



Nieuwstraat 194/2 - 3590 Diepenbeek - Tel. 011/33 31 88 - Fax. 011/33 29 28  
<http://www.connectivitysolutions.be>

## Beveiliging draadloze netwerken

Wat is er nu handiger dan overal in huis of op kantoor draadloos te internetten, wat dankzij de eenvoudige toegangspunten en draadloze routers van tegenwoordig snel geregeld is? Zonder de juiste beveiligingsmethoden is uw internetverbinding echter te misbruiken voor het versturen van spam en kan het zonder dat u het weet worden ingezet voor een DoS-aan-val. Of de deur naar het internet wordt opengezet, zodat hackers uw privé-gegevens kunnen achterhalen. Wij nemen alle noodzakelijke stappen met u door voor het beveiligen van een draadloos netwerk.



### WEP en WPA

De twee bekendste beveiligingsmethoden voor draadloze LAN-netwerken zijn WEP (Wired Equivalent Privacy) en WPA (WiFi Protected Access). WEP is een beveiligingsprotocol dat specifiek voor draadloze netwerken is bedoeld en is vastgelegd in de 802.11b-standaard.

In theorie biedt WEP dezelfde beveiliging als een bekabeld netwerk, maar dat is feitelijk een utopie, omdat een bekabeld netwerk fysiek beter afgeschermd is voor vreemden. Een netwerk waarbij de gegevens vrijelijk door de lucht worden getransporteerd, is in principe kwetsbaarder.

WEP versleutelt de data die door de ether wordt gestuurd, maar is - zeker als er gebruik wordt gemaakt van oudere routers - redelijk eenvoudig te kraken.

Encryptie via WEP of WPA heeft bovendien invloed op de snelheid van uw netwerk. Zonder versleuteling kunnen we een bestand van 250 MB aan 2 MB/s transporteren. Met WPA-encryptie geactiveerd zakt de snelheid tot 1,3 MB/s en met WEP daalt de snelheid tot 1,1 MB/s. Dat is een vertraging van respectievelijk 35 en 45 procent.

WPA is een WiFi-standaard die is bedoeld als uitbreiding op de beveiligingsfuncties van WEP. In principe zijn WiFi-routers die met WEP overweg kunnen na een firmware-upgrade vaak in staat ook beveiliging via WPA te bieden. De laatste methode is op twee punten een stuk veiliger dan WEP.

Om te beginnen, worden gegevens beter versleuteld via het TKIP-protocol (Temporal Key Integrity Protocol), dat gebruikmaakt van een hashing-algoritme - inclusief extra controle die de garantie biedt dat er niet is geknoeid met de sleutels.

Ten tweede kent WPA een vorm van gebruikersbeheer, een eigenschap die WEP ontbeert. Daarvoor maakt WPA gebruik van het Extensible Authentication Protocol (EAP). WEP kan alleen toegangsbeveiliging uitvoeren op basis van het Mac-adres van een computer, dat eenvoudig op te sporen en na te bootsen is.

EAP bedient zich van een sleutelsysteem om te waarborgen dat alleen geautoriseerde gebruikers toegang krijgen tot het netwerk. De meest gebruikte EAP-methode is afkomstig van Cisco, en is ook wel gekend als LEAP en EAP-FAST.

Als beveiligingsstandaard zal die uiteindelijk worden vervangen door de beveiliging in de 802.11i-standaard, de opvolger van 802.11g.



### Instellingen

WPA en WEP kunnen beschouwd worden als basisbeveiliging, die u altijd moet instellen om toevallige passanten buiten de deur te kunnen houden. Het instellen is niet moeilijk: vaak volstaat het opgeven van een uitgebreid wachtwoord (pass-phrase), waarna u de router of het toegangspunt moet herstarten. Dit is een stuk makkelijker dan het met de hand invoeren van een sleutel waarbij u een minimaal aantal tekens moet gebruiken die lastig te onthouden zijn. Tegenwoordig is vrijwel alle apparatuur voorzien van een passphrase-optie, waarbij er een sleutel wordt gegenereerd aan de hand van het door u opgegeven wachtwoord.

