers van buiten

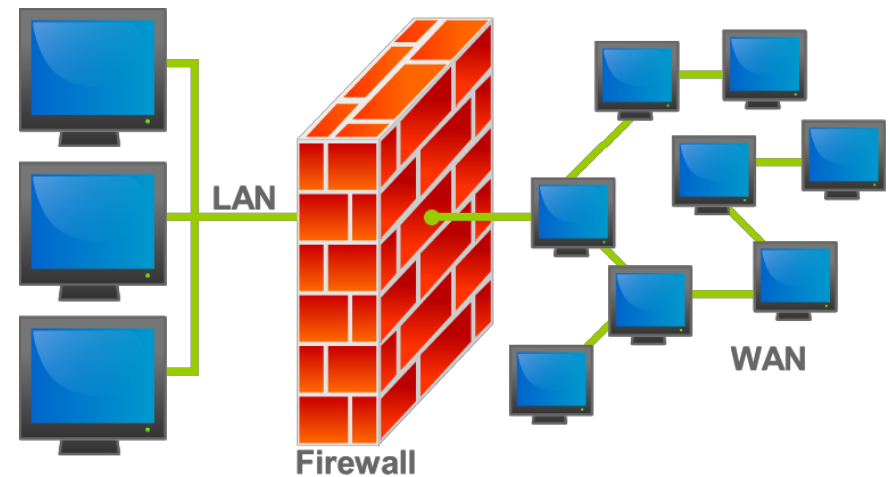
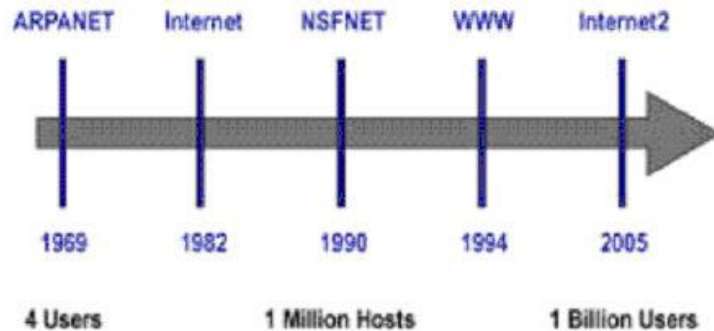


MAP 4 September 1971



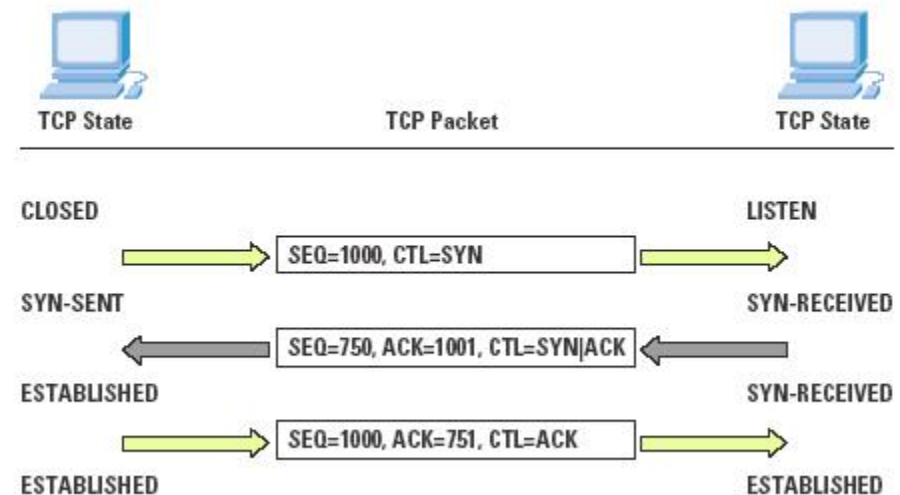
# Network security: Firewall

- Firewall
- Hoe werkt een firewall?
- Hoe zet je een firewall in als bedrijf?



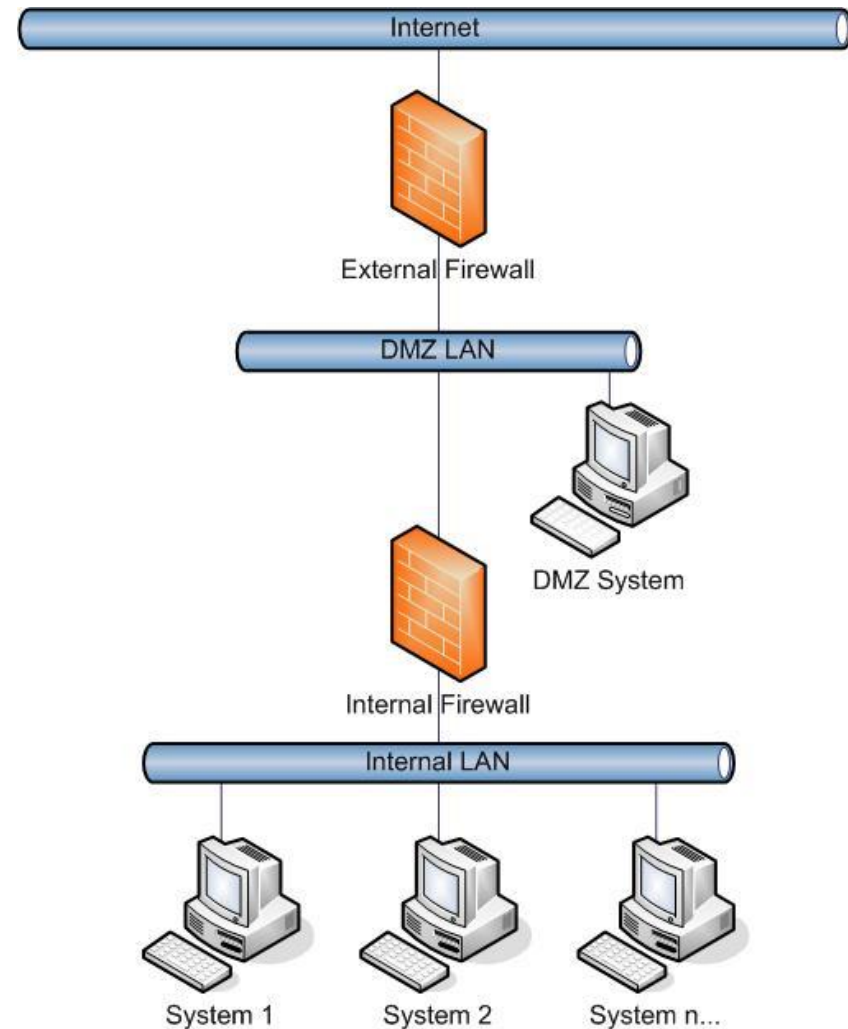
# Network security: Firewall

- Hoe werkt een moderne level 4 firewall
  - Statefull firewall
  - Per poort instelbaar
  - Richting van het verkeer
  - TCP verkeer



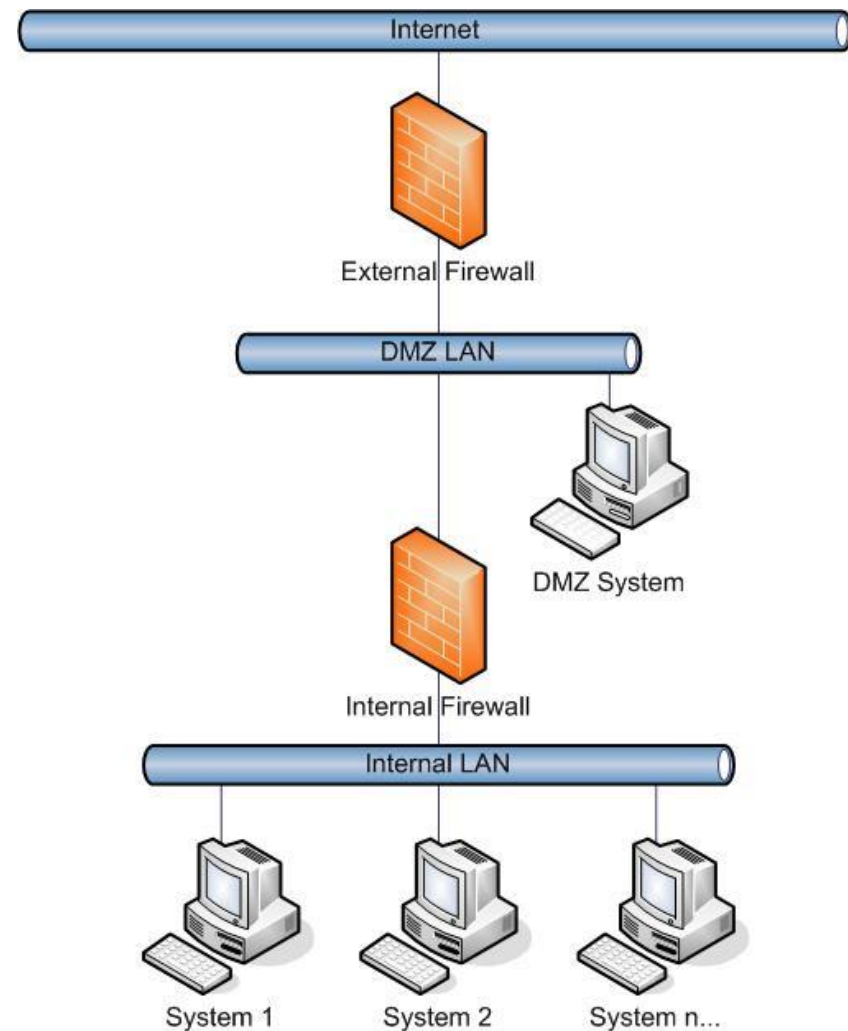
# Network security: Firewall

- Hoe zet je een firewall in als bedrijf?
- DMZ
- Hotel california
- Trapped in the DMZ?



