



# Managed Firewall

Internet is een onmisbare, bedrijfskritische voorziening geworden voor bedrijven en instellingen. Tegelijkertijd neemt de complexiteit en het aantal bedreigingen afkomstig van internet toe. Denk hierbij aan virussen, spyware, phishing, malware, hacking, DDoS aanvallen en bedrijfsinformatie die ongewenst op internet wordt geplaatst. Dit kan een grote bedreiging vormen voor de continuïteit van uw organisatie. Een traditionele firewall biedt hier onvoldoende bescherming tegen; er zijn aanvullende technologieën, software en kennis nodig om tegenwoordig voldoende bescherming te bieden. Dat is vaak duur en ingewikkeld. Previder biedt hiervoor een geïntegreerde, betaalbare oplossing.

## Next Generation Firewall

U hoeft niet meer te investeren in verschillende apparaten of software voor de bescherming van uw IT-omgeving. Previder biedt met Managed Firewall een complete, geïntegreerde oplossing voor beveiliging van uw IT-omgeving. De dienst wordt als een service geleverd, wat betekent dat er geen apparatuur op locatie nodig is en er ook geen investeringen nodig zijn. Previder zorgt ervoor dat alle componenten altijd up-to-date zijn, voor een zo optimaal mogelijke bescherming. Managed Firewall wordt geleverd voor een vast maandelijks bedrag.

## Belangrijkste voordelen

- Complete, geïntegreerde oplossing voor beveiliging van uw IT-omgeving
- Geen investering, maar vast bedrag per maand
- Geen apparatuur op locatie nodig
- Altijd up-to-date
- Schaalbaar
- Beheer door security experts van Previder

## Toepassingen

- Beveiliging van (web)servers, gehoste applicaties en data
- Beveiliging Cloud Servers, Virtual DataCenter of Private Cloud omgevingen
- Beveiliging van aan internet gekoppelde bedrijfsnetwerken

## Technische eigenschappen

Managed Firewall is gebaseerd op technologie van Fortinet; de wereldwijde leider op het gebied van IT-beveiliging. Op basis van een redundant uitgevoerd FortiGate platform biedt Previder een robuuste, schaalbare en betrouwbare oplossing.



## Technische eigenschappen

Managed Firewall is gebaseerd op technologie van Fortinet; de wereldwijde leider op het gebied van IT-beveiliging. Op basis van een redundant uitgevoerd FortiGate platform biedt Previder een robuuste, schaalbare en betrouwbare oplossing.

De volgende technologieën maken onderdeel uit van de service:

- Basis firewall functionaliteit
- Antivirus, antispysware en antimalware
- Antispam
- Webfiltering
- Application control
- Intrusion Prevention System (IPS)
- Data Leakage Prevention(DLP)
- IPsec/SSL VPN
- Beperkte DDoS-attack preventie
- Load balancing
- Vulnerability scan

## Inrichting & management

Managed Firewall wordt initieel opgeleverd met een standaard set aan regels, die kan worden aangepast op uw specifieke wensen en eisen.

Het firewall platform wordt volledig gemanaged door Previder en gegarandeerd middels een SLA. Na de initiële inrichting kunnen changes op twee manieren plaatsvinden:

### 1. Fully managed

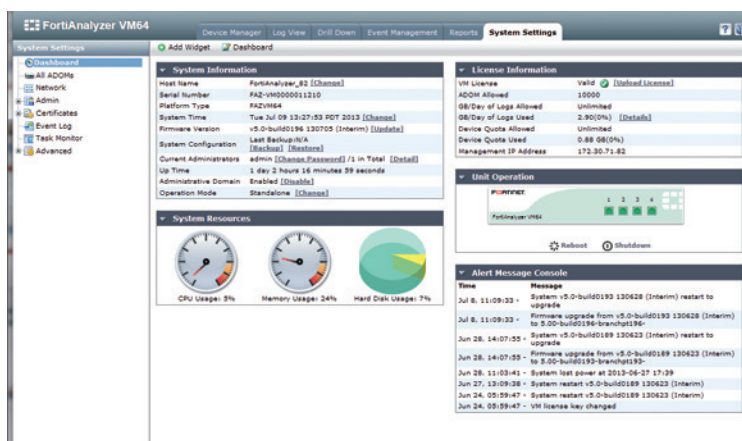
Hierbij is het beheer in handen van de experts van Previder. Wijzigingsverzoeken kunt u via een online formulier aanvragen. Deze changes zullen vervolgens door een medewerker van Previder worden uitgevoerd.