Logt u met uw notebook in op het draadloos netwerk, dan moet u opnieuw het wachtwoord invoeren, waarna uw besturingsstelsel de goede sleutel doorzendt en u toegang krijgt tot het netwerk. Kies daarbij voor een zo sterk mogelijke versleuteling, bijvoorbeeld 128-bit encryptie.

Verder verdient het aanbeveling alleen bepaalde computers toegang tot uw draadloos netwerk te verschaffen. Daartoe vult u in uw router of toegangspunt op een lijstje de geautoriseerde MAC-adressen in, en klaar is kees. Het Mac-adres van uw net-werkkaart kunt u vinden door in een DOS-venster het commando ipconfig /all in te toetsen: u ziet dan onder Physical Address het Mac-adres van uw netwerkadapter.

Naast WEP en WPA zijn er diverse andere manieren om uw draadloos netwerk te beveiligen. We zullen een groot aantal daarvan de revue laten passeren, die vooral een aanvulling zijn op WEP of WPA. Ook is het niet in alle gevallen mogelijk of noodzakelijk de onderstaande methoden toe te passen.

U dient zelf te bepalen welke beveiligingsmethoden op uw eigen netwerk van toepassing zijn. Vaak is het noodzakelijk de activering van WEP of WPA te combineren met één van onderstaande methoden.

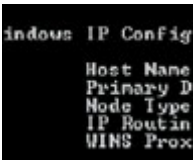


## SSID-herkenning

Een SSID is een tekenreeks van 32 karakters die staat vermeld in de header van elk pakketje dat over een draadloos netwerk wordt verstuurd. De header bevat de naam van de zender en het ontvangende toegangspunt van het pakketje. De meeste routers of toegangspunten hebben een standaard SSID die is gebaseerd op de merknaam en zo is ingesteld dat deze zichzelf bekendmaakt in de ether. Ideaal als u een hotspot beheert, maar bij een thuis- of bedrijfsnetwerk hoeft niet iedereen te weten dat u een draadloos netwerk bezit.

Zet de SSID-broadcasting dus bij voorkeur uit. Een draadloos netwerk waarop SSID-broadcasting is uitgeschakeld, is nog steeds niet veilig: u voorkomt er alleen maar mee dat er 'per ongeluk' iemand op uw netwerk 'botst'.

Er zijn diverse softwaretooltjes beschikbaar die ook draadloze netwerken kunnen opsporen die geen gebruikmaken van SSID.



## Mac-adresfilter en IP-adres

Vrijwel elk goed toegangspunt of router ondersteunt het filteren van clients op Mac-adres. Dit Mac-adres is het unieke adres van uw netwerkkaart, en in de router stelt u in welke Mac-adressen wel en welke geen verbinding mogen maken. Erg sterk is deze beveiliging echter niet, omdat Mac-adressen met niet al te veel moeite door een hacker gekloond kunnen worden. Toch zorgt deze maatregel voor een extra beveiligingslaagje.

Een kwaadaardige hacker kan in elk geval ontmoedigd worden door deze maatregel, zeker als uw buurman zijn netwerk wel gewoon open heeft staan. Een drive-by hacker zal in dat geval niet de moeite nemen om uw netwerk te kraken, maar eenvoudigweg doorrijden om een paar honderd meter verderop zijn slag te slaan.

De meeste draadloze routers zijn zo ingesteld dat ze automatisch IP-adressen uitgeven via een DHCP-server. Als er in een draadloos netwerk echter maar weinig gebruikers zijn, is het aan te raden DHCP uit te schakelen en met statische IP-adressen te werken.

Ook dit is weer een dun beveiligingslaagje, maar in combinatie met voorgaande stappen is het een extra hulpmiddel bij het weren van indringers.



