

2010

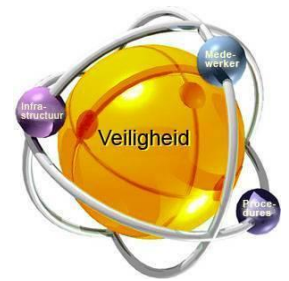
Beveiliging ICT



Yvan Gielens

Welzijnskoepel West-Brabant

1-1-2010



Inleiding

Voorwoord

Via workshops zal ik te samen met de systeembeheerders proberen punten uiteen te zetten en deze op een eenvoudige manier uitleggen die betrekking hebben i.v.m. werken van op afstand.. De map is een basis waarop men moet letten en kan als leidraad dienen voor gebruikers in te lichten of informatie door te geven.

Index

Beveiliging van uw DATA .

- **Back-up**

Beveiliging van uw SOFTWARE

- **Update**
 - **OS (Operating System)**
 - **Anti Virus**
 - **Spyware**

Beveiliging van uw COMPUTER.

- **Sterke wachtwoorden**
 - **Controle lijst voor sterke wachtwoorden**
 - **Een sterk en gemakkelijk te onthouden wachtwoord**
 - **Uw wachtwoord geheim houden**
- **Drie manieren om uw laptop veilig mee te nemen**

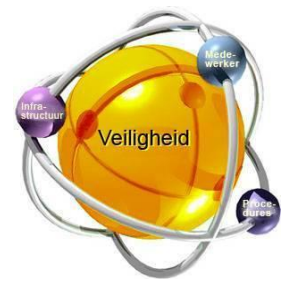
Beveiliging van uw NETWERK(thuis).

- **KABEL beveiliging**
- **WIFI beveiliging**
 - **Sleutels (Wachtwoord, MacAdress, Encryptie, SSID hidden)**

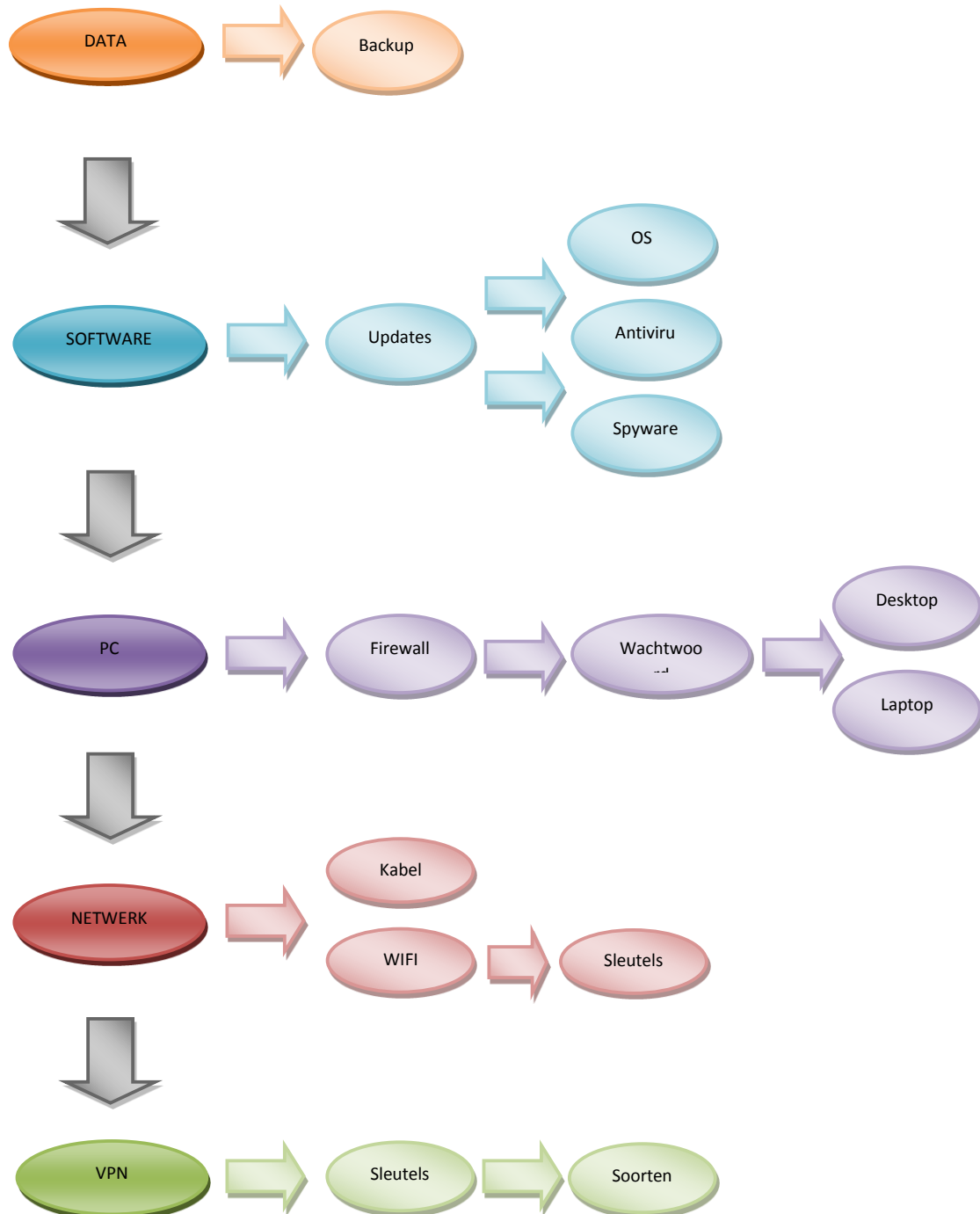
Beveiliging van uw VPN.

- **Sleutels**
- **Soorten**

Deze map geeft niet weer wat je moet gebruiken, maar zijn enkel punten waar je moet op letten.



Schema Beveiliging:





Bescherm uw computer als u vanuit thuis werkt.

Gebruik een firewall. Een firewall ontzegt hackers, virussen en wormen de internettoegang tot de computer of het netwerk van uw thuishkantoor.

Als u Windows Vista of Windows XP Service Pack 2 (SP2) gebruikt, beschikt u al over een firewall die standaard is ingeschakeld.

Werk uw software bij. Regelmatige software-updates kunnen van cruciaal belang zijn om uw computer of het netwerk van uw thuishkantoor zo veilig mogelijk te houden. Met Microsoft Update kunt u belangrijke beveiligingssoftware-updates downloaden voor zowel Windows- als Microsoft Office-programma's, zoals Microsoft Word, Microsoft Excel en Microsoft PowerPoint.

Gebruik antivirussoftware. Computervirussen kunnen ernstige gevolgen voor uw bedrijf hebben. Ze kunnen uw werk vertragen, belangrijke documenten vernietigen, enzovoort.

U kunt uw zakelijke pc's beveiligen door antivirussoftware zoals Windows Live OneCare te gebruiken en deze up-to-date te houden.

Gebruik antispyware-software. Spyware kan waardevolle gegevens van uw computer stelen, controle over uw internetbrowser krijgen of uw werk verstoren door u te bestoken met advertenties.

Windows Defender, de nieuwste versie van de antispyware-software van Microsoft, gebruikt real-time beveiligingsfuncties om spyware en andere ongewenste software op te sporen en te verwijderen.

