
Guia de segurança de redes wireless

Postado por Nikon - 2007/06/22 04:13

Eu tinha muitas duvidas em relação a como proteger a minha rede wireless, achei no forum hardmob esse guia muito bem feito pelo usuario ThunderBolt.

Tendo em vista o grande número de tópicos presentes aqui no Telefonía, TV, Rede e Conectividade sobre esse tema, vou tentar fazer um guia rápido de configuração de redes sem fio. Este guia vai ter como base um WRT54G com a firmware DD-WRT e um modem virtua, mas eu vou tentar usar termos mais gerais, para que este guia possa ter aplicação em qualquer roteador sem fio.

Antes de mais nada, uma breve introdução as redes wireless e porque precisamos proteger a nossa rede contra os amigos do alheio.

As redes wireless finalmente se popularizaram. Hoje é possível comprar um roteador sem fio por até R\$150,00, o que facilitou para que diversas pessoas conseguissem adquirir um aparelho. Uma conexão wireless se estabelece toda vez que dois ou mais aparelhos se comunicam sem a presença de cabos, ou seja, usando o espaço aberto como meio de transmissão de dados. Justamente por esse fato, o sinal de uma rede sem fio pode chegar não apenas aos computadores desejados quanto a um outro computador que a priori não deveria fazer parte da rede. Por esse motivo foi necessário o desenvolvimento de tecnologias de segurança para que apenas os computadores desejados tenham acesso a rede.

Todas as configurações são feitas através de uma interface WEB, que todos os roteadores sem fio possuem. Cada marca tem uma interface diferente, portanto procure entre os diversos menus pelos termos de segurança. Para acessar a página de configuração do seu modem, basta abrir uma página de internet e digitar o endereço IP do roteador. No caso de um WRT54G com DD-WRT, o endereço é o <http://192.168.1.1>

Para descobrir qual é o endereço do seu modem, abra um console do MS-DOS (no win 2k/XP clique em iniciar depois em executar, digite cmd e aperte enter), digite ipconfig e aperte enter. Vai aparecer a descrição de todas as placas de rede que estão ativas e conectadas no seu computador. o endereço de IP que estiver na linha "Gateway padrão" é o endereço do seu roteador. Cada roteador também tem um nome de usuário e senha padrão. Para descobrir o seu, consulte o google ou o manual dele.

Vou apresentar agora os níveis de proteção disponíveis e as configurações mais recomendadas:

Primeiro nível de Segurança: O primeiro nível de proteção é o próprio nome da sua rede sem fio, conhecido como SSID. A proteção consiste em você permitir que o nome da sua rede seja divulgado ou não (ou seja, a rede é detectada ou não pelos PCs com wi-fi). Como hoje em dia já existem níveis bem maiores de proteção, não tem problemas em divulgar o nome da sua rede. "Esconder" pouco adianta, pois já existem programas que monitoram o espaço ao redor de um dispositivo WI-Fi e conseguem detectar pacotes de rede wireless, encontrando assim a rede.

Na maioria dos roteadores e no WRT54G com DD-WRT, essa função é conhecida como SSID broadcast, com a opção de Enable e Disable. Portanto, para SSID Broadcast escolha a opção Enable

Segundo nível de proteção: A proteção de segundo nível é a mais importante: A criptografia (ou encriptação) do sinal wireless. Normalmente existem 4 opções. São elas:

Nenhum ou Disabled: É a opção padrão e nunca deve ser utilizada, pois a rede fica muito vulnerável. Muitas pessoas deixam seus roteadores desprotegidos, confiando na proteção de redes VPN. Isso não deve ser feito, pois o hacker fica com liberdade de interceptar os pacotes e assim tentar quebrar a proteção.

WEP: É a sigla de Wired Equivalent Privacy ou Privacidade Equivalente às Cabeadas. Foi a primeira tentativa organizada de se trazer segurança para redes wireless. Contudo essa proteção se mostrou falha com o passar do tempo, e só deve ser utilizada se um ou mais componentes da rede não ter suporte aos outros tipos de criptografia. Se tiver que utilizar a WEP, opte por uma chave de proteção de 104 bits.

WPA: É a segunda tentativa de proteção de redes wireless, que foi criada para corrigir as falhas existentes na WEP. Significa Wi-Fi Protected Access (Acesso protegido para redes Wi-Fi). É uma proteção muito melhor que a WEP, pois substitue a chave hexadecimal de tamanho fixo da WEP por uma frase-senha (passphrase) que deve ser previamente configurada pelo usuário. A autenticação pode ser feita de duas maneiras: Por um protocolo de chaves temporárias (TKIP), o mesmo utilizado na WEP, mas com mudanças visando aumentar a segurança ou por um servidor externo de autenticação (RADIUS) que é usado mais em ambientes corporativos. Tem a vantagem de ser compatível com equipamentos WEP necessitando apenas de um update de firmware. Seu único ponto fraco é poder ser forçada, ou seja, alguém pode ficar tentando diversas frases até conseguir. Para evitar isso, use frases longas e não triviais (nada de usar o sobrenome da família, por exemplo). Se bem configurado, o WPA já é um nível muito bom de proteção.

