Como definir configurações básicas de firewall no RV130 e RV130W

Objetivo

As Configurações Básicas do Firewall podem proteger sua rede criando e aplicando regras que o dispositivo usa para bloquear e permitir seletivamente o tráfego de entrada e saída da Internet.
Recursos como Universal Plug and Play facilitam a conexão de dispositivos entre si na rede sem configurações adicionais.

O UPnP (Universal Plug and Play) permite a descoberta automática de dispositivos que podem se comunicar com o dispositivo. O bloqueio de conteúdo pode ajudar a proteger o computador, pois determinados conteúdos podem ser enviados para o dispositivo, o que pode comprometer a segurança ou infectar o computador com software mal-intencionado. A capacidade de bloquear conteúdo específico nas portas de sua escolha é útil para maior segurança de firewall.

O objetivo deste documento é mostrar a você como definir as configurações básicas do firewall no RV130 e RV130W.

Dispositivos aplicáveis

RV130

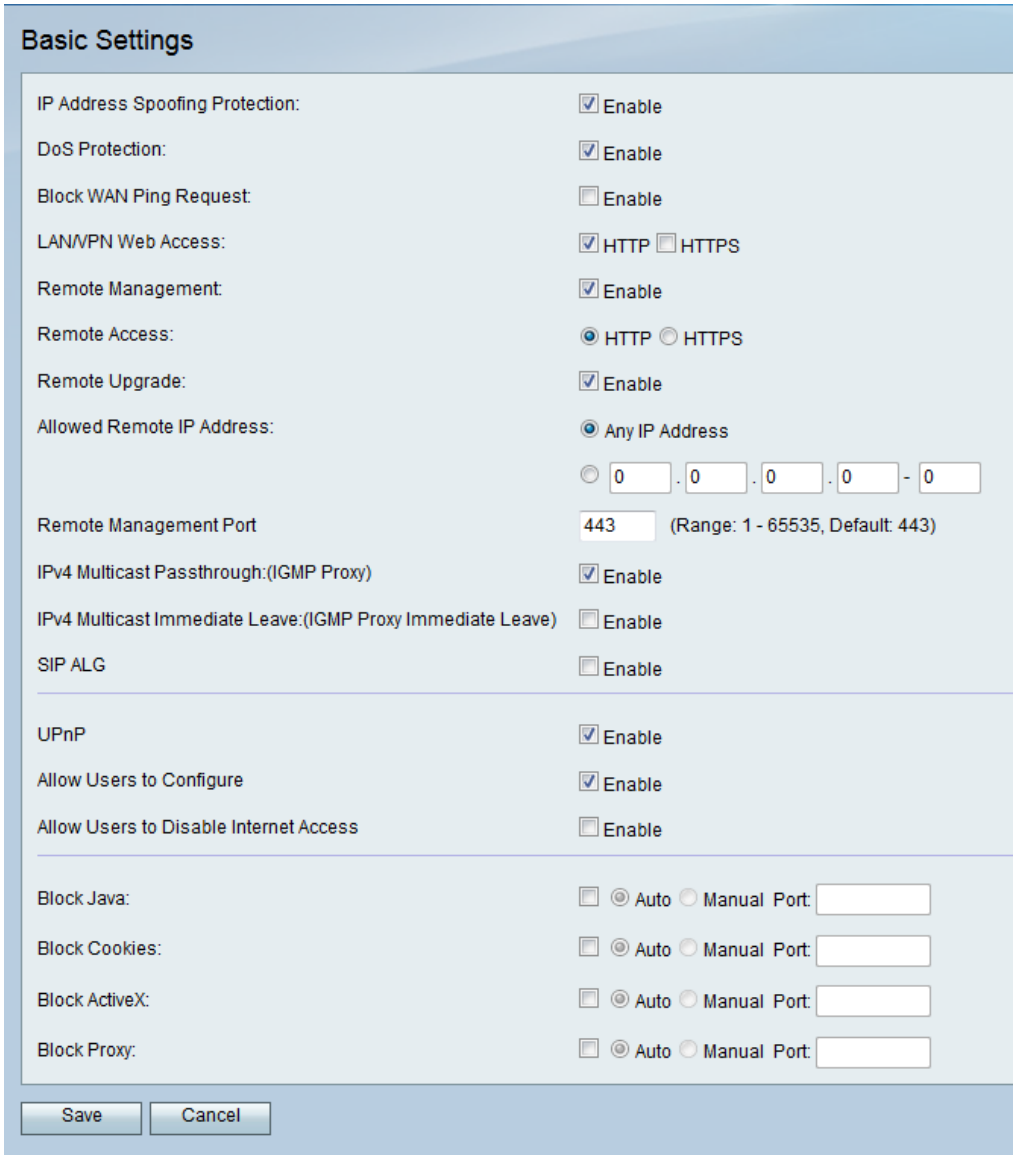
RV130W

Versão de software

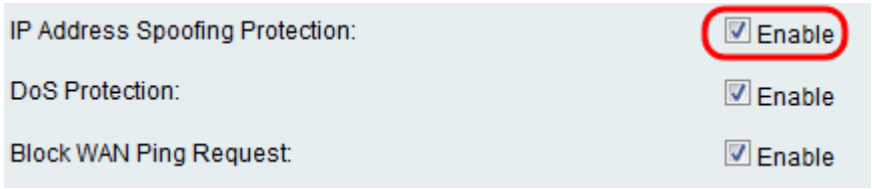
•v1.0.1.3

