bjørn®

# De ‘comeback’ van lokale netwerken en DMZ

## Overlay networks met IAM-policies

Microsoft Kennisevent Noord-Nederland
Woensdag 28 oktober 2026, Heerenveen

*Er is geen cloud. Alleen andermans computer, andermans netwerk en een SLA.*

**bjørn** regelt het!

**DMZ** demilitarized zone **IAM** Identity and Access Management **SLA** service level agreement



# Het gesloten netwerk komt terug.

Zonder kabel.

- Een overlay in plaats van een DMZ.
- Identiteit beslist wie erdoor mag.
- Oude architectuur. Nieuwe kijk op controls.

*Terwijl salesmensen bij Microsoft twee keer per zin ‘Copilot’ roepen, krijgt een nieuwe kijk op netwerktoegang nauwelijks aandacht.*

**DMZ** demilitarized zone



# Abstracties in IT

Elke trede verbergt de trede eronder. Wij volgen Access.

| Compute | Storage | Access |
|---|---|---|
| | | overlay |
| applicatie | | SDN software |
| framework | S3 (objectopslag) | L7 applicatie |
| compiler | bestandssysteem | L4 transport |
| machinecode | structuur | L3 routering |
| processor | opslag | L2 switch |

**IT** Information Technology **S3** Simple Storage Service
**L2/L3/L4/L7** layer 2, 3, 4 or 7 of the OSI model (Open Systems Interconnection) **SDN** software-defined networking



# Elk antwoord roept een nieuwe vraag op

Telkens als de grens verzwakte, kwam er een laag compensatie bij.



# Het gesloten netwerk

- Risico: meeluisteren op de kabel (sniffing)
- Maatregel: fysieke toegang en vertrouwd personeel
- Deur dicht: netwerk veilig
- ‘Implicit Trust’ model
- ‘Vertrouwd’ is relatief (zie Stuxnet)

*De eerste firewall was een deur.*

**Deur** · Extranet · Zones · Versleuteld · Directory · Op afstand · Federatie · Inzicht · Overlay



# Delen: het extranet

- Probleem: partners hebben jouw gegevens nodig, niet je hele netwerk
- Oplossing: vaste lijn of VPN tussen vertrouwde partijen
- Prijs: je vertrouwt op de beveiliging van je partner
- De reikwijdte is vaak het hele netwerk

*Vertrouwen is transitief: je partner heeft ook partners.*

Deur · **Extranet** · Zones · Versleuteld · Directory · Op afstand · Federatie · Inzicht · Overlay

**VPN** virtual private network



# DMZ en reverse proxy

Onbekenden mogen bij een dienst, niet bij je netwerk.




- Zones met een eigen vertrouwensniveau
- Prijs: de applicatie staat nu op het internet

*Servers die je niet vertrouwt, achter een firewall die je wel vertrouwt.*

Deur · Extranet · **Zones** · Versleuteld · Directory · Op afstand · Federatie · Inzicht · Overlay

**DMZ** demilitarized zone **TLS** Transport Layer Security



# Versleuteld, maar wie staat garant?

- 1995 SSL, 1999 TLS: versleuteling én een servercertificaat
- ‘Is dit echt mijn bank?’ beantwoordt een certificaatautoriteit (CA)
- Nu moet je die autoriteit vertrouwen
- 2011: DigiNotar gehackt. Oktober 2026: eMudhra.

*Het slotje betekent: iemand heeft er ooit voor getekend.*

Deur · Extranet · Zones · **Versleuteld** · Directory · Op afstand · Federatie · Inzicht · Overlay

**SSL** Secure Sockets Layer **TLS** Transport Layer Security **CA** certificate authority

verdieping

# DigiNotar, 2011

- Juli 2011: inbraak bij DigiNotar
- Vals Google-certificaat: naar schatting 300.000 Iraanse gebruikers blootgesteld
- 531 valse certificaten; alle acht CA-servers gecompromitteerd
- 2 september 2011: de Nederlandse overheid trekt het vertrouwen in
- Netwerk in 24 segmenten, maar bestaande firewallregels gaven de aanvaller de weg