Wees voorzichtig met e-mail en expresberichten. Zelfs als een bericht lijkt te komen van iemand die u kent, kan een bestand dat aan een e-mailbericht of expresbericht is toegevoegd, een virus bevatten. Neem dan ook via een andere weg dan via e-mail contact op met de afzender om u ervan te vergewissen dat de bijlage legitiem is.

Verstrek dus nooit persoonlijke of professionele gegevens als reactie op een verzoek per e-mail, ongeacht van wie het afkomstig lijkt - uw pc kan het doelwit van phishing-praktijken zijn.

Maak back-ups van uw bestanden. Maak een back-upschema en houd u daaraan om geen belangrijke bestanden te verliezen.

Gebruik sterke wachtwoorden en wijzig ze vaak. Sterke wachtwoorden bieden betere beveiliging tegen indringing door hackers en dieven.

U kunt ook sterke wachtwoorden gebruiken om bestanden van bepaalde Microsoft Office-programma's te beveiligen, zoals Microsoft PowerPoint of Microsoft Word.

Laat uw kinderen uw zakelijke computer niet zonder toezicht gebruiken.

Idealiter moet u uw kinderen uw zakelijke pc niet laten gebruiken. Als uw computer zowel voor uw bedrijf als door uw gezin wordt gebruikt, houd dan toezicht op uw kinderen als ze erachter zitten.

Leer oudere kinderen om geen programma's te downloaden of e-mailbijlagen te openen zonder uw toestemming, omdat deze spyware en virussen kunnen bevatten.



Beveiliging van uw DATA

back-up bestanden.

Het maken van back-ups is slechts een eerste stap.

U wilt ook op elk gewenst moment kunnen beschikken over belangrijke persoonlijke en of professionele bestanden en gegevens.

Hieronder volgen enkele suggesties om dergelijke bestanden en gegevens te beschermen:

	Sla uw gegevens buitenshuis of buiten kantoor op. Sla back-ups niet op de computer op, maar in een aparte ruimte en in een vuurvast archief. Als u een kluis gebruikt om uw belangrijke papieren documenten te beschermen, kunt u hierin ook de back-upschijven bewaren.
	Maak meerdere kopieën. Bewaar de back-ups op twee afzonderlijke locaties, zodat u over een tweede back-up kunt beschikken als er op één van de locaties een calamiteit plaatsvindt.
	Schoon uw opslag op. Zorg ervoor dat u regelmatig oude bestanden verwijdert (vooral als u voor opslag betaalt) of gebruik compressiesoftware om uw gegevens te comprimeren, zodat deze minder ruimte in beslag nemen.
	Bescherm uw gegevens met een wachtwoord. Sommige media beschikken over de mogelijkheid om gegevens met een wachtwoord te beschermen. Deze functie moet u zeker overwegen als u een back-up maakt van persoonlijke of gevoelige gegevens.

Schrijf uw wachtwoord op en bewaar het op een veilige locatie, zoals in een kluis.

Hierdoor kan uw werkgever toegang krijgen tot de gegevens als u daartoe geen mogelijkheden hebt.




Beveiliging van uw computer.

Sterke wachtwoorden maken en gebruiken.

Uw wachtwoorden zijn de sleutels die u gebruikt om uw computer en online accounts te ontgrendelen. Hoe sterker het wachtwoord, des te beter is de beveiliging tegen aanvallen door hackers en dieven die uw gegevens zouden kunnen gebruiken voor het openen van nieuwe creditcardrekeningen, het afsluiten van een hypotheek of zelfs het online chatten onder uw naam - en u zou er pas achterkomen als het al te laat is. Het is niet moeilijk sterke wachtwoorden te maken. Met een klein beetje inspanning van uw kant en een aantal trucjes uit dit artikel kunt u de beveiliging van uw computer verbeteren.

Controlelijst voor sterke wachtwoorden

Een goed, sterk wachtwoord moet aan de volgende drie criteria voldoen:

	<p>Meer dan acht tekens lang. Korte wachtwoorden zijn gemakkelijker te kraken dan lange wachtwoorden.</p>
	<p>Combineer letters, cijfers en symbolen, maar:</p> <ul style="list-style-type: none">• Geen opeenvolgende of herhalende combinaties, zoals '12345678', '222222', 'abcdefg' of aangrenzende letters op het toetsenbord.• Geen gewone woorden waarbij de letters vervangen zijn door cijfers of symbolen, zoals 'M1cr0\$0ft' of 'W@chtw00rd'. Helaas kennen hackers deze trucjes ook.
	<p>Voor u gemakkelijk te onthouden, maar door anderen moeilijk te raden. Vermijd ook het volgende:</p> <ul style="list-style-type: none">• Niet uw aanmeldingsnaam, de naam van uw partner of uw geboortedatum.• Geen woorden uit het woordenboek, uit welke taal dan ook. Hackers gebruiken geraffineerde hulpmiddelen die snel wachtwoorden kunnen raden die gebaseerd zijn op woorden uit het woordenboek, uit een groot aantal talen, en die achterstevoren zijn gespeld.• Niet moeilijk te onthouden. Als u toevallige combinaties van letters, cijfers en symbolen gebruikt die u alleen onthoudt als u ze opschrijft, kan het gebeuren dat u deze verkeerd invoert of dat deze door anderen worden gevonden en gebruikt.



Beveiliging van uw computer.

Een sterk en gemakkelijk te onthouden wachtwoord in vier stappen

Een manier om een sterk en gemakkelijk te onthouden wachtwoord te maken, is het verzinnen van een 'wachtzin'. Hier is een manier om in vier stappen een wachtwoord te maken dat op een wachtzin is gebaseerd:

1	Bedenk een zin die u kunt onthouden, zoals "Mijn zoon André is drie jaar ouder dan mijn dochter Anna". Dit is dan uw wachtzin.
2	Maak meerdere kopieën. Bewaar de back-ups op twee afzonderlijke locaties, zodat u over een tweede back-up kunt beschikken als er op één van de locaties een calamiteit plaatsvindt.
3	Neem de eerste letter van elk woord uit de zin om een nieuw woord te maken. In ons voorbeeld krijgt u: 'mzaidjodmda'.
4	Vervang tot slot enkele tekens door speciale tekens die op letters lijken, om het wachtwoord nog sterker te maken. Deze trucjes leiden in dit voorbeeld uiteindelijk tot het volgende wachtwoord: 'Mz@i3jodmd@'.

Als u twijfelt of u de wachtzin kunt onthouden, neem dan eerst een gewone zin als uw wachtzin, zoals "Je kunt een oude hond geen nieuwe trucjes leren", en voeg minstens één cijfer of symbool aan het wachtwoord toe. Zo kan 'jkeohgnt!' worden omgezet in 'JkeOHgnTL' of zelfs in 'Jke@HgnT1'.



Beveiliging van uw computer.

Uw wachtwoorden geheim houden

Spring voorzichtig met uw wachtwoorden en wachzinnen om.

1	Geef ze niet aan vrienden of familieleden (in het bijzonder kinderen) die ze weer aan andere, onbetrouwbare personen zouden kunnen doorgeven.
2	Bewaar opgeschreven wachtwoorden niet in uw bureau. Het briefje waarop u de wachtwoorden voor uw eigen gemak hebt genoteerd kan dieven die het vinden eenvoudig toegang verschaffen tot uw computer.
3	Verstrek nooit uw wachtwoord via e-mail, zelfs als het verzoek van een betrouwbaar bedrijf of persoon komt. Bij phishing kan frauduleuze e-mail gebruikt worden om u ertoe te verleiden uw gebruikersnamen en wachtwoorden prijs te geven, zodat criminelen toegang kunnen krijgen tot uw accounts, uw identiteit kunnen stelen, enzovoort.

