Configuração SNMP no roteador VPN RV315W

Objetivo

O Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) é um protocolo TCP/IP para gerenciamento de rede. O SNMP permite que os administradores supervisionem o desempenho da rede, as taxas de erro. O SNMP também pode mapear a disponibilidade da rede. A estrutura SNMP consiste em três elementos; um gerenciador SNMP, um agente SNMP e um MIB. A função do gerenciador SNMP é controlar e monitorar as atividades dos hosts de rede que utilizam SNMP. O agente SNMP está dentro do software do dispositivo e auxilia na manutenção de dados para gerenciar o sistema. Por fim, a Base de Informações de Gerenciamento (MIB - Management Information Base) é uma área de armazenamento virtual para informações de gerenciamento de rede. Esses três se combinam para monitorar e gerenciar os dispositivos em uma rede.

Este artigo ajuda a explicar como configurar o SNMP no RV315W VPN Router.

Dispositivo aplicável

RV315W

Versão de software

•1.01.03

Configurar SNMP

O SNMP v1 é a versão original do SNMP, que não tem certas funcionalidades e só funciona em redes TCP/IP, o SNMP v2 é uma iteração melhorada de v1. O SNMP v1&v2 deve ser escolhido somente para redes que utilizam SNMPv1 ou SNMPv2. O SNMP v3 é o mais novo padrão de SNMP e aborda muitos dos problemas de SNMP v1 e v2. Em particular, ele lida com muitas das vulnerabilidades de segurança de v1 e v2. O SNMP v3 também permite que os administradores mudem para um padrão SNMP comum.

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Gerenciamento do sistema > SNMP**. A página *SNMP* é aberta:

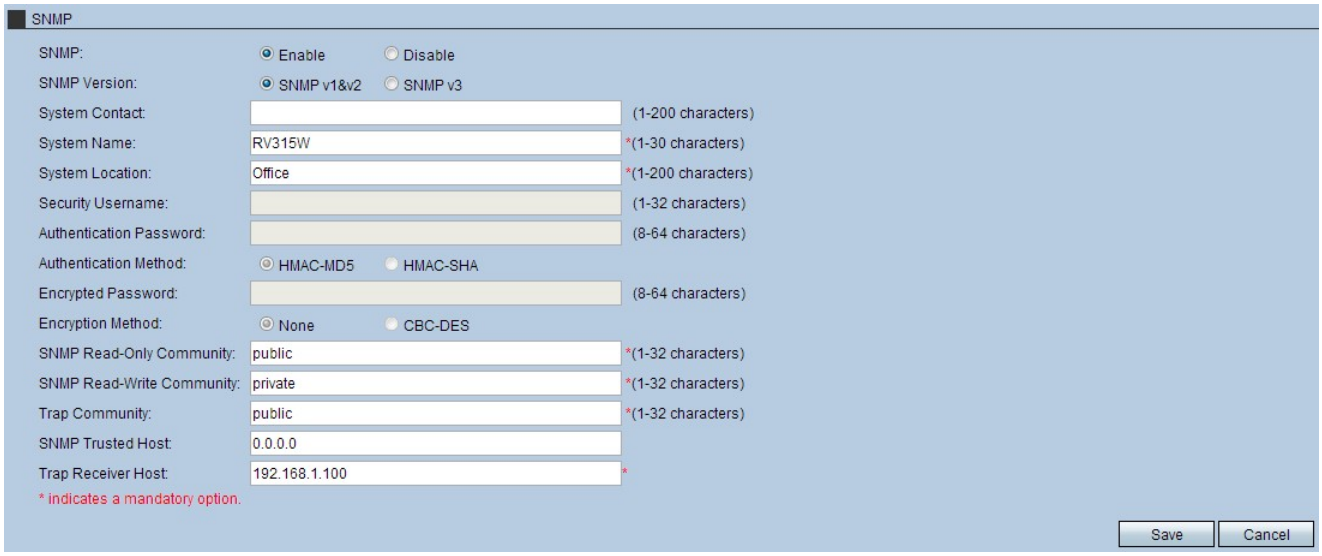
Etapa 2. Clique no botão de opção **Enable** para ativar o SNMP.

Etapa 3. Clique no botão de opção desejado para a versão SNMP.

SNMP v1&v2 — SNMP v1 é a iteração original do SNMP e não possui determinada funcionalidade, SNMP v2 é a versão mais recente que melhora a funcionalidade, mas essa opção deve ser escolhida somente para redes que executam SNMP v1 ou SNMP v2.

SNMP v3 — SNMP 3 é a versão mais recente, que permite que os administradores utilizem um padrão. Essa opção deve ser escolhida porque corrige muitas falhas de segurança em v1 e v2.

