Configuração de um servidor VPN IPSec em RV130 e RV130W

Objetivo

A VPN IPSec (Virtual Private Network) permite que você obtenha acesso remoto aos recursos corporativos com segurança, estabelecendo um túnel criptografado pela Internet.

O objetivo deste documento é mostrar como configurar um servidor VPN IPSec em RV130 e RV130W.

Note: Para obter informações sobre como configurar um servidor VPN IPSec com o cliente VPN Soft Shrew em RV130 e RV130W, consulte o artigo *Uso do cliente VPN Soft Shrew com o servidor VPN IPSec em RV130 e RV130W*.

Dispositivos aplicáveis

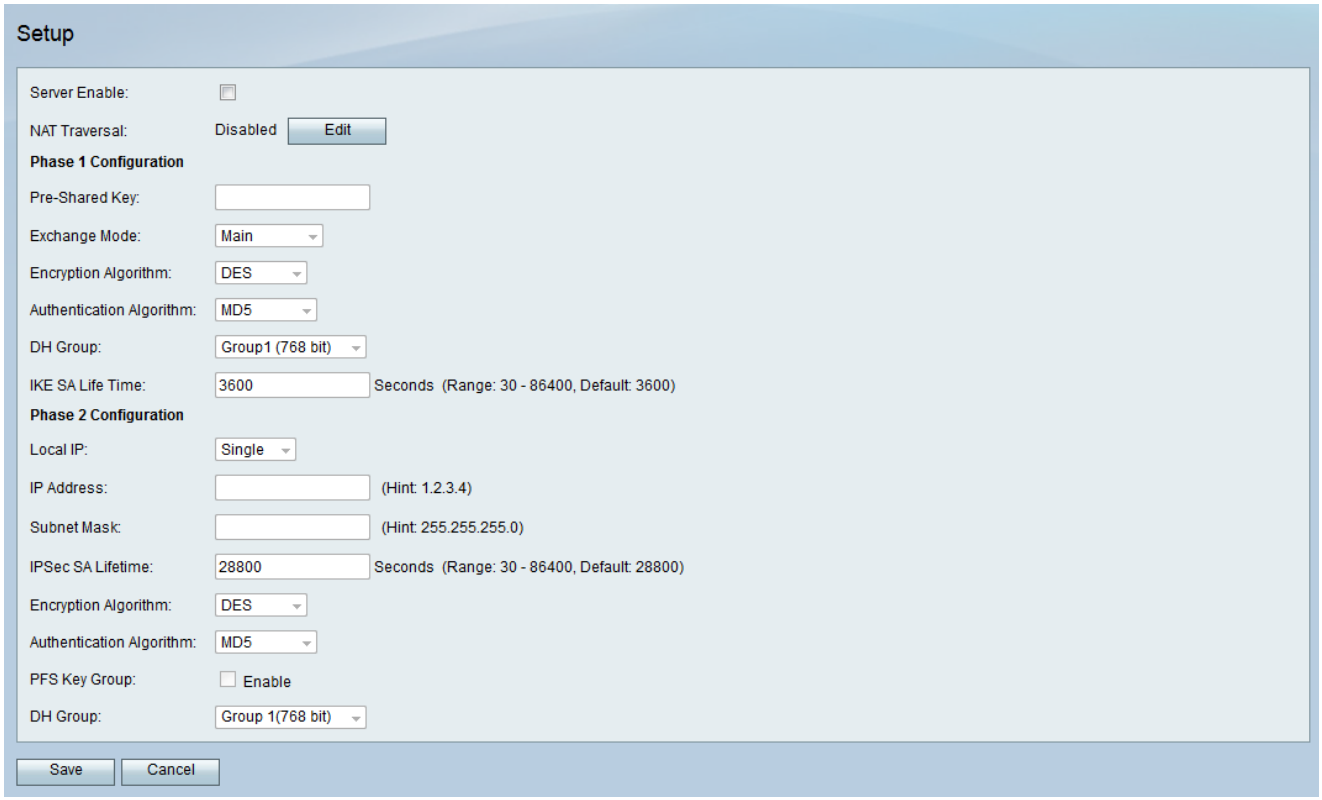
·Firewall VPN Wireless-N RV130W
· Firewall VPN RV130

