

Rede virtual privada sem complicação

# Vias privadas

O SSL-Explorer fornece uma interface para simplificar a configuração de uma rede virtual privada. Tudo via navegador

POR HOLGER REIBOLD

**F**uncionários que trabalham fora da empresa precisam acessar suas redes corporativas a partir de diferentes locais. Nesse quesito, redes virtuais privadas (ou VPN, Virtual Private Network) são a solução. Elas fornecem acesso remoto e privado pela Internet, protegendo o tráfego e impedindo acessos indevidos aos dados na rede através de criptografia. No entanto, muitas VPNs são bem complicadas de configurar, além de exigir ajustes finos nos firewalls.

O *SSL-Explorer* [1] é uma alternativa fácil. Ele configura uma VPN baseada na web. O único requisito é um navegador (com *Java*) como cliente. Uma interface web funciona como o front-end de configuração. O programa encapsula (tunneling) todo tráfego *TCP* (como *SMTP*, *POP* e *HTTP*) em uma conexão protegida por *SSL* (Secure Sockets Layer).

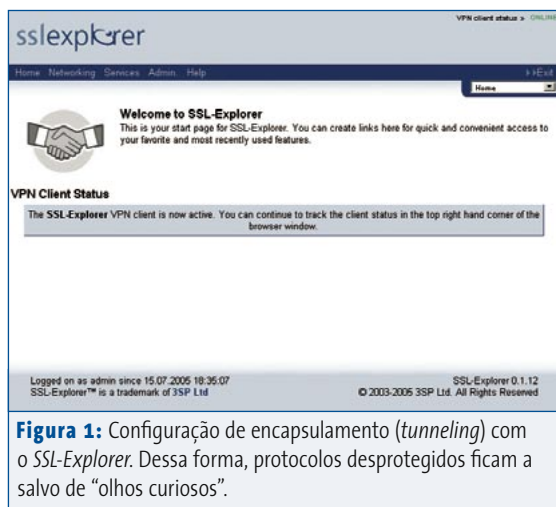
Escrito em *Java*, o *SSL-Explorer* roda em *Linux* ou *Windows*®. Para controlar o sistema “de longe”, os administradores podem usar ferramentas de acesso remoto como *SSH*, *SFTP*, *VNC*, *Citrix* e outros serviços de terminal. E um gerenciamento integrado de perfis acrescenta a habilidade de definir configurações variadas para múltiplos pontos de acesso. Há ainda uma extensão comercial ao programa – o *Xtra*, da *3sp* [2] – que adiciona mecanismos de autenticação (*LDAP*, *PIN*, *SMS* e chave pública), assim como suporte técnico e outras melhorias.

## Banco de dados de usuários

O *SSL-Explorer* tem seu próprio banco de dados para autenticação, mas também é compatível com autenticação centralizada, baseada no *Active Directory*. Funções de interoperabilidade incluem suporte a políticas e “pastas web” do *Windows* (o suporte a servidores *LDAP* está disponível com o plugin comercial *Xtra*, citado anteriormente).

Os requisitos para rodar o programa (que ocupa 140 MB do disco rígido) exigem, no mínimo, um *Pentium III* (1 GHz) e 512 MB de *RAM*. O arquivo *.zip* em [1] vem com um pacote *RPM* que instala o *SSL-Explorer* em `/opt/sslexplorer`. Para iniciar a ferramenta de configuração via web, simplesmente digite `/opt/sslexplorer/setup-sslexplorer`. A instalação leva você a uma URL que é a interface via navegador. Por padrão, ela “ouve” a porta 28080.

Antes de tudo, é preciso ajustar alguns parâmetros críticos no modo de configuração. A primeira página da interface se chama *Web Security*. Ela permite criar ou importar certificados. Se quiser apenas testar o programa, crie



**Figura 1:** Configuração de encapsulamento (tunneling) com o *SSL-Explorer*. Dessa forma, protocolos desprotegidos ficam a salvo de “olhos curiosos”.

seu próprio certificado. Mas em um servidor operacional e em produção, você vai precisar de uma chave de alguma *Autoridade de Certificação* que todos os navegadores respeitem.

Após completar a configuração, os usuários têm três opções para iniciar o SSL-Explorer. O comando na distribuição *Red Hat* (por enquanto a única suportada oficialmente) é `service sslexplorer start`. Digite `/etc/init.d/sslexplorer console` ou, talvez, `/opt/sslexplorer/sslexplorer console`, em outras distribuições.

## Começando

Use o protocolo *HTTPS* localmente (`https://localhost/`) para acessar a interface. A senha padrão do administrador (usuário `admin`) é `admin`. Depois de se logar, você verá quatro menus:

*Home*, *Networking*, *Serviços* e *Admin*. Na primeira vez que o programa roda, a página inicial informa o status do cliente VPN. Um cliente rodando é uma condição para algumas funções do SSL-Explorer. O botão *Launch* inicia o *applet*.

