Telenet Security Whitepaper

# Veiliger zaken doen en samenwerken op het internet

Business

# 150 000

Elke dag worden in Europa bijna 150 000 computers besmet met een virus.

# 290 miljard

Symantec raamt de schade van cybercriminaliteit over de hele wereld op 290 miljard euro per jaar.

# 18%

Uit de Eurobarometer-enquête over cyberbeveiliging blijkt dat 18 % van de internetgebruikers minder snel via internet koopt wegens zorgen omtrent cyberbeveiliging.

# 1/4

Volgens Eurostat heeft maar een kwart van de bedrijven een duidelijk ICT-beveiligingsbeleid.

Bron: europa.eu - maart 2014

# Veiliger zaken doen en samenwerken op het internet

## Inhoud

Inleiding

# Benut de kansen, beheer de risico's

Met een performant, snel en betrouwbaar internet kunt u effectiever samenwerken en op nieuwe manieren zakendoen. Bij Telenet zijn we dan ook dag in, dag uit in de weer om u de beste toegang tot het internet te verschaffen. Daarbij hebben we oog voor de risico's die uw connectiviteit —en dus de goede werking van uw bedrijf— in gevaar brengen.

Het internet confronteert ons nu eenmaal ook met bedreigingen als diefstal van data, schending van privacy, virussen en lastercampagnes. De meeste ondernemers zijn zich bewust van de gevaren en van de noodzaak van een degelijke beveiliging. Maar ze weten niet altijd hoe ze zo'n beveiliging moeten aanpakken. Telenet kan helpen. Wij stellen expertise en oplossingen ter beschikking om de risico's te beperken en weg te nemen.

**"Elke onderneming is vandaag kwetsbaar op het internet, ongeacht omvang of activiteit."**

Martine Tempels, Senior Vice-President,
Telenet Business

Zo kan uw bedrijf de kansen die het internet biedt ten volle benutten. Deze whitepaper geeft u alvast inzicht in de risico's, bespreekt oplossingen en producten en laat zien hoe bedrijven in de praktijk met beveiliging omgaan. In het eerste deel legt Xavier Mertens, Principal Security Consultant, uit met welke bedreigingen u vandaag best rekening houdt en aan welke beveiligingsaspecten u zeker niet voorbij mag gaan. In het tweede deel gaan we dieper in op de manieren waarop Telenet u helpt bij de beveiliging van uw connectiviteit en data. Het derde deel bespreekt een aantal beveiligingstechnologieën. Tenslotte laten we u aan de hand van enkele cases zien hoe we werken, welke oplossingen we in praktijk hebben gebracht, en wat het resultaat ervan is.

Wij hopen dat deze informatie zal bijdragen tot een veiliger gebruik van het internet in uw onderneming. Ze is bedoeld voor alle bedrijven, want elke onderneming is vandaag kwetsbaar op het internet, ongeacht omvang of activiteit. Natuurlijk geven we hier geen volledig antwoord op al uw concrete vragen. Dat is onmogelijk. Uw Telenet accountmanager en onze securityspecialisten kunnen wel dieper ingaan op uw specifieke noden.

Wij helpen u graag verder.

Martine Tempels
Senior Vice-President
Telenet Business

# “Elk bedrijf is vandaag een potentieel doelwit”

**“Security is te veel een zaak van securityspecialisten alleen. We moeten meer doen om de eindgebruiker te bereiken”. Dat zegt Xavier Mertens, Principal Security Consultant. Volgens hem is de mens de zwakste schakel in beveiliging en moeten er meer inspanningen geleverd worden om inbreuken een halt toe te roepen. Want het slechte nieuws is: ze gaan in stijgende lijn.**

Xavier Mertens: “Bij het Belgische CERT.be (*Cyber Emergency Team*) heeft men de indruk dat de situatie verslechtert. Internationaal wordt die negatieve trend bevestigd. Het *Data Breach Investigations Report* heeft wereldwijd meer dan 47. 000 veiligheidsincidenten onderzocht en stelt duidelijk dat elke onderneming vandaag een potentieel doelwit is. Het rapport zegt ook dat de snelheid en het vernuft waarmee criminelen te werk gaan, sterk toenemen. Maar verrassend is dat in 78% van de gevallen geen hooggespecialiseerde kennis of speciale middelen nodig waren om bij een bedrijf binnen te dringen. Het rapport geeft aan dat in 84% van de gevallen de criminelen in enkele minuten hun doel al bereikt hadden. Ondernemingen maken van gegevensbeveiliging nog onvoldoende een prioriteit. Dat heeft zeker te maken met de kosten van die beveiliging, die bedrijven liever niet willen maken. Nochtans kunnen de gevolgen van één incident enorm zijn, zowel op de werking van het bedrijf, de financiële situatie als het imago. Daarnaast speelt ook de factor tijd mee. Door concurrentiedruk zet men bijvoorbeeld sterk in op de ontwikkeling van nieuwe producten en verliest men de beveiliging van de onderneming uit het oog.”

## Meer comfort, meer risico’s

“De situatie is des te alarmerender als je weet dat het Internet of Things in volle ontwikkeling is: steeds meer voorwerpen en machines worden via het internet verbonden, waardoor ze onderling of met mensen informatie kunnen uitwisselen. Die evolutie op zichzelf is fantastisch. Zo kan je met je smartphone via mobiel internet je centrale verwarming van op afstand regelen. Gemakkelijk, maar dergelijke verbindingen kunnen ook misbruikt worden. Denk bijvoorbeeld aan kopieermachines in bedrijven. Die hebben tegenwoordig allemaal een IP-adres. Criminelen kunnen via die machines op uw bedrijfsnetwerk raken en data uit het buffergeheugen van de machines lezen. Hebt u gevoelige bedrijfsinformatie gekopieerd, dan bent u die kwijt zonder dat u het beseft.”

## Denk aan veiligheidsaspecten bij outsourcing

"Criminelen proberen het ene bedrijf binnen te raken via het andere. Uw bedrijf kan dus een interessant doelwit zijn, niet op zichzelf, maar omdat u zaken doet met een ander bedrijf. Technologiebedrijven die via *remote access* diensten leveren op een VPN zijn om die reden een geliefd doelwit. Als u zelf met externe IT-leveranciers werkt, zorg dan altijd dat u goed weet waar uw data zich bevinden, hoe de toegang is geregeld en welke personen betrokken zijn. Als u alles goed controleert, is er geen reden tot overdreven paniek. Het *Data Breach Investigations Report* geeft aan dat nieuwe toepassingen, zoals cloud computing, geen grotere risico's met zich meebrengen. Integendeel zelfs. De meeste inbreuken gebeuren nog altijd via klassieke laptops, desktops en servers."