WPA2: É o maior nível de proteção para redes wireless domésticas. Seu funcionamento é muito parecido com o WPA, mas ele abandona o protocolo de chaves temporárias (TKIP) a favor de um protocolo de encriptação mais avançado chamado AES - Advanced Encryption Standard (Padrão avançado de encriptação), que protege ainda mais a autenticação nas redes wireless. Por utilizar o AES, o WPA2 não é compatível com equipamentos WEP. Ele também proporciona a autenticação via servidor externo (RADIUS).

Se o seu router tiver suporte a WPA2 e a AES, essa é a melhor opção. Não se esqueça de usar uma passphrase longa e não trivial.

No WRT54G + DD-WRT, na aba "Wireless Security" que fica dentro da aba "Wireless", no campo Security Mode selecione WPA2 Shared Key Only e em WPA Algorithms selecione AES. No campo "WPA shared key" coloque a frase-senha. Essa frase deve ser configurada também em cada computador que vai acessar a rede via conexões wireless.

Terceiro nível de proteção ou proteção adicional: Após configurar o nível de encriptação, podemos aumentar a segurança da rede wireless limitando a faixa de IPs disponíveis e/ou Filtrando os endereços de MAC. Atenção! Isto deve ser encarado como segurança adicional! A mais importante é a segurança de encriptação!

MAC Filter: O Endereço de MAC é um número que identifica cada placa de rede. Alguns roteadores permitem cadastrar os endereços de rede das placas wireless de dispositivos conectados a ele em uma lista, e só permitir o acesso a rede dos endereços cadastrados nesta lista. É uma proteção que nunca deve ser encarada como principal, porque um hacker pode descobrir os endereços de MAC conectados e depois alterar o seu próprio para um que tenha acesso liberado. No WRT54G + DD-WRT, ele é configurado na aba "MAC filter" dentro da parte "Wireless".

Limitar IP range: Consiste em liberar apenas a quantidade de endereços de IP de acordo com o número de computadores que acessa a rede wireless. Isso é feito na configuração do protocolo DHCP. É uma proteção que só funciona quando todos os PCs wireless estão ligados na rede e se o hacker não fixar o IP da placa de rede dele. Ou seja, é uma proteção muito baixa e que na maioria das vezes não é utilizada.

No WRT54G + DD-WRT, isto é feito na aba "Basic Setup", dentro da aba "Setup". É só ajustar o campo "Maximum DHCP users" para a quantidade de usuários wireless da sua rede"

Esses são os níveis de proteção em redes wireless.

Agora para quem tem acesso via cabo, segue uma funcionalidade dos roteadores sem fio muito útil: A Clonagem de endereço de MAC:

Clonar endereço de MAC: É um recurso que copia o endereço da placa de rede do computador para a placa de rede da saída de internet do roteador (porta WAN). Assim o provedor de internet "encheria" o endereço físico da placa de rede do computador e não o endereço físico do roteador. Isso é útil para sistemas a cabo (Virtua) que usam o endereço MAC dos computadores como forma de autenticação de conexão.

No WRT54G + DD-WRT, ele fica na aba MAC address clone, dentro de Setup.

Basicamente é isso! Acréscimos e correções são sempre bem vindos!

's

=====

Re:Guia de segurança de redes wireless

Postado por admin - 2007/06/22 09:49

Muito bom! Posso colocar como artigo e voce como autor?

=====

Re:Guia de segurança de redes wireless

Postado por luizgeoffroy - 2007/06/22 13:28

Eu já copieei aqui para meu HD. Valeu!

Postagem editada por: luizgeoffroy, em: 2007/06/22 13:28

=====

Re:Guia de segurança de redes wireless

Postado por Nikon - 2007/06/22 18:08

admin escreveu:

Muito bom! Posso colocar como artigo e voce como autor?

Acho que não teria problema de colocar como artigo, mas eu não posso levar o credito por uma coisa que não fiz, o justo é você postar o artigo e dar o credito para o Thunderbolt que fez esse excelente guia!

Segue abaixo, o link do guia no forum do Hardmob:

<http://www.hardmob.com.br/showthread.php?t=297532>

Ps:Acharia legal você avisar ele que vai postar o guia, não custa nada dar os parabens pelo excelente trabalho que ele fez!

Abs

Postagem editada por: Nikon, em: 2007/06/22 18:26