### 2. Co-administration

Hierbij krijgt u toegang tot de managementinterface van uw eigen omgeving. Hiermee kunt u alle instellingen zonder tussenkomst van Previder wijzigen.

## Rapportage & SLA

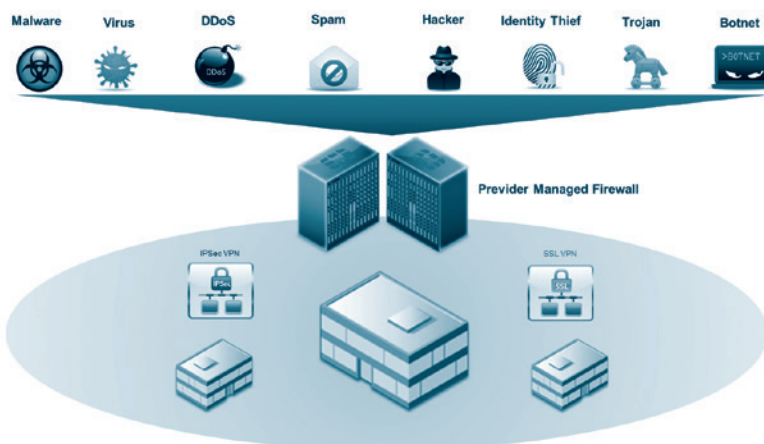
Via het online portal krijgt u toegang tot rapportages die u inzicht geven in het functioneren van de service. De service heeft een eigen SLA, die we u op verzoek toesturen.





## Meer informatie?

Neem contact op met de afdeling verkoop van Previder via [info@previder.nl](mailto:info@previder.nl) of 088 - 332 33 33. Op verzoek sturen we u de complete dienstbeschrijving en SLA.



### Bedreiging in de praktijk

Bedrijf X ontvangt per e-mail een factuur in PDF-formaat, die ogenschijnlijk afkomstig is van een leverancier. In werkelijkheid is deze afkomstig van een kwaadwillende cybercrimineel. De controller opent de bijlage, en daarmee wordt ongemerkt spyware geïnstalleerd op de PC van de controller. Via de spyware worden passwords achterhaald, waarmee de cybercrimineel toegang krijgt tot het bedrijfsnetwerk en vertrouwelijke documenten met klantgegevens. De cybercrimineel gebruikt deze gegevens om valse facturen naar klanten te sturen, met een ander bankrekeningnummer. Bedrijf X merkt dit op, maar doordat de cybercrimineel op hetzelfde moment een DDoS aanval uitvoert op het bedrijf, kan bedrijf X haar klanten niet snel op de hoogte brengen van de fraude.

De Managed Firewall dienst van Previder had bovenstaande aanval op verschillende manieren kunnen blokkeren.

- De met spyware besmette PDF zal door het antispyware filter worden geblokkeerd;
- Door gebruik van IPS kan worden voorkomen dat de cybercrimineel inbreekt op het bedrijfsnetwerk;
- Door gebruik van DLP kan worden voorkomen dat vertrouwelijke documenten bewust of onbewust worden verstuurd vanuit het bedrijfsnetwerk naar het internet;
- De DDoS-attack kan worden geneutraliseerd door de DDoS attack\* bescherming.

\*DDoS protectie is beperkt. Vraag naar de randvoorwaarden.