## Mensen blijven zwakste schakel

"Hacking van machines blijft een groot risico, maar een ander én snel toenemend probleem is phishing. Het gaat hier om vervalsingen van echte websites en mails met het doel gevoelige informatie te stelen, zoals kredietkaartnummers of inloggegevens. Phishing kent een enorme vlucht omdat mensen maar blijven klikken op links en buttons zonder zich veel vragen te stellen. Enerzijds zijn er de phishingmails die zo slecht gemaakt zijn dat de meeste mensen wel zien dat het om vervalsingen gaat. Maar doordat die mails naar miljoenen mensen worden gestuurd, werpen ze voor de criminelen toch vruchten af. Het volstaat dat een paar goedgelovigen zich door de mail laten misleiden. Verontrustender voor bedrijven is de trend van *spear phishing*: uitstekende vervalsingen gericht aan specifieke personen. Ze zijn zo goed gemaakt dat ze nog nauwelijks als vervalsing te herkennen zijn. Je denkt dat je te maken hebt met een echte mail van een echte collega. Dikwijls is aan deze mails dan ook maanden voorbereiding voorafgegaan. Bewustmakingsprogramma's zijn heel belangrijk om werknemers op dit soort risico's attent te maken. Ze moeten ook weten dat criminelen tegenwoordig via sociale netwerksites en call centers werken."

**"Uw bedrijf kan een interessant doelwit zijn, niet op zichzelf, maar omdat u zaken doet met een ander bedrijf."**

Xavier Mertens, Principal Security Consultant

Wie medewerkers bewuster maakt van de problematiek, kan al snel meer veiligheid in zijn onderneming tot stand brengen. Wie geen initiatieven neemt, zal uiteindelijk door de wetgever aangemaand worden. Zo lanceerde het Europees Parlement vorig jaar een nieuwe *Data Protection Directive*, die, eenmaal omgezet in wetgeving, bedrijven zal verplichten om *personal data breaches* te melden. Ook zal de Privacycommissie administratieve boetes kunnen opleggen, wat nu nog niet het geval is. Zo'n boete zal niet alleen een financiële straf zijn, maar ook de reputatie van een bedrijf schaden.

## Veel voorkomende gevaren

### Botnets

Overal ter wereld zijn computers besmet zonder dat hun gebruikers daar weet van hebben. Veel van die computers vormen samen een botnet, een netwerk dat vanuit een centraal commandopunt kan aangestuurd worden om te spammen, virussen te verspreiden, ongemerkt data door te sluizen of aanvallen op computersystemen uit te voeren. Botnetcomputers zijn voor een besmet bedrijf nadelig, want ze gebruiken bandbreedte en kunnen een netwerk vertragen. Je kan ook juridisch aansprakelijk gesteld worden, als je computers bij een misdaad betrokken blijken te zijn.

### DDoS attacks

Botnets worden vaak gebruikt om DDoS-aanvallen (*Distributed Denial-of-Service attacks*) uit te voeren. Bij DDoS maken de besmette botnetcomputers gelijktijdig een verbinding met een (web)server. Door het grote aantal gelijktijdige verbindingen wordt die server dan onbereikbaar voor anderen of crasht hij. Zo kunnen systemen van bedrijven en overheidsinstellingen stilgelegd worden.

### Phishing

Phishing is een vorm van *social engineering* waarbij mensen, vaak via mail, naar een valse (bank)website worden gelokt. Aan de nietsvermoedende gebruikers wordt vervolgens gevraagd om inloggegevens, een kredietkaartnummer of andere gevoelige informatie achter te laten.

### Trojaanse paarden

Een Trojaans paard lijkt op een gewoon programma of bestand, maar bevat verborgen functies die toegang tot de besmette computer van buitenaf mogelijk maken. Trojaanse paarden, dikwijls verstuurd als e-mailbijlage, worden gebruikt om wachtwoorden en e-mailadressen te verzamelen of om toegang tot een bankrekening te krijgen. Een Trojaans paard is niet te verwarren met een virus, dat schade toebrengt aan een computer, of een worm die zich van computer naar computer verspreidt.

***Xavier Mertens*** *is Principal Security Consultant. Hij specialiseert zich sinds 2006 in security assessments en audits, beveiligingsarchitectuur en security monitoring. Net als de andere veiligheidsspecialisten van Telenet schoolt hij zich permanent bij. Hij heeft tal van internationaal erkende veiligheidscertificaten verworven.* ***Volg Xavier op blog.rootshell.be***

# Security volgens Telenet

## 01 Beveiliging als continu proces

**Hoe beveiligt u uw connectiviteit, uw data en uw systemen? Op die vraag valt helaas geen eenduidig en simpel antwoord te geven. Elk bedrijf is anders. En geen enkel beveiligingsproduct biedt een volledige pasklare oplossing. Onze security-aanpak verschilt dan ook sterk van die van product resellers.**

### Hier zijn de 7 belangrijkste troeven van onze benadering:

#### 1 Procesmatige aanpak

Telenet ziet beveiliging als een continu proces. Dit proces begint met een assessment of een audit van uw huidige situatie en het analyseren van uw behoeften. Monitoring en bijsturing zijn essentiële onderdelen.

#### 2 Architectuurbenadering

We zijn ervan overtuigd dat beveiliging veel verder moet gaan dan louter producten. Wij kiezen resoluut voor een architectuurbenadering en niet voor technische ad-hoc oplossingen die u, in het beste geval, alleen maar tijdelijk uit de problemen helpen.

#### 3 Partnership in alle onafhankelijkheid

Wij promoten geen producten, maar gaan partnerships aan in functie van wat onze klanten nodig hebben. Zo zijn we als eerste in Europa gestart met Palo Alto Networks. Als enige in België hebben we nu het hoogste partnership voor zowel Palo Alto Networks als Check Point. Het zijn de leiders in het Magic Quadrant van Gartner voor enterprise firewalls. Ons partnership met beide toont dat we een hoog niveau van expertise bezitten, over een grote installed base beschikken en goede back-to-back support verlenen.

