Configuração básica de firewall no RV215W

Objetivo

Um firewall é um conjunto de recursos projetados para manter uma rede segura. Um roteador é considerado um firewall de hardware forte. Isso se deve ao fato de que os roteadores podem inspecionar todo o tráfego de entrada e descartar todos os pacotes indesejados.

Este artigo explica como definir as configurações básicas de firewall no RV215W.

Dispositivos aplicáveis

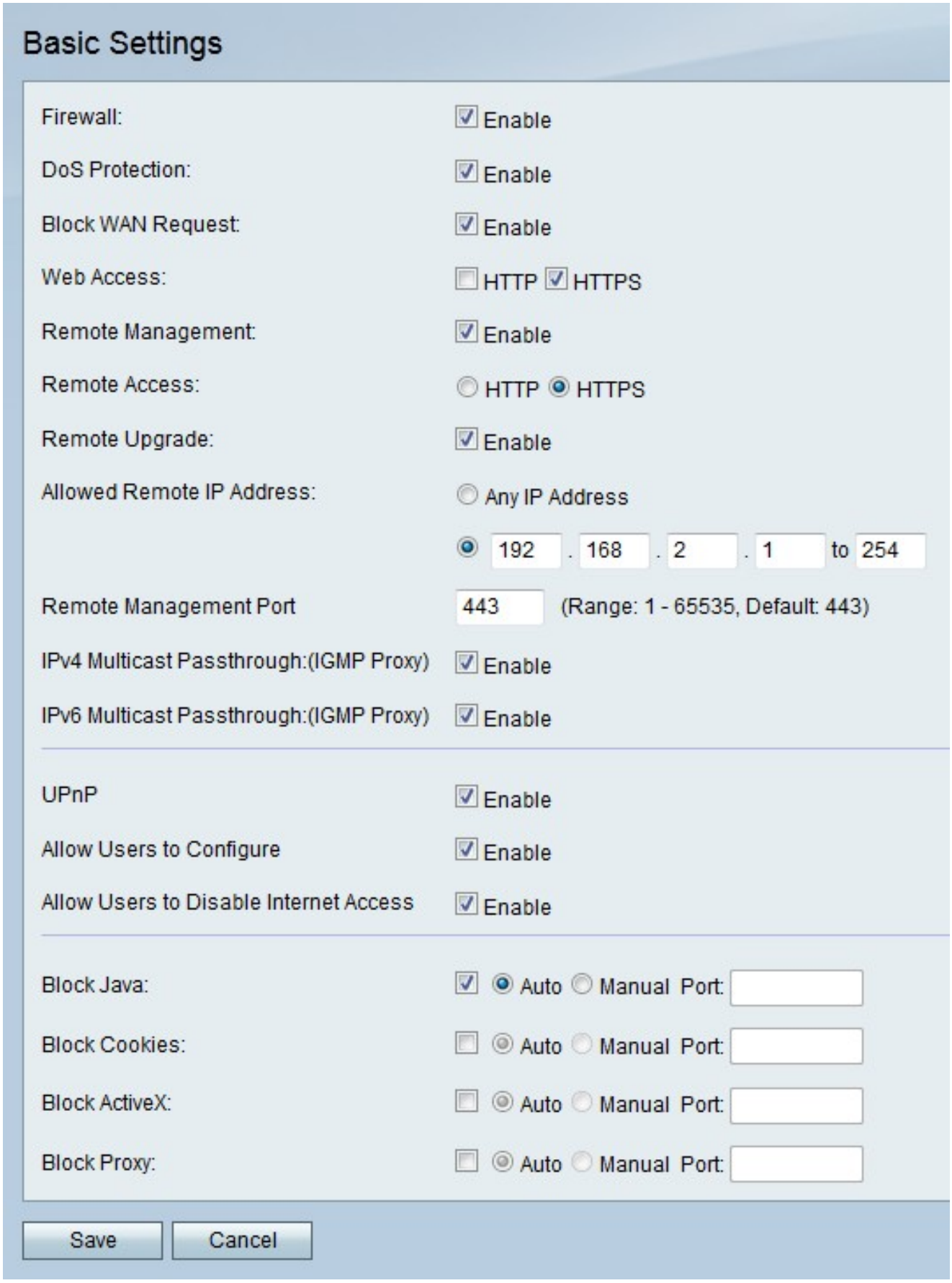
RV215W

Versão de software

•1.1.0.5

Configurações básicas

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Firewall > Basic Settings**. A página *Configurações básicas* é aberta:



Etapa 2. Marque **Enable (Habilitar)** no campo Firewall para habilitar a configuração de firewall no RV215W.

Etapa 3. Marque **Enable** no campo DoS Protection (Proteção do DoS) para habilitar a proteção DoS (Negação de Serviço) no RV215W. A proteção DoS é usada para impedir que uma rede seja atacada por negação de serviço distribuído (DDoS). Os ataques de DDoS

têm o objetivo de inundar uma rede até o ponto em que os recursos da rede ficam indisponíveis. O RV215W usa proteção DoS para proteger a rede através da restrição e remoção de pacotes indesejados.

