



# Beveiliging voor ondernemers



# Inleiding

Voor u ligt een boekje over netwerkbeveiliging. Beveiliging is één van de meest urgente problemen in het bedrijfsleven.

Uit Nederlands onderzoek blijkt dat 64% van de middelgrote en kleine bedrijven in hoge mate afhankelijk is van ICT en internet, maar dat 80% geen gestructureerd beveiligingsbeleid heeft. In dit boekje kunt u lezen hoe u de beveiliging van uw bedrijf wél gestructureerd kunt aanpakken.

Aan de hand van een groeiscenario laten wij u zien welke stappen u moet nemen als uw bedrijf nieuwe diensten gaat ontwikkelen waarbij u intensiever gebruik gaat maken van internet. U leest hoe een Cisco Self Defending Netwerk is opgebouwd en welke producten zich het best lenen voor uw specifieke situatie en bedrijfsomvang. In het laatste deel leest u meer over de Cisco MKB Business Partner services en aantrekkelijke financieringsopties.

Cisco helpt mensen en bedrijven om op een slimmere, veiligere en efficiëntere manier te werken. Door uw problemen centraal te stellen, zijn wij in staat technologie te ontwikkelen die uw bedrijf verder helpt. Wij kijken altijd eerst naar uw bedrijfsvraagstukken en bepalen aan de hand daarvan welke technologie zich het best leent om die aspecten te verbeteren. Specifiek daarom heeft Cisco een Smart Business Communications Aanpak ontwikkeld, een stappenplan dat u stap voor stap helpt bij het realiseren van vier belangrijke bedrijfsdoelstellingen: verhogen van de productiviteit, verlagen van de kosten, beter reageren op de klant en beveiligen van uw bedrijfskritische informatie.

In deze serie is een boekje verschenen over de Cisco Smart Business Communications Aanpak. Daarin leest u alles over deze methode. De andere boekjes in deze serie behandelen de onderwerpen Unified Communications voor ondernemers, draadloos werken voor ondernemers, en Routing & Switching voor ondernemers. Kijk voor meer informatie op de Cisco MKB website: [www.cisco.nl/mkb](http://www.cisco.nl/mkb)



# Inhoud

- 5 Groeiende beveiligingsrisico's
- 8 Hoe kan het ook?
- 10 De onderdelen van een Cisco Self Defending Network
- 16 Voorbeelden Cisco beveiligings-oplossingen
- 22 Onze dienstverlening aan u



## Groeiende beveiligingsrisico's

### Informatiebeveiliging grootste uitdaging MKB

Uit onderzoek blijkt dat informatiebeveiliging de grootste uitdaging is waarvoor ondernemingen tot 250 medewerkers zich geplaatst zien.

Het is nog niet zo lang geleden dat het merendeel van de bedrijven een inbelverbinding had. Tegenwoordig heeft vrijwel iedere onderneming een vaste verbinding, waardoor het bedrijf continu blootstaat aan bedreigingen zoals virussen, wormen en andere netwerkindringers. We noemen hier een aantal aspecten die invloed hebben op de beveiligingmaatregelen die u zou moeten nemen.

### E-commerce

E-commerce is sterk in opkomst: steeds meer bedrijven hebben een website waarop klanten transacties kunnen doen. De website is geëvolueerd van online brochure naar transactiemedium. Dat stelt echter specifieke eisen aan de beveiliging, niet alleen van de website maar van uw gehele ICT-omgeving.

### Online software

Hosted diensten worden steeds populairder. Daarbij kunt u software afnemen als online dienst vergelijkbaar met internetbankieren. Met name boekhoudsoftware en klantenbeheersystemen worden volop op deze wijze aangeboden. Dat betekent dat bedrijfskritische informatie zoals financiële gegevens en klantinformatie op een server bij de dienstverlener wordt opgeslagen en via internet toegankelijk is voor alle medewerkers met een gebruikersnaam en wachtwoord. Zonder goede beveiliging kunnen die gegevens gemakkelijk op straat komen te liggen.



