Exibir/adicionar certificado IPSec confiável em roteadores VPN RV320 e RV325

Objetivo

Os certificados são usados para verificar a identidade do usuário em um computador ou na Internet e para aprimorar uma conversação privada ou segura. No RV320, você pode adicionar um máximo de 50 certificados por assinatura automática ou autorização de terceiros. Você pode exportar um certificado para um cliente ou administrador, salvá-lo em um PC ou USB e importá-lo. O IPsec é usado na troca de dados de geração e autenticação de chaves, protocolo de estabelecimento de chaves, algoritmo de criptografia ou mecanismo de autenticação de autenticação segura e validação de transações on-line com certificados SSL.

Este artigo explica como exibir e adicionar certificado de IPSec confiável na série de roteadores VPN RV32x.

Dispositivos aplicáveis

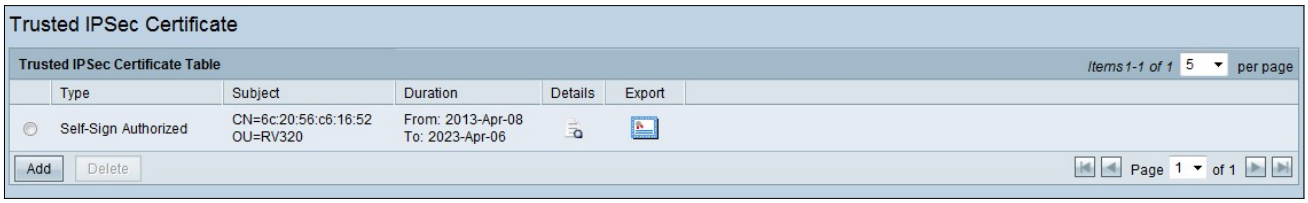
RV320 Roteador VPN WAN duplo
Roteador VPN WAN duplo RV325 Gigabit

Versão de software

•v1.1.0.09

Certificado IPSec confiável

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Certificate Management > Trusted IPSec Certificate**. A página *Certificado IPSec confiável* é aberta:



A página *Certificado IPSec confiável* contém os seguintes campos:

Tipo — Estão disponíveis dois tipos de certificados

- Autoassinado — é um certificado SSL (Secure Socket Layer) assinado por seu próprio criador. Ela é menos confiável, pois não pode ser cancelada se a chave privada for comprometida de alguma forma pelo invasor.

- Solicitação de assinatura certificada — é uma infraestrutura de chave pública (PKI) que é enviada à autoridade de certificação para solicitar um certificado de identidade digital. É mais segura do que autoassinada, já que a chave privada é mantida em segredo.

Assunto — Indica a quem é emitido o certificado.

Duração — Mostra a data em que o certificado expira. Não é possível garantir a segurança do Web site se esta data tiver sido excedida.

Detalhes — Mostra todos os detalhes sobre o Emissor do certificado, o Número de série do certificado e a Data de expiração gerados pelo serviço CA. As informações são usadas quando uma solicitação de criação de assinatura de certificado é criada e enviada ao serviço CA para validação.

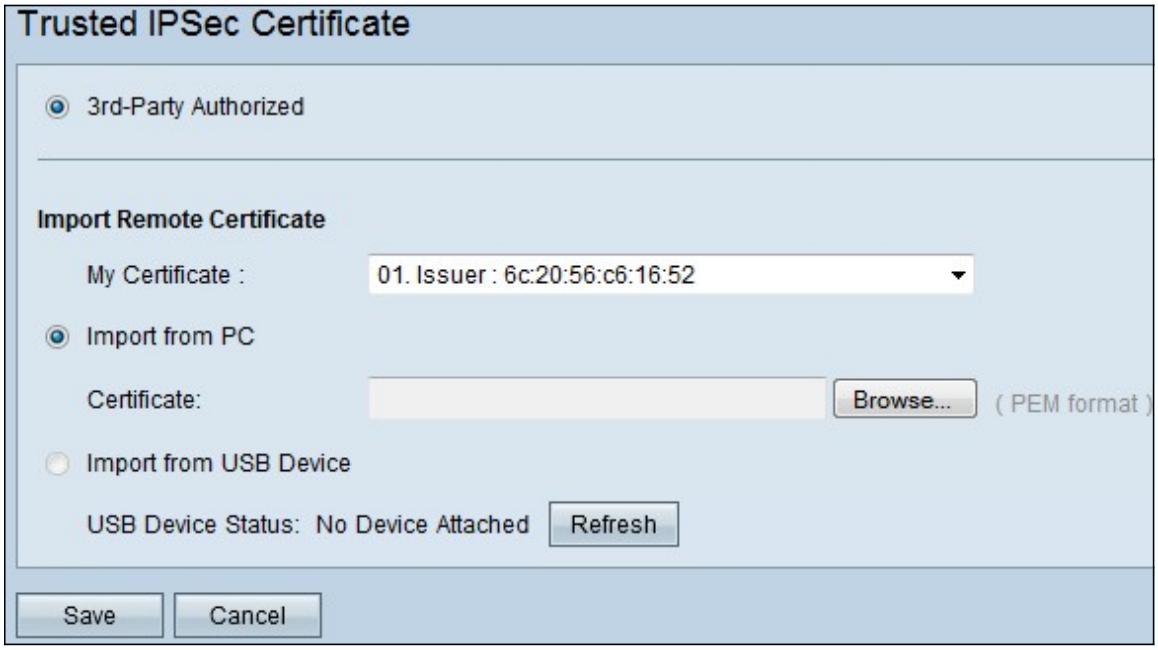
Exportar — Para exportar ou exibir um certificado, clique no ícone Exportar certificado. Uma janela pop-up é exibida onde você pode Abrir o certificado para inspeção ou Salvar o certificado em um PC.

