Remote Access Microdata Infrastructure

Marc Schillings, Infrastructure Advisor ICT

Centraal Bureau voor de Statistiek

Agenda

Basic infrastructure

Security infrastructure

Remote Access Microdata infrastructure

- History
- Infrastructure
- Future / transition

Basic infrastructure : locations

Almere
Primary DC

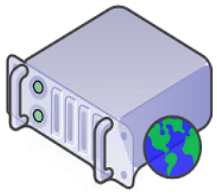
Oude Meer
Backup DC

2 x 1 Gb/s

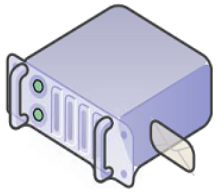
Den Haag
Office location

Heerlen
Office location

Basic Infrastructure: some numbers

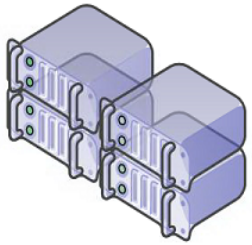


>350.000 hits/month op cbs.nl



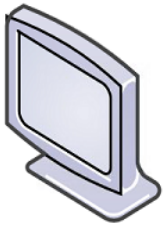
>7 miljoen mails/month

80-90% spam



1200 VMWare virtual servers

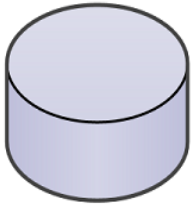
Microsoft standardised



4000 virtual Windows 7

desktops

1800 users

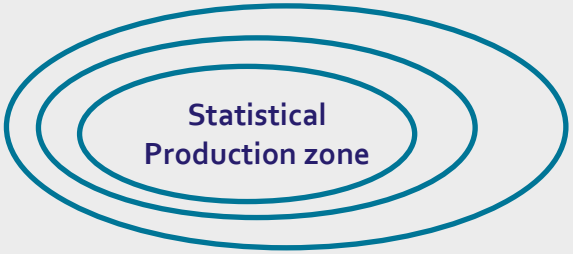


> 1 pByte data

Security principles

Several security zones (rings)

- *No zone hopping allowed*
- *Network segmentation within security zones*
- *Security audits for new internet facing services*