Configurar SNMP para SNMP v1 e v2



Etapa 4. (Opcional) Insira as informações de contato no campo Contato do sistema. Esse é o indivíduo para entrar em contato para obter assistência de rede.

Etapa 5. Digite um nome no campo Nome do sistema. Este é o nome alocado para a configuração SNMP.

Etapa 6. Insira um local no campo System Location (Local do sistema). É aqui que o sistema está localizado.

Passo 7. Insira uma comunidade no campo SNMP Read-Only Community. Este é o

parâmetro do cliente para acesso somente leitura da configuração SNMP.

Etapa 8. Insira uma comunidade no campo SNMP Read-Write Community. Este é o parâmetro do cliente para acesso de leitura e gravação da configuração SNMP.

Etapa 9. Insira uma comunidade no campo Comunidade de interceptações. Essa é a comunidade com a capacidade de utilizar armadilhas SNMP. As interceptações são notificações direcionadas enviadas ao administrador. O Traps permite que o administrador gerencie cada dispositivo permitindo que o usuário o notifique usando uma interceptação.

Etapa 10. Insira um host no campo SNMP Trusted Host. Este é o endereço IP do host confiável para a configuração SNMP.

Etapa 11. Insira um host no campo Trap Receiver Host. Esse é o endereço IP do administrador para receber as armadilhas.

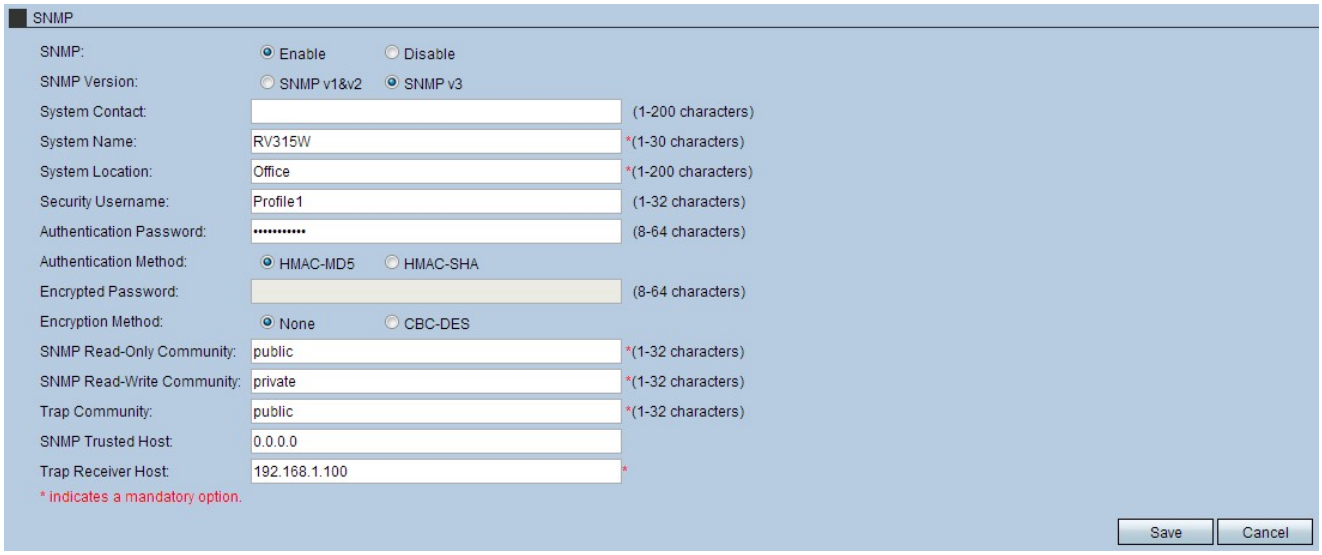
Etapa 12. Clique em **Salvar** para aplicar as configurações.

Configurar SNMP para SNMP v3

Etapa 4. (Opcional) Insira as informações de contato no campo Contato do sistema. Esse é o indivíduo para entrar em contato para obter assistência de rede.

Etapa 5. Digite um nome no campo Nome do sistema. Este é o nome alocado para a configuração SNMP.

Etapa 6. Insira um local no campo System Location (Local do sistema). É aqui que o sistema está localizado.