### 4 Pragmatisme

Naast firewalling werkt Telenet aan dossiers rond application delivery control, MDM en meer. We pakken die dossiers pragmatisch aan en houden maximaal rekening met wat voor uw omgeving echt van tel is. Onze technische consultants zorgen ervoor dat u ook mee bent met de nieuwigheden. Zij doen tests in ons labo, proberen nieuwe versies uit en houden op tal van andere manieren een vinger aan de pols.

### 5 Doorgedreven kennis en ervaring

Wij hebben sinds 1998 de kennis en ervaring die nodig zijn voor het invoeren en optimaliseren van complexe beveiligingsarchitectuur. In ons Security Competence Center werken meer dan 30 ervaren specialisten met verstand van producten, technologieën en bedrijfsprocessen.

### 6 Open samenwerking

Een groot deel van onze klanten beheert hun oplossingen zelf. Wij zorgen voor training, geven advies en delen onze expertise in regelmatige meetings. Ook wie niet voor managed services kiest, kan bij ons werken met een vast technisch aanspreekpunt. We communiceren regelmatig en houden u bijvoorbeeld via documentatie op de hoogte.

### 7 Comfort

Wie managed services wil, kan kiezen tussen verschillende SLA's (Service Level Agreements). Alles kan voor u geregeld worden: upgrades, policy clean-up, licentiebeheer, documentatie, rapportering, changes enzovoort. Is bijsturing op bepaalde punten nodig, dan geven wij de nodige actiepunten aan. Managed services zijn onder meer voor kmo's zeer interessant omdat zij meestal niet de kennis en infrastructuur bezitten om hun beveiliging zelf te regelen. Bij managed services maakt uw bedrijf gebruik van apparatuur die bij Telenet staat of beheren wij in uw plaats de apparatuur in uw bedrijf.

**"Vroeger moest je bijna een universitair diploma hebben om een veilige VPN-verbinding op te zetten, nu gaat voor onze gebruikers alles seamless."**

Bart Colson, VP IT Operations bij Telenet

**“Security is in de eerste plaats een businesskwestie, alles begint met het in kaart brengen van de grootste businessrisico’s.”**

Eric De Smedt, Manager Cyber Security bij Telenet

# 02 Van security policy naar implementatie

**Telenet biedt niet alleen beveiligingsproducten als Check Point en Palo Alto Networks aan, maar gebruikt ze ook zelf. Bart Colson, VP IT Operations bij Telenet en Eric De Smedt, Manager Cyber Security, over hun aanpak.**

“De *implementatie* van beveiliging is een IT-aangelegenheid, maar verder is security toch in de eerste plaats een businesskwestie”, benadrukt Eric De Smedt. “Beveiliging begint met de businessrisico’s in kaart te brengen, te beginnen met de grootste risico’s. De security policy die daar op het hoogste niveau uit voortvloeit, is een management policy waar je op IT-vlak nog niet veel mee kunt doen. Je gaat hem aanbieden aan de verschillende domeinen in je organisatie en hem zo verder uitwerken in de vorm van vereisten. Daarna ga je controlenormen vastleggen en bepalen hoe je policy compliance gaat controleren. Verder moet je natuurlijk voortdurend je omgeving testen, bijvoorbeeld aan de hand van vulnerability scans.”

## Naadloze verbinding

Operations, de afdeling van Bart Colson, vertaalt de policies en richtlijnen van Cyber Security in technische oplossingen. “We hebben vorig jaar onze infrastructuur globaal herbekeken en Palo Alto Networks geïmplementeerd. Onze hele user community, zo’n 3000 gebruikers, is heel enthousiast over de migratie naar het nieuwe systeem. Vroeger moest je bijna een universitair diploma hebben om een veilige VPN-verbinding op te zetten. Nu gebeurt dat voor onze gebruikers *seamless* in de achtergrond, of je nu van thuis werkt, in een hotel of op kantoor. Valt je pc in sleepmodus, dan ben je nadien toch weer direct vertrokken. Achter dat gebruiksgemak en de transparante omschakeling naar Palo Alto Networks, zit wel heel veel werk in de back-office. Je moet een systeem als Palo Alto Networks zorgvuldig configureren, en daar komt heel wat bij kijken.”

## Vroegtijdige detectie

Bart Colson: “Dankzij Palo Alto Networks  hebben we nu een duidelijker beeld van wie wat doet, en waar. We beheren niet alleen meer de rechten van een gebruiker. We kunnen nu bijvoorbeeld vroegtijdig problemen aanpakken omdat het systeem zelf abnormaal gedrag gaat signaleren. En daarvoor moeten we niet eerst zelf gaan bepalen wat ‘abnormaal’ is. Het systeem doet dat in onze plaats. Dat is heel belangrijk, want er komt vandaag zoveel op ons af dat het onmogelijk is om alle gevaren vooraf te definiëren en in te schatten. Als er iets gebeurt, weten we dat nu onmiddellijk en kunnen we onmiddellijk ingrijpen.”

## Stapsgewijs model

Eric De Smedt: “Veiligheid is voor ons uiterst belangrijk. Wij volgen de internationale norm ISO 27001/2 en moeten, als beursgenoteerd bedrijf met Amerikaanse hoofdaandeelhouder, ook voldoen aan de Amerikaanse SOX-reglementering. Maar ook als je niet aan die strenge normen wilt of kunt voldoen, kan je nog altijd onze stapsgewijze benadering volgen. Zet eerst de strategie uit en kijk dan naar oplossingen. Vergeet ook niet dat een complexe omgeving moeilijker te beveiligen valt. Complexiteit reduceren is dus altijd een goede zaak.”

### Klaar voor IPv6?

In deze tijd, waar het tekort aan IPv4-adressen zich meer en meer laat voelen, besteedt Telenet expliciet aandacht aan IPv6. We zorgen ervoor dat u klaar bent voor de evolutie naar IPv6.

De designs en producten die wij aan onze klanten voorstellen houden al rekening met IPv6 en onze consultants kennen deze materie goed. Vraag hen gerust om uitleg en advies.

**“Dankzij Palo Alto Networks hebben we nu een duidelijker beeld van wie wat doet, en waar.”**

Bart Colson, VP IT Operations bij Telenet

# Van ID-controle tot DDoS-bescherming

Door de overname van C-CURE bezit Telenet expertise inzake beveiligings-technologieën die teruggaat tot 1998. Momenteel tellen we 15 gecertificeer-de security engineers en consultants die samen zeer goed thuis zijn in een brede waaier securitytechnologieën. Telenet werkt onder meer met Check Point, Palo Alto Networks, F5 en andere geavanceerde producten.
Een beknopt overzicht.