## Network security: Proxy

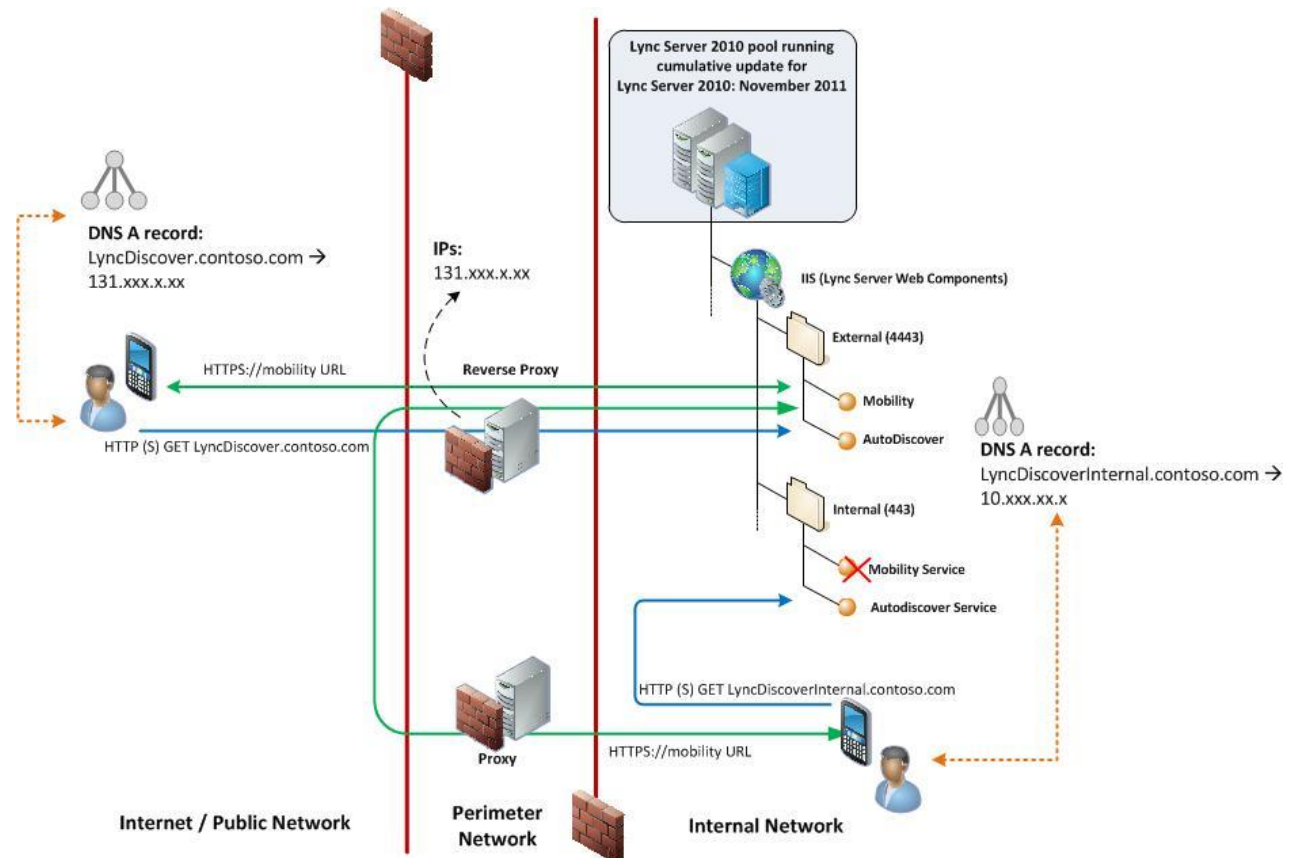
- Proxy als uitzondering op DMZ regels
- Meestal ook voor inspectie
- Dus niet om anoniem te worden





# Network security: Reverse Proxy

- Doorgeef luik
- Inspectie moment
- Load balancer
- Fail over
- Data control
- SSL termination
- Caching



# Voorbeeld: Oracle Database Firewall

## Overview

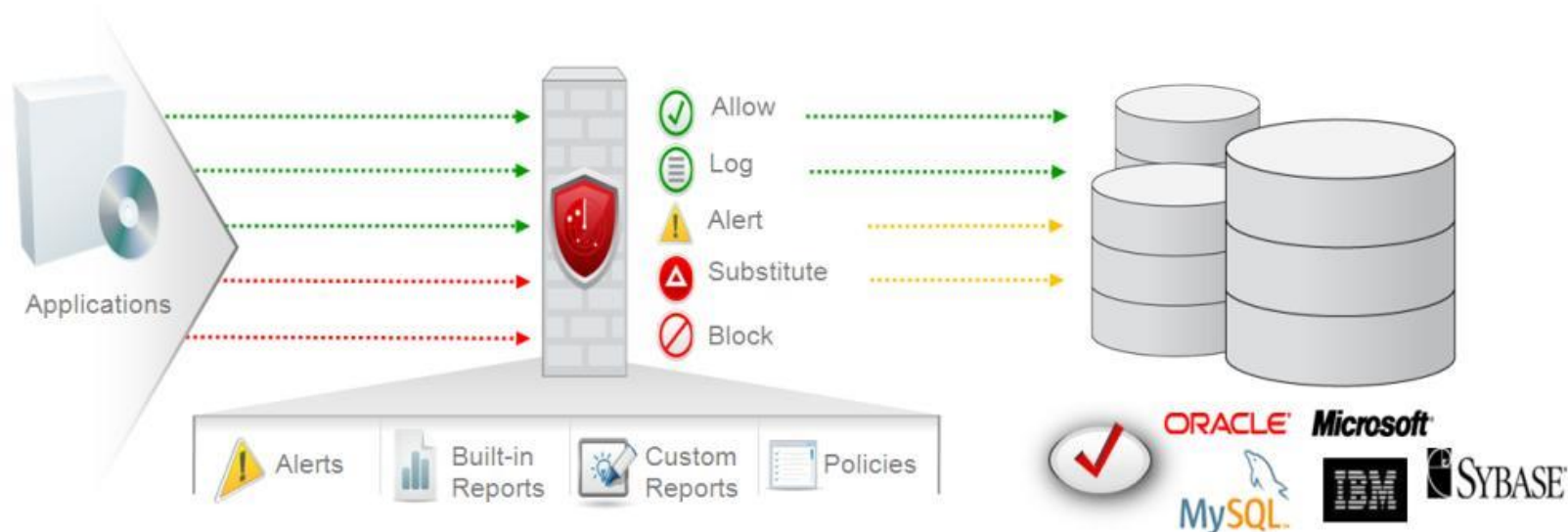
- Accurately detects and blocks unauthorized database activity including SQL injection attacks by monitoring traffic to Oracle and non-Oracle databases
- Consolidates audit data and logs generated by databases, operating systems, directories, file systems, and custom sources into a secure centralized repository
- Provides enterprise security intelligence and efficient compliance reporting by combining monitoring and audit data
- Utilizes a unique SQL grammar analysis engine and easy-to-define whitelists and blacklists to ensure high accuracy and performance
- Delivers horizontal and vertical scalability through easy-to-deploy "software appliances"

## Benefits

- First line of defense: Transparently detect and block SQL injection attacks, privilege escalation, and other threats against Oracle, Microsoft SQL Server, IBM DB2, SAP Sybase, and MySQL databases
  - Faster response: Automatically detect unauthorized database activities that violate security policies, and thwart perpetrators from covering their tracks
  - Simplified compliance reporting: Easily analyze audit and event data and take action in a timely fashion with out-of-the-box compliance reports
- 
- <http://www.oracle.com/us/products/database/security/audit-vault-database-firewall/overview/index.html>

## Voorbeeld: Oracle Database Firewall

- Dus, een reverse proxy met de naam firewall
- Waarom wordt het een firewall genoemd als het een r-proxy is?
- Puriteinse fout