## Mobiel werken

De risico's nemen tevens toe doordat medewerkers steeds vaker mobiel willen werken. Ze nemen hun laptop van de zaak mee naar huis. Het netwerk thuis is vaak niet of matig beveiligd. De draadloze verbinding staat vaak wagenwijd open, met alle risico's van dien voor de bedrijfskritische informatie die zich op de laptop bevindt.

De toegenomen populariteit van mobiel werken betekent ook dat zakenrelaties een verloren kwartiertje graag willen benutten om bij u op kantoor de laptop even aan te zetten om hun e-mail te checken. U weet niet welke virussen, wormen of spyware op deze manier uw bedrijfsnetwerk binnenkomen. Dit soort geavanceerde diensten vraagt om een geavanceerde beveiliging.

## Spam

Een ander groot risico is spam. Niet alleen komt er zoveel ongevraagde mail binnen dat medewerkers gemakkelijk een belangrijk mailtje over het hoofd zien, ook worden uw servers onnodig belast. Spamfilters kunnen gelukkig steeds beter filteren, maar het is niet de bedoeling dat een spamfilter goede berichten tegenhoudt. Spamfilters moeten de juiste berichten tegenhouden. Daarnaast leidt spam mensen ook vaak naar webcontent met spyware en andere malware wat een bijkomend risico is.

## Wet- en regelgeving

De steeds veranderende bedreigingen voor de beveiliging, zowel van binnen als van buiten het bedrijfsnetwerk, kunnen ernstige gevolgen hebben voor de bedrijfsactiviteiten en daarmee voor de winstgevendheid en klanttevredenheid. Daarnaast moet u voldoen aan nieuwe regels en wetten ter bescherming van persoonsgegevens en beveiliging van elektronische transacties, die enerzijds door de EU worden opgelegd en anderzijds door de Nederlandse overheid of door brancheverenigingen. Een voorbeeld hiervan is de Payment Card Industry (PCI) Data Beveiliging Standard, die geldt voor alle bedrijven die met credit card transacties te maken hebben.

## Kosten

Als er wordt ingebroken op een netwerk brengt dat zowel zichtbare als onzichtbare kosten met zich mee. De meeste inbreuken op de beveiliging, zoals een virus op een pc, veroorzaken relatief weinig schade. De kosten die ermee gemoeid zijn, zijn vooral de tijd om het virus van de geïnfecteerde systemen te verwijderen en de daarmee gepaard gaande verloren werktijd omdat een werknemer moet wachten totdat zijn computer is geschoond.

Ernstiger wordt het wanneer het gehele netwerk dermate geïnfecteerd raakt dat het uitvalt. In dat geval is er niet alleen sprake van verloren werktijd, maar ook van gemiste orders, weggelopen klanten en een verslechterde reputatie.

De grootste schade als gevolg van slechte beveiliging ontstaat vaak bij diefstal of uitlekken van gegevens. Als uw klantenbestand op straat komt te liggen, is de kans groot dat dit de publiciteit haalt, met alle imagoschade van dien, om nog maar niet te spreken over de kans op een rechtszaak die klanten tegen u kunnen aanspannen. Bij een retailketen die e-mailadressen van klanten verzamelt om ze regelmatig een mailing te kunnen sturen, zal de schade van het uitlekken van gegevens meevallen, bij een incassobureau of a accountantskantoor is het vertrouwen dat klanten hebben natuurlijk volledig weg.

# Hoe kan het ook?

## Cisco Self Defending Network

Niemand kan voorspellen wat de toekomst in petto heeft. Wel is duidelijk dat hoe meer onze economie afhankelijk wordt van computernetwerken, hoe interessanter deze netwerken worden voor criminelen, spammers en andere niet gewenste gasten. De beste verdediging is er een die zich gemakkelijk aanpast aan toekomstige bedreigingen en die niet te kostbaar is.

