GUIA DE CONFIGURAÇÃO

Conexões VPN SSL (Rede a Rede)

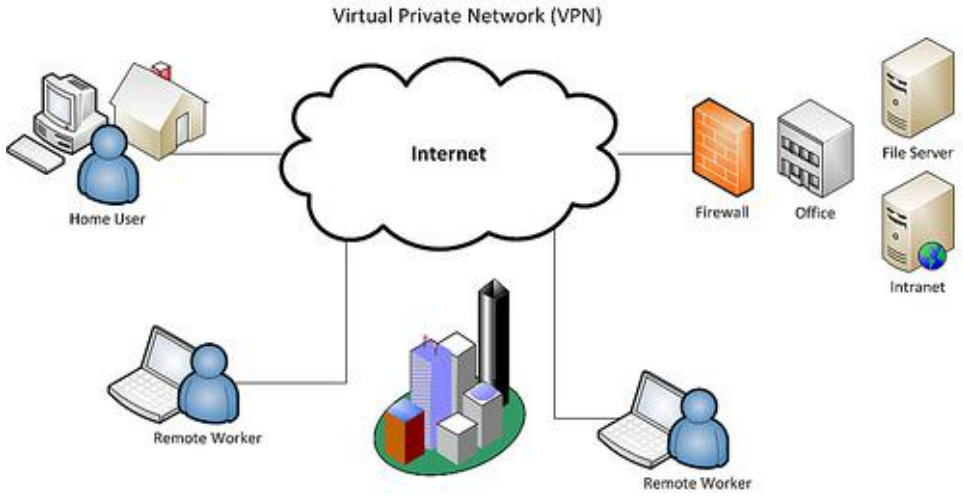
Conexões VPN SSL (Rede a Rede)

1 – Introdução

Uma VPN (Virtual Private Network, ou rede virtual privada) é, como o nome sugere, uma rede virtual, criada para interligar duas redes distantes, através da Internet. Usar uma VPN permite que você compartilhe arquivos e use aplicativos de produtividade e de gerenciamento, como se todos os micros estivessem conectados à mesma rede local. Você pode até mesmo imprimir em impressoras da rede remota, da mesma forma que faria com uma impressora local.Antigamente, a única forma de interligar redes em dois locais diferentes era usar linhas de frame-relay. Para quem não é dessa época, uma linha de frame-relay oferece um link dedicado de 64 kbits entre dois pontos (a matriz e a filial de uma empresa, por exemplo), com um custo mensal fixo. Você pode combinar várias linhas frame-relay em uma única conexão, de acordo com a necessidade, o problema nesse caso é o preço. Atualmente, existem outras opções de conexões dedicadas e de conexões de alta disponibilidade, oferecidas pelas operadoras, mas elas ficam fora do orçamento da maioria das pequenas e médias empresas.

Usando uma VPN, você pode obter todos os benefícios de ter uma conexão dedicada entre dois pontos usando conexões via ADSL ou cabo, que são muito mais baratas. Dependendo do volume de uso da rede, você pode tanto utilizar a conexão que já tem quanto utilizar uma segunda conexão apenas para a VPN, evitando assim que o tráfego prejudique a navegação dos usuários. Além de interligar duas ou mais redes, a VPN pode (dependendo da configuração) ser acessada também por funcionários trabalhando remotamente.

Todos dados que trafegam através da VPN são encriptados, o que elimina o risco inerente à transmissão via



Internet. Naturalmente, nenhuma VPN pode ser considerada "100% segura", já que sempre existe um pequeno risco de alguém conseguir obter acesso aos servidores, de forma a roubar as chaves de encriptação (por exemplo), mas, em uma VPN bem configurada, o risco é realmente muito pequeno. É muito mais provável que um funcionário descontente sabote a rede interna, ou envie informações sigilosas para fora, do que algum invasor consiga efetivamente obter acesso à rede via Internet.

Nesse tópico, estudaremos como criar VPNs usando o OpenVPN. Além de ser mais simples de configurar que a maioria das outras soluções de VPN e ser bastante seguro e flexível, ele possui versões Linux e Windows, o que permite criar túneis interligando máquinas rodando os dois sistemas sem grandes dificuldades.