Versão de software

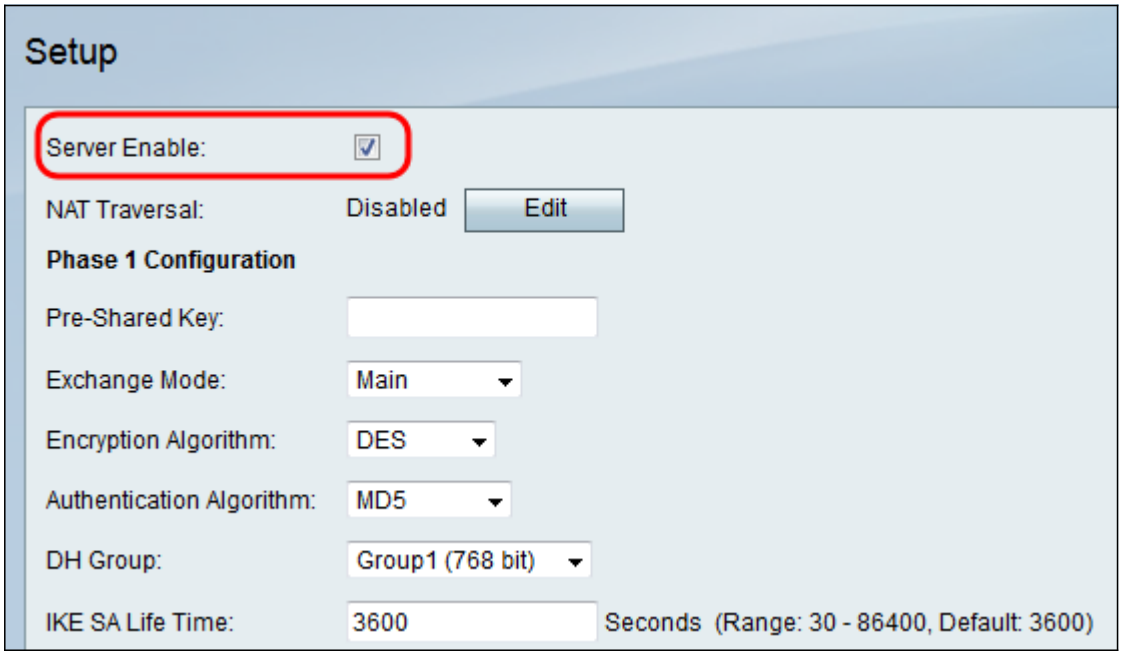
•v1.0.1.3

Configurar o servidor VPN IPSec

Etapa 1. Inicie a sessão no utilitário de configuração da Web e selecione **VPN > IPSec VPN Server > Setup**. A página Setup é aberta.

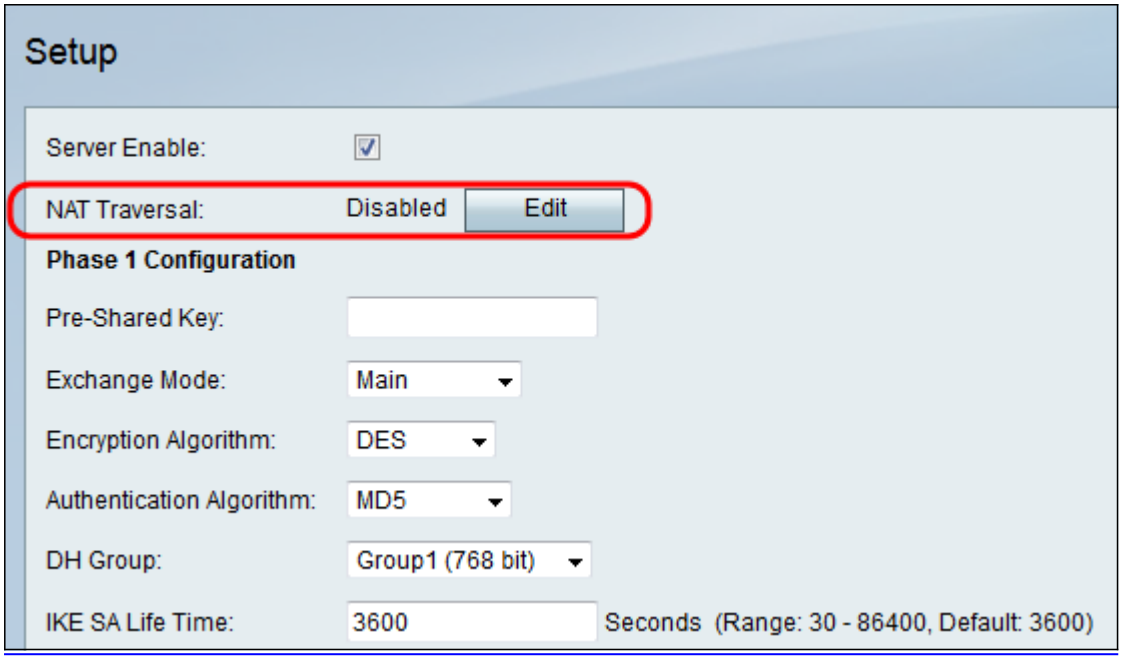


Etapa 2. Marque a caixa de seleção **Server Enable** para habilitar o certificado.

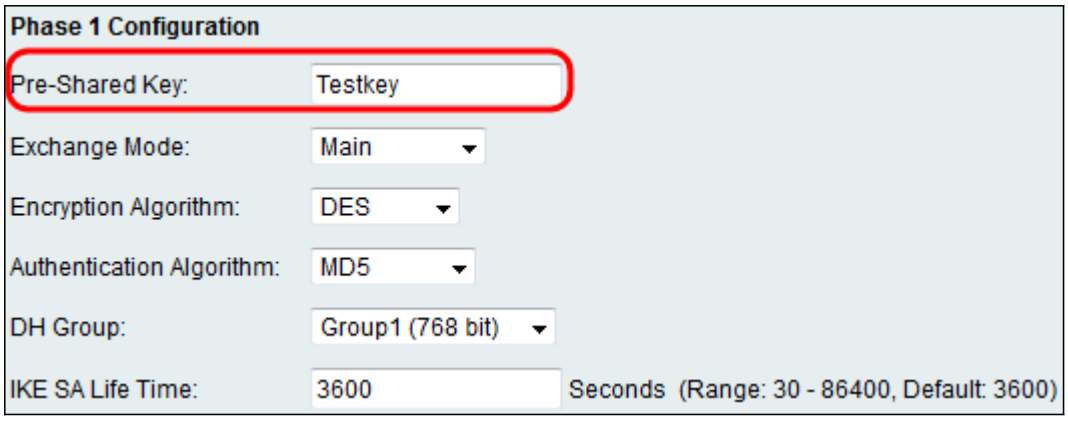


Etapa 3. (Opcional) Se o roteador VPN ou o cliente VPN estiver atrás de um gateway NAT, clique em **Editar** para configurar o NAT Traversal. Caso contrário, deixe NAT Traversal desabilitado.

