GIDS

De complete gids voor managed firewall services

Kosten, soorten, selectiecriteria, NIS2-compliance en Nederlandse marktdata. Voor MKB-organisaties die netwerkbeveiliging willen uitbesteden.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De Nederlandse markt voor managed firewall services groeit snel, gedreven door stijgende dreigingen en nieuwe regelgeving. Dit zijn de feiten.

USD 5,5 mrd

Wereldwijde FWaaS-markt in 2025, groei naar USD 11,7 miljard in 2030

Mordor Intelligence [1]

16,5%

Jaarlijkse groei (CAGR) van de Firewall-as-a-Service markt tot 2030

Mordor Intelligence [1]

4.875

Cybersecurity-incidenten in de EU geanalyseerd door ENISA (juli 2024 - juni 2025)

ENISA Threat Landscape 2025 [2]

EUR 270K

Gemiddelde schade per cyberincident voor MKB in Nederland

Verzekercyber.nl [3]

76%

MFA-gebruik bij bedrijven (10-50 pers.) in 2024, was 29% in 2017

CBS Cybersecuritymonitor 2024 [4]

~10.000

Nederlandse bedrijven die onder de Cyberbeveiligingswet (NIS2) gaan vallen

Digitale Overheid [5]

75%

Van system-intrusion breaches waarbij ransomware betrokken is

Verizon DBIR 2025 [6]

241 dgn

Gemiddelde tijd om een datalek te detecteren en in te dammen

IBM Cost of Data Breach 2025 [7]

1. Wat is een managed firewall service?

Een managed firewall service is de uitbesteding van het volledige firewallbeheer aan een gespecialiseerde security-partner. Je krijgt professionele netwerkbeveiliging zonder dat je zelf een security-team hoeft op te bouwen.

Bij een managed firewall neemt een Managed Security Service Provider (MSSP) of Managed Service Provider (MSP) de installatie, configuratie, monitoring, updates en incidentrespons van je firewall over [8]. De firewall wordt 24/7 bewaakt en dreigingen worden gestopt voordat ze schade aanrichten [9].

De dienst is beschikbaar in verschillende vormen. Bij Firewall-as-a-Service (FWaaS) draait de firewall in de cloud of wordt hardware meegeleverd in een abonnementsmodel. Bij een managed service bovenop bestaande hardware behoudt je je eigen apparatuur, maar wordt het beheer uitbesteed.

KERNFUNCTIES

- **Firewallconfiguratie en -optimalisatie** -- regels worden afgestemd op jouw netwerk en bedrijfsprocessen
- **Continue monitoring** -- 24/7 of 8×5 bewaking van netwerkverkeer op verdachte patronen
- **Patch- en updatebeheer** -- firmware en signatures worden proactief bijgehouden
- **Incident response** -- bij een alarm wordt direct actie ondernomen
- **Rapportage** -- periodieke overzichten van dreigingen, verkeer en incidenten
- **Compliance-ondersteuning** -- documentatie en logging voor NIS2/AVG-audits

TIP

Een managed firewall is geen vervanging voor een breder beveiligingsbeleid. Het is een fundamenteel onderdeel van je security stack, samen met endpoint protection, identity management en security awareness.

2. Waarom is het belangrijk?

Het dreigingslandschap wordt complexer en de regelgeving strenger. Zonder professioneel firewallbeheer loop je als MKB-organisatie aanzienlijke risico's.

De ENISA Threat Landscape 2025 laat zien dat 81,1% van alle cybercrime-incidenten in de EU ransomware betreft [2]. DDoS-aanvallen zijn goed voor 77% van alle incidenten en phishing blijft met circa 60% de meest gebruikte inbraakpoging [2]. Een firewall is je eerste verdedigingslinie tegen dit soort aanvallen.

DE BUSINESS CASE

De gemiddelde schade per cyberincident voor MKB in Nederland bedraagt EUR 270.000 [3]. Een managed firewall service kost EUR 6.000-18.000 per jaar -- een fractie van de potentiele schade. Bovendien gaat 60% van kleine bedrijven failliet binnen zes maanden na een ernstige cyberaanval [3].

