

Rede privada de um modo simples

Segredo simples

O SocialVPN oferece uma abordagem simples e rápida para configurar uma conexão segura para comunicação e troca de informações.

por **Christoph Langner**

Imagine que um dia um funcionário esteja fora dos muros da empresa – ou pior, atrás de um roteador sem fio com NAT – e seja preciso acessar o computador dele. Ou então, talvez você precise de uma conexão criptografada para trocar dados confidenciais através de redes inseguras e tenha preocupação com a complexidade de se configurar um servidor VPN. O SocialVPN oferece uma técnica simples para a troca de dados por um canal criptografado entre redes e roteadores.

A VPN (*Virtual Private Network*) já provou seu valor como um meio seguro e eficaz para troca de dados entre computadores pela Internet. Os computadores em uma VPN agem como se estivessem na mesma rede local – por isso, serviços como o Samba, RDP, VNC ou SSH podem ser usados sem perigo de intercep-

tação por invasores. Logicamente, uma VPN típica requer muita configuração. Por isso, produtos como o *Hamachi* [1], com suporte a VPNs por firewalls e roteadores sem a necessidade de configurações complexas, se estabeleceram. Infelizmente, o Hamachi tem o código fechado, o que elimina parte da segurança da VPN.

Além do mais, a empresa por trás do programa, a LogMeIn, cobra uma taxa de licença para uso comercial, e é preciso ter sempre uma conta com a LogMeIn. Pior do que isso, a versão do software para Linux não é bem mantida e a LogMeIn não oferece uma interface gráfica.

O projeto SocialVPN [2] oferece uma alternativa licenciada sob a GPLv2 ao produto comercial com a mesma funcionalidade. O SocialVPN está disponível para Windows e Linux; a versão para Mac OS X está atualmente na fase alfa.

O SocialVPN combina o trabalho de três projetos de código aberto para estabelecer uma VPN entre qualquer número de hosts. A biblioteca *Brunet* [3] suporta redes *peer-to-peer* através de roteadores sem a necessidade de enca-

minhamento de portas do roteador para um computador por trás dele. O IPOP [4] faz o roteamento dos pacotes entre as redes, enquanto que a interface XMPP (Jabber) [5] autentica usuários e troca chaves através de um canal seguro. Além do mais, o SocialVPN possui uma interface web fácil de usar.

A autenticação via Jabber é necessária e, por isso, é preciso ter uma conta em um servidor compatível para se usar o SocialVPN. Caso você possua uma conta de e-mail com um provedor de webmail, como o Gmail, automaticamente já tem uma conta no Jabber.

Seu endereço no Jabber será exatamente o mesmo do seu endereço de e-mail – quer dizer, seu_nome@gmail.com. Na falta de uma conta no Gmail, os servidores públicos do Jabber estão listados no site jabber.org [6], e é possível registrar-se em qualquer um deles para abrir uma conta.

Instalação

No Linux, é preciso ter o ambiente Mono instalado. Instalar o SocialVPN é bem fácil. Basta baixar o arquivo do programa [7], descompactá-lo e executar o script `setup.sh` para configurá-lo. Depois, execute o script sem os privilégios de root (**listagem 1**) e forneça seu ID do Jabber, um

Listagem 1: Instalação do SocialVPN

```
$ ./setup.sh
Ent er userid (jabberid@host.com):
    joe.public@jabber.example.com
Enter PCID (home-pc): samplehost
Enter Name (Jane Doe): Joe Public
Creating certificate...
Certificate creation successful
Run ./socialvpn as root
```

nome de máquina e um nome de usuário na janela de configuração.

O script permite gerar certificados individuais. No Windows, o SocialVPN requer a instalação do framework Microsoft .NET [8] primeiro. Depois, basta clicar duas vezes no ícone do programa para executar `setup.cmd`. A primeira medida tomada pelo script é desinstalar o SocialVPN (mesmo que ele nunca tenha sido instalado) e depois instalar a nova versão. Os drivers do dispositivo não estão assinados, portanto, será necessário aceitar o aviso apresentado pela rotina de instalação.

