



GUIA DE CONFIGURAÇÃO

CONEXÕES VPN SSL (CLIENT TO
SERVER)

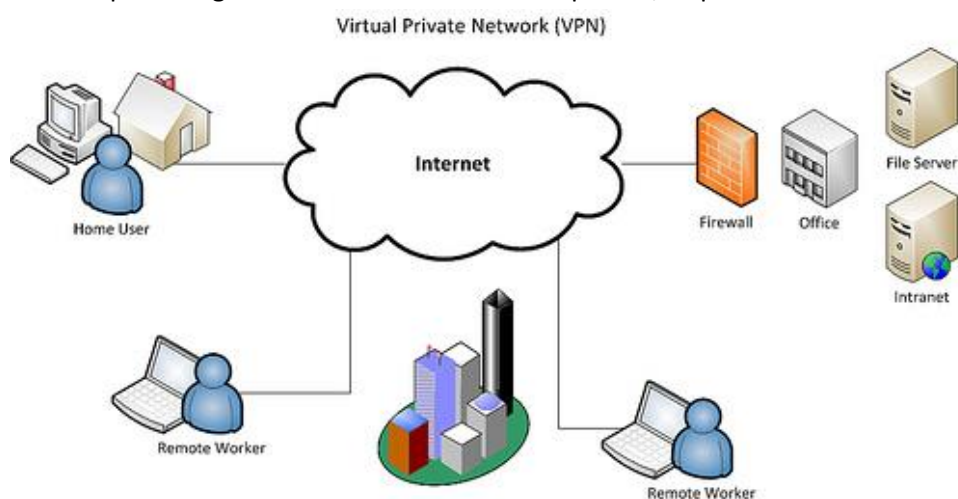
Conexões VPN SSL (Client to Server)

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 NetdeepSecure vá no 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 “Gerar Certificados Raiz/Host”.

Obs.: não utilize acentos em nenhum dos campos.

Gerar Certificados Raiz/Host:

Nome da Organização:	<input type="text" value="Netdeep Tecnologia"/>
Nome de host do Netdeep Secure:	<input type="text" value="192.168.1.42"/>
Seu E-Mail:	<input type="text" value="suporte@netdeep.com.br"/>
Seu Departamento:	<input type="text" value="Suporte"/>
Cidade:	<input type="text" value="Orlandia"/>
Estado ou Província:	<input type="text" value="Sao Paulo"/>
País:	<input type="text" value="Brazil"/>
Nome alternativo para o sujeito (subjectAltName=email:*,URI:*,DNS:*,RID:*)	<input type="text"/>
Válido até:	<input type="text" value="2030"/> <input type="text" value="Junho"/> <input type="text" value="5"/>
Message digest algorithm:	<input type="text" value="sha256"/>
Certificado Raiz:	<input type="text" value="2048 bits"/>
Certificado do Host:	<input type="text" value="2048 bits"/>

ATENÇÃO: A geração dos certificados de raiz e de host pode levar um longo tempo, até vários minutos em equipamentos mais antigos. Por favor, seja paciente.

Enviar um arquivo PKCS12: Nenhum arquivo selecionado

Arquivo de Senha PKCS12:

Este campo pode ficar vazio.

Após gerar o certificado iremos realizar as configurações SSL. Vá no menu “VPN” → “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 clique no botão “Salvar Configurações Avançadas”.

Enviar Rotas
Redirecionar todo o tráfego através do túnel: (redirect-gateway def1)
Green Network:
Blue Network:

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 clique no botão “**Iniciar VPN SSL**”, em “**VPN SSL**”.

Configurações globais:

VPN SSL: ❗ Parado

Habilitar VPN SSL na interface RED:
Habilitar VPN SSL na interface BLUE:

Hostname/IP da VPN local.: Sub-rede do túnel:
(ex.: 10.0.10.0/255.255.255.0)

Protocolo: Porta de destino:

Tamanho do MTU:

Usar compactação LZO: Criptografia:

Se tudo ocorrer bem, o status do serviço irá aparecer **Ativo** e em verde.

