# Acesso remoto em *firewalls* e topologia para *gateways* VPN

Francisco José Candeias Figueiredo
Instituto de Computação - UNICAMP

Paulo Lício de Geus
Instituto de Computação - UNICAMP

**Abstract**

VPNs are being hailed as the solution for several situations involved in the Internet these days. Firewalls have seen a decade of evolution and sophistication to deal with specific problems. However, we are also seeing the proliferation of VPN configurations on otherwise secure networks based on firewalls.

This paper discusses the security problems incurred by the adoption of VPN gateways in standard firewalls. It also suggests more secure topology solutions for the standard VPN uses, as well as for the remote access client. We also propose an implementation based on freely available software that satisfies the security issues brought about by this paper.

## 1. Introdução

Desde que as empresas começaram a usar computadores em mais de uma localidade, apareceu o desejo e a necessidade de conectá-las de maneira privada e segura para facilitar as comunicações corporativas. Contudo a instalação de uma rede corporativa envolvendo escritórios ou plantas localizadas a quilômetros de distância, pode ser bastante difícil. Em muitos casos, não há outro recurso a não ser o de usar linhas dedicadas para ligar localidades separadas geograficamente. Contudo, este tipo de tecnologia oferece problemas operacionais importantes para as empresas, tais como: alto custo, dificuldades de escalabilidade e baixa flexibilidade.

Uma solução, para este tipo de problema, é o uso da infra-estrutura aberta e distribuída da Internet para transmissão de dados, de modo privado, entre localidades diversas de uma empresa. A isso chamamos de VPN – Virtual Private Network - Rede Privada Virtual.

Como a Internet é uma rede pública com transmissão aberta da maior parte dos dados, cabe às VPNs prover o suporte criptográfico necessário para se obter a privacidade desejada. Isto inclui o ciframento, a verificação e a assinatura dos dados que trafegam entre as localidades, protegendo os dados de escuta, alteração e impostura por parte de agentes não autorizados. Como vantagem adicional, a VPN permite conexões seguras para usuários móveis, em virtude das conexões discadas que os provedores de Internet oferecem em seus POPs [Ko98].

Contudo devemos estar atentos aos aspectos de segurança envolvidos, pois a instalação de funcionalidade VPN poderá implicar numa revisão das políticas de segurança e numa nova formulação da estrutura lógica e física dos componentes de um *firewall*.

Um conceito envolvido na definição de VPN é o conceito de túnel, que possui relação estreita com o termo “virtual” da VPN. É o tunelamento que permite esconder dos elementos da rede privada, local ou remota, as infra-estruturas do provedor de Internet e da própria Internet [FH98].

O tunelamento cria uma conexão especial entre dois pontos. Para criar-se um túnel, a extremidade iniciadora encapsula os pacotes da rede privada para o trânsito através da Internet. Para as VPNs sobre redes IP esse encapsulamento pode significar cifrar o pacote original, adicionando um novo cabeçalho IP ao pacote. Na extremidade receptora, o *gateway* remove o cabeçalho IP convencional, do pacote usado como meio de transporte na Internet, e, se necessário, decifra o pacote; repassando o original para o seu destino [FH98] [Ko98].

O protocolo de tunelamento mais utilizado é o IPsec, desenvolvido pelo IETF, que possui três componentes:

- AH (Authentication Header): fornece serviço de autenticação ao pacote IP [KA98a].
- ESP (Encapsulating Security Payload): fornece cifragem de pacotes mais a autenticação [KA98b].

- IKE (Internet Key Exchange): negocia parâmetros de conexão para os outros dois, incluindo chaves [HC98].

Este artigo visa a estabelecer uma configuração de um *gateway* VPN dentro de uma estrutura de *firewall*, utilizando-se regras de filtragem claras e simples, de modo a possibilitar que o cliente de acesso remoto seja visualizado como sendo pertencente à rede interna da corporação. São propostas sugestões para a implementação de acesso remoto de forma segura, utilizando software sob licença GNU GPL[1].