Beveiliging is geen probleem dat eenmalig kan worden opgelost. Een bedrijf dat weinig zakendoet via internet en alleen intern communiceert, heeft een heel andere beveiliging nodig dan een bedrijf dat grotendeels afhankelijk is van internet, bijvoorbeeld een webwinkel. Dat betekent dat u bij iedere nieuwe dienst die u ontwikkelt of afneemt, na moet gaan welke impact dat heeft op de beveiligingsrisico's en welke stappen u zou moeten nemen. Denkt u erover om online software af te nemen? Inventariseer dan eerst welke risico's dat met zich meeneemt. Wilt u uw medewerkers vanuit huis toegang geven tot uw bedrijfsnetwerk? Idem dito.

Stel uw bedrijf heeft de laatste jaren internet ontwikkeld tot belangrijk verkoop- en communicatiekanaal. U heeft uw netwerk daarop aangepast. Bij iedere uitbreiding heeft u gekozen voor producten waarin beveiliging geïntegreerd is. Toen uw website zich ontwikkelde van online brochure naar productcatalogus met bestelmogelijkheid heeft u gekozen voor geïntegreerde routers en switches die niet alleen zorgen voor snelle communicatie, maar die door ingebouwde beveiligingsfunctionaliteit uw netwerk ook in de verschillende netwerklagen optimaal beveiligen. Toen u een draadloos netwerk implementeerde, bent u op dezelfde manier te werk gegaan en heeft u gekozen voor wireless access points en een wireless LAN controller met ingebouwde beveiliging. Nu ook alle medewerkers thuis kunnen inloggen op het bedrijfsnetwerk, heeft u het netwerk uitgebreid met VPN-connectiviteit waardoor medewerkers via een beveiligde verbinding thuis kunnen werken.

Alle onderdelen waaruit uw netwerk bestaat, werken nauw met elkaar samen om informatie uit te wisselen en de beveiliging verder te verbeteren en kunnen vanuit een enkel punt beheerd worden. Ze waarschuwen elkaar van het bestaan van een nieuwe dreiging. Ze herkennen een mogelijk gevaar omdat ze zijn uitgerust met software voor innovatieve gedragsherkenning, die dreigingen identificeert. Herkennen ze een nieuw virus of identificeren ze een aanval van een hacker, dan ontwikkelen de netwerkdelen razend-snel nieuwe verdedigingsmechanismen. Het netwerk is zowel van binnenuit als van buitenaf beveiligd.

Uw IT-medewerker is blij dat hij niet bij nacht en ontij wordt gewaarschuwd en in actie hoeft te komen. Dit bespaart hem de nodige tijd en stress. Doordat de beveiliging grotendeels is geïntegreerd in de netwerkdelen die hij toch al moet beheren, kost het onderhoud van de beveiliging-omgeving hem nauwelijks extra tijd. Hij heeft daarnaast gekozen voor een separaat beveiligingsplatform dat overzicht over alle beveiligingsonderdelen en -functies. Dit bespaart hem nog meer tijd.

Met een Cisco Self Defending Network bent u voorbereid op alle wet- en regelgeving op het gebied van integriteit van financiële data en bescherming van de privacy van uw klantgegevens. Ook bespaart u fors op kosten die gerelateerd zijn aan een virusuitbraak of gegevensdiefstal. De kans daarop is immers geminimaliseerd.



# De onderdelen van een Cisco Self Defending Netwerk

De stappen die u dient te nemen om uw eigen bedrijf te beveiligen, zijn uiteraard geheel afhankelijk van uw situatie, dat wil zeggen de manier waarop u zakendoet. Een webwinkel loopt tegen andere problemen aan dan een bedrijf dat buiten e-mail nauwelijks gebruikmaakt van internet. Ook zijn de toekomstplannen belangrijk om in overweging te nemen. Toch is er een aantal standaardstappen te definiëren. Cisco werkt samen met een landelijk netwerk van lokale MKB Business Partners die u kunnen helpen door onderstaand stappenplan heen te gaan:

- **Stap1. Inventariseren**

Test je eigen vaardigheden en kennis en die van medewerkers/collega's en bepaal of er hulp nodig is. Ga na welke apparatuur en informatie beschermd moet worden, inclusief de hardware, software en papieren documentatie. Bepaal met welke bedreigingen en risico's het bedrijf te maken kan krijgen en welke maatregelen reeds getroffen zijn.

