

MFWs-addendum SmartDefense

IntrusionPrevention-Light van Check Point

Inhoudsopgave

1	Inleiding.....	2
2	Algemeen.....	2
2.1	Achtergrond.....	2
2.2	Extra dienst, extra veiligheid	2
2.3	Allen in combinatie met 'Klant aan de knoppen'	3
2.4	Versiebeheer.....	3
3	Beschrijving van de dienst	3
3.1	SmartDefense van Check Point	3
4	Aanbiedingsvorm	3
4.1	Critical, high, medium & low	3
4.2	Software.....	3
4.3	Handelingen.....	4
4.4	Rapportage	4
5	Het proces.....	4
5.1	Als er een advisory binnenkomt	4
5.2	Er ontstaat een probleem.....	4
5.3	Escalatie	4
5.4	Security	4
6	Contract	4
6.1	Duur	4
6.2	Verplichtingen	4
7	Kosten.....	5
8	Voorwaarden.....	5

1 Inleiding

Dit document beschrijft de dienst SmartDefense van KPN, die uitsluitend in combinatie met de Managed Firewall dienst van KPN kan worden afgenomen.

De dienst is gebaseerd op het abonnement met dezelfde naam van Check Point software technologies uit Israël, dat de basis vormt van de Managed Firewall dienst (hierna MFWs) van KPN.

2 Algemeen

2.1 Achtergrond

De dreiging van aanvallen vanuit het internet wordt voortdurend groter waardoor de markt om verdergaande beveiliging vraagt, die zowel completer als tijdiger beveiliging biedt dan met alleen een firewall mogelijk is.

Makers van firewall-oplossingen proberen steeds meer extra beveiliging in hun producten te stoppen. Check Point technologies heeft hiervoor het product SmartDefense toegevoegd aan hun firewall software. Dit product bevat een subset van een volledig Intrusion Prevention Systeem (IPS).

2.2 Extra dienst, extra veiligheid

Indien MFWs zonder SmartDefense dienst wordt afgenomen is een standaard-set van beschermende maatregelen onderdeel van de dienst. Dit is de standaardinstelling (volgens Check Point advies) waarbij een aantal opties aanstaan die onmisbaar zijn voor basis veiligheid.

Wanneer de SmartDefense dienst van KPN wordt afgenomen wordt een uitgebreide set extra beveiligingsopties geactiveerd door specialisten van KPN.

2.3 Allen in combinatie met 'Klant aan de knoppen'

Omdat de instellingen en werking van Smartdefense diep ingrijpt op uw internet-verkeer, is het van groot belang dat u zelf aan de knoppen zit: niemand weet beter dan u welke server welk OS draait, in welke versie en wat de kwetsbaarheden zijn. Alleen u kent uw kritische assets en kunt de juiste keuzes maken, en dan ook nog snel genoeg. KPN kan daarom nooit genoeg waarde toevoegen bij Smart Defense.

2.4 Versiebeheer

Om het product volledig te benutten is het noodzakelijk dat er altijd met de laatste versie van de firewall software wordt gewerkt. Hiertoe heeft KPN haar releasemanagement op de MFWs nadrukkelijk verscherpt. Nieuwe versies van de firewallsoftware zullen steeds binnen enkele maanden op alle firewalls onder beheer bij KPN worden geïnstalleerd.

3 Beschrijving van de dienst

3.1 SmartDefense van Check Point

Sinds enige tijd nemen de bedreigingen voor aangesloten individuen en bedrijven vanuit het Internet hand over hand toe. Zowel de snelheid alsook de complexiteit van de aanvallen nemen toe, maar ook het achterliggende economische belang neemt sterk toe.

Check Point's Firewalls hebben in de loop der tijd steeds beter kunnen inspelen op de behoefte aan verdediging tegen kwaadaardige invloeden door de toepassing van Stateful Inspection (waarmee verkeer aan een geldige sessie gerelateerd) en Securityengines (die gebruikers-authenticatie toepassen).

Als aanvulling op de bekende Firewall-1 en VPN-1 software levert Check Point in met SmartDefense nu ook bescherming tegen wormen, trojaanse paarden en directe aanvallen op systemen die achter of 'naast' (in de DMZ) staan opgesteld.

De doelen zijn:

Afdwingen van correct gebruik van protocollen & standaarden (vaak verraden fouten aanvallen);

Blokken van MMC = Malicious Mobile Code = uitvoerbare code-elementen die op servers en PC's programma's installeren als virussen, wormen, trojans, phishing-software, SPAM- & DDOS-bots.

Sneller zijn dan degenen die van kwetsbaarheden in systemen gebruik willen maken

SmartDefense bestaat uit:

Engine-updates: herziene & opgewaardeerde versies van de Stateful Inspection en Application Intelligence engines (software) die het hart van de Firewall vormen)

Advisories: adviezen, opgesteld en uitgegeven door Check Point die tot doel hebben bekende en onbekende dreigingen af te wenden door het aanpassen van de instellingen en de 'ruleset' van de firewall.