De Verizon DBIR 2025 toont dat credential abuse (22%) en exploitatie van kwetsbaarheden (20%) de belangrijkste initiële aanvalsvectoren zijn [6]. Een goed geconfigureerde en beheerde firewall detecteert en blokkeert veel van deze aanvallen aan de netwerkperimeter.

> **Tekort aan security-professionals:** Een security engineer verdient gemiddeld EUR 60.000-92.000 per jaar in Nederland [10]. Voor MKB is het aantrekken en behouden van dit talent vaak niet haalbaar. Uitbesteding lost dit probleem op.

REGELGEVING DWINGT ACTIE

De Cyberbeveiligingswet (NIS2-implementatie) treedt naar verwachting Q2 2026 in werking en treft circa 10.000 Nederlandse organisaties [5]. De wet verplicht "passende technische en operationele maatregelen" voor netwerkbeveiliging [11]. Boetes kunnen oplopen tot EUR 10 miljoen of 2% van de wereldwijde jaaromzet [12].

3. Hoe werkt het? Het implementatieproces

Van inventarisatie tot operationeel beheer: zo verloopt de implementatie van een managed firewall service, stap voor stap.

1 Inventarisatie en assessment

1-2 WEKEN

De MSSP brengt je huidige netwerkomgeving in kaart: locaties, internetverbindingen, bestaande firewalls, applicaties en gebruikersgroepen. Er wordt een risico-inventarisatie gemaakt.

2 Ontwerp en configuratie

1-2 WEKEN

Op basis van het assessment wordt een firewall-ontwerp gemaakt met zones, regels, VPN-configuratie en integratie met andere beveiligingssystemen. De configuratie wordt afgestemd op jouw specifieke bedrijfsprocessen.

3 Implementatie en migratie

1-3 WEKEN

De nieuwe firewall wordt geïnstalleerd (of de bestaande geconfigureerd). Bij FWaaS wordt de cloud-component geconfigureerd. Migratie van bestaande regels en VPN-tunnels wordt uitgevoerd met minimale downtime.

4 Testfase en finetuning

1-2 WEKEN

De firewall draait in monitoring-modus. Valse positieven worden geëlimineerd, regels worden aangescherpt en de baseline voor normaal verkeer wordt vastgesteld.

5 Operationeel beheer

DOORLOPEND

De MSSP neemt het dagelijks beheer over: 24/7 monitoring, incidentrespons, firmware-updates, regeloptimalisatie en periodieke rapportage.

> **Totale doorlooptijd:** 4-8 weken van start tot volledig operationeel, afhankelijk van de complexiteit van je netwerkomgeving en het aantal locaties.

4. Wat kost het?

De kosten van een managed firewall service hangen af van het aantal locaties, de gewenste monitoring-intensiteit en de complexiteit van je netwerk.

MAANDELIJKSE KOSTEN PER LOCATIE

SEGMENT	MAANDPRIJS	WAT JE KRIJGT
Klein MKB (10-50 mdw)	EUR 150-400	Basis NGFW, 8×5 monitoring, maandrapportage [13]
Middelgroot MKB (50-150 mdw)	EUR 400-800	NGFW met IPS/IDS, 24/7 monitoring, incident response [13]
Groot MKB (150-250 mdw)	EUR 800-1.500	Multi-site, redundantie, 24/7 SOC-koppeling [13]

EIGEN BEHEER: DE VERBORGEN KOSTEN

KOSTENPOST	EIGEN BEHEER (PER JAAR)	MANAGED SERVICE (PER JAAR)
Hardware/licenties	EUR 3.000-15.000 [14]	Inbegrepen
FTE security engineer (0,3 FTE)	EUR 18.000-28.000 [10]	Inbegrepen
Training/certificering	EUR 2.000-5.000	Inbegrepen
24/7 monitoring	EUR 6.000-12.000	Inbegrepen
Totaal	**EUR 29.000–60.000**	**EUR 6.000–18.000**

PRIJSBEPALENDE FACTOREN

- **Aantal locaties** -- elke locatie vereist een eigen firewall of VPN-koppeling
- **Monitoring-niveau** -- 8×5 vs. 24/7 monitoring en respons
- **Complexiteit** -- aantal zones, VPN-tunnels, applicatie-integraties
- **SLA-niveau** -- responstijd bij incidenten (15 min, 1 uur, 4 uur)
- **Hardware-eigendom** -- eigen hardware vs. meegeleverd in abonnement
- **Contractduur** -- langere contracten geven vaak korting

TIP

Vraag altijd naar een TCO-berekening (Total Cost of Ownership) voor zowel eigen beheer als managed service. De maandelijkse kosten van managed service lijken hoger, maar als je alle verborgen kosten van eigen beheer meerekent, is uitbesteding voor de meeste MKB-organisaties voordeliger.