## Antennes

Bij de meeste toegangspunten of routers wordt een standaardantenne meegeleverd. Dit is vaak een antenne die slechts in twee richtingen gedraaid kan worden. Een dergelijke antenne heeft een 'karakteristiek' (oftewel de vorm van het dekkingsgebied) die vergelijkbaar is met een volmaakte bol met de antenne in het midden.

In sommige (goede) handleidingen wordt de karakteristiek van een antenne vaak aangeduid met een schematische tekening, waarbij het bereik is verdeeld over de azimut (de horizontale as) en de elevatie (de verticale as). Andere antennetypes hebben een bereik waarbij het radiosignaal over de azimut en de elevatie niet gelijk is.

Zo verspreidt bijvoorbeeld een omnidirectionele antenne radiostraling in een cirkel rond de horizontale as, waarbij de elevatie maar minimaal is. Een schotelantenne is vooral zinvol bij point-to-point-verbindingen, waarbij de radiosignalen gericht naar een bepaald punt worden gestuurd.

Voor de antennes die vooral in grote bedrijven worden toegepast, zijn deflectors te koop die het radiosignaal naar één kant blokkeren. Op die manier wordt een antenne aan een buitenmuur 'gedwongen' om alleen het gebouw in te zenden, en niet naar buiten.

Ook dit is een vorm van netwerkbeveiliging, omdat hackers buiten de muren zo geen verbinding kunnen maken met uw draadloos netwerk.

Is er geen speciale deflector te koop voor uw WiFi-antenne, dan kunt u ook aluminiumfolie gebruiken. Ook kunt u door het terugschroeven van de zendkracht van een toegangspunt het bereik van uw draadloos netwerk beperken, zodat het alleen uw bedrijfsgebouw of woning dekt en bijvoorbeeld niet het huis van de buren.

Door antennes strategisch te plaatsen en het zendvermogen aan te passen, maakt u uw netwerk alleen

voor uw eigen locatie geschikt en bent u niet meteen de internetleverancier voor de hele straat. Voor een zo goed mogelijke dekking in een gebouw of woning plaatst u de antenne enkele meters boven de grond, maar niet tegen het plafond.



## VPN

Een alternatief voor WEP en WPA is een beveiligde verbinding tussen een draadloze computer en diensten in een bekabeld netwerk middels IPSec Virtual Private Network (VPN). Daarvoor is wel de aanwezigheid van een VPN-server of -gateway vereist. Met VPN wordt er een beveiligde 'tunnel' aangelegd tussen de gebruiker en de dienst, waar anderen niet op kunnen inbreken. Voor de beveiliging draagt het Internet Key Exchange-protocol (IKE) zorg dat sleutels en certificaten onder de verschillende gebruikers distribueert.

Een hacker die zich niet op het netwerk bevindt, kan vrijwel onmogelijk inbreken op een VPN-verbinding, omdat er heel lange, vrijwel niet te kraken sleutels worden gebruikt. Het nadeel van VPN in combinatie met draadloze verbindingen is dat er geen mechanisme is dat controleert of er vreemde clients op het draadloos netwerk actief mogen zijn.

VPN-verbindingen zijn ook mogelijk via de browser, middels SLL-versleuteling. Hierbij is er echter alleen sprake van een beveiligde verbinding tussen de browser en VPN-server. Een bestandsoverdracht via FTP is bijvoorbeeld niet beveiligd als deze niet via de browser verloopt.



## Subnet-instellingen en beveiligingsapparatuur

Een extra beveiligingsmethode is een draadloos netwerk inrichten, apart van het bestaand bekabeld netwerk, door gebruik te maken van een apart subnet, en een eigen router en firewall voor zowel het WiFi-netwerk als het bekabeld netwerk. Nog beter is een volledig standalone WiFi-netwerk dat niet is verbonden met het bekabeld netwerk.