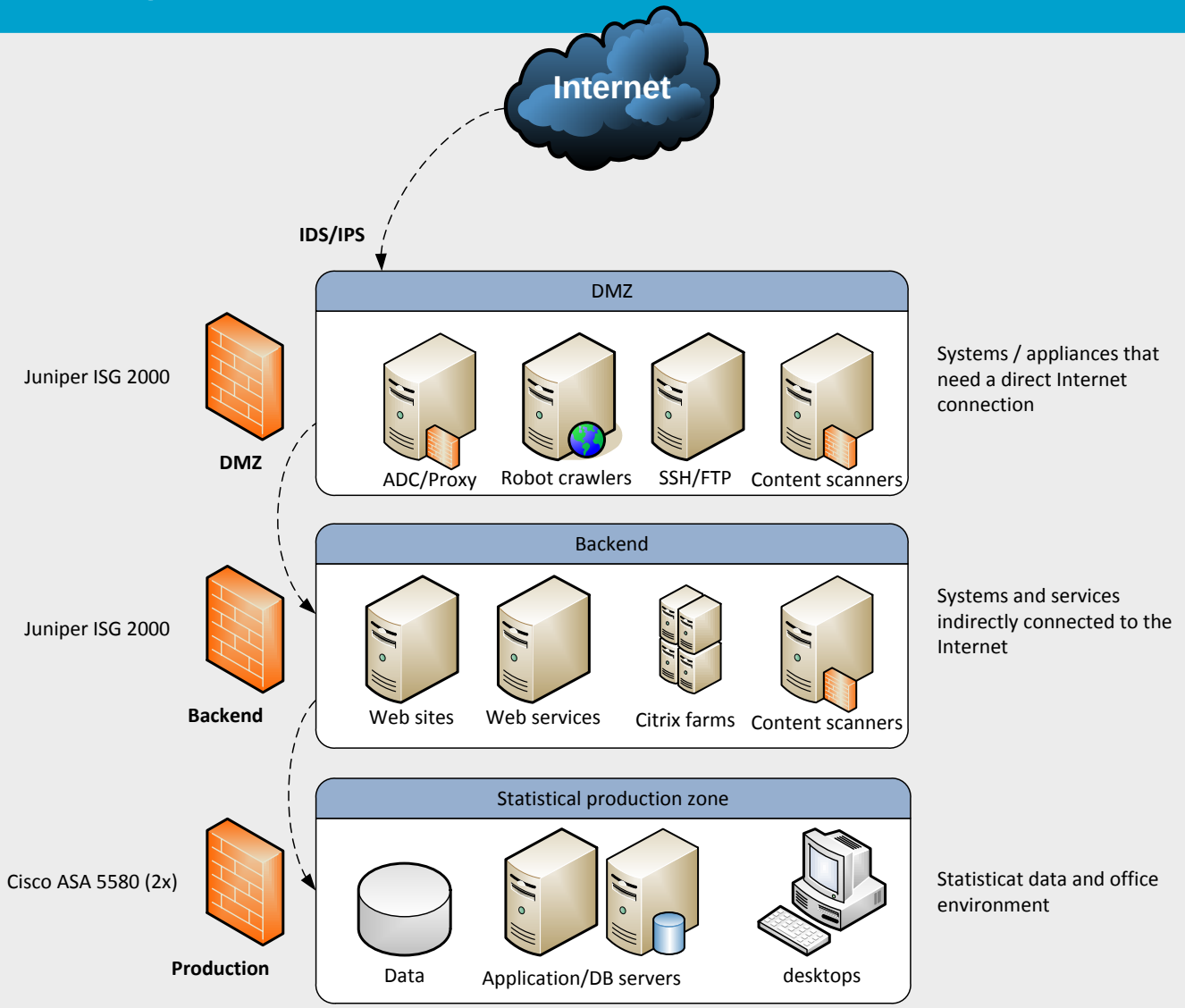


Layered security

- *IDS/IPS*
- *Firewalls*
- *Several layers of content scanning (web-traffic/e-mail)*
- *Endpoint Security on servers and desktops*
- *system hardening, Patch-management, password policy*

Periodic audits / pentests
ISO27001 certified in 2017

Security zones



Security Future challenges

More open infrastructure for the employees
Internet directly from the desktop (is now indirectly via Citrix farm)

More use of cloud services
Connecting data center with private/public cloud

2 factor authentication
initially for administrators

Implementation of a SIEM
Security Information and Event Management system

IDS/IPS for internal LAN

more LAN segmentation

More focus on Endpoint Security

Next Generation Firewalls / DLP

Remote Access Microdata Principles

- ***Confidentiality*** **is crucial**
- **For *statistical* or *scientific* research only**
  not for fiscal, administrative, or legal goals
- **Open to (governmental) research institutes as mentioned by Dutch law or approved by the DG (formally CCS central statistical commission)**
- **Results must be *publicly available***
- **No responsibility of SN for quality of analyses**
- **Pricing policy:**
  data is free, but there's a charge for use of services, for linking datasets and for additional documentation

Remote Access Microdata History

Pre 2005 only On Site and Remote Execution was available

On Site

- *Analyses performed **within** premises of SN.*
- *Only authorized users are able to make use of this facility*
- *On Site workstations disconnected from SN main production facility.*
- *Applications such as SPSS, Stata, StatTransfer, Ox, Gauss, SAS etc.*
- *Intermediate results are sent to the institute, after a disclosure check.*

Remote Execution

- *Send in script by email (based on test set) and receive results by email after disclosure check.*
- *limited in use.*

Remote Access Microdata History

Remote Access v1 2005-2008

- *Access to microdata from institutes using a secure Internet connection.*
- *Based on Citrix Terminal Server technology micro data remains at SN*
- *Authentication via fingerprint scan and smartcard with PKI certificates and username / password (3-way authentication)*