5. Waar moet je op letten bij de keuze?

Niet elke managed firewall provider levert dezelfde kwaliteit. Deze selectiecriteria helpen je de juiste partner te kiezen.

SELECTIECRITERIA

1. Monitoring en respons

Vraag naar het verschil tussen 8×5 en 24/7 monitoring. Bij 24/7 monitoring worden dreigingen ook buiten kantooruren direct opgepakt. Gezien het feit dat aanvallers geen kantooruren hanteren, is 24/7 monitoring sterk aan te raden [9].

2. SLA-afspraken

Wat is de maximale responstijd bij een kritiek incident? Wat is de uptime-garantie? Een goede SLA bevat concrete afspraken over escalatieprocedures, rapportagefrequentie en beschikbaarheid.

3. Transparante rapportage

Je moet inzicht hebben in wat er op je netwerk gebeurt. Vraag naar dashboards, maandelijkse rapportages en real-time alerting. Goede providers geven je een portaal waar je zelf kunt meekijken.

4. Ervaring en certificeringen

Heeft de provider ervaring met jouw sector en bedrijfsgrootte? Zijn de engineers gecertificeerd (Fortinet NSE, Palo Alto PCNSE, Cisco CCNP Security)? Vraag naar referenties van vergelijkbare organisaties.

5. NIS2-compliance ondersteuning

Kan de provider aantonen dat de dienst bijdraagt aan de zorgplicht onder de Cyberbeveiligingswet? Zijn er compliance-rapportages beschikbaar?

10 VRAGEN VOOR JE AANBIEDER

1. Wat is jullie gemiddelde detectietijd bij een beveiligingsincident?
2. Hoe ziet jullie escalatieprocedure eruit bij een kritiek incident?
3. Welke firewall-merken en -modellen ondersteunen jullie?
4. Wat is de uptime-garantie en wat gebeurt er als die niet wordt gehaald?
5. Hoe worden firmware-updates en patches gepland en uitgevoerd?
6. Welke rapportages ontvang ik en hoe vaak?
7. Hoe ondersteunen jullie NIS2/Cyberbeveiligingswet compliance?
8. Wat zijn de exit-voorwaarden als ik wil overstappen?
9. Hebben jullie ervaring met multi-site omgevingen?
10. Kunnen jullie referenties geven van vergelijkbare MKB-organisaties?

RED FLAGS

Wees alert als een provider: geen SLA wil afgeven, geen transparante rapportage biedt, geen ervaring heeft met jouw sector, geen exit-clausule hanteert, of geen 24/7 optie aanbiedt.

6. Veelgemaakte fouten

Deze fouten zien we regelmatig bij MKB-organisaties die een managed firewall service afnemen of overwegen.

1. Alleen op prijs selecteren

De goedkoopste provider is niet altijd de verstandigste keuze. Een lage maandprijs kan betekenen dat monitoring beperkt is, responstijden lang zijn of dat er geen proactief beheer plaatsvindt. Vergelijk altijd op basis van TCO en kwaliteit.

2. Firewall als enige beveiligingsmaatregel

Een firewall beschermt de netwerkperimeter, maar biedt geen bescherming tegen phishing die via e-mail binnenkomt, insider threats of aanvallen via gecompromitteerde endpoints. Combineer altijd met endpoint protection en security awareness.

3. Firewallregels niet periodiek reviewen

Firewallregels verzamelen zich over tijd. Oude regels voor voormalige medewerkers, opgeheven applicaties of verouderde VPN-tunnels blijven staan en vormen een beveiligingsrisico. Een goede provider plant regelmatige rule reviews.