Definindo configurações básicas de firewall

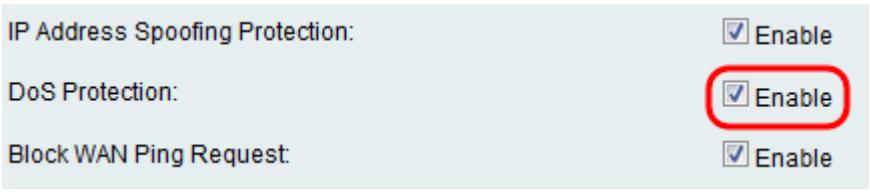
Etapa 1. Inicie a sessão no utilitário de configuração da Web e selecione **Firewall > Basic Settings**. A página Basic Settings é aberta:



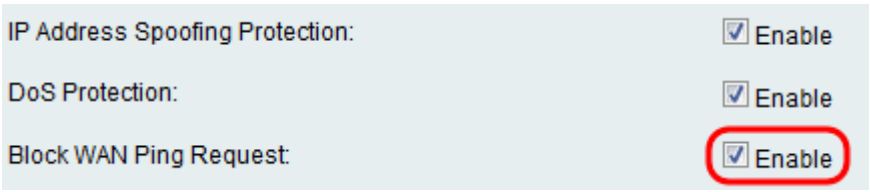
Etapa 2. No campo *IP Address Spoofing Protection*, marque a caixa de seleção **Enable** para proteger sua rede contra falsificação de endereço IP. A Falsificação de endereço IP ocorre quando um usuário não autorizado tenta obter acesso a uma rede ao se passar por outro dispositivo confiável usando seu próprio endereço IP. É recomendável habilitar *IP Address Spoofing Protection (Proteção contra falsificação de endereço IP).*



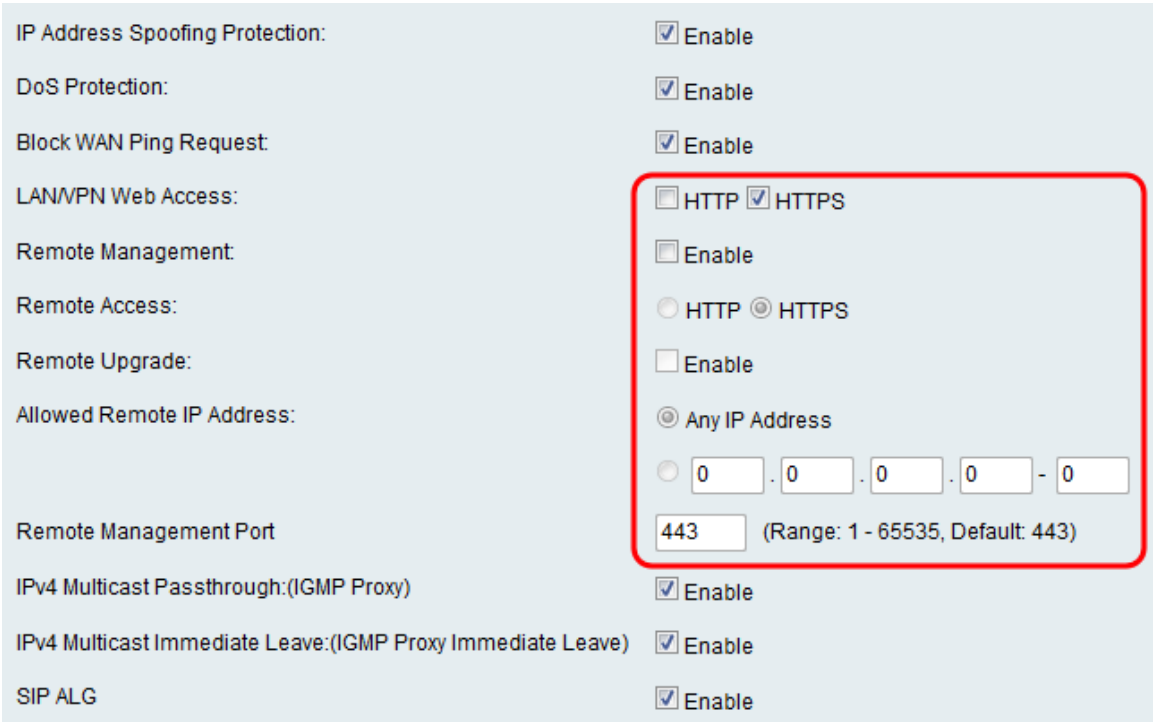
Etapa 3. No campo *DoS Protection*, marque a caixa de seleção **Enable** para proteger sua rede de ataques de negação de serviço. A Proteção contra Negação de Serviço é usada para proteger uma rede de um ataque de negação de serviço distribuído (DDoS). Os ataques de DDoS servem para inundar uma rede até o ponto em que os recursos da rede se tornam indisponíveis.