Wijzig wachtwoorden regelmatig.

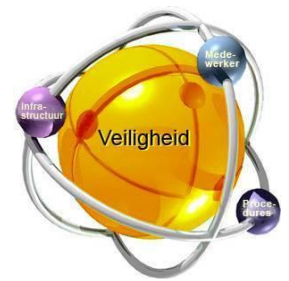
Idealiter moet u elke paar maanden nieuwe, sterke wachtwoorden voor uw accounts maken. Dit laat hackers in het ongewisse als ze een website in de gaten houden die u regelmatig bezoekt.

Gebruik niet dezelfde wachtwoorden voor meerdere accounts.

U moet elke keer dat u een nieuwe account opent een nieuw, sterk wachtwoord maken.

Schakel de optie 'Wachtwoord opslaan' niet in.

Als u een dialoogvenster te zien krijgt waarin u wordt gevraagd of uw computer het wachtwoord moet opslaan, kies dan **Nee**. Met deze optie kan iedereen die van uw computer gebruikmaakt, uw opgeslagen wachtwoorden voor deze accounts gebruiken.



Beveiliging van uw computer

Drie manieren om u laptop veilig mee te nemen

De nieuwste laptops zijn krachtig, licht en dun en passen gemakkelijk in de kleinste handbagage. Hierdoor zijn ze uitermate geschikt om mee te nemen, maar ook gemakkelijker te verliezen of te stelen.

Het is verstandig om extra waakzaam te zijn, dieven maken graag gebruik van deze situatie. Maar ook als u extra voorzichtig bent, kunt u uw laptop nog steeds kwijtraken. Als u de laptop beveiligd voordat u op weg gaat, doet u al veel om te voorkomen dat uw persoonlijke of professionele gegevens in verkeerde handen vallen.

Hier volgt de top drie van onze tips om de gegevens op uw laptop te beschermen.

	<p>Beveilig uw gegevens</p> <p>Als u veel persoonlijke of professionele informatie op uw computer bewaart, investeer dan in een besturingssysteem met ingebouwde bestandsbeveiliging. In Windows Vista en Windows XP Professional kunt u uw informatie met behulp van codering beveiligen.</p>
	<p>Beveilig uw laptop met een sterk wachtwoord</p> <p>Als u regelmatig uw laptop meeneemt, beveilig die dan met een sterk wachtwoord. Ga naar de sectie Help en ondersteuning voor informatie over het toevoegen en wijzigen van uw systeemwachtwoord.</p>
	<p>Maak back-ups voordat u vertrekt</p> <p>Maak altijd een back-up van de gegevens op uw laptop voordat u deze meeneemt. Het financiële verlies van uw apparatuur is niet altijd te vermijden, maar u kunt wel voorkomen dat u ook nog al uw gegevens kwijtraakt.</p>



Beveiliging WIFI netwerk

Wel, om te beginnen is het in gebruik nemen van WiFi relatief simpel. Waarom?






Omdat er geen rekening gehouden wordt met beveiliging. Standaard staat deze niet aan wat inhoud dat wanneer een hacker besluit om eens rond te gaan rijden om te zien waar onbeveiligde toegangen zijn (wardriving genoemd)

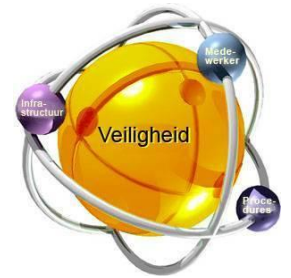
De onbeveiligde netwerkverbinding kan gebruikt worden om

1 het netwerk aan te vallen of

2 gebruik maken van het netwerk om het internet op te gaan.

Nu is het laatste niet zo spannend (of je moet een internet verbinding hebben waarbij per MB betaald moet worden) maar de eerste is voor de meeste mensen reden genoeg om WiFi niet te gaan gebruiken of om in ons geval een beveiliging op te zetten

	<p>Wijzig de standaard instellingen:</p> <p>Draadloze routers en access points zijn ingesteld met een standaard administrator wachtwoord en SSID (netwerk naam). Deze zijn hetzelfde voor alle routers/AP's van die serie, en soms gebruikt een fabrikant voor alle modellen dezelfde gegevens.</p>
	<p>Schakel SSID broadcasting uit:</p> <p>Dit maakt het netwerk zichtbaar voor iedereen die in de buurt is en over een WiFi machine beschikt. Het uitschakelen zorgt er niet voor dat je apparatuur voor WLAN "sniffers" verborgen is, maar het zorgt ervoor dat doorsnee surfers niet weten wie er in de buurt is.</p>
	<p>Filter op MAC-adres:</p> <p>Dit zorgt ervoor dat alleen computers wiens MAC-adres is ingesteld verbinding met het netwerk en router kunnen maken. Het is mogelijk om MAC-adressen te spoofen, maar het is wel een extra beveiligingslaag.</p>
	<p>Geef je draadloze clients een statisch IP-adres en schakel DHCP uit,</p> <p>zodat ongeautoriseerde personen die verbinding maken niet automatisch een IP-adres krijgen.</p>
	<p>Gebruik encryptie:</p> <p>Gebruik WPA2 of WPA (Wi-Fi Protected Access) encryptie in plaats van WEP (Wired Equivalent Privacy).</p>



Beveiliging van uw VPN

Waarom VPN

Een Virtual Private Network wordt wel omschreven als een 'tunnel' door het publieke internet, waardoor uw communicatie is afgeschermd van gluurders en dieven. Deze tunnel wordt gevormd door versleuteling en veiligheidsprotocollen. Vroeger werd tussen twee of meer vestigingen van hetzelfde bedrijf een huurlijn gelegd, tegen aanzienlijke kosten. Hetzelfde kan met een VPN, maar dan stukken goedkoper. De basis is nu een breedband internetverbinding (ADSL of kabel) en die heeft u al vanaf zo'n 20 euro per maand. Via een VPN kunt u grote bestanden versturen, tekstberichten, maar u kunt er ook door praten (VOIP) of virtueel vergaderen (teleconferencing).

Opstelling VPN

Er zijn twee courante opstellingen waarin een VPN geconfigureerd kan worden.