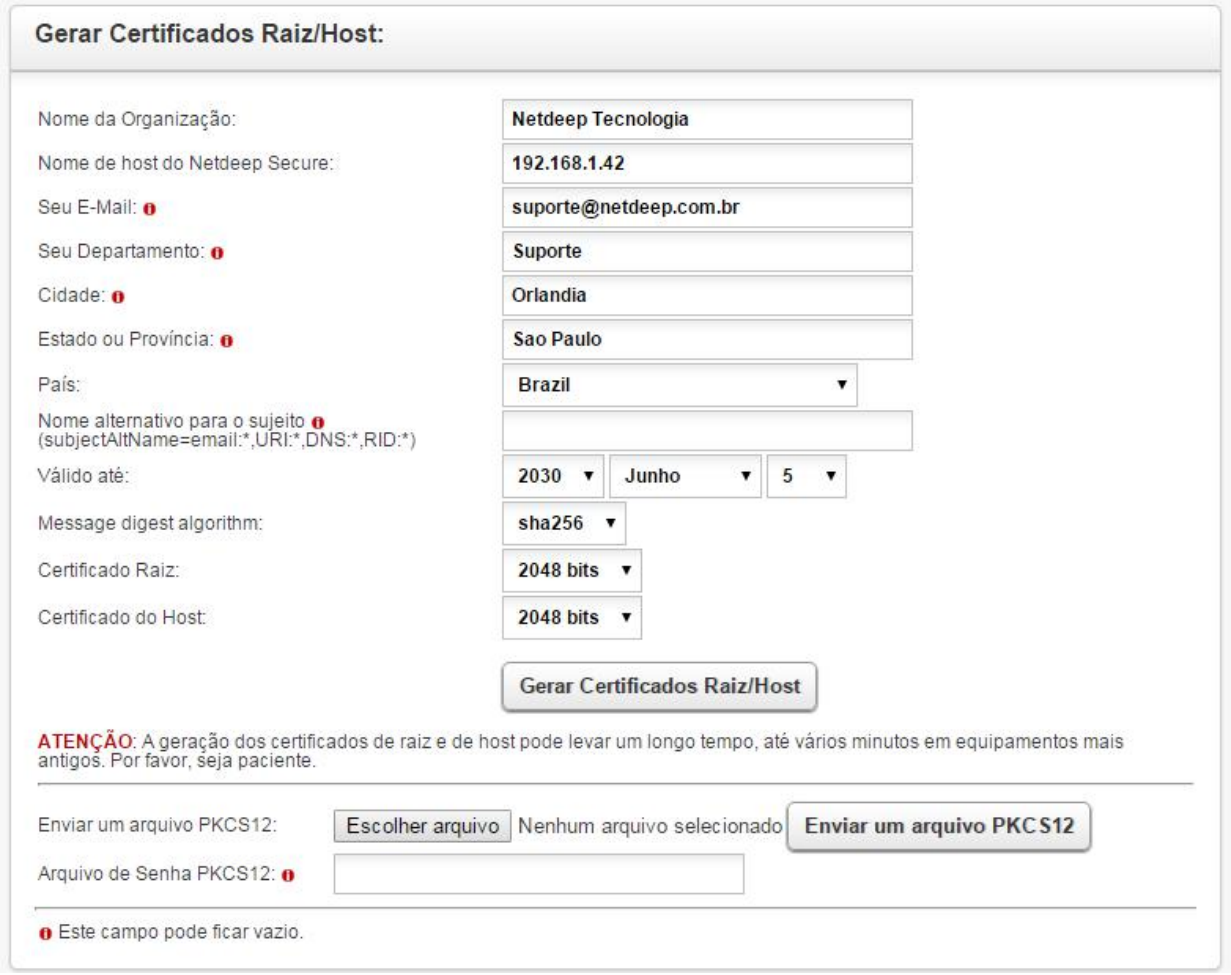
Outras vantagens são que ele pode ser usado por clientes conectando através de uma conexão compartilhada via NAT (apenas o servidor precisa de portas abertas) e a boa tolerância contra conexões ruins, ou ao uso de conexões com IP dinâmico. A VPN pode ser configurada para ser restabelecida de forma automática em caso de interrupção na conexão, o que torna o link bastante confiável.

Com relação à segurança, o OpenVPN pode ser configurado para utilizar chaves estáticas, que oferecem um nível mediano de segurança, em troca de uma configuração mais simples, ou para utilizar certificados X509, onde a configuração é um pouco mais complexa, mas, em compensação, a segurança é muito maior (bem superior à da maioria das soluções comerciais). Isso permite que você escolha a melhor relação entre praticidade e segurança de acordo com a situação.

2- Configurando a conexão do servidor

O primeiro passo é gerar o certificado raiz da Autoridade Certificadora. Na interface de administração do Netdeep Secure vá ao menu "**VPN**" → "**CA (Autoridade Certificadora)**". Clique no botão "**Gerar Certificados Raiz/Host**", será exibido um formulário. Preencha o formulário com suas informações e clique no botão **"Gera Certificados Raiz/Host"**.

Obs.: não utilize acentos em nenhum dos campos.