## The security toy chest!

- Network security
- Endpoint security
- Application security
- Data security
- Entity Security



**THIS IS LEGAL**

But Marijuana Is Not



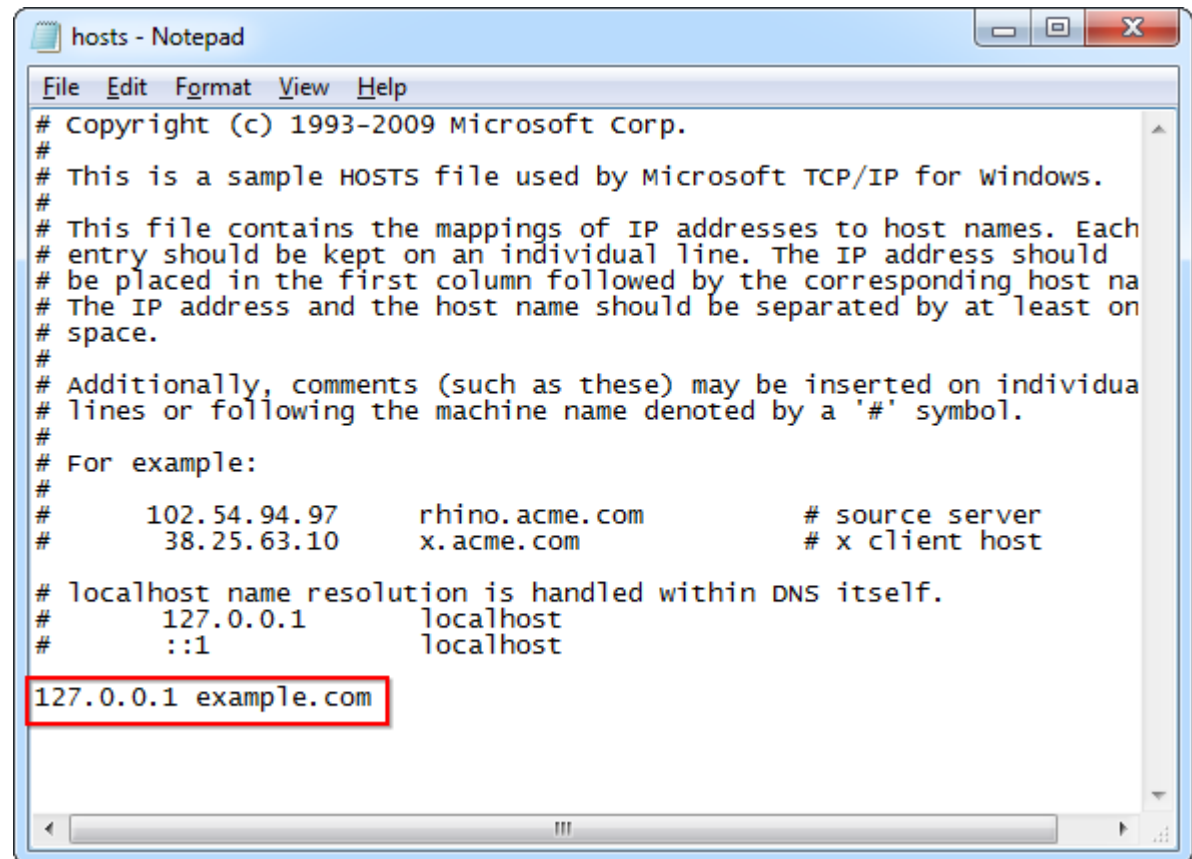
## Endpoint security

- DNSSEC
- SSL
- Sandboxing



# Endpoint security: DNS

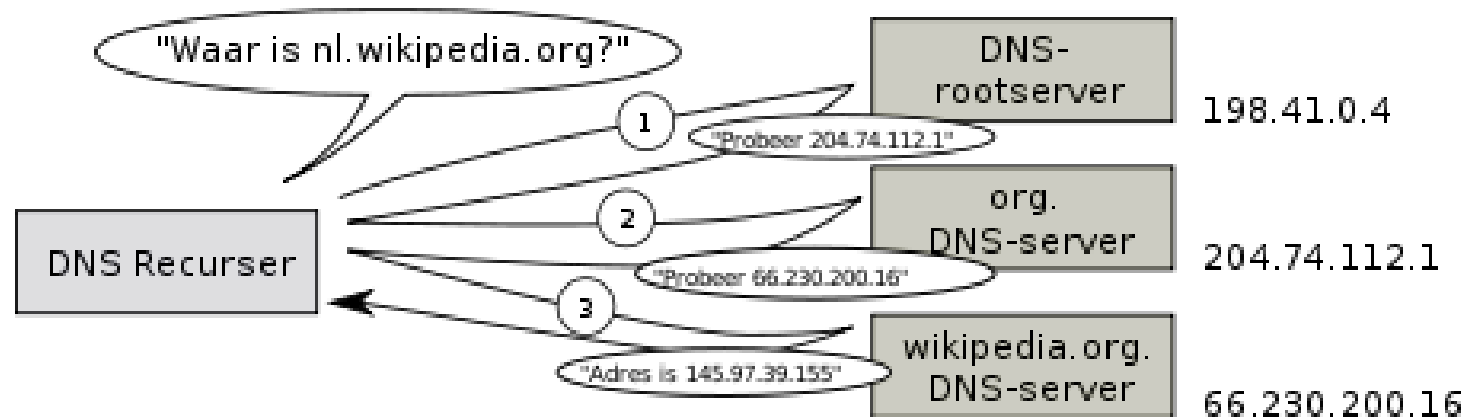
- Hostfile



```
hosts - Notepad
File Edit Format View Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host na
# The IP address and the host name should be separated by at least on
# space.
#
# Additionally, comments (such as these) may be inserted on individua
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com           # source server
#       38.25.63.10       x.acme.com               # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1        localhost
#       ::1              localhost
127.0.0.1 example.com
```