Na seção 2 discutem-se questões referentes à colocação de VPN dentro de uma configuração de *firewall*, tendo em mente o cenário do acesso remoto tratado na seção 3. Na seção 4 é apresentada uma solução usando-se software livre, enquanto que na seção 5 são apresentadas as conclusões.

## 2. Colocação do VPN na configuração do *Firewall*.

Em [Ki 99] são analisadas diversas configurações referentes ao posicionamento da VPN dentro do *firewall*. Nesta análise são levados em conta os seguintes posicionamentos: em frente ao *firewall*, atrás do *firewall*, no *firewall*, paralelo ao *firewall* e na interface dedicada do *firewall*. A posição aconselhada no artigo é a colocação da VPN na interface dedicada do *firewall*, dado que numa configuração deste tipo todos os pacotes que chegam ao *gateway* VPN passam antes por um filtro de pacotes ou de estados, o que fornece uma certa proteção contra ataques diretos. Após passarem pelo *gateway*, terem os cabeçalhos de tunelamento retirados e serem decifrados, os pacotes originais podem passar agora por processo de filtragem, o que não podia ser feito ao entrarem no *firewall* por estarem completamente cifrados.

Apesar de [Ki 99] concluir que esta é a melhor configuração para a colocação de um *gateway* VPN dentro de um *firewall*, existem outros detalhes referentes à correta integração do *gateway* de VPN no *firewall*. Questões importantes aparecem quando pensamos na integração da funcionalidade VPN com as regras de *firewall*.

A colocação de uma VPN dentro de uma arquitetura de *firewall* deve levar em conta o possível aumento de complexidade das regras de filtragem, pois muitas vezes é necessário lidar com cenários complexos de acesso de clientes VPN, por exemplo: parceiros de *extranet*, funcionários com acesso remoto e filiais da própria corporação. Esta complexidade crescente pode comprometer a administração segura dos equipamentos, podendo gerar brechas que facilitem um ataque.

Porém, com o uso do *ipchains* [Ru00] [Na00] [NG00] como software de filtragem, é possível construir as regras de modo que todas as filtragens referentes à VPN se localizem numa única cadeia. Ou ainda, caso a complexidade das regras específicas à VPN o justifique, pode-se quebrar tal cadeia em regras menores, sempre na tentativa de facilitar a administração da segurança.

Outra questão a ser levantada refere-se à posição específica do *gateway* VPN: em conjunto com outros equipamentos de uma DMZ[2], numa DMZ separada, numa configuração de múltiplas DMZs [CZ95]. Serão consideradas a seguir cada uma das configurações acima, tendo em mente uma configuração de acesso remoto na qual o cliente apareça como tendo endereço válido na rede interna.

### 2.1. Em conjunto com outros equipamentos de uma DMZ

Para os pacotes que chegam ao *gateway* VPN, têm-se após a retirada do cabeçalho ESP (no modo túnel), endereços de origem de dois tipos: de rede privada, válidos Internet (sejam eles internos ou externos à rede na qual se localiza o *gateway* VPN).

Para os endereços de rede privada, existem circulando num mesmo cabo pacotes com endereços de origem privados e com endereços de origem roteáveis externamente. Conforme as regras de filtragem existentes, isto pode vir a ser um problema. Normalmente, para se evitar o *spoofing* de endereços IP, é aconselhável não

[1] O texto da licença pode ser encontrado em http://www.gnu.org/copyleft/gpl.html.
[2] Rede colocada entre a rede protegida e a externa, proporcionando uma camada adicional de segurança [CZ95]

permitir a entrada numa interface de rede, de pacotes cujos endereços de origem não sejam daqueles que normalmente circulariam naquele segmento de rede. Abrindo uma exceção à alguns endereços pode-se gerar precedente perigoso de ataque à uma rede. Entretanto, se os pacotes não possuem endereços de origem internos (privados ou não), não se pode usufruir de imediato, da vantagem de se ver a outra rede, ou máquina, como integrante lógica da rede interna.