Etapa 2. Clique na caixa de seleção **Habilitar** para habilitar um certificado IPSec específico.

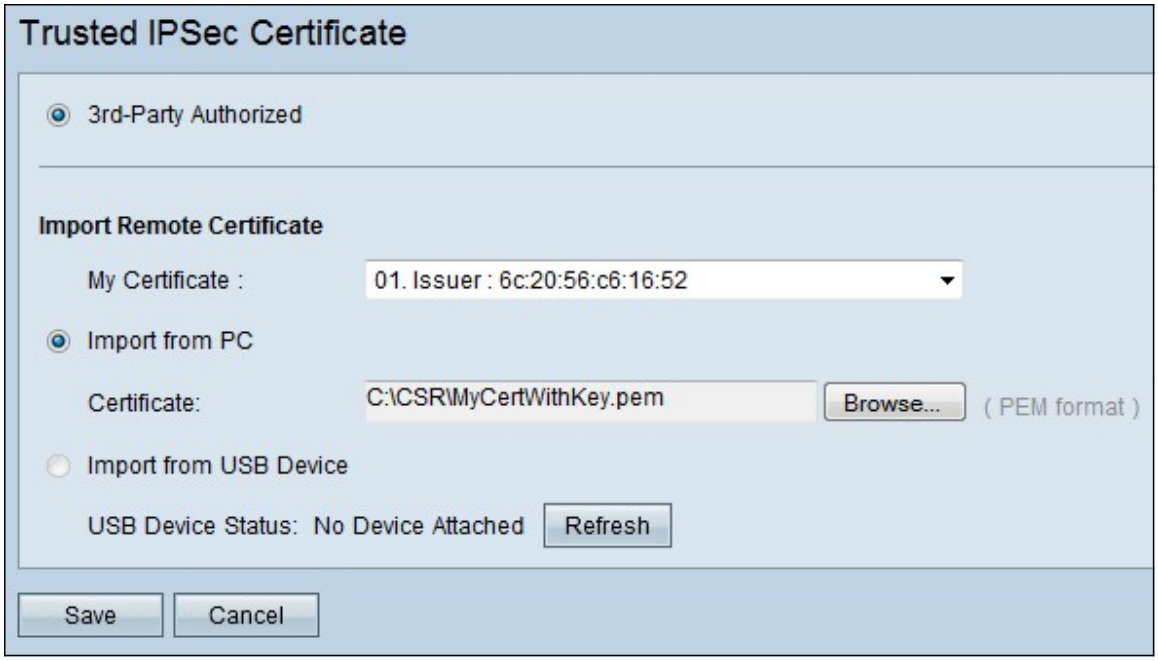
Etapa 3. Clique em **Adicionar** para obter um novo certificado do PC ou do USB.

Importar do PC — Do PC, você pode localizar o certificado e importar para o dispositivo

Importar do USB — Do USB conectado ao dispositivo, você também pode importar o certificado.



Etapa 3. Clique em **Procurar** para localizar o certificado CA do PC.



Etapa 4. Clique em **Salvar** para adicionar o certificado à Tabela de certificados IPSec confiáveis.