4. Geen exit-strategie

Als je firewall-configuratie eigendom is van de provider en er geen duidelijke exit-afspraken zijn, zit je vast. Zorg dat configuratiedata, logging en documentatie altijd beschikbaar zijn.

5. SLA niet lezen

Veel organisaties tekenen een contract zonder de SLA-details te lezen. Wat is "responstijd" precies -- tijd tot eerste reactie of tijd tot oplossing? Wat valt onder de SLA en wat niet?

6. Geen integratie met andere beveiligingssystemen

Een firewall die losstaat van je SIEM, EDR en identity management mist context. Integratie zorgt voor betere detectie en snellere respons.

7. Interne IT niet betrekken

Het uitbesteden van firewallbeheer betekent niet dat je interne IT-team er niets meer mee te maken heeft. Zorg voor heldere afspraken over wie wat doet en hoe de communicatie verloopt.

7. NIS2 en de Cyberbeveiligingswet

De Cyberbeveiligingswet stelt concrete eisen aan netwerkbeveiliging. Wat betekent dat voor je firewall?

De Cyberbeveiligingswet (de Nederlandse implementatie van de Europese NIS2-richtlijn) treedt naar verwachting in Q2 2026 in werking [5]. De wet richt zich op de beveiliging van netwerk- en informatiesystemen en geldt voor circa 10.000 Nederlandse organisaties.

ZORGPLICHT

Organisaties moeten een risicoanalyse uitvoeren en op basis daarvan "passende en evenredige technische, operationele en organisatorische maatregelen" nemen [11]. De minimummaatregelen omvatten onder andere:

- Risicoanalyses en informatiebeveiligingsbeleid
- Incidentenbehandeling
- Bedrijfscontinuiteit en back-upbeheer
- Beveiliging van de toeleveringsketen
- Cyberhygienepraktijken en cybersecurityopleidingen
- Multifactorauthenticatie

Een professioneel beheerde firewall draagt bij aan meerdere van deze maatregelen: netwerkbeveiliging, incidentdetectie, logging voor audit-doeleinden en bescherming tegen externe aanvallen.

BOETES

TYPE ENTITEIT	MAXIMALE BOETE
Essentieel	EUR 10 miljoen of 2% wereldwijde jaaromzet [12]
Belangrijk	EUR 7 miljoen of 1,4% wereldwijde jaaromzet [12]

Naast financiele sancties kunnen toezichthouders waarschuwingen opleggen, verboden uitvaardigen of specifieke herstelmaatregelen eisen. Bestuurders kunnen persoonlijk aansprakelijk worden gesteld [12].

> **Meldplicht:** Significante incidenten moeten binnen 24 uur worden gemeld bij het CSIRT [11]. Een managed firewall met 24/7 monitoring helpt bij het tijdig detecteren en melden van incidenten.

8. Managed firewall vs. eigen beheer

Wanneer kies je voor uitbesteding en wanneer voor eigen beheer? Een objectieve vergelijking.

CRITERIUM	EIGEN BEHEER	MANAGED SERVICE
Kosten (per jaar)	EUR 29.000-60.000 [10][14]	EUR 6.000-18.000 [13]
Expertise	Zelf aantrekken en bijhouden	Team van specialisten inbegrepen [8]
Monitoring	8×5 (tenzij extra investeringen)	24/7 beschikbaar [9]
Flexibiliteit	Volledig maatwerk mogelijk	Afhankelijk van provider-aanbod
Controle	Volledige controle [8]	Gedeelde controle via dashboards
Schaalbaarheid	Grote investering per locatie	Eenvoudig op te schalen
NIS2 compliance	Zelf documenteren	Compliance-rapportages inbegrepen

> **Vuistregel:** Heb je minder dan 3 dedicated security-medewerkers in dienst? Dan is een managed firewall service vrijwel altijd voordeliger en veiliger dan eigen beheer. De meeste MKB-organisaties vallen in deze categorie.

9. Trends 2025-2026

De markt voor managed firewall services verandert snel. Deze trends bepalen de komende jaren.

1. SASE/SSE-convergentie

Managed firewalls worden steeds vaker onderdeel van bredere Secure Access Service Edge (SASE) architecturen. In plaats van een losstaande firewall koop je een geintegreerd pakket met firewall, ZTNA, CASB en SD-WAN. Meer dan 60% van organisaties plant om FWaaS te combineren met Zero Trust Network Access tegen 2026 [1].