## Endpoint security: DNS

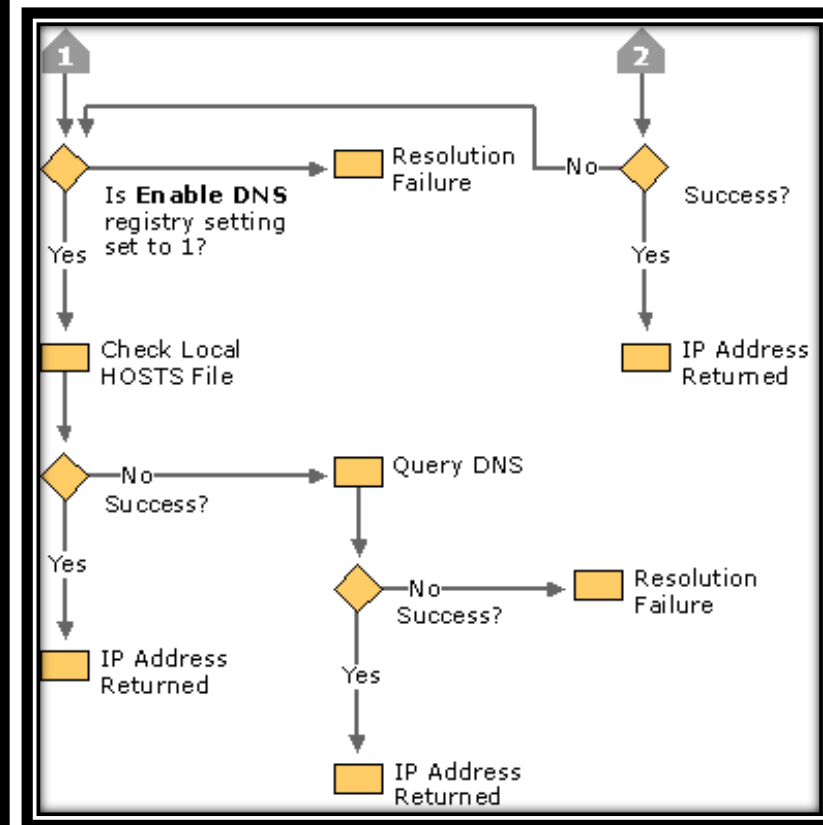
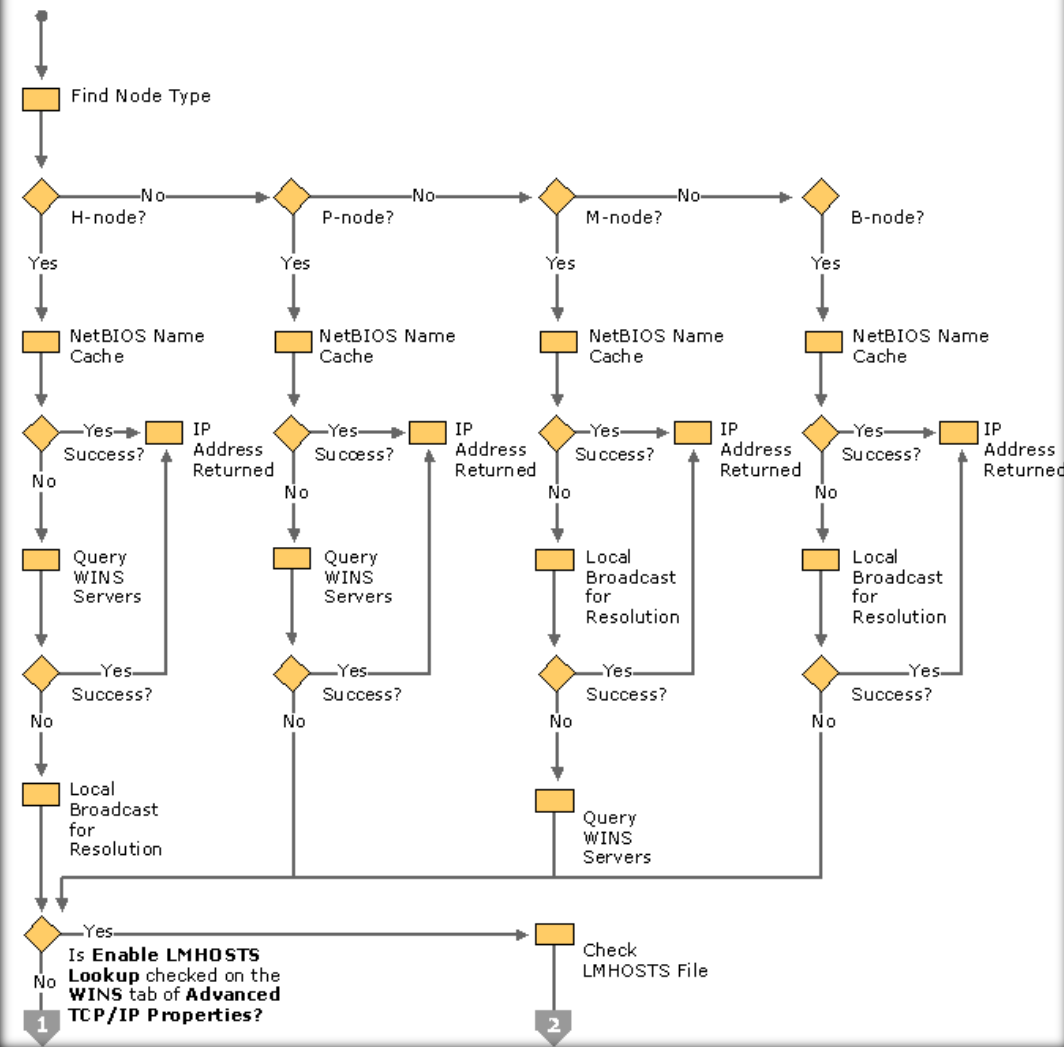
- Wat is dns?
- Hoe werkt dns op jouw pc?





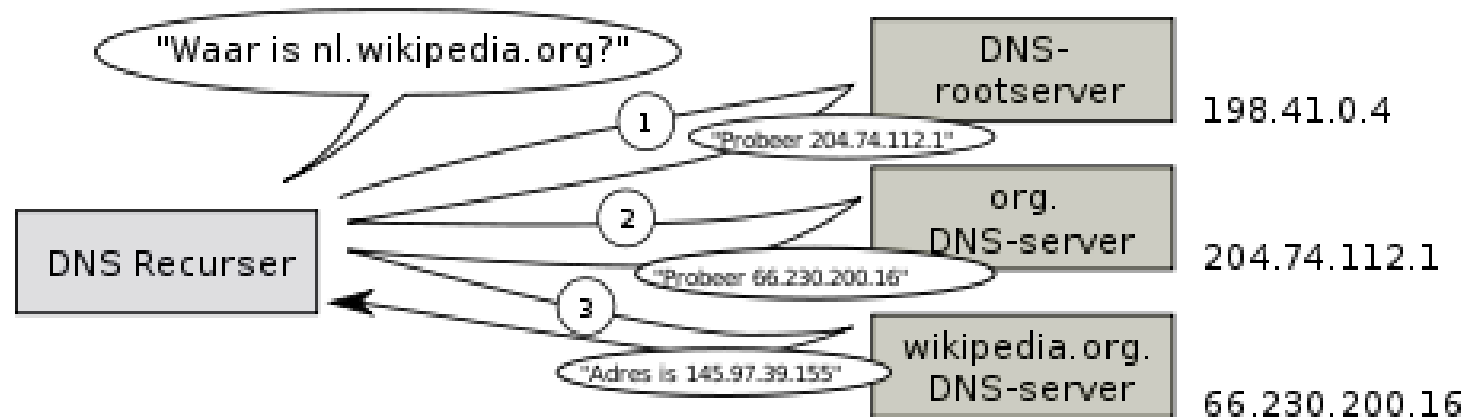
# Voorbeeld, Microsoft implementatie

Start



## Endpoint security: DNS

- Wat is dns?
- Hoe werkt dns op jouw pc?