SmartDefense van Check Point wordt geleverd in abonnementsvorm.

4 Aanbiedingsvorm

De dienst wordt aangeboden als abonnement en kan alleen worden afgenomen in combinatie met alle modellen Managed Firewall uit de KPN-dienst. Raadpleeg hiervoor uw AccountManager van KPN.

4.1 Critical, high, medium & low

De advisories van SmartDefense vallen uiteen in de (door Check Point toegekende) categorieën critical, high, medium & low.

Deze categorisering is de neerslag van het oordeel van Check Point tav de ernst van de vulnerability die het betreft: criteria die tot dit oordeel leiden zijn oa:

- aantal kwetsbare systemen in de wereld,
- eenvoud van exploit

4.2 Software

Zowel bij de SmartDefense dienst als de MFWs blijven licentie en abonnement eigendom van KPN en krijgt u gebruiksrecht in het kader van de dienst.

4.3 Handelingen

U verricht de handelingen op de firewall, hetgeen alleen mogelijk is wanneer u de beschikking over een beheer-account op KPN's beheer-omgeving. Die toegang geeft u het recht en de plicht de rule-set én SmartDefense zelf te onderhouden. Indien er problemen zijn, kunt u altijd de hulp van KPN inroepen. Onze 1^e-lijns engineers zullen – met inachtneming van de normale doorlooptijden van 3-5 dagen - de aanpassingen voor u doorvoeren.

Raadpleeg voor meer informatie over 'functioneel beheer door Contractant' (oftewel: klant aan de knoppen) de dienstbeschrijving R9.1 of later.

4.4 Rapportage

De bestaande Managed Firewall rapportage op www.kpn.net wordt uitgebreid met SmartDefense-logging. Deze meldt in het standaard Check Point formaat de gebeurtenissen die aan SmartDefense gerelateerd zijn, zoals de aanvallen waartegen specifiek beschermd wordt. Deze rapportage wordt elk uur ververs (tijdens kantooruren).

5 Het proces

5.1 Als er een advisory binnenkomt

U bewaakt steeds de SmartDefense-berichtgeving van Check Point teneinde direct te kunnen reageren als een advisory/update (hierna advisory) beschikbaar komt. Hiertoe dient u een proces in te richten.

U verwerkt de advisory (of niet) afhankelijk van uw oordeel over de impact van de dreiging op uw situatie.

5.2 Er ontstaat een probleem

Indien de uitvoering van een advisory een probleem veroorzaakt bij de afnemer van de dienst (een applicatie doet het niet meer, het Internetverkeer stopt etc.) kan dit probleem op de normale manier worden aangemeld bij de 1e lijns helpdesk (détails beschikbaar op <http://www.kpn.net> -> support). Het is verstandig hierbij aan te geven dat er een samenhang wordt vermoed met de uitgevoerde advisory. Het probleem zal met voorrang worden behandeld.

5.3 Escalatie

Indien de oplossing van een probleem niet voldoende voortvarend wordt opgepakt naar uw mening, is escalatie mogelijk. De helpdesk kan u hierbij van dienst zijn.

5.4 Security

Zowel de MFWs- als de SmartDefense-dienst zijn qua security diensten die op basis van best-effort worden geleverd. Niemand kan volledige veiligheid garanderen, slechts een optimale prestatie nastreven door de inzet van gekwalificeerde (en gecertificeerde) mensen en gebruik van dito (ITSec, ICSA) componenten van gerenommeerde leveranciers als Check Point, Sun, MessageLabs en Finjan.

Verder is de securitydienstverlening van KPN op onderdelen gecertificeerd door externe partijen tegen de BS7799 / ISO17799.

6 Contract

6.1 Duur

SmartDefense van KPN is een dienst die alleen per heel jaar kan worden afgenomen. Zij kan starten en eindigen onafhankelijk van de looptijd van de Firewall.

6.2 Verplichtingen

Extra verplichtingen van de klant: aanvullend aan de verplichtingen die gelden in het kader van de MFWs-dienst van KPN gelden geen verplichtingen. Klant dient functioneel beheer van de firewall zélf ter hand te nemen.



7 Kosten

De kosten vallen uiteen in een eenmalig en maandelijks bedrag die recht geven op gebruik van het abonnement van Check Point. Eventuele dienstverlening van KPN er omheen wordt separaat afgerekend op dezelfde manier als met reguliere Service Requests (changes) wordt omgegaan.

NB: Het is mogelijk dat het uitvoeren van Smartdefense advisory negatieve invloed heeft op de prestaties van de door KPN geleverde Firewall (voornamelijk bij lichtere platformen). U kunt er dan voor kiezen te upgraden naar een ander hardware platform of een beperktere set aan beveiligingsadviesories te activeren.

Kosten voor een platform upgrade zijn niet inbegrepen bij de dienst en zullen apart in rekening worden gebracht

8 Voorwaarden

Op deze dienst zijn van toepassing de Algemene Voorwaarden voor Managed Firewalls van KPN.