	<p>Remote-access VPN</p> <p>Hierbij zal een gebruiker toegang krijgen tot de private LAN van een organisatie door middel van een VPN. Dan denken we in de eerste plaats aan werknemers die thuis of op verplaatsing toegang zullen hebben tot het private bedrijfsnetwerk.</p>
	<p>Site-to-site VPN</p> <p>Hierdoor kan een organisatie de netwerken van geografisch gescheiden vestigingen met elkaar verbinden. Het resultaat van deze verbinding wordt een intranet VPN genoemd. Een andere mogelijkheid is dat verwante organisaties (bv. leveranciers en magazijniers) elkanders netwerken onderling verbinden om zo een intelligent geheel te bekomen opdat de productiviteit verhoogt. Hier spreken we over een extranet VPN. Daarnaast bestaan er natuurlijk nog andere opstellingen afhankelijk van de reële situatie, deze zijn meestal te herleiden tot een variant op de bovenvernoemde opstellingen</p>

Beveiliging van uw VPN



Mogelijkheden VPN

<p>1</p>	<p>Software VPN U kunt uw VPN softwarematig opzetten door het gebruik van een speciaal programma, dat op beide computers aan de uiteinden van het VPN is geïnstalleerd. Zo'n VPN maakt gebruik van de webbrowser en het SSL-veiligheidsprotocol om te zorgen dat u niet al te eenvoudig bent af te luisteren. Het is zelfs geheel gratis verkrijgbaar, of u legt wat geld neer voor een business-versie met toegevoegde veiligheid. Een 'instant' VPN als dit is zeer handig voor rondreizende medewerkers, die contact kunnen maken met het bedrijfsnetwerk, hun agenda bijhouden en databases synchroniseren waar ze ook maar even online zijn. Het kan ook gebruikt worden voor een tijdelijke tunnel, voor een eenmalig zakelijk gesprek of uitwisseling van gegevens.</p>
<p>2</p>	<p>Firewall of router met VPN Bij de keuze van een firewall kunt u erop letten dat deze ook VPN-functionaliteit biedt. De software regelt in dat geval zelf de versleuteling die nodig is. Uiteraard is het wel vereist dat beide uiteinden van de tunnel van hetzelfde pakket zijn voorzien, of u kunt voor thuiswerkers een speciale client-versie aanschaffen. Routers hebben tegenwoordig vaak zowel een firewall als een VPN-optie aan boord, en zijn daarbij niet veel duurder dan exemplaren zonder. Prijzen beginnen bij zo'n 70 euro bij elke pc-winkel. U hebt met deze apparaten een snelle en betrekkelijk eenvoudig te installeren oplossing in huis, die een redelijk veiligheidsniveau biedt. Ruim voldoende voor de gemiddelde telewerker.</p>
<p>3</p>	<p>VPN over connect-verbinding Semi-privé. Vindt u het publieke internet te riskant voor uw gevoelige informatie, dan neemt u de laatste halte vóór de ouderwetse huurlijn. U maakt hierbij gebruik van een fysiek afgescheiden netwerk, dat u echter wel moet delen met andere afnemers van dezelfde dienst. Dit is een zeer robuuste en veilige methode, die op maat wordt aangeboden door de grotere ICT-leveranciers.</p>



Beveiliging van uw VPN

Veiligheidsprotocol

Net als in de 'echte' wereld is een veiligheidsprotocol op het web of netwerk een set afspraken die de veiligheid moeten bevorderen. Die afspraken kunnen gaan over identificatie van gebruikers (digitale handtekening)), het toedelen van bevoegdheden, het versleuten van communicatie (encryptie) en het controleren van de integriteit van verstuurd gegevens. Bekend voorbeeld is SSL (Secure Socket Layer).




Vormen van VPN

VPN verbindingen verschillen op twee manieren van elkaar:

de gebruikte manier van versleuteling en envelop en de manier waarop zender en ontvanger met elkaar communiceren.

Onderscheid 1: versleuteling en enveloppe

Het gebruik van een extra "VPN-envelop" binnen de normale envelop wordt "tunneling" genoemd. Er zijn verschillende vormen van enveloppen:

	<p>PPTP PPTP staat voor point-to-point protocol. Het is een manier om informatie te versturen waarbij de inhoud van de VPN envelop NIET wordt versleuteld. PPTP zit standaard bijvoorbeeld in Windows ingebouwd. Gezien de beperkte beveiligingsmogelijkheden van deze vorm van VPN wordt deze vorm niet als volwaardig VPN gezien. Dit betekent dat voor het beveiligen van de gegevensstroom extra maatregelen buiten VPN om nodig zijn.</p>
	<p>L2TP L2TP staat voor "layer 2 tunneling protocol". De voor- en nadelen zijn te vergelijken met PPTP.</p>
	<p>IPsec IP sec is volgens velen de "echte" vorm van VPN, omdat het de tunneling altijd combineert met een bepaalde vorm van encryptie. Meerdere vormen van encryptie zijn mogelijk:</p> <ul style="list-style-type: none">○ DES. Algemeen bruikbaar bij programma's en apparaten welke VPN aan kunnen. Redelijk veilig.○ 3DES. Dit is niet meer dan DES welke 3x achter elkaar gebruikt wordt. Vrijwel alle programma's en apparaten welke DES aan kunnen kunnen ook 3DES aan. 3DES is veilig○ AES. Deze vrij nieuwe standaard geldt als zeer veilig, maar wordt niet standaard in ieder VPN programma ondersteund.

Er bestaat een wisselwerking tussen de gebruikte vorm van VPN en de belasting van de verbinding. Veiliger vormen van encryptie (versleuteling) vragen meer rekenwerk en een hogere belasting van de hardware. Bij veel VPN dataverkeer kan dit van belang zijn, maar in de meeste situaties heeft het de voorkeur om de meest veilige vorm van versleuteling te gebruiken.



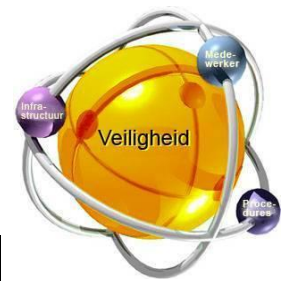
Beveiliging van uw VPN

Onderscheid 2: het netwerk aan beide kanten van de verbinding

<p style="text-align: center;">1</p>	<p>Rechtstreeks van computer tot computer twee computers respectievelijk een VPN client en VPN serverprogramma nodig: Het gebruik van een computer als VPN client of server maakt standaard deel uit van sommige versies van Windows. Dit soort VPN verbindingen zijn vrij recht-toe-recht-aan. Een PPTP of L2TP VPN kan al worden opgezet tussen twee computers welke beiden gebruik maken van Windows XP.</p>
<p style="text-align: center;">2</p>	<p>Tussen twee routers welke VPN ondersteunen Om een netwerk van computers toegang tot het internet te geven heeft men een router nodig. Als men een tweetal netwerken via VPN met elkaar wil verbinden kan men er voor kiezen de VPN verbinding niet te laten maken door de individuele computers maar bijvoorbeeld door de routers af te laten handelen. De verschillende aangesloten computers hoeven in dit geval geen aparte VPN software te gebruiken. Bij een goede configuratie ontstaat een transparant netwerk dat over meer dan een lokatie gespreid kan zijn. De firewall in de router schermt tegelijkertijd het hele netwerk achter de router af. Deze configuratie is ideaal voor het koppelen van bijvoorbeeld een aantal filialen en een hoofdkantoor.</p> <p>Een paar opmerkingen over deze opzet:</p> <ul style="list-style-type: none"> ○ De verschillende routers moeten compatibel met elkaar zijn. ○ De modems moeten het VPN verkeer normaal doorlaten en de firewalls in de routers moeten goed zijn geconfigureerd. ○ De routers houden de "broadcast" van de verschillende in het netwerk opgestelde computers soms tegen. Hierdoor <i>lijken</i> de computers aan de andere kant van de tunnel niet te zijn. Dit is bij voorbeeld door gebruik van WINS of LMhost bestand te verhelpen. De nieuwste modellen zijn voorzien van een mogelijkheid om de "broadcasts" toch door te laten waardoor deze extra instelling niet langer nodig is. ○ De netwerken aan de verschillende kanten van de tunnel mogen niet hetzelfde IP-bereik gebruiken. <p>Conclusie Om boven genoemde redenen verdient het de voorkeur om van te voren goed uit te werken hoe de netwerken aan weerszijde van de VPN verbinding er uit moeten gaan zien. Bekijk aan de hand van de specificaties van de betrokken programma's en routers of het kan werken.</p>
<p style="text-align: center;">3</p>	<p>Mengvormen Soms wordt de VPN verbinding opgezet door de computers zelf maar maakt een of beide kanten van de verbinding gebruik van een router. Neem bijvoorbeeld een groep thuiswerkers welke allen verbinding moeten krijgen met een centrale server. De server staat in het netwerk van het bedrijf achter een router, welke op het bedrijf wordt gebruikt om het internet te delen en in zijn geheel af te schermen met een firewall. Maar het kan ook andersom: een VPN Client PC achter een router welke met een losse VPN server contact probeert te maken. Of neem een verbinding tussen twee netwerken met routers waarbij de VPN verbinding niet door de routers maar door de computers verzorgd wordt.</p> <p>Dit gaat niet altijd goed. Deze configuraties kunnen werken, maar niet bij ieder type verbinding, router en VPN programma. Er kunnen zich de verschillende problemen voordoen.</p>