## Check Point

Telenet is Platinum-partner van Check Point Software Technologies, een van de marktleiders in next generation firewalling. De oplossingen van Check Point bieden, naast geavanceerde identiteits- en applicatiecontrole, tal van virtualisatiemogelijkheden. Met behulp van zogenaamde software blades kunt u de beveiliging van uw omgeving bovendien volledig op uw specifieke behoeften afstemmen. De modulaire blades kunnen snel geïnstalleerd en geconfigureerd worden.

### Kenmerken

- Identiteitscontrole
- Applicatiecontrole
- Intrusion Prevention System (IPS)
- URL-filtering
- Antivirus
- Antibot
- Threat Emulation
- Beveiligde mobiele toegang tot bedrijfsapps via een SSL-portaalsite en SSL VPN
- Geïntegreerde virtuele firewall (VSX)
- Uitgebreide rapportering met SmartEvent/SmartReporter
- Redundatie-opties (clustering) voor gateway en beheer

### Voordelen

- Gestructureerde policybenadering
- Geschikt voor meerdere platformen
- Uitstekend centraal beheer
- Krachtige malwarebescherming

### Nieuwigheden in Check Point R77

- Threat Emulation blade met bescherming tegen zero-day en ongekende bedreigingen, analyse van vijandig gedrag in een sandbox, en delen van bevindingen via ThreatCloud
- Compliance blade
- HyperSPECT engine met verhoogde performantie

## Palo Alto Networks

Palo Alto Networks ontwikkelde de eerste next generation firewall met een hoogperformante single-pass engine. Het bedrijf blijft ook vandaag zeer vooruitstrevende, geïntegreerde securityoplossingen aanbieden. In 2013 plaatste technologieconsultant Gartner Palo Alto Networks dan ook opnieuw bij de leiders in zijn Magic Quadrant for Enterprise Firewalls. Telenet is Platinum-partner van Palo Alto Networks en Palo Alto Networks Authorized Training Center.

### Kenmerken

- Identiteitscontrole
- Applicatiecontrole
- Intrusion Prevention System (IPS)
- URL-filtering
- Antivirus
- Antispyware
- WildFire-bescherming tegen zero-day en ongekende malware
- GlobalProtect
- IPSec VPN
- Virtualisatie
- Redundatie-opties (clustering) voor gateway en beheer

### Voordelen

- Eenvoudige policy met application based security
- Multiple platforms (50 Mbps tot 20 Gbps)
- Uniform OS cross-platform
- Web-based management
- On-demand reporting
- Eenvoudig licentiemodel

### Nieuwigheden in Palo Alto Networks 6.0

- Wildfire-verbeteringen (nieuwe bestandstypes en OS)
- VM-Series firewall op Citrix SDX
- VM-Series NSX Edition firewall

## Palo Alto Networks Authorized Training Center

Telenet is Palo Alto Networks Authorized Training Center. Wij organiseren onder meer een driedaagse, genormeerde securityopleiding voor gebruikers van Palo Alto Networks.

Ook kunt u vrijblijvend en hands-on kennismaken met de mogelijkheden van Palo Alto Networks tijdens een Ultimate Test Drive workshop.

## F5 BIG-IP

F5 is bekend als specialist in het sneller en beter beschikbaar stellen van applicaties, vooral via load balancing, maar is inmiddels ook een belangrijke speler in security. Met de BIG-IP Application Delivery Controllers (ADC's) van F5 kunt u nu zowel de snelheid, de beveiliging als de beschikbaarheid van applicaties optimaliseren.

**Enkele modules die beschikbaar zijn op de F5 ADC**

- **BIG-IP Local Traffic Manager (LTM)** verbetert uw operationele efficiëntie en garandeert de performantie van uw netwerk, ook tijdens piekbelasting. Gebruik LTM om uw kritische applicaties te beschermen, de downtime te reduceren, uw werkzaamheden te versnellen en voor taken als load balancing en offloading.
- **BIG-IP Access Policy Manager (APM)** maakt authenticatie en single sign-on, ongeacht locatie en toestel, mogelijk. APM consolideert functionaliteiten als remote access, web access management en VDI en vereenvoudigt het beheer van access policies. Uw infrastructuur wordt minder complex, wat de kosten doet dalen.

**"Check Point is heel geschikt voor het beheer op grote schaal van vele firewalls en services."**

Andries De Lombaerde, Senior Security Consultant bij Telenet

- **BIG-IP Application Security Manager (ASM)** omvat een gecertificeerde firewall voor uitgebreide policy-based web application security. Gebruik deze toepassing voor meer visibiliteit, analyse van bedreigingen en voor compliance. ASM is flexibel, performant en schaalbaar.
- **BIG-IP Global Traffic Manager (GTM)** stuurt gebruikers automatisch naar de dichtstbijzijnde of meest performante fysische, virtuele of cloudomgeving. GTM beschermt uw DNS-infrastructuur tegen DDoS en is een volledige realtime DNSSEC-oplossing die u beschermt tegen kaping.

## Kenmerken

### LTM

- Accelereren en optimaliseren van applicaties
- Analyse in realtime
- Load balancing
- SSL-acceleratie en offloading
- Eenvoudige protocolimplementatie
- Protocoloptimalisering
- Sterke beveiliging
- Aangepaste controle
- Virtuele en cloudflexibiliteit
- Hoge performantie en schaalbaarheid

### ASM

- Geavanceerde handhaving
- Preventie van webscraping
- Session awareness en handhaving
- Geïntegreerde XML-firewall
- Dataprotectie en cloaking
- Correlatie van overtredingen en groepering van incidenten
- Automatische updates van attack signatures
- Geolocatie- en reputatiegebaseerde controle

### GTM

- Hoge DNS-performantie en -beveiliging
- DNS caching en resolving
- Volledige DNSSEC-beveiliging
- Globale server load balancing
- Permanente monitoring
- Application health monitoring
- Locatiegebaseerde routering

### APM

- Geschikt voor IPv6
- AAA-serversupport
- Eenvoudige integratie
- Single sign-on (SSO)
- Sterke beveiliging
- Realtime access health data
- Hoge performantie en schaalbaarheid

## Nieuwigheden in BIG-IP

BIG-IP 11.3

- SSL forward proxy
- ICAP services
- Network HSM
- Unified logging framework

Big-IP 11.4

- met flexibele allocatie
- iApps
- Analytics

Big-IP 11.5

- iControl REST Interface
- New anti-DDOS features op ASM
- APM Secure Web Gateway

**“Bij Palo Alto Networks staat de applicatie-controle altijd aan.”**

Bruno Gysels, Security Consultant bij Telenet

## Infoblox

Infoblox is een oplossing voor het centraal beheer van IP-adressen en van DNS en DHCP vanuit IP Addres Management (IPAM). Met Infoblox controleert u alle IP-adressen in uw organisatie. De DNS service van Infoblox biedt DNSSEC en DNS firewall security.