*Segmentatie die niet wordt afgedwongen is decoratie.*

**CA** certificate authority



# eMudhra, oktober 2026

- 17 oktober: zwakke privésleutels bij acht tussen-CA's van eMudhra, één sleutel was simpelweg het getal 4
- Chrome, Mozilla en Apple blokkeerden de certificaten binnen uren; eMudhra trok ze in
- Volgens eMudhra gaven deze tussen-CA's geen certificaten uit aan websites of gebruikers
- Software met een eigen trust store (bijvoorbeeld Go, containers, buildpipelines) blijft kwetsbaar tot de update
- 22 oktober: eMudhra stopt met het uitgeven van TLS-certificaten

Bron: Google Security Blog

*Een certificaat is zo sterk als de sleutel van de uitgever.*

**CA** certificate authority **TLS** Transport Layer Security



# Identiteit in huis: directory services

- Eerst: een account per systeem
- Toen: één directory met Kerberos (Active Directory) en single sign-on
- Eén wachtwoord, overal binnen
- Nog steeds 'Implicit Trust'






# De perimeter verdwijnt

- Thuiswerk, partners, BYOD: 'binnen' is overal
- VPN verlengt het netwerk naar de gebruiker
- 2004: het Jericho Forum noemt dit de-perimeterisatie
- Prijs: netwerktoegang voor iedereen die verbonden is
- Microsoft DirectAccess?

*BYOD: Bring Your Own Disaster.*




**BYOD** Bring Your Own Device **VPN** virtual private network

# Cloud en federatie

- SaaS-apps overal, elk met een eigen login
- Federatie: SAML (2005), OAuth2 (2012), OIDC (2014)
- Het token: SAML-assertion (XML) of JWT (JSON)
- Authenticatie (AuthN): wie ben je. Autorisatie (AuthZ): wat mag je, per applicatie
- Prijs: de identity provider is de nieuwe perimeter én het nieuwe SPOF

*Single sign-on, single point of failure.*




**SaaS** software as a service **SAML** Security Assertion Markup Language **OAuth2** Open Authorization
**OIDC** OpenID Connect **XML** Extensible Markup Language **JWT** JSON Web Token **JSON** JavaScript Object Notation
**AuthN** authentication **AuthZ** authorization **SPOF** single point of failure



# Authenticatie en autorisatie

**Authenticatie**

Wie ben je?

Federatie maakt dit overdraagbaar: SAML, OIDC.

**Autorisatie (AuthZ)**

Wat mag je?

Blijft per applicatie: RBAC, ABAC, ACL.

- Toegangscontrole is niet centraal: elke applicatie beslist zelf
- OAuth2 gaat over autorisatie: gedelegeerde toegang
- OIDC voegt identiteit toe bovenop OAuth2; het ID-token is een JWT

*Een geldig token is geen vrijbrief.*

**SAML** Security Assertion Markup Language **OIDC** OpenID Connect **AuthZ** authorization **RBAC** role-based access control
**ABAC** attribute-based access control **ACL** access control list **OAuth2** Open Authorization **ID** identity
**JWT** JSON Web Token



# Versleuteld en verspreid: inzicht kwijt

- TLS overal: sensoren in het netwerk zien niets meer
- Wildgroei van clouddiensten: wie gebruikt wat?
- Inspecterende proxies (zoals Zscaler) openen TLS onderweg
- CASB (2012): beleid en inzicht tussen gebruiker en SaaS
- TLS 1.3 (2018): passief meekijken stopt

*Eerst versleutelen we alles, dan kopen we iets om te kunnen kijken.*




**TLS** Transport Layer Security **CASB** cloud access security broker **SaaS** software as a service



# TLS 1.3 en inspectie

- Elke sessie krijgt nieuwe sleutels (forward secrecy)
- TLS 1.3 (RFC 8446, augustus 2018) verplicht dit
- Een opgenomen sessie ontsleutelen met de serversleutel kan niet meer
- Traditionele IDS-sensoren kunnen passief niet meer meelezen
- Inspectie verhuist naar eindpunt, proxy of broker

*Privacy voor iedereen. Ook voor de aanvaller.*

**TLS** Transport Layer Security **RFC** Request for Comments **IDS** intrusion detection system / intrusion prevention system

# De lappendeken

| Firewall | VPN | IdP | CASB | Proxies |
|---|---|---|---|---|
| eigen beleid | eigen beleid | eigen beleid | eigen beleid | eigen beleid |

- Elke stap loste iets op en haalde iets weg.