# Endpoint security: DNSSEC

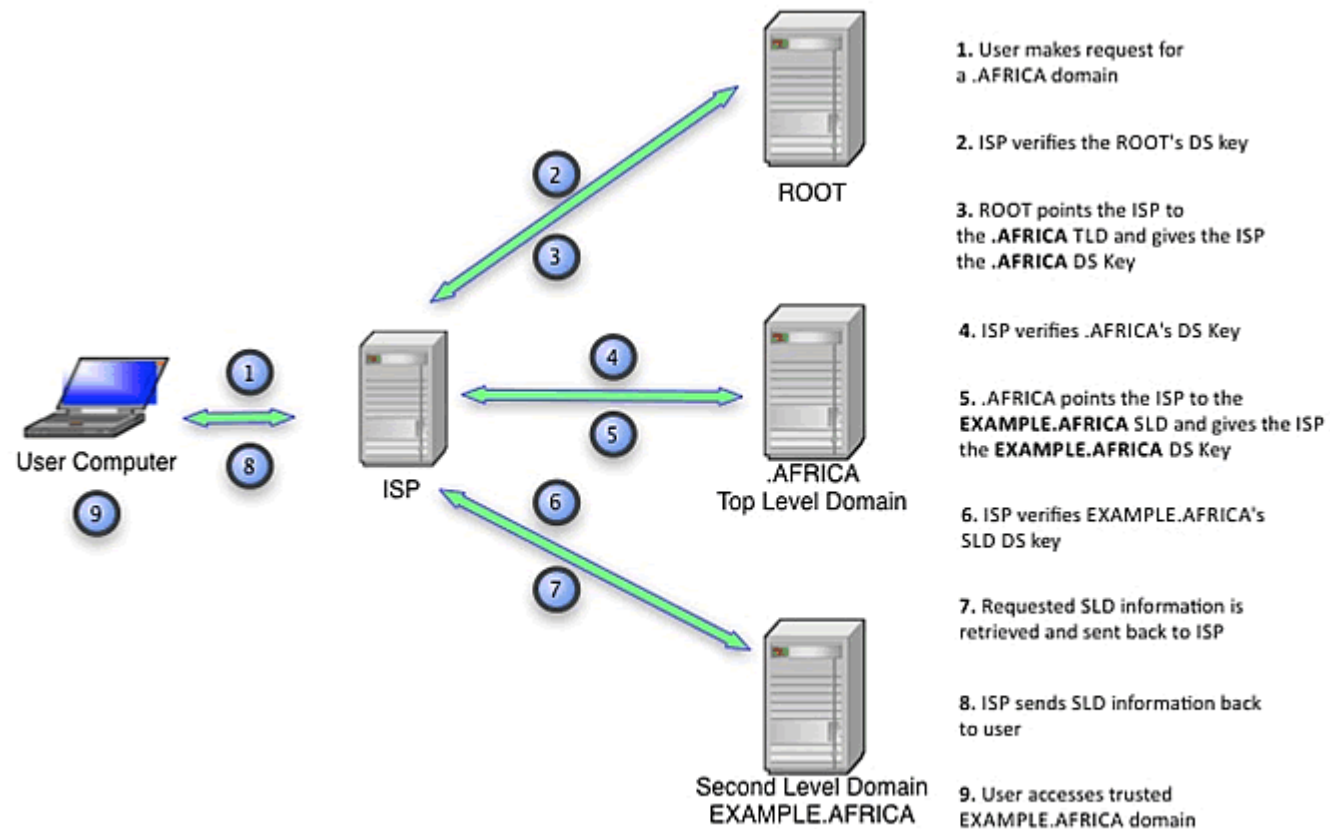


Figure 1: Example of Trust Chain Using DNSSEC

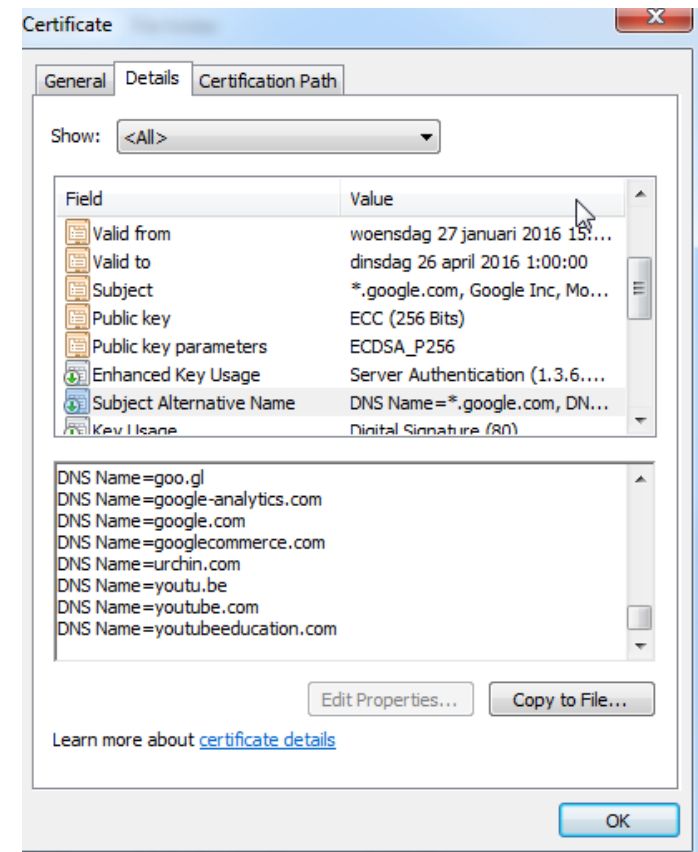
## Endpoint security: SSL

- Transport encryption
- A-Symmetrische encryptie naar symmetrische encryptie
- Niet de one stop shop



# Endpoint security: SSL

- Wat is een certificaat?
- Parameters die je zelf moet controleren!
- Public key
- Revocation list
- En in sommige gevallen een private key (voor installatie op een server)



## Endpoint security: SSL

- Key infrastructure
- Wie vertrouwt jij?
- Diginotar



## Endpoint security: SSL

- Certificate generation
- Random generator en noise
- HSM

```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
              // guaranteed to be random.  
}
```

**DEBIAN**

GUARANTEED ENTROPY.



## Endpoint security: Sandboxing

- Virtual machines
- Virtual networking
- Network segmentation



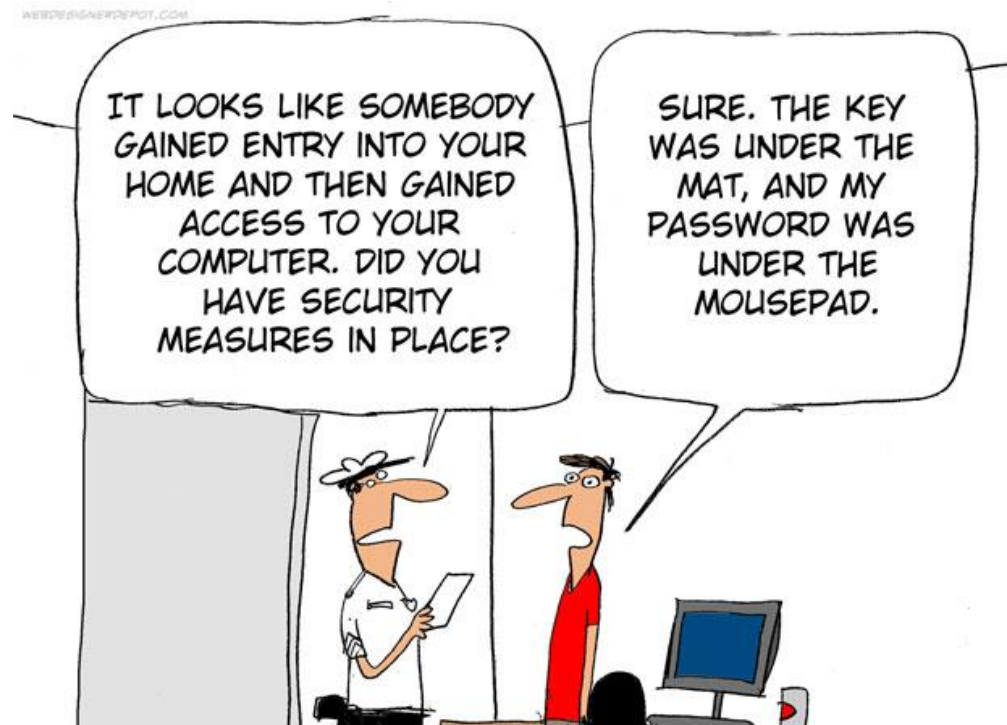
## The security toy chest!

- Network security
- Endpoint security
- Application security
- Data security
- Entity Security



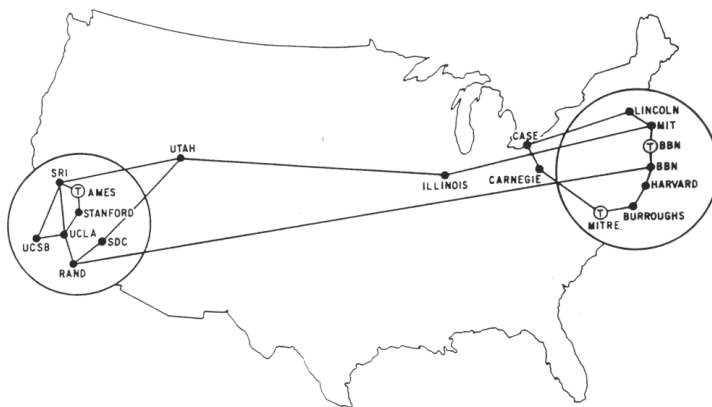
## Application security

- Directory services
- Intrusion detection / prevention systems
- Security Incident Event Management



# Application security: Directory services

- Telefoon nummers
- Eigen protocol en query taal, LDAP
- Novell the world in a directory – Azure AD