Para os endereços Internet válidos, têm-se pacotes de origem externos à rede, pertencentes à DMZ ou internos (porém não da faixa privada). Em relação aos pacotes com endereços internos, o problema foi discutido no parágrafo anterior. Os demais pacotes não teriam a aparência de serem originários de uma máquina da rede interna[3].

### 2.2. Numa DMZ separada

Na DMZ separada não se tem quaisquer dos problemas anteriormente mencionados, contudo a complexidade de configuração nas regras do filtro escrutinador são maiores: mais uma interface para administração e aplicação de regras. Todavia pode-se controlar de modo mais transparente os acessos aos recursos da VPN. Pode-se aproveitar a existência desta DMZ para inclusão de alguns outros serviços necessários aos usuários de *extranet* ou de redes externas cooperativas [Na00], evitando o acesso desnecessário à rede interna para responder a solicitações de HTTP, FTP e outras, de usuários não totalmente confiáveis. Uma desvantagem seria a duplicação de recursos. Uma solução seria a instalação de *proxies* para esses recursos.

### 2.3. Numa Configuração De Múltiplas DMZs

Nesta situação têm-se um filtro externo e um interno exclusivamente para a VPN. As vantagens são a simplificação de endereçamento, a divisão entre o tráfego Internet comum e o tráfego para redes confiáveis via VPN e a possibilidade de uma filtragem exclusiva (no roteador interno) das solicitações de conexões oriunda da faixa de endereços internos atribuídos à máquinas de *extranet* ou de acesso remoto.

Qualquer alteração na regras desse tipo de acesso não acarretam reflexo nas regras de filtragem mais geral, que estão no outro roteador. É claro que uma configuração deste tipo significa uma duplicação de recursos físicos necessários. Todavia isto pode ser contornado quando colocado o filtro externo e a VPN num único equipamento. Tanto algumas soluções comerciais, quanto não comerciais podem atender este tipo de topologia, porém deve-se atentar para o enfraquecimento da segurança quando se tem um único ponto de falha.

## 3. O Problema do Acesso Remoto

Segundo [KR00], o acesso remoto seguro pode ser definido como sendo o tipo de acesso no qual o usuário remoto não reside necessariamente num local fixo, ou seja, o endereço IP do usuário não é fixo, não sendo previamente conhecido antes do estabelecimento da conexão. A segurança dessa conexão é efetuada com os elementos do protocolo IPsec.

Este tipo de definição aplica-se a um cliente remoto qualquer, que deseja acessar de modo seguro os recursos situados internamente a uma rede corporativa. Os cenários desta situação podem ser muito diferentes: o cliente está situado numa outra rede corporativa, ou conectado a um provedor via acesso discado, via ADSL ou via *modem* a cabo.

Deve-se notar que estão excluídos clientes de *extranet*, pois neste caso os endereços IP são bem conhecidos. O caso do acesso remoto aplica-se ao caso de usuários de rede corporativa que estejam momentaneamente fora de seu local e queiram utilizar-se dos recursos desta mesma rede como se estivessem no seu local normal de trabalho.

---

[3] Uma solução é utilizar-se, no roteamento entre a DMZ e a rede interna, de um serviço de NAT reverso. Deste modo pode-se ter pacotes tunelados com endereços de origem externos, sendo que o NAT reverso se encarregaria de transformá-los em endereços válidos dentro da rede interna. A rede interna veria estes pacotes como oriundos dela.

Para se ter um acesso remoto seguro deve-se levar em conta o problema da autenticação. O protocolo IPsec é capaz de garantir a autenticidade com relação à origem dos dados, via AH ou ESP. Já a questão da autenticidade da terminação (ou máquina) pode ser resolvida através do IKE. Neste caso também é de importância crucial a autenticação do usuário final da máquina, sem o que a rede corporativa pode ser atacada por *trojans* ou por usuários mal intencionados que tenham acesso a sistemas já autenticados. Esta proteção pode ser realizada através da exigência de algum segredo (senha, *token*, *one-time passphrase*) possuído pelo usuário final.