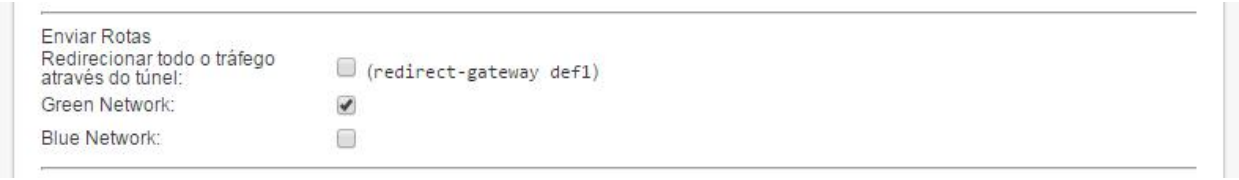


Após gerar o selecione as opções **"Habilitar VPN SSL na interface RED"**e as opção **Usar compactação LZO**(o sistema compactará os pacotes, diminuindo o consumo de banda, aumentando a performance).

No campo "Hostname/IP da VPN local", você deve especificar o hostname ou Endereço IP do túnel VPN. Este endereço será usado para os usuários conectarem.Se você estiver atrás de um modem com NAT, especifique o endereço IP fixo.

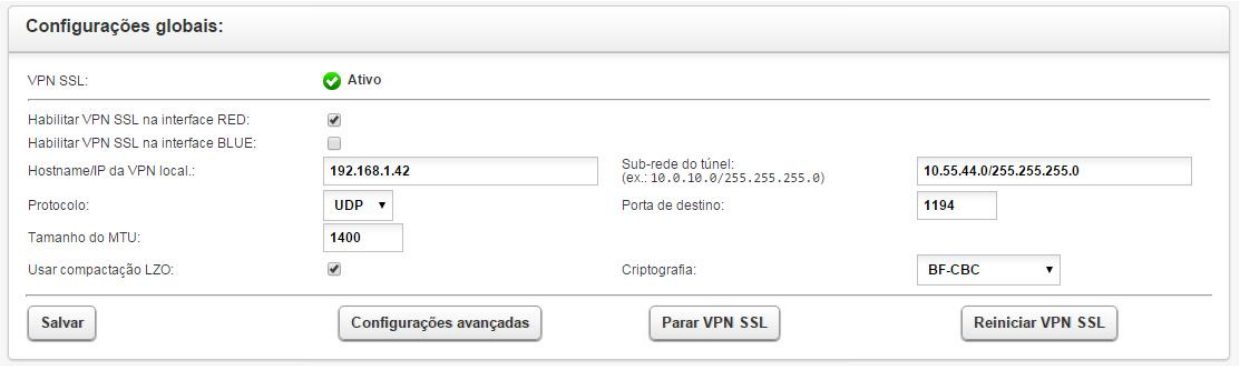
Em seguida clique no botão **“Salvar”**.

Agora iremos realizar as configurações SSL. Clique no botão **“Configurações avançadas”**. Na seção **“Enviar rotas”.** Selecione a opção **Green Network.** Esta opção envia as rotas das redes selecionadas, deixando acessíveis para clientes conectados na VPN. Em seguida cliquem no botão “**Salvar Configurações Avançadas”**.



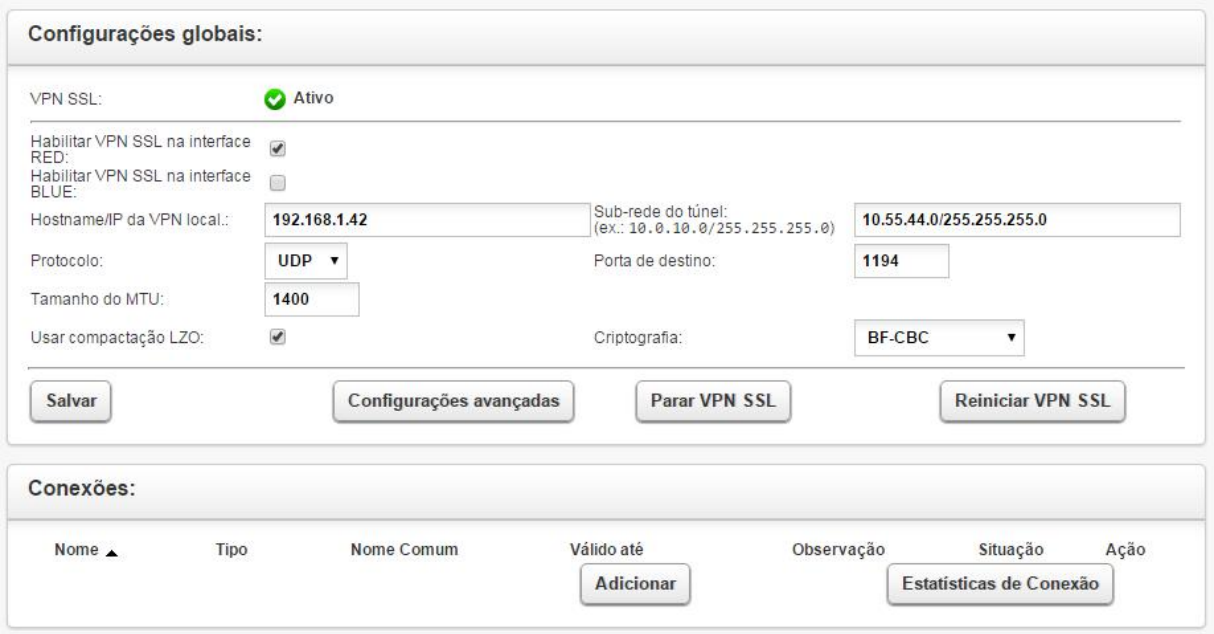
Agora clique no botão **“Iniciar VPN SSL”**, em **“VPN SSL”** irá aparecer **Ativo** e em verde.