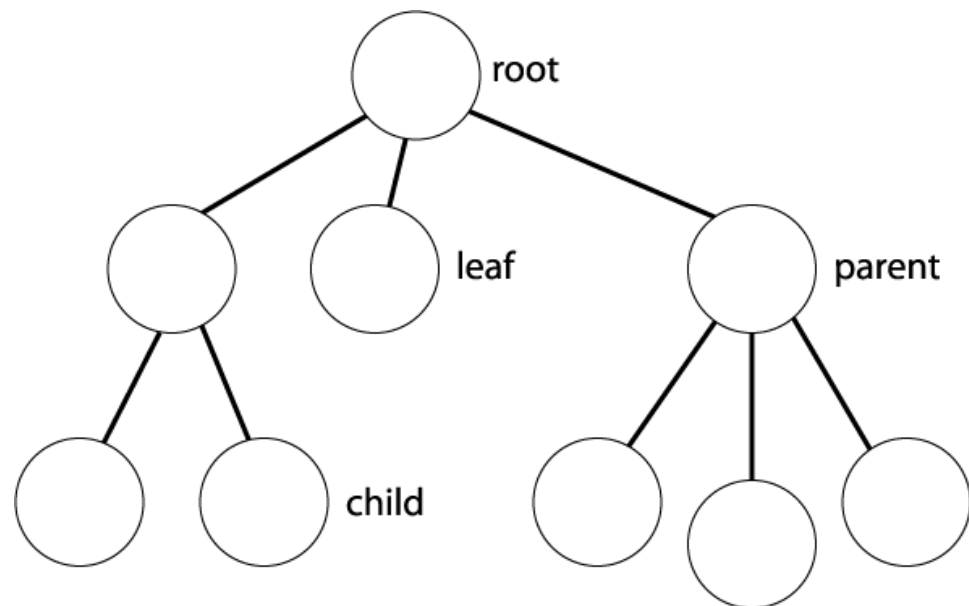


MAP 4 September 1971



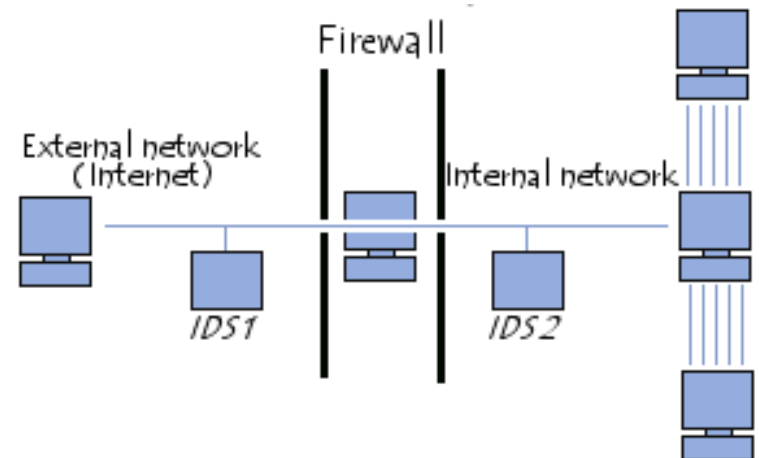
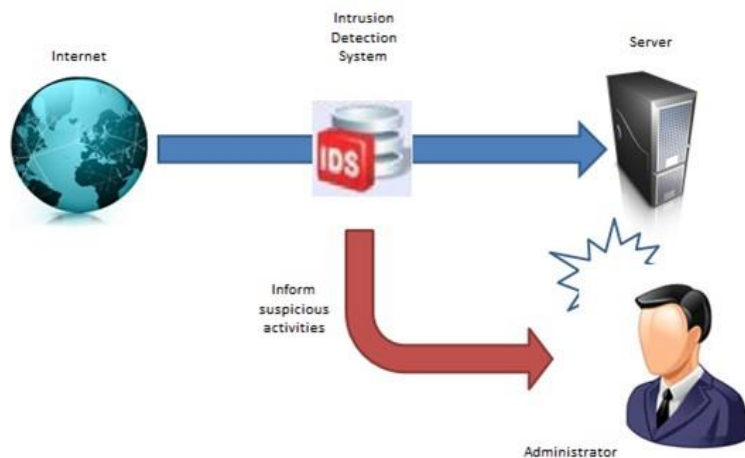
# Application security: Directory services

- Hoe werkt een directory
- Snelle zoekacties
- Vrijwel altijd bedoeld voor login acties / gebruikers gegevens
- Virtual directories





- Wat is een IDS
- Wat is een IPS





## Hoe werkt een IDS / IPS

- In-line IDS: denk reverse proxy
  - Hang hem aan de switch 0 poort
  - Vrij nutteloos als niemand reageert op de meldingen
  - Heeft een babysitter nodig
- 
- IPS: heeft in het begin veel klachten
  - Let op dat je deze niet te slap instelt, ander is ook dit nutteloos



## Voorbeeld: Waf!

- Web Application Firewall

- A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as [cross-site scripting \(XSS\)](#) and [SQL injection](#). By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.
- Moet volledig transparant zijn (Dus onzichtbaar kuch kuch)

### WAFW00F

WAFW00F identifies and fingerprints Web Application Firewall (WAF) products.

#### How does it work?

To do its magic, WAFW00F does the following:

- Sends a *normal* HTTP request and analyses the response; this identifies a number of WAF solutions
- If that is not successful, it sends a number of (potentially malicious) HTTP requests and uses simple logic to deduce which WAF it is
- If that is also not successful, it analyses the responses previously returned and uses another simple algorithm to guess if a WAF or security solution is actively responding to our attacks

For further details, check out the source code on the main site, [github.com/sandrogauci/wafw00f](https://github.com/sandrogauci/wafw00f).

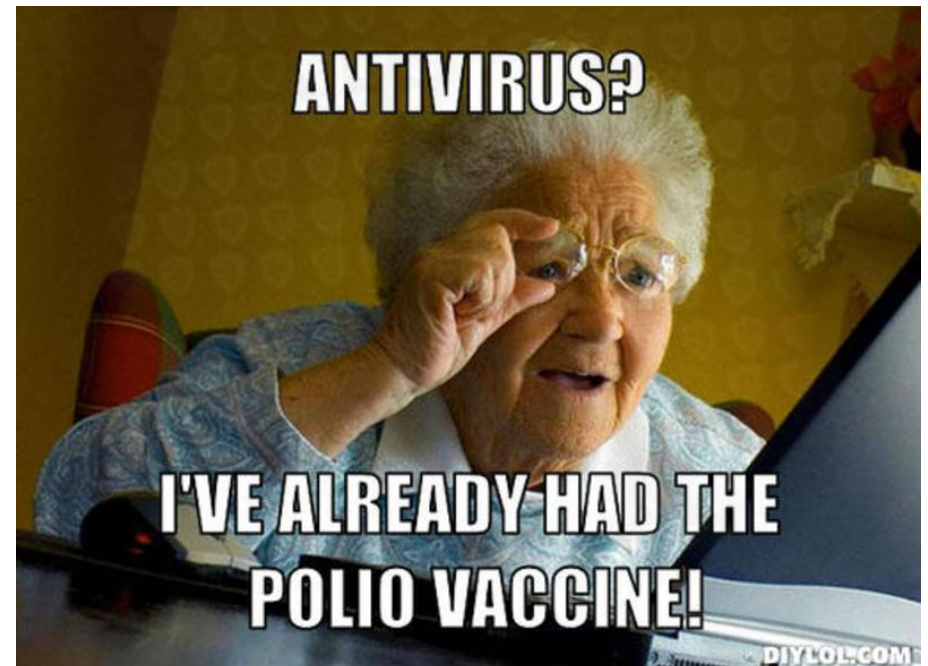
## Application security: Security Incident Event Management

- Wat doe jij met je logs?
- Log aggregation
- Analysis
- Wanneer gebeurde wat
- Nuttig bij meerdere systemen



## The security toy chest!

- Network security
- Endpoint security
- Application security
- Data security
- Entity Security



# Entity Security

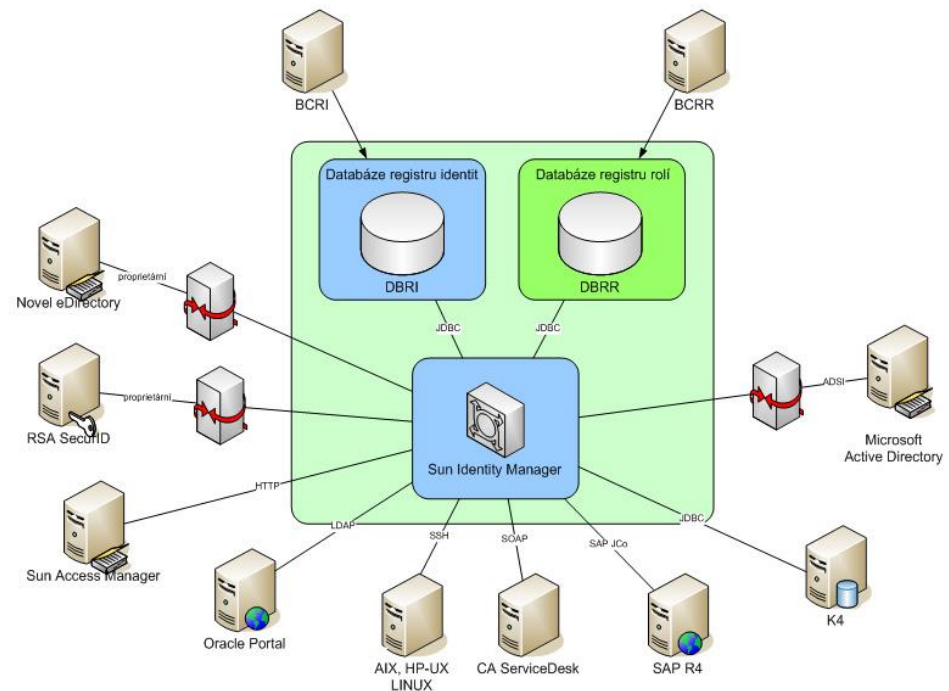
- Identity management
- Certificate management
- Access management





