GIDS

De complete gids voor Zero Trust Network Access

VPN vervangen, veilige toegang, kosten, NIS2 en implementatie. Met actuele marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

VPN's zijn verouderd, hybride werk is de standaard en NIS2 noemt zero trust expliciet. De feiten.

63%
van organisaties wereldwijd heeft een (gedeeltelijke) zero trust-strategie geimplementeerd
Gartner 2024 [1]

70%+
van nieuwe remote access deployments verloopt via ZTNA in plaats van VPN (was <10% in 2021)
Gartner 2025 [2]

289%
ROI over 3 jaar bij implementatie van ZTNA ter vervanging van VPN
Forrester/Zscaler TEI [3]

80%
reductie in remote access support tickets bij overgang van VPN naar ZTNA
Appgate [4]

76%
van Nederlandse bedrijven (10--50 pers.) heeft MFA -- verdubbeld sinds 2017
CBS Cybersecuritymonitor 2024 [5]

USD 1,3B
ZTNA-marktomvang 2025 -- groeit naar USD 4,2B in 2030 (CAGR 25,5%)
MarketsandMarkets [6]

65%
van enterprises plant VPN te vervangen door ZTNA
Diverse bronnen [7]

Preambule 89
NIS2 instrueert organisaties expliciet om zero trust-principes te adopteren
NIS2-richtlijn [8]

1. Wat is ZTNA?

Zero Trust Network Access (ZTNA) is een beveiligingsoplossing die toegang tot applicaties verleent op basis van continue verificatie -- niet op basis van netwerklocatie.

Het kernprincipe is "never trust, always verify". In plaats van een gebruiker na een eenmalige VPN-login toegang te geven tot het hele netwerk, verifieert ZTNA continu de identiteit, het apparaat en de context, en verleent alleen toegang tot de specifieke applicatie die nodig is [9].

Stel je een kantoorgebouw voor: een VPN is als een sleutel die de voordeur opent -- daarna heb je toegang tot elke kamer. ZTNA is als een gepersonaliseerde badge die alleen de kamers opent waar jij moet zijn, en die continu controleert of je er nog mag zijn.

DRIE PRINCIPES VAN ZTNA

- **Never trust, always verify** -- elke toegangspoging wordt individueel beoordeeld, ook vanuit het "eigen" netwerk
- **Least-privilege access** -- toegang alleen tot wat nodig is, niet tot het hele netwerk
- **Assume breach** -- ga ervan uit dat het netwerk al gecompromitteerd is en beperk de schade

2. ZTNA vs VPN

VPN's zijn ontworpen voor een tijd waarin medewerkers op kantoor werkten en applicaties in het datacenter stonden. Die tijd is voorbij.

KENMERK	VPN	ZTNA
Toegangsmodel	Volledig netwerk na authenticatie	Per applicatie, continue verificatie
Authenticatie	Eenmalig bij verbinding	Continu (identiteit + apparaat + context)
Laterale beweging	Mogelijk -- hele netwerk toegankelijk	Geblokkeerd -- applicaties geïsoleerd [10]
Prestatie	Traag door backhauling via hoofdkantoor	Snel via directe cloud-verbinding
Schaalbaarheid	Beperkt door hardware	Cloud-native, elastisch
Gebruikerservaring	Omslachtig, traag	Transparant, naadloos
Beheer	Complex, hardware-afhankelijk	Centraal via cloud dashboard
MKB-kosten (50 pers.)	EUR 15.000--35.000/jaar	EUR 4.800--18.000/jaar

VPN-RISICO'S

Meer dan de helft van organisaties noemt beveiliging en slechte gebruikerservaring als grootste VPN-uitdagingen. VPN's verlenen "alles-of-niets" netwerktoegang -- in directe strijd met NIS2's proportionaliteitseis [8].

3. Hoe ZTNA werkt

ZTNA plaatst een broker tussen de gebruiker en de applicatie die elke toegangspoging beoordeelt.

1. **Gebruiker vraagt toegang aan**
   De gebruiker opent een applicatie. De ZTNA-agent (of browser) stuurt het verzoek naar de ZTNA-broker.

2. **Identiteitsverificatie**
   De broker verifieert de identiteit via MFA en SSO. Wie is deze gebruiker?

3. **Apparaatcontrole**
   Is het apparaat compliant? Zijn updates geïnstalleerd? Draait er antivirus? Is de schijf versleuteld?

4. **Contextbeoordeling**
   Vanwaar logt de gebruiker in? Op welk tijdstip? Past dit bij het normale gedragspatroon?

5. **Toegangsbesluit**
   Op basis van identiteit, apparaat en context wordt toegang verleend tot alleen de gevraagde applicatie.

6. **Continue monitoring**
   Tijdens de sessie wordt de verbinding continu beoordeeld. Bij afwijkingen wordt de toegang ingetrokken.

4. ZTNA vs verwante oplossingen

ZTNA is een onderdeel van het bredere zero trust-landschap.