Het gebruik van een ander subnet (vaak wordt standaard voor 255.255.255.0 gekozen) voorziet in een fysieke scheiding van beide netwerken en biedt een vangnet tegen hackers als alle andere beveiligingsmaatregelen gefaald hebben.

De firewall moet ervoor zorgen dat alleen geautoriseerd verkeer van het draadloos naar het bekabeld netwerk mag gaan; al het andere verkeer dat van het draadloos netwerk op het bekabeld netwerk wil komen, moet worden geblokkeerd.

Zet u een draadloos netwerk alleen in voor internettoegang, dan is het verstandig om daarvoor een draadloze router of toegangspunt te gebruiken, die voor een aparte verbinding zorgt. Toegang tot het bekabeld thuis- of bedrijfsnetwerk is dan niet mogelijk.

Voor draadloze netwerken is er extra netwerkapparatuur beschikbaar die specifiek gericht is op het vergroten van de beveiliging van uw netwerk. Zo zijn er apparaten die gebruikers autoriseren via bestaande of eigen databanken, of via communicatie met bijvoorbeeld een externe Active Directory- (Microsoft), LDAP- (adresboekserver) of Radius-databank. Vaak kan deze apparatuur ook dienstdoen als VPN-server.

Andere 'toegangsmanagers', zoals dergelijke apparatuur vaak genoemd wordt, stellen de beheerder in staat om gebruikers alleen op bepaalde toegangspunten toegang te geven.



## Bestands- en printerdeling

Wie op uw draadloos netwerk weet in te loggen en ook meteen toegang krijgt tot uw bekabeld netwerk, kan ook bij uw gedeelde mappen en harde schijven. Om dit te voorkomen, moet u de bestands- en printerdeling uitschakelen, of niet meer door TCP/IP laten afhandelen.

U kunt bestands- en printerdeling onder meer toewijzen aan NetBEUI. Dat stelt u in bij de eigenschappen van uw netwerkverbinding op de computer waar de harde schijven worden gedeeld. U kunt daar een verbinding aanmaken tussen bestands- en printerdeling, en NetBEUI. Vergeet echter niet de verbinding tussen TCP/IP en bestandsdeling te verwijderen.

Denk eraan zo min mogelijk mappen of harde schijven te delen. Mocht u wel iets willen delen, zet de map of schijf dan op Alleen Lezen-bevoegdheid. Stel voor elke harde schijf en map een wachtwoord in. Dit kunt u doen in het venster waarin u ook de gedeelde map of schijf instelt. Gebruik lange wachtwoorden die zowel letters als cijfers bevatten.

Zorg er tot slot voor dat uw router of toegangspunt beschermd is met een wachtwoord. Stel uw eigen wachtwoord in en vertrouw niet op het standaardwachtwoord van de fabrikant. Inbrekers kennen deze wachtwoorden en zullen ze als eerste uitproberen.



## Bereik vergroten

Vaak kunt u door het toegangspunt een andere plek te geven de dekking van uw draadloos netwerk verbeteren. Dikke muren met stalen balken vormen echter nogal eens een spelbreker. Een uitkomst biedt dan de installatie van een zogenoemde WiFi-repeater. Dat is een apparaatje dat u in de buurt van het gebied plaatst waar u geen dekking hebt, waarna de repeater het signaal verlengt. Let er wel op dat u de repeater op hetzelfde kanaal instelt als uw toegangspunt en de SSID van uw originele toegangspunt

ingeeft.

Over het algemeen kunt u met een repeater een dekkingstoename van 150 procent behalen. Een nadeel is echter de vertraging die veroorzaakt wordt op het netwerk. Gebruik daarom niet meer repeaters dan strikt noodzakelijk.