Maak een prioriteitenlijst van zaken die beveiligd moeten worden.

- **Stap2. Plannen**

Schrijf procedures over hoe bedreigingen voorkomen en opgespoord kunnen worden, en hoe erop gereageerd moet worden. Maak ook in de organisatie duidelijk wie verantwoordelijk is voor het uitvoeren en controleren van deze procedures. Stel een tijdschema op voor de implementatie. Zorg ook voor afspraken en regels voor werknemers over hoe zij om moeten gaan met bedrijfscomputers en -netwerk, internet, e-mail enzovoort.

- **Stap3. Uitvoeren**

Voer de plannen uit en introduceer het beleid. Communiceer over de voortgang naar de werknemers en praat er met hen over. Bied hen waar nodig ook trainingen aan.

- **Stap4. Controleren**

Controleer regelmatig of de procedures en afspraken worden gevolgd en of bijsturing nodig is. Wanneer er veranderingen optreden in personeel, hardware of software kan het namelijk noodzakelijk zijn plannen aan te passen.

- **Stap5. Herhalen**

Een incident kan reden zijn om de plannen en procedures te herzien.

Maar sowieso kan het geen kwaad om met regelmaat (bijvoorbeeld jaarlijks) de plannen en procedures te evalueren en waarnodig aan te passen. Blijf de mogelijke bedreigingen inventariseren om de beveiliging optimaal te houden.

## Smart Business Communications Aanpak

Beveiliging maakt het mogelijk om IT op een efficiënte manier te kunnen gebruiken. En IT op zijn beurt maakt het weer mogelijk dat bepaalde bedrijfsdoelstellingen kunnen worden gehaald, en dat is waar het uiteindelijk om draait.

Om de IT-plannen af te stemmen op de prioriteiten van uw bedrijf biedt Cisco een Smart Business Communications Aanpak: een geïntegreerd bedrijfs- en technologieplan dat ervoor zorgt dat de IT-omgeving meegroeit met uw bedrijf en dat de beveiliging ervan is afgestemd op de situatie.

Om groeiende ondernemingen door elke ontwikkelingsfase te leiden – beginfase, groeifase en geoptimaliseerde fase – biedt de Cisco Smart Business Communications Aanpak een benadering die bestaat uit drie fases. In de eerste fase wordt de Secure Network Foundation gelegd: een basisbeveiliging die voldoende is voor bedrijven die buiten e-mail nauwelijks

gebruikmaken van internet en die een uitstekende basis biedt om in een later stadium beveiligingsfuncties aan toe te voegen. In de tweede fase ontstaan nieuwe risico's doordat medewerkers ook vanuit huis toegang willen tot het bedrijfsnetwerk en doordat klanten via internet bestellingen bij u plaatsen. De maatregelen in deze fase zijn daarop afgestemd. In de derde fase is internet een belangrijke levensader van uw bedrijf. U past uw netwerk daarop aan door het zo in te richten dat het zichzelf kan verdedigen. Daarnaast gaat u uw applicaties en data via het web ontsluiten. Cisco noemt dit een Self Defending Network.

## Cisco Self Defending Network

Het Cisco Self Defending Network is een geavanceerde beveiligingsoplossing waarmee uiterst betrouwbare, zichzelf verdedigende netwerken worden gebouwd. De beveiliging is voor een groot deel ingebouwd in de al aanwezige netwerkcomponenten, zoals routers en switches. Door deze geïntegreerde benadering bent u er niet alleen zeker van dat uw netwerk op alle onderdelen is beveiligd, het vergemakkelijkt ook nog eens de installatie, onderhoud en beheer. Een Self Defending Network is in staat zichzelf aan te passen aan nieuwe omstandigheden. Het kan bijvoorbeeld zelf nieuwe verdedigingsmechanismen ontwikkelen. Daardoor hoeft uw systeembeheerder of Cisco MKB Business Partner niet in actie te komen als er een nieuwe dreiging ontstaat.