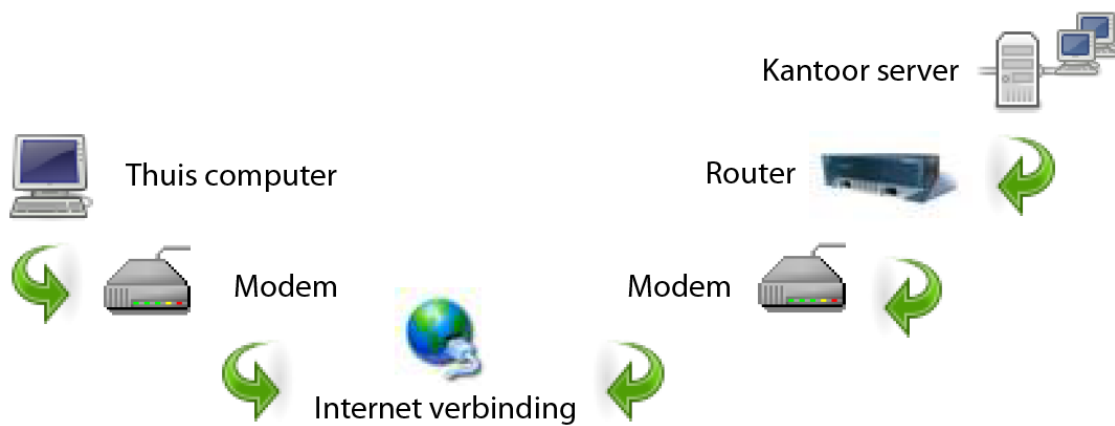
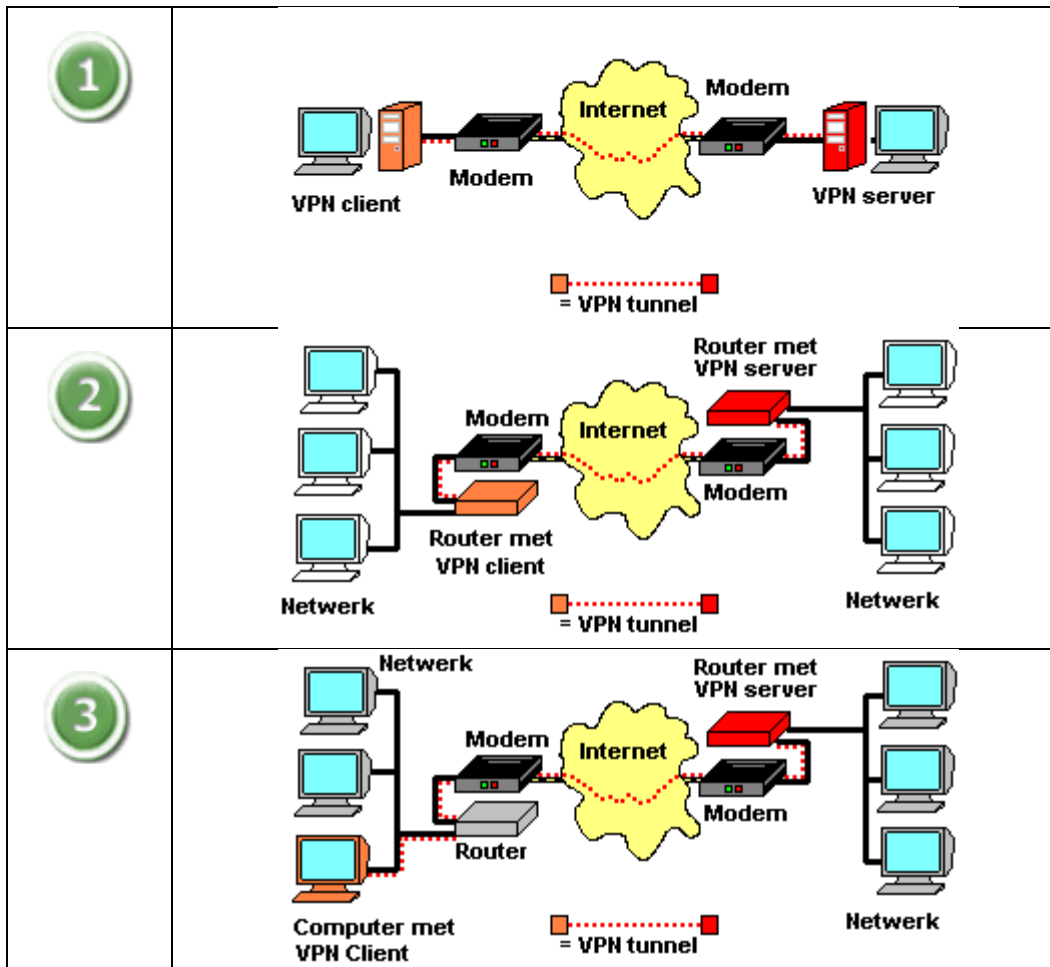
Voor het opzetten van een VPN verbinding moet een van de betrokken computers als server en een andere computer als cliënt worden ingesteld.

Er zijn drie combinaties van VPN tussen computers en netwerken mogelijk.



Beveiliging van uw VPN

VPN SCHEMA





Beveiliging van uw VPN

VPN en andere vormen van veiligheid

VPN maakt het dataverkeer tussen twee punten veilig.

Maar de veiligheid van een VPN verbinding is maar één vorm van veiligheid, waar men zich niet volledig op kan verlaten. Hoewel het transport van de gegevens over het internet met VPN veilig verloopt kan een kwaadwillende "hacker" bij een onbeschermd computer er achter komen wat de versleuteling van de VPN- tunnel is. Hiermee kan hij of zij de informatie wél ontcijferen met alle ongewenste effecten van dien.

Om deze reden valt het aan te raden om een computer of een computernetwerk welke gebruik maakt van VPN tegelijkertijd ook te voorzien van een goede firewall.

Op die manier zijn ook de in- en uitgang van de "tunnel" beveiligd.