Obs.: caso não consiga iniciar a VPN reveja os passos anteriores.



3- Configurando VPN na Matriz (ponto principal)

Para criar a VPN na matriz, vá ao menu “**VPN**” → “**SSL**”. Em “**Conexões**” clique no botão **Adicionar**.



Em "**Tipo de conexão**" selecione a opção "**VPN Rede-à-Rede**" e clique no botão **Adicionar**. Preencha os campos e em seguida clique em **Salvar**.

Em conexão, preencha os campos "**Nome**" e "**Observação**".

Modo de operação: selecione a opção **Servidor**, pois ele será o servidor da conexão entre os firewalls.

Servidor Remoto: caso a filial tenho um IP válido preencha este campo com o IP, caso contrário deixe em branco.

Protocolos: para conexões VPN utilizamos o protocolo UDP

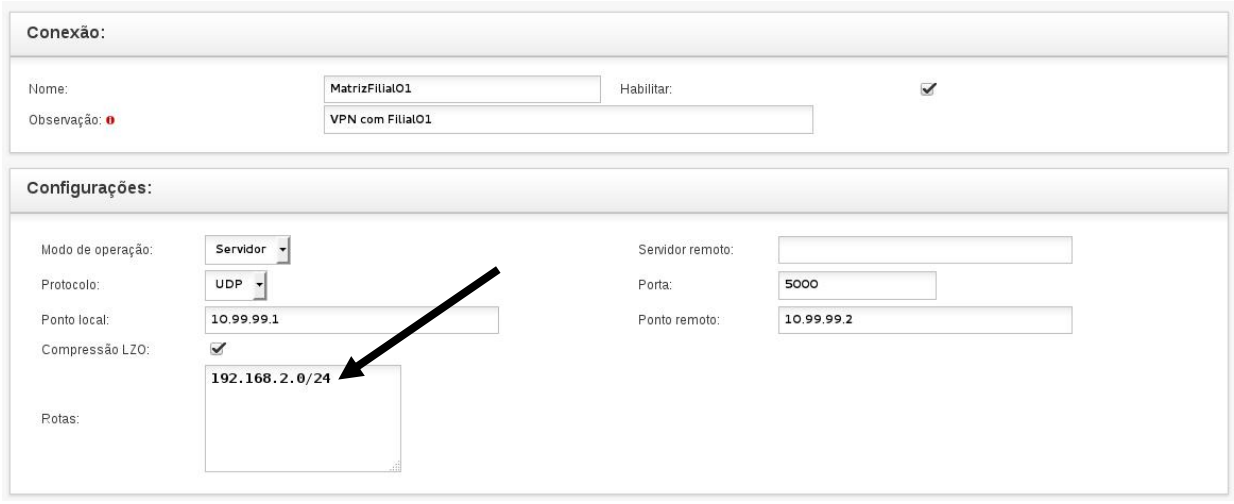
Porta: escolha uma porta que não esteja sendo utilizada e que será a mesma porta nas configurações da filial. Se você estiver criando vários túneis VPN (várias filiais), use uma porta para cada túnel.

Ponto local: Escolha o endereço IP do túnel VPN (lado da Matriz). Deve ser uma faixa IP diferente da rede. Exemplo: **10.99.99.1**