## 802.1X en 802.11i

Het IEEE is druk bezig met de introductie van 802.1x, een beveiligingsset die authenticatie van gebruikers centraal regelt en kan samenwerken met WPA. De standaard kan overweg met meerdere versleutelingen en is opengesteld voor fabrikanten, zodat de implementatie snel kan verlopen. 802.1x maakt gebruik van EAP (Extensible Authentication Protocol), dat we al eerder tegenkwamen bij WPA. Een client die zich aanmeldt op een netwerk waarop 802.1x actief is, moet zich eerst (draadloos) bekendmaken, waarbij alleen 802.1x-verkeer wordt verzonden. Het verzenden van data via HTTP, FTP, SMTP of ander verkeer is op dat moment nog geblokkeerd.

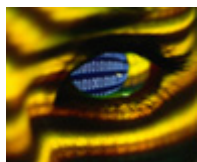
Het voor 802.1x geschikte toegangspunt vraagt de client daarna om een EAP-identiteit, die vervolgens naar de authenticatieserver (een Radius-server) wordt verzonden. Die bepaalt of de client toegang mag krijgen tot het draadloos netwerk of niet.

Standaard is er in de 802.1x-implementatie geen optie voor sleutels of passphrases. Die opties laat het IEEE over aan de markt, ofwel de fabrikanten van routers en toegangspunten. 802.1x, dat vooral geschikt is voor grote bedrijven, belooft voor de toekomst een vereenvoudigde toegangsbeveiliging voor draadloze netwerken.

Afgelopen zomer werd de opvolger van de huidige draadloze beveiligingsstandaarden geïntroduceerd: 802.11i. Het is geen nieuwe draadloze standaard met een andere snelheid en radioband, maar eerder een tweede versie van WPA. Officieel heet de versie dan ook MAC Enhancements for Enhanced Security - officieus WPA2.

802.11i heeft alle eigenschappen van WPA, dat medio 2003 als een soort lapmiddel voor het lekke en onbetrouwbare WEP werd geïntroduceerd. WPA introduceerde toen verbeterde encryptie via TKIP (Temporal Key Integrity Protocol), sleutelrotatie, een consumentenvariant (met eenvoudige installatie) en een zakelijke variant (Radius).

802.11i (WPA2) voegt daar verbeterde versleuteling via AES (Advanced Encryption Standard) aan toe, netwerkondersteuning voor ad hoc en pre-shared secret authentication, waarbij de verificatie plaatsvindt zonder dat er sleutels door de lucht worden getransporteerd. De AES-versleuteling moet - volgens planning - beschikbaar worden in de AES-variant Operation Cipher Block, die ook door de Amerikaanse overheid als vervanger voor de 3DES-versleuteling is aangewezen.



## Hackers en scriptkiddies

Het merendeel van de 'aanvallen' op uw netwerk is het werk van zogenoemde scriptkiddies, jonge computergebruikers die met behulp van kant-en-klare programmatuur en scripts geautomatiseerd zoeken naar slecht beveiligde computers. Dit soort aanvallers is relatief ongevaarlijk, als u er tenminste voor zorgt dat uw computer up-to-date blijft via het regelmatig uitvoeren van Windows Update en het installeren van de nodige servicepacks.

De scriptkiddies gebruiken immers software die bekende veiligheidslekken uitbuit. Als u deze (oude) lekken dicht, zullen ze uw computer links laten liggen - zeker als u deze maatregelen combineert met een goede firewall.

Echte hackers vormen een potentieel grotere bedreiging. Zij gebruiken meestal de nieuwste zwakheden in uw software en zijn zo moeilijker buiten de deur te houden. Hun motivatie om juist u aan te vallen kan zorgwekkend zijn. Onder 'hackers' verstaan we namelijk niet alleen de 'zolderkamernerds', maar ook mensen die bijvoorbeeld uit zijn op geheime informatie over uw bedrijf.

Het verlies van uw administratie, e-mails of klantencontacten kan rampzalig uitpakken voor uw bedrijf. Hackers die het op deze gegevens hebben gemunt, houdt u buiten de deur door uw firewall bewust te kiezen en uitgebreid de tijd te nemen om deze te configureren.