## Onderdelen geïntegreerde beveiligingsstrategie

Het Cisco Self Defending Network bestaat uit verschillende onderdelen:

- **Firewall:**  
firewalls en IPS-voorzieningen bij ieder toegangspunt op het netwerk houden wormen, spyware en hackers tegen zodat er geen informatie van het bedrijfsnetwerk kan worden gestolen. Bovendien kan met firewalls worden voorkomen dat gebruikers binnen het bedrijf toegang krijgen tot gevoelige informatie. Interne firewalls kunnen zo worden ingesteld dat onbevoegde werknemers geen toegang kunnen krijgen tot bijvoorbeeld de computers van de financiële afdeling, personeelszaken of de boekhouding. Ook kan het gegevensverkeer niet worden bekeken.
- **Cisco Intrusion Prevention Systems (IPS):**  
deze zijn beschikbaar in beveiligingsapparatuur, routers en switches van Cisco. Ze scannen en inspecteren real-time al het binnenkomende verkeer op zoek naar onregelmatigheden die kunnen wijzen op een aanval. Als er een onregelmatigheid wordt geconstateerd, schat het IPS de ernst van het risico in en vindt vervolgens communicatie plaats met andere netwerkonderdelen met beveiligingsfunctionaliteit om de bedreiging bij de bron onschadelijk te maken en te verhinderen dat deze zich door het netwerk verspreidt. Een IPS is het best te vergelijken met een alarmfunctie in huis: het slot op de voordeur is de firewall, de IPS het alarm. Mocht er ondanks het slot op de deur een inbraak plaatsvinden, dan zorgt de IPS ervoor dat inbrekers worden gesignaleerd en gepakt.

- **Virtual Private Networks (VPN):**

door middel van deze technologie kunnen kleine vestigingen en externe werknemers (thuiswerkers) volkomen veilig met elkaar en met het hoofdkantoor communiceren, zelfs wanneer ze dat via het openbare internet doen. Gebruikersverificatie zorgt ervoor dat alleen bevoegde gebruikers toegang krijgen tot het VPN-netwerk. Encryptie garandeert dat de gegevens onleesbaar zijn voor iedereen die de VPN-communicatie via het openbare netwerk probeert te onderscheppen. Thuiswerkers kunnen gebruik maken van een VPN oplossing zonder dat zij hiervoor software hoeven te installeren op de PC (web VPN). Via de browser ontsluiten we outlook, bestanden en bedrijfsapplicaties.

- **Cisco Secure Desktop:**

deze technologie beveiligt alle 'eindpunten' die aan het netwerk verbonden zijn zoals PC's, laptops, IP-telefoons en printers. Cisco Secure Desktop voorkomt dat gegevens zoals cookies, browsergeschiedenis, tijdelijke bestanden en gedownload content worden achtergelaten als de verbinding wordt verbroken.

- **Virtuele LANs (VLANs):**

hiermee kan de interne communicatie van een bedrijf verder worden gesegmenteerd. Gevoelige financiële informatie of klantgegevens kunnen in een virtueel afgescheiden LAN worden geplaatst, dat geheel gescheiden is van de LAN's waarop de werknemers werken.

- **Anti-X beveiling:**

deze functionaliteit biedt anti-virus, anti-spyware, anti-spam, URL filtering en scanning van pagina's.

- **Network Admission Control:**

deze functionaliteit controleert alle apparatuur die op het netwerk wil inloggen op de aanwezigheid van onder meer virussen en spyware en checkt of de apparatuur is voorzien van de laatste anti-virus updates.



# Voorbeelden Cisco beveiligings-oplossingen

In dit hoofdstuk vindt u een aantal voorbeelden van een Cisco beveiligings-oplossing. Deze overzichten dienen om een indruk te geven van de producten waaruit de oplossing kan worden opgebouwd en de functionaliteiten die kunnen worden toegevoegd. Voor de juiste oplossing voor uw bedrijf adviseren we u om contact op te nemen met een Cisco MKB Business Partner. Zij adviseren u graag en terzakekundig.

## MKB-bedrijven tot 50 medewerkers

Voor een bedrijf tot 50 medewerkers heeft Cisco de ASA5505 ontwikkeld.

