# Cinco dicas para fortalecer sua rede sem fio

## Objetivo

O rádio é o componente físico do ponto de acesso sem fio (WAP) que cria uma rede sem fio. As configurações de rádio no WAP e no roteador sem fio controlam o comportamento do rádio e determinam os sinais que o dispositivo transmite. Embora as redes Wi-Fi sejam convenientes, elas podem se tornar vulneráveis a clientes sem fio que usam a largura de banda e aumentar os riscos de segurança quando não são protegidas corretamente. É recomendável ter as seguintes configurações para segurança adicional:

- Habilitar Criptografia de Dados
- Permitir que apenas dispositivos conhecidos se conectem à rede com Filtragem de Controle de Acesso ao Meio (MAC - Media Access Control)
- Altere a senha da rede sem fio regularmente
- Habilitar firewalls internos
- Ocultar o identificador do conjunto de serviços (SSID)

Este artigo tem como objetivo fornecer dicas que seriam úteis para proteger sua rede sem fio.

## Dispositivos aplicáveis

- Série RV
- Pontos de acesso sem fio
- Comunicações Unificadas da Cisco

## Fortaleça sua rede sem fio

### Habilitar Criptografia de Dados

Os dispositivos de rede sem fio normalmente suportam algum tipo de criptografia para poder se conectar a uma rede sem fio com segurança. Sempre que possível, use o WPA (Wi-Fi Protected Access) ou o WPA2 (Wi-Fi Protected Access 2), pois eles oferecem melhor segurança com o método de criptografia AES (Advanced Encryption Standard). As etapas para habilitar a criptografia de dados diferem um pouco por dispositivo. Para obter um guia para ativar a segurança sem fio em um roteador sem fio, clique aqui. Para obter um guia para habilitar a segurança sem fio em um ponto de acesso, clique aqui.

### Permitir somente dispositivos conhecidos com filtragem de MAC

A filtragem de endereços MAC permite listar os endereços MAC dos clientes sem fio conectados à sua rede, criando efetivamente uma lista de dispositivos apenas conhecidos. Você pode, então, conceder ou negar aos dispositivos acesso à rede, dependendo de sua necessidade. Os endereços MAC que não estão na lista são automaticamente excluídos da condição. As etapas para habilitar a filtragem de endereços MAC diferem um pouco por dispositivo. Para obter um guia para ativar a filtragem de endereços MAC em um roteador sem fio, clique aqui. Para obter um guia para habilitar a filtragem de endereços MAC em um ponto de acesso sem fio, clique aqui.

## Altere a senha da rede sem fio regularmente

A configuração de uma senha de rede sem fio é a maneira mais fácil de proteger uma rede sem fio. Eles frequentemente precisam ser sincronizados com outros pontos de acesso sem fio na rede, para uma conexão sem fio contínua. As senhas de rede sem fio normalmente precisam ser alteradas regularmente para garantir que apenas dispositivos autorizados estejam conectados à rede. As etapas de configuração de uma senha de rede sem fio diferem um pouco de acordo com o dispositivo. Para obter um guia sobre como definir as configurações sem fio em um roteador, clique aqui. Para obter um guia sobre como alterar a senha de um ponto de acesso, clique aqui.

## Habilitar firewalls integrados

Muitos roteadores sem fio, como o Roteador VPN Wireless-N RV130W, têm firewalls integrados que impedem que tráfego mal-intencionado entre na sua rede. As etapas de ativação do firewall são ligeiramente diferentes para cada dispositivo. Para obter um guia sobre como ativar o firewall em um roteador, clique aqui.

## Ocultar o SSID

A desativação da transmissão de SSID torna a rede invisível para um dispositivo quando procura uma rede sem fio. Assim como configurar uma senha sem fio, ocultar o SSID dificulta a conexão à rede sem fio, já que a conexão terá que ser configurada manualmente no dispositivo. As etapas de desabilitação da transmissão de SSID diferem um pouco por dispositivo. Para obter um guia sobre como desativar a transmissão de SSID em um ponto de acesso, clique aqui. Para obter um guia sobre como desativar a transmissão de SSID em um roteador sem fio, clique aqui.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.