A configuração de rede do sistema remoto pode ser fixa ou dinâmica. Neste trabalho foi abordada a configuração dinâmica, cujo interesse reside na possibilidade da rede corporativa visualizar a máquina de acesso remoto como sendo pertencente à rede lógica da corporação, conforme mostra a figura 1.

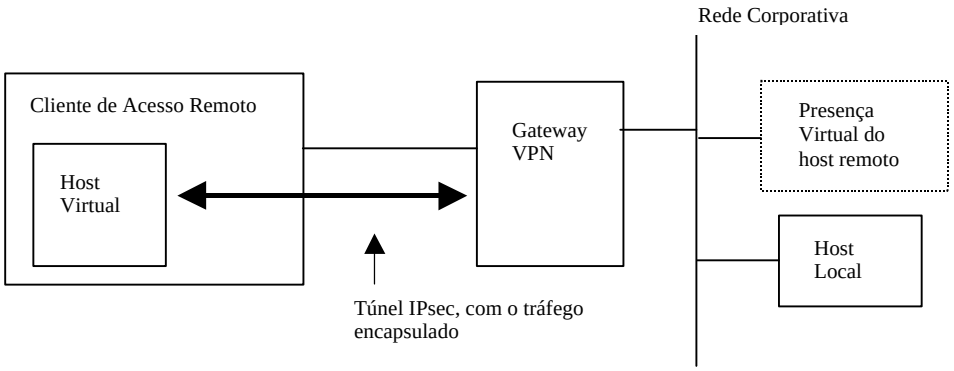


Figura 1: Cenário de Acesso Remoto

Neste caso a máquina de acesso remoto aparece com um endereço externo roteável. Este endereço deve ser fornecido ou pelo provedor, ou pelo administrador da rede na qual a máquina está temporariamente inserida. Este também deve fornecer informações referentes à rota padrão a ser seguida pelos pacotes que deixam a máquina de acesso remoto. Pode-se notar que a máquina agora possui dois endereços ativos: um referente a rede física na qual ela está colocada, e o outro virtual, associado à rede corporativa na qual ela deveria residir. Associados ao endereço virtual, a máquina deverá estar configurada de acordo com os parâmetros de rotas, servidores DNS etc, da rede corporativa. Assim, após a conexão na rede corporativa, a máquina passa a se comportar como se estivesse fisicamente localizada na parte interna da rede [KR00].

É importante ressaltar que as políticas de segurança da rede corporativa devem ser também aplicadas ao acesso remoto, tarefa de difícil execução, dado que muitas das vezes, esta máquina pode não estar sob responsabilidade direta do administrador da rede corporativa cooperante. Como por exemplo no caso de máquinas de acesso remoto utilizados por parceiros de *extranet*. Em contrapartida, no caso de funcionários da própria empresa utilizando acesso remoto, esta tarefa pode ser mais fácil.

Certos detalhes de segurança necessitam ser levados em conta quando existe uma conexão deste tipo. A máquina que executa o acesso remoto muitas vezes possui conexão direta com a Internet; e, como conseqüência, a Internet possui a acesso à ela. Com isto, é possível que a máquina seja utilizada para um ataque à rede corporativa. Deste modo deve-se fazer com que, uma vez estabelecido o túnel, todo o acesso a qualquer parte da Internet deva passar pelo túnel, para que as políticas internas de segurança quanto ao acesso ao mundo exterior possam ser aplicadas. Ao mesmo tempo, todo e qualquer tráfego que chega à máquina, que não aquele advindo do túnel deve ser bloqueado. Desta forma, pode ser estabelecida uma configuração segura de acesso. Isto é possível com o que se convencionou chamar *personal firewalls*, isto é, *firewalls* para máquinas individuais, como os que vêm nativamente em Windows 2000, Linux e FreeBsd.