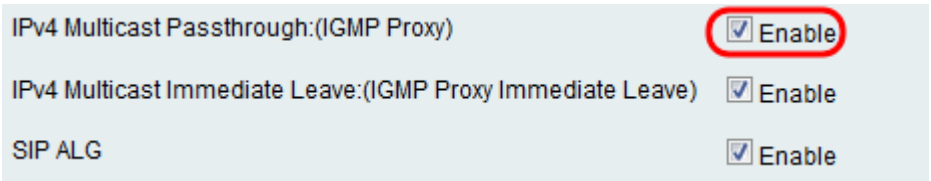
Etapa 4. No campo *Block WAN Ping Request*, marque a caixa de seleção **Enable** para interromper as solicitações de ping ao seu dispositivo a partir da rede WAN externa.



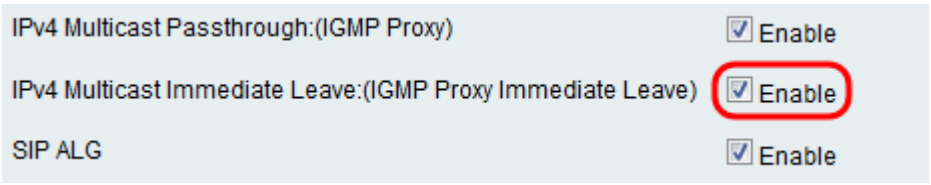
Etapa 5. Os campos listados de *LAN/VPN Web Access to Remote Management Port* são usados para configurar LAN e Remote Management Web Access. Para saber mais sobre essas configurações, consulte Configuração de LAN e Acesso via Web de Gerenciamento Remoto no RV130 e RV130W.



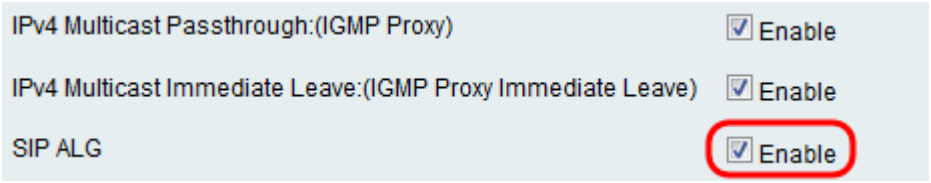
Etapa 6. No campo *IPv4 Multicast Passthrough:(IGMP Proxy)*, marque a caixa de seleção **Enable** para habilitar a passagem multicast para IPv4. Isso encaminhará pacotes IGMP de grupo da rede WAN externa para sua LAN interna.



Etapa 7. No campo *IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)*, marque a caixa de seleção **Enable** para habilitar o Multicast Immediate Leave. Habilitar a licença imediata garante que o gerenciamento de largura de banda ideal seja fornecido aos hosts em sua rede, mesmo durante momentos de uso simultâneo de grupos multicast.



Etapa 8. No campo *Protocolo de Iniciação da Sessão (SIP - Session Initiation Protocol) Gateway da Camada de Aplicação (ALG - Application Layer Gateway)*, marque a caixa de seleção **Enable** para permitir que o tráfego do Protocolo de Iniciação da Sessão (SIP - Session Initiation Protocol) passe pelo Firewall. O Protocolo de Iniciação de Sessão (SIP - Session Initiation Protocol) equipe as plataformas para sinalizar a configuração de chamadas de voz e multimídia sobre redes IP. O Application Layer Gateway (ALG) ou também conhecido como Application Level Gateway é um aplicativo que converte informações de endereço IP dentro do payload de um pacote de aplicativos.

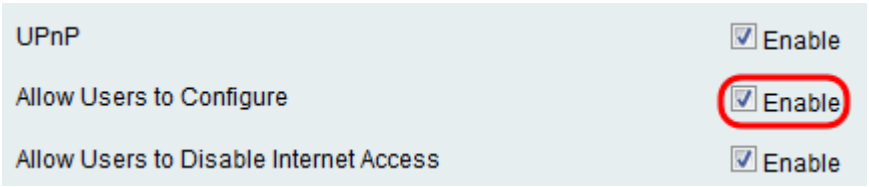


Note: O dispositivo suporta um máximo de 256 sessões ALG SIP.