# Entity Security: Identity management

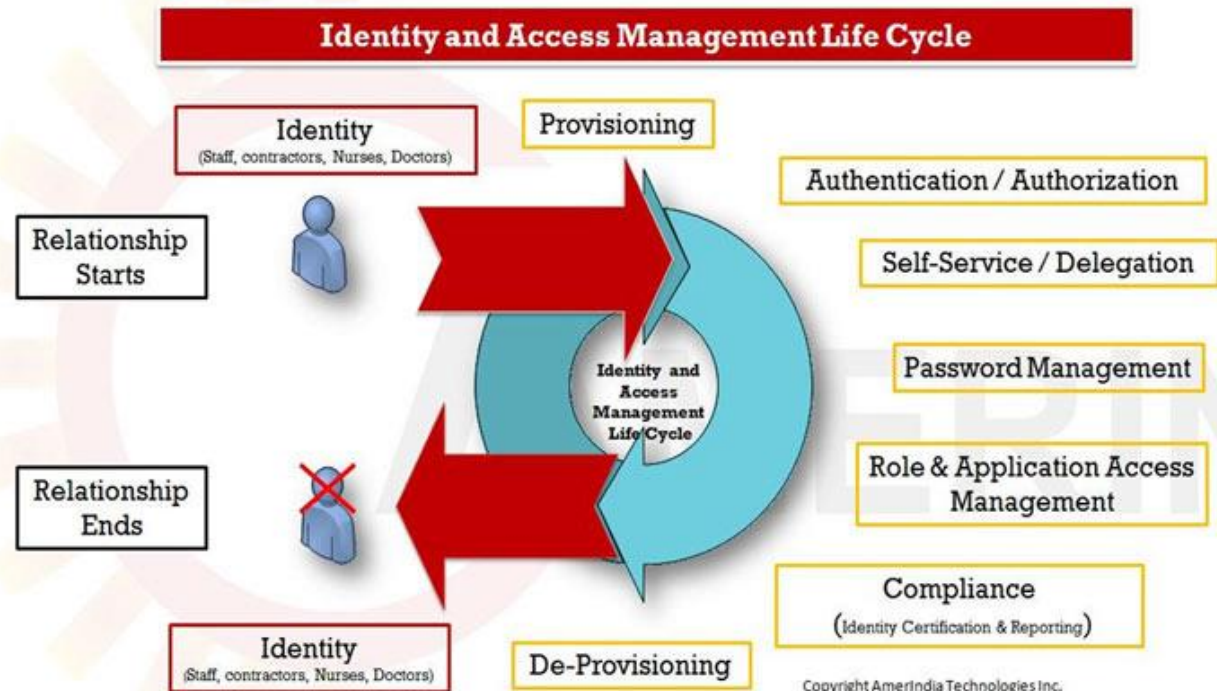
- Wie ben jij?
- Waar heb jij toegang toe?
- Wat moet ik van jou bewaren?
- Waar moet ik jouw spullen bewaren?
- Wat heb jij van mij in bezit?





# Entity Security: Identity management

- Sync engine
- Self service
- Workflows
- Controle slagen
- Identity Lifecycle

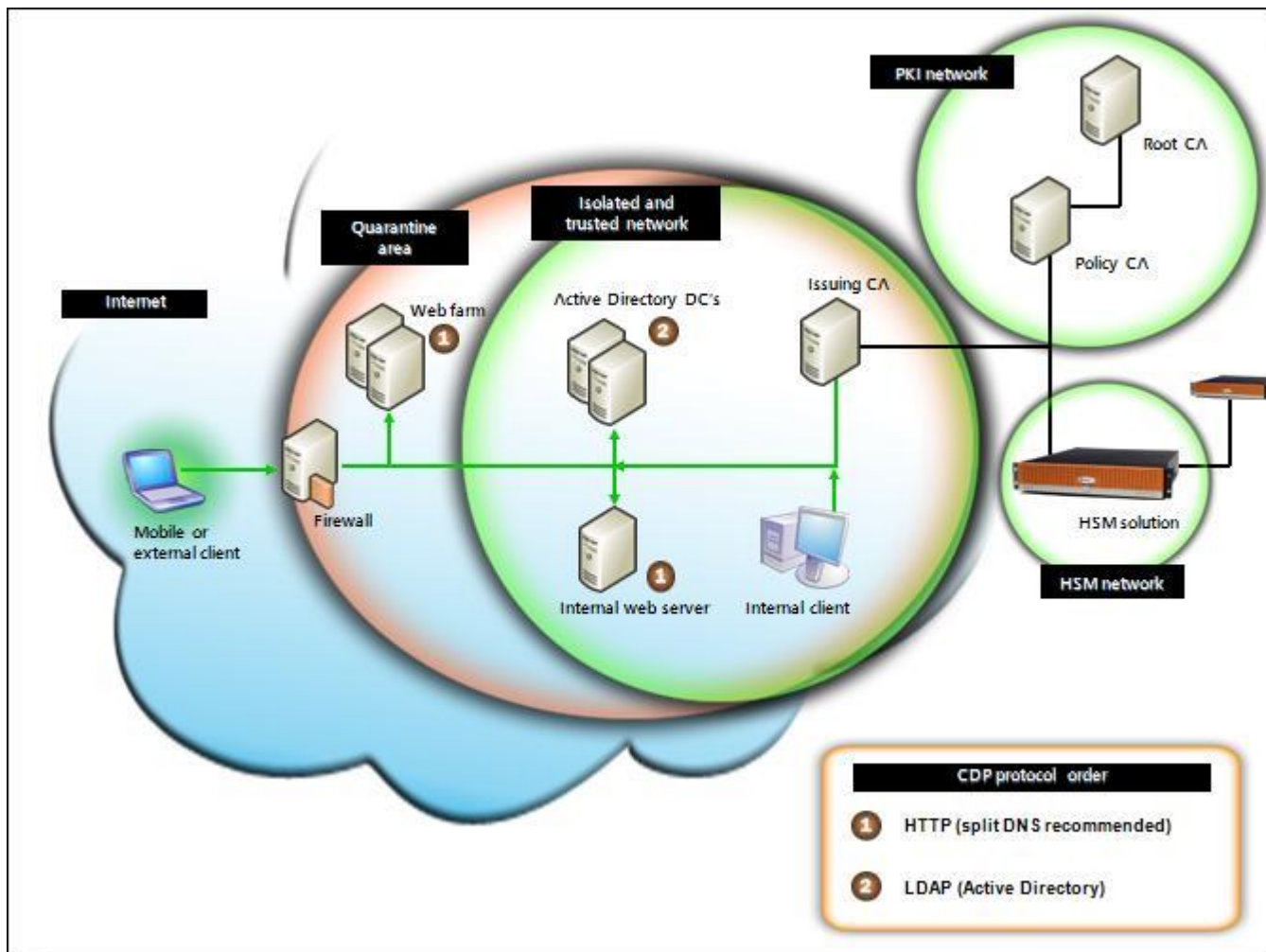


# Entity Security: Certificate management

- Bijhouden van certificaten, smart cards, rsa tokens
- Uitgifte certificaten
- Intrekken van certificaten