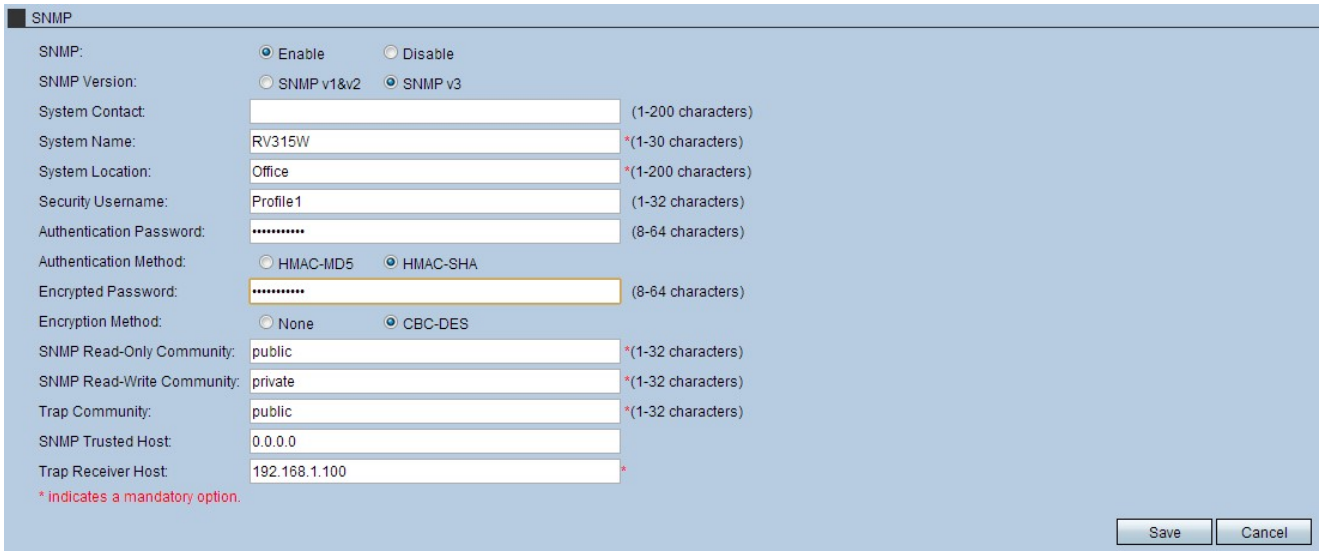
Passo 7. (Opcional) Insira um nome de usuário no campo Nome de usuário de segurança. Este é o nome de usuário usado para obter acesso à configuração SNMP.

Etapa 8. (Opcional) Insira uma senha no campo Authentication Password (Senha de autenticação). Esta é a senha usada para obter acesso à configuração SNMP.

Etapa 9. Clique no botão de opção HMAC-MD5 ou HMAC-SHA no campo Authentication Method. O HMAC (Hash-based message authentication code) é um código criptografado que combina um código de autenticação e uma chave criptográfica secreta. A finalidade principal do HMAC é a segurança da mensagem. Um HMAC autenticará os dados com base em chaves secretas produzidas.

HMAC MD5 — Este algoritmo hash tem várias falhas de segurança e os dados podem ser comprometidos. O HMAC MD5 é um mecanismo de autenticação de mensagens usando funções de hash criptográfico. O MD5 é utilizado em situações em que a velocidade de desempenho superior é vital para um sistema, embora menos segura.

HMAC SHA — Esse algoritmo de hash é muito mais seguro, pois o método de criptografia é superior. Este é um mecanismo mais seguro para autenticação de mensagens usando funções de hash criptográfico. HMAC SHA deve ser usado quando a segurança é de importância vital.



Etapa 10. Insira uma senha no campo Senha criptografada.

Etapa 11. Clique no botão de opção CBC-DES no campo Encryption Method (Método de criptografia). CBC e DES são padrões de criptografia que se combinam para proteger os dados transferidos.

Etapa 12. Insira uma comunidade no campo SNMP Read-Only Community. Este é o parâmetro do cliente para acesso somente leitura da configuração SNMP.

Etapa 13. Insira uma comunidade no campo SNMP Read-Write Community. Este é o parâmetro do cliente para acesso de leitura e gravação da configuração SNMP.

Etapa 14. Insira uma comunidade no campo Comunidade de interceptações. Essa é a comunidade com a capacidade de utilizar armadilhas SNMP. As interceptações são notificações direcionadas enviadas ao administrador. O Traps permite que o administrador gerencie cada dispositivo permitindo que o usuário o notifique usando uma interceptação.

Etapa 15. Insira um host no campo SNMP Trusted Host. Este é o endereço IP do host confiável para a configuração SNMP.

Etapa 16. Insira um host no campo Trap Receiver Host. Esse é o endereço IP do administrador para receber as armadilhas.

Etapa 17. Clique em **Salvar** para aplicar as configurações.