2. AI-gedreven detectie

Machine learning wordt ingezet voor anomaliedetectie in netwerkverkeer. AI herkent patronen die traditionele regelgebaseerde systemen missen en verlaagt het aantal false positives. IBM rapporteert dat AI-powered verdediging de detectietijd significant verlaagt [7].

3. Cloud-first

Software-gebaseerde firewalls groeien sneller dan hardware (15% CAGR voor software vs. dalende hardware-groei) [15]. Steeds meer organisaties kiezen voor virtuele firewalls in multi-cloud omgevingen.

4. NIS2-gedreven adoptie

Met de verwachte inwerkingtreding van de Cyberbeveiligingswet in Q2 2026 wordt een piek verwacht in de vraag naar managed firewall services, vooral bij MKB-organisaties die voor het eerst onder de wet vallen [5].

10. Aan de slag

Klaar om je netwerkbeveiliging professioneel te laten beheren? Zo pak je het aan.

STAPPENPLAN

1. **Breng je huidige situatie in kaart** -- hoeveel locaties, welke firewalls, welke internetverbindingen?
2. **Bepaal je eisen** -- 24/7 of 8×5 monitoring? Multi-site? NIS2-compliance?
3. **Vraag minimaal 3 offertes aan** -- vergelijk op TCO, SLA, rapportage en referenties
4. **Check referenties** -- vraag naar ervaringen van vergelijkbare organisaties
5. **Plan de implementatie** -- reken op 4-8 weken doorlooptijd

Bronnenlijst

[1] **Mordor Intelligence** -- Firewall-as-a-Service Market Size & Forecast to 2030. mordorintelligence.com/industry-reports/firewall-as-a-service-market

[2] **ENISA** -- Threat Landscape 2025. enisa.europa.eu/publications/enisa-threat-landscape-2025

[3] **Verzekercyber.nl / Laurus Verzekeringen** -- Gemiddelde schade cyberincident MKB Nederland (via marktdata)

[4] **CBS** -- Cybersecuritymonitor 2024. cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[5] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2-richtlijn). digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[6] **Verizon** -- 2025 Data Breach Investigations Report. verizon.com/business/resources/reports/dbir/

[7] **IBM** -- Cost of a Data Breach Report 2025. ibm.com/reports/data-breach

[8] **Direct.eu** -- Wat is een managed firewall. blog.direct.eu/wat-is-een-managed-firewall-en-wat-zijn-de-voordelen-van-het-inhuren-van-een-managed-firewall-service-provider

[9] **KPN Zakelijk** -- Managed firewall voor optimale beveiliging. kpn.com/zakelijk/thedigitaldutch/blog/managed-firewall-optimale-beveiliging

[10] **Glassdoor Nederland** -- Security Engineer salarissen 2025. glassdoor.nl/Salarissen/security-engineer-salarissen-SRCH_KO0,17.htm

[11] **NCSC** -- FAQ Cyberbeveiligingswet (NIS2). ncsc.nl/cyberbeveiligingswet-nis2/bereid-je-voor/faq-cyberbeveiligingswet-nis2

[12] **Nieuwhuisconsult** -- Boetes bij niet-naleving NIS2. nieuwhuisconsult.nl/nieuws/wat-zijn-de-boetes-bij-niet-naleving-van-nis-2

[13] **1ConnectCloud / Tardigrade Technology / NTNT** -- Managed Firewall Pricing 2025 SME Guide. 1connectcloud.com/managed-firewall-pricing/

[14] **PeerSpot** -- Fortinet FortiGate pricing ervaringen. peerspot.com/questions/what-is-your-experience-regarding-pricing-and-costs-for-fortinet-fortigate

[15] **Precedence Research** -- Enterprise Firewall Market Size. precedenceresearch.com/enterprise-firewall-market

[16] **Nomios Group** -- Managed firewall services. nomios.com/managed-services/managed-firewall/

[17] **Fundaments** -- Firewall as a Service / Managed Firewall. fundaments.nl/en/services/firewall-as-a-service/managed-firewall