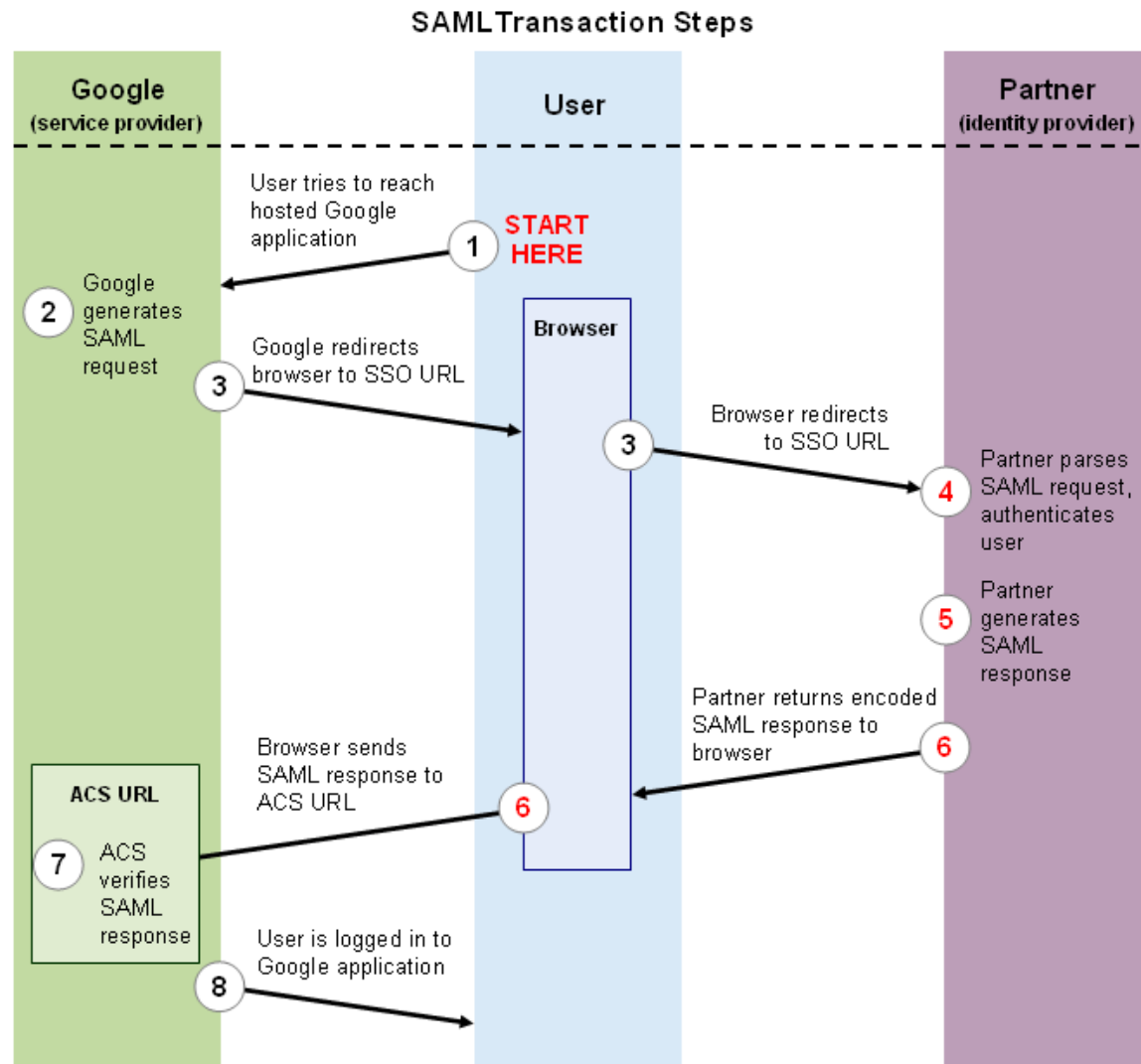


# Voorbeeld ADCS landschap

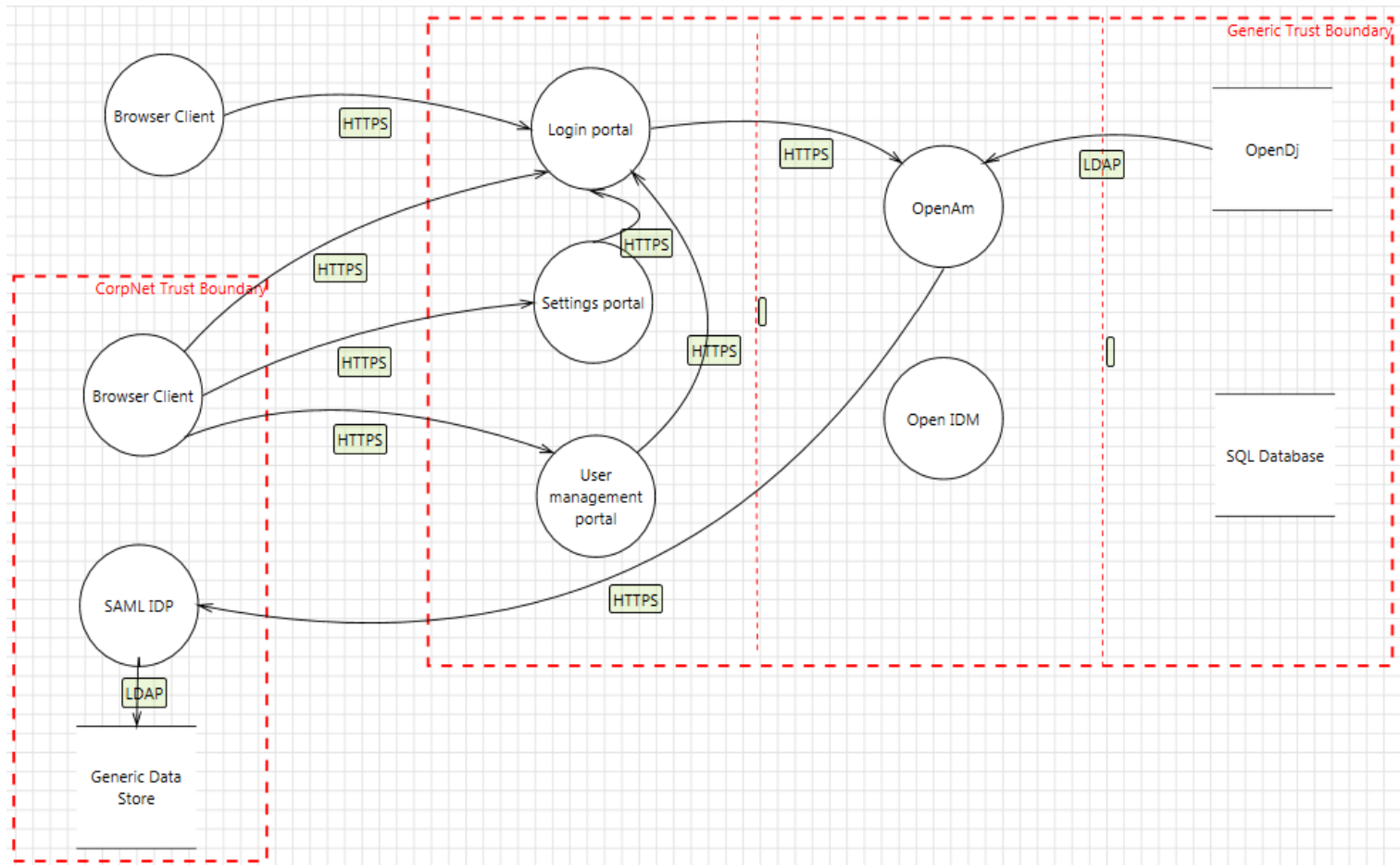


# Entity Security: Access management

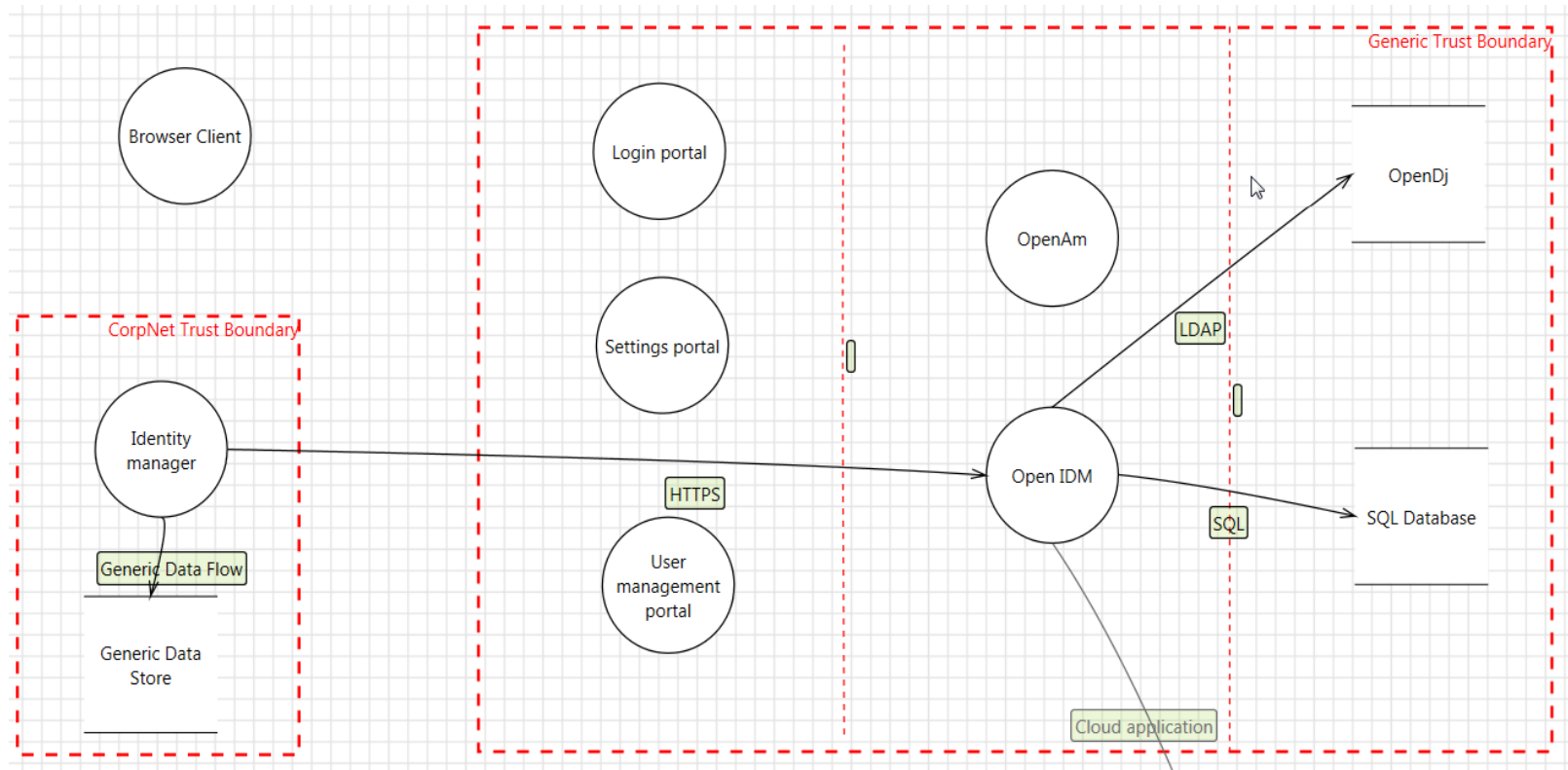
- Wie ben jij
- Hoe kom jij binnen
- Federatie



# Voorbeeld: COSI



# Voorbeeld: COSI





Vragen?