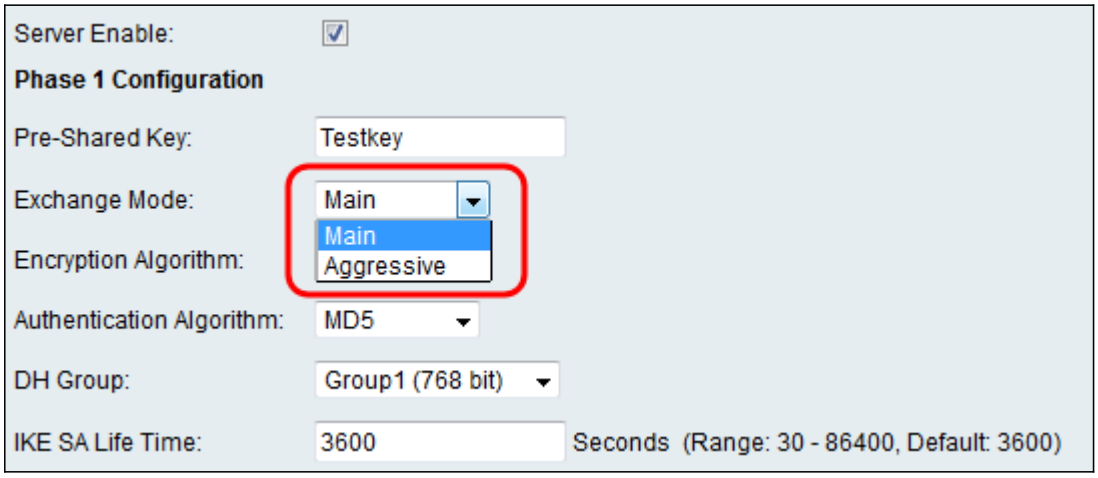
Note: Para obter mais informações sobre como definir as configurações de NAT Traversal, consulte *Internet Key Exchange (IKE) Policy Settings on RV130 and RV130W VPN Routers*.



Etapa 4. Insira uma chave com 8 a 49 caracteres que será trocada entre seu dispositivo e o endpoint remoto no campo *Pre-Shared Key*.



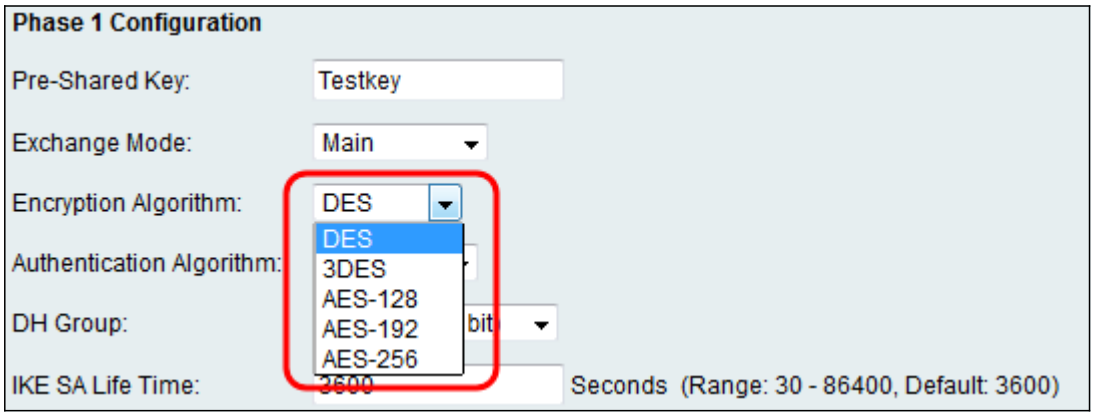
Etapa 5. Na lista suspensa *Exchange Mode*, escolha o modo para a conexão VPN IPSec. **Main** é o modo padrão. No entanto, se a velocidade da rede for baixa, escolha o modo **Agressivo**.



Note: O modo agressivo troca as IDs dos pontos finais do túnel em texto claro durante a conexão, o que requer menos tempo para troca, mas é menos seguro.

Etapa 6. Na lista suspensa **Encryption Algorithm**, escolha o método de criptografia

apropriado para criptografar a Pre-Shared Key na Fase 1. O AES-128 é recomendado por sua alta segurança e rápido desempenho.O túnel VPN precisa usar o mesmo método de criptografia para ambas as extremidades.



As opções disponíveis são definidas da seguinte forma:

·DES — O Data Encryption Standard (DES) é um método de criptografia antigo de 56 bits que não é muito seguro, mas pode ser necessário para compatibilidade com versões anteriores.

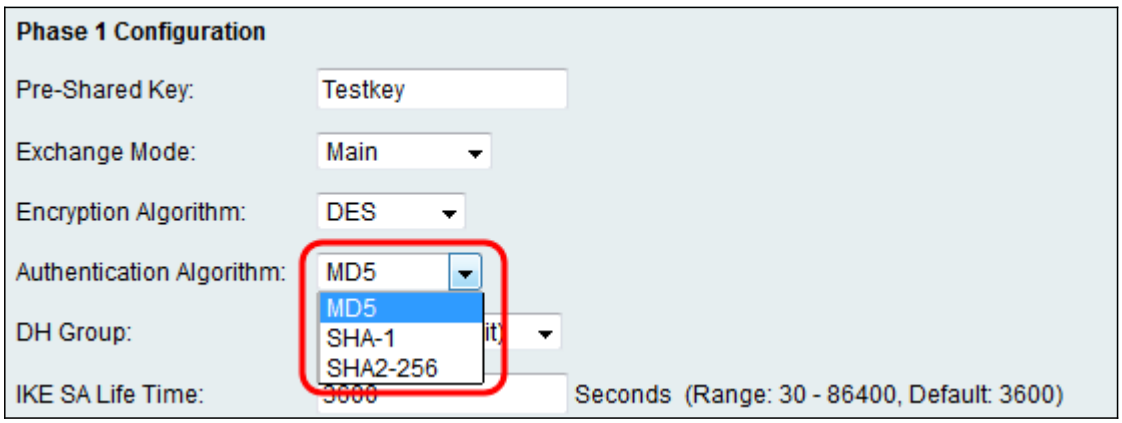
3DES — O 3DES (Triple Data Encryption Standard) é um método simples de criptografia de 168 bits usado para aumentar o tamanho da chave, pois criptografa os dados três vezes. Isso fornece mais segurança que o DES, mas menos segurança que o AES.