Configurações globais:

VPN SSL: ✅ Ativo

Habilitar VPN SSL na interface RED:
Habilitar VPN SSL na interface BLUE:

Hostname/IP da VPN local.: Sub-rede do túnel:
(ex.: 10.0.10.0/255.255.255.0)

Protocolo: Porta de destino:

Tamanho do MTU:

Usar compactação LZO: Criptografia:

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

3- Criando as conexões para os usuários

Para criar as conexões para os usuários, vá no menu “**VPN**” → “**SSL**”. Em “**Conexões**” clique no botão **Adicionar**.

Configurações globais:

VPN SSL: Ativo

Habilitar VPN SSL na interface RED:
Habilitar VPN SSL na interface BLUE:

Hostname/IP da VPN local.: Sub-rede do túnel: (ex.: 10.0.10.0/255.255.255.0)

Protocolo: Porta de destino:

Tamanho do MTU:

Usar compactação LZO: Criptografia:

Conexões:

Nome ▲	Tipo	Nome Comum	Válido até	Observação	Situação	Ação
			<input type="button" value="Adicionar"/>			<input type="button" value="Estatísticas de Conexão"/>

Em “**Tipo de conexão**” deixe marcada a opção “**VPN Host-para-Rede (RoadWarrior)**” e clique no botão **Adicionar**. Preencha os campos e em seguida clique em **Salvar**.

Nome: Habilitar:

Observação:

Autenticação:

Enviar uma requisição de certificado: Nenhum arquivo selecionado

Enviar um certificado:

Gerar um certificado:

Nome Completo do Usuário ou Hostname do Sistema:

Endereço de Email do usuário:

Departamento do usuário:

Nome da Organização:

Cidade:

Estado ou Província:

País:

Arquivo de Senha PKCS12:

Arquivo de Senha PKCS12: (Confirmação)

Válido até:

Certificado:

Este campo pode ficar vazio.

Defina uma senha se quiser que os usuários autenticuem antes de conectar.

4- Copiando os arquivos de configuração

Para baixar os arquivos para conexão da VPN, vá no menu “VPN” → “SSL”. Baixe o arquivo clicando no pacote **.zip** e extraia os arquivos para dentro da pasta **config** de seu **OpenVPN**.

Nome	Tipo	Nome Comum	Válido até	Observação	Situação	Ação
Netdeep	Host (Certificado)	netdeep	Jun 5 18:33:59 2030 GMT	VPN para Suporte da Netdeep Tecnologia	FECHADO	<input type="checkbox"/> Exibir certificado <input type="checkbox"/> Baixar Certificado <input type="checkbox"/> Editar <input type="checkbox"/> Download do pacote do Cliente (zip)

Clique para desabilitar
 Clique para habilitar

5- Liberando a conexão no firewall

Agora iremos liberar a conexão externa da VPN nas regras de firewall. Vá no menu “Firewall” → “Regras”. Clique no botão “Acesso externo” em **Serviços padrões** escolha o serviço “Netdeep OpenVPN (1194)” e em “Observação” escolha uma descrição para regra depois clique no botão **Salvar**.

Adicionar uma nova regra: Acesso externo

Origem

Interfaces padrão: RED

Endereço: Any
 Formato do Endereço: IP Endereço de origem (MAC ou IP da rede):
 Invertido

Usar porta de origem:
 Porta origem:
 Invertido

Destino

Acesso externo

Serviços padrões: Netdeep OpenVPN (1194)

Adicional

Regra Ativada
 Registrar
 Ação da Regra: ACCEPT
 Observação: Libera Acesso OpenVPN
 Este campo pode ficar vazio.

Configurações avançadas

Match limit: Habilitar registro

--limit avg 10 minute
 --limit-burst number 5

6- Para saber mais

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

<http://www.openvpn.net>