## Pulse Secure Access

Met Pulse Secure Access geeft u mobiele gebruikers beveiligde toegang tot een bedrijfsnetwerk via authenticatie vanop elk web-enabled device. Deze oplossing combineert SSL-beveiliging, standards-based access control en policycreatie op maat.

## Cisco Ironport

Cisco Ironport is een oplossing voor het veilig versturen en ontvangen van e-mails met een dedicated operating system. De antispam- en antivirusmogelijkheden zijn zeer krachtig. U controleert binnenkomende mails op basis van IP-reputatie, beschikt over SPF en domainkey support en kunt Sophos security checks uitvoeren. Cisco Ironport biedt u een volledig en aanpasbaar dashboard voor het opvolgen van alle mailactiviteiten.

## Oplossingen tegen DDoS

Telenet biedt verschillende oplossingen om uw bedrijf te beschermen tegen DDoS aanvallen (Distributed Denial-of-Service attacks):

- Prolexic ('cleaning in the cloud')
- Check Point anti-DDoS appliance
- Arbor Networks Pravail appliance
- Anti-DDoS features op F5 Big IP.

## BlueCoat

BlueCoat biedt u een schaalbare proxyplatformarchitectuur voor veilige webcommunicatie en snelle application delivery. Met ProxySG gaat u op een flexibele en fijnmazige manier na of content, gebruikers, applicaties en protocollen aan uw policies voldoen.

## MobileIron

Met MobileIron beheert u op een gecentraliseerde manier al uw mobiele toestellen, apps en documenten. U bepaalt welke applicaties een werknemer mag gebruiken en welke gegevens geëncrypteerd worden. In geval van verlies of diefstal kunt u apps en data selectief wissen vanop afstand.

**"We zien dat grotere bedrijven die voor vele kleine vestigingen een VPN opzetten, er nu dikwijls onze Secured Internet Breakout bijnemen."**

Bart Van den Branden, Product Manager Security bij Telenet

## Telenet Secured Internet Breakout en SSL VPN

Telenet heeft op basis van zijn jarenlange ervaring met beveiliging ook zelf enkele securityproducten ontwikkeld. Secured Internet Breakout is een op applicaties gerichte next generation firewall voor bedrijven met een VPN. “We zien dat grotere bedrijven die voor vele kleine vestigingen een nieuw VPN opzetten, er nu dikwijls onze Secured Internet Breakout bijnemen”, zegt Bart Van den Branden, Product Manager Security. De oplossing biedt een volledige bescherming tegen inbraak, diefstal, malware en virussen. Ze wordt als een managed service aangeboden en dus door Telenet zelf beheerd. Door Secured Internet Breakout uit te breiden met SSL VPN kunnen ook mobiele gebruikers veilig en eenvoudig op het bedrijfsnetwerk. De beveiliging gebeurt door authenticatie op gebruikersniveau door middel van een token en door versleuteling van de data.

## Belgian Cyber Security Guide


Eind vorig jaar verscheen de allereerste Belgian Cyber Security Guide, een initiatief van onder meer het VBO, de Kamers van Koophandel, EY en Microsoft. De gids bevat aanbevelingen, een security self assessment, cases en een overzicht van de belangrijkste security frameworks en contactadressen. Volgens de gids zijn dit uw 10 ‘must-do’ acties inzake security:

01 Maak gebruikers bewust en leid ze op
02 Hou systemen up-to-date
03 Bescherm uw informatie
04 Beveilig mobiele toestellen
05 Geef alleen toegang tot informatie wanneer dat noodzakelijk is
06 Dwing regels voor veilig surfen af
07 Gebruik sterke wachtwoorden en bewaar ze op een veilige manier
08 Maak en controleer back-ups van uw bedrijfsdata en –informatie
09 Pak virussen en andere malware op een gelaagde manier aan
10 Doe aan preventie, detecteer problemen en reageer

20

**“Telenet bood ons een totaalconcept aan.”**

Rik Van Oost, ICT-manager, AZ Sint-Blasius

04 I Case 01

# Nieuwe firewall bij AZ Sint-Blasius

**Enkele jaren geleden startte AZ Sint-Blasius met een grootschalige vernieuwing van zijn IT-infrastructuur. De capaciteit van het interne netwerk werd uitgebreid en alle thuiswerkers kregen een betere verbinding. Ook de oude firewall werd aangepakt. Rik Van Oost, ICT-manager: “Onze firewall was 6 à 7 jaar oud. Dat is in security ‘hoogbejaard’, zelfs ‘palliatief’. Hij draaide op één server en begon een echte bottleneck te worden. We zijn op zoek gegaan naar een nieuwe oplossing en zijn zo bij Telenet uitgekomen.”**

De IT-afdeling van AZ Sint-Blasius is zoals in andere, vergelijkbare ziekenhuizen, eerder klein. Het ziekenhuis zocht daarom een partner met een totaalbenadering. “Een bedrijf dat zowel voor software, hardware, support als migratie kon instaan”, legt Rik Van Oost uit. “Wij hebben intern noch de tijd noch de kennis om een firewall up-to-date te houden en helemaal zelf op te volgen. Daarin worden we nu ondersteund door Telenet. Zij boden ons een totaalconcept.”

## Totaalconcept

Rik Van Oost: “Telenet helpt ons met regelmatige reviews en zorgt er mee voor dat onze firewall rules coherent blijven. Ook kunnen zij de firewall 24 uur op 24 actief monitoren, wat wij met onze beperkte bezetting onmogelijk kunnen. We hebben eerst samen gekeken naar wat er was, dan de nieuwe hardware ingevoerd, vervolgens de configuratie van de oude firewall overgenomen, dan de rules herbekeken en opgekuist, en uiteindelijk zijn we overgeschakeld. Omdat we het Klinisch Werkstation (KWS) van het UZ Gasthuisberg gebruiken en met de campus ervan via glasvezel verbonden zijn, moesten we ook rekening houden met hun securityvereisten.”