*Vijf consoles, vijf beleidsregels, nul overzicht.*

Deur — Extranet — Zones — Versleuteld — Directory — Op afstand — Federatie — **Inzicht** — Overlay

**VPN** virtual private network **IdP** identity provider **CASB** cloud access security broker



# Pauze

15 minuten

*Warme reboot.*



# Eén beleidsvlak

IAM-policies als nieuwe perimeter.

**overlay: de zone als software**

**gebruiker** en apparaat —versleuteld→ **beleid** wie, wat, welke app, welke toestand —versleuteld→ **applicatie** in elke omgeving

- Overlay: de zone als software, bereikbaar vanaf elke locatie
- Conditional Access op basis van identiteit en signalen

*Alles komt terug. Behalve de kabelbomen.*

Deur — Extranet — Zones — Versleuteld — Directory — Op afstand — Federatie — Inzicht — **Overlay**

**IAM** Identity and Access Management



# Waar wordt het beleid afgedwongen?

Elke oplossing heeft een centrale broker. Twee dingen verschillen.

| afhankelijkheid van de leverancier | **Bij de apparaten** L2 of L3, direct waar het kan | **In het pad: edge of broker** Per applicatie, alle verkeer via de edge |
|---|---|---|
| **Hoog** leverancier draait het | Tailscale | Entra Global Secure Access, Cloudflare Access, Zscaler |
| **Middel** dienst of zelf hosten | ZeroTier, NetBird, Nebula | Pangolin |
| **Laag** zelf gehost | Headscale | |

- Mesh: direct via STUN waar het kan, relay (TURN) als terugval. Edge: altijd via de broker

*Kies waar je afdwingt, kies wie je vertrouwt.*

**L2/L3** layer 2, 3, 4 or 7 of the OSI model (Open Systems Interconnection) **STUN** Session Traversal Utilities for NAT
**TURN** Traversal Using Relays around NAT

# Zo werkt het, ongeacht het merk

1 Aanmelden: gebruiker en/of apparaat worden geïdentificeerd

2 Beleid: wie mag naar welke applicatie, onder welke voorwaarden

3 Pad: direct, via een relay of via een broker

4 Log en toets: dashboard en werkelijkheid naast elkaar

*Authentication, Authorization, Accounting.*



# Entra Global Secure Access

In vogelvlucht, op principeniveau.

- Twee onderdelen: Private Access (ZTNA voor apps on-premises of in je eigen cloud) en Internet Access (SWG voor web)
- Client op het apparaat; connector bij de on-premises applicaties
- Drie verkeersprofielen: Microsoft 365, private en internet
- Beleid per applicatie; Conditional Access als beleidsmotor
- 'L7' is hier beleid per applicatie, niet per se protocolinspectie

Microsoft Learn: Global Secure Access

**ZTNA** Zero Trust Network Access **SWG** secure web gateway
**L7** layer 2, 3, 4 or 7 of the OSI model (Open Systems Interconnection)



# Voorbeelden

**Via een leverancier**

- Entra Global Secure Access
- Cloudflare One
- Zscaler
- Netskope
- Palo Alto Prisma Access
- Cisco Secure Access
- Tailscale

**Zelf te hosten**

- ZeroTier
- NetBird
- Headscale
- Nebula
- Pangolin
- OpenZiti

**Europees of EU-gehost***

- Jimber (België)
- Systancia (Frankrijk)
- Open Systems (Zwitserland)
- Zscaler op STACKIT

*Land volgens eigen opgave van de leverancier; vermelding is geen aanbeveling. Peildatum oktober 2026.