AES-128 — Advanced Encryption Standard com chave de 128 bits (AES-128) usa uma chave de 128 bits para criptografia AES. O AES é mais rápido e mais seguro que o DES. Em geral, o AES também é mais rápido e mais seguro que o 3DES. AES-128 é mais rápido, mas menos seguro que AES-192 e AES-256.

AES-192 — AES-192 usa uma chave de 192 bits para a criptografia AES. O AES-192 é mais lento, mas mais seguro que o AES-128, e mais rápido, mas menos seguro que o AES-256.

AES-256 — AES-256 usa uma chave de 256 bits para a criptografia AES. AES-256 é mais lento, mas mais seguro que AES-128 e AES-192.

Etapa 7. Na lista suspensa *Authentication Algorithm*, escolha o método de autenticação apropriado para determinar como os pacotes de cabeçalho do protocolo ESP (Encapsulating Security Payload) são validados na Fase 1. O túnel VPN precisa usar o mesmo método de autenticação para ambas as extremidades da conexão.



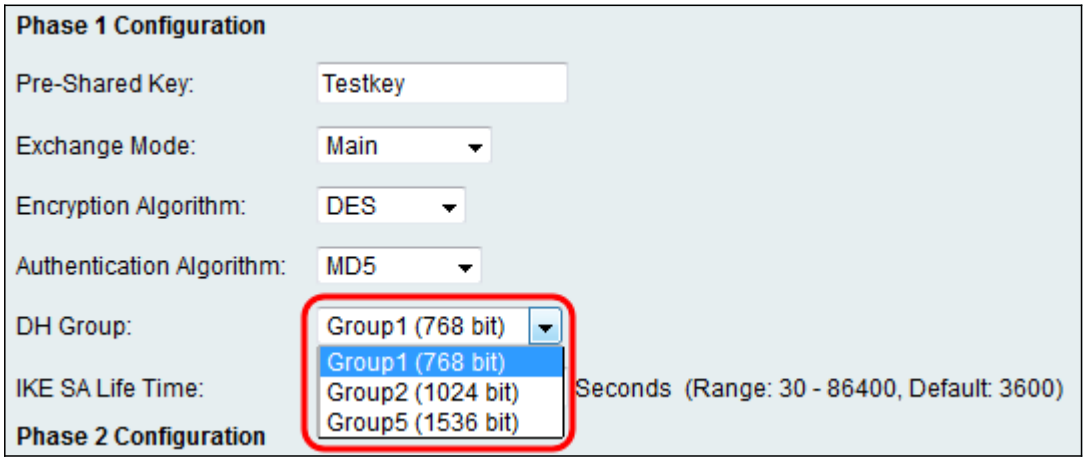
As opções disponíveis são definidas da seguinte forma:

·MD5 — MD5 é um algoritmo de hash unidirecional que produz um resumo de 128 bits. MD5 computa mais rápido que SHA-1, mas é menos seguro que SHA-1. MD5 não é recomendado.

SHA-1 — SHA-1 é um algoritmo de hash unidirecional que produz um resumo de 160 bits. SHA-1 computa mais lentamente que MD5, mas é mais seguro que MD5.

SHA2-256 — Especifica o Algoritmo de Hash Seguro SHA2 com o resumo de 256 bits.

Etapa 8. Na lista suspensa *Grupo DH*, escolha o grupo Diffie-Hellman (DH) apropriado a ser usado com a chave na Fase 1. Diffie-Hellman é um protocolo de troca de chave criptográfica usado na conexão para trocar conjuntos de chave pré-compartilhados. A força do algoritmo é determinada por bits.



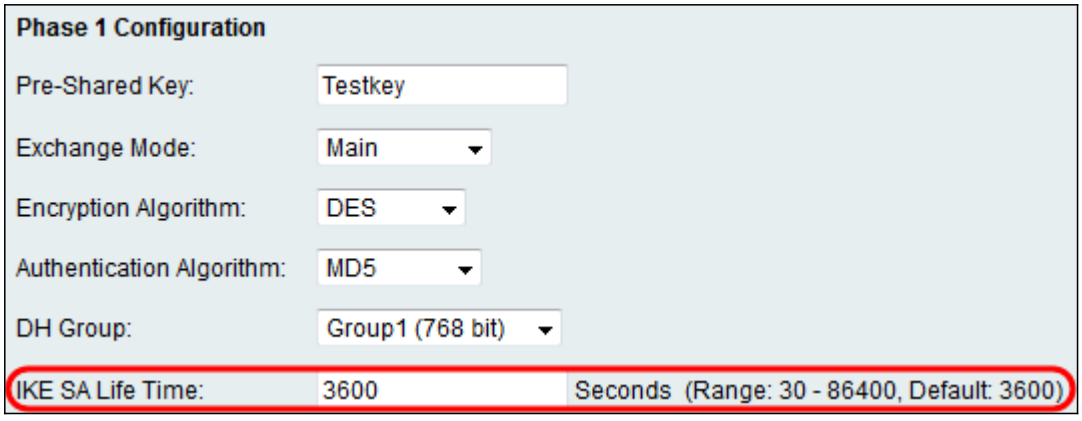
As opções disponíveis são definidas da seguinte forma:

·Grupo1 (768 bits) — Calcula a chave mais rapidamente, mas é a menos segura.

·Grupo2 (1024 bits) — Calcula a chave mais lentamente, mas é mais seguro que o Grupo1.