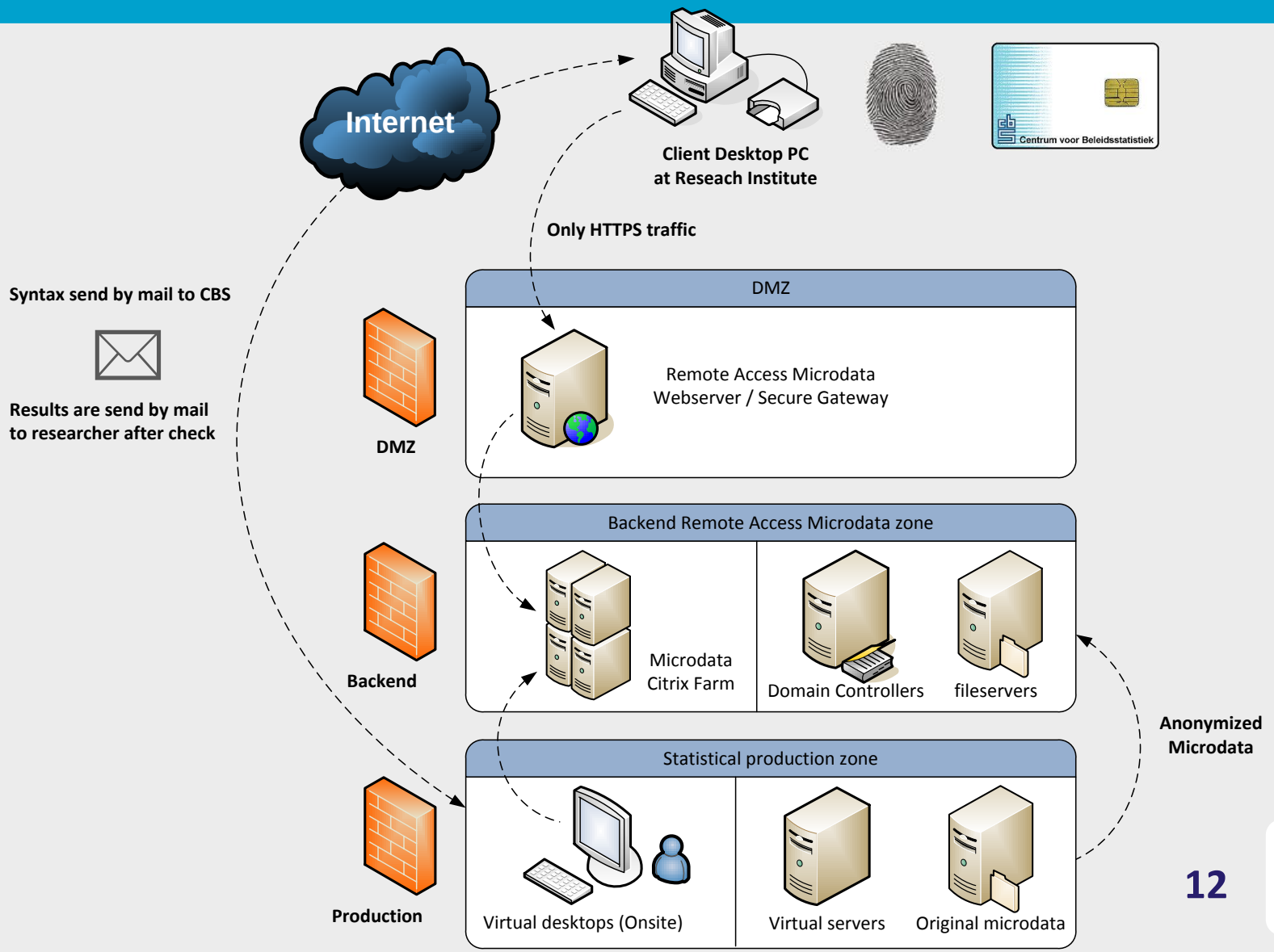
Remote Access v2 SSO 2008-2017

- *Introduced a Single Sign-On solution using two-way authentication (no username / password)*
- *Fingerprints stored centrally in CBS data center*
- *Re-authentication using random intervals (20-30 min)*