Deze herbergt de volgende functies:

- Netwerkinfrastructuur: 8 poorten (waarvan twee met power over ethernet) waarop switches (eventueel met vlan's) kunnen worden aangesloten
- Firewall met diepgaande inspectie voor bijvoorbeeld instant messaging (doorvoer tot 150 Mb/s)
- VPN remote access server om gebruikers via Internet een veilige verbinding op te laten zetten naar het interne netwerk.  
Voor zowel IPsec VPN's als Web VPN (SSL VPN), doorvoer tot 100 Mb/s.
- VPN site-to-site om VPN's op te zetten tussen verschillende vestigingen, doorvoer tot 100 Mb/s
- Toekomstige mogelijkheid voor uitbreiding van functies
- Geïntegreerd beheer voor alle beveiligingsfuncties. Hiermee kan de ASA5505 eenvoudig worden ingesteld. Tevens kan nauwlettend worden bekeken welke beveiligingsrisico's zich voordoen.

## Tot 10 gebruikers

| ASA5505 firewall en VPN |   |
|-------------------------|---|
| ASA5505-BUN-K9          | ASA 5505 oplossing met SW, 10 gebruikers, 8 poorten, 3DES/AES                                 |
| ASA5505-SEC-PL          | ASA 5505 Sec. Plus Lic. met HA, DMZ, VLAN trunk, meerdere aansluitingen.                      |
|                         | optioneel: alleen nodig voor support van DMZ zone, VLAN's en ISP backup                       |
| ASA5500-SSL-10          | ASA 5500 SSL VPN 10 User License  |
|                         | optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dat uit tot 10 |

## Tot 50 gebruikers

| ASA5505 firewall en VPN |   |
|-------------------------|---|
| ASA5505-50-BUN-K9       | ASA 5505 oplossing met SW, 50 gebruikers, 8 poorten, 3DES/AES                                 |
| ASA5505-SEC-PL          | ASA 5505 Sec. Plus Lic. met HA, DMZ, VLAN trunk, meerdere aansluitingen.                      |
|                         | optioneel: alleen nodig voor support van DMZ zone, VLAN's en ISP backup                       |
| ASA5505-SSL25-K9        | ASA 5505 VPN Editie met 25 SSL gebruikers, 50 Fire Wall gebruikers, 3DES/AES                  |
|                         | optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dat uit tot 25 |

## Ongelimeerd aantal gebruikers

| ASA5505 firewall en VPN |   |
|-------------------------|---|
| ASA5505-UL-BUN-K9       | ASA 5505 oplossing met SW, ongelimeerd aantal gebruikers, 8 poorten, 3DES/AES                 |
| ASA5505-SEC-PL          | ASA 5505 Sec. Plus Lic. met HA, DMZ, VLAN trunk, meerdere aansluitingen.                      |
|                         | optioneel: alleen nodig voor ondersteuning van DMZ zone, VLAN's en ISP backup                 |
| ASA5505-SSL25-K9        | ASA 5505 VPN Editie w/ 25 SSL Users, 50 Fire Wall Gebruikers, 3DES/AES                        |
|                         | Optioneel: standaard licentie gaat tot 2 SSL VPN sessies, deze licentie breidt dat uit tot 25 |

## MKB-bedrijven tussen de 50 en 250 medewerkers

Voor een bedrijf tussen de 50 en 250 medewerkers heeft Cisco de ASA5510 ontwikkeld. Deze herbergt de volgende functies:

- Netwerkinfrastructuur: 4 poorten waarop switches (eventueel met vlan's) kunnen worden aangesloten
- Firewall met diepgaande inspectie voor bijvoorbeeld instant messaging (doorvoer tot 300 Mb/s)
- VPN remote access server om gebruikers via Internet een veilige verbinding op te laten zetten naar het interne netwerk. Voor zowel IPsec VPN's als Web VPN (SSL VPN), doorvoer tot 170 Mb/s.
- VPN site-to-site om VPN's op te zetten tussen verschillende vestigingen, doorvoer tot 170 Mb/s
- Mogelijkheid voor uitbreiding van functies met behulp van secure services module kaarten zoals:

### **Intrusion Prevention Service:**

om kwaadaardig verkeer, inclusief wormen en netwerk virussen te detecteren en stoppen voordat ze uw netwerk kunnen beïnvloeden.