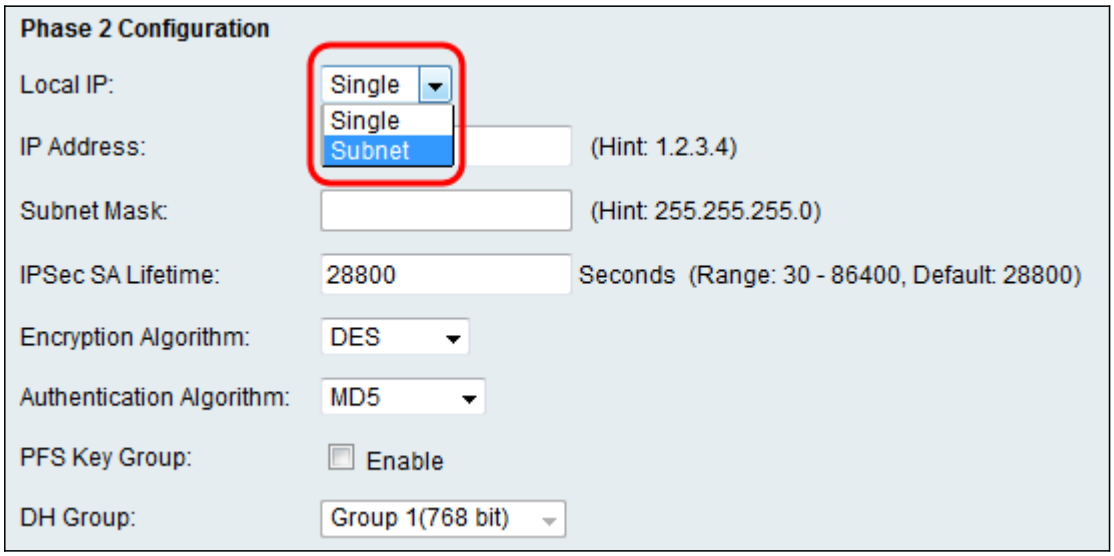
·Grupo 5 (1536 bits) — Calcula a chave mais lentamente, mas é a mais segura.

Etapa 9. No campo *IKE SA Life Time*, digite o tempo, em segundos, em que a chave automática de IKE é válida. Quando esse tempo expirar, uma nova chave será negociada automaticamente.

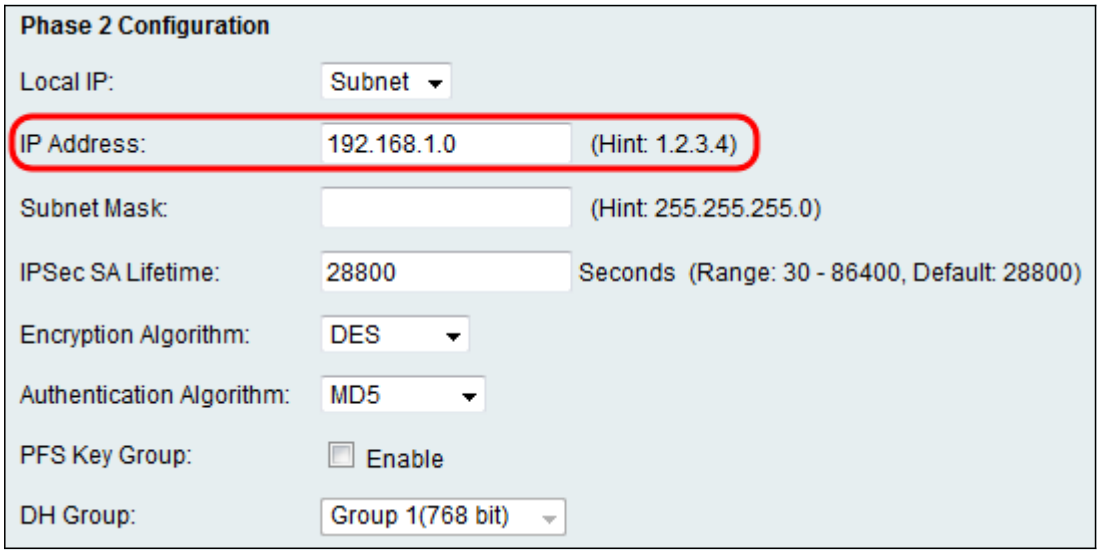


Etapa 10. Na lista suspensa *Local IP*, selecione **Single** se quiser que um único usuário de

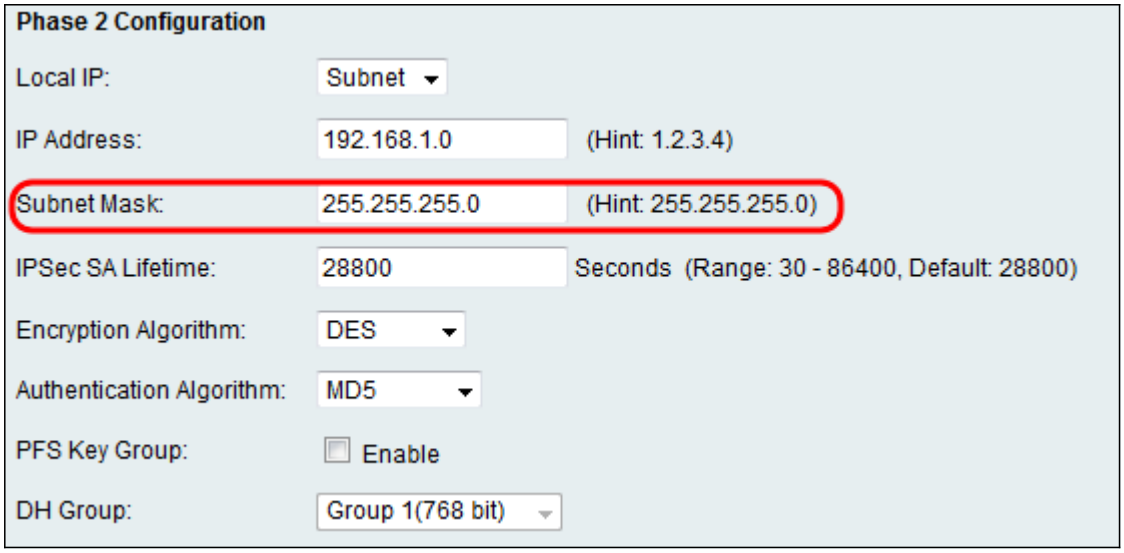
LAN local acesse o túnel VPN, ou **Subnet** se quiser que vários usuários possam acessá-lo.