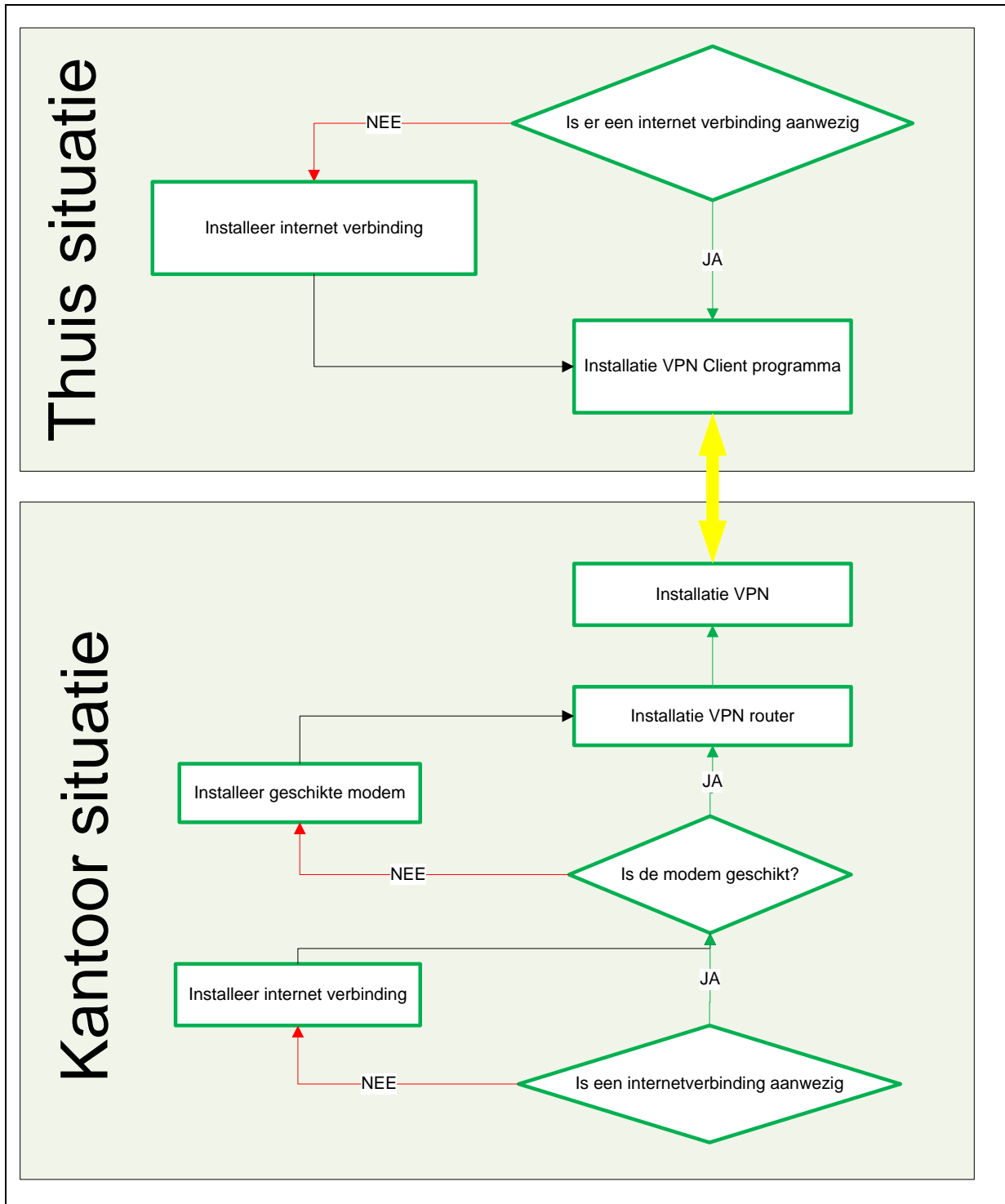
Eenzelfde probleem doet zich voor indien bij het uiteinde van de tunnel gebruik wordt gemaakt van een draadloos netwerk. Deze zijn door iedereen in de buurt op te vangen. Indien de VPN is opgezet tussen twee routers maar het draadloze netwerk achter een van de routers niet goed is beschermd kan iedereen het verkeer opvangen en inzien. Voorzie daarom in dit soort gevallen het draadloze netwerk van afdoende beveiliging als WEP, WPA en wireless VPN.

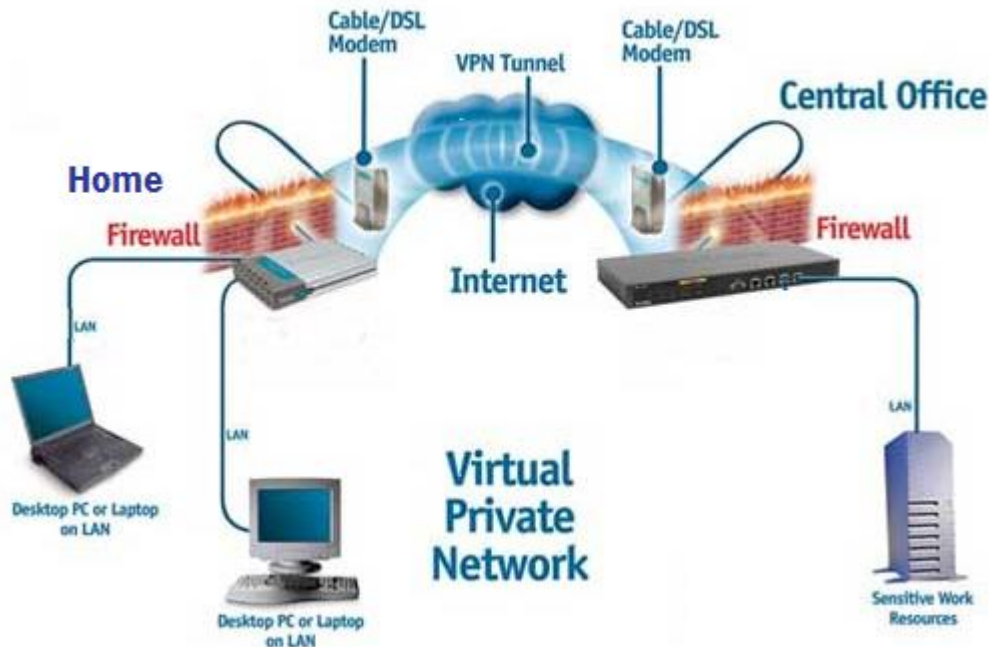
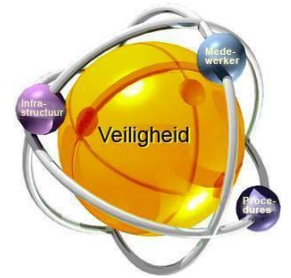
Als laatste waarschuwing: VPN is afhankelijk van het gebruik van "sleutels". Als de sleutel gemakkelijk te voorspellen is kan een kwaadwillend iemand alsnog de beveiliging ongedaan maken door de sleutel correct te raden of te voorspellen.

Beveiliging van uw VPN



Stappenplan: Thuis-Kantoor VPN





Principe

Een firewall (vrij vertaald: vuur muur of vuurscherm) kan worden vergeleken als een afsluiting (muur) om de negatieve krachten buiten je eigendom te houden. In die afsluiting zit een poort. Die poort wordt streng gecontroleerd. Je bepaald zelf wie erin mag. Deze beschrijving is vrij figuurlijk natuurlijk.