De meeste 'aanvallen' op uw systemen hoeft u echter niet persoonlijk op te vatten. Hackers gebruiken meestal poortscanners voor het scannen van grote reeksen IP-adressen en het opsporen van openstaande services. Ze dringen meestal pas ergens binnen als ze hebben geconcludeerd dat een systeem niet afdoende is beveiligd.



## Hoe werkt een firewall?

Hoewel het concept en de technologie achter firewalls soms nogal complex lijken, zijn de meeste exemplaren verrassend eenvoudig te installeren, te configureren en te onderhouden. Voor we specifieke firewall-methodes bekijken, eerst even wat basisinformatie over de werking van deze poortwachters voor netwerken en pc's.

Het internet draait al sinds de vroege jaren zeventig op TCP/IP, een relatief eenvoudige combinatie van twee protocollen die zorgt voor de adressering en veilige verzending van datapakketjes. IP (Internet Protocol) breekt de datastream die een computer genereert op in kleine pakketjes en voorziet deze van IP-adres- en prioriteitslabels.

TCP (Transmission Control Protocol) garandeert op zijn beurt dat de pakketjes worden verzonden en dat ze daadwerkelijk aankomen op hun bestemmingsadres. Mochten er pakketjes ontbreken, dan wordt het verzoek nogmaals verstuurd. Bij aankomst assembleert TCP de datastroom en geeft deze door aan de ontvangende machine.

Een firewall scheidt uw computer of netwerk van de rest van het internet en controleert de integriteit van alle IP-pakketjes die naar binnen en buiten willen. De firewall accepteert de datastroom en vergelijkt de IP-headers met de door u gedefinieerde firewallregels. Op basis van deze regels worden de datapakketjes doorgelaten of de toegang tot uw domein ontzegd.

Een firewall vertrouwt daarbij op twee basismethodes: hij consulteert vooraf opgestelde lijsten van vertrouwde bronadressen, evenals van toegestane poorten.



## Welk poorten openstellen?

Bij een verbinding met het internet worden er gegevens van en naar de computer verzonden door applicaties zoals de browser en e-mailprogramma's. Daarbij dient de pc te weten welke gegevens voor welk programma bedoeld zijn. Door voor elk programma een aparte poort te reserveren, zijn de gegevens op het juiste 'adres' af te leveren.

Deze primaire toegangspunten tot uw systeem noemen we IP-poorten. Dit zijn virtuele poorten, geen fysieke poorten zoals USB-aansluitingen. Over het algemeen zijn de zend- en ontvangspoorten op de communicerende machines gelijk aan elkaar. In totaal zijn er ruim 65.000 poorten, via welke programma's en services op uw computer kunnen communiceren.

Om uw machine op een degelijke manier af te sluiten, moet uw firewall dus alle poorten in de gaten houden. Gelukkig is er een eenvoudige methode om deze enorme klus te klaren, waarbij alles standaard wordt afgesloten, behalve de poorten die u definieert.

Elke poort heeft een specifiek nummer. Dit nummer is opgeslagen in de IP-headerinformatie, zodat uw firewall de bedoelingen van het IP-pakket kan analyseren. Eén van de bekendste poorten is poort 80, waardoor informatie van het internet via HTTP wordt verzonden en ontvangen. Een ander bekend voorbeeld is poort 21, die gebruikt wordt voor FTP-verkeer.

U dient er bij uw firewall voor te zorgen dat u alleen poorten opent waarvan u zeker weet dat u ze nodig hebt; de overige poorten horen gesloten te zijn. Alleen op die manier kunt u de optimale balans vinden tussen maximale beveiliging en functionaliteit.

Als u een eenvoudige firewall configureert en slechts een beperkt aantal services (zoals een antivirusprogramma of server) wil gebruiken, doet u er verstandig aan de volgende TCP-poorten in uw firewallconfiguratie op te nemen:

- \*
- \* HTTP: poort 80.
- \* FTP: poort 21.
- \* SMTP: poort 25.
- \* POP3: poort 110
- \* Login (Login Host Protocol): poort 49.
- \* Auth (Authentication service): poort 113.
- \* MSN (chatprotocol): poort 1863.