*Zelf hosten kan alleen als je kunt zwemmen.*

**EU** European Union



# IPsec in transportmodus

De standaardroute. In IPv6 is IPsec 'aanbevolen', niet verplicht (RFC 8504, 2019).

| | IPsec transportmodus | Overlay |
|---|---|---|
| **Standaard** | Open internetstandaarden (RFC's) | Meestal productspecifiek |
| **Authenticatie** | Wederzijds, via Kerberos of certificaten | Via je identity provider |
| **Inzicht** | Kop zichtbaar, inhoud en poorten versleuteld | Alles in de tunnel versleuteld |
| **Beheer** | Beleid aan beide kanten, domein of certificaten nodig | Centraal in controller of broker |
| **Doorgang** | Kan geblokkeerd worden, NAT vraagt een omweg | Relay en uitgaande tunnels ingebouwd |

*IPsec kan alles. En dat is precies het probleem, sinds 1995.*

**IPsec** Internet Protocol Security **IPv6** Internet Protocol version 6 **RFC** Request for Comments
**NAT** network address translation

# Windows: Server and Domain Isolation

- Windows-firewall met ‘connection security rules’ gebruikt IPsec
- Transportmodus: end-to-end tussen twee machines
- Authenticatie via Kerberos of certificaat; beheer via Group Policy
- ‘Boundary zone’ voor machines die nog niet mee kunnen
- Documentatie uit de Windows Server 2008-tijd: controleer de actuele versie

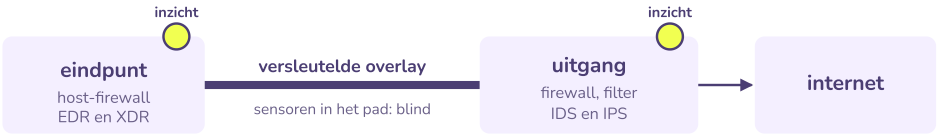
*Het idee is oud. Het beheer was het probleem.*

**IPsec** Internet Protocol Security



# De lagere lagen blijven nodig

- Segmentatie binnen de bubbel: een platte overlay is weer een plat LAN
- Filteren en firewallen: op het eindpunt en bij de uitgang
- Inspectie en monitoring (IDS en IPS) verhuizen naar eindpunt, uitgang en broker
- Loggen van identiteit en verkeersstromen




*Een overlay is geen reden om je firewall met pensioen te sturen.*

**LAN** local area network **IDS/IPS** intrusion detection system / intrusion prevention system
**EDR** endpoint detection and response **XDR** extended detection and response



# ISO en IEC: de maatregelen

**ISO/IEC 27002:2022**

- 8.20 Netwerkbeveiliging
- 8.21 Beveiliging van netwerkdiensten
- 8.22 Netwerksegregatie
- 8.23 Webfiltering
- 8.15 Logging
- 8.16 Monitoring (nieuw in 2022)

**Daarnaast**

- IEC 62443: gecontroleerde paden tussen zones hebben firewalls, authenticatie, versleuteling en logging
- NIS2 art. 21: netwerkbeveiliging is een verplicht onderdeel

*Het stond er al. Nu nog doen.*

**ISO** International Organization for Standardization **IEC** International Electrotechnical Commission
**NIS2** Network and Information Security Directive 2



# Wat komt terug, wat niet

**Komt terug**

- Het ontwerpbeeld: duidelijke zones
- Inzicht in wie bij wat kan
- Beleid op één plek

**Komt niet vanzelf terug**

- Controle over wat applicaties doen
- Hygiëne: patchen, inventaris, minste rechten
- Veilige integraties en toeleveringsketen

*Een goede grens geeft duidelijkheid, geen veiligheid.*

# Masker of bindmiddel?

**Gebroken organisatie**
- ZTNA verbergt het probleem
- Groen dashboard, rommel eronder

**Zorgvuldige organisatie**
- Eén regelset bindt een bekende goede staat
- Minder beheerlast

- Volgorde: assets, identiteit, wijzigingsbeheer, dan de overlay

*Een groen vinkje is geen controle.*

**ZTNA** Zero Trust Network Access



# De poort is dicht, de app niet

- OWASP Top 10:2025, nr. 1: A01 Broken Access Control
- In alle geteste applicaties kwam het voor
- A02 Security Misconfiguration: gestegen naar nr. 2
- A03 Software Supply Chain Failures: nr. 3
- Proxy en WAF helpen, maar zijn geen toegangscontrole op applicatieniveau