Soorten Firewalls

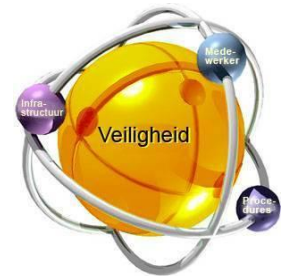
De firewalls kunnen in twee grote families geplaatst worden. Je hebt de firewall die als een programma op je computer geïnstalleerd wordt en je hebt een firewall die je als afzonderlijk apparaat in je thuisnetwerk plaatst. Deze laatste wordt via een webinterface vanaf je eigen computer ingesteld. Voor thuisnetwerken zal de firewall al aanwezig zijn in de (ADSL / Broadband) router of draadloze router.

Beide soorten firewalls (software- en hardware firewalls) hebben een gelijkaardige werking. De gebruikte terminologie is op beide versies van toepassing.

Filter

In onze principe beschrijving hadden we het over een poort. Via deze poort wordt gecontroleerd welke gegevens binnenkomen en welke naar buiten gaan. Algemeen kunnen we stellen dat de informatie die van het Internet komt, wordt gefilterd. Een filter bestaat uit een reeks regels waarbij men de toegang van bepaalde toepassingen blokkeert, of doorlaat. Bv. om bestanden van het Internet af te halen, maakt men doorgaans gebruik van FTP (File Transfer Protocol). De filter van de firewall zou dan kunnen bepalen dat FTP niet wordt toegelaten voor jouw computer. In dat geval zal je geen bestanden kunnen downloaden van het Internet. Dezelfde filter kan bepalen dat het wel kan voor een andere computer in jouw netwerk. Zodat ieder scenario kan worden vastgelegd.

Firewalls gebruiken drie methodes om het Internet verkeer te controleren in- en uit- het lokale netwerk:

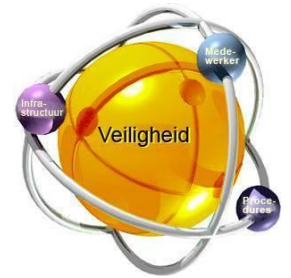


- Packet Filtering:** Gegevens pakketten (kleine gegevens blokken die zich via het netwerk verplaatsen van de ene- naar de andere computer) dragen een soort signatuur. Het is precis die signatuur die aangeeft over welk soort pakket het gaat. Het zijn de filters die aan de hand van de signatuur bepalen of een pakket al dan niet wordt doorgelaten.
- Proxy Service:** Proxy Service biedt de mogelijkheid om het internetverkeer te reguleren. De benodigde hoeveelheid internetbandbreedte wordt geoptimaliseerd door veel opgevraagde Internet bladzijden lokaal op te slaan. Daarnaast wordt de functie van de Proxy Service als toegangscontrolepunt naar het Internet steeds belangrijker. Het biedt de mogelijkheid om de toegang van en naar het Internet per gebruikersgroep of zelfs per medewerker te regelen.
- Stateful Inspection:** In tegenstelling tot Packet Filtering wordt de signatuurinhoud van elk pakket niet gecontroleerd. Er worden bepaalde sleutelwaarden die in het pakket voorkomen vergeleken met het model dat in een database is opgeslagen. Hiermee wordt bepaald of een bepaald pakket al dan niet wordt toegelaten.

Een firewall op maat

Firewalls kunnen op maat worden ingesteld. Je kan filters toevoegen, verwijderen en aanpassen.

- IP-adressen:** Elke computer (server) die op het Internet is aangesloten heeft zijn eigen IP-adres. Een IP-adres bestaat uit 32 bit getallen (met een waarde tussen 0 en 255), uitgedrukt in vier delen gescheiden door een punt (IPv4). Een typisch IP-adres ziet er als volgt uit: "216.18.1.1". Indien een gebruiker binnen het netwerk abnormaal veel bestanden zou downloaden, dan zou de netwerkbeheerder dit specifieke adres kunnen weren. Dit IP-adres wordt aan een lijst van IP-adressen toegevoegd.
- Domein-namen:** In onze uitleg over IP-adressen schreven we dat elke (Web-) server beschikt over zijn eigen IP-adres. Het spreekt voor zich dat het aanroepen van deze servers dmv een IP-adres weinig gebruiksvriendelijk is. Het is veel gemakkelijker op trefwoorden te gebruiken. Vandaar dat men de zgn. "Domein Names" (Domein-namen) heeft geïntroduceerd. Elke domein-naam is verbonden met een IP-adres. Ook hier kunnen bepaalde domeinen geweerd worden. De ongewenste domeinen worden in een lijst opgenomen.
- Protocols:** Een "protocol" is een afgesproken wijze van communiceren met een andere gebruiker of dienst op het Internet. Vb. je opent je webbrowser en je surft naar een bepaalde website. In dat geval maak je gebruik van het zgn. web-protocol waarmee http-bestanden worden opgeroepen. Enkele bekende protocols zijn:
- IP:** Dit is de afkorting van "Internet Protocol". Het is het basisprotocol voor de communicatie over het Internet.
 - TCP:** Dit is de afkorting van "Transmission Control Protocol". Zorgt voor het opsplitsen in kleine pakketten van de digitale informatie die over het Internet wordt verstuurd en het terug samenbrengen van de opgesplitste pakketten bij aankomst.
 - HTTP:** Dit is de afkorting van "Hyper Text Transfer Protocol" en dient om webpagina's door te sturen over het Internet.
 - FTP:** Dit is de afkorting van "File Transfer Protocol" en dient voor het downloaden of uploaden van bestanden over het Internet.
 - UDP:** Dit is de afkorting voor "User Datagram Protocol". Dit protocol wordt gebruikt indien er geen controle is op de goede ontvangst van gegevensstroom. Dit wordt oa. gebruikt bij de ontvangst van muziek en videobeelden (streaming video).
 - SMTP:** Dit is de afkorting van "Simple Mail Transport Protocol". Dit wordt gebruikt om tekstgebaseerde informatie door te sturen via het Internet zoals email-berichten.
 - Telnet:** Hiermee kan men commando's doorsturen naar een afgelegen computer.
- Er zijn nog veel meer protocols dan deze opgenomen in deze korte lijst. De firewall-instellingen laten toe om bepaalde protocols te weren.
- Poorten:** Elke server op het Internet stelt zijn diensten ter beschikking op genummerde poorten. Per dienst zal een poort worden gedefinieerd. De keuze van een poort gebeurt op basis van afspraken. Gewoonlijk zal poort 80 gebruikt worden voor



“HTTP” EN POORT 21 VOOR “FTP”. INDIEN MEN POORT 21 BLOKKEERT IN DE FIREWALL DAN ZULLEN DE GEBRUIKERS GEEN FTP-DIENST KUNNEN AANROEPEN.

Termen: Deze methode laat toe om pakketten te blokkeren waarin een bepaald woord voorkomt. Je kan zoveel woorden en zinnen definiëren als je maar wilt.

Sommige besturingsprogramma's beschikken over hun eigen firewall-oplossing. We hebben het hier over een geïntegreerde software firewall. Op de computermarkt worden heel wat alternatieve software firewalls aangeboden. Indien je enkel over een software firewall beschikt, zou je je thuis netwerk als volgt kunnen samenstellen. Stel dat je over twee of meerdere computers beschikt en je wilt dat elke computer toegang heeft tot het Internet dan definieer je één computer als zgn. “**gateway**”. Het is deze computer die de toegangspoort vormt tussen je lokale netwerk en het Internet. Op die computer zal de firewall software actief moeten zijn. Je zult eveneens de verschillende firewall-parameters moeten instellen.