KENMERK	ZTNA	VPN	SDP	SASE
Type	Toegangscontrole	Netwerktunnel	Toegangscontrole	Geïntegreerd platform
Scope	Per applicatie	Volledig netwerk	Per applicatie	Netwerk + security
Kosten MKB	EUR 5--20/pers/mnd	EUR 3--15/pers/mnd + hardware	EUR 8--25/pers/mnd	EUR 15--40/pers/mnd

5. Wat kost het?

ZTNA is vaak goedkoper dan VPN als je alle kosten meeneemt: hardware, licenties, beheer en bandbreedte.

SEGMENT	GEBRUIKERS	ZTNA JAARKOSTEN	VPN JAARKOSTEN
Klein MKB	10--25	EUR 1.200--4.800	EUR 5.000--15.000
Middelgroot MKB	50--100	EUR 4.800--18.000	EUR 15.000--35.000
Groot MKB	150--250	EUR 14.400--48.000	EUR 30.000--75.000

> **ROI**
>
> Forrester berekende een ROI van 289% over 3 jaar bij ZTNA-implementatie: EUR 16,4 miljoen aan baten vs. EUR 4,2 miljoen aan kosten. Plus: 80% minder support tickets en ~EUR 1 miljoen besparing op breach-kosten [3].

6. Veelgemaakte fouten

Deze valkuilen ondermijnen je zero trust-implementatie.

1. Zero trust als product behandelen

Zero trust is een strategie, geen product. ZTNA is een onderdeel, niet de volledige invulling. Zonder bredere principes (segmentatie, monitoring, least privilege) mis je het doel [11].

2. Bestaande tools als zero trust beschouwen

Firewalls en VPN's zijn bouwstenen, geen zero trust-architectuur [12].

3. Onvolledig IAM

IAM is het fundament. Alleen wachtwoorden of zwakke MFA (SMS) creëert risico's [11].

4. Gebrek aan zichtbaarheid

Zonder overzicht van alle apparaten, gebruikers en applicaties blijft zero trust half werk [12].

5. Overmatige verificatie zonder context

Contextbewuste verificatie -- niet constant alles opnieuw verifiëren. Balans tussen veiligheid en gebruikerservaring [11].

6. Statische implementatie

Dreigingen en werkpatronen veranderen constant. Policies moeten adaptief zijn, niet vast.

7. Onvoldoende budget en capaciteit

MKB onderschat vaak de benodigde investering in training en beheer [13].

7. NIS2 en DORA

NIS2 noemt zero trust expliciet als aanbevolen beveiligingsmaatregel.

Preambule 89 van de NIS2-richtlijn instrueert organisaties om zero trust-principes te adopteren [8]. ZTNA draagt direct bij aan compliance:

NIS2-EIS	HOE ZTNA HELPT
Toegangsbeheer	Least-privilege per applicatie i.p.v. netwerk-breed [8]
Proportionaliteit	Context-aware toegangscontrole proportioneel aan risico
Incidentdetectie	Gedetailleerde logging van alle toegangspogingen
Aantoonbaarheid	Continue compliance-rapportage via centraal dashboard
Supply chain	Beveiligde leverancierstoegang zonder VPN

NIS2-BOETES

Essentiële entiteiten: tot EUR 10.000.000 of 2% jaaromzet. Belangrijke entiteiten: tot EUR 7.000.000 of 1,4% jaaromzet. ~10.000 Nederlandse organisaties vallen onder NIS2.

8. Een oplossing kiezen

De juiste ZTNA-oplossing hangt af van je omgeving, gebruikers en bestaande infrastructuur.

1. **Agent-based vs agentless** -- agent biedt meer controle, agentless is makkelijker voor third parties
2. **Identity provider integratie** -- SSO met Azure AD, Okta, Google
3. **Device posture checks** -- apparaatcompliance controleren
4. **Multi-cloud en on-premises** -- toegang tot zowel cloud als legacy apps
5. **Granulariteit van policies** -- per app, per groep, contextafhankelijk
6. **Migratiepas** -- geleidelijk van VPN overstappen
7. **Compliance-rapportage** -- NIS2, SOC 2, ISO 27001
8. **Kosten per gebruiker** -- transparant en voorspelbaar

SITUATIE	ADVIES
< 25 gebruikers	Gratis tier (Cloudflare Access) of lightweight (Tailscale)
Vooral webapps	Agentless ZTNA volstaat
Legacy systemen	Agent-based met connector/gateway
Bestaande firewall	Check ZTNA van je huidige vendor

9. Implementatie-aanpak

Een pragmatisch stappenplan voor de overgang van VPN naar ZTNA.

1 **Inventarisatie**

1--2 WEKEN

Breng alle applicaties, gebruikers en huidige toegangsmethoden in kaart.

2 **Identity foundation**

2--4 WEKEN

Zorg dat SSO en MFA correct werken voor alle gebruikers.

3 **Tool selectie**

2--3 WEKEN

Evalueer en selecteer ZTNA-oplossing op basis van je criteria.

4 **Pilot**

2--4 WEKEN

Start met 1--2 niet-kritieke applicaties en een kleine gebruikersgroep.