*De poort is dicht. En de aanvaller heeft een geldig token…*

**OWASP** Open Worldwide Application Security Project **A01/A02/A03** category in the OWASP Top 10
**WAF** web application firewall



# A01 uitgelegd

- Toegangscontrole werkt alleen in server-side code die de aanvaller niet kan aanpassen
- Standaard weigeren; één keer bouwen en overal hergebruiken
- BOLA: andermans object benaderen door een verwijzing te wijzigen
- BFLA: een functie gebruiken waar je geen recht op hebt
- SSRF zit sinds 2025 in A01: de server haalt een door de aanvaller gekozen adres op

OWASP: A01 Broken Access Control

*Controleer rechten per object, niet per scherm.*

**A01** category in the OWASP Top 10 **BOLA** Broken Object Level Authorization **BFLA** Broken Function Level Authorization
**SSRF** Server-Side Request Forgery **OWASP** Open Worldwide Application Security Project



# Afhankelijkheden en integraties

- Integraties lopen buiten je grens: OAuth2-tokens tussen SaaS-apps
- Een gestolen token is een geldige identiteit (OIDC) of autorisatie (OAuth2)
- Centrale identiteit en centrale perimeter: één storing raakt iedereen
- Noodtoegang (Break Glass Account) buiten je identity provider hoort in je ontwerp

*Het is nooit de configuratiewijziging. Het was de configuratiewijziging.*

**OAuth2** Open Authorization **SaaS** software as a service **OIDC** OpenID Connect

# Salesloft Drift, augustus 2025

- Aanvallers stalen OAuth2-tokens van een AI-chatintegratie (Drift)
- Toegang tot Salesforce-omgevingen van meer dan 700 organisaties
- Ook Zscaler, Cloudflare en Palo Alto Networks bevestigden blootstelling van klantgegevens
- Zij melden dat hun producten niet geraakt zijn
- Geen netwerk, geen VPN, geen overlay in beeld: wel een geldig token

Onderzoek: Google Threat Intelligence Group

*De grens hield stand. De integratie niet.*

**OAuth2** Open Authorization **AI** artificial intelligence **VPN** virtual private network



# Azure Front Door, 29 oktober 2025

- Configuratiewijziging bij Azure Front Door, het wereldwijde randnetwerk van Microsoft
- Ruim 8 uur verstoring (ongeveer 15:45 tot 00:05 UTC)
- Inloggen via Entra en Microsoft 365 raakte verstoord
- Centrale rand en centrale identiteit zijn samen één afhankelijkheid

*Eén vinkje, wereldwijd.*

**UTC** Coordinated Universal Time



# Kaders: ISO, EU en Nederland

| Kader | Waarom relevant |
|---|---|
| **ISO/IEC 27001 en 27002 (2022)** | Netwerken 8.20 tot 8.23, toegang 5.15 tot 5.18, clouddiensten 5.23 |
| **IEC 62443** | Zones en gecontroleerde paden als ontwerpmodel |
| **NIS2 (EU)** | Netwerkbeveiliging, toegangsbeheer, toeleveringsketen, MFA |
| **Cyberbeveiligingswet** | In werking sinds 15 augustus 2026 (Cbw) |
| **NCSC** | Factsheet ‘Bereid u voor op Zero Trust’ (2021, herziening aangekondigd) |

*Het mooie aan standaarden: er zijn er zoveel.*

**ISO** International Organization for Standardization **EU** European Union **IEC** International Electrotechnical Commission
**NIS2** Network and Information Security Directive 2 **MFA** multi-factor authentication **Cbw** Cyberbeveiligingswet
**NCSC** Nationaal Cyber Security Centrum