## Thuisgebruikers

Rik Van Oost: "Hadden we vroeger nog wat eilandjes die niet door onze oude firewall gecontroleerd werden, dan gaat alle verkeer nu door onze nieuwe firewalls. We hebben nu één uniforme beveiliging voor iedereen, zonder failures, zonder intrusion van buitenaf en met een betere responstijd. Ook onze 120 zelfstandige en thuiswerkende artsen gaan we langs de nieuwe firewall laten werken." Fréderic Vannieuwenhuyse, ICT-coördinator: "Onze nieuwe beveiliging is volledig redundant met twee firewalls van Check Point. Omdat we geen controle hebben op de computers van thuisgebruikers, zijn daar nog wat compatibiliteitsproblemen, maar die zouden met de introductie van de Mobile Access Software Blade van Check Point ook opgelost moeten raken."

## Procedures

Fréderic Vannieuwenhuyse: "Telenet heeft twee van onze mensen opgeleid, zodat zij de firewall kunnen beheren. Maar het grotere beheer, zoals de updates en de rapportering, laten we aan Telenet over." Nu de firewall goed draait, kan AZ Sint-Blasius zich verder concentreren op het verfijnen van de procedures. Rik Van Oost: "Vanuit de overheid komen heel wat eisen op ons af, zowel wat de communicatie binnen als buiten het ziekenhuis betreft. Door de koppeling met mutualiteiten, de Kruispuntbank en dergelijke zijn we verplicht om ons veiligheidsbeleid nog meer te formaliseren. Die formalisering van de procedures is ook belangrijk omdat we met ons ziekenhuis voor een JCI-accreditering gaan. We moeten kunnen aantonen dat we op elk moment kunnen zien wie tot wat toegang heeft."

---

*Het Algemeen Ziekenhuis Sint-Blasius in Dendermonde, waarvan de wortels tot in 1202 reiken, is een modern centrum voor hoogkwalitatieve medische hulpverlening. Het ziekenhuis kenmerkt zich door zijn vernieuwingsdurf, patiëntgerichtheid en excellentie in minimaal-invasieve technieken. Rond de kernwaarden Veiligheid, Informatie, Comfort, Klinische kwaliteit en Snelheid (VICKS) heeft het bestuur een strategische toekomstvisie uitgebouwd. Het ziekenhuis telt 446 bedden, verdeeld over de campussen in Dendermonde en Zele. Dagelijks zetten meer dan 1.100 mensen zich met hart en ziel in om de patiënten met de allerbeste zorgen te omringen.*

**"Het grotere beheer, zoals de updates en de rapportering, laten we aan Telenet over."**

Fréderic Vannieuwenhuyse, ICT-coördinator, AZ Sint-Blasius

**“Omdat IT niet tot onze core business behoort, besteden we de security van onze omgeving liever uit aan een bedrijf als Telenet.”**

Frank De Winter, CEO en directeur IT van Arista



# Arista: veilig in de cloud

**Grote organisaties die alles in de cloud hebben staan? Ze zijn er. Arista, een externe dienst voor preventie en bescherming op het werk, is er zo een. In de private cloud van de organisatie zitten 800.000 medische dossiers en alle 250 medewerkers maken gebruiken van de infrastructuur. “Ga je zoals wij volledig naar de cloud, dan wordt security wel heel belangrijk”, zegt Frank De Winter, CEO en directeur IT van Arista.**

De beslissing om naar de cloud te gaan, nam Arista toen het autonoom werd. Frank De Winter: “We werkten vroeger samen met HDP en deelden onze infrastructuur met hen. Toen we autonoom werden, kon dat niet meer. We konden toen een migratieproces in gang zetten, maar de impact ervan was moeilijk in te schatten. Migraties zijn kostelijk en risicovol. Hun tijd is eigenlijk voorbij, want je kunt in de cloud makkelijker een nieuwe omgeving opzetten, naast de oude. Het gaat sneller dan migreren en kost minder geld.”

## Beheer en security gescheiden houden

Frank De Winter: “Onze hele ERP-infrastructuur zit in de cloud. Omdat de cloud een gedeelde omgeving is, is onafhankelijke controle heel belangrijk. Daarom dat we, naast onze partner voor het datacenter, een tweede partner voor security hebben gekozen. Als je de twee aan dezelfde leverancier toevertrouwt, verlies je een stuk controle. Om de security van een omgeving als de onze goed te regelen, komen in België maar twee bedrijven in aanmerking. Telenet is een van die twee. Het kan de juiste hardware leveren en installeren, heeft een grondig kennis van

netwerkinfrastructuur, begrijpt de cloudproblematiek enzovoort. Het is security-expertise die je bijna nergens anders vindt. Wij kunnen die ook nooit zelf aantrekken. Omdat IT niet tot onze core business behoort, besteden we de security van onze omgeving liever uit aan een bedrijf als Telenet. Zij bieden ons beveiliging in de vorm van managed services. Dat is gemakkelijk."

## Waarom Telenet?

Bij de keuze voor Telenet speelden niet alleen de expertise en knowhow een rol. Frank De Winter: "Ook de manier van werken. De servicedesk van Telenet behoort tot de beste van België. En Telenet biedt ook de nodige capaciteit. Op drie maanden tijd moesten we van 'niets' tot een volledige ERP-architectuur in de cloud gaan. Dan heb je partners nodig die dit aankunnen. Samen met hen zijn we in ons opzet geslaagd."