### **Anti-X beveiliging:**

biedt anti-virus, anti-spyware, anti-spam, URL filtering en scanning van pagina's.

- Geïntegreerd beheer voor alle beveiligingsfuncties. Hiermee kan de ASA5510 eenvoudig worden ingesteld. Tevens kan nauwlettend worden bekeken welke beveiligingsrisico's zich voordoen.



## Voor meer dan 50 gebruikers

| ASA5510 firewall en VPN |   |
|-------------------------|---|
| ASA5510-BUN-K9          | ASA 5510 oplossing met SW, 3FE, 3DES/AES  |
| ASA5510-SEC-PL          | ASA 5510 Security Plus Licentie w/ A/S HA, meer VLANs + aansluitingen                         |
|                         | optioneel: voor support van hoge beschikbaarheid, 5 10/100 ethernet poorten                   |
| ASA5510-SSL50-K9        | ASA 5510 VPN Editie met 50 SSL Gebruikers Licentie, 3DES/AES                                  |
|                         | optioneel: standaard licentie gaat tot 2 ssl vpn sessies, deze licentie breidt dat uit tot 50 |

## Voor meer dan 50 gebruikers

| ASA5510 firewall en VPN, en Anti-X module |  |
|---|--|
| ASA5510-CSC10-K9                          | ASA 5510 oplossing met CSC10, SW, 50 gebruikers AV/Spy, 1 jaar registratie   |
| ASA5510-SEC-PL                            | ASA 5510 Security Plus Licentie met A/S HA, meer VLANs + aansluitingen   |
|   | optioneel: voor ondersteuning van hoge beschikbaarheid, 5 10/100 ethernet poorten, aantal vlans wordt verhoogd van 50 naar 100                             |
| ASA5510-SSL50-K9                          | ASA 5510 VPN Editie met 50 SSL Gebruikers Licentie, 3DES/AES   |
|   | optioneel: standaard licentie gaat tot 2 ssl vpn sessies, deze licentie breidt dat uit tot 50  |
| ASA-CSC10-PLUS                            | ASA 5500 CSC SSM10 Plus Lic. (Spam/URL/Phish, 1Yr Subscript)   |
|   | optioneel: Anti-X module ondersteunt standaard anti-virus en anti-spyware, dit breidt de mogelijkheden uit met anti-spam, anti-phishins. Content filtering |
| ASA-CSC10-USR-100                         | ASA 5500 Content Security SSM-10 100 Gebruikers Licentie   |
|   | optioneel: anti-x module ondersteunt standaard 50 actieve gebruikers, dit breidt dat aantal uit tot 100  |

## Voor meer dan 50 gebruikers

| ASA5510 firewall en VPN, en IPS module |  |
|--|--|
| ASA5510-AIP10-K9                       | ASA 5510 oplossing met AIP-SSM-10, SW, 3FE, 3DES/AES   |
| ASA5510-SEC-PL                         | ASA 5510 Security Plus Licentie met A/S HA, meer VLANs + aansluitingen   |
|  | optioneel: voor ondersteuning van hoge beschikbaarheid, 5 10/100 ethernet poorten, aantal vlans wordt verhoogd van 50 naar 100                             |
| ASA5510-SSL50-K9                       | ASA 5510 VPN Editie met 50 SSL Gebruikers Licentie, 3DES/AES   |
|  | optioneel: standaard licentie gaat tot 2 ssl vpn sessies, deze licentie breidt dat uit tot 50  |
| ASA-CSC10-PLUS                         | ASA 5500 CSC SSM10 Plus Lic. (Spam/URL/Phish, 1 jaar registratie)  |
|  | optioneel: Anti-X module ondersteunt standaard anti-virus en anti-spyware, dit breidt de mogelijkheden uit met anti-spam, anti-phishins. Content filtering |
| ASA-CSC10-USR-100                      | ASA 5500 Content Security SSM-10 100 Gebruikers Licentie   |
|  | optioneel: anti-x module ondersteunt standaard 50 actieve gebruikers, dit breidt dat aantal uit tot 100  |