Remote Access Microdata Infrastructure

- **All servers are virtualized using VMware ESX 5.5**
- **Dedicated Remote Access Active Directory domain**
  used for access control to applications and micro data
- **Separated from regular statistical production environment**
- **Client workspace is installed by a CBS employee**
  Software and a biometric smart card reader is installed
- **Biometrics solution is custom build using the Webkey SDK from Bio-key**
- **Secure FTP is used for data transport (micro data and user imports/results) between the statistical production environment and the Remote Access environment.**
- **Remote Access farm is build on Citrix XenApp 6.5 and Windows 2008 R2**
  - 28 standard servers (4 CPU / 16 GB)
  - 1 dedicated SAS server (4 CPU / 16 GB)
  - 12 power servers (4 CPU / 64 GB)

Remote Access Microdata Infrastructure

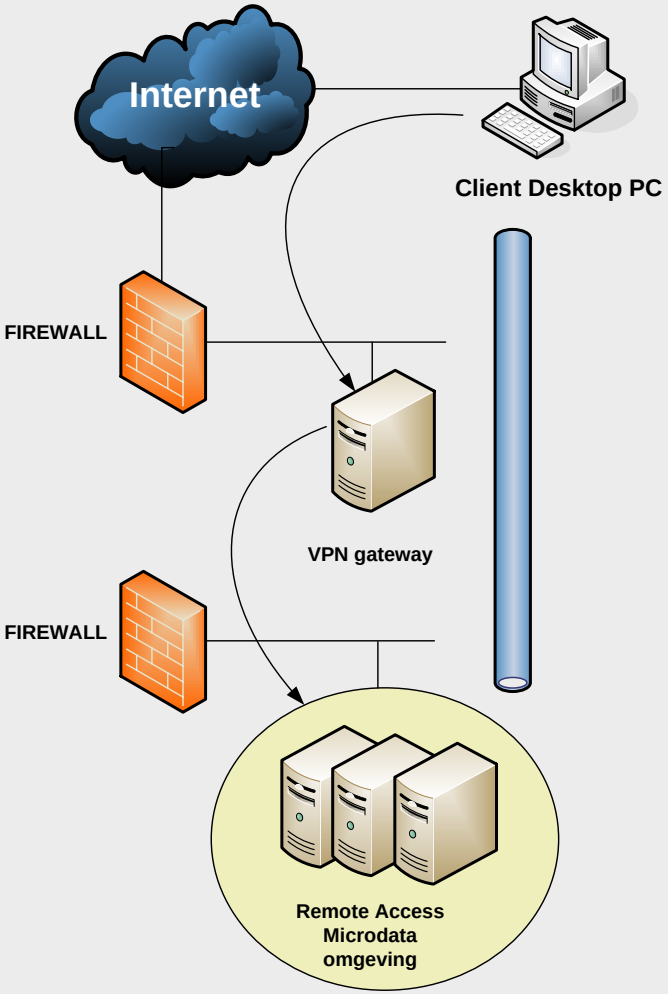


Remote Access Microdata transition

Remote Access 2017 - …

- *CBS Remote Access Microdata environment is only accessible through VPN*
- *VPN uses 2-factor authentication: RSA hardware tokens*
- *For logging into the Microdata environment 2-factor authentication is used: RSA on-demand SMS tokens (smartphone researcher)*
- *No other internet access possible after setting up the VPN*
- *RA client PC does not have to be installed by SN*
- *Less technical requirements for client PC*
  (before it had to be 32-bit Windows + Internet Explorer)
- *No more re-authentication*

Remote Access Microdata transition



Step 1

VPN session

Create VPN session with CBS Microdata site using username and RSA hardware token

Step 2

Internet Browser

Login to the Remote Access Microdata environment using username/password + SMS code

Step 3

Start a Remote Access Microdata session

Questions?

Demonstration