Execução

Após completar a instalação, inicie o VPN no Linux executando o script `socialvpn` (listagem 2). Note que é necessário ser root para configurar as rotas e a interface da rede virtual. Supondo que o script não tenha encontrado nenhum erro, abra o navegador web e visite o endereço <http://127.0.0.1:58888> para acessar a interface web do SocialVPN.

No Windows, o SocialVPN deve ser iniciado e parado, respectivamente, com os scripts `start_socialvpn` e `stop_socialvpn`. No Windows Vista ou no Windows 7, é necessário clicar com o botão direito no ícone e escolher *Executar como Administrador*: é impossível configurar a interface de rede virtual de outra maneira.

Novos contatos

Após os dois interlocutores configurarem e iniciarem o SocialVPN, é necessário adicionar contatos ao SocialVPN, da mesma forma como se faz num programa de mensagens instantâneas. Certifique-se de clicar em Login para se conectar ao servidor, com o uso de seu ID Jabber e senha correspondente. Depois do login, aparecerá a mensagem *Online* ao lado do link de login.

A partir desse momento, já é possível adicionar seus contatos da VPN.

Listagem 2: Execução do script `socialvpn`

```
$ sudo ./socialvpn
Set 'tapipop' nonpersistent
Set 'tapipop' persistent and owned by uid 1000
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/
Listening on LPF/tapipop/0e:b0:52:6e:66:f7
Sending on LPF/tapipop/0e:b0:52:6e:66:f7
Sending on Socket/fallback
DHCPDISCOVER on tapipop to 255.255.255.255 port 67 interval 3
DHCPOFFER of 172.31.0.2 from 172.31.0.1
DHCPREQUEST of 172.31.0.2 on tapipop to 255.255.255.255 port 67
DHCPACK of 172.31.0.2 from 172.31.0.1
* Reloading /etc/samba/smb.conf smb only
...done.
bound to 172.31.0.2 -- renewal in 1294 seconds.
Point your browser to http://127.0.0.1:58888
```

A interface web possui um link *Add Friends* para isso. No campo de entrada, digite seu contato na forma de um *fingerprint* de ID do Jabber (figura 1); por exemplo, para fulano@jabber.exemplo.br, essa *fingerprint* é `SVPN:123456789`. Ou seja, não basta saber apenas o ID Jabber de um contato; também é necessário ter a *fingerprint* do cliente para configurar a conexão VPN.

Certifique-se de usar um canal de comunicação seguro para trocar *fingerprints* com seus contatos; caso contrário, seria um convite a intrusos. Para uma comunicação bidirecional, é preciso também enviar seu ID Jabber e a *fingerprint* ao seu contato para que ele possa adicioná-lo à sua lista.

Após informar os IDs Jabber e as *fingerprints*, seus contatos aparecerão como *Online*. Neste ponto, seus computadores já estão em rede, e já é possível ver os IPs e nomes das máquinas de seus contatos (figura 2) na interface usada para se comunicar com eles. Como teste inicial, tente um ping no computador do outro lado da conexão. O SocialVPN irá fornecer os detalhes para isso.

Caso o ping funcione, é possível começar a usar serviços mais complexos. Repare que o SocialVPN é apenas uma rede entre computadores remotos; ele não possui serviços de acesso remoto à área de trabalho ou de compartilhamento de arquivos. Caso você precise de algo assim, tecnologias como NX, RDP e VNC provavelmente são as melhores escolhas.

Em nosso laboratório, serviços baseados em Avahi mostraram-se bem eficientes. Por exemplo, não tivemos problemas para usar o *Vinagre/Vino* para acessar remotamente a área de trabalho remota, conversar usando o *Pidgin* e o *Bonjour* ou transferir arquivos e pastas usando o *Giver* e tudo sem a necessidade de configurar com antecedência os servidores correspondentes.