---

ARISTA

*Frank De Winter is CEO en directeur IT van Arista, een externe dienst voor preventie en bescherming op het werk. De organisatie doet medisch onderzoek, adviseert organisaties inzake risicobeheer en biedt psychologische bijstand aan werknemers.*

**“De samenwerking met Telenet is gebaseerd op vertrouwen en proactiviteit.”**

Bruno Delcourt, verantwoordelijke voor de dienst Netwerken van de Universiteit van Namen



# Een firewall op maat voor de Universiteit van Namen

**De Universiteit van Namen telt momenteel zes faculteiten, 62 laboratoria, ongeveer 6.400 studenten en een duizendtal onderzoekers. Vandaag de dag zijn vaste en mobiele informaticatools op de Universiteit niet meer weg te denken. “De Universiteit moet haar infrastructuren en technologieën voortdurend aanpassen aan de nieuwste evoluties”, legt Bruno Delcourt, verantwoordelijke voor de dienst Netwerken van de Universiteit van Namen, ons uit.**

“We zien dat het gedrag van de gebruikers in vergelijking met een tiental jaren geleden erg veranderd is. Gewoon hun mailbox kunnen checken volstaat niet meer. Daarnaast is het aantal gebruikers exponentieel toegenomen. Hetzelfde geldt voor het aantal mobiele toestellen die op het netwerk kunnen worden aangesloten. Als je stelt dat elke gebruiker 2 of 3 toestellen heeft, dan komen we uit op een totaal van 13.000 tot 18.000 toestellen die mogelijk kunnen worden aangesloten op het netwerk van de Universiteit. Bovendien willen de studenten ook altijd en overal toegang hebben tot hun gegevens”, aldus Bruno Delcourt. “We hebben voor een nieuwe beveiligingsoplossing gekozen omdat we het gevoel hadden dat de verwachtingen met onze vorige oplossing niet langer werden ingelost. Dat was het momentum! We vonden het tijd om méér te doen dan alleen enkele poorten te controleren”, verduidelijkt hij.

## Een vertrouwenskwestie

“Om er zeker van te zijn dat alles perfect zal werken, is het uiteraard belangrijk om met een goed product te starten, maar dat alleen is niet voldoende. De securitypartner moet ook proactief en bij de pinken zijn. Ook dat is een van de elementen die hebben bijgedragen tot het succes.” Bruno Delcourt heeft de kwaliteit en de waardevolle input van de Telenet-specialisten altijd weten op prijs te stellen, zowel op

technisch als op commercieel vlak. Maar uiteindelijk hebben andere elementen hem overtuigd: de nieuwe next-generation firewall van Palo Alto Networks werd helemaal op maat van de Universiteit geïnstalleerd en er werd een opleiding ter plaatse voorzien.

## Een continu proces

Een netwerk beveiligen is een continu proces dat veel verder gaat dan enkel de technische kenmerken. "Één van de grote uitdagingen bestond erin een infrastructuur en een reeks maatregelen te implementeren die rekening houden met de verscheidenheid van de gebruikers en hun behoeften. Iedereen die actief is op het netwerk moet op een maximale beveiliging kunnen rekenen, en daar tegelijk zo weinig mogelijk hinder van ondervinden", verklaart Bruno Delcourt. "Het netwerk moet voor iedereen relatief makkelijk beschikbaar zijn. Daarvoor is er een goed evenwicht nodig tussen respect voor de individuele vrijheid enerzijds en controle anderzijds. Het belang van de gemeenschap staat immers voorop."

## Opvolging en rapportering

Dankzij de gedetailleerde opvolging en rapportering van de Palo Alto Networks-oplossing kwam er meer transparantie. "De oplossing voert grondige analyses uit, waarbij wordt gecontroleerd of de ingevoerde maatregelen correct werken." Bruno Delcourt is ook bijzonder tevreden over de rapportering: "Zeer vaak volstaan schermafbeeldingen. Ik hoef zelf niet langer tijd te stoppen in de voorstelling van de gegevens. Ook niet-specialisten begrijpen de rapporten gemakkelijk. Zo winnen we enorm veel tijd!"

## Fijnere analyses en naadloze integratie

Met de next-gen firewall van Palo Alto Networks worden doelgerichte acties op het vlak van beveiliging mogelijk. Het systeem voert veel fijnere analyses uit: die wijzen op nieuwe tendensen op het netwerk en maken het mogelijk potentiële bedreigingen te elimineren. "De veranderingen die de nieuwe firewall met zich meebrengt, kunnen we eigenlijk goed vergelijken met een versterkte stad in de Middeleeuwen: die stad is geëvolueerd naar een modernere en meer open stad, maar wordt toch nog op een efficiënte manier gecontroleerd", legt Bruno Delcourt uit. Bovendien zorgt de firewall er ook voor dat de informatie optimaal wordt gesynchroniseerd met de andere systemen en databases die binnen de Universiteit worden ontwikkeld. "Dankzij de nieuwe firewall heeft het volledige netwerk van de Universiteit van Namen aan globaal vermogen en souplesse gewonnen", erkent Bruno Delcourt.

## Positieve feedback

"De feedback van de gebruikers is positief omdat het systeem vrij transparant is gebleven. We blijven bescherming bieden zonder de internetervaring van de gebruikers al te veel te verstoren. Hoe minder zij merken van de beveiligingsoplossingen, des te meer het ons tevreden stelt", glundert Bruno Delcourt. "Dankzij de intuïtieve interface van Palo Alto Networks is het vrij eenvoudig om verschillende netwerkzones te definiëren, die elk voorzien zijn van specifieke beveiligingsmaatregelen. Men kan bepaalde interventies zelfs toevertrouwen aan leden van het team die er niet regelmatig mee werken."

## Resultaten en evoluties

De behaalde resultaten voldoen aan de verwachtingen van de Universiteit. De installatie van de nieuwe Palo Alto Networks-firewall en de integratie ervan met de bestaande tools zijn zonder incidenten verlopen. De verschillende gebruikersprofielen hebben aan comfort en gebruiksgemak gewonnen. Ook het team van Bruno Delcourt heeft zijn skills kunnen perfectioneren. De nieuwe structuur is open en evolutief: "De regels die we hebben ingesteld zijn bruikbaar voor de komende 3 tot 5 jaren. We leggen nu de basis van een systeem waarop we later verder kunnen bouwen", besluit Bruno Delcourt.

> **“Een referentieklant gaf ons positieve feedback over de Telenet-aanpak. Er was geen woord van gelogen.”**
>
> Louis Mahy, CIO Record Bank



# Record Bank zet agenten snel en veilig aan het werk

**Om zijn producten en diensten te promoten, vertrouwt Record Bank op een breed netwerk van zelfstandige agenten. Via een op coax-gebaseerd WAN-netwerk staan zij in contact met de lokale zetels van de bank. “Dankzij de combinatie van IP-VPN en Secured Internet Breakout van Telenet kunnen onze agenten snel en veilig online klantendossiers aanmaken en beheren”, zegt Louis Mahy, CIO bij Record Bank.**

Record Bank ontstond uit de fusie van Sodefina, De Vaderlandsche Spaarbank, SEFB Record Bank en Dipo. In de periode 2001-2006 nam Record Bank vervolgens vier andere spaarbanken over. Hoewel ze het tweede retailnetwerk van ING Bank is, kon Record Bank garen spinnen uit de bankencrisis van 2008. Het volume aan deposito’s nam sinds 2008 toe van 8 tot 14 miljard euro.