Etapa 4. Marque **Enable** no campo Block WAN Request (Bloquear solicitação de WAN) para bloquear todas as solicitações de ping para o RV215W da WAN.

Etapa 5. Marque a caixa de seleção que corresponde ao tipo desejado de acesso à Web que pode ser usado para se conectar ao firewall no campo Acesso à Web.

Etapa 6. Marque **Habilitar** no campo Gerenciamento remoto. O gerenciamento remoto permite o acesso do RV215W a partir de uma rede WAN remota.

Passo 7. Clique no botão de opção que corresponde ao tipo desejado de acesso à Web que pode ser usado para se conectar ao firewall da WAN remota no campo Acesso remoto.

Etapa 8. Marque **Remote Upgrade** para permitir que usuários remotos atualizem o RV215W.

Etapa 9. Clique no botão de opção que corresponde aos endereços IP desejados que têm permissão para acessar o RV215W remotamente no campo Allowed Remote IP Address (Endereço IP remoto permitido).

Qualquer endereço IP — Todos os endereços IP são permitidos.

Endereço IP — Insira um intervalo de endereços IP permitidos.

Etapa 10. Insira uma porta na qual o acesso remoto é permitido no campo Remote Management Port (Porta de gerenciamento remoto). Um usuário remoto deve usar a porta remota para acessar o dispositivo.

Note: O formato para acesso remoto é https://<*remote-ip*>:<*remote-port*>

Etapa 11. Marque **Enable** no campo IPv4 Multicast Passthrough (Passagem Multicast IPv4) para permitir que o tráfego multicast IPv4 passe pelo RV215W da Internet. O multicast IP é um método usado para enviar datagramas IP a um grupo designado de receptores em uma única transmissão.

Etapa 12. Marque **Enable** no campo IPv6 Multicast Passthrough (Passagem Multicast IPv6) para permitir que o tráfego multicast IPv6 passe pelo RV215W da Internet.

Etapa 13. Marque **Enable (Habilitar**) no campo UPnP para habilitar o UPnP (Universal Plug and Play). O UPnP permite a descoberta automática de dispositivos que podem se comunicar com o RV215W.

Etapa 14. Marque **Habilitar** no campo Permitir que os usuários configurem para permitir que os usuários com dispositivos compatíveis com UPnP configurem regras de mapeamento de portas UPnP. O mapeamento de portas ou o encaminhamento de portas é usado para permitir comunicações entre hosts externos e serviços fornecidos em uma LAN privada.

Etapa 15. Marque **Enable** no campo Allow Users to Disable Internet Access (Permitir que os usuários desabilitem o acesso à Internet) para permitir que os usuários desabilitem o acesso à Internet para o dispositivo.

Etapa 16. Marque **Bloquear Java** para bloquear o download de miniaplicativos java. Os miniaplicativos Java feitos para fins mal-intencionados podem representar uma ameaça à segurança de uma rede. Após o download, um miniaplicativo java hostil pode explorar

recursos de rede. Clique no botão de opção correspondente ao método de bloqueio desejado.

Auto — Bloqueia automaticamente o java.

Porta manual — Insira uma porta específica na qual bloquear o java.

Etapa 17. Marque **Bloquear cookies** para filtrar cookies de serem criados por um site. Os cookies são criados por sites para armazenar informações desses usuários. Os cookies podem rastrear o histórico do usuário na Web, o que pode levar a uma invasão de privacidade. Clique no botão de opção correspondente ao método de bloqueio desejado.

Auto — Bloqueia automaticamente cookies.

Porta manual — Insira uma porta específica na qual bloquear cookies.

Etapa 18. Marque **Bloquear AtiveX** para bloquear o download de miniaplicativos AtiveX. AtiveX é um tipo de miniaplicativo que não tem segurança. Quando um miniaplicativo AtiveX é instalado em um computador, ele pode fazer qualquer coisa que um usuário possa fazer. Ele pode inserir código prejudicial no sistema operacional, navegar em uma intranet segura, alterar uma senha ou recuperar e enviar documentos. Clique no botão de opção correspondente ao método de bloqueio desejado.

Auto — Bloquear automaticamente o AtiveX.

Porta manual — Insira uma porta específica na qual bloquear AtiveX.

Etapa 19. Marque **Bloquear proxy** para bloquear servidores proxy. Os servidores proxy são servidores que fornecem um link entre duas redes separadas. Os servidores proxy mal-intencionados podem gravar todos os dados não criptografados enviados a eles, como logins ou senhas. Clique no botão de opção correspondente ao método de bloqueio desejado.

Automático — Bloquear automaticamente servidores proxy.

Porta manual — Insira uma porta específica na qual os servidores proxy serão bloqueados.

Etapa 20. Click **Save**.