Conclusões

O SocialVPN é realmente útil para ultrapassar obstáculos criados por roteadores com NAT entre dois computadores com uma conexão à Internet. Ele pode ser usado até em jogos que possuam recursos de

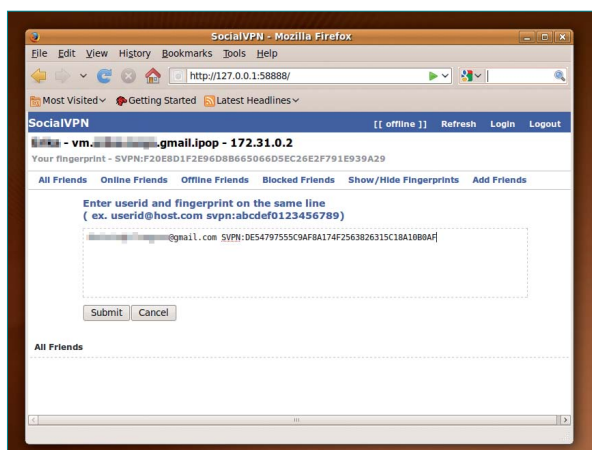


Figura 1 Adicionando contatos ao SocialVPN.

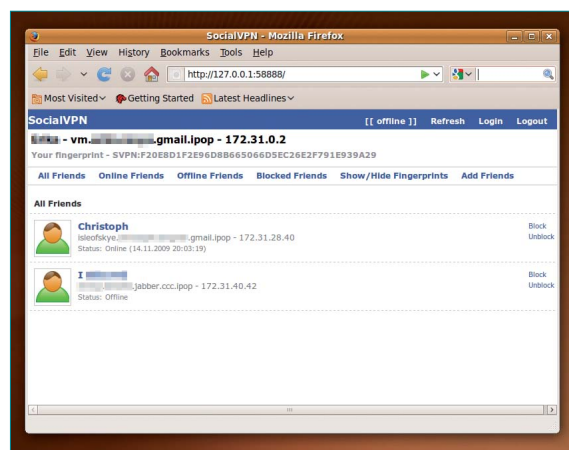


Figura 2 O SocialVPN lista seus contatos e os dados de suas redes na interface.

LAN, mas não de Internet, e é uma ótima escolha para usar o VNC para resolver os problemas do desktop de um cliente sem precisar configurar o encaminhamento de portas nem criar um túnel SSH. Configurar uma VPN entre dois ou mais computadores é uma experiência rápida e fácil.

Dito isso, o SocialVPN é incapaz de ajudar em tarefas mais complexas. Não conseguimos usá-lo para estabelecer uma VPN em uma rede na qual o firewall bloqueava todas as conexões de saída e permitia apenas HTTP e HTTPS através de um proxy. Também não conseguimos executar o SocialVPN juntamente com outra conexão VPN. Portanto, é impossível usar o SocialVPN em uma rede com apenas uma interface VPN.

O SocialVPN é perfeito para configurar uma rede privada virtual de forma fácil e rápida em máquinas com diferentes sistemas operacionais. Pequenas empresas ou usuários domésticos em particular, que usam DSL para se conectar à Internet, irão se beneficiar do SocialVPN, pois ele elimina a necessidade de configurações de rede complexas. Porém, um programa de configuração para o Windows e pacotes para várias distribuições Linux poderiam simplificar ainda mais as coisas. ■

Mais informações

- [1] Hamachi: <https://secure.logmein.com/products/hamachi2/>
- [2] SocialVPN: <http://socialvpn.wordpress.com>
- [3] Brunet: <http://github.com/johnynek/brunet/tree>
- [4] IPOP: <http://www.grid-.org/wiki/index.php/IPOP>
- [5] Jabber-Net-XMPP-API: <http://code.google.com/p/jabber-net/>
- [6] Lista de servidores públicos Jabber: <http://www.jabberes.org/servers/>
- [7] Download do SocialVPN: <http://code.google.com/p/sociavpn/downloads/list>
- [8] Microsoft .NET Framework 3.5: <http://tinyurl.com/1u1002-dotnet>

O autor

Christoph Langner trabalha com gerenciamento de testes na PTV em Karlsruhe, na Alemanha, e é membro ativo da comunidade de software de código aberto há muitos anos. Veja seu blog sobre GNU/Linux em <http://linuxundich.de>.

Gostou do artigo?

Queremos ouvir sua opinião. Fale conosco em cartas@linuxmagazine.com.br

Este artigo no nosso site: <http://lnm.com.br/article/3505>