Já o menu *Home* permite a configuração de parâmetros como os usados no gerenciamento de usuários. *Home* | *My Account* | *Configuration* leva a um grande formulário com configurações de usuário (**Figura 2**). Os administradores podem configurar suas próprias contas e criar perfis individuais para os usuários. O menu *Admin* permite a criação de novos usuários.

**Figura 2:** Esse formulário de configuração permite o gerenciamento de parâmetros das contas de usuários.

A configuração padrão traz dois perfis. Você pode adicionar mais se precisar. Esses perfis permitem especificar propriedades para diferentes situações. O SSL-Explorer usa um controle de acessos hierárquico, baseado nas “funções” de

# LinuxWorld Conference & Expo – Worldwide Series



|                  |                        |  |
|------------------|------------------------|--|
| • Mexico City:   | February 14 – 17, 2006 | <a href="http://www.linuxworldexpo.com.mx">www.linuxworldexpo.com.mx</a>     |
| • Sydney:        | March 28 – 30, 2006    | <a href="http://www.linuxworldexpo.com.au">www.linuxworldexpo.com.au</a>     |
| • Boston:        | April 3 – 6, 2006      | <a href="http://www.linuxworldexpo.com">www.linuxworldexpo.com</a>           |
| • Madrid:        | April 18 – 19, 2006    | <a href="http://www.linuxworldexpo.com">www.linuxworldexpo.com</a>           |
| • Kuala Lumpur:  | April 20, 2006         | <a href="http://www.linuxworldexpo.com">www.linuxworldexpo.com</a>           |
| • Toronto:       | April 24 – 26, 2006    | <a href="http://www.linuxworldcanada.com">www.linuxworldcanada.com</a>       |
| • Shanghai:      | May 2006               | <a href="http://www.linuxworldchina.com">www.linuxworldchina.com</a>         |
| • Milan:         | May 15 – 16, 2006      | <a href="http://www.linuxworldsummit.it">www.linuxworldsummit.it</a>         |
| • Johannesburg:  | May 16 – 19, 2006      | <a href="http://www.linuxworldexpo.co.za">www.linuxworldexpo.co.za</a>       |
| • São Paulo:     | May 23 – 25, 2006      | <a href="http://www.linuxworldbrasil.com.br">www.linuxworldbrasil.com.br</a> |
| • Tokyo:         | May 31 – June 2, 2006  | <a href="http://www.linuxworldexpo.com">www.linuxworldexpo.com</a>           |
| • Seoul:         | June 5 – 7, 2006       | <a href="http://www.linuxworldkorea.com">www.linuxworldkorea.com</a>         |
| • Warsaw:        | June 21 – 22, 2006     | <a href="http://www.linuxworldexpo.com">www.linuxworldexpo.com</a>           |
| • Singapore:     | July 7, 2006           | <a href="http://www.linuxworldexpo.com">www.linuxworldexpo.com</a>           |
| • Beijing:       | August 2006            | <a href="http://www.linuxworldchina.com">www.linuxworldchina.com</a>         |
| • San Francisco: | August 14 – 17, 2006   | <a href="http://www.linuxworldexpo.com">www.linuxworldexpo.com</a>           |
| • Moscow:        | September 4 – 6, 2006  | <a href="http://www.linuxworldexpo.ru">www.linuxworldexpo.ru</a>             |
| • Utrecht:       | October 11 – 12, 2006  | <a href="http://www.linuxworldexpo.nl">www.linuxworldexpo.nl</a>             |
| • London:        | October 25 – 26, 2006  | <a href="http://www.linuxworldexpo.co.uk">www.linuxworldexpo.co.uk</a>       |
| • Guangzhou:     | November 2006          | <a href="http://www.linuxworldchina.com">www.linuxworldchina.com</a>         |
| • Cologne:       | November 14 – 16, 2006 | <a href="http://www.linuxworldexpo.de">www.linuxworldexpo.de</a>             |



World's leading Trade Event for Linux and Open Source in business

Where open minds meet!

cada usuário. Isso permite um controle preciso das permissões. Em vez de associar permissões a um usuário, o administrador associa permissões a uma função e, depois, associa um ou mais usuários a essa função. Por exemplo, as permissões para usuários do departamento de marketing podem ser diferentes das fornecidas para a equipe de vendas.

Definir uma função manualmente não é difícil. Apenas digite um nome na caixa *Create Role* e clique em *Create*. Será acrescentada uma nova função à lista. A função é sublinhada em vermelho para indicar o status *Revoked* (revogada). É preciso acionar essa função antes de começar a usá-la. Ferramentas de configuração bastante detalhadas ajudam a editar as propriedades de cada perfil. Se você estiver em uma rede do tipo Active Directory, será possível importar as configurações de grupos de usuários.