Met een hardware oplossing is de situatie helemaal anders. In dat geval zullen we het hebben over een router (kabel of DSL-router) gecombineerd met een firewall en al naar gelang het model met een draadloos gedeelte (Wifi). Dat apparaat zal fungeren als “**gateway**”. Indien je over een Internet aansluiting beschikt via de kabel distributie, dan zal je een kabel router nodig hebben. Indien het om een ADSL-aansluiting gaat, gebruik je best een DSL-router. Bij een DSL-router liggen de verschillende aansluitingen voor de hand. Indien het om een kabel-router gaat moet je erop toezien dat de netwerkkabel die van je Internetaansluiting komt, aangesloten wordt op de “WAN” aansluiting van je router. De verschillende computers van je thuisnetwerk kunnen aangesloten worden op de “LAN”-aansluitingen van de router. Meestal staat de WAN heel duidelijk aangegeven op het apparaat. Bij de aanschaf van een router hou je best rekening met het aantal computers dat je erop wilt aansluiten.

Het instellen van de router- en firewall-parameters gebeurt via een zgn. webinterface. Hiervoor moet je de computer dmv een netwerkkabel aansluiten met de router en de webbrowser opstarten. In de adresbalk van de browser tik je het IP-adres van de router (vb. 192.168.1.1) in en je krijgt meteen een loginscherm te zien. In de handleiding staat aangegeven welke login en welk wachtwoord je moet invullen. Het gaat om de fabrieksinstellingen. Je doet er goed aan om deze parameters meteen te wijzigen.

Zowel bij de software firewalls als bij hardware firewalls zal je alle instellingen moeten overlopen. Bij een goede firewall zullen de ‘default’-instellingen zeer streng zijn ingesteld. Het is dan aan jou om sommige diensten toch toe te laten...

Welke bescherming biedt een firewall

Sommige Internet-gebruikers zijn zeer creatief als het gaat om anderen het leven zuur te maken. Ze vinden allerlei middelen om in te breken in computers die op het Internet zijn aangesloten.

Om aan te geven op welke manier Internet-gebruikers worden aangevallen maakt men gebruik van heel specifieke (Engelstalige) termen. Zie hier een kort overzicht:

Remote login:	Wanneer iemand in staat is om op afstand de controle van je eigen computer over te nemen, dan spreekt men over “remote login”. In sommige gevallen kan dit zeer nuttig zijn als je iemand op afstand wil helpen of als je op afstand bepaalde taken op je eigen computer wil uitvoeren. Als het over een kwaadwillige inbreker gaat dan is de situatie helemaal anders. Indien iets dergelijks wordt toegelaten dan moet je zorgen dat dit slechts tijdelijk mogelijk is of dat de beveiliging optimaal is (vb. via VPN geïncrypteerd, enz...).
Application backdoors:	Sommige programma's laten toe bepaalde handelingen op afstand uit te voeren. Meestal is dat voldoende beveiligd. Andere programma's bevatten fouten (bugs) die gelijkaardige handelingen toelaten, maar dan ongecontroleerd. Men spreekt over “backdoor” of “hidden access” (toegang via een achterdeur).
SMTP session	SMTP is het protocol dat doorgaans wordt gebruikt om emails naar andere Internet-gebruikers te sturen. Door zich toegang te verlenen tot je email-adresbestand kunnen hackers ervoor zorgen dat reclame (junk) mails naar je correspondenten wordt doorgestuurd. Je computer fungeert als vertrekpunt voor duizenden mails. Reacties van vrienden en kennissen zullen niet lang uitblijven...
hijacking:	
Software bugs:	Zowel het besturingssysteem als de verschillende programma's die op je computer zijn geïnstalleerd kunnen fouten vertonen. Men gebruikt hier de term “bugs”. Hackers maken graag gebruik van deze onvolkomenheden om de bescherming van je computer te omzeilen.
Denial of service:	Deze term wordt gebruikt wanneer bepaalde servers worden



	<p>aangevallen en waardoor ze buiten dienst geraken. Om die aanvallen tot stand te brengen, maken hackers gebruik van de computers van onwetende gebruikers. Het is dan de bedoeling dat al die besmette computers één bepaalde server aanspreken op hetzelfde ogenblik. De server kan deze grote hoeveelheid aanvragen niet aan en hij geraakt buiten dienst...</p>
E-mail bombs:	<p>In dit geval worden duizende mails naar jouw email adres toegestuurd tot je email providers geen mails meer kan toelaten.</p>
Macros:	<p>Wanneer men binnen een toepassing een handeling veelvuldig moet herhalen, dan wordt vaak een macro geschreven. Op die manier kan men met weinig moeite de handeling telkens opnieuw uitvoeren. Hackers gebruiken ook macro's om oa. gegevens te vernietigen. Deze macro's zitten verborgen in bv. document-bestanden die ze via email doorsturen. Het openen van het document zal de macro opladen en uitvoeren.</p>
Virussen:	<p>"Computer virussen" zal wellicht de meest gekende term zijn. Het zijn meestal kleine programma's die zich in de computer nestelen en die de goede werking van de computer aantasten. Dit gaat van het volledig wissen van de harde schijf tot het beïnvloeden van de opstartpagina van de Internet browser.</p>
Spam:	<p>Een ongewenste email wordt meestal als spam beschouwd. Op zichzelf is die niet echt gevaarlijk maar door de grote hoeveelheid zeer vervelend. een spam mail kan ook een link bevatten naar een website. Zodra deze wordt aangeklik wordt een stukje code opgeroepen (cookie) waardoor opnieuw een handeling wordt uitgevoerd. Je kan dit ook beschouwen als een soort "backdoor".</p>
Source routing:	<p>De weg die pakketten over het Internet volgen is moeilijk voorspelbaar. Dit hangt af van meerdere parameters en wordt bepaald door de routers. Bepaalde parameters laten toe om de pakketten gecontroleerd een bepaalde weg te doen volgen. Het is precies die mogelijkheid die door hackers wordt gebruikt om extra informatie te bekomen vanuit het internet netwerk. De meeste firewalls laten toe om de zgn. "source routing" af te leggen.</p>

Besluit

Het concept van de firewall is relatief eenvoudig. De eigen terminologie rond het gebruik van firewalls maakt het dan weer ingewikkelder. Vandaar dat we het accent gelegd hebben op het overlopen van de belangrijkste trefwoorden. Bepaalde vormen van Internet aanvallen zijn moeilijk of zelfs niet tegen te houden door een firewall. De firewall biedt geen totale bescherming. Het hoogste niveau van bescherming zal zo goed als niks doorlaten. Vermits we gebruik maken van het Internet zijn we verplicht om één en ander door te laten. Wees zeer selectief in het bepalen wie wat nodig heeft. De combinatie met andere vormen van bescherming zoals het plaatsen van een anti virusprogramma en het gebruik van een antispam zullen samen een goede oplossing bieden. In vele gevallen zal de houding van elke gebruiker bepalend zijn of bepaalde vormen van malware al dan niet worden binnengelaten. Blijf dus steeds waakzaam en zorg ervoor dat de programma's up-to-date blijven.