Verder dient u op uw firewall in te stellen dat al het inkomende verkeer wordt geblokkeerd.



## Routers

De beveiliging van de afzonderlijke client-pc's in een netwerk lijkt op papier een goed idee, maar is wel arbeidsintensief, soms kostbaar en zeker niet altijd noodzakelijk. Want als u uw bedrijfsnetwerk achter een centrale server plaatst en een hardwarematige router of gatewayserver hebt, zit daar vaak al een firewall in.

Daarbij komt nog dat een particulier- of klein bedrijfsnetwerk over het algemeen via Network Address Translation (NAT) aan het internet is gekoppeld, waardoor alle computers binnen het netwerk een eigen lokaal IP-adres krijgen, dat wordt toegewezen door de router of gatewayserver.

Voor de computers van hackers ogen IP-verzoeken van deze machines als verzoeken van de gateway; ze zullen eventuele aanvallen daarom op de gateway richten. Als u die goed afschermt met een firewall, hoeft u de aparte clientmachines in het netwerk niet van extra persoonlijke firewalls te voorzien.

De meeste routers die u tegenwoordig bij uw ADSL- of kabelabonnement geleverd krijgt, zijn verrassend geavanceerd. Deze losse, geïntegreerde kastjes maken de verkeersregeling op uw netwerk veel eenvoudiger. Ze bevatten een besturingssysteem, een ingebouwde DHCP-server voor de adressering van uw lokaal netwerk, NAT-functies en hebben veelal een firewall aan boord.

Dankzij gebruikersvriendelijke webinterfaces laten ze zich binnen een half uurtje instellen en testen. De prijzen van dit soort oplossingen zijn tegenwoordig zeer schappelijk: voor nog geen 500 euro sluit u uw bedrijfsnetwerk snel en veilig op het internet aan.

Als u een bedrijfserver met ingebouwde routeringsfunctie hebt - zoals via Windows Internet Connection-sharing - kunt u deze uitrusten met een firewallapplicatie. Het is echter veel veiliger om de router met firewall op een aparte machine onder te brengen en uw server met bedrijfskritische informatie van het internet af te scherm.



## Conclusie

Een honderd procent veilige omgeving is een utopie. De veiligste computer is nog altijd een computer zonder besturingssysteem en toetsenbord, opgeborgen in een kluis. Het veiligste draadloos netwerk is een niet-actief WiFi-netwerk. Dat neemt niet weg dat u door de genoemde maatregelen te nemen zoveel mogelijk zekerheid kunt inbouwen.

WPA in combinatie met EAP lijkt op dit moment de veiligste authenticatiemogelijkheid voor draadloze netwerken, maar is voor consumenten soms iets te complex. Een combinatie van WEP of WPA en een deel van bovenstaande procedures is een bruikbaar alternatief.

In extreem kwetsbare omgevingen is het niet verstandig een draadloos netwerk te implementeren. En voor alleen internettoegang is een draadloos netwerk in een eigen subnet met een strenge firewall een must.

Voor elk draadloos netwerk, of het nu in uw bedrijf of bij u thuis draait, raden we aan om SSID-broadcast uit te schakelen en de Mac-adresfiltering te activeren. Verder is het verstandig om een DHCP-server in de router uit te schakelen, ook al is die nog zo handig.

Als alle clients een vast (statisch) IP-adres gebruiken, is uw netwerk voor een beginnende hacker of hobbyist al iets moeilijker binnen te dringen.

Als iemand echter vastbesloten is in te breken op uw draadloos netwerk, dan lukt dat bijna altijd. Maar hebt u een goed beveiligd netwerk, dan zullen negen van de tien hackers liever een poging wagen bij het netwerk even verderop, dat wagenwijd openstaat.