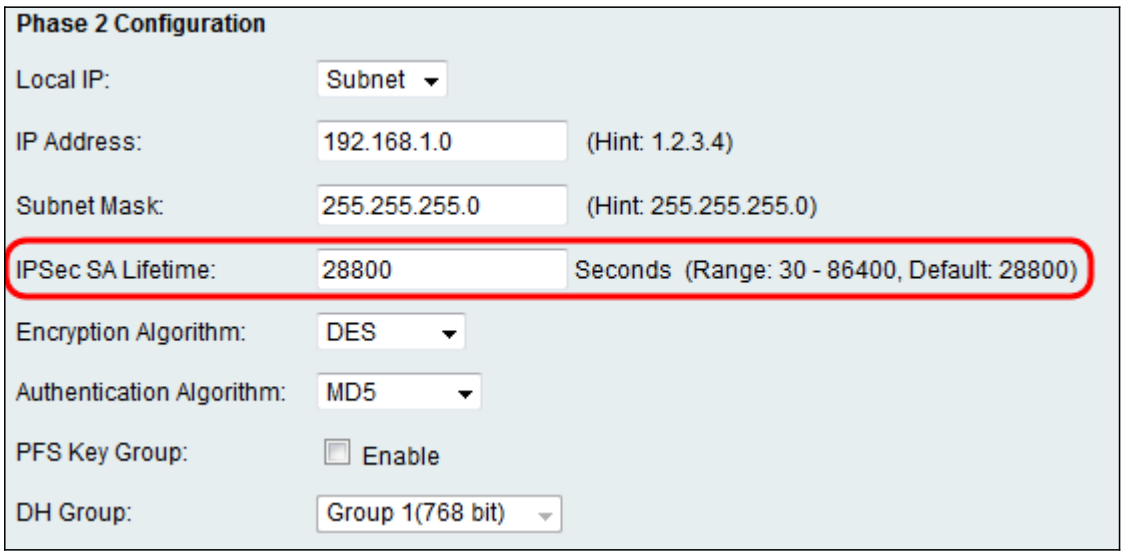
Etapa 11. Se a opção **Sub-rede** tiver sido escolhida na Etapa 10, insira o endereço IP de rede da sub-rede no campo Endereço IP. Se **Single** tiver sido escolhido na Etapa 10, insira o endereço IP do usuário único e vá para a Etapa 13.



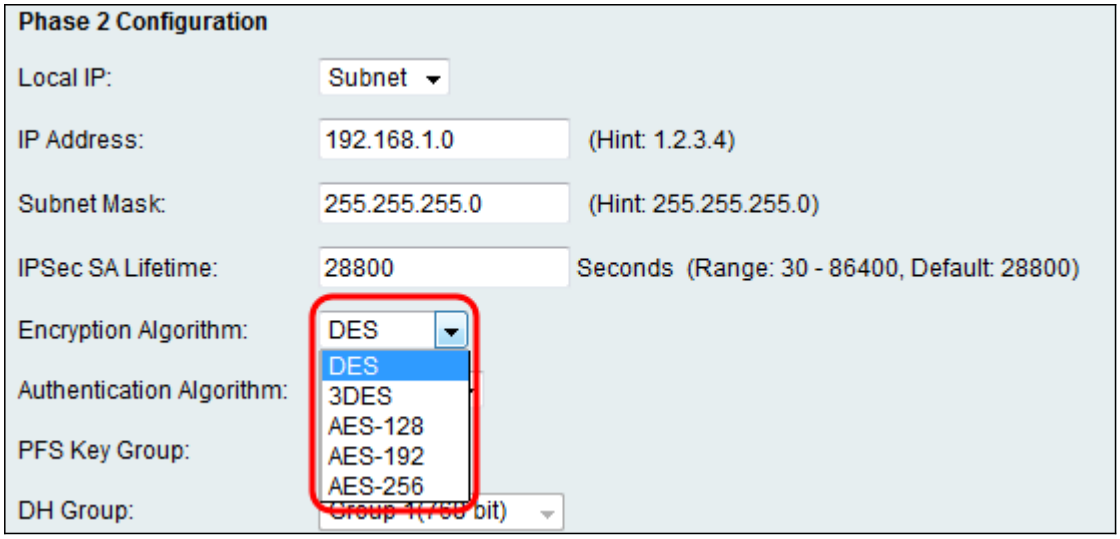
Etapa 12. (Opcional) Se a opção **Sub-rede** tiver sido escolhida na Etapa 10, insira a máscara de sub-rede da rede local no campo *Máscara de sub-rede*.



Etapa 13. No campo *IPSec SA Lifetime*, insira o tempo em segundos em que a conexão VPN permanece ativa na Fase 2. Quando esse tempo expirar, a IPSec Security Association da conexão VPN será renegociada.



Etapa 14. Na lista suspensa *Encryption Algorithm*, escolha o método de criptografia apropriado para criptografar a chave pré-compartilhada na Fase 2. O AES-128 é recomendado por sua alta segurança e rápido desempenho. O túnel VPN precisa usar o mesmo método de criptografia para ambas as extremidades.



As opções disponíveis são definidas da seguinte forma:

·DES — O Data Encryption Standard (DES) é um método de criptografia antigo de 56 bits que é o menos seguro, mas pode ser necessário para compatibilidade com versões anteriores.