# NIS2, artikel 21: tien maatregelen

- Risicoanalyse en beveiligingsbeleid
- Incidentafhandeling
- Bedrijfscontinuïteit en crisisbeheer
- Beveiliging van de toeleveringsketen
- Beveiliging bij aanschaf, ontwikkeling en onderhoud
- Beoordeling van de effectiviteit van maatregelen
- Cyberhygiëne en training
- Cryptografie en versleuteling
- Personeel, toegangsbeheer en assetbeheer
- MFA of continue authenticatie, beveiligde communicatie

*Tien maatregelen, nul excuses.*

**NIS2** Network and Information Security Directive 2 **MFA** multi-factor authentication

# Soevereiniteit is een keten

- Drie vragen: waar staat het, wie beheert het, welk recht geldt?
- EU Cloud Sovereignty Framework (oktober 2025): acht doelstellingen, niveaus 0 tot 4
- Per doelstelling een minimumniveau: schiet er één tekort, dan valt de aanbieding af
- Datalocatie is maar één factor in één van de acht doelstellingen
- Persoonsgegevens naar de Verenigde Staten: Data Privacy Framework, hoger beroep loopt

*De zwakste schakel zit meestal in het contract.*



# Acht doelstellingen, vijf niveaus

**Sovereignty Objectives**

- Strategic
- Legal & Jurisdictional
- Data & AI
- Operational
- Supply Chain
- Technology
- Security & Compliance
- Environmental Sustainability

**SEAL**

- SEAL-0: No Sovereignty
- SEAL-1: Jurisdictional Sovereignty
- SEAL-2: Data Sovereignty
- SEAL-3: Digital Resilience
- SEAL-4: Full Digital Sovereignty

Cloud Sovereignty Framework v1.2.1 (PDF)

*Eén zwakke doelstelling en je zakt door het minimum.*



# Data Privacy Framework in één minuut

- Wat: een besluit van de Europese Commissie (2023): persoonsgegevens mogen naar gecertificeerde Amerikaanse bedrijven
- Eerdere regelingen sneuvelden bij het Hof van Justitie: Safe Harbor (2015) en Privacy Shield (2020)
- 3 september 2025: het Gerecht van de EU hield het framework in stand (Latombe)
- Hoger beroep loopt (C-703/25 P); een uitspraak is niet te voorspellen
- Relevant voor brokers van Amerikaanse leveranciers: IP-adressen kunnen persoonsgegevens zijn

*Een veilige haven met een houdbaarheidsdatum.*



# Het gesloten netwerk komt terug, zonder kabel.

- De overlay is je nieuwe intranet
- Identiteit is de nieuwe perimeter
- Het netwerk blijft het netwerk: baselines blijven

*Maar: implicit trust wordt zero trust!*

# Vragen?

**bjørn** regelt het!



## Bronnen


- ISO/IEC 27001:2022 en 27002:2022
- IEC 62443: zones en conduits
- Richtlijn (EU) 2022/2555 (NIS2)
- Cyberbeveiligingswet
- NCSC: Prepare for Zero Trust, 2021
- OWASP Top 10:2025
- EU Cloud Sovereignty Framework v1.2.1
- Microsoft Learn: Global Secure Access
- RFC 2246, 8446 (TLS), 4120 (Kerberos), 6749 (OAuth2), 7519 (JWT), 8504 (IPv6), 2401 (IPsec)
- SAML 2.0 (OASIS), OpenID Connect Core 1.0
- Fox-IT: DigiNotar-rapport
- Google Security Blog: eMudhra
- Google Threat Intelligence Group: Salesloft Drift
- Azure Front Door incident
- Lettertype Nunito: © 2014 The Nunito Project Authors, SIL Open Font License 1.1


**ISO** International Organization for Standardization **IEC** International Electrotechnical Commission **EU** European Union
**NIS2** Network and Information Security Directive 2 **NCSC** Nationaal Cyber Security Centrum
**OWASP** Open Worldwide Application Security Project **RFC** Request for Comments **TLS** Transport Layer Security
**OAuth2** Open Authorization **JWT** JSON Web Token **IPv6** Internet Protocol version 6 **IPsec** Internet Protocol Security
**SAML** Security Assertion Markup Language **OASIS** Organization for the Advancement of Structured Information Standards
**SIL** SIL International