## Online diensten voor agentennetwerk

Het feit dat de bank een verschillend model hanteert dan de moederbank, gebaseerd op een netwerk van onafhankelijke agenten en makelaars, is hier niet vreemd aan. Drie lokale zetels in Evere, Luik en Gent, samen 700 interne medewerkers, ondersteunen een netwerk van 700 zelfstandige agenten en 300 makelaars. Zij doen een beroep op de experten van de bank om de gratis rekening, de spaaraanbiedingen en de woon-, auto- en persoonlijke kredieten te promoten. “We willen ons profileren als de beste keuze voor de consument en de lokale handelaar, die op een eenvoudige, veilige en transparante manier willen bankieren”, zegt CIO Louis Mahy. “Als IT-afdeling willen we op ons netwerk online diensten aanbieden en zo bijdragen om het evenwicht te vinden tussen de versnellende groei van internet- en direct banking en de adviesrol van ons netwerk van zelfstandige agenten. Dat is onze grootste uitdaging.”

## Netwerk loskoppelen van internet

"De moderne informatica heeft geleid tot een ruime waaier aan digitale oplossingen in de bankwereld", onderstreept Louis Mahy. IT mag hierbij geen remmende rol spelen, vindt hij, maar moet zich aanpassen aan de veranderende mentaliteit. "Vandaag krijgen we af te rekenen met mobiele toepassingen. Omdat we sinds enkele jaren over een uniek 'Core Banking System' beschikken, kunnen we via ons bestaande platform heel wat distributiekanalen bedienen, zodat we trends als BYOD meteen kunnen integreren."

Eerst nam IT wel het agentennetwerk onder de loep. "Het verhaal van beveiligde VPN-verbindingen over internet op een klassiek ADSL-netwerk liep op zijn einde en de behoefte aan hogere bandbreedtes vroeg om een nieuwe aanpak", aldus Louis Mahy. "We wilden ons netwerk toch wat performanter en internetonafhankelijker maken en we stonden ook voor de migratie van de betaalterminals naar ons eigen netwerk. Ook daar verkozen we niet zomaar over internet te gaan." Telenet stelde voor om een op coax-gebaseerd WAN-netwerk uit te bouwen via de MPLS IP-VPN-backbone, een oplossing die Louis Mahy meteen kon bekoren. "De toegang tot het Telenet-netwerk is niet afstandsgevoelig en biedt daarom gegarandeerde bandbreedte. Bovendien is de oplossing flexibel en vatbaar voor uitbreiding: we kunnen de beginsnelheid van elke site minimaal instellen en zonder on-site interventie connecties upgraden waar nodig."

"Daarnaast had Telenet met Secured Internet Breakout ook de ideale beveiligingsoplossing in huis", gaat Louis Mahy verder. Deze next generation firewall ontwikkelde Telenet speciaal voor bedrijven met VPN. "Met Secured Internet Breakout beheren wij met één oplossing het internetverkeer van al onze agenten. Het stelt ons in staat om ze veilig toegang te geven tot de online applicaties die ze nodig hebben."

Slechts in enkele gevallen bleek het niet mogelijk om een coaxverbinding tot stand te brengen en daar opteerde Louis Mahy voor een VDSL/ADSL2-connectie, die steeds door Telenet beheerd wordt. "Mocht in een kantoor een connectie voor langere tijd uitvallen, dan staan '3G-koffers' in hot stand-by, zodat de agent via een draadloze 3G-connectie toch online blijft."

## Snelle en onberispelijke uitvoering

De 700 agenten werden in zes maanden tijd op het netwerk aangesloten. "De uitrol is perfect te noemen, je merkt dat Telenet die expertise echt onder de knie heeft. Voor Telenet zijn deadlines heilig. In de piek realiseerden we tot 50 aansluitingen per week." Louis Mahy is onder de indruk van de snelheid van Telenet, bij de uitvoering maar ook bij de rapportering. "Het projectbeheer is uitstekend en het accountteam heeft toegang tot de bedrijfstop. Dat versnelt de besluitvorming en de soepelheid bij de uitvoering. Kwalitatieve overeenkomsten inzake dienstenniveau (SLA's) worden bovendien aangevuld met accurate opvolging en snelle en lokale support van beslagen technici. Tijdens een bezoek aan een referentieklant van Telenet kregen we positieve feedback over de Telenetaanpak. Er was geen woord van gelogen."

---

Record
recordbank.be

*Als dochteronderneming van ING focust Record Bank op de Belgische markt van basisbankproducten. Particulieren, zelfstandigen en kleine bedrijven kunnen er terecht voor hun financiële behoeften. Met 12 miljard euro aan uitstaande leningen staat Record Bank in voor 7% van de Belgische hypotheekmarkt. Samen met moederbank ING wil ze de eerste plaats innemen voor wat betreft leningen op afbetaling. Ongeveer 800.000 klanten openden samen al ongeveer 1 miljoen rekeningen bij Record Bank. Van de 350.000 zichtrekeningen met gratis bankkaart zijn er bijna 200.000 die geregeld gebruikt worden bij internetbankieren.*

# Veiliger zaken doen en samenwerken op het internet

Telenet helpt u om beter zaken te doen op het internet en wij zorgen ervoor dat uw medewerkers digitaal vlot met mekaar kunnen samenwerken. Maar we willen ook dat uw bedrijf in complete veiligheid kan werken. Daarom hebben we specifieke beveiligingsoplossingen voor kmo's met een beperkt budget ontwikkeld en hebben we specialisten die de meest complexe securityvraagstukken van grote ondernemingen aan kunnen. Lees in deze whitepaper waarom beveiliging zo belangrijk is en hoe wij u kunnen helpen. Telenet is thuis in firewalling, antispam en antivirus, malwaredetectie, pentests, auditing, vulnerability scanning en meer.

**0800 66 066**
**telenet.be/business**

Business

V.U.: Telenet n.v., Liersesteenweg 4, 2800 Mechelen Versie juli 2015