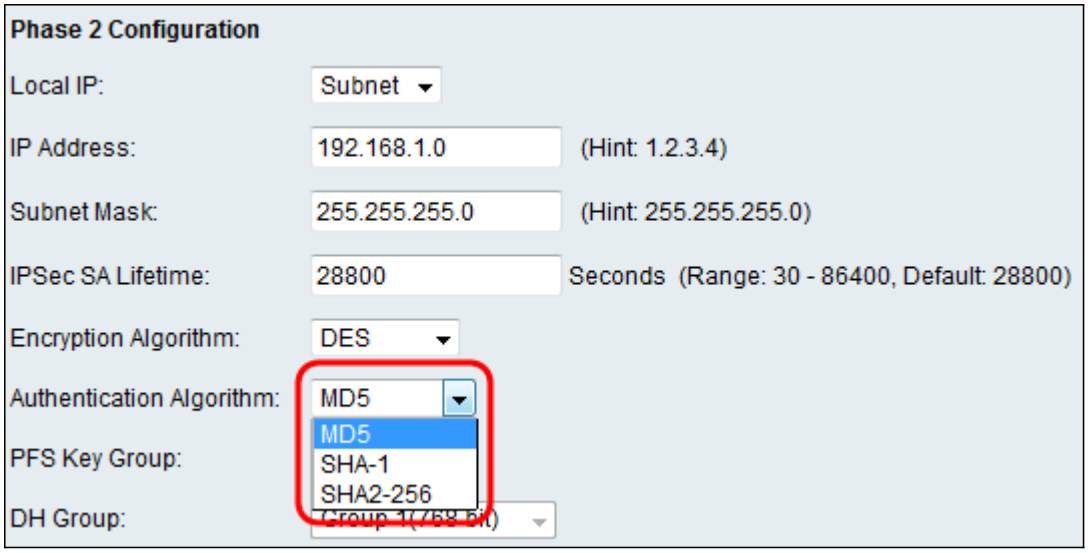
3DES — O 3DES (Triple Data Encryption Standard) é um método simples de criptografia de 168 bits usado para aumentar o tamanho da chave, pois criptografa os dados três vezes. Isso fornece mais segurança que o DES, mas menos segurança que o AES.

AES-128 — Advanced Encryption Standard com chave de 128 bits (AES-128) usa uma chave de 128 bits para criptografia AES. O AES é mais rápido e mais seguro que o DES. Em geral, o AES também é mais rápido e mais seguro que o 3DES. AES-128 é mais rápido, mas menos seguro que AES-192 e AES-256.

AES-192 — AES-192 usa uma chave de 192 bits para a criptografia AES. O AES-192 é mais lento, mas mais seguro que o AES-128, e mais rápido, mas menos seguro que o AES-256.

AES-256 — AES-256 usa uma chave de 256 bits para a criptografia AES. AES-256 é mais lento, mas mais seguro que AES-128 e AES-192.

Etapa 15. Na lista suspensa *Authentication Algorithm*, escolha o método de autenticação apropriado para determinar como os pacotes de cabeçalho do protocolo ESP (Encapsulating Security Payload) são validados na Fase 2. O túnel VPN precisa usar o mesmo método de autenticação para ambas as extremidades.



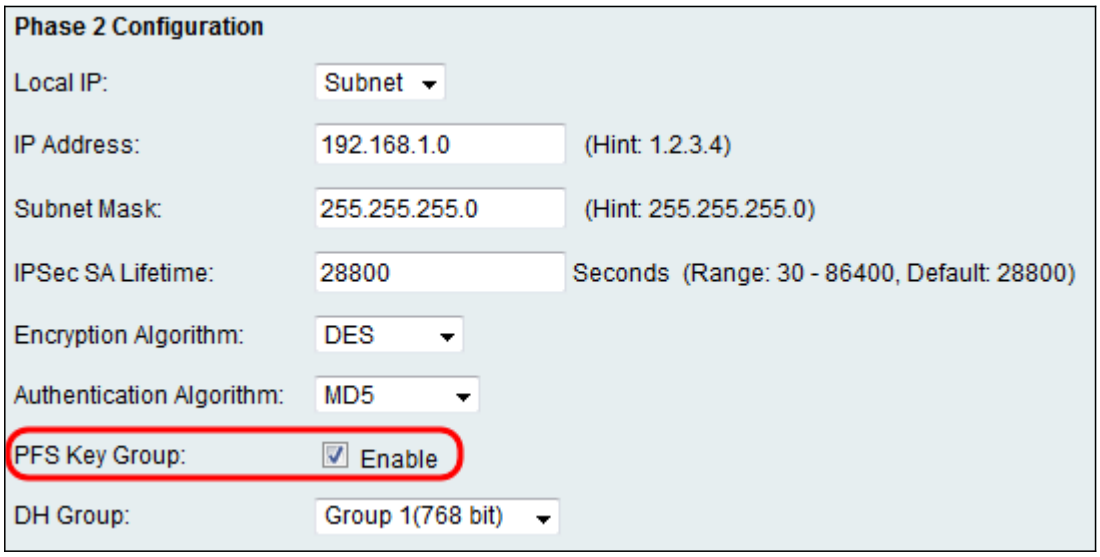
As opções disponíveis são definidas da seguinte forma:

·MD5 — MD5 é um algoritmo de hash unidirecional que produz um resumo de 128 bits. MD5 computa mais rápido que SHA-1, mas é menos seguro que SHA-1. MD5 não é recomendado.