**4. Implementação**

O FreeS/WAN[4] foi escolhido para implementar a VPN e o acesso remoto, devido à robustez da implementação, à sua interoperabilidade com um conjunto importante de outras implementações IPsec, e a facilidade de integração com o *ipchains*.

O FreeS/WAN é uma implementação para Linux dos protocolos IPsec, construído sob GNU GPL, que pretende ser interoperável com outras implementações IPsec. Esta implementação fornece o AH, o ESP e o IKE.

Nesta implementação existem três partes principais:

- KLIPS (kernel IPsec): implementa AH, ESP e tratamento dos pacotes dentro do kernel.
- Pluto (um *daemon* IKE): implementa o IKE, negociando conexões com outros sistemas.
- Vários *scripts*, fornecendo uma interface do administrador com a máquina.

Dentre as implementações que apresentam compatibilidade de operação com o FreeS/WAN, destaca-se: Open BSD IPSEC, Windows 2000 IPSEC, NAI PGPnet, Raptor Firewall, Gauntlet firewall GVPN, Checkpoint Firewall-1 e roteadores Cisco.

Foi escolhido colocar o *gateway* VPN em uma DMZ separada, satisfazendo tanto uma configuração do *gateway* para o tipo de acesso remoto desejável, quanto para o estabelecimento de túneis com outras redes corporativas. O FreeS/WAN permite a criação de múltiplos túneis a partir de um mesmo *gateway*. Deste modo obtêm-se uma configuração de regras de filtragem mais clara e administrável.

Podem ser criados *scripts* que permitem, no momento da ativação do túnel, fazer com que as regras de filtragem da máquina cliente de acesso remoto sejam modificadas, permitindo somente a entrada de pacotes oriundos do *gateway* VPN com o qual o cliente deseja se comunicar, impedindo assim a tentativa, por parte de um usuário externo malicioso, de se utilizar do cliente VPN como "ponte" conforme descrito em [NG00]. Após o encerramento da sessão, o túnel é desativado, as regras de filtragem referentes ao tunelamento são apagadas e as regras anteriores são novamente colocadas.

No caso do acesso remoto ser realizado através de linha discada, não se sabe que endereço IP será atribuído à máquina em questão. Isto gera um problema para a configuração do *gateway* VPN, já que este endereço é necessário para o estabelecimento do túnel. A solução recomendada por [Fr00] estabelece que o *gateway* VPN considere como a outra ponta do túnel qualquer endereço Internet. Este tipo de solução traz problemas de segurança, pois teria que ser liberado no filtro a passagem de pacotes oriundos de qualquer destino endereçados ao *gateway* VPN.

Uma solução foi proposta por [DB99], envolvendo a modificação dos arquivos de configuração do *gateway* no momento da conexão. Esta solução é trabalhosa e complexa demais para o caso do acesso remoto de uma única máquina, tendo sido proposta para uma filial da rede principal que se comunica via acesso discado e similares.

Uma solução intermediária é o conhecimento prévio do conjunto de endereços fornecidos pelo ISP, que será utilizado pelo acesso remoto, ao seus clientes, para poder configurar o *gateway* permitindo somente tentativas de conexão a partir de uma determinada faixa de endereços, diminuindo a fragilidade do sistema.

Para a simulação de uma presença virtual do cliente (conforme figura1) de acesso remoto na rede, foi escolhido estabelecer uma interface virtual [Pi97], com o propósito de fazer com este *host* possua um endereço da rede interna na qual ele deve estar localizado. É claro que ativação dessa configuração se dará no momento de ativação do túnel.

O funcionamento desta configuração depende da configuração correta do *gateway* VPN, que aceitar para si os pacotes destinados a um endereço que não se encontra fisicamente, mas sim logicamente, neste

[4] O endereço do projeto FreeS/WAN é http://www.freeswan.org. Neste *site* podemos obter os códigos fonte e suas instruções para compilação, documentação referente ao *software*, referências bibliográficas e endereços de listas de discussão.

segmento de rede. Isto pode ser feito através de um *proxy* ARP, de modo a que o *gateway* possa responder a solicitações ARP para o endereço em questão, mesmo não sendo este seu endereço original.