5 **Uitrol en VPN-afbouw**

4--12 WEKEN

Migreer geleidelijk meer applicaties. Schakel VPN af per applicatie.

6 **Monitoring en compliance**

1--2 WEKEN

Configureer logging, alerting en compliance-rapportage.

QUICK WINS -- EERSTE 30 DAGEN

1. Activeer MFA voor alle externe toegang. 2. Inventariseer alle apps met remote access. 3. Start PoC met gratis ZTNA-tier. 4. Documenteer huidige VPN-kosten als baseline. 5. Identificeer top-5 meest gebruikte remote apps.

10. Trends 2025--2026

Zeven ontwikkelingen die ZTNA de komende jaren vormgeven.

1. VPN-vervanging accelereert

70%+ van nieuwe deployments via ZTNA. VPN wordt legacy [2].

2. ZTNA als onderdeel van SASE

ZTNA wordt steeds vaker aangeboden als onderdeel van een breder SASE-platform.

3. AI-gestuurde risicoanalyse

Adaptieve, risicogebaseerde toegangscontrole op basis van gedragspatronen.

4. Universal ZTNA

Dezelfde toegangscontrole overal -- kantoor, thuis, onderweg. Geen verschil meer tussen intern en extern.

5. NIS2 als adoptie-accelerator

NIS2 noemt zero trust expliciet. De Cyberbeveiligingswet (Q2 2026) versnelt adoptie [8].

6. Agentless ZTNA groeit

Voor webapplicaties en third-party toegang verlaagt agentless de implementatiedrempel.

7. Identity-first security

Focus verschuift van netwerk-centrisch naar identiteit-centrisch. ZTNA integreert met IAM-platforms.

Bronnenlijst

[1] **Gartner** -- 63% of Organizations Have Implemented Zero Trust Strategy. gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy

[2] **Gartner** -- 70%+ nieuwe remote access via ZTNA i.p.v. VPN (2025). (via Fortinet) fortinet.com/resources/cyberglossary/ztna-vs-vpn

[3] **Forrester/Zscaler** -- Total Economic Impact of ZPA: ROI 289%, NPV USD 12,2M. tei.forrester.com/go/Zscaler/PrivateAccess/

[4] **Appgate** -- ROI of Universal ZTNA: 80% minder support tickets. appgate.com/blog/what-is-the-return-on-investment-of-universal-ztna

[5] **CBS** -- Cybersecuritymonitor 2024: MFA 76% bij 10--50 pers. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024

[6] **MarketsandMarkets** -- ZTNA Market USD 1,34B (2025) naar USD 4,18B (2030). marketsandmarkets.com/Market-Reports/zero-trust-network-access-ztna-market-23387374.html

[7] **Cato Networks** -- ZTNA vs VPN: 65% enterprises plant VPN-vervanging. catonetworks.com/zero-trust-network-access/ztna-vs-vpn/

[8] **GoodAccess** -- NIS2 to require zero trust as essential security measure (preambule 89). goodaccess.com/blog/nis2-require-zero-trust-essential-security-measure

[9] **Nomios** -- What is ZTNA? nomios.com/resources/what-is-ztna/

[10] **Fortinet** -- ZTNA vs VPN: laterale beweging geblokkeerd. fortinet.com/resources/cyberglossary/ztna-vs-vpn

[11] **Kennisportal** -- Veelgemaakte fouten bij zero trust implementatie. kennisportal.com/veelgemaakte-fouten-bij-de-implementatie-van-zero-trust-en-zo-voorkom-je-ze/

[12] **Computable** -- De 5 grootste fouten bij implementeren zero trust. computable.nl/2024/09/10/dit-zijn-de-5-grootste-fouten-bij-implementeren-zero-trust/

[13] **ChannelConnect** -- Zero trust in het MKB: hype of noodzaak? channelconnect.nl/security-en-privacy/zero-trust-in-het-mkb-hype-of-noodzaak/

[14] **Eyer.ai** -- ZTNA ROI: Cost-Benefit Analysis & Savings. eyer.ai/blog/ztna-roi-cost-benefit-analysis-and-savings/

[15] **HPE** -- Zero trust and NIS2 compliance. community.hpe.com/t5/networking/how-zero-trust-enhances-nis2-compliance-and-cybersecurity/ba-p/7244366

[16] **Reinvent IT** -- Zero trust: praktische aanpak voor MKB. reinventit.nl/zero-trust-beveiliging-een-praktische-aanpak-voor-het-mkb/

[17] **AIMultiple** -- Top 10+ ZTNA Solutions: Ratings, Size & Pricing. aimultiple.com/ztna-solutions

[18] **Cloudflare** -- Zero Trust Plans & Pricing. cloudflare.com/plans/zero-trust-services/

Deze gids is samengesteld door IBgids.nl op basis van openbare bronnen en marktonderzoek. Alle genoemde prijzen zijn indicatief (peildatum: maart 2026). IBgids.nl is een onafhankelijk platform.