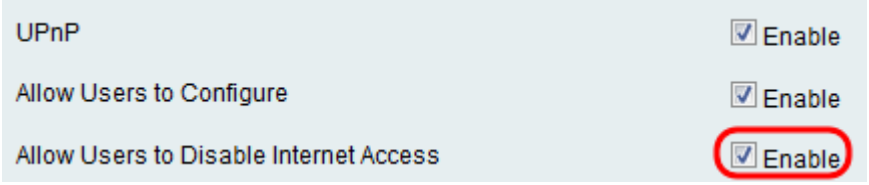
Configuração do Universal Plug and Play

Etapa 1. No campo *UPnP*, marque **Enable** para ativar o UPnP (Universal Plug and Play).

Etapa 2. No campo *Allow Users to Configure*, marque a caixa de seleção **Enable** para permitir que as regras de mapeamento de porta UPnP sejam definidas por usuários que tenham suporte UPnP habilitado em seus computadores ou outros dispositivos UPnP habilitados. Se desabilitado, o dispositivo não permite que o aplicativo adicione a regra de encaminhamento.



Etapa 3. No campo *Allow Users to Disable Internet Access*, marque a caixa de seleção **Enable** para permitir que os usuários desabilitem o acesso à Internet.



Bloqueando conteúdo

Etapa 1. Marque a caixa de seleção no campo que corresponde ao conteúdo que você deseja bloquear no dispositivo.

As opções disponíveis são definidas da seguinte forma:

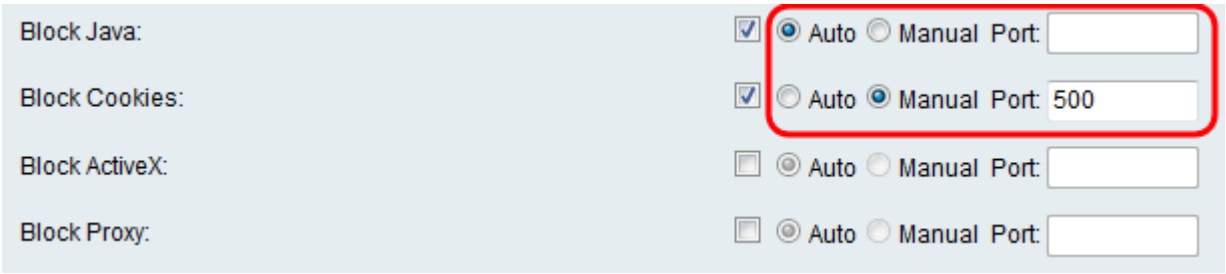
·Bloquear Java — Bloqueia o download de miniaplicativos Java.

·Bloquear cookies — Bloqueia o dispositivo de receber informações de cookies de páginas da Web.

·Bloquear AtiveX — Bloqueia miniaplicativos AtiveX que podem estar presentes ao usar o Internet Explorer no sistema operacional Windows.

·Bloquear proxy — Impede que o dispositivo se comunique com dispositivos externos por meio de um servidor proxy. Isso impede que o dispositivo contorne qualquer regra de firewall.

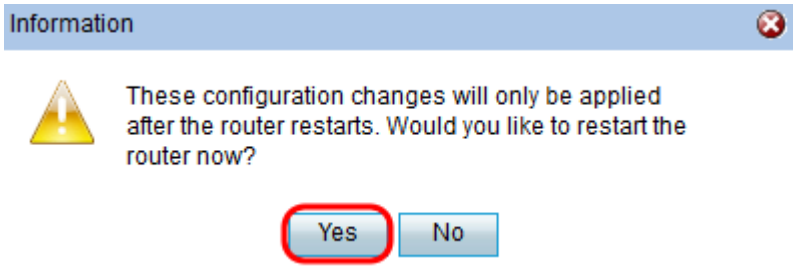
Etapa 2. Selecione o botão de opção **Auto** para bloquear automaticamente todas as ocorrências desse conteúdo específico ou clique no botão de opção **Manual** e insira uma porta específica no campo correspondente no qual o conteúdo será bloqueado.



Note: Você pode digitar qualquer número desejado no intervalo (1-65535) para o valor da porta.

Etapa 3. Clique em **Salvar** para salvar suas configurações.

Etapa 4. Uma janela será exibida solicitando que você reinicie o roteador. Clique em **Yes** para reiniciar o roteador e aplicar as alterações.


Information
These configuration changes will only be applied after the router restarts. Would you like to restart the router now?
Yes
No

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.