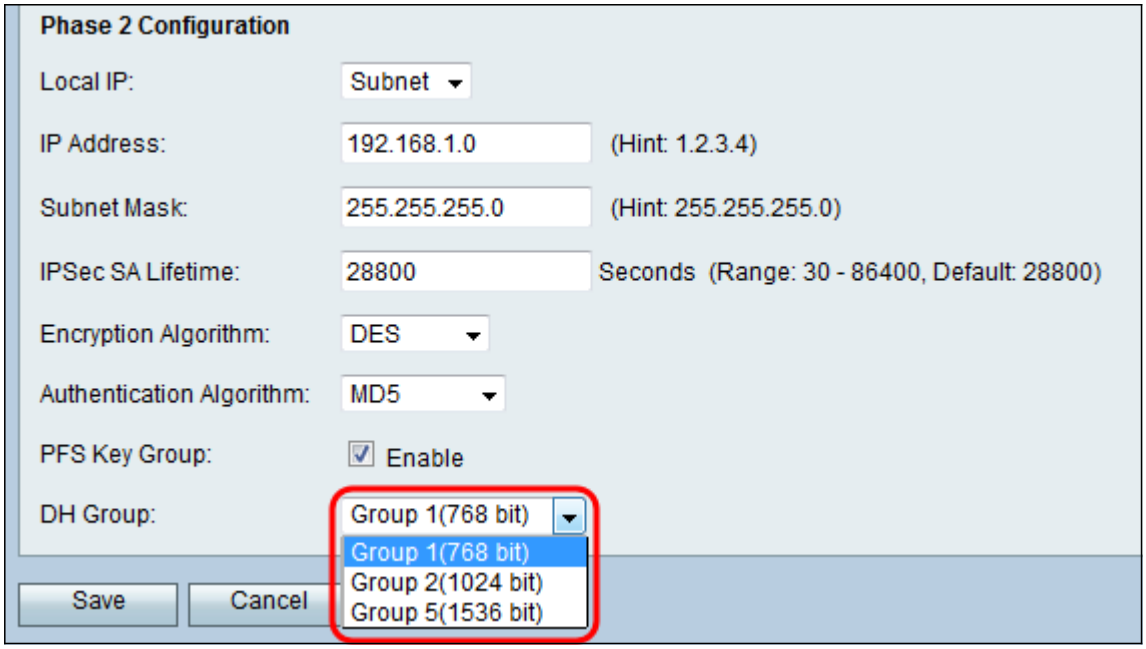
SHA-1 — SHA-1 é um algoritmo de hash unidirecional que produz um resumo de 160 bits. SHA-1 computa mais lentamente que MD5, mas é mais seguro que MD5.

SHA2-256 — Especifica o Algoritmo de Hash Seguro SHA2 com o resumo de 256 bits.

Etapa 16. (Opcional) No *campo Grupo de chaves PFS*, marque a caixa de seleção **Habilitar**. O PFS (Perfect Forward Secrecy) cria uma camada adicional de segurança para proteger seus dados, garantindo uma nova chave DH na Fase 2. O processo é realizado caso a chave DH gerada na Fase 1 seja comprometida em trânsito.



Etapa 17. Na lista suspensa *Grupo DH*, escolha o grupo Diffie-Hellman (DH) apropriado a ser usado com a chave na Fase 2.



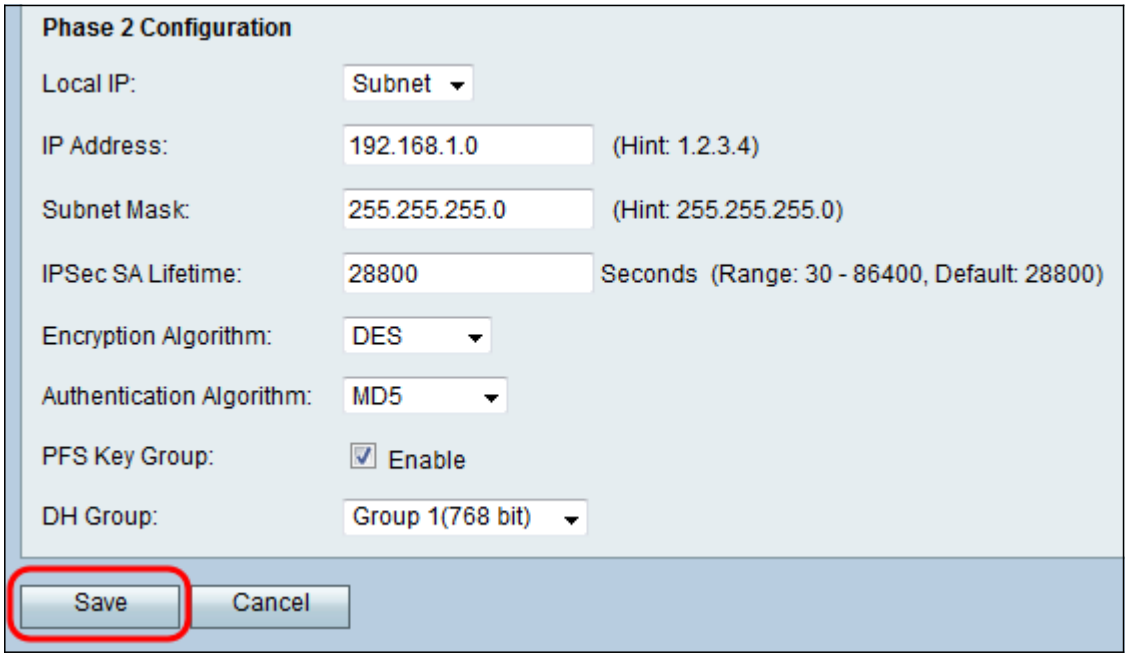
As opções disponíveis são definidas da seguinte forma:

·Grupo1 (768 bits) — Calcula a chave mais rapidamente, mas é a menos segura.

·Grupo2 (1024 bits) — Calcula a chave mais lentamente, mas é mais seguro que o Grupo1.

·Grupo 5 (1536 bits) — Calcula a chave mais lentamente, mas é a mais segura.

Etapa 18. Clique em **Salvar** para salvar suas configurações.



Para obter mais informações, consulte a seguinte documentação:

- Data sheet do RV130 - explica os recursos de VPN para os roteadores da série RV130
- Página do produto RV130 - inclui links para todos os artigos RV130 da Cisco

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.