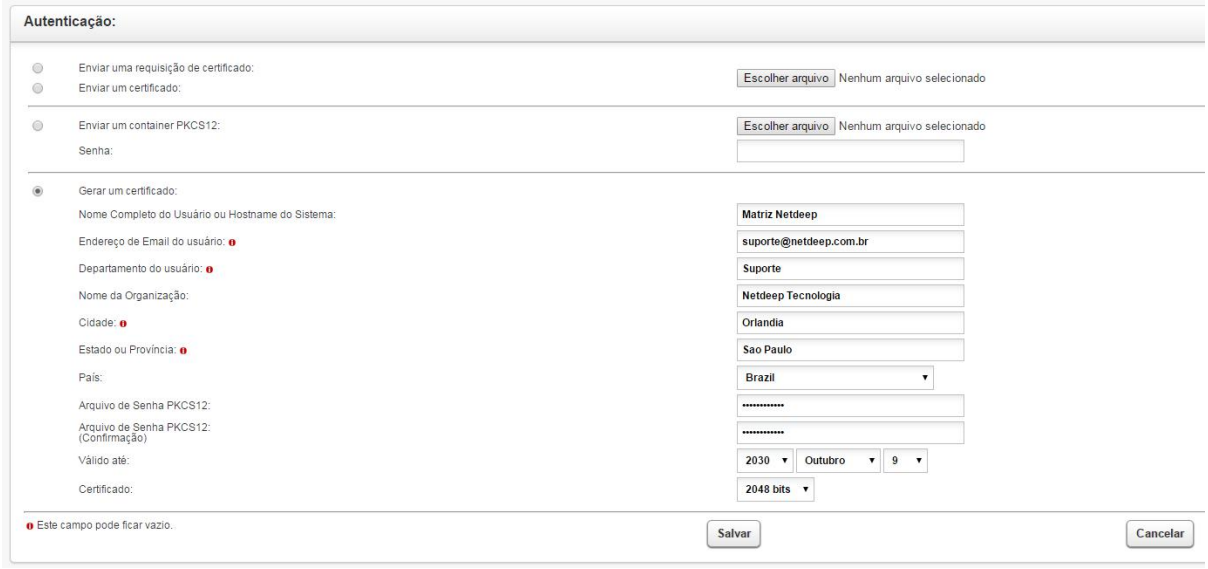
Ponto remoto: Este será o endereço IP do túnel VPN do ponto remoto (lado da filial). Preencha com IP da mesma faixa do **Ponto local**. Exemplo: **10.99.99.2**

Compressão LZO: Marque esta opção para utilizar compressão do protocolo, reduzindo o tamanho do pacote trafegado e economizando banda de rede.

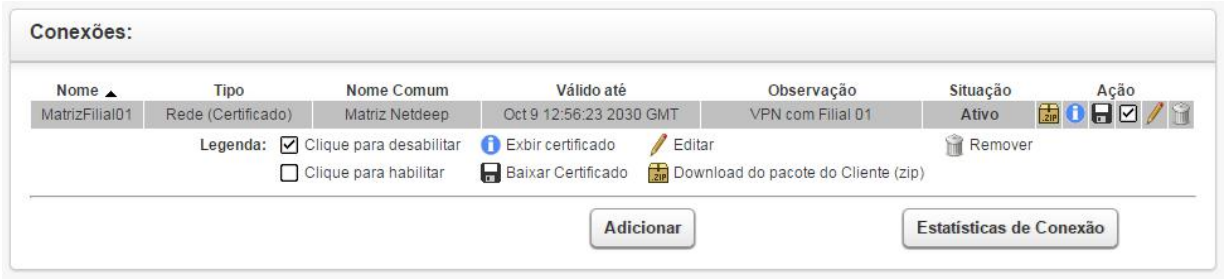
Rotas: Este campo é responsável por subir as rotas necessárias para determinadas faixas IP, então preencha com a faixa IP da filial. Exemplo: **192.168.2.0/24**



Em “**Autenticação**” preencha os campos e clique em **Salvar**.

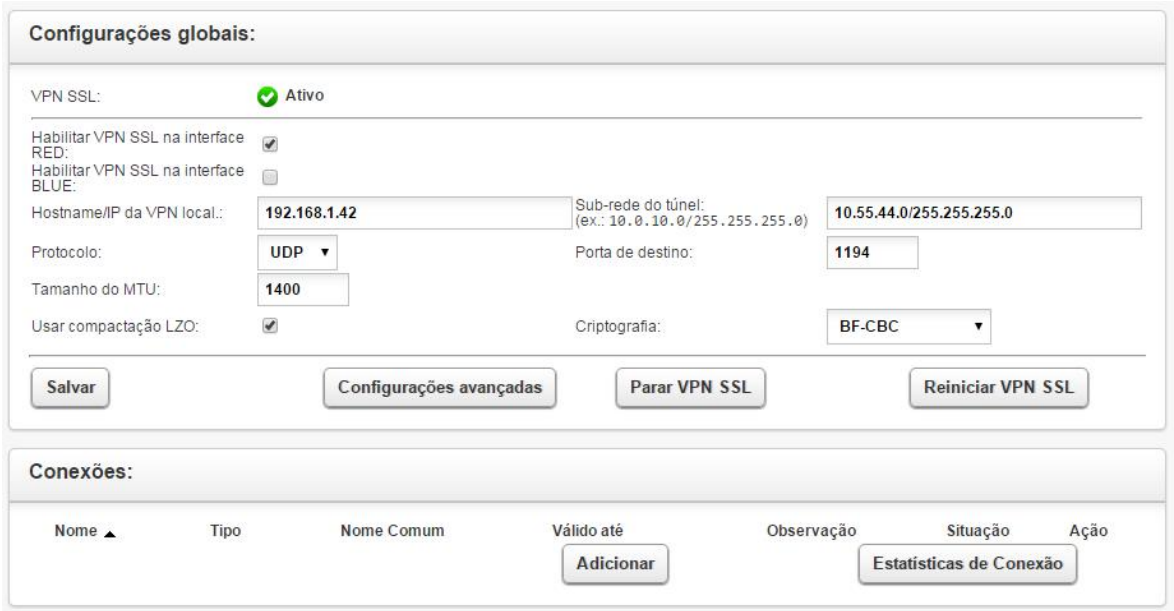


Na página “**Configurações da VPN SSL**” vá em “**Conexões**” e clique no símbolo do “**Disquete**” para realizar download do arquivo **PKCS12** que utilizaremos para realizar as configurações no firewall da filial 01.