## Contas de usuários

O item de menu *Admin | Access Control | Accounts* leva ao gerenciamento das contas. É aqui que usuários são associados a determinadas funções. Independente de você estar criando ou editando uma conta, a janela que aparece é a mesma. Aqui é preciso especificar o número de identificação do usuário, o nome completo dele e, possivelmente, um endereço de email.

O SSL-Explorer permite restringir o acesso a partir de IPs específicos. Para acessar o formulário responsável por essa configuração, acesse *Admin | Access Control | IP-Restrictions*. O administrador pode permitir ou negar o acesso a partir de determinado IP. Para fazer isso, digite um IP em *IP Address*. Para cobrir uma subrede completa, use algo como `192.168.1.*`. Depois, o formulário vai exibir a seção *Current Rules* (regras atuais) atualizada, com a lista de permissões e restrições aos endereços de IP.

## Seguindo as regras

O item *Admin | Access Control* abre a página *Security Options* (figura 3). Esse formulário permite criar ou modificar configurações gerais de segurança. Elas incluem o tipo de banco de dados, que pode ser tanto o formato interno do SSL-Explorer ou o Active Directory.

Também é possível especificar o número de tentativas de login antes que uma conta seja desativada, especificar a complexidade das senhas exigidas e dar privilégios de administração para grupos e usuários, além de permitir ou não conexões de múltiplas sessões.

A opção *Strict Checking* do cliente VPN é bem interessante. Ela controla o acesso às configurações do sistema operacional e da instalação Java do cliente.

## Outros recursos

O SSL-Explorer tem recursos de encapsulamento (tunneling) bem abrangentes e, ao mesmo tempo, de simples configuração. É possível proteger qualquer serviço *TCP* e configurar o acesso ao *POP3*, por exemplo. Para proteger o tráfego *POP3*, os administradores precisam acessar as opções de encapsulamento via *Networking | SSL Tunnels* e digitar a porta do servidor de email (tipicamente 110), o hostname e a porta alvo (de novo, 110 por padrão) no formulário *Create Tunnel*.

Clique em *Add* para configurar o primeiro encapsulamento. Agora basta que os usuários modifiquem os parâmetros em seus clientes de email de acordo com a configuração VPN. Isso significa substituir o servidor *POP3* por `localhost`. O cliente VPN local e o servidor VPN pro-

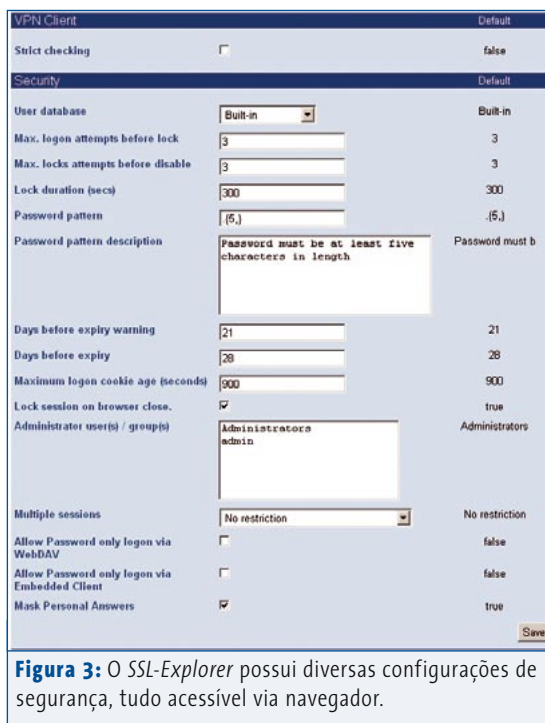


Figura 3: O SSL-Explorer possui diversas configurações de segurança, tudo acessível via navegador.

tegem a conexão. O procedimento para configuração de *SMTP* e outros serviços seguem o mesmo padrão.

O menu *Network | Network Places* permite que os usuários acessem a rede Windows. Esse menu permite reservar o acesso de funcionários fora da empresa. Outros recursos interessantes incluem acesso a repositórios *WebDAV* e extensões *XML*.

## Conclusão

O SSL-Explorer traz conectividade VPN, com controle via navegador. Administradores profissionais podem sentir falta da configuração mais detalhada oferecida por ferramentas como o *Openswan* e outras. Mas, para tarefas mais simples, ele é mais do que suficiente para o trabalho. ■

## INFORMAÇÕES

[1] SSL-Explorer: [sourceforge.net/projects/sslexplorer](http://sourceforge.net/projects/sslexplorer)

[2] Extensões comerciais: [www.sstools.com/showSslExplorerXtra.do](http://www.sstools.com/showSslExplorerXtra.do)