# Onze dienstverlening aan u

## Cisco MKB Business Partners

Cisco werkt samen met een landelijk netwerk van in totaal 250 regionale MKB Business Partners. Het doel van onze MKB Business Partners is om u een zo goed mogelijke klantervaring te bieden. Van nuttige trainingen tot betrouwbare en waardevolle ondersteuning. De partners van Cisco zijn specialisten die precies weten hoe ze het beste uit uw netwerkinfrastructuur kunnen halen op het gebied van Routing & Switching, Unified Communications, draadloos en beveiliging. Daarnaast hebben zij diepgaande kennis en expertise op het gebied van ontwerp, implementatie, service en onderhoud. Ze kunnen u helpen om uw infrastructuur zo op te zetten dat deze perfect past bij de specifieke eisen die uw bedrijf daaraan stelt. Zodat u uw doel kunt bereiken.

## Cisco Services: SMARTnet & MKB Support Assistent

Cisco biedt twee services: SMARTnet en MKB Support Assistent.

SMARTnet staat voor Software Maintenance Advance Replacement en Technical assistance. Dit betekent dat in geval apparatuur stuk gaat, deze de volgende werkdag wordt vervangen. U profiteert van voortdurende software updates en upgrades. Vanuit het Technical Assistance Centre in Brussel verlenen wij 24 uur per dag online support aan klanten met een SMARTnet-contract.

Onze MKB Business Partners kunnen u meer vertellen over de voorwaarden.

De Cisco MKB Support Assistent is een gemakkelijk te gebruiken en voordelig programma dat ondersteuning biedt bij de meest voorkomende problemen en dat ervoor zorgt dat het netwerk beschikbaar en veilig blijft. Het geeft tijd aan waar problemen zijn opgetreden, hoe die kunnen worden opgelost en wanneer er een nieuw onderdeel moet worden besteld. De Cisco MKB Support Assistent Portal is een beveiligde online verzameling van hulpmiddelen waarmee klanten wachtwoorden kunnen herstellen, ondersteuningsdocumentatie kunnen raadplegen, het netwerk kunnen controleren, software-patches kunnen downloaden en ondersteuningscases kunnen openen wanneer dat nodig is.

## Cisco Financieringsoplossingen

U weet dat u een netwerk nodig heeft om meer te doen voor uw bedrijf, om te reageren op de behoeften van uw klanten, om uw efficiëntie te maximaliseren, uw kosten te minimaliseren en om te garanderen dat uw bedrijfsgegevens en bedrijfscommunicatie beschermd en veilig zijn.

Maar u wilt minder kapitaal investeren om die doelen te bereiken.

Dankzij de financieringsregelingen van Cisco Capital Easy Lease voldoet u aan uw bedrijfsbehoeften zonder uw kapitaal te blokkeren.

De belangrijkste voordelen van een financieringsoplossing van Cisco Capital Easy Lease zijn:

- Behouden van kapitaal. Voorspelbare en beheersbare betalingen helpen om de liquiditeit te verbeteren en kredietlijnen open te houden.
- Vermijden van technologische veroudering. Er kan een technologische upgrade-optie in de leaseovereenkomst worden ingebouwd. Daardoor kunt u op een gegeven moment tijdens de leaseperiode upgraden naar de nieuwste technologie.
- Maximale flexibiliteit. Laat u bij de keuze en implementatie van een oplossing leiden door uw bedrijfsbehoeften en niet door mogelijke budgettaire restricties. Dat zorgt ervoor dat uw technologie nieuw blijft en gelijke tred houdt met de gebruiksbehoeften.

Cisco Capital Easy Lease biedt financieringsoplossingen om te garanderen dat de technologie die u gebruikt gelijke tred houdt met de onvoorspelbare behoeften van uw gebruikers en klanten. Ze bieden een voorspelbaar en betaalbaar betalingschema zonder dat het nodig is om de hele investering in een keer vooraf te betalen.



**Europe Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: +31 0 800 020 0791  
Fax: +31 0 20 357 1100