4- Configurando VPN na Filial

Para criar a VPN na Filial, vá ao menu “**VPN**” → “**SSL**”. Em “**Conexões**” clique no botão **Adicionar**.



Em “**Tipo de conexão**” selecione a opção “**VPN Rede-à-Rede**” e clique no botão **Adicionar**. Preencha os campos e em seguida clique em **Salvar**.

Em conexão, preencha os campos “**Nome**” e “**Observação**”.

Modo de operação: selecione a opção **Cliente.**

Servidor Remoto: preencha este campo com o IP válido da Matriz.

Protocolos: para conexões VPN utilizamos o protocolo UDP

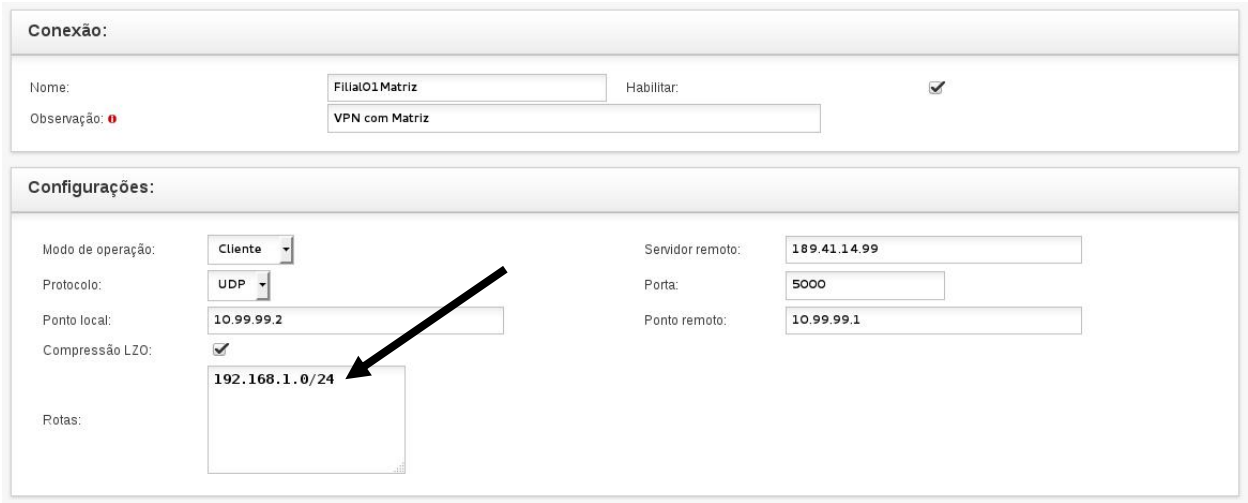
Porta: preencha com a mesma porta utilizada na configuração da Matriz.

Ponto local: preencha com os mesmos endereços IP utilizados na configuração da VPN na Matriz, porém agora os endereços IP são invertidos. O IP que na Matriz era local será o remoto na filial e vice-versa. No nosso exemplo: **10.99.99.2**

Ponto remoto: Mesma coisa do ponto local. Inverta, nesse nosso exemplo será: **10.99.99.1**

Compressão LZO: Marque esta opção para utilizar compressão do protocolo, reduzindo o tamanho do pacote trafegado e economizando banda de rede.

Rotas: Este campo é responsável por subir as rotas necessárias para determinadas faixas IP, então preencha com a faixa IP da matriz. Exemplo: **192.168.1.0/24**