Na atual fase do presente projeto o *gateway* VPN foi configurado e colocado dentro de uma DMZ própria, e as regras de filtragem foram definidas. Os *scripts* referentes à máquina cliente estão sendo elaborados.

## 5. Conclusão

Neste artigo procurou-se discutir algumas questões referentes ao posicionamento de uma VPN dentro de uma configuração de *firewall*. Pode-se notar que existem múltiplas variáveis a serem consideradas, sendo que uma solução foi proposta para o caso de um cliente de acesso remoto com endereço pertencente a rede situada atrás do *firewall*. Esta solução também pode ser aplicada para o caso de conexões *extranet* ou com filiais da mesma empresa.

Foi proposta uma implementação de acesso remoto utilizando como *software* para o tunelamento IPsec o FreeS/WAN. Esta implementação possui vantagens quando comparada a outras propostas, no que se refere a maior simplicidade de implementação, a possibilidade de aplicação das regras de segurança à máquina de acesso remoto e a uma maior transparência na aplicação das regras de *firewall* para as conexões VPN.

## 6. Bibliografia


[CZ95] Chapman, D.B.; Zwicky, E.D, *Building Internet Firewalls*, O'Reilly & Associates, 1995.

[DB99] Denker, J. S.; Bellovin, S. M., Daniel, H.; Mintz, N. L.; Killian, T.; Plotnick, M. A., *Moat: a Virtual Private Network Appliance and Services Plataform*, Proceedings of LISA '99, Seatle, WA, USA, Novembro 1999

[FH98] Ferguson, P.; Huston, G., *What is a VPN?*, http://www.employees.org/ ferguson/vpn.pdf

[Fr00] *Linux FreeS/WAN 1.8 HTML Documentation tree*, http://www.freeswan.org/freeswan_trees/freeswan-1.8/doc/index.html.

[HC98] Harkins, D.; Carrel, D., *The Internet Key Exchange*, RFC 2409, Novembro 1998, ftp://ftp.isi.edu/in-notes/rfc2409.txt

[KA98a] Kent,S.; Atkinson, R., *IP Authentication Header*, RFC 2402, IETF, Novembro 1998, ftp://ftp.isi.edu/in-notes/rfc2402.txt

[KA98b] Kent,S.; Atkinson, R., *IP Encapsulating Security Payload (ESP)*, RFC 2406, IETF, Novembro 1998, ftp://ftp.isi.edu/in-notes/rfc2406.txt

[Ki99] King, Christopher M. Information Security. *The 8 Hurdles to VPN Deployme*nt. March, 1999. http://www.infosecuritymag.com/mar99/cover.htm.

[Ko 98] Kosiur, D., *Building and Managing Virtual Private Networks*, John Wiley & Sons, Inc, 1998

[KR00] Kelly, S.; Ramamoorthi, S., *Requirements for IPsec Remote Access Scenarios*, draft-ietf-ipsra-reqmts-02, IPsec Remote Access Working Group, http://search.ietf.org/internet-drafts/draft-ietf-ipsra-reqmts-02.txt, Novembro 2000,

[Na00] Nakamura, E. T., *Um Modelo de Segurança de Redes para Ambientes Cooperativos*, Tese de Mestrado, IC – UNICAMP, Campinas, Setembro 2000

[NG00] Nakamura, E. T.; Geus, P. L., *Análise de Segurança do Acesso Remoto VPN*, Anais do SSI'2000, II Simpósio sobre Segurança em Informática, S. José dos Campos, SP, 24-26/10/2000, pp29-37.

[Pi97] Pillay, H., *Mini How-to on Setting Up IP Aliasing On A Linux Machine*, http://home1.pacific.net.sg/~harish/linuxipalias.html

[Ru 00] Russel, R. *Linux IP Firewalling Chains*, http://netfilter.filewatcher.org/ipchains/