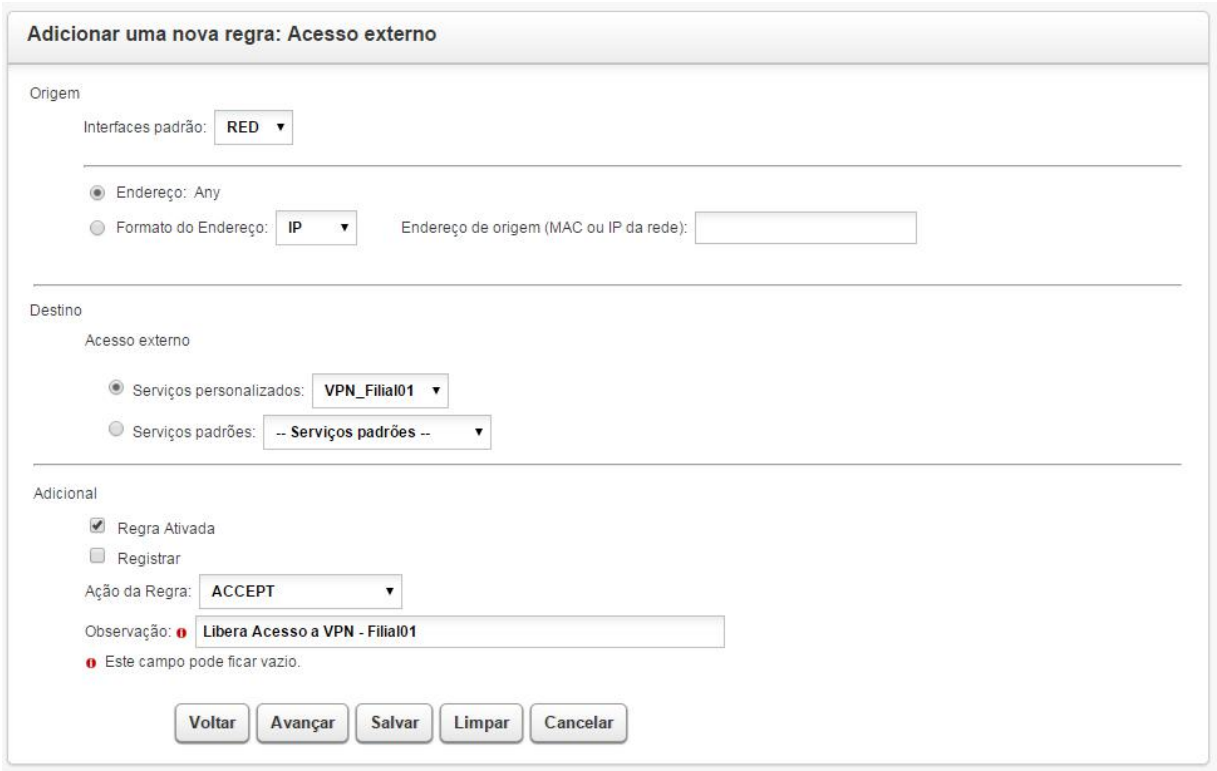


Em “**Autenticação**” selecione a opção “**Enviar um container PKCS12**” e em seguida clique no botão “**Escolher arquivo**” e selecione o arquivo salvo anteriormente, digite a senha utilizada para gerar o arquivo e clique em **Salvar**.

5- Liberando a conexão no firewall

Agora iremos liberar a conexão externa da VPN nas regras do firewall da matriz. Primeiramente precisamos criar o serviço de acordo com a porta que escolhemos na configuração da VPN. Vá ao menu “**Firewall**” → “**Serviços**”. Preencha os campos e clique no botão **Adicionar**.

Agora iremos configurar a regra no firewall. Vá no menu "**Firewall**" → "**Regras**". Clique no botão **"Acesso externo"** em **Serviços personalizados** escolha o serviço criado anteriormente **"VPN_Filial01"** e em **"Observação"** escolha uma descrição para regra depois clique no botão **Salvar.**



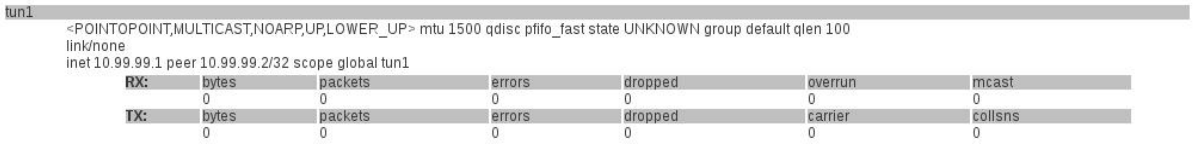
A regra deve ficar igual a imagem abaixo:

IMPORTANTE: Caso tenha mais de uma filial, faça o procedimento 3, 4 e 5 para cada filial.

Você poderá monitorar a situação de cada VPN em "VPN"->"SSL". Na tela "Conexões":

6- Liberando a comunicação entre as redes

Agora vamos permitir a comunicação vindo da interface da VPN com nossa interface de rede interna(lan-1). No firewall da Matriz, vá ao menu "**Situação**" → "**Situação da rede**" e verifique como subiu a interface da VPN, no nosso exemplo **tun1**(10.99.99.1)



Certifique-se que a opção "Modo Avançado" esteja habilitada em seu firewall, para isso acesse "**Firewall**" → "**Configuração do firewall**". Se a opção estiver desabilitada, habilite e clique no botão "**Salvar**".

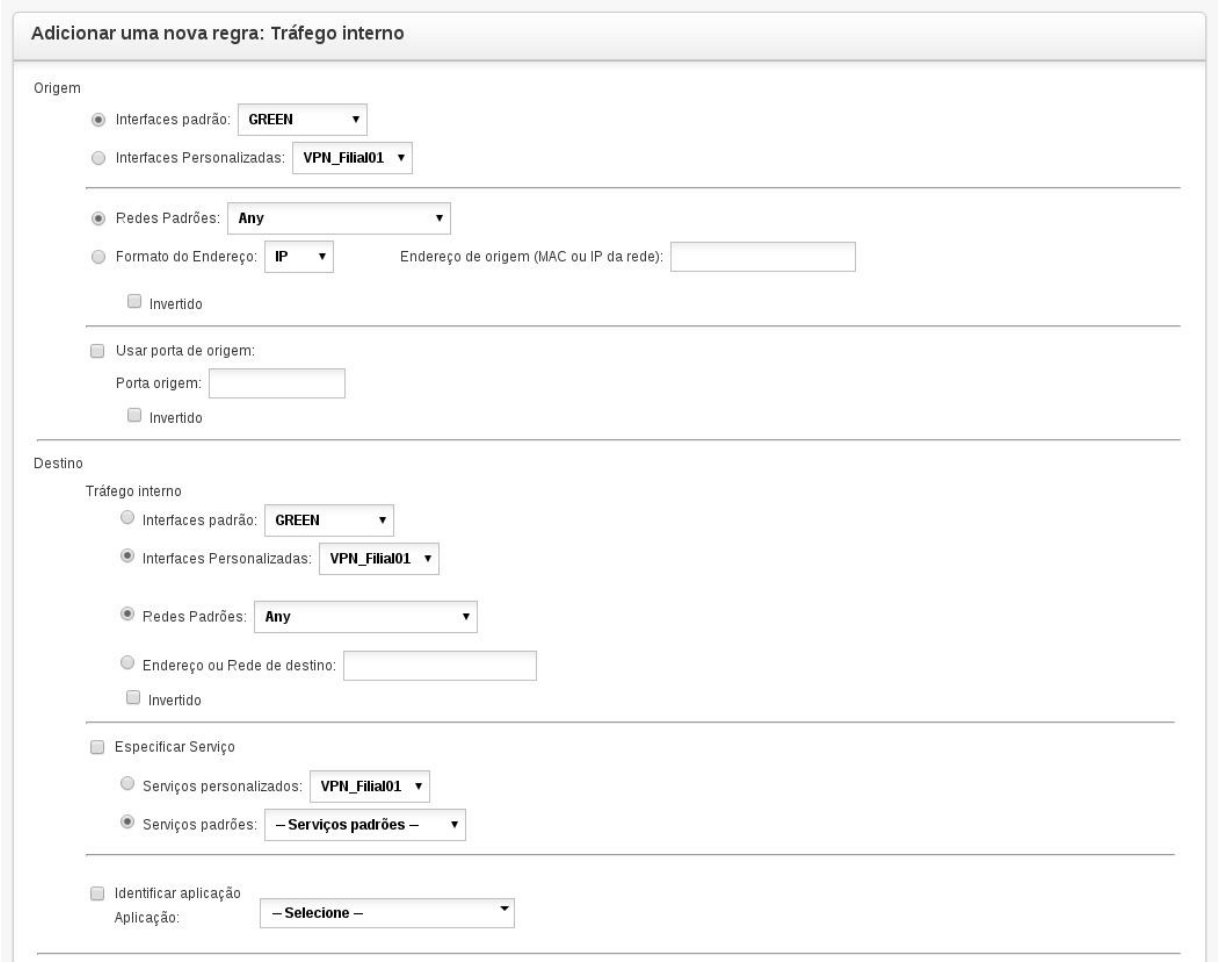
Agora vamos criar uma interface para esta **tun1**. Vá ao menu "**Firewall**" → "**Interfaces**".

Nome: escolha um nome da interface.
Interface: em nosso exemplo: **tun1**

Em seguida clique no botão "**Adicionar**".

Agora, vamos criar as regras permitindo a comunicação da interface GREEN com a interface VPN_Filial01(em nosso exemplo). Vá ao menu "**Firewall**" → "**Regras**", em seguida clique no botão "Tráfego interno".

Em **Origem** "Interfaces padrão" selecione **GREEN**, "Redes Padrões" selecione **Any**. Em **Destino** "Interfaces Personalizadas" selecione **VPN_Filial01**, "Redes Padrões" selecione **Any**. Depois coloque uma observação indicando o que a regra faz e clique no botão "Salvar".



A regra deverá estar da seguinte maneira:

Agora para facilitar vamos criar uma regra parecida só invertendo a origem e destino, então clique nos "papelzinhos" em frente a regra criada para copiar a mesma. Agora a **Origem** é **VPN_Filial01** e o **Destino** é **GREEN**. Clique em salvar e o resultado das 2 regras deverá estar da seguinte maneira:

7- Para saber